	Carátula para entrega de prácticas	Código	FODO-42
		Versión	01
		Página	1/1
		Sección ISO	
		Fecha de emisión	04 de agosto de 2015
Secretaría/División: División de Ingeniería Eléctrica		Área/Departamento: Laboratorio de Redes y Seguridad	

Laboratorio de Redes y Seguridad

Profesor: _____

Asignatura: _____

Grupo: _____

No de Práctica(s): _____

Integrante(s): _____

_____

_____

Semestre: _____

Fecha de entrega: _____

Observaciones: _____

_____

CALIFICACIÓN:_____

PRÁCTICA ADICIONAL

Redes Privadas Virtuales (VPN)

1.- Objetivos de Aprendizaje

- El alumno será capaz de configurar una red privada virtual empleando el software Cisco Packet Tracer.

2.- Conceptos teóricos

Una VPN o Red Privada Virtual es una tecnología que permite la extensión de una red pública como Internet a un espacio de red local.

En la informática una Red Privada Virtual (RPV) o Virtual Private Network (VPN) supone una tecnología de red que, por razones de costo y comodidad, brinda la posibilidad de conectarse a una red pública generando una extensión a nivel de área local. Este tipo de redes se utilizan a la hora de conectar dos o más oficinas de una empresa a través de Internet. Esto facilita la conexión y el intercambio a un bajo costo económico, y permite que miembros de un mismo equipo se conecten entre sí desde locaciones remotas.

Las VPN funcionan de manera tal que, si bien se utiliza una red pública como es la de conexión a Internet, los datos son transmitidos por un canal privado, de forma que no peligra la seguridad ni la integridad de la información interna. Los datos son cifrados y descifrados alternativamente, ahorrando dinero y problemas a empresas de distinta escala.

Si se tiene en cuenta el costo que supondría conectar dos oficinas en dos países distintos, las VPN son una excelente alternativa que se vale de una tecnología ya existente de redes interconectadas para crear una red más pequeña y privada.

En esta forma de comunicación, se hace uso de una Banda Ancha dada por un proveedor en común que actúa como una especie de Servidor principal, en la que solo los Clientes autorizados pueden tener acceso a los privilegios y servicios que allí se proveen, teniendo una estructura que le permite estar incluida dentro de una Red Pública, dada su semejanza en diseño y arquitectura.

Existen tres tipos fundamentales a la hora de establecer una Red Privada Virtual (VPN):

a) **VPN de Acceso Remoto:** En las redes empresariales es el más utilizado, teniendo como punto principal un Proveedor que se conecta a una red perteneciente a la compañía desde otros puntos lejanos, que pueden ser desde Hoteles, Aviones exclusivos, Oficinas Comerciales, Sucursales, etc. utilizando como sustento la de red pública que está a mayor disponibilidad, esto es, una conexión a Internet.
En esta ocasión, la forma de ingresar a esta Red Privada Virtual está dada por la asignación a cada Cliente de una forma de autenticación, que generalmente lleva este acceso la modalidad de Usuario y Contraseña, o bien a través del acceso en primera instancia a una Red de Área Local dentro de la empresa.

b) **VPN de Punto a Punto:** En este caso se utiliza una conexión permanente a Internet para poder establecer un enlace directo de un punto específico (por ejemplo, Oficinas Comerciales) hacia un nodo principal que tendría la base de datos sobre la cual se trabaja, o los servicios de los cuales depende cada cliente (una Sede Central de una compañía)
En este caso las conexiones se efectúan teniendo la conexión local de Internet que permite no solo abaratar costos al no tener que contratar una red exclusiva para poder establecer este vínculo entre Servidor y Cliente de la VPN.

c) **VPN over LAN:** Esta arquitectura de redes es una de las más eficientes para el gestión empresarial de redes, ya que si bien es una variante del VPN de Acceso Remoto, no utiliza como sustento la conexión a Internet, sino que está establecida, como su nombre lo indica, sobre una Red de Área Local (LAN) provista por la compañía. Es muy útil para poder trabajar en distintos sectores dentro de una compañía, sobre todo cuando la información allí tratada no debe ser vista por todos los sectores, o es necesario agregar distintas formas de seguridad cuando se traten de datos sensibles (en lo cual se suele recurrir al Cifrado además de a personal idóneo para el acceso a un sector específico)

3.- Equipo y material necesario

Equipo del Laboratorio:

- Computadoras con sistema operativo Windows 7
- Software Cisco Packet Tracer

4.- Desarrollo:

Modo de trabajar
La práctica se desarrollará en parejas.

***4.1* Configuración de los dispositivos**

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 Vaya a Inicio > Todos los programas > Cisco Packet Tracer Student y ejecute la aplicación Cisco Packet Tracer Student.

4.1.4 Arrastre dos switches 2950-24, 2 PC, 2 routers 2811 al área de trabajo de Packet Tracer y construya la topología de la figura 1, atendiendo las indicaciones de su profesor y considerando lo siguiente:

a) Conecte cada PC con el switch empleando cable directo
b) Conecte cada switch con el router empleando cable directo.
c) Interconecte los routers empleando un cable cruzado. Cada extremo del cable debe conectarse en las interfaces FastEthernet0/1

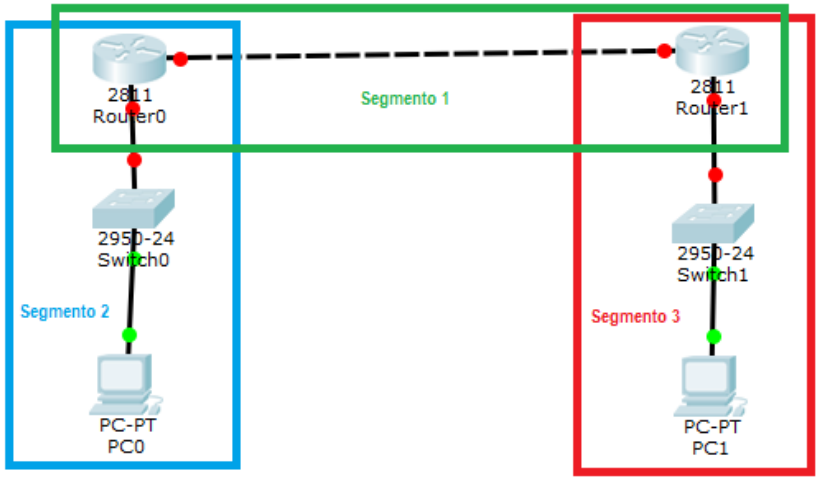

Figura 1. Diagrama

4.1.5 Complete la Tabla 1 con los datos que utilizará para configurar los diferentes dispositivos. Emplee una dirección IP clase C.

Tabla 1. Configuración de dispositivos

	Dirección IP	Máscara	Gateway
Segmento 1			
Segmento 2			
Segmento 3			
PC0			
PC1			
Interfaz Fa0/0 Router0			
Interfaz Fa0/0 Router1			
Interfaz Fa0/1 Router0			
Interfaz Fa0/1 Router1			

4.1.6 Dé clic sobre la PC0 y vaya a la pestaña de Desktop (ver figura 2).

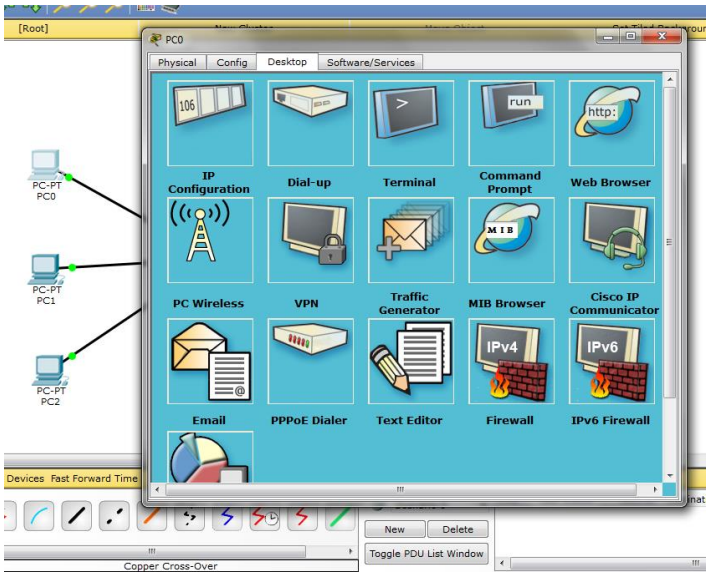

Figura 2. Pestaña de configuración de dispositivo.

4.1.7 Dé clic sobre la opción IP configuration y coloque la dirección IP, máscara de subred y Gateway. Siga las indicaciones dadas por su profesor, tomando los datos de la tabla 1.

4.1.8 Repita los pasos 4.1.6 y 4.1.7 para la PC1.

4.1.9 Haga clic sobre el router0 y seleccione la pestaña CONFIG. Dé clic sobre la interfaz que se encuentra conectada al switch (Fa0/0). Configure la dirección IP y la máscara de subred con base en los datos de la tabla 1. Habilite la opción de encendido (ON) (Figura 3)

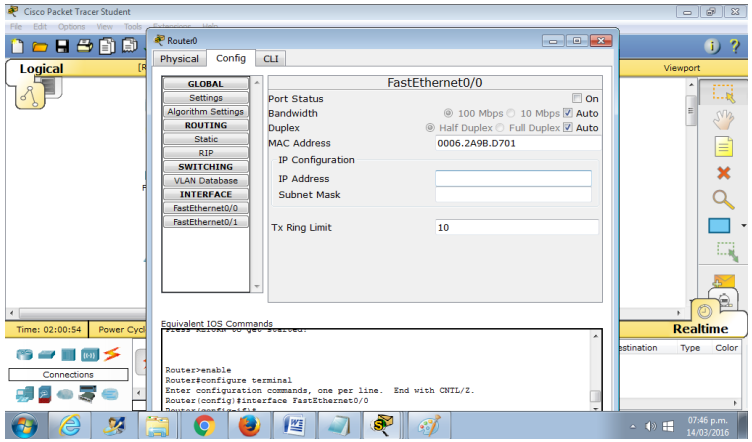

Figura 3. Configuración de las interfaces del router

4.1.10 Repita el paso 4.1.9 para configurar la interfaz que se encuentra conectada con el router1.

4.1.11 Haga clic sobre el router0 y seleccione la pestaña CONFIG y la opción RIP, enseguida deberán añadirse los dos segmentos de red con los que se encuentra conectado directamente dicho router. Para ello se escribe primero una dirección de segmento y se da clic en Add, la segunda dirección se añade de la misma manera. Tomar como base los datos de la tabla 1.

4.1.12 Para configurar al router1 debe repetir los pasos desde el 4.1.9 hasta el 4.1.11.

4.2 Configuración de la VPN

4.2.1 Dar clic sobre el router0 y seleccionar la pestaña CLI.

4.2.2 Teclear los siguientes comandos:

Router(config-router)#exit
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#hash sha
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
Router(config-router)#exit
Router(config)#crypto isakmp key toor address *dirección_IP*

Nota: La dirección_IP se sustituye por la dirección IP de la interfaz Fa0/1 del router1

Router(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac
Router(config)#access-list 101 permit ip *dirección_IPa* 0.0.0.255 *dirección_IPb* 0.0.0.255

Nota: La dirección_IPa se sustituye por la dirección IP del segmento 2 y la dirección_IPb se sustituye por la dirección IP del segmento 3

Router(config)#crypto map CMAP 10 ipsec-isakmp

Router(config-crypto-map)#set peer *dirección_IP*

Nota: La dirección_IP se sustituye por la dirección IP de la interfaz Fa0/1 del router1

Router(config-crypto-map)#match address 101
Router(config-crypto-map)#set transform-set TSET
Router(config-crypto-map)#exit
Router(config)#interface fa0/1
Router(config-if)#crypto map CMAP
Router(config-if)#do wr

Explique para qué sirven los comandos tecleados

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

4.2.3 Dar clic sobre el router1 y seleccionar la pestaña CLI.
4.2.4 Teclear los siguientes comandos:

Router(config-router)#exit
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#hash sha
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
Router(config-router)#exit
Router(config)#crypto isakmp key toor address *dirección_IP*

Nota: La dirección_IP se sustituye por la dirección IP de la interfaz Fa0/1 del router0

Router(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac
Router(config)#access-list 101 permit ip *dirección_IPa* 0.0.0.255 *dirección_IPb* 0.0.0.255

Nota: La dirección_IPa se sustituye por la dirección IP del segmento 3 y la dirección_IPb se sustituye por la dirección IP del segmento 2

Router(config)#crypto map CMAP 10 ipsec-isakmp

Router(config-crypto-map)#set peer *dirección_IP*

Nota: La dirección_IP se sustituye por la dirección IP de la interfaz Fa0/1 del router0

Router(config-crypto-map)#match address 101
Router(config-crypto-map)#set transform-set TSET
Router(config-crypto-map)#exit
Router(config)#interface fa0/1
Router(config-if)#crypto map CMAP
Router(config-if)#do wr

4.2.5 Seleccione el botón Add Simple PDU (P), el cual se representa mediante un sobre cerrado color naranja. Haga clic sobre la PC0 y la PC1 que se encuentran conectadas a los dos switches.

¿La conexión fue exitosa?¿Por qué?

_____
_____
_____
_____
_____
_____
_____
_____

4.2.6 Dar clic sobre el router0 y seleccionar la pestaña CLI.
4.2.7 Teclear los siguientes comandos:

Router>en
Router# show crypto isakmp sa
Router# show crypto ipsec sa

Indique la información que se observa al teclear los comandos e interprétela.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

5.-Cuestionario

1. ¿Por qué es importante realizar y trabajar con VPN?

_____
_____
_____
_____

2. ¿Qué ventajas presenta una VPN?

_____
_____
_____
_____

3. ¿Qué desventajas presenta una VPN?

_____
_____
_____
_____

4. ¿En qué casos se utilizaría una VPN?

_____
_____
_____

6.-Conclusiones

Revise los objetivos planteados al inicio de la práctica y escriba sus conclusiones

PRÁCTICA ADICIONAL

Redes Privadas Virtuales (VPN)

Cuestionario Previo

Nombre del alumno:_____
Gpo. de Laboratorio:_____

1. ¿Qué es una VPN?
2. ¿Qué es un troncal? Hablando de redes de datos
3. ¿Cuáles son los tipos existentes de VPN?
4. ¿Cuáles son los elementos de una VPN?
5. Escriba 5 ventajas de una VPN
6. Escriba 5 desventajas de una VPN