UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERÍA
SEGURIDAD DE REDES
SDR404

G01T
FORO #2

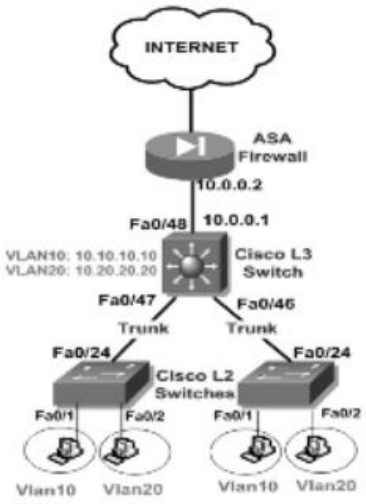
Integrantes:

Carlos Eduardo Peñate Salazar. PS190756
Jairo José Hernández Abrego HA190640

Contenido

1-Primera pregunta

Basándose en la distribución de dispositivos dentro de las capas del Modelo de Referencia OSI. Analizar el diagrama y determinar los dispositivos de una Capa y los dispositivos Multicapa a utilizar. Se tiene que justificar el porqué de cada uno de los dispositivos y explicar la función que cada uno de ellos dentro de la topología.



Capa 1:

- Computadoras (Dispositivos).

Capa2 (Enlace):

- Switch Cisco L2, este dispositivo pertenece a esta capa puesto que realiza la función de crear las redes lógicas independientes de los dispositivos físicos y estas se puedan enlazar bajo las interfaces señaladas en el diagrama, las cuales son: Vlan10 Fa0/1, Vlan20 Fa0/2, siendo esta configuración para ambos switches.

Capa3 (Red):

- Switch Cisco L3, este dispositivo pertenece a esta capa debido a que esta realiza el proceso de enrutamiento para que ambas Vlan creadas anteriormente puedan comunicarse entre sus semejantes, por ejemplo, la Vlan10 del switchL2-1 pueda comunicarse con la Vlan10 del switchL2-2, además de ello este Switch L3 puede realizar procesos de enrutamiento tales como: RIP, RIP2, OSPF, Etc. Como también conexión a internet.
- Router ASA Firewall, de igual manera este dispositivo pertenece a capa 2 porque esta realiza la función de garantizar o enviar los paquetes de datos hacia internet si este lo desea, a la vez cumple con un requerimiento de seguridad al administrar amenazas que estas pueden presentar.

Multicapas (Capa 2- Capa 3):

- Router ASA Firewall, este dispostivo pertenece a ambas capas debido a que encarga de proporcionar los medios funcionales para establecer la comunicación de los elementos físicos hacia los dispositivos exteriores conectados mediante VPN para protección y seguridad de datos.

- Switch Cisco L3, por igual manera este dispositivo forma parte de ambas capas puesto que enlaza y enruta los paquetes mediante redireccionamiento lógico y administra el control de las Vlan, además comprueba las direcciones IP de origen y destino de cada paquete de la tabla correspondiente de enrutamiento, para finalmente regresar cada paquete a su destino tal y como lo realiza un router, pero con la diferencia que este lo desarrolla dentro de la LAN.

Funciones de cada dispositivo:

Router ASA Firewall

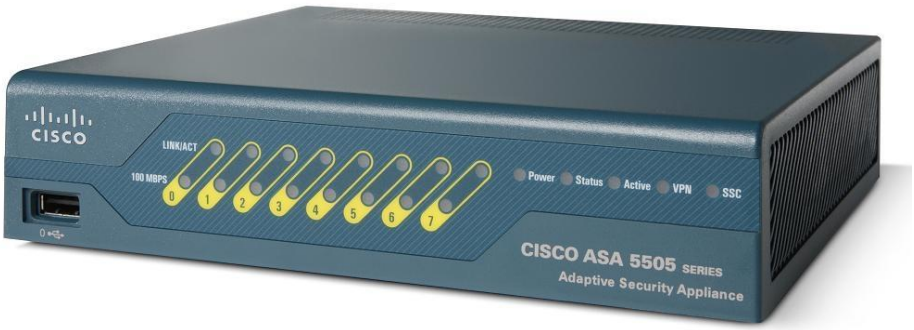
En esta topología se está utilizando el router ASA Firewall donde este realiza la función de garantizar o enviar los paquetes de datos hacia internet si este lo desea para proporcionar comunicación y enrutamiento entre los elementos físicos pertenecientes a la red física con los dispositivos exteriores conectados mediante VPN siempre cumpliendo con los requisitos de protección de seguridad de datos. Cabe recalcar que esta comunicación muchas veces tiene un tiempo de duración máxima desde 5 hasta 10 horas o más. De igual manera el funcionamiento de este se basa en el inicio de sesión con usuarios pertenecientes a grupos de trabajos los cuales permite a estos conectarse a sus áreas de trabajos ya sea dentro de áreas físicas en un mismo lugar o en el exterior permitiendo así comunicación entre todos los usuarios conectados.

Ventajas:

- Protección de información privada: Define que usuarios de la red y que información va a obtener cada uno de ellos.
- Optimización de acceso: Define de manera directa los protocolos a utilizarse
- Protección de intrusos: Protege de intrusos externos restringiendo los accesos a la red.

Desventajas:

- No protege de la copia de datos importantes si se ha obtenido acceso a ellos.
- No protege de ataques de ingeniería social (ataques mediante medios legítimos. Por ejemplo, el atacante contacta a la víctima haciéndose pasar por empleado de algún banco, y solicita información confidencial, o en otro caso trabajar desde casa en un Call Center)



Switch Capa 3

Los dispositivos switch realizan la función de interconexión de redes y conecta varios dispositivos en la red, pasando paquetes entre los diferentes dispositivos, pero en este caso el Switch capa 3 es quien está realizando la acción de conmutar los dispositivos y es el encargado del enrutar de paquetes mediante el direccionamiento lógico y el control de subredes.

Algunas de las diferencias que se pueden encontrar entre un switch l2 y un l3 es que los switch l2 funciona por la dirección MAC y no considera la dirección IP ni ningún elemento de capa superior, pero los switch de l3 aun siendo diferente a un switch de capa 2 también hace las funciones de un switch de capa 2, además un switch de capa 3 puede ejecutar enrutamiento estático y enrutamiento dinámico (RIP, OSPF, etc.), en otras palabras un switch de capa 3 dispone de una tabla de direcciones MAC y una tabla de enrutamiento IP, adicional a esto también controla todas las comunicaciones VLAN sin necesidad de router. Los switch de capa 3 además de los paquetes de enrutamiento incluyen funciones que requieren la capacidad de comprender la información de la dirección IP de los datos que ingresan al switch como por ejemplo identificar el tráfico de VLAN según la dirección IP.

También se debe de tener en cuenta que los switch de capa 3 son recomendados para la segmentación o división de redes LAN que son demasiadas grandes donde la simple utilización de switch de capa 2 provocaría una pérdida de rendimiento.

Ventajas switch de copa 3 son:

- Tienen mayor velocidad en las tareas de conmutación de las tramas (envíos de paquetes).
- Tiene una densidad de puertos con los que cuenta el switch.

Y una de las más grandes desventajas es que los switch l3 no funcionan en redes WAN

Switch Capa 2

El switch capa 2 en esta topología se encarga de realizar el proceso de enrutamiento para que ambas Vlan creadas anteriormente puedan comunicarse entre sus semejantes, por ejemplo, la Vlan10 del switchL2-1 pueda comunicarse con la Vlan10 del switchL2-2. Por tanto, este es quien proporciona transferencia directa de datos entre dos dispositivos dentro de la LAN, funcionando así a través de una tabla de direcciones de control de acceso al medio (MAC).

¿Pero cuál es la diferencia entre Switch capa 2 y capa3?

La diferencia principal entre el Switch capa 2 y el Switch Capa 3 radica en la función de enrutamiento, porque el Switch Capa 2 funciona sólo con direcciones MAC y no considera la dirección IP ni ningún elemento de capas superiores, mientras tanto un switch de Capa 3 de igual manera hace las funciones de un Switch Capa 2, pero el Switch Capa 3 a la vez puede ejecutar enrutamiento estático y enrutamiento dinámico. En otras palabras, un switch de Capa 3 dispone de una tabla de direcciones MAC y de una tabla de enrutamiento IP. Adicional a esto, también controla la comunicación intra-VLAN y el enrutamiento de paquetes entre diferentes VLANs.

Ventajas:

- La mayor ventaja que tienes es que el ancho de banda no se divide entre el número de computadoras como sucede con un Hub.
- Agregar mayor ancho de banda.
- Acelerar la salida de tramas.
- Reducir tiempo de espera.

Desventajas:

- Cuando se tiene un gran número de usuarios conectados (computadoras) se tendrá una gran latencia, que es notable y molesta.
- No tiene salida o acceso a internet.
- Funciona sólo con direcciones MAC.

2- Segunda Pregunta

Contestar la siguiente pregunta: ¿Por qué no se utilizan Routers en las nuevas topologías? Tomando en cuenta que en la topología se trabaja con diferentes VLAN's y es necesario enrutar tráfico entre ellas.

Debido a que a que las tecnologías de enrutamiento permiten el acceso a la red a más de un equipo como un router que nos ayudan para gestionar el tráfico de datos que se está procesando en la red, los procesos que realiza tales como mirar cada paquete de datos, leer sus direcciones de origen y destino, encontrar la IP de destino en la tabla de ruteo y luego regresa cada paquete al destino, de manera pueden llegar a saturar la cantidad de procesos que puede llegar a hacer y a la vez afectar de manera drástica al ancho de bando, además otra desventaja de utilizar routers es que los routers al permitir varios equipos también se abren espacios para que los ciberdelincuentes encuentren vulnerabilidades en la red y así poder dañar o intersecar los datos. Dado a esto se tienen a utilizar nuevas tecnologías para enrutar y proteger el acceso a la red.

La implementación de la tecnología de VLAN permite que la red admita se pueda crear varias redes lógicas independientes entre sí, pero siempre dentro de la misma red, distribuyendo mejor la organización de los equipos con esto logrando disminuir las posibilidades de que ocurran violaciones de información confidencial. Además, se reducen costos dado que el ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y más usos eficientes de enlaces y ancho de banda existente.

Otra ventaja de la utilización de VLAN es el mejor rendimiento dado que la división de las redes planas creadas de la capa 2 en múltiples grupos de trabajo reduce el tráfico innecesario en la red y mejora el rendimiento.

Por lo tanto, en estas nuevas topologías para la creación de redes de trabajo no se utilizan routers por el hecho que el Layer 3 Switch es quien está realizando el trabajo de comunicación, soportando todas las características del Switching, mientras que también mantienen algunas funciones de ruteo básicas para rutear entre los VLAN ofreciendo así un mayor rendimiento de red y la segmentación vlan. Es importante conocer de igual manerea que el switch de capa 3 se concibe como una tecnología para mejorar el rendimiento de enrutamiento de red en GRANDES LAN por lo cual hace perfecto a estas nuevas topologías. Por lo último puedo mencionar que la seguridad es mayor comparado a la de router, permitiendo así una mayor seguridad ante cualquier ataque.

Dado a esto, se puede concluir que la utilización de estos Switch es mucho más factible en la mayoría de casos para estas nuevas topologías por las funciones y ventajas que estas ofrecen desde rendimiento, seguridad y hasta un mayor número de puertos para utilizar, por lo cual recomendamos a todos que antes de elegir entre un Switch de capa 3 o un router, es necesarios que comprendan los requisitos o recuersos que el negocio necesita para un mayor rendimiento y funcionamiento.

Bibliografía

T. (2018, febrero). VENTAJAS Y DESVENTAJAS DE LAS VLAN. VENTAJAS Y DESVENTAJAS DE LAS VLAN. https://techandlan.blogspot.com/2018/02/ventajas-y-desventajas-de-las-vlan.html

Systems, T. (2017, 7 diciembre). The Differences Between Routers and Firewalls in Network Security. Taylored Systems | Indianapolis. https://www.taylored.com/blog/the-differences-between-routers-and-firewalls-in-network-security/

Ohlhorst, F. (2014, 11 marzo). Solving the mystery of next-generation firewalls. TechRepublic. https://www.techrepublic.com/article/solving-the-mystery-of-next-generation-firewalls/

Layer 3 Switch Vs Router: What Is Your Best Bet? - FS.COM. (2020, 3 octubre). Blog. https://community.fs.com/blog/layer-3-switch-vs-router-what-is-your-best-bet.html

A. (2017). 7.4.3.1 ¿Por qué utilizar protocolos de estado de enlace? ¿Por qué utilizar protocolos de estado de enlace? https://www.itesa.edu.mx/netacad/switching/course/module7/7.4.3.1/7.4.3.1.html

Anónimo, ActualidadGadget https://www.actualidadgadget.com/tipos-de-firewalls-ventajas-y-desventajas/