Ministerio de Educación
Gobierno de Chile

UNIVERSIDAD CATÓLICA DE TEMUCO

Configuración de seguridad en puertos de un switch, implementando segmentación de redes *(vlan, inter vlan)* y servicio DHCP para direccionamiento IPv4 e IPv6

Módulo 4: **Configuración y puesta en servicio de aplicaciones en redes de área local.**

Conectividad y Redes

Objetivos de Aprendizaje de la Especialidad

Módulo 1	**OA1** Leer y utilizar técnicamente proyectos de conectividad y redes, considerando planos o diagramas de una red de área local (red LAN), basándose en los modelos TCP/IP y OSI. **OA3** Instalar y mantener cableados estructurados, incluyendo fibra óptica, utilizados en la construcción de redes, basándose en las especificaciones técnicas correspondientes. **OA7** Instalar y configurar una red inalámbrica según tecnologías y protocolos establecidos.
Módulo 2	**OA2** Instalar y configurar sistemas operativos en computadores personales con el fin de incorporarlos a una red LAN, cumpliendo con los estándares de calidad y seguridad establecidos. **OA11** Armar y configurar un equipo personal, basándose en manuales de instalación, utilizando las herramientas apropiadas y respetando las normas de seguridad establecidos.
Módulo 3	**OA8** Aplicar herramientas de software que permitan obtener servicios de intranet e internet de manera eficiente.
Módulo 4	**OA4** Realizar pruebas de conexión y señales en equipos y redes, optimizando el rendimiento de la red y utilizando instrumentos de medición y certificación de calidad de la señal, considerando las especificaciones técnicas.
Módulo 5	**OA5** Aplicar métodos de seguridad informática para mitigar amenazas en una red LAN, aplicando técnicas como filtrado de tráfico, listas de control de acceso u otras.
Módulo 6	**OA9** Mantener y actualizar el hardware de los computadores personales y de comunicación, basándose en un cronograma de trabajo, de adcuerdo a las especificaciones técnicas del equipo.
Módulo 7	**OA10** Mantener actualizado el software de productividad y programas utilitarios en un equipo personal, de acuerdo a los requerimientos de los usuarios.
Módulo 8	**OA6** Aplicar procedimientos de recuperación de fallas y realizar copias de respaldo de los servidores, manteniendo la integridad de la información.
Módulo 9	No esta asociado a Objetivos de Aprendizaje de la Especialidad (OAE), 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

Estudio de Caso

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

.

Aprendizaje Esperado

- **AE3:** Configura solución de redes redundantes en switches (STP, Etherchannel) y routers(HSRP), manteniendo la estabilidad y seguridad a las redes, considerando normativa y estándares de la industria.

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

- **Configurar** la seguridad en puertos de un switch, implementando segmentación de redes vlan e inter vlan con direccionamiento IP mediante el servicio DHCPv4 y DHCPv6.

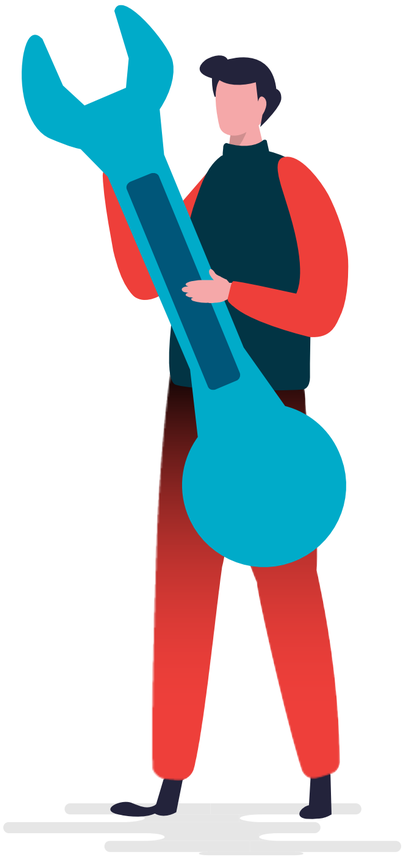
Contenidos:

¿Qué situación te sugiere 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

- Ingresaremos al modo configuración global, ingresar a la interfaz de la (SVI) e ingresar la dirección IP y mascara 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
```

Fuente propia

Configuración de interfaz de administración

- En la configuración global ingresaremos la dirección IP del 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#
```

Fuente propia

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

01 Configuración de dominio.

02 Generar clave RSA.

03 Configurar un usuario local para la administración.

04 Habilitar versión 2 de SSH.

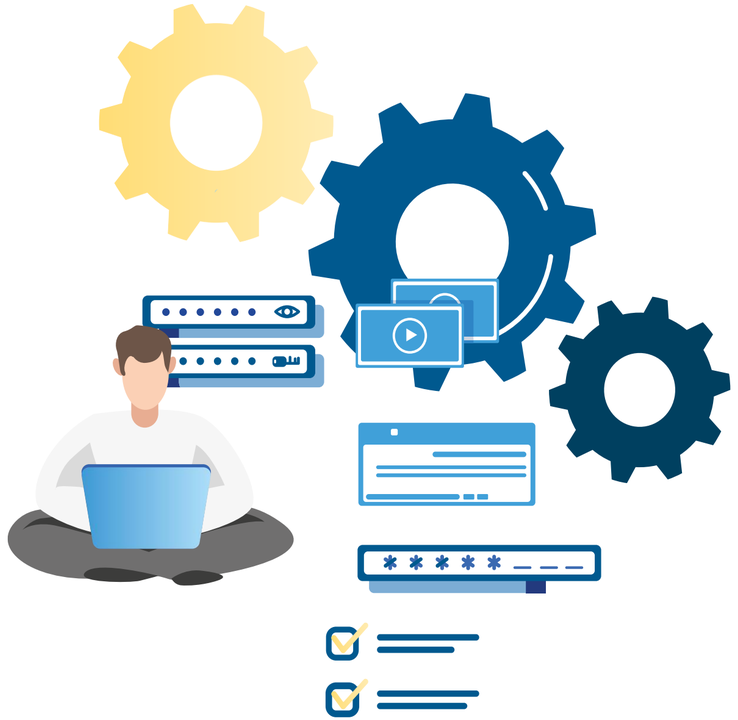
05 Y configurar la conexión remota con SSH.

```
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)#
```

Fuente propia

¿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:

01 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.

02 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 esta deshabilitada de manera predeterminada en los switch.

```
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#
```

Fuente propia

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
```

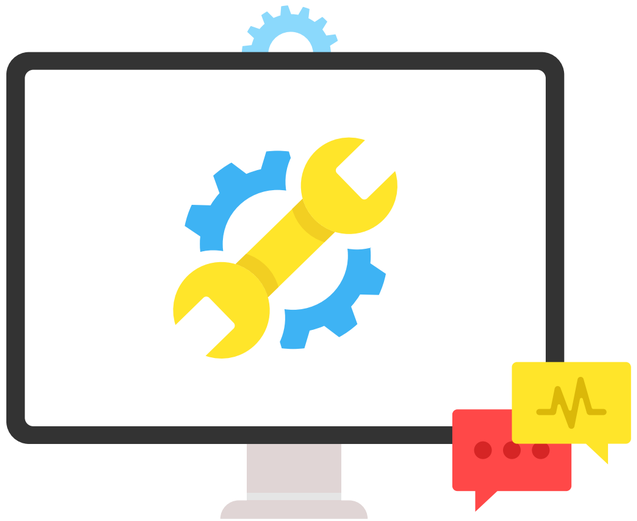
Fuente propia

Configuración de seguridad de puerto

- Una vez habilitada la seguridad de un puertos, 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>
```

Fuente propia



Configuración de seguridad de puerto

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

```
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, digitaremos 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)#
```

Fuente propia

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)#
```

Fuente propia

- Un ejemplo para configurar una interfaz:

01 Se habilita el modo acceso en la interfaz del switch.

02 Se habilita la seguridad del puerto.

03 Se habilita el máximo de direcciones que debe aceptar.

04 Se habilita que una de las MAC sea configurada de forma estática.

05 Se habilita que las demás direcciones MAC se las aprenda de forma automática.

```
Switch(config)#interface fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 4
Switch(config-if)#switchport port-security mac-address 00D0.D3EA.B19A
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#
```

Fuente propia

Describan con sus palabras, ¿para qué sirve la seguridad de puertos?

Acciones en una interfaz si se produce una violación

Las acciones en un puerto se pueden activar cuando se alcance el numero 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:

- Protect.
- Restrict.
- Shutdown (viene por defecto activa en los switch).

```
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)#
```

Fuente propia

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 descarto todo el tráfico que se envié 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 trafico que se envié 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

01 Entramos a la interfaz que deseamos configurar.

02 Ponemos el puerto en modo de acceso para la conexión de equipos terminales.

03 Habilitamos la seguridad en el puerto.

04 Habilitamos el máximo de direcciones MAC.

05 Habilitaremos que las direcciones MAC las aprenda.

06 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
```

Fuente propia

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#
```

Fuente propia

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 desplegará 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#
```

Fuente propia

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
```

Fuente propia

Reflexionemos

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

Segmentación de redes en un switch utilizando vlan.

Estructura de una dirección IPv4

- Las **vlan** son redes de área local virtuales. Este método permite poder crear redes lógicamente independientes, pero que 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 switch:

  - **Vlan de datos de los usuarios:** de forma predeterminada la vlan que se utiliza en un switch es la vlan1.

  - Vlan nativa: se utiliza para el tráfico sin etiquetar cuando un puerto está en estado trunk 802.1q.

  - 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

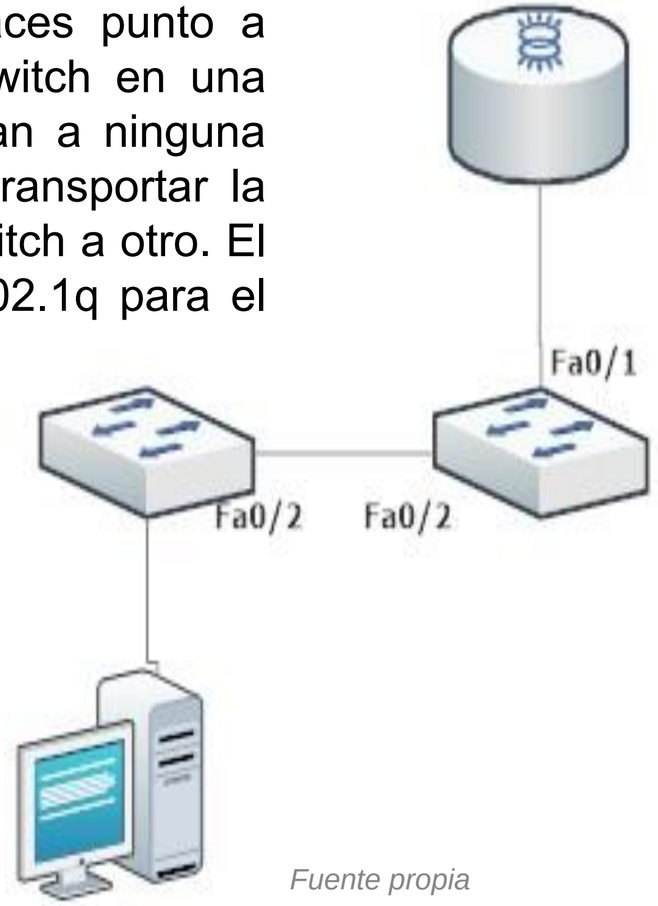
- La vlan predeterminada la podemos visualizar con el comando **show vlan brief**, la cual nos indica que la vlan1 es de forma predeterminada, la vlan nativa, vlan de administración y como se puede observar, todos los puertos del switch están asignadas a esta vlan predeterminada.

```
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#
```

Fuente propia

Enlace troncal

- Los enlaces troncales son enlaces punto a punto en la interconexión de switch en una 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.



Fuente propia

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)#
```

Fuente propia

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
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
Switch#
```

Fuente propia

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#
```

Fuente propia

Eliminación de vlan

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

```
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
```

Fuente propia

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"...
#########
```

Fuente propia

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)#
```

Fuente propia

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#
```

Fuente propia

Reflexionemos

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

Inter-vlan routing

¿Qué es inter-vlan routing?

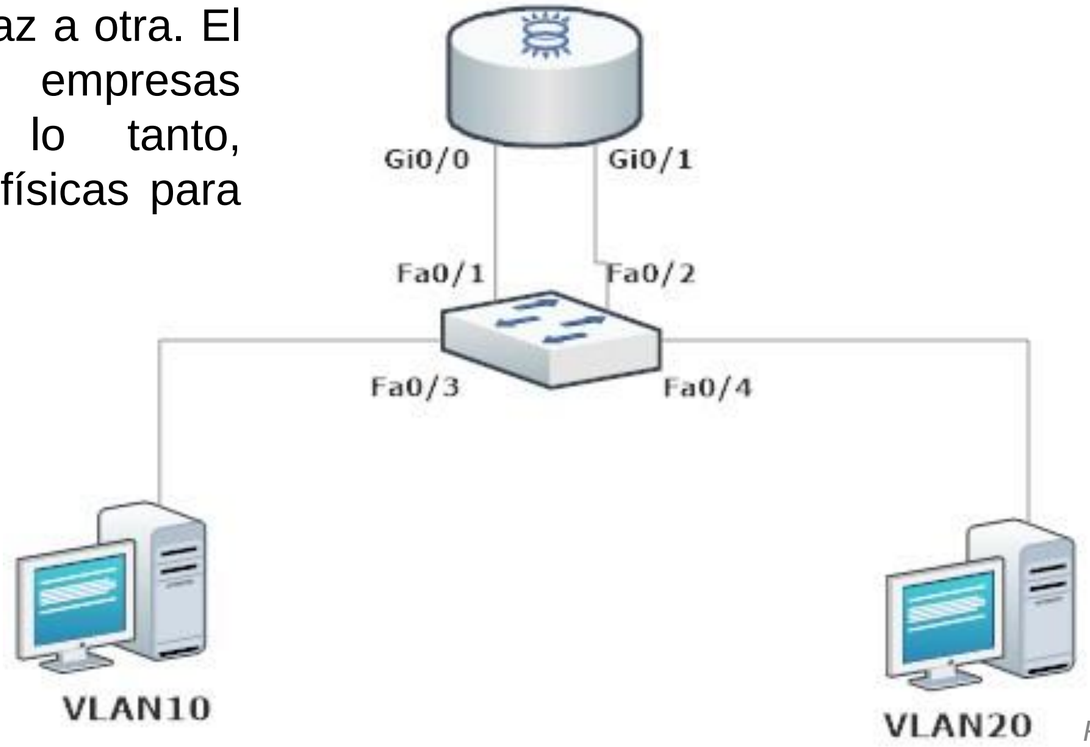
Es el proceso para poder comunicar las distintas vlan creadas en nuestra red mediante un router, ya que los switch de capa 2 no pueden enrutar tráfico entre las vlan.

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

- Ruteo de vlan antiguo.
- 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 enrutaban 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.



Fuente propia

Configuración de ruteo antiguo

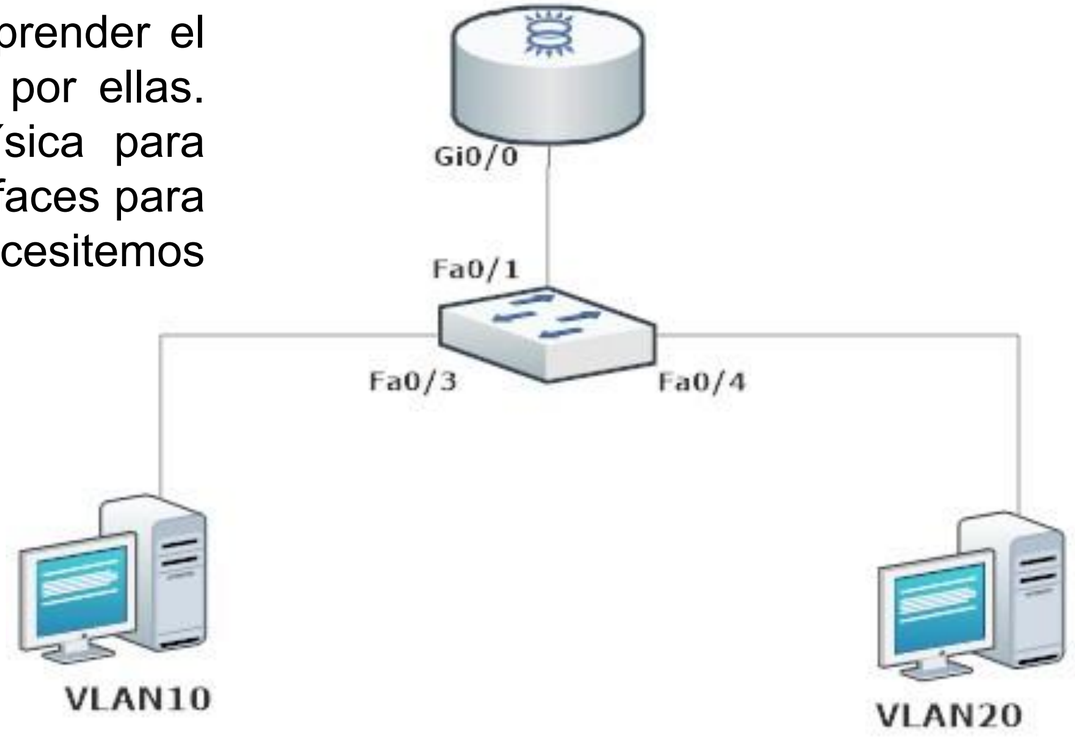
- Como se puede observar, este tipo de ruteo configuraba las interfaces físicas con el direccionamiento IP de cada vlan.

```
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-if)#exit
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)#
```

Fuente propia

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.



Fuente propia

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
```

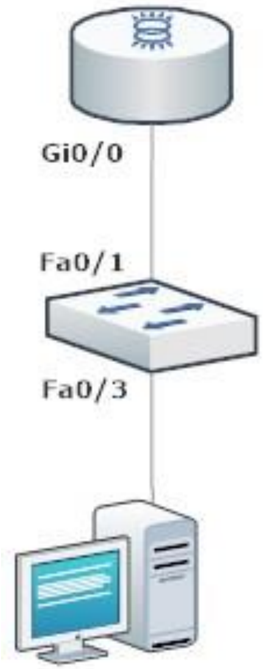
Fuente propia

Configuración routing-on-a-stick

- En el extremo de la conexión del switch debemos tener creadas nuestras vlan y dejar el puerto en modo 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)#
```

Fuente propia



Reflexionemos

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

Configuración de servicio DHCP.

¿Qué es DHCP?

DHCP significa protocolo de configuración de host dinámico y es utilizado para poder asignar direccionamiento IP de forma automática a los host de una red, simplificando la administración de direccionamiento IP en las redes.

Los datos asignados a un host pueden ser lo siguientes:

- Dirección IP y máscara de subred.
- Dirección IP de Servidor DNS.
- Dirección IP de puerta de enlace.
- Nombre de un dominio.

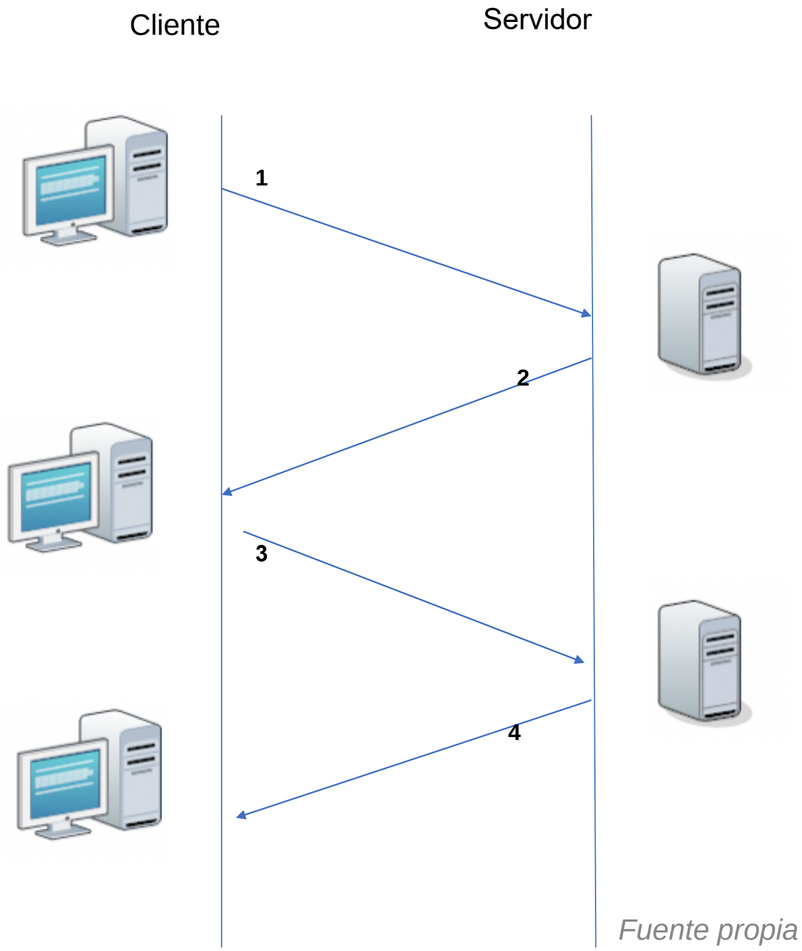
Funcionamiento DHCPv4

01 El cliente hace un broadcast de un mensaje de descubrimiento solicitando una IP.

02 El servidor manda un broadcast con un mensaje de oferta de un a dirección IP.

03 El cliente responde con un mensaje de “aceptando la dirección IP”.

04 El servidor hace acuso de recibo de la aceptación de la dirección IP del cliente.



Fuente propia

Configuración de DHCPv4

Podemos excluir direcciones que no se necesite asignar a los host y estarán reservadas.

Asignaremos un nombre al pool de direcciones que se asignan a los dispositivos de la red.

```
Router(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
Router(config)#ip dhcp excluded-address 192.168.10.254
Router(config)#ip dhcp pool NOMBRE-POOL
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#dns-server 192.168.10.10
Router(dhcp-config)#domain-name dominio.cl
Router(dhcp-config)#exit
Router(config)#
```

Fuente propia

Configuración de cliente DHCPv4

Debemos entrar a la interfaz que necesitamos que adquiera dirección IP por dhcp e ingresamos **IP address dhcp**, habilitamos la interfaz y debería asignar la dirección como se observa en la imagen.

```
Router(config)#interface gi0/1
Router(config-if)#ip address dhcp
Router(config-if)#no shutdown

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0/1 assigned DHCP address 200.0.0.2, mask
255.255.255.252, hostname Router0


Router(config-if)#do show ip interface gi0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Internet address is 200.0.0.2/30
  Broadcast address is 255.255.255.255
  Address determined by DHCP
  MTU is 1500 bytes
```

Fuente propia

Configuración de DHCPv6 con estado

El servicio DHCPv6 con estado funciona muy similar al de IPv4, el cual asignará direccionamiento IP a nuestros clientes de la red.
Habilitamos el servicio routing para IPv6 y realizamos nuestro Pool DHCPv6. Para finalizar habilitamos el servicio en la interfaz que está conectada a los clientes que necesiten IP por DHCPv6.

```
Router(config)#Ipv6 unicast-routing
Router(config)#ipv6 dhcp pool POOL-IPV6
Router(config-dhcpv6)#address prefix 2001:1234:ABCD:1::/64
Router(config-dhcpv6)#dns-server 2001:1234:ABCD:2::10
Router(config-dhcpv6)#domain-name dominio.cl
Router(config-dhcpv6)#exit
Router(config)#interface GigabitEthernet0/0.10
Router(config-subif)#ipv6 address 2001:1234:ABCD:1::1/64
Router(config-subif)#ipv6 nd managed-config-flag
Router(config-subif)#ipv6 dhcp server POOL-IPV6
Router(config-subif)#
```

Fuente propia

Configuración de cliente DHCPv6

Para configurar una interfaz de un router para que pueda recibir parámetros de red, debemos habilitar ipv6 en la interfaz y configurar la IP con dhcp.

```
Router(config)#interface gi0/1
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address dhcp
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ipv6 interface gi0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::201:63FF:FE15:3A02
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:AAA:2222:2:70A2:621F:621F:621F, subnet is 2001:AAA:2222:2::/64
  Joined group address(es):
```

Fuente propia

Reflexionemos

¿En qué ocasiones se necesita transmitir el servicio DHCP? ¿Por qué?

¿Tienes preguntas de lo trabajado hasta aquí?

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

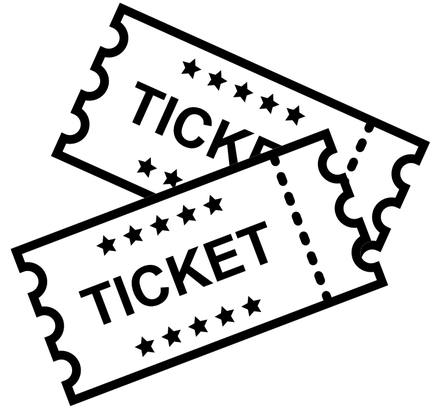
Referencias de imágenes por orden de aparición en el ppt :

- https://www.reuter.com.ar/CCNA/CCNA2/mod2_ccna2/index_clip_image007_0000.png

  https://dan1t0.files.wordpress.com/2010/11/principal.png

Las demás imágenes son de autoría personal.

Ticket de salida



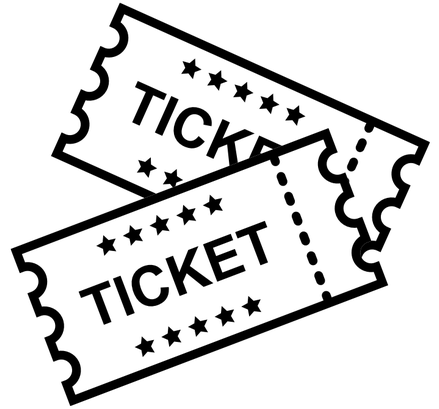
01

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

02

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

Ticket de salida



03

¿Podrías aplicar los conocimientos de servicios de DHCP a una situación práctica? ¿Podrías dar un ejemplo?

04

¿Qué debilidades percibiste en tu desempeño durante el desarrollo de la actividad? ¿Cómo puedes trabajarlas para convertirlas en fortalezas?