UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

FACULTAD DE INGENIERÍA

MANUAL DE PRÁCTICAS DEL LABORATORIO DE REDES DE DATOS SEGURAS

T E S I S

PARA OBTENER EL TÍTULO DE:

INGENIERA EN COMPUTACIÓN

P R E S E N T A :

MARÍA EUGENIA BAUTISTA GONZÁLEZ

DIRECTORA DE TESIS:

ING. MAGDALENA REYES GRANADOS

MEXICO, D.F. **ENERO 2016**

Agradecimientos

Primero quiero agradecer a Dios por permitirme culminar esta meta, por darme la oportunidad de conocer a la gente que ha estado conmigo en las buenas y en las malas, por darme la fuerza para seguir adelante cada día.

Agradecer a mis papas, a mis hermanos, a mi hijo por su paciencia, apoyo incondicional y sobre todo por creer en mí.

A cada uno de mis amigos por compartir este camino juntos, algunos se subieron y otros se bajaron de este viaje. A mis profesores por sus enseñanzas, paciencia e interés de compartir sus conocimientos.

A Magda, mi amiga, profesora y asesora de este proyecto de tesis, donde aprendimos, crecimos y nos tropezamos juntas, sin su apoyo no se habría logrado esta meta.

A Aldo por enseñarme con paciencia y cariño, agradezco a Dios el que te pusiera en mi camino.

A las maestras Jaquelina y Cintia por confiar en mí, por darme la oportunidad de crecer personal y profesionalmente, por darme su amistad, su cariño y sobre todo su confianza.

ÍNDICE

INTRODUCCIÓN

Introducción

En la actualidad las redes de datos han evolucionado a pasos agigantados debido a la necesidad de compartir recursos, información y ofrecer servicios de manera rápida y eficaz, generando nuevas modalidades de interacción y comunicación. Dado su crecimiento constante y vertiginoso también le permite ser vulnerable a posibles amenazas como lo son; la interrupción, que atenta contra la disponibilidad; la intercepción, que atenta contra la confidencialidad y la modificación, que atenta contra la integridad.

El uso continuo de la red, genera la necesidad de que exista comunicación en distintas partes del mundo, lo cual se logra gracias a las instituciones encargadas de crear estándares, normas y manuales de buenas prácticas como son; ANSI, OSI, EIA, TIA, ITU, incluyendo las instituciones normalizadoras de cada país. Estos estándares han permitido que los desarrolladores los usen como base en la creación de protocolos, los cuales se encuentran integrados en el Modelo OSI el cual está compuesto por siete capas. Cada capa del Modelo OSI, tiene una función específica que va desde la conexión de equipos de cómputo hacia los dispositivos de interconexión.

Los administradores de redes son los encargados de monitorear, crear, aplicar, implementar y diseñar métodos y políticas de seguridad, garantizando en la medida de lo posible, que la información o cualquier activo no sufra algún tipo de ataque o alteración.

Dado el panorama actual, durante la revisión de planes de estudio en la Facultad de Ingeniería de la Universidad Nacional Autónoma de México, se acordó que en la carrera de Ingeniería en Computación la asignatura de Redes de Datos sería sustituida por la asignatura de Redes de Datos Seguras, con el objetivo de

proporcionar a los estudiantes conocimientos sólidos en el ámbito de las redes, así como de la seguridad de la información.

Por lo cual se tomaron en cuenta los temas de teoría en la realización de las prácticas, quedando como se enuncian a continuación:

En el tema 1, *Conceptos básicos,* el objetivo es conocer e identificar los elementos que conforman a una red de datos y los principios básicos de seguridad. La práctica 1 seguridad en la red, tiene como objetivo dar a conocer a los alumnos la importancia de la protección de los dispositivos móviles así como la información.

En el tema 2, *Estándares y arquitectura,* el objetivo es dar a conocer y explicar los protocolos y estándares que se manejan en las redes de datos. Se diseño la práctica 2 normatividad, donde se utilizarán las normas más importantes en el cableado estructurado, construcción de edificios comerciales y armado de cables.

En el tema 3, *Capa física,* el objetivo es dar a conocer y explicar los protocolos y estándares que se manejan en las redes de datos. Primer capa del Modelo OSI, encargada de realizar la conexión entre los medios físicos y lógicos, tomando en cuenta esto se desarrollaron dos prácticas. La práctica 3 construcción de cables UTP y jacks , tiene como objetivo enseñar a los alumnos la construcción de cables UTP directo y cruzado, así como la instalación del jack para el uso de rosetas. La práctica 4 topología de red y cableado estructurado, el objetivo principal es dar a conocer a los alumnos las normas y estándares internacionales para la correcta instalación de una red física.

En el tema 4, *Capa de enlace de datos,* el objetivo es analizar, comprender y utilizar los diferentes protocolos, métodos y estándares que se utilizan en esta capa en los dispositivos de interconexión. En la práctica 5 compartición de archivos por Hub y Switch en Linux, el objetivo es dar a conocer la metodología

para compartir archivos por medio de los dispositivos de interconexión así como el análisis de la simulación de una colisión. En la práctica 6 creación y configuración de una VLAN, tiene como objetivo dar a conocer los comandos básicos para la utilización de las redes VLAN.

En el tema 5, *Capa de red,* el objetivo es analizar y comprender el funcionamiento del intercambio de información por medio de la red. En este tema se decidió dedicar tres prácticas. La práctica 7 red inalámbrica “ad hoc” y compartición de archivos en Windows, se explicará la diferencia de compartir archivos por medio de una red inalámbrica y alámbrica. En la práctica 8 enrutamiento (estático y dinámico), la práctica 9 tipos de enrutamiento (OSPF y EIGRP), el objetivo es dar a conocer los comandos básicos para realizar enrutamiento estático y dinámicos en la misma red de datos.

En los tema 6,7 y 8, *Capas de transporte, sesión y presentación,* los objetivos son analizar y comprender los diferentes tipos de protocolos en cada una de las capas y en la unión con el resto de las capas del modelo OSI. Se tomó la decisión por la naturaleza de las capas utilizarlas dentro del manual de prácticas del Redes de Datos Seguras.

En el tema 9, *Capa de aplicación,* el objetivo es analizar, comprendé y utilizar los diferentes protocolos, métodos y estándares que se utilizan en esta capa en los dispositivos de interconexión, se utilizarán tres prácticas. Práctica 10 instalación de un servidor Apache, el objetivo es dar a conocer los comandos necesarios en el levantamiento de un servidor en un sistema operativo Linux. Práctica 11 TCP y UDP, su objetivo es explicar el funcionamiento de una arquitectura cliente-servidor. La práctica 13 configuración de VPN y DMZ en Packet Tracer, el objetivo es dar a conocer el funcionamiento de las zonas desmilitarizadas y la red privada virtual así como su configuración básica.

Debido a lo amplio e importante de la última capa del modelo OSI, se tomó la decisión de intercalar una práctica exclusiva sobre seguridad, para demostrar la importancia que tiene este rubro en los administradores de las Redes de Datos. Práctica 12 ruptura de claves WPA Y WEP.

Capítulo 1.

Conceptos básicos de redes y seguridad

Introducción

Las redes de datos se han convertido en el medio de comunicación más importante a nivel mundial donde se puede obtener información de casi cualquier tipo e inclusive idioma. El intercambio de información y el manejo de base de datos son primordiales para toda institución educativa, gubernamental, empresarial, entre otras.

Las organizaciones normalizadoras son las encargadas de facilitar el intercambio de datos, permitiendo que exista comunicación a nivel mundial, algunas de estas organizaciones son; ISO, ANSI, EIA, TIA e instituciones normalizadoras de cada país.

El Modelo OSI es un estándar encargado de dividir por capas cada una de las etapas por las que debe viajar un paquete, desde el origen hasta su destino, garantizando que la misma cantidad de bits enviados, sean los que se reciban, en el mismo orden y sin alteraciones.

Con los avances tecnológicos, los administradores de redes han descubierto vulnerabilidades y amenazas del hardware y software utilizado para el manejo de información, por lo que este capítulo tiene la finalidad de dar a conocer los conceptos básicos sobre las redes de datos y seguridad.

1.2 Definición de redes de datos.

Una red es un conjunto de dispositivos interconectados entre sí, para poder compartir servicios e información. La red está constituida por hardware que hace referencia a los equipos de cómputo, dispositivos de interconexión (switch, routers, hub, repetidores, bridges, gateway), protocolos, servidores, tarjetas de red, entre otras. Al punto final de una red se le denomina host. En el uso de la redes de datos, se utilizan distintos protocolos, los cuales son interpretados por los distintos dispositivos.

Las redes de datos se clasifican por su topología y aplicación, como se describe a continuación.

1.3 Topología de redes.

Una topología de red se define como la forma física o lógica de comunicar estaciones de trabajo individuales, por muros, techos y suelos, a través del tendido de cable o conexiones lógicas. La cual dependerá del uso, número de nodos, dispositivos interconectados, costo e instalaciones.

El objetivo de una topología es facilitar la comunicación entre equipos, por medio de protocolos de encaminamiento adecuados, reducción de costos y detección oportuna de fallos.

Están conformadas por tres elementos:

- ***Nodo:*** Es un punto de intersección donde se unen dos o más elementos de red.
- ***Enlace:*** Vínculo que existe entre dos nodos, para que exista una comunicación.

- ***Protocolo:*** Conjunto de reglas o métodos para que dos procesos intercambien información.

La conexión que existe entre nodos es por medio de enlaces, los cuales a su vez se subdividen en dos y son:

- ***Enlace punto a punto:*** Es la conexión entre dos equipos en un instante mientras no haya alguna interferencia.
- ***Enlace multimodo*****:** Es la conexión de un punto hacia varios equipos o dispositivos que se interconectan para que exista un flujo de información.

Existen dos tipos de topologías: forma física y lógica (protocolos de comunicación entre equipos de trabajo), de esta última existen dos más comunes que son broadcast y transmisión de tokens. La topología física es una red de cables conectados entre sí que permite exista una interconexión entre dispositivos finales.

La topología broadcast (ethernet), cada host envía sus datos por medio de la red a los hosts conectados. La topología de transmisión de tokens (tokens ring), controla la red mediante la transmisión de un Token a cada host de forma secuencial.

Las topologías adquieren su nombre por la forma de comunicación utilizada, así como se ilustra en la figura 1.1.

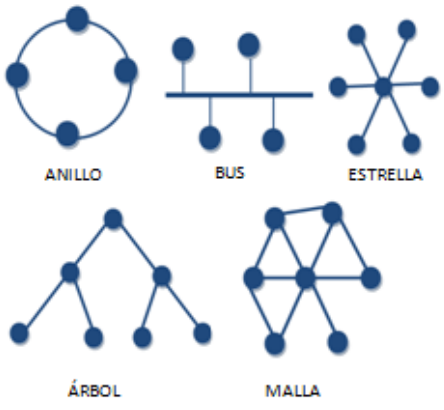


Figura 1.1 Topología de red.

1.3.1 Bus.

La topología de bus se caracteriza por tener a todos los nodos conectados a un mismo cable, lo que es poco conveniente, ya que el flujo de información corre en una sola dirección, es decir, solo un nodo puede transmitir a la vez y si otros nodos envían información se vuelve un conflicto, ocasionando colisiones y la caída del servicio.

En caso de colisiones, los nodos esperan una cantidad mínima de tiempo al azar y vuelven a intentar retransmitir la información.

1.3.2 Anillo.

La topología de anillo toma su nombre por la forma que adquieren los dispositivos interconectados, donde el primer dispositivo se conectará con el último para cerrar la red. Cada estación tiene un transmisor y receptor, lo cual le permite pasar la información al siguiente nodo.

En caso de que algún equipo de la topología falle, la red puede cambiar el sentido de envío de información, la calidad de envío de datos no decae con la carga de usuarios. Una desventaja es que cuando se envía un mensaje a alguna estación, éste puede ser visto por las estaciones intermedias mientras llega a su destino.

1.3.3 Estrella.

La topología de estrella está basada en un nodo central (switch o router), el cual se encarga de recibir y enviar la información a cada destinatario, los dispositivos pertenecientes a esta red no se encuentran conectados entre sí.

Se utiliza está topología en redes locales, por la ventaja que tiene para administrar los fallos y garantizar el servicio de envío/recepción de datos, sus desventajas son: en caso de que el nodo central se dañe, toda la red se caerá, además de que este tipo de topología ocupa una gran cantidad de cable para su construcción.

1.3.4 Árbol.

Esta topología es llamada así porque forma un árbol al ser conectada, en vez de manejar un nodo central, maneja un nodo troncal que es ocupado por un switch o router. La desventaja principal es la cantidad de cable que ocupa para realizar su conexión.

La topología de árbol puede verse como la variación de las topologías de estrella y bus, aunque maneja repetidores para enviar y recibir datos.

1.3.5 Malla.

La topología de malla se caracteriza porque todos los nodos están conectados entre sí, lo que garantiza que la comunicación se mantenga constante, en caso de que algún nodo llegue a fallar no afectará la red, esto se debe a la forma de conexión.

Esta topología es usada en áreas donde es importante mantener la red funcionando, por ejemplo bancos, empresas dedicadas al manejo de valores, empresas transnacionales, instituciones gubernamentales, instituciones educativas, entre otras.

1.4 Modelo OSI.

El Modelo OSI (Open System Interconnection), es un modelo creado en 1984 por la ISO (International Organization Standardization) con el fin de normalizar la comunicación de redes de datos.

El modelo está compuesto por siete capas (como se ilustra en la figura 1.2), donde se utilizan uno o más protocolos que permiten realizar la interconexión de dispositivos. Cada capa del Modelo OSI tiene sus funciones específicas, su

identificador único e irremplazable, lo que facilita la introducción de nuevos protocolos y el empleo en diferentes arquitecturas.

Figura 1.2 Modelo OSI

1.4.1 *Capa 1:* física.

La capa física es la encargada de realizar la conexión de los medios físicos y eléctricos como son:

- ***Medios guiados;*** el cable UTP (par trenzado no blindado), STP (par trenzado blindado), cable coaxial o fibra óptica.
- Interconexión con dispositivos como son router, switch y equipos de computo.
- Envío de señales eléctricas de 0 y 1, garantizando que el bit que se envíe sea el mismo que se reciba.

1.4.1.1 Cableado Estructurado.

El cableado estructurado es una guía de buenas prácticas para la correcta implementación de una topología de red, flexible y con un tiempo de vida útil de diez a quince años, capaz de soportar cambios y crecimientos futuros. La

implementación de este sistema reduce costos en la instalación y el mantenimiento así como la facilidad de incorporación de nuevos sistemas.

Está regido por las normas ANSI/TIA/EIA 568 A, ANSI/TIA/EIA 568 B y estándares nacionales (NOM) e internacionales (ISO y NEC) que facilitan su administración, monitoreo y resolución de conflictos en las comunicaciones. Su objetivo es maximizar la eficiencia y seguridad en una red, independientemente de la transmisión de datos que circule por ésta.

Los componentes físicos son:

- ***Cables:*** Cable UTP, STP y fibra óptica.
- ***Dispositivos:*** Rack, patch panel, router y switch.
- ***Conectores:*** Canaletas y RJ-45 (macho y hembra).

El cableado estructurado se divide en 6 subsistemas que son:

- Entrada al edificio.
- Backbone.
- Armario de telecomunicaciones.
- Cableado horizontal.
- Área de trabajo.
- Cuarto de equipos.

a) Entrada al edificio.

La entrada al edificio es el punto donde los servicios de telecomunicaciones tienen acceso al interior para realizar la conexión con el cuarto de entrada de servicios. En esta área se encuentran los dispositivos para regular el voltaje, el tendido de cable de los servicios de voz y datos.

Las tuberías, conectores y uniones, deben mantenerse protegidas de las inclemencias del tiempo así como los roedores y no estar expuestos a cualquier usuario ya que pueden dañar y destruir los servicios.

Este subsistema maneja la entrada y salida de servicios con conexiones a la red (internet), pueden ser terrestres (las más comunes) por medio de tuberías o aéreas por medio de antenas ubicadas en las partes altas de los edificios.

b) Backbone.

El backbone o cableado vertical es la columna principal que sirve de comunicación y distribución de servicios dentro de la infraestructura de red, con gran ancho de banda, es la parte del cableado que realiza la conexión entre el cuarto de entrada de servicios, los cuartos de equipo y los cuartos de telecomunicaciones.

La distancia máxima para el uso de cableado principal UTP categoría 6 o 6e (STP-A) 150 ohms, es de 90m, para fibra óptica multimodo es de 62.5 µm, la distancia máxima es de 2000m y para fibra óptica monomodo es de 3000m.

Cables aceptados:

Los medios reconocidos que pueden ser usados individualmente o en combinación son:

- Cable de par trenzado sin blindaje (UTP), 100 ohms, 24 AWG.
- Cable de par trenzado con blindaje (STP-A), 150 ohms, 22 AWG.
- Fibra óptica multimodo de dos fibras 62.5/125 µm.
- Cable de fibra óptica monomodo.

Backbone de fibra óptica

Existen tres razones por las que el uso de la fibra óptica es más efectiva para el cableado estructurado y son:

- No permiten el paso del ruido así como las interferencias de radiofrecuencias
- No son conductoras de corrientes.
- Cuentan con un ancho de banda elevado, facilita que funcionen a altas velocidades.

La fibra óptica multimodo puede cubrir longitudes de hasta 2,000m.

La fibra óptica monomodo puede cubrir longitudes de hasta 3,000m.

c) Armario de telecomunicaciones.

Es el área del edificio utilizada como punto de conexión entre el backbone y el cableado horizontal, alberga equipo de telecomunicaciones, terminaciones de cable y el cableado de interconexión asociado. Aquí se realiza la conexión cruzada de las terminaciones del cableado horizontal y backbone mediante paneles de parcheo, permitiendo una conectividad flexible de servicios. Se recomienda que exista al menos un cuarto de telecomunicaciones por piso.

Las especificaciones para el armario de telecomunicaciones son las siguientes:

- Los racks de telecomunicaciones cuentan con más de 82cm libres alrededor como espacio de trabajo.
- Deben existir al menos tres tomacorrientes de 110 V C.A., para alimentar los equipos electrónicos del cuarto de telecomunicaciones.
- La temperatura del cuarto se mantiene continuamente entre 18 °C y 24 °C con una humedad relativa entre 30% y 55%.
- Se deben proteger las paredes, pisos y techo para reducir el polvo y la electricidad estática.
- No se permite el uso de piso o techo falso.

- No debe establecerse cerca de escaleras, elevadores, baños o lugares de fácil acceso.

d) Cableado horizontal.

Es la porción de cableado que conecta las salidas del área de trabajo con el armario de telecomunicaciones. El objetivo es satisfacer los requerimientos de telecomunicaciones, así como tomar en cuenta las necesidades presentes y futuras de los usuarios antes de realizar la implementación.

La topología recomendada para este tipo de subsistema es la de estrella, ya que por su forma es más apta para soportar aplicaciones de voz y datos. La distancia máxima desde el área de trabajo hasta el cuarto de telecomunicaciones es de 90m y se consideran 10m adicionales para realizar la conexión horizontal con el área de trabajo, puentes, cuerdas auxiliares y cuerdas de equipo en el armario de telecomunicaciones, entre otras.

Al ser una continuación del cableado vertical utiliza los mismos cables aceptados, además de manejar una canaleta principal, por donde correrá el cableado horizontal, distribuido por pared o techo.

e) Área de trabajo.

El área de trabajo es la zona donde se encuentran ubicados los distintos puestos de trabajo que comprenden las terminales de datos, videoconferencias y teléfonos, así como adaptadores, filtros o acopladores en caso de ser requeridos.

El cableado se extiende a partir de la roseta de conexión a la terminal, puede llegar a cambiar dependiendo de las necesidades del usuario. La longitud máxima para el cable auxiliar en el área de trabajo es de 3m.

Comúnmente se usan cables de conexión con conectores iguales en ambos extremos, pero es posible utilizar adaptaciones específicas externas a la salida de telecomunicaciones, por ejemplo, conectores coaxiales, fibra óptica, BNC, entre otros.

f) Cuarto de equipos.

Es el espacio centralizado donde residen los equipos de telecomunicaciones del edificio, así como cables y conectores que permiten enlazarlos con otros dispositivos para compartir servicios. La naturaleza, costo y complejidad del equipo que contiene un cuarto de equipo lo diferencia de los cuartos de telecomunicaciones. Las funciones que desempeña el cuarto de telecomunicaciones pueden ser realizadas por el cuarto de equipos.

En ocasiones el cuarto de equipos y la entrada de servicios son unidos para compartir: aire acondicionado, seguridad, control de fuego, iluminación y acceso limitado. Adicionalmente incluye un área para el personal de telecomunicaciones manteniéndola alejada de las fuentes de interferencia electromagnética.

Las recomendaciones para el cuarto de equipos son las siguientes:

- Se recomienda un tamaño de $0.07m^2$ de uso de espacio entre las guías para voz y datos por cada $10m^2$ de área utilizable.
- La temperatura se mantiene entre 18°C y 24°C y las paredes se pintan de blanco o colores claros para mejorar la visibilidad.
- Las paredes no deben de estar en común con las áreas de fácil acceso como son las escaleras, los elevadores, los baños y cocinetas (en caso de existir).
- Se recomiendan las siguientes dimensiones del cuarto de equipo, en relación al número de estaciones de trabajo (véase la Tabla 1.1):

Número de Estaciones de Trabajo	Tamaño del Cuarto de Equipo (m^2)
1 – 100	10
101 – 400	20
401 – 800	40
801 – 1200	70

Tabla 1.1 Estaciones de trabajo por cada m^2.

1.4.2 Capa 2: enlace de datos.

La capa de enlace de datos es la encargada de realizar envío de mensajes (tramas) a dos equipos conectados directamente a través de un cable.

Las funciones que debe realizar son las siguientes:

- Crear e identificar las tramas.
- Detección y manejo de errores.
- Control de flujos de datos.
- Adecuación de protocolos.

1.4.2.1 Protocolos de la capa de enlace de datos.

Los protocolos son un conjunto de reglas y procedimientos que se deben llevar a cabo para enviar y recibir datos a través de una red. Existen diversos protocolos para que trabajen en la red, por ejemplo; HTTP, TCP/IP, FTP, IPv6, IPv4, ICMP, etcétera.

Los protocolos más importantes de esta capa se describen a continuación.

a) SDLC

SDLC (Synchronous Data Link Control) es un protocolo muy antiguo de IBM utilizado en la arquitectura de red SNA(System Networks Architecture), emplea los métodos síncronos, orientados a bit y Vuelta-atrás-N. Funciona con línea

dúplex, semi-duplex, conmutadas o privadas y se encuentra administrado por una estación maestra. IBM realizó una mejora al protocolo SDLC y este es HDLC, el cual fue normalizado por la ISO y la UIT-T.

La estación maestra inicia la transmisión hacia las estaciones secundarias y espera la respuesta de estas. Una estación maestra puede ser una estación secundaria para otra estación maestra.

El envío de mensajes SDLC es a través de una trama (véase la figura 1.3). Un indicador final sirve como referencia para el siguiente indicador, así como el elemento SYN.

INDICADORES. Formados por octetos	DIRECCIÓN	CONTROL	DATOS DE USUARIO	SVT	INDICADORES. Formados por octetos

Figura 1.3 Trama de envío de mensajes SDLC

La trama al encontrar más de cinco unos juntos inserta un cero al quinto uno y al recibir el paquete el protocolo revisa la trama y al encontrar más de cinco unos juntos, en el quinto uno extrae el cero y recibe la trama íntegra.

La dirección identifica la estación secundaria. El área de control se define el funcionamiento de la trama, invocando la lógica del protocolo SDLC en las estaciones transmisoras y receptoras. Puede encontrarse en alguno de los siguientes formatos:

- ***Trama con formato sin numeración:*** Empleadas para el control de inicialización de estaciones secundarias.
- ***Trama con formato de supervisión:*** Empleadas para la lógica de respuesta de afirmación o negación.

- ***Trama de Transferencia de Información:*** Contiene los datos de los usuarios.

SVT es la secuencia de la verificación de la trama, la cual contiene 16 bits.

b) PPP

El protocolo PPP (Point to Point Protocol), es un conjunto de protocolos que permiten la interacción de software por medio de acceso remoto, así como la conexión a internet de un punto en especifico a través de un módem.
Los componentes que integran al protocolo PPP son:

- ***Un método para encapsular datagramas:*** Método que permita la fragmentación de paquetes y así facilitar el encapsulamiento del mismo.
- ***Un protocolo de control de enlace:*** Permite establecer una comunicación y detección de problemas en dos partes de un formato de encapsulamiento.
- ***Una familia de protocolos de control de nivel de red:*** Para establecer comunicación con diferentes protocolos.

1.4.2.1.3 Análisis de tráfico y colisiones.

Para realizar un análisis de tráfico y colisiones es necesario tener en cuenta los siguientes conceptos:

- ***Tasa de transferencia:*** Es el número de bits, que se transmite en una unidad de tiempo (bits/segundo) bps.
- ***Troughput*****:** Se le denomina así a la cantidad de información que fluye a través de una red.
- ***Pérdida de paquetes:*** Es la medición probable de pérdida de información en el envío y recepción de paquetes.
- ***Retrasos:*** Indica la pérdida de tiempo, ya sea por colisiones, pérdida de trama u otros factores.

Existen diferentes software que tienen la función de realizar análisis de tráfico, es decir, observar que pasa por una red determinada. Algunos son; Wireshark, nmap, netflow, entre otros.

Al realizar el análisis de la red, se pueden encontrar algunas de las causas que impiden el funcionamiento estable del envío/recepción de datos.

1.4.3 Capa 3: de red.

La capa de red es la encargada de encaminar los paquetes, entregarlos aunque el origen y el destino no tengan una conexión directa, se determina la ruta más viable a seguir. Los routers son los encargados de convertir las direcciones lógicas (direcciones IP) a direcciones físicas (direcciones de la NIC), así como manejar los diferentes tipos de encaminamientos entre redes, por lo que se vuelven un dispositivo fundamental en la comunicación en una red.

La comunicación con distintas tecnologías no debe de afectar, ya que la capa de red utiliza distintos protocolos para garantizar dicha comunicación.

Maneja dos tipos de servicios que son:

- ***No orientados a la conexión:*** La ruta no está definida, pero el router determina el camino o ruta por el cual debe de enviar los paquetes.
- ***Orientados a la conexión:*** Primero se establece el enlace lógico de comunicación y después se envían los paquetes por dicho camino.

1.4.3.1 Protocolos de la capa de red.

Los protocolos de la capa red, le permiten tener el acceso hacia diferentes puntos gracias a su uso y conexión a internet. Algunos de estos protocolos se describen a continuación.

a) Protocolo IPv4.

El protocolo IPv4 (Internet Protocol versión 4), es utilizado actualmente para internet, se encuentra administrado por la IANA (Internet Assigned Numbers Authority), consta de cuatro octetos separados por un punto, por ejemplo: 192.168.15.7.

La función principal es enviar paquetes de un nodo fuente a un nodo destino. Este proceso se logra identificado cada paquete que se envía a una dirección IP (dirección numérica) en específico.

En la actualidad las direcciones de internet se han agotado, ya que al inicio se proporcionaban bloques, sin tener la precaución y organización necesaria para preservar este protocolo. El protocolo se creó con más de 4000 millones de direcciones, pensando que serían suficientes en un futuro. Intentando mitigar este problema, se implementaron las IP públicas y privadas.

Las IP privadas (direcciones privadas o direcciones no homologadas) son direcciones manejadas dentro de las organizaciones sin tener acceso a la red (internet), estas direcciones no se asignan y por lo regular los hosts utilizan el nateo o traducción de red (NAT), lo que les permite la libre navegación por la red (internet), la ventaja de este esquema es que permite la reutilización de direcciones en distintas instituciones, previniendo el abuso de las IP públicas.

Existen tres bloques principales de direcciones privadas o no homologadas, definidas en el RFC 1918:

- 10.0.0.0 (prefijo 10/8): los rangos válidos para este bloque serían 10.0.0.0 hasta 10.255.255.255. Siendo un identificador de red de clase A que permite hacer uso de hasta 24 bits de dirección.

- 172.16.0.0 (prefijo 172.16/12): los rangos válidos para este bloque serían 172.16.0.0 hasta 172.31.255.255. Formado por 16 bloques de clase B que permite hacer uso de hasta 20 bits de dirección.
- 192.168.0.0 (prefijo192.168/16): los rangos válidos para este bloque serían 192.168.0.0 hasta 192.168.255.255. Formado por 256 bloques de clase C que permite hacer uso de hasta 16 bits de dirección.

Las IP públicas son asignadas por la IANA, asegurando que no se repitan y queden registradas en los routers conectados directamente a internet, en caso de que en alguna parte de la red se llegue a duplicar una dirección IP, los paquetes enviados no llegarán al destino correcto, causando la pérdida del paquete.

b) Protocolo IPv6.

Es un protocolo de Internet versión 6, que cuenta con 340 sextillones de direcciones, bajo la administración de LACNIC (Latin America & Caribbran Network Information Centre), que desde el año 2009, se ha dedicado a hacer promoción a este nuevo protocolo de internet, con la finalidad de realizar la migración.

Las características de este protocolo son:

- Las direcciones IP, son poco legibles a comparación del protocolo IPv4, ya que están en hexadecimal.
- Enrutamiento eficaz.
- Las direcciones IP se clasifican en unicast, multicast y anycast.

Cabe mencionar que se siguen manejando los mismos mecanismos de seguridad que el protocolo IPv4.

1.4.3.2 Enrutamiento.

El encaminamiento o enrutamiento consiste en encontrar la ruta más óptima para realizar el envío de paquetes de un origen hacia un destino, tomando en cuenta que debe de existir más de una ruta, para garantizar la comunicación entre dos o más dispositivos.

Para calcular la ruta más optima, es necesario generar tablas de enrutamiento, que contendrán los datos en pares (del origen y el destino). El dispositivo encargado de realizar los enrutamientos es el router, el cual en su sistema operativo (IOS de Cisco) almacenará tanto las tablas de enrutamiento como los posibles cambios que se realice, tomará en cuenta la métrica del salto más corto.

Los encaminamientos se dividen en dos y son los siguientes:

- ***Encaminamientos estáticos:*** Como su nombre lo dice solo mantendrá comunicación con la tabla establecida y no reaccionara ante cambios en la red.
- ***Encaminamiento dinámico:*** Este tipo de encaminamiento se mantendrá al tanto de los cambios generados en la red.

a) Enrutamientos dinámicos.

El encaminamiento dinámico es un protocolo encargado de comunicar a los equipos pertenecientes de una red, utiliza métricas, tablas de enrutamiento, protocolos vector-distancia y estado de enlace.

Los encaminamientos pertenecientes a este rubro son:

- ***RIP:*** Es un protocolo vector-distancia, que divide las rutas en activas y pasivas, utiliza la métrica de saltos para obtener la ruta óptima. Se mantiene al tanto de las actualizaciones de las rutas vecinas, existen dos variantes de este protocolo (RIPv1, RIPv2).

- ***IGRP:*** Es un protocolo vector-distancia, que considera el ancho de banda, el retardo, la carga y la confiabilidad, es un protocolo con clase. Tiene una versión mejorada EIGRP.
- ***EIGRP:*** *E*s la versión mejorada de IGRP, maneja las mismas métricas pero está diseñado para redes más robustas.
- ***OSPF:*** Es un protocolo estado de enlace, tiene una versión para el protocolo IPv6, la métrica que utiliza está definida por el costo, es un protocolo sin clase, lo que le permite estar al tanto del envío de mensajes.

En el protocolo vector-distancia las actualizaciones se hacen constantemente, sin embargo en el protocolo enlace de datos las actualizaciones se hacen por eventos, lo que genera que el gasto de recursos sea menor en comparación con el primer protocolo.

b) **Enrutamiento estático.**

Es un protocolo que utiliza las rutas estáticas, son configuradas manualmente, ocasionando que exista una carga de recursos en el sistema del router. Los comandos que utiliza son la dirección de red y la máscara asociada, así como el destino del envío de mensajes.

El mantenimiento de esta red es muy caro, el administrador de redes debe estar al pendiente de los cambios que se generan y así mantener actualizada la tabla de enrutamiento. Este tipo de encaminamientos no es ideal en el uso de redes robustas.

1.4.3.3 Monitoreo de la red.

Se le denomina monitoreo de la red al proceso de utilizar un sistema automatizado de monitoreo, es decir que se dedica a indagar el tiempo de respuesta en el envío de paquetes y recepción de los mismos.

Para realizar esta actividad se requiere de alguno del siguiente softwares; Tcpdump, Wireshark, Hyperic, Nagios, entre otros.

El administrador de redes, puede configurar alertas vía internet a su dispositivo móvil por medio de mensajes, correos electrónicos o la activación de la interfaz de monitoreo de red a distancia.

En el momento que el sistema encuentre una falla de latencia, envía el mensaje de alerta al administrador, le permite realizar las configuraciones necesarias y solucionar dicho problema (el software nagios, tiene esa funcionalidad).

1.4.4 Capa 4: de transporte.

La capa de transporte, es la encargada de transferencia de datos libre de errores, deberá de ser capaz de la segmentación de la información, llegar al destino y volver a unir los datos sin alteración, aunque estos no se encuentren conectados directamente.

Los protocolos de transporte que se utilizan en esta capa, están creados con la finalidad de lograr la comunicación y compatibilidad entre distintas aplicaciones.

Los pasos básicos de un transporte sencillo serían:

- ***Listen:*** Permanece en escucha hasta que algún proceso haga contacto.
- ***Connect:*** Realiza la recepción de petición del proceso.
- ***Send:*** Envía la información solicitada.
- ***Receive:*** Bloquea el canal de comunicación, hasta asegurar la recepción de los datos solicitados.
- ***Disconnect:*** *C*ierra la comunicación con ese canal y vuelve a permanecer en espera, hasta nueva solicitud.

Cabe mencionar que la aplicación de Sockets de Berkeley, es una variante de este proceso, con mejor flexibilidad y características.

1.4.4.1 Protocolo a nivel de transporte.

Los protocolos que permiten la transferencia de datos libre de errores en la capa de transporte se describen a continuación.

a) TCP (Transmission Control Protocol).

TCP, es un protocolo orientado a conexión y fiable en la capa de transporte, ya que garantiza la entrega de paquetes, además de dar soporte a aplicaciones como son: HTTP, SMTP, SSH y FTP.

Durante la comunicación, dos máquinas realizan una conexión llamada cliente-servidor (como se ilustra en la figura 1.4). La maquina que realiza la petición se le conoce como cliente y la máquina que contesta a esta petición se le llama servidor.

La comunicación se realiza en los siguientes pasos:

- La máquina denominada servidor, permanece con los puertos TCP abiertos.
- Se encuentra en espera de una petición por parte del cliente.
- El cliente envía una solicitud, la cual será recibida por el servidor y atendida por medio de datagramas.
- Una vez completada la solicitud del cliente, el servidor cierra esa comunicación y regresa al estado pasivo en espera de una nueva petición.

Una de las ventajas más importantes de este protocolo es la confirmación del envío y recepción de datos, en dicho proceso el protocolo envía constantemente la confirmación del último datagrama recibido.

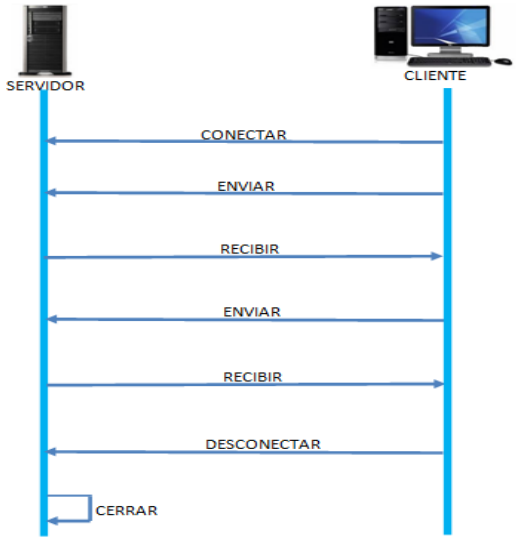


Figura 1.4 Modelo de conexión TCP

b) UDP (User Datagram Protocol)

UDP, es un protocolo no orientado a conexión y poco fiable, ya que no proporciona una detección de errores en el envío y recepción de datos.

Trabaja a través de datagramas, por medio de un canal unidireccional es decir, por el mismo canal que envía, recibe y no podrá atender a más de un cliente a la vez, cosa que el protocolo TCP realiza

c) TTL (Time To Live).

TTL, es una herramienta de la capa red y es utilizada por la capa de transporte en el protocolo TCP. Esta herramienta se activa a través del ping, la cual nos dirá el número de saltos que puede dar un paquete antes de ser descartado por la red o bien devuelto a su origen, conforme a la figura 1.5.

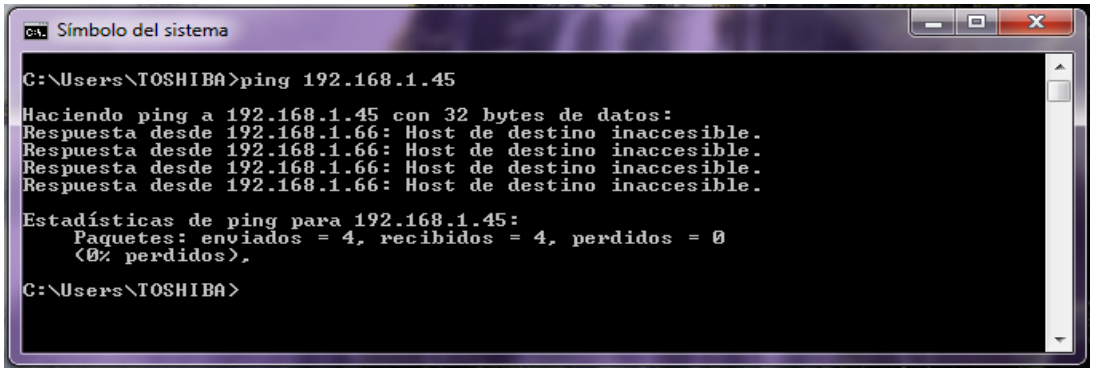


Figura 1.5 Uso del TTL.

d) ACL, SSL y TLS.

ACL (Access Control List) son listas de acceso que permiten o deniega el tráfico por alguna red. El administrador de red gestiona los permisos necesarios para que los routers de cierta topología puedan tener acceso entre sí o solo en algunos segmentos. Existen dos tipos de listas y son:

- Listas fijas, las cuales no cambian.
- Listas variables, las cuales se modifican constantemente.

Las ACL normalmente se usan para:

- ***Brindar un control de flujo de datos:*** Es decir, restringen el envío/recepción de paquetes que pasan a través del router, permitirá el paso exclusivo declarado en las listas de control de acceso.
- ***Proporcional un nivel básico de seguridad:*** Al crear las listas de control de acceso, se permite la intrusión solo a una parte de la red.

Algunos inconvenientes de utilizar las ACL son:

- Declaración incorrecta del uso de las ACL.
- Denegación o permiso total del acceso a la red.

SSL (Secure Socket Layer) y TLS (Transport Layer Segurity) son protocolos criptográficos, que permiten que la comunicación sea segura y viaje de manera

cifrada, la primera versión de este protocolo fue SSL, el cual tuvo demasiadas fallas y fue sustituido por el TLS.

El protocolo SSL/TLS, permiten tener una conexión segura en la web (internet), es decir cuando un usuario hace una petición a alguna página web, existe un intercambio de información de certificados, firma digital que a su vez cifra la información para evitar que sea leída en claro.

Cuando la verificación ha sido exitosa en el navegador se verá un candado y el protocolo HTTPS en verde o bien si el protocolo no ha podido verificar alguna información mandará un mensaje y el protocolo HTTPS se observará en rojo, como se observa en la figura siguiente.

Figura 1.6 Cifrado de protocolo HTTPS.

Es conveniente verificar el certificado de autenticidad del protocolo HTTP, para evitar robo de identidad, falsificación de autenticidad de certificado.

1.4.5 Capa 5: Capa de sesión.

La Capa de Sesión es la encargada de proporcionar los mecanismos necesarios para controlar el dialogo entre las aplicaciones de los sistemas finales, el uso de esta capa es necesaria, ya que administra almacenamiento, periféricos, memoria y procesos.

1.4.5.1 Capa 6: Capa de presentación

La Capa de Presentación se encarga de la presentación de los datos, es decir actúa como un traductor, permitiendo que distintos equipos se puedan comunicar entre sí. Cumple tres funciones principales que son; formateo, cifrado y compresión de datos.

1.4.5.2 Capa 7: Capa de aplicación.

La Capa de Aplicación, permite la comunicación entre dos aplicaciones y define los protocolos para que pueda interactuar con los servicios de correo electrónico, protocolos de transferencia de archivos, entre otros. Esta capa no interactúa directamente con el usuario.

1.4.5.3 Interacción entre capas.

La interacción entre las capas de sesión, presentación y aplicación, se trabaja dentro del modelo TCP/IP, aquí se definen las aplicaciones de la capa de red y de los servicios utilizados para internet, incluyendo los protocolos correspondientes.

Cada programa de aplicación, selecciona la forma de transporte para el envío de datos. Los servicios de la interacción entre capas son:

- Servicios de aplicaciones de internet.
- Servicios de conexión de red.
- Servicio de transferencia de datos, entre otros.

1.4.5.4 Protocolos a nivel de aplicación.

Algunos de los protocolos que interactúan con el usuario, para que éste pueda realizar una conexión exitosa con el servidor son:

- ***TELNET:*** Basado en el protocolo TCP, crea una conexión tipo cliente/servidor y es útil en el manejo de maquinas virtuales.

- ***FTP y TFTP:*** Protocolo de transferencia de archivos, utiliza la conexión cliente/servidor, donde el cliente efectúa transferencias directas de un servidor a otro.
- ***HTTP y HTTPS:*** Protocolos utilizados en sistemas de redes, permite la transferencia de información del lenguaje HTLM desde servidores web a navegadores.
- ***DNS:*** Sistema de nomenclatura jerárquica para determinar nombres a las diferentes direcciones existentes en internet o alguna red privada
- ***TCP:*** Protocolo orientado a conexión y fiable en la capa de transporte.
- ***IP:*** Protocolo encargado de permitir la conexión en forma digital.

1.4.6 DNS.

DNS (Domain Name System), es un sistema de nomenclatura jerárquica para determinar nombres a las diferentes direcciones existentes en internet o alguna red privada.

Los servidores DNS realizan la traducción de Direcciones IP para que al usuario le sea más fácil recordar el nombre, lo que se le conoce como nombre de resolución de nombres de dominio.

La resolución de nombres de dominio se realiza de la siguiente manera:

- La dirección IP será traducida al revés en forma FQDN.
- El nombre de dominio se creara en forma de árbol.
- Dependiendo su fin, llevara las siglas correspondientes a su país o institución.

Un FQDN (Fully Qualified Domain Name), formado en forma correcta es: *www.hola.com,* como se muestra en la figura 1.7.

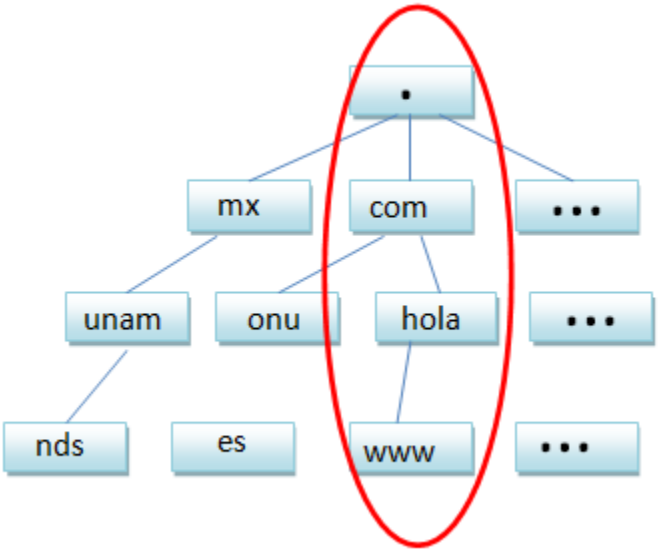


Figura 1.7 Creación de los nombres de dominio.

Cada ramificación se encuentra separada por un punto, la dirección IP la muestra de forma invertida, esto se conoce como resolución inversa.

La resolución inversa es el proceso de averigua el nombre de dominio asociado a una dirección IP (en lugar de la resolución normal que averigua la IP asociada a un dominio), es muy practica ya que ahorra tiempo en buscar alguna dirección IP.[1]

1.4.6.1 DHCP.

DHCP (Dynamic Host Configuration Protocol), es un protocolo encargado de proporcionar direcciones IP a los diferentes equipos de cómputo conectados a una red de forma dinámica o estática.

Cada dispositivo deberá contar con una dirección IP única, para evitar conflictos o pérdidas de información.

[1] **APRENDE DNS Y APACHE,** David del Barrio Prat

1.4.6.2 HTTP y HTTPS.

HTTP (Hypertext Transfer Protocol) es un protocolo utilizado en sistemas de redes que permite la transferencia de información del lenguaje HTML desde servidores web a navegadores.

El protocolo HTTP trabaja a través del puerto 80, en la capa de red del Modelo OSI y no es confiable la navegación, no solicita certificados y la información navega en claro, permitiendo ser blanco fácil para los ataques como; man in the middle (ataque encargado de escuchar todo el tráfico que pasa por un segmento de red en específico, puede tener la variación de realizar usurpación de identidad, duplicación de páginas web).

HTTPS (Hypertext Transfer Protocol Secure) es un protocolo utilizado para tener una conexión segura, trabaja por el puerto 443 y en la capa de transporte del Modelo OSI además de estar unido al protocolo SSL/TLS.

Al navegar por el puerto 443, da una conexión entre el servidor y el cliente únicamente, no es blanco fácil de los ataques man in the middle, lo único que puede ver el atacante es una comunicación cifrada.

1.5 Definición de seguridad.

El termino seguridad se refiere a la ausencia de riesgo o a la confianza en algo o alguien. Sin embargo, puede tomar diversos sentidos según el área o campo al que haga referencia.

La seguridad informática se define como un conjunto de medidas que impidan la ejecución de operaciones no autorizadas sobre un sistema o red informática, estas medidas son un conjunto de reglas, planes, actividades y herramientas.

La operación no autorizada en un sistema informático puede dañar la información, comprometer la triada de seguridad (véase la figura 1.8) confidencialidad,

autenticidad e integridad, además de llegar a disminuir el rendimiento de los equipos, desactivar los servicios o bien bloquear el acceso a usuarios autorizados

Figura 1.8 Triada de la información.

1.5.1 Confidencialidad.

La confidencialidad es un servicio de seguridad de la información, cuya función es garantizar en medida de lo posible que la información se encuentre accesible únicamente al personal autorizado.

Para garantizar la confidencialidad es necesario hacer uso de la criptografía, por medio de algoritmos criptográficos se podrá cifrar la información delicada entre el emisor y receptor.

1.5.2 Disponibilidad.

La disponibilidad es un servicio de seguridad de la información, cuya función es garantizar que las aplicaciones, datos y servicios se encuentren disponibles para cualquier usuario y en cualquier momento.

1.5.3 Integridad.

Con este servicio se completa la triada de la seguridad de la información, cuya finalidad es mantener, en la medida de lo posible los datos íntegros, así como evitar que dicha información sea corrupta o modificada por personal no autorizado.

1.6 Vulnerabilidad.

Por vulnerabilidad se entiende como un riesgo latente existente en un sistema. Las vulnerabilidades son puntos débiles de los sistemas, procesos, hardware, personas o cualquier bien importante para una persona o grupo de personas, por donde los intrusos pueden dañar la triada de la seguridad.

1.6.1 Tipos de Vulnerabilidades.

Existen diferentes tipos de vulnerabilidad, como son:

- ***Físicos:*** Todo acceso no autorizado a un lugar físico con la intención de generar algún daño o hurto.
- ***Natural:*** Daño generado por cuestiones naturales que no son previstas por el hombre como inundaciones, incendios, terremotos, entre otros.
- ***De hardware:*** Daño físico a los componentes de equipos de cómputo o bien nula compatibilidad entre estos.
- ***De software:*** Sistemas dañados o con aplicaciones maliciosas incluidas.
- ***Humana:*** Personal en desacuerdo con las políticas de la empresa o con fines de lucro (pagadas por externos) para dañar la institución.
- ***De red:*** Mal uso de las aplicaciones disponibles para el cuidado del equipo en la red, puede ser software vencido, incompatible o acceso libre al equipo de cómputo.

1.7 Amenaza.

Las amenazas son hechos intencionales o no intencionales de dañar a un dispositivo, persona, institución, organización o equipo de cómputo. Si existe una vulnerabilidad por ende puede existir una amenaza.

1.7.1 Tipos de Amenazas.

Existen diferentes tipos de amenazas como son:

- ***Humanas:*** Personal de la misma empresa con poca o nula capacitación del manejo de dispositivos.
- ***Natural:*** Desastres naturales no previstos por el ser humano.
- ***De hardware:*** Daño físico a los componentes de equipos de cómputo.
- ***Lógicas:*** Mala administración de la red, ya que se permite el acceso a todo tipo de aplicaciones, sin tomar en cuenta las vulnerabilidades que esto conlleva.
- ***De red:*** Deficiente administración y creación de la topología a usar, puede tener un canal inseguro para el flujo de información prevista.

Capítulo 2.

Normatividad

Introducción

El uso de normas, estándares y manuales de buenas prácticas permiten que distintos equipos, dispositivos portátiles conectores, protocolos, entre otros, puedan establecer una comunicación confiable en distintos lugares, permitiendo así el intercambio de información. Es decir, cuando se navega en la red, se hace una petición de información la cual es respondida por servidores que pueden encontrarse del otro lado del mundo.

Lo mismo sucede con los conectores, por ejemplo: una entrada usb tiene las mismas especificaciones técnicas, mecánicas y eléctricas en todas partes del mundo.

Anteriormente las grandes empresas creaban sus propios protocolos, adaptadores, conectores con las especificaciones técnicas exclusivas al producto que fabricaban, lo que las hacía incompatibles con los dispositivos similares o complementarios, ocasionando que el usuario fuese el más perjudicado al no tener compatibilidad con estos dispositivos. En la actualidad las instituciones normalizadoras (OSI, IEC, ANSI, TIA, entre otras) han logrado que exista la compatibilidad entre dispositivos y protocolos, logrando que los usuarios hagan uso de diferentes marcas.

2.1 Definición de Norma.

Una norma o estándar es un documento de aplicación voluntaria que contiene especificaciones técnicas, basadas en los resultados de experiencias y desarrollo tecnológico. Son documentos aprobados por un organismo normalizador reconocido.

Las normas contienen criterios precisos asegurando que los materiales, productos, procesos y servicios están hechos con la calidad necesaria para alcanzar sus objetivos, incrementar la fiabilidad y efectividad de los bienes y servicios que se utilizan en los diferentes rubros, como son telecomunicaciones, servicios, alimentos, papelería, entre otras.

2.2 Tipos de normas.

En la actualidad existen normas por rubros, como son:

1. ***Normas sociales:*** Son dictadas a partir de una serie de costumbres, tradiciones, entre otras, que prevalecen dentro de una sociedad que se les impone como no obligatorias, pero que las llevan a cabo por ser parte de sus costumbres.
2. ***Normas religiosas:*** Tienen su origen a la creencia de Dios y éste dicta las reglas del comportamiento esperado y deseado de los seres humanos. En caso de que estas normas no se lleven a cabo; el individuo será castigado en su conciencia en forma de pecado.
3. ***Normas morales:*** A diferencia de las demás normas, éstas no son dictadas por nadie más que por el individuo en cuestión y están destinadas a responder a la propia conciencia, de lo contrario el auto castigo será su propio remordimiento.
4. ***Normas jurídicas:*** Son dictadas por orden gubernamental y van dirigidas a todos los individuos de una comunidad política en particular.
5. ***Normas técnicas:*** Documento basado en experiencias y desarrollo tecnológico, avalado por algún organismo normalizador.

2.3 Normas Internacionales de Telecomunicaciones.

La función de las normas internaciones es regular las telecomunicaciones a nivel internacional. Existen instituciones encargadas de estandarizar y regular los medios de comunicación, las cuales se describen a continuación:

1. Unión Internacional de Telecomunicaciones (ITU).

Es un organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), tiene como objetivo, regular las telecomunicaciones a nivel internacional en conjunto con empresas públicas y privadas. Con sede en Ginebra, Suiza.

Se creó en 1865 con el fin de crear un estándar en todas las telecomunicaciones, desde el teléfono, radio hasta los dispositivos móviles. En 1947 se convirtió en un organismo de la ONU y desde 1998 hasta 2003, absorbió empresas relacionadas como la "Asociación de la Tecnología Informática de América" (ITAA) y el "Consejo Internacional para la Administración Tecnológica" (IBTA).

Las normas generadas por la ITU son conocidas como "*Recomendaciones"*, por pertenecer a la ONU, sus publicaciones tienen más validez que otras organizaciones similares.

2. Estándares y Normas más relevantes desarrolladas por la ITU.

Las recomendaciones de la ITU tienen como objetivos lo siguiente:

a) ***Simplificación:*** Tratar de reducir los procesos y protocolos, quedándose únicamente los o básicos indispensables.
b) ***Unificación:*** Permitir la interconexión a nivel internacional.
c) ***Especificación:*** Evitar errores de codificación, es decir, que la programación y el lenguaje sea claro y preciso.

Los principales manuales son:

a) 1984 - Compendio de los métodos de medición de cables.

b) 2004 - Calidad de servicio y calidad de funcionamiento de la red: pretende especificar los parámetros necesarios para cubrir las expectativas y necesidades del cliente.

c) 2008 - Medidas de mitigación en las instalaciones de telecomunicaciones: proporciona casos de estudio, los cuales analizan las emisiones y ruidos inducidos, sobretensión y sobrecorriente y los problemas de frecuencia de alimentación.

d) 2009 - Fibras ópticas, cables y sistemas: manual encargado de ser una guía para la instalación de práctica de los sistemas basados en fibra óptica.

e) 2011 - Realización de pruebas en redes de la próxima generación: describe en forma general el enfoque que se debe de dar a la realización de pruebas tanto por administradores como fabricantes, así como tratar los problemas de interoperabilidad que puede surgir durante la instalación de la red o la prestación de servicio.

f) 2012 - La seguridad de las telecomunicaciones y las tecnologías de la información: tiene por objetivo presentar una introducción general a los trabajos realizados por la UIT-T (2003, 2004, 2006 y 2009) en el tema de la seguridad.

Las principales recomendaciones son:

a) ***E.408:*** Plantea los requisitos de seguridad y hace referencia a las amenazas en cuanto a seguridad de redes en las telecomunicaciones. Se plantean soluciones posibles y medidas para contrarrestar los riesgos de amenazas.

b) ***E.409:*** Hace referencia a los métodos de seguridad en la red, donde son más vulnerables y tienen mayor riesgo de caer en manos de los ciberatacantes, donde se han presentado casos de robo de identidad y

suplantación de la misma, hace hincapié de cuáles son las mejores recomendaciones para tratar de evitar un ataque.

c) ***E.412:*** Se establecen recomendaciones e indicaciones para el mejor manejo de controles de gestión de red. Está recomendación por ser de las más importantes tiene un subsecuente directo que es la norma **E.412.1.**

Las normas que comprenden de la E.413 a la E.419, hacen referencia al manejo correcto y dirección por parte de los gestores de redes de datos.

d) ***E.490:*** Recomendaciones necesarias para el monitoreo de una red de datos.

La serie comprendida de la E.490 a la E.505, hace recomendaciones para monitorear y evaluar el tráfico en la red.

e) ***Serie X:*** La serie x, está relacionada a las redes de datos, seguridad, interconexión y la nube. Dentro de esta serie, existen recomendaciones para el Modelo de Interconexión de Sistemas Abiertos.

3. Organización Internacional de Normalización (ISO)

Creada en 1947 con sede central en Ginebra, Suiza, es una organización independiente no gubernamental, principal desarrollador de Normas internacionales. Se encuentra presente en 163 países, en cada país existe un miembro de esta organización, con el fin de garantizar la estandarización de los productos y servicios a nivel internacional.

La composición de los miembros es por tres niveles:

a) Miembros simples, existe un miembro por cada país asociado, el cual representa a la organización.

b) Miembros correspondientes, referente a países en vías de desarrollo, estos no toman parte activa del proceso de normalización pero están informados de las normas que les interesan.

c) Miembros suscritos, países con limitantes económicas, se les solicita cuotas más bajas que los miembros correspondientes.

Hasta el año 2015 la ISO, ha publicado más de 19 500 Normas Internacionales cubriendo casi todas las industrias, desde alimentos hasta los servicios de telecomunicaciones, pasando por los servicios de salud. Dentro del área de redes de datos se encuentran las siguientes:

a) ***ISO 8402:*** Fue publicada en 1986, siendo un complemento de la serie de normas ISO 9000, la cual define términos básicos y fundamentales relacionados con los conceptos de la calidad. La necesidad de contar con un manual de terminología adecuada para la atención y calidad del cliente, se impulsó el desarrollo de esta norma, para evitar malentendidos acerca de la atención al cliente.

b) ***Serie ISO 9000:*** Normas que definen los conceptos básicos para la Gestión de Calidad, así como las recomendaciones para la calidad del servicio, certificación y auditorias

c) ***ISO/IEC 11801:*** Indica las normas y estándares para el cableado estructurado. Define varias clases de cable de par trenzado de cobre, dependiendo de su frecuencia, las cuales son:

- Clase A: hasta 100 kHz.
- Clase B: hasta 1 MHz.
- Clase C: hasta 16 MHz.
- Clase D: hasta 100 MHz.
- Clase E: hasta 250 MHz.
- Clase F: hasta 600 MHz.
- Clase Fa: hasta 1000 MHz.

d) ***ISO/IEC 12207:*** Normas referentes al tiempo de vida del software. Contiene los procesos, actividades y tareas que se van a aplicar durante la adquisición de un producto de software o servicio y durante el suministro,

desarrollo, operación, mantenimiento y eliminación de los productos de software. El software incluye la parte de firewall.[2]

Algunas de las normas mencionadas, están elaboradas en conjunto con la Comisión Electrónica Internacional (IEC).

4. Comisión Electrónica Internacional (IEC)

Fue fundada en 1906, teniendo como principal sede San Luis (Misuri), en 1948 se traslada a Ginebra, Suiza. En 2015, cuenta con 83 miembros, cada uno representa a un país asociado (60 “Miembros Plenos” y 23 “Miembros Asociados”).

Al ser parte de los miembros de la IEC, tienen la posibilidad de influir en el desarrollo de normas internacionales, además de mantenerse actualizado en la tecnología de punta a nivel mundial.

Es la principal organización mundial en crear y publicar normas internacionales para las tecnologías eléctricas y relacionadas. El desarrollo de normas es en colaboración con la ISO.

5. Instituto de Ingeniería Eléctrica Electrónica (IEEE)

Es una asociación mundial de técnicos e ingenieros dedicados a la estandarización y el desarrollo en áreas técnicas.

En la primavera de 1884, después de sentir la necesidad de crear un foro para el intercambio de información, se estable el Instituto Norteamericano de Ingenieros Eléctricos de la ciudad de Nueva York. En 1922 se creó una sucursal de la IEEE México a petición del Sr. H.W. Fraser, gerente de la Compañía Mexicana de Luz y Fuerza Motriz, S.A., en 1948 se efectuó en México la Convención Mundial del IEEE, reuniendo a más de 600 ingenieros de todo el mundo en la Cd. de México.

[2] www.iso.org

El IEEE da atención a más de 367,395 ingenieros, estudiantes de Ingeniería, científicos y demás profesionistas en más de 150 países, esta divido en: 10 regiones, 17 consejos, 311 secciones, 1, 570capítulos técnicos, 217 grupos afines, 1,434 ramas estudiantiles, 382 capítulos técnicos en ramas estudiantiles, 60 grupos afines de ramas estudiantiles.[3]

Dentro de las ramas estudiantiles se encuentran las siguientes instituciones:

- UNAM, Facultad de Ingeniería.
- UNAM, ENEP Aragón.
- IPN-CINVESTAV.
- IPN, ESIME Culhuacán.
- Instituto Tecnológico de Hermosillo.
- ITESM, Cd. de México.
- TEC de Estudios Superiores de Ecatepec.
- UAM Iztapalapa.

Estas son solo algunas de las 97 instituciones que forman parte de las Ramas Estudiantiles en la Sección México.

Dentro de las normas de la IEEE, se encuentra la serie 802, que define los estándares para las redes LAN, estos estándares se crearon en los años 80´s cuando se iniciaba el uso de redes entre computadoras personales.

- ***802.1:*** Define la relación entre los estándares IEEE y el modelo de referencia para interconexión de sistemas abiertos de la ISO.
- ***802.2:*** Define el uso del protocolo de control de enlaces lógicos (LLC), el cual asegura que los datos sean trasmitidos de forma correcta. Este estándar se utiliza en la capa de enlace de datos del modelo OSI.

[3] https://www.ieee.org/index.html

- ***802.3:*** El estándar 802.3 se encuentra definido dentro de la norma ISO 8802-3.
- ***802.4:*** Define los lineamientos del ancho de banda para la utilización de las redes Token Bus.
- ***802.5:*** Este estándar también es llamado ANSI 802.1-1995, utilizado por IBM, utiliza el método de acceso de paso de tokens y se conecta físicamente a una topología tipo estrella.
- ***802.6:*** Define un protocolo donde analiza la velocidad de las Redes de Área Metropolitana (MAN), el cual está diseñado para proveer de los servicios de voz, datos y video en área determinada.

De la familia 802.11, se mencionarán algunos de los estándares más importantes en las redes que la componen:[4]

- ***802.11d:*** Múltiples dominios reguladores (restricciones de países al uso de determinadas frecuencias).
- ***802.11e:*** Calidad de servicio (QoS).
- ***802.11f:*** Protocolo de conexión entre puntos de acceso (AP), protocolo IAPP: Inter Access Point Protocol.
- ***802.11i:*** Seguridad (aprobada en Julio de 2004).
- ***802.11k:*** Mejora la gestión de las redes WLAN.
- ***802.11m:*** Mantenimiento redes wireless.
- ***802.11r:*** Pensado para conmutación rápida y segura entre puntos de acceso.
- ***802.11s:*** Interoperatibilidad entre fabricantes.
- ***802.11v:*** Configuración remota de dispositivos cliente.
- ***802.11w:*** Mejora en la capa de control de acceso al medio en cuanto su autenticación y codificación.

[4] Seguridad por Niveles. Corletti, Alejandro

6. Instituto Nacional Estadounidense de Estándares (ANSI)

En 1918 se fundó el Comité Estadounidense de Estándares para la Ingeniería (AESC, por su siglas en inglés), en 1928 cambia su nombre a Asociación de Estándares Estadounidenses (ASA), en 1966 ASA, sufre una reorganización y se convierte en Instituto de Estándares de los Estados Unidos de América (USASI), para 1969 adquiere el nombre con que el actualmente se conoce. Su sede se encuentra ubicada en Washington, D.C.

Es el único Instituto que representa a los Estados Unidos como miembro activo de la ISO y la IEC, lo que le permite tener acceso inmediato a los procesos de desarrollo de las normas de estas dos instituciones. Es una organización sin fines de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos.

7. Alianzas de Industrias Electrónicas (EIA)

Es una organización formada por la asociación de las compañías electrónicas y de alta tecnología de los Estados Unidos en 1997, tiene su sede en Arlington, Virginia y abarca a casi 1300 compañías del sector, desde los componentes electrónicos más pequeños hasta complejos sistemas usados en la defensa o sectores espaciales.

2.3.1 Normas básicas de redes y seguridad.

En el manejo de seguridad de la información se debe tomar en cuenta, ciertas normas, estándares y buenas prácticas que ayuden a minimizar los posibles riesgos, que existan en el manejo de las redes de datos y seguridad.
A continuación se enuncian algunas normas importantes para este rubro:

a) SGSI (Sistema de Gestión de Seguridad de la Información).

El SGSI (Sistema de Gestión de Seguridad de la Información) es un concepto en el que se basan las normas de la serie ISO 27001 y la serie ISO 20000.

Para las empresas, instituciones y organizaciones son la forma de diseñar, implementar y dar mantenimiento a los procesos utilizados en la Seguridad de la Información, con el único fin de mantener la Confidencialidad, Integridad y Disponibilidad de los bienes en información, minimizando o en algunos casos anulando los riesgos de modificación, suplantación o perdida de información.

La ISO/IEC 27001 implementa el ciclo de Deming o mejor conocido como Plan-Do-Check-Act. (PDA), como se describe a continuación (véase figura 2.1):

- ***Plan (planificar):*** En este punto se deben establecer las actividades del proceso que está en curso, tomando en cuenta el tiempo, la situación, recopilación de datos y la definición de actividades.
- ***Do (hacer):*** Ejecución del plan, donde se va a organizar, dirigir, asignar recursos humanos y económicos.
- ***Check (verificar):*** Pasado el tiempo de prueba, recopilar los resultados, analizarlos, así como revalorar el procedimiento, los objetivos y seguir las metas propuestas.
- ***Act(actuar):*** Con base en los resultados anteriores, se debe tomar una decisión para llevar a cabo el mejor plan y obtener el máximo de rendimientos.

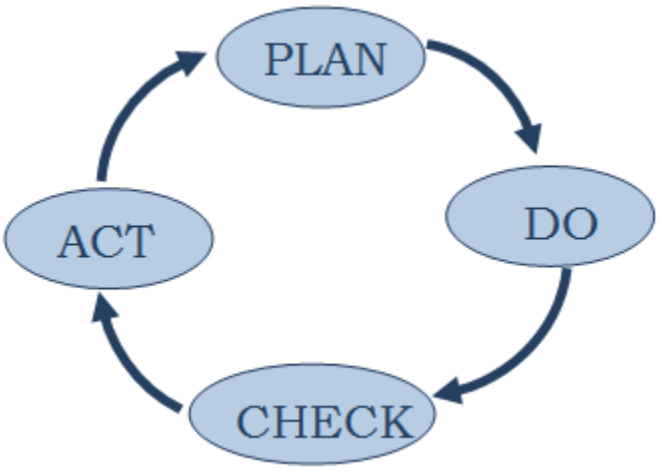


Figura 2.1 PDCA.

BENEFICIOS DE LA NORMA ISO/IEC 27001:[5]

- Establecer una metodología en la gestión de la seguridad para que sea clara y estructurada, es decir, el manual de buenas prácticas de seguridad sebera de ser claro y conciso para un mejor entendimiento de la gestión de seguridad.
- Reducir los riesgos de pérdida, robo o modificación de la información por parte de los usuarios o bien personal externo.
- Los clientes acceden a la información por medio de medidas de seguridad, donde la empresa proporcionará claves de acceso, nombres de usuarios y restricción de información.
- Los controles de acceso se encontrarán en monitoreo constante para evitar problemas a futuro.
- La confianza entre clientes y socios estratégicos, se dará gracias a la garantía de calidad y confidencialidad entre ambos lados.
- Las auditorías externas ayudan a identificar las debilidades del sistema para así mejorar las áreas de trabajo y metodologías implementadas.
- Posibilidad de integración con otros sistemas de gestión, con el fin de mantener una actualización constante de la gestión de la seguridad.
- Reducción de costos y mejoras en los procesos y servicios, evitando que existan fugas de ingresos en tecnologías innecesarias, lo que permitirá una mejora de la seguridad en base a la gestión de procesos.
- Aumento de la motivación y satisfacción personal, para que estos se sientan parte de una empresa y logren mayor productividad y trabajo en equipo.

b) ISO 17799.

Manual de buenas prácticas para realizar la gestión de la seguridad de la información. En la actualidad ha sido sustituido por la norma ISO/IEC 27002:2013

[5] www.iso27000.es/sgsi.html.

c) ISO/IEC 27000.

Son un conjunto de estándares desarrollados o en fase de desarrollo que ayuda a las organizaciones a mantener los activos de información seguros como son: la información financiera, propiedad intelectual, información proporcionada a terceros.

La primera entidad de normalización a nivel mundial fue BSI (British Standars Institution, equivalente a AENOR en España), publicó normas importantes como son:[6]

- BS 5750 publicada en 1979 antecesora de la norma ISO 9001.
- BS 7750 publicada en 1992 antecesora de la norma ISO 14001.
- BS 8800 publicada en 1996 antecesora de la norma ISO 18001.
- BS 7799-1, BS 7799-2 antecesora de la norma ISO 17799.

Las cuales en conjunto dieron paso a la serie de normas ISO 27000.

d) Serie 20000

Normas publicadas el 14 de diciembre de 2005, definen los conceptos básicos para la Gestión de Servicio en Tecnologías de la Información (SGSTI). Esta norma sustituye a la BS 15000, la cual está disponible en dos partes: especificaciones auditable y código de buenas prácticas.

Está dividida en 5 partes que son:

- Parte 1: ISO/IEC 2000-1:2005- Especificaciones
- Parte 2: ISO/IEC 2000-2: 2005- Código de Practicas.
- Parte 3: ISO/IEC 2000-3: 2009- Guía de la definición del alcance y su aplicabilidad
- Parte 4: ISO/IEC 2000-4: 2010- Modelo de referencia de procesos.
- Parte 5: ISO/IEC 2000-5: 2010- Ejemplo de implementación.

[6] http://www.iso27000.es/iso27000.html#seccion1

e) Criterios comunes

El TCSEC (Trusted Computer Security Evaluation Criteria or Orange Book) creado a mediados de los ochentas, era un libro donde se daban las normas para los niveles de seguridad para un entorno en particular. El ITSEC (Information Technology Security Evaluation Criteria by the governments of France, Germany, the Netherlands and the United Kingdom), a principios de los noventas, creó un manual de buenas prácticas donde indicaba los niveles de seguridad de un producto desarrollado. Con el paso del tiempo se dieron cuenta de que no era satisfactorio el producto generado por separado y decidieron combinarlo para crear uno nuevo. Así es como nace a finales de 1998, Criterios comunes para evaluación de seguridad de tecnología de la información (Common Criteria for Information Technology Security - CCITSE) mejor conocido como CC.

Los CC es una norma internacional para evaluar la seguridad de los productos de tecnología de la información basados en los criterios europeos, norteamericanos y canadienses existentes, que tienen como objetivo principal proporcionar protección a la información.

Los criterios comunes (versión 3.1) están formados por tres partes: introducción y modelo general, requerimientos de seguridad funcional y requerimientos de garantía de seguridad.

f) ISO 14764.

Requerimientos para el proceso de mantenimiento de software**.**

g) ISO 14001.

Norma encargada de crear un plan de manejo ambiental que incluya: objetivos, políticas, metas y procedimientos ambientales.

h) IEEE 802.11.

Estándar de protocolo de comunicaciones que define el funcionamiento de una WLAN.

i) ANSI/EIA/TIA 568 A Y 568 B.

Estándar que define la implementación de la construcción de cables para el cableado estructurado.

j) EIA/TIA 569 A Y 569 B.

Estándar que define el alambrado de telecomunicaciones para edificios comerciales.

k) ANSI/EIA/TIA 606.

Norma de administración para la infraestructura de telecomunicaciones en edificios comerciales.

l) ANSI/EIA/TIA 607.

Requisitos de aterrizado y protección para telecomunicaciones en edificios comerciales.

2.4 Normas nacionales de seguridad, construcción y telecomunicaciones.

a) ***Norma Oficial Mexicana (NOM):*** Organización encargada de regular las telecomunicaciones a nivel nacional.

- ***NOM-001-STPS:*** Regula las condiciones de seguridad de los edificios, locales, instalaciones y áreas en los centros de trabajo para su adecuado funcionamiento y conservación con la finalidad de prevenir riesgos a los trabajadores.
- ***NOM-017-STPS:*** Regula los requisitos mínimos para que el patrón proporcione equipo de protección personal correspondiente para

protegerlos de los agentes del medio ambiente, de trabajo que puedan dañar su integridad física y su salud.

- ***NOM-025-STPS:*** Regula los requerimientos de iluminación en las áreas de trabajo, con el fin de proveer un ambiente seguro y saludable en la realización de las tareas desarrolladas por los trabajadores.
- ***NOM-026-STPS:*** Establece los requerimientos en cuanto a los colores y señales de seguridad e higiene.
- ***NOM-029-STPS:*** Regula las condiciones de seguridad para la realización de actividades de mantenimiento de las instalaciones eléctricas en los centros de trabajo.
- ***NOM-031-STPS:*** Regula las condiciones de trabajo en el área de la construcción, con el fin de evitar accidentes en la salud y seguridad.

En el ámbito de la seguridad de la información, existen las siguientes leyes que regulan el uso y manejo de datos.[7]

a) ***Ley Federal del Derecho de Autor:*** esta ley reglamenta la difusión, promoción del acervo cultural de la nación así como la protección de los derechos de los autores, artistas, intérpretes, editores, productores y de los organismos de radiodifusión, en relación con sus obras literarias o artísticas en todas sus manifestaciones, interpretaciones o ejecuciones, como lo indica el artículo 28 de la Constitución Política de los Estados Unidos Mexicanos.

b) ***Ley Federal de Telecomunicaciones:*** esta ley es de orden público y tiene por objeto regular el uso, aprovechamiento y explotación del espectro radioeléctrico, de las redes de telecomunicaciones, de la comunicación vía satélite.

c) ***Ley de INEGI:*** la presente ley es de orden público e interés social y sus disposiciones rigen a la información estadística y geográfica del país que son elementos circunstanciales de la soberanía nacional, la

[7] Apuntes de Seguridad Informática. López, Jaquelina y Quezada, Cintia

utilización de esta información, es requerida en las dependencias y entidades de la Administración Pública Federal.

d) ***Código Penal Federal:*** sanciona a toda persona no autorizada al acceso ilícito a sistemas y equipos de informática (libro segundo, título noveno, capítulo dos).

Capítulo 3.

Políticas de Seguridad en Redes.

Introducción

Las políticas de seguridad ayudan a mantener los activos de la organización protegidos y dentro de lo posible libres de vulnerabilidades y amenazas. En la actualidad los activos de las organizaciones incluyen los datos (documentos, fotos, libros, archivos), los dispositivos de interconexión, equipos de cómputo, hardware, software e inclusive las aplicaciones.

Para definir el tipo de políticas a usar, se deben tomar en cuenta las siguientes preguntas; ¿qué es lo que se desea proteger?, ¿Por cuánto tiempo?, ¿a quién afecta?, ¿cómo se puede proteger?, ¿en dónde de piensa proteger? Cada una de ellas tiene que contener un plan a seguir y un plan de contingencias en caso de algún fallo o problema.

Existen herramientas que son necesarias en la gestión de seguridad en la Información como son; controles de acceso, listas de acceso, contraseñas, contratos de confidencialidad, etcétera, que permiten mantener un control y bitácora de hechos en puestos de seguridad.

De la misma manera en las recomendaciones X.800 y el estándar ISO 7498-2, enuncia los servicios de seguridad, los cuales sirven para garantizar la triada de la información y el no repudio, que hace referencia a la no negación de recepción/envío de datos por medio del internet.

3.1 Definición de políticas.

Es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma. La política define la seguridad informática para una organización, especificando tanto las propiedades del sistema como las responsabilidades de seguridad de las personas.[8]

Dentro de las instituciones se manejan dos tipos de políticas que son (véase la figura 3.1 Definición de Políticas):

- **Políticas prohibitivas;** son aquellas en las que se prohíbe todo aquello que no se ha permitido de forma verbal o escrita.
- **Políticas permisivas;** en este tipo de política se describe todo lo que se va a prohibir pero al mismo tiempo todo lo que es permitido.

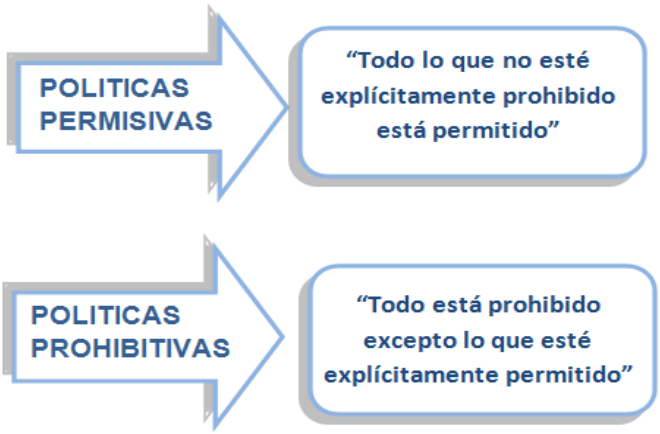


Figura 3.1 Definición de Políticas.

Al crear las políticas se debe tener presente, que la redacción tiene que ser clara, concisa, visible y distribuida tanto al personal, como al público en general, con el fin de evitar malos entendidos o bien problemas futuros.

[8] Apuntes de Seguridad Informática. López, Jaquelina y Quezada, Cintia

3.2 Seguridad lógica.

La seguridad lógica es el método utilizado para garantizar que el personal o software autorizado puede tener acceso a la información privilegiada.

Los objetivos que se plantean para lograr este fin son:

- Restricción de acceso del personal a archivos e información sensible.
- Asegurar que la información que se transmite sea recibida única y exclusivamente por el destinatario.
- Utilizar equipo de resguardo que genere copias de seguridad a distancia.

Algunas de las causas que llegan a afectar la seguridad lógica son:

- Poca o nula capacitación del personal sobre el software utilizado.
- Manipulación excesiva del software.
- Virus, software malicioso, spam.
- Ingeniería social.

Por estas y otras razones se deben crear políticas claras y precisas para la utilización, manipulación e instalación de software necesario en la organización.

3.2.1 Administración y Seguridad de acceso de usuarios.

La administración de los usuarios debe de contener distintos protocolos para garantizar el acceso y uso de los sistemas informáticos de la institución.

La seguridad de acceso de usuarios es aquella donde el administrador, debe de salvaguardar la seguridad de la base de datos que contienen la información de los distintos usuarios con acceso al sistema. Para llevar a cabo esta labor, hace uso de las herramientas que en seguida se mencionan.

3.2.2 Monitoreo de acceso a la red.

El monitoreo de acceso a la red describe el uso de herramientas utilizadas para registrar la monitorización de la red en busca de fallas en la transmisión de datos, equipo dañado o lento, para informar al Administrador de redes ya sea por mensaje de texto, aplicaciones conectadas al celular de las herramientas usadas o por correo electrónico, la forma de alerta dependerá de la aplicación y el tipo de configuración.

Algunas de las aplicaciones más usadas son:

- ***TCPDump;*** trabaja bajo el Sistema Operativo Linux, maneja una serie de herramientas que permiten monitorear por medio de la consola, el tráfico que circula por la interfaz deseada.
- ***Wireshark;*** esta herramienta trabaja bajo los Sistemas Operativos Linux y Windows, la interfaz gráfica facilita su uso y manejo.
- ***Nmap;*** herramienta utilizada tanto para monitorear la red como para obtener información del equipo (Sistema Operativo, puertos abiertos, entre otros), esto se logra con solo saber el host al que está conectado.
- ***Nagios;*** trabaja en el entorno Linux, permite configurar el tipo de monitoreo, el envío de alarmas así como la solución de manera remota desde un dispositivo móvil.

La utilización de estas herramientas permite crear políticas de acceso, creación de una base de datos de cada uno de los equipos que están conectados a la red, monitoreo constante del flujo de información, usuarios y uso de la red.

3.3 Seguridad física.

La seguridad física consiste en la aplicación de barreras físicas, protocolos de control de acceso para mantener la integridad de los equipos dispositivos de interconexión y bienes inmuebles.

Algunos de los objetivos de la seguridad física son:

- Proteger los activos de las instituciones de los desastres naturales, amenazas y/o vulnerabilidades.
- Reducir al mínimo la probabilidad de perdida, manejando un costo aceptable de recuperación de activos.
- Crear políticas de acceso para mantener el control del uso de los equipos por parte de los usuarios.

3.3.1 Seguridad física y ambiental.

La norma ISO 27000 trata de la seguridad física y ambiental, la cual menciona algunos aspectos que se deben de tomar en cuenta para prevenir desastres naturales como pueden ser:

- ***Incendios;*** son ocasionados por fallas eléctricas defectuosas, uso inadecuado de combustible, descuidos humanos con material inflamable.
- ***Inundaciones;*** son causados por instalaciones descuidadas filtraciones de agua, tuberías dañadas, estas algunas de las causas que llegan a dañar equipo de computo en las instalaciones.
- ***Sismos;*** son movimientos aleatorios de la tierra, pueden ser casi imperceptible que ni un instrumento los pueda detectar o tan intensos que pueden llegar a ocasionar destrucción de inmuebles o pérdidas humanas.
- ***Humedad;*** filtraciones constantes de agua por estructuras dañadas por el paso del tiempo o desastres naturales.

Algunas de las recomendaciones que da esta norma son:

- ***Mantener áreas seguras;*** se refiere al uso de bitácoras, listas de control de acceso del personal autorizado a areas sensibles de las instituciones.
- ***Perímetro de seguridad física;*** crear puntos de acceso que sean controlados por recepcionistas y/o sistemas automatizados Los perímetros

que contienen información relevante de la institución, deberán ser físicamente sólidos (inaccesibles en caso de amenaza).

- ***Controles de acceso físico;*** se refiere a la utilización de personal especializado en seguridad o controles automatizados de identificación.

3.3.2 Seguridad de los equipos.

La seguridad de los equipos tiene como objetivo evitar la pérdida, daño, robo o interrupción de los activos de la organización. Algunas de las recomendaciones para salvaguardar los equipos son:

- Crear políticas en contra de las amenazas físicas, lógicas y ambientales.
- Considerar la ubicación de los equipos en uso y su forma de eliminación de la organización.
- Proteger los equipos de descargas eléctricas o fallas en la misma.
- Proteger el cableado de telecomunicaciones, energía, voz y dato de posibles intercepciones.
- Dar constante mantenimiento a los equipos para detectar posibles vulnerabilidades.
- Verificar dispositivos de almacenamiento.
- El traslado de equipo debe ser con la autorización de la institución.

3.3.3 Seguridad de la información.

La Seguridad de la Información hace referencia a la prevención y protección de datos, utilizando ciertos mecanismos para evitar que de manera delimitada o accidental, exista la modificación, difusión, destrucción no autorizada de información privada de una persona o institución.

La correcta gestión de resguardo de la información permite garantizar:

- Confiabilidad.

- Integridad.
- Disponibilidad

Adicional a estos tres rubros está la autenticidad, donde la información que se envía en efecto es la misma que se recibe.

Dentro de las normas mexicanas en abril de 2014 se crea el INAI (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales), cuyas funciones principales son:

- Garantizar el derecho de acceso de las personas a la información pública gubernamental.
- Proteger los datos personales que están en manos tanto del gobierno federal, como de los particulares.
- Resolver sobre las negativas de acceso a la información que las dependencias o entidades del gobierno federal hayan formulado.

Un mecanismo importante para la seguridad de la Información es, en caso de desechar documentos importantes no se tiren en los cestos de basura, habrá que utilizar los trituradores de papel para evitar que los intrusos puedan tener acceso a dicha información.

3.4 Seguridad organizacional.

La información es un bien activo valioso, que dependiendo su manejo puede hacer crecer o destruir una organización. La seguridad organizacional dependerá de las políticas que el administrador de Redes de datos y Seguridad implemente, la bitácora de acceso a la información confidencial de la organización.

La ISO/IEC crearon la serie de normas 27000, la cual tiene como objetivo dar a conocer a nivel internacional las buenas prácticas para el manejo de la seguridad

en la organización, puesto que son las principales observaciones en esta norma son:

- Compromiso por parte de los Directores de la Organización.
- Designación de roles y actividades.
- Proceso de autorización para el manejo de la información.
- Acuerdos de confidencialidad.
- Contacto con las autoridades.
- Revisión independiente de la seguridad de la información.

3.4.1 Políticas de los usuarios.

Dentro de las organizaciones se deben manejar políticas para las distintas categorías de usuarios, las cuales dependerán de la naturaleza de sus funciones, algunas recomendaciones son:

- ***Usuarios Internos;*** proporcionar contraseñas de autenticación, acceso dactilar o facial (dependiendo del área de acceso).
- ***Usuarios externos;*** solicitud de identificación oficial, declaración de bienes que ingresen a la organización.

3.4.2 Control de equipos.

El control de equipos se puede llevar a cabo de diferentes maneras como son:

- Uso de software donde se registren los datos del equipo.
- Utilización de bitácoras (este método es efectivo para el préstamo de equipo).
- Monitoreo del equipo por el personal técnico.

Cuando se dan de baja equipos (ya sea por alguna falla, desuso o porque se adquirió un nuevo dispositivo), también se debe llevar un control.
Todo esto se hace con el fin de evitar problemas de ubicación más adelante.

3.5 Servicios de Seguridad.

La recomendación X.800 define un servicio de seguridad como un servicio proporcionado por una capa de protocolo de sistemas abiertos de comunicación, que garantiza la seguridad adecuada de los sistemas o de las transferencias de datos.[9]

El estándar ISO 7498-2 lo define un como el servicio proporcionado por un nivel de un sistema abierto que garantiza la seguridad de los sistemas abiertos: Los servicios que maneja son:

3.5.1 Autenticación

Asegurar que las entidades que establecen una comunicación sean quienes dicen ser.

a) **Autenticación del origen de los datos;** servicio aplicado a comunicaciones no orientadas a conexión donde los datos son independientes. Este servicio puede ofrecerse en aplicaciones como el correo electrónico, donde no hay comunicación previa entre entidades finales..
b) **Autenticación de entidades pares;** servicio aplicado a comunicaciones orientadas a conexión, asegura la identidad de las dos entidades que se comunican. Garantiza que no exista la suplantación en ni una de las dos entidades que se comunican.

3.5.2 Control de acceso.

El control de acceso es un procedimiento con el cual se puede verificar la autenticidad de una persona para acceder a algún lugar físico en especifico o bien el acceso autorizado a una base de datos.

[9] Fundamentos de seguridad en redes: aplicaciones y estándares, William Stallings

Los componentes del control de acceso son:

- ***Mecanismos de autenticación;*** por sí solo este mecanismo no es útil, pero es la fase inicial para que los otros dos puedan funcionar ya que permite verificar que la persona que solicita su acceso es quien dice ser.
- ***Mecanismo de autorización;*** encargado de permitir el acceso a cierta área o base de datos, después de pasar el primer filtro de autenticación.
- ***Mecanismo de trazabilidad;*** encargado de utilizar un sistema criptográfico para garantizar la seguridad a un sistema.

Se manejan dos tipos de control de acceso, control de acceso interno y control de acceso externo.

a) Control de acceso interno; determina las reglas hacia los usuarios para del uso de los sistemas internos, algunos de estos controles son:

- ***Password;*** son contraseñas que se les proporcionan a los usuarios para su acceso al sistema.
- ***Listas de control de acceso;*** llevar una bitácora donde quede registrado el acceso, tiempo de uso y salida de los usuarios.
- ***Limitación de uso;*** decidir hasta donde pueden tener acceso.

b) Control de acceso externo; medidas necesarias para permitir el acceso a usuarios externos a la institución, algunas de estas medidas son:

- ***Dispositivos de apertura automática;*** permiten el acceso únicamente a las personas que se identifiquen, cumplan con los lineamientos de acceso o bien sea solicitada su presencia en al institución.
- ***Firewall;*** (cortafuegos), implementar las políticas necesarias para denegar o permitir el acceso del flujo de datos por medio de la red. Se manejan dos tipos de control de acceso, control de acceso interno y control de acceso externo.

c) ***Control de acceso físico;*** determinar el personal que podrá tener acceso a ciertas áreas bajo control escrito, algunas medidas son:

- ***Recepción;*** primer filtro para identificar tanto a los empleados como visitantes que ingresan a la institución.
- ***Acceso a terceras personas;*** ingreso de personas ajenas a la institución que tiene como objetivo prestar sus servicios profesionales o bien solicitar los de la organización.
- ***Identificación del personal;*** toda persona que accede a la organización debe de portar su gafete de identificación, para en caso de algún incidente se pueda identificar al agresor.
- ***Guardias de seguridad;*** personal encargado exclusivamente al acceso, áreas de control estricto o bien resguardo del edificio.
- ***Firma de entrada y salida;*** política implementada por la organización que le permite crear bitácora del movimiento del personal que labora.
- ***Entradas con dobles puertas;*** mecanismo que se debe implementar para acceder al lugares restringidos y de vital importancia para la organización (en este tipo de áreas no debe estar a la vista de todos).

Figura 3.2 Métodos de Control de Acceso

3.5.3 Confidencialidad

La confidencialidad hace referencia a la capacidad de resguardar un servicio dado, impidiendo su uso, divulgación y explotación del mismo.

a) **Acuerdos de confidencialidad.**

Los acuerdos de confidencialidad son contratos que hacen entre personas y empresas, donde se comprometen a no divulgar información importante, contratos y demás documentos importantes entre ellos.

Algunas de las características que deben cumplir los acuerdos de confidencialidad son:

- Descripción del motivo del contrato.
- Datos personales de ambas partes.
- Plazo de vencimiento del contrato.
- Clausuras.
-
  - Acción legal que se llevará a cabo en caso de no cumplir con el contrato.

Figura 3.3 Contrato de confidencialidad

b) **Confidencialidad en modo con conexión:** protección de los datos del usuario en una comunicación orientada a conexión.

c) **Confidencialidad en modo sin conexión:** protección de los datos del usuario contenidos en una comunicación no orientada a conexión.

d) **Confidencialidad selectiva por elementos:** protección de campos específicos de unidades de datos tanto en una conexión orienta a conexión y no orientada a conexión.

e) **Confidencialidad del flujo de datos:** protección de datos frente a un análisis del tráfico originado por una comunicación entre entidades pares.

3.5.4 Integridad

Permite garantizar que los datos que se envían no han sufrido alguna modificación de cualquier tipo, es decir sin duplicaciones, retransmisiones o inserciones.

Cuando se detecta que la integridad de los datos ha sido violada, el servicio de integridad puede avisar que se ha producido alguna alteración dando la oportunidad de recuperar los datos originales.

a) **Integridad en modo de conexión con recuperación:** proporciona la integridad de las unidades de datos de usuarios de comunicaciones orientadas a conexión de nivel N, detectando cualquier modificación o retransmisión de datos permitiendo la recuperación en caso de ser necesario.
b) **Integridad en modo de conexión sin recuperación:** es muy semejante su funcionamiento con el punto anterior, con la diferencia de que este solo detecta las violaciones en la integridad de datos y no utiliza alguna herramienta para la recuperación de los mismos.
c) **Integración orientada a conexión sobre campos seleccionados:** encargado de proporcionar la integridad de los campos seleccionados en los datos usados por los usuarios en un bloque de conexión en especifico y determina si dichos campos han sufrido algún tipo de modificación.
d) **Integridad no oriente a la conexión:** proporciona la integridad de los datos sin conexión, puede detectar algún tipo de modificación y puede proporcionar de alguna manera limitada la detección de repetición.
e) **Integridad no orientada a la conexión de campos seleccionados:** encargada de proporciona integridad en los campos seleccionados aunque no haya conexión, determina si los campos han sufrido alguna alteración.

3.5.5 No repudio

El no repudio, garantiza que el emisor o el receptor no nieguen el envío o transmisión de datos, es decir cuando un mensaje es enviado el receptor puede

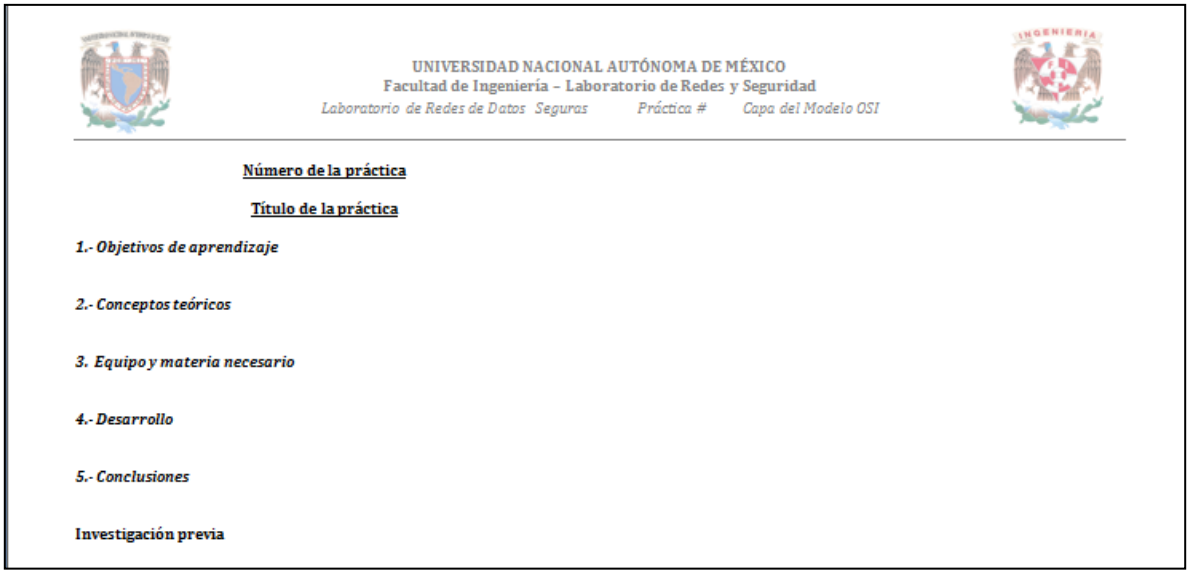
verificar quien es el emisor y a su vez el emisor no puede negar que ha enviado el mensaje y viceversa.

a) **No repudio origen:** mecanismo que envía pruebas de que el emisor en efecto es quien dice ser, el creador del mensaje sin posibilidad de error.
b) **No repudio de envío:** provee de la información necesaria del destinatario, asegurando que éste ha recibido correctamente la información.

Capítulo 4.

Manual de Prácticas del Laboratorio de Redes de Datos Seguras.

Para la realización del manual de prácticas de redes de datos seguras se tomó en cuenta el actual formato de realización de las prácticas que consta de los rubros siguientes (véase la figura 4.1):


UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
Facultad de Ingeniería – Laboratorio de Redes y Seguridad
Laboratorio de Redes de Datos Seguras *Práctica #* *Capa del Modelo OSI*

Número de la práctica

Título de la práctica

1.- Objetivos de aprendizaje

2.- Conceptos teóricos

3. Equipo y materia necesario

4.- Desarrollo

5.- Conclusiones

Investigación previa

Figura 4.1 Formato de prácticas del laboratorio de redes de datos.

En el encabezado llevará el nombre de la UNAM, Facultad de Ingeniería, nombre del laboratorio, número de práctica y la capa del Modelo OSI a la que pertenece cada práctica. Dentro del cuerpo tendrá los apartados siguientes:

1. **Número de práctica:** Todas las prácticas de la asignatura llevarán un número consecutivo, correspondiente a las semanas de clase.
2. **Título de la práctica:** El nombre de cada práctica se deberá tanto a la capa del Modelo OSI a la que corresponde así como el contenido de está.
3. **Objetivo de aprendizaje:** Se plantearan los objetivos de aprendizaje esperados de los alumnos, para que conozcan de que se tratara cada práctica que realizarán.
4. **Conceptos teóricos:** Información relevante y puntual sobre el tema de la práctica a realizar.

5. **Equipo y material necesario:** Se indicará el material necesario por parte del alumno así como el material que será proporcionado en el laboratorio de redes de datos y seguridad.
6. **Desarrollo:** Indicará el desarrollo puntual de cada práctica a realizar.
7. **Conclusiones:** El alumno anotará sus conclusiones referentes a la práctica, a los aprendizajes esperados y a sus propios aprendizajes.
8. **Investigación previa:** Se le solicitará a los alumnos información necesaria e indispensable para la realización de las prácticas.

Conforme al temario de la nueva asignatura de Redes de Datos Seguras, se llevó a cabo el análisis correspondiente de las horas asignadas por cada uno de los temas quedando la distribución de la manera siguiente:

En el tema 1, *Conceptos básicos,* el objetivo es conocer e identificar los elementos que conforman a una red de datos y los principios básicos de seguridad.

- Práctica 1. Seguridad en la red.

  Objetivo de aprendizaje:

  - El alumno conocerá el funcionamiento de la herramienta NMAP, así como el ataque ARP spoofing.

En el tema 2, *Estándares y arquitectura,* el objetivo es, dar a conocer y explicar los protocolos y estándares que se manejan en las redes de datos.

- Práctica 2. Normatividad.

  Objetivo de aprendizaje:

  - El alumno utilizará e identificará las normas y estándares para el cableado estructurado.

En el tema 3, *Capa física,* el objetivo es, dar a conocer y explicar los protocolos y estándares que se manejan en las redes de datos.

- Práctica 3. Construcción de cables UTP y jacks.

  Objetivo de aprendizaje:

  - El alumno adquirirá la capacidad de construir cables de conexión directa y cruzada con base en las normas ANSI/EIA/TIA T568-B, así como la instalación del jack en el panel de parcheo, utilizando cable UTP categoría 6 o superior.
  - El alumno realizará la conexión entre dispositivos con el cable adecuado a cada situación.

- Práctica 4. Topología de red y cableado estructurado.

  Objetivos de aprendizaje:

  - El alumno conocerá la aplicación de los estándares ANSI/EIA/TIA 568 y 569 para el diseño de una red de datos con cableado estructurado.

En el tema 4, *Capa de enlace de datos,* el objetivo es analizar, comprender y utilizar los diferentes protocolos, métodos y estándares que se utilizan en esta capa en los dispositivos de interconexión.

- Práctica 5. Compartición de archivos por Hub y Switch en Linux.

  Objetivo de aprendizaje:

  - El alumno conocerá el manejo y seguridad de los dispositivos de interconexión (hub y switch), así como la compartición de archivos por medio de estos dispositivos.
  - El alumno visualizará la colisión de los dispositivos en forma simulada, por medio del software Cisco Packet Tracer en su versión más reciente.

- Práctica 6. Creación y configuración de una VLAN.

  Objetivo de aprendizaje:

- El alumno conocerá el funcionamiento, configuración y qué son las VLAN´s por el método de MAC, así como designación por puertos, para lo cual utilizará el simulador de redes Cisco Packet Tracer en su versión más reciente.

En el tema 5, *Capa de red,* el objetivo es, analizar y comprender el funcionamiento del intercambio de información por medio de la red.

- Práctica 7. Red inalámbrica “ad hoc” y compartición de archivos en Windows.

  Objetivo de aprendizaje:

  - El alumno analizará y realizará una conexión punto a punto de forma inalámbrica, así como la compartición de archivos entre dos dispositivos, dentro del sistema operativo Windows.

- Práctica 8. Enrutamiento (estático y dinámico).

  Objetivo de aprendizaje:

  - El alumno conocerá el funcionamiento de los protocolos de enrutamiento estático y dinámico, analizará su funcionamiento dentro de una red de área local mediante el simulador de redes: Cisco Packet Tracer en su versión más reciente.

- Práctica 9. Tipos de enrutamiento (OSPF y EIGRP).

  Objetivo de aprendizaje:

  - El alumno conocerá y configurará protocolos de enrutamiento OSPF y EIGRP, analizará su funcionamiento dentro de una red de área local mediante un simulador de redes: Cisco Packet Tracer en su versión más reciente.
  - El alumno conocerá y realizará la redistribución de redes con distintos protocolos, dinámicos y estático.

En los tema 6,7 y 8, *Capas de transporte, sesión y presentación,* los objetivos son analizar y comprender los diferentes tipos de protocolos en cada una de las capas y en la unión con el resto de las capas del modelo OSI.

En el tema 9, *Capa de aplicación,* el objetivo es analizar, comprender y utilizar los diferentes protocolos, métodos y estándares que se utilizan en esta capa en los dispositivos de interconexión.

- Práctica 10. Instalación de un servidor Apache.

  Objetivo de aprendizaje:

  - El alumno desarrollará las habilidades necesarias para realizar la instalación de un servidor apache en la distribución Kali Linux.

- Práctica 11. TCP y UDP.

  Objetivo de aprendizaje:

  - El alumno configurará un programa que le permitirá enviar y recibir información utilizando los protocolos TCP y UDP, reafirmando los conceptos teóricos.
  - El alumno será capaz de crear un socket servidor y un socket cliente.

- Práctica 13. Configuración de VPN y DMZ en Packet Tracer

  Objetivo de aprendizaje:

  - El alumno conocerá el manejo eficiente de las redes públicas y privadas, utilizando las configuraciones VPN y DMZ.

Debido a lo amplio e importante de la última capa del modelo OSI, se tomó la decisión de intercalar una práctica exclusiva sobre seguridad, para da a conocer la importancia que tiene éste rubro en los Administradores de las Redes de Datos.

- Práctica 12. Ruptura de claves WPA Y WEP

  Objetivo de aprendizaje:

  - El alumno conocerá y aplicará el algoritmo para descifrar claves WPA y WEP, atacando la debilidad de su cifrado.

Conclusiones

El realizar este proyecto de tesis, me permitió ampliar mis conocimientos en el área de las redes de datos, la seguridad, las normas que las rigen, así como los protocolos correspondientes a cada capa del modelo OSI.

El objetivo principal de este proyecto, ha sido la elaboración del manual de prácticas de redes de datos seguras, siguiendo la misma línea de formato que se ha estado trabajando. Este formato incluye los siguientes rubros:

- Objetivos de aprendizaje
- Información teórica relacionada a la práctica.
- Material necesario por parte del Laboratorio de Redes de Datos y Seguridad así como por parte de los alumnos de la Facultad de Ingeniería.
- Desarrollo de las prácticas.
- Cuestionario relacionado con las prácticas
- Investigación previa por parte de los alumnos de la Facultad de Ingeniería.

Al ir desarrollando cada una de las prácticas, se pensó en los conocimientos que se desean transmitir a las nuevas generaciones, tomando en cuenta los avances tecnológicos, la importancia de la Seguridad de la Información, el manejo de las redes de datos y sobre todo el tiempo destinado a cada tema.

El uso del Modelo OSI y seguridad en la red son parte primordial del desarrollo de las prácticas como se enuncian a continuación:

Aprender el uso de las herramientas Nmap y Arp Spoofing para el monitoreo de las redes de datos así como la importancia del resguardo de la información.

- Práctica 1. Seguridad en la red.

Conocer las normas y estándares existentes en le area de las redes de datos y el cableado estructurado.

- Práctica 2. Normatividad.

En las siguientes prácticas se hace uso de la Capa Física del Modelo OSI, la creación de cables que se utilizan en el cableado estructurado, la norma vigente así como la definición de las topologías de red, su funcionamiento y características de uso.

- Práctica 3. Construcción de cables UTP y jacks.
- Práctica 4. Topología de red y cableado estructurado.

En la capa de enlace de datos del Modelo OSI, se enuncia y aplica el concepto de colisión por medio de dos dispositivos de interconexión (Hub y Switch), el uso de protocolos para la configuración de VLAN´s.

- Práctica 5. Compartición de archivos por Hub y Switch en Linux.
- Práctica 6. Creación y configuración de una VLAN.

En la capa de red del Modelo OSI, se utilizan los protocolos de enrutamiento, compartición de archivos por medio de una red inalámbrica y alámbrica en el entorno del Sistema Operativo Windows.

- Práctica 7. Compartición Red inalámbrica “ad hoc” y compartición de archivos en Windows
- Práctica 8. Enrutamiento (estático y dinámico).
- Práctica 9. Enrutamiento (estático y dinámico).

La utilización de las capas de transporte, sesión y presentación, se combina con la aplicación de las distintas prácticas ya que por sí solas es complejo el entendimiento de su función.

En la capa de capa de aplicación, la función principal es la interacción del usuario con las distintas aplicaciones que se utilizan hoy en día como servidores de correo web, servidores de bases de datos, la arquitectura cliente-servidor. De la misma manera se intercalo una práctica exclusiva de ruptura de Seguridad en los Access Point.

- Práctica 10. Instalación de un servidor Apache
- Práctica 11. TCP y UDP.
- Práctica 12. Ruptura de claves WPA Y WEP
- Práctica 13. Configuración de VPN y DMZ en Packet Tracer

La presentación de las prácticas se hace en un CD anexo, para que sea más fácil su manejo y utilización, se puede observar que se tomo en cuenta la parte proporcional del tema en teoría para que se vea reflejado en el Laboratorio de Redes de Datos y Seguridad.

Al concluir el semestre, los alumnos podrán conocer, utilizar y manejar las herramientas, el software y hardware necesario para la administración adecuada de las redes de datos. Cabe destacar que en cada práctica se buscó el uso de software adecuado para la simulación de redes así como la forma de configuración en su versión más reciente.

Anexos

1. Práctica 1. Seguridad en la red.
2. Práctica 2. Normatividad.
3. Práctica 3. Construcción de cables UTP y jacks.
4. Práctica 4. Topología de red y cableado estructurado
5. Práctica 5. Compartición de archivos por Hub y Switch en Linux.
6. Práctica 6. Compartición Creación y configuración de una VLAN.
7. Práctica 7. Compartición Red inalámbrica “ad hoc” y compartición de archivos en Windows
8. Práctica 8. Enrutamiento (estático y dinámico).
9. Práctica 9. Enrutamiento (estático y dinámico).
10. Práctica 10. Instalación de un servidor Apache.
11. Práctica 11. TCP y UDP.
12. Práctica 12. Ruptura de claves WPA Y WEP
13. Práctica 13. Configuración de VPN y DMZ en Packet Tracer

El presente anexo, se encuentra contenido en el disco adjunto a este trabajo.

Bibliografía, Referencias Electrónicas

27000, I. (2005). Obtenido de http://www.iso27000.es/

Aguilera, P. (2010). *Seguridad Informatica.* España: Editex, S.A.

Andreu, J. (s.f.). *Servicios en red.* España: Editex, S.A.

Atelin, J. D. (2006). *Redes informáticas.* España: Eni.

Autogestión. (s.f.). *Marco normativo de seguridad y salud en el trabajo*. Obtenido de http://asinom.stps.gob.mx:8145/Centro/CentroMarcoNormativo.aspx

Ayllon, B. (2011). *Colisiones*. Obtenido de http://es.slideshare.net/Betty77ma/colisiones-dominios-de-colisin-y-segmentacin

Barceló, J. M. (2008). *Protocolos y aplicaciones internet.* España: UOC.

Black, U. D. (1987). *Redes de transmisión de datos y procesos redistribuido.* España: Díaz Santos.

Boquera, M. d. (2003). *Servicios avanzados de telecomunicación.* España: Díaz de Santos.

Cantabria, U. d. (2007). *Normas, estándares, recomendaciones.* Obtenido de http://ocw.unican.es/historico-de-cursos/como-buscar-informacion-en-electronica-y/como-buscar-informacion-en-electronica-y-comunicaciones/pdf/03.pdf

Cañizares, R. (Abril de 2006). *Revistadintel*. Obtenido de www.revistadintel.es/Revista1/DocsNum02/HoyHablamosDe/SegFisica02.pdf

Castrejón, R. V. (2013). Obtenido de http://rd.udb.edu.sv:8080/jspui/bitstream/123456789/265/1/033380_tesis.pdf

Cofepris. (s.f.). *Normas Oficiales Mexicanas*. Obtenido de http://www.cofepris.gob.mx/MJ/Paginas/Normas-Oficiales-Mexicanas.aspx

Corletti, A. (2011). *Seguridad por Niveles.* España: DarFe.

EIA. (s.f.). Obtenido de http://www.eia.gov/

Enrique, H. P. (2003). *Tecnologías y redes transminisión de datos.* México: Limusa Noriega Editores.

Gema Sánches, Jorge Romero. (2010). *Servicios en red.* España: Paraninfo.

Guillermo Cicileo, Roque Gagliano, Christian O´Flaherty. (2009). *IPv6 para todos: guía de uso y aplicación para diversos entornos.* Argentina: Internet Sociedad.

IETF/RFC 1918. (s.f.). Obtenido de http://www.ietf.org/rfc/rfc1918.txt

ISO. (s.f.). Obtenido de http://www.iso.org/iso/home/about.htm

ITU. (s.f.). Obtenido de http://www.itu.int/es/about/Pages/whatwedo.aspx

Jaquelia López, Cintia Quezada. (2005). *Apuntes de seguridad informatica.* México: Facultad de Ingeniería, UNAM.

José Dordoigne, Philippe Atelin. (2007). *TCP/IP. Protocolos de internet.* España: Eni.

Joskowicz, J. (2008). *Apuntes redes de datos.* Uruguay.

Joskowicz, J. (2013). *Apuntes de cableado estructurado.* Uruguay.

López, D. O. (s.f.). *El cifrado Web (SSL/TLS)*. Obtenido de http://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls

Microsoft. (2005). Obtenido de https://msdn.microsoft.com/es-es/library/cc786282%28v=ws.10%29.aspx

Modelo OSI. (s.f.). Obtenido de http://blyx.com/public/docs/pila_OSI.pdf

Normas de las comunicaciones de red. (2011). Obtenido de https://sites.google.com/site/stigestionydesarrollo/recuperacion/desarrollo-1/recuperacion-tema-2---desarrollo/4

Oracle. (s.f.). *Inbtroducción al conjunto de protocolos TCP/IP*. Obtenido de http://docs.oracle.com/cd/E24842_01/html/820-2981/ipov-6.html

Osvaldo Solis, Daniel Zavadszky. (2009). *Comunicación de datos y redes de Pc´s.* Uruguay.

Pantaleon, M. E. (2003). *Apuntes redes de datos y conectividad.*

Prat, D. d. (s.f.). *Aprende DNS y Apache.* Klinde.

Redes de datos. (2010). Obtenido de https://sites.google.com/site/comdatosgrupo4/contenidos/cap5_arendredes#TOC-An-lisis-de-Trafico-en-Redes-Locales

Redes locales globales. (s.f.). Obtenido de https://sites.google.com/site/redeslocalesyglobales/home

social, S. d. (13 de noviembre de 2014). *Reglamento Federal de Seguridad y salud en el trabajo*. Obtenido de http://asinom.stps.gob.mx:8145/upload/RFSHMAT.pdf

Stalling, W. (2004). *Comunicaciones y redes de computadoras.* (7ma., Ed.) Madrid, España: Pearson Educación, S.A.

Stalling, W. (2004). *Fundamentos de seguridad en redes, Aplicaciones y estándares* (2° ed.). Madris, España: Pearson Educación.

Tecnología UIB. (s.f.). Obtenido de http://tecnologiauib.com/es/portfolio/show/protocolo-de-resolucion-de-colisiones-para-redes-de-comunicaciones-de-acceso-aleatorio/15

Tena, J. G. (s.f.). *Protocolos criptográficos y seguridad en redes.* Santander: Servicio de publicaciones de la Universidad sw Cantabria.

UNAM. (s.f.). *Las 10 normas más importantes sobre seguridad industrial*. Obtenido de http://www.ingenieria.unam.mx/~guiaindustrial/seguridad/info/2/1.htm

Xatakaon. Tecnologías de redes. (2011). Obtenido de http://www.xatakaon.com/tecnologia-de-redes/nat-network-address-translation-que-es-y-como-funciona

Glosario

ACL	(Access Control List)Listas de control de acceso
Amenaza	Son hechos intencionales o no intencionales de dañar a un dispositivo, persona, institución, organización o equipo de cómputo.
ANSI	Acrónimo de Instituto Nacional Estadounidense de Estándares
Anycast	Es una forma de direccionamiento en la que la información es enrutada al mejor destino posible dentro de una red.
ARP	(Address Resolution Protocol); es un protocolo encargado de traducir direcciones MAC en direcciones IP.
Ciberatacantes.	Se refiere a personas cuya función, es monitorear la red en busca de vulnerabilidades en los distintos equipos de cómputo y crear ataques cibernéticos.
Cifrado	Procedimiento que utiliza algoritmos para proteger la información y no viaje en claro.
Colisión	Es cuando dos paquetes tratan de pasar por un mismo punto al mismo tiempo.
Confidencial	Hace referencia a la capacidad de resguardar un servicio dado, impidiendo su uso, divulgación y explotación del mismo.
Dirección IP	(Internet Protocol); son cuatro octetos de números únicos e irrepetibles, para identificar los dispositivos conectados a una red.
Dirección MAC	Es un número serial único e irrepetible de los diferentes dispositivos
Disponibilidad	Permite garantizar que la información o bien este siempre visible para su uso.
Dispositivos	Periféricos utilizados en el funcionamiento de los

	equipo de cómputo.
DNS	Sistema de nomenclatura jerárquica para determinar nombres a las diferentes direcciones existentes en internet o alguna red privada
EIA	Acrónimo de Alianzas de Industrias Electrónicas
Encaminamiento	Es un procedimiento utilizado para encontrar la ruta más optima en el ámbito de las redes de datos.
Enlace	Vínculo que existe entre dos nodos, para que exista una comunicación.
Enlace multimodo	Conexión de un punto hacia varios equipos o dispositivos que se interconectan para que exista un flujo de información.
Enlace punto a punto	Conexión entre dos equipos en un instante mientras no haya alguna interferencia
FTP	Protocolo de transferencia de archivos, utiliza la conexión cliente/servidor, donde el cliente efectúa transferencias directas de un servidor a otro.
Hardware	Es la parte física que compone a los equipos de cómputo.
Host	Son nodos que funcionan como punto inicial y final de una conexión que hacen uso de servicios a internet y transferencia de datos.
HTTPS	Protocolos utilizados en sistemas de redes, permite la transferencia de información del lenguaje HTLM desde servidores web a navegadores.
IANA	(Internet Assigned Numbers Authority) organismo encargado de administrar las direcciones IPv4.
Integridad	Permite garantizar que los datos que se envían no han sufrido alguna modificación de cualquier tipo, es decir sin duplicaciones, retransmisiones o inserciones.

IP	(Internet Protocol), protocolo de Internet, existen actualmente dos versiones IPv4 e IPv6.
ITU	Unión Internacional de Telecomunicaciones organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), tiene como objetivo regular las telecomunicaciones a nivel internacional en conjunto con empresas públicas y privadas
ITU	Acrónimo de Unión Internacional de Telecomunicaciones
LANIC	(Latin America & Caribbran Network Information Centre)
Modelo OSI	(Open System Interconnection), es un modelo creado en 1984 por la ISO (International Organization Standardization) con el fin de normalizar la comunicación de redes de datos.
Monomodo	Utilizado en la fibra óptica, se refiere a que la luz se propaga únicamente por un modo.
Multicast	Envío de información por múltiples canales por medio de la red.
Multimodo	Utilizado en la fibra óptica, se refiere a que la luz se propaga por varios modos.
NIC	(Network Information Center), es la autoridad que se encarga de delegar los nombres de los dominios de cada país.
Nodo	Punto de intersección donde se unen dos o más elementos de red.
Políticas	Es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma

Protocolo	Conjunto de reglas o métodos para que dos procesos intercambien información
Puerto	Son interfaces por las cuales se pueden enviar y recibir diferentes datos, pueden ser de tipo físico (entradas de usb, interface, entre otras) o lógicos (puertos de internet).
Seguridad	Característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo.
Seguridad de la Información	Hace referencia a la prevención y protección de datos importantes para cualquier persona u organización.
Seguridad Física	Consiste en la aplicación de barreras físicas, protocolos de control de acceso para mantener la integridad de los equipos dispositivos de interconexión y bienes inmuebles
Seguridad Informática	Se define como un conjunto de medidas que impidan la ejecución de operaciones no autorizadas sobre un sistema o red informática, estas medidas son un conjunto de reglas, planes, actividades y herramientas.
Seguridad lógica	conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma
Software	Conjunto de programas encargados de hacer funcionar los distintos equipos electrónicos.
SSL	(Secure Socket Layer) es un protocolo criptográfico, que permiten que la comunicación sea segura y viaje cifrada.
SYN	Bit de control dentro del segmento TCP, utilizado para sincronizar los numero secuenciales iniciales.
Tarjetas de red	(Network Interface Card), tarjeta encargada de conectar

	distintos dispositivos entre sí.
Tasa de transferencia	Número de bits, que se transmite en una unidad de tiempo (bits/segundo) bps.
TCP	Transmission Control Protocol), es un protocolo orientado a conexión
TELNET	Basado en el protocolo TCP, crea una conexión tipo cliente/servidor y es útil en el manejo de maquinas virtuales
TIA	Acrónimo de Estándares de Infraestructura de Telecomunicaciones.
Topología de red	Se define como la forma física o lógica de comunicar estaciones de trabajo individuales, por muros, techos y suelos, a través del tendido de cable o conexiones lógicas.
Trama	Son unidades de envío de datos, son series sucesivas de red organizadas en forma cíclica
TTL	(Time To Live) es una herramienta de la capa red y es utilizada por la capa de transporte en el protocolo TCP.
UDP	User Datagram Protocol), es un protocolo no orientado a conexión
Unicast	Envío de información por un canal por medio de la red.
Vulnerablidad	Por vulnerabilidad se entiende como un riesgo latente existente en un sistema.

PRÁCTICA 1

Seguridad en la red

1.- Objetivos de aprendizaje

- El alumno conocerá el funcionamiento de la herramienta NMAP, así como el ataque ARP spoofing de monitoreo.

2.- Conceptos teóricos

El caso de estudio proporcionado por el profesor requiere saber cuáles de sus equipos cumplen con los requisitos mínimos indispensables de seguridad (firewall, antivirus, entre otro software). De la misma manera, se solicita que se encuentren monitoreadas las páginas a las que accede su personal.

Nmap es una aplicación de código abierto que sirve para rastrear puertos; permite evaluar la seguridad de sistemas informáticos, así como descubrir servicios en una red de datos.

Algunas características de esta aplicación son:

- Descubre todos los equipos conectados a la red, así como las versiones de sus sistemas operativos.
- Identifica los puertos abiertos con la dirección IP obtenida.
- Obtiene la dirección MAC de los dispositivos en red.
- Puede usarse solo o como antesala para preparar otro ataque.

Esta herramienta la utilizan algunos administradores de red para buscar fallas dentro de sus propias redes o para detectar dispositivos que no cumplen con los requisitos mínimos de seguridad.

Los hosts son nodos que funcionan como punto inicial y final de una conexión que hacen uso de servicios a internet y transferencia de datos.

Lo puertos son interfaces por las cuales se pueden enviar y recibir diferentes datos, pueden ser de tipo físico (entradas de usb) o lógicos (puertos de internet).

Las tramas son unidades de envío de datos, son series sucesivas de red organizadas en forma cíclica.

La dirección IP (Internet Protocol); está formada por octetos de números únicos e irrepetibles, para identificar los dispositivos conectados a una red.

La dirección MAC es un número serial único e irrepetible de los diferentes dispositivos.

ARP (Address Resolution Protocol); es un protocolo encargado de traducir direcciones MAC en direcciones IP. Las tablas ARP pertenecen a la capa 2 del modelo OSI

ARP spoofing

El ARP spoofing o envenenamiento de tablas ARP, es una técnica que altera las tablas ARP mediante tramas ARP modificadas. El objetivo del ataque es suplantar hosts, monitorear o bloquear el tráfico de red.

Por medio de este ataque se puede obtener información sensible, por ejemplo vulnerabilidades del sistema operativo que permitan realizar una intrusión a su equipo.

3.- Equipo y material necesario

Equipo del laboratorio:

- 1 Computadora con un sistema operativo Kali Linux (local o booteable).
- 1 Computadora con un sistema operativo Windows 7 Profesional.
- 1 NIC inalámbrica en cada equipo.
- 1 Router Inalámbrico.

Nota para el laboratorio: Se requiere construir y configurar una red inalámbrica controlada, por medio de la cual los equipos se conectarán y realizarán las pruebas de monitoreo (Ver Figura No. 1).

Nota para el profesor: El grupo se dividirá en dos secciones (atacantes y objetivos) la división dependerá del tamaño del grupo.

Figura No. 1 Creación de la LAN.

4.- Desarrollo

4.1 Sección A: atacados.

4.1.1 Inicie sesión en el sistema operativo Windows y navegue en Internet, según le indique su profesor, para observar los resultados en la máquina atacante

4.2 Sección B: atacantes.

4.2.1 Inicie el equipo en Kali Linux (por medio de una memoria booteable). Una vez ejecutado el sistema, abra una terminal, para ello, de clic en Aplicaciones > Accesorios > Terminal (Ver la figura No. 2)**.**

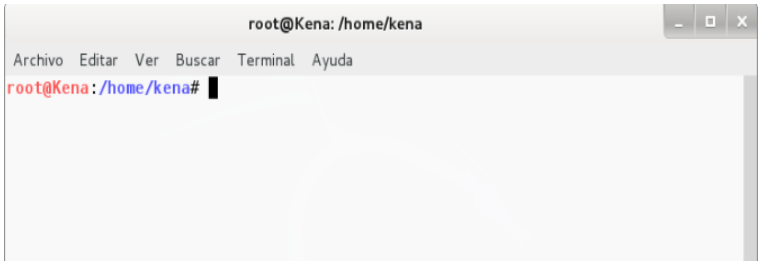


Figura No. 2 Terminal de Kali Linux.

Nota: Al momento de bootear la máquina, el sistema operativo Kali Linux trabaja con los permisos de super usuario.

4.2.2 Es necesario obtener la dirección IP de su equipo de cómputo, para ponerla en escucha de todo lo que pasa en ese segmento de red. Para obtener la dirección IP de su equipo escriba el siguiente comando (Ver figura No. 3):

 # ifconfig

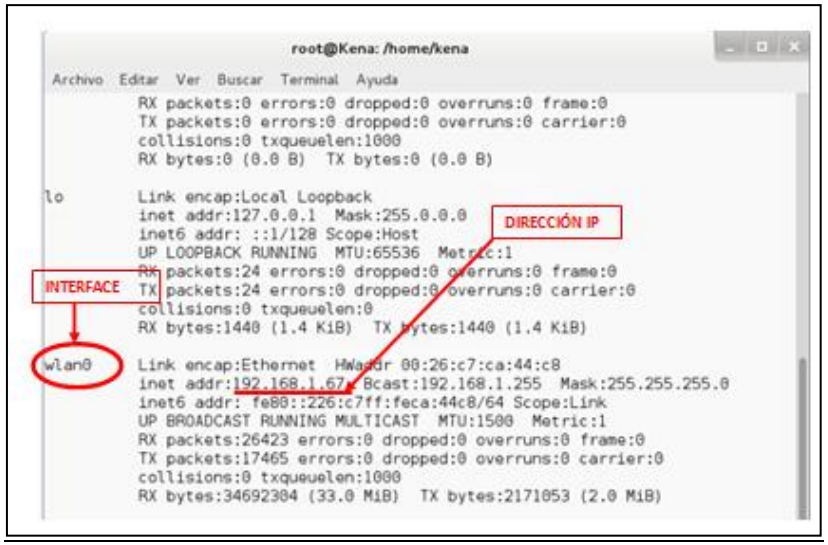


Figura No.3 Dirección IP e interface.

4.2.3 Para habilitar la interface en modo promiscuo o en modo monitor, con la finalidad de que la interface se encuentre a la escucha de todo lo que pasa en ese segmento, escriba la siguiente instrucción:

#airmon-ng start ***INTERFACE***

Donde ***INTERFACE*** será la interface inalámbrica del equipo en la cual está trabajando (Ver figura No. 3).

4.2.4 Con el siguiente comando escaneará la red, observando los puertos que tiene levantados.

#nmap ***SEGMENTO _DE _RED/PREFIJO***

Donde el **SEGMENTO DE RED** y su **PREFIJO** serán proporcionados por el profesor.

Nota para el profesor: Deberá utilizar un segmento que pertenezca a la clase C. Recuerde cambiar las direcciones IP para que estén dentro del mismo segmento.

I. Analice los resultados obtenidos. Justifique su respuesta

4.2.5 El profesor indicará qué dirección IP (IP ADDRESS) se atacará.

4.2.6 Una vez obtenido el host a atacar ejecute los siguientes comandos e indique qué acción realiza.

a) #nmap –O ***IP ADDRESS***

*b) #nmap –sT **IP ADDRESS***

*c) #nmap –sU **IP ADDRESS***

*d) #nmap –sP **IP ADDRESS***

*e) #nmap –Pn **IP ADDRESS***

4.3 Ataque ARP spoofing.

4.3.1 La dirección IP del router indicará cual es la puerta de enlace para realizar la suplantación de host en el ataque ARP spoofing de monitoreo permite ara realizar el ataque se debe obtener la dirección IP del router con el siguiente comando (Ver figura No. 4):

#ip route show

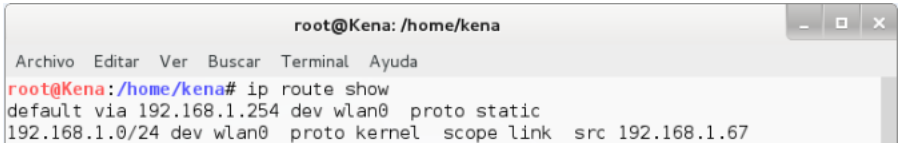


Figura No.4 Obtención de la IP del router.

4.3.2 Verifique la tabla de enrutamiento con el siguiente comando (Ver figura No. 5):

#arp -a

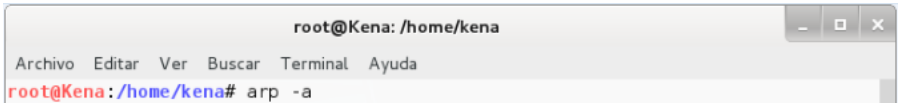


Figura No.5 Tabla arp.

II. Analice los resultados obtenidos. Justifique su respuesta.

4.3.3 Abra una nueva terminal. Para reenviar los paquetes a los verdaderos destinatarios, ingrese el siguiente comando:

#echo 1 > /proc/sys/net/ipv4/ip_forward

Verifique dicha instrucción mediante el siguiente comando, y comente el resultado obtenido:

#cat /proc/sys/net/ipv4/ip_forward

4.3.4 Abra una tercera terminal en donde realizará el ataque ARP spoofing

#arpspoof -i ***INTERFACE –t GATEWAY IP_ADDRESS***

Donde **INTERFACE** corresponde a la interface de red del atacante, **GATEWAY** es la dirección del router que obtuvo en el punto 4.2.1, **IP_ADDRESS** es la dirección IP de la máquina atacada.

4.3.5 Abra el software Wi*reshark* desde línea de comandos mediante el siguiente comando:

#wireshark

Active el servicio y seleccione la interfaz adecuada (Ver figura No. 6)

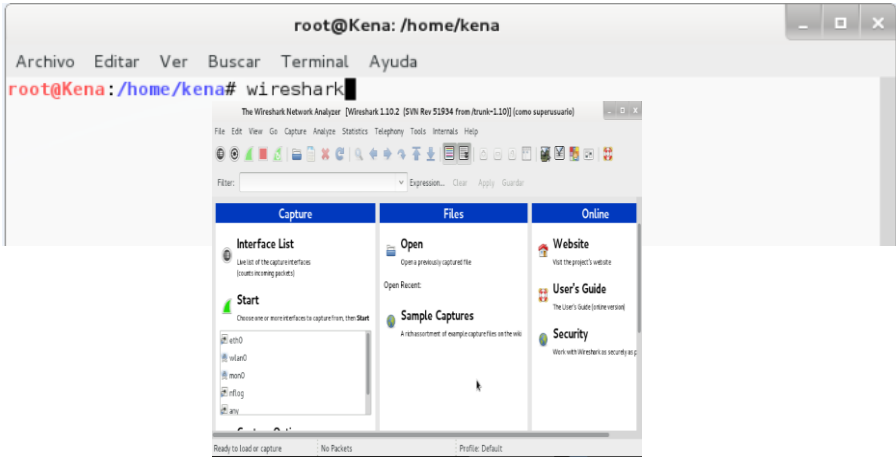


Figura No. 6 Interfaz wireshark.

4.3.6 La siguiente instrucción le permite escuchar lo que pasa a través de la red.

 # ettercap -T -i ***INTERFACE -P dns_spoof -M arp / GATEWAY / / IP_ADDRESS /***

Donde **INTERFACE** corresponde a la interface de red del atacante, **GATEWAY** es la dirección del router que obtuvo en el punto 4.2.1, **IP_ADDRESS** es la dirección IP de la máquina atacada (Ver figura No. 7 y No. 8).

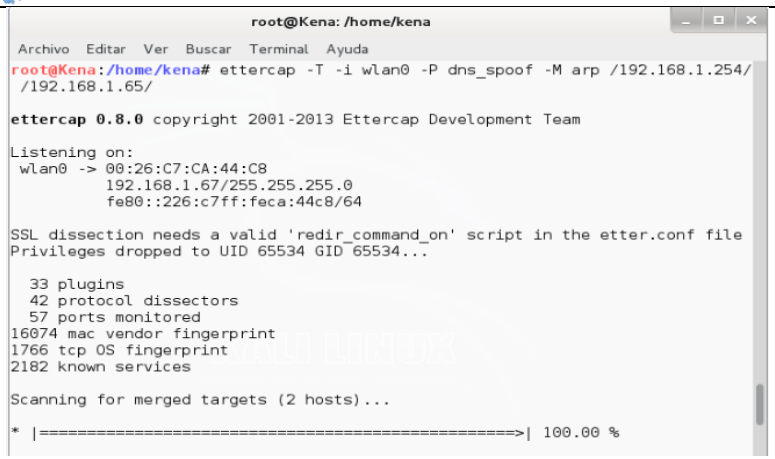


Figura No. 7 Interface ettercap.

Figura No. 8. Capta la actividad de la máquina atacada.

III. Analice los resultados obtenidos. Justifique su respuesta.

Nota final: Una vez realizada la práctica intercambiar lugares, es decir los atacantes seran los objetivos y los objetivos serán los atacantes

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

PRÁCTICA 1

Seguridad en la red

Cuestionario Previo

***Nombre del alumno:*_____**

***Gpo. de Laboratorio:*_____ *Gpo. de Teoría:*_____**

1. Indique la función de la aplicación NMAP.
2. ¿Cuál es la diferencia entre una dirección IP y una dirección MAC?
3. Mencione al menos 5 opciones para utilizar la aplicación NMAP.
4. Indique la importancia de la seguridad en su equipo.

PRÁCTICA 2

Normatividad y estándares

1.- Objetivos de aprendizaje

- El alumno utilizará e identificará las normas y estándares para el cableado estructurado.

2.- Conceptos teóricos

Las normas de redes son descripciones técnicas con el fin de lograr una intercomunicación uniforme entre diferentes dispositivos.

En la actualidad existen organismos encargados de crear normas y estándares para la construcción y creación del cableado estructurado.

a) **ANSI (American National Standards Institute).** Es la encargada de supervisar el desarrollo para productos, servicios, procesos y sistemas en los Estados Unidos.

b) **TIA (Telecomunications Industry Association).** Encargada de mejorar el entorno de las diferentes industrias de la comunicación.

c) **EIA (Electronic Industries Alliance).** Encargada de promover el mercado y la alta tecnología en los Estados Unidos.

d) **ISO (International Organization for Standardization).** Es una organización encarga de promover estandares a nivel internacional de creación, construcción y aplicación de las ramas de servicios de telecomunicaciones, construcciones, entre otras.

Existen más normas encargadas de la creación de manuales, documentos y estándares para la calidad y seguridad de servicios.

3.- Equipo y material necesario

Equipo del laboratorio:

- Computadora con un sistema operativo Windows 7 Profesional.

4.- Desarrollo

4.1.1 Investigue y describa otras normas existentes en el área de las redes de datos y telecomunicaciones.

4.1.2 ¿Cuál es la utilidad del uso de las normas y estándares?

4.1.3 Ingrese a la página www.rfc-editor.org, describa brevemente su contenido.

4.1.4 Investigue y describa la función de la IANA.

4.1.5 Visite la siguiente página www.ietf.org e indique cuál es su función.

4.1.6 Menciona qué norma hace referencia a la etiquetación por colores y descríbala brevemente.

4.1.7 Con base en la norma del punto 4.1.6, describa brevemente cuál es el uso de cada color.

4.1.8 En el laboratorio de redes y seguridad, indique en qué puntos se cumple la norma ANSI/EIA/TIA 606

_____

_____

_____

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

_____

_____

_____

_____

_____

_____

_____

_____

_____

PRÁCTICA 2

Normatividad y estándares

Cuestionario Previo

Nombre del alumno:_____

Gpo. de Laboratorio:_____ ***Gpo. de Teoría:***_____

1. Indique la diferencia entre normas y estándares.
2. Mencione las ventajas y desventajas de utilizar normas.
3. ¿Cuáles son las normas y estándares que se utilizan en México?
4. Indique las normas internacionales para el cableado estructurado.

PRÁCTICA 3

Construcción de cables UTP y jacks.

1.- Objetivos de aprendizaje

- El alumno adquirirá la capacidad de construir cables de conexión directa y cruzada con base en las normas ANSI/EIA/TIA T568-B, así como la instalación del jack en el panel de parcheo, utilizando cable UTP categoría 6 o superior.
- El alumno realizará la conexión entre dispositivos con el cable adecuado a cada situación.

2.- Conceptos teóricos

La construcción del cable de red UTP de conexión directa se utiliza para conectar la tarjeta de red, o NIC, de la estación de trabajo al jack de datos, o también para conectar el patch panel a un switch. El cable de conexión cruzada sirve para conectar dos dispositivos del mismo tipo.

Para mantener la seguridad física de la infrsestructura de red, se deben tomar en cuenta las siguientes recomendaciones:[1]

a) **Respaldo de datos**: Generar copias de la información de los diferentes sistemas, en lugares seguros o servidores especiales para dicho caso.
b) **Detectores de humo**: Son alarmas diseñadas para detectar la presencia de humo en el aire, activando una señal acústica.
c) **Sistema de alimentación ininterrumpida (SAI)**: Es un dispositivo que convierte la corriente continua en corriente alterna. Si se interrumpe la fuente de alimentación primaria, el SAI asegurará que no se pierda la corriente electrica en los equipos.
d) **Acceso restringido**: Acción de permitir ingresar a personas en ciertos ámbitos como académicos, científicos o políticos.
e) **Alarmas contra intrusos**: Alarmas diseñadas para detectar individuos ajenos a lugares restringidos.

3.- Equipo y material necesario

Material por alumno:

- 6 metros de cable UTP Cat.6 o superior.
- 10 conectores RJ-45.
- 1 conector hembra (*jacks*) RJ-45.
- Flexómetro.

Equipo del laboratorio (Ver Figura No. 2)***:***

- 1 Pinzas engarzadoras.
- 1 pinza de impacto.
- 1 panel de parcheo.
- 1 Pinzas de corte.
- 1 Pinzas de punta.
- 1 Analizador de continuidad de cableado UTP o *tester.*

[1] Purificación Aguilar López, Seguridad informática.

Figura No. 2. Material necesario

4.- Desarrollo:

4.1 Construcción de cables

El cable categoría 6 o superior está formado de cuatro pares trenzados formando una sola unidad. Estos cuatro pares vienen recubiertos por un tubo de plástico que mantiene el grupo unido mejorando la resistencia ante interferencias externas. Es importante notar que cada uno de los cuatro pares tiene un color diferente, pero a su vez, cada par tiene un cable de un color específico y otro cable blanco con algunas franjas del color de su par.

Esta disposición de los cables permite una adecuada y fácil identificación de los mismos, con el objeto de proceder a su instalación. (Ver Figura No. 3)

A continuación se construirá un cable de conexión directa de acuerdo con la configuración T568-B.

4.1.1 Cable de conexión directa T568-B

4.1.1.1 Corte un trozo de cable de par trenzado no blindado categoría 6 o superior, de una longitud de 2 metros.

4.1.1.2 Retire 3 cm de la envoltura de uno de los extremos del cable.

4.1.1.3 Sostenga la envoltura y el cable, destrence y ordene los pares de hilos de modo que cumplan con el diagrama de color del cableado T568-B (Ver Figura No. 3).

Figura No. 3. Configuración del cableado T568-B

4.1.1.4 Aplane, enderece y haga coincidir los hilos, luego recórtelos en línea recta con una distancia de 3mm a partir del borde del forro (Ver Figura No. 4).

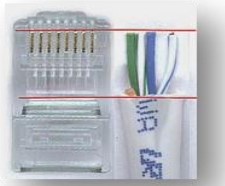


Figura No. 4 Distancia de corte de los alambres.

4.1.1.5 Coloque un conector RJ-45 en el extremo del cable, de tal forma que se cumpla la configuración correcta mostrada en la Figura No. 3.

4.1.1.6 Empuje suavemente los hilos dentro del conector hasta que pueda ver los extremos de cobre de éstos a través del extremo del conector. Asegúrese de que el extremo de la envoltura del cable también esté dentro y de que todos los hilos estén en el orden correcto (Ver figura No. 5).

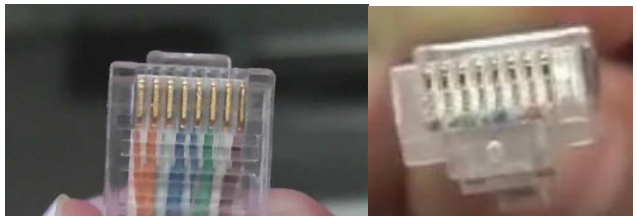


Figura No.5. Alambres y forro en el lugar adecuado dentro del conector

4.1.1.7 Utilice las pinzas engarzadoras (Ver Figura No. 6) y apriete el conector con suficiente fuerza como para forzar los contactos a través del aislamiento en los hilos, completando así el camino conductor.

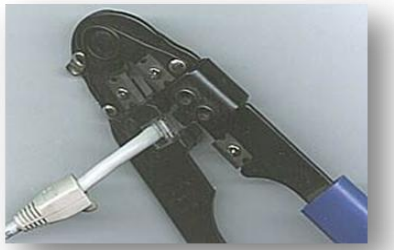


Figura No. 6 Uso de las pinzas engarzadoras

4.1.1.8 Finalizando así la construcción de un extremo del cable (Ver Figura No.7).

Figura No. 7. Cable de conexión finalizado.

4.1.2 Cable de conexión cruzada (crossover) gigabit ethernet.

4.1.2.1 Repita desde el paso 4.1.1.1 hasta el paso 4.1.1.7, ordenando los pares de hilos de acuerdo con el estándar de cableado Gigabit Ethernet, que se le solicitó en la investigación previa.

5.- Pruebas

5.1 Finalmente pruebe los cables terminados empleando el tester.

5.2 En las pruebas de continuidad del tester; si falla una conexión, el cable estará mal construido, por lo que tendrá que rehacerse nuevamente.

6.- Instalación del jack RJ-45

6.1 A continuación se explicará la instalación del Jack RJ-45 utilizando la configuración según la norma T658-B.

6.2 Corte un trozo de cable de par trenzado no blindado categoría. 6 o superior, de una longitud de 1 metro.

6.3 Retire 3 cm del forro de ambos extremos del cable .

6.4 Destrence los hilos e insértelos en cada uno de los canales del jackRJ-45 siguiendo la configuración T568-B en el Jack (Ver figura No. 8).

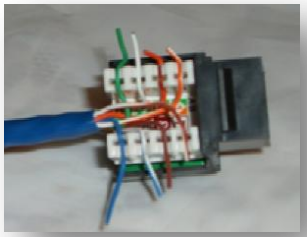


Figura No. 8. Construcción de Jack.

6.5 Utilice la pinza de impacto para introducir los hilos del cable hasta el fondo de cada canal y para cortar el excedente de cable (Ver Figura No. 9)

Figura No. 9 Uso de las pinzas de Impacto.

7 Instalación del panel de parcheo

7.1 La instalación se llevará a cabo según lo que indique el profesor.

8.- Actividad a realizar

8.1 Realice la conexión entre dispositivos con el cable adecuado.

Cable directo ——————— Cable cruzado — — — —

9.- Cuestionario

1. Realice el diagrama representando la conexión del Jack con el patch panel.

2. Indique, además de los mencionados en la práctica, otros factores para mantener seguros los elementos físicos del cableado estructurado.

3. Enliste los componentes del cuarto de equipos y del cuarto de telecomunicaciones.

4. ¿Un cable de conexión cruzada a un Gigabit Ethernet se puede utilizar en dispositivos a 100 mbs? ¿Por qué?

_____

_____

_____

_____

10- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

_____

_____

_____

PRÁCTICA 3

Construcción de cables UTP y jacks

Cuestionario Previo

Nombre del alumno:_____

Gpo. de Laboratorio:_____ ***Gpo. de Teoría:***_____

1. Investigue el diagrama de color para la elaboración del cable cruzado Gigabit Ethernet.
2. Indique los tipos de cable utilizados para realizar conexión entre dispositivos.
3. Mencione otras normas utilizadas para la creación de cables UTP
4. Indique la diferencia entre el cable UTP de la categoría 5e y categoría 6.

PRÁCTICA 4

Topología de red y cableado estructurado

1.- Objetivos de aprendizaje

- El alumno conocerá la aplicación de los estándares ANSI/EIA/TIA 568 y 569 para el diseño de una red de datos con cableado estructurado.

2.- Conceptos teóricos

El cableado estructurado es una topología física de red, con un tiempo de vida útil de diez a quince años. Es flexible y capaz de soportar cambios y crecimientos futuros.

La implementación de este sistema reduce costos en la instalación y el mantenimiento así como la facilidad de incorporar nuevos sistemas.

El diseño del sistema de cableado es independiente de la información que se transmite a través de él, de este modo es posible disponer de servicio de datos, voz, video, audio, seguridad, control y monitoreo.

La norma ANSI/EIA/TIA 568-A contiene los siguientes subsistemas para el cableado estructurado (Ver Figura No. 1):

1. Subsistema de cableado horizontal.
2. Subsistema de cableado vertical (backbone).
3. Subsistema de área de trabajo.
4. Subsistema de cuarto de telecomunicaciones.
5. Subsistema de cuarto de equipos.
6. Subsistema de entrada de servicios.

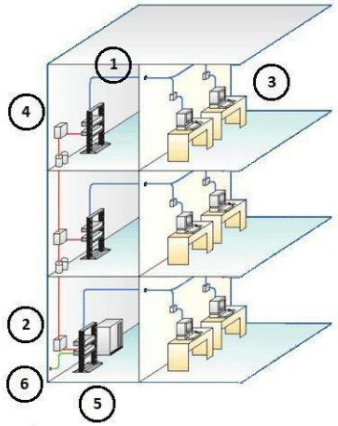


Figura No.1. Subsistemas del cableado estructurado.

Las redes también se pueden clasificar de acuerdo con su topología física; ésta define la representación geométrica de todos los enlaces de una red y los dispositivos físicos enlazados entre sí. Las principales son (Ver Figura No. 2):

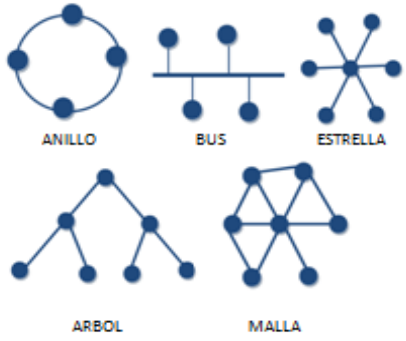


Figura No.2. Topologías de red.

a) **Topología de bus**
b) **Topología de estrella**
c) **Topología de anillo**
d) **Topología jerárquica**
e) **Topología de malla**

Nota: La topología que se utilizará dependerá de las necesidades que el cliente (el profesor) solicita en el proyecto. Se debe analizar el grado de escalabilidad tomando en cuenta las instalaciones y los avances de los medios de telecomunicación.

3.- Equipo y material necesario

Material del alumno:

- Planos del proyecto indicados por el profesor.
- Colores (bolígrafos, lápices, marcadores).
- Hojas blancas

Equipo del Laboratorio:

- 1 Computadora con un sistema operativo Windows 7 Profesional.

4.- Planos:

Con base en los planos del proyecto, determine la ubicación de los subsistemas del cableado estructurado, tomando en cuenta las siguientes consideraciones:

Nota para el profesor: Los Planos deberán ser de un edificio de dos pisos como máximo. Se anexa la imagen de una sugerencia.

Sugerencia de planos.

- Los cuartos de equipos deben ser accedidos únicamente por personal autorizado.
- El equipo de contingencias (barreras contra fuego, extintores, entre otros) debe ser visible y de fácil aspecto.
- La red eléctrica debe de estar asilada de la red de datos.

Las siguientes áreas se deben de representar en los planos proporcionados.

- Área de vigilancia.
- Recepción o módulo de información.
- Servicio de Wi Fi en áreas comunes.
- Área de trabajo con un número de equipos proporcionados por el profesor.

4.1 Costo de la propuesta del cableado estructurado.

4.1.1 Con base en su investigación previa, en hojas blancas realice la cotización de su propuesta de cableado estructurado. Justique su propuesta ante el grupo.

4.1.2 Analice las propuestas mencionadas e indique qué tan factible fue su propuesta. Justifique su respuesta.

5.- Cuestionario

1. ¿Qué topología utilizó para su propuesta? Argumente su respuesta.

2. ¿Cuáles son las ventas y desventajas de la topología mencionada en la pregunta anterior?

3. Anexe en hojas blancas un cuadro donde mencione las ventajas y desventajas de usar fibra óptica o cable de par trenzado.

   Nota para el profesor. Las ventajas y desventajas se deben basar en las normas internacionales.

FIBRA OPTICA		*CABLE PAR TRENZADO*	
VENTAJAS	*DESVENTAJAS*	*VENTAJAS*	*DESVENTAJAS*

6.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

PRÁCTICA 4

Topología de red y cableado estructurado

Cuestionario Previo

Nombre del alumno: _____

Gpo. de Laboratorio: _____ ***Gpo. de Teoría:*** _____

1. Investigue el material necesario para realizar un cableado estructurado.
2. Investigue los costos de la lista de material que obtuvo en el punto anterior.
3. Investigue las normas en el cableado estruturado.
4. Mencione las normas de seguridad para el cableado estructurado en edificios comerciales.

PRÁCTICA 5

Compartición de archivos por Hub y Switch en Linux

1.- Objetivos de aprendizaje

- El alumno conocerá el manejo y seguridad de los dispositivos de interconexión (hub y switch), así como la compartición de archivos por medio de estos dispositivos.
- El alumno visualizará la colisión de los dispositivos en forma simulada por medio del software Cisco Packet Tracer en su versión más reciente.

2.- Conceptos teóricos

Para un administrador de red, es necesario e indispensable conocer los equipos, mecanismos y técnicas para extender las capacidades de las redes que están bajo su cargo. En algunas ocasiones es necesario extender físicamente una red para añadir nuevas estaciones así como para interconectarlas a una LAN con localización geográfica distinta. De igual forma, es conveniente planear el crecimiento de una LAN en términos de ancho de banda para hacer frente a necesidades de comunicación actuales.

La extensión de las capacidades de una red, se logra mediante dispositivos hardware definidos para cada uno de los tipos de redes, en el caso de las LAN encontramos los *hubs*, *switches*, repetidores, puentes, *access point*; para las redes *MAN*, tenemos repetidores, canalizadores, módems analógicos, modéms cable; en el caso de las redes **WAN**, encontramos routers, multicanalizadores, módems satelitales, etc.

Hub

Dispositivo que opera en la capa 1 del modelo OSI que tiene la finalidad de interconectar a los dispositivos finales en una red de datos mediante la transmisión de paquetes a todos y cada uno de los hosts conectados no importándole cuál sea el destinatario.

El *hub* es un dispositivo activo que actúa como elemento central. Cada estación se conecta al *hub* mediante dos enlaces: transmisión y recepción. El *hub* actúa como un repetidor: cuando transmite una única estación, el *hub* replica la señal en la línea de salida hacia cada host conectado. Regularmente el enlace consiste en dos pares trenzados no apantallados. Dada la alta velocidad y baja calidad de transmisión del par trenzado no apantallado, la longitud de un enlace está limitada a un entorno de 100m. Como alternativa se puede usar un enlace de fibra óptica en cuyo caso la longitud máxima dependerá si es multimodo (2 km) o monomodo (300 km) aproximadamente.

Varios niveles de hub se pueden colocar en cascada formando una configuración jerárquica, teniendo un hub raíz denominado HUB. Encabezado Hub (Header Hub) y uno o más hubs intermedios denominados IHUB, Hub Intermedios (Intermediate Hub). Esta estructura se adecúa bien a edificios cableados donde regularmente existe un armario de interconexiones en cada planta del edificio.

Existen hubs pasivos y activos, los primeros sólo interconectan dispositivos, mientras que los segundos además regeneran la señal recibida, como si fuera un repetidor, de ahí la denominación de repetidor multipuerto.

Switch

Dispositivo que opera en la capa 2 del modelo OSI que tiene el fin de integrar a los equipos finales en una red de datos, empleando la transmisión de paquetes únicamente al destinatario seleccionado para transmitir.

Un switch es un dispositivo hardware que incluye componentes similares a una computadora personal: CPU, RAM y un IOS, Sistema Operativo de Red (Internetworking Operating System). Puede ser administrado de la misma forma que un router o bien mediante una consola conectada a un puerto ya sea por Telnet o bien vía FTP.

Estos dispositivos de interconexión corresponden con la capa de enlace de datos, regularmente son implementados para preservar el ancho de banda de la red al utilizar la segmentación, ya que reenvían paquetes a un segmento en particular, utilizando el direccionamiento de hardware MAC.

Los *switches* pueden ser clasificados de acuerdo con la técnica que emplean, para el reenvío de los paquetes al segmento apropiado en:

a) *Store-and-forward*, en esta técnica los switches procesan completamente el paquete incluyendo el campo del algoritmo CRC y la determinación del direccionamiento del paquete. Esto requiere el almacenamiento temporal del paquete antes de ser enviado al segmento apropiado. Su principal ventaja es la eliminación del número de paquetes dañados que son enviados a la red.
b) *Cut-through*, esta técnica implementada por los switches hace que sean más rápidos, debido a que envían los paquetes tan pronto la dirección MAC es leída.

El switch implementado en el Laboratorio utiliza la primera técnica: store and forward.

3.- Equipo y material necesario

Equipo del Laboratorio:

- 1 Computadora con un sistema operativo Windows 7 Profesional.
- Software de simulación de Cisco, Packet Tracer en su versión más reciente.
- 1 Switch FastEthernet.
- 1 Hub.

4.- Desarrollo

4.1 **Compartición de archivos en Debian**.

4.1.1 Inicie el equipo de cómputo, abra la máquina virtual en el sistema operativo Debian, en el usuario redes. Una vez ejecutado el sistema, abra una terminal, de clic en Aplicaciones > Accesorios > Terminal**.** Instale samba, con la siguiente instrucción:

#apt-get install samba

4.1.2 Cree un nuevo directorio para realizar la compartición de archivos mediante la instrucción:

#mkdir ***DIR***

Donde ***DIR*** será el nombre del directorio a crear.

4.1.3 Para dar los permisos necesarios y puedan compartirse archivos, ejecute el siguiente comando:

#chown redes ***DIR***

4.1.4 Para compartir archivos se requiere el uso de una contraseña (que será de su elección); con el siguiente comando se crea dicha contraseña y se solicita su confirmación (Ver Figura No. 4):

#smbpasswd redes –a

```
root@debian:/home/redes# nano /etc/samba/smb.conf
root@debian:/home/redes# smbpasswd redes -a
New SMB password:
Retype new SMB password:
Added user redes.
```

Figura No. 4. Creación de contraseña en Linux.

NOTA: La contraseña se deberá proporcionar al usuario que deseé tenga acceso a su carpeta compartida.

4.1.5 Al realizar la compartición de archivos, se le debe informar a samba el nombre de la carpeta, así como los permisos de lectura/escritura que se le están dando, para ello debe acceder al archivo de configuración con el siguiente comando (Ver Figura No. 4):

#nano /etc/samba/smb.conf

```
[carperta_compartida]
path = /home/redes/kena
writeble = yes
share = yes
guest ok = yes
```

Figura No. 5. Permisos carpeta compartida

4.1.6 Reinicie el servicio con el siguiente comando:

#/etc/init.d/samba restart

4.1.7 Para acceder a la carpeta compartida debe tener a la mano la dirección IP. Abra un navegador en Linux y teclee la dirección IP de donde se encuentra la carpeta que acaba de compartir.

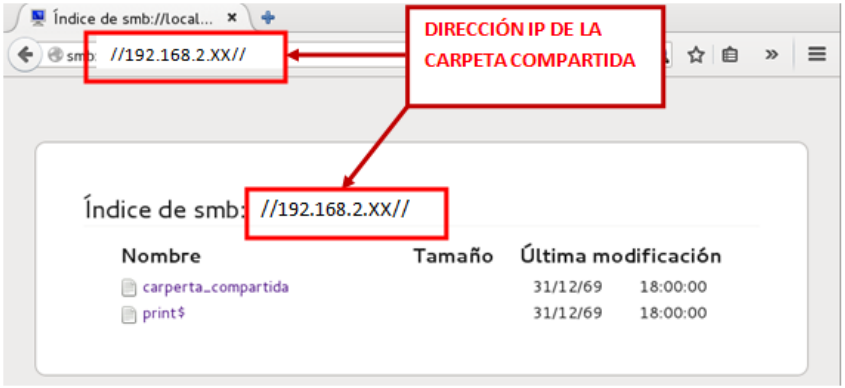


Figura No. 6. Acceso a la carpeta compartida

4.1.8 Comparta un archivo a través de un hub y un switch con base en la investigación previa.

i. Mencione si tuvo algún problema, indique ¿cuál fue su solución?

_____

_____

_____

_____

_____

4.2 Conociendo la interfaz de Packet Tracer.

4.2.1 Ejecute Cisco Packet Tracer desde Inicio > Todos los programas > Cisco Packet Tracer > Cisco Packet Tracer; aparecerá la interface gráfica (Ver Figura No. 6).

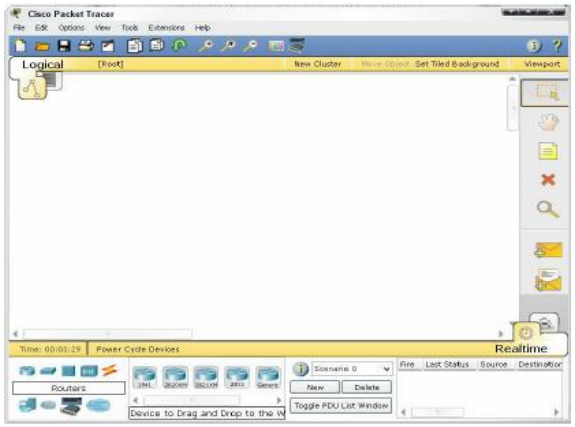


Figura No.7. Interface gráfica de Cisco Packet Tracer.

4.2.2 Cuando Cisco Packet Tracer es iniciado muestra por defecto una vista lógica de red; el área de trabajo lógica es el espacio central en blanco donde se pueden colocar y conectar los dispositivos.

4.2.3 En la esquina inferior izquierda de la interface se encuentran las secciones para elegir y colocar dispositivos en el área lógica de trabajo.

4.2.4 La sección 1 contiene símbolos que representan Grupos de Dispositivos. Cuando se coloca el puntero del mouse sobre alguno de los símbolos en el cuadro de texto del centro aparece el nombre de este grupo.

4.2.5 La sección 2 muestra los Dispositivos Específicos al grupo seleccionado en la sección 1. Si se da clic sobre algún grupo de la sección 1, los dispositivos de la sección 2 se actualizarán (Ver figura No. 7).

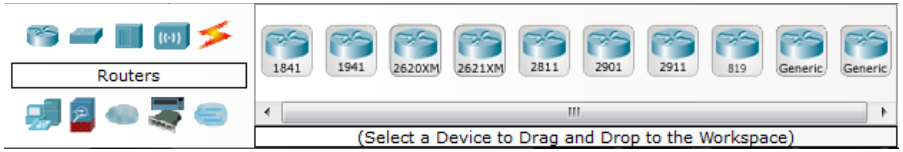


Figura No. 8. Secciones de dispositivos. A la izquierda grupos de dispositivos y a la derecha contenido del grupo de dispositivos.

4.2.6 Realice la siguiente topología compuesta por 1 Switch 2950-24, 6 PC-PT y un Hub –PT (véase la figura No. 8)

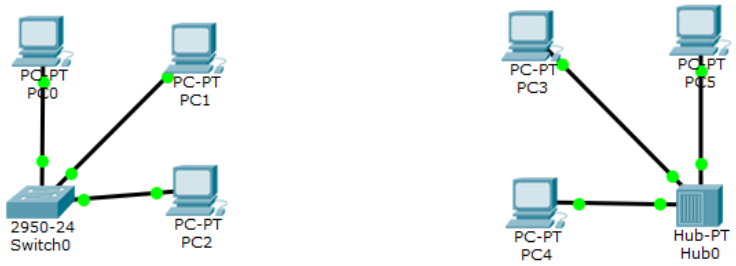


Figura No. 9. Topología de red.

4.3 Configuración de dirección IP en Cisco Packet Tracer.

Nota para el profesor: Indique a los alumnos el segmento de red a utilizar, el cual deberá pertenecer a la clase C.

4.3.1 Dé clic sobre una computadora, diríjase a Desktop, posteriormente a IP Configuration (vea la figura No. 9). Utilice los datos proporcionados por el profesor.
Los datos que se deben llenar son: IP Address, Subnet Mask, Defaul Gateway.

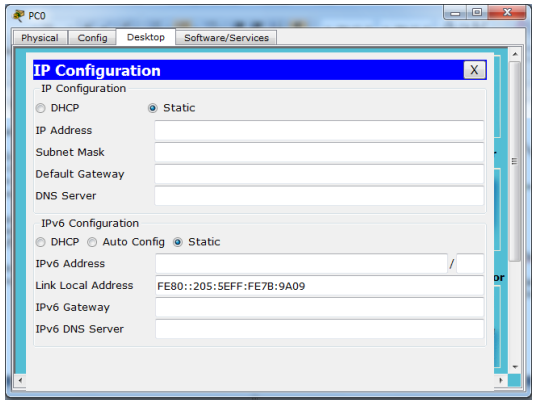


Figura No. 10. Configuración de la PC.

4.3.2 Una vez configurados los equipos de cómputo verifique que exista comunicación. Dé clic en el icono del sobre y posiciónelo sobre la PC 0 a la PC1. Repita el procedimiento en cada PC del switch y cada PC del hub.

4.3.3 En la parte de abajo del escritorio, hay un botón que dice "Delete" dé clic, borrará todo envío de paquetes. Diríjase a el modo de simulación. Dé clic en el sobre, (trabaje sobre la topología del switch) posteriormente dé clic en la PC0 y en la PC1, repita la operación para la PC1 y PC2 (véase la figura No. 10). Observe los resultados, analice y comente. Justifique su respuesta.

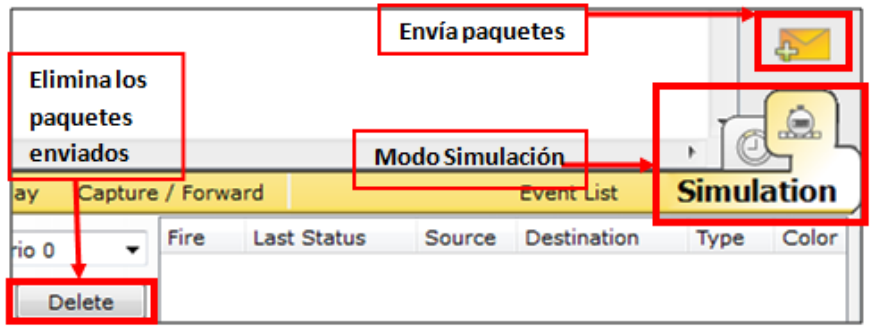


Figura No. 11. Envío de paquetes.

4.3.4 Repita la operación del paso 4.3.3 en la topología del hub. Observe los resultados, analice y comente. Justifique su respuesta.

5.- Cuestionario

1. ¿Cuál es la diferencia de descarga al compartir archivos entre ambos dispositivos? Argumente su respuesta

2. Mencione otros métodos para realizar la compartición de archivos e indique a qué sistema operativo pertenecen.

3. Mencione las características del hub y switch.

4. ¿Qué es una colisión?

6.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

PRÁCTICA 5

Compartición de archivos por Hub y Swith en Linux

Cuestionario Previo

Nombre del alumno:_____

Gpo. de Laboratorio:_____ Gpo. de Teoría:_____

1. Investigue al menos un método que existen para compartir archivos, entre los sistemas operativos Linux, Windows y IOS.

2. Investigue los tipos de colisiones en la transmisión de datos existentes

3. Investigue la forma de compartir archivos por medio de dispositivos de interconexión (hub y switch):

PRÁCTICA 6

Creación y configuración de una VLAN

1.- Objetivos de Aprendizaje

- El alumno conocerá el funcionamiento, configuración y que son las VLAN´s por el método de MAC, así como la designación por puertos para lo cual utilizará el simulador de redes Cisco Packet Tracer en su versión más reciente.

2.- Conceptos teóricos

Una VLAN (Virtual LAN) es un segmento de red lógico. Las VLAN permiten que las redes IP y subredes existan en una misma red, son útiles para reducir los dominios de broadcast y ayudan a la administración de la red, separando segmentos lógicos de una red de área local.

Una VLAN consiste en redes de computadoras que se comportan como si estuviesen conectados a un mismo cable, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local, los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles.

Tipos de VLAN

a) **VLAN de datos:** Se utiliza sólo para enviar tráfico de datos generado por el usuario.
b) **VLAN predeterminada:** VLAN que se le asignan todos los puertos del switch al iniciarlo.
c) **VLAN nativa:** Está asignada a un puerto troncal 802.1Q, que admite el tráfico que va desde y hacia una VLAN. Sirve como un identificador común en extremos opuestos de una red troncal.
d) **VLAN de administración:** Es cualquier VLAN que el administrador configura para acceder a la información de un switch.

Dirección MAC

Las direcciones MAC (Media Access Control) son identificadores de 48 bits que corresponden a una tarjeta o dispositivo de red. Se le conoce también como dirección física y es única para cada dispositivo. Está determinada y configurada por el IEEE y el fabricante.

Cisco IOS (Internetwork Operating System) es el software utilizado en la mayoría de los routers y switches de Cisco Systems. IOS es un paquete de funciones de enrutamiento, conmutamiento y trabajo en equipo.

Existen tres modos de configuración, se accede dando clic en el dispositivo, posteriormente en la pestaña CLI y son:

a) **Modo usuario (Switch>):** En este tipo de modo se pueden realizar configuraciones telnet y enviar ping.
b) **Modo privilegiado (Switch#):** En este modo se pueden consultar las configuraciones del switch y se pueden eliminar la información de la memoria RAM.
c) **Modo de configuración global (Switch(config#)):** En este modo se realizan la mayoría de las configuraciones del dispositivo como acceder a las interfaces, VLAN, seguridad, entre otros.

3.- Equipo y material necesario

Equipo del Laboratorio:

- 1 Computadora con un sistema operativo Windows 7 Profesional.
- Software de simulación Cisco Packet Tracer en su versión más actual.

4.- Desarrollo

Modo de trabajar:

4.1 Dé clic en Inicio > Todos los programas > Cisco Packet Tracer > Cisco Packet Tracer y construya en el área de trabajo la topología de red que se muestra en la Figura No. 1. Utilice los siguientes dispositivos: 6 PC-PT, 2 Switches 2950-24 (switch0 y switch1), 1 router 1841 (router0).

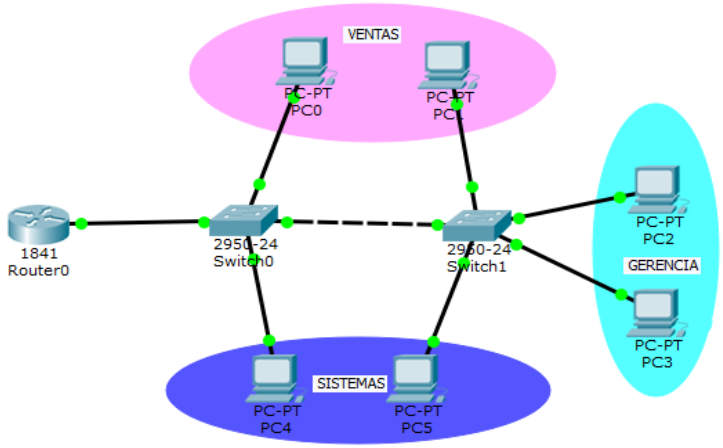


Figura No. 1. Topología.

4.2 Configuración de los segmentos y las VLAN's.

4.2.1 Seleccione el **Switch0,** diríjase a la pestaña CLI y entre en modo global.

4.2.2 Para crear una VLAN es necesario ingresar a la interface correspondiente, introduciendo los siguientes comandos:

Switch(config)#vlan ***ID_VLAN***
Switch(config-vlan)#name ***NOMBRE_VLAN***
Switch(config)#exit

Donde **ID_VLAN** es el número que identifica a cada VLAN y **NOMBRE_VLAN** es un nombre asignado a la VLAN. En esta topología se deben crear tres VLAN. La tabla No. 1 muestra los datos necesarios para crearlas.

Tabla 1. VLAN.

ID VLAN	NOMBRE	DISPOSITIVO INCIAL	DISPOSITIVO FINAL	Rango
	TRONCAL 1	Router	Switch 0	Fa 0/1
2	VENTAS	Switch0	PC	Fa 0/2-9
		Swirch1	PC	Fa 0/2-9
4	SISTEMAS	Switch0	PC	Fa 0/10-15
		Swirch1	PC	Fa 0/10-15
	TRONCAL 2	Switch0	Switch1	Fa 0/24
8	GERENCIA	Swirch1	PC	Fa 0/16-20
		Swirch1	PC	Fa 0/16-20

4.2.3 Repita la configuración en el **Switch1**.

4.3 Asignación de Puertos.

4.3.1 Para la asignación de puertos de un switch, en cada vlan es necesario configurar rangos específicos, utilice los siguientes comandos:

Switch(config)# interface range ***INT_INICIAL - INT_FINAL***
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan ***ID_VLAN***
Switch(config-if-range)# exit

Donde **INT_INICIAL** es la primera interface del rango para cada VLAN e **INT_FINAL** es la última interface del rango. El rango de puertos para cada VLAN se encuentra en la tabla 1, en la columna de **Rango** (Por ejemplo: Fa 0/18-22)

4.3.2 Realice la misma configuración para **Switch0** y **Switch1.**

4.3.3. Los administradores de redes, deben proteger los puertos que no utilizan, para lograr esta protección es necesario ingresar los siguientes comandos:

Switch(config)# interface ***INTERFAZ***
Switch(config)# shutdown

Donde ***INTERFAZ*** serán las interfaces que en este momento no se están usando o se desean desactivar por tener fallas en la conexión. Las cuales dependerán de la tabla 1, es decir, las interfaces que no se ocupan en ese rango de configuración.

4.4 Comunicación entre VLAN

4.4.1 Para comunicar las VLAN's es necesario crear un enlace troncal, que es un enlace punto a punto entre dos dispositivos de red.

Este enlace no pertenece a una VLAN en específico. Para la configuración de enlaces troncales entre switches debe introducir los siguientes comandos en ambos switches:

Switch(config)# interface ***INTERFAZ***
Switch(config)# switchport mode trunk
Switch(config)# exit

Donde **INTERFAZ**, son las interfaces del switch que se van a configurar de modo troncal.

Nota: Recuerde que en el **Switch0**, hay dos redes troncales, la primera es la conexión entre el Switch0 y el router (con su respectiva interface). La segunda red troncal es entre switches.

4.4.2 Escriba los datos que se le solicitan en la tabla No. 2, con el segmento de red proporcionado por el profesor para la VLAN.

Tabla No. 2. Direccionamiento.

ID VLAN	Dirección de red	Máscara de subred
2		
4		
8		

La dirección de red es la última dirección útil de cada segmento perteneciente a la topología.

4.4.3 Para configurar el enlace troncal en el router, es necesario crear interfaces, para encaminar paquetes. La configuración se realiza especificando un número de subinterface. De clic en el router, diríjase a la pestaña CLI y entre en modo global e introduzca los siguientes comandos:

Router(config)# interface Fa 0/0. ***ID_VLAN***
Router(config-subif)# encapsulation dot1q ***ID_VLAN***
Router(config-subif)# ip address ***IP_ADDRESS MASK***
Router(config-subif)# exit

Donde **IP_ADDRESS *y* MASK** hacen referencia a los valores contenidos en la Tabla No. 2. Por último, habilite la interfaz física del router.

4.4.4 Verifique que exista comunicación entre los dispositivos haciendo ping de una PC´s a otra perteneciente a su VLAN. Guarde su archivo.

4.5 Configuración de VLAN por MAC.

4.5.1 Dé clic en una PC de la topología de red y obtenga su dirección MAC, para ello, vaya a Desktop > IP Configuration y diríjase al rubro ***Link Local Address*** . La dirección MAC son los últimos 12 dígitos (Ver Figura No. 2).

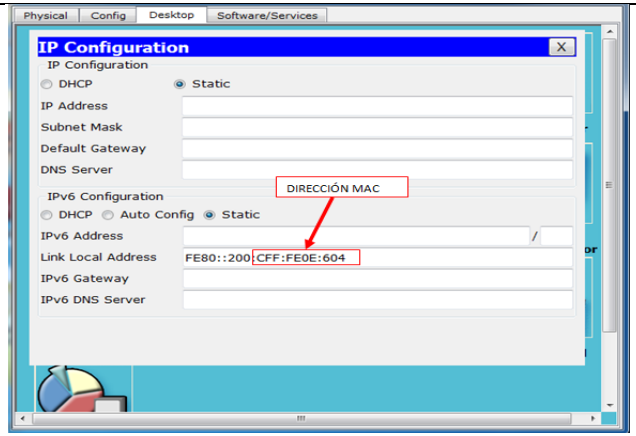


Figura No. 2. Obtención de la dirección MAC.

4.5.2 Escriba los datos que se le solicitan en la tabla No. 3:

Tabla No. 3. VLAN por MAC.

PC	MAC	ID_VLAN	INTERFACE
0			
1			
2			
3			
4			
5			

4.5.3 Para configurar las direcciones **MAC** en cada switch es necesario que ingrese en modo de configuración global, utilizando los siguientes comandos:

Switch(Config)# mac-address-table static ***MAC_ADDRESS*** vlan ***ID_VLAN*** interface ***INTERFAZ***

Donde ***MAC_ADDRESS,*** es la dirección MAC de cada PC conectada, ***ID_VLAN*** es la VLAN a la que se encuentra conectada y la ***INTERFAZ*** es la interfaz de la PC conectada al switch.

Nota: Este procedimiento se debe realizar para todas las PC´s que estén conectadas a la red.

4.5.4 Conforme a la investigación previa referente a la configuración de contraseñas, realice en los dispositivos de interconexión, la configuración necesaria, además ingrese los comandos necesarios para desactivar el puerto en caso de violar la seguridad. Analice sus resultados y muestre a su profesor.

5. Cuestionario.

1. Tecleé el comando **Show vlan brief.** Analice y describa el resultado obtenido.

2. ¿Cuál es la ventaja de configurar una VLAN?

3. ¿Por qué razón una VLAN mitiga los dominios de broadcast?

4. ¿Qué ventajas tiene el realizar la configuración de una VLAN por MAC?

6.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

PRÁCTICA 6

Creación y configuración de una VLAN

Cuestionario Previo

Nombre del alumno:_____

Gpo. de Laboratorio:_____ ***Gpo. de Teoría:***_____

1. Investigue qué es el enlace troncal en VLAN
2. Investigue cómo se configuran las contraseñas de un switch y router.
3. Investigue cómo se configura la interfaz física de un router.
4. Investigue los comandos para restringir los puertos dinámicos en el switch, en caso de que haya alguna violación de seguridad.

PRÁCTICA 7

Red inalámbrica "ad hoc" y compartición de archivos en Windows.

1.- Objetivos de aprendizaje

- El alumno analizará y aprenderá a crear una conexión punto a punto de forma inalámbrica, así como compartir archivos entre dos dispositivos, dentro del sistema operativo Windows 7 Profesional.

2.- Conceptos teóricos

Las redes inalámbricas son conexiones de nodos que se comunican por medio de ondas electromagnéticas, sin necesidad de una red cableada o alámbrica, la transmisión y la recepción se realiza a través de puertos.

La principal ventaja es la reducción de costos al eliminar las conexiones físicas entre equipos de cómputo y dispositivos de interconexión (router y access point), pero también tiene una desventaja, por el tipo de red requiere una seguridad más robusta y exigente para evitar en la medida de lo posible vulnerabilidades.

Existen tres tipos de redes inalámbricas, las cuales son:

a) WPAN: Wireless Personal Area Network.
b) WMAN: Wireless Metropolitan Area Network.
c) WWAN: Wireless Wide Area Network.

Red "ad hoc"

Una red "ad hoc", consiste en un grupo de equipos de cómputo que se comunican entre sí, a través de señales de radio sin usar un punto de acceso.

Las configuraciones "ad hoc", son comunicaciones de tipo punto a punto donde los ordenadores se encuentran en un rango definido. Permite la adhesión de nuevos dispositivos, con solo estar dentro del rango de alcance. Es regido por el protocolo de comunicaciones IEEE 802.11 que define todos los parámetros necesarios para establecer la comunicación entre dispositivos inalámbricos.

Cada nodo que retrasmite la información implica un salto, cuanto mayor sea el número de saltos, mayor será el tiempo que tardará en transmitir la información.

Las redes *ad hoc* se clasifican según su aplicación y son:

- **Mobile ad hoc networks (MANET):** Son dispositivos conectados por wireless y que poseen propiedades de auto-configuración.
- **Red inalámbrica Mesh:** Es una red en malla implementada sobre una red inalámbrica LAN.
- **Redes de sensores:** Están formadas por un grupo de sensores con ciertas capacidades sensitivas y de comunicación inalámbrica, sin infraestructura física preestablecida ni administración central.

3.- Equipo y material necesario

Equipo del Laboratorio:

- 1 Computadora con un sistema operativo Windows 7 Professional.
- NIC inalámbrica en cada equipo.

4.- Desarrollo

Creación de red ad hoc.

Para crear una red ad hoc, es necesario tener un equipo que realice la función de servidor, el cual proveerá de los documentos que se requieran en un grupo de trabajo.

4.1 Configuración del servidor.

4.1.1 Para configurar el servidor que proveerá los documentos debe dar clic en Inicio > Panel de control > Ver el estado y las tareas de redes. Posteriormente dé clic en Configurar una nueva conexión o red > Configurar una red ad hoc inalámbrica (Ver Figura No. 1).

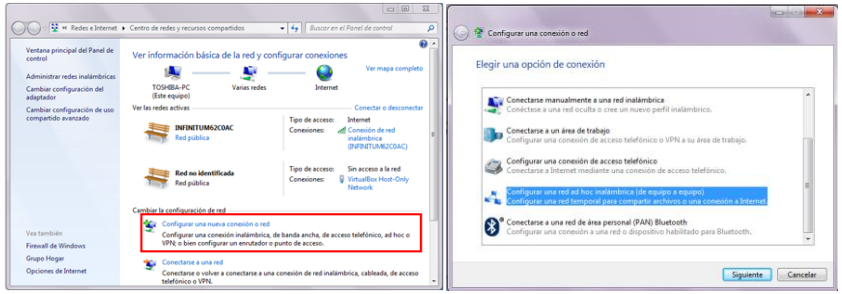


Figura No. 1. Configuración de red ad hoc.

4.1.2 Dé clic en "siguiente" hasta llegar a la opción donde le solicita un nombre y una contraseña (Ver Figura No. 2).

Nota: Guarde el nombre de la red y la contraseña, más adelante la requerirá.

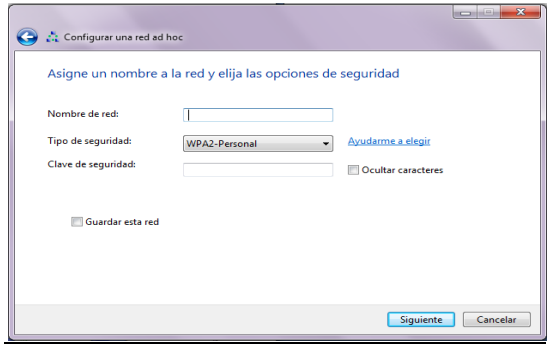


Figura No.2. Asignación de nombre y contraseña.

4.1.3 Una vez configurado el nuevo servidor (red), mostrara la siguiente pantalla (Ver Figura No. 3):

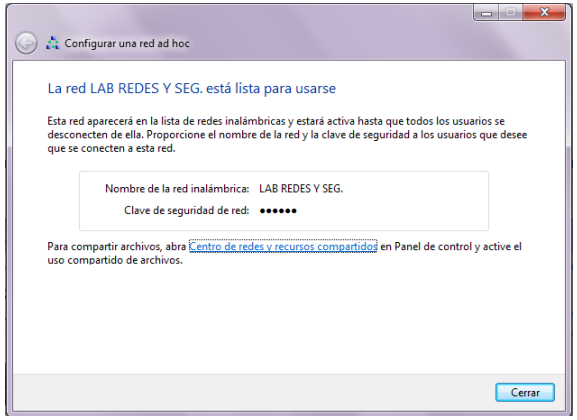


Figura No.3. Creación correcta de la red ad hoc.

i. Analice ¿qué función tiene la creación del servidor en este caso?

4.2 Configuración de la dirección IP.

4.2.1 Para que exista una comunicación entre el cliente (usuario) y el servidor es necesario que las maquinas cuenten con una dirección IP.

4.2.2 Diríjase al panel de control, ubicado en Inicio > Panel de Control. A continuación seleccione la opción Redes e Internet > Conexiones de Red, en seguida dé clic en Centro de redes y recursos compartidos. Finalmente abra la opción en el menú izquierdo que dice cambiar la Configuración del adaptador.

4.2.3 En la ventana aparecerán todas las interfaces de red instaladas en el equipo de cómputo. Seleccione la interface de Conexión de área local, active el menú emergente y seleccione Propiedades.

4.2.4 En el cuadro de diálogo dé clic en Protocolo de Internet (TCP/IPv4) y presione el botón Propiedades. Proceda a configurar el protocolo según las indicaciones de su profesor (Ver figura No.1).

Nota para el profesor: La configuración del protocolo IPv4 tendrá que ser de manera estática y pueda existir una comunicación entre el cliente y servidor.

ii. Indique qué tipo de direccionamiento utilizó y por qué. Justifique su respuesta.

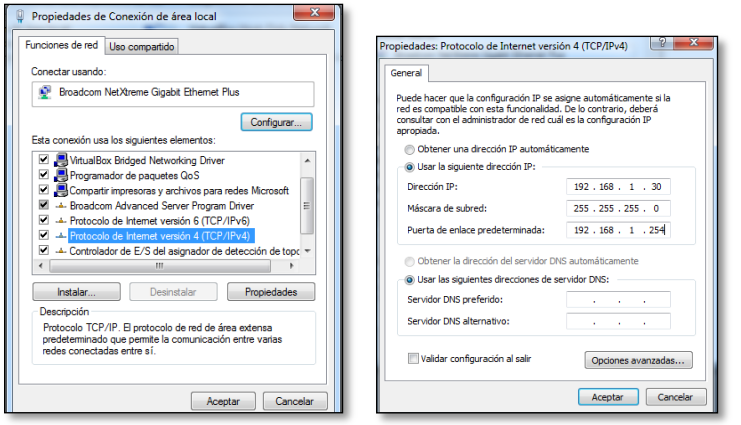


Figura No. 1. Protocolo TCP/IP y Configuración.

4.3 Creación de la carpeta compartida.

La red ad hoc tiene la función de compartir archivos de manera inalámbrica, por lo cual requiere la creación de una carpeta compartida para que exista esté intercambio de información.

4.3.1 Diríjase al panel de control, ubicado en Inicio > Panel de Control. A continuación seleccione la opción **ver iconos grandes** y busque **Opciones de carpeta**, dé clic; le mostrará un cuadro de diálogo, seleccione la pestaña **Ver** y dé clic en **Usar el Asistente para compartir** (Ver Figura No. 2).

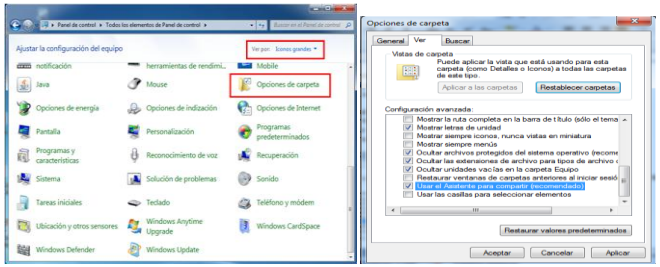


Figura No. 2. Asistente de compartición de carpetas.

4.3.2 Cree una carpeta en el escritorio y dé clic derecho, seleccione compartir con > Uso compartido avanzado…
En el cuadro de diálogo, seleccione Uso compartido avanzado. Posteriormente en el nuevo cuadro seleccione la opción Compartir esta carpeta. (Ver figura No.3).

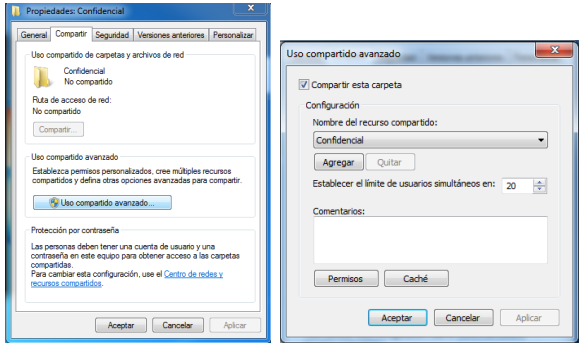


Figura No. 3. Permisos para compartir archivos.

Para modificar e incluso borrar los archivos que se encuentren dentro de esta carpeta, es necesario darle permisos. Dé clic en permisos y seleccione todas las casillas en permitir. Al terminar dé clic en aceptar en todos los cuadros de diálogo.

4.4 Configuración del usuario.

4.4.1 Para conectar los equipos de los usuarios, es necesario que dé clic en el icono de conexión inalámbrica, seleccione la red que se creó y escriba la contraseña (que se le solicitó en el punto 4.1.2) correcta para acceder al dispositivo (Ver Figura No. 5).

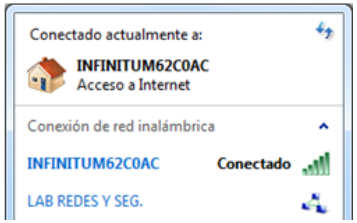


Figura No.5. Conexión al equipo servidor.

4.4.2 Para acceder a los archivos de la red ad hoc, dé clic en Inicio > Equipo > Red, seleccione el nombre del equipo que funciona como servidor (que se le solicitó en el punto 4.1.2), para permitir el acceso a los archivos compartidos.

5.- Cuestionario

1. Describe brevemente las diferentes conexiones inalámbricas existentes.

2. Mencione algunos beneficios de usar redes ad hoc.

3. En una empresa encargada de realizar diseño gráfico, requieren hacer la compartición de archivos de una manera segura y fiable. ¿Cuál conexión inalámbrica usaría? Argumente su respuesta

6.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

PRÁCTICA 7

Red inalámbrica "ad hoc" y compartición de archivos en Windows.

Cuestionario Previo

Nombre del alumno:_____

Gpo. de Laboratorio:_____ Gpo. de Teoría:_____

1. ¿Qué es una red ad hoc?
2. ¿Cuáles son las ventajas y desventajas de utilizar redes ad hoc?
3. Indique la diferencia entre usar direcciones IP estáticas y direcciones IP dinámicas.
4. ¿Qué tipo de direccionamiento es más usado?. Justifique su respuesta.

PRÁCTICA 8
Enrutamiento (estático y dinámico)

1.- Objetivos de Aprendizaje

- El alumno comprenderá el funcionamiento de los protocolos de enrutamiento estático y dinámico, analizará su funcionamiento dentro de una red de área local mediante el simulador de redes: Cisco Packet Tracer en su versión más reciente.

2.- Conceptos teóricos

El administrador de redes, requiere que los diferentes departamentos mantengan una comunicación fiable dentro de su red interna, para lo cual se necesitan utilizar los enrutamientos estáticos y dinámicos (OSPF, EIGRP y Rip v2)

El enrutamiento es fundamental para cualquier red de datos, siendo el router el encargado de transmitir información de una red origen a una red destino.

El **encaminamiento estático** funciona por medio de rutas estáticas, definidas por el administrador de redes, obtenidas de las tablas de ruteo. Dicho encaminamiento es recomendado para redes pequeñas, por su bajo costo de mantenimiento y fiabilidad para transmitir paquetes, en cambio en redes grandes requiere de una configuración y mantenimiento constante por parte del administrador y es más vulnerable a errores por los cambios en la topología de red.

El **encaminamiento dinámico** es utilizado en redes más grandes, ya que tiene la capacidad de determinar rutas y priorizar la más óptima de acuerdo con la información de los routers en el envío de paquetes.

El **Routing Information Protocol (RIP)** es un protocolo vector – distancia y se especificó originalmente en el RFC 1058. Tiene por características principales las siguientes:

- Protocolo de enrutamiento con clase.
- Utiliza el conteo de saltos como métrica.
- Se emplea si el conteo de saltos de una red es mayor de 15.
- Por defecto se envía un broadcast o multicast de las actualizaciones de enrutamiento cada 30 segundos.

RIP v2 es un protocolo de enrutamiento sin clase, las máscaras de subred se incluyen en las actualizaciones de enrutamiento, lo que hace que RIP v2 sea compatible con los ambientes de enrutamiento modernos.

Este protocolo es una mejora de las funciones y extensiones de RIP v1, algunas de estas funciones mejoradas incluyen:

- Direcciones de siguiente salto incluidas en las actualizaciones de enrutamiento.
- Uso de direcciones multicast al enviar actualizaciones.
- Opción de autenticación disponible.

Los cables seriales se utilizan para interconexión de datos entre dispositivos digitales. La mayoría de estos cables seriales, usan la entrada RS-232 que es la interface estándar para las comunicaciones entre este tipo de dispositivos.

El cable DTE y DCE, se utilizan para comunicar un equipo terminal de datos y una equipo de comunicaciones de datos. DTE se refiere al punto de terminación para inicio de sesión y DCE se refiere a punto de una sesión de comunicacion de reenvío.

3.- Equipo y material necesario

Equipo del Laboratorio:

- 1 Computadora con un sistema operativo Windows 7 Profesional.
- Software de simulación de Cisco Packet Tracer en su versión más reciente.

4.- Desarrollo

4.1.1 Arrastre al área de trabajo los dispositivos necesarios para crear la topología de la figura No 1, los dispositivos a utilizar son: 4 routers 1841, 4 switches 2950-24, 4 PC-PT

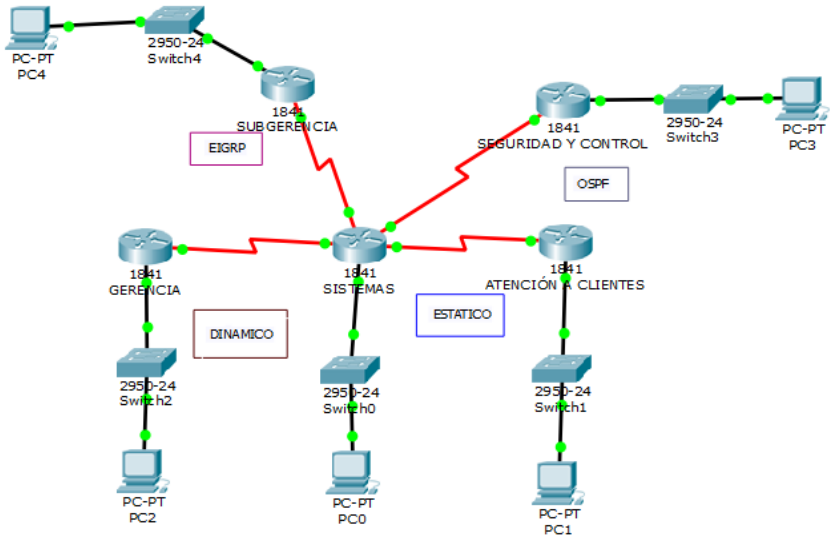


Figura No. 1. Topología de dispositivos.

4.2 Configuración del router.

4.2.1 Dé clic sobre un router, apáguelo y conecte el slot WIC-2T, sirve para permitir la comunicación entre dos dispositivos digitales. Posteriormente vuelva a encenderlo y realice el mismo procedimiento en cada router (Ver Figura No. 2).

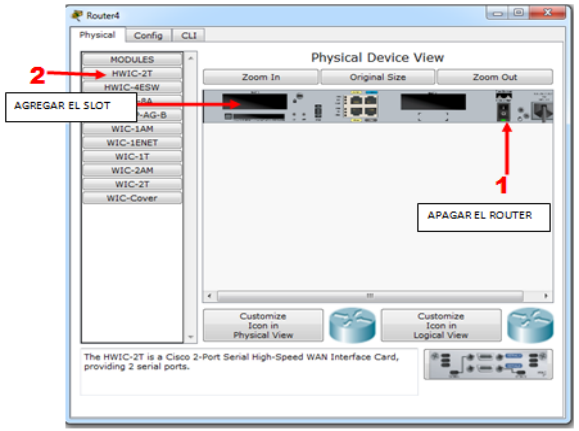


Figura No. 2. Agregar tarjetas seriales al router.

4.3 Enrutamiento estático.

4.3.1 Complete la información que se le solicita en la tabla de ruteo para el encaminamiento estático.

Tabla 1. Encaminamiento Estático

Router	Dirección IP	Máscara	Salto Siguiente
SISTEMAS			
ATENCIÓN A CLIENTES			

4.3.2 Para configurar la ruta estática entre los routers **Atención a Clientes** y **Sistemas,** se utilizan los siguientes comandos (debe acceder a modo global):

Router(config)# ip route ***NETWORK*** ***NET_MASK*** ***NEXT_HOP_ADDRESS***
Router(config)#exit
Router#copy run start

Reemplace el parámetro ***NETWORK*** con el segmento de red con el cual desea tener comunicación (red remota), el parámetro ***NET_MASK*** corresponde a la máscara de subred de la red remota. El parámetro ***NEXT_HOP_ADDRESS*** corresponde a la siguiente dirección de red de la interface del router conectado directamente, es decir, la siguiente interface con la que se requiere tener comunicación.

4.3.3 Guarde su proyecto, vaya al menú File>Save, le preguntará si desea sobrescribir el archivo, haga clic en yes.

4.4 Verificación de configuración.

4.4.1 Envie ping entre las redes configuradas y verifique que el resultado sea exitoso, de lo contrario verifique su topología

4.5 Enrutamiento dinámico.

I. De acuerdo con la investigación previa, indique ¿Cuál es la versión de RIP que debe utilizar? _____.

4.5.1 Complete la información que se le solicita en la tabla de ruteo para el encaminamiento dinámico.

Tabla 2.Encaminamiento Dinámico

Router	**Subred conectada directamente**	**Máscara de subred**
GERENCIA		
SISTEMAS		

4.5.2 Ingrese a modo global en el router y configure el protocolo de enrutamiento RIP. Seleccione la versión que debe configurar.

Router(config)#router rip
Router(config-router)#version ***NÚMERO_DE_VERSIÓN***

4.5.3 Configure las subredes asignadas a este protocolo de acuerdo con la Tabla 2, en el comando network ***NETWORK_ADDRESS*** reemplace los parámetros por la subred correspondiente, es importante que indique todas y cada una de las subredes conectadas directamente en un comando network independiente.

La ***ID_INTERFACE*** corresponde a la interfaz en la que se encuentra conectado el dispositivo.

Router0(config-router)#network ***NETWORK_ADDRESS***
Router0(config-router)#passive-interface ***ID_INTERFACE***
Router0(config-router)#exit
Router#copy run start

4.5.4 Configure el resto del área asignada a este protocolo.

4.5.5 Guarde su proyecto, vaya al menú File>Save, le preguntará si desea sobrescribir el archivo, haga clic en yes.
Su proyecto lo utilizará en la práctica siguiente (Práctica 9 (Tipos de enrutamiento OSPF y EIGRP))).

5. Cuestionario.

1. **Indique lo que se requiere para incluir seguridad en el router central.**

2. **En caso de que algún router pierda conexión con el resto de la topología ¿cómo lo resolvería?**

3. **Investigue algunos métodos de seguridad en la red.**

6.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

PRÁCTICA 8

Enrutamiento (estático y dinámico)

Cuestionario Previo

Nombre del alumno:_____

Gpo. de Laboratorio:_____ Gpo. de Teoría:_____

1. Investigue los comandos para poner contraseñas en el router.
2. Investigue como se configuran las tablas de ruteo.
3. Investigue como se realiza el VLSM.

PRÁCTICA 9
Tipos de enrutamiento (OSPF y EIGRP)

1.- Objetivos de Aprendizaje

- El alumno conocerá y configurará protocolos de enrutamiento OSPF y EIGRP, analizará su funcionamiento dentro de una red de área local mediante un simulador de redes: Cisco Packet Tracer en su versión más reciente.

- El alumno aprenderá y realizara la Redistribución de redes con distintos protocolos dinámicos y estático.

2.- Conceptos teóricos

El protocolo EIGRP (Enhanced Interior Gateway Routing Protocol), es un protocolo de encaminamiento vector distancia avanzado, que ofrece lo mejor de los algoritmos de vector - distancia y del estado de enlace. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado - enlace.

El enrutamiento EIGRP mantiene información de ruta y topología a disposición de la RAM para que pueda reaccionar rápidamente a los cambios.

Las características más importantes de EIGRP son:

- Protocolo de transporte confiable (RTP).
- Algoritmo de actualización por difusión (DUAL).
- Establecimiento por adyacencias.
- Tablas de vecinos, topología y encaminamiento.

Cuando un router detecta que un dispositivo cercano no está disponible, intenta encontrar rutas alternas para todas aquellas que se encuentren en la tabla de encaminamiento y están dirigidas a ese vecino.

El protocolo OSPF son las siglas de Open Shortest Path First, utiliza el algoritmo Dijkstra enlace-estado, para calcular la ruta más idónea. Toma en cuenta diversos parámetros como son el ancho de banda y la congestión de los enlaces, construye una base de datos idéntica a los routers de la zona.

Puede operar con seguridad usando MD5(Message-Digest Algoritmo 5, es un algoritmo de reducción criptográfico) para autenticar sus puntos antes de realizar nuevas rutas y aceptar avisos de enlace-estado.

Redistribución de Rutas.

La redistribución de rutas, es utilizada para lograr la comunicación dentro de una topología con distintos tipos de enrutamiento dinámico y estático. Según la definición de Cisco System “El uso de un protocolo de ruteo para publicitar rutas conocidas por algunos otros medios, como por otro protocolo de ruteo, rutas de estadísticas o rutas conectadas directamente, se denomina redistribución”.

La redistribución de rutas utiliza métricas que deben de contener los siguientes datos y varían dependiendo del protocolo a redistristribuir (Ver Tabla No. 1).

Tabla No. 1. Métricas.

METRICO	VALOR
Ancho de banda	En unidades de kilobits por segundo, 10000 para Ethernet.
Retraso	En unidades de decenas de microsegundos, para Ethernet es 100-10 microsegundos = 1 ms.
Confiabilidad	255 para 100 por ciento confiable
Carga	Carga efectiva en el enlace, expresada como un número de 0 a 255 (255 es una carga del 100 por ciento).
MTU (Unidad de transmisión básica)	MTU mínimo de la ruta, generalmente equivale a aquél para la interfaz Ethernet que es 1500 bytes.

Cada protocolo utiliza sus métricas para lograr la comunicación con los diferentes segmentos de red, para entender mejor el uso de las métricas analiza la tabla No. 2.

Tabla No. 2. Métricas de los protocolos de enrutamiento.

PROTOCOLO	MÉTRICAS
EIGRP	Métrica del ancho de banda en Kbits por segundo. EIGRP métrica de retardo , en 10 unidades de microsegundos. EIGRP métrica fiabilidad , donde 255 es 100 % confiable. EIGRP métrica del ancho de banda efectivo (Cargando) , donde 255 es 100 % cargado EIGRP MTU de la trayectoria.
OSPF	Métrica por default (siempre es 1) La redistribución de rutas OSPF Redistribuir rutas externas OSPF Redistribuir tipo externo 1.
ESTATICAS	Métrica para las rutas redistribuidas. Considere subredes para la redistribución en OSPF. Set para rutas redistribuido en OSPF

3.- Equipo y material necesario

Equipo del Laboratorio:

- 1 Computadora con un sistema operativo Windows 7.
- Software de simulación de Cisco, Packet Tracer en su versión más reciente.

Equipo del alumno:

- Archivo realizado en la práctica anterior (Practica 8, Enrutamiento (estático y dinámico)).

4.- Desarrollo

4.1 Enrutamiento EIGRP.

4.1.1 Abra el archivo que utilizó en la práctica anterior. Dé clic sobre el router Sistemas >CLI y presione enter, ingrese al modo global del router.

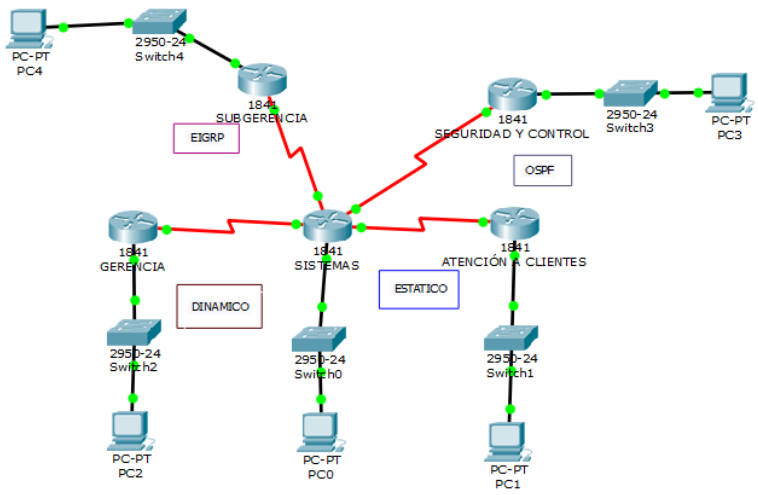


Figura No. 1. Topología de dispositivos.

4.1.2 Realice la tabla de ruteo para el encaminamiento EIGRP y OSPF

Tabla 2. Encaminamiento EIGRP y OSPF.

Router	Subred conectada directamente	Wilcard
SISTEMAS		
SUBGERENCIA		
SEGURIDAD		

4.1.3 Ingrese al modo de configuración del protocolo de enrutamiento EIGRP, con el siguiente comando:

Router(config)#router EIGRP ***ID DEL AREA***

Donde **ID DEL AREA,** será un número asignado por el administrador de redes (en este caso será asignado por el alumno) para identificar a todos los routers que pertencen a esa internetwork, deberá de ser el mismo identificador en todos los routers perteneciente a la red.

4.1.4 Configure las subredes **Subgerencia – Sistemas.** De acuerdo con la Tabla 2, en el comando **NETWORK_ADDRESS** reemplace los parámetros por la subred correspondiente, es importante que indique todas y cada una de las subredes conectadas directamente, la **WILDCARD** corresponde a la máscara invertida de la **NETWORK_ADDRESS**.

Router0(config-router)#network ***NETWORK_ADDRESS WILDCARD***
Router0(config-router)#no auto-summary

I. ¿Cuál es la función de los siguientes comandos?

#eigrp log-neighnor-changes
#bandwidth kilobits

4.1.5 Guarde su proyecto, vaya al menú File>Save, le preguntará si desea sobrescribir el archivo, haga clic en yes.

4.2 Enrutamiento OSPF.

4.2.1 Ingrese al modo global del router. Configure el segmento comprendido entre **Seguridad y Control – Sistemas.** Ingrese al modo de configuración global del protocolo de enrutamiento OSPF.

Router(config)#router OSPF ***ID DEL PROCES0***

Donde el **ID DEL PROCESO,** será un número asignado por el administrador de redes (en este caso será asignado por el alumno) y cambia en cada router.

4.2.2 Configure las subredes **Sistemas - Seguridad**. De acuerdo con la Tabla 2., en el comando **NETWORK_ADDRESS** reemplace los parámetros por la subred correspondiente, es importante que indique todas y cada una de las subredes conectadas directamente, seguida de la **WILDCARD** correspondiente al segmento de red proporcionado por el profesor. El **AREA X**, donde X es un valor numérico y **NO** cambia en cada router (en este caso será asignado por el alumno).

Router0(config-router)#network ***NETWORK_ADDRESS WILDCARD*** *area* ***X***

4.3 Redistribución de rutas

Para realizar la redistribución de rutas, se debe de analizar qué router lleva toda la carga. En este caso es el router **Sistemas**, quien es al que se le configurarón todos los enrutamientos.

El objetivo es que haya comunicación entre todas las subredes, para ello se debe ingresar a modo global y realizar las siguientes instrucciones:

En este punto utilizará el **ID DEL AREA,** que designó en el punto 4.1.3, el **ID DEL PROCESO** que fue asignado en el punto 4.2.1.

REDISTRIBUCIÓN DE EIGRP A OSPF

Router0(config)# router EIGRP ***ID DEL AREA***
Router0(config-router)#redistribute OSPF ***ID DEL PROCES0*** metric 1658031 514560 255 255 1500
Router0(config-router)#exit

Router0(config)# router OSPF ***ID DEL PROCES0***
Router0(config-router)#redistribute EIGRP ***ID DEL AREA*** metric 65
Router0(config-router)#exit

REDISTRIBUCIÓN OSPF, RIP y EIGRP

Router0#configure terminal
Router0(config)#router rip
Router0(config-router)#redistribute OSPF ***ID DEL PROCES0*** metric 1 match internal external 1
Router0(config-router)#redistribute EIGRP ***ID DEL AREA*** metric 1

Router0(config-router)#exit

Router0(config)#router EIGRP ***ID DEL AREA***
Router0(config-router)#redistribute rip metric 1658031 514560 255 255 1500
Router0(config-router)#exit

Router0(config)#router OSPF ***ID DEL PROCES0***
Router0(config-router)#redistribute rip metric 65 subnets tag 65
Router0(config-router)#exit

REDISTRIBUCIÓN STATIC, OSPF, RIP y EIGRP

Router0#configure terminal
Router0(config)#ip route ***SEGMENTO MASK INTERFACE***

Router0(config)# router EIGRP ***ID DEL AREA***
Router0(config-router)#redistribute static
Router0(config-router)#exit

Router0(config)# router OSPF ***ID DEL PROCES0***
Router0(config-router)#redistribute static metric 65 subnets tag 65
Router0(config-router)#exit

Router0(config)# router rip
Router0(config-router)#redistribute static
Router0(config-router)#exit

Donde **SEGMENTO,** es la LAN del enrutamiento estático, **MASK** es la máscara de dicho segmento, **INTERFACE** es la interface de redistribución central (Ver figura No.2)

REDISTRIBUCIÓN STATIC, OSPF, RIP y EIGRP

Router0#configure terminal

Router0(config)# ip route ***SEGMENTO_1 MASK INTERFACE***
Router0(config)# exit

Donde **SEGMENTO_*1*** corresponde al segmento de LAN existente en la red, **MASK** es la mascara del segmento, **INTERFACE** es la interface de redistribución estatica (Ver figura No.2)

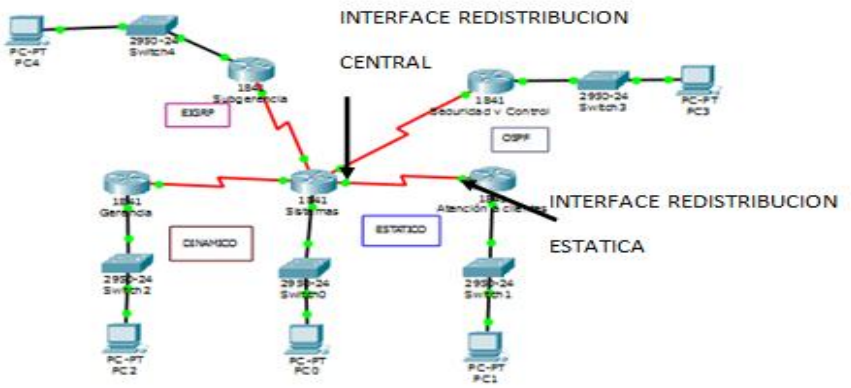


Figura No. 2. Interfaces a configurar.

4.3.1. Verifique la conectividad entre subredes.

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

PRÁCTICA 9

Tipos de enrutamiento (OSPEF y EIGRP)

Cuestionario Previo

Nombre del alumno:_____

Gpo. de Laboratorio:_____ ***Gpo. de Teoría:***_____

1. Investigue qué es la sumarizacion de rutas
2. Investigue cómo se obtiene la máscara wilcard
3. Mencione ¿cuál es el uso de los identificadores de área?
4. Investigue qué pasa al escoger diferentes identificadores de áreas en cada subred.

PRÁCTICA 10

Instalación de un servidor Apache

1.- Objetivos de aprendizaje

- El alumno desarrollará las habilidades necesarias para realizar la instalación de un servidor apache en la distribución Kali Linux.

2.- Conceptos teóricos

El servidor HTTP apache es un servidor HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, entre otros), Microsoft Windows y otras, que implementa el protocolo HTTP/1.1.

Comenzó su desarrollo en 1995, se basó inicialmente en código del popular NCSA HTTPd que era un Servidor web desarrollado originalmente en el National Center for Supercomputing Applications por Robert McCool y una lista de colaboradores.

El desarrollo del NCSA HTTPd se suspendió en 1998, pero el código sobrevivió durante un tiempo en manos del Proyecto Apache, el cual es utilizado actualmente por dos terceras partes de los servidores web de Internet. Prácticamente todo el código de NCSA se ha ido reescribiendo progresivamente en versiones de Apache.

Apache presenta, entre otras características, mensajes de error altamente configurables, bases de datos de autenticación y negociación de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

Módulos

El servidor de base puede ser extendido con la inclusión de módulos entre los cuales se encuentran:

- mod_perl - Páginas dinámicas en Perl.
- mod_php - Páginas dinámicas en PHP.
- mod_python - Páginas dinámicas en Python.
- mod_jk - Conector para enlazar con el servidor Jakarta Tomcat de páginas dinámicas en Java (servlets y JSP).
- mod_ssl - Comunicaciones Seguras.
- mod_rewrite - Reescritura de direcciones servidas.

HTTP

HTTP es el protocolo usado para la transferencia de hipertexto en Internet, las letras significan Hyper Text Transfer Protocol. El hipertexto es el contenido de las páginas web y el protocolo de transferencia, es el sistema mediante el cual se envían las peticiones para acceder a una página web y la respuesta de ésta web, remitiendo la información que se verá en pantalla. También sirve para enviar información adicional en ambos sentidos, como formularios con mensajes y otros similares.

HTTPS

Es una versión segura del protocolo HTTP. El sistema HTTPS utiliza un canal de cifrado (cuyo nivel de seguridad depende del servidor remoto y el navegador utilizado por el cliente) basado en Secure Socket Layers (SSL), más apropiado para el tráfico de información sensible que el protocolo HTTP.

Es utilizado principalmente por entidades bancarias, tiendas en línea y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas. El puerto estándar para este protocolo es el 443.

Estructura básica de apache

Cuando el servidor de páginas (apache) recibe la requisición para alguna página, éste reconoce cuando debe enviar un documento estático (HTML) o ejecutar algún tipo de aplicación. La solicitud de alguna página invoca un programa en *Perl* y éste a su vez solicita información a una base de datos, para llevar a cabo esta operación debieron iniciarse *2 procesos* nuevos.

Ventajas de apache

- Es capaz de utilizar otros interpretadores y lenguajes como "Tcl", "Php" y "Python".
- Puede conectarse directamente a una Base de datos.
- Posee diversos módulos que le permiten utilizar una gran gama de lenguajes y desarrollar funcionalidades avanzadas.

Existen otros servidores web además de apache, por ejemplo:

- AOLServer
- IIS
- Zope
- Tomcat o Jakarta Apache

El servidor web apache, es uno de los más utilizados actualmente en Internet desde finales de los 90´s.

Apache generalmente se inicia como usuario root, enseguida atiende las peticiones recibidas. Hay que tener cuidado de que esté protegido a modificaciones por otros usuarios. No sólo los ficheros deben ser modificables sólo por root, sino también los directorios y los padres de estos directorios. Por ejemplo, si situamos la raíz del servidor en */usr/local/apache* (este directorio debe crearse como root).

Arranque y parada del servidor

Si se desea que el servidor escuche por el puerto 80 (predeterminado), que es un puerto reservado, habrá que lanzarlo como root. Tenemos dos posibilidades y son:

- Ejecutar httpd *(usr/local/apache/bin/httpd,)*
- Ejecutar apachectl start. *(usr/local/apache/bin/apachectl start)* esta última siendo la opción más recomendable.

Esto buscará el fichero de configuración (*httpd.conf*) en el lugar compilado en el código (por defecto */usr/local/apache/conf/httpd.conf*). Si está en otro sitio se puede indicar con la opción -f.

Localhost:/home/redes# /usr/sbin/httpd -f /etc/httpd/httpd.conf

Una vez arrancado se puede acceder a la documentación utilizando el navegador:

Localhost:/home/redes# http://localhost

Cuando el servidor arranque creará varios procesos hijos para atender las solicitudes. Si se inició apache como usuario root, el proceso apache continuará ejecutándose como root mientras los hijos cambiarán al usuario indicado en el httpd.conf.

Si se desea que el servidor continúe ejecutándose tras reiniciar el sistema debe incluirse en uno de los ficheros de inicio (por ejemplo: rc.local).

Configuración del servidor

Entre los archivos de configuración *(/usr/local/apache/conf*) tenemos:

a) **httpd.conf**: Establece los atributos generales del servidor, número de puerto en el que escucha, usuario que lo ejecuta, raíz del árbol de documentos, etc. Se recomienda establecer todas las opciones de configuración necesarias en este fichero, y dejar los otros dos ficheros de configuración vacíos, esto simplifica la administración del servidor.
b) **srm.conf**: Se utilizaba para establecer la raíz del árbol de documentos.
c) **access.conf**: Establece la política de acceso.

Además de estos tres ficheros el comportamiento del servidor puede configurarse directorio a directorio mediante ficheros, ***.htaccess*** en los directorios – que contienen documentos html - a los que el servidor accede.

Es muy importante recordar que **cuando se cambia la configuración de los ficheros es necesario reiniciar el servidor apache** *(apachectl restart)* o enviarle una señal de SIGHUP con kill para que los cambios tengan efecto. Hay que estar seguro de que se envía la señal al proceso padre y no al hijo. El padre en general es el que tiene un número de proceso menor. El id del proceso del padre está también en el fichero *httpd.pid* en el directorio *log.*

3.- Equipo y material necesario

Equipo del Laboratorio:

- 1 Computadora con un sistema operativo Kali Linux.

Material del alumno:

- Archivos necesarios para la creación de páginas html.

4.- Desarrollo

4.1.1 Inicie el equipo en Kali Linux. Una vez ejecutado el sistema, abra una terminal, de clic en Aplicaciones > Accesorios > Terminal (Ver la figura No. 1).

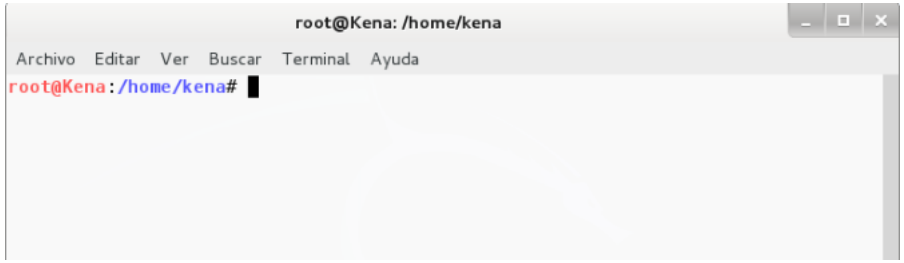


Figura No.1. Terminal de Kali Linux.

4.1.2 El servidor Apache se encuentra pre-instalado en Kali Linux, para instalarlo debe tener los privilegios de súper usuario. Con los siguientes comandos instalamos el servidor Apache.

 # apt-get install apache2 elinks

En el momento de su instalación, solicitará permisos para usar el disco duro, lo cual debe aceptar para completar la instalación.

4.1.3 Para que el servidor Apache funcione correctamente reinicie los servicios, ingrese los siguientes comandos :

/etc/init.d/apache2 restart

4.1.4 Es necesario la creación de un alias, para brindar los permisos necesarios a las páginas www. La creación será dentro del directorio */var/www/pub*. Ingrese a la siguiente ruta:

 # cd /etc/apache/sites-avaible

4.1.5 En esa ruta se creará el archivo de configuración, el cual se llamará alias, ingrese los siguientes comandos:

#vim alias.conf

Este archivo deberá contener la siguiente información:

alias /pub/var/www/pub
<Directory "/var/www/pub"> Options Indexes Includes FollowSymLins all </Directory>}}}
(Ver Figura No.2):

Figura No.2. Configuración del archivo.

Guarde y salga del archivo con los siguientes comandos:
:wq

4.1.6 Diríjase a la siguiente ruta:

 # cd /var/www

4.1.7 Cree el directorio pub, de los permisos de uso. Ingrese los siguientes comandos:

 # mkdir pub
 # chown root.www-data pub –R

4.1.8 Al finalizar reinicie el servidor apache:

#/etc/init.d/apache2 reload

4.1.9 Conforme a la investigación previa ingrese los datos necesarios para visualizar su página web. Muestre a su profesor

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

PRÁCTICA 10

Instalación de un servidor Apache

Cuestionario Previo

Nombre del alumno:**_____**

Gpo. de Laboratorio:**_____** ***Gpo. de Teoría:*****_____**

1. Investigue cómo crear una página web sencilla.
2. Investigue cómo incluir los archivos de una página web en un servidor apache.
3. Investigue la función de las siguientes herramientas:

   Nickto
   W3af
4. Investigue las vulnerabilidades del servidor Apache e indique posibles soluciones.

PRÁCTICA 11

TCP y UDP

1.- Objetivos de Aprendizaje

- El alumno configurará un programa que le permitirá enviar y recibir información utilizando los protocolos TCP y UDP, reafirmando los conceptos teóricos.
- El alumno será capaz de crear un socket servidor y un socket cliente

2.- Conceptos teóricos

El programa Sock

El programa sock ofrece un modo de acceder a la interfaz de los sockets sin tener que programar. Conecta la entrada/salida estándar (teclado/pantalla) con un socket cuyas características se especifican mediante parámetros al ejecutar la orden. Mediante la redirección de la entrada o la salida se puede enviar el contenido de un archivo o almacenar en un archivo la información recibida.

Los sockets pueden ser de dos tipos: UDP que no garantiza ni la entrega ni el orden de entrega de la información o TCP que garantiza la entrega ordenada y sin errores de la información.

Además, se sabe que una aplicación puede comenzar iniciando la comunicación (enviando información) o bien puede esperar pacientemente hasta que la otra le solicite el inicio de la comunicación (espera petición).

El programa sock va a permitir imitar cualquiera de estas situaciones, entre otras.

3.- Equipo y material necesario

3.1 Material del alumno:

- Imagen extensión BMP con calidad de una imagen fotográfica.

3.2 Equipo del Laboratorio:

- Programa sock (sock-1.1.tar.tar).

4.- Desarrollo:

4.1 Preparación del programa Sock

4.1.1 Encienda el sistema y elija la opción de cargar *Linux*.

4.1.2 Inicie sesión como usuario **redes**, el profesor le proporcionará la contraseña.

4.1.3 Abra una terminal de comandos (Figura No. 1)

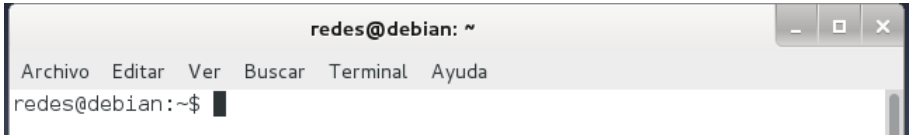


Figura No. 1. Terminal de comandos

4.1.4 Cree el subdirectorio ***practica*** dentro del directorio actual (Ver Figura No. 2)

NOTA: Evite cambiarle el nombre al subdirectorio, deberá llamarse ***practica*****,** sin ningún número posteriormente ni abreviatura alguna, nombres como prac8, p8, practica8, etcétera, serán inválidos.

mkdir practica

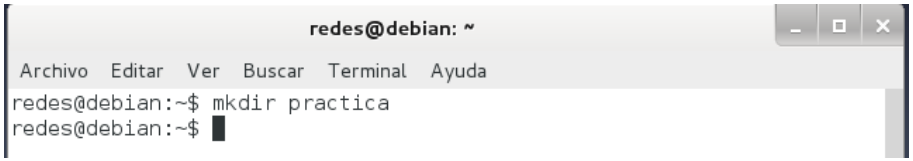


Figura No. 2. Creación del subdirectorio "practica"

4.1.5 Copie el archivo sock-1.1.tar.tar dentro del subdirectorio ***práctica***. (Ver figura No. 3)

cp sock-1.1.tar.tar /home/redes/practica

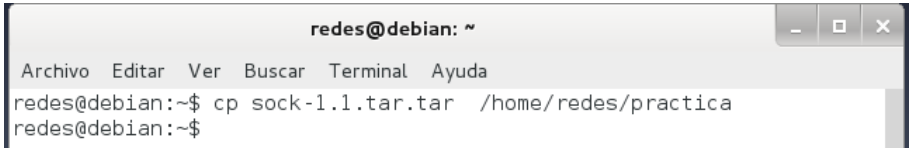


Figura No. 3. Copia del archivo sock

4.1.6 Cámbiese al subdirectorio ***practica*** y descomprima el archivo *sock-1.1.tar.tar* (Ver Figura No. 4)

cd practica
tar xvf sock-1.1.tar.tar

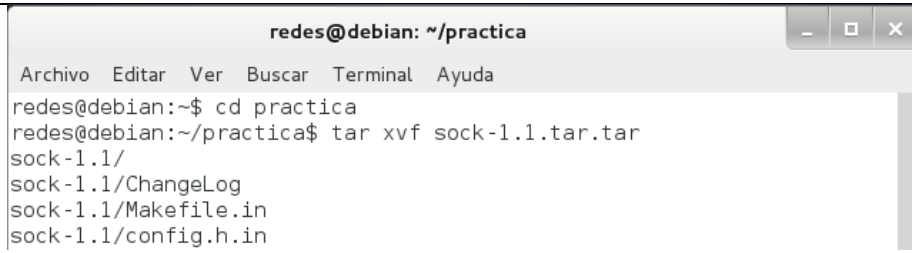


Figura No. 4. Archivos en sock antes comprimidos.

4.1.7 Sitúese dentro del subdirectorio sock-1.1 y ejecute la orden **./configure** con la que el programa quedará preparado para su compilación y montaje. (Ver Figura No. 5)

cd sock-1.1
./configure

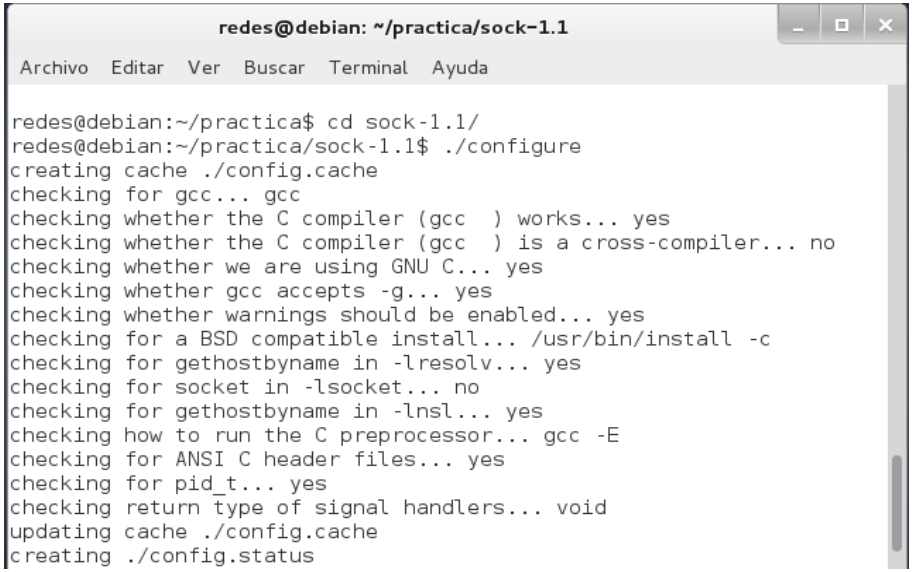


Figura No. 5. Configuración de archivos y creación de un "Makefile"

4.1.8 Compile el programa. Ahora ya disponemos del programa sock ejecutable. (Ver figura No. 6)

make

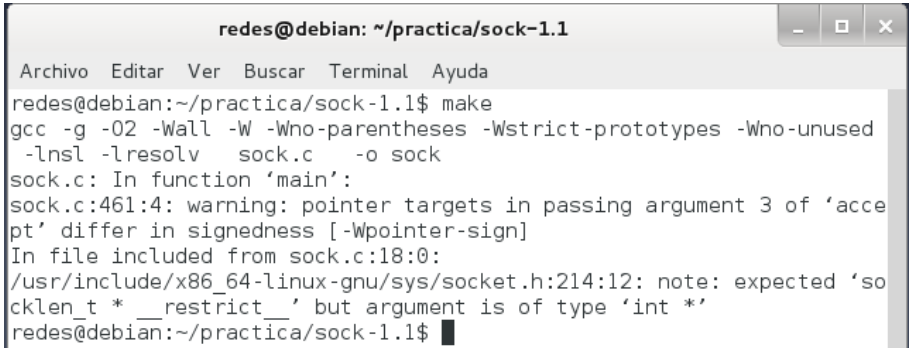


Figura No. 6. Compilación de archivos

4.2 Clientes TCP

4.2.1 Vamos a comenzar viendo qué sucede cuando un navegador se dirige a un servidor de web y le solicita una página. En el shell teclee lo siguiente **. /sock –e www.fi-b.unam.mx:80** y después de pulsar la tecla "ENTER", escriba el texto **GET / HTTP/1.0** Finalice presionando dos veces "ENTER"(Ver figura No. 7).

. /sock –e www.fi-b.unam.mx:80
GET / HTTP/1.0

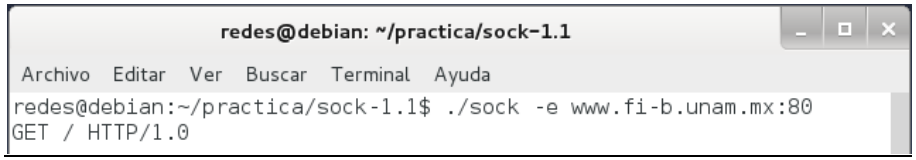


Figura No.7. Socket hacia www.fi-b.unam.mx

Con esto se está conectando al servidor www.fi-b.unam.mx (que es el servidor web de la DIE) al puerto 80, que es donde se encuentra este servicio habitualmente (well-known port) y se utiliza el protocolo TCP. Lo que estamos haciendo es crear un socket en nuestra computadora.

Ese socket, que actúa como cliente, lo conectamos al servidor de web de la DIE y le solicitamos que nos envíe el contenido de su página web inicial. La conexión iniciada por el programa sock se realiza al puerto 80 del servidor www.fi-b.unam.mx y dura sólo lo indispensable hasta que se entrega la página web solicitada. Es importante destacar que la respuesta del servidor contiene una información del protocolo HTTP (o cabecera) a la que sigue, después de una línea en blanco, el código HTML de la página solicitada. Tras enviar esa información el servidor cierra la conexión, con lo cual la ejecución de la orden sock finaliza.

4.3 Servidor TCP

Los programas pueden esperar pacientemente a que se les solicite algo antes de enviar alguna información. Éste es el comportamiento de muchos servidores. Utilizando el programa sock va a crear un servidor cuya única función es esperar a que un cliente se conecte y luego conecta la entrada y salida estándar con ese cliente.

4.3.1 Para crear un socket servidor, teclee lo siguiente en el shell:

./sock -le :7701

4.3.2 Ahora, abra un nuevo shell, sitúese en el subdirectorio sock-1.1 y ejecute la siguiente orden: (Ver figura No. 9).

./sock -e :7701

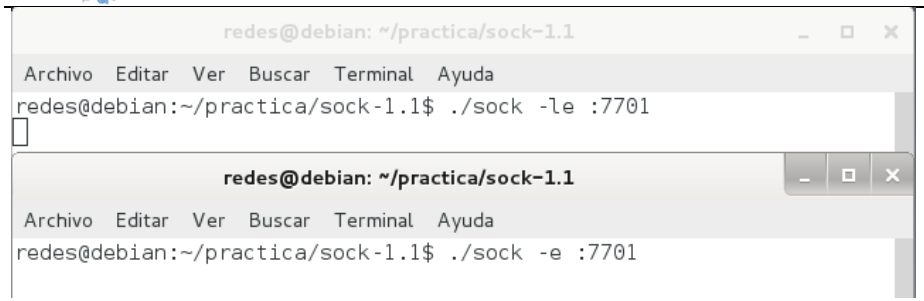


Figura No. 9. Creación de un socket servidor y de un socket cliente

4.3.3 Escriba en el Shell cliente y después teclee "ENTER" observe los que sucede en el Shell servidor. Seguidamente escriba en el Shell servidor, ¿qué sucede en el Shell cliente? (Ver figura No. 10).

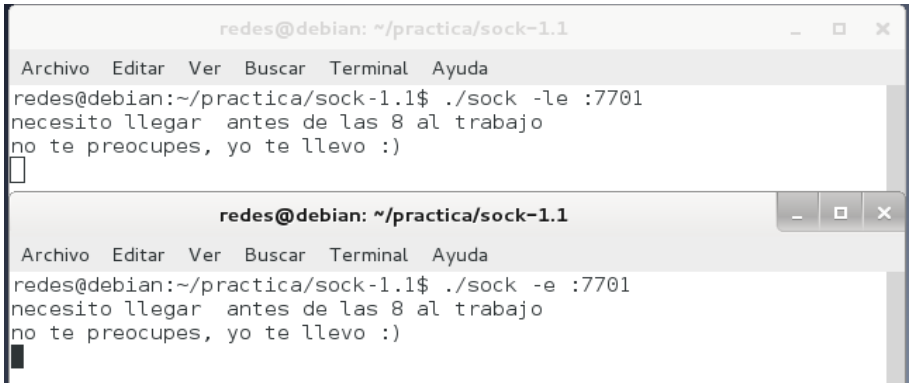


Figura No. 10. Comunicación entre terminales

Salga con CTRL + C

La orden del punto 4.3.2 es equivalente a: *telnet localhost 7701*

El parámetro -l hace que la aplicación configure el socket en modo escucha (*listen*) y acepte peticiones. Por tanto, en el punto 4.3.1 ha puesto en marcha, en su computadora, un servidor que escucha en el puerto 7701. Mientras que las órdenes de los pasos 4.3.2 y 4.3.3 han arrancado clientes TCP que se han conectado a ese puerto.

4.3.4 En un shell, sitúese en el subdirectorio sock-1.1 y cree un socket servidor tecleando lo siguiente:

./sock -l :7701 -d ls

4.3.5 Ahora, en otro shell, sitúese en el subdirectorio sock-1.1 y cree un socket cliente ejecutando la orden: (Ver figura No. 11).

./sock -e :7701

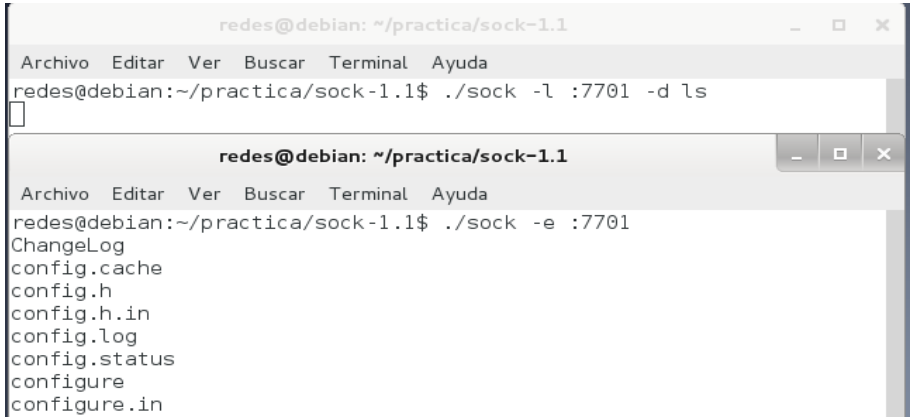


Figura No. 11. Creación de un socket servidor y cliente

4.3.6 Observe lo que sucede.

En este experimento se ha construido un **"miniservidor"**. Lo que hace el programa es esperar la conexión de un usuario al puerto indicado (7701 en este caso) y cuando el cliente se conecta (mediante la orden sock o el programa telnet) entonces ejecuta la orden *ls* que lista el contenido del directorio y lo envía a través del socket. Una vez finalizada la orden *ls* el servidor corta la conexión del cliente telnet, pero sigue escuchando en el puerto para atender nuevas peticiones de otros clientes.

Si se sustituye la orden ***'ls'*** por la orden ***'date'*** en el punto 4.3.4 tendrá un miniservidor de fecha y hora.

4.4 El protocolo UDP

Del mismo modo que en los ejemplos anteriores ha utilizado el protocolo TCP, ahora va a ver cómo se puede enviar información mediante el protocolo UDP. Para ello mantendrá los dos shells que tiene abiertos.

4.4.1 En un shell cree un socket servidor tecleando lo siguiente:

./sock -ul :7701

4.4.2 Y en otro shell ejecute la orden: (Ver Figura No. 12).

./sock -u :7701

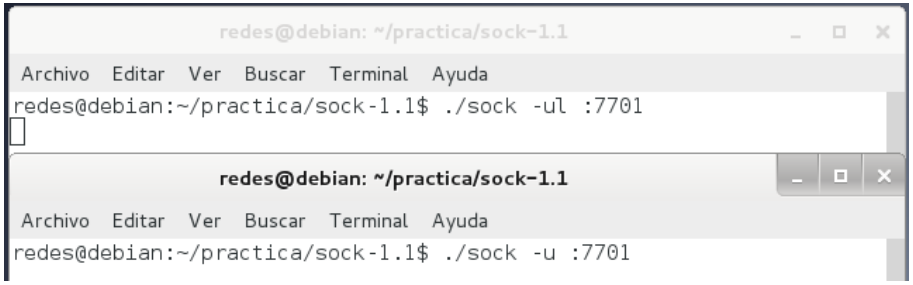


Figura No.12. Socket servidor y cliente.

4.4.3 Escriba en el Shell cliente y después del ENTER observe lo que sucede en el Shell servidor. (Ver figura No. 13). Realice la prueba del shell servidor hacia el cliente.

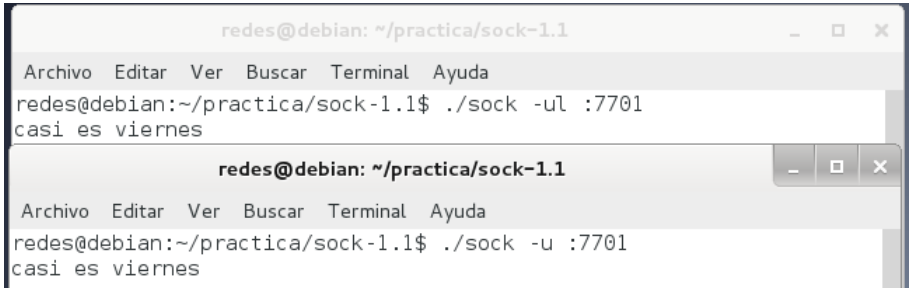


Figura No. 13. Comunicación entre terminales.

Comente lo que sucede

Salga con CTRL + C, en el Shell del cliente.

4.4.4 Ahora en el Shell cliente cambie la orden del paso número 4.4.2 por la siguiente: (Ver figura No. 14).

date | ./sock -u :7701

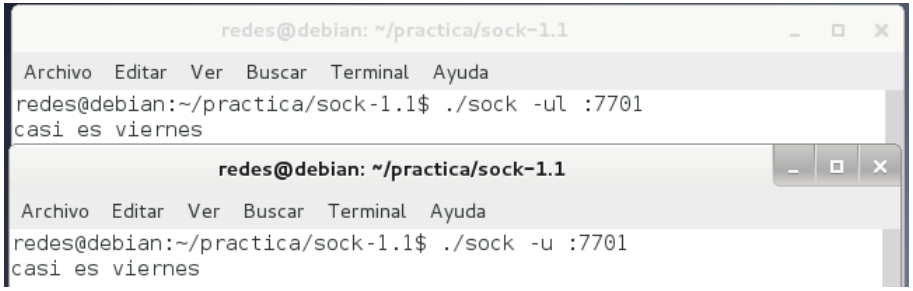


Figura No. 14. Comunicación entre terminales.

Como ve el funcionamiento es bastante similar, pero al carecer UDP del concepto de conexión no se puede construir un servidor de manera tan sencilla.

Pero la razón que hace que UDP tenga utilidad para muchas aplicaciones es su capacidad para hacer difusiones (enviando a la dirección 255.255.255.255 realmente se envía un datagrama que será recibido por todas las computadoras de la misma red IP). Sin embargo y por motivos de seguridad, el uso de esta característica está restringido y no se empleará en esta práctica.

Una forma de evitar esta restricción es emplear la dirección IP de multicast que esté configurada en todos sus equipos como si se tratara de una dirección de difusión.

4.5 Transferencia de archivos

En los ejercicios anteriores ha visto algunos de los usos que nos permite un socket. Ahora va a utilizar los servicios de TCP y UDP para el envío de archivos entre dos computadoras.

En el siguiente ejercicio se mostrará cómo transferir un archivo empleando el programa sock:

4.5.1 Copie una imagen al subdirectorio (por ejemplo dibujo.bmp) /home/redes/practica/sock-1.1

4.5.2 Ahora va a enviar la imagen tecleando en el Shell emisor (Ver figura No. 15):

NOTA1: *cat* es un comando que no puede ser omitido.

NOTA2: "dibujo.bmp" es el nombre original de la imagen.

./sock -l :8888 -d 'cat dibujo.bmp'

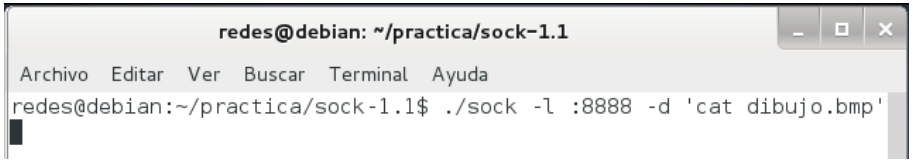


Figura No.15. Envío de la imagen desde el Shell emisor.

4.5.3 Conéctese a la máquina que le indique su profesor con la cuenta **redes** desde uno de los Shells tecleando: (Ver figura No. 16).

ssh –l redes XX

NOTA: XX se sustituirá por la IP de la computadora.

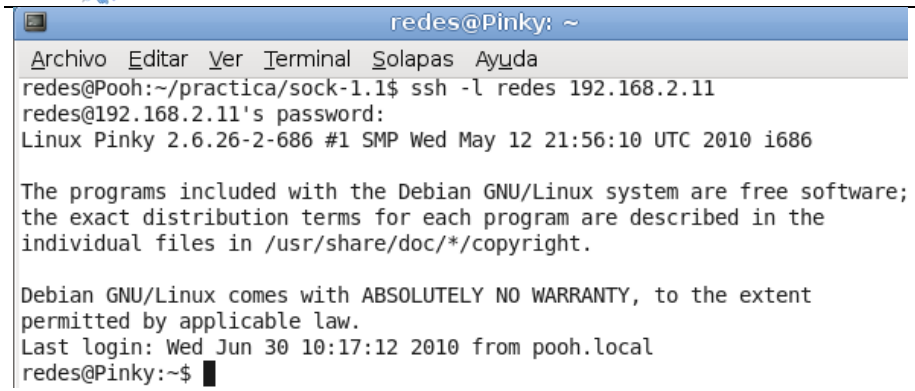


Figura No. 16. Conexión por medio de ssh en el Shell receptor

4.5.4 En el Shell del paso anterior, sitúese en el subdirectorio sock-1.1 y teclee: (Ver figura No. 17).

cd practica/sock-1.1
./sock –e XX:8888>imagen2.bmp

NOTA: XX se sustituirá por la IP de su computadora

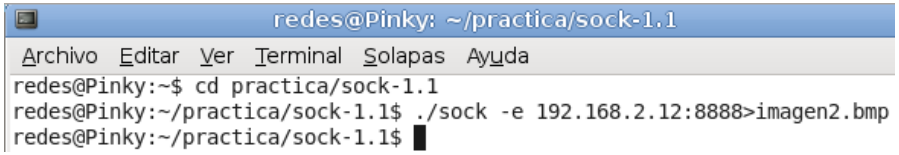


Figura No. 17. Recepción de la imagen en el Shell receptor

NOTA 2: "imagen2.bmp" es un segundo nombre para la imagen

4.5.5 Compruebe que el archivo recibido en la máquina con la cual se conectó tiene el mismo tamaño que el original, utilice el comando: *ls -la*. (Ver figura No. 18).

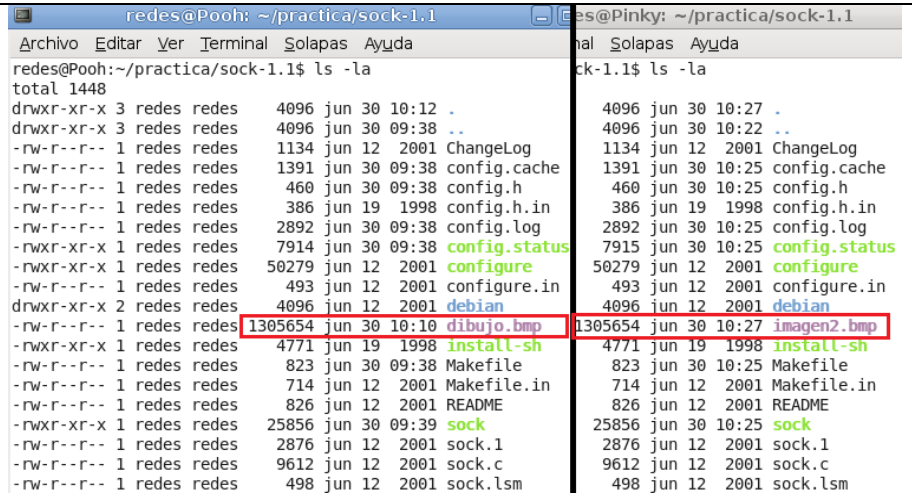


Figura No.18. Comparación de los archivos.

En este ejercicio se ha realizado la transferencia del archivo mediante el protocolo TCP. Su computadora ha quedado a la espera de un cliente en el paso 4.5.2. Y desde la máquina de al lado se ha conectado como tal cliente en el paso 4.5.4.

Es interesante resaltar que aunque el archivo resultante tenga el mismo tamaño, eso no garantiza que la transferencia ha tenido éxito (¿y sí el contenido fuera diferente?). Ahora enviará el archivo de vuelta para poderlo comprobar, pero empleando el protocolo UDP.

Escriba "exit" en ambos Shells hasta cerrarlos.

4.5.6 Abra un shell, sitúese en el subdirectorio sock-1.1 y teclee (Ver figura No. 19):

cd practica/sock-1.1
./sock -ul :8888>dibujo2.bmp

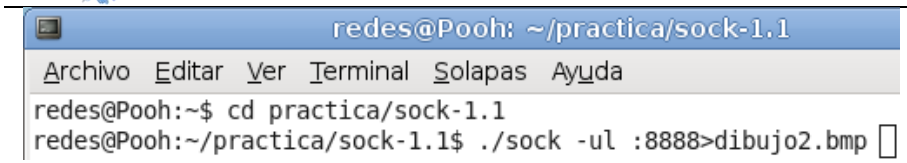


Figura No.19. Recepción del archivo

Lo que le prepara para recibir el archivo, -u indica UDP

NOTA: "dibujo2.bmp" es un tercer nombre para la imagen para diferenciarlo de los anteriores.

4.5.7 Abra un segundo Shell y conéctese con la cuenta redes a la máquina con la que realizó la conexión anterior desde un shell tecleando: (Ver figura No. 20).

ssh –l redes XX

NOTA: XX se sustituirá por la IP de la computadora remota.

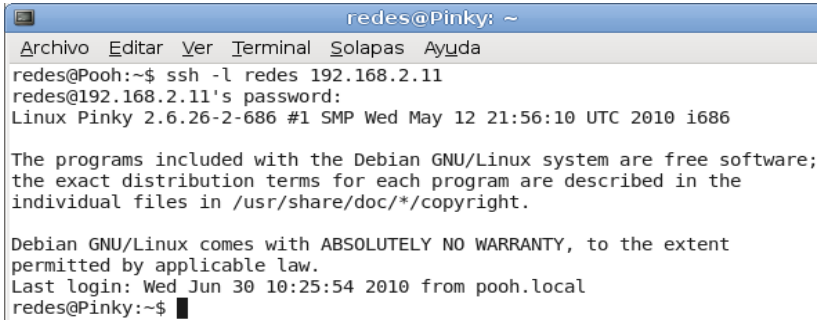


Figura No. 20. Conexión por medio de ssh

4.5.8 En el mismo Shell del paso anterior, sitúese en el subdirectorio sock-1.1 y teclee lo siguiente para enviar el archivo: (Ver figura No. 21).

cd practica/sock-1.1
cat imagen2.bmp | ./sock –u XX:8888

NOTA: XX se sustituirá por la IP de su computadora

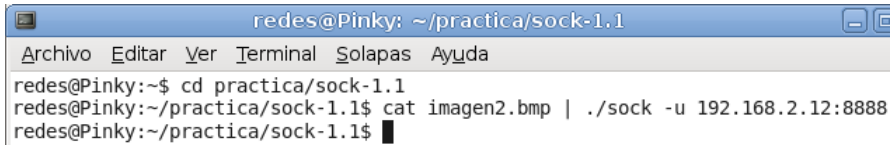


Figura No.21. Envío del archivo

4.5.9 A continuación, finalice la orden del paso 4.5.8 pulsando <Ctrl>+<c> en el primer shell (asegúrese de que la ha seleccionado primero, haciendo clic con el ratón). (Ver figura No. 22).

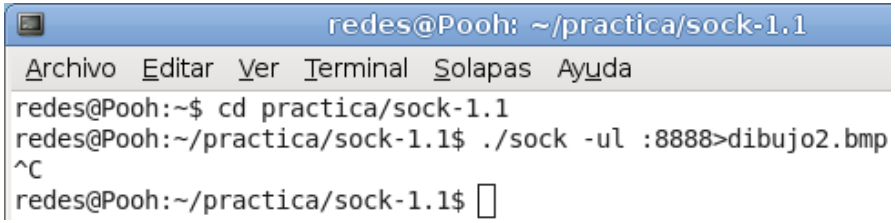


Figura No. 22. Final de la instrucción

4.5.10 Compruebe que los archivos "imagen2.bmp" (enviado) y "dibujo2.bmp" (recibido) son iguales con la orden *ls -la*. (Ver figura No. 23).

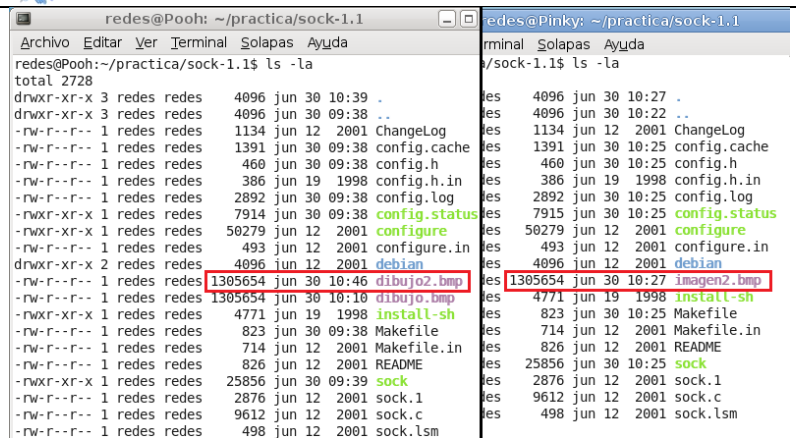


Figura No. 23. Comparación de la imagen enviada y recibida

Si ambos archivos son iguales entonces podrá concluir que tanto la transmisión desde su computadora a la de al lado, empleando TCP, como la vuelta, empleando UDP, no han sufrido errores. Si repite la operación con un archivo mayor (por ejemplo, el enunciado de esta práctica en pdf) encontrará que la transmisión por TCP no tiene problemas pero la de UDP fallará eventualmente, aunque este punto no se realizará.

4.5.11 Cierre el shell que está conectado a la sesión remota. (Ver figura No. 24).

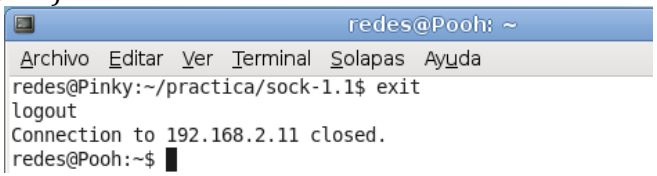


Figura No. 24. Cierre de la conexión por ssh.

4.5.12 En el otro Shell, borre el subdirectorio sock-1.1, el subdirectorio ***práctica*** y cierre el shell.

rm –rf practica
exit

4.5.13 Reinicie el equipo.

5.-Cuestionario

1. De acuerdo con lo visto en el desarrollo de la práctica ¿qué diferencias sustanciales existen entre TCP y UDP?

2. ¿Por qué la conexión iniciada por el socket al servidor sólo dura lo necesario para recibir la información requerida?

3. Mencione algunos ejemplos de los usos de TCP y UDP

6.- Conclusiones.

Revise los objetivos planteados al inicio de la práctica y concluya.

PRÁCTICA 11

TCP y UDP

Cuestionario Previo

Nombre del alumno:_____

Gpo. de Laboratorio:_____ ***Gpo. de Teoría:_____***

1. ¿Qué es un socket y qué se necesita para crearlo?
2. ¿Qué es un puerto?
3. ¿Cuáles son los rangos de puertos existentes?
4. ¿Qué rangos de puertos pueden utilizarse para establecer comunicaciones?
5. ¿Qué es el modelo cliente servidor?

PRÁCTICA 12

Ruptura de claves WPA2 Y WEP

1.- Objetivos de Aprendizaje

- El alumno conocerá y aplicará el método para descifrar claves WPA y WEP, atacando la debilidad de su cifrado..

2.- Conceptos teóricos

El término ***seguridad*** cotidianamente se refiere a la ausencia de riesgo o a la confianza en algo o en alguien. Sin embargo, puede tomar diversos sentidos según el área o campo al que haga referencia.

La ***Seguridad informática*** se define como un conjunto de medidas que impidan la ejecución de operaciones no autorizadas sobre un sistema o red informática, estas medidas son un conjunto de reglas, planes, actividades y herramientas.

La operación no autorizada en un sistema informático puede dañar la información, comprometer la triada de seguridad (confidencialidad, autenticidad, integridad), además de llegar a disminuir el rendimiento de los equipos, desactivar los servicios o bien bloquear el acceso a usuarios autorizados.

El sistema Wi-Fi es uno de los medios más utilizados para conectarse a Internet, aunque esto no implica que sea el método más seguro. El no contar con una cultura de buenas prácticas al momento de realizar la conexión, permite que haya vulnerabilidades disponibles para intrusos, dando como resultado el daño del sistema.

La **encriptación WEP** es poco segura ya que es abierta y cualquiera puede tener acceso a la clave del Wi-Fi, que se está usando.

La **encriptación WPA Enterprise** es la más segura, pero poco conocido, consiste en guardar el usuario y la contraseña en un servidor especial y dedicado para este servicio.

La encriptación mas recomendada es **WPA/WPA2**, ya que la clave únicamente se puede obtener por medio de un ataque conocido como fuerza bruta. Este ataque se realiza ocupando un diccionario con varias claves de router haciendo que alguna coincida.

WPA es un sistema para proteger las redes inalámbricas (Wi-fi), creado para corregir las deficiencias del sistema. Adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red.

WEP es el acrónimo de “Privacidad Equivalente a Cableado” este sistema de cifrado se encuentra incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite.

La vulnerabilidad más importante que existe es la de dejarle la clave por defecto que trae el fabricante, este tipo de claves vienen incluidas en los diccionarios existentes, lo que hace que sea más fácil el ataque.

Para realizar el análisis, Kali cuenta con la suite Aircrack la cual se especializa en la recolección e inyección de paquetes y el cálculo del ataque mediante ataques específicos.

Dentro de esta suite hay cuatro utilidades importantes:

a) Airmon-ng. Ayuda a poner al interfaz en modo monitor (modo sniffer):
b) Airodump-ng. Detecta y recopila información de las redes cercanas a la interface de la red.
c) Aireplay-ng. Permite inyectar tráfico, desconectar usuarios y falsear autenticaciones en los puntos de acceso.
d) Aircrack-ng. Es un analizador de paquetes que permite calcular la clave con base en la información proporcionada por aidodump-ng.

Se recomienda la desactivación de WPS para eliminar esta vulnerabilidad, algunos proveedores han desarrollado guías especiales para su desactivación.

3.- Equipo y material necesario

Material del alumno:

- 1 Laptop con sistema Operativo Kali Linux (por parejas).
- Diccionario para ataque de fuerza bruta.

Nota para el profesor: Indicar las especificaciones del diccionario, así como el idioma.

Equipo del Laboratorio:

- 2 Routers inalámbricos con seguridad WAP.

4.- Desarrollo:

Modo de trabajar

Esta práctica se realiza por parejas, donde al menos uno deberá de contar con su computadora personal con red inalámbrica y el sistema operativo.

4.1 Encriptación WPA2

4.1.1 Ejecute una terminal de Kali (en modo de súper usuario), verifique cuál es la interface de red inalámbrica.

 # ifconfig

4.1.2 Es importante saber a qué interface se hace referencia en el modo monitor. Una vez conocida la interface ejecute.

 # airmon-ng stop ***INTERFACE***

donde ***INTERFACE*** es el identificador de la tarjeta inalámbrica. El modo monitor está detenido.

4.1.3 El modo monitor es utilizado para poner la interfaz en modo promiscuo, lo cual le permitirá escuchar todo lo que pasa en la red, iníciela con el siguiente comando:

 # airmon-ng start ***INTERFACE***

4.1.4 Busque las redes inalámbricas cercanas mediante el comando:

 # airodump-ng ***INTERFACE***

4.1.5 Una vez que se registre en la lista la red que se desea atacar se debe poner atención en los campos **BSSID** (dirección MAC del punto de acceso), **CHANNEL** (canal de transmisión) y **ESSID** (nombre de la red). Detén la auditoría de redes con CTRL+C. Ejecute nuevamente airodump-ng con los datos recolectados:

*# airodump-ng –bssid **BSSID** –c **CHANNEL** –w **ARCHIVO** **INTERFACE***

donde **ARCHIVO** especifica un fichero .CAP en el cual airodump almacenará los paquetes capturados de la red. Esta terminal deberá permanecer activa durante el ataque.

4.1.6 Abra una nueva terminal (en modo super usuario), donde aplicará una falsa autenticación, con la intención que el punto de acceso confíe en la interface atacante. Esto se realiza con la siguiente instrucción:

*# aireplay-ng -1 0 –a **BSSID** –h **MAC_FALSA** **INTERFACE***

Se enviará una falsa autenticación una vez al punto de acceso. El parámetro **MAC_FALSA** permite ocultar la dirección MAC real de la interface inalámbrica.

Si hay pocos clientes conectados, necesitamos inyectar más paquetes en este caso en la instrucción anterior modificamos el -1 por -3, con esto generamos más tráfico al inyectar paquetes ARP.

4.1.7 En una nueva terminal ejecute aircrack-ng para comenzar a deducir la clave de acceso a la red.

*# aircrack-ng –b **BSSID** –z **ARCHIVO***

Si el número de vectores de inicialización es suficiente, entonces la clave aparecerá en poco tiempo. De lo contrario, el ataque se reinicia cada que se colecten 5000 vectores de inicialización.

4.1.8 En una nueva terminal se aplicará una desconexión a alguna estación de trabajo con la intención de capturar el 4-way handshake, que la estación autorizada y el punto de acceso realizan para acordar comunicarse. La desconexión se realiza con aireplay.

*# aireplay-ng –death –a **BSSID** –c **MAC_CLIENTE** **INTERFACE***

donde **BSSID** es la dirección física del punto de acceso y **MAC_CLIENTE** es la dirección física del dispositivo conectado a la red WPA que se desconectará; es necesario que al menos un cliente esté conectado a la red para capturar su 4-way hanshake.

4.1.9 Una vez capturado el handshake se requiere el auxilio de un diccionario para atacar los mensajes cifrados que se han capturado en el archivo airodump. Un diccionario es un archivo de texto que contiene palabras frecuentemente utilizadas como claves. Puesto que el ataque es la aplicación de la fuerza bruta, el tiempo para encontrar la clave es variable y no necesariamente se tendrá éxito. La sintaxis de aircrack en este caso es la siguiente:

*# aircrack-ng –b **BSSID** –w **DICCIONARIO** –z **ARCHIVO***

donde **DICCIONARIO** es el archivo de texto que contiene las palabras a probar como posibles claves y **ARCHIVO** el archivo .CAP que contiene las tramas capturadas junto con los paquetes especiales del 4-way handshake.

4.2 Encriptación WEP

4.2.1 Para realizar la ruptura de claves del protocolo WEP, es necesario repetir los pasos 4.1.1 al 4.1.7.

5.- Cuestionario

1. Indique que es lo que se muestra en pantalla con el siguiente comando: **airmon-ng stop INTERFACE**

2. ¿Que pasa si cambiamos el -1 del siguiente comando por -5?
   # aireplay-ng -1 0 –a BSSID –h MAC_FALSA INTERFACE

3. ¿Qué aparece en pantalla al utilizar el DICCIONARIO?

4. Mencione al menos tres beneficios de usar la suite de Aircrack.

6.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

_____

_____

_____

_____

_____

_____

_____

_____

PRÁCTICA 12

Ruptura de claves WPA2 Y WEP

Cuestionario Previo

Nombre del alumno:_____

Gpo. de Laboratorio:_____ ***Gpo. de Teoría:_____***

1. ¿Qué es 4-way handshake?.
2. Mencione las vulnerabilidades de WPA.
3. ¿Para poder realizar el ataque se necesita forzosamente el diccionario? o ¿Existe alguna otra manera?
4. ¿Este tipo de ataques se pueden realizar en otras distribuciones de Linux? ¿Por qué?

PRÁCTICA 13

Configuración de VPN y DMZ en Packet Tracer

1.- Objetivos de Aprendizaje

- El alumno conocerá el manejo eficiente de las redes públicas y privadas, utilizando las configuraciones VPN y DMZ.

2.- Conceptos teóricos

Una Red Privada Virtual (VPN)) es una tecnología de red que permite crear una conexión segura de la red LAN sobre una red pública. Permiten el intercambio de información entre una red compartida o publica como si se tratase de una red privada con toda la funcionalidad, seguridad y políticas de gestión.

Las características de esta tecnología son:

- Requiere autenticación y autorización.
- Utiliza funciones has y sha.
- Utiliza los algoritmos de cifrado como DES, AES, 3DES, para tener confidencialidad/privacidad.
- Control de acceso.
- No repudio, es decir que el mensaje va firmado y el remitente no puede negar su envió.
- Reducción de costos y sencillez de uso.

Maneja 3 tipos de conexión y son:

- Conexión de acceso remoto.
- Conexión VPN router a router.
- Conexión VPN firewall a firewall.

IPsec es un protocolo utilizado en Internet, cuya función es asegurar las comunicaciones IP autenticando y cifrando cada paquete IP en un flujo de datos.

Algunas de sus características son:

- La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad.
- Asegura el flujo de paquetes.
- Garantiza la autenticación mutua.
- Establece parámetros criptográficos.

Consta de tres protocolos que son:

a) ***Authentication Header (AH):*** encargado de proporcionar integridad, autenticación y no repudio, eligiendo los algoritmos criptográficos apropiados.
b) ***Encapsulating Security Payload (ESP):*** proporciona confidencialidad.
c) ***Internet key Exchange (IKE):*** emplea un algoritmo tipo Diffie-Helman con el fin de establecer el secreto compartido de sesión.

El aislamiento por red es una arquitectura utilizada para crear políticas de seguridad, los firewall permiten definirlas solo entre dos redes y las grandes empresas manejan varias redes.

La DMZ (Zona desmilitarizada) es la creación de una red utilizada para separar la red interna de la externa, con el fin de evitar el uso indebido de los datos informáticos de servidores de alguna empresa. Los servidores DMZ (también conocidos como “servidores bastion”), por ser encargados de ofrecer seguridad en una red interna y son utilizados con el único fin de recibir los ataques de las redes externas.

Por lo general las políticas de seguridad son las siguientes:

- El tráfico de la red externa a la DMZ está autorizado.
- El tráfico de la red externa a la red interna está prohibido.
- El tráfico de la red interna a la DMZ está autorizado.
- El tráfico de la red interna a la red externa está autorizado.
- El tráfico de la DMZ a la red interna está prohibido.
- El tráfico de la DMZ a la red externa está denegado.

Listas de control de acceso.

Las ACL permiten controlar el flujo del tráfico en equipo de redes, donde el principal objetivo es permitir o denegar el tráfico de red de acuerdo a alguna condición.

Existen dos tipos de listas de control de acceso y son:

- ACL estándar; controlan el tráfico por medio de la comparación de la dirección de origen de los paquetes IP con las direcciones configuradas en la ACL.
- ACL extendida; Controlan el tráfico por medio de la comparación de las direcciones de origen y destino de los paquetes IP con las direcciones configuradas en la ACL

3.- Equipo y material necesario

Equipo del Laboratorio:

- 1 Computadora con un sistema operativo Windows 7 Profesional.
- Software de simulación de Cisco, Packet Tracer en su versión más reciente.

4.- Desarrollo

***4.1* Configuración de VPN.**

4.1.1 Arrastre al área de trabajo los dispositivos necesarios para crear la topología de la figura No. 1, los dispositivos a utilizar son: 3 router 2811, 3 switches 2950-24, 4 PC-PT y 3 Servidores Server-PT (FTP, HTTP, DNS) (véase la figura No. 1).

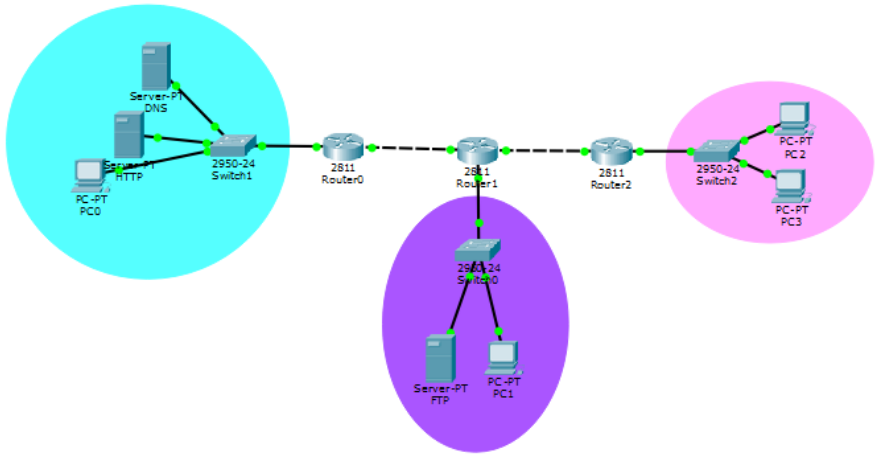


Figura No. 1. Topología VPN.

Nota: *Guarde su archivo de la siguiente manera; una copia con el nombre VPN y otra copia con el nombre DMZ.*

4.1.2 Dé clic sobre un router central (**Router1**), apáguelo y conecte el slot NM-1FE-TX que es un puerto Ethernet adicional. Posteriormente vuelva a encenderlo (Ver Figura No. 2).

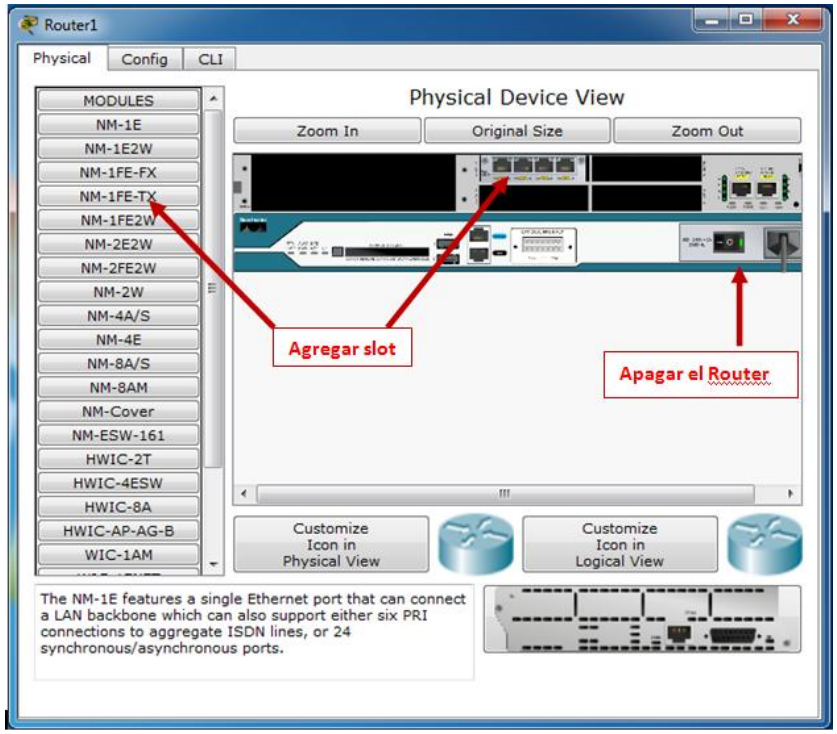


Figura No. 2. Inserción de slot.

4.1.3 Realice la configuración de los dispositivos e incluya el enrutamiento RIP v2. El segmento de red será proporcionado por el profesor. Verifique que haya comunicación

4.1.4 Para lograr la configuración es necesario crear una comunicación entre los routers que puedan establecer una autenticación y negociación. Esto se hace por medio del servicio isakm, que indicará las políticas de cifrado y autenticación, la cual se debe realizar en cada uno de los canales de comunicación. Acceda al R***outer0*** en modo global.

Router(config)#crypto isakm policy 5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#hash sha
Router(config-isakmp)#encryption aes
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#exit

Repetir en cada uno de los routers de la topología.

4.1.5 Una vez que se ha establecido la política, es necesario crear las claves de autenticación entre los routers de la topología. Ingrese al ***Router0.***

Router(config)#crypto isakmp key ***KEYVPN*** *address* ***IPADDRESS***
Router(config)#crypto ipsec transform-set ***EAGLE*** *esp-aes esp-sha-hmac*

Donde ***KEYVPN*** es la clave de autenticación para la política (que será la misma en cada router y elegida por los alumnos), ***IPADDRESS,*** es la dirección de la **"interface de *salida*"** al siguiente router de la red LAN, ***EAGLE*** será el nombre que llevará la transformación (elegida por los alumnos).

Repetir en cada uno de los routers de la topología

4.1.6 Para garantizar una comunicación segura se debe agregar una lista de control de acceso, ingrese los siguientes comandos:

Router(config)#access-list ***NUMBER*** *permit ip* ***ORIGEN WILDCARD DESTINO WILDCARD***

Donde ***NUMBER,*** es el número de la lista de control de acceso extendida (seleccionado por el alumno), ***ORIGEN*** *y* ***WILDCARD*** es el segmento de red origen del router, seguido de su wildcard, ***DESTINO*** *y* ***WILDCARD*** es el segmento de red destino al router que desea comunicarse, seguido de su wildcard.

NOTA.- La lista de acceso debe de realizarse de ambos lados de cada router, de lo contrario no habrá comunicación.

1. **¿Qué tipo de listas de acceso se debe usar y por qué?**

_____

_____

_____

4.1.7 Realizadas las autenticaciones y lista de control en cada router, se necesita hacer un mapa criptográfico que indicará el camino a seguir, para ello ingrese lo siguiente:

Router(config)#crypto map ***MAPNAME*** *10 ipsec-isakmp*
Router(config-crypto-map)#set peer ***IPADDRESS***
Router(config-crypto-map)#match address ***NUMBER***
Router(config-crypto-map)#set transform-set ***EAGLE***
Router(config-crypto-map)#exit

Donde ***MAPNAME***, es el nombre que llevará el mapa criptográfico, ***IPADDRESS*** es la dirección de la **"interface de salida"** del router, ***NUMBER***, es el número de la lista de control de acceso extendida, ***EAGLE*** será el nombre que llevará la transformación.

Nota: Los datos **MAPNAME**, **EAGLE** y **NUMBER** serán elegidos por los alumnos

4.1.8 Ahora le indicaremos al router en qué interfaz va a aplicar dichas reglas, cabe mencionar que siempre será a la salida del router (Ver figura No. 3).

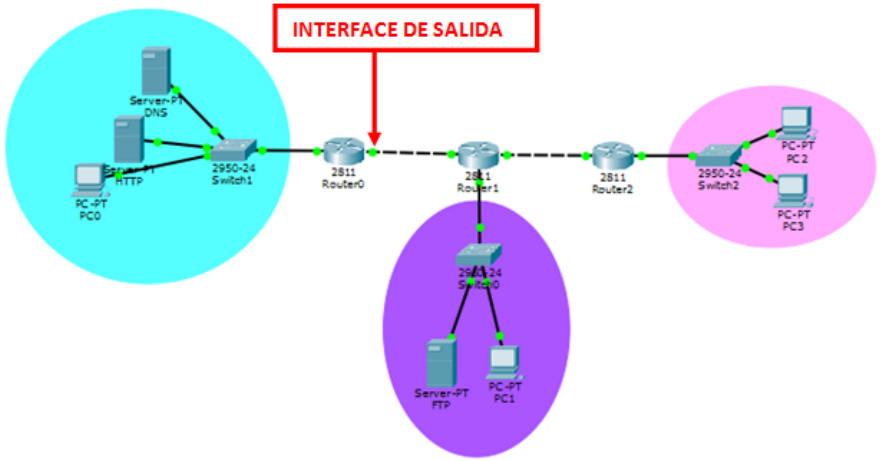


Figura No. 3. Interface de salida.

Router(config)#interface ***ID_INTERFACE***
Router(config-if)#crypto map ***MAPNAME***
Router(config-if)#do write
Router(config-if)#exit

Donde ***ID_INTERFACE*** corresponde a la interface de restricción fastethernet.

4.1.9 Para que haya comunicación entre las LAN es necesario incluir el método de enrutamiento rip versión 2. Ingrese los comandos necesarios y muestre a su profesor que haya comunicación.

2. **En el router central ingrese en modo privilegiado el siguiente comando e indique el resultado, analizando la imagen (véase la figura No. 4).**

#show crypto isakmp sa

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA
```

Figura No. 4. Resultados del comando crypto isakmp.

3. **En el router central ingrese en modo privilegiado el siguiente comando e indique el resultado, analizando la imagen (véase la figura No. 5).**

#show crypto ipsec sa

```
Router#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: SYSTEM, local addr 10.10.5.5

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.8.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current_peer 10.15.8.12 port 500
    PERMIT, flags={origin_is_acl,}
```

Figura No. 5. Resultados del comando crypto ipsec.

4.2 Configuración DMZ.

4.2.1 Abra el archivo nombrado DMZ, ingrese a modo privilegiado.

Router(config)#access-list ***NUMBER*** *permit ip* ***ORIGEN WILDCARD DESTINO WILDCARD***
Router(config)#access-list ***NUMBER*** *permit any*

Donde ***NUMBER,*** es el número de la lista de control de acceso extendida (seleccionada por el alumno), ***ORIGEN*** y ***WILDCARD*** es el segmento de red origen del router, seguido de su wildcard, ***DESTINO*** y ***WILDCARD*** es el segmento de red destino al router que desea comunicarse, seguido de su wildcard.

4.2.2 Debe indicar al router en que interface va a aplicar las reglas de acceso o denegación de trafico de red, lo cual será en la salida del router (Ver figura No. 6).

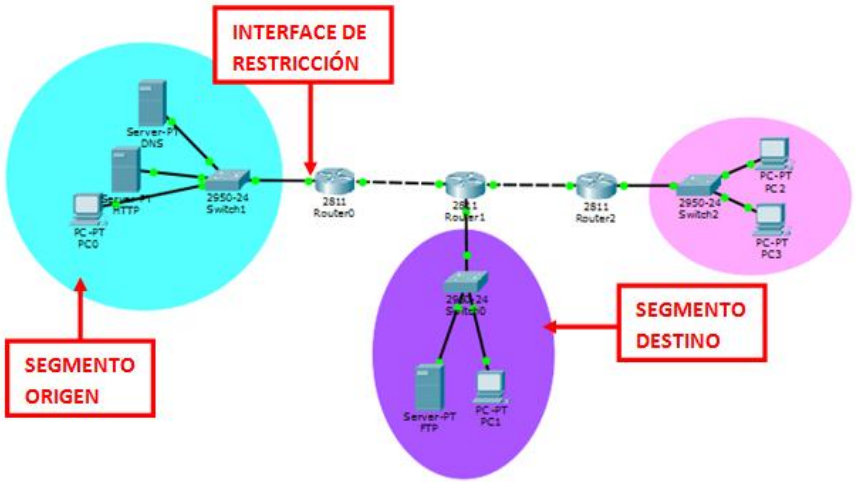


Figura No. 6. Identificación de segmentos.

Router(config)# interface ***ID_INTERFACE***
Router(config-if)#ip access-group ***NUMBER*** *out*
Router(config-if)#exit

Donde **ID_INTERFACE** corresponde a la interface de restricción fastethernet.

4. Ingresa el comando show running-config, analice el resultado.

6.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

PRÁCTICA 13

Configuración de VPN y DMZ en Packet Tracer

Cuestionario Previo

Nombre del alumno:_____

Gpo. de Laboratorio:_____ Gpo. de Teoría:_____

1. Investigue cómo se obtiene la Wildcard
2. Investigue los rangos que existen en las ACL.
3. Investigue para qué sirven las VPN y DMZ.