TALLER DE NETWORKING

AIEP Barrio Universitario
Escuela de Ingeniería, Energía & Tecnología
Ingeniería en Ciberseguridad

Marzo 2025

Módulo : Taller de Networking
NRC : 14413 // CIB101

Karina Loyola Monsalve
Coordinadora Escuela de Ingeniería, Energía & Tecnología
Correo: Karina.Loyola.m@aiep.cl

Nallely Castro Arqueros
Coordinadora Escuela de Ingeniería, Energía & Tecnología
Correo: nallely.castro@aiep.cl

Karina Bravo Segura
Jefa Escuela de Ingeniería, Energía & Tecnología
Correo: Karina.bravo.s@aiep.cl

CONDICIONES FAVORABLES PARA LA CLASE

Práctica la puntualidad

Mantén tus dispositivos electrónicos en silencio

Mantén todos tus sentidos activos

Respeta el turno de participación

PRESENTACIÓN DE LA CLASE

2ª Unidad : Fundamentos de enrutamiento y de conmutación de LAN.

Contenidos:

A.E.3.- Resuelven problemas comunes de conectividad en redes LAN, considerando técnicas de segmentación de red.

A.E.4.- Realizan formulación de red LAN, considerando cálculos asociados a direccionamiento IP.

PRESENTACIÓN DE LA CLASE

2ª Unidad : Fundamentos de enrutamiento y de conmutación de LAN.

Contenidos:

A.E.5.- Configuran redes estáticas y predeterminadas en IPv4 e IPv6, de acuerdo con estándares de las comunicaciones IP.

A.E.6.- Ejecutan diferentes rutas de acceso a una red, considerando comandos IOS Cisco en software de simulación de redes informáticas, según requerimientos.

MOMENTO DE CONOCER

TELNET

MOMENTO DE CONOCER

Telnet es un método para establecer una sesión de CLI de un dispositivo en forma remota, mediante una interfaz virtual, a través de una red. A diferencia de la conexión de consola, las sesiones de Telnet requieren servicios de redes activos en el dispositivo. El dispositivo de red debe tener, por lo menos, una interfaz activa configurada con una dirección de Internet. Por ejemplo, una dirección IPv4.

Los dispositivos Cisco IOS incluyen un proceso de servidor Telnet que permite a los usuarios introducir comandos de configuración desde un cliente Telnet. Además de admitir el proceso de servidor Telnet, el dispositivo Cisco IOS también contiene un cliente Telnet. Esto permite que los administradores de red accedan mediante Telnet a cualquier otro dispositivo que admita un proceso de servidor Telnet desde la CLI del dispositivo Cisco.

MOMENTO DE CONOCER

SSH

MOMENTO DE CONOCER

El protocolo de Shell seguro (SSH) proporciona un inicio de sesión remoto similar al de Telnet, excepto que utiliza servicios de red más seguros. El SSH proporciona autenticación de contraseña más potente que Telnet y usa encriptación cuando transporta datos de la sesión. De esta manera se mantienen en privado la ID del usuario, la contraseña y los detalles de la sesión de administración. Se recomienda utilizar el protocolo SSH en lugar de Telnet, siempre que sea posible.

La mayoría de las versiones de Cisco IOS incluyen un servidor SSH. En algunos dispositivos, este servicio se activa en forma predeterminada. Otros dispositivos requieren que el servidor SSH se habilite en forma manual. Los dispositivos IOS también incluyen un cliente SSH que puede utilizarse para establecer sesiones SSH con otros dispositivos.

MOMENTO DE CONOCER

Cisco Auto Secure

MOMENTO DE CONOCER

La configuración de seguridad se establece en los valores predeterminados cuando se instala un nuevo sistema operativo en un dispositivo. En la mayoría de los casos, este nivel de seguridad es inadecuado.

Para los Routers Cisco, la función Cisco Auto Secure se puede utilizar para ayudar a proteger el sistema, como se muestra en el ejemplo.

```
Router# auto secure
--- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router but it will not make router absolutely secure
from all security attacks ***
```

MOMENTO DE CONOCER

Además, hay algunos pasos simples que se deben seguir que se aplican a la mayoría de los sistemas operativos:

- ✓ Los nombres de usuario y contraseñas predeterminados deben cambiarse de inmediato.
- ✓ El acceso a los recursos del sistema debe restringirse solo a las personas que están autorizadas a usar esos recursos.
- ✓ Todos los servicios y aplicaciones innecesarios deben apagarse y desinstalarse cuando sea posible.

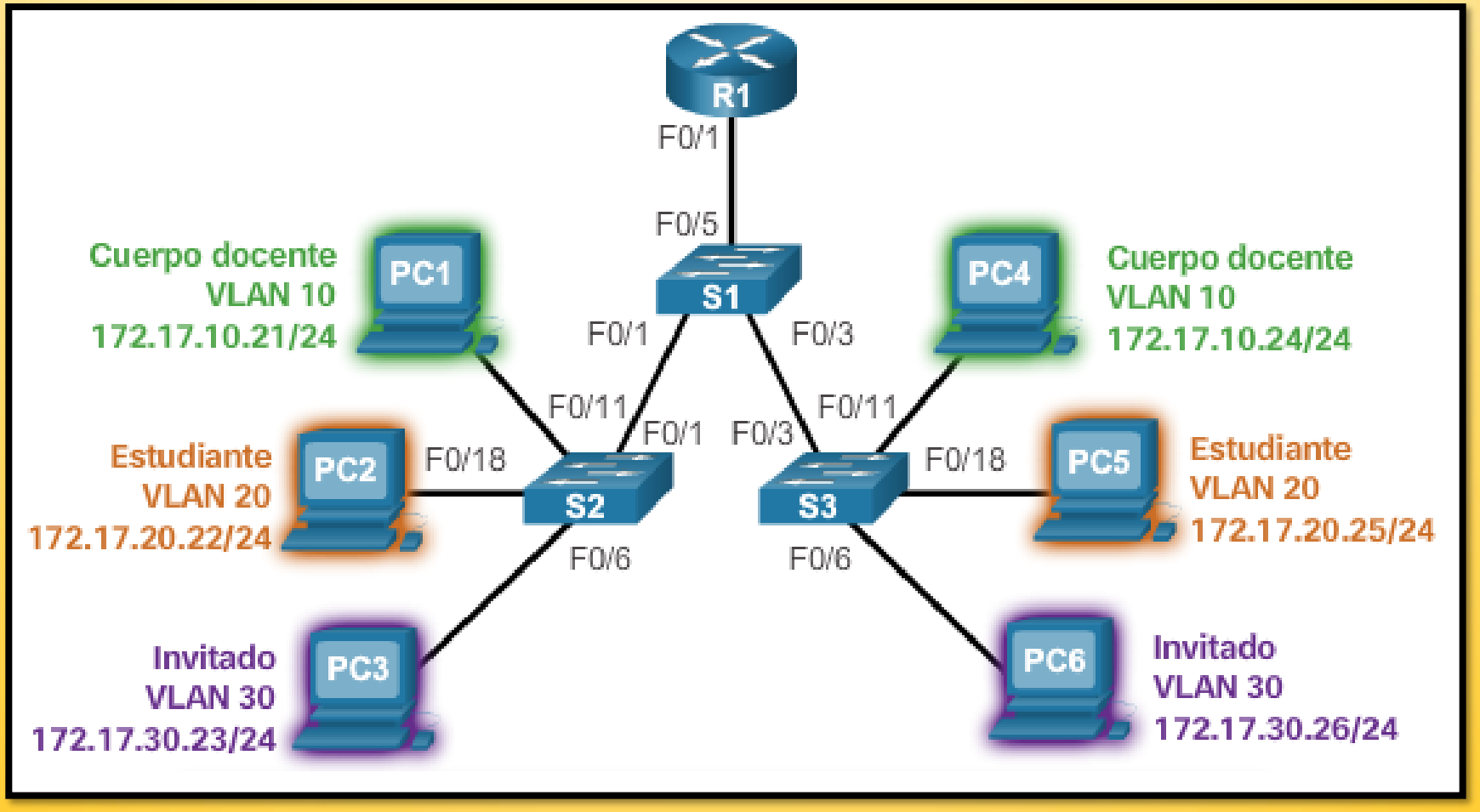
MOMENTO DE CONOCER

- ✓ A menudo, los dispositivos enviados por el fabricante han estado almacenados en un almacén durante un período de tiempo y no tienen instalados los parches más actualizados.

- ✓ Es importante actualizar cualquier software e instalar cualquier parche de seguridad antes de la implementación.

MOMENTO DE CONOCER

VLAN



MOMENTO DE CONOCER

Una Virtual Local Area Network (VLAN) o red de área local virtual es un grupo flexible de dispositivos que se encuentran en cualquier ubicación de una red de área local pero que se comunican como si estuvieran en el mismo segmento físico. Con las Vlan’s se puede segmentar la red sin restringirse a las ubicaciones o conexiones físicas.

MOMENTO DE CONOCER

Existen diferentes tipos de redes VLAN, los cuales se utilizan en las redes modernas. Algunos tipos de VLAN se definen según las clases de tráfico. Otros tipos de VLAN se definen según la función específica que cumplen.

✓ **VLAN de datos**

Una VLAN de datos es una VLAN configurada para transportar tráfico generado por usuarios. Una VLAN que transporta tráfico de administración o de voz no sería una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. A veces a una VLAN de datos se la denomina VLAN de usuario. Las VLAN de datos se usan para dividir la red en grupos de usuarios o dispositivos.

MOMENTO DE CONOCER

✓ **VLAN predeterminada**

Todos los puertos de switch se vuelven parte de la VLAN predeterminada después del arranque inicial de un switch que carga la configuración predeterminada. Los puertos de switch que participan en la VLAN predeterminada forman parte del mismo dominio de difusión.

Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch. La VLAN predeterminada para los switches Cisco es la VLAN 1.

La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no se le puede cambiar el nombre ni se puede eliminar. Todo el tráfico de control de capa 2 se asocia a la VLAN 1 de manera predeterminada.

MOMENTO DE CONOCER

✓ **VLAN nativa**

Una VLAN nativa está asignada a un puerto troncal 802.1Q. Los puertos de enlace troncal son los enlaces entre switches que admiten la transmisión de tráfico asociado a más de una VLAN.

Los puertos de enlace troncal 802.1Q admiten el tráfico proveniente de muchas VLAN (tráfico con etiquetas), así como el tráfico que no proviene de una VLAN (tráfico sin etiquetar). El tráfico con etiquetas hace referencia al tráfico que tiene una etiqueta de 4 bytes insertada en el encabezado de la trama de Ethernet original, que especifica la VLAN a la que pertenece la trama.

El puerto de enlace troncal 802.1Q coloca el tráfico sin etiquetar en la VLAN nativa, que es la VLAN 1 de manera predeterminada.

MOMENTO DE CONOCER

Las VLAN nativas se definen en la especificación IEEE 802.1Q a fin de mantener la compatibilidad con el tráfico sin etiquetar de modelos anteriores común a las situaciones de LAN antiguas.

Una VLAN nativa funciona como identificador común en extremos opuestos de un enlace troncal.

Se recomienda configurar la VLAN nativa como VLAN sin utilizar, independiente de la VLAN 1 y de otras VLAN.

De hecho, es común utilizar una VLAN fija para que funcione como VLAN nativa para todos los puertos de enlace troncal en el dominio conmutado.

MOMENTO DE CONOCER

✓ **VLAN de administración**

Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch.

La VLAN 1 es la VLAN de administración de manera predeterminada. Para crear la VLAN de administración, se asigna una dirección IP y una máscara de subred a la interfaz virtual de switch (SVI) de esa VLAN, lo que permite que el switch se administre mediante HTTP, Telnet, SSH o SNMP.

Dado que en la configuración de fábrica de un switch Cisco la VLAN 1 se establece como VLAN predeterminada, la VLAN 1 no es una elección adecuada para la VLAN de administración.

MOMENTO DE CONOCER

Ventajas de las Vlan's

Las VLAN permiten que los administradores de red organicen las LAN de forma lógica en lugar de física. Ésta es una ventaja clave. Esto permite que los administradores de red realicen varias tareas:

- ✓ Trasladar fácilmente las estaciones de trabajo en la LAN
- ✓ Agregar fácilmente estaciones de trabajo a la LAN
- ✓ Cambiar fácilmente la configuración de la LAN
- ✓ Controlar fácilmente el tráfico de red
- ✓ Mejorar la seguridad

MOMENTO DE CONOCER

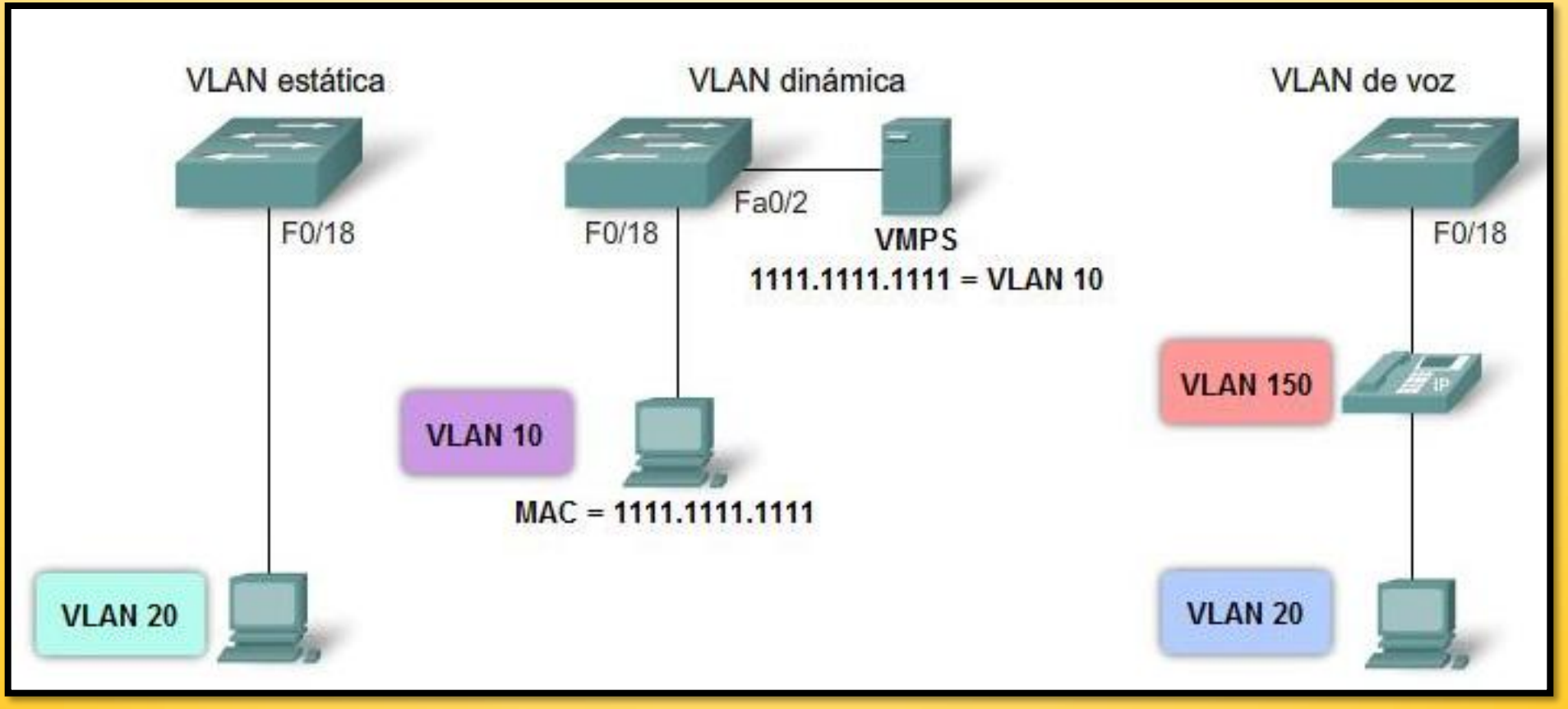
Tipos de VLAN

Los tipos de VLAN que se utilizan para determinar y controlar de qué manera se asignan un frame y/o paquete: Estos son:

- ✓ VLAN basadas por puerto
- ✓ VLAN basadas por direcciones MAC
- ✓ VLAN basadas por protocolo

MOMENTO DE CONOCER

VLAN por puerto



MOMENTO DE CONOCER

Se configura por una cantidad “n” de puertos en el cual podemos indicar que puertos pertenecen a cada VLAN.

Ventajas:

- ✓ Facilidad de movimientos y cambios.
- ✓ Microsegmentación.
- ✓ Reducción del dominio de Broadcast.
- ✓ Multiprotocolo, debido a que independiente de la Vlan usada, los protocolos utilizados no tienen limitaciones en cuanto a sus características, incluso permitiendo el uso de protocolos dinámicos.

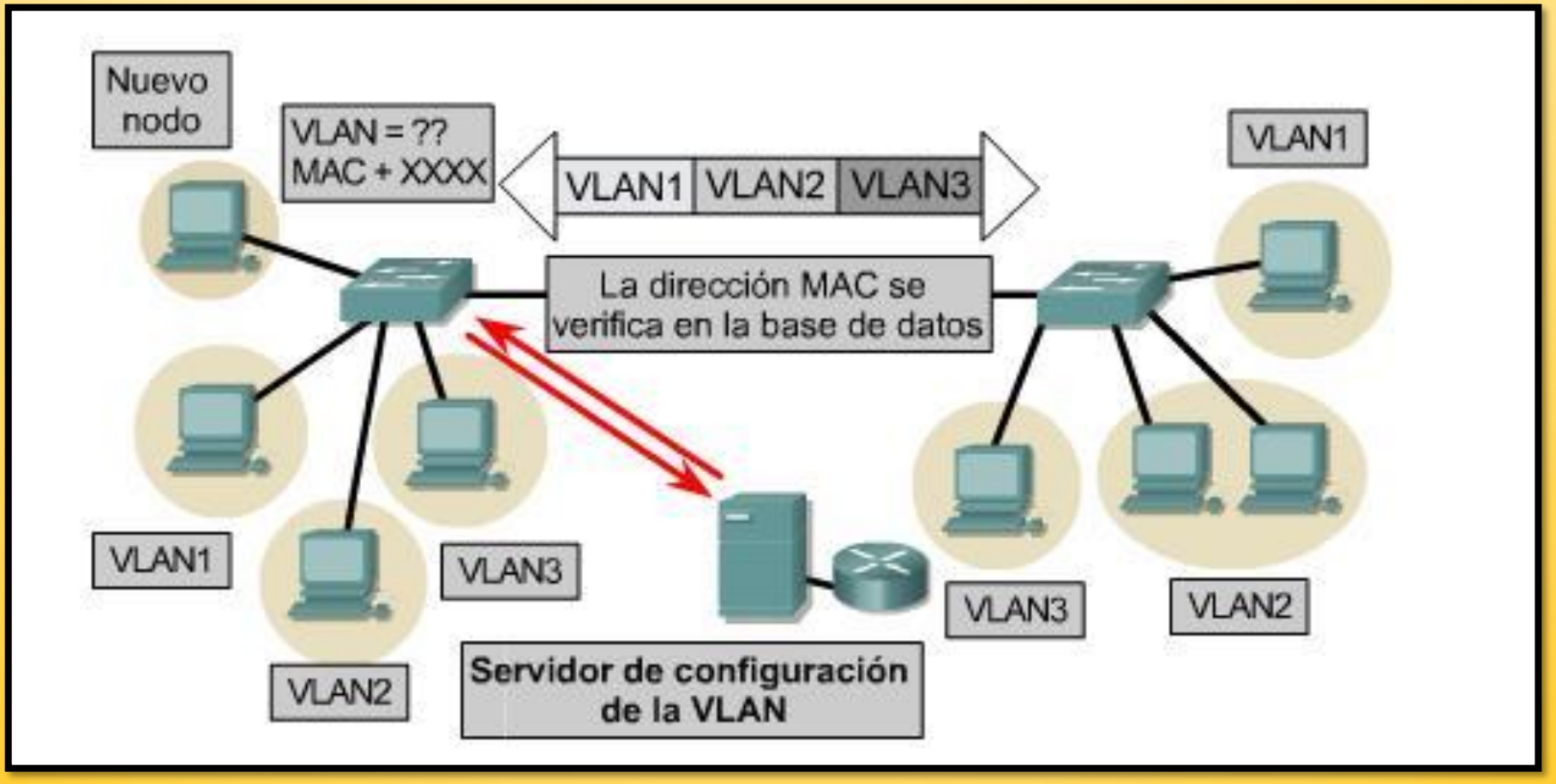
MOMENTO DE CONOCER

Desventajas:

- ✓ Administración, debido a que un movimiento en las estaciones de trabajo hace necesaria la reconfiguración del puerto del switch al que está conectado el usuario. Esto se puede facilitar combinando con mecanismos de LAN Dinámicas.

MOMENTO DE CONOCER

VLAN por MAC



MOMENTO DE CONOCER

Los miembros de la VLAN están especificados en una tabla por su dirección MAC.

Ventajas:

- ✓ Facilidad de movimientos, ya que no es necesario en caso de que una terminal de trabajo cambia de lugar la reconfiguración del switch.

- ✓ Multiprotocolo, ya es permitido tener miembros en múltiples Vlan’s.

MOMENTO DE CONOCER

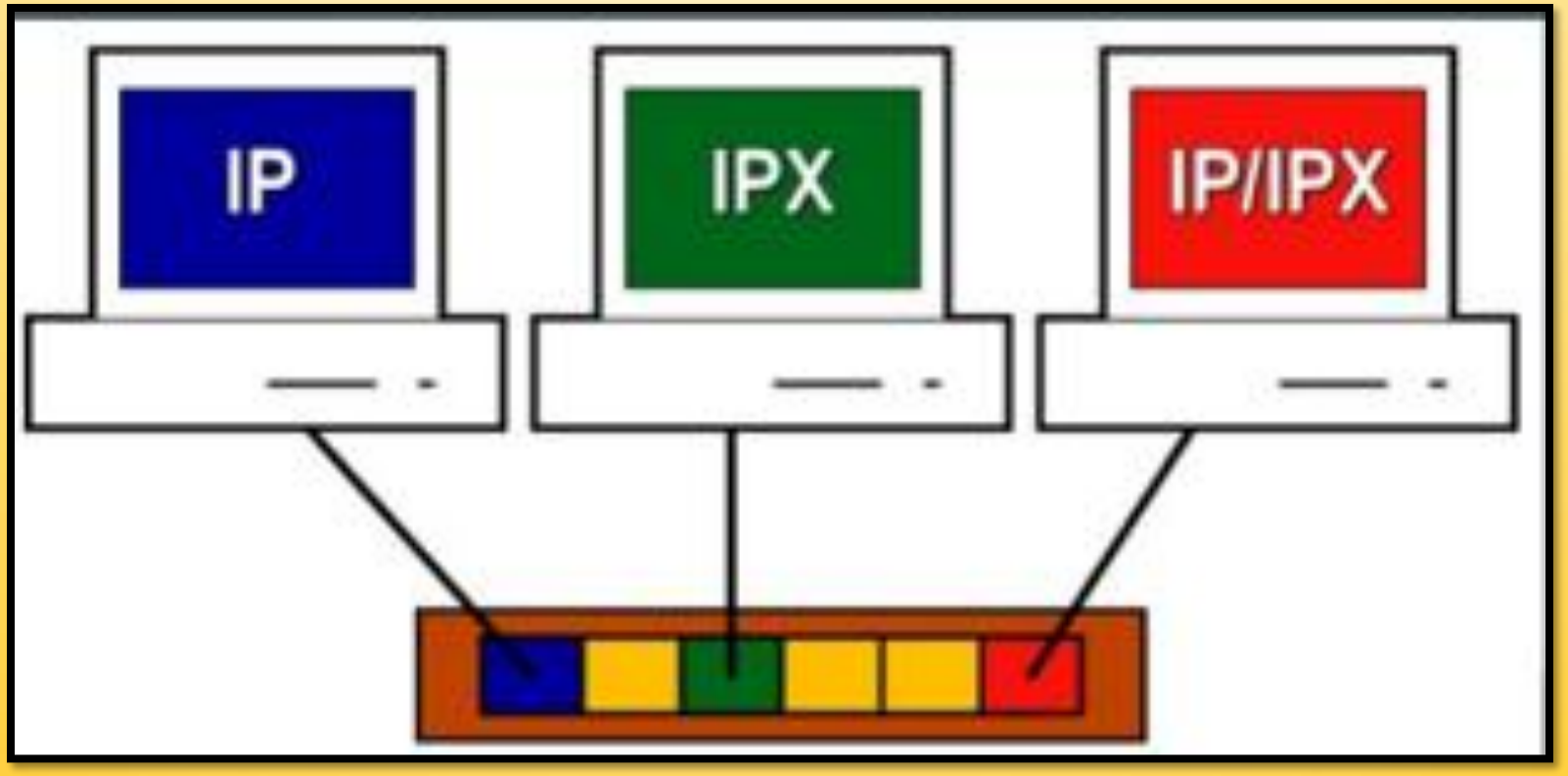
Desventajas:

- ✓ Problemas de rendimiento y control de Broadcast: el tráfico de paquetes de tipo Multicast y Broadcast se propagan por todas las Vlan’s.

- ✓ Complejidad en la administración, ya que en un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.

MOMENTO DE CONOCER

VLAN por protocolo



MOMENTO DE CONOCER

Asigna a un protocolo una VLAN. El switch se encarga de, dependiendo el protocolo por el cual venga la trama, derivarlo a la VLAN correspondiente.

Ventajas:

✓ Segmentación por protocolo.

✓ Asignación dinámica.

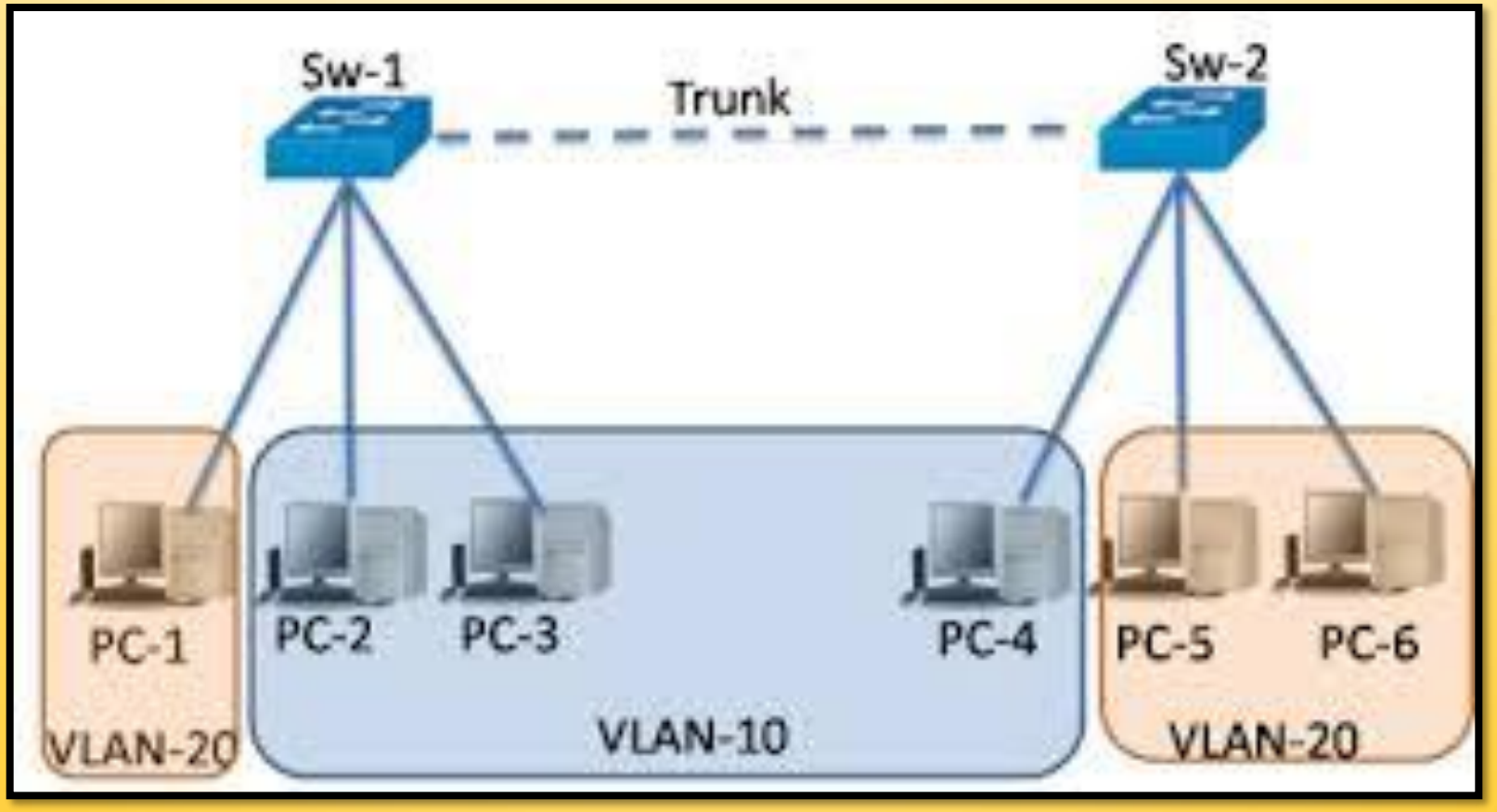
MOMENTO DE CONOCER

Desventajas:

- ✓ Problemas de rendimiento y control de Broadcast: Por las búsquedas en tablas de pertenencia se pierde rendimiento en la VLAN.
- ✓ No soporta protocolos de nivel 2 ni dinámicos.

MOMENTO DE CONOCER

Estándar IEEE 802.1Q



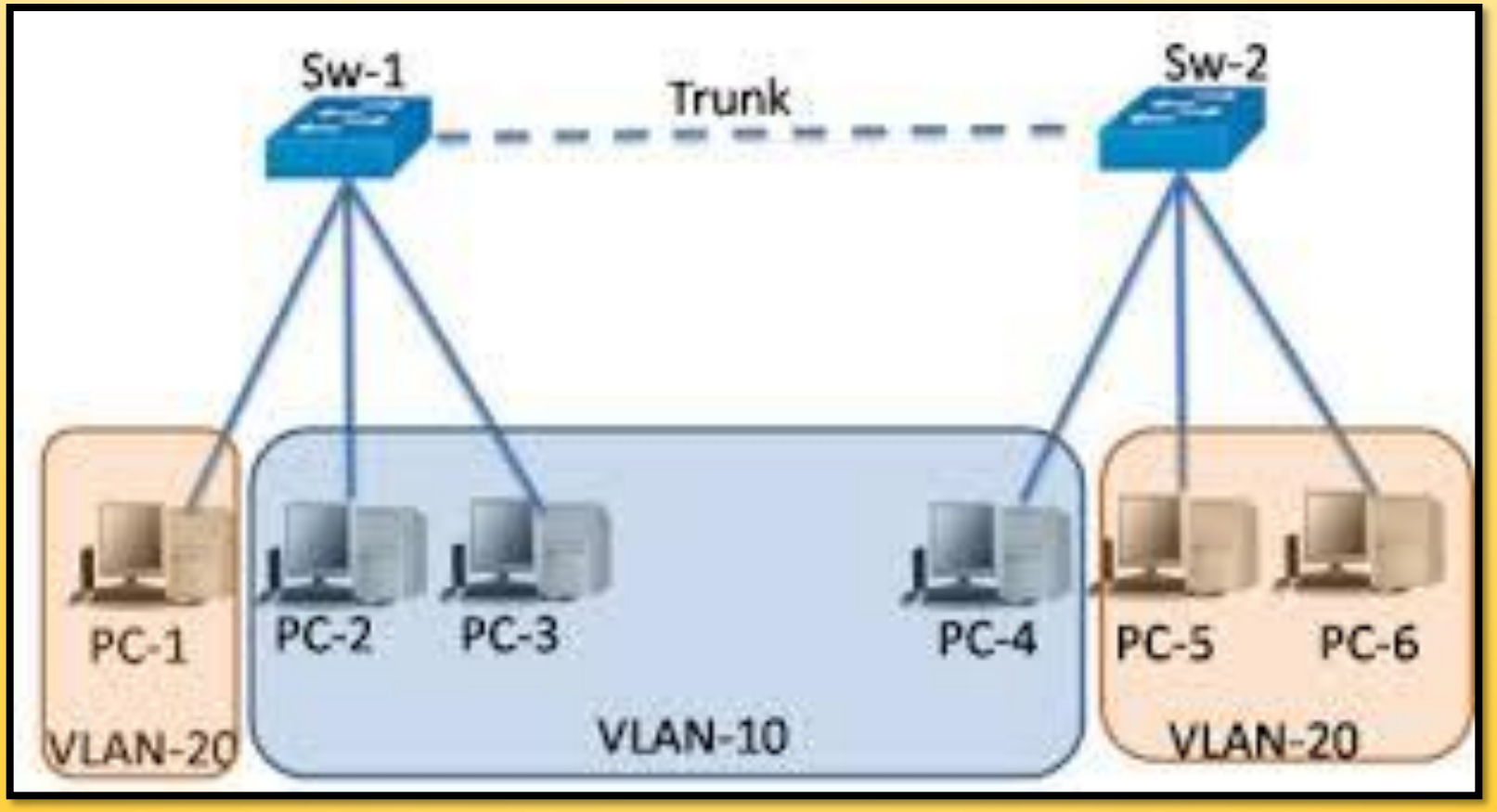
MOMENTO DE CONOCER

Es una modificación al estándar de Ethernet. El protocolo IEEE 802.1Q fue un proyecto del grupo de trabajo 802 de IEEE para desarrollar un mecanismo que permita a múltiples redes con interconectadas con puentes o switches compartir transparentemente el mismo medio físico sin problemas de interferencia entre las redes que comparten el medio (Trunking).

Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet. Permite identificar a una trama como proveniente de un equipo conectado a una red determinada. Una trama perteneciente a una VLAN sólo se va a distribuir a los equipos que pertenezcan a su misma VLAN, de forma que se separan dominios de broadcast.

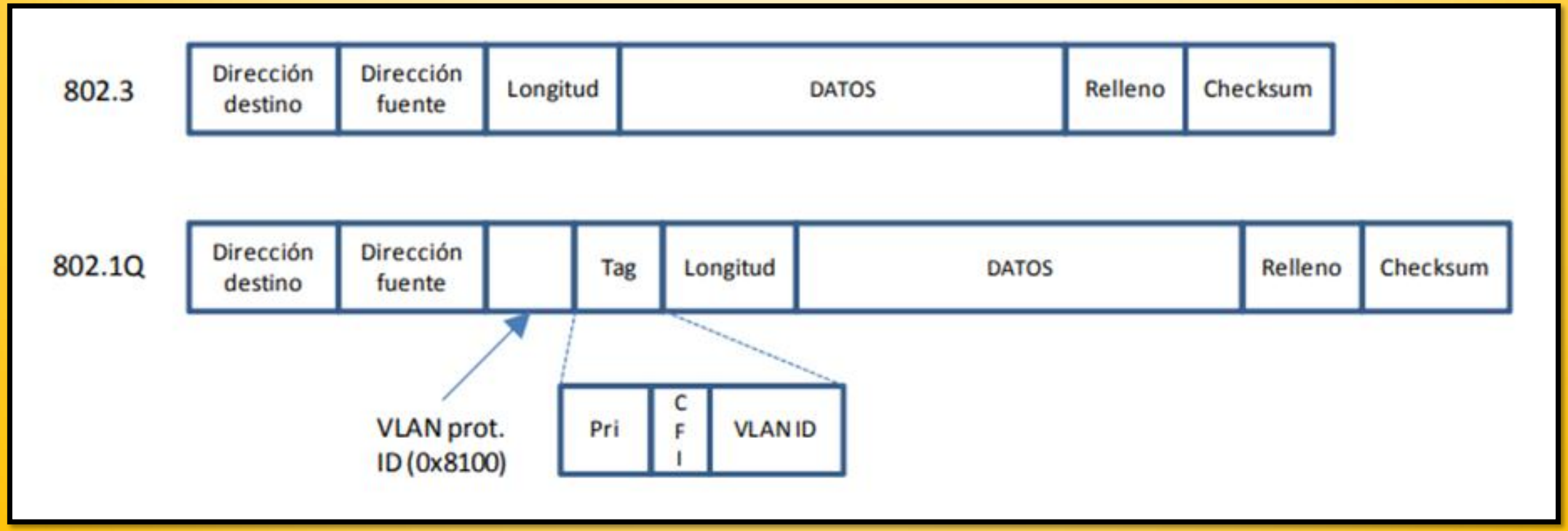
MOMENTO DE CONOCER

Trama IEEE 802.1Q



MOMENTO DE CONOCER

El protocolo 802.1Q propone añadir 4 bytes al encabezado Ethernet original en lugar de encapsular la trama original. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama.



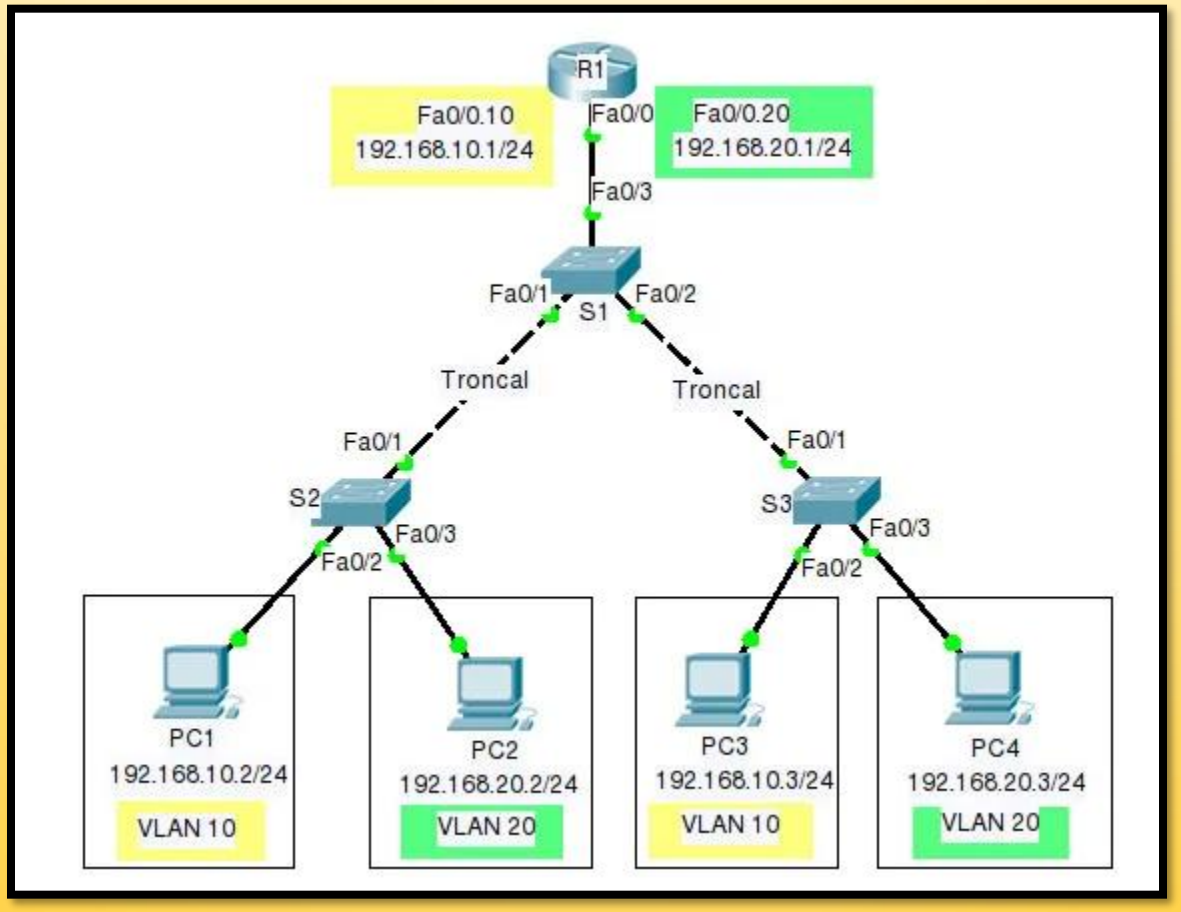
MOMENTO DE CONOCER

En la trama 802.1Q, la VLAN tag se inserta en la trama Ethernet entre el campo “Dirección fuente” y “Longitud. Los primeros 2 bytes del VLAN tag consisten en el “Tag Type" (tipo de tag) de 802.1Q y siempre está puesto a 0x8100. Los últimos 2 bytes contienen la siguiente información:

- ✓ Los primeros 3 bits son el campo User Priority Field que pueden ser usados para asignar un nivel de prioridad.
- ✓ El próximo bit es el campo Canonical Format Indicator (CFI) usado para indicar la presencia de un campo Routing Information Field (RIF).
- ✓ Los restantes 12 bits son el VLAN Identifier (VID) que identifica de forma única a la VLAN a la cual pertenece la trama Ethernet.

MOMENTO DE CONOCER

Enrutamiento Inter Vlan



MOMENTO DE CONOCER

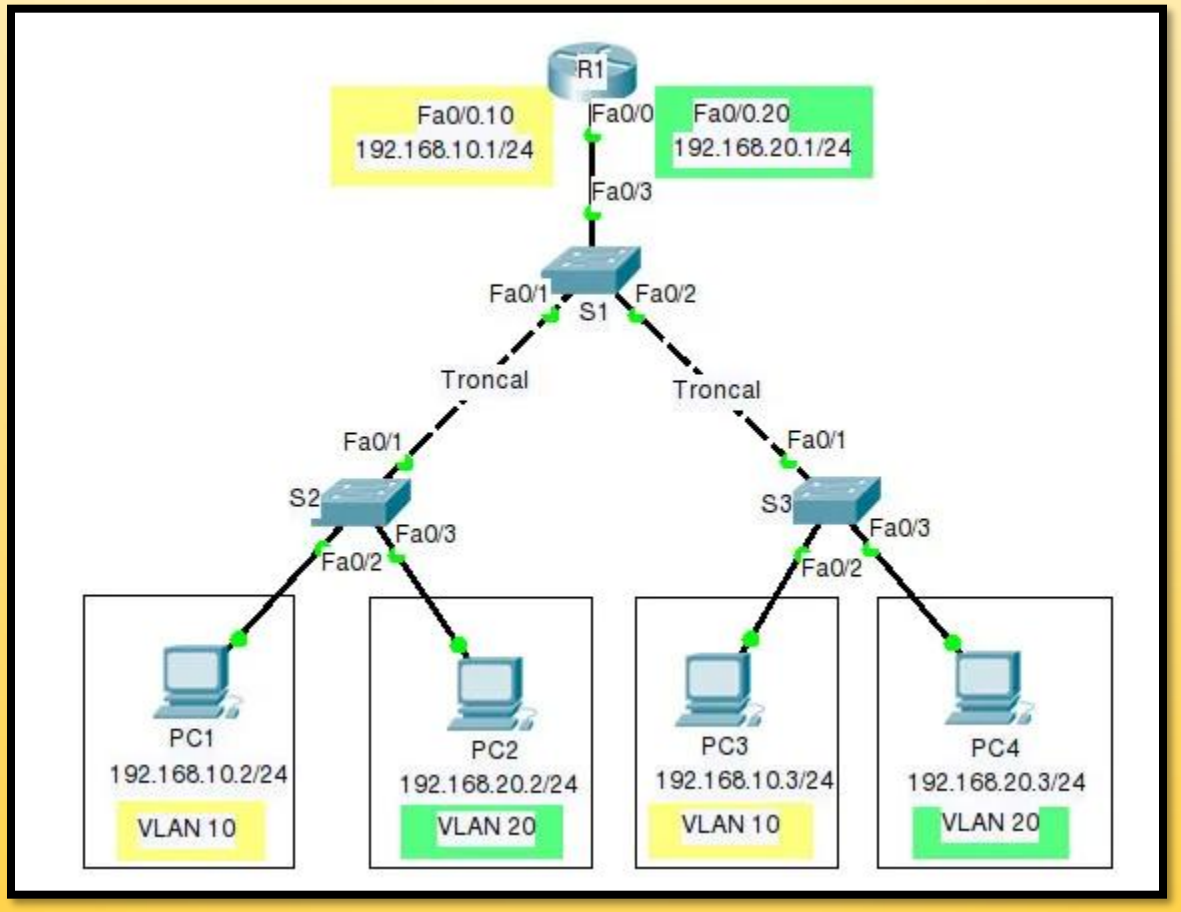
Las VLAN se utilizan para segmentar las redes de switch de Capa 2 por diversas razones.

Independientemente del motivo, los hosts de una VLAN no pueden comunicarse con los hosts de otra VLAN a menos que haya un Router o un switch de capa 3 para proporcionar servicios de enrutamiento.

El Enrutamiento Entre VLAN (Inter-VLAN Routing) es el proceso de reenviar el tráfico de red de una VLAN a otra VLAN.

MOMENTO DE CONOCER

Tipos de enrutamiento Inter Vlan



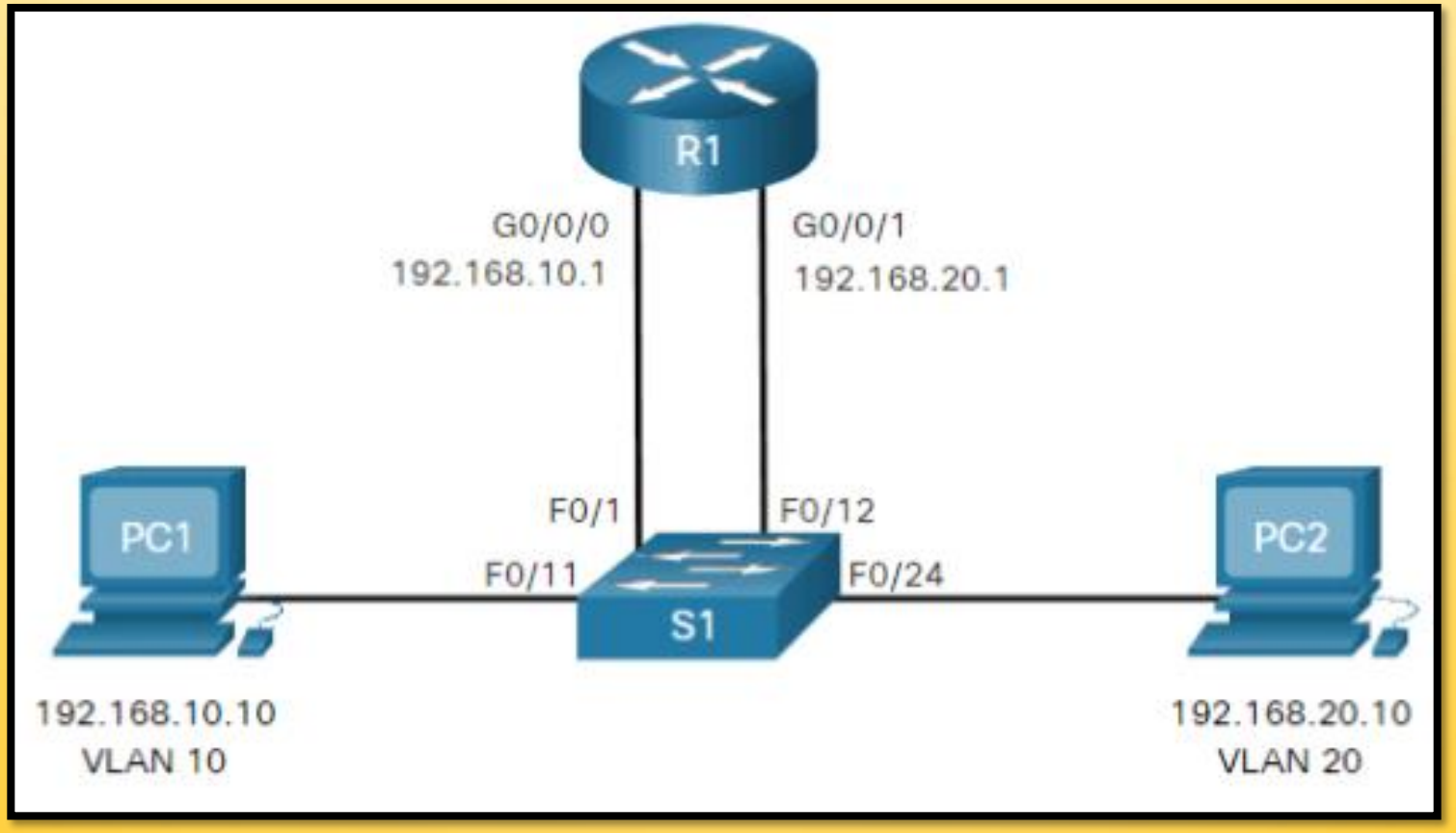
MOMENTO DE CONOCER

Enrutamiento inter-VLAN:

- ✓ Inter-VLAN Routing heredado.
- ✓ Router on a stick.
- ✓ Switch de capa 3 con interfaces virtuales (SVIs).

MOMENTO DE CONOCER

Enrutamiento Inter-VLAN Heredado



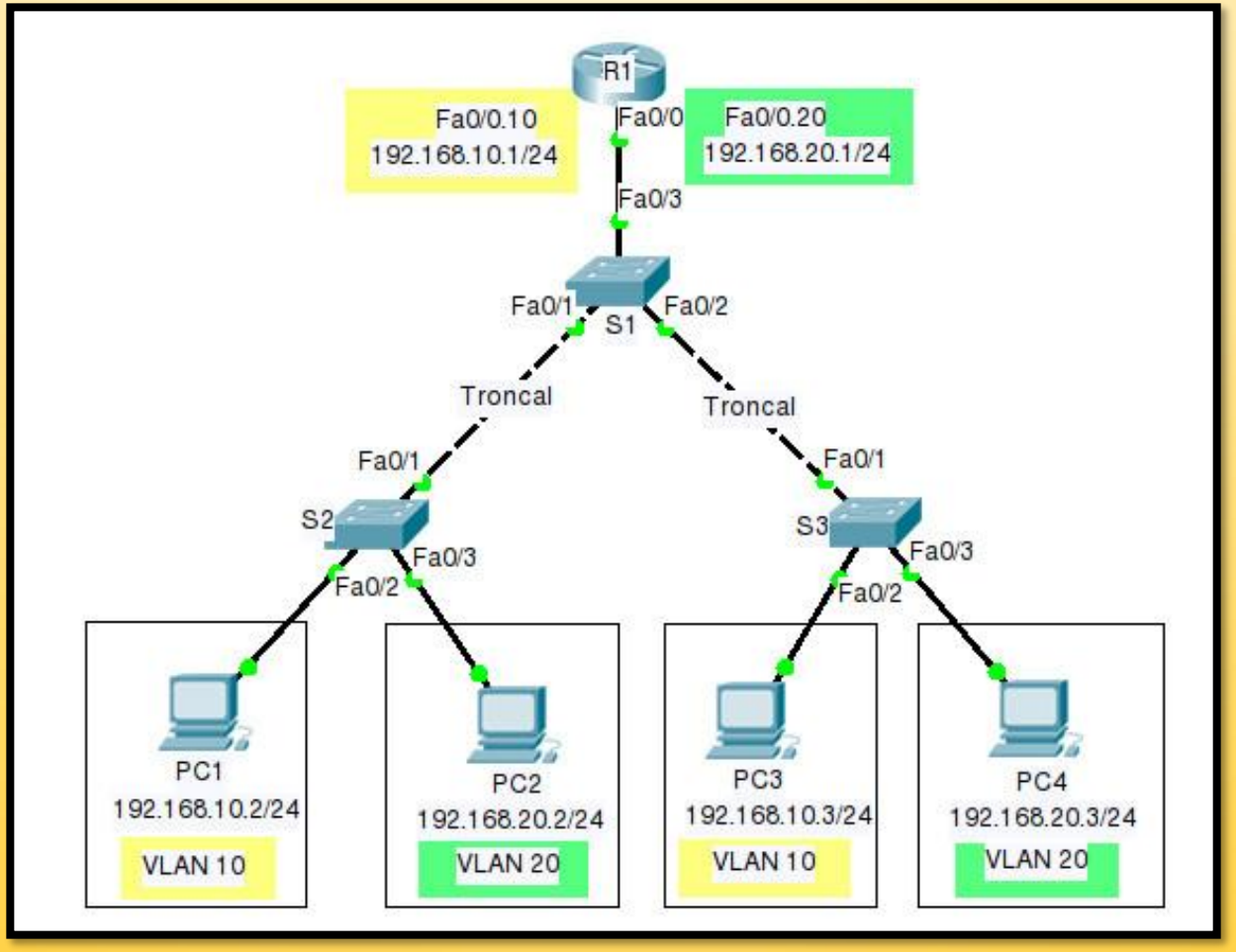
MOMENTO DE CONOCER

La primera solución de enrutamiento inter-VLAN se basó en el uso de un Router con múltiples interfaces Ethernet. Cada interfaz del Router estaba conectada a un puerto del switch en diferentes VLAN. Las interfaces del Router sirven como puertas de enlace predeterminada para los hosts locales en la subred de la VLAN.

El enrutamiento entre VLAN heredado usando interfaces físicas funciona, pero tiene una limitación significativa. No es razonablemente escalable porque los Routers tienen un número limitado de interfaces físicas. Requerir una interfaz física de Router por VLAN agota rápidamente la capacidad de interfaz física de un Router.

MOMENTO DE CONOCER

Enrutamiento Inter-VLAN Router-on-a-Stick



MOMENTO DE CONOCER

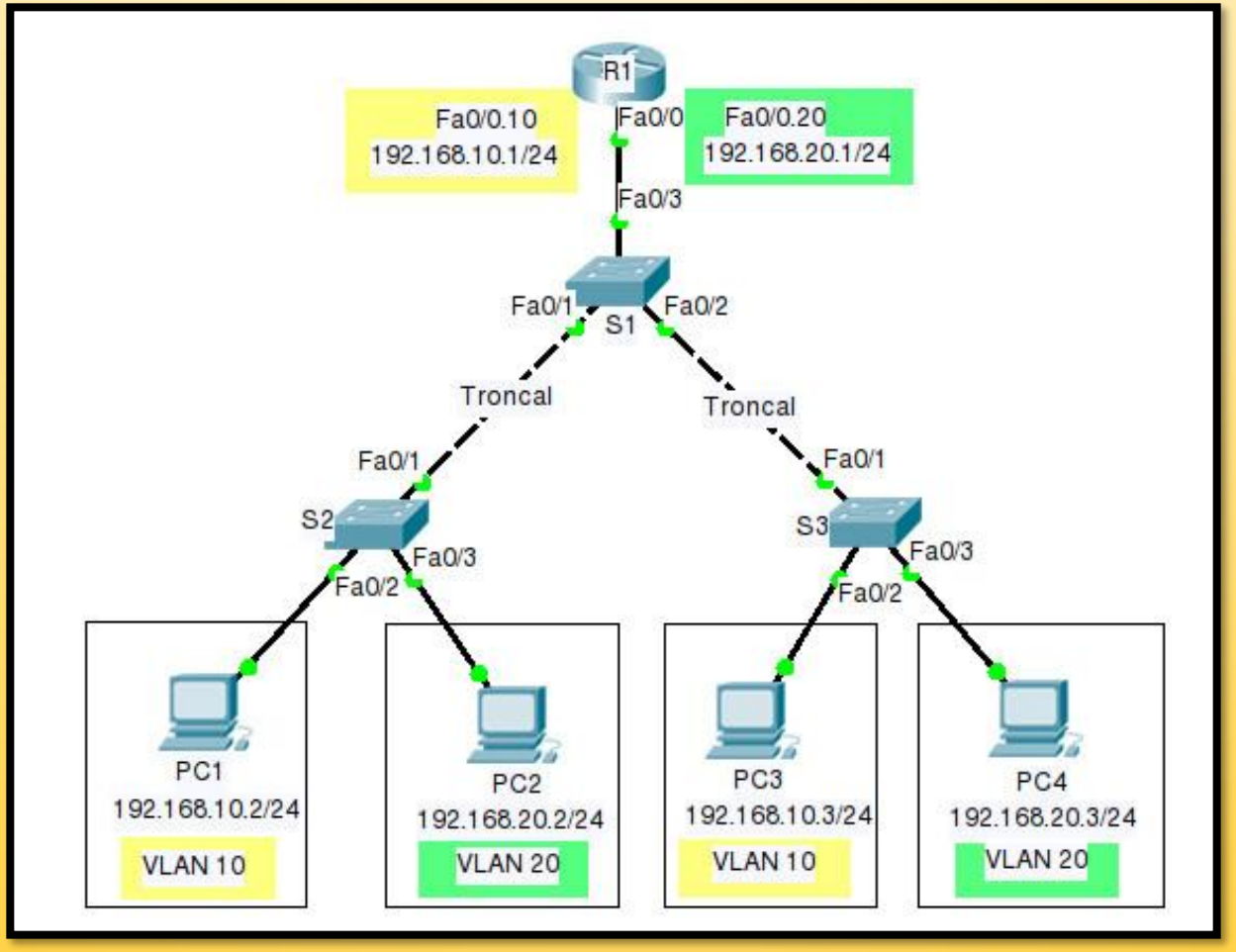
El método de enrutamiento inter-VLAN ‘Router-on-a-stick’ supera la limitación del método de enrutamiento inter-VLAN heredado. Solo requiere una interfaz Ethernet física para enrutar el tráfico entre varias VLAN de una red.

Una interfaz Ethernet del Router Cisco IOS se configura como un troncal 802.1Q y se conecta a un puerto troncal en un switch de capa 2. Específicamente, la interfaz del Router se configura mediante subinterfaces para identificar VLAN enrutables.

Las subinterfaces configuradas son interfaces virtuales basadas en software. Cada uno está asociado a una única interfaz Ethernet física. Estas subinterfaces se configuran en el software del router. Cada una se configura de forma independiente con sus propias direcciones IP y una asignación de VLAN. Las subinterfaces se configuran para subredes diferentes que corresponden a su asignación de VLAN. Esto facilita el enrutamiento lógico.

MOMENTO DE CONOCER

Enrutamiento Inter-VLAN en Switch Capa 3



MOMENTO DE CONOCER

El método moderno para realizar inter-VLAN routing es utilizar switches de capa 3 e interfaces virtuales del switch (SVI). Una SVI es una interfaz virtual configurada en un switch de capa 3.

Los SVIs entre VLAN se crean de la misma manera que se configura la interfaz de VLAN de administración. El SVI se crea para una VLAN que existe en el switch. Aunque es virtual, el SVI realiza las mismas funciones para la VLAN que lo haría una interfaz de router. Específicamente, proporciona el procesamiento de Capa 3 para los paquetes que se envían hacia o desde todos los puertos de switch asociados con esa VLAN.

MOMENTO DE CONOCER

Ventajas del uso de switches de capa 3 para el enrutamiento inter-VLAN:

- ✓ Es mucho más veloz que router-on-a-stick, porque todo el switching y el routing se realizan por hardware.
- ✓ El routing no requiere enlaces externos del switch al router para el enrutamiento.
- ✓ No se limitan a un solo enlace porque los EtherChannels de Capa 2 pueden ser usados como enlaces troncales entre los switches para aumentar el ancho de banda.
- ✓ La latencia es mucho más baja, dado que los datos no necesitan salir del switch para ser enrutados a una red diferente.
- ✓ Se implementan con mayor frecuencia en una LAN de campus que en Routers.

MOMENTO DE CONOCER

Comandos Generales de CISCO

```
Router(config)#hostname name
Router(config)#enable secret password
Router(config)#line console 0
Router(config-line)#password password
Router(config-line)#login
Router(config)#line vty 0 4
Router(config-line)#password password
Router(config-line)#login

Router(config)#banner motd # message #
```

MOMENTO DE CONOCER

- **Enable**

Inicia el modo de habilitación, que también se conoce como modo de ejecución de usuario o modo privilegiado.

- **Configure terminal**

Hace login en el modo de configuración.

- **Interface fastEthernet o gigabitEthernet / number**

Accede al modo de configuración de la interfaz para la interfaz fast ethernet especificada.

MOMENTO DE CONOCER

- **Hostname**

Cambiar el nombre del host.

- **Write memory**

Salvar la configuración del equipo.

- **Shutdown**

Se utiliza en el modo de configuración de la interfaz. "Shutdown" apaga o deja deshabilitada la interfaz.

- **No shutdown**

Se utiliza en el modo de configuración de la interfaz. Levanta la interfaz

MOMENTO DE CONOCER

- **Ip default-gateway ip_address**

Establece la puerta de enlace predeterminada en un dispositivo Cisco.

- **Show running-config**

Un comando de modo de habilitación que muestra la configuración actual.

- **Description name-string**

Un comando de interfaz de configuración para describir o nombrar una interfaz.

- **Show running-config interface interface slot / number**

Un comando de modo de habilitación para mostrar la configuración en ejecución para una interfaz específica.

MOMENTO DE CONOCER

- **Show ip interface [type number]**

Muestra el estado de las interfaces que están configuradas para IP.

- **Show versión**

Mostrar la versión de la imagen del IOS.

- **Description name-string**

Un comando de interfaz de configuración para describir o nombrar una interfaz.

- **Show running-config interface interface slot / number**

Un comando de modo de habilitación para mostrar la configuración en ejecución para una interfaz específica.

MOMENTO DE CONOCER

Comandos VLAN de CISCO

```
Router(config)#hostname name
Router(config)#enable secret password
Router(config)#line console 0
Router(config-line)#password password
Router(config-line)#login
Router(config)#line vty 0 4
Router(config-line)#password password
Router(config-line)#login

Router(config)#banner motd # message #
```

MOMENTO DE CONOCER

- **VLAN**

Crea una VLAN e ingresa al modo de configuración de VLAN para obtener y crear más definiciones.

- **Switchport access vlan**

Establece la VLAN a la que pertenece la interfaz.

- **Name (dentro de la vlan)**

Establece el nombre de la vlan dentro del equipo.

MOMENTO DE CONOCER

- **Switchport mode { access | trunk }**

Configura el modo de pertenencia a VLAN de un puerto. El puerto de acceso está configurado para acceder incondicionalmente y funciona como una interfaz VLAN única sin enlace troncal que envía y recibe tramas no encapsuladas (no etiquetadas). Se puede asignar un puerto de acceso a una sola VLAN.

El puerto troncal envía y recibe tramas encapsuladas (etiquetadas) que identifican la VLAN de origen. Un tronco es un enlace punto a punto entre dos conmutadores o entre un conmutador y un enrutador.

switchport trunk {encapsulation {dot1q} Establece las características del tronco cuando la interfaz está en modo de enlace. En este modo, el conmutador admite tráfico etiquetado y no etiquetado simultáneo en un puerto.

MOMENTO DE CONOCER

Comandos Routing de CISCO

```
Router(config)#hostname name
Router(config)#enable secret password
Router(config)#line console 0
Router(config-line)#password password
Router(config-line)#login
Router(config)#line vty 0 4
Router(config-line)#password password
Router(config-line)#login

Router(config)#banner motd # message #
```

MOMENTO DE CONOCER

- **Ip route network-number network-mask {dirección-ip | interfa**ce}

Establece una ruta estática en la tabla de enrutamiento IP.

- **Router rip**

Pone el router Habilitando un proceso de enrutamiento del Protocolo de información de enrutamiento (RIP).

- **Version 2**

En el modo de configuración del router, configura el software para recibir y enviar solo paquetes RIP versión 2

MOMENTO DE CONOCER

- **No auto-summary**

En el modo de configuración del router deshabilita el resumen automático.

- **Default-information originate**

En el modo de configuración del router, genera una ruta predeterminada en RIP.

- **Passive-interface interface**

En el modo de configuración del router, establece solo esa interfaz en el modo RIP pasivo. En el modo RIP pasivo, las actualizaciones de enrutamiento RIP son aceptadas por la interfaz especificada, pero no enviadas desde ella.

MOMENTO DE CONOCER

- **Show ip rip database**

Muestra el contenido de la base de datos de enrutamiento RIP.

- **Ip nat [inside | outside]**

Un comando del modo de configuración de la interfaz para designar que el tráfico que se origina o se destina a la interfaz está sujeto a NAT.

- **Ip nat inside source {list{access-list-number | access-list-name}} interface type number[overload]**

Un comando de modo de configuración para establecer la traducción de fuente dinámica. El uso de la palabra clave "lista" le permite utilizar una ACL para identificar el tráfico que estará sujeto a NAT. La opción de "sobrecarga" permite al enrutador utilizar una dirección global para muchas direcciones locales.

MOMENTO DE CONOCER

- **Asignar ip a una interfaz**

(config)#interface
(config-if)#ip address

Ejemplo:

(config)#interface serial 0/0
(config-if)#ip address 10.1.1.1 255.255.255.252

MOMENTO DE CONOCER

- **Habilitar enrutamiento**

(config)#router [id de proceso]
(config-router)#network [wildcard]

Ejemplo 1:
(config)#router rip
(config-router)#network 172.16.0.0

(config-router)#versión2
Exclusivo para rip (habilitar enrutamiento que soporte subredes de máscara variable)

Ejemplo 2:
(config)#router ospf 1
(config-router)#network 172.16.4.0 0.0.3.255 area 0

MOMENTO DE CONOCER

- **Visualizar la configuración del router**

#show running-config

- **Visualizar la tabla de enrutamiento de un router**

#show ip route

MOMENTO DE CONOCER

- **Visualizar el estado de todas las interfaces**

#show interfaces

- **Visualizar el estado de una interfaz**

#show interface <#>

Ejemplo:

#show interface serial 0/0/0

MOMENTO DE CONOCER

- **Agregar una ruta estática**

(config)#ip route

Ejemplo:

ip route 192.168.2.0 255.255.255.0 serial2/0

MOMENTO DE CONOCER

- **Ping {hostname | system-address} [source source-address]**

Se utiliza en el modo de habilitación para diagnosticar la conectividad de red básica.

- **Speed {10 | 100 | 1000 | auto}**

Un comando de modo de interfaz que establece manualmente la velocidad al valor especificado o la negocia automáticamente.

- **Duplex {auto | full | half}**

Un comando de modo de interfaz que configura manualmente dúplex en medio, completo o automático.

MOMENTO DE CONOCER

- **Show mac address-table**

Muestra la tabla de direcciones MAC.

- **Show interfaces**

Muestra información detallada sobre el estado, la configuración y los contadores de la interfaz.

- **Show interface status**

Muestra el estado de la línea de la interfaz.

MOMENTO DE CONOCER

- **Show interfaces switchport**

Muestra una gran variedad de opciones de configuración y el estado operativo actual, incluidos los detalles del enlace troncal VLAN.

- **Show interfaces trunk**

Enumera información sobre los troncales actualmente operativos y las VLAN compatibles con esos troncales.

- **Show vlan / show vlan brief**

Enumera cada VLAN y todas las interfaces asignadas a esa VLAN, pero no incluye troncales.

MOMENTO DE CONOCER

Crear una VLAN

```
1 switch#configure terminal
2 switch(config)# vlan 5
3 switch(config-vlan)# name contabilidad
4 switch(config-vlan)# state active
5 switch(config-vlan)# no shutdown
6 switch(config-vlan)# exit
7 switch(config)#exit
8 switch#
```

MOMENTO DE CONOCER

Habilitar un puerto para acceder a una VLAN.

En este ejemplo, el puerto 1/32 tendrá configurada la VLAN 17 sin taguear

```
1 switch#configure terminal
2 switch(config)#interface ethernet 1/32
3 switch(config-if)#switchport mode access
4 switch(config-if)#switchport access vlan 17
5 switch(config-if)#no shutdown
```

MOMENTO DE CONOCER

Habilitar un puerto para acceder a varias VLAN con tag .

En este ejemplo, el puerto 1/34 tendrá configurada la VLAN 17,18,19,100,132,200,201 tageadas

```
1 switch#configure terminal
2 switch(config)#interface ethernet 1/34
3 switch(config-if)#switchport mode trunk
4 switch(config-if)#switchport trunk allowed vlan add 17-19,100,132,200-201
5 switch(config-if)#no shutdown
```

MOMENTO DE CONOCER

Habilitar un puerto para acceder a varias VLAN con tag .

En este ejemplo, el puerto 1/34 tendrá configurada la VLAN 17,18,19,100,132,200,201 tageadas

```
1 switch#configure terminal
2 switch(config)#interface ethernet 1/34
3 switch(config-if)#switchport mode trunk
4 switch(config-if)#switchport trunk allowed vlan add 17-19,100,132,200-201
5 switch(config-if)#no shutdown
```

MOMENTO DE RETROALIMENTAR

MUCHAS GRACIAS