Laboratorio 3

Thenison Encina *2803016-9*
Daniel Romero *2873039-k*

Valparaíso, 15 de mayo de 2016

1. Introducción

1.1. Descripción del laboratorio

Para poder crear redes de computadores, es necesario comprender los distintos com- ponentes que se conectan para poder lograr la comunicación, seguridad, conectividad y otras características importantes que se requieren. En este laboratorio, se pretende que se interiorice con la capa de red y de enlace de datos del modelo OSI que abarcan componentes que cumplen con la implementación de las características mencionadas anteriormente. Después de esta experiencia, el alumno deber??a poder diseñar sus propias redes de computadores y tener herramientas para comprobar su funcionamiento.

2. Desarrollo

2.1. Trabajo previo

Estudie los temas de la sección Anexos y busque los comandos Cisco
Desde la documentación de CISCO

Device Configuration

Description	Commands
Configure device system name	`Switch(config)#hostname sw1`
Sets the encrypted enable password	`Switch(config)#enable secret cisco`
Sets the unencrypted enable password	`Switch(config)#enable password cisco`
Enable password encryption on all clear text password within the configuration file	`Switch(config)#service password-encryption`
Configure a Message Of The Banner, with an ending character of $	`Switch(config)#banner motd $`
Assign IP address to vlan	`Switch(config)#int vlan 1` `Switch(config-if)#ip addr 172.22.1.11 255.255.255.0`
Assign Default gateway, note the mode	`Switch(config)#ip default-gateway 10.1.1.1`
Select one interface	`Switch(config)#int fa0/1`
Select a range of interfaces (version dependant)	`Switch(config)#int range fa0/1 – 12`
Set the interface description	`Switch(config-if)#description`
Add vlan using config mode	`switch(config)#vlan 11` `switch(config-vlan)#name test`
Configure Interface fa0/1 @ speed 100 Mbps and full duplex	`Switch(config-if)#speed 100` `Switch(config-if)#duplex full`
Assign interface to vlan	`switch(config-if)#switchport access vlan 11`

Enable Port Security.	`Switch(config-if)#switchport mode access`
	`Switch(config-if)#switchport port-security`
	`Switch(config-if)#switchport port-security mac-address sticky`

Disable Interface	`Switch(config-if)shutdown`
Enable Interface	`Switch(config-if)no shutdown`

Configures 5 Telnet sessions each with a password of 'cisco'	`Switch(config)#line vty 0 4`
	`Switch(config-line)#login`
	`Switch(config-line)#password cisco`

Enable and define console password of 'cisco'	`Switch(config)#line con 0`
	`Switch(config-line)#login`
	`Switch(config-line)#password cisco`

Synchronise console messages (keep what you have typing on the screen)	`Switch(config-line)#logging synchronous`
Set the timezone and automatically adjust	`Switch(config)#clock timezone gmt 0` `Switch(config)#clock summer-time gmt recurring`
Sets the switch priority for the vlan. This combined with the switch mac address creates the switch BID	`Switch(config)#spanning-tree vlan 1 priority 4096`
Enables portfast	`Switch(config)#int fa0/1` `Switch(config-if)#spanning-tree portfast`
Enables RSTP. Other options are, PVST and MST	`Switch(config)#spanning-tree mode rapid-pvst`
Creates a vlan. Note this now done in config mode not vlan database. Also note the 'int vlan' command does **NOT** create vlans	`Switch(config)#vlan 2` `Switch(config-vlan)#name sales`
Assign an interface to vlan 2	`Switch(config-if)#switchport access vlan 2`
Unconditionally forces an interface into trunking. Other options are access and dynamic	`Switch(config-if)#switchport mode trunk`
Manually assign a switch to a VTP domain. A switch will automatically become part of a VTP domain if it's currently in the 'null' domain and receives a VTP frame	`Switch(config)#vtp domain lab`
Changes the VTP mode from the default 'server' mode to client mode. In client mode no changes can be made	`Switch(config)#vtp mode client`
Enable the http server to SDM can be used	`Router(config)#ip http server`

1. Mostrar listado de direcciones MAC conectadas al switch.

enable
show mac-adress table

2. Habilitar ruteo de IPv6.

   enable
   configure
   ipv6 unicast-routing

3. Acceder a la interfaz X del router.

   enable
   configure
   interface X

4. Asignar dirección IP y máscara a la interfaz X.

   enable
   configure
   interface ïnterface name"
   ip(v6 o v4) address ïp")/(mascara de subred)

5. Configurar enrutamiento estático del router.

   enable
   configure
   ip route ïpnombre interfaz"

6. Configurar enrutamiento dinámico con RIP del router.

   enable
   configure
   ip(v6) rip id1 enable

7. Eliminar dirección IP asignada a interfaz X del router.

   enable
   configure
   no ip address

En esta experiencia se emulan routers y switches Cisco, pero en la vida real es posible que nos toque interactuar con otras marcas y es necesario tener conocimientos generales de su manipulación. Investigue 2 marcas aparte de Cisco que ofrezcan switches y/o routers con características similares.

1. Switch SuperStack 3C16471-US 3

Puertos: 24 puertos 10BASE-T/100BASE-TX con auto-detección y auto-configuración MDI/MDIX Interfaces para medios: RJ-45 Funciones de switching Ethernet: Velocidad total sin bloqueo en todos los puertos Ethernet, auto-negociación y control de flujo bidireccional / semi-dúplex, establecimiento de prioridades de tráfico, 802.1p Direcciones MAC que se soportan: 4,000

2. Alcatel OmniStack LS 6224

Número de interruptor de puertos: 24 x Ethernet de 10/100 Mbits/s; Uplink: 2 x Ethernet 10/100/1000 Mbit/s; Soporte de trabajo en la pila: sí; Interna de ancho de banda: 12,8 GB/s; Tamaño de tabla de dirección MAC: 8192;

3. Switch 24 Puertos D-Link xSTack Des-3528

Listas de control de acceso centralizadas. Q-in-Q selectivo. Funcionamiento sin ventilador. Safeguard Engine^{TM} de D-Link. Seguridad de red proactiva con mecanismo ZoneDefense. Apilamiento físico de hasta 8 conmutadores.* Soporte de multidifusión global. Control de acceso basado en MAC/web (MAC/WAC).

4. TRENDnet TE100-S24D

El conmutador de 24 puertos a 10/100 Mbps, modelo TE100-S24D, es una solución confiable Plug-and-Play en un factor de forma compacto. Aumente la eficiencia de la red con una capacidad de conmutación total de 4.8 Gbps y modo Full Dúplex.

¿Cuál es más intuitiva? ¿Cuál ofrece más posiblidades de configuración? ¿Son similares?.

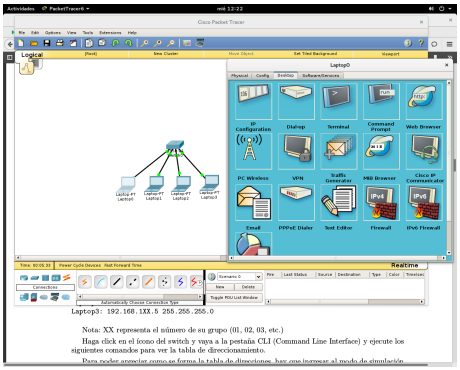
Configuración:

Respecto a configuración la marca Cisco nos ofrece mayor configuración en comparación al resto de las marcas, el resto son similares dejando al final en libertad de configuraciones las marcas menos conocidas.

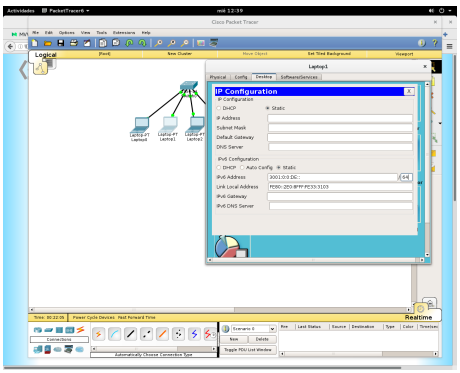
2.2. Trabajo en el laboratorio

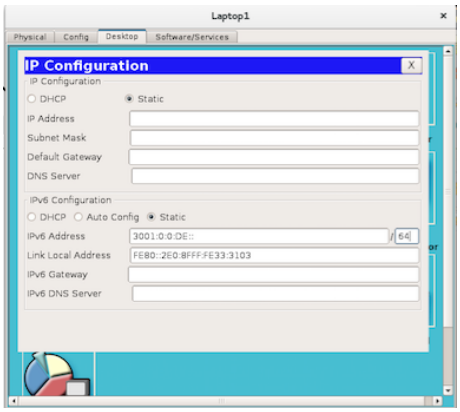
2.2.1. Conectividad mediante Switch

Primero, se deben agregar 4 laptop's al logical workspace de Packet Tracer y deben conectarse con cables FastEthernet directos a un switch 2950-24

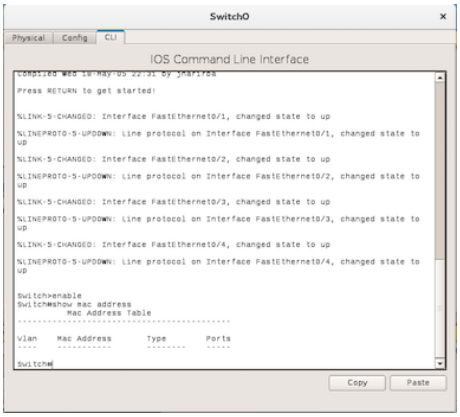


Es importante que se configure cada host con su respectiva dirección IPv6 de manera manual, donde la dirección de cada host será consecutiva dentro de la misma red,esto será utilizado para comprobar la conectividad.

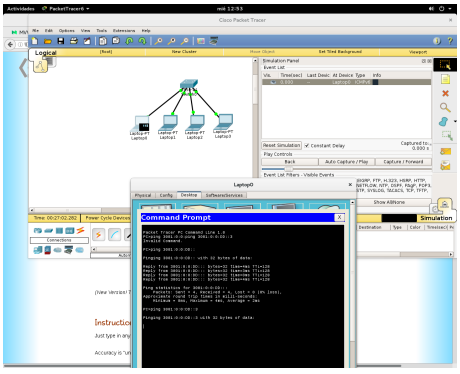


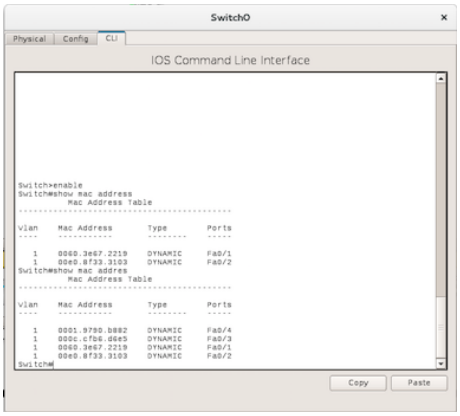


Haga click en el ícono del switch y vaya a la pestaña CLI (Command Line Interface) y ejecute los comandos necesarios para ver la tabla de direccionamiento.



Para poder apreciar como se forma la tabla de direcciones, hay que ingresar al modo de simulación de Packet Tracer y hacer click en Edit Filters, asegurarse de que soló quede seleccionado ICMPv6.





2.2.2. Preguntas

1. Si cada computador conectado al switch es capaz de ver el tráfico de la red ¿Qué ventajas tiene usar un switch?.

   Partiremos definiendo que es un switch.

   SWITCH: es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

   La ventaja es que el switch permite conectar varios equipos en una red Ethernet con el mismo ancho de banda para todos.

2. Si hay 2 redes conectadas a un switch ¿Es posible que un computador de una red sea capaz de ver el tráfico de la otra red? Fundamente.

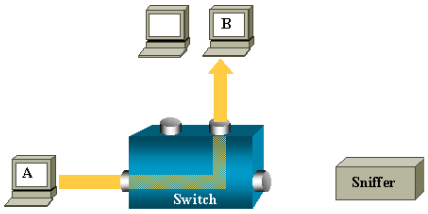
   Primero debemos decir que no es posible conectar dos redes a un switch único, para lograr realizar dicha acción debemos usar VLAN.

   VLAN: Es un método para crear redes lógicas independientes dentro de una misma red física.

   Recordemos que cuando un switch recibe una trama Ethernet en uno de sus puertos y no conoce a que puerto esta conectado el host con la MAC destino, el switch realiza un "flooding" de tráfico unicast. Es decir, el switch transmite la trama a través de todas sus interfaces. Cuando el host para el que estaba dirigida la trama responde o envía tráfico, el switch guarda la información y el puerto asociado a esa dirección MAC.

   Una vez que el switch completa su tabla en memoria, el tráfico unicast ya no aparece en todos los puertos, en vez de eso, el switch envía el tráfico al puerto en el que sabe que esta ubicada la dirección MAC destino. De esta manera el tráfico entre dos hosts (A y B) no puede ser visualizado por un tercero, simplemente por que el switch no lo transmite hacia su interfaz de red.

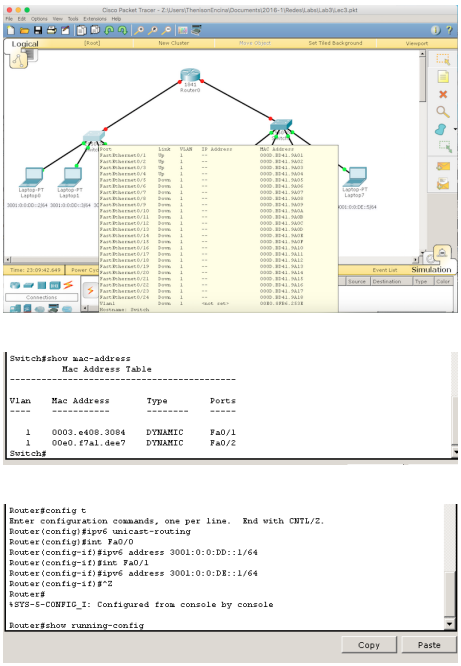
   Es por ello la necesidad de crear una red de área local virtual.



3. ¿Cómo se puede separar la información de cada red conectada a un switch?.

   La mejor solución a esta necesidad es utilizar VLANs (Virtual Local Area Network) para separar el tráfico completamente y darles su propia salida a Internet a cada red.

2.2.3. Conectividad mediante Router



4. ¿Qué pasaría si la interfaz del router se configura con una máscara distinta a la del host?.

   Cada interfaz debe pertenecer a una red diferente, se pueden configurar dos interfaces para pertenecer a la misma red, sin embargo solo UNA podrá estar ACTIVA. Si se configuran dos interfaces con dos IP de la misma red aparecerá este mensaje:

   " ip overlaps with otra ip".

   Si se intenta habilitar la interfaz aparecerá el siguiente mensaje:

R1(config-if) no shutdown ip overlaps with otra ip FastEthernet0/1: incorrect IP address assignment

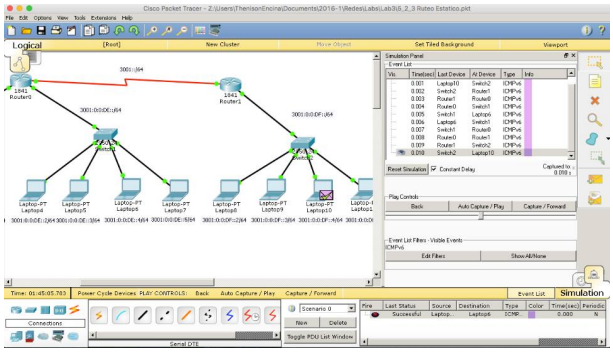
5. Si se configura de forma incorrecta la interfaz del router ¿Cuál sería el comando para eliminar la configuración?.

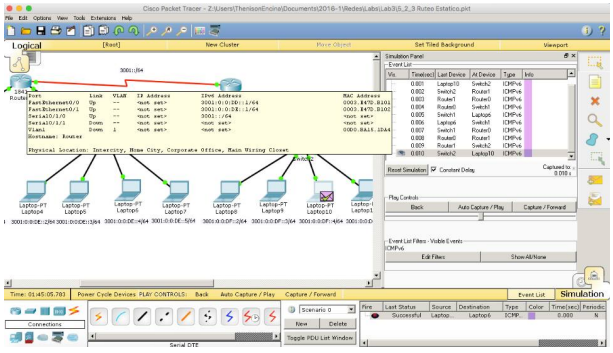
   El comando es “no ip address”.

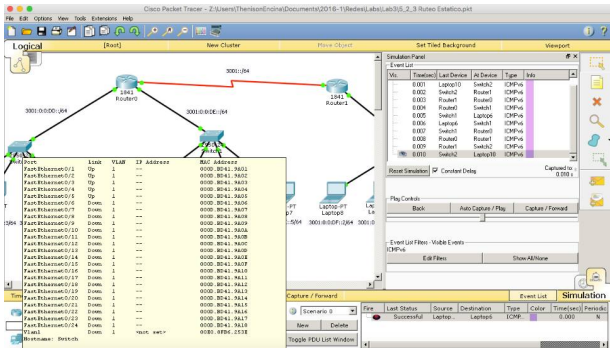
   Para borrar la configuración del router:

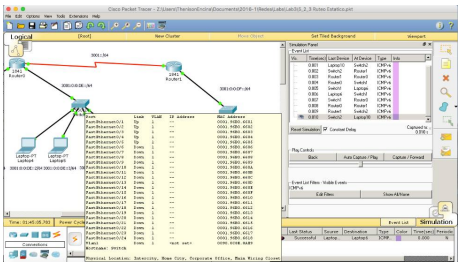
   “erase nvram”.

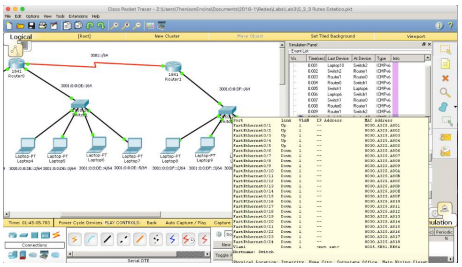
2.2.4. Ruteo Estático

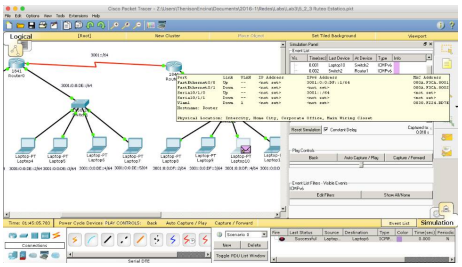












6. ¿Hay conectividad?, si la respuesta es negativa ¿Por qué no hay conectividad?.

   No hay conectividad, esto porque falta hacer el ruteo estático, es decir la tabla de enrutamiento para que se pueda acceder a la redes que no están conectadas directamente, es otras palabras, enseñarle al router los caminos que tiene que seguir para llegar al otras redes.

7. Si se hizo el enrutamiento en el Router0, ¿Por qué el ping no es efectivo si el Router0 conoce como llegar a la red destino?. Configure adecuadamente el Router1 para conseguir la conexión entre las redes.

   Simplemente porque desconoce el camino para llegar al destino, en este caso Router0, al realizar el ping este se realiza enviando y recibiendo pero como no conoce el camino de vuelta, el ping falla.

2.3. Trabajo fuera del laboratorio

2.3.1. Enrutamiento Dinámico usando RIPng

8. ¿Qué ventajas presenta el uso de RIPng respecto a OSPF?. Indicar 2 situaciones donde RIP sea mejor que el enrutamiento estático.

   RIP posee las siguientes características clave:

a) RIP es un protocolo de enrutamiento vector distancia.

b) RIP utiliza el conteo de saltos como su única métrica para la selección de rutas.

c) Las rutas publicadas con conteo de saltos mayores que 15 son inalcanzables.

d) Se transmiten mensajes cada 30 segundos.

En comparación con otros protocolos de enrutamiento, RIP es más fácil de configurar. Además, es un protocolo abierto, soportado por muchos fabricantes.

En las redes grandes, la convergencia de RIP puede tardar varios minutos dado que la tabla de enrutamiento de cada router se copia y se comparte con routers directamente conectados a diferencia de OSPF, que el mantenimiento de un estado convergente es más rápido porque se inundan los otros routers del área con los cambios en la red.

Es por ellos que si se va a mantener una pequeña red, RIP está bien, si se va más allá de 3 o 4 routers entonces tal vez es mejor un protocolo de enrutamiento como OSPF.