2024

TRABAJO DE LABORATORIO Nº 1

Configuración de Switches LAN para el funcionamiento de Capa 2 en redes Ethernet / IEEE 802.3 y 802.1Q (VLAN)

ACTIVIDAD DE FORMACION PRACTICA

1. Formación experimental (laboratorio).

OBJETIVOS

1. Comprender el funcionamiento de la conmutación de capa 2 en redes Ethernet.
2. Incorporar habilidades básicas de configuración de dispositivos *switch* LAN.
3. Extender las habilidades de configuración para el diseño lógico y seguro de redes LAN.
4. Comprender el funcionamiento del Protocolo Spanning – Tree y su configuración básica.

CONOCIMIENTOS PREVIOS

1. Modelo OSI: funciones y servicios de cada capa, comunicaciones entre capas, proceso de comunicaciones entre capas, de la capa *N (par a par)*, primitivas de servicios.
2. LAN / Conmutación LAN: técnicas de almacenamiento y envío, de corte (libre de fragmentos y envío rápido)
3. ETHERNET / IEEE 802.3: transmisión / recepción, funcionamiento del modelo CSMA/CD.
4. Direccionamiento MAC
5. Filtros de tramas basado en MAC
6. VLAN/ IEEE 802.1Q
7. IEEE 802.1D (SPANNING TREE): conceptos de SWITCH RAÍZ, puerto RAÍZ, puerto DESIGNADO y puerto BLOQUEADO, funcionamiento del algoritmo.
8. Lectura comprensiva de los apuntes **19642-126.pdf** y **swethchl.pdf**.
9. **EJERCICIOS RESUELTOS DE LAS GUÍAS DE EJERCICIOS DE ESCRITORIO (GEE):**

2.1.3.	Configuración
2.3.6. a 2.3.14.	Configuración
3.1.2.	Configuración
5.4.1. a 5.4.15.	Configuración
5.6.1. a 5.6.5.	Configuración

MATERIAL NECESARIO

1. Una PC de escritorio con el simulador PacketTracer, versión indicada en el aula virtual de laboratorios.
2. Archivo **TL1-switch2024.pkt** con la configuración para el práctico.
3. Guía de configuración de switch Cisco Catalyst 2950 y Catalyst 2955 (archivo **2950SCG**).
4. Resumen de comandos de configuración básica de switch Cisco (archivo **Comandos de Configuración Switch Cisco**).
5. Archivo de IEEE **802.1D-2004.pdf**
6. Apunte **INTRODUCCIÓN AL PROTOCOLO SPANNING TREE.doc**

DESCRIPCION

Este trabajo será desarrollado de manera individual o en grupo de dos alumnos en una PC con simulador y **evaluado individualmente** mediante preguntas orales, un ejercicio en el simulador y un cuestionario escrito.

1. Caso de Estudio

Se grafica en el archivo **TL1-switch2024.pkt** **(se dispondrá en el directorio TL1 del aula virtual Laboratorio Redes de Información)**

2. Requerimientos para el alumno (Objetivos Técnicos)

a. Configurar los dispositivos en base a las tareas descriptas y lograr el funcionamiento correcto de la red en todos sus segmentos.

b. Demostrar el funcionamiento de la red, sus dispositivos y equipos en los siguientes puntos de verificación:

1) Acceso TELNET desde la PC a cada switch.
2) Seguridad de puerto del switch para una PC determinada.
3) Funcionamiento correcto dentro y fuera de la **VLAN 10 Logística**.
4) Comunicación entre las PC de la VLAN 1, entre las de la VLAN 1 y la VLAN 10 y entre las de la VLAN 10?
5) Correcto funcionamiento de las troncales entre VLANs y acceso al servidor desde la VLAN correspondiente.
6) Correcto funcionamiento de la configuración del protocolo STP.

c. Resguardar las configuraciones para futuras actividades de laboratorio.

d. Realizar la configuración de evaluación automática en el simulador.

e. Responder las preguntas que se le formulen en particular.

3. Tareas

PRIMERA PARTE - CONFIGURACION DE SWITCHES DE ACCESO

a. Conectar los dispositivos para armar la red del diagrama que representa el caso de estudio.

1) Abrir el archivo **TL1-switch2024.pkt** con *PacketTracer*.
2) En la barra inferior, seleccionar *connections* y arrastrar el cable apropiado, haciendo clic en los dispositivos a conectar (tomar nota de los puertos de cada conexión).

a) Las placas de red de las PC a los switches.
b) Los switches entre sí.
c) Los puertos RS232 de las PC a los puertos de consola de los switches.

b. Iniciar la administración del *switch*

Haciendo clic en las PC selecciona *desktop*, *Terminal*; esto simula un acceso por *hyperterminal* que ingresa al modo de ejecución usuario.

c. Explorar los distintos modos dela CLI (Interfaz de Línea de Comando)

1) Ha ingresado a modo de ejecución de usuario, ¿que *prompt* tiene?
2) Liste y documente los comandos del modo usuario, ingresando el comando: *?* (será de utilidad en todos los modos de ejecución)
3) Liste y documente todos los comandos *show* disponibles, ejecutando el comando:
   show ?
4) Pase al modo privilegiado mediante el comando: *enable* (no se solicitará contraseña, si no está configurada específicamente)
5) Liste y documente todos los comandos *show* disponibles. ¿Son los mismos?
6) Liste la configuración activa (es la que se está ejecutando en memoria RAM) utilizando el comando: *show running-config.* Haga lo equivalente para la memoria FLASH con: *show startup-config*
7) Muestre el estado de las interfaces mediante el comando:*show interface.* Identifique información de las capas 1 y 2 OSI.
8) Ingrese al modo de configuración global, con el comando *configure terminal* ¿Qué *prompt* tiene?
9) Liste y documente los comandos del modo de configuración global.
10) Asigne un nombre al *switch* mediante el comando: *hostname* ***switch-100***
11) Configure la contraseña para el modo privilegiado mediante: *enable secret* ***utn***
12) Salga de modo de configuración global ingresando *exit* en la CLI. Liste nuevamente la configuración activa.
13) Resguarde la configuración activa mediante una copia en la memoria flash utilizando el comando *copy running-config start* (presione la tecla `TAB´ y observe su utilidad).
14) Salga del modo privilegiado con *exit* y vuelva a ingresar.
15) Observe la utilidad de las flechas del teclado RETROCESO / AVANCE DE LÍNEA.

d. Configuración del acceso remoto por medio del protocolo *TELNET*.

Telnet y SSH permiten la administración del dispositivo en forma remota, a través de una red TCP/IP. Ambos son protocolos de nivel Aplicación, por lo que tanto cliente como servidor deben estar configurados en la capa 3 (IP).
Dado que todavía no se ha desarrollado el tema IP, tanto las PC como los switches ya se encuentran configurados.

1) Pruebe la conectividad entre todas las computadoras y los switchs con la utilidad PING, ejecutando en la línea de comandos PING 192.168.1.xxx, donde xxx es el número del dispositivo.
2) Habilite el acceso a los *switches* vía TELNET
3) En el modo de configuración global ejecute:
   Line vty **0 1**
   Password **clase**
   exec-timeout <**número minutos**>
   Login
4) Pruebe el acceso TELNET del escritorio de las PC a los *switches*.

e. Configuración de interfaces.

Para configurar las interfaces se debe pasar al modo *interface,* ejecutando *interface* **f 0/x,** donde **x** es el número de la interfaz a configurar.
Si se quieren ejecutar comandos en varias interfaces simultáneamente (en el ejemplo de la 1 a la 10), puede hacerlo ejecutando el comando *interface range* **f0/1 – 10**

1) Liste y documente los comandos del modo
2) Desactive todas la interfaces con el comando *shutdown*.
3) Active sólo las interfaces que tienen dispositivos conectados.
4) Salga al modo ejecución y liste la configuración activa con *show running-config*.
5) Configure la seguridad de puerto en las interfaces donde esta conectadas las PC para que en cada uno de los mismos se conecte una PC con una MAC especifica y evitando así conexión de PC no autorizadas y ataques al dispositivo. Utilice los comandos de interface

   Switch(config-if)#switchport mode access
   Switch(config-if)#switchport port-security
   Switch(config-if)#switchport port-security maximum **1**
   Switch(config-if)#switchport port-security mac-address **hhhh.hhhh.hhhh**
   Switch(config-if)#switchport port-security violation shutdown

6) Realice la captura de la configuración activa en un archivo de texto, edítala eliminando saltos de página y agregando los comandos *exit* necesarios para pasar entre modos de configuración. Copie y pegue los comandos en el otro switch.
7) ¿Cuántos dominios de broadcast hay en la red?, ¿cuántos dominios de colisión hay en la red?

f. Configuración de redes virtuales VLAN.

1) Liste y documente las VLANs definidas y la asignación de puertos a las mismas, ejecute *show vlan*.
2) Cree en los switchs 100 y 200 una VLAN con el número 10, y asígnele el nombre logística. En configuración global ejecute:
   vlan **10**

name **logística**

3) Cree en los switches 100 y 200 una vlan con el número 20, y asígnele el nombre marketing.
4) Regrese al modo ejecución y liste las vlans definidas y la asignación de puertos a las mismas.
5) Asigne los puertos de las PC 101 y 201 a la vlan 10. En el modo de configuración de interface ejecute: *switchport access vlan* **10**
6) Asigne los puertos de las PC 102 y 202 a la vlan 20, de manera similar a la anterior.
7) Verifique la conectividad entre las PC, ¿hay respuesta de PING en las PC de la vlan 10, entre las de la 10 y la 20, y entre las de la vlan 20?
8) ¿Cuántos dominios de broadcast hay en la red?, ¿cuántos dominios de colisión hay en la red?

g. Configuración de troncales, extensión de las redes virtuales.

1) Configure las interfaces de los switches conectadas al cableado vertical para que envíen tráfico de todas las VLAN. En el modo de configuración de interface ejecute:
   Switch(config-if)#switchport mode **trunk**
2) Verifique la conectividad entre las PC, ¿hay respuesta de PING en las PC de la vlan 10, entre las de la 10 y la 20, y entre las de la vlan 20?

SEGUNDA PARTE - CONFIGURACIÓN DE SWITCHES DE DISTRIBUCIÓN Y NÚCLEO

En la sala de distribución principal, MDF, se han conectado los switches de distribución mediante dos interfaces de 1Gb de FO al switch de núcleo y mediante otra interfaz entre sí, formando loops de capa 2 a fin de asegurar la disponibilidad.

La configuración de spanning tree está por defecto en los tres switches.

a. Identificación del switch RAÍZ y la configuración de puertos.

1) Identifique el switch raíz. ¿Por qué ha sido seleccionado como tal?
2) Identifique los puertos raíz, los puertos designados y los puertos bloqueados.

b. Configuración de STP con agregado de enlace.

1) Configure el switch de núcleo para que sea seleccionado como raíz.

   Switch1(config)# spanning-tree vlan **1,10,20 root primary**

2) Configure agregado de enlace LACP entre los switches de distribución y el de núcleo, con el fin de duplicar el ancho de banda, evitando que *spanning tree* bloquee uno de ellos y aplicando correctamente los conceptos de *dst-mac* / *src-mac* para el balanceo de carga:

   Switch1(config)# port-channel load-balance {dst-mac | src-mac}

   Switch1(config)# interface gigabitethernet **1/1**

   Switch1(config-if)# switchport mode **trunk**

   Switch1(config-if)# channel-protocol **LACP**

Switch1(config-if)# channel-group **1** *mode active*

Switch1(config-if)# exit

3) Verifique la configuración de *spanning tree* con los comandos:

Switch#show spanning-tree summary

Switch#show spanning-tree active

Switch#show spanning-tree detail

c. INTERCONECTE LOS SWITCHES DE LAS 3 CAPAS Y PRUEBE EL ESCENARIO DE LAN.

TERCERA PARTE - CONFIGURACIÓN DE ACCESO REMOTO SEGURO

En la capa funcional NÚCLEO mejora la seguridad del acceso remoto al Switch NÚCLEO:

(*por razones de simplicidad en la ejecución del ejercicio, los nombres de usuario y contraseñas no aplican las buenas prácticas de control de acceso*[1]).

a. Configuración de SSH (Secure SHell)

1) Obtenga información del fabricante sobre las opciones de configuración del protocolo SSH en https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html#req
2) Analice las instrucciones y verifique la compatibilidad del IOS que dispone el switch NUCLEO. Utilice el comando ***show version*** para identificar las opciones de configuración.
3) En base a los comandos utilizados en la primera parte, configure el switch para el acceso remoto en la red LAN Núcleo.
   a) Asigne el nombre NUCLEO al switch de la capa NÚCLEO y la contraseña ´cisco´ para el modo privilegiado.

   Switch(config)#hostname NUCLEO

   NUCLEO(config)#

   NUCLEO(config)#enable password cisco

   b) Configure una dirección IP de administración en la VLAN 1 dentro de la red 192.168.1.0/24 y active la interfaz.

   NUCLEO(config)#interface vlan 1

   NUCLEO(config-if)#ip address 192.168.1.251 255.255.255.0

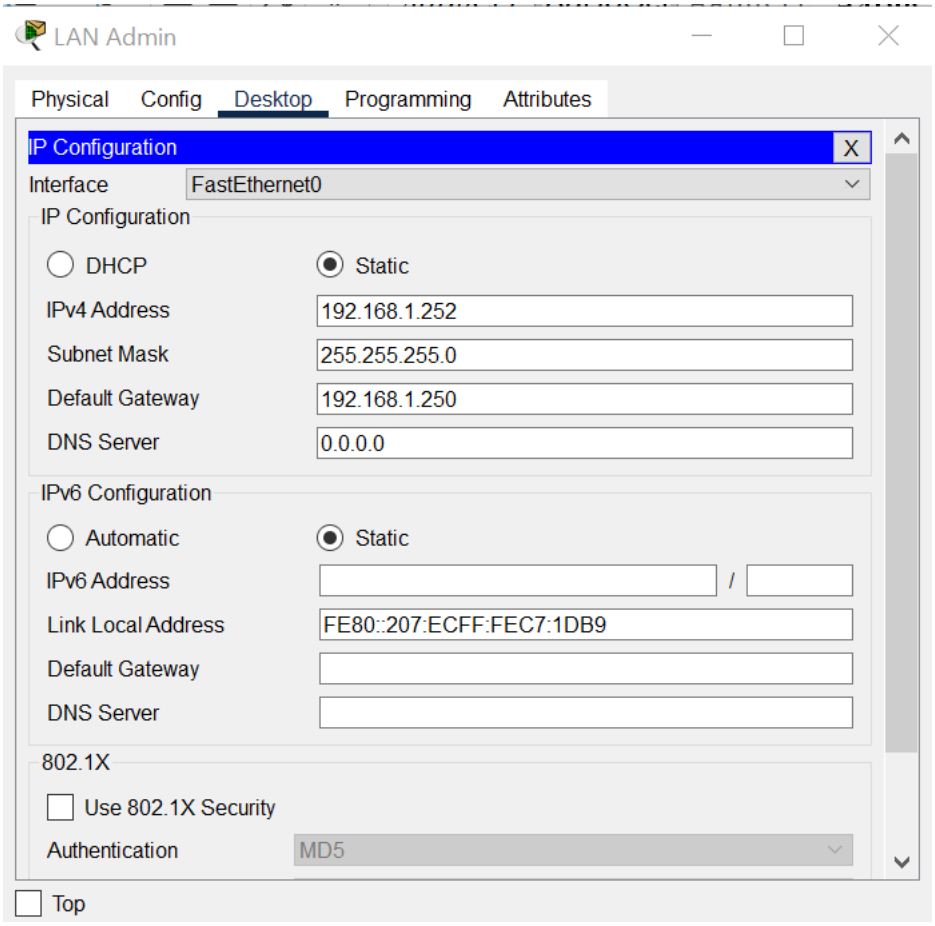
   NUCLEO(config-if)#no shutdown

   NUCLEO(config-if)#exit

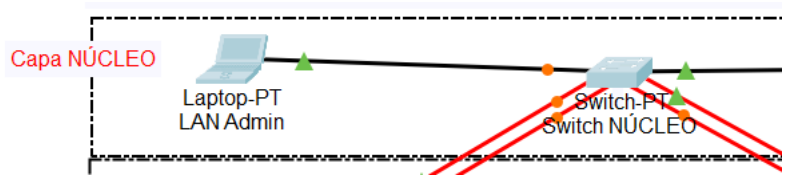
   NUCLEO(config)#

[1] Se pueden consultar en: https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/13608-21.html

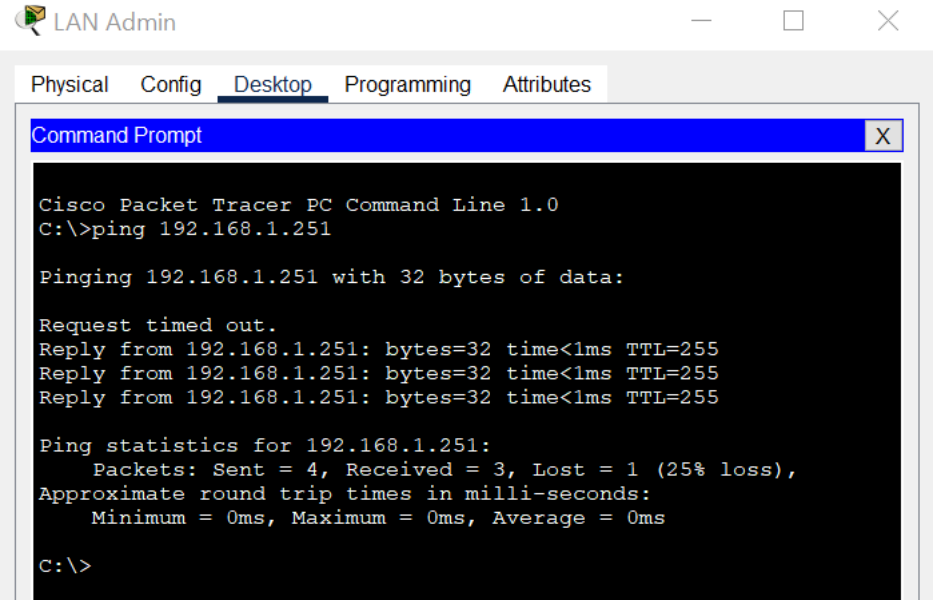
4) Verifique su funcionamiento en la capa 3 (IP con ICMP).
   a) Configure una dirección IP estática en la PC LAN Admin:



   b) Conecte la PC LAN Admin al switch NUCLEO mediante un cable UTP.



   c) Ejecute la aplicación PING desde la PC LAN Admin hacia el switch NUCLEO para verificar el funcionamiento del tráfico de paquetes IP.



5) Configure la opción de acceso remoto para el modo **SSH versión 2.0** para UN SOLO USUARIO REMOTO.
   a) Configuración de nombre de dominio

      NUCLEO(config)#ip domain-name tl1.com

   b) Generación de Claves RSA

      NUCLEO(config)#crypto key generate rsa

   c) Cambiar SSH versión 1 a la versión 2

      NUCLEO(config)#ip ssh version 2

   d) Configuración de Line VTY para un solo usuario

      NUCLEO(config)#line vty 0

      NUCLEO(config-line)#transport input ssh

      NUCLEO(config-line)#login local

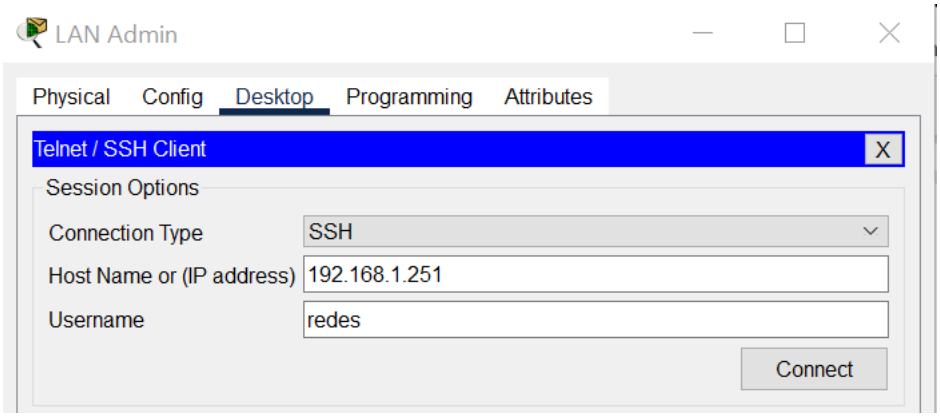
   e) Crear nombre de usuario ´redes´ con el nivel de privilegio más alto (15) y contraseña ´cisco´.

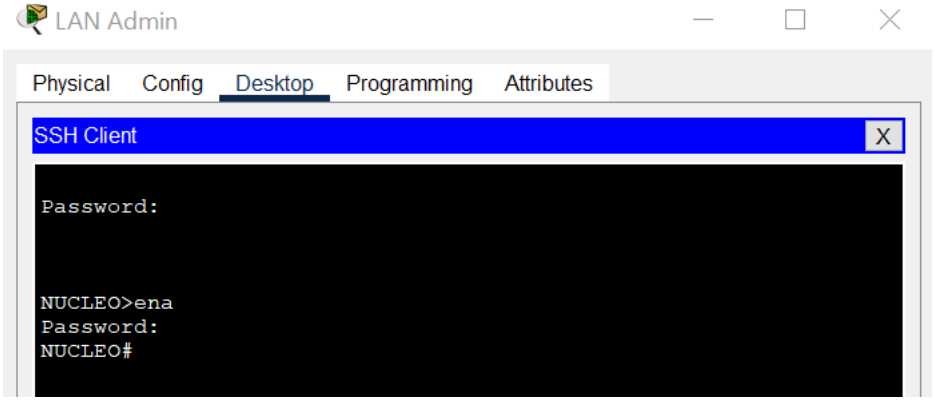
      NUCLEO(config)# username redes privilege 15 password cisco

   f) Habilitar una nueva contraseña para modo privilegiado *´cisco123´*

      NUCLEO(config)#enable secret cisco123

6) Pruebe el acceso remoto SSH desde la PC LAN Admin al switch NUCLEO en modo usuario con usuario ´redes´ y contraseña ´cisco´; luego use la contraseña ´cisco123´ para acceder al modo privilegiado mediante el acceso remoto SSH.





b. Desactivación de TELNET

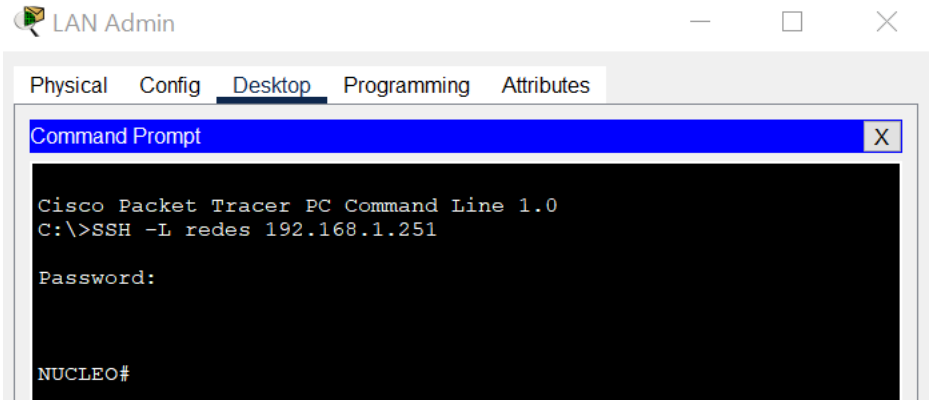
1) Desactive el resto de las terminales de acceso remoto mediante TELNET.

NUCLEO(config)#line vty 1 15

NUCLEO(config-line)#no transport input

NUCLEO(config-line)#transport input ssh

2) Verifique el funcionamiento correcto de SSH y la desactivación de TELNET mediante la línea de comandos DOS.



```
C:\>telnet 192.168.1.251
Trying 192.168.1.251 ...Open

[Connection to 192.168.1.251 closed by foreign host]
C:\>
```

TIEMPO ASIGNADO: 180 minutos

CRITERIO DE EVALUACION

Se aprobará el TLab si se alcanzan los siguientes resultados:

1. Ejecución correcta de las actividades experimentales y logro de los objetivos técnicos.
2. Respuestas satisfactorias a evaluaciones orales individuales sobre situaciones de configuración en el simulador.
3. Aprobación de evaluación de configuración del dispositivo en el simulador con calificación SUFICIENTE o MUY BUENO.