TRABAJO COLABORATIVO MOMENTO 5

GELVER LÓPEZ PADILLA
ALVARO PLATA PAEZ
LUIS CARLOS CADAVID VARGAS
CLAUDIA NOEMI PULIDO MONCADA

TUTORA
NANCY AMPARO GUACA

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
DIPLOMADO DE PROFUNDIZACIÓN CISCO
2015

TABLA DE CONTENIDO

RESUMEN

Al desarrollar los siguientes ejercicios se refuerza el conocimiento adquirido en la unidad “Configuración de Sistemas de Red Soportados en VLANs “donde se examinan algunos modelos de diseño de red y el modo en que lo switches LAN crean tablas de reenvío usando la información de direcciones MAC para conmutar datos entre los hosts de forma eficaz.

También se analizan algunas de las opciones de configuración básica de switch que se requieren para mantener un entorno LAN conmutado seguro y disponible, accediendo al router, configurando los parámetros básicos del router y verificando la configuración.

INTRODUCCIÓN

Con la evolución de las telecomunicaciones y redes informáticas ha permitido el intercambio de recursos en tiempo real entre varias personas en sitios remotos como si estuvieran en la misma ubicación física. Los servicios avanzados dependen de la disponibilidad de una infraestructura sólida de routing y switching, infraestructura que se debe diseñar, implementar y administrar cuidadosamente para proporcionar una plataforma estable necesaria.

En una red diseñada correctamente, los switches son responsables de controlar el flujo de datos en la capa de acceso y de dirigirlo a los recursos conectados en red y los routers trasladan la información entre las redes, utiliza su tabla de routing para encontrar la mejor ruta para reenviar un paquete.

Con el desarrollo de los siguientes ejercicios se refuerza el conocimiento adquirido en esta unidad “Configuración de Sistemas de Red Soportados en VLANs “donde se examinan algunos de los modelos actuales de diseño de red y el modo en que lo switches LAN crean tablas de reenvío y usan la información de direcciones MAC para conmutar datos entre los hosts de forma eficaz.

Igualmente se analizan algunas de las opciones de configuración básica de switch que se requieren para mantener un entorno LAN conmutado seguro y disponible, e igualmente cómo acceder al router, cómo configurar los parámetros básicos del router y cómo verificar la configuración.

También se analizan cuestiones y estrategias de seguridad relacionadas con las VLAN y los enlaces troncales, los métodos utilizados para la implementación del routing entre VLAN y técnicas estándar de resolución de problemas. Se realiza la configuración de rutas estáticas IPv4 e IPv6, métodos de máscara de subred de longitud variable (VLSM), y técnicas de sumarización

1) Ejercicio 2.1.1.6 Práctica de laboratorio: configuración de los parámetros básicos de un switch

OBJETIVO

Realizar el cableado correspondiente a la topología planteada y configurar los parámetros básicos de los dispositivos, comprobando la conectividad extremo a extremo y la capacidad de administración remota con telnet

Topología

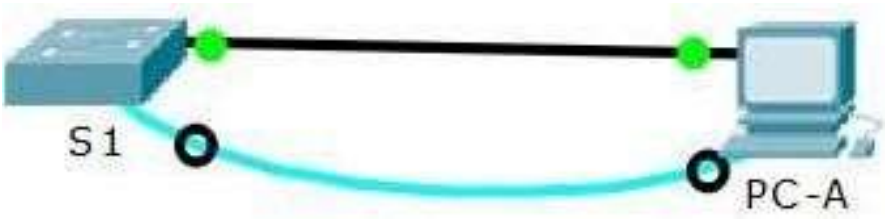


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Síntesis

Con esta práctica se realiza la configuración básica del switch, asignado contraseñas de seguridad a los puertos de consola y vty como método de autenticación de seguridad necesario para evitar posibles ataques informáticos. Igualmente siguiendo la guía de trabajo se configura la interfaz virtual del switch a manera de administrar el

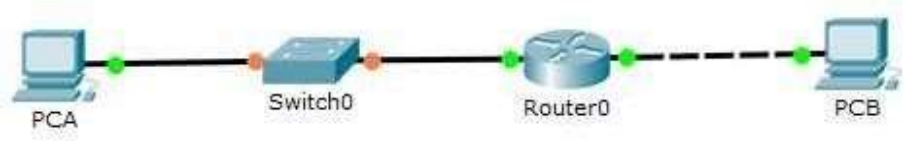
switch de forma remota a través de telnet. Finamente se realiza la configuración de la MAC dinámica a MAC estática con el fin de brindar más seguridad en la conectividad en los puertos al momento de leer las MAC.

Con el desarrollo de esta actividad se aprende a tener en cuenta la responsabilidad de brindar seguridad a los equipos con el fin de minimizar el riesgo de ataque informáticos, se enfatiza en aprender a conocer tanto es software como el hardware de los switches que se utilizan en una red informática, enfatizando a identificar tan el número de puertos de cada interfaz que lo componen como las versión que se utiliza. Se enfatiza en la seguridad en el acceso a los equipos, y el método de encriptación de contraseñas para texto cifrado, y se aprenden nuevos comandos para conocer el estado de la interfaz virtual como físicas como para configurar las mismas, y que un administrador de be conocer en profundidad.

En el ejercicio se aprende administrar la tabla de direccionamiento MAC identificando los tipos de direcciones MAC en la tabla de direccionamiento MAC, la forma de poder pasar una MAC dinámica a una MAC estática e igual manera poderlas eliminar.

Es importante para la seguridad de los equipos y sobre todo en los switches y rauters establecer contraseñas seguras que impidan el acceso remoto, cambiar la VLAN predeterminada a una VLAN diferente, y establecer direcciones MAC estáticas de manera de poder limitar que solo la MAC configurada sea aprendida y no otras que se puedan conectarse a la interfaz.

2) Ejercicio 4.1.4.6 Configuring_Basic_Router_Settings_with_IOS_CLI
Topología



En el router se realizan las configuraciones básicas como el nombre del equipo hasta algunas avanzadas como la configuración de contraseñas en las que se establece una longitud mínima de la misma permitiendo otras formas de aportar seguridad como lo son utilizar mayúsculas, números y caracteres especiales.

Se debe tener en cuenta que así como se configura una IPv4 igualmente se realiza con una IPv6 tanto en los routers como en los host finales esto se debe realizar para que exista comunicación entre los equipos de la red, puede pasar que un equipo este configurado en IPv4 y el otro en IPv6 por tanto no existirá comunicación entre ellos, para poder determinar una falla como esta en un router se puede hacer uso del comando show Ipv6 interface Brief para verificar la configuración de las interfaces y descartar posibles causas de falla.

También se destaca el comando exec-timeout el cual permite agregarle un tiempo para poder ingresar el password. Se debe guardar la configuración realizada al router mediante el comando **copy running-config startup-config** ya que si el router se reinicia sin guardar se pierden la configuración realizada.

3) Ejercicio 6.4.2.5 Práctica de laboratorio: cálculo de rutas resumidas IPv4 e IPv6

OBJETIVO

Determinar las rutas resumidas en IPv4 e IPv6 para las LAN de HQ, WEST y EAST y su ruta resumida general.

Topología

En la topología planteada se tiene un router central HQ el cual contiene dos LAN locales, e igualmente se comunica con tres routers a través de las interfaces seriales. El router WEST como el router EAST cada uno tienen dos LAN Locales asociadas

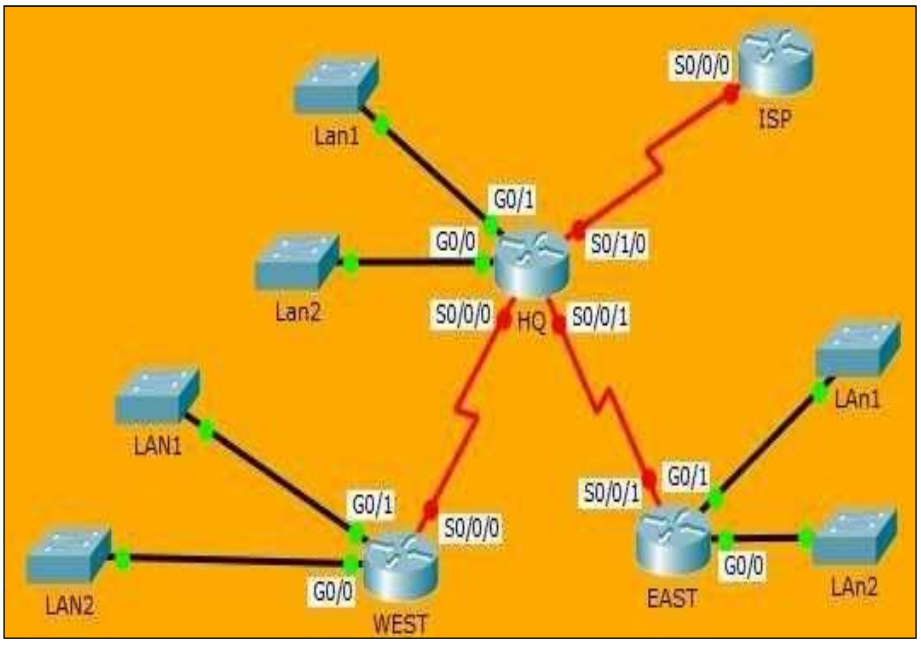


Tabla de direccionamiento

Subred	Dirección IPv4	Dirección IPv6
LAN1 de HQ	192.168.64.0 /23	2001:DB8:ACAD:E ::/64
LAN2 de HQ	192.168.66.0 /23	2001:DB8:ACAD:F ::/64
LAN1 de EAST	192.168.68.0 /24	2001:DB8:ACAD:1 ::/64
LAN2 de EAST	192.168.69.0 /24	2001:DB8:ACAD:2 ::/64
LAN1 de WEST	192.168.70.0 /25	2001:DB8:ACAD:9 ::/64
LAN2 de WEST	192.168.70.1 28/25	2001:DB8:ACAD:A ::/64
Enlace desde HQ a ESTE	192.168.71.4 /30	2001:DB8:ACAD:1 000::/64
Enlace desde HQ a WEST	192.168.71.0 /30	2001:DB8:ACAD:2 000::/64
Enlace desde HQ a ISP	209.165.201. 0/30	2001:DB8:CC1E:1 ::/64

Calculo de rutas resumidas IPv4

En la siguiente tabla se Muestra el cálculo de rutas resumidas en IPv4 y de las cuales se tienen también la máscara de subred para las redes resumidas.

					128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
HQ LAN1	192.168.64.0/23		192	168	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HQ LAN2	192.168.66.0/23		192	168	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0
Red sumarizada 1 HQ	192.168.64.0/22		192	168	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAST LAN1	192.168.68.0/24		192	168	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
EAST LAN2	192.168.69.0/24		192	168	0	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0
Red sumarizada 2 EAST	192.168.68.0/23		192	168	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
WEST LAN1	192.168.70.0/25		192	168	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0
WEST LAN2	192.168.70.128/ 25		192	168	0	1	0	0	0	1	1	0	1	0	0	0	0	0	0	0

Red sumarizada 3 WEST	192.168.70.0/24		192	168	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0
Red sumarizada 1	192.168.64.0/22		192	168	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Red sumarizada 2	192.168.68.0/23		192	168	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Red sumarizada 3	192.168.70.0/24		192	168	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0
Red general sumarizada 1,2,3	192.168.64.0/21		192	168	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Tabla de direccionamiento IPv6

Subred	Dirección IPv6
LAN1 de HQ	2001:DB8:ACAD:E::/64
LAN2 de HQ	2001:DB8:ACAD:F::/64
LAN1 de EAST	2001:DB8:ACAD:1::/64
LAN2 de EAST	2001:DB8:ACAD:2::/64
LAN1 de WEST	2001:DB8:ACAD:9::/64
LAN2 de WEST	2001:DB8:ACAD:A::/64
Enlace desde HQ a ESTE	2001:DB8:ACAD:1000::/64
Enlace desde HQ a WEST	2001:DB8:ACAD:2000::/64
Enlace desde HQ a ISP	2001:DB8:CC1E:1::/64

Calculo de rutas resumidas IPv6

En la siguiente tabla se muestra el cálculo de rutas resumidas en IPv6 y de las cuales también presentan la máscara de subred para las redes resumidas calculadas.

HQ LAN1	2001:D88:ACAD:E::/64	2001	D88	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	16 BIT EN 0
HQ LAN2	2001:D88:ACAD:F::/64	2001	D88	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	16 BIT EN 0
Red sumarizada 1 HQ	2001:D88:ACAD:E::/63	2001	D88	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	16 BIT EN 0
EAST LAN1	2001:D88:ACAD:1::/64	2001	D88	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	16 BIT EN 0
EAST LAN2	2001:D88:ACAD:2::/64	2001	D88	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	16 BIT EN 0
Red sumarizada 2 EAST	2001:D88:ACAD:0::/62	2001	D88	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16 BIT EN 0
WEST LAN1	2001:D88:ACAD:9::/64	2001	D88	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	16 BIT EN 0
WEST LAN2	2001:D88:ACAD:A::/64	2001	D88	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	16 BIT EN 0
Red sumarizada 3 WEST	2001:D88:ACAD:8::/62	2001	D88	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	16 BIT EN 0
Red sumarizada 1	2001:D88:ACAD:E::/63	2001	D88	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	16 BIT EN 0
Red sumarizada 2	2001:D88:ACAD:0::/62	2001	D88	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16 BIT EN 0
Red sumarizada 3	2001:D88:ACAD:8::/62	2001	D88	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	16 BIT EN 0
Red sumarizada 1,2,3	2001:D88:ACAD:0::/60	2001	D88	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16 BIT EN 0

Con el desarrollo del ejercicio se puede determinar que una dirección IPv4 está determinada en 32 bits comprendida en 4 grupos de octetos y su transformación se realiza mediante números binarios. Para una IPv6 está determinada en 128 bits y su transformación se realiza de hexadecimal a números binarios.

Las rutas resumidas reducen el número de entradas en las tablas de routing y hacen que el proceso de búsqueda en dichas tablas sea más eficaz. Facilitan que el router fácilmente pueda buscar redes, en vez de buscar en una lista inmensa de direcciones y solo busque en una red resumida haciéndolo eficiente. Este proceso también disminuye los requisitos de memoria del router.

4) Ejercicio 3.2.2.4 Configuring Trunks

OBJETIVO

Establecer una conexión trunk para transmitir información entre computadores, por medio de switches. Teniendo en cuenta el comando Show vlan Brief que permite mostrar la asignación de VLAN para todos los puertos del switch. Realizar verificación las VLAN, configurar enlaces troncales

Topología

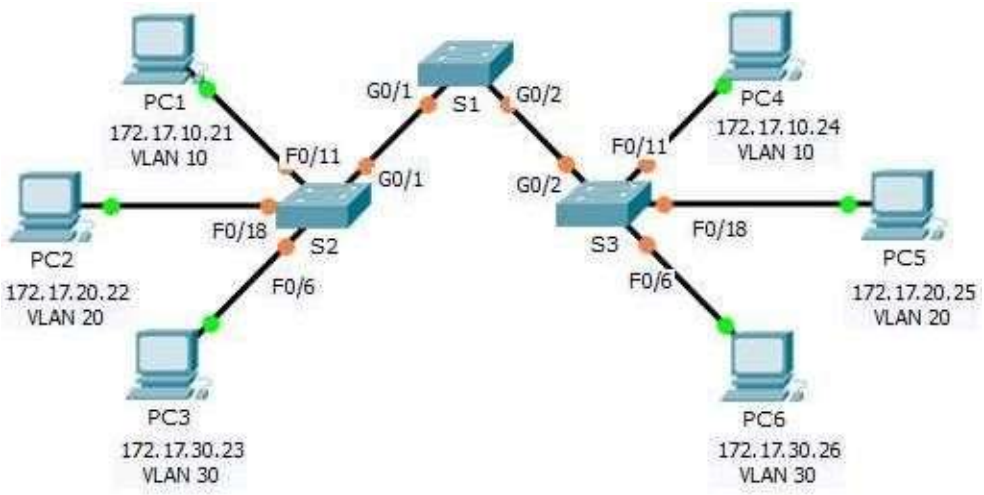


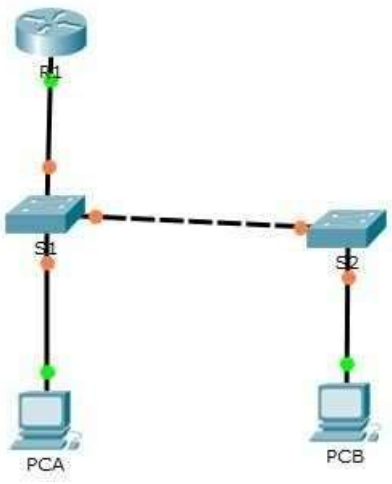
Tabla de direccionamiento

Device	Interface	IP Address	Subnet Mask	Switch	VLA
PC1	NIC	172.17.10.21	255.255.255.0	S2 F0/11	10
PC2	NIC	172.17.20.22	255.255.255.0	S2 F0/18	20
PC3	NIC	172.17.30.23	255.255.255.0	S2 F0/6	30
PC4	NIC	172.17.10.24	255.255.255.0	S3 F0/11	10
PC5	NIC	172.17.20.25	255.255.255.0	S3 F0/18	20
PC6	NIC	172.17.30.26	255.255.255.0	S3 F0/6	30

Mediante el desarrollo de la práctica se logra entender el porque es importante implementar las VLAN en los Switch, ya que permiten que redes IP y subredes múltiples existan dentro de la misma red, ya que sirven para reducir el tamaño del broadcast y ayudan en la administración de la misma separando segmentos lógicos como departamentos para una empresa, oficina, universidades, etc.

Los puertos troncales pueden transportar el tráfico de múltiples VLANs y las pueden extender a través de toda la red, mediante el protocolo estándar de la industria IEEE 802.1Q, para transportar el tráfico de las múltiples VLAN sobre un solo enlace.

5) Ejercicio 5.1.3.7 Configuring_802.1Q_Trunk-Based_Inter-VLAN_Routing
Topología



Enrutamiento on-a-stick

- Este tipo de enrutamiento permite que una única interfaz del router realice el enrutamiento del tráfico de varias VLAN.
- Se configura la interfaz del router en modo troncal y se conecta a una interfaz el switch configurada en modo troncal.

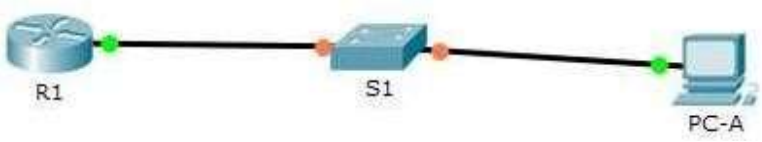
En el router se creará por cada VLAN una subinterfaz. En cada subinterfaz se especifica el tipo de encapsulación dot1q donde se indica las tramas estarán etiquetadas. Dentro de las ventajas que presenta este tipo de enrutamiento esta que las subinterfaces permiten ampliar el número de VLAN que las interfaces físicas y se reduce el número de cables de conexión entre el router y el switch

6) Ejercicio 2.2.4.11 Configuring_Switch_Security_Features

OBJETIVO

Configurar los parámetros básicos de los dispositivos y verificar la conectividad e igualmente verificar el acceso por SSH en S1

Topología



Durante la práctica de este laboratorio se crea la VLAN 99 en el switch y se le asigna una IP, y al revisarla con el comando show vlan nos indica que esta se encuentra activa, luego procedemos a verificar mediante el comando show ip interface brief cuál es el estado que en este caso es “up” que nos indica que esta activo y el protocolo “down” o abajo porque a pesar de haber ejecutado el comando no shutdown para la interfaz 99 hasta el momento no hay un puerto físico en el switch que haya sido asignado a la VLAN99. Cuando asignamos los puertos f0/5 y f0/6 a la VLAN 99 ejecutamos el comando show ip interface brief y nos muestra que están activos y al realizar un ping desde la PC-A al S1 el resultado es satisfactorio porque hay conectividad y todos los paquetes son entregados.
Al Configurar y verificar el acceso por SSH en el S1 En las instrucciones mostradas en la guía se presenta un error: S1(config)# crypto key generate rsa modulus 1024 (packet tracer no admite este commando por lo tanto se hace de la siguiente manera: S1(config)# crypto key generate rsa

¿Por qué habilitaría la seguridad de puertos en un switch? Y ¿Por qué deben deshabilitarse los puertos no utilizados en un switch?

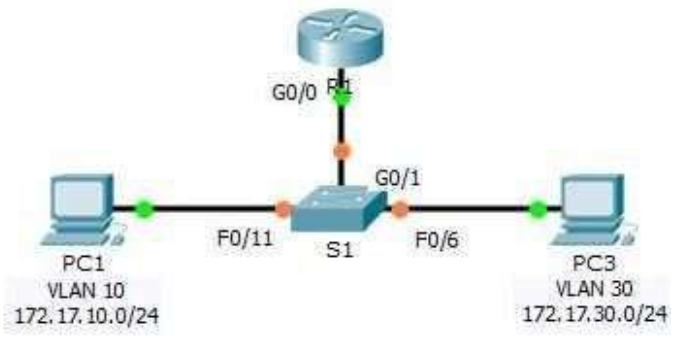
Al habilitar la seguridad de los puertos a ayuda a prevenir el acceso no autorizado de dispositivos no autorizados a la red y se debe tener claro que aquellos puertos que no están en uso se deben deshabilitar para que ningún usuario o personal no autorizado se conecta al switch y pueda acceder desde este puerto a la red.

7) Ejercicio 5.1.3.6 Configuring_Router-on-a-Stick_Inter-VLAN_Routing

OBJETIVO

Realizar la prueba de conectividad sin enrutamiento entre VLAN y con el enrutamiento entre VLAN después de añadir la VLAN al switch

Topología



Se realiza Ping de PC 1 a PC 2 y esta falla porque la pc1 está en una red diferente a la PC 3 y la PC 1 no puede obtener la dirección MAC de la PC 3.
Al crear la VLAN 10 Y VLAN 30 en el switch y asignar los puertos verificamos la conectividad mediante un ping de la PC1 a la PC3 y nos damos cuenta que no hay comunicación ya que cada VLAN está en una red diferente y se requiere de un router o un switch capa 3 para que haya comunicación entre las pc.

Para dar solución a lo anterior configuramos en el router R1 las subinterfaces G0/0.10 y G0/0.30 asignando las direcciones IP mediante encapsulación 802.1Q y luego el puerto de conexión al router debe ser configurado como una troncal (Trunk) ya que en el paso anterior el router fue configurado con múltiples subinterfaces asignadas a diferentes VLAN.
Se comprueba la conectividad y el ping es satisfactorio entre la PC1 y la PC3.

8) Ejercicio 6.2.4.5_Lab_-_Configuring_IPv6_Static_and_Default_Routes

OBJETIVO

Armar y configurar toda la red mediante los parámetros básicos de los dispositivos estableciendo la comunicación con redes remotas que no están conectadas directamente a través de la configuración de rutas estáticas y predeterminadas IPv6, y de forma automática para los host finales.

Topología

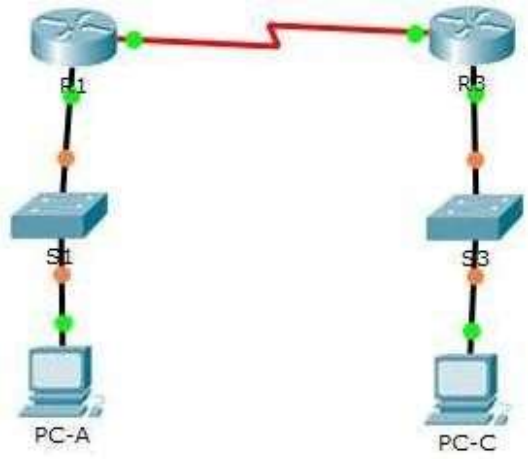


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6/longitud de prefijo	Gateway predeterminado
R1	G0/1	2001:DB8:ACAD:A::/64 eui-64	N/A
	S0/0/1	FC00::1/64	N/A
R3	G0/1	2001:DB8:ACAD:B::/64 eui-64	N/A
	S0/0/0	FC00::2/64	N/A
PC-A	NIC	SLAAC	SLAAC
PC-C	NIC	SLAAC	SLAAC

Al configurar los dispositivos siguiendo la guía de trabajo y verificando la conectividad, el ping falla. Porque los routers no tienen configuradas las rutas estáticas o dinámicas y solamente conocen acerca de sus redes, sin las rutas apropiadas ellos descartan los paquetes hacia redes desconocidas.

Al utilizar diversos comandos como el ping y el ipconfig, nos damos cuenta si en verdad quedó bien construida nuestra red, o si fallamos en algo en la parte de la configuración, si quedó bien elaborada tendremos una conectividad satisfactoria, además con estos comandos podemos conocer las direcciones de nuestros equipos, la global, local y enlace.

Es importante conocer y saber configurar los diferentes dispositivos que conforman nuestra red. Para poder verificar lo anterior usamos el comando Show el cual nos muestra toda la información que deseemos consultar a la hora de validar nuestra red.

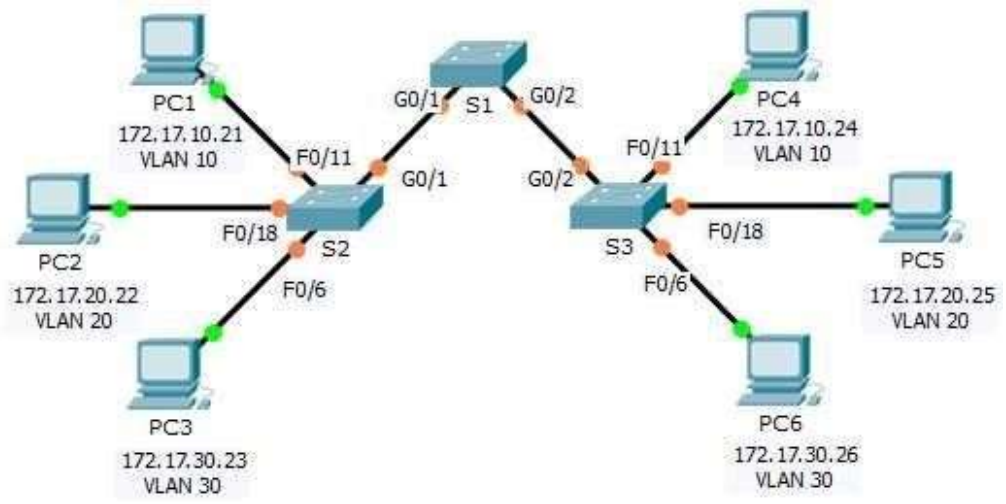
Muchos proveedores de servicios de comunicaciones están implementando direccionamiento IPv6 y hacia un futuro no muy lejano se requerirá la implantación en los dispositivos de red el direccionamiento IPv6 de tal manera que como administrador de red se puede requerir la reconfiguración de los equipos de IPv4 a IPV6.

La configuración de rutas estáticas y predeterminadas en IPv6 es similar a la configuración de rutas estáticas y predeterminadas en IPv4. Existen algunas diferencias mínimas al momento de configurar las rutas estáticas y predeterminadas entre IPv4 e IPv6 como el comando **IPv6 route** para IPv6 en lugar de **IP route** para IPv4 cuando se configura una ruta estática e igual manera para verificar la tabla de ruteo en IPv6 se Utiliza el comando **show IPv6 route** en lugar de **show IP route** utilizado en IPv4.

9) Ejercicio 3.2.1.7 Packet Tracer - Configuring VLANs

OBJETIVO

Realizar la Verificación de la configuración por defecto de la VLAN y reconfigurar la VLAN asignándola a los puertos.



Topología

Las VLAN son útiles en la administración de grupos lógicos, permitiendo a los miembros de un grupo que se pueden mover fácilmente, cambiar o añadir.

Tabla de direccionamiento

Device	Interface	IP Address	Subnet Mask	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	10
PC2	NIC	172.17.20.22	255.255.255.0	20
PC3	NIC	172.17.30.23	255.255.255.0	30
PC4	NIC	172.17.10.24	255.255.255.0	10
PC5	NIC	172.17.20.25	255.255.255.0	20
PC6	NIC	172.17.30.26	255.255.255.0	30

- Al realizar la verificación de la Vlan, todos los puertos están asignados a la Vlan1
- Al realizar el ping del Pc1 al Pc4, del Pc2 al Pc5 y del Pc3 al Pc6, su resultado fue satisfactorio, ya que estos equipos pertenecen a la misma red
- Al realizar el ping a otra pc, por ejemplo del Pc1 al Pc6, el ping falla, a pesar de que se encuentran en el mismo dominio de broadcast, hay solo una vlan, pero el PC6 se encuentra en otra red.
- Al Crear y nombrar la Vlan en S1, no hay puertos asignados a la Vlan.
- Al Asignar los puertos al S2 y S3 no existe conectividad entre Pc1 a Pc4 ya que aunque están asignados no están configurados, por tanto se debe configurar los puertos entre los switchs como troncales para permitir pasar muchas Vlan a través del mismo enlace.
- Después de configurar los puertos como troncales se realiza de nuevo el ping siendo este satisfactorio.

Es importante realizar la verificación de la Vlan, para observar dónde se encuentran asignados los puertos.

- Al realizar ping a diversos equipos pertenecientes a la misma red, su resultado siempre será satisfactorio.
- Al realizar el ping a otros equipos, no pertenecientes a la misma red, el ping falla, a pesar de que se encuentren en el mismo dominio de broadcast.

Es muy útil crear las Vlan para prevenir que haya mucho tráfico de broadcast y que todo sea un solo dominio de colisión, necesitamos muchas láminas de colisión para prevenir las tormentas de broadcast, para que no haya mucha congestión con paquetes broadcast en la red, además de la reducción de costos y mayor rendimiento.

Después de configurados los puertos para las diferentes Vlan, si se presenta fallo en la realización de los ping, debemos configurar los puertos entre los interruptores como troncales, los cuales permiten pasar muchas Vlan a través del mismo enlace, después de configurar los puertos como troncales el ping debe ser satisfactorio.

10) Ejercicio 6.2.2.5 Configuring_IPv4_Static_and_Default_Routes

OBJETIVO

Configurar los parámetros básicos de los dispositivos, estableciendo la topología y configurar las rutas estáticas de las mismas permitiendo probar la configuración y revisar conectividad.
Establecer la topología e inicializar los dispositivos, configurar los parámetros básicos de los dispositivos y verificar la conectividad, configurar rutas estáticas.

Topología

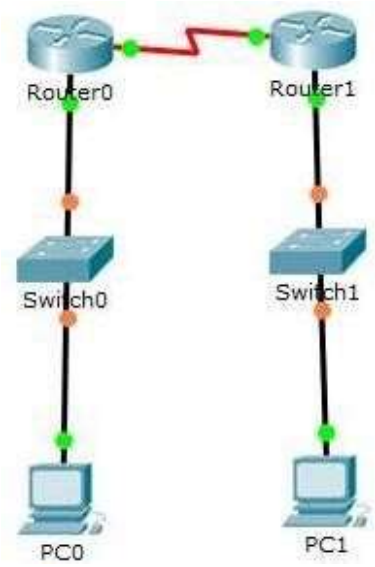


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.0.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.25	N/A
R3	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.2	255.255.255.25	N/A
	Lo0	209.165.200.22	255.255.255.22	N/A
	Lo1	198.133.219.1	255.255.255.0	N/A
PC-A	NIC	192.168.0.10	255.255.255.0	192.168.0.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Con la elaboración de la práctica se logra entender como configurar los parámetros básicos teniendo en cuenta la topología, de igual manera las rutas estáticas son muy comunes y no requieren la misma cantidad de procesamiento y sobrecarga que los protocolos de routing dinámico, el enrutamiento es fundamental para cualquier red de datos, ya que transfiere información a través de una internetwork de origen a destino. Los routers son dispositivos que se encargan de transferir paquetes de una red a la siguiente.

En la nueva red 192.168.3.0/24 está conectada a la interfaz G0/0 del R1. Se podría utilizar para configurar una ruta estática a R3 la siguiente configuración:

R3(config) ip route 192.168.3.0 255.255.255.0 **10.1.1.1(**IP del siguiente salto) o la interfaz directamente conectada **s0/0/0** de R3

También se puede utilizar la ruta por defecto R3(config) ip route 0.0.0.0. 0.0.0.0 **10.1.1.1**

De igual manera en la configuración de una ruta estática conectada directamente la interfaz de salida se resuelve en una sola búsqueda mientras que por medio de una reuta estática necesitara dos búsquedas para resolver la interfaz de salida recursiva. También es importante configurar una ruta predeterminada en un router ya que ayuda a reenviar paquetes hacia rutas desconocidas.

11) Ejercicio 2.2.4.9 Configuring_Switch_Port_Security

OBJETIVO

Entender e implementar como se establece la seguridad en los puertos del Switch, y de igual manera limitar o restringir las direcciones MAC, autorizadas para enviar o recibir tráfico, Configurar y Verificar la seguridad de los puertos.

Topología

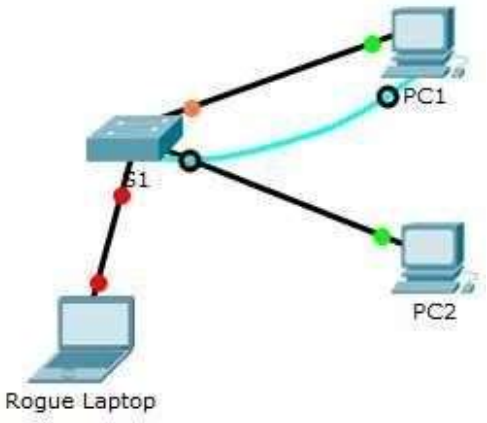


Tabla de direccionamiento

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0
Rogue Laptop	NIC	10.10.10.12	255.255.255.0

Esta actividad está diseñada para mostrar cómo se debe implementar la seguridad en los puertos del switch, de igual manera realizar bloqueos de ciertas MAC de diferentes equipos, para tener un control de la cantidad de equipos que se podrían conectar en la red evitando que puedan enviar trafico mediante los puertos, también se podría aplicar para que los intrusos no puedan obtener información de forma fraudulenta.

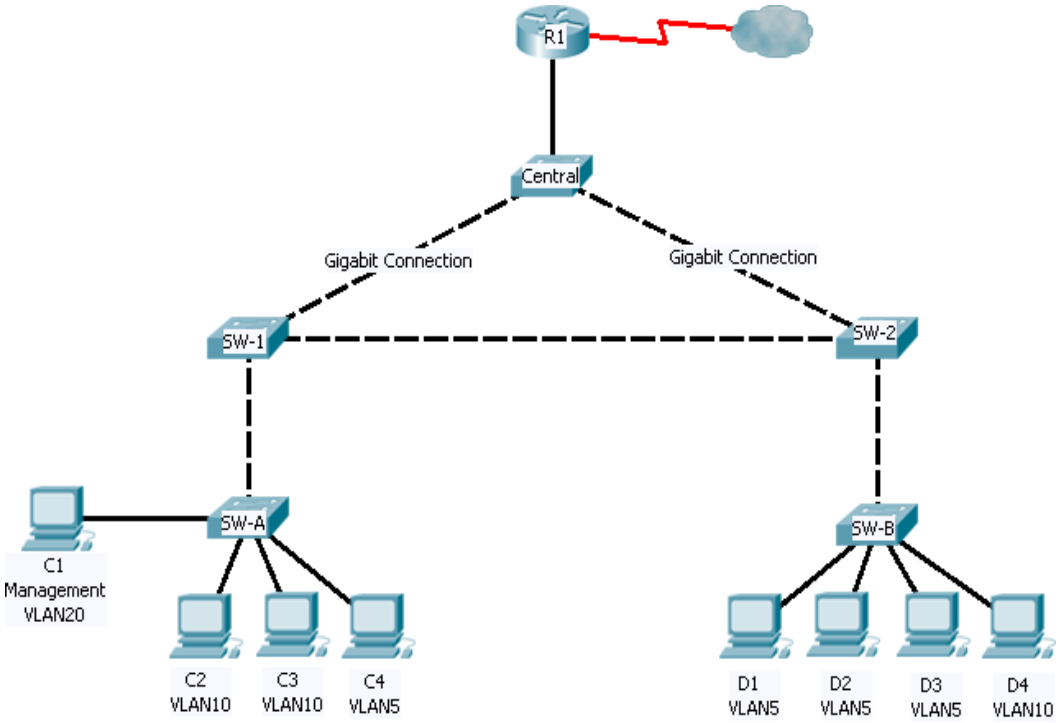
12) Ejercicio 6.5.1.3 Layer_2_VLAN_Security

OBJETIVO

Entender e implementar como se establece la seguridad en los puertos trúncales del Switch, y de igual manera limitar o restringir el acceso a usuarios externos, en la red y la creación del VLANS.

- Conecte un nuevo enlace redundante entre SW-1 y SW-2
- Habilitar y configurar la seguridad de los enlaces en el nuevo puerto troncal entre SW-1 y SW-2
- Implementar una ACL para evitar acceso de usuarios externos la VLAN de administración.

Topología



Esta práctica de laboratorio está diseñada para mostrar cómo se debe implementar la seguridad en los puertos del switch, de igual manera realizar bloqueos en puertos troncales para evitar que usuarios externos se puedan conectar a la red, también es muy importante la creación de las VLAN, ya que es un método para crear redes lógicas independientes dentro de una misma red física, ya que permiten mejorar la administración de la misma dividiéndola en los diferentes departamentos en una empresa.

13) Ejercicio 3.3.2.2 Implementing VLAN Security

OBJETIVO

Armar la red y configurar los parámetros básicos de seguridad para los puertos de enlace troncal y de acceso en los switches, verificar la conectividad y analizar su comportamiento.

Topología

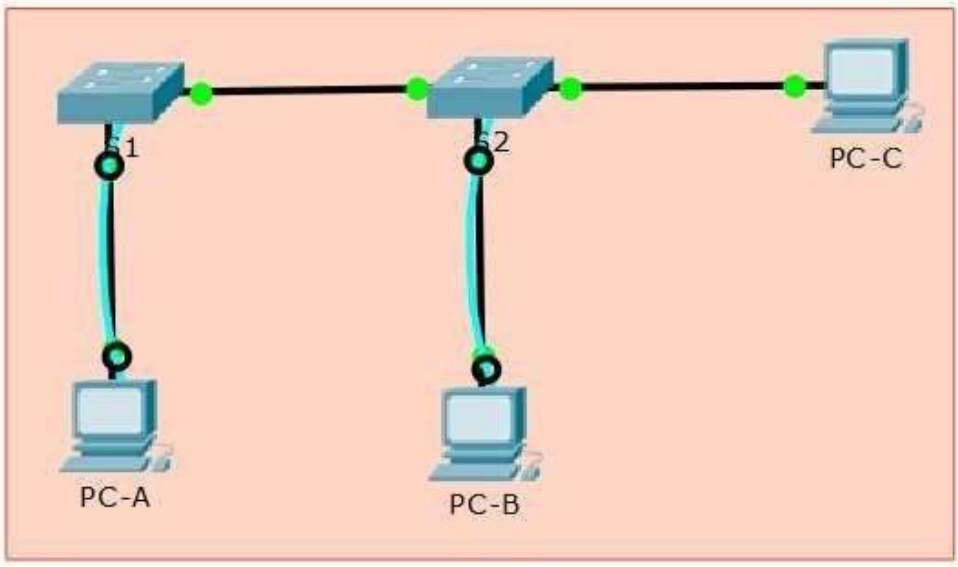


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de	Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
PC-A	NIC	172.17.99.3	255.255.255.0	172.17.99.1
PC-B	NIC	172.17.10.3	255.255.255.0	172.17.10.1
PC-C	NIC	172.17.99.4	255.255.255.0	172.17.99.1

Asignaciones de VLAN

VLAN	Nombre
10	Datos
99	Management&Native
999	BlackHole

Para esta actividad de laboratorio se utiliza la herramienta de simulación packet tracer. Se arma la topología planteada configurando los equipos en forma básica siguiendo la tabla de direcciones IP relacionada y habilitando la autenticación de los mismos con fines de seguridad en la red y acceso a los enlaces troncales.

Con lo estudiado en las temáticas se aprende a crear VLAN e implementar su seguridad, como protección contra ataques de VLAN y la posible detección de tráfico de la red dentro de esta. Así los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.
Con el desarrollo del ejercicio se pudo evidenciar:

1. observa que un puerto sin asignar siempre va a pertenecer a la VLAN 1 predeterminada.
2. En el simulador Packet Tracer no se pude realizar la función de deshabilitar el servicio web básico en ejecución pero en esencia si se puede realizar en un equipo real.
3. Para que se puede establecer comunicación entre los equipos se debe cumplir estar en la misma red, en la misma VLAN, establecer enlaces troncales que permitan la extensión entre los switches, adicionalmente tener un Reuter para conectar las LAN.
4. Como seguridad es importante cambiar la VLAN nativa para los puertos de enlace troncal de la VLAN 1 a otra VLAN.
5. Por motivos de seguridad, se recomienda permitir que solo se transmitan las VLAN deseadas y específicas a través de los enlaces troncales en la red.
6. El mensaje %CDP-4-NATIVE_VLAN_MISMATCH en los switches indica que las VLAN nativas en los switches no coinciden. Por ejemplo para S1 la VLAN nativa es la VLAN 99 y para S2 la VLAN nativa es la VLAN 1
7. Se recomienda colocar todos los puertos sin utilizar en una VLAN de “agujero negro”. Ya que aunque se deshabiliten los puertos sin utilizar en los switches, si se conecta un dispositivo a uno de esos puertos y la interfaz está habilitada, se podría producir un enlace troncal.
8. En este ejercicio los puertos que se envían a la VLAN 99 no pueden negociar su puerto con nadie y se restringe el paso a la VLAN 999 que es la que presenta los puertos que no se utilizan y solo pasan por la troncal creada de la f0/1 la VLAN 10 y la 99.

VLAN Nativa

El punto 9 del estándar define el protocolo de encapsulamiento usado para multiplexar varias VLAN a través de un solo enlace, e introduce el concepto de las VLAN nativas. Las tramas pertenecientes a la VLAN nativa no se etiquetan con el ID de VLAN cuando se envían por el trunk. Y en el otro lado, si a un puerto llega una trama sin etiquetar, la trama se considera perteneciente a la VLAN nativa de ese puerto. Este modo de funcionamiento fue implementado para asegurar la interoperabilidad con antiguos dispositivos que no entendían 802.1Q.

La VLAN nativa es la vlan a la que pertenecía un puerto en un switch antes de ser configurado como trunk. Sólo se puede tener una VLAN nativa por puerto. Para establecer un trunking 802.1q a ambos lados debemos tener la misma VLAN nativa

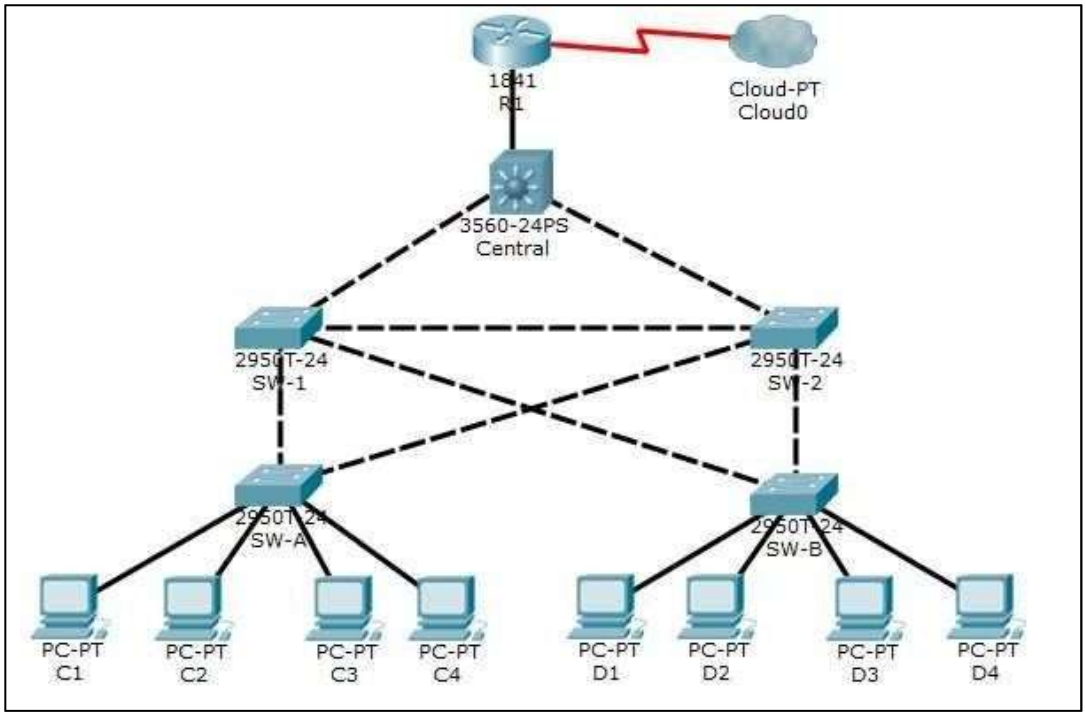
porque la encapsulación todavía no se ha establecido y los dos switches deben hablar sobre un link sin encapsulación (usan la native VLAN) para ponerse de acuerdo en estos parámetros.
Si se tiene una configuración predeterminada todos los puertos en la VLAN 1 se corre el riesgo en la seguridad ya que cualquiera que tenga un conocimiento amplio de programación podría acceder remotamente a la red.

14) Ejercicio 6.5.1.2 Layer 2 Security

OBJETIVO

Asignar el router central como switch raíz, habilitar y asegurar los parámetros necesarios para evitar tormentas broadcast, manipulación STP (spanning –tree) y desbordamiento de la tabla de direcciones MAC en la red.

Topología



Si se tiene una configuración predeterminada todos los puertos en la VLAN 1 se corre el riesgo en la seguridad ya que cualquiera que tenga un conocimiento amplio de programación podría acceder remotamente a la red.
Con el desarrollo de esta actividad se obtiene el conocimiento sobre que es en comunicaciones el protocolo de red nivel 2 **STP** (**S**panning **T**ree **P**rotocol) donde su

importancia radica en garantizar la disponibilidad de las conexiones a través de la gestión a la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes que pueden dejar inutilizada la red.

Dentro de estos problemas de enlaces redundantes tenemos:

Tormentas de broadcast: los broadcast en la red son reenviados una y otra vez y permanecen circulando en la misma sin fin. Lógicamente, al no eliminarse la situación se agrava con cada nuevo broadcast.
Múltiples copias de una trama: con la redundancia es muy probable que un host reciba una trama repetida, dado que la misma podría llegar por dos enlaces diferentes.
Tabla MAC: una trama que proviene de una MAC en particular podría llegar desde enlaces diferentes.
Bucles recursivos: un bucle puede generar un nuevo bucle y estos crecer de forma exponencial. En una situación así la red quedará inusable en pocos segundos.

El Protocolo de Spanning Tree (STP) resuelve estos problemas obteniendo así una red redundante y dinámica libre de los problemas asociados a la redundancia. El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice la eliminación de bucles.
Con la realización del ejercicio igualmente se pudo observar que SWITCH RAIZ es el que tiene el BRIDGE ID PRIORITY más bajo de la toda la red. Y se tienen nuevos comandos para la implementación de seguridad de capa 2.

15) Ejercicio 3.2.2.5 Configuring VLANs AND Trunking

OBJETIVO

La red configurando los parámetros básicos de los dispositivos, las redes VLAN y asignación de los puertos de switch salvaguardando la base de datos de VLAN, para luego configurar un enlace troncal 802.1Q entre los switches y eliminar la base de datos de VLAN

Topología

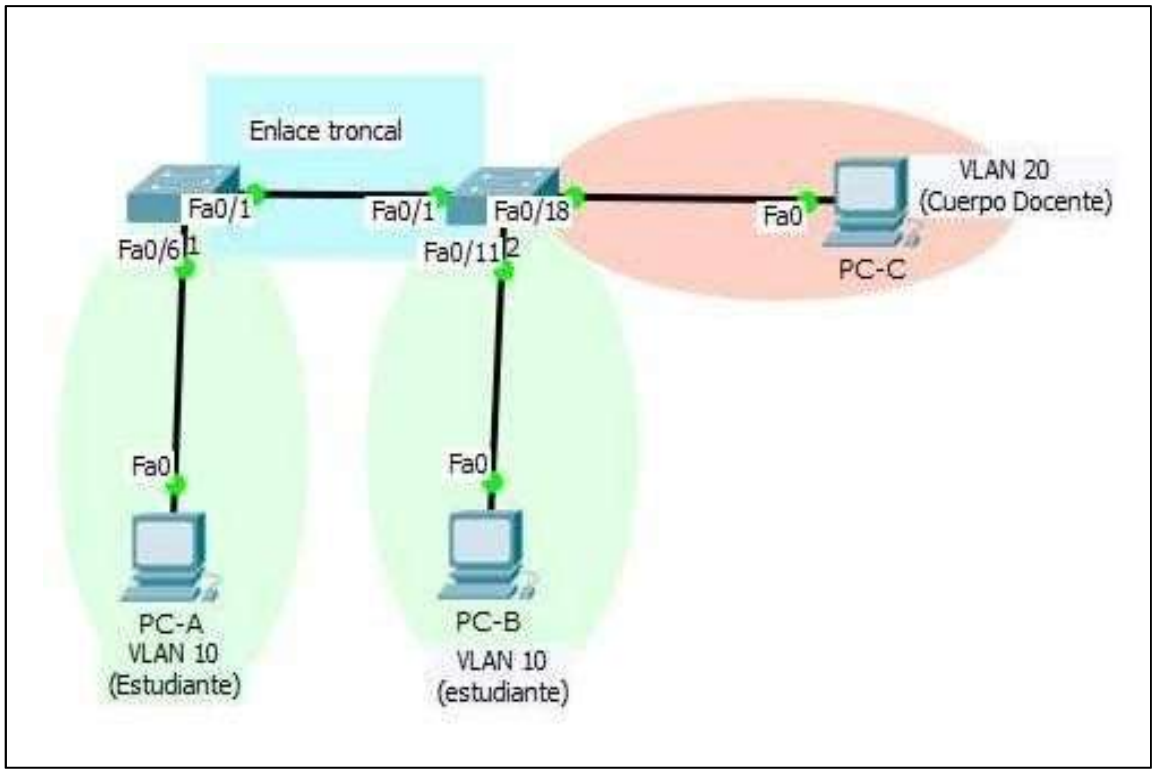


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de	Gateway
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

En el desarrollo de esta actividad se utiliza la herramienta de simulación packet tracer, para el laboratorio. Primeramente se configuran los switches de forma básica, habilitando la autenticación de los mismos con fines de seguridad en la red. Teniendo en cuenta la topología de red se configuran los equipos host siguiendo a tabla de direccionamiento.

En síntesis con el desarrollo del ejercicio se pudo evidenciar:

1. los equipos finales no pueden comunicarse por estar en diferentes redes y los únicos que se comunican son los switches ya que están en la misma red.

2. Al crear las VLAN los puertos se asignan a la VLAN predeterminada o default.
3. Cuando se asigna la dirección IP y la máscara de red a la VLAN 99 está queda en estado de apagado debido a que no se la ha asignado ningún puerto.
4. Al asignar las VLAN a la interfaces del switch de manera correcta se pierde la conectividad entre la PC-A a la PC-B así como los switch S1 y S2, aunque estén en la VLAN 10, pero los puertos de las fastethernet 0/1 de los switches están en la VLAN 1 que no está activa por lo tanto no hay comunicación por la F0/1 de S1 y la F0/1 de S2.
5. Al eliminar una asignación VLAN de una interfaz, dicha interfaz queda asociada a la VLAN determinada. Antes de eliminar una VLAN de la base de datos, se recomienda reasignar todos los puertos asignados a esa VLAN.
6. Al agregar un VLAN desconocida a la base de datos la VLAN toma el nombre predeterminado del número asignado.
7. Todas las VLAN de manera predeterminada permiten un enlace troncal y permite que todas las VLAN atraviesen F0/1.
8. Para permitir que los hosts en la VLAN 10 se comuniquen con los hosts en la VLAN 20 se necesita implementar un router capa 3.
9. Los beneficios principales que se puede obtener mediante el uso eficaz de las VLAN son seguridad, dominios de broatcast
10. Se identifican nuevos comandos para la implementación de la red en la creación de la VLAN y en la creación de troncales de VLAN.

Con la información suministrada en los módulos de trabajo y el ejercicio para esta actividad se aprende a crear VLAN, redes de área local virtual que mejoran el rendimiento de la red mediante la división de grandes dominios de difusión de capa 2 en otros más pequeños. Adicionalmente se realiza el aprendizaje en la creación de troncales de VLAN para englobar la red VLAN a través de varios dispositivos y poderse comunicar.

Una VLAN es un método para crear redes lógicas independientes, agrupa un conjunto de equipos de manera lógica y no física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, también se pueden usar como medida de seguridad al controlar qué hosts se pueden comunicar.

Una VLAN consiste en dos redes de ordenadores que se comportan como si estuviesen conectados al mismo PCI. Es posible liberarse de las limitaciones de la arquitectura física como limitaciones geográficas, limitaciones de dirección, entre otras, ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, números de puertos, protocolo, etc.) aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local.

Un enlace troncal es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red, permiten transferir el tráfico de varias VLAN a través de un

único enlace y conservar intactas la segmentación y la identificación de VLAN. Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

16) Ejercicio 6.3.3.7
Designing_and_Implementing_IPv4_Addressing_with_VLSM

Enviado en forma individual por cada integrante al correo nancy.guaca@unad.edu.co

CONCLUSIONES

Con la realización de los ejercicios correspondientes a la unidad 3 (Configuración de Sistemas de Red Soportados en VLANs). se profundiza en el contenido propuesto de la misma y se evidencia la importancia de varios factores que se deben tener en cuenta en el momento de diseñar una red confiable y segura.

La seguridad de puertos del switch es un requisito importante para evitar los ataques como la saturación de direcciones MAC y la suplantación de identidad de DHCP, lo cual se deben configurar para permitir que ingresen solo las tramas con direcciones MAC de origen específico y rechazar las direcciones MAC de origen desconocidas.

Se aprende que el enrutamiento inter VLAN es el proceso de tráfico de enrutamiento entre diferentes VLAN, mediante un router dedicado o un switch multicapa y se analiza la configuración y la verificación de redes VLAN y de enlaces troncales, considerando los principios básicos de seguridad y de diseño en el contexto de las redes VLAN.

La tabla de enrutamiento, en realidad, es una estructura jerárquica que se usa para acelerar el proceso de búsqueda cuando se ubican rutas y se reenvían paquetes.

Se aprendió cómo pueden utilizarse las rutas estáticas IPv4 e IPv6 para alcanzar redes remotas que son redes a las que se puede llegar únicamente mediante el envío del paquete a otro router.

Finamente se realiza y se comprende el método de rutas resumidas las cuales tienen menos entradas tabla de enrutamiento y el proceso de búsqueda en la tabla será más rápido y eficiente.

BIBLIOGRAFÍA

Cisco Networking Academy. (2015). CP CISCO CCNA 2-2015. Routing y switching de CCNA: Principios básicos de routing y switching.
Recuperado de https://1314297.netacad.com/courses/253834

Universidad Nacional Abierta y a Distancia. (2015). Curso de Profundización. Guía Integrada de Actividades. Escuela. ECBTI.

Universidad Nacional Abierta y a Distancia. (2015). Aula virtual. Foro Entorno de Aprendizaje Colaborativo. Tarea Unidad 3. Foro momento 5
Recuperado de
http://66.165.175.209/campus17_20151/mod/forum/discuss.php?d=6095