# Manual de prácticas del laboratorio de Administración de Redes

**(PAPIME PE101414)**

| Elaborado por: | Revisado por: | Autorizado por: | Vigente desde: |
|---|---|---|---|
| **M.C. Cintia Quezada Reyes**<br>**Ing. Magdalena Reyes Granados** | **M.C. Ma. Jaquelina López Barrientos**<br>**Ing. Edgar Martínez Meza**<br>**M.C. Cintia Quezada Reyes** | **Dra. Rocío Alejandra Aldeco Pérez** | **11 de agosto de 2023** |

# Índice de prácticas

# Práctica 1

# Configuración Básica de Redes

## Planeación

### *1.- Objetivo de aprendizaje*

- El alumno o la alumna aplicará los conocimientos adquiridos para la configuración del hardware, protocolos y software asociado a las redes locales de computadoras en los sistemas operativos Linux en su versión Debian y Windows.

- El alumno o la alumna empleará los parámetros y elementos que se deben considerar en el diseño de redes.

### *2.- Conceptos teóricos*

Una red de computadoras es un sistema de interconexión entre equipos que permite compartir recursos e información; para ello, es necesario contar no sólo con las computadoras, también con tarjetas de red, cables de conexión, dispositivos periféricos y el software conveniente.

Inicialmente, la instalación de una red se realiza con el objetivo de compartir dispositivos e información, pero a medida que crece, permite el enlace entre personas mediante diversas aplicaciones, como el correo electrónico, mensajes instantáneos, etcétera.

Las redes se clasifican de acuerdo con su alcance geográfico en PAN, LAN, MAN y WAN. Una red de área local está formada por computadoras, periféricos y los elementos de conexión de los mismos.

Las computadoras pueden desarrollar dos funciones: como servidores o estaciones de trabajo. Los elementos de conexión son los cables, tarjetas de red y los dispositivos de interconectividad como los hubs.

Dentro de los cables de conexión se tienen: el cable UTP, que consiste en dos hilos trenzados en forma independiente y recubiertos de una capa aislante, y que es considerado de fácil instalación; el cable STP, consistente en dos hilos trenzados en forma independiente y recubiertos de una malla metálica que ofrece una protección contra las interferencias externas; el cable coaxial, hilo de cobre envuelto en una malla trenzada, separado por un material aislante; y, finalmente, la fibra óptica, formada por un núcleo de material transparente fino cuyo funcionamiento se basa en la transmisión de las refracciones de luz.

En la actualidad, en el mundo de los sistemas de cableado estructurado existen diferentes tipos de servicios, por ejemplo, voz, datos, video, monitoreo, control de dispositivos, etcétera; éstos pueden transmitirse sobre un mismo tipo de cable. El estándar más conocido de cableado estructurado está definido por la EIA/TIA, y específicamente sobre el cable de par trenzado UTP de categoría 5e, 6 y 6a, estos estándares son: EIA/TIA 568A y EIA/TIA 568B.

Los dispositivos de interconexión proporcionan la capacidad de extender la distancia de cobertura de una LAN, interconectar redes distantes o distintas y acceder a recursos centralizados; de la misma manera, reducen los dominios de colisión y mejoran el rendimiento de las redes.

### *3.- Equipo y material necesario*

#### *3.1 Material que debe traer el alumno o la alumna*

- 1 Cable de conexión directa configuración T568-B UTP, categoría 5e o superior.
- 1 Cable de conexión cruzada categoría 5e o superior.
- 1 Flexómetro.

#### *3.2 Equipo del Laboratorio*

- 2 PC's Pentium con una NIC Ethernet 10/100 Mbps instalada en cada una de ellas.
- 1 Switch.
- 1 hub.

### *4.- Desarrollo*

#### *Modo de trabajar*

La práctica se desarrollará en equipos.

**NOTA:** Las actividades en este punto serán realizadas haciendo uso de un video como base y las explicaciones del profesor o profesora cuando la sesión de la clase se realice en modalidad a distancia.

#### *4.1 Cableado Estructurado aplicado en el laboratorio*

Esta primera parte consiste en analizar las características del cableado estructurado implementado en la red LAN Ethernet del Laboratorio de Redes y Seguridad. Se analizará la trayectoria que sigue el cable desde un nodo a través de la canaleta, hasta llegar al rack, donde es distribuido por el panel de parcheo y enlazado con cables patch cord al switch.

#### *Actividad opcional:*

Realice un diagrama físico de la red del Laboratorio, indicando los subsistemas del cableado estructurado y mostrando la ubicación de los equipos dentro del espacio geográfico, remarcando las conexiones con los jacks, número de nodos y cómo el cable UTP viaja a través de las canaletas hasta llegar al rack. El diagrama debe presentar las longitudes, así como el nombre específico de los hosts que integran a la red.

**El diagrama de red, se debe presentar y entregar al profesor o a la profesora en la siguiente sesión de laboratorio**; debe elaborarse con base en las indicaciones del profesor o de la profesora, de manera que sea entendible y permita la documentación de la red.

El panel de parcheo consiste en un bloque con un número determinado de tomas, el cual corresponde a la cantidad de puertos; es decir, un bloque de 24 tomas es un panel para 24 puertos. Vea la Figura No. 1.

**Figura No. 1 Panel de parcheo**

Indique en el siguiente diagrama, que muestra una sección de la parte frontal del panel de parcheo del Laboratorio de Redes, cada una de sus nombres y características. Véase la Figura No. 2.

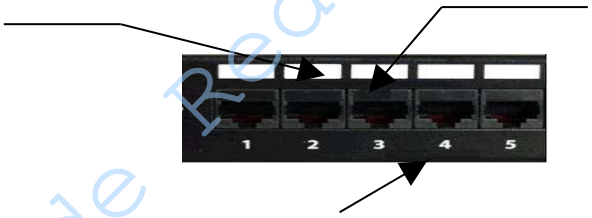



**Figura No. 2 Una sección frontal del panel de parcheo**

Indique los componentes de la parte trasera del panel de parcheo y su funcionamiento, tal como se muestra en la Figura No. 3.

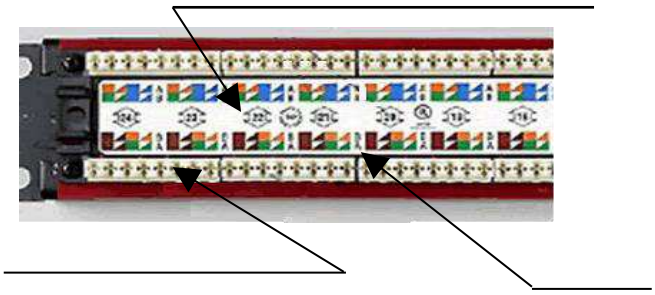


**Figura No. 3 Vista trasera del panel de parcheo**

### *4.2 Sistema Operativo Windows*

#### *4.2.1 Conexión punto a punto*

Esta segunda parte consiste en crear una red LAN Ethernet entre dos computadoras sin un dispositivo intermedio. Además de las conexiones físicas (capas de enlace de datos y física), será necesario realizar la configuración del protocolo TCP/IP de modo que exista comunicación.

**NOTA: No es necesario un hub o algún otro dispositivo de red para la interconexión en esta primera etapa.**

***Actividad:***

Anote la configuración IP existente en la Tabla 1.1 para poder restaurarla al final de la práctica.

***Tabla 1.1 Configuración de la IP en host A y en host B***

| Parámetros de configuración | Host A | Host B |
|---|---|---|
| **Dirección IP** | | |
| **Máscara de subred** | | |
| **Puerta de enlace predeterminada** | | |
| **Servidor DNS preferido** | | |
| **Servidor DNS alternativo** | | |

Realice la configuración necesaria para la interconexión punto a punto entre dos PC's, como se observa en la Figura No. 4.

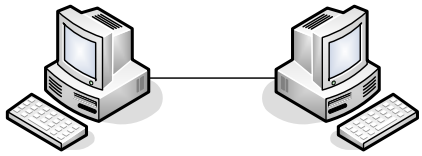


**Figura No. 4. Conexión punto a punto, sistema Windows**

Cuando termine de realizar la configuración punto a punto y las pruebas de conectividad, llame a su profesor o profesora para que revise la actividad.

### *4.2.2 Conexión a un hub o switch*

Los hubs son dispositivos que permiten interconectar cables de manera que simulan el comportamiento de un bus en común; se le puede considerar como un repetidor multipuerto, pues toma la señal que entra por un puerto y la repite en todos los demás. Un hub sirve para segmentar la red, pero no crea nuevos dominios de colisión.

Entre las principales ventajas de contar con un hub encontramos:

- En estándares como IEEE 802.3 y 803.5 se permite la interconexión de dispositivos mediante cables pares a un punto central, facilitando la incorporación de nuevos elementos a la red.
- Permite la implementación de la topología en estrella extendida, facilitando la extensión de la red.

Los hubs son los dispositivos más utilizados para la implementación de redes LAN, siendo la base de instalaciones del cableado estructurado.

Un hub Ethernet funciona de la siguiente manera: recibe la señal por un puerto a través del par de transmisión 3 y 6 del cable, la regenera, sincroniza y reenvía por todos los pares de recepción (par 1 y 2 del cable) al resto de los puertos.

***Actividad:***

En esta parte de la práctica el objetivo consiste en crear una red LAN Ethernet con dos o tres computadoras y un dispositivo de la capa 1 o 2, el dispositivo será proporcionado por el profesor o la profesora (Figura No. 5). Realice las conexiones y configuraciones necesarias.

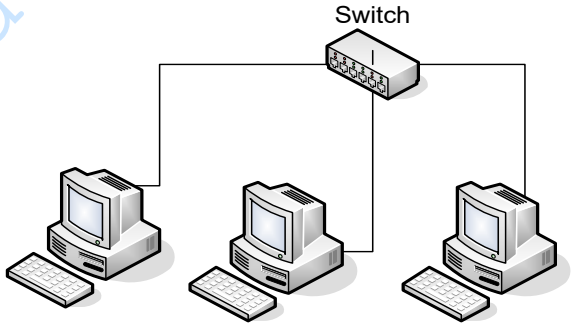



**Figura No. 5 Conexión con un hub, sistema Windows**

Cuando termine de realizar la configuración punto a punto y las pruebas de conectividad, llame a su profesor o profesora para que revise la actividad.

***Restablecimiento de la configuración***

Restablezca la configuración IP original de las computadoras, desconecte los equipos.

### *4.3 Sistema Operativo Linux*

#### *4.3.1 Conexión punto a punto*

El sistema operativo Linux es la base de muchos servidores en la red; conocer sus características de comportamiento, así como la manera de resolver problemas de configuración de red, es vital para los administradores.

Este punto de la práctica tiene por objetivo conectar dos computadoras directamente, creando una red, empleando el cable cruzado (crossover) en el sistema Debian.

***4.3.1.1*** Abra la aplicación VirtualBox

**NOTA: Antes de iniciar la máquina virtual verifique en la opción Red que se encuentre marcada la opción Habilitar adaptador de red->Conectado a: Adaptador puente (Figura No. 6).**

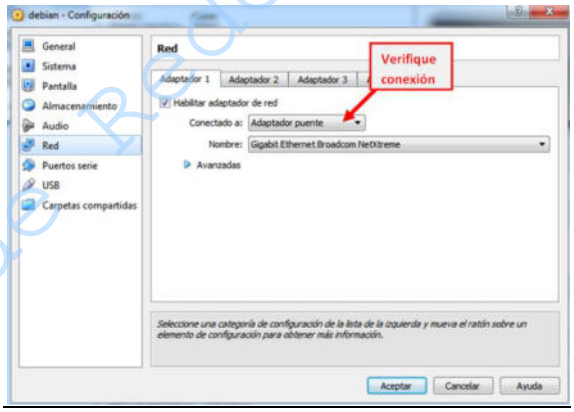



**Figura No. 6. Conexión de red.**

***4.3.1.2*** Encienda la máquina virtual

***4.3.1.3*** Elija la opción de cargar Linux, distribución Debian.

**NOTA: En caso de que le aparezca la imagen de instalación (Figura No. 7), dé clic derecho sobre el disco duro. Seleccione la opción que se encuentra palomeada para deseleccionarla, apague la máquina virtual y vuelva a iniciarla**.

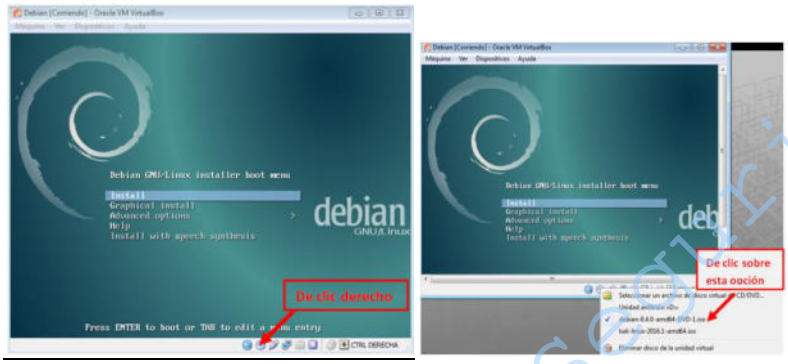



**Figura No. 7. Inicio de Máquina Virtual.**

***4.3.1.4*** Inicie sesión en la cuenta de **redes**.

***4.3.1.5*** Abra una terminal e ingrese como super usuario, para ello teclee el comando que se muestra a continuación. (Ver Figura No. 8)

**redes@debian:~$ su**

**NOTA: *su* significa super usuario, por lo que se emplea la misma contraseña de root**


**Figura No. 8. Terminal de comandos como root.**

***Actividad:***

Es indispensable iniciar la práctica con todos los dispositivos encendidos, en la sesión de root y el cableado desconectado.

**NOTA: Cualquier cambio que se realice en la configuración del equipo será responsabilidad de los alumnos asignados al equipo.**

**NOTA: Para realizar la práctica exitosamente debe tener instalado el paquete ifconfig.**
Escriba el siguiente comando para ver la configuración actual de la tarjeta de red.
**root@debian:/home/redes# ifconfig enp0s3**

Con la información obtenida del comando anterior complete los campos correspondientes en la Tabla No. 1.2. Para llenar la tabla revise el archivo de configuración *interfaces*, el cual se encuentra en la siguiente ruta, teclee:

**root@debian:/home/redes# nano /etc/network/interfaces.**

***Tabla No. 1.2 Configuración de parámetros iniciales de la IP en host A y en host B***

| Parámetros de configuración | Host A | Host B |
|---|---|---|
| **Dirección IP** | | |
| **Máscara de subred** | | |
| **Broadcast** | | |
| **Gateway** | | |

Realice la configuración necesaria para la interconexión punto a punto entre dos PC's, como se observa en la Figura No. 9.

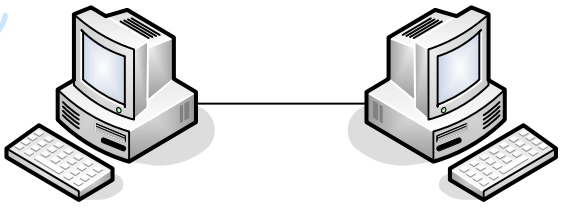


**Figura No. 9 Conexión punto a punto, en el sistema operativo Linux Debian.**

Cuando termine de realizar la configuración punto a punto y las pruebas de conectividad, llame a su profesor o profesora para que revise la actividad.

### *4.3.2 Conexión a un hub o switch*

Los hubs o concentradores son dispositivos que permiten centralizar el cableado de una red. Cuentan con varios puertos y requieren una conexión a la red eléctrica por medio de un transformador de 12V. Son la base de la topología estrella. Hay que tomar en cuenta las siguientes características:

- El número de puertos; los hay con 5, 8, 16, 32 o más.

- La velocidad; principalmente es de 10Mb, de 100Mb, y los que son 10/100Mb a la vez. También los hay de 1000Mb.

La configuración del protocolo TCP/IP para los sistemas Linux es posible realizarla a través de la interfaz gráfica proporcionada por Debian y mediante línea de comando.

***Actividad:***

En este punto de la práctica el objetivo consiste en crear una red LAN Ethernet con tres computadoras y un dispositivo de la capa 1 o 2, el dispositivo será proporcionado por el profesor o la profesora, ver Figura No. 10.

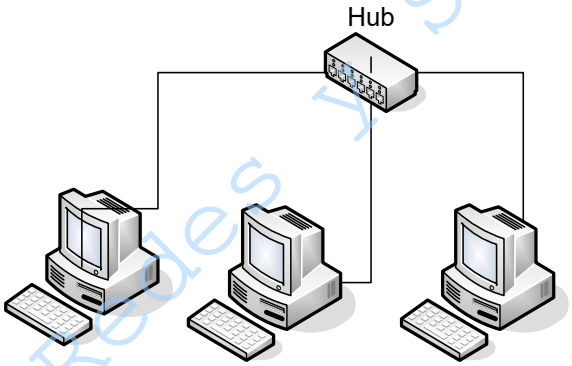



**Figura No. 10 Conexión con un hub, sistema Linux Debian**

Cuando termine de realizar la configuración punto a punto y pruebas de conectividad, llame a su profesor o profesora para que revise la actividad.

***Restablecimiento de la configuración***

Restablezca la configuración IP y los parámetros originales de las computadoras.

***Actividad:***

Un administrador de redes debe saber configurar los servicios de red en línea de comando, debido a que existen ocasiones en las que no es posible levantar el GUI o bien la administración requiere hacerse remotamente. La herramienta necesaria para realizar la administración por línea de comandos de una tarjeta de red es *ifconfig*.

Conecte el cable de la roseta a la NIC de la computadora asignada, identifique el nodo y verifique que su cable correspondiente del panel de parcheo corresponda al puerto indicado del switch.

Configure la tarjeta de red mediante la herramienta *ifconfig*; ejecute el comando con la dirección IP.

**root@debian:/home/redes# ifconfig enp0s3 192.168.2.X netmask 255.255.255.0**
**NOTA: La X hay que sustituirla por la dirección IP de la máquina que está empleando.**

Verifique la configuración del dispositivo de red enp0s3 a través del comando *ifconfig enp0s3*. Observe que la tarjeta tenga la dirección IP configurada.
Pruebe la conectividad entre las estaciones de trabajo haciendo ping a la dirección IP de la otra computadora.

Apague la máquina virtual, cierre sesión en la computadora sin apagar el equipo.

***Explique qué sucede con la configuración y fundamente su justificación.***

_____
_____
_____
_____

***¿Con qué otro comando se puede obtener el mismo efecto de reboot?***

_____
_____
_____
_____

### *4.4 Cuestionario*

1. ¿Cuáles son los elementos del diseño de una red que se utilizaron en la práctica?

_____
_____
_____
_____

2. ¿Para crear una red con acceso a Internet que parámetros de red se necesitan?

_____
_____
_____
_____

### *5.- Conclusiones*

Revise los objetivos de la práctica y las actividades realizadas y emita sus conclusiones.

**PRÁCTICA 1**
**Configuración Básica de Redes**
***Cuestionario Previo***

1. ¿Qué es la planeación y cuál es su importancia?
2. ¿Cuáles son los parámetros necesarios para la configuración de una red de computadoras?
3. En Debian, ¿cuáles son los archivos necesarios para la configuración de la red?, dé una breve explicación de su contenido.
4. ¿Cuáles son los elementos del diseño de red?
5. ¿Para qué se usa el comando apt-get install ifconfig o apt install ifconfig?
6. ¿Con qué otros nombres se pueden identificar a la NIC además de eth0?
7. Investigue a qué se le conoce como estándares de Internet.
8. ¿Qué es cableado estructurado?
9. ¿Cuáles son los principales estándares que se refieren al cableado de telecomunicaciones en edificios?
10. ¿Qué significa nivel de confianza en los dispositivos de redes de datos?
11. ¿Cómo se deshabilita un firewall en Windows y en Linux?
12. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

# Práctica 2

# Manejo de VLAN

## Planeación

***1.- Objetivo de aprendizaje***

- El alumno o la alumna realizará el análisis y la configuración de una VLAN empleando el software de simulación de red Cisco Packet Tracer.

***2.- Conceptos teóricos***

Una VLAN (Virtual LAN) funciona igual que una LAN, pero con la diferencia de que los equipos o estaciones de trabajo no necesariamente deben estar ubicados en un mismo segmento físico, es decir, agrupa a un conjunto de dispositivos de red de manera lógica.

Las ventajas que proporciona el uso de las VLAN son, por ejemplo; la seguridad, ya que los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial; la reducción de costos; aumento de la flexibilidad; un mejor rendimiento, debido a que reduce el tráfico innecesario en la red y aumenta el rendimiento de ésta.

***Rangos de los ID de una VLAN.***

Un ID es un número identificador que se emplea para definir a una VLAN de otra. Por ejemplo; VLAN 10, VLAN 20, etcétera.

***Los rangos se clasifican en:***

***a) VLAN de rango normal.***
- Se utiliza en redes de pequeñas y medianos negocios y empresas.
- Se identifica mediante un ID de VLAN entre 1 y 1005, de 1002 a 1005 se reserva para token ring y las VLAN FDDI.
- El ID 1, y de 1002 a 1005 se crean automáticamente y no se pueden eliminar.
- Se guarda en el archivo vlan.dat en la memoria flash.

***b) VLAN de Rango extendido:***
- Se identifican mediante un ID de VLAN entre 1006 y 4094.
- Se diseñan para los proveedores de servicios.
- Poseen menos opciones que las VLAN de rango normal.

***Tipos de VLAN***

**a) VLAN de datos:** Es configurada para transportar tráfico generado por los usuarios.

**b) VLAN predeterminada:** Todos los puertos del switch se vuelven parte de la VLAN predeterminada, los puertos del switch que participan en la VLAN predeterminada forman parte del mismo dominio de difusión. La VLAN predeterminada para los switches Cisco es la VLAN 1.

La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no se le puede cambiar el nombre, ni se puede eliminar.

**c)** **VLAN nativa:** Una VLAN nativa está asignada a un puerto troncal 802.1Q. Los puertos de enlace troncal son los enlaces entre switches que admiten la transmisión de tráfico asociado a más de una VLAN.

**d)** **VLAN de administración:** Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades administrativas de un switch. La VLAN 1 es la VLAN de administración de manera predeterminada.
Para crear la VLAN de administración, se asigna una dirección IP y una máscara de subred a la interfaz virtual del switch, lo que permite que el switch se administre mediante HTTP, Telnet, SSH o SNMP.

**e)** **VLAN de voz:** El tráfico de VoIP requiere de ancho de banda garantizado para asegurar la calidad de la voz, prioridad de la transmisión sobre los tipos de tráfico de red, capacidad para ser enrutado en áreas congestionadas de la red.

## *3.- Equipo y material necesario*

### *3.1 Equipo del Laboratorio*

- Computadora con Cisco Packet Tracer.

## *4.- Desarrollo.*

### *Modo de trabajar*

La práctica se desarrollará por parejas

***4.1*** Diseño de las VLAN

***4.1.1*** Encienda el sistema y elija la opción de cargar *Windows*.
***4.1.2*** Inicie sesión en una cuenta con privilegios de administrador.
***4.1.3*** Ejecute la aplicación Cisco Packet Tracer. (Ver Figura No. 1)

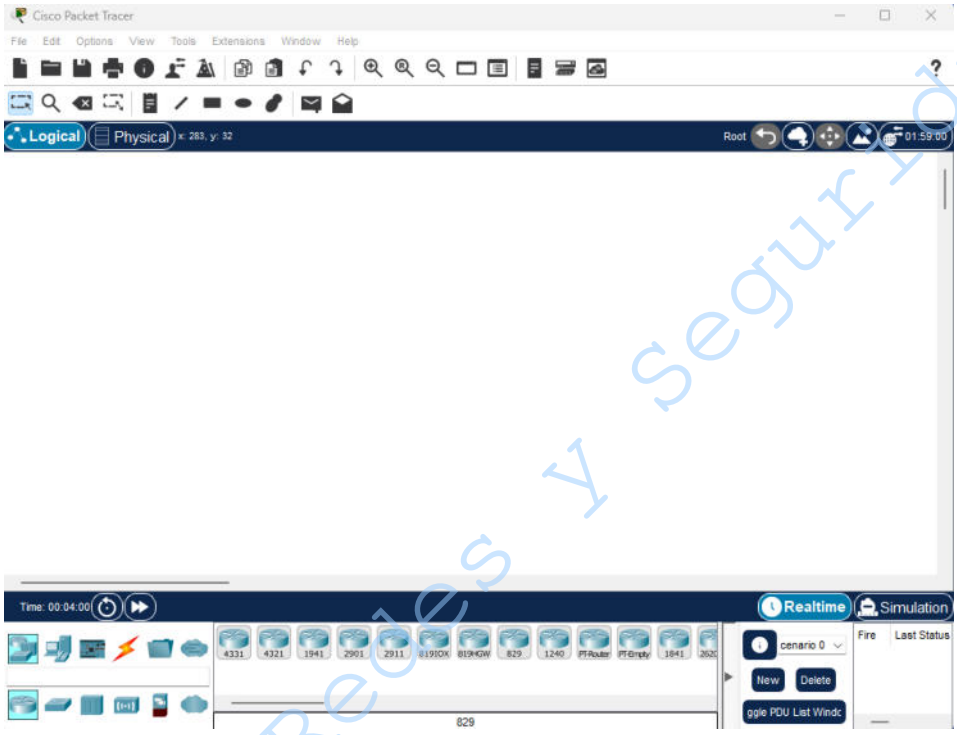



**Figura No. 1. Simulador de CISCO Packet Tracer**

El objetivo de la Figura No. 2 será conocer la aplicación y los elementos importantes:

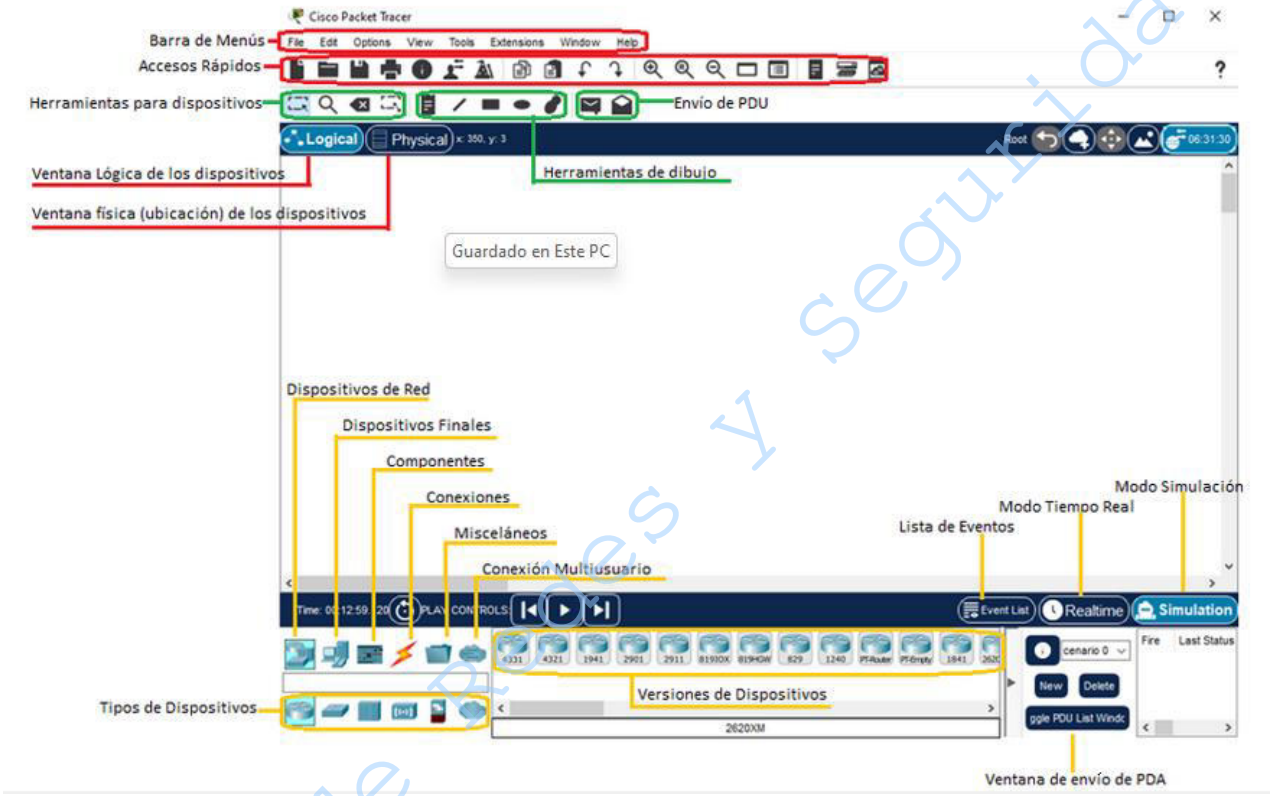



**Figura No. 2. Área de trabajo del Simulador de CISCO Packet Tracer**

***4.1.4*** Agregue al área de trabajo los siguientes componentes así como se muestra en la figura No. 3.

3 switches 2950-24
1 Router-PT
9 Computadoras PC-PT

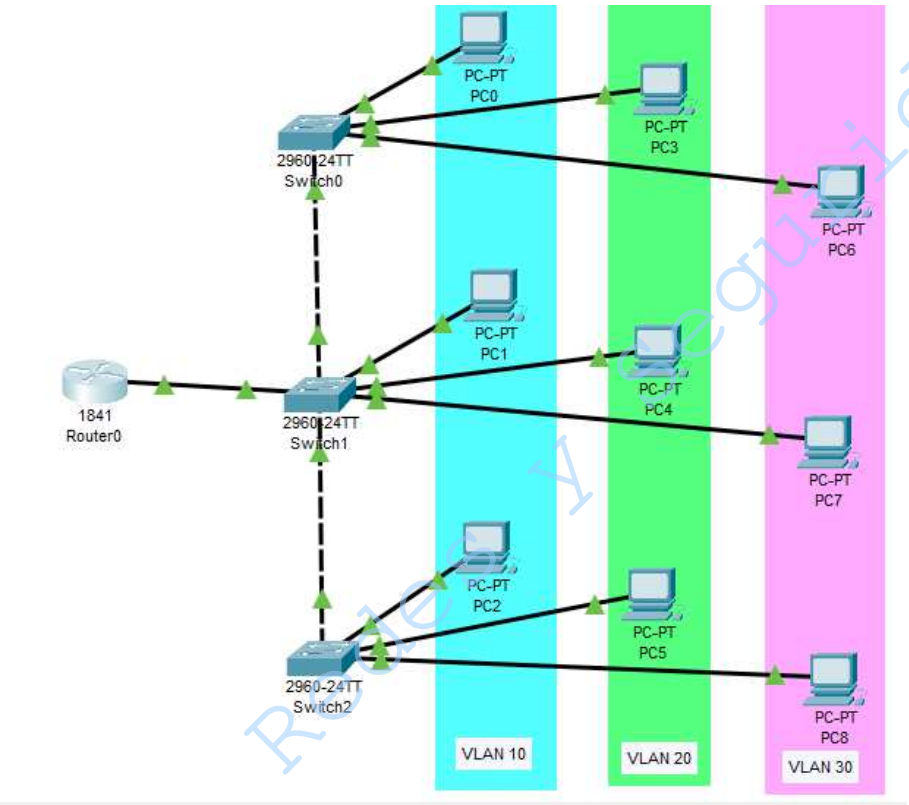



**Figura No. 3. Topología de Red.**

***4.1.5*** Las conexiones deben realizarse conforme a la tabla 1.

**Tabla 1. Enlaces de la red.**

| Red | Dispositivo Inicial e interfaz | Dispositivo Final e interfaz |
|---|---|---|
| | Router0 Fa0/0 | Switch1 Fa0/1 |
| | Switch0 Fa0/1 | Switch1 Fa0/2 |
| | Switch1 Fa0/3 | Switch2 Fa0/1 |
| VLAN 10 | PC0 | Switch0 Fa0/2 |
| | PC1 | Switch1 Fa0/4 |
| | PC2 | Switch2 Fa0/2 |
| VLAN 20 | PC3 | Switch0 Fa0/3 |
| | PC4 | Switch1 Fa0/5 |
| | PC5 | Switch2 Fa0/3 |
| VLAN 30 | PC6 | Switch0 Fa0/4 |

| | | |
|---|---|---|
| | PC7 | Switch1 Fa0/6 |
| | PC8 | Switch2 Fa0/4 |

### *4.2* Configuración de las VLAN

***4.2.1*** Para agregar una VLAN es necesario configurar su identificador y su nombre en el switch. Dé clic sobre el switch0 y diríjase a la pestaña CLI, en donde debe introducir los siguientes comandos:

Switch0>enable
Switch0#configure terminal
Switch0(config)#vlan **vlan-id**
Switch0(config-vlan)# name **nombre-de-vlan**
Switch0(config-vlan)#exit

Donde:
**vlan-id:** Se sustituye por el número que identifica a cada VLAN. (ejemplo, para la VLAN 10 su número identificador es el **10**).
**nombre-de-vlan:** Se sustituye por el nombre asignado a cada VLAN. (ejemplo: para la VLAN 10 le corresponde el nombre **DOCENTE**). Este proceso debe realizarse en todos los switches para todas las VLAN.

***4.2.2*** Realice el procedimiento del paso anterior (4.2.1) para el resto de las VLAN, con los nombres e identificadores que se muestran en la tabla 2.

**Tabla 2. Nombres y ID de cada VLAN**

| VLAN | NOMBRE | ID |
|---|---|---|
| VLAN 10 | DOCENTE | 10 |
| VLAN 20 | ESTUDIANTE | 20 |
| VLAN 30 | INVITADO | 30 |

***4.2.3*** Es necesario configurar las interfaces de un switch que fueron asignados a una VLAN específica. Para ello, debe ingresar al modo de configuración de la interfaz del switch0 (dé clic sobre el switch0 y diríjase a la pestaña CLI, tal como lo hizo en el punto 4.2.1) y seleccionar la interfaz correspondiente, introduciendo los siguientes comandos:

**Ejemplo para la VLAN 10:**
Switch0>enable
Switch0#configure terminal
Switch0(config)# interface **interface-id**
Switch0(config-if)# switchport mode access

Switch0(config-if)# switchport access vlan **vlan-id**
Switch0(config-if)# exit

**NOTA:** La interfaz **fa0/2** del switch0 está conectada a la PC0 y se encuentra asociada a la VLAN 10.

Donde:

- **interface:** Es el comando para entrar al modo de configuración de interfaz.
- **interface-id:** se sustituye por el puerto a configurar (por ejemplo: **fa0/2**).
- **switchport mode access:** Define el modo de asociación a la VLAN para el puerto.
- **switchport acces vlan:** Asigna un puerto a la VLAN.
- **vlan-id:** se sustituye por el número identificador de la VLAN(ejemplo; **10)**

***4.2.4*** Realice el proceso del paso **4.2.3** para las VLAN 20 y 30 dentro del switch0. A continuación, configure de la misma forma las interfaces del switch1 y del switch2. Recuerde considerar las conexiones mostradas en la **tabla 1** para saber qué interfaces pertenecen a cada VLAN.

***4.2.5*** Dé clic sobre el switch0, seleccione la pestaña CLI y entre en modo usuario empleando el comando:

Switch0> enable

Introduzca el comando show running-config (presione enter o barra espaciadora para avanzar). Localice la información referente a las interfaces y analice el resultado obtenido.

***4.2.6*** Defina con su profesor o profesora y escriba en la tabla 3 qué dirección IP, máscara de subred y gateway utilizará en cada VLAN, de acuerdo con cada segmento de red proporcionado.

**Tabla 3. Direcciones de red.**

| VLAN | Segmento de red | Rango de direcciones IP | Máscara | Gateway |
|---|---|---|---|---|
| 10 | | | | |
| 20 | | | | |
| 30 | | | | |

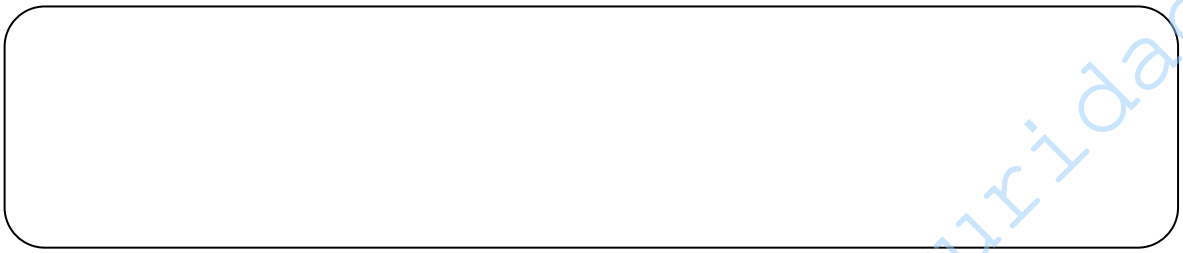
Investigue qué configuración debe realizarse para acceder a un switch Cisco mediante dirección IP en red de área local.

### *4.3* Configuración de un enlace troncal 802.1Q

Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva el tráfico de varias VLAN. Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre dispositivos de red intermedios.

Existen diferentes modos de enlaces troncales como el 802.1Q y el ISL. En la actualidad se utiliza el 802.1Q dado que el ISL es empleado por las redes antiguas. Un puerto de enlace troncal IEEE 802.1Q admite tráfico etiquetado y sin etiquetar, el enlace troncal dinámico DTP es un protocolo propiedad de cisco, éste administra la negociación del enlace troncal sólo si el puerto en el otro switch se configura en modo de enlace troncal que admita DTP.

***4.3.1*** Mencione cuáles son los enlaces (interfaces) troncales de acuerdo con la topología que ha construido (ver figura No. 3).



***4.3.2*** Entre en modo privilegiado al switch0 (dé clic sobre el switch y diríjase a la pestaña CLI) y teclee los siguientes comandos:

```
switch0>enable
switch0#configure terminal
switch0(config)# interface interface-id
switch0(config-if)# switchport mode trunk
switch0(config-if)# exit
```

Donde:

- **interface-id:** se sustituye por el puerto del enlace troncal (ejemplo para el switch0: fa0/1).
- **switchport mode trunk:** Define que el enlace que conecta a los switches sea un enlace troncal.
- **id-vlan:** se sustituye por el número identificador de la VLAN.

***4.3.3*** Entre en modo privilegiado al switch1 (dé clic sobre el switch y diríjase a la pestaña CLI) y teclee los siguientes comandos:

```
Switch1>enable
Switch1#configure terminal
Switch1(config)# interface interface-id
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# exit
```

Donde:

- **interface-id:** se sustituye por el puerto del enlace troncal .
- **switchport mode trunk:** Define que el enlace que conecta a los switches sea un enlace troncal.
- **id-vlan:** se sustituye por el número identificador de la VLAN.

### *4.4* Intercomunicación entre VLAN's

Por sí sólo, un switch de capa 2 no tiene la capacidad de enrutar paquetes entre VLAN's diferentes. Si ya han sido creadas las VLAN y se han asignado más de una computadora a cada VLAN, entonces las computadoras que se encuentran en la misma VLAN pueden comunicarse entre sí.

***4.4.1*** Explique. ¿Qué sucedería si por ejemplo, la VLAN 10 se quiere comunicar con la VLAN 20?

### *4.5* Configuración de subinterfaces en un router.

Un router sólo puede tener una dirección IP por interface. Puesto que el enlace troncal entre switch y router es único y cada VLAN requiere su propia puerta de enlace, es necesario crear subinterfaces. Una subinterfaz es una interfaz lógica dada de alta en una interfaz física del router. Sea crearán tres subinterfaces en el router0 y cada una será designada para cada VLAN (Ver tabla 3). Dé clic sobre el router0 y diríjase a la pestaña CLI. Introduzca los siguientes comandos:

router0>enable
router0#configure terminal
router0(config)# interface **interface-id.vlan-id**
router0(config-subif)# encapsulation dot1q **vlan-id**
router0(config-subif)# ip address **dirección_ip máscara**
router0(config-subif)# exit

Donde:

- **interface-id.vlan-id:** se sustituye para crear una subinterfaz para una VLAN. (ejemplo para la VLAN 10; **fa0/0.10)**
- **encapsulation dot1q:** configura la subinterfaz para que funcione en una VLAN específica.
- **vlan-id:** se sustituye por el identificador de la VLAN. (ejemplo para la vlan 10, su id es 10).
- **dirección_ip:** Se sustituye por la dirección IP de la puerta de enlace predeterminada para la subred de la VLAN.
- **máscara:** máscara de subred de la puerta de enlace

***4.5.1*** Levante el resto de subinterfaces para las VLAN 20 y 30. Recuerde que es necesario habilitar las interfaces de un router para que comiencen a transmitir; en el caso de las subinterfaces solo se requiere habilitar la interfaz física respectiva con el comando

router0(config-subif)# no shutdown

***4.5.2*** Finalmente asigne direcciones IP, máscara y Gateway a cada una de las PC's, de acuerdo a los segmentos de red proporcionados en la tabla 3. Para ello de clic sobre la PC y diríjase a la pestaña "Desktop", posteriormente de clic en "IP Configuration" y escriba las direcciones IP correspondientes en cada PC.

***4.5.3*** Si las VLAN han sido configuradas correctamente, realice las pruebas necesarias (haciendo ping de una PC a otra) para verificar que toda la red funciona correctamente. Para ello dé clic sobre una PC y seleccione la pestaña "Desktop", posteriormente dé clic sobre "comand prompt" y finalmente mande ping a una dirección destino perteneciente a una VLAN diferente a aquella donde se encuentra la PC sobre la cual dio clic.

***4.5.4*** Repita el paso anterior en diferentes PC's. Muestre a su profesor o profesora y comente el resultado obtenido.

### *4.3 Cuestionario*

1.- Mencione las ventajas y desventajas de configurar una VLAN.

_____
_____
_____
_____
_____

2.- Describa cuáles son los tipos de VLAN que existen.

_____
_____
_____
_____
_____

3. Investigue e introduzca el comando "show vlan brief" en el switch0.

_____
_____
_____
_____
_____

4.- Investigue cómo se elimina la configuración de una VLAN.

_____
_____
_____
_____
_____

***5.- Conclusiones***

Revise los objetivos de la práctica y las actividades realizadas y emita sus conclusiones.

_____
_____
_____
_____
_____
_____
_____

**PRÁCTICA 2**
**Manejo de VLAN**
***Cuestionario Previo***

1. ¿Qué es una VLAN?
2. ¿Cuáles son los las principales ventajas y desventajas de utilizar una VLAN?
3. ¿Cuáles son los tipos de VLAN que existen?
4. Mencione qué es un enlace troncal y cómo se configuran.
5. Investigue para qué sirven los siguientes comandos en cisco packet tracer:
   - show vlan **brief**
   - show id **vlan-id**
   - show vlan name **nombre de vlan**
   - show vlan **resumen**
6. Investigue cómo se elimina la configuración de una VLAN.
7. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

# Práctica 3

# Direccionamiento y configuración de los dispositivos: routers

## Planeación

### *1.- Objetivos de Aprendizaje*

- El alumno o la alumna diseñará el direccionamiento de una topología, utilizando el esquema de direccionamiento VLSM.
- El alumno o la alumna manipulará y configurará routers como equipos de interconexión.

### *2.- Conceptos teóricos*

A lo largo de la historia han cambiado los esquemas de direccionamiento para ajustarse a las necesidades de la creación de redes y subredes IP. En un inicio el esquema utilizado era el direccionamiento *Classfull*, el cual presentaba serios problemas de desperdicio de direcciones al asignar la dirección de red de acuerdo con las direcciones con clase (clase A, B y C); como solución a este gran inconveniente surgió el esquema de direccionamiento Subnetting (subneteo). Este nuevo esquema permite dividir una red con clase en subredes, pero aún no soluciona eficientemente el problema de desperdicio de direcciones IP ya que todas las subredes deben utilizar la misma máscara de subred de longitud fija.
El problema con este esquema de direccionamiento se presenta cuando las subredes no tienen un número homogéneo de hosts, como la máscara de subred se asigna de acuerdo con la subred con mayor número de hosts, las subredes que requieran menor número de hosts aún desperdiciarán direcciones IP.

VLSM (Máscara de subred de longitud variable - *Variable Length Subnet Mask*) es el esquema de direccionamiento que surgió a continuación. Utilizando este esquema se pueden aprovechar de una mejor manera las direcciones IP. Este esquema, como su nombre lo indica, permite dividir una red en subredes utilizando una máscara de subred de longitud variable, por lo tanto, en caso de que las subredes no tengan un número homogéneo de hosts la máscara de subred podrá ir cambiando de acuerdo con los requerimientos de cada subred. Utilizando este esquema de direccionamiento aún se desperdician algunas direcciones IP pero se aprovechan mejor que con los esquemas antes mencionados.

En la actualidad, la técnica empleada es CIDR (Classless Interdomain Routing), la cual utiliza y combina el concepto y funcionamiento del esquema de direccionamiento VLSM y otro esquema llamado Supernetting (superneteo).

El router es un dispositivo hardware o bien un software corriendo sobre una computadora, encargado principalmente de tomar decisiones de reenvío de paquetes de acuerdo con las tablas de enrutamiento que tiene almacenadas. Este dispositivo trabaja en la capa 3, capa de Red, del modelo de referencia OSI.

Este dispositivo puede ser configurado desde una aplicación de emulación de terminal, como la Hyperterminal de Windows, desde la CLI (Command Line Interface - Interfaz de Línea de Comandos), desde alguna aplicación de administración del dispositivo (generalmente, proporcionada al momento de realizar la compra del dispositivo o comprada por separado) o desde una aplicación de

administración basada en Web. Estas opciones de configuración varían de acuerdo con el dispositivo utilizado, es posible que sólo una de éstas esté disponible o bien, que exista más de una de estas opciones para el dispositivo.

En esta práctica utilizaremos la CLI para configurar algunos parámetros básicos en el router. Existen distintos parámetros que podemos configurar en nuestro dispositivo, los que nosotros configuraremos son:

- Nombre del host
- Contraseña de acceso por líneas VTY
- Contraseña de acceso por línea de consola
- Contraseña cifrada para ingresar al modo privilegiado
- Mensaje de inicio de sesión (MOTD)
- Dirección IP de las interfaces del router
- Descripción de las interfaces del router
- Señal de sincronización para los routers (Dispositivo DCE)
- Rutas estáticas

### *3.- Equipo y material necesario*

***Equipo del Laboratorio:***

- PC's Pentium con una NIC Ethernet 10/100 Mbps instalada en cada una de ellas.
- Software de simulación de Cisco, Packet Tracer.

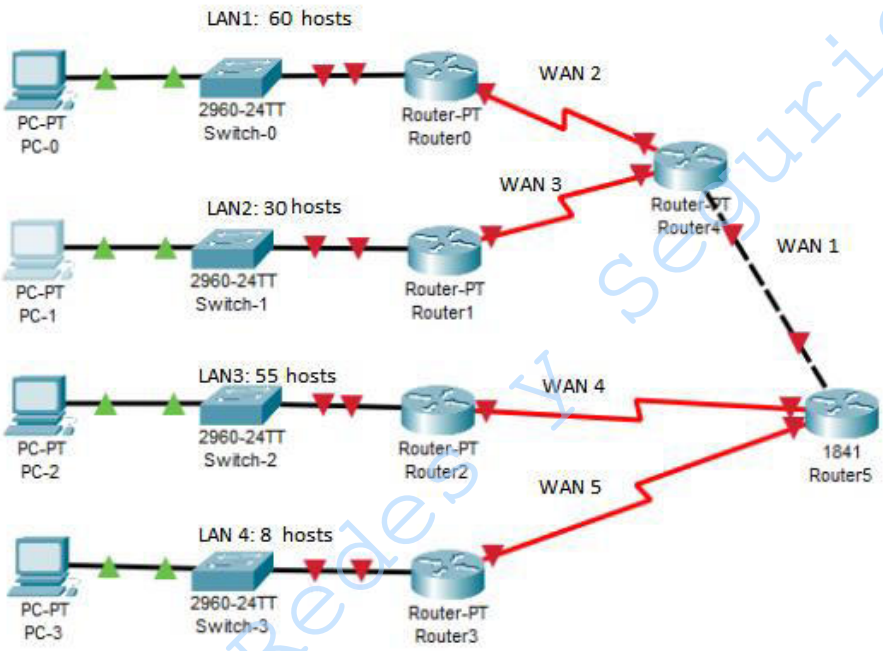
### *4.- Desarrollo*

***Modo de trabajar***

La práctica se desarrollará en parejas.

### *4.1 Esquema de direccionamiento VLSM (Variable Lenght Subnet Mask)*

***4.1.1*** La topología utilizada en esta práctica es la que se muestra a continuación (ver Figura 1.1). El segmento de red asignado es el mismo que le proporcionó su profesor o profesora para resolver la última pregunta del cuestionario previo.




***4.1.2*** Ordenar las LAN y WAN en orden descendente de acuerdo con la cantidad de hosts que necesitan. Las WAN deben conservar el orden indicado en la Figura No. 1 de acuerdo con el número de WAN.

1) _____ 6) _____
2) _____ 7) _____
3) _____ 8) _____
4) _____ 9) _____
5) _____

***4.1.3*** Realizar el direccionamiento de acuerdo con el orden anterior comenzando desde la subred cero y llenar la Tabla 1.1. Es importante conservar el orden en ambas tablas.

**Tabla 1.1. Tabla de direccionamiento VLSM**

| No. Subred | Segmento | Prefijo | Rango de direcciones asignables | Broadcast |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |

| | | | | |
|---|---|---|---|---|
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |

***4.1.4*** Asignar las direcciones a los dispositivos de acuerdo con la Tabla 1.2. La primera dirección utilizable de cada LAN se debe asignar a la PC de la LAN correspondiente. La última dirección utilizable de cada LAN se debe asignar a la interfaz LAN del router correspondiente. En los enlaces WAN, la primera dirección utilizable se debe asignar al router ubicado en el extremo izquierdo del enlace, la última dirección utilizable se debe asignar al router ubicado en el extremo derecho del enlace.

**Tabla 1.2. Tabla de asignación de direcciones**

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred | Puerta de Enlace |
|---|---|---|---|---|
| Router0 | | | | |
| Router1 | | | | |
| Router2 | | | | |
| Router3 | | | | |
| Router4 | | | | |
| Router5 | | | | |

| | | | | |
|---|---|---|---|---|
| PC 0 | | | | |
| PC 1 | | | | |
| PC 2 | | | | |
| PC 3 | | | | |

### *4.2* Configuración de un router

***4.2.1*** Inicie el simulador PacketTracer (Ver Figura No. 2)

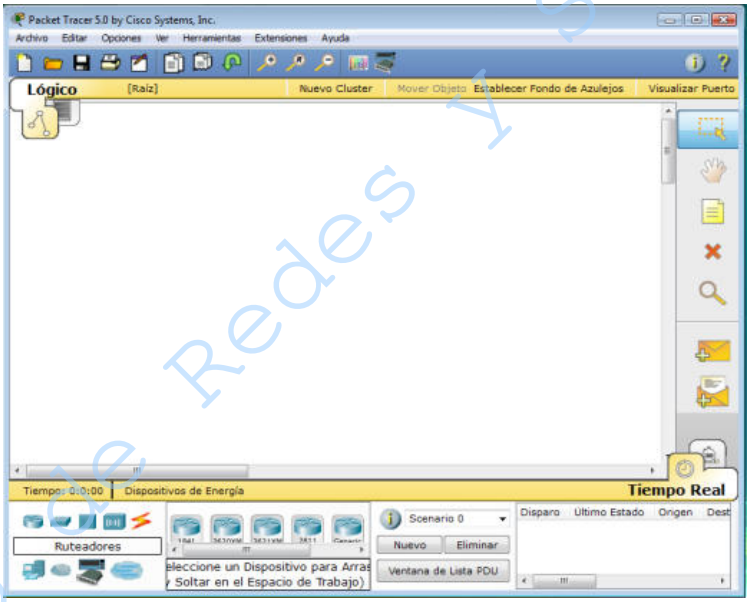



**Figura No. 2. Simulador de CISCO Packet Tracer**

***4.2.2*** Abra el archivo correspondiente a la topología realizada en el punto 12 del Cuestionario previo (Ver Figura No. 3):

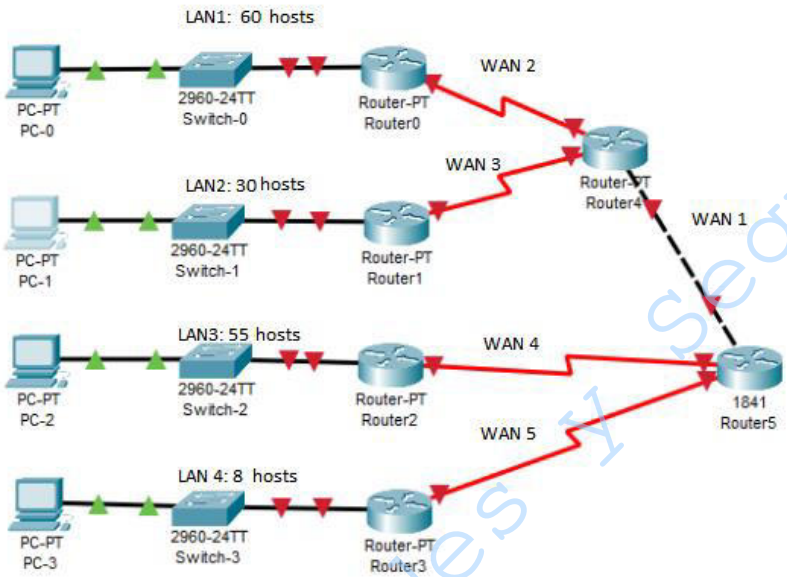



**Figura No. 3. Topología de red**

***4.2.3*** Haga clic sobre el Router 0, seleccione la pestaña de CLI, **le preguntará que si desea realizar la configuración inicial del router, responda NO en la línea de comando, presione la tecla Enter y presione nuevamente la tecla Enter para ingresar el modo usuario del router**.

***4.2.4*** Configure el nombre del router

```
Router>enable
Router# config t
Router (config)#hostname Router0
```

***4.2.5*** Configure la descripción de interfaces, los mensajes de inicio de sesión (banners), la contraseña de acceso por líneas VTY y a través de Consola y configure una clave secreta cifrada de inicio de sesión (enable secret).

**NOTA: Para fines prácticos esta configuración únicamente se realizará para el Router 0 ya que no es tema de esta sesión.**

```
Router0 (config)#enable secret xyzpassword
Router0 (config)#line con 0
Router0 (config-line)#password linepassword
Router0 (config-line)#login
```

```
Router0 (config-line)#exit
Router0 (config)#line vty 0 4
Router0 (config-line)#password linepassword
Router0 (config-line)#login
Router0 (config-line)#exit
Router0 (config)#banner motd # Este es el Router0 #
```

***4.2.6*** Asigne la dirección IP a cada interfaz de acuerdo con la Tabla 1.2. Reemplace los parámetros NETWORK_ADDRESS, SUBNET_MASK, ID_INTERFACE por el valor correspondiente de acuerdo con la Tabla 1.2. En el caso de las interfaces conectadas a una LAN el parámetro xxxx debe ser reemplazado por el número de LAN de la cual se trata (1, 2, 3 y 4 respectivamente). En el caso de las interfaces conectadas directamente a otro Router el parámetro X debe ser reemplazado por el identificador del router al cual se conecta (0, 1, 2, 3, 4 y 5 respectivamente).

```
Router0 (config)#interface ID_INTERFACE
Router0 (config-if)#ip address NETWORK_ADDRESS SUBNET_MASK
Router0 (config-if)#description conexion a LAN xxxx
Router0 (config-if)#no shutdown
Router0 (config-if)#exit
Router0 (config)#interface ID_INTERFACE
Router0 (config-if)#ip address NETWORK_ADDRESS SUBNET_MASK
Router0 (config-if)#description conexion al routerX
Router0 (config-if)#no shutdown
Router0 (config-if)#exit
Router0 (config)#exit
Router0#copy run start
```

***4.2.7*** Presione la tecla Enter para aceptar los cambios en el archivo *startup-config* y presione nuevamente Enter para sobrescribir la configuración.

***4.2.8*** Cierre la ventana de configuración de Router0.

***4.2.9*** Para guardar su proyecto, vaya al menú Archivo y haga clic en el botón Guarda Como, coloque el nombre de **admon2b_INICIALES**, en la carpeta de Mis Documentos haga clic en guardar.

***4.2.10*** Configure los dispositivos Router1, Router2 y Router3 con base en los pasos 4.2.4 y 4.2.6. No olvide cambiar los parámetros xxxx (número de LAN) y X (identificador de Router) por el correspondiente, así como NETWORK_ADDRESS, SUBNET_MASK y ID_INTERFACE de acuerdo con la Tabla 1.2.

***4.2.11*** La configuración de Router4 y Router5 varía de los routers anteriores, la diferencia radica en que estos routers actúan como el extremo DCE, el cual se encarga de proporcionar una señal de sincronización. Para proporcionar la señal de sincronización solamente es necesario agregar un comando de configuración en cada interfaz serial.

***4.2.12*** Configure el Router4 y el Router5 de acuerdo con los comandos siguientes. Recuerde cambiar los parámetros NETWORK_ADDRESS, SUBNET_MASK, ID_INTERFACE, xxxx y X por los

correspondientes. Las interfaces que se configuran en el ejemplo son las interfaces Fastethernet, debe notar que este tipo de interfaz no necesita una señal de temporización en ningún extremo.

**Ejemplo configuración del Router4**

```
Router>enable
Router# config t
Router (config)#hostname Router4
Router4 (config)#enable secret xyzpassword
Router4 (config)#line con 0
Router4 (config-line)#password linepassword
Router4 (config-line)#login
Router4 (config-line)#exit
Router4 (config)#line vty 0 4
Router4 (config-line)#password linepassword
Router4 (config-line)#login
Router4 (config-line)#exit
Router4 (config)#banner motd # Este es el Router4 #
Router4 (config)#interface ID_INTERFACE
Router4 (config-if)#ip address NETWORK_ADDRESS SUBNET_MASK
Router4 (config-if)#description conexion al RouterX
Router4 (config-if)#no shutdown
Router4 (config-if)#exit
Router4 (config)#interface ID_INTERFACE
Router4 (config-if)#ip address NETWORK_ADDRESS SUBNET_MASK
Router4 (config-if)#description conexion al RouterX
Router4 (config-if)#clock rate 64000
Router4 (config-if)#no shutdown
Router4 (config-if)#exit
Router4 (config)#interface ID_INTERFACE
Router4 (config-if)#ip address NETWORK_ADDRESS SUBNET_MASK
Router4 (config-if)#description conexion al RouterX
Router4 (config-if)#clock rate 64000
Router4 (config-if)#no shutdown
Router4 (config-if)#exit
Router4 (config)#exit
Router4#copy run start
```

***4.2.13*** Guarde su proyecto, vaya al menú Archivo y haga clic en el botón Guardar, le preguntará que si desea ¿sobreescribir el archivo?, haga clic en el botón sí.

**NOTA: Guarde dos copias adicionales de este proyecto, las utilizará en la siguiente práctica. La primera copia debe tener el siguiente formato: admon2b_INICIALES_RIPv2. La segunda copia debe tener el siguiente formato: admon2b_INICIALES_OSPF.**

***4.2.14*** Haga clic sobre la PC0, seleccione la pestaña Desktop y haga clic en la opción IP Configuration. Asigne la dirección IP, la máscara de subred y el Gateway predeterminado de acuerdo con la Tabla No 1.2 de la práctica.

***4.2.15*** Configure el resto de las PCs de manera similar al punto anterior.

***4.2.16*** Entender cómo se configuran los routers es indispensable para los administradores de redes. Verifique las conexiones realizadas mediante los siguientes comandos en cada uno de los routers desde el Router0 hasta el Router5.

```
Router0# show running-config
Router0# show ip route

Router1# show running-config
Router1# show ip route

Router2# show running-config
Router2# show ip route

Router3# show running-config
Router3# show ip route

Router4# show running-config
Router4# show ip route

Router5# show running-config
Router5# show ip route
```

Explique la salida de las instrucciones show ip route.

***4.2.17*** Con ayuda de los comandos del punto anterior, identifique los segmentos de red que se encuentran conectados directamente en cada dispositivo.

Elabore la tabla 1.3 donde se incluyan los segmentos de red conectados directamente a cada dispositivo Router y a través de qué interfaz.

**Tabla 1.3. Tabla de segmentos de red**

| *Dispositivo* | *Segmento de red* | *Interfaz* |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

### *5.-* Conclusiones

Revise los objetivos de la práctica y las actividades realizadas y emita sus conclusiones.

**PRÁCTICA 3**

**Direccionamiento y configuración de los dispositivos: router.**

***Cuestionario Previo***

1. La Figura A muestra el aspecto de alto nivel de una arquitectura genérica de un router, en la cual se identifican cuatro componentes principales, investigue en qué consiste cada uno.

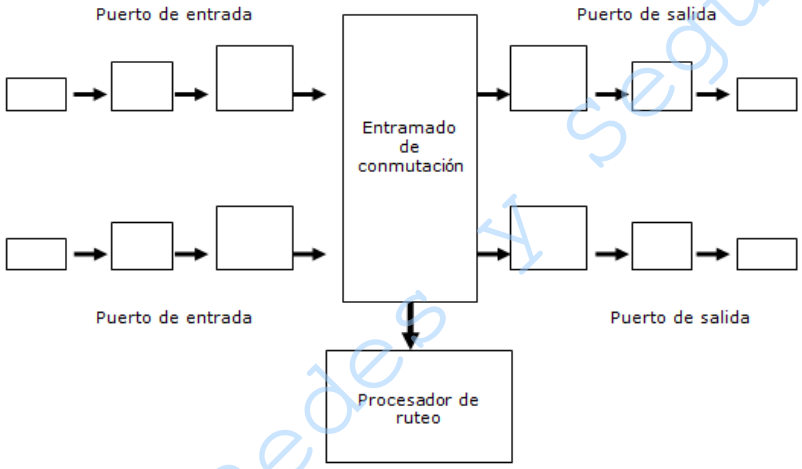



**Figura A. Estructura genérica de un router**

2. ¿Qué es un segmento de red?
3. ¿Qué es una máscara de red?
4. ¿Qué es una subred?
5. ¿Qué es un sistema autónomo, en el área de redes?
6. ¿Qué es y cómo funcionan el protocolo de ruteo interno y externo?
7. ¿Qué es y cómo funciona el protocolo de ruteo estático y el protocolo de ruteo dinámico?
8. ¿Cómo funciona el enrutamiento por vector-distancia y el enrutamiento por estado-enlace?
9. Investigue ¿qué es la conexión DTE y la conexión DCE?
10. ¿Cómo se lleva a cabo el direccionamiento con subnetting?
11. ¿Cómo se lleva a cabo el direccionamiento con VLSM?
12. La topología que se utilizará en esta práctica emplea diferentes modelos de routers cisco y puede observarse en la Figura B. Realice las siguientes actividades:
    a) Realizar el direccionamiento a mano a través de VLSM. El segmento de red asignado será proporcionado por su profesor o profesora o usted debe proponer uno.
    b) Completar la Tabla 1.1 de la práctica empleando la información obtenida en el inciso a)
    c) Deberá traer el archivo .pkt con la topología ya construida, emplee la versión de Packet Tracer que está en el laboratorio.

**NOTA 1: Algunos modelos de routers necesitan la inserción de módulos para poder hacer uso de más interfaces de las que traen por defecto, para armar la topología indicada es necesario que investigue cómo deben incluirse dichos módulos.**

**NOTA 2: Es importante elegir la opción DCE cuando se hacen las conexiones seriales entre routers. Primero se debe seleccionar el router situado en el extremo derecho de cada enlace y por último el router situado en el extremo izquierdo del enlace. Lo cual significa que el router del extremo izquierdo será el dispositivo DCE, por lo tanto, proporcionará la señal de sincronización.**

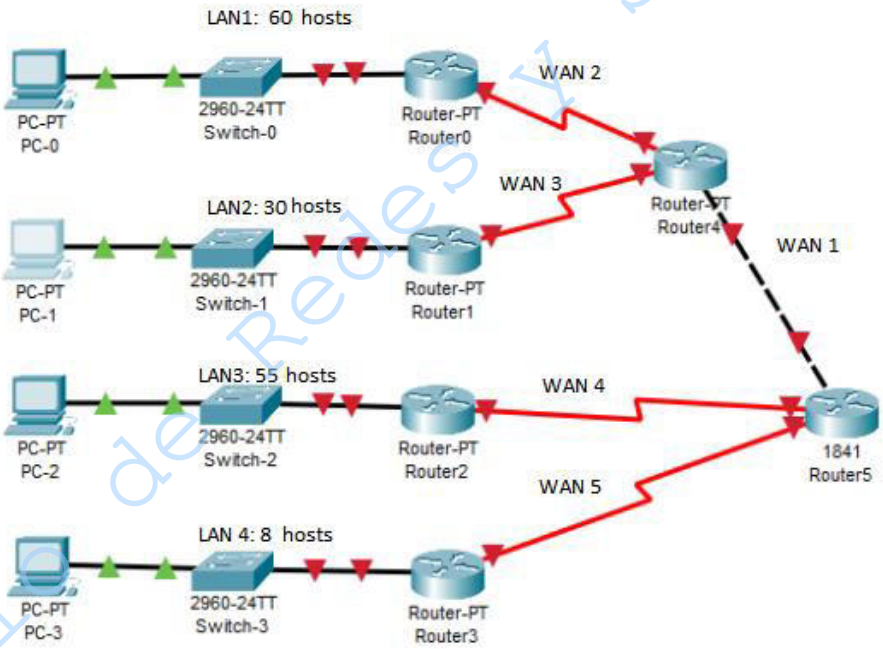



**Figura B. Topología de red**

13. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

# Práctica 4

# Protocolos de Enrutamiento Estático y Dinámico

## Planeación

### *1.- Objetivos de Aprendizaje*

- El alumno o la alumna manipulará equipos de interconexión como son los routers.
- El alumno o la alumna configurará algunos protocolos de enrutamiento estático y dinámico y analizará su funcionamiento dentro de una red de área local mediante una herramienta de simulación de redes: Packet Tracer.

### *2.- Conceptos teóricos*

El Routing Information Protocol (RIP) es un protocolo vector – distancia, 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.

RIPv2 es un protocolo de enrutamiento sin clase, las máscaras de subred se incluyen en las actualizaciones de enrutamiento, lo que hace que RIPv2 sea más compatible con los ambientes de enrutamiento modernos.

En realidad, RIPv2 es una mejora de las funciones y extensiones de RIPv1, más que un protocolo completamente nuevo. 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

Open Shortest Path First (OSPF) es un protocolo de enrutamiento de estado de enlace desarrollado como reemplazo del protocolo de enrutamiento por vector de distancia: RIP. RIP constituyó un protocolo de enrutamiento aceptable en los comienzos del networking y de Internet; sin embargo, su dependencia en el conteo de saltos como la única medida para elegir el mejor camino rápidamente se volvió inaceptable en redes mayores que necesitan una solución de enrutamiento más sólida. OSPF es un protocolo de enrutamiento sin clase que utiliza el concepto de áreas para realizar la escalabilidad. RFC 2328 define la métrica OSPF como un valor arbitrario llamado costo. El IOS de Cisco utiliza el ancho de banda como la métrica de costo de OSPF.

Las principales ventajas de OSPF frente a RIP son su rápida convergencia y escalabilidad a implementaciones de redes mucho mayores.

***3.- Equipo y material necesario***

***Equipo del Laboratorio:***

- PC's Pentium con una NIC Ethernet 10/100 Mbps instalada en cada una de ellas.
- Software de simulación de Cisco, Packet Tracer.

***Material de alumno:***

- Los tres archivos de Packet Tracer creados en la práctica anterior.

***4.- Desarrollo***

***Modo de trabajar***

La práctica se desarrollará en parejas.

***4.1* Configuración del protocolo estático.**

El objetivo de este punto es configurar las tablas de enrutamiento manualmente, esto es crear tablas de enrutamiento estáticas en cada router que permitan la comunicación en toda la red.

**NOTA:** El ruteo no funciona hasta que todos los routers tengan ya configuradas sus tablas de enrutamiento estáticas.

***4.1.1*** Abra el archivo admon2b_INICIALES y realice las configuraciones pertinentes en cada router.

***4.1.2*** Como usted notó, en la salida del comando show ip route sólo aparecían las redes conectadas directamente a cada router. Para agregar una ruta estática hacia una red se utiliza el comando:
***ip route NETWORK NET_MASK {ID_INTERFACE | NEXT_HOP_ADDRESS}***
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 comando puede utilizar dos parámetros diferentes que indican por dónde salen los paquetes. Sólo es posible utilizar uno de los dos parámetros, el parámetro ID_INTERFACE corresponde a la interfaz del router local por la cual tendrán salida los paquetes; el parámetro NEXT_HOP_ADDRESS corresponde a la dirección IP de la interfaz del otro router que se encuentra conectado directamente al router que está configurando, es decir, la siguiente interfaz con la que se requiere tener comunicación y que representa al gateway por donde saldrán los paquetes para llegar a la red remota.
Configure las rutas estáticas apropiadas para que todas las redes sean accesibles desde cualquier red. Utilice el parámetro NEXT_HOP_ADDRESS.

```
Router0#config t
Router0(config)# ip route NETWORK1 NET_MASK NEXT_HOP_ADDRESS
Router0(config)# ip route NETWORK2 NET_MASK NEXT_HOP_ADDRESS
Router0(config)#exit
Router0#copy run start
```

***4.1.3*** Guarde su proyecto, vaya al menú Archivo y haga clic en el botón Guardar, le preguntará que si desea ¿sobreescribir el archivo?, haga clic en el botón sí.

***4.1.4*** Configure las rutas estáticas apropiadas en cada dispositivo (router) de tal manera que todas las redes sean accesibles desde cualquier origen. En todas las rutas estáticas utilice el parámetro NEXT_HOP_ADDRESS.

***4.1.5*** Guarde su proyecto, vaya al menú Archivo y haga clic en el botón Guardar, le preguntará que si desea ¿sobreescribir el archivo?, haga clic en el botón sí.

### *4.2* Verificación de las tablas de enrutamiento

El objetivo de este apartado es la comprobación de las tablas de ruteo configuradas en el punto anterior, para lo cual se emplea el comando ***show ip route.***

***4.2.1*** Abra la CLI de cada router y use el comando show ip route para verificar la tabla de enrutamiento.

```
Router0# show ip route
Router1# show ip route
Router2# show ip route
Router3# show ip route
Router4# show ip route
Router5# show ip route
```

***4.2.2*** Una vez comprobadas las tablas de enrutamiento en todos los routers, verifique la conectividad entre los routers haciendo ping a las direcciones de las interfaces de cada router:

```
Router0#ping ADDRESS_1
Router0#ping ADDRESS_2
```

***4.2.3*** Todas las pruebas de ping deben tener éxito, de lo contrario observe cuál falla y revise las rutas estáticas referentes a dicha prueba.
Muestre a su profesor o profesora las pruebas de ping realizadas.

### *4.3* Configuración básica del protocolo OSPF

***4.3.1*** Abra el archivo que guardó en el punto 4.2.13 de la práctica anterior (Práctica 3) y que hace referencia al protocolo de enrutamiento OSPF.

***4.3.2*** Haga clic sobre la PC0, seleccione la pestaña Desktop y haga clic en la opción IP Configuration. Asigne la dirección IP, la máscara de subred y el Gateway predeterminado de acuerdo a la Tabla 1.2 de la práctica anterior.

***4.3.3*** Configure el resto de las PCs de manera similar al punto anterior.

***4.3.4*** El objetivo de este punto es configurar los routers de la topología, ver Figura 1.1, con un protocolo de enrutamiento dinámico para que se comuniquen entre sí.

***4.3.5*** Haga clic sobre el Router0, seleccione la pestaña de CLI y presione una vez la tecla Enter; cuando lo solicite, coloque la contraseña para ingresar al router. Entre al modo privilegiado del router, recuerde que se realiza a través del comando enable. Por último, ingrese al modo de configuración global del router a través del comando configure terminal.

***4.3.6*** Ingrese al modo de configuración del protocolo de enrutamiento OSPF.

***De acuerdo con el funcionamiento de OSPF, para ingresar al modo de configuración del protocolo OSPF ¿Qué parámetro debemos utilizar en el comando router ospf?*** _____.

```
Router0 (config)# router ospf X
```

***¿Cómo se obtiene la WILDCARD de una subred? Obtenga la WILDCARD de cada subred y complete la Tabla 1.3.***

_____
_____
_____
_____

**Tabla 1.1. Tabla de máscaras wildcard**

| ***Dispositivo*** | ***Subred conectada directamente*** | ***Wildcard*** |
|---|---|---|
| ***Router0*** | | |
| | | |
| ***Router1*** | | |
| | | |
| ***Router2*** | | |

| | | |
|---|---|---|
| | | |
| ***Router3*** | | |
| | | |
| ***Router4*** | | |
| | | |
| | | |
| ***Router5*** | | |
| | | |
| | | |

***4.3.7*** Configurar las subredes que se encuentran conectadas directamente al Router0. De acuerdo con la Tabla 1.1, en el comando ***network NETWORK_ADDRESS WILDCARD area Y*** reemplace los parámetros NETWORK_ADDRESS y WILDCARD por los valores correspondientes. El parámetro Y que corresponde al número de área será 0. Es importante que indique todas y cada una de las subredes conectadas directamente en un comando network independiente.

```
Router0(config-router)#network NETWORK_ADDRESS1 WILDCARD1 área Y
Router0(config-router)#network NETWORK_ADDRESS2 WILDCARD2 area Y
```

***4.3.8*** No permita que las actualizaciones de enrutamiento se envíen a las interfaces conectadas a la LANX. Para esto tiene que colocar la interfaz Fast Ethernet en modo pasivo. Cambie el parámetro ID_INTERFACE por la interfaz correspondiente. Salga del modo de configuración del protocolo de enrutamiento y guarde su configuración.

```
Router0(config-router)#passive-interface ID_INTERFACE
Router0(config-router)#exit
Router0(config)#exit
Router0#copy run start
```

***4.3.9*** Configure el resto de los routers de manera similar a las configuraciones del Router0, no olvide cambiar los parámetros NETWORK_ADDRESS y WILDCARD por los valores correspondientes de acuerdo con la Tabla 1.2 y el parámetro ID_INTERFACE por la interfaz adecuada para cumplir con los requerimientos indicados.

***4.3.10*** Guarde su proyecto, vaya al menú Archivo y haga clic en el botón Guardar, le preguntará que si desea ¿sobreescribir el archivo?, haga clic en el botón sí.

### *4.4* Verificación de las tablas de ruteo

El objetivo de este apartado es la comprobación de las tablas de ruteo configuradas en el punto anterior, para lo cual se emplea el comando ***show ip route.***

***4.4.1*** Compruebe las tablas de enrutamiento en cada uno de los routers y verifique si las tablas de enrutamiento contienen una ruta para cada una de las subredes de la topología.

```
Router0 (config)#show ip route
```

***4.4.2*** Una vez comprobadas las tablas de ruteo en todos los routers, verifique la conectividad entre los mismos mediante las siguientes pruebas de ping (Tabla 1.2). Muestre la tabla a su profesor o profesora:

**Tabla 1.2. Pruebas de conectividad**

| **Prueba** | **¿Exitoso?** |
|---|---|
| **PC0 → PC1** | |
| **PC1 → PC2** | |
| **PC2 → PC3** | |
| **PC3 → PC0** | |
| **PC0 → Fa0/0 de Router4** | |
| **PC3 → Fa0/0 de Router5** | |

***4.4.3*** Si alguna de las pruebas de ping no tuvo éxito solucione el problema, si la salida del comando show ip route no reveló algún problema en las tablas de ruteo, verifique que las direcciones IP se encuentran asignadas correctamente a cada dispositivo.

**EJERCICIO OPCIONAL**

### *4.5* Configuración básica del protocolo RIPv2

***4.5.1*** Abra el archivo que guardó como **admon2b_INICIALES_RIPv2** de la práctica anterior y que hace referencia al protocolo de enrutamiento RIPv2.

***4.5.2*** El objetivo de este punto es configurar los routers de la topología, ver Figura No. 1, con un protocolo de enrutamiento dinámico para que se comuniquen entre sí.

***4.5.3*** Llene la Tabla 1.3. indicando las subredes que se encuentran conectadas directamente a cada uno de los routers, no olvide indicar la máscara de subred que le corresponde a cada subred.

***4.5.4*** Haga clic sobre el Router0, seleccione la pestaña de CLI y presione una vez la tecla Enter; cuando lo solicite, ingrese la contraseña para ingresar al router. Ingrese al modo privilegiado del router, recuerde que se realiza a través del comando enable. Por último, ingrese al modo de configuración global del router a través del comando configure terminal.

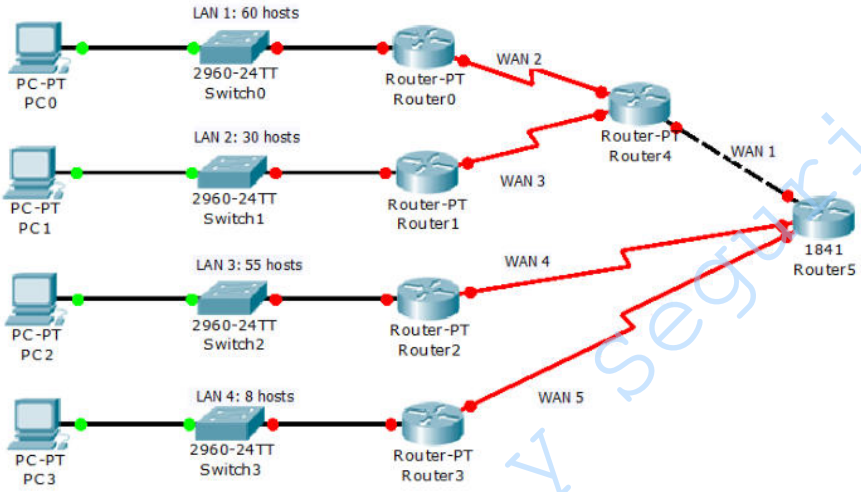



**Figura No. 1. Topología del laboratorio**

**Tabla 1.3. Subredes conectadas directamente a los routers**

| *Dispositivo* | *Subred conectada directamente* | *Máscara de subred* |
|---|---|---|
| ***Router0*** | | |
| | | |
| ***Router1*** | | |
| | | |
| ***Router2*** | | |
| | | |
| ***Router3*** | | |
| | | |
| ***Router4*** | | |
| | | |
| | | |
| ***Router5*** | | |
| | | |
| | | |

***De acuerdo con el esquema de direccionamiento obtenido anteriormente y a su investigación del previo de esta práctica, ¿Qué versión de RIP debemos utilizar?***
_____.

***4.5.5*** Ingrese al modo de configuración del protocolo de enrutamiento RIP. Y seleccione la versión que debemos configurar.

```
Router0(config)#router rip
Router0(config-router)#version numero_de_version
```

***4.5.6*** Configurar las subredes que se encuentran conectadas directamente al Router0. De acuerdo con la Tabla 1.1, en el comando ***network NETWORK_ADDRESS*** reemplace los parámetros NETWORK_ADDRESS por la subred correspondiente, es importante que indique todas y cada una de las subredes conectadas directamente empleando un comando network por cada subred.

```
Router0(config-router)#network NETWORK_ADDRESS1
Router0(config-router)#network NETWORK_ADDRESS2
```

***4.5.7*** No permita que las actualizaciones de enrutamiento se envíen a las interfaces conectadas a la LANX. Para esto tiene que colocar la interfaz Fast Ethernet en modo pasivo. Cambie el parámetro ID_INTERFACE por la interfaz correspondiente. Salga del modo de configuración del protocolo de enrutamiento y guarde su configuración.

```
Router0(config-router)#passive-interface ID_INTERFACE
Router0(config-router)#exit
Router0(config)#exit
Router0#copy run start
```

***4.5.8*** Configure el resto de los routers de manera similar a las configuraciones del Router0, no olvide cambiar el parámetro NETWORK_ADDRESS por el valor correspondiente de acuerdo con la Tabla 1.1 y el parámetro ID_INTERFACE por la interfaz adecuada para cumplir con los requerimientos indicados.

***4.5.9*** Guarde su proyecto, vaya al menú Archivo y haga clic en el botón Guardar, le preguntará que si desea ¿sobreescribir el archivo?, haga clic en el botón sí.

### *4.6* Verificación de las tablas de ruteo

El objetivo de este apartado es la comprobación de las tablas de ruteo configuradas en el punto anterior, para lo cual se emplea el comando ***show ip route.***

***4.6.1*** Compruebe las tablas de enrutamiento en cada uno de los routers y verifique si las tablas de enrutamiento contienen una ruta para cada una de las subredes de la topología.

Router0 (config)#show ip route

Una vez comprobadas las tablas de ruteo en todos los routers, verifique la conectividad entre los mismos mediante las siguientes pruebas de ping (Tabla 1.4). Muestre la tabla a su profesor o profesora:

**Tabla 1. 4. Pruebas de conectividad**

| Prueba | ¿Exitoso? |
|---|---|
| **PC0 → PC1** | |
| **PC1 → PC3** | |
| **PC2 → PC3** | |
| **PC3 → PC0** | |
| **PC0 → Fa0/0 de Router4** | |
| **PC3 → Fa0/0 de Router5** | |

***4.6.2*** Si alguna de las pruebas de ping no tuvo éxito solucione el problema, si la salida del comando show ip route no reveló algún problema en las tablas de ruteo, verifique que las direcciones IP se encuentran asignadas correctamente a cada dispositivo.

## *5* Conclusiones

Revise los objetivos de la práctica y las actividades realizadas y emita sus conclusiones.

**PRÁCTICA 4**

**Protocolos de Enrutamiento Estático y Dinámico**

***Cuestionario Previo***

1. ¿Cómo se lleva a cabo la configuración del protocolo estático?
2. ¿Cuáles son las características del protocolo RIP versión 1?
3. ¿Cuáles son las características del protocolo RIP versión 2?
4. ¿Cuál es la sintaxis para configurar RIP?
5. ¿Cuáles son las características de OSPF?
6. ¿Cómo funciona el algoritmo shortest path first (SPF)?
7. ¿Qué es el término de WILDCARD en el entorno de ruteo dinámico?
8. ¿Cuál es la sintaxis para configurar OSPF?
9. ¿Qué es convergencia en los protocolos de enrutamiento?
10. Explique cómo se emplea el siguiente comando, escriba 5 ejemplos representándolos en un diagrama de subredes en Packet Tracer: ip route Network Net_Mask ID_Interface
11. Explique cómo se emplea el siguiente comando, escriba 5 ejemplos representándolos en un diagrama de subredes en Packet Tracer: ip route Network Net_Mask Next_Hop_Address
12. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

# Práctica 5

# Administración con SNMP en Cisco Packet Tracer

## Organización

### *1.- Objetivo de aprendizaje*

- El alumno o la alumna analizará y explorará el significado y utilidad de los diferentes objetos de la MIB-II, consultando los valores a un agente SNMP.
- El alumno o la alumna configurará a través de la interfaz de línea de comandos el protocolo de mantenimiento SNMP en algunos dispositivos Cisco.

### *2.- Conceptos teóricos*

SNMP, Protocolo Simple de Administración (Simple Network Manager Protocol) es un protocolo del nivel de aplicación que proporciona una estructura de mensajes para el intercambio de información entre administradores y agentes SNMP, es decir, proporciona un entorno de trabajo estandarizado y un lenguaje común empleado para el monitoreo y administración de dispositivos de la red. El protocolo SNMP se conforma de 3 elementos:

a) Un administrador SNMP es un sistema empleado para controlar la actividad de los componentes de la red mediante SNMP, regularmente denominado NMS, Sistema de Administración de Red (Network Management System).

b) Un agente SNMP es el componente software dentro del dispositivo administrado que mantiene los datos del mismo e informa al administrador acerca de ellos, cuando se requiere. Contiene variables de la MIB cuyos valores pueden ser solicitados o modificados por el administrador SNMP, mediante operaciones get y set.

c) Una MIB es una colección de objetos de información de administración, residente en el dispositivo administrado. Sus colecciones de objetos están definidos como módulos escritos en un lenguaje especial.

El protocolo funciona de la siguiente manera: el administrador puede leer un valor de un agente o almacenar un valor en dicho agente, éste último obtiene los datos de la MIB, donde se almacenan los parámetros del dispositivo y datos del funcionamiento de la red. El agente responde a las solicitudes de los administradores y les puede enviar notificaciones no solicitadas en forma de informes o interrupciones (traps) para dar a conocer las condiciones de la red. Existen 6 operaciones básicas que se realizan entre administradores y agentes SNMP, las cuales se resumen en la Tabla 1.1.

**Tabla 1.1 Operaciones básicas entre agentes y administradores SNMP**

| Operación | Funcionamiento |
|---|---|
| get-request | Solicita el valor de una variable específica. |

| | |
|---|---|
| get-next-request | Solicita el valor de una variable sin conocer su nombre, se emplea en búsqueda secuencial en tablas. |
| get-bulk-request | Solicita bloques grandes de datos, por ejemplo, varias filas de una tabla. |
| get-response | Es la respuesta a una petición get-request, get-next-request o set-request. |
| inform-request | Permite la comunicación entre administradores SNMP. |
| trap | Se refiere a los mensajes no solicitados enviados por los agentes al administrador SNMP si ocurre algún evento inesperado. |

**NOTA: El protocolo SNMP funciona de acuerdo con el modelo cliente/servidor, donde el proceso servidor se ejecuta en los agentes y permanece escuchando las peticiones por parte del administrador SNMP.**

***3.- Equipo y material necesario***

***Equipo del Laboratorio:***

- PC's Pentium con una NIC Ethernet 10/100 Mbps instalada en cada una de ellas.
- Software de simulación de Cisco, Packet Tracer.

***4.- Desarrollo***

***Modo de trabajar***

La práctica se desarrollará en parejas.

***4.1*** **Iniciando Packet Tracer**

*4.1.1* Inicie el simulador Packet Tracer (Ver Figura No. 1).

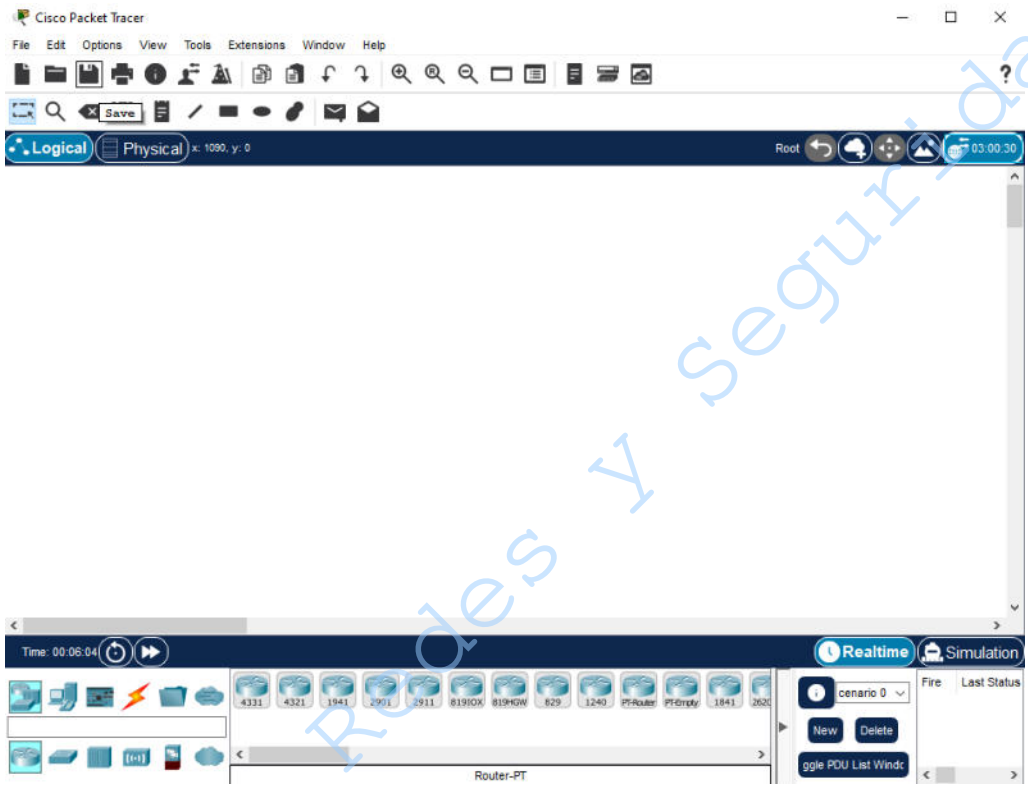



**Figura No. 1 Simulador CISCO Packet Tracer**

*4.1.2* Abra el archivo de Packet Tracer realizado durante el cuestionario previo.

*4.1.3* Encienda la interfaz del Router0 conectado al SwitchLabRyS y pruebe que hay comunicación a través de toda la red.

### *4.2* Configuración de la topología

*4.2.1* Complete la topología con los dispositivos y conexiones como lo muestra la figura No. 2, asigne la etiqueta correspondiente para poder identificarlos (es importante que verifique que los modelos de los dispositivos sean los mismos que la topología mostrada):

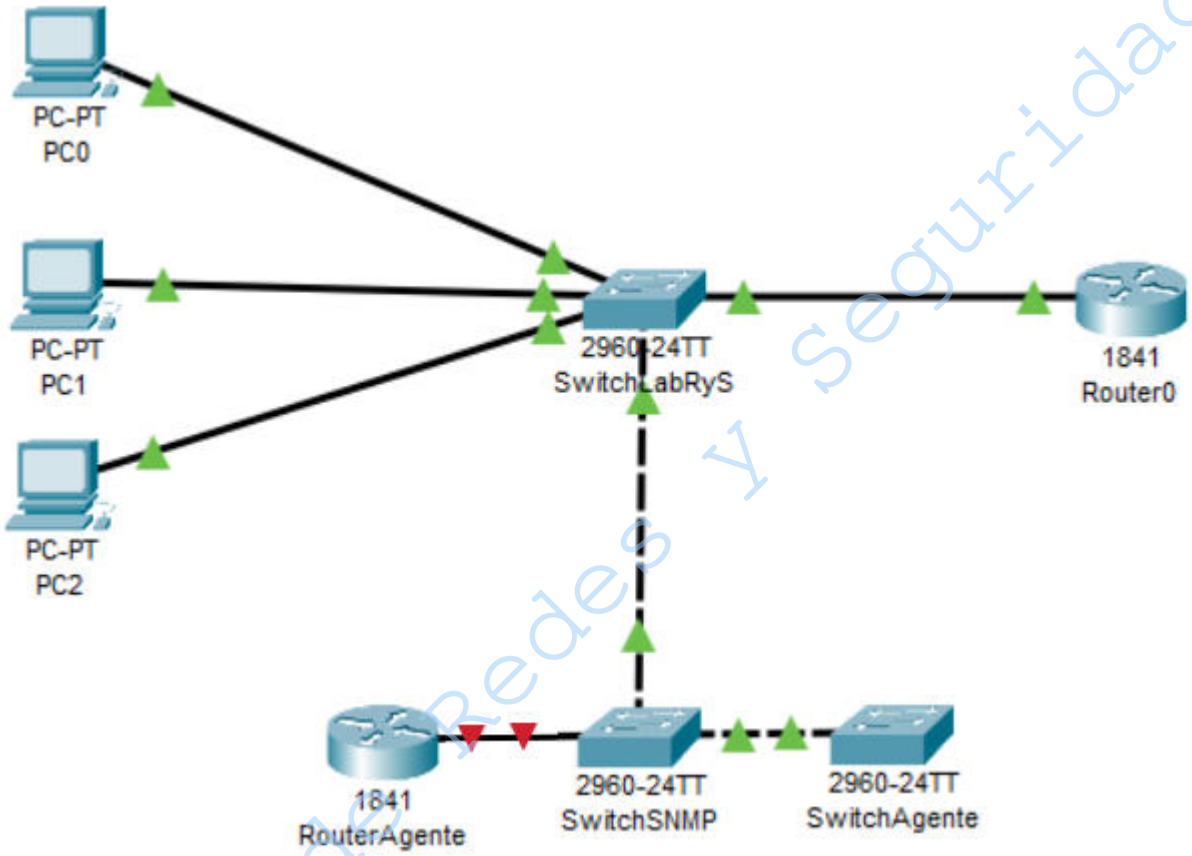



**Figura No. 2 Topología**

*4.2.2* Con ayuda de su profesor o profesora conecte PC1 y PC2 mediante un cable consola al SwitchAgente y al RouterAgente respectivamente, utilice la interfaz RS232 de las PC y la interfaz Console del Switch y del Router como lo muestra la Figura No. 3.

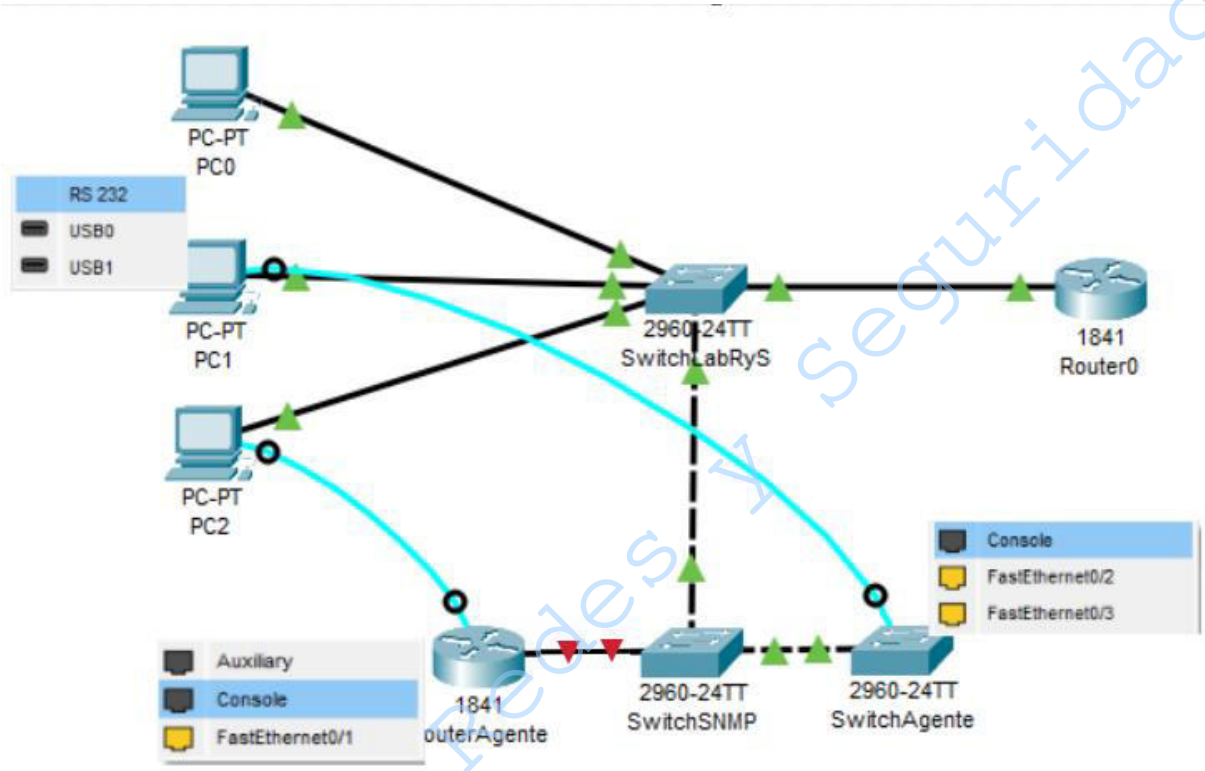



**Figura No. 3 Conexiones**

**NOTA:** Guarde constantemente su archivo para no perder su progreso.

### *4.3* Configuración del Switch SNMP

*4.3.1* Seleccione el SwitchSNMP y asígnele el nombre ***SwitchSNMP*** mediante el comando hostname como lo realizó en el cuestionario previo con el SwitchLabRyS.

*4.3.2* Configure la contraseña para el modo privilegiado del Switch empleando los siguientes comandos:

**SwitchSNMP>enable**
**SwitchSNMP>configure terminal**
**SwitchSNMP(config)#enable password CONTRASEÑA**

**SwitchSNMP(config)#exit**

Donde **CONTRASEÑA** será sustituida por alguna de su preferencia. Anote la contraseña utilizada: _____

*4.3.3* Configure la contraseña para la consola del Switch empleando los siguientes comandos:

**SwitchSNMP>enable**
**SwitchSNMP>configure terminal**
**SwitchSNMP(config-line)#line console 0**
**SwitchSNMP(config-line)#password CONTRASEÑA**
**SwitchSNMP(config-line)#login**
**SwitchSNMP(config-line)#exit**

Donde CONTRASEÑA será sustituida por alguna clave de su preferencia. Anote la contraseña utilizada:_____

*4.3.4* Asigne una dirección IP al SwitchSNMP dentro del rango relacionado con el segmento de red 192.168.2.0, utilice vlan 1 como interfaz y enciéndala con los siguientes comandos

**SwitchSNMP>enable**
**SwitchSNMP#configure terminal**
**SwitchSNMP(config)#interface vlan 1**
**SwitchSNMP(config-if)#ip address IP_SWITCHSNMP MÁSCARA_RED**
**SwitchSNMP(config-if)#no shutdown**
**SwitchSNMP(config-if)#exit**

IP_SWITCHSNMP: Es la dirección IP del SwitchSNMP dentro del segmento 192.168.2.0
MÁSCARA_RED: Es la máscara de red para el segmento 192.168.2.0
Anote la dirección IP utilizada: _____

### *4.4* Configuración de comunidades SNMP

*4.4.1* Configure la comunidad SNMP de lectura en el SwitchSNMP ingresando los comandos:

**SwitchSNMP>enable**
**SwitchSNMP#configure terminal**
**SwitchSNMP(config)#snmp-server community s0l0le0 ro**
**SwitchSNMP(config)#exit**

Donde:
El símbolo "***0***" se trata de ceros no de la letra "O" mayúscula.
**ro** significa Read Only y con ella se puede consultar la configuración de los equipos que pertenecen a la comunidad

### 4.5 Configuración del Switch Agente

*4.5.1* Para configurar el Switch que será administrado de manera remota, seleccione la terminal en la pestaña Desktop (Figura No. 4) de la PC1 conectada al SwitchAgente mediante la interfaz consola, emplee los parámetros que se muestran en la figura No. 5.

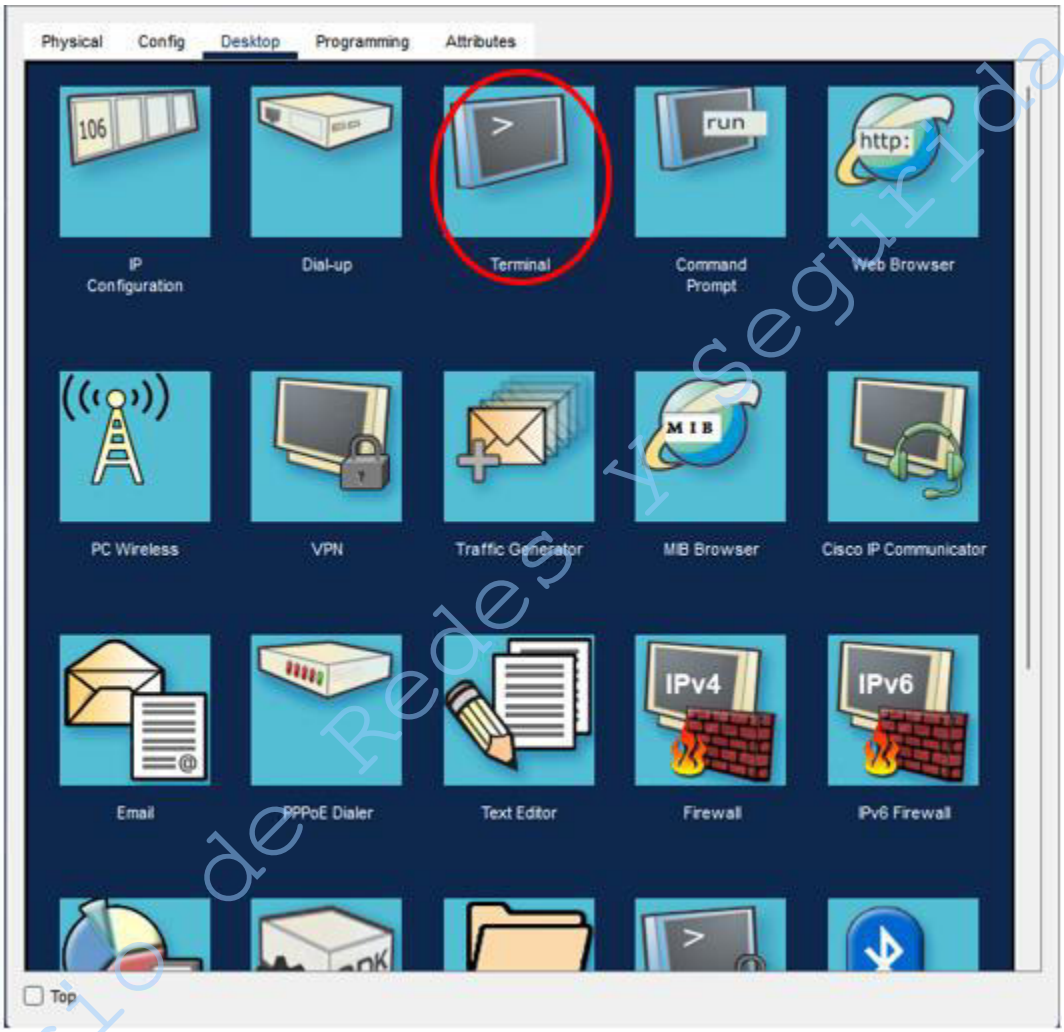



**Figura No.4 Terminal**

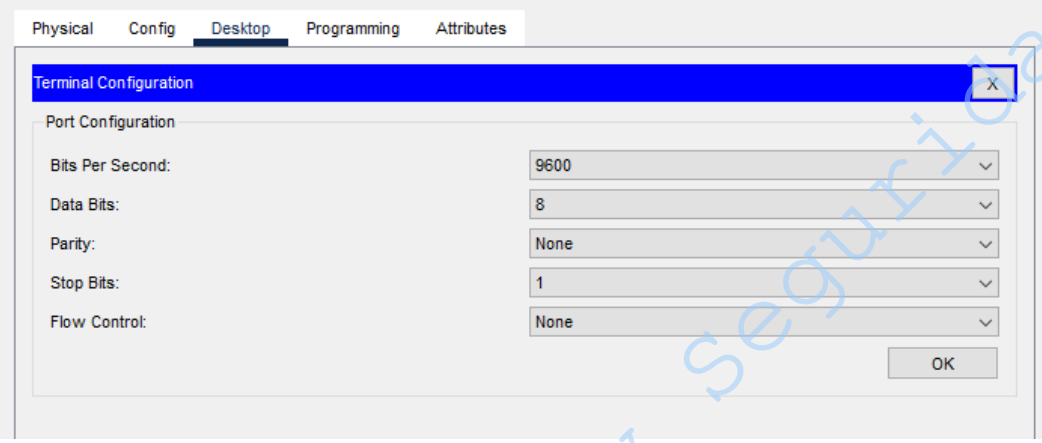



**Figura No. 5 Parámetros**

*4.5.2* Emplee la ventana correspondiente a la pestaña CLI del Switch. Presione Enter y asígnele el nombre SwitchAgente mediante el comando hostname como lo realizó en el cuestionario previo con el SwitchLabRyS.

*4.5.3* Asigne una dirección IP al SwitchAgente utilizando vlan 1 como interfaz y enciéndala con los siguientes comandos:

**SwitchAgente>enable**
**SwitchAgente#configure terminal**
**SwitchAgente(config)#interface vlan 1**
**SwitchAgente(config-if)#ip address IP_SWITCHAGENTE MÁSCARA_RED**
**SwitchAgente(config-if)#no shutdown**
**SwitchAgente(config-if)#exit**

**IP_SWITCHAGENTE**: Es la dirección del SwitchAgente dentro del segmento 192.168.2.0
**MÁSCARA_RED**: Es la máscara de red para el segmento 192.168.2.0
Anote la dirección utilizada: _____

### 4.6 Configuración de las comunidades SNMP en el Switch Agente

*4.6.1* Configure la comunidad SNMP de lectura en el *SwitchAgente* ingresando los comandos:

```
SwitchAgente>enable
SwitchAgente#configure terminal
SwitchAgente(config)#snmp-server community s0l0le0 ro
SwitchAgente(config)#snmp-server community le0escrib0 rw
SwitchAgente(config)#exit
```

**Donde:**
El símbolo "0" se trata de ceros no de la letra "O" mayúscula.
**ro** significa Read Only y con ella se puede consultar la configuración de los equipos que pertenecen a la comunidad.
**rw** significa Read Write y con ella se puede consultar y modificar la configuración de los equipos que pertenecen a la comunidad.

## 4.7 Configuración del Router Agente

*4.7.1* Para configurar el Router que será administrado de manera remota, ingrese a la terminal en Desktop de la PC2 conectada al RouterAgente mediante consola (Figura No. 6), emplee los parámetros que se muestran en la figura No. 7.


**Figura No. 6. Terminal**

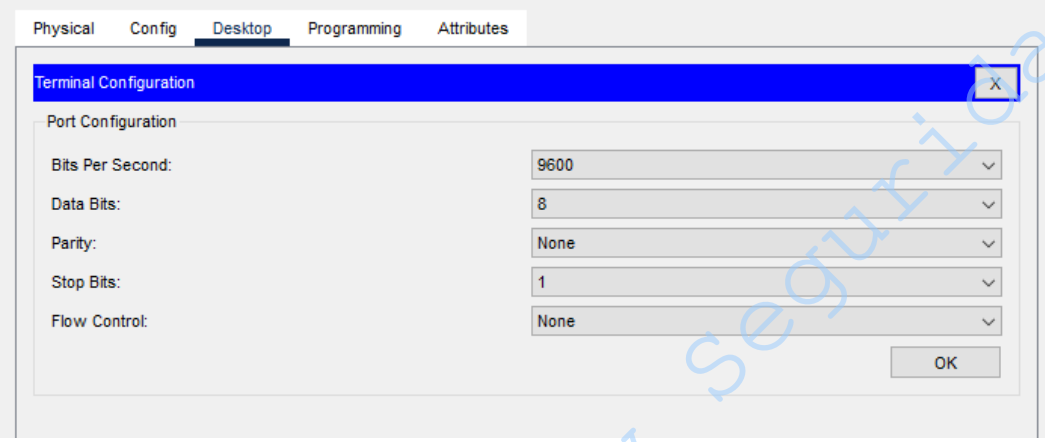



**Figura No. 7. Parámetros**

*4.7.2* Ahora seleccione la ventana correspondiente a la pestaña CLI del Router. Escriba no y presione Enter. Asígnele el nombre RouterAgente mediante el comando hostname como lo realizó en el cuestionario previo con el SwitchLabRyS.

*4.7.3* Asigne una dirección IP al *RouterAgente*, utilice la interfaz que está conectada al SwitchSNMP en INTERFACE y enciéndala con los siguientes comandos:

**RouterAgente>enable**
**RouterAgente#configure terminal**
**RouterAgente(config)#interface INTERFACE**
**RouterAgente(config-if)#ip address IP_ROUTERAGENTE MÁSCARA_RED**
**RouterAgente(config-if)#no shutdown**
**RouterAgente(config-if)#exit**

**IP_ROUTERAGENTE**: Es la dirección del *RouterAgente* dentro del segmento 192.168.2.0.
**MÁSCARA_RED**: Es la máscara de red para el segmento 192.168.2.0

Anote la dirección IP utilizada

_____

## 4.8 Configuración de las comunidades SNMP – RouterAgente

*4.8.1* Configure la comunidad SNMP de lectura en el *RouterAgente* ingresando los comandos:

**RouterAgente>enable**
**RouterAgente#configure terminal**
**RouterAgente(config)#snmp-server community s0l0le0 ro**
**Router(config)#snmp-server community le0escrib0 rw**
**Router(config)#exit**

**Donde:**
El símbolo "0" se trata de ceros no de la letra "O" mayúscula.
**ro** significa Read Only y con ella se puede consultar la configuración de los equipos que pertenecen a la comunidad
**rw** significa Read Write y con ella se puede consultar y modificar la configuración de los equipos que pertenecen a la comunidad

## 4.9 Uso de MIB Browser

*4.9.1* Dé clic sobre la PC que está conectada únicamente a *SwitchLabRyS* y abra MIB Browser dando clic en su aplicación en la pestaña Desktop (Figura No. 8).

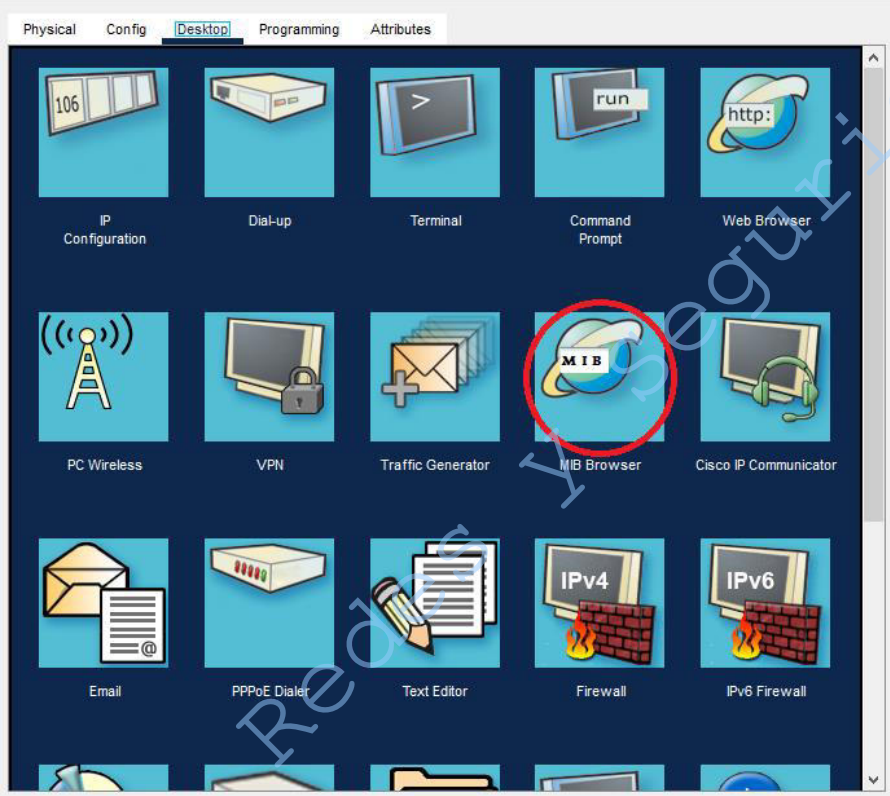



**Figura No. 8 Aplicación MIB Browser en PC**

*4.9.2* En la sección de *Address de la ventana MIB Browser* escriba la dirección IP del *RouterAgente* (Figura No. 9).

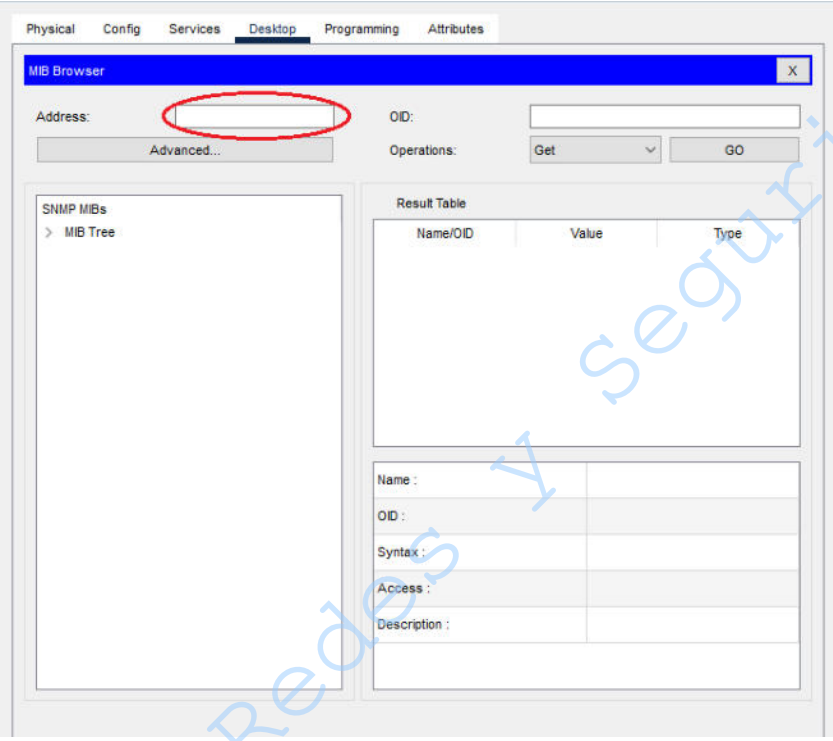



**Figura No. 9. Ventana MIB Browser**

*4.9.3* Despliegue el árbol MIB hasta llegar a *system*, para ello haga clic en la flecha al lado de *MIB tree* y en las flechas subsecuentes como lo muestra la Figura No. 10.

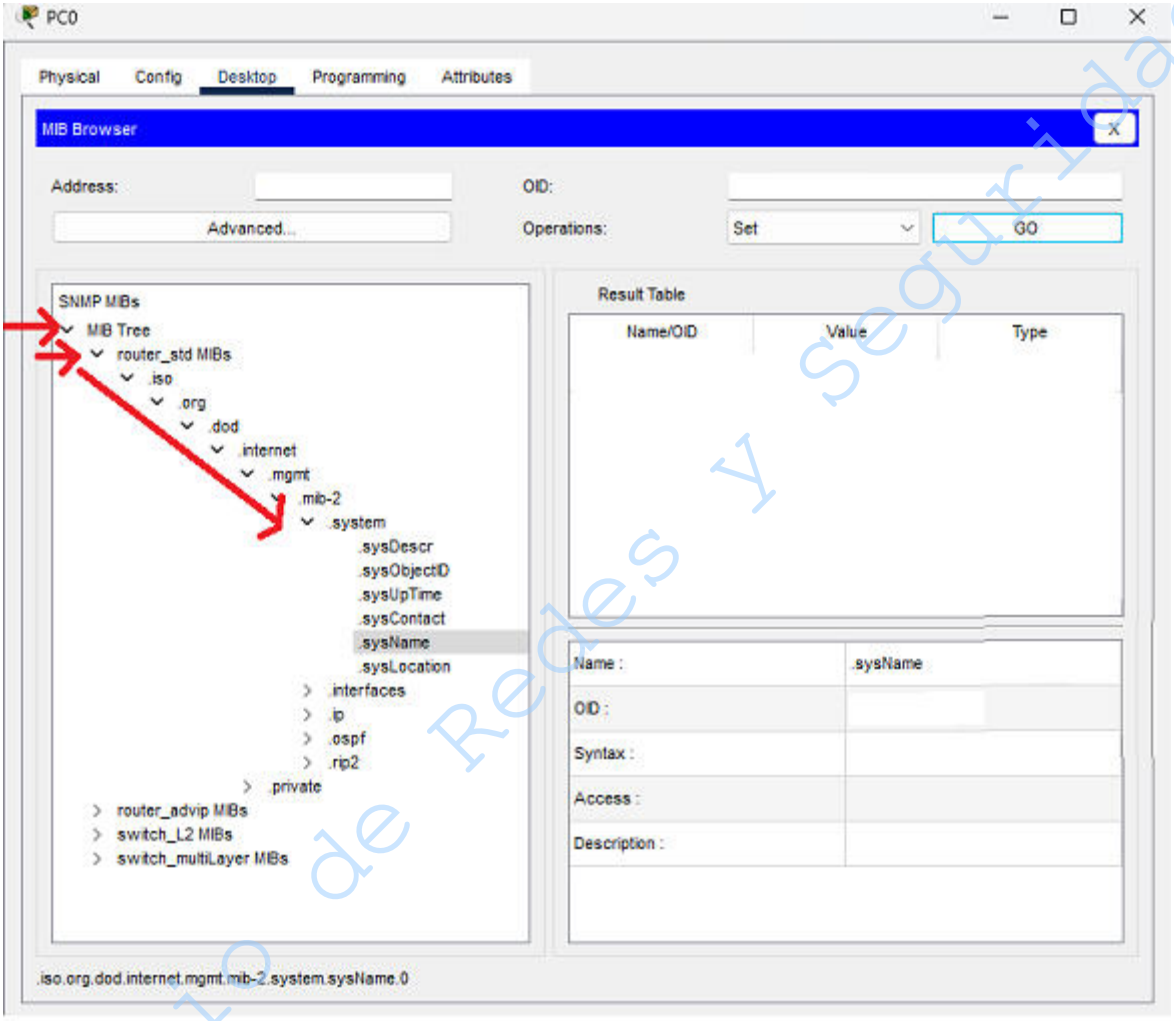



**Figura No. 10. Árbol MIB**

**I.** ***Anote los parámetros de administración definidos en el grupo de system***

_____

_____

_____

_____

_____

*4.9.4* Para especificar las preferencias del protocolo SNMP, seleccione la opción *Advanced.* (Figura No. 11).

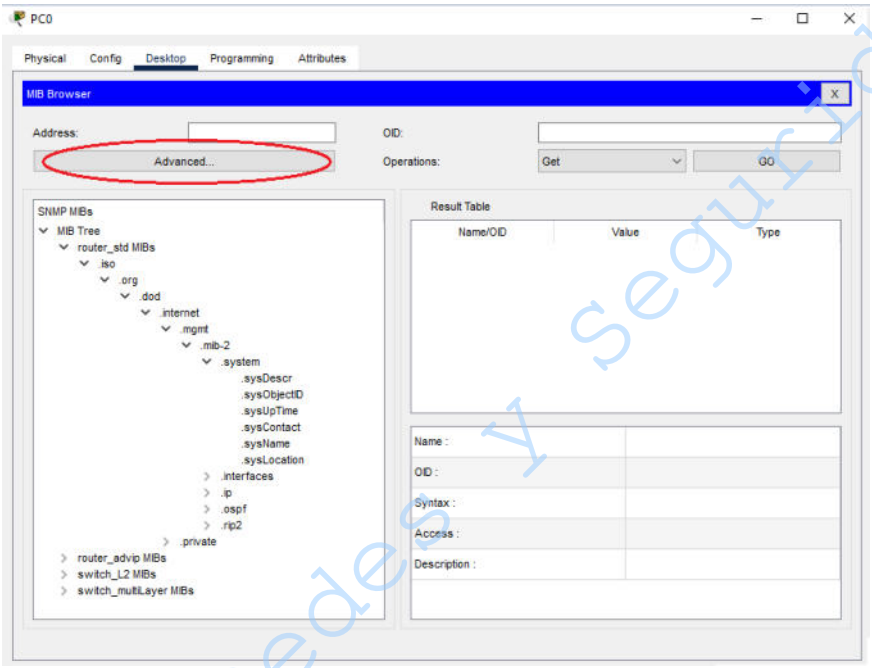



**Figura No. 11. Opciones avanzadas**

*4.9.5* Una vez ingresada a la opción, ingrese la dirección IP utilizada en el punto 4.9.2, posteriormente escriba 161 en la opción Port, que es el número de puerto por defecto para SNMP, y seleccione v2 en la sección SNMP Versión. (Figura No. 12).

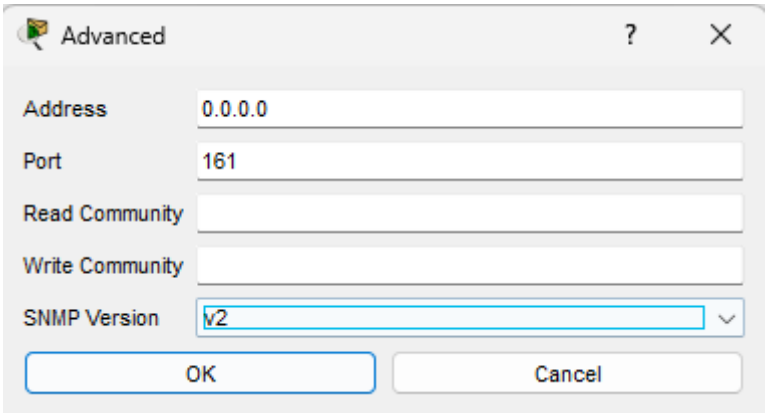



**Figura No. 12. Preferencias de SNMP**

*4.9.6* En la sección de Read Community escribir ***s0l0le0*** y en la sección Write Community ***le0escrib0,*** donde los "0" son ceros no la letra O mayúscula, al finalizar dé clic en OK.

*4.9.7* Consulte el nombre del RouterAgente en el apartado *Value* de la sección *Result Table*, seleccionando *.sysName* en el Árbol MIB y dando clic en GO (Figura No. 13).

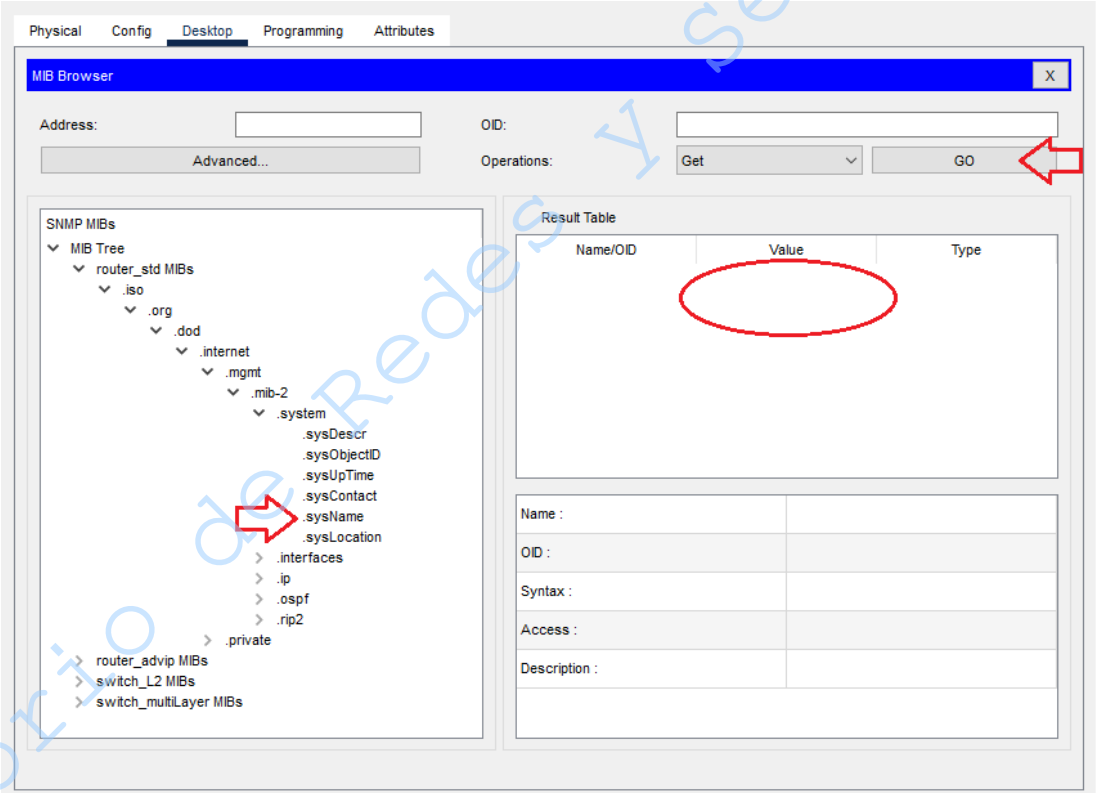



**Figura No. 13. Consulta del nombre del Router.**

**NOTA: Es posible que tarde en responder el programa y aparezca una ventana emergente de error. Para solucionarlo guarde su progreso, cierre Packet Tracer, espere un momento, abra nuevamente el archivo y ejecute la consulta siguiendo los pasos desde el 4.9.1 hasta el 4.9.7.**

*4.9.8* Cambie el nombre del router por Administracion, para ello seleccione la opción Set en el apartado *Operations,* (Figura No. 14).

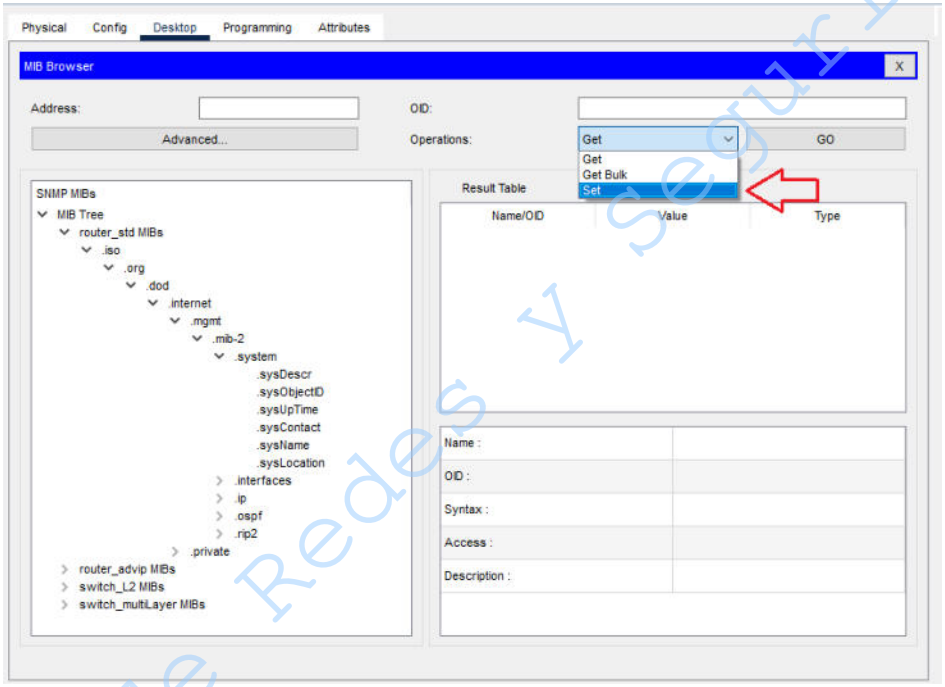



**Figura No. 14. Opción Set para modificar valores**

*4.9.9* En la ventana emergente seleccione en campo *Data Type* el tipo de dato que coincida con el *Type* que se observa en la consulta anterior (Figura No. 15).

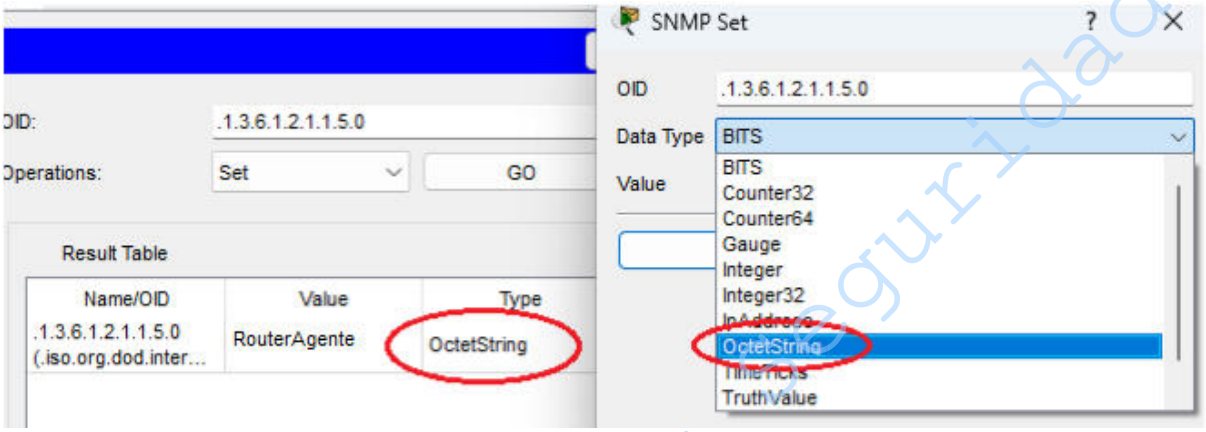



**Figura No. 15. Ventana de modificación**

*4.9.10* Escribe el nuevo nombre en el campo de *value* y dé clic en OK (Figura No. 16).

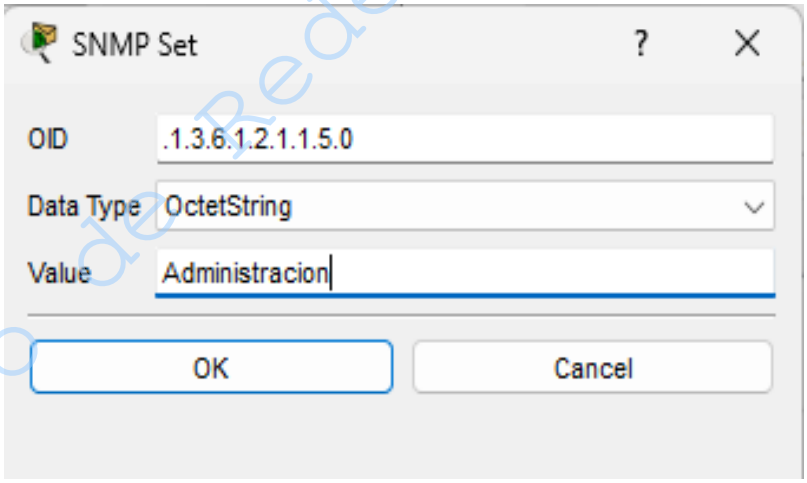



**Figura No. 16. Cambio de nombre al Router**

El cambio se verá reflejado al dar clic sobre GO en la ventana MIB Browser (Figura No. 17).

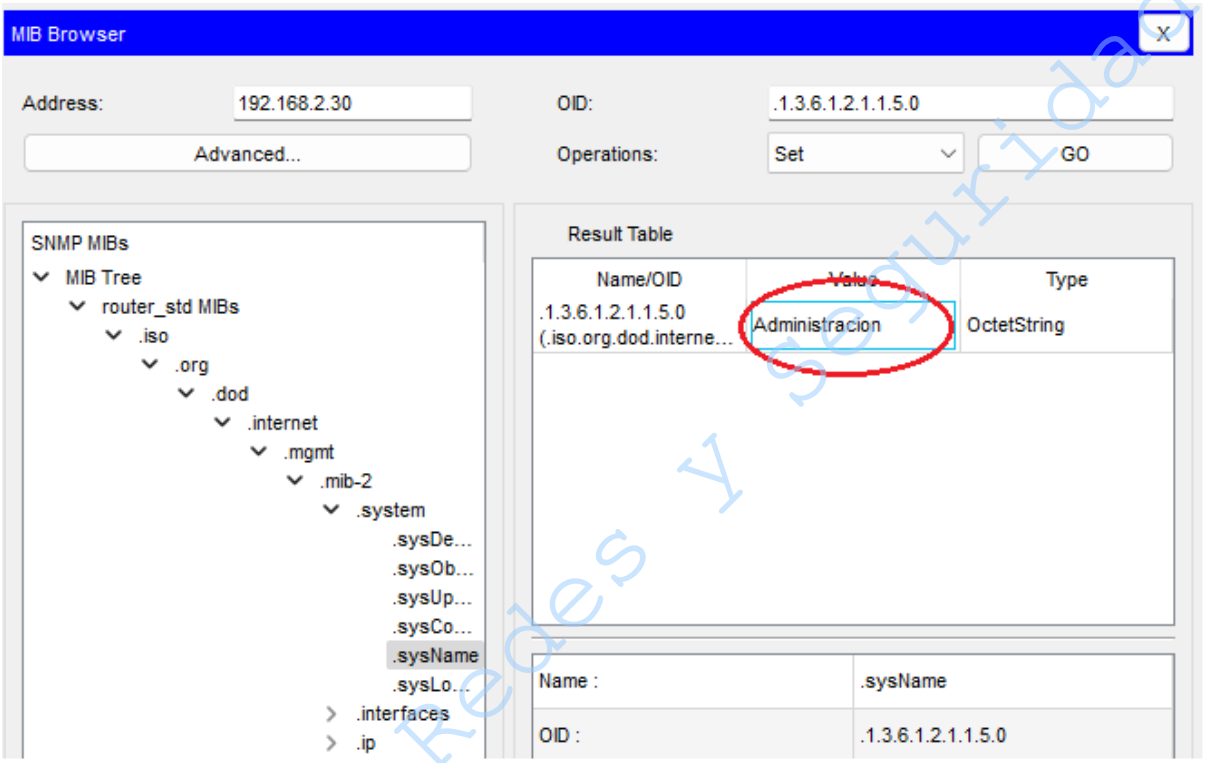



**Figura No. 17. Nombre de Router actualizado a Administración**

*4.9.11* Para comprobar el cambio en el RouterAgente, entre a la Terminal de la PC2 que tiene conectada mediante consola como lo realizó en el paso 4.7.1.

***II. Describa lo que observa***

_____
_____
_____
_____

## 4.10 Consulta de interfaces en Switch

*4.10.1* Dentro del MIB Browser, cambie la IP del campo *Address* por la del *SwitchAgente* (Figura No. 18).

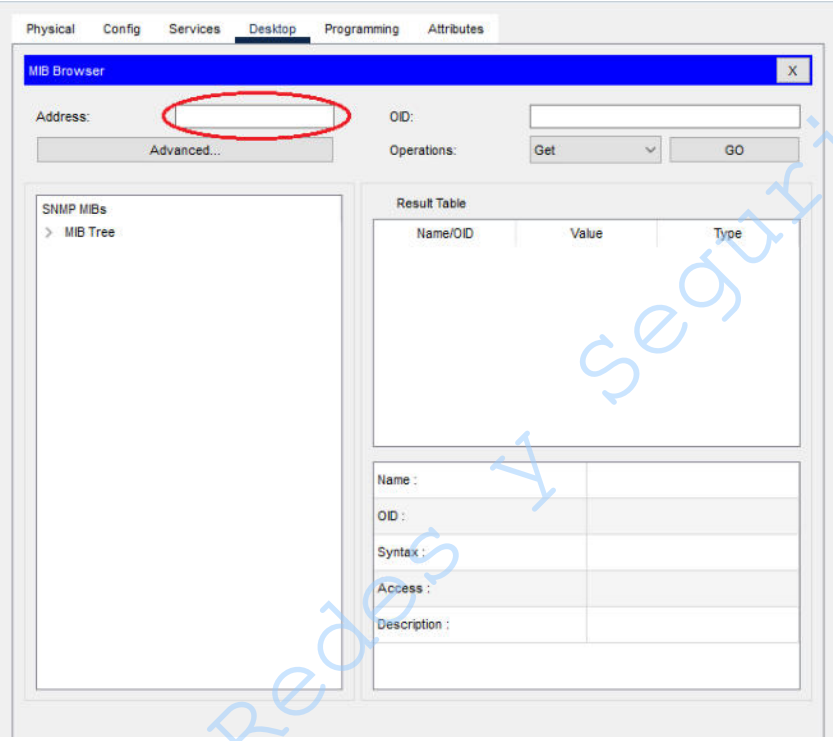



**Figura No. 18. Dirección IP**

*4.10.2* Seleccione ahora la opción *interfaces* dando clic en el Árbol MIB como se muestra en la Figura No. 19.

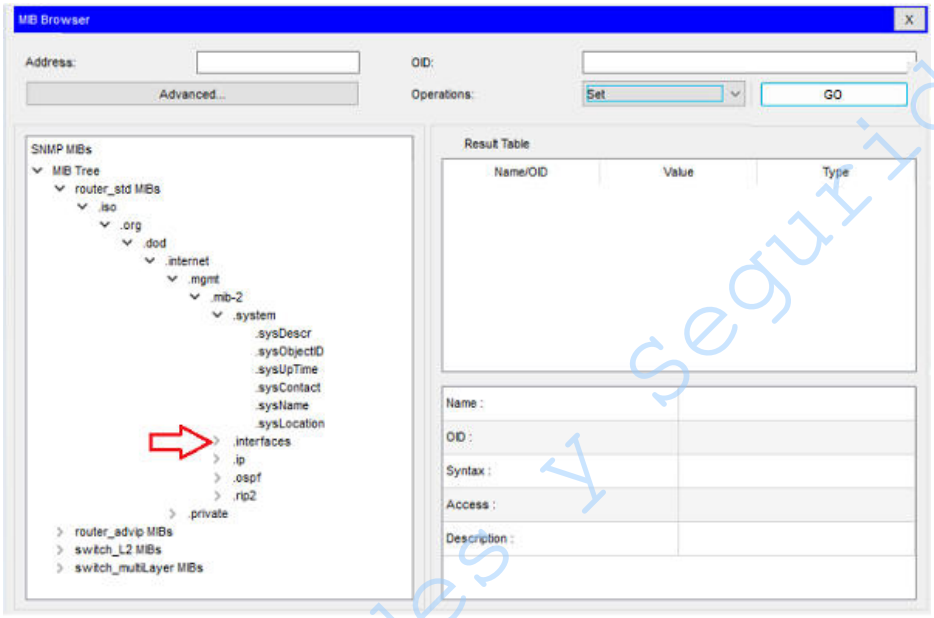



**Figura No. 19. Selección de nodo interfaces**

Seleccione la opción Get Bulk en el apartado Operations y dé clic en GO (Figura No. 20).

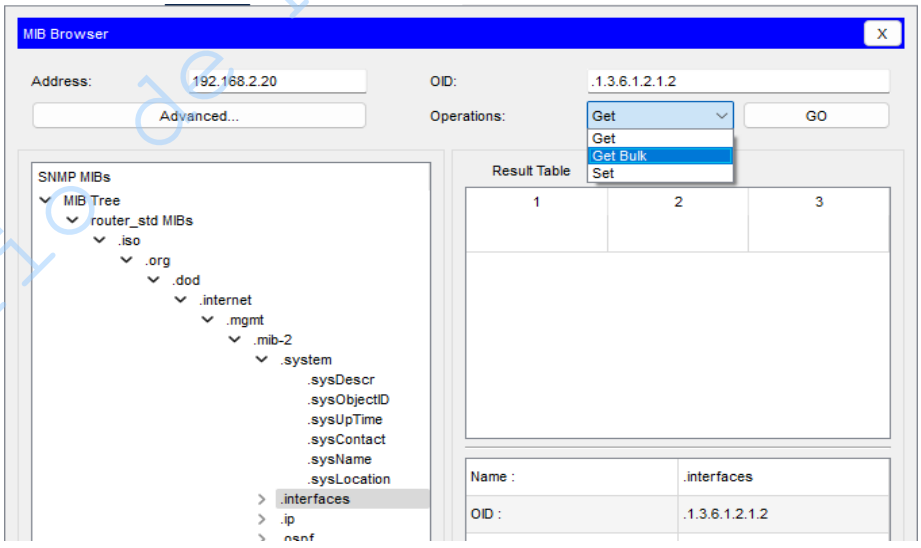



**Figura No. 20 Uso de Get Bulk**

***I. Describa lo que observa en la sección Result Table***

4.10.3 Seleccione la opción *Get* en el apartado *Operations* y dé clic en GO. Notará que da error al hacer la consulta.

***II. ¿Cuál es la diferencia entre Get y Get Bulk, y por qué la consulta de interfaces da error al utilizar Get?***

**5.- Conclusiones**

Revise los objetivos de la práctica y las actividades realizadas y emita sus conclusiones.

**PRÁCTICA 5**
**Administración con SNMP en Windows**
***Cuestionario Previo***

1. ¿Qué es un modelo de administración de red?
2. Investigue las características principales de los protocolos de administración de red: SNMP.
3. Investigue los orígenes del protocolo SNMP, así como las versiones de snmpV1 snmpV2 y snmpV3 mencionando la diferencia principal entre éstas.
4. Investigue la estructura de la MIB.
5. Investigue la estructura jerárquica de la MIB.
6. Investigue el concepto de identificador de objeto.
7. Investigue qué es una comunidad en SNMP.
8. Investigue qué es una comunidad pública y una comunidad privada en SNMP.
9. ¿Qué son las notificaciones, los traps y las peticiones de informe de SNMP?
10. Investigue qué es una MMC (Microsoft Management Console).
11. Investigue la sintaxis y el funcionamiento de los siguientes comandos para la configuración del SNMP en un switch: a) snmp-server community. b) snmp-server view phred c) access-list
12. Configure la siguiente topología en Cisco Packet Tracer para realizar los ejercicios de la práctica (Figura A):

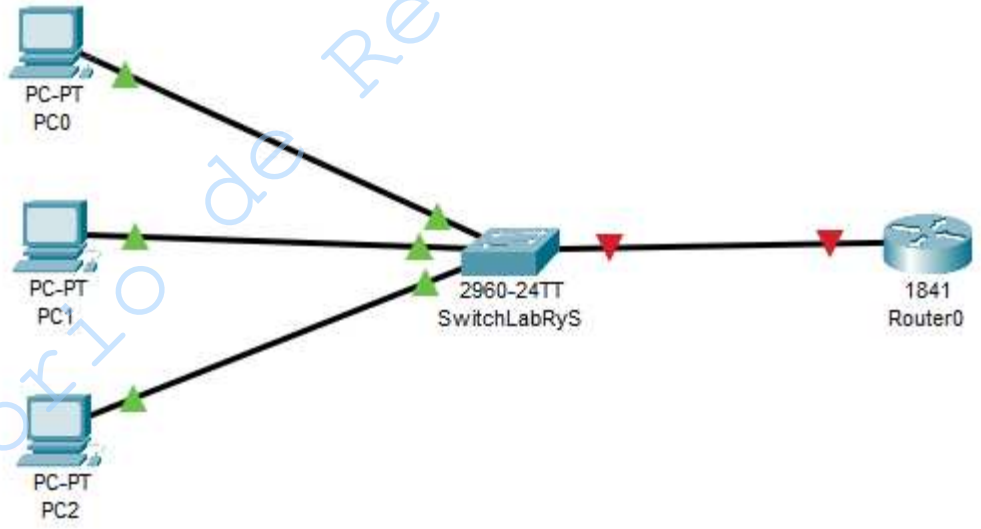



**Figura A. Topología de red para trabajar**

Modifique la etiqueta y el nombre del Switch por SwitchLabRyS como se muestra en la figura A utilizando los siguientes comandos en la pestaña CLI:

**Switch> enable**
**Switch# configure terminal**
**Switch(config)# hostname NOMBRE**

**enable**: Este comando habilita el modo privilegiado en el Switch
**configure terminal**: Este comando habilita la configuración global del Switch
**hostname**: Con este comando se asigna el nombre al Switch, sustituya **NOMBRE** por el solicitado.

**NOTA: Estos comandos se pueden utilizar tanto en Switches como en Routers**

Configure la dirección IP del Router y las PC 's. Con esa información complete la siguiente tabla No. 1 utilizando 192.168.2.0 como segmento de red.

**NOTA: Recuerde encender la interfaz del Router para que haya comunicación.**

**Tabla No. 1. Asignación de direcciones**

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred | Puerta de Enlace |
|---|---|---|---|---|
| Router0 | | | | |
| PC0 | | | | |
| PC1 | | | | |
| PC2 | | | | |

13. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

# Práctica 6

# Configuración de VoIP

## Integración

### *1.- Objetivos de Aprendizaje*

- El alumno o la alumna adquirirá los conocimientos básicos acerca de VoIP como medio de comunicación, así como los protocolos de señalización y transmisión para poder llevar a cabo una llamada telefónica por medio de redes IP.

- El alumno o la alumna configurará un conmutador de VoIP empleando el software Asterisk para el PBX versión 1.2.7.1 y X-Lite Softphone para establecer una llamada VoIP.

### *2.- Conceptos teóricos*

Los elementos principales de una red corporativa de voz son los sistemas de conmutación, a los que hay que añadir los elementos de transmisión, de supervisión y los propios equipos de usuarios. Como elementos de conmutación existen varios tipos de dispositivos que pueden desempeñar esta función:

- KTS, Sistemas Multilínea (Key Telephone System).
- PBX, Central Privada de Intercambio (Private Brand eXchange).
- Centrex, Oficina Central de Intercambio de Servicio (Central Office Exchange Service).

En esta práctica utilizará la conmutación por PBX, que es un sistema de telefonía que interconecta las extensiones telefónicas internas, con las troncales telefónicas; además usa métodos de conmutación digitales que pueden soportar la instalación de teléfonos y líneas tanto analógicas como digitales.

Un softphone (combinación de Software y de Telephone) es un software que hace una simulación de teléfono convencional por computadora, permite usar la computadora para hacer llamadas a otros softphones o a otros teléfonos convencionales usando un VSP, Proveedor de Servicios de VoIP (VoIP Service Provider).

Asterisk, es una PBX completamente diseñada en software que funciona en Linux y proporciona todas las características de una PBX. Trabaja con VoIP en varios protocolos (SIP, H.323) e interactúa con casi todo el equipo estándar basado en telefonía IP.

El funcionamiento de VoIP (Voz sobre el Protocolo Internet - Voice Over Internet Protocol) consiste en la conversión de las señales de voz estándar en paquetes de datos comprimidos que son transportados a través de redes de datos en lugar de líneas telefónicas tradicionales. La evolución de la transmisión conmutada por circuitos basada en paquetes toma el tráfico de la red pública telefónica y lo coloca en redes IP bien aprovisionadas. Las señales de voz se encapsulan en paquetes IP que pueden transportarse como IP nativo o como IP por Ethernet, Frame Relay, ATM o SONET.

La operación básica de VoIP consiste fundamentalmente en:

1. Digitalizar la voz en el extremo que emite.
2. Compactar la voz digitalizada.
3. Transmitirla como un conjunto de paquetes de datos por IP.

4. Recibir los paquetes en el otro extremo de la comunicación.
5. Descompactarlos.
6. Reproducirlos para ser escuchados.

La convergencia de las redes de voz y de datos, han tenido como consecuencia profundos cambios en el desarrollo y la implementación de soluciones corporativas para la pequeña y mediana empresa fundamentalmente. Es por ello que un administrador de redes debe tener la capacidad de llevar a cabo la integración total de los servicios de comunicación.

## *2.1* Estándares de VoIP

Para poder llevar a cabo una llamada telefónica a través de Internet, son necesarios los protocolos de señalización y transporte.

El soporte de una llamada telefónica sobre una red de paquetes, que en la mayoría de los casos es una red IP consta de dos fases:

1. Establecimiento de la llamada, esto es el equivalente a la obtención de tono de invitación a marcar, la marcación de número destino, la obtención de timbre de llamada o de la señal de ocupado y el descolgado del receptor para contestar la llamada.
2. La propia conversación.

En cualquiera de estas dos fases es necesaria una serie de estándares que regulen y permitan la interconexión de equipos de distintos fabricantes como los protocolos de señalización y los protocolos de transporte.

### 2.1.1 *Protocolos de señalización*

Los protocolos de señalización tienen como objetivo el establecimiento de las llamadas y son básicamente el corazón de la voz sobre paquetes, distinguiéndose de otros tipos de servicios. Las funciones que realizan son:

1. *Localización de usuarios*, si un usuario A se desea comunicar con un usuario B, en primer lugar A necesita descubrir la localización actual de B en la red con el fin de que la petición del establecimiento de sesión pueda establecerse.
2. *Establecimiento de sesión*, el protocolo de señalización permite al usuario llamado aceptar la llamada, rechazarla o desviarla a otra persona, buzón de voz o página Web.
3. *Negociación de la sesión*, la sesión multimedia que se está estableciendo puede comprender diferentes tipos de flujo de información (audio, video, etcétera). Cada uno de estos flujos puede utilizar algoritmos de compresión de audio y video diferentes, dado que puede tener lugar en diferentes puertos y direcciones unicast o multicast. El proceso de negociación permite a las partes implicadas acordar un conjunto de parámetros de inicialización.

4. *Administración de los participantes en la llamada*, es posible añadir y/o eliminar miembros de una sesión ya establecida.
5. *Otras funciones*, como transferir una llamada o el colgar dicha llamada, requiere la conmutación entre los dos extremos.

Para cumplir con todos estos requisitos, existen fundamentalmente tres protocolos:

- H.323, fue concebido para comunicaciones multimedia en redes de área local, pero se ha extendido a la VoIP, proporciona control de llamadas, funciones de conferencia, administración de llamadas, capacidad de negociación de parámetros y otros servicios complementarios.
- SIP (Protocolo para Inicio de Sesión - Session Initiation Protocol), ha sido diseñado para soportar el control de llamadas y la negociación de sesiones de forma distribuida.
- MGCP, Protocolo de Control de Pasarela de Medios (Media Gateway Control Protocol), se trata de un control de protocolo que permite a un controlador centra,l el monitoreo de eventos que ocurren en los teléfonos IP y en las pasarelas, les impone el envío de información a direcciones específicas, etc.

### 2.1.2 Protocolos de Transporte

Los protocolos de transporte tienen como objetivo asegurar la comunicación de voz para el establecimiento de una red para transportar contenidos multimedia bajo demanda de las aplicaciones que la utilizan, siendo ésta una tarea no trivial. Podemos contar con al menos tres dificultades que son:

1. Mayores requerimientos de ancho de banda.
2. La mayoría de las aplicaciones multimedia requieren el tráfico en tiempo real.
3. Secuencia de carácter crítico en la generación de los datos multimedia.

Para solucionar estos problemas se crearon los protocolos de transporte, cuya misión es trasladar la información útil del origen al destino, cumpliendo con los requerimientos exigidos por las aplicaciones multimedia en general y por la voz en particular. Los protocolos de transporte más empleados en la integración de voz y de datos son RTP (Protocolo de Transporte en Tiempo Real - Real Time Transport Protocol) y el RTCP (Protocolo de Control en Tiempo Real - Real Time Control Protocol).

## 2.2 Asterisk

La solución de telefonía basada en Asterisk ofrece las funciones propias de las centralitas clásicas y además características avanzadas, logrando trabajar tanto con sistemas de telefonía estándar tradicionales como con sistemas de VoIP.

Asterisk está dotado con características que sólo ofrecen los grandes sistemas PBX propietarios como: buzón de voz, conferencia de voz, llamadas en espera y registros de llamadas detalladas. Para funcionar con VoIP no necesita de ningún hardware adicional, para interconectar con la telefonía tradicional requiere de tarjetas especiales de muy bajo costo (tarjetas FXO, FXS).

### 2.2.1 Instalación del servidor VoIP

Para la instalación del servidor de VoIP, se requiere de una PC que sea destinada para funcionar como conmutador telefónico. A esta PC le será cargado una versión de la distribución Linux CentOS que incluye Asterisk@home. (Ver Figura No. 1)


**Figura No. 1. Interfaz de la aplicación CentOS**

**NOTA: Hay que tener en cuenta que Asterisk@home no es únicamente la aplicación como tal; la instalación borrará sin previo aviso todas las particiones que se encuentren en el equipo, eliminando los datos.**

Ya que se tiene instalado el sistema operativo y una vez reiniciado el equipo, el sistema estará ocupado compilando las aplicaciones. Trascurridos entre 30 y 45 minutos y tras un segundo reinicio, aparecerá el login del equipo para que el administrador se valide. (Ver Figura No. 2)

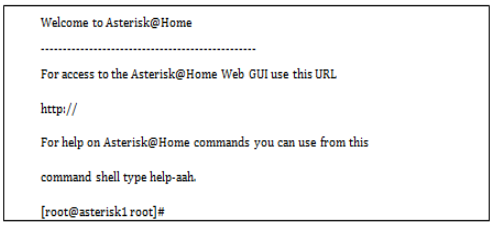



**Figura No. 2. Vista por primera vez del servidor VoIP, Asterisk@home**

El sistema viene con un usuario por defecto ***root*** y una contraseña también por defecto ***password***, así que será necesario cambiarla mediante el comando ***passwd*** desde la línea de comandos.

A continuación se tendrá que ejecutar la aplicación ***netconfig***, para configurar los parámetros de la tarjeta de red (IP, máscara, DNS, gateway), el equipo se tendrá que reiniciar para que los cambios sean efectivos.

Una vez arrancado el servidor, aparecerá de nuevo el mismo mensaje de bienvenida, pero esta vez con la dirección Web a la que se llamará para ejecutar la administración del servidor. (Ver Figura No. 3)


**Figura No. 3 Vista configurada del servidor VoIP, Asterisk@home**

Hasta este punto se tiene ya instalado completamente el servidor, ahora será necesario configurar la herramienta vía Web.

***3.- Equipo y material necesario***

***Material del alumno o de la alumna:***

- Diademas con micrófono y audífonos
- Audífonos y micrófono por separado.

***Equipo del Laboratorio:***

- PC's Pentium con una NIC Ethernet 10/100 Mbps instalada en cada una de ellas.
- Un switch Ethernet 10BaseT o FastEthernet
- Servidor de VoIP Asterisk
- Software X-Lite softphone

***4.- Desarrollo***

***Modo de trabajar***

La forma de trabajar será por parejas.

### 4.1. Configuración Vía Web

El objetivo de este punto es la configuración manual del servidor de VoIP accediendo a él a través de la conexión Web.

**4.1.1** Abra un navegador Web como Internet Explorer y escriba la dirección 192.168.2.122 en el campo del URL, ésta es la dirección que se asignó al servidor para poder ser administrado. (ver Figura No. 4)

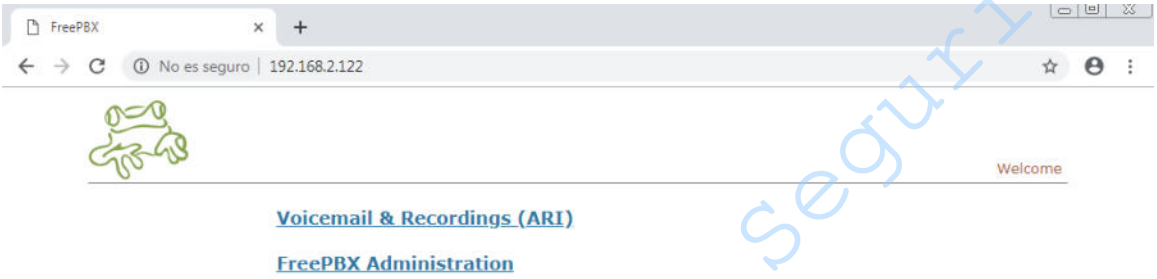



**Figura No. 4 Aplicaciones de la administración vía Web**

**4.1.2** El navegador nos muestra la ventana de bienvenida, podrá entrar a Voicemail & Recordings(ARI) y FreePBX Administration; navegue por estos menús de ser posible, en caso de no poder hacerlo investigue la funcionalidad de ellos.

**I. Anote las características que proporciona el menú Voicemail & Recordings (ARI)**

_____
_____
_____
_____
_____

**II. Anote las características que proporciona el menú FreePBX Administration**

_____
_____
_____
_____
_____

**4.1.3** Para FreePBX Administration, es necesario entrar como administrador, coloque en los campos de usuario y contraseña, **admin** como nombre de usuario y **admin** como contraseña. Estos campos son los predeterminados en la configuración inicial. (ver Figura No. 5)

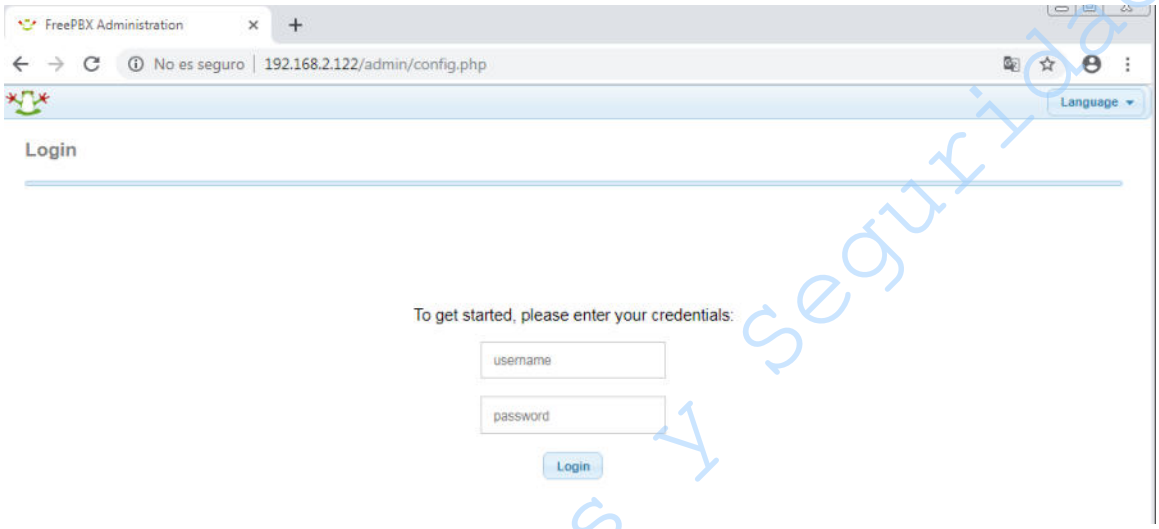



**Figura No. 5 Solicitud de usuario y contraseña**

**4.1.4** Una vez validados se tiene acceso a una serie de aplicaciones de administración: Admin, Applications, Connectivity, Reports, Settings

**Nota:** Dentro de esta aplicación es posible administrar al servidor en todos sus aspectos, incluso editando vía texto los archivos de configuración.

**4.1.5** En la parte superior izquierda, observe el menú Applications, haga clic en él, seleccione el elemento Extensions (Extensiones). A través de un sencillo formulario Web podrá dar de alta y modificar las cuentas de usuario y extensiones de teléfono. (ver Figuras No. 6 y 7)

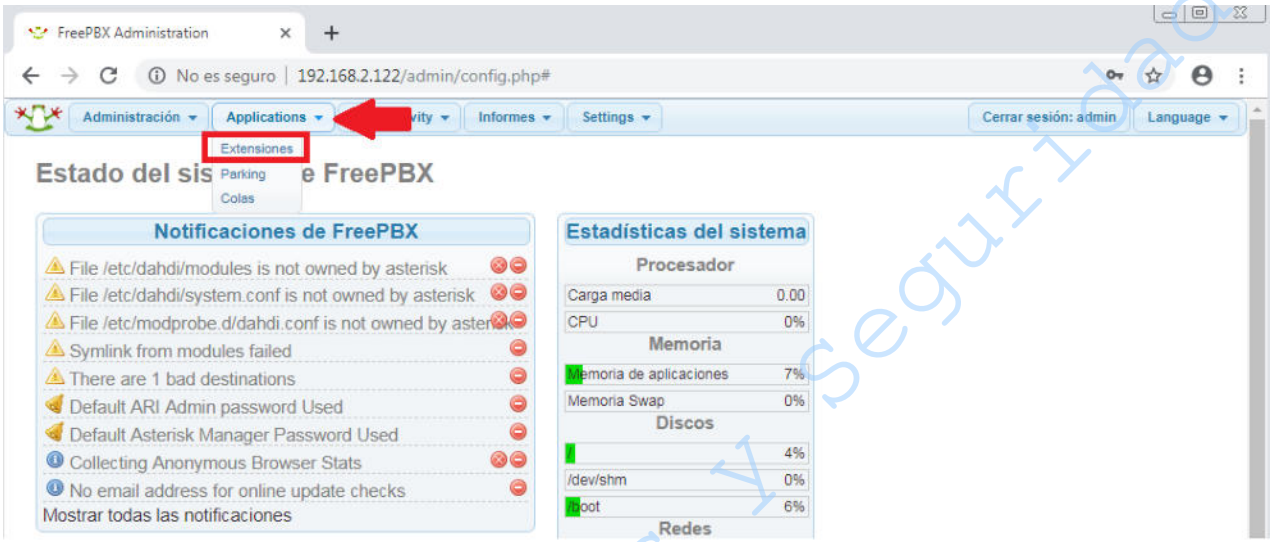



**Figura No. 6. Menú Applications**


**Figura No. 7 Menú Extensions**

**4.1.6** En este punto se dará de alta como usuario. Para inciar la configuración de la extensión debe seleccionar en Device la opción Generic SIP Device y después dar clic en Submit. Llene el

formato únicamente con los valores que se muestran en la Tabla 1.1, el resto se deja con los valores por defecto. Dar clic en Submit y en Apply Config

**NOTA: Al final de la práctica deberá eliminar la extensión que está por crear tal y como se indica en el apartado 4.4**

**Tabla 1.1. Valores de configuración para los usuarios**

| Características | Valores |
|---|---|
| User Extension | Número que está en el rango 200 – 320 |
| Display Name | Primer nombre + Primer apellido |
| secret | Iniciales_numextensión |
| dtmfmode | RFC2833 |
| nat | Yes |

## 4.2 Softphone

Un softphone es típicamente parte de un entorno VoIP y puede estar basado en el estándar SIP/H.323 o basarse en un protocolo propietario.

Los softphones son parte del grupo tecnológico CTI (Integración Computadora-Telefonía - Computer Telephony Integrated). Hay varios tipos de softphones, algunos son a través de VoIP, otros funcionan utilizando teléfonos USB y algunos están implementados completamente en software que se comunica con las PBX a través de una red de área local usando TCP/IP para controlar y marcar a través del teléfono físico. Comúnmente esto se hace a través de un entorno de centro de llamadas para comunicarse desde un directorio de clientes o para recibir llamadas, donde la información del cliente emerge en la pantalla de la computadora cuando el teléfono suena, dando a los agentes del centro de llamadas un volumen de información sobre quién está llamando, cómo recibirlo y dirigirse a él o ella.

### 4.2.1 Instalación softphone X-Lite

El X-Lite es un software muy amigable y robusto que permite realizar llamadas por Internet a través de un servidor de VoIP.

En esta parte de la práctica aprenderá a configurar un softphone para poder establecer una llamada telefónica.

**4.2.1.1** Borre el registro de la aplicación vía *INICIO>EJECUTAR>REGEDIT.EXE* , localice la siguiente subestructura del registro: HKEY_CURRENT_USER e ingrese a ella. Busque la carpeta de Software, ingrese y elimine la carpeta XtenNetwork Inc en caso de existir.

**4.2.1.2** Localice en el escritorio el software X-Lite Setup y haga clic dos veces sobre él, a continuación haga clic en el botón Next para continuar con la instalación.

**4.2.1.3** Verifique que esté seleccionada la opción I accept the agreement y después haga clic en el botón Next.

**4.2.1.4** Posteriormente el asistente le informa sobre la versión que se va a instalar, para continuar haga clic en el botón Next; a continuación le preguntará dónde desea instalar la aplicación, dejará la ubicación por default, por lo tanto haga clic en Next.

**4.2.1.5** Nuevamente haga clic en Next, y verifique que sólo esté seleccionada la casilla de Create a desktop icon y haga clic en Next.

**4.2.1.6** Haga clic en el botón Install, espere unos segundos y para completar la instalación haga clic en Finish.

### 4.2.2 Configuración softphone X-Lite

En este punto de la práctica aprenderá la configuración del softphone para poder establecer una llamada.

**4.2.2.1** Para iniciar la configuración del programa X-Lite haga doble clic en el icono creado en el escritorio.

**4.2.2.2** En el siguiente diagrama se muestran los elementos de softphone, para que se familiarice con la herramienta. (ver Figura No. 8)


**Figura No. 8 Elementos de softphone X-Lite**

**4.2.2.3** A continuación se mostrará en el escritorio el softphone y el menú para poder configurar la herramienta. (ver Figura No. 9)


**Figura No. 9 Softphone y el menú listo para configurar**

**4.2.2.4** Haga clic derecho sobre el softphone y elija del menú desplegable la opción ***Audio Tuning Wizard…***, ver Figura No. 10, posteriormente aparecerá la ventana de Audio Tuning Wizard para poder configurar el audio y micrófono.

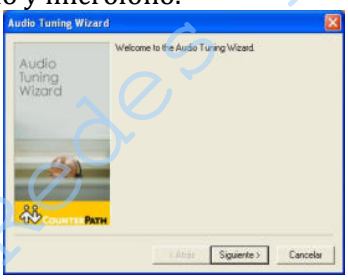



**Figura No. 10 Ventana de bienvenida al Audio Tuning Wizard**

**4.2.2.5** Conecte la Diadema (audífonos y micrófono) a la computadora, verificando que estén conectados correctamente en el lugar correspondiente.

**4.2.2.6** Haga clic en el botón Siguiente para configurar la aplicación, seleccione el tipo de micrófono que se va a utilizar y haga clic en siguiente.

**4.2.2.7** En las siguientes dos ventanas debe ajustar el volumen de los audífonos y la intensidad del micrófono, una vez realizado esto haga clic en Siguiente en cada ventana respectivamente, a continuación calibre el micrófono y posteriormente haga clic en Siguiente.

**NOTA: Si escucha sonido distorsionado, haga clic en panel de control, doble clic sobre Dispositivos de audio y sonidos, elija la pestaña Voz y posteriormente seleccione el botón prueba de hardware, siga el asistente para configuración de voz y audio.**

**4.2.2.8** Elija la opción Cable / DSL / LAN y haga clic en Siguiente, para finalizar con la configuración del Audio Tuning Wizard haga clic en Finalizar.

**NOTA: Con el Audio Tunning Wizard se han configurado automáticamente las opciones Speaker Audio device, Mic Audio device y Ring Audio Device del menú System Settings, que posteriormente serán analizados.**

**4.2.2.9** Configure el softphone a la red de acuerdo con los parámetros que se muestran en la Tabla 1.2, en el menú de Network.

**NOTA: Este menú se encuentra en *Main Menu> System Settings> Network*.**

**Tabla 1.2 Parámetros que deben configurarse en el menú Network**

| Características | Valores |
|---|---|
| **Auto_Detect_IP:** | Yes |
| **Listen_on_IP** | Dejar en blanco |
| **Use X-NAT to Choose SIP/RTP Ports** | Never |
| **Listen SIP Port** | 5060 |
| **Listen RTP Port** | 8000 |
| **NAT Firewall IP** | en blanco |
| **Out Bound SIP Proxy** | en blanco |
| **Force Firewall Type** | (do not force firewall type) |
| **Primary STUN Server** | Dejar en blanco |
| **Secondary STUN Server** | Dejar en blanco |
| **Primary DNS Server** | 132.248.204.1 ( o bien la dirección LAN, en presencia de LAN con DNS interno) |
| **Secondary DNS Server** | 132.248.10.2 ( o bien la dirección LAN, en presencia de LAN con DNS secundario interno) |
| **Provider DNS Server** | Dejar en blanco |

**4.2.2.10** Realizado el punto anterior haga clic en BACK, a continuación seleccione SIP Proxy haciendo clic en SELECT, posteriormente haga clic dos veces en [Default], para poder configurar los parámetros siga la Tabla 1.3. (ver Figuras No. 11 y No. 12)


**Figura No. 11. Configurando parámetros SIP**

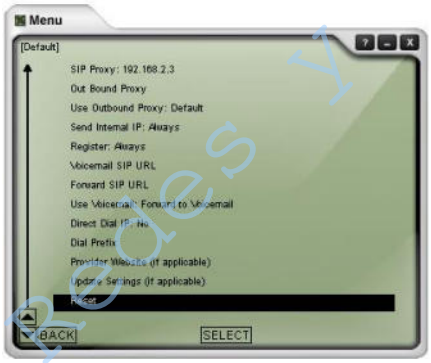



**Figura No. 12. Configurando parámetros SIP1116**

**Tabla 1.3. Valores que deben configurase en el menú SIP Proxy> [Default]**

| Características | Valores |
|---|---|
| **Enabled :** | Yes |
| **Display Name** | Primer nombre + Primer apellido |
| **Username** | Numero de extensión asignado por el administrador |
| **Authorization User** | Numero de extensión asignado por el administrador |
| **Password** | Contraseña registrada como secret en la configuración vía web como Iniciales_numextensión |
| **Domain/Realm** | 192.168.2.122 |
| **SIP Proxy** | 192.168.2.122 |
| **Out Bound Proxy** | Dejar en blanco |
| **Use Out Bound Proxy** | default |
| **Send Internal IP** | Always |
| **Register** | Always |
| **Voicemail SIP URL** | Dejar en blanco |

| | |
|---|---|
| **Forward SIP URL** | Dejar en blanco |
| **Use Voicemail** | Forward to Voicemail |
| **Direct Dial IP** | no |
| **Dial Prefix** | Dejar en blanco |
| **Provider WebSite** | n/a (if applicable) |
| **Update Settings** | n/a (if applicable) |

**4.2.2.11** Haga dos veces clic en BACK, para regresar al menú System Settings.
Como se observa, este menú muestra otras opciones, los parámetros X-Tunnel, X-Cipher e X-Vox son soportados por X-PRO. Los últimos menús Speaker Audio Device, Mic Audio Device y Ring Audio Device se configuran automáticamente durante el ***Audio Tuning Wizard***.

**4.2.2.12** Ahora regrese al Main Menú, haciendo clic en BACK.

**4.2.2.13** A continuación haga clic en la opción Advanced System Setting y seleccione SELECT, posteriormente seleccione SIP Settings, en este punto sólo configurará dos parámetros de acuerdo con la Tabla 1.5, los demás los dejará con los valores predeterminados, haga clic dos veces en BACK y cierre la ventana del menú. (ver Figura No. 13)

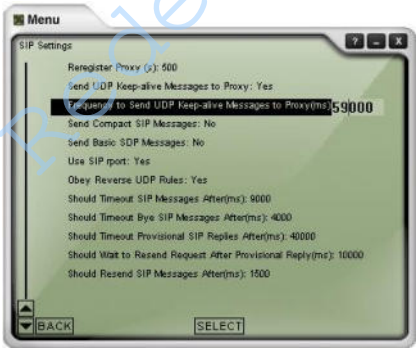



**Figura No. 13 Menú SIP Settings configurado**

**Tabla 1.5. Valores que deben configurase en el menú SIP Settings**

| Características | Valores |
|---|---|
| Reregister Proxy (s) | 500 |
| Frequency to send UDP message... | 59000 |

### 4.3 Estableciendo la llamada

**NOTA: Verifique que el firewall se encuentre desactivado para todas las pruebas con el servidor de VoIP.**

Para poder establecer la llamada deberá seguir los siguientes pasos:

**4.3.1** Elija la línea por la cual desea hacer la llamada, para nuestro primer caso elegiremos la línea 1.

**VI. En la siguiente tabla coloque el número de extensión de todas las máquinas (Tabla 1.6).**

**Tabla 1.6. Asignación para establecer la llamada**

| Nombre | Extensión |
|---|---|
| | |
| | |
| | |
| | |
| | |

| Nombre | Extensión |
|---|---|
| | |
| | |
| | |
| | |
| | |

**4.3.2** Marque el número de la computadora que se le ha asignado de acuerdo con la Tabla 1.6 y complete la tabla.

**NOTA: Pida el número de extensión a su compañero de laboratorio de la máquina que se le asignó y que está ubicado en esa computadora.**

**4.3.3** Haga clic en el botón llamar y converse con la persona.

**VII. ¿Pudo establecer la llamada?, argumente su respuesta.**

_____
_____
_____
_____

**VIII. ¿Por qué línea estableció la llamada?**

_____
_____
_____
_____

**IX. Investigue cuales son los requerimientos para establecer una llamada VoIP.**

_____
_____
_____
_____

Cuelgue haciendo clic en el botón colgar.

**4.3.4** Ahora, vuelva a marcar a cualquier otra extensión por la línea 1, espere a que le contesten y pase a la línea 2, marque al número de extensión que se le asignó en la Tabla 1.6.

**X. ¿Qué ocurrió con la llamada que tiene en la línea 1?**

_____
_____
_____
_____

Acceda a las estadísticas del servidor.

**XI. ¿Qué relevancia tienen para el administrador de redes, contar con esta información?**

_____
_____
_____
_____

**XII. Mencione al menos 5 aplicaciones de la tecnología VoIP.**

_____
_____
_____
_____

### 4.4 Recuperación del ambiente original

Para recuperar los parámetros originales y dejar listo el equipo para el siguiente grupo, realice los siguientes pasos:

**4.4.1** Abra un navegador Web y escriba la dirección 192.168.2.122 en el campo del URL. Se mostrará la página del servidor, haga clic en el menú FreePBX Administration, coloque en los campos de usuario y contraseña, admin como nombre de usuario y admin como contraseña en caso de que se requieran.

**4.4.2** Entrar a Applications->*Extensions*, seleccione la cuenta creada con anterioridad (por ejemplo: "cuenta" <extensión>), ingrese; localice y oprima la opción Delete Extension (Figura 1.5).

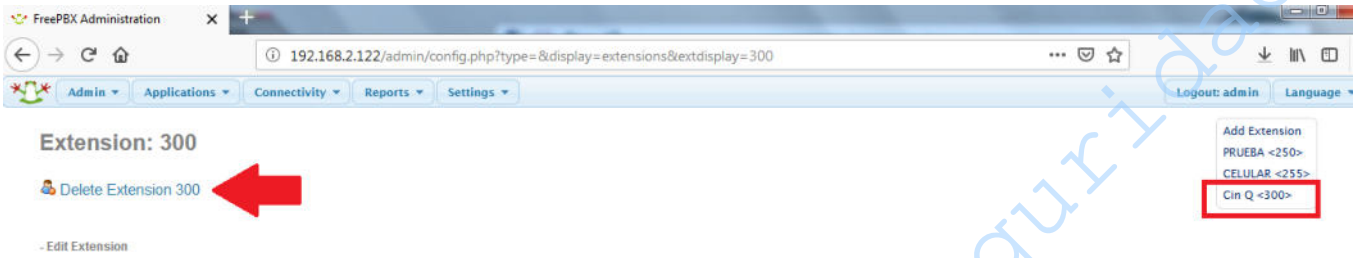



**Figura 1.15. Borrado de cuenta**

### *5. Conclusiones*

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

**PRÁCTICA 6**
**Configuración de VoIP**
***Cuestionario Previo***

1. Defina VoIP
2. Liste las características tradicionales de VoIP
3. ¿En dónde y cuándo es conveniente utilizar VoIP?
4. Describa cómo se lleva a cabo una llamada utilizando la Telefonía Tradicional.
5. ¿Qué es el SS7 y cuál es su función?
6. Describa cómo se lleva a cabo una llamada utilizando VoIP.
7. Describa las características de los siguientes protocolos de señalización: H.323, SIP Y MGCP.
8. Mencione al menos tres funciones de cada uno de los protocolos de trasporte RTP Y RTCP.
9. Investigue en qué consiste Linux CentOS.

# Práctica 7

# Comunicaciones Inalámbricas: red tipo infraestructura

## Integración

## 1. *Objetivos de Aprendizaje*

- El alumno o la alumna configurará una red inalámbrica tipo infraestructura vía Web, habilitará en un router inalámbrico un sistema de filtrado basado en MAC (a veces llamado también filtrado por hardware) que únicamente permitirá el acceso a la red a ciertas tarjetas de red, identificadas con su MAC.
- El alumno o la alumna implementará un mecanismo de seguridad en la red inalámbrica a través de los cifrados WEP y WPA2.

## 2. *Conceptos teóricos*

En sus inicios, las aplicaciones de las redes inalámbricas fueron confinadas a industrias y grandes almacenes. Hoy en día las WLAN (Redes Inalámbricas de Área Local - Wireless Local Area Network) son instaladas en Universidades, oficinas, hogares y hasta en espacios públicos. Las WLAN se componen de computadoras portátiles o de escritorio (terminales) que se conectan a dispositivos fijos llamados AP (Puntos de Acceso - Access Point) vía señales de radio o infrarrojo.

Las estaciones de trabajo se comunican entre sí, gracias a que utilizan la misma banda de frecuencias e internamente tienen instalados el mismo conjunto de protocolos, las redes Wi-Fi utilizan el estándar de comunicaciones IEEE 802.11.

IEEE 802.11 define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando las normas de funcionamiento en una WLAN que emplea ondas de radio en la banda de 2.4 GHz y 5 GHz.

a) Nivel físico, establece dos posibles topologías y tres tipos de medios inalámbricos que funcionan a cuatro velocidades posibles.

   El bloque constructivo fundamental de una LAN inalámbrica es el BSS (Conjunto de Servicios Básicos - Basic Services Set), el cual es un área geográfica en la que las estaciones inalámbricas se pueden comunicar. La configuración y el área BSS dependen del tipo de medio inalámbrico que se use y de la naturaleza del entorno.

El estándar define dos tipos de topologías de red inalámbrica:

- La topología ad hoc, todos los dispositivos de la red dentro de BSS son móviles o portátiles, es decir, inalámbricos, está limitada a un máximo de 10 dispositivos.
- La topología de infraestructura, la cual consta de al menos un AP inalámbrico que puede estar conectado a una red fija estándar por medio de un cable y por dos o más estaciones inalámbricas.

b) Nivel de enlace de datos, el estándar define la funcionalidad del subnivel MAC (Control de Acceso al Medio - Medium Access Control) que consiste en un servicio de transporte no orientado a la conexión que lleva los datos LLC (Control de Enlace Lógico - Logical Link Control)

a un destino de la red en forma de MSDU (Unidades de Datos de Servicio MAC). Este servicio se define por un formato de trama y un mecanismo de control de acceso al medio.
El estándar define tres tipos básicos de trama del nivel MAC:

- Tramas de datos, utilizadas para transmitir datos de los niveles superiores entre estaciones.
- Tramas de control, utilizadas para regular el acceso al medio de la red y para reconocer las tramas de datos transmitidas.
- Tramas de administración, utilizadas para intercambiar información de administración de la red para realizar funciones de red, como asociación y autenticación.

### *3. Equipo y material necesario*

***Equipo del Laboratorio:***

- 2 PC's Pentium con una NIC Ethernet 10/100 Mbps inalámbrica instalada en cada una de ellas.
- 1 Router inalámbrico.

***Equipo del alumno o la alumna:***

- Dispositivo inalámbrico que cuente con Wi-Fi (Laptop con tarjeta inalámbrica, Iphone, etcétera) en el que pueda observarse su dirección MAC).

### *4. Desarrollo*

***Modo de trabajar***

La práctica se desarrollará en parejas.

### *4.4* Red inalámbrica tipo infraestructura

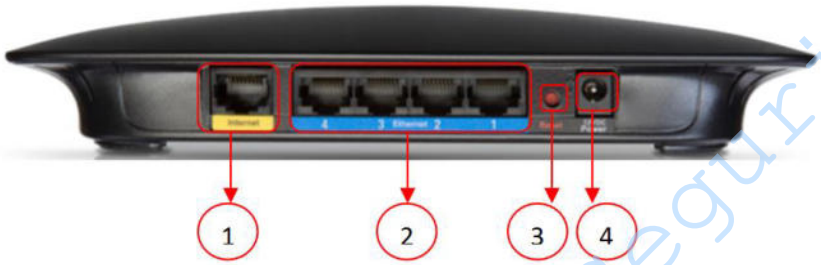
#### *4.4.1* Conociendo el dispositivo inalámbrico

AP (Puntos de Acceso - Access Points) es una estación base utilizada para administrar las comunicaciones entre las distintas terminales, funciona de manera autónoma, sin necesidad de ser conectada directamente a ninguna computadora.

El AP no sólo es el medio de interconexión de todas las terminales inalámbricas, sino que también es el puente de interconexión con la red fija e Internet.

***I. Indique en la tabla 1.1 de la Figura No. 1. los componentes del router inalámbrico que esté utilizando.***

***a)***




***b)***

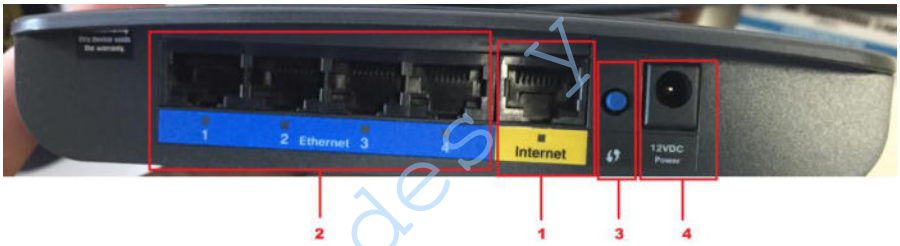



**Figura No. 1. a) Vista trasera del router Linksys WTR120N b) Vista trasera Lynksys E900**

**Tabla 1.1 Componentes**

| | Especificación |
|---|---|
| **1** | |
| **2** | |
| **3** | |
| **4** | |
| **Modelo:** | |

***II. Analice los indicadores de luz del router inalámbrico que esté utilizando y complete, de ser posible, la tabla 1.2 de la Figura No. 2.***


**Figura No. 2. Vista delantera del router Linksys WTR120N**

**Tabla 1.2 Indicadores de luz del router Linksys WTR120N**

| | Especificación |
|---|---|
| **1** | |
| **2** | |
| **3** | |
| **4** | |
| **5** | |

**Conexión y configuración del router inalámbrico.**

***4.4.2*** Realice las conexiones físicas, conecte el host de administración con el router utilizando un puerto Ethernet (Ver Figura No. 3).

**Figura No. 3. Conexión punto a punto**

En este punto de la práctica realizará la configuración vía Web, este método resulta intuitivo y gráfico para la administración del dispositivo.

***4.4.3*** Abra un navegador Web y escriba la dirección IP 192.168.1.1 en el campo del URL (ver Figura 1.4).

**NOTA**: En caso de que el modelo del router sea **Lynksys E900** siga los siguientes pasos (del 4.4.3.1 al 4.4.3.3)

***4.4.3.1*** En caso de ser necesario, instale el software que viene incluido en el CD.

***4.4.3.2*** Dé clic sobre la opción *Continuar con una red abierta y no segura* para iniciar la instalación (Figura No. 4).


**Figura No. 4 Inicio de la instalación**

***4.4.3.3*** Habilite la opción *Entiendo que mi red está actualmente abierta y no es segura* para continuar con la instalación (Figura No. 5).

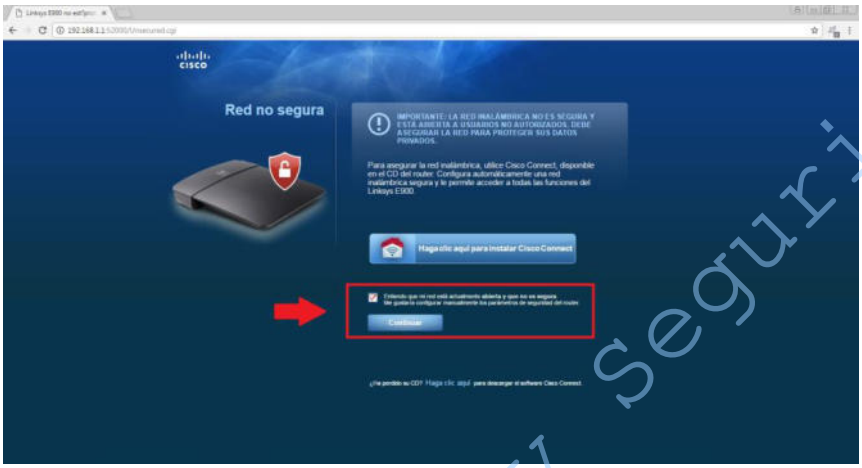



**Figura No. 5. Continuar con la instalación**

***4.4.4*** Independientemente del modelo, coloque como nombre de usuario: admin y contraseña: admin (Figura No. 6).

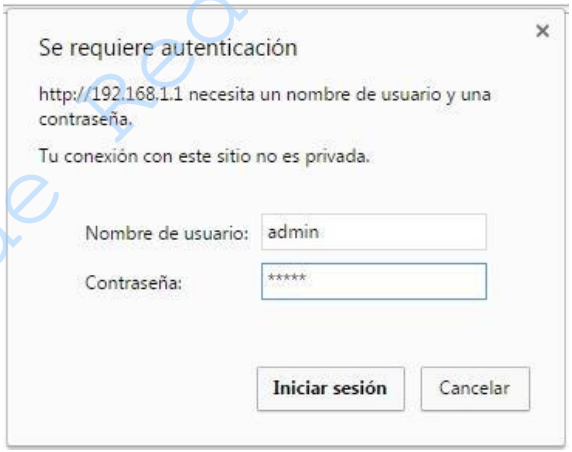



**Figura No. 6. Solicitud de usuario y contraseña**

**NOTA: Dependiendo del modelo puede salir alguna ventana de Advertencia, solamente ciérrela y continúe con la configuración.**

***4.4.5*** Se abrirá una ventana con las configuraciones por default del dispositivo, navegue por las opciones que se presentan para configurarlo y administrarlo correctamente (Figura No. 7).

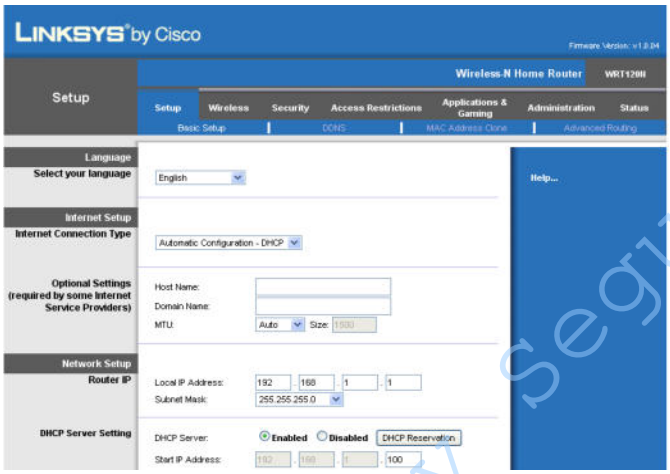



**Figura No. 7. Ventana de Setup (Configuración) del router inalámbrico.**

***4.4.6*** En la parte superior se muestran las opciones que presenta la configuración vía Web del dispositivo, ingrese en cada una de ellas y verifique qué se puede configurar, resumiendo en la Tabla 1.3 las características generales.

**Tabla 1.3. Características Generales de la configuración del router inalámbrico**

| Opción | Características Generales |
|---|---|
| Setup (Configuración) | |
| Wireless (inalámbrico) | |
| Security (Seguridad) | |
| Access Restrictions | |
| Applications & Gaming (Aplicaciones y Juegos) | |
| Administration (Administración) | |
| Status (Estado) | |

**NOTA: Deje en blanco la opción Access Restrictions si el modelo del router empleado es E900**

***I. ¿Qué pasa si el access point tiene una dirección IP fuera del segmento de red del laboratorio?***

_____
_____
_____
_____
_____

***4.4.7*** El siguiente paso es configurar los parámetros de red necesarios, haga clic en el menú *Setup→Basic Setup* (Configuración→ *Configuración básica)* y en la sección de Internet Setup

(Configuración de Internet) del menú despegable seleccione Static IP (IP Estática); observe que cambian las opciones.

***4.4.8*** Coloque los parámetros de red solicitados de acuerdo con la Tabla 1.4.

**Tabla 1.4. Parámetros de red de la sección Internet Setup**

| Nombre | Valor |
|---|---|
| Internet IP Address (Dirección IP de Internet) | 192.168.2.X |
| Subnet Mask (Máscara de subred) | 255.255.255.0 |
| Default Gateway (Puerta de enlace predeterminada) | 192.168.2.254 |
| DNS 1 | 132.248.204.1 |
| DNS 2 | 132.248.10.2 |

**NOTA: X se sustituye por la IP de su máquina+200.**
**Por ejemplo: si su máquina es 192.168.2.1 colocará 192.168.2.201**

***4.4.9*** En la sección Optional Settings (Parámetros opcionales) colóquele al dispositivo el nombre **Linksys_susIniciales**.

**NOTA:** susIniciales serán cambiadas por las iniciales de los integrantes del equipo.

***4.4.10*** A continuación en la sección Network *Setup → Router IP (Configuración de red → Dirección IP del router)*, coloque los parámetros indicados en la Tabla 1.5.

**Tabla 1.5. Parámetros de red de la sección Network Setup (Configuración de red)**

| Nombre | Valor |
|---|---|
| IP Address (Dirección IP) | 192.168.3.1 |
| Subnet Mask (Máscara de subred) | 255.255.255.0 |

***4.4.11*** El siguiente paso será configurar el DHCP del dispositivo, para que se asignen de forma automática los parámetros de red a los dispositivos finales inalámbricos; para ello vaya *a*

*Network Setup → DHCP Server Settings (Configuración de red → Parámetro de servidor DHCP)* y coloque los parámetros que se muestran en la tabla 1.6.

***4.4.12*** Guarde los cambios efectuados en el dispositivo haciendo clic en el botón Save Settings (Guardar parámetros).

**Tabla 1.6. Parámetros de red del DHCP Server Settings (Parámetro de servidor DHCP)**

| Nombre | Valor |
|---|---|
| DHCP Server (Servidor DHCP) | Enable |
| Start IP Address (Dirección IP inicial) | 192.168.3.100 |
| Maximum Numbers of Users (Número máximo de usuarios) | 50 |
| Cliente Lease Time (Tiempo de concesión del cliente) | 10 |
| Static DNS 1 (DNS estático 1) | 132.248.204.1 |
| Static DNS 2 (DNS estático 2) | 132.248.10.2 |

***4.4.13*** Vaya a la sección *Time Settings → Time Zona* (Parámetros de hora → *Zona horaria*) y elija del menú despegable la zona horaria.

***4.4.14*** Guarde los cambios efectuados en el dispositivo haciendo clic en el botón Save Settings (Guardar parámetros)..

La IP que se asignó anteriormente permitirá administrar el dispositivo, por lo cual será necesario cambiar la IP del host que está administrado por una que se encuentre contenida en el rango definido.

***4.4.15*** Realice las siguientes configuraciones físicas, conecte el puerto de Internet del router a un nodo disponible del laboratorio (el nodo está conectado a un puerto del switch).

***4.4.16*** El siguiente paso es realizar la configuración de los dispositivos inalámbricos disponibles, verifique que las tarjetas de red inalámbricas usan asignación de los parámetros de red a través de un servidor DHCP.

***4.4.17*** Con base en lo investigado en el previo, cambie el SSID del router que está configurando.

Anote el nuevo SSID_____

***4.4.18*** A continuación conéctese a la red inalámbrica con el SSID del punto 4.1.16

Hasta este punto se realizó la configuración del router, pero tiene una gran desventaja; cualquier usuario se puede conectar a la red; así que el siguiente paso será configurar la seguridad en el dispositivo.

### *4.5* Cifrado por WEP

WEP (Privacidad Equivalente a Cableado - Wired Equivalent Privacy), es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Está basado en el algoritmo de cifrado RC4 y utiliza claves de 64 bits o de 128 bits. Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.

Para configurar el cifrado por WEP en el router inalámbrico realizará los siguientes pasos:

***4.5.1*** Haga clic en el menú de *Wireless* → *Wireless Security (Inalámbrico* → *Seguridad Inalámbrica)*.

***4.5.2*** Habilite el modo de seguridad en WEP.

***4.5.3*** Con base en la tabla 1.7 llene los campos indicados, cuando coloque la frase haga clic en el botón Generate.

**Tabla 1.7. Parámetros de seguridad.**

| **Nombre** | **Valor** |
|---|---|
| Security Mode (Modo de seguridad) | WEP |
| Encrytion (Encriptación) | 40/64 bits |
| Passphrase (Frase de paso) | *Seguridad* |

***4.5.4*** Se ha generado la clave WEP, tome nota de la clave para configurar posteriormente el dispositivo inalámbrico.

Clave Wireless:_____

***4.5.5*** El siguiente paso es realizar la conexión a la red inalámbrica creada.

***4.5.6*** Realice la configuración pertinente en su dispositivo inalámbrico para conectarse a la red inalámbrica creada usando la clave WEP.

***4.5.7*** Verifique que tenga conexión a la red inalámbrica.

El router inalámbrico cuenta con otros dos tipos de cifrado, WPA-Personal y WPA-Enterprise.

***II. ¿Qué es el cifrado WPA, WPA-Personal y WPA-Enterprise?***

_____
_____
_____

***III. ¿Qué es el cifrado TKIP?***

_____
_____
_____

***IV. Explique en qué consiste el cifrado AES***

_____
_____
_____

***4.5.8*** Realice la configuración pertinente en su dispositivo inalámbrico para conectarse a la red inalámbrica usando la clave WPA2-Personal.

***4.5.9*** Seleccione la opción WPA2-Enterprise y observe que este método ofrece utilizar RADIUS server.

***V. ¿Qué es y para qué sirve RADIUS?***

_____
_____
_____

***VI. Realice un diagrama lógico de la red inalámbrica, indicando los dispositivos inalámbricos involucrados, puertos, IP asignadas.***

### *4.6* Filtrado por MAC

En la mayoría de los casos no es necesario conocer o utilizar la dirección física del adaptador de red, ya que no es indispensable para configurar la conexión a Internet, ni para montar la red.

El caso más usual en el que se puede necesitar el dato de la dirección MAC, es en el que se desea configurar una red WiFi, el punto de acceso en el sistema de configuración tiene la opción de filtrado basado en MAC (a veces llamado también filtrado por hardware) el cual únicamente permitirá o denegará el acceso a la red a adaptadores de red concretos, identificados con su MAC. Todos los adaptadores de red inalámbricos tienen una dirección MAC única.

Es muy recomendable utilizar el filtrado por MAC en combinación con el cifrado WEP o WPA para tener una mayor seguridad.

La MAC address es un número único asignado a cada tarjeta de red es también conocida como la dirección física.

***VII. ¿Qué comando se puede utilizar para determinar la dirección MAC de la tarjeta en Windows y en Linux?***

Windows _____

Linux _____

Para configurar el filtrado por MAC, en el router inalámbrico realizará los siguientes pasos:

***4.6.1*** Obtenga la dirección MAC del dispositivo inalámbrico

***4.6.2*** Anote la dirección MAC del dispositivo inalámbrico.

**Dirección MAC** _____

***4.6.3*** Vaya al menú de *Wireless* → *Wireless MAC Filter (Inalámbrico* → *Filtro de MAC inalámbrico)*.

***4.6.4*** De la sección Wireless MAC Filter (*Filtro de MAC inalámbrico*) seleccione Enable (Activado) para filtrar por MAC a los dispositivos inalámbricos.

***4.6.5*** La opción ***Prevent listed computers from accessing the wireless network (Evitar que los siguientes PC accedan a la red inalámbrica)*** bloqueará el acceso inalámbrico por dirección MAC.

***4.6.6*** La opción ***Permit listed computers to access the wireless network (Permitir que los siguientes PC accedan a la red inalámbrica)*** permitirá el acceso inalámbrico por dirección MAC, haga clic en esta opción.

***4.6.7*** Haga clic en la opción Wireless Client List (Lista de clientes inalámbricos), se desplegará una ventana con las direcciones MAC de los dispositivos conectados a la red

***4.6.8*** Haga clic en el botón ***Save settings*** (Guardar parámetros) para guardar la nueva configuración.

***4.6.9*** Realice la configuración pertinente en su dispositivo inalámbrico para conectarse a la red inalámbrica.

***4.6.10*** Verifique que tenga conexión a la red inalámbrica.

***VIII. ¿En qué casos es útil filtrar por MAC?***

_____
_____
_____
_____
_____

***IX. Si filtramos únicamente por MAC, ¿está la red completamente segura? Justifique su respuesta.***

_____
_____
_____
_____
_____
_____

***X. ¿En qué casos es preferible tener una red inalámbrica tipo infraestructura?***

_____
_____
_____
_____
_____
_____

### *4.7* Restauración de la configuración

***4.7.1*** Restaure la SSID del router inalámbrico. Dé clic en el botón de Reset

### *5. Conclusiones*

Revise los objetivos de la práctica y las actividades realizadas y emita sus conclusiones.

_____
_____
_____
_____
_____
_____
_____
_____
_____

**PRÁCTICA 7**

**Comunicaciones Inalámbricas: red tipo infraestructura**

***Cuestionario Previo***

1. ¿Qué es una red inalámbrica?
2. Liste las características de las ondas de radio como medio de transmisión
3. Liste las características del infrarrojo como medio de transmisión
4. ¿A qué se refiere el estándar IEEE 802.11?
5. ¿Cuáles son las topologías que admite el estándar 802.11?
6. Investigue las características de los estándares 802.11a, 802.11b, 802.11g y 802.11n; indicando frecuencia, ancho de banda, velocidad de transmisión, alcance, método de acceso.
7. ¿Qué es la certificación Wi-Fi?
8. ¿Qué significa SSID?
9. ¿A qué se refiere el estándar IEEE 802.16?
10. Investiga las características de la tecnología GSM.
11. ¿Qué tipos de seguridad se pueden manejar en un router inalámbrico?
12. ¿Cuál es el significado de un punto de acceso (AP) en redes inalámbricas?
13. Investigue cómo se cambia el SSID (Nombre de la red o Network Name) en los routers Linksys WTR120N y Linksys E900

# Práctica 8

# Manejo de conflictos en el área de redes

## Dirección

### 1. *Objetivos de Aprendizaje*

- El alumno o la alumna definirá el concepto de conflicto, identificando las razones que lo provocan y la forma en que las personas lo manejan. De la misma manera reconocerá técnicas para la evasión y resolución de conflictos.

- El alumno o la alumna aplicará estrategias de supervisión, que minimicen el conflicto y mejoren las relaciones humanas que favorecen el buen funcionamiento del área.

### 2. *Conceptos teóricos*

En 1923 el investigador Charles E. Mayo, completó un estudio en el que se respalda la tesis que sostiene que el trabajo individual no es el que genera los mejores frutos, pues el ser humano requiere de satisfacciones en la labor que desarrolla tanto individual como grupalmente.

En el mundo tecnológico en que nos desenvolvemos las cosas deben ser administradas para obtener los objetivos propuestos.

El conflicto se inicia cuando individuos o grupos no obtienen lo que necesitan, buscando su interés propio. Los conflictos son inevitables, se desarrollan al entrar en contacto con personas, trabajos y el individuo mismo. Sin embargo, deben minimizarse y resolverse a través de estrategias.

El conflicto se considera destructivo cuando controla toda la atención, divide a las personas y reduce la cooperación, aumenta las diferencias para finalmente conducir a un comportamiento destructivo.

El conflicto se puede considerar constructivo cuando da lugar a la clarificación de problemas y controversias, generando soluciones basadas en una comunicación auténtica que permite desarrollar entendimiento y destrezas.

### 3. *Equipo y material necesario*

### 4. *Desarrollo*

***Modo de trabajar***

La práctica se desarrollará en parejas.

***4.1*** **Manejo de conflictos**

Analice el siguiente caso real, dentro del área de administración de redes en una organización proveedora de servicios de tecnología de información.

*Eric Humbolt, administrador del área de redes, en una organización dedicada a proveer servicios de telecomunicaciones, dedica su tiempo intentando que su equipo de trabajo sea capaz de desenvolverse en las reuniones de trabajo, sin que la tensión alcance límites insoportables, con el objetivo de contar con un equipo conjuntado con una persona proveniente de cada división y desarrollar un plan integral, que tenga como meta, el realineamiento estratégico de la empresa, su puesta en marcha y buen funcionamiento en un lapso de 6 meses.*

*Seis de los altos directivos involucrados parecían estar decididos a dar un cambio drástico a la empresa, pero el séptimo daba la sensación de estar igualmente determinado a sabotear el proceso. Ya habían tenido lugar 3 reuniones y Eric no había conseguido que todos los participantes se pusieran de acuerdo en los asuntos tratados.*

*Randy Louderback, administrador de bases de datos, regularmente dominaba la discusión del grupo o bien pasaba de todo y empezaba a tamborilear con su pluma sobre la mesa en señal de aburrimiento. Este individuo que sometía al grupo con su personalidad y fuerte relación con el gerente general de la empresa, era capaz de retener información vital para el debate en el grupo y en otras ocasiones intervenía para denigrar fríamente las opiniones de cualquiera de los presentes. En la primera reunión realizada hacía un mes, insinuó lo que en ese momento pareció un chiste, que él no estaba hecho para trabajar en equipo con otros, a través del siguiente comentario: "los líderes, dirigen; los gregarios…bueno mejor callémonos", mientras lo pronunciaba esbozando una sonrisa plena de encanto y el resto del grupo había reído a carcajadas por la gracia.*

*La empresa tenía problemas, no muy graves, pero sí lo bastante como para requerir por parte del área de dirección un reposicionamiento estratégico.*

*Eric preparó una estructura y directrices para los debates en grupo, las discrepancias y la toma de decisiones con la intención de proponérselas al grupo de directivos para que realizaran su aportación antes de empezar a trabajar juntos. En un principio previó ciertas discrepancias con algunos directivos, temores que resultaron infundados. A pesar de sus planificaciones, siempre hubo quien desbarató el proceso.*

*La tercera reunión, que había tenido lugar la semana anterior, terminó en un caos completo. Se había decidido presentar una serie de propuestas por cada uno de los directivos, exposición que se desarrolló sin problemas hasta que tocó el turno a Randy, nuestro integrante conflictivo.*

*Finalmente, en la cuarta reunión todo el equipo estaba dentro de la sala, excepto Randy. Después de 10 minutos de conversaciones superficiales, Eric podía observar en cada una de las caras, la frustración reflejada en todos ellos, así que decidió que el tema de esa reunión sería la conducta de Randy para tratarlo abiertamente y tomar una decisión. Sin embargo, justo en el momento en que empezaba, éste entró pausadamente en la sala sonriendo y diciendo: "Lo siento, chicos", mientras sostenía una taza de café, como si ésta fuese la explicación suficiente para justificar su retraso. Eric, afirmó: "Randy, me alegro de que estés aquí, porque pienso que hoy debemos hablar del grupo". Randy interrumpió e hizo un comentario sarcástico que provocó la salida de más de un integrante del equipo, la sala de juntas entonces quedó en silencio.*

1. ***Identifique la fuente del conflicto.***

_____

_____

_____

2. ***Investigue las consecuencias en una organización causadas por un conflicto como el anterior.***

_____
_____
_____

3. ***Enumere al menos 5 actitudes de una persona conflictiva.***

_____
_____
_____

Existen algunas técnicas para evadir o resolver conflictos, las cuales implican los siguientes pasos:

- Reconocimiento del conflicto.
- Establecimiento de metas.
- Establecimiento de comunicación frecuente.
- Comunicaciones de preocupaciones.
- Espíritu creativo.
- Discusión de las diferencias abiertamente.

Entre algunos puntos claves que deben considerarse a la hora de resolver conflictos encontramos:

- Se debe negociar antes de cerrar el trato.
- No se debe ser intransigente: ser justo, ofrecer más respeto por la parte opositora que por lo que se está negociando.
- No negociar en estado de ira.
- Nunca pensar que una negociación es insignificante.
- La técnica de la negociación debe llevar a un acuerdo inteligente, no a la confrontación.
- Una negociación efectiva no debe dejar resentimientos.
- Debe ser perdurable.
- En la negociación se debe privilegiar el bien común, dejando de lado el ego.

4. ***Investigue al menos 3 razones que den lugar a los conflictos.***

_____
_____
_____

5. ***¿Por qué no funciona este equipo de trabajo? Analice su respuesta y discuta en grupos de 3 personas, las coincidencias y diferencias.***

_____
_____
_____

### *4.2 Casos prácticos de liderazgo*

El objetivo de este punto es analizar los tipos de liderazgos empleados por 2 personajes de la industria informática.
Examine los siguientes casos reales de dos personajes que han dado lugar a dos fuertes empresas informáticas: Apple y Microsoft. Posteriormente responda las preguntas.
Dos hombres han dirigido la revolución de las computadoras personales. Sin embargo, la forma en que cada uno de estos hombres enfrentó su propia búsqueda ha sido distinta. Steve Jobs y Bill Gates han cambiado la forma en la que el mundo hace negocios, pero la historia de sus liderazgos requiere ser estudiada.

#### *4.2.1 Bill* Gates

*Bill Gates empezó a desarrollar sus habilidades relativas a las computadoras con su amigo de la infancia, Paul Allen, en Lakeside School, Seatle. A los 14 años, los dos constituyeron su primera compañía de computadoras. Al terminar la preparatoria Allen y Gates partieron hacia Boston.*
*Gates fue aceptado en Harvard y Allen empezó a trabajar en Honeywell. Después de pasar solamente dos años en Harvard, Gates y Allen abandonaron Boston, para desarrollar en Albuquerque un lenguaje de computadora que sirviera a la nueva computadora personal Altair 8080. Este lenguaje se convertiría en BASIC, cimiento de Microsoft, la cual fue creada como una sociedad en 1975.*
*Después de 5 años en Nuevo México, Microsoft fue trasladada a Bellevue, Washington, en 1980, con BASIC y otros dos lenguajes de programación (COBOL y FORTRAN) en su arsenal. Posteriormente en ese mismo año IBM empezó a desarrollar su primera PC y tuvo necesidad de un sistema operativo. Microsoft desarrolló el MS-DOS (Microsoft Disk Operating System) para IBM, mientras otras compañías creaban sistemas que competirían con Microsoft. La determinación y persuasión de Gates, en relación con el desarrollo de programas para MS-DOS, hizo de este sistema operativo la plataforma estándar de IBM.*
*Conforme Microsoft se volvió más exitoso Gates se dio cuenta de que necesitaba ayuda para su administración. Su entusiasmo, visión y trabajo arduo fueron la fuerza motriz detrás del crecimiento de la compañía, pero él reconoció la necesidad de una administración profesional. Gates introdujo a otro de sus amigos de Harvard, Steve Ballmer, quien había trabajado para Procter & Gamble después de graduarse de Harvard y en ese entonces cursaba la maestría de Administración de Empresas en Standford. La persuasión de Gates logró que Ballmer abandonara la escuela y se uniera a Microsoft. A lo largo de los años Ballmer se convirtió en un activo indispensable tanto para Gates como para Microsoft.*
*En 1983 Gates siguió mostrando su inteligencia, al contratar a Jon Shriley, quien ordenó y modernizó la estructura de la organización, mientras Ballmer servía como consejero y portavoz de Gates. Microsoft continuó creciendo y prosperando en los 90, convirtiendo a Gates en el hombre más rico del mundo.*
*Microsoft domina tanto el mercado del sistema operativo, con su aplicación Windows, como el mercado del software de oficina, Microsoft Office.*
*Gates reconoció que su papel era ser el visionario de la compañía y que necesitaba administradores profesionales para dirigirla. Gates combinó su determinación y pasión inexorables con un equipo administrativo bien estructurado para hacer de Microsoft el gigante que el día de hoy es.*

*Microsoft adquirió Hotmail en 1998 y a pesar de ser visto como algo pasado de moda por los usuarios más jóvenes, fue el servicio de correo electrónico gratuito más popular del mundo hasta 2012, cuando fue superado por Gmail.*

*En mayo de 2011 Microsoft realizó la compra de Skype, un firma que en el 2003 creara en Luxemburgo, un software que permite hacer llamadas de voz y video, entre usuarios de Internet, para sustituir a Windows Live Messenger, el cual dejó de funcionar en 2013.*

*De lo que nadie duda es que hoy Microsoft no sólo es una de las empresas más valiosas en bolsa sino que tiene muchos negocios y productos. Participa en la MSNBC, el tercer canal de televisión por cable de EE UU, que además tiene una web del mismo nombre. Y, por si fuera poco, ha lanzado productos de entretenimiento, como la XBOX; programas para móviles y palms, como el Windows Mobile, y promete seguir pensando en el futuro.*

### *4.2.2* Steve Jobs

*El otro visionario, Steve Jobs y su amigo Steve Wosniak iniciaron en 1976 Apple Computer, en el garage de Jobs, en Los Altos, California. En contraste con Bill Gates, Jobs y Wosniak eran expertos en hardware e iniciaron una visión para una computadora personal que fuera económica y fácil de utilizar.*
*Cuando Microsoft ofreció BASIC a Apple, Jobs inmediatamente descartó la idea afirmando que él y Wosniak crearían su propia versión de BASIC en un fin de semana. Éste era el perfil típico de Jobs: firme y casi maníaco, en ocasiones.*
*Finalmente Jobs aceptó BASIC de Microsoft, mientras trataba de consolidar su propia visión, es decir, el desarrollo de una interfaz más amigable y fácil de utilizar para una PC.*
*Muchos ven a Jobs como el anti-Gates. Jobs es un precursor y creador, en contraste con Gates, quien es más un individuo con el potencial de consolidar parámetros industriales.*
*El objetivo de Jobs era cambiar al mundo con sus computadoras. Por otra parte era muy exigente con sus empleados. Jobs era distinto a Gates, Allen y Wosniak. No era un programador de computadoras dotado sino la persona que vendía la idea de la computadora personal al público. Jobs tomó la decisión de cambiar la dirección de Apple para desarrollar Macintosh utilizando una GUI (Interfaz Gráfica de Usuario - Graphic Interface User) que introdujo al mundo el ratón y los iconos en pantalla. Jobs forzó a la gente a escoger entre el sistema operativo Microsoft-IBM Dos y su GUI Macintosh OS.*
*En un principio Jobs fue el visionario que cambió el mundo de las computadoras y Apple empequeñeció a Microsoft. Con todo este éxito, había un problema mayor gestándose en Apple: Steve Jobs tenía una confianza excesiva y no vio que Gates y Microsoft constituían una seria amenaza para Apple.*
*Poco tiempo después de la aparición de la computadora Macintosh, Jobs pidió a Microsoft desarrollar un software para el sistema operativo Mac. Gates así lo hizo y procedió a lanzar un proyecto que copiara y mejorara la interfaz del usuario Apple. El resultado de esta empresa fue la aplicación Windows de Microsoft.*
*La actitud arrogante de Jobs, así como su carencia de habilidades administrativas, lo convirtió en una amenaza para el éxito de Apple. Nunca se preocupó por desarrollar presupuestos y se ha criticado su relación con los empleados. Wosniak abandonó Apple después de la aparición de Macintosh debido a las diferencias con Jobs.*

*En 1985, John Scully, director general de Pepsi Cola sustituyó a Steve Jobs como presidente y director general de Apple Computer.*
*La década de los 90 vio a Microsoft y Apple tomar muy distintas direcciones. Microsoft se convirtió en una de las compañías más lucrativas del mundo. Jobs fundó NEXT, una empresa fabricante de computadoras y PIXAR, la empresa de animación que ha producido Toy Story y A Bug's Life.*
*Jobs cambió el modelo de negocio de la industria musical: aprobó el lanzamiento del iPod en 2001 y en 2003 iTunes, que en siete años vendió más de 10 000 millones de canciones y dominó completamente el negocio de música en línea. En 2009 acaparó el 25 por ciento de la venta de música en los Estados Unidos y es la mayor tienda musical por volumen de ventas de la historia. Según el registro de patentes de los Estados Unidos, 317 patentes de Jobs figuran a nombre de Apple. Otra de sus aportaciones fue el iPhone, el cual se puso a la venta en el mercado estadounidense el 29 de junio de 2007.*
*En el año de su muerte, su fortuna se valoraba en 8300 millones de dólares y ocupaba el puesto 110 en la lista de grandes fortunas de la revista* Forbes*.*

### *4.2.3 Microsoft y Apple, al final del siglo*

*Apple tomó una dirección opuesta, el anticuado sistema operativo y la caída en la participación del mercado condujeron a una disminución del desarrollo para el software en Mac. En 1998 Jobs regresó a Apple, como director general interino. Su visión, una vez más resultó en la innovadora iMac. El diseño era clásico de Jobs. Desarrolló una computadora simple, elegante y compatible con Internet para agregar algo de emoción al mercado de las computadoras. Jobs también cambió como administrador y líder. Maduró y solicitó a su grupo de asesores profesionales consejos e ideas. Aunque fue el director general interino, Jobs vendió todas menos una de sus acciones. Larry Ellison, director general de Oracle y miembro de la junta directiva de Apple, atribuye a Jobs, en cuanto a la dirección de Apple, el siguiente hecho:*
*"Si bien posee sólo una acción de Apple, Jobs claramente es dueño del producto y la idea de la compañía. Mac es una expresión de su creatividad y Apple, como un todo, es una expresión de Steve. Ésta es la razón por la que a pesar de la palabra interino en su título, permanecerá en Apple durante largo tiempo."*
*El 24 de agosto de 2011 Jobs presentó su renuncia como CEO de Apple, y fue sustituido por Tim Cook. A partir de esta fecha y hasta su muerte, fue el presidente de la Junta Directiva de Apple. Jobs presentó públicamente el iPad 2, sin embargo, desde su residencia seguiría ocupándose de las decisiones más relevantes de la compañía. Tras su muerte, el Apple Watch, el primer smartwatch creado por Apple, fue presentado el 9 de septiembre de 2014 por Tim Cook.*
*Con el éxito del sistema operativo Windows, la serie de aplicaciones Office y el software Internet Explorer, Microsoft se ha convertido en una palabra familiar. Bill Gates ha sido aclamado como genio de los negocios.*
*Seguido del lanzamiento de los teléfonos inteligentes con sistema operativo Windows, Microsoft se enfocó en un cambio de imagen de sus productos desde el 2011 al 2012; el logo de la compañía, productos, servicios y el sitio web de Microsoft adoptaron el concepto del diseño Metro. En junio de 2011 en la conferencia anual de Taiwán Computex Microsoft mostró al público su nueva versión de Windows, un sistema operativo diseñado para computadores de escritorio, portátiles y tabletas. Una versión para desarrolladores (Developer Preview) fue lanzada en septiembre 13 del mismo año y el 31 de mayo de 2012 fue lanzada la versión de prueba.*

*En este año Microsoft, con ayuda de usuarios avanzados llamados Insiders, lanzaron la última versión de su línea de sistemas operativos. Esta versión se llama Windows 10, que según Microsoft es la mejor versión desarrollada.*
*El hecho de que los competidores de Microsoft, la prensa y el Departamento de Justicia de Estados Unidos hayan llamado a Microsoft un monopolio, refuerza la determinación de éxito en Gates.*

6. ***¿Cómo difieren Bill Gates y Steve Jobs en su estilo de liderazgo?***

_____
_____
_____

7. ***Compare y contraste las prácticas administrativas de Gates y Jobs.***

_____
_____
_____

8. ***¿Cuál es su opinión sobre el futuro de Microsoft y Apple Computers?***

_____
_____
_____

9. ***Para usted, ¿cuál es la esencia del liderazgo?***

_____
_____
_____

10. ***Si usted fuera elegido para ser líder de grupo en un proyecto de clase, ¿qué conducta adoptaría con aquellos elementos conflictivos del grupo? ¿por qué?***

_____
_____
_____

11. ***Haga una interpretación del siguiente párrafo y dé un ejemplo práctico de su aplicación:***

"En una organización no se puede gobernar a los hombres, sino dirigir hacia unos objetivos a hombres que se gobiernan a sí mismos."
Stephan Cambien

_____
_____
_____

***4.2.4 El profesor o la profesora realizará diversas actividades para que en equipos identifiquen los conflictos que se presentan en ciertas situaciones y la mejor forma de solucionarlos. Cada equipo deberá anexar a esta práctica las hojas con sus resoluciones.***

***5. Conclusiones***

Revise los objetivos de la práctica y las actividades realizadas y emita sus conclusiones.

_____
_____
_____
_____
_____
_____
_____
_____

**PRÁCTICA 8**

**Manejo de conflictos en el área de redes**

***Cuestionario Previo***

1. ¿Qué es un proceso administrativo?
2. ¿Cuáles son las cinco etapas del proceso administrativo?
3. ¿Cuáles son las habilidades directivas del administrador de redes?
4. Defina el concepto de conflicto e investigue al menos 5 tipos de conflictos en el ámbito laboral.
5. Defina el conflicto funcional
6. Defina el conflicto disfuncional

# Práctica 9

# Ruptura de claves WEP y WPA2-Personal

## Control

## *1.- Objetivos de Aprendizaje*

- El alumno o la alumna realizará un ataque informático explotando las vulnerabilidades de los cifrados WEP y WPA2 para obtener sus respectivas claves.
- El alumno o la alumna conocerá la importancia de la asignación de claves robustas en los dispositivos (Access Points) para incrementar la seguridad de éstos.

## *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, lo que cual no implica que sea el 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.

El cifrado **WEP** es poco segura ya que es abierta y cualquiera puede tener acceso a la clave del Wi-Fi, que se está utilizando.

El cifrado **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.

El cifrado más 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 interfaz 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*

***Equipo del Laboratorio:***

- Routers inalámbricos Linksys E900

***Equipo del alumno o la alumna:***

- Memoria USB booteable con sistema operativo Kali Linux, el profesor o la profesora definirá la versión.
- Archivo electrónico de un diccionario para realizar un ataque de fuerza bruta (El archivo de Diccionario en Español puede descargarlo desde la misma ubicación que la práctica).

### *4.- Desarrollo:*

***Modo de trabajar***

Esta práctica se realizará por parejas

**NOTA:** Las actividades en este apartado serán meramente demostrativas haciendo uso de un video como base y las explicaciones del profesor o profesora cuando la sesión de la clase se realice en modalidad a distancia.

### 4.1 Cifrado WEP

**NOTA PARA EL PROFESOR O LA PROFESORA**

**Abra un navegador Web y escriba la dirección IP 192.168.1.1 en el campo del URL (ver Figura No. 1).**

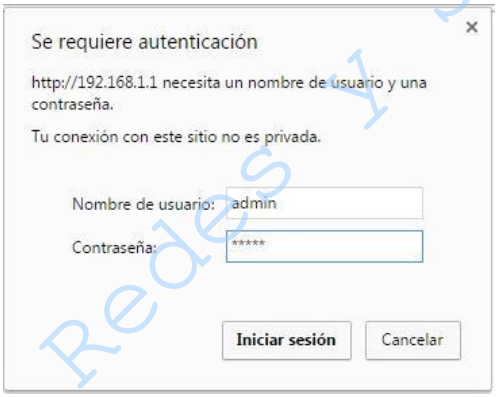



**Figura No. 1. Solicitud de usuario y contraseña**

**Coloque como nombre de usuario: admin y contraseña: admin.**

**4.1.1** Haga clic en el menú de Wireless → Wireless Security.

**4.1.2** Coloque en Network Name (SSID) el nombre que prefiera para identificar al dispositivo.

**4.1.3** En la opción *Wireless* → *Wireless Security* habilite el modo de seguridad en WEP.

**4.1.4** Con base en la tabla 1.1 llene los campos indicados, cuando coloque la frase haga clic en el botón Generate.

**Tabla 1.1. Parámetros de seguridad.**

| Nombre | Valor |
|---|---|
| Security Mode | WEP |
| Encrytion | 40/64 bits |
| Passphrase | |

**NOTA 1: En Passphrase coloque una palabra clave que se encuentre contenida en el diccionario.**

**NOTA 2: Recuerde generar tráfico en la red.**

### 4.2 Realizando el ataque del cifrado WEP

**4.2.1** Abra una terminal de Kali, verifique que la interfaz de red inalámbrica sea wlan0. Tal como se muestra en la figura No. 2. Para ello teclee el siguiente comando

**NOTA: Para realizar la práctica exitosamente debe tener instalado el paquete ifconfig.**

**root@kali# ifconfig**

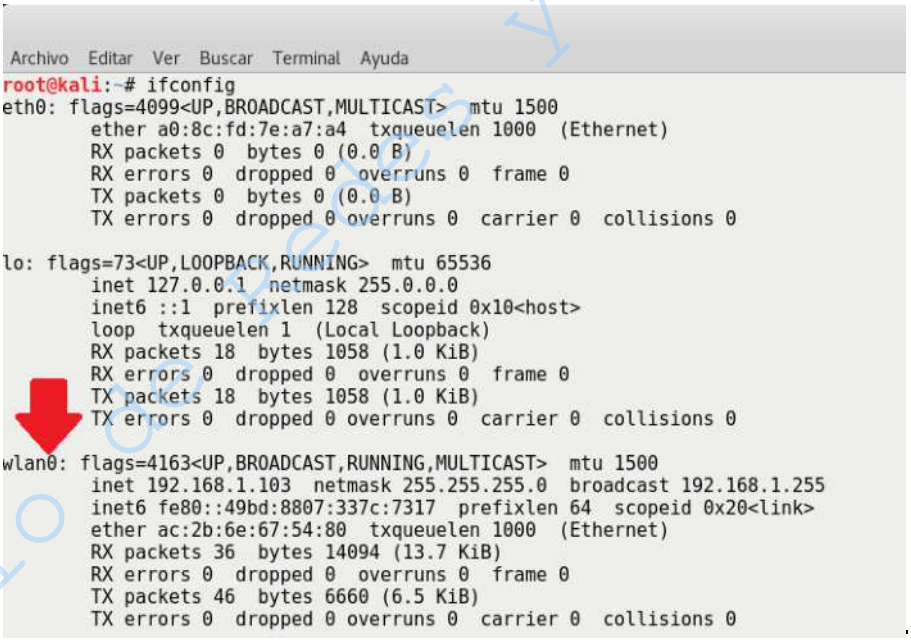



**Figura No. 2. Terminal.**

**4.2.2** Una vez que ya se identificó la interfaz de red inalámbrica wlan0 es importante colocarla en modo monitor. Para ello ejecute los siguientes comandos.

**root@kali:~#** ***airmon-ng stop INTERFACE***

**NOTA: Donde *INTERFACE* es el identificador de la tarjeta inalámbrica (Figura No. 3).**

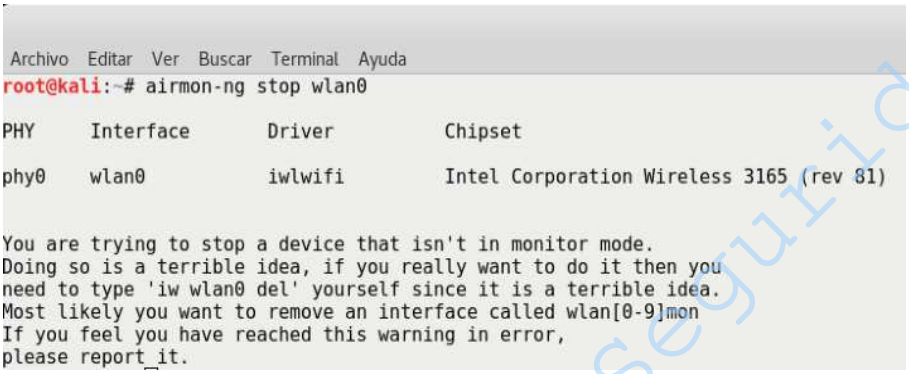



**Figura No. 3. Empleando el comando airmon-ng**

**root@kali:~#** ***airmon-ng start INTERFACE***

**NOTA: Donde *INTERFACE* es el identificador de la tarjeta inalámbrica (Figura No. 4). En caso de existir un problema por los procesos que están corriendo, teclee primero**

**root@kali:~#** ***airmon-ng check kill***

**y posteriormente**

**root@kali:~#** ***airmon-ng start INTERFACE***

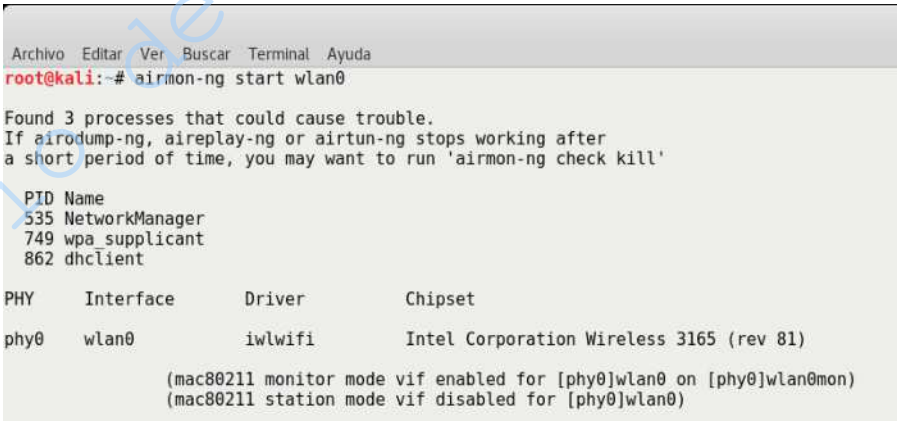



**Figura No. 4. Empleando el comando airmon-ng**

Indique lo que observa al teclear cada uno de los comandos, ¿cuál es el objetivo de haberlos ejecutado?

_____

_____

_____

**4.2.3** Teclee el siguiente comando para ver el nuevo nombre de la interfaz en modo monitor (Figura No. 5).

**root@kali:~# ifconfig**

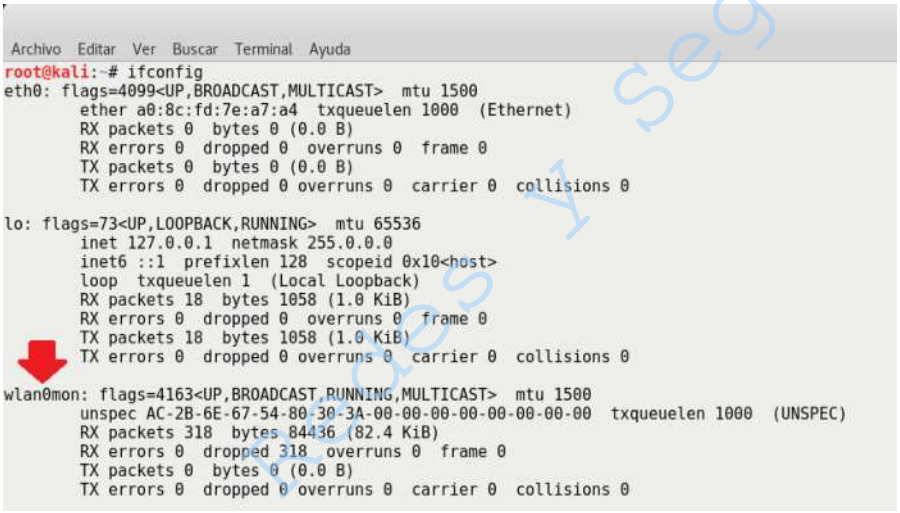



**Figura No. 5 Ejecución del comando ifconfig**

**4.2.4** Busque las redes inalámbricas cercanas mediante el comando siguiente (Figura No. 6)

**root@kali:~# airodump-ng INTERFACE_MODOMONITOR**

**NOTA: Donde *INTERFACE_MODOMONITOR* es el identificador de la tarjeta inalámbrica en modo monitor.**

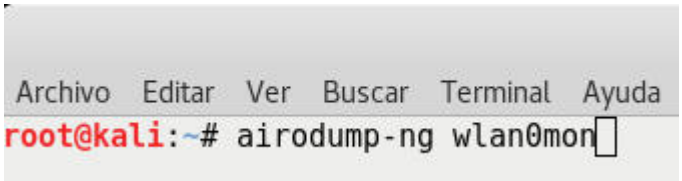
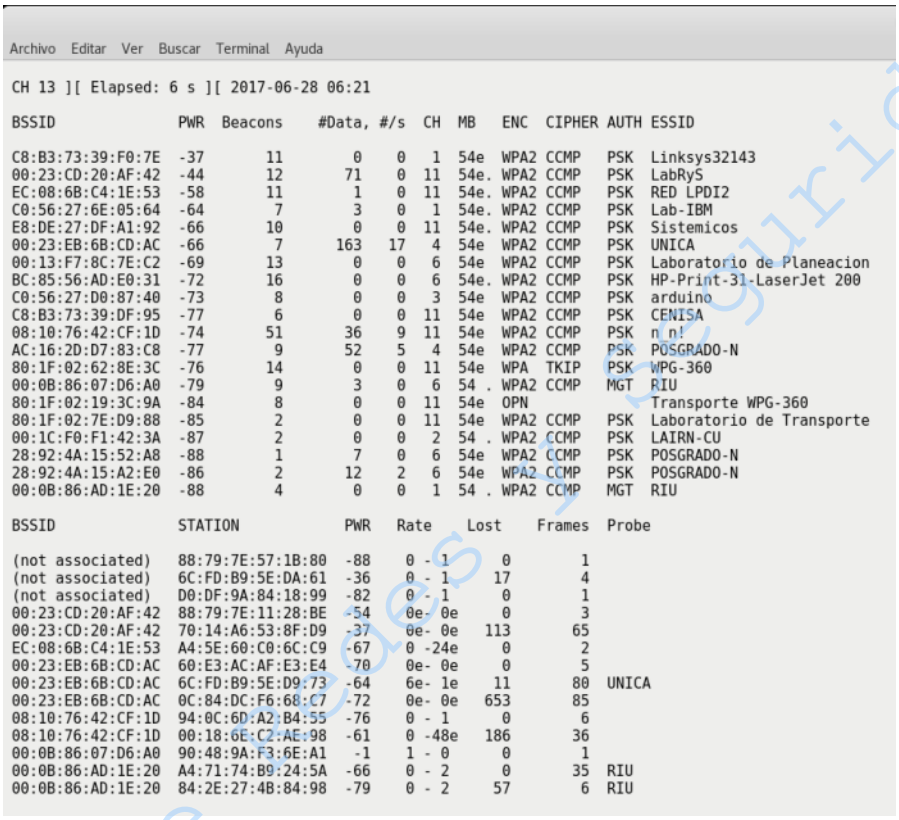



**Figura No. 6 Buscando redes cercanas**

Deberá salir algo parecido a la Figura No. 7:



```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

CH 13 ][ Elapsed: 6 s ][ 2017-06-28 06:21

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C8:B3:73:39:F0:7E  -37       11        0    0   1  54e  WPA2 CCMP   PSK  Linksys32143
00:23:CD:20:AF:42  -44       12       71    0  11  54e. WPA2 CCMP   PSK  LabRyS
EC:08:6B:C4:1E:53  -58       11        1    0  11  54e. WPA2 CCMP   PSK  RED LPDI2
C0:56:27:6E:05:64  -64        7        3    0   1  54e. WPA2 CCMP   PSK  Lab-IBM
E8:DE:27:DF:A1:92  -66       10        0    0  11  54e. WPA2 CCMP   PSK  Sistemicos
00:23:EB:6B:CD:AC  -66        7      163   17   4  54e  WPA2 CCMP   PSK  UNICA
00:13:F7:8C:7E:C2  -69       13        0    0   6  54e  WPA2 CCMP   PSK  Laboratorio de Planeacion
BC:85:56:AD:E0:31  -72       16        0    0   6  54e. WPA2 CCMP   PSK  HP-Print-31-LaserJet 200
C0:56:27:D0:87:40  -73        8        0    0   3  54e  WPA2 CCMP   PSK  arduino
C8:B3:73:39:DF:95  -77        6        0    0  11  54e  WPA2 CCMP   PSK  CENISA
08:10:76:42:CF:1D  -74       51       36    9  11  54e  WPA2 CCMP   PSK  n_n!
AC:16:2D:D7:83:C8  -77        9       52    5   4  54e  WPA2 CCMP   PSK  POSGRADO-N
80:1F:02:62:8E:3C  -76       14        0    0  11  54e  WPA  TKIP   PSK  WPG-360
00:0B:86:07:D6:A0  -79        9        3    0   6  54 . WPA2 CCMP   MGT  RIU
80:1F:02:19:3C:9A  -84        8        0    0  11  54e  OPN             Transporte WPG-360
80:1F:02:7E:D9:88  -85        2        0    0  11  54e  WPA2 CCMP   PSK  Laboratorio de Transporte
00:1C:F0:F1:42:3A  -87        2        0    0   2  54 . WPA2 CCMP   PSK  LAIRN-CU
28:92:4A:15:52:A8  -88        1        7    0   6  54e  WPA2 CCMP   PSK  POSGRADO-N
28:92:4A:15:A2:E0  -86        2       12    2   6  54e  WPA2 CCMP   PSK  POSGRADO-N
00:0B:86:AD:1E:20  -88        4        0    0   1  54 . WPA2 CCMP   MGT  RIU

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   88:79:7E:57:1B:80  -88    0 - 1      0         1
(not associated)   6C:FD:B9:5E:DA:61  -36    0 - 1     17         4
(not associated)   D0:DF:9A:84:18:99  -82    0 - 1      0         1
00:23:CD:20:AF:42  88:79:7E:11:28:BE  -54    0e- 0e     0         3
00:23:CD:20:AF:42  70:14:A6:53:8F:D9  -37    0e- 0e   113        65
EC:08:6B:C4:1E:53  A4:5E:60:C0:6C:C9  -67    0 -24e     0         2
00:23:EB:6B:CD:AC  60:E3:AC:AF:E3:E4  -70    0e- 0e     0         5
00:23:EB:6B:CD:AC  6C:FD:B9:5E:D9:73  -64    6e- 1e    11        80  UNICA
00:23:EB:6B:CD:AC  0C:84:DC:F6:68:C7  -72    0e- 0e   653        85
08:10:76:42:CF:1D  94:0C:6D:A2:B4:55  -76    0 - 1      0         6
08:10:76:42:CF:1D  00:18:6E:C2:AE:98  -61    0 -48e   186        36
00:0B:86:07:D6:A0  90:48:9A:F3:6E:A1   -1    1 - 0      0         1
00:0B:86:AD:1E:20  A4:71:74:B9:24:5A  -66    0 - 2      0        35  RIU
00:0B:86:AD:1E:20  84:2E:27:4B:84:98  -79    0 - 2     57         6  RIU
```

**Figura No. 7. Búsqueda de redes inalámbricas.**

### *I. Analice los resultados obtenidos*

_____
_____
_____
_____
_____
_____
_____
_____
_____

**4.2.5** 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). Detenga la auditoría de redes con CTRL+C. Ejecute nuevamente airodump-ng con los datos recolectados (Figura No. 8):

**root@kali:~# airodump-ng --bssid BSSID -c CHANNEL –w ARCHIVO INTERFACE**

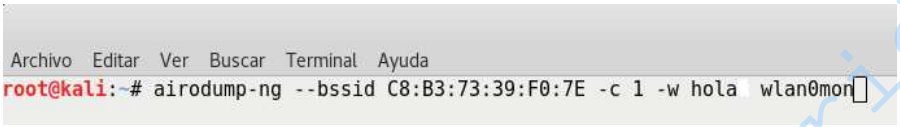



**Figura No. 8. Ejecución de airodump-ng.**

Donde **ARCHIVO** especifica el nombre de un fichero que se creará y guardará por defecto como **ARCHIVO**-01.cap extensión.cap en el cual **airodump** almacenará los paquetes capturados de la red. Esta terminal deberá permanecer activa durante el ataque. En la pantalla aparecerá la información como en la Figura No. 9.

**NOTA: El profesor o la profesora deberá generar tráfico conectándose inalámbricamente al dispositivo en cuestión.**

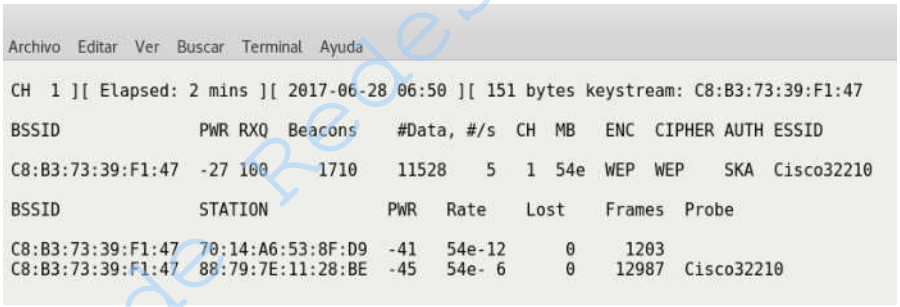



**Figura No. 9. Captura de datos.**

### *II. Analice los resultados obtenidos*

_____
_____
_____
_____
_____
_____
_____
_____

**4.2.6** Abra una nueva terminal, donde aplicará una falsa autenticación, con el objetivo de que el punto de acceso confíe en la interfaz atacante. Esto se realiza con la siguiente instrucción:

**root@kali:~# 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 interfaz inalámbrica que está conectada al dispositivo. Véase la figura No. 10.

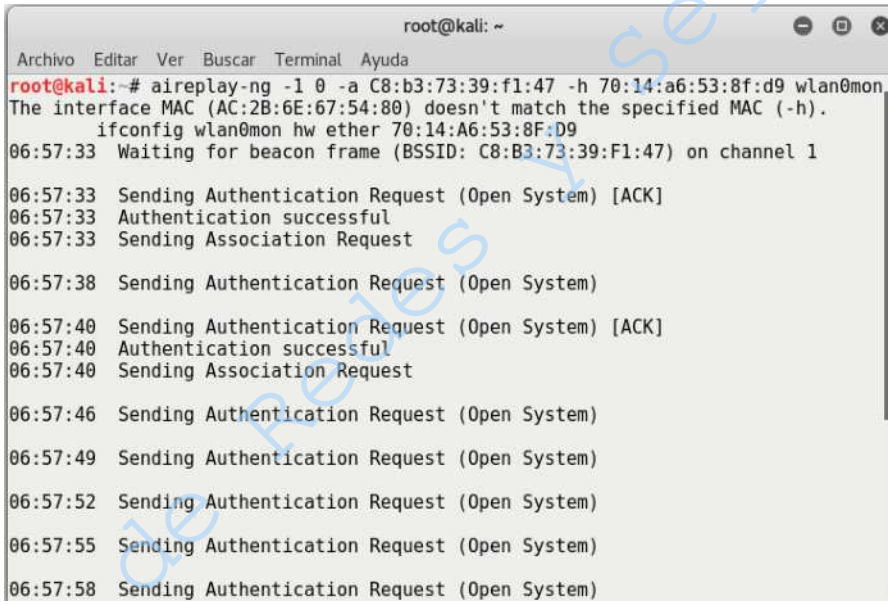



**Figura No. 10. Autenticación de la MAC.**

**4.2.7** En una nueva terminal verifique el nombre del archivo para escribirlo correctamente con todo y extensión al emplear el siguiente comando, sustituir el nombre completo del archivo (**ARCHIVO**-01.cap) en **ARCHIVO.**

Donde **ARCHIVO** es el nombre del fichero que se creó y guardó por defecto con extensión.cap, por lo cual se necesitará realizar un listado de archivos con el siguiente comando para saber el nombre completo del **ARCHIVO** (Figura No. 11).

**root@kali:~# ls**

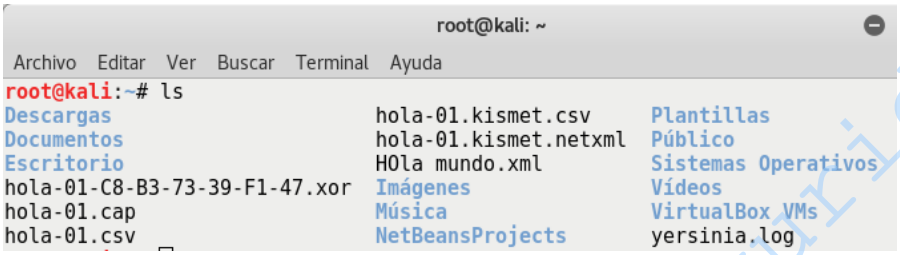



**Figura No. 11. Listado de archivos**

**4.2.8** Ejecute aircrack-ng para comenzar a obtener la clave de acceso a la red. Véanse las figuras No. 12 y 13.

**root@kali:~# aircrack-ng –b BSSID –z ARCHIVO**

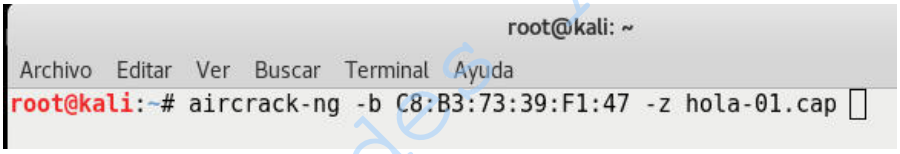



**Figura No. 12 Ejecución de aircrack-ng**

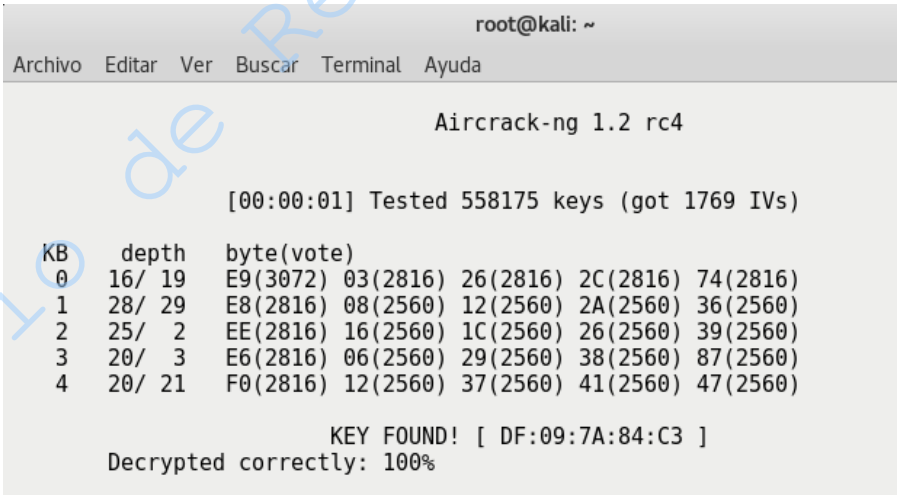



**Figura No. 13. Deducción de clave.**

***III. Indique a que hace referencia la información obtenida en pantalla y ¿cuál fue el resultado final?***

_____
_____
_____
_____
_____
_____
_____
_____

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.

### 4.3 Cifrado WPA2

**NOTA PARA EL PROFESOR O LA PROFESORA**

Haga clic en el menú de *Wireless* → *Wireless Security*.

Coloque en Network Name (SSID) el nombre que prefiera para identificar al dispositivo..

En la opción *Wireless* → *Wireless Security* habilite el modo de seguridad en WPA2-Personal.

Con base en la tabla 1.2 llene los campos indicados, cuando coloque la frase haga clic en el botón Generate.

**Tabla 1.2. Parámetros de seguridad.**

| Nombre | Valor |
|---|---|
| Security Mode | WPA2-Personal |
| Encrytion | 40/64 bits |
| Passphrase | |

**NOTA: En Passphrase coloque una palabra clave que se encuentre contenida en el diccionario**

**4.3.1** Para realizar la ruptura de claves del protocolo WPA2, es necesario repetir los pasos 4.2.1 al 4.2.5.

**4.3.2** 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 (Figura No. 14).

**root@kali:~# aireplay-ng --deauth 0 –a BSSID –c MAC_CLIENTE INTERFACE**

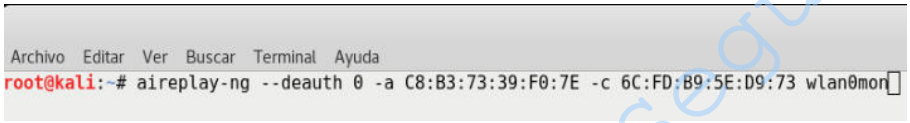



**Figura No. 14 ejecución de aireplay**

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 (Figura No. 15).

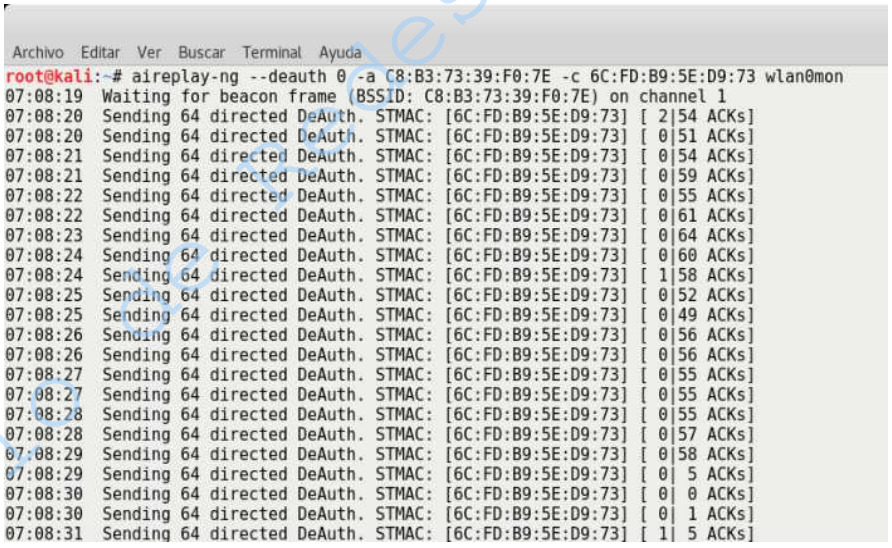



**Figura No. 15 Captura del 4-way handshake**

**4.3.3** 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 (Figura No. 16):

**root@kali:~# aircrack-ng –b BSSID –w DICCIONARIO –z ARCHIVO**

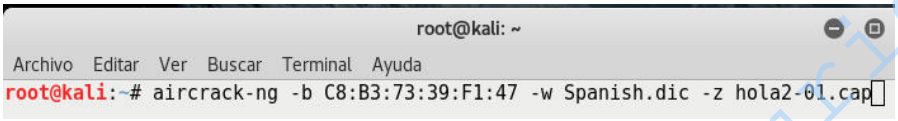



**Figura No. 16 Ejecución de aircrack**

Donde **DICCIONARIO** es el archivo de texto que contiene las palabras a probar como posibles claves y **ARCHIVO** el **ARCHIVO**-01.cap que contiene las tramas capturadas junto con los paquetes especiales del 4-way handshake.

***IV. Indique a qué hace referencia la información obtenida en pantalla y ¿cuál es el resultado final?.***

_____
_____
_____
_____
_____
_____
_____
_____

***5.- Cuestionario***

1. Mencione la importancia de manejar claves seguras

_____
_____
_____
_____
_____
_____
_____

2. 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 9**

**Ruptura de claves WPA2 Y WEP**

***Cuestionario Previo***

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?
5. Abra una terminal de Kali (en modo de súper usuario), y verifique que en su dispositivo detecte la interfaz de red (wlan0) inalámbrica con el comando ifconfig como se muestra en la figura A.

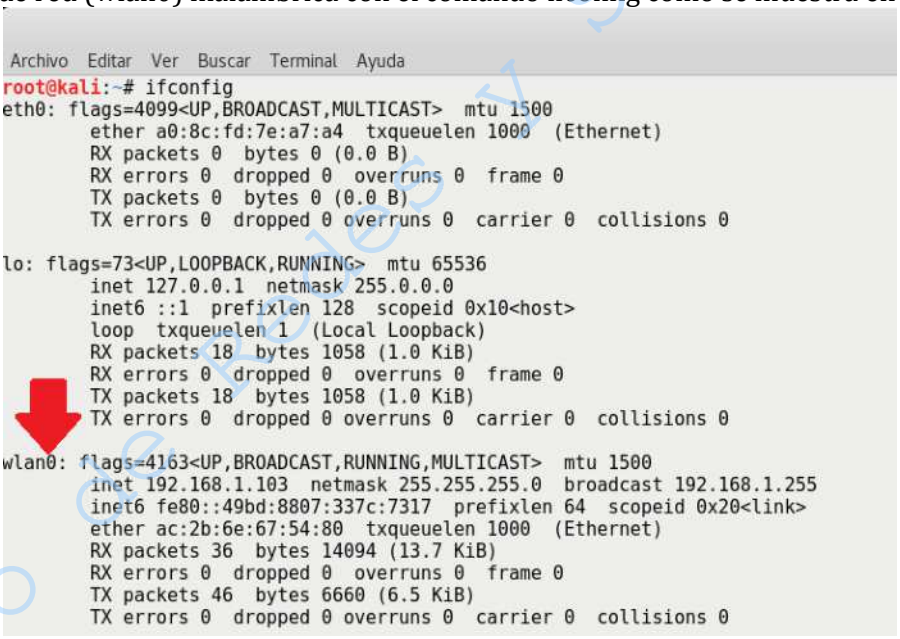



**Figura A. Terminal.**

6. Investigar por qué es necesario colocar una interfaz inalámbrica en modo monitor

# Práctica 10

# Mecanismos de Seguridad, Firma Digital

## Control

## 1. *Objetivos de Aprendizaje*

- El alumno o la alumna se familiarizará con herramientas básicas relacionadas con la seguridad en la red, las cuales podrán ser estudiadas a profundidad en subsecuentes materias.

- El alumno o la alumna realizará una aplicación que permita el proceso de firmado de un documento a través de la infraestructura de claves asimétricas, en el lenguaje orientado a objetos Java.

## 2. *Conceptos teóricos*

En diversas organizaciones, tanto públicas como comerciales, el uso de Internet se ha convertido en un foro principal para hacer negocios, sirviendo como medio principal para la publicidad, el *marketing*, las ventas y la atención al cliente. Ha permitido que las empresas crezcan y a las grandes corporaciones, expandir su dominio.

Junto a las oportunidades que ofrece Internet se encuentran riesgos de seguridad importantes. Los servidores Web pueden ser sustituidos y a veces, las páginas Web han sido desconfiguradas. Los datos privados de los consumidores podrían ser revelados. Las transacciones financieras pueden ser falsificadas. Los cortafuegos de las empresas pueden ser infringidos y las redes de la empresa saboteadas. Todos estos escenarios conllevan a un uso seguro de Internet.

La comunicación segura dentro de una red debe cumplir con las siguientes características: confidencialidad, autenticación, integridad del mensaje, disponibilidad y control de acceso. Las 3 primeras características se han considerado componentes claves de una red segura, sin embargo, se han añadido en las últimas décadas la necesidad de mantener la red operando.

El concepto de firma digital fue introducido por Diffie y Hellman en 1976, siendo un bloque de caracteres que acompaña a un documento acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad).

El proceso de firmado digital se inicia cuando el autor de un documento utiliza su clave secreta dentro del esquema de cifrado asimétrico, a la que sólo él tiene acceso, esto impide que pueda negar su autoría (revocación o no repudio). De esta forma el autor es vinculado al documento de la firma. El software del autor aplica un algoritmo hash sobre el texto a firmar, obteniendo un extracto de longitud fija y absolutamente específico del mensaje. Un cambio mínimo en el mensaje dará lugar a una cadena hash distinta. El extracto tiene una longitud de 128 a 160 bits, dependiendo del algoritmo utilizado, entre los que se encuentran: MD5 o SHA-1. El algoritmo más utilizado en el proceso de encriptación asimétrica es el RSA.

La validez de la firma es probada por cualquier persona que disponga de la clave pública del autor.

La identificación indubitable de las personas y organizaciones se sustenta en la firma digital que opera bajo la denominada Infraestructura de Clave Pública.

La "despapelización", como resultado de la utilización de la firma digital, da origen al Documento Digital, garantizando la autenticidad, integridad, no repudio y eventualmente la confidencialidad del mismo.

Es así que vistos los tiempos en que vivimos, es aplicable entre otras a:

- Identificación como usuario ante redes internas o externas (abiertas o cerradas).
- Correos electrónicos.
- Identificación de sitios en Internet.
- Transacciones EDI (Electronic Data Interchange).
- Comercio electrónico.
- Información que se obtenga de Internet.
- Transacciones financieras.
- Software y hardware.
- Comercio exterior.
- Comercio interno.
- Toda documentación que precise movilizarse rápidamente o por el contrario que posea un alto costo de movilización

Aplicaciones sobre la firma digital

- Firma y/o cifrado de correo electrónico, tanto interno como externo.
- Firma y/o cifrado de documentos (Pericias, dictámenes, planos, software, políticas, procedimientos, normativas, minutas, y otros).
- Identificación de personas ante sistemas internos en redes locales y abiertas (intranets), sitios Web (sin necesidad de registrar datos) determinación implícita del perfil de usuario.
- Identificación de sistemas ante el usuario (¿Cómo sé que es el sistema que dice ser?).
- Auditoría de transacciones.
- Seguridad al operar comercialmente (Compra-venta de acciones, transacciones bancarias, operaciones con tarjeta de crédito, y otras).
- Identificación de los componentes físicos de una red (Computadores, routers, teléfonos celulares, y otros).

Aplicaciones sobre el documento digital firmado digitalmente

- Fidelización de documentos digitalizados.
- Recibos de pago.
- Certificaciones.
- Cheque electrónico.
- Solicitudes de prestación de servicios
- Adjudicaciones.
- Factura electrónica.
- Invitaciones.

- Promociones.
- Remitos de entrega.
- Solicitudes de adhesión.
- Actas.
- Planificaciones.
- Reservas o turnos para distintas prestaciones (Talleres, médicos, hoteles, pasajes, etc.).
- Autorizaciones de prestaciones médicas.
- Historia clínica única.
- Confirmaciones.
- Diseños
- Acreditaciones de puntaje.
- Órdenes de compra.
- Contratos.
- Planos.
- Circulares internas y/o externas.
- Cotizaciones de bienes y servicios (tanto el pedido como la cotización y condiciones del proveedor).
- Receta médica electrónica.
- Declaraciones juradas.
- Proyectos.

Es indudable que otras tantas aplicaciones particulares hacen o pueden hacer uso de la tecnología. Sin embargo, detrás de ésta, por las connotaciones que conlleva, la certificación por autoridad competente especializada del adecuado funcionamiento de las aplicaciones, acorde con las normativas en la materia, las transforma en un tema sumamente delicado. A modo de ejemplo, una aplicación que mayoritariamente contempla el uso de certificados digitales y concordantemente la firma digital es la de correo electrónico y si bien su funcionamiento es razonablemente adecuado a esta situación, adolecen de garantías contra defectos que le son imputables, más aún de cara a esta nueva realidad digital/legal.

## *3. Equipo y material necesario*

***Equipo del Laboratorio:***

- JDK instalado en el sistema operativo Linux.

## *4. Desarrollo*

***Modo de trabajar***

La práctica se desarrollará en parejas.

La aplicación Java a realizar se compone de dos programas, el primero hará el firmado del documento y el segundo verificará la firma de dicho documento. El programa que realiza el primer procedimiento debe cumplir con los siguientes requerimientos:

- Solicitar mediante la entrada estándar, el nombre del archivo que contiene la información a firmar (Archivo A).
- La salida del programa que firma el documento, deben ser dos archivos, el primero contendrá la clave pública generada y el segundo la firma del documento (Archivo B, Archivo C).
- El programa que recibe el Archivo A debe generar internamente el par de claves.

El programa que realiza el segundo procedimiento debe cumplir con los siguientes requerimientos:

- Solicitar mediante la entrada estándar, el nombre del archivo que contiene la clave pública generada en el primer punto, además del nombre del archivo que contiene la información firmada (Archivo B, Archivo C).
- Indicar mediante una cadena si la firma es correcta.

### *4.1* Firma Digital

Una firma digital es un bloque de caracteres que se anexa a un documento con el fin de acreditar quién es su autor, se basa en la criptografía de clave pública, donde quién firma el mensaje lo cifra con su clave privada de forma que puede ser descifrado por todo aquel que posea la clave pública, correspondiente a la clave privada empleada para firmar el mensaje.

**NOTA: La firma digital no hace cifrado de mensajes, únicamente garantiza el origen.**

***I. ¿Cuál es el objetivo de la firma digital?***

_____
_____
_____
_____

El cifrado de un mensaje con la clave privada consume un tiempo elevado de proceso, por lo que resulta imprescindible contar con un texto más corto que el mensaje original, éste es obtenido mediante una función hash y comúnmente denominado huella digital o fingerprint. Si el mensaje original se altera, también varía la huella digital y lo que se cifra con la clave privada no es el mensaje original, sino la huella digital, el resultado se añade al documento a transmitir.

### *4.2* Criptografía

#### *4.2.1* Criptografía de clave privada

La criptografía tradicional también denominada de clave secreta se basa en que tanto emisor como receptor, cuentan con una misma clave, que es empleada por el primero para cifrar el mensaje, dando

lugar a un mensaje ilegible, el segundo utiliza la misma clave de cifrado para descifrar y obtener el mensaje original.

***II. Investigue la principal desventaja de la criptografía tradicional.***

_____
_____
_____
_____

### *4.2.2* Criptografía de clave pública

En este tipo de cifrado, el emisor y receptor cuentan con claves distintas. La clave pública es aquella que todo el mundo conoce y que puede ser empleada por cualquiera para cifrar mensajes. La clave privada es aquella que únicamente conoce quién envía el mensaje y es capaz de descifrar los mensajes generados por la clave pública.

***III. Investigue el algoritmo de cifrado más comúnmente utilizado por este tipo de cifrado.***

_____
_____
_____
_____

Una de las principales ventajas de la criptografía asimétrica es la simplificación de la administración de claves al permitir que varias personas utilicen un par de claves, únicamente existe un problema: ¿cómo distribuir una clave pública de forma que el usuario pueda encontrarla y saber que es válida?

### *4.3* Firma de un documento

El programa que genera las claves para firmar un documento, hará uso del API de Seguridad del JSDK.

***4.3.1*** Inicie la máquina virtual e ingrese como usuario redes.

***4.3.2*** Cree una carpeta en /home/redes con el nombre de **Practica10aINICIALES**, de manera que sea donde almacene los archivos generados.

**NOTA: La palabra INICIALES son las iniciales de su nombre y apellidos.**

***4.3.3*** Emplee el comando **nano GeneraFirmaINICIALES.java** y teclee el siguiente código, el cual es la estructura inicial del programa, ver Figura No. 1.

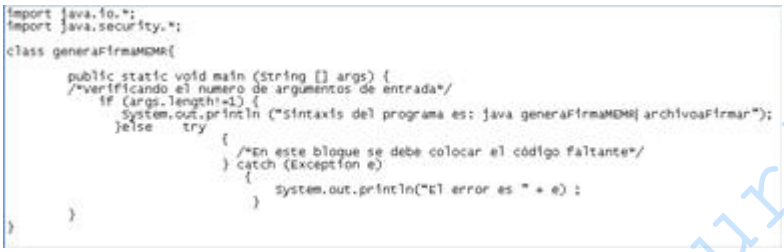



**Figura No. 1. Código de la estructura inicial para generar la firma**

```
import java.io.*;
import java.security.*;
class GeneraFirmaINICALES
{
    public static void main (String [] args)
        {
            /*Verificando el numero de argumentos de entrada*/
            if (args.length!=1)
                {
                    System.out.println ("Sintaxis del programa es: java
                    GeneraFirmaINICIALES archivoaFirmar");
                }
            else   try
            {
/*En este bloque se debe colocar el código faltante*/
            }
            catch (Exception e)
            {
                System.out.println("El error es " + e) ;
            }
        }
    }
```

El programa importa el paquete java.security.*; ya que ahí se encuentran las clases necesarias para generar las claves y firmar un documento. De la misma manera se importa el paquete java.io.*; porque en ese paquete se encuentran las clases necesarias para manipular los archivos de entrada.

**NOTA: Inserte las siguientes líneas del código que se encuentran en negritas y cursiva, en el programa debajo de la línea /*En este bloque se debe colocar el código faltante*/**

***4.3.4*** Para generar una firma digital, se requiere una clave privada que inicie el proceso. La clase KeyPairGenerator permite esa funcionalidad mediante el siguiente código:

***KeyPairGenerator genClave=KeyPairGenerator.getInstance("RSA");***

***4.3.5*** Inicie el objeto genClave a través del método initialize, el cual tiene dos argumentos:

a. Tamaño de clave, el cual es de 1024 bits.

b. La fuente aleatoria, en el caso de la práctica haremos uso de la clase Secure Random.

***SecureRandom aleatorio=SecureRandom.getInstance("SHA1PRNG","SUN");***
***genClave.initialize(1024, aleatorio);***

El objeto SecureRandom, pretende aleatorizar el estado interno del propio generador utilizando el algoritmo de generación de números pseudoaleatorios llamado SHA1PRNG.

***4.3.6*** El siguiente paso es la generación del par de claves para almacenarlas en objetos del tipo PrivateKey y PublicKey, mediante el siguiente código:

***KeyPair pardeClaves= genClave.generateKeyPair();***
***PrivateKey privada=pardeClaves.getPrivate();***
***PublicKey publica=pardeClaves.getPublic();***

**NOTA: Guarde los cambios efectuados en el código**

***4.3.7*** El paso final de esta primera aplicación es el firmado de los datos, ya que se han creado la clave pública y la clave privada. Cree un archivo de nombre datosaFirmar.txt con una nueva ventana de la aplicación de bloc de notas y guarde el archivo en la carpeta creada con el siguiente contenido:

*"Pensar en seguridad se vuelve necesario una vez que permitimos que nuestros recursos computacionales entren en contacto con el resto del mundo. Un puerto de comunicación abierto casi siempre está expuesto a ataques externos o a abusos; es necesario tomar medidas de seguridad para evitar el mal uso de los recursos."*

**NOTA: Guarde los cambios efectuados en el código.**

***4.3.8*** Una firma digital se crea o bien se verifica usando una instancia de la clase Signature, mediante el siguiente código:

***Signature firma=Signature.getInstance ("MD5withRSA");***

***4.3.9*** Antes de que el objeto Signature sea usado para firmar o verificar datos, requiere ser inicializado, el cual requiere de la clave privada.

***firma.initSign(privada);***

***4.3.10*** Antes de firmar es necesario suministrar al objeto "firma" los datos a firmar, los cuales se almacenan dentro de un archivo. Las siguientes líneas abren el archivo, su contenido lo guarda en un buffer y posteriormente se lo hace llegar al objeto "firma".

```
FileInputStream archivo=new FileInputStream(args[0]);
BufferedInputStream buferEntrada=new BufferedInputStream(archivo);
byte[] buffer=new byte[1024];
int longitud;

while (buferEntrada.available() !=0)
        {
            longitud =buferEntrada.read(buffer);
            firma.update(buffer, 0, longitud);
         }
buferEntrada.close();
```

***4.3.11*** Finalmente, una vez que se han suministrado los datos al objeto "firma", se genera la firma digital de los datos.

***byte[] firmaReal=firma.sign();***

***4.3.12*** Generada la firma es necesario enviarla a un archivo de la misma manera que la clave pública para el proceso de verificado de firma digital.

```
                    /*Guardando los datos firmados en un archivo*/
FileOutputStream archivoFirma=new FileOutputStream("firmaINICIALES.txt");
archivoFirma.write(firmaReal);
archivoFirma.close();
                        /*Guardando la clave pública en un archivo*/
byte[] clave=publica.getEncoded();
FileOutputStream clavePublica=new FileOutputStream("clavePublicaINICIALES.txt");
clavePublica.write(clave);
clavePublica.close();
```

El método getEncoded obtiene los bytes codificados de la clave pública y luego se envían a un archivo.

**NOTA: Guarde los cambios efectuados en el código.**

***4.3.13*** Debe ubicarse en el directorio **/home/redes/Practica10aINICIALES**, para compilar el programa mediante la instrucción ***javac GeneraFirmaINICALES.java***, en la línea de comando y observe el resultado.

***4.3.14*** Ejecute el programa con la instrucción ***java GeneraFirmaINICALES datosaFirmar.txt*** y observe en su directorio de trabajo la creación de los archivos esperados.

### *4.4* Verificación de la firma de un documento

La verificación de la firma de un documento implica que quien recibe el mensaje, en primer lugar aplica la función hash al documento recibido, descifra la huella digital cifrada y compara ésta con la obtenida al procesar el documento, si son iguales el documento no ha sido alterado y efectivamente ha sido enviado por quien firma.

***IV. Indique los argumentos que debe recibir el programa que verifica la firma digital de un documento.***

_____
_____
_____
_____

***4.4.1*** Emplee el comando **nano VerificaFirmaINICIALES.java** y teclee el siguiente código, el cual es la estructura inicial del programa, ver Figura No. 2.

**NOTA: No olvide guardar el archivo VerificaFirmaINICIALES.java en la misma carpeta /home/redes/Practica10aINICIALES.**

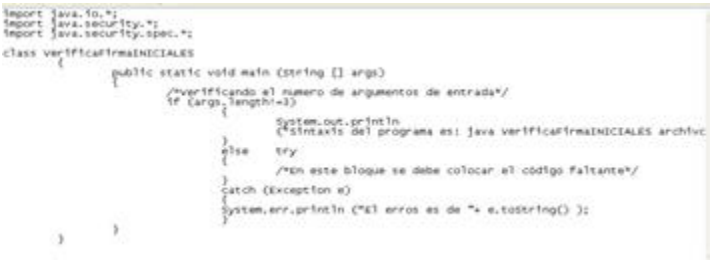



**Figura No. 2. Código de la estructura inicial para verificar la firma**

```
import java.io.*;
import java.security.*;
```

```
import java.security.spec.*;

class VerificaFirmaINICIALES
{
    public static void main (String [] args)
    {
            /*Verificando el numero de argumentos de entrada*/
            if (args.length!=3)
            {
                System.out.println
                ("Sintaxis del programa es: java VerificaFirmaINICIALES
                archivoaFirmarINICIALES.txt clavepublicaINICIALES.txt firmaArchivo");
              }
            else   try
            {
                /*En este bloque se debe colocar el código faltante*/
              }
            catch (Exception e)
            {
                System.err.println ("El error es de "+ e.toString() );
              }
      }
    }
```

El programa importa el paquete java.security.spec, ya que éste contiene la clase X509EncodedKeySpec.

**NOTA: Inserte las siguientes líneas del código que se encuentran en negritas y cursiva en el programa debajo de la línea /*En este bloque se debe colocar el código faltante*/**

***4.4.2*** El primer paso consiste en importar los bytes codificados de la clave pública del archivo que lo contiene y convertirlos en un objeto del tipo PublicKey mediante el siguiente código:

```
FileInputStream clavepublica=new FileInputStream (args[0]);
byte[] clave=new byte[clavepublica.available()];
clavepublica.read(clave);
clavepublica.close();
```

El arreglo de bytes clave contiene los bytes codificados de la clave pública.

***4.4.3*** El siguiente paso consiste en obtener el valor de la clave pública, para lo cual hacemos uso de una clase KeyFactory que proporciona conversión entre claves opacas (del tipo Key) y especificaciones de claves, que son representaciones transparentes del material de la clave. Primero es necesario una especificación de clave mediante el estándar X.509, con el siguiente código:

***X509EncodedKeySpec pubKeySpec=new X509EncodedKeySpec(clave);***

***4.4.4*** Se requiere de un objeto KeyFactory para realizar la conversión, éste debe trabajar con claves RSA.

***KeyFactory keyFactory = KeyFactory. getInstance("RSA");***

***4.4.5*** Empleando el objeto keyFactory se genera un objeto PublicKey de la siguiente manera:

***PublicKey pubKey=keyFactory.generatePublic(pubKeySpec);***

***4.4.6*** El siguiente paso consiste en introducir los bytes firmados desde el archivo especificado en el segundo argumento de la línea de comandos:

```
FileInputStream archivoFirmado=new FileInputStream(args[1]);
byte[] firmaVerificada=new byte[archivoFirmado.available()];
archivoFirmado.read(firmaVerificada);
 archivoFirmado.close();
```

Hasta este punto el arreglo de bytes firmaVerificada contiene los bytes de la firma de documento.

***4.4.7*** Una firma se verifica usando una instancia de la clase Signature, definiendo los algoritmos utilizados en el proceso de la firma del documento:

***Signature firma=Signature.getInstance ("MD5withRSA");***

***4.4.8*** Inicialice el objeto Signature con el método verificar que recibe como argumentos la clave pública:

***firma.initVerify(pubKey);***

***4.4.9*** Suministre al objeto firma los datos para los cuales se generó la firma, éstos se encuentran en el archivo original.

```
FileInputStream datos=new FileInputStream(args[2]);
BufferedInputStream
buferEntrada=new BufferedInputStream(datos);
```

```
byte[] buffer=new byte[1024];
int longitud;

while (buferEntrada.available() !=0)
        {
         longitud= buferEntrada.read(buffer);
        firma.update(buffer,0,longitud);
        }
buferEntrada.close();
```

***4.4.10*** El proceso de verificación de la firma permite reportar el resultado.

```
boolean verifica=firma.verify(firmaVerificada);
System.out.println ("Verificación de la firma  " +verifica);
```

**NOTA: Guarde los cambios efectuados en el código.**

***4.4.11*** Compile el programa mediante la instrucción ***javac VerificaFirmaINICIALES.java*** en la línea de comandos.

***4.4.12*** Ejecute el programa con la instrucción ***java VerificaFirmaINICIALES clavepublicaINICIALES.txt firmaINICIALES.txt datosaFirmar.txt*** y observe el resultado.

***4.4.13*** Modifique el archivo clavePublica.txt en el bloc de notas, ejecute nuevamente el programa con la instrucción ***java VerificaFirmaINICALES clavepublicaINICIALES.txt firmaINICIALES.txt datosaFirmar.txt*** y observe el resultado.

***V. Investigue el error obtenido en el punto anterior.***

_____
_____
_____
_____

**NOTA: Ejecute nuevamente la instrucción *java GeneraFirmaINICIALES datosaFirmar.txt* para restablecer la clave pública.**

***4.4.14*** Modifique el archivo datosaFirmar.txt en el bloc de notas, ejecute nuevamente el programa con la instrucción **java VerificaFirmaINICIALES clavePublicaINICIALES firmaINICIALES datosaFirmar.txt** y observe el resultado.

***VI. Defina el escenario que representa el punto anterior.***

_____
_____
_____
_____

***Elabore un diagrama en el cuál indique el funcionamiento y los elementos de los programas realizados anteriormente.***

### *5. Conclusiones*

**PRÁCTICA 10**
**Mecanismos de Seguridad, Firma Digital**
***Cuestionario Previo***

1. ¿Qué son los mecanismos de seguridad?
2. ¿A qué se refieren los mecanismos de seguridad generalizados? y menciona 2 ejemplos.
3. ¿A qué se refieren los mecanismos de seguridad específicos? y menciona 3 ejemplos.
4. Investigue en qué consisten las funciones hash y mencione al menos 3 ejemplos.
5. Investigue en qué consisten los algoritmos de clave pública.
6. Mencione al menos 3 algoritmos de cifrado simétrico o de criptografía tradicional.
7. Investigue el contenido básico del estándar X.509.
8. Investigue el uso de las sentencias try y catch dentro del lenguaje java
9. Investigue el funcionamiento del método getPrivate y getPublic

# Práctica 11

# Mecanismos de Seguridad, Certificados Digitales

## Control

### 1. *Objetivos de Aprendizaje*

- El alumno o la alumna identificará los diversos tipos de certificados, así como su importancia dentro de los esquemas de seguridad en las redes, utilizando una herramienta de software libre que permite la administración de certificados digitales, OpenSSL

### 2. *Conceptos teóricos*

El panorama de las telecomunicaciones de datos se ha visto afectado por un gran cambio en los últimos años del siglo XXI. Las innovaciones y cambios tecnológicos suceden con gran velocidad a medida que se perfeccionan y se depuran las ideas y técnicas que han permitido la unión entre la informática, la electrónica y las comunicaciones.

En las transacciones comunes los retos de identificación, autenticación y privacidad son resueltas, con marcas físicas, tales como las firmas. En las transacciones electrónicas, el equivalente a un sello tiene que ser codificado en información. El verificar que el sello se encuentra presente y no ha sido alterado, es la forma en la que el que recibe la información puede confirmar la identidad del que lo envió y de esta manera se asegura que el mensaje no ha sido alterado ni modificado en el camino. Para crear un equivalente electrónico a la seguridad física se usa la llamada criptografía.

Un certificado digital es un documento electrónico mediante el cual un tercero confiable (una autoridad de certificación) garantiza la relación entre la identidad de un sujeto o entidad y su clave pública.

Existen varios formatos de certificado digital, los más comúnmente empleados se rigen por el estándar UIT-T X.509v3. El certificado contiene usualmente el nombre de la entidad certificada, un número serial, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital) y la firma digital de la autoridad emisora del certificado de forma que el receptor pueda verificar que ésta última ha establecido realmente la asociación.
Para los usuarios, los certificados digitales proporcionan un mecanismo para verificar la autenticidad de programas y documentos obtenidos a través de la red, el envío de correo cifrado o firmado digitalmente así como el acceso a recursos, etcétera.

### 3. *Equipo y material necesario*

***Equipo del Laboratorio:***

- PC con sistema operativo Linux, Debian.
- Paquete de instalación de OpenSSL.

## *4. Desarrollo*

***Modo de trabajar***

La práctica se desarrollará en parejas.

### *4.1* Certificado Digital

Un certificado permite obtener la clave pública de otra entidad ya sea una persona o institución. Se considera como una declaración firmada digitalmente por una entidad indicando que la clave pública de otra persona tiene un valor específico.

Existen diferentes clases de certificados de acuerdo con su utilidad:

- Certificados de servidor, aportan a un sitio Web la característica de seguridad para poder intercambiar información como: números de cuenta, contraseñas, etcétera.
- Certificados para WAP, permiten a los sitios Web la realización de transacciones seguras con sus usuarios móviles. Los certificados WAP permiten mantener conexiones seguras basadas en cifrado y autenticación con dispositivos de telefonía móvil.
- Certificados personales, otorgan seguridad a los correos móviles basados en el estándar S/MIME asegurando que el receptor designado sea el lector del mensaje.
- Certificados para firmar código, permiten a los administradores o desarrolladores de software firmar su código para la distribución segura entre sus clientes.
- Certificados para IPSec-VPN, son los elementos necesarios para que la organización aproveche las cualidades y ventajas del uso de las VPN (Redes Virtuales Privadas - Virtual Network Private).

#### *4.1.1* Instalación de OpenSSL

OpenSSL es una herramienta de software libre desarrollado por los miembros de la comunidad OpenSource que permite la creación y administración de certificados digitales, además de contar con librerías relacionadas con la criptografía, útiles para proporcionar funciones criptográficas, como OpenSSH y navegadores Web (https). Este paquete es importante para cualquiera que esté planeando implementar un cierto nivel de seguridad en una máquina Linux.

***4.1.1.1*** Abra la aplicación VirtualBox

**NOTA: Antes de iniciar la máquina virtual verifique en la opción Red que se encuentre marcada la opción Habilitar adaptador de red->Conectado a: Adaptador puente (Figura No. 1).**

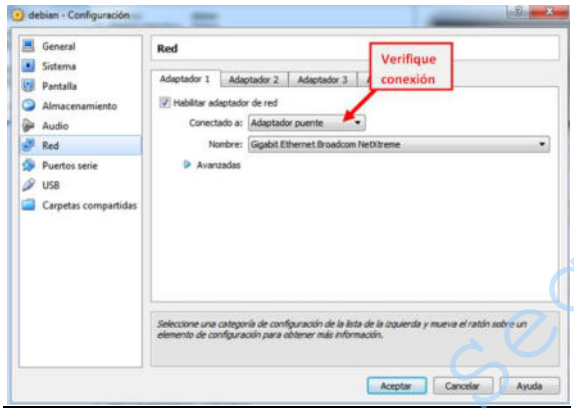



**Figura No. 1. Conexión de red.**

***4.1.1.2*** Encienda la máquina virtual

***4.1.1.3*** Elija la opción de cargar Linux, distribución Debian.

**NOTA: En caso de que le aparezca la imagen de instalación (Figura No. 2), dé clic derecho sobre el disco duro. Seleccione la opción que se encuentra palomeada para deseleccionarla, apague la máquina virtual y vuelva a iniciarla**.

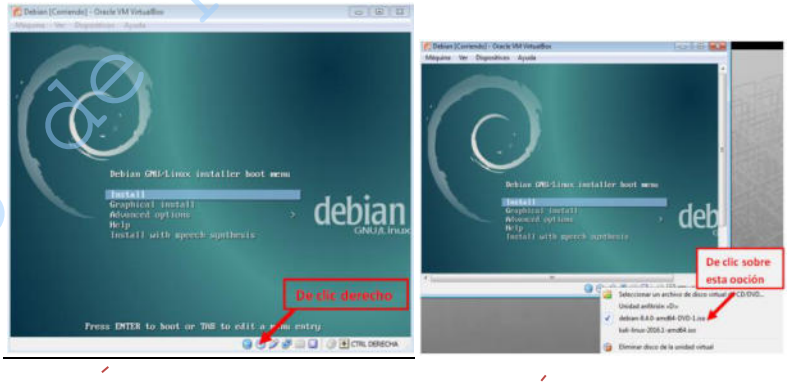



**Figura No. 2. Inicio de Máquina Virtual.**

***4.1.1.4*** Inicie sesión en la cuenta de redes.

***4.1.1.5*** Abra una terminal e ingrese como super usuario, para ello teclee el comando que se muestra a continuación. (Ver Figura No. 3)

**NOTA: *su* significa super usuario, por lo que se emplea la misma contraseña de root**
**redes@debian:~$ su**

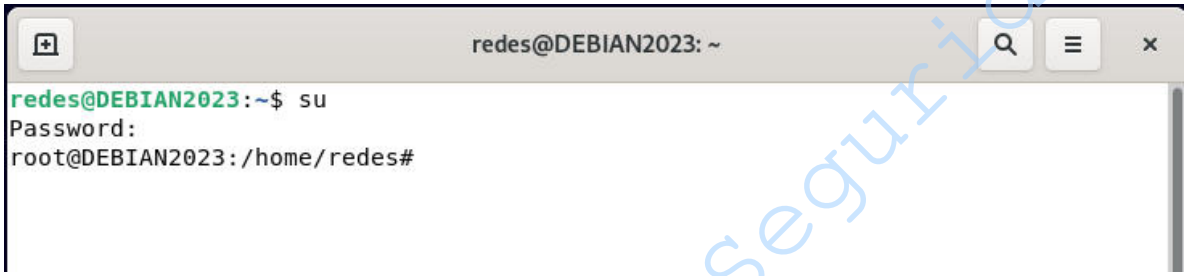



**Figura No. 3. Terminal de comandos como root.**

***4.1.1.6*** Cree una carpeta llamada openssl en la carpeta personal del usuario con el cual se registró.

**redes@debian:/home/redes# mkdir openssl**

***4.1.1.7*** Ejecute el comando:

**redes@debian:/home/redes# apt-get install openssl**

Con este comando se instala el servicio de openssl.

### *4.2* Comandos básicos en OpenSSL

El objetivo de este punto es conocer los comandos básicos de OpenSSL para construir una infraestructura de clave pública.

***4.2.1*** Abra una terminal de shell, cree una carpeta con el nombre de OpenSSL_iniciales, en el directorio openssl.

**NOTA: *iniciales* se sustituirá por el conjunto representativo de letras que decida el equipo**

**redes@debian:/home/redes# cd openssl**
**redes@debian:/home/redes/openssl# mkdir OpenSSL_iniciales**

***4.2.2*** Cambie de directorio a **OpenSSLiniciales**, el cual será el directorio de trabajo.

**redes@debian:/home/redes/openssl# cd OpenSSL_iniciales**

***4.2.3*** Ejecute el siguiente comando:

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl version**

***I. Anote la versión instalada en el equipo asignado.***

_____
_____
_____

***4.2.4*** Cree un archivo de texto sin contenido alguno (Figura No. 4)

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# touch nombre_archivo.txt**

***4.2.5*** Aplique las siguientes funciones hash a un archivo de texto creado en la carpeta de trabajo, y anote el resultado en las siguientes líneas (Figura No. 4).

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl md5 nombre_archivo.txt**

***II. ¿Qué representa la salida del comando anterior?***

_____
_____
_____

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl sha1 nombre_archivo.txt**

***III. ¿Qué representa la salida del comando anterior?***

_____
_____
_____

***IV. ¿Qué diferencias hay al ejecutar el comando con SHA1 y MD5?***

_____
_____
_____

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl sha1 –out hash.bin nombre_archivo.txt**

***V. ¿Cuál es la diferencia que existe entre el comando* openssl sha1 nombre_archivo.txt *y el anterior?***

_____
_____
_____

```
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab# touch hola.txt
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab# openssl md5 hola.txt
MD5(hola.txt)= d41d8cd98f00b204e9800998ecf8427e
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab# openssl sha1 hola.txt
SHA1(hola.txt)= da39a3ee5e6b4b0d3255bfef95601890afd80709
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab# openssl sha1 -out hash.bin hola.txt
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab#
```

**Figura No. 4 Aplicación de las funciones hash**

OpenSSL cuenta con librerías que permiten el cifrado de archivos, con diferentes algoritmos.

***4.2.6*** Cree otro archivo con nombre entrada.txt y teclee algunos datos (Figura No. 5)

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# nano entrada.txt**

***4.2.7*** Posteriormente aplique los siguientes comandos (Figura No. 5):

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl enc –des3 –pbkdf2 –in entrada.txt –out cifra_a.bin –pass pass:iniciales**

***VI. ¿Qué fue lo que realizó con el comando anterior?***

_____
_____
_____

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl enc –des-ede3-cbc –pbkdf2 –in cifra_a.bin –out descifradoa3des.txt**

***VII. ¿Qué fue lo que realizó con el comando anterior?***

_____
_____
_____

```
root@DEBIAN2023:/home/redes# nano entrada.txt
root@DEBIAN2023:/home/redes# openssl enc -des3 -pbkdf2 -in entrada.txt -out cifr
a_a.bin -pass pass:lab
root@DEBIAN2023:/home/redes# openssl enc -des-ede3-cbc -pbkdf2 -in cifra_a.bin -
out descifradoa3des.txt
enter des-ede3-cbc encryption password:
Verifying - enter des-ede3-cbc encryption password:
root@DEBIAN2023:/home/redes#
```

**Figura No. 5 Ejecución de comandos**

### *4.3* Creación de una AC, Autoridad Certificadora

Una AC (Autoridad Certificadora - Certification Authority) es una organización confiable que recibe solicitudes de certificados de entidades, las valida, genera certificados y mantiene la información de su estado.

Entre las principales tareas de una AC encontramos:

- Admisión de certificados.
- Autenticación del sujeto.
- Generación de certificados.
- Distribución de certificados.
- Anulación de certificados.
- Almacenes de datos.

Los certificados digitales proporcionan un mecanismo criptográfico para implementar la autenticación, siendo seguro y escalable para distribuir claves públicas en comunidades grandes.

Para crear un certificado digital en primera instancia se debe realizar una solicitud de certificado a una AC que respalde la información del certificado solicitado. Algunas AC reconocidas son VerigSign, Visa, etcétera, éstas previo pago devuelven certificados firmados por ellas. Para sustituir a dichas AC se creará una propia para firmar los certificados que se generen.

***4.3.1*** Estando en el directorio de trabajo teclee el siguiente comando. (ver Figura 1.1)

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl req −x509 −newkey rsa:2048 −keyout cakey.pem −days 365 −out cacert.pem**

El comando anterior crea una AC para certificados X509 con algoritmo de cifrado RSA de 2048 bytes. La opción –keyout permite que la clave privada de la AC se almacene en el archivo cakey.pem y la clave pública –out en el cacert.pem.

El formato de certificados X.509, es un estándar del ITU-T, (Internacional Telecommunication - Union-Telecommunication Standarization Sector) y el ISO/IEC (Internacional Standards Organization-International Electrotechnical Commission) publicado en 1988.

***4.3.2*** Seguidamente se solicita una frase password para la AC, introduzca la palabra: **.r3d3s.** y confirme la frase.

***4.3.3*** En el país introduzca el código identificador MX.

***4.3.4*** El siguiente campo solicita el estado o provincia, introduzca Distrito Federal.

***4.3.5*** En el nombre de la localización que solicita introduzca Lab Redes y Seguridad.

***4.3.6*** En el nombre de la organización introduzca UNAM.

***4.3.7*** En la unidad organizacional introduzca FI.

***4.3.8*** En el campo del nombre común introduzca su primer nombre y apellido.

***4.3.9*** Finalmente proporcione su correo electrónico (Figura No. 6).

```
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab# openssl req -x509 -newkey rsa:2048
-keyout cakey.pem -days 365 -out cacert.pem
Generating a RSA private key
.....................................................................................
.....................+++++
.....................................................................................
.....................................................................................
.....................................................................................
.....................................................................+++++
writing new private key to 'cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:MX
State or Province Name (full name) [Some-State]:CDMX
Locality Name (eg, city) []:Lab
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LAR
Organizational Unit Name (eg, section) []:LAR
Common Name (e.g. server FQDN or YOUR name) []:LabRyS
Email Address []:lab.redyseguridad@gmail.com
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab#
```

**Figura No. 6. Creación de la Autoridad Certificadora**

Hasta este punto se ha creado la AC que validará los certificados que se generen durante la práctica.

***4.3.10*** Verifique que los archivos que contienen el certificado de la AC y su clave se han creado en el directorio actual, esto a través de los siguientes comandos:

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# cat cakey.pem**
**redes@debian:/home/redes/openssl/OpenSSL_iniciales# cat cacert.pem**

***VIII. Investigue en qué consiste el formato pem.***

_____
_____
_____

### *4.4* Petición y Generación de certificados

Es posible obtener un certificado digital a través de dos formas:

a) Petición on-line, en este tipo regularmente se solicitan certificados personales, para lo cual se requiere de llenar un formulario, enviar alguna documentación y esperar el certificado firmado por la AC.
b) Petición postal, resulta óptimo para la obtención de certificados de servidor, siendo una combinación ya que el CSR (Solicitud de Firma de Certificado - Certificate Sign Request) se envía por correo y la documentación se hace llegar por correo.

Un CSR es un archivo que incluye la información necesaria para solicitar un certificado digital.

El objetivo de este punto es generar un CSR después de crear la AC en el punto anterior.

***4.4.1*** El primer paso para la generación de un certificado digital es la creación de la clave privada del mismo. Teclee el siguiente comando que crea una clave privada con un algoritmo de cifrado RSA de 2048 bytes y se almacena en el archivo priv.pem, con la opción –passout pass: en la cual le indicará la frase privada para la clave privada. (ver Figura No. 8)

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl genrsa –aes256 –out priv.pem –passout pass:clave 2048**

**NOTA : clave se sustituye por la clave privada que desee el equipo, puede ser una frase o una palabra.**

```
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab# openssl genrsa -aes256 -out priv.pe
m -passout pass:clave 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................+++++
.....................................+++++
e is 65537 (0x010001)
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab#
```

**Figura No. 8. Creación de la clave privada del certificado**

***4.4.2*** Verifique que el archivo priv.pem se haya creado en su home e identifique en su contenido los encabezados.

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# cat priv.pem**

***4.4.3*** El segundo paso es realizar una CSR donde se define el propietario del mismo. El siguiente comando hace una petición con el parámetro subj en donde especificamos a quién pertenece el certificado dentro de las comillas separadas por la /. Así mismo, se indica la clave privada que será utilizada con el certificado además de la frase password.

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl req –new –subj "/DC=fi-b.unam.mx/OU=LabRedes/CN=fi-b" –key priv.pem –passin pass:clave –out peticion.pem**

***IX. Investigue los argumentos del parámetro subj.***

_____
_____
_____

***X. Indique el nombre del archivo de salida de este comando y el parámetro que lo genera.***

_____
_____
_____

***4.4.4*** Verifique que el archivo peticion.pem se haya creado en el directorio actual.

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# ls**

### *4.5* Firma del certificado digital

Los certificados permiten que un individuo demuestre que es quien dice ser, ya que está en posesión de la clave secreta asociada a su certificado y únicamente son útiles si existe una AC que los valide, pues si uno mismo se certifica no hay garantía de que la identidad que se muestra sea auténtica.

Un administrador de redes debe ser capaz de verificar que un AC ha emitido un certificado y detectar si un certificado no es válido. Para evitar la falsificación de certificados la entidad certificadora después de autenticar la identidad del sujeto, firma digitalmente el certificado.

***4.5.1*** Contando con el archivo de configuración, teclee el siguiente comando que genera el certificado firmado por la AC ya creada.

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl x509 –CA cacert.pem –CAkey cakey.pem –req –in peticion.pem –days 365 –sha1 –CAcreateserial –out servidorcert.pem**

***XII. Investigue el funcionamiento del comando anterior.***

_____
_____

***4.5.2*** La aplicación solicita el password de la AC que firma el certificado, introduzca el password configurado inicialmente (**.r3d3s.**), ver Figura No. 9.

```
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab# openssl x509 -CA cacert.pem -CAkey cakey.pem
-req -in peticion.pem -days 365 -sha1 -CAcreateserial -out servidorcert.pem
Signature ok
subject=DC = fi-b.unam.mx, OU = LabRedes, CN = fi-b
Getting CA Private Key
Enter pass phrase for cakey.pem:
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab#
```

**Figura No. 9. Solicitud de la frase password**

***4.5.3*** Verifique que el certificado se haya creado y analice su contenido. (ver Figura No. 10)

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# ls**
**redes@debian:/home/redes/openssl/OpenSSL_iniciales# cat servidorcert.pem**

```
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab# cat servidorcert.pem
-----BEGIN CERTIFICATE-----
MIIDSzCCAjMCFB7dhH+pal/34hbG25Vg2qIKl50fMA0GCSqGSIb3DQEBBQUAMIGD
MQswCQYDVQQGEwJNWDENMAsGA1UECAwEQ0RNWDEMMAoGA1UEBwwDTGFiMQwwCgYD
VQQKDANMQVIxDDAKBgNVBAsMA0xBUjEPMA0GA1UEAwwGTGFiUnlTMSowKAYJKoZI
hvcNAQkBFhtsYWIucmVkeXNlZ3VyaWRhZEBnbWFpbC5jb20wHhcNMjMwNjE2MjIx
OTUxWhcNMjQwNjE1MjIxOTUxWjBAMRwwGgYKCZImiZPyLGQBGRYMZmktYi51bmFt
Lm14MREwDwYDVQQLDAhMYWJSZWRlczENMAsGA1UEAwwEZmktYjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMdY6suBacM312SCf4kH890eAShLTX3d1/nY
Cf0sZPr4HAcDvQUJnnFKMbRGZmmlDU8jt8SQGyTLBZiDm9BnlKDJd07PaI6lm7ar
mIUkkuccOR08Sf1U3bD2aN7lpOB9sXiQozoXVntAB6cA3ysvYG9ZWhJgtTAnoKof
4VyFJk6r15qbNgFDN8tuSiWuxdEJkna7CwaFWdN3nerTpzAa/qip1+Dr6OXkr9fD
6sgXVwve9IL5sRF5QpJiXIkaHnSMg2LPq8UwSasSRPcGhZkPYLKiJIetimGFa25V
v5kFkiVgMPwwcnZE+2w1QJ0k3Lx1VOcDcge16acX2lGszICPWXUCAwEAATANBgkq
hkiG9w0BAQUFAAOCAQEAN6ojCnVwKMxvGG4Md2tiAW3XKBSeRF+6hALHnT2upqjb
8NMXfq31OT4atakmJ8Pwzkoq8WFBDD6YldoIQ0iGYTltYvGSDrbChskbwyqJLHYj
7oOr4nj0/xhFIHBScHf/8LVrClB181eki2ex6IV5v0pfQoqCiiac+TIODFanAozl
MkAHQKCaiPXaS+Og7jcUnYA341Ij/o8ekIbZVdXPzfdnfp44/JSolyCiJqSIDktg
cfWwKJvNEL4DRARZgouoGGpixkDWnez9SUcP0jR1zFJTKJq42lJZ7aLw+kfkYhfw
07M22L7Z2XuVZ+TrEm/8PSdJh0a8fRLlbN6Zw9uBMg==
-----END CERTIFICATE-----
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab#
```

**Figura No. 10. Contenido del certificado creado**

Hasta este punto se ha creado un certificado que puede ser empleado para implementar un servidor que permita dar soporte a sitios Web certificados bajo SSL, Capa de Socket Seguros (Secure Socket Layer) en servidores Apache, por ejemplo.

***4.5.4*** Ejecute el siguiente comando que permite obtener información sobre el certificado recién creado (ver Figura No. 11).

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl x509 –in servidorcert.pem –text –noout**

```
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab# cat servidorcert.pem
-----BEGIN CERTIFICATE-----
MIIDSzCCAjMCFB7dhH+pal/34hbG25Vg2qIKl50fMA0GCSqGSIb3DQEBBQUAMIGD
MQswCQYDVQQGEwJNWDENMAsGA1UECAwEQ0RNWDEMMAoGA1UEBwwDTGFiMQwwCgYD
VQQKDANMQVIxDDAKBgNVBAsMA0xBUjEPMA0GA1UEAwwGTGFiUnlTMSowKAYJKoZI
hvcNAQkBFhtsYWIucmVkeXNlZ3VyaWRhZEBnbWFpbC5jb20wHhcNMjMwNjE2MjIx
OTUxWhcNMjQwNjE1MjIxOTUxWjBAMRwwGgYKCZImiZPyLGQBGRYMZmktYi51bmFt
Lm14MREwDwYDVQQLDAhMYWJSZWRlczENMAsGA1UEAwwEZmktYjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMdY6suBacM312SCf4kH890eAShLTX3d1/nY
Cf0sZPr4HAcDvQUJnnFKMbRGZmmlDU8jt8SQGyTLBZiDm9BnlKDJd07PaI6lm7ar
mIUkkuccOR08Sf1U3bD2aN7lpOB9sXiQozoXVntAB6cA3ysvYG9ZWhJgtTAnoKof
4VyFJk6r15qbNgFDN8tuSiWuxdEJkna7CwaFWdN3nerTpzAa/qip1+Dr6OXkr9fD
6sgXVwve9IL5sRF5QpJiXIkaHnSMg2LPq8UwSasSRPcGhZkPYLKiJIetimGFa25V
v5kFkiVgMPwwcnZE+2w1QJ0k3Lx1VOcDcge16acX2lGszICPWXUCAwEAATANBgkq
hkiG9w0BAQUFAAOCAQEAN6ojCnVwKMxvGG4Md2tiAW3XKBSeRF+6hALHnT2upqjb
8NMXfq31OT4atakmJ8Pwzkoq8WFBDD6YldoIQ0iGYTltYvGSDrbChskbwyqJLHYj
7oOr4nj0/xhFIHBScHf/8LVrClB181eki2ex6IV5v0pfQoqCiiac+TIODFanAozl
MkAHQKCaiPXaS+Og7jcUnYA341Ij/o8ekIbZVdXPzfdnfp44/JSolyCiJqSIDktg
cfWwKJvNEL4DRARZgouoGGpixkDWnez9SUcP0jR1zFJTKJq42lJZ7aLw+kfkYhfw
07M22L7Z2XuVZ+TrEm/8PSdJh0a8fRLlbN6Zw9uBMg==
-----END CERTIFICATE-----
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab#
```

**Figura No. 11. Información del certificado creado**

***XIII. Indique la información proporcionada por el comando anterior.***

_____

_____

_____

### *4.6* CRL, Listas de Anulación de Certificados

Los certificados tienen un periodo de validez, durante el cual la AC debe mantener la información de las entidades. Entre los datos más importantes que deben ser actualizados se encuentra el estado de anulación del certificado, el cual indica que el periodo de validez ha terminado antes de tiempo y el sistema que lo emplee no debe confiar en él.

***XIV. Investigue las razones por las cuales un certificado ya no es válido.***

_____
_____
_____

Las CRL (Listas de Anulación de Certificados - Certification Revocation List) son un mecanismo a través del cual la AC da a conocer y distribuye la información acerca de los certificados anulados a las aplicaciones que los emplean. Estas estructuras de datos firmadas por la AC contienen su fecha y hora de publicación, el nombre de la entidad certificadora y los números de series de los certificados anulados que aún no han expirado.

Un administrador de redes debe obtener la última CRL de la entidad que firma el certificado que emplean sus aplicaciones y verificar que los números de series de sus certificados no estén incluidos en tal lista.

***XV. Mencione 2 métodos de actualización de CRL.***

_____
_____
_____

El objetivo de este punto es manipular el archivo de configuración de OpenSSL así como los comandos que permiten revocar certificados y generar listas de revocaciones.

***4.6.1*** Modifique el archivo de configuración openssl.cnf

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# nano /etc/ssl/openssl.cnf**

y reemplace la línea ***dir=./demoCA*** por ***dir=.***

**NOTA: Existen dos dir=./demoCA, uno en [CA default] y otro en [tsa_config1]**

***4.6.2*** En el mismo archivo del punto anterior, coloque un signo # para comentar las siguientes líneas:

**# unique_subject = no**
**# crlnumber = $dir/crlnumber**

***4.6.3*** Cree un archivo de nombre index.txt en el directorio de trabajo.

**Redes:OpenSSL_iniciales# touch index.txt**

***4.6.4*** Revoque el certificado creado mediante el siguiente comando. (ver Figura No. 12)

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl ca –keyfile cakey.pem –cert cacert.pem -revoke servidorcert.pem**

```
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab# openssl ca -keyfile cakey.pem -cert
cacert.pem -revoke servidorcert.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for cakey.pem:
Adding Entry with serial number 1EDD847FA96A5FF7E216C6DB9560DAA20A979D1F to DB for /D
C=fi-b.unam.mx/OU=LabRedes/CN=fi-b
Revoking Certificate 1EDD847FA96A5FF7E216C6DB9560DAA20A979D1F.
Data Base Updated
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab#
```

**Figura No. 12. Revocando un certificado**

Esta operación no modifica el certificado, simplemente actualiza el contenido del archivo de la base de datos index.txt.

***XVI. Describa el contenido de dicho archivo.***

_____
_____
_____

**NOTA: La revocación de un certificado no es conocida hasta la publicación de la CRL.**

***4.6.5*** Genere una CRL a través del siguiente comando introduciendo la frase password de la clave privada de la AC (**.r3d3s.**) (ver Figura No. 13).

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl ca –gencrl –keyfile cakey.pem –cert cacert.pem –out ejemplo.crl**

```
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab# openssl ca -keyfile cakey.pem -cert
cacert.pem -revoke servidorcert.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for cakey.pem:
Adding Entry with serial number 1EDD847FA96A5FF7E216C6DB9560DAA20A979D1F to DB for /D
C=fi-b.unam.mx/OU=LabRedes/CN=fi-b
Revoking Certificate 1EDD847FA96A5FF7E216C6DB9560DAA20A979D1F.
Data Base Updated
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab# openssl ca -gencrl -keyfile cakey.pe
m -cert cacert.pem -out ejemplo.crl
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for cakey.pem:
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab#
```

**Figura No. 13. Creación de una CRL, Lista de Revocación de Certificados**

***4.6.6*** Visualice el contenido del archivo creado en el punto anterior (Figura No. 14).

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# cat ejemplo.crl**

```
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab# cat ejemplo.crl
-----BEGIN X509 CRL-----
MIIB8zCB3DANBgkqhkiG9w0BAQsFADCBgzELMAkGA1UEBhMCTVgxDTALBgNVBAgM
BENETVgxDDAKBgNVBAcMA0xhYjEMMAoGA1UECgwDTEFSMQwwCgYDVQQLDANMQVIx
DzANBgNVBAMMBkxhYlJ5UzEqMCgGCSqGSIb3DQEJARYbbGFiLnJlZHlzZWd1cmlk
YWRAZ21haWwuY29tFw0yMzA2MTYyMjQ3MzhaFw0yMzA3MTYyMjQ3MzhaMCcwJQIU
Ht2Ef6lqX/fiFsbblWDaogqXnR8XDTIzMDYxNjIyNDUzOFowDQYJKoZIhvcNAQEL
BQADggEBABZvcfox2lPHe1xX9/l9JCFUaRHypS+gzEpoQWv7Nc1zunuVERk32SMd
YANwqNbrTd74T6sHQIWpkWb18uO2IA4ru+9J0XYe7yony3NrEjiZmPuDOLG0XI+H
kex0OmCxS+EVuXzzWIAdE8ScDZUxtWOuIOqbbOqaxFvRrIuxPqAmbkOSePuqqLcB
6yIIsS+hoAwOWDdlz7+xFLiI56Q70xsG1Fp39TqZ6UxUC5qjGAgZku0AILuwRRGa
fMuPonzjFk70EGNJFIYXJDMAsWgV6JS4YtjpTYMoe/yv8QkWSmPUPUi/c2hBB3gj
QSgVkJj/3bY9FFXmZFdMXcylBOv0oHU=
-----END X509 CRL-----
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab#
```

**Figura No.14 Contenido del ejemplo ejemplo.crl**

***4.6.7*** Para obtener información acerca de la lista de revocación de certificados, ejecute el siguiente comando y observe que la salida debe ser similar a la Figura No. 15.

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl crl –in ejemplo.crl –text –noout**

```
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab# openssl crl -in ejemplo.crl -text
-noout
Certificate Revocation List (CRL):
        Version 1 (0x0)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = MX, ST = CDMX, L = Lab, O = LAR, OU = LAR, CN = LabRyS, emailAd
dress = lab.redyseguridad@gmail.com
        Last Update: Jun 16 22:47:38 2023 GMT
        Next Update: Jul 16 22:47:38 2023 GMT
Revoked Certificates:
    Serial Number: 1EDD847FA96A5FF7E216C6DB9560DAA20A979D1F
        Revocation Date: Jun 16 22:45:38 2023 GMT
    Signature Algorithm: sha256WithRSAEncryption
         16:6f:71:fa:31:da:53:c7:7b:5c:57:f7:f9:7d:24:21:54:69:
         11:f2:a5:2f:a0:cc:4a:68:41:6b:fb:35:cd:73:ba:7b:95:11:
         19:37:d9:23:1d:60:03:70:a8:d6:eb:4d:de:f8:4f:ab:07:40:
         85:a9:91:66:f5:f2:e3:b6:20:0e:2b:bb:ef:49:d1:76:1e:ef:
         2a:27:cb:73:6b:12:38:99:98:fb:83:38:b1:b4:5c:8f:87:91:
         ec:74:3a:60:b1:4b:e1:15:b9:7c:f3:58:80:1d:13:c4:9c:0d:
         95:31:b5:63:ae:20:ea:9b:6c:ea:9a:c4:5b:d1:ac:8b:b1:3e:
         a0:26:6e:43:92:78:fb:aa:a8:b7:01:eb:22:08:b1:2f:a1:a0:
         0c:0e:58:37:65:cf:bf:b1:14:b8:88:e7:a4:3b:d3:1b:06:d4:
         5a:77:f5:3a:99:e9:4c:54:0b:9a:a3:18:08:19:92:ed:00:20:
         bb:b0:45:11:9a:7c:cb:8f:a2:7c:e3:16:4e:f4:10:63:49:14:
         86:17:24:33:00:b1:68:15:e8:94:b8:62:d8:e9:4d:83:28:7b:
         fc:af:f1:09:16:4a:63:d4:3d:48:bf:73:68:41:07:78:23:41:
         28:15:90:98:ff:dd:b6:3d:14:55:e6:64:57:4c:5d:cc:a5:04:
         eb:f4:a0:75
root@DEBIAN2023:/home/redes/openssl/OpenSSL_lab#
```

**Figura No. 15. Contenido de una CRL, Lista de Revocación de Certificados**

***XVII. Indique qué significa la salida del comando anterior***

_____
_____
_____

En este momento el certificado creado ha sido revocado. El profesor o la profesora indicará cual es el procedimiento para que los usuarios revisen la validez de los certificados.

***5. Conclusiones***

_____
_____
_____
_____
_____

**PRÁCTICA 11**

**Mecanismos de Seguridad, Certificados Digitales**

***Cuestionario Previo***

1. Investigue en al menos 3 aplicaciones de los certificados digitales.
2. Investigue al menos 2 herramientas adicionales que permitan la administración de certificados.
3. Describa brevemente el funcionamiento básico de un certificado digital.
4. Investigue en qué consiste el estándar ISO 27002.
5. Investigue qué es una CPS (Declaración de Prácticas de Certificación - Certification Practice Statement) dentro de una AC (Autoridad Certificadora).
6. Investigue los elementos del formato de un certificado X.509

# Anexo

# Manual para la creación de una cuenta en Skills for All para descargar y emplear Cisco Packet Tracer

## 1. *Objetivo*

El alumno o la alumna realizará el proceso correspondiente para la creación de una cuenta personal en el software Cisco Packet Tracer.

## 2. *Instrucciones*

Lea detenidamente y siga cada uno de los pasos que se describen a continuación para obtener su cuenta personal.

Es importante que cada estudiante obtenga su cuenta para emplear Cisco Packet Tracer, en caso contrario NO podrá realizar las prácticas de la asignatura.

**a) Proceso para la obtención de cuenta personal.**

2.1 Para realizar la instalación de Cisco Packet Tracer, ingrese al siguiente sitio:

https://prelogin-authoring.netacad.com/es/courses/packet-tracer

El sitio debe de tener una vista similar a la de la Figura No. 1, busque y dé clic en el curso *Getting Started with Cisco Packet Tracer.*

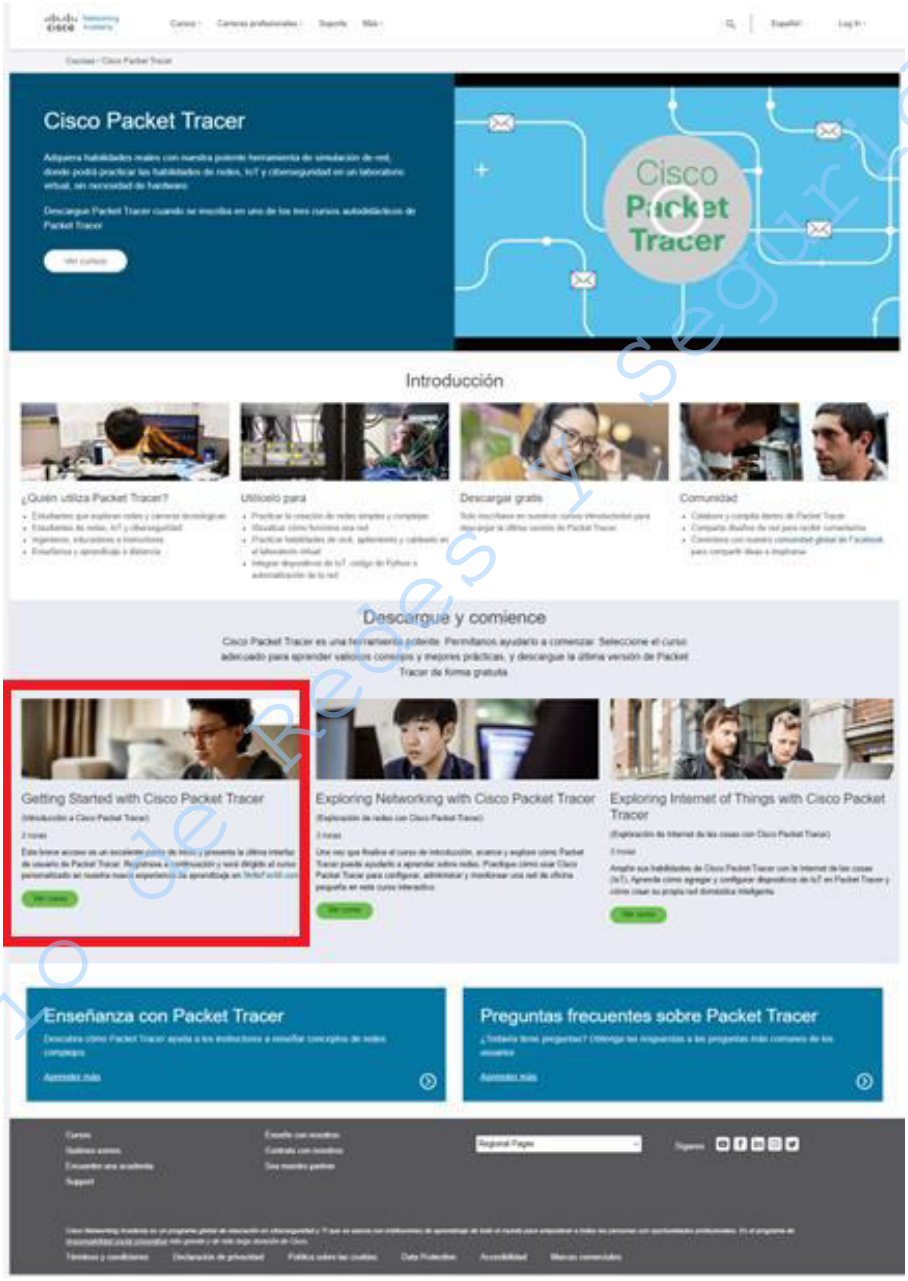



Figura No. 1. Sitio NETACAD

2.2 Al dar clic aparecerá una ventana emergente indicando que se le redireccionará a un nuevo sitio (Figura No. 2).

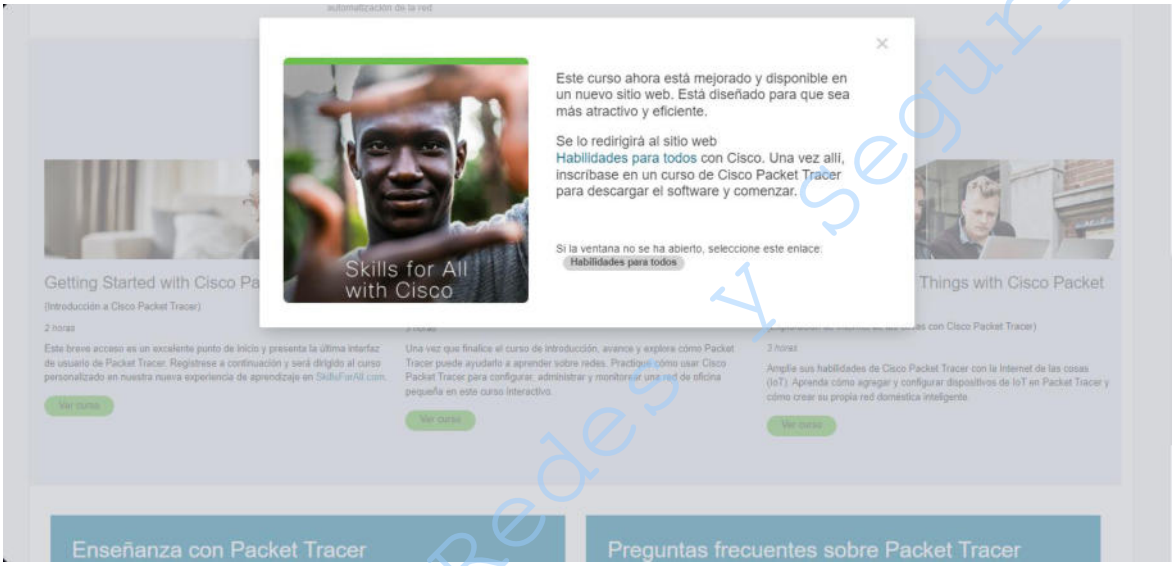



Figura No. 2. Ventana emergente

2.3 Una vez dentro del sitio *Skills for All*, seleccione el idioma de su preferencia y dé clic en *Comenzar* (Figura No. 3).

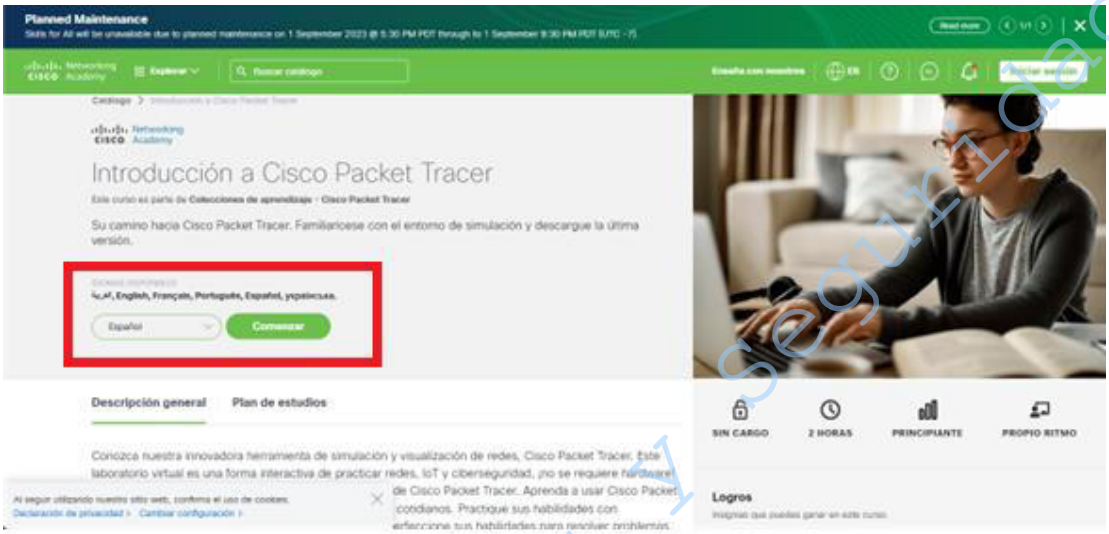



Figura No. 3. Selección de idioma

2.4 Si tiene una cuenta inicie sesión, de lo contrario dé clic en *Crear cuenta* (Figura No. 4).

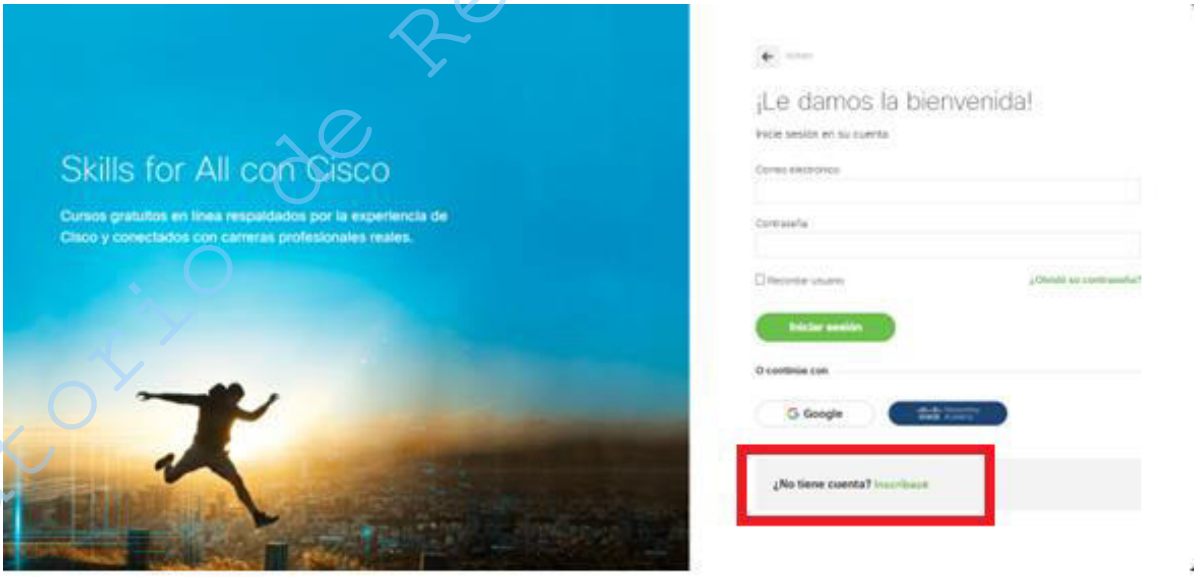



Figura No. 4. Creación de cuenta

2.5 Complete los campos con la información que se le pide, seleccionando la opción que mejor se adapte a su caso (Figura No. 5).

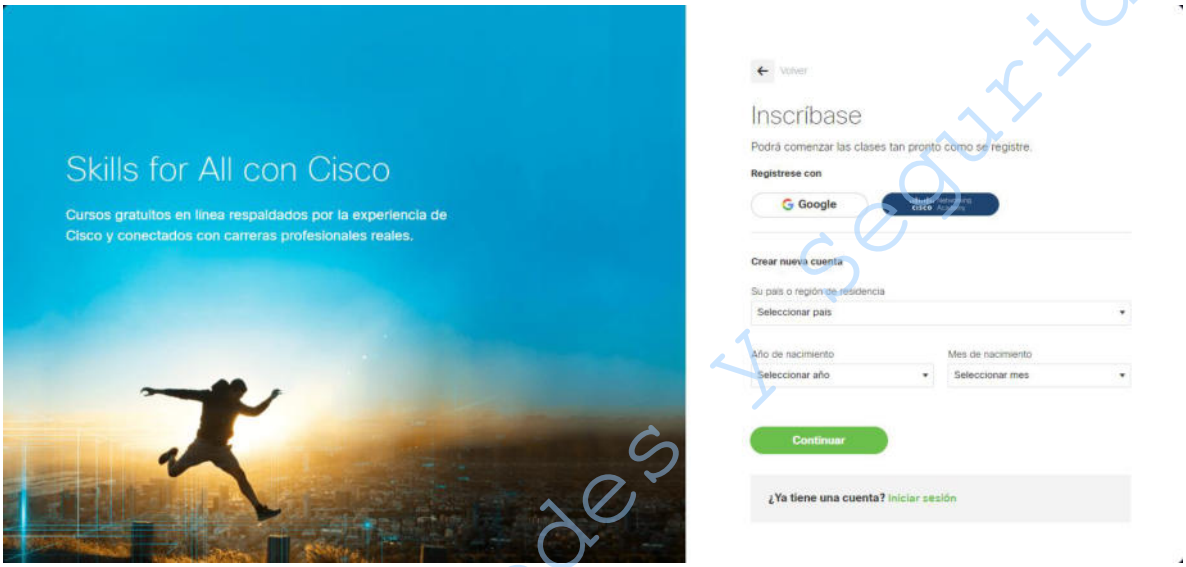



Figura No. 5. Datos del usuario

2.6 Una vez completado, se aceptan términos y condiciones (Figura No. 6).

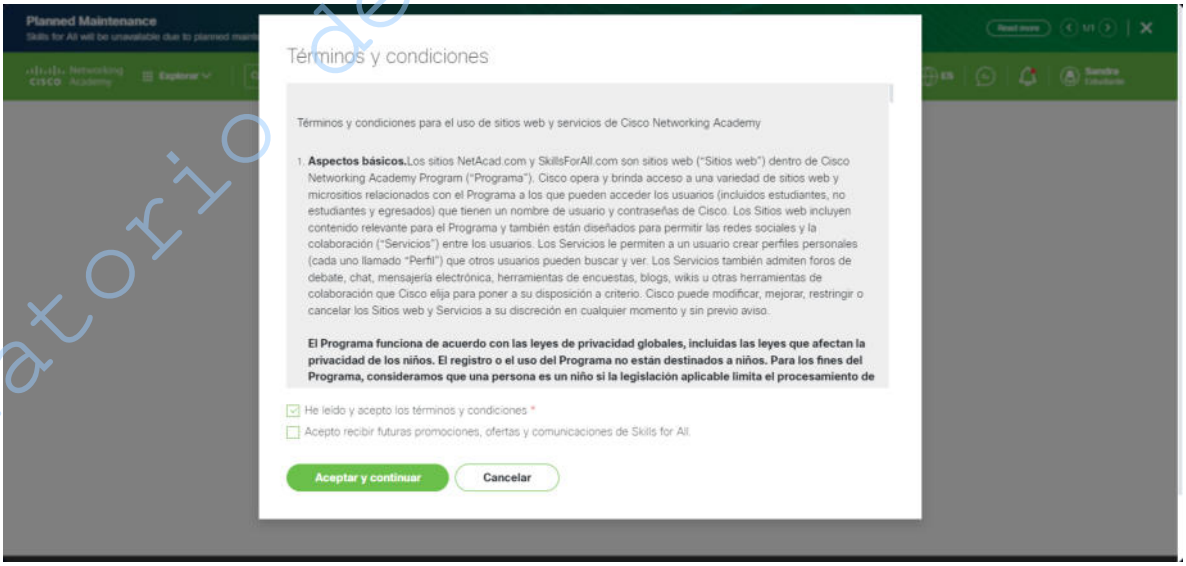



Figura No. 6. Términos y condiciones

2.7 Al finalizar el procedimiento de registro se accede al sitio donde se encuentra el curso, en el primer módulo, en el apartado *1.0.3 Descargue Cisco Packet Tracer* se encuentra el enlace al sitio de descarga (Figura No. 7).

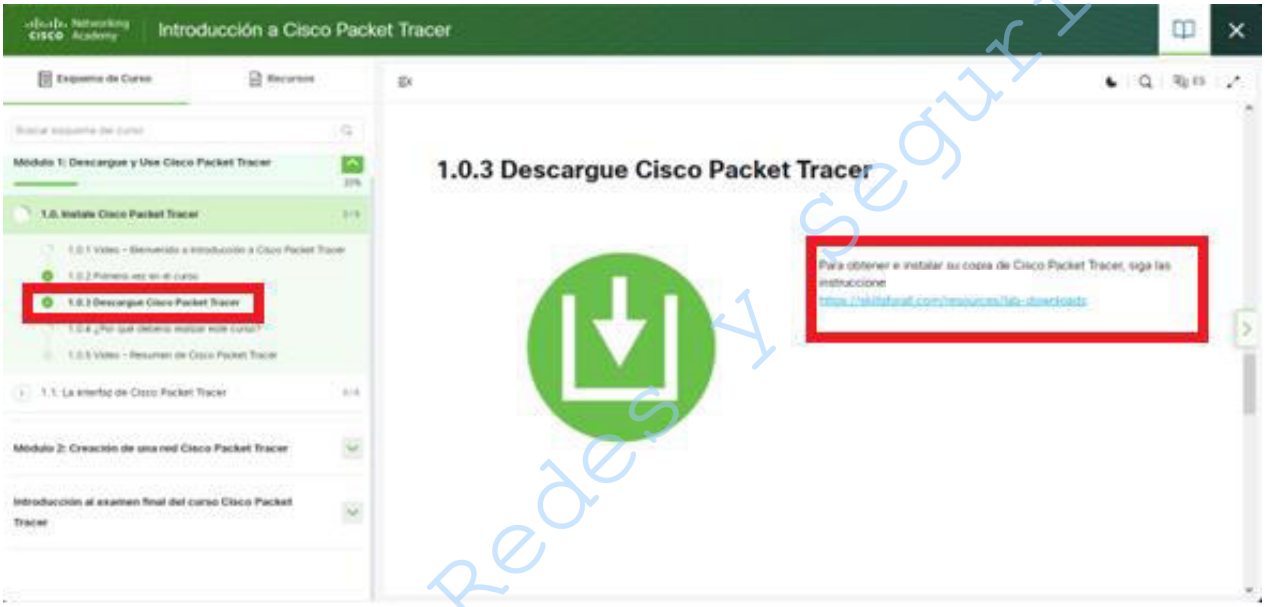



Figura No. 7. Enlace de descarga

2.8 Dé clic en el enlace y lo redireccionará a un nuevo sitio donde se encuentran los pasos a seguir para realizar la descarga e instalación del programa (Figura No. 8).

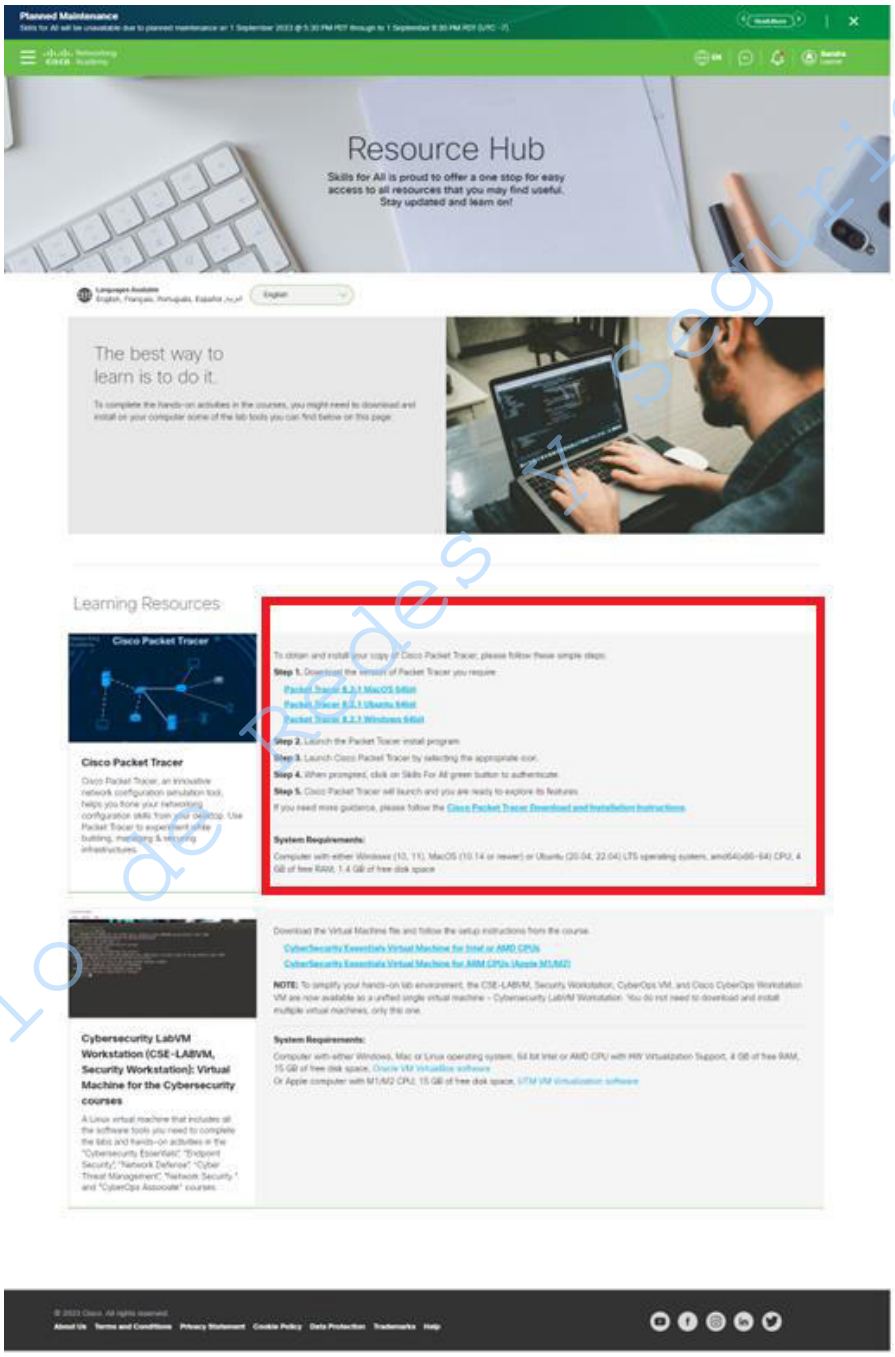



Figura No. 8. Instalación

**b) Proceso para la utilización de Cisco Packet Tracer**

2.1 Al ejecutar la aplicación Cisco Packet Tracer aparecerá la Figura No. 9, debe seleccionar la opción Skills for All

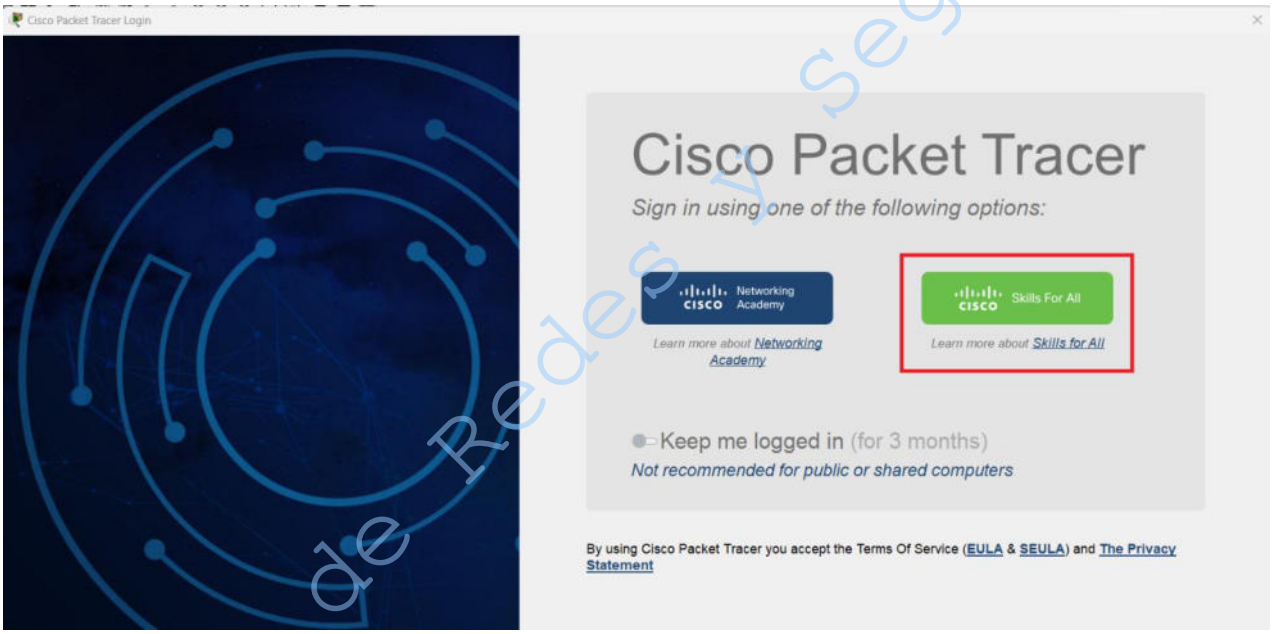



Figura No. 9. Cisco Packet Tracer

2.2 Será dirigido a la página que se observa en la Figura No. 10, en ella deberá ingresar su correo electrónico y contraseña correspondientes a la cuenta creada.

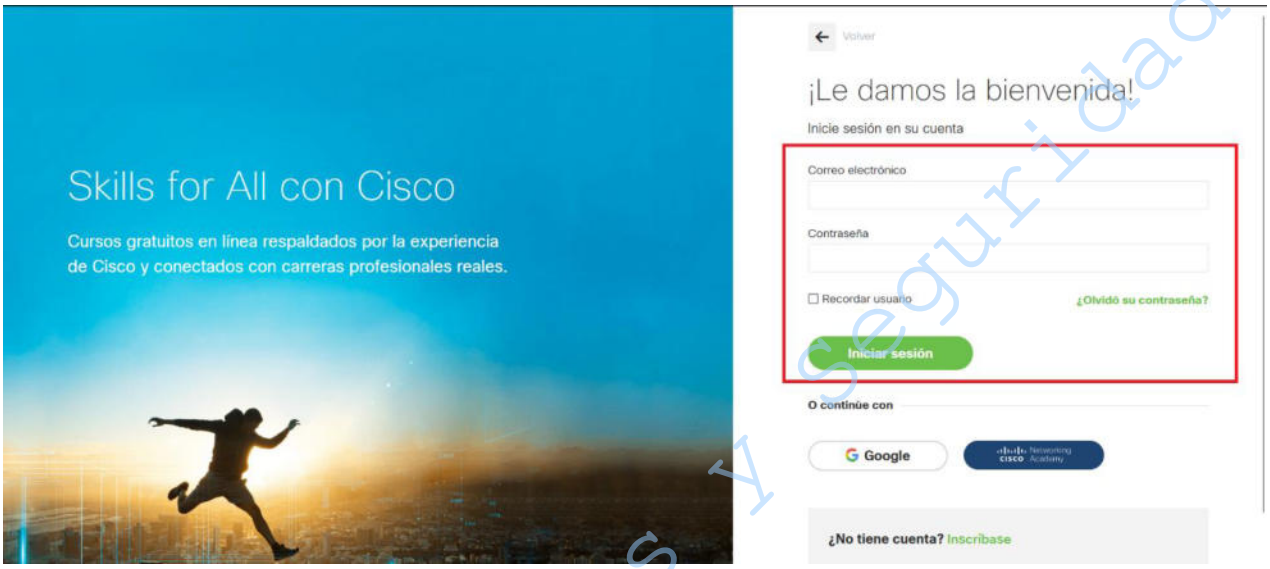



Figura No. 9. Cuenta en Cisco Packet Tracer

2.3 Al ingresar la información del paso anterior visualizará la Figura No 11, podrá cerrar dicha pestaña y comenzar a trabajar en la aplicación Cisco Packet Tracer (Figura No. 12).

---

You have successfully logged in to Cisco Packet Tracer. You may close this tab.

Figura No. 11. Acceso correcto a Cisco Packet Tracer

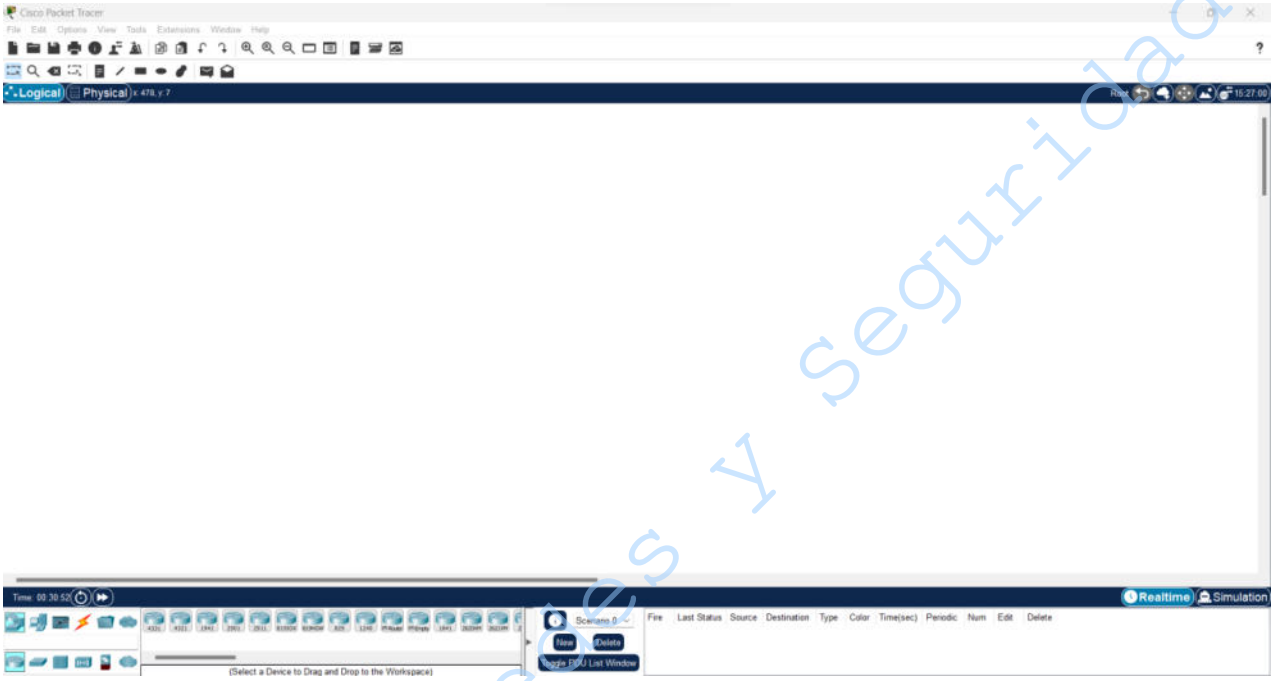



Figura No. 12. Aplicación Cisco Packet Tracer