



Carátula para entrega de prácticas

Facultad de Ingeniería

Laboratorios de docencia



Laboratorio de Redes y Seguridad

Profesor: Magdalena Reyes Granados

Asignatura: Administración de redes

Grupo: 01

No de Práctica(s): 02

Integrante(s): Gutierrez Silvestre Griselda

Sanchez Bautista Velia


*No. de Equipo de
cómputo empleado:*

Semestre: 2021-1

Fecha de entrega: 06 de octubre de 2020

Observaciones:


CALIFICACIÓN: _____

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	16/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica 2

Manejo de VLAN

Planeación

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	17/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

1.- Objetivo de aprendizaje

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

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 medianas empresas y negocios.
- 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

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

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	18/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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 Student.


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 Student. (Ver Figura No. 1)

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	19/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

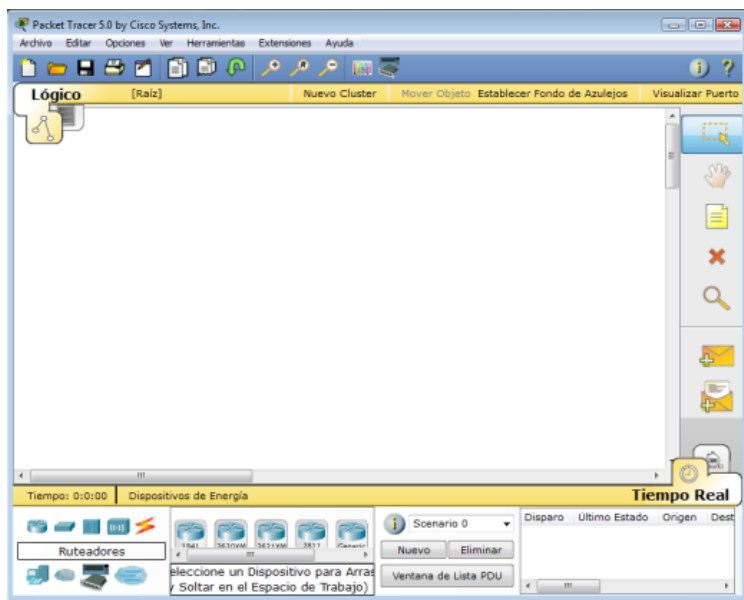


Figura No. 1. Simulador de CISCO Packet Tracer

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

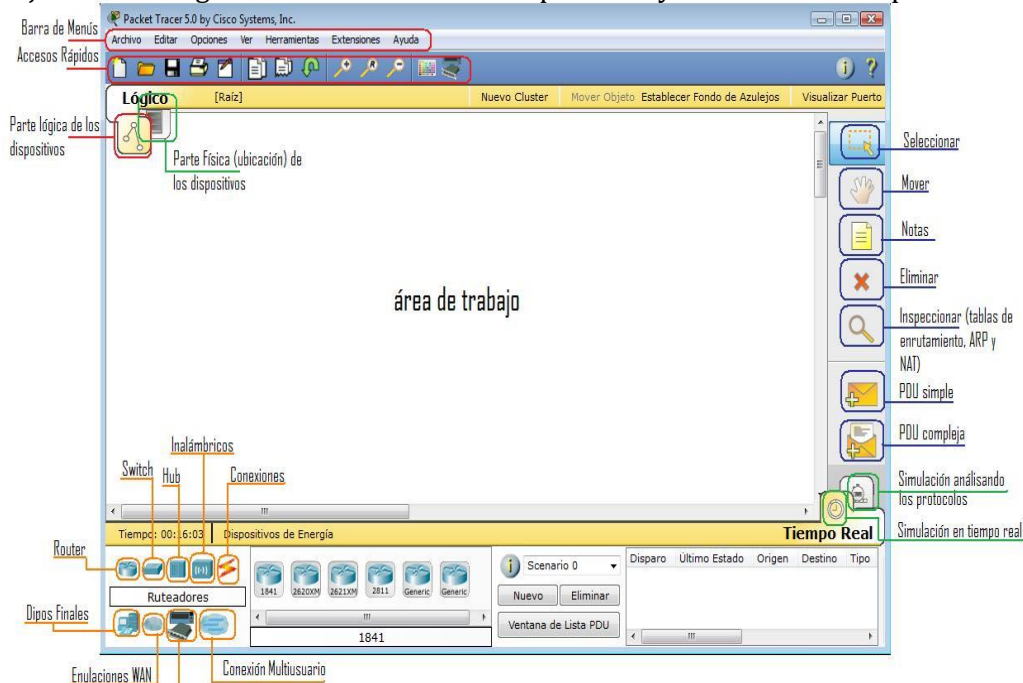



Figura No. 2. Área de trabajo del Simulador de CISCO Packet Tracer

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	20/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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

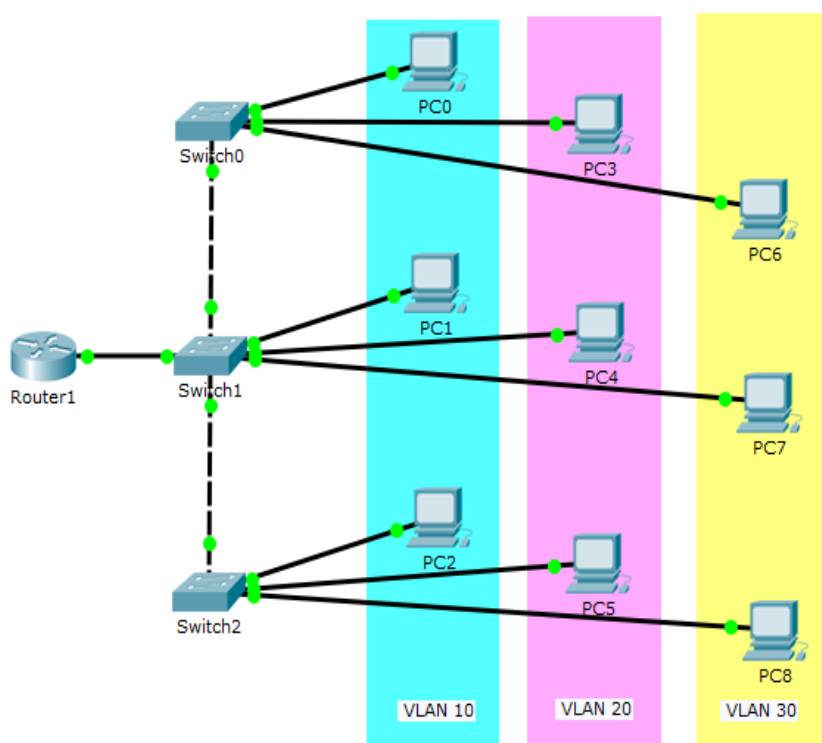



Figura No. 3. Topología de Red.

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

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	21/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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:

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	22/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```
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.

Nos muestra las configuraciones de todas las VLAN, desde el puertos (fast ethernet) y el id de la VLAN.

4.2.6 Defina con su profesor 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.


	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	23/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Tabla 3. Direcciones de red.

VLAN	Segmento de red	Rango de direcciones IP	Máscara	Gateway
10	192.168.1.0	192.168.1.1-192.168.1.3	255.255.255.0	192.168.1.254
20	192.168.2.0	192.168.2.1-192.168.2.3	255.255.255.0	192.168.2.254
30	192.168.3.0	192.168.3.1-192.168.3.3	255.255.255.0	192.168.3.254

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

```
ip ssh version 2
line vty 0 15
transport input ssh
login 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).

```
Switch0 --> Switch1 enlace 1
Switch1 --> Switch0 enlace 2
Switch1 --> Switch2 enlace 3
Switch1 --> Router enlace 4
Switch2 --> Switch1 enlace 5
```

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	24/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



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.

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	25/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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?

No se pueden comunicar ya que es necesario enrutamiento dinámico RIPv2.


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

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	26/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 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 y comente el resultado obtenido.

4.3 Cuestionario

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

Ventajas: mayor seguridad, reducción de costos, mejor rendimiento.

Desventajas: limitaciones en la transmisión, limitaciones del aparato ya que el número de Ethernet que se puede apoyar por cada aparato es de 500.

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

VLAN nativa: esta asignada a un puerto troncal 802.1Q, permite la transmisión del tráfico

VLAN datos: tráfico de datos de los usuarios


VLAN voz: tráfico VoIP requiere de una ancho de banda para asegurar la calidad de la voz

VLAN predeterminada: todos los puertos del switch se vuelven parte del VLAN predeterminado

VLAN administración: cualquier VLAN que se configura

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

Muestra el tipo de asignación y pertenencia de VLAN para todos los puertos del switch y cada VLAN debe corresponder a una subred IP única

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	27/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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

```

configure terminal
interface fastethernet__
no switchport access vlan__

```

5.- Conclusiones

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

Griselda:

~~Los objetivos de la práctica se cumplieron, ya que se logro implementar una VLAN a través del software cisco packet tracer. Se comprobo que una VLAN permite asignar un segmento de la red a las computadoras que lo forman pese a que estas esten distribuidas en distintos switches. También se comprobo que para la comunicación sea exitosa se necesitan configurar los puertos de switch y las interfaces del router.~~

Velia:

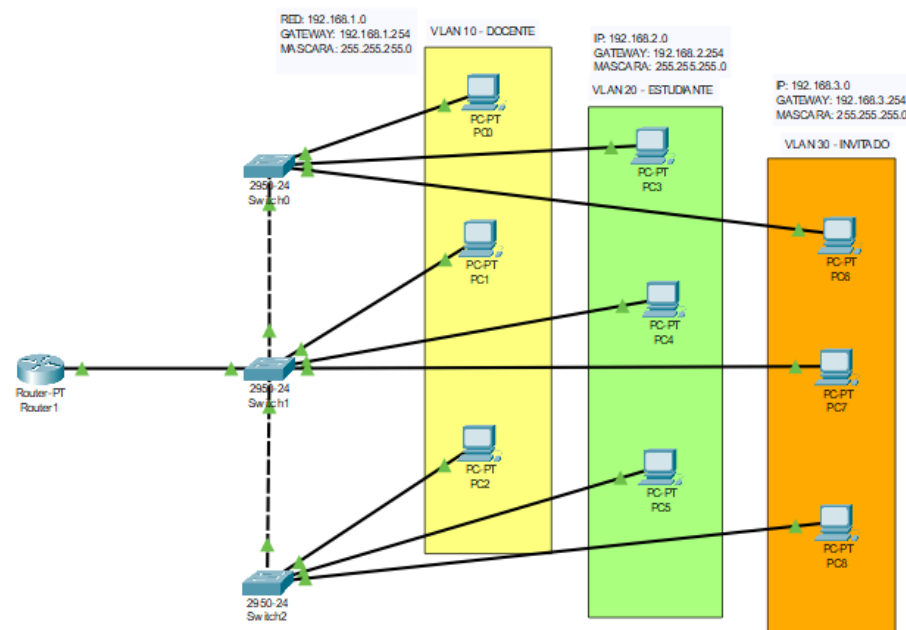
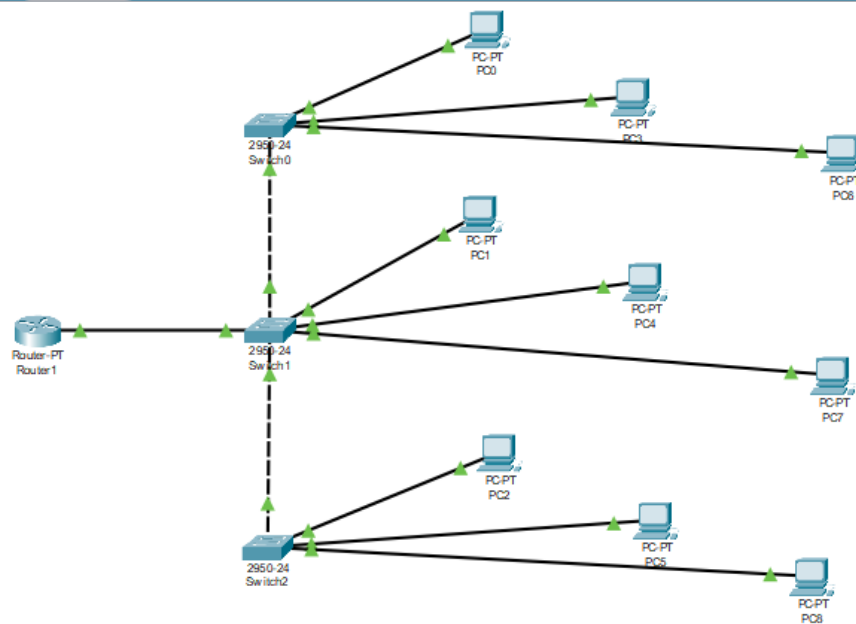
El objetivo de la configuración VLAN se cumplio, implementamos Packet Tracer y configuramos la topología señalada, por medio de comandos agrupamos las PCs por medio de las VLAN sin importar que los dispositivos finales estuvieran en diferentes switches.

Bibliografía:

https://cursos.clavijero.edu.mx/cursos/069_clll/modulo4/contenidos/tema4.2.6.html?opc=1
<https://techandlan.blogspot.com/2018/02/ventajas-y-desventajas-de-las-vlan.html>
<https://www.raulprietofernandez.net/blog/packet-tracer/configuracion-de-vlans-en-packet-tracer>

Capturas de Griselda:

al Physical x: 1269, y: 343



Pings:

→VLAN 10 DOCENTE

- COMUNICACIÓN DE LA PC0 A LA PC1 Y PC2

PC0

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=7ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 1ms

C:\>
```

- COMUNICACIÓN DE LA PC1 A LA PC0 Y PC2.

PC1

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=3ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>
```

→ VLAN 20 ESTUDIANTE

- COMUNICACIÓN DE LA PC3 A LA PC4 Y PC5

PC3

Physical Config Desktop Programming Attributes

Command Prompt

```
Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time=11ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms

C:\>
```

- COMUNICACIÓN DE LA PC5 A LA PC3 Y PC4.

PC5

Physical Config Desktop Programming Attributes

Command Prompt

```
Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=3ms TTL=128
Reply from 192.168.2.1: bytes=32 time<1ms TTL=128
Reply from 192.168.2.1: bytes=32 time<1ms TTL=128
Reply from 192.168.2.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time=1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

➔ VLAN 30 INVITADO

- COMUNICACIÓN DE LA PC6 A LA PC7 Y PC8

Command Prompt

```
Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.3.3

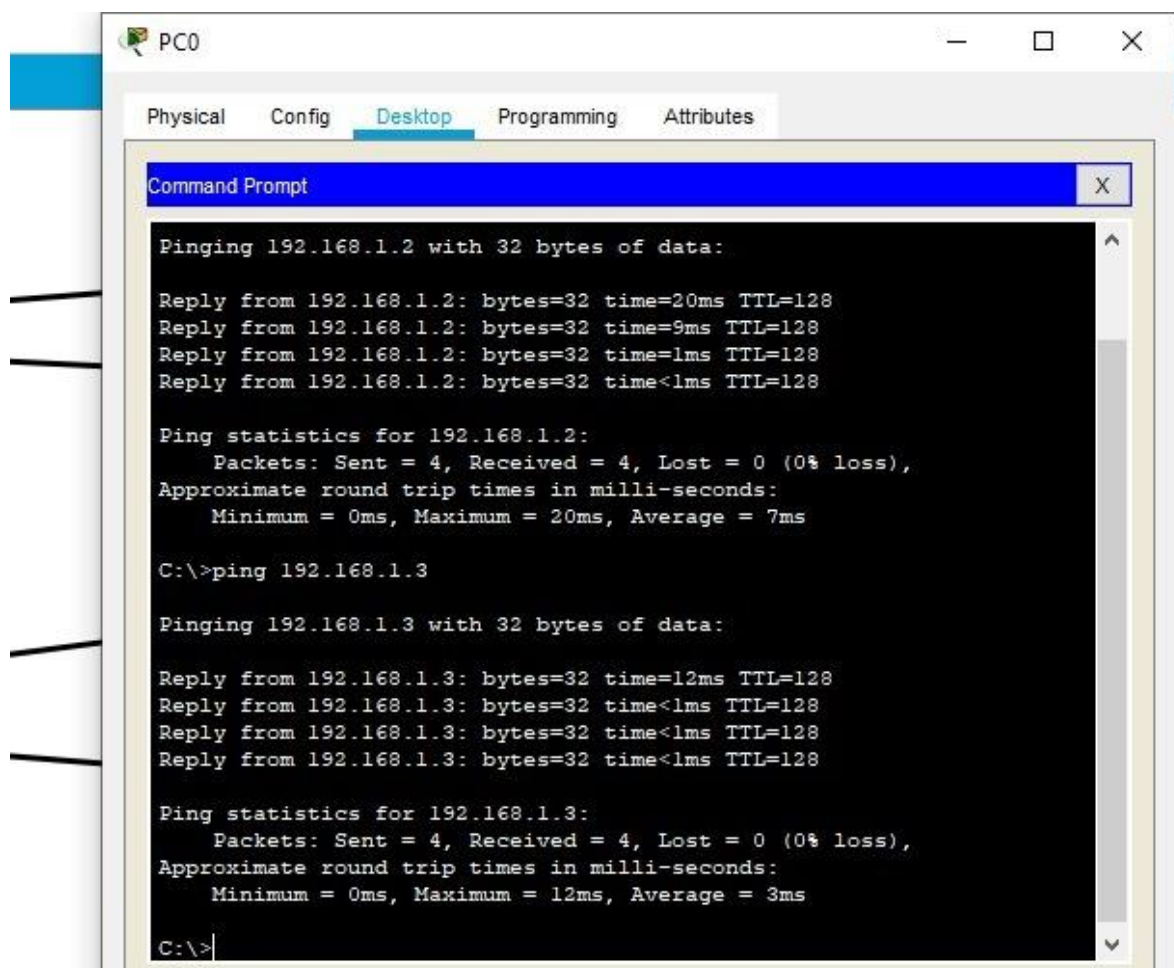
Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Capturas de Velia:



The screenshot shows a window titled "PC0" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the execution of two ping commands. The first command is "ping 192.168.1.2", which results in four successful replies with 32 bytes of data, times ranging from 0ms to 20ms, and a TTL of 128. The statistics for 192.168.1.2 show 4 packets sent and received, 0% loss, and an average round trip time of 7ms. The second command is "ping 192.168.1.3", which also results in four successful replies with 32 bytes of data, times ranging from 0ms to 12ms, and a TTL of 128. The statistics for 192.168.1.3 show 4 packets sent and received, 0% loss, and an average round trip time of 3ms. The Command Prompt prompt is "C:\>".

```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
X

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=20ms TTL=128
Reply from 192.168.1.2: bytes=32 time=9ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 20ms, Average = 7ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=12ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>
```

