Ministerio de Educación
Gobierno de Chile

UNIVERSIDAD CATÓLICA DE TEMUCO

IMPLEMENTANDO SEGMENTACIÓN DE REDES, SEGURIDAD DE PUERTOS, PROTOCOLOS DE ENRUTAMIENTO Y ELABORACIÓN DE INFORME TÉCNICO

Módulo 9: **Mantenimiento de redes de acceso y banda ancha.**

Telecomunicaciones

Perfil de Egreso - Objetivos de Aprendizaje de la Especialdad

Módulo 1

OA1 Leer y utilizar esquemas, proyectos y en general todo el lenguaje simbólico asociado a las operaciones de montaje y mantenimiento de redes de telecomunicaciones.

Módulo 2

OA6 Realizar mantenimiento y reparaciones menores en equipos ysistemas de telecomunicaciones, utilizando herramientas y pautas de mantención establecidas por el fabricante.

OA7 Aplicar la normativa y los implementos de seguridad y protección relativos almontaje y el mantenimiento de las instalaciones de telecomunicaciones y la normativa del medio ambiente.

Módulo 3

OA2 Instalar equipos y sistemas de telecomunicaciones de generación, transmisión, repetición, amplificación, recepción, y distribución de señal de voz, imagen y datos, según solicitud de trabajo y especificaciones técnicas del proyecto.

OA10 Determinar los equipos y sistemas de comunicación necesarios para una conectividad efectiva y eficiente, de acuerdo a los requerimientos de los usuarios.

Módulo 4

OA9 Detectar y corregir fallas en circuitos de corriente continua de acuerdo a los requerimientos técnicos y de seguridad establecidos.

Módulo 5

OA2 Instalar equipos y sistemas de telecomunicaciones de generación, transmisión, repetición, amplificación, recepción y distribución de señal de voz, imagen y datos, según solicitud de trabajo y especificaciones técnicas del proyecto.

OA4 Realizar medidas y pruebas de conexión y de continuidad de señal eléctrica, de voz, imagen y datos- en equipos, sistemas y de redes de telecomunicaciones, utilizando instrumentos de medición y certificación de calidad de la señal autorizada por la normativa vigente.

Módulo 6

OA8 Instalar y configurar una red inálambrica según tecnologías y protocolos establecidos.

OA7 Aplicar la normativa y los implementos de seguridad y protección relativos al montaje y el mantenimiento de las instalaciones de telecomunicaciones y la normativa del medio ambiente.

Módulo 7

OA5 Instalar y configurar una red de telefonía (tradicional o IP) en una organización según los parámetros técnicos establecidos.

Módulo 8

OA3 Instalar y/o configurar sistemas operativos en computadores o servidores con el fin de incorporarlos a una red laN, cumpliendo con los estándares de calidad y seguridad establecidos.

Módulo 9

OA10 Determinar los equipos y sistemas de comunicación necesarios para una conectividad efectiva y eficiente, de acuerdo, a los requerimientos de los usuarios.

OA6 Realizar el mantenimiento y reparaciones menores en equipos y sistemas de telecomunicaciones, utilizando herramientas y pautas de mantención establecidas por el fabricante.

Módulo 10

No está asociado a Objetivos de Aprendizaje de la Especialidad (AOE), sino a genéricos. No obstante, puede asociarse a un OAE como estrategia didáctica.

Perfil de Egreso – Objetivos de Aprendizaje Genéricos

A- Comunicarse oralmente y por escrito con claridad, utilizando registros de habla y de escritura pertinentes a la situación laboral y a la relación con los interlocutores.	**B-** Leer y utilizar distintos tipos de textos relacionados con el trabajo, tales como especificaciones técnicas, normativas diversas, legislación laboral, así como noticias y artículos que enriquezcan su experiencia laboral.	**C-** Realizar las tareas de manera prolija, cumpliendo plazos establecidos y estándares de calidad, y buscando alternativas y soluciones cuando se presentan problemas pertinentes a las funciones desempeñadas.
D- Trabajar eficazmente en equipo, coordinando acciones con otros in situ o a distancia, solicitando y prestando cooperación para el buen cumplimiento de sus tareas habituales o emergentes.	**E-** Tratar con respeto a subordinados, superiores, colegas, clientes, personas con discapacidades, sin hacer distinciones de género, de clase social, de etnias u otras.	**F-** Respetar y solicitar respeto de deberes y derechos laborales establecidos, así como de aquellas normas culturales internas de la organización que influyen positivamente en el sentido de pertenencia y en la motivación laboral.
G- Participar en diversas situaciones de aprendizaje, formales e informales, y calificarse para desarrollar mejor su trabajo actual o bien para asumir nuevas tareas o puestos de trabajo, en una perspectiva de formación permanente.	**H-** Manejar tecnologías de la información y comunicación para obtener y procesar información pertinente al trabajo, así como para comunicar resultados, instrucciones e ideas.	**I-** Utilizar eficientemente los insumos para los procesos productivos y disponer cuidadosamente los desechos, en una perspectiva de eficiencia energética y cuidado ambiental.
J- Emprender iniciativas útiles en los lugares de trabajo y/o proyectos propios, aplicando principios básicos de gestión financiera y administración para generarles viabilidad.	**K-** Prevenir situaciones de riesgo y enfermedades ocupasionales, evaluando las condiciones del entorno del trabajo y utilizando los elementos de protección personal según la normativa correspondiente.	**L-** Tomar decisiones financieras bien informadas, con proyección a mediano y largo plazo, respecto del ahorro, especialmente del ahorro previsional, de los seguros, y de los riesgos y oportunidades del endeudamiento crediticio así como de la inversión.

Marco de Cualificaciones Técnico Profesional (MCTP) Nivel 3 y su relación con los OAG

HABILIDADES

1. Información
1. Analiza y utiliza información de acuerdo a parámetros establecidos para responder a las necesidades propias de sus actividades y funciones.
2. Identifica y analiza información para fundamentar y responder a las necesidades propias de sus actividades.

2. Resolución de problemas
1. Reconoce y previene problemas de acuerdo a parámetros establecidos en contextos conocidos propios de su actividad o funcion.
2. Detecta las causas que originan problemas en contextos conocidos de acuerdo a parámetros establecidos.
3. Aplica soluciones a problemas de acuerdo a parámetros establecidos en contextos conocidos propios de una función.

3. Uso de recursos
1. Selecciona y utiliza materiales, herramientas y equipamiento para responder a una necesidad propia de una actividad o función especializada en contextos conocidos.
2. Organiza y comprueba la disponibilidad de los materiales, herramientas y equipamiento.
3. Identifica y aplica procedimientos y técnicas específicas de una función de acuedo a parámetros establecidos.

4. Comunicación
4. Comunica y recibe información relacionada a su actividad o función, a través de medios y soportes adecuados en contextos conocidos.

APLICACIÓN EN CONTEXTO

5. Trabajo con otros
1. Trabaja colaborativamente en actividades y funciones coordinándose con otros en diversos contextos.

6. Autonomía
1. Se desempeña con autonomía en actividades y funciones especializadas en diversos contextos con supervisión directa.
2. Toma decisiones en actividades propias y en aquellas que inciden en el quehacer de otros en contextos conocidos.
3. Evalua el proceso y el resultado de sus actividades y funciones de acuerdo a parámetros establecidos para mejorar sus prácticas.
4. Busca oportunidades y redes para el desarrollo de sus capacidades

7. Ética y responsabilidad
1. Actúa de acuerdo a las normas y protocolos que guían su desempeño y reconoce el impacto que la calidad de su trabajo tiene sobre el proceso productivo o la entrega de servicios.
2. Responde por cumplimiento de los procedimientos y resultados de sus actividades.
3. Comprende y valora los efectos de sus acciones sobre la salud y la vida, la organización, la sociedad y el medio ambiente.
4. Actúa acorde al marco de sus conocimientos. experiencias y alcance de sus actividades y funciones

CONOCIMIENTO

8. Conocimientos
1. Demuestra conocimientos especificos de su área y de las tendencias de desarrollo para el desempeño de sus actividades y funciones.

Metodología seleccionada

Aprendizaje Basado en Problemas (ABP)

- Esta presentación les ayudará a poder comprender los conceptos necesarios para el desarrollo de su actividad.

Aprendizaje Esperado

- **AE2.** Establece comunicación entre dispositivos en redes LAN/WAN utilizando protocolos de comunicaciones de acuerdo a las especificaciones técnicas del proyecto y estándares de la industria.

¿Qué vamos a lograr con esta actividad para llegar al Aprendizaje Esperado (AE)?

Implementar segmentación de redes VLAN e inter VLAN, configurar seguridad en los puertos de un switch, configurar protocolos de enrutamiento y elaborar informe técnico con los resultados.

Contenidos

01 Segmentación de redes en un switch utilizando VLAN e Inter-VLAN

02 Configuración de seguridad de puertos en un switch.

03 Configuración de protocolos de enrutamiento wan.

04 Elaboración de informe técnico.

Segmentación de redes en un switch utilizando VLAN

¿Qué observamos en esta imagen?

¿Qué es un VLAN?

- Las VLAN son redes de área local virtuales, este método permite poder crear redes lógicamente independientes, pero existen en una misma red física, donde se agrupan los equipos en un determinado segmento.

- Las VLAN tienen su propio segmento de dirección IP, organizando de mejor forma la red y se crean dominios de difusión más pequeños, el cual mejorará el rendimiento de las redes.

Beneficios de las VLAN

- Disminución de transmisión de tráfico entre las VLAN.
- Mayor seguridad, encapsulando la información de las diferentes VLAN.
- Reducción de costos, sacando mayor provecho a los dispositivos físicos agrupando sus interfaces de forma lógica.
- Administración, es mucho más fácil administrar las redes y asignar recursos.

Tipos de VLAN

La VLAN existente en los switches:

a. **VLAN de datos de los usuarios:** de forma predeterminada la VLAN que se utiliza en un switch es la VLAN1.

b. **VLAN nativa:** se utiliza para el tráfico sin etiquetar cuando un puerto esta en estado trunk 802.1q.

c. **VLAN de administración:** Se utiliza para el tráfico de la VTY ya sea por conexión telnet o SSH para a la administración de los dispositivos.

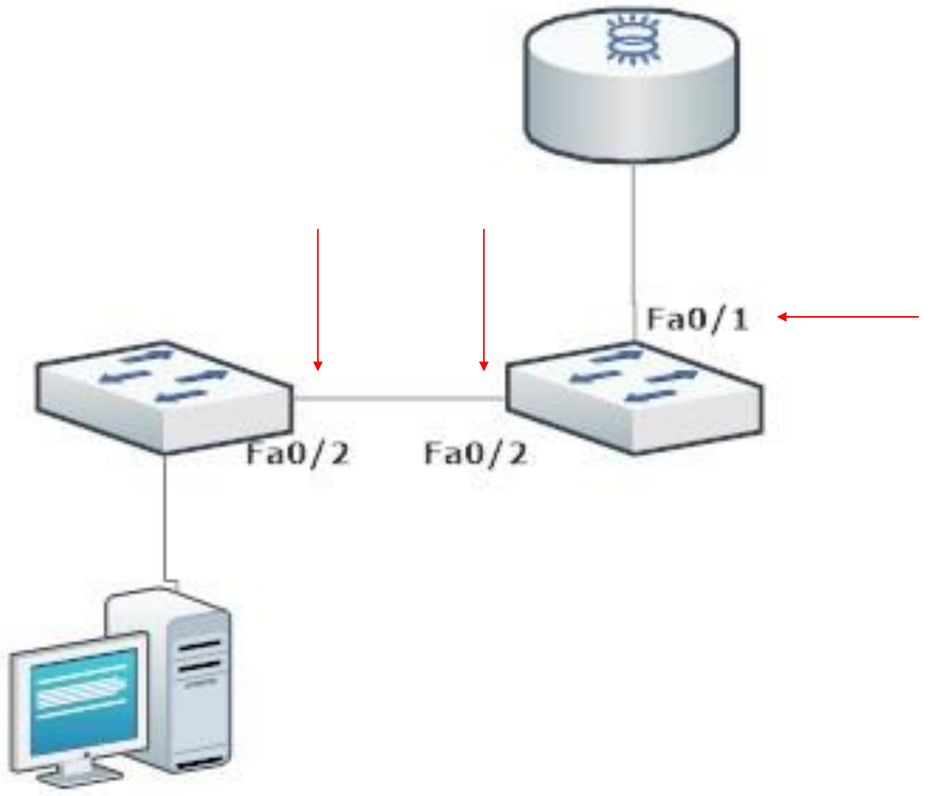
VLAN predeterminada

La VLAN predeterminada la podemos visualizar con el comando **show VLAN brief**, la cual nos indica que la VLAN1 es de forma predeterminada la VLAN nativa, VLAN de administración y como se puede observar, todos los puertos del switch están asignadas a esta VLAN predeterminada.

```
Switch#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                   Gig0/1, Gig0/2
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
Switch#
```

Enlace troncal

Los enlaces troncales son enlaces punto a punto en la interconexión de switch en un red. Estos puertos no se asignan a ninguna VLAN y son los encargados de transportar la información de las VLAN de un switch a otro. El protocolo que utilizan es IEEE802.1q para el etiquetado de las VLAN.



Creación de VLAN

Para poder crear VLAN en un switch debemos entrar a la configuración global y utilizar el comando **VLAN ID** y luego podremos darle un nombre **name VLAN-NAME** para poder identificarla.

```
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Estudiantes
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Profesores
Switch(config-vlan)#
```

Creación de VLAN

- Al visualizar con el comando **show VLAN brief** encontraremos dos VLAN en el sistema con sus nombres respectivos:

```
Switch#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                   Gig0/1, Gig0/2
10   Estudiantes                         active
20   Profesores                          active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
Switch#
```

Asignación de puertos a una VLAN

- Ya que hemos podido crear algunas VLAN, estamos en condiciones de poder asignar puertos a esas VLAN.

```
Switch(config)#interface  fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
```

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
10   Estudiantes                      active    Fa0/3
20   Profesores                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Eliminación de VLAN

- Para poder eliminar una VLAN solo debemos escribir el comando **no VLAN ID** y se eliminará del listado de VLAN.

```
Switch(config)#no vlan 20
Switch(config)#do show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                   Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                   Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                   Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                   Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                   Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                   Gig0/2
10   Estudiantes                         active    Fa0/3
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
```

Eliminación de VLAN

- En el caso de eliminar todas las VLAN podemos usar el comando **delete flash:VLAN.dat o delete VLAN.dat**, una vez que confirmamos sólo nos quedaría reiniciar nuestro switch.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]

Switch#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0000.0C47.9884
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 2 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4416258
flashfs[0]: Bytes available: 59600126
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
#########
```

Configuración de puertos troncales

- Ingresamos a la interfaz troncal y habilitamos el modo troncal, la VLAN nativa y permitir las VLAN que utilizarán el enlace troncal.

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#switchport trunk allowed vlan 10,20,99
Switch(config-if)#
```

Visualizar configuración en un troncal

- Para visualizar las configuraciones de una interfaz troncal utilizaremos el comando **show interface trunk.**

```
Switch#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,20,99

Port        Vlans allowed and active in management domain
Fa0/1       10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,20

Switch#
```

Reflexionemos

¿Cuál es el propósito de utilizar VLAN en una red?

Inter-VLAN routing

¿Qué es inter-VLAN routing?

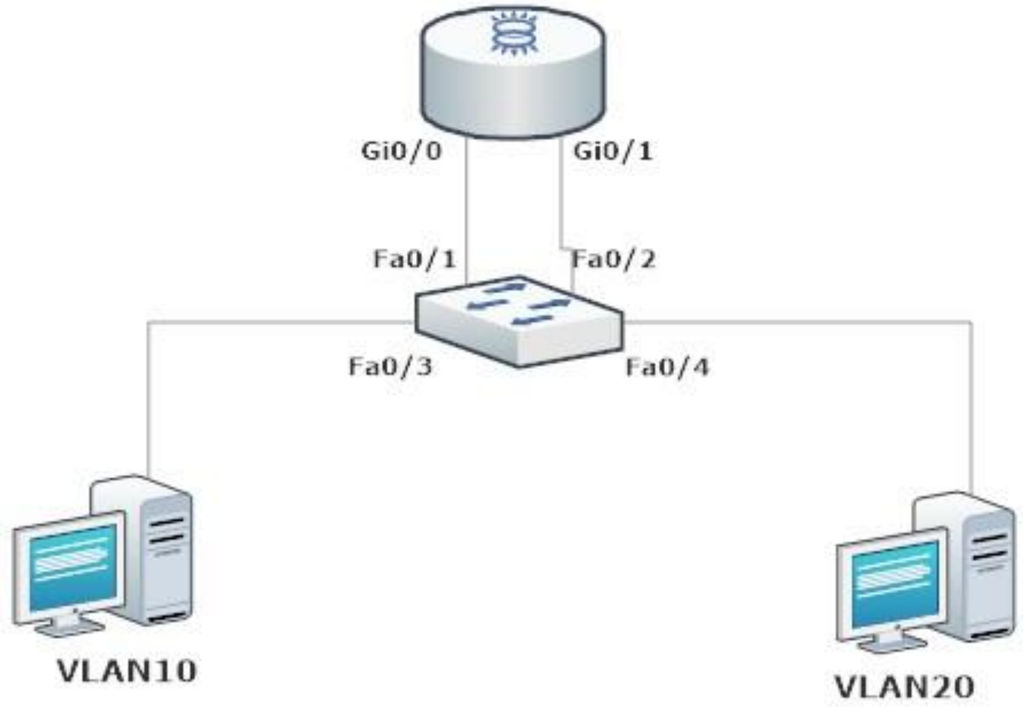
- Es el proceso para poder comunicar las distintas VLAN creadas en nuestra red mediante un router, ya que los switches de capa 2 no pueden enrutar tráfico entre las VLAN.

  Existen dos formas de ruteo de VLAN para una red existente:

1. **Ruteo de VLAN antiguo.**
2. **Ruteo de VLAN con routing on-a-stick.**

Ruteo de VLAN antiguo

- Se utilizaban los router con una interfaz física para cada VLAN, de esta forma enrutan las VLAN de una interfaz a otra. El problema ocurría cuando las empresas tenían muchas VLAN, por lo tanto, necesitaban muchas interfaces físicas para poder comunicarlas.



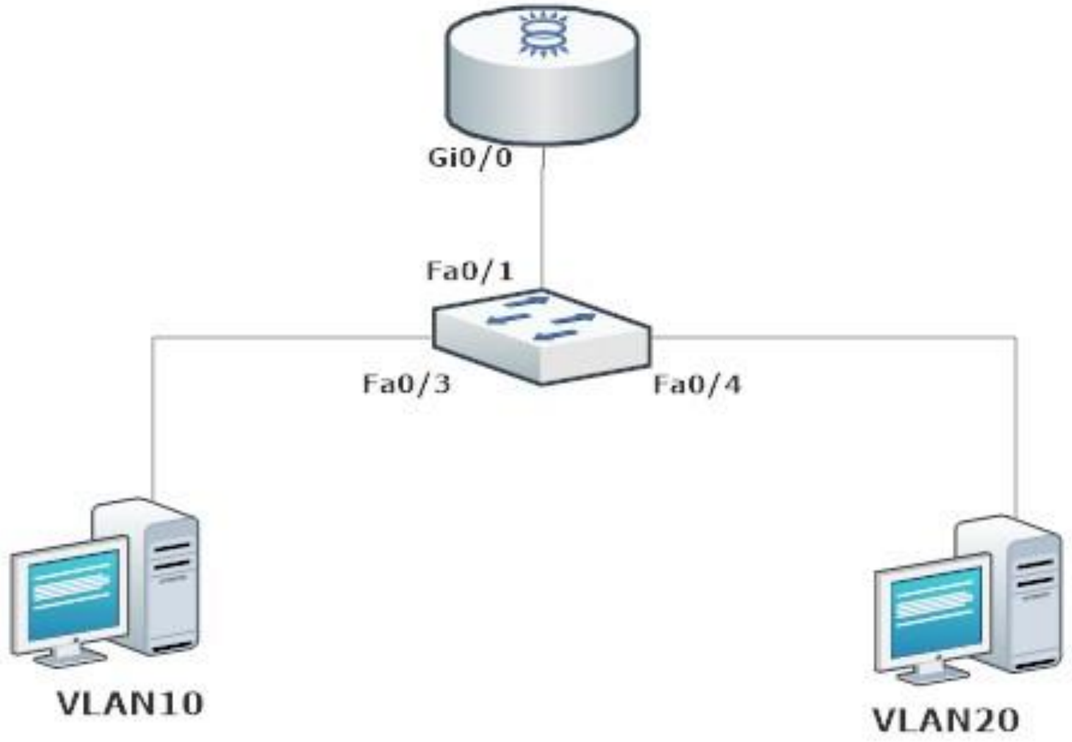
Ruteo de VLAN antiguo

- Como se puede observar, este tipo de ruteo configuraban las interfaces físicas con el direccionamiento IP de cada VLAN.

```
Router(config)#int gi0/0
Router(config-if)#ip add 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config)#int gi0/1
Router(config-if)#ip add 192.168.20.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

Router(config-if)#
```

Ruteo de VLAN con routing-on-a-stick

- Este tipo de ruteo utiliza una interfaz física del router como troncal para poder comprender el etiquetado de las VLAN que viajarán por ellas. Para hacer uso de esta interfaz física para diferentes VLAN, se utilizarán sub interfaces para cada una de las VLAN que necesitemos comunicar en la red.



Configuración routing-on-a-stick

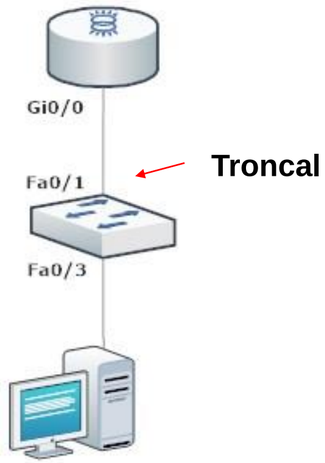
- Al configurar las subinterfaces del router se asocian a un número de VLAN y en cada una especificaremos el protocolo de etiquetado y la dirección IP asignada a esa VLAN, utilizándose como puerta de enlace.

  Un punto importante es siempre habilitar la interfaz física.

```
Router(config)#interface gi0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#interface gi0/0.20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gi0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up
```

Configuración routing-on-a-stick

- En el extremos de la conexión del switch debemos tener creadas nuestras VLAN y dejar el puerto en modo troncal.



Troncal

```
Switch(config)#vlan 10
Switch(config-vlan)#name Estudiantes
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Profesores
Switch(config-vlan)#exit
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#
```

Reflexionemos

¿Cuáles son las diferencias y similitudes del sistema de ruteo antiguo de VLAN con el rute routing-on-a-stick?

¿Qué piensas al ver estas imágenes? ¿Por qué?

Configuración de seguridad de puertos en un switch

¿Qué es la seguridad de puertos?

- Es la encargada de dar seguridad a todas las interfaces de un switch (puertos). La seguridad de los puertos parte desde el acceso por consola de forma local o por alguna conexión VTY de forma remota, como por ejemplo, telnet o SSH. Para ello configuraremos la interfaz virtual del switch para su administración y luego el acceso remoto con SSH.

Configuración de interfaz de administración.

- Ingresamos al modo configuración global, ingresar a la interfaz de la (SVI) e ingresar la dirección IP y máscara de la interfaz de administración y finalmente habilitamos la interfaz.

```
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 99
Switch(config-if)#ip address 192.168.0.10 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

Configuración de interfaz de administración.

En la configuración global ingresamos la dirección IP de la puerta de enlace del router.

Al finalizar los ingresos siempre es muy importante guardar los cambios.

```
Switch(config)#ip default-gateway 192.168.0.1
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

Configuración del acceso remoto con SSH

- **SSH** es un protocolo de conexión remota a dispositivos en una red, utilizando el **puerto 22** para realizar esta operación y toda la información viaja por la red de forma **cifrada**, dando mayor seguridad a la conexión y administración remota que necesitemos. Este tipo de protocolo sobrepasa los niveles de seguridad del protocolo telnet, que también es un protocolo de conexión remota.

Configuración del acceso remoto con SSH

1. Configuración de dominio.
2. Generar clave RSA.
3. Configurar un usuario local para la administración.
4. Habilitar versión 2 de SSH.
5. Y configurar la conexión remota con SSH.

```
S1(config)#ip domain-name dominio.cl
S1(config)#crypto key generate rsa
The name for the keys will be: S1.dominio.cl
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#username admin secret cisco
*Mar 1 0:9:12.285: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#ip ssh version 2
S1(config)#line vty 0 4
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
S1(config)#
```

¿Para qué sirve la seguridad de puertos?

- El método de seguridad de puertos realizará acciones analizando las direcciones MAC de los dispositivos que se están conectando a las interfaces de un switch y verifica si la dirección MAC es permitida o no. Para poder habilitar la seguridad de puertos lo haremos con el comando **switchport port-security** en las interfaces que queramos proteger.

Configuración de seguridad de puertos.

Antes de realizar la configuración de puertos, debemos saber dos cosas importantes:

1. **Toda interfaz que no esté ocupando en un switch, se recomienda apagar y solo habilitar en el caso que sea necesario con el comando shutdown al interior de la interfaz solicitada**

2. **De forma predeterminada la seguridad de puertos viene deshabilitada, tiene como condición conocer una MAC en su puerto y por defecto tiene la opción de violación en shutdown.**

Configuración de seguridad de puertos.

- Como podemos observar la seguridad de puerto está deshabilitada de manera predeterminada en los switches.

```
Switch#show port-security interface fa0/1
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
Switch#
```

Configuración de seguridad de puerto.

Para poder configurar la seguridad de un puerto debemos entrar a la configuración global e ingresar a una interfaz la cual queramos proteger, pero arroja un error por estar en estado dinámico. Para ello debemos especificar el modo de la interfaz, en este caso debe estar en modo de acceso para los equipos terminales que se conecten y luego nos permitirá habilitar la seguridad en un puerto sin problemas.

```
Switch(config)#interface fa0/3
Switch(config-if)#switchport port-security
Command rejected: FastEthernet0/3 is a dynamic port.
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
```

Configuración de seguridad de puerto

- Una vez habilitada la seguridad de un puerto podremos configurar sus parámetros.

```
Switch(config-if)#switchport port-security ?
  aging          Port-security aging commands
  mac-address    Secure mac address
  maximum        Max secure addresses
  violation      Security violation mode
  <cr>
```

Configuración de seguridad de puerto.

- Las direcciones MAC se pueden ingresar manualmente con el comando especificando una dirección MAC válida:

```
Switch(config-if)#switchport port-security mac-address ?
  H.H.H    48 bit mac address
  sticky   Configure dynamic secure addresses as sticky
Switch(config-if)#switchport port-security mac-address 00D0.FF84.4AA4
```

- Y para que pueda aprender las direcciones MAC y mantenerlas guardadas en su configuración digitamos lo siguiente:

```
Switch(config-if)#switchport port-security mac-address ?
  H.H.H    48 bit mac address
  sticky   Configure dynamic secure addresses as sticky
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#
```

Configuración de seguridad de puerto.

- Configuración del número máximo de direcciones MAC que puede permitir un puerto, por defecto permite una, pero podemos permitir hasta 132 direcciones en el caso que se requiera.

```
Switch(config-if)#switchport port-security maximum ?
  <1-132>  Maximum addresses
Switch(config-if)#switchport port-security maximum 4
Switch(config-if)#
```

Configuración de seguridad de puerto.

Un ejemplo para configurar una interfaz:

1. **Se habilita el modo acceso en la interfaz del switch.**
2. **Se habilita la seguridad del puerto.**
3. **Se habilita el máximo de direcciones que debe aceptar.**
4. **Se habilita que una de las MAC sea configurada de forma estática.**
5. **Se habilita que las demás direcciones MAC se las aprenda de forma automática.**

Describan con sus palabras,

¿Para qué sirve la seguridad de puertos?

Configuración de seguridad de puertos en un switch

Acciones en una interfaz si se produce una violación.

- Las acciones en un puerto se pueden activar cuando se alcance el número máximo de direcciones MAC permitidas, una dirección MAC que se aprende en un puerto y se lo aprende por otro.

- Para ello se establecen modos de configuración de violaciones para detectar estas acciones.

Los tipos de acciones son los siguientes:

1. **Protect.**
2. **Restrict.**
3. **Shutdown (viene por defecto activa en los switches).**

```
Switch(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#
```

Acciones en una interfaz si se produce una violación.

- **Protect:** Solo se autorizará el tráfico de las direcciones MAC permitidas y para las MAC no permitidas descartó todo el tráfico que se envíe por esa interfaz. No dará aviso al administrador.

- **Restrict:** Solo se autorizará el tráfico de las direcciones MAC permitidas y para las MAC no permitidas descartarán todo el tráfico que se envíe por esa interfaz. Dará aviso al administrador.

- **Shutdown:** La interfaz se deshabilita quedando en un estado de error(err-disabled) y envía un aviso al administrador.

Ejemplo de seguridad en un puerto

1. Entramos a la interfaz que deseamos configurar.
2. Ponemos el puerto en modo de acceso para la conexión de equipos terminales.
3. Habilitamos la seguridad en el puerto.
4. Habilitamos el máximo de direcciones MAC.
5. Habilitaremos que las direcciones MAC las aprenda.
6. Habilitamos la violación, en este caso, con restrict descartará todo el trafico en el puerto.

```
Switch(config)#interface fa0/3
Switch(config-if)#switchport mode acces
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation restrict
```

Visualizar las configuraciones de puertos.

Una vez configuradas nuestras interfaces, podremos revisar la seguridad de las interfaces configuradas con el comando **show port-security**, donde visualizamos sus contadores correspondientes del máximo de direcciones MAC permitidas, contador de MAC aprendidas, su contador de violaciones ocurridas y la acción de cada interfaz.

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)         (Count)
-------------------------------------------------------------------------
        Fa0/3        2           1                0          Restrict
        Fa0/4        4           0                0          Shutdown
-------------------------------------------------------------------------
Switch#
```

Visualizar las configuraciones de puertos.

Para revisar de forma más completa la seguridad de una interfaz en particular, utilizaremos el comando **show port-security interface [Numero interfaz]**, el cual desplegar[a toda la información aplicada en dicha interfaz.

```
Switch#show port-security interface fa0/3
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 000A.F393.C2D8:1
Security Violation Count   : 0

Switch#
```

Habilitar interfaces con estado err-disabled.

Cuando configuremos alguna interfaz con acción de **shutdown** y detecte una violación, la interfaz quedará en estado de deshabilitada por error. Por lo tanto, cuando ocurra esta acción tendremos que manualmente apagar la interfaz y habilitar nuevamente.

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
-------------------------------------------------------------------------
        Fa0/3        2           2                1          Shutdown
        Fa0/4        4           0                0          Shutdown
-------------------------------------------------------------------------
Switch#show port-security interface fa0/3
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 2
Last Source Address:Vlan   : 0004.9AA6.9A92:1
Security Violation Count   : 1
```

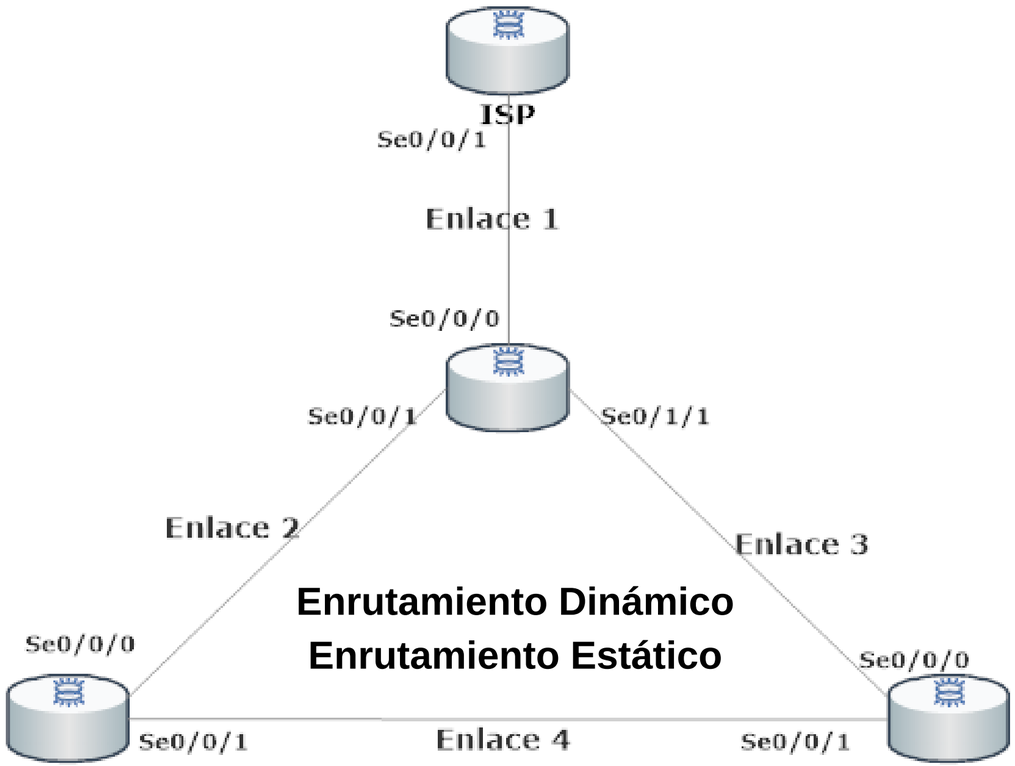
```
Switch(config)#interface fa0/3
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
```

Reflexionemos

¿Podrías establecer los pasos para configurar la seguridad de puertos en un switch?

Protocolos de enrutamiento

RECORDEMOS LA CONFIGURACIÓN DE PROTOCOLOS DE ENRUTAMIENTO



Protocolo de enrutamiento

Una vez configurada nuestras redes, podremos hacer uso de protocolos de enrutamiento para poder comunicarnos con otras sucursales o empresas que queramos interconectar, para ello recordaremos algunos protocolos compatibles con IPv4 e IPv6:

a. **Protocolo de enrutamiento dinámico:** Ripv2 y RIPng.

b. **Protocolo de enrutamiento estático:** Ip route para IPv4 e IPv6.

Los revisaremos en un entorno práctico para su mejor comprensión.

Pruebas de conectividad

Recordaremos algunos comandos para verificar la conectividad, adicional a los ya vistos en nuestra presentación:

Comandos par probar conectividad:

a. **Ping.**
b. **Traceroute.**
c. **Tracert.**

Comando show comunes para verificar configuraciones:

a. **Show ip route.**
b. **Show ip interface.**
c. **Show ip interface fa0/0.**

POR ÚLTIMO….RECORDEMOS LA ESTRUCTURA DE INFORME TÉCNICO

Estructura de un informe técnico

Ahora nos encontramos en condiciones de poder realizar un informe técnico, empleando un lenguaje técnico para poder evidenciar el trabajo realizado y recordaremos su estructura:

a. **Presentación:** está constituida por la portada y el índice, donde la portada contiene el título del informe, integrantes, la fecha de presentación y el índice nos indicará la tabla de contenidos del informe.

b. **Introducción:** se presenta brevemente una descripción de lo que se va a tratar el informe.

c. **Objetivo:** es el propósito del informe, lo que se piensa lograr, investigar, demostrar o conocer.

Estructura de un informe técnico

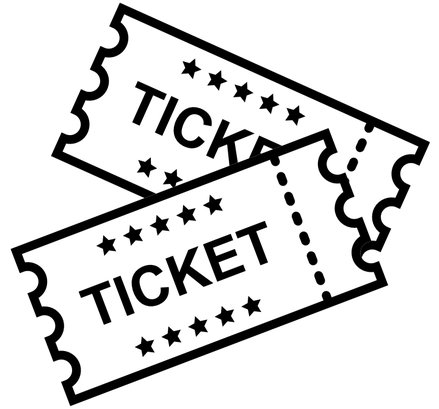
d. Desarrollo: es la parte más extensa del informe, que puede estar conformada por varios capítulos, los cuales nos indicarán todo el proceso el cual desarrollarán en este informe técnico. La información debe organizarse de tal modo que se muestre como un todo a lo largo del texto.

e. Conclusión: es el final de cualquier proceso de investigación, donde se señala lo más importante del informe. Debe ser clara y precisa, siendo el resultado de lo realizado en el informe.

f. Recomendaciones: son sugerencias que ofrece el técnico una vez que se han expuesto los resultados del trabajo.

¿Tienes preguntas de lo trabajado hasta aquí?

Ticket de salida



01

¿Cómo explicarías el funcionamiento de las redes con VLAN e inter-VLAN a un compañero o compañera que no entiende mucho este tema?

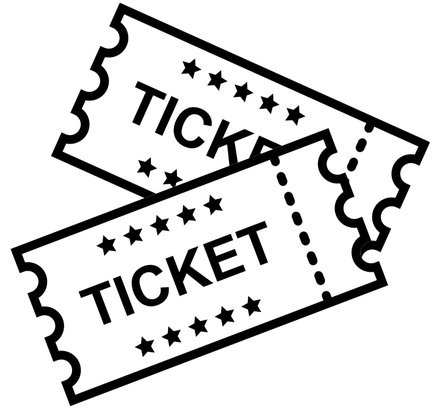
02

¿Estás en condiciones de poder configurar las interfaces de un switch con seguridad en sus puertos? Si consideras que sí, argumenta porqué. Si no fuera así, ¿cómo solucionarías esta situación?

03

¿Te sientes en condiciones de poder comunicar las redes con VLAN mediante un protocolo de enrutamiento? ¿Por qué?

Ticket de salida



04

¿Cuál es la importancia de un informe técnico en un proyecto?

05

¿Qué debilidades percibiste en tu desempeño durante el desarrollo de la actividad?

¿Cómo puedes trabajarlas para convertirlas en fortalezas?

REFERENCIAS DE CONTENIDO

- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book/ip6-dhcp.html
- https://www.cisco.com/c/es_mx/support/docs/lan-switching/inter-VLAN-routing/41860-howto-L3-interVLANrouting.html
- https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-3750-series-switches/72846-layer2-secftrs-catl3fixed.html
- https://www.netacad.com/

- **Libro Cisco CCENT/CCNA ICND1 100-105**

REFERENCIAS DE IMÁGENES POR ORDEN DE APARICIÓN EN EL PPT

- https://articulo.mercadolibre.cl/MLC-519910953-switch-cisco-sg350-52p-48p-gigabit-poe-2-sfp-VLAN-_JM
- https://www.reuter.com.ar/CCNA/CCNA2/mod2_ccna2/index_clip_image007_0000.png
- https://dan1t0.files.wordpress.com/2010/11/principal.png
- https://es.123rf.com/photo_79412921_informe-m%C3%A9dico-azul-dibujos-animados-vector-dise%C3%B1o-gr%C3%A1fico.html

- ***Las demás imágenes son de autoría personal.***