Glosario de términos del Switches

Objetivo

Este artículo contiene la lista de términos usada en configurar, configurar, y resolver problemas el Switches de la Pequeña empresa de Cisco.

Dispositivos aplicables

Sx200 Series

Sx250 Series

Sx300 Series

Sx350 Series

Serie SG300X

Sx500 Series

Serie Sx550X

Lista de términos

supplicant del 802.1x — El supplicant es uno de los tres papeles en la norma IEEE del 802.1x. El 802.1x fue desarrollado para proporcionar la Seguridad en la capa 2 del modelo de OSI. Se compone de los componentes siguientes: Supplicant, authenticator, y servidor de autenticación. Un supplicant es el cliente o el software que conectan con una red de modo que pueda acceder los recursos en esa red. Necesita proporcionar las credenciales o los Certificados para obtener una dirección IP y para ser la parte de que red determinada. Un supplicant no puede tener acceso a los recursos de red hasta que se haya autenticado.

ACL — Una lista de control de acceso (ACL) es filtros de tráfico de una lista de redes y acciones correlacionadas usados para mejorar la Seguridad. Bloquea o permite que los usuarios accedan los recursos específicos. Un ACL contiene los host se permiten que o acceso negado al dispositivo de red. El router o el Switch examina cada paquete para determinar si remitir o caer el paquete, en base de los criterios especificados dentro de las Listas de acceso. Los criterios de lista de acceso podían ser la dirección de origen del tráfico, la dirección destino del tráfico, el Upper-Layer Protocol, o la otra información.

IGMP Snooping — El Internet Group Management Protocol (IGMP) es un protocolo que actúa

encendido el Switches que permite que él aprenda dinámicamente sobre el tráfico Multicast. El IGMP Snooping es una característica que permite que un switch de red escuche la conversación IGMP entre los host y el Routers. El IGMP Snooping realiza un mecanismo de filtración que se habilite en el router para remitir el tráfico Multicast de un grupo solamente a los puertos que se ha unido a al grupo. Así con el IGMP Snooping, el tráfico en la red se reduce y la mejora en el funcionamiento de los host detrás del router es posible. Los Multicast se pueden filtrar de los links que no los necesitan.

IPv4 — El IPv4 es un sistema direccional de 32 bits usado para identificar un dispositivo en una red. Es el sistema direccional usado en la mayoría de las redes informáticas, incluyendo Internet.

IPv6 — El IPv6 es un sistema direccional del 128-bit usado para identificar un dispositivo en una red. Es el sucesor al IPv4 y a la mayoría de la versión reciente del sistema direccional usado en las redes informáticas. El IPv6 se está desarrollando actualmente en todo el mundo. Un direccionamiento del IPv6 se representa en ocho campos de los números hexadecimales, cada campo que contiene 16 bits. Un direccionamiento del IPv6 se divide en dos porciones, cada parte integrada por 64 bits. La primera parte que es la dirección de red, y la segunda parte la dirección de host.

Flap del link — El flap del link es una situación en la cual una interfaz física en el Switch entra continuamente hacia arriba y hacia abajo, tres o más mide el tiempo de un segundo para la duración por lo menos de 10 segundos. La causa común se relaciona generalmente con el cable malo, sin apoyo, o no estándar o el pequeño (SFP) enchufable de Form Factor, o relacionado a otro los problemas de sincronización del link. La causa para el link inestable puede ser intermitente o permanente.

ACL MAC basado — Media Access Control (MAC) - la lista de control de acceso (ACL) basada es una lista de MAC Address de origen. Si un paquete está viniendo de un unto de acceso de red inalámbrica a un puerto del red de área local (LAN) o vice versa, este dispositivo marcará si el MAC Address de origen del paquete hace juego cualquier entrada en esta lista y marca las reglas ACL contra el contenido del bastidor. Entonces utiliza los resultados correspondidos con al permit or deny este paquete. Sin embargo, los paquetes del LAN al puerto LAN no serán marcados.

MLD snooping — El Multicast es la técnica de la capa de red que transmite los paquetes de datos a partir de un host a los host seleccionados en un grupo. En la capa inferior, el Switch transmite el tráfico Multicast en todos los puertos, incluso si solamente un host quiere recibirlo. El snooping de la detección del módulo de escucha del Multicast (MLD) se utiliza para remitir el tráfico del Multicast IPv6 solamente a los host deseados. Cuando MLD el snooping se habilita en el Switch, detecta MLD los mensajes intercambiados entre el router del IPv6 y los host del Multicast asociados en la interfaz. Entonces mantiene una tabla que restrinja el tráfico del Multicast IPv6 y adelante lo dinámicamente a esos puertos que quieran recibirlo.

MSTP — El protocolo multiple spanning-tree (MSTP) es un protocolo que crea los árboles de expansión múltiple (casos) para cada Virtual LAN (VLAN) en una sola red física. Esto permite para que cada VLA N tenga una topología configurada del Root Bridge y de la expedición. Esto reduce el número de las Unidades (BPDU) a través de la red y reduce la tensión en las

unidades de procesamiento central (CPU) de los dispositivos de red.

Puerto/Reflejo del VLA N — El Reflejo es un método usado para monitorear el tráfico de la red. Con el puerto o el Reflejo del VLA N, las copias de entrante y los paquetes de salida en los puertos (puertos de origen) de un dispositivo de red se remiten a otro puerto (puerto de destino) donde se estudian los paquetes. Esto es utilizada como herramienta de diagnóstico por el administrador de la red.

Seguridad de puerto — Configurar la Seguridad de puerto es una manera de aumentar la seguridad de la red. Puede ser configurada en un grupo específico de la agregación del puerto o del link (RETRASO). UN RETRASO combina las interfaces individuales en un solo link lógico, que proporciona un ancho de banda total de hasta ocho vículos físicos. Usted puede limitar o permitir el acceso a diversos usuarios en un port/LAG dado. La Seguridad de puerto se puede también utilizar con dinámicamente docto y los Static MAC Address para limitar el Tráfico de ingreso de un puerto.

VLA N basado en protocolos — Los grupos basados en protocolos pueden ser definidos y estar limitados a un puerto; por lo tanto, cada paquete que origina de los grupos de protocolos se asigna al VLAN configurado en la página. El VLA N basado en protocolos divide la red física en los grupos VLAN lógicos para cada protocolo requerido. En el paquete de entrada, se marca la trama y la calidad de miembro de VLAN se puede determinar sobre la base del Tipo de protocolo. Los grupos basados en protocolos a la asignación del VLA N ayudan a asociar a un grupo de protocolos a un puerto único.

QoS — El Calidad de Servicio (QoS) permite que usted dé prioridad al tráfico para diversas aplicaciones, los usuarios o los flujos de datos. Puede también ser utilizado para garantizar el funcionamiento a un nivel especificado, así, afectando a la calidad de servicio del cliente. QoS es afectado generalmente por los factores siguientes: jitter, tiempo de espera, y pérdida del paquete.

Servidor de RADIUS — El Remote Authentication Dial-In User Service (RADIUS) es un mecanismo de autenticación para que los dispositivos conecten y utilicen un servicio de red. Se utiliza para la autenticación centralizada, la autorización, y los fines contables. Un servidor de RADIUS regula el acceso a la red verificando la identidad de los usuarios a través de las credenciales del login ingresadas. Por ejemplo, una red pública del Wi-Fi está instalada en un campus de la universidad. Solamente esos estudiantes que tienen la contraseña pueden acceder estas redes. El servidor de RADIUS marca las contraseñas ingresadas por los usuarios y concede o niega el acceso como apropiado.

RSTP — El protocolo rapid spanning-tree (RSTP) es una mejora del STP. El RSTP proporciona una convergencia del árbol de expansión más rápida después de un cambio de la topología. El STP puede tardar 30 a 50 segundos a responder a un cambio de la topología mientras que el RSTP responde en el plazo de tres veces el tiempo de saludo configurado. El RSTP es al revés compatible con el STP.

SNMP — El Simple Network Management Protocol (SNMP) es un estándar de red para salvar y compartir la información sobre los dispositivos de red. El SNMP facilita la Administración de redes, el troubleshooting, y el mantenimiento.

Spanning-tree — El Spanning Tree Protocol (STP) es un Network Protocol usado en un red de área local (LAN). El propósito del STP es asegurar una topología sin Loops para un LAN. El STP quita los loopes con un algoritmo que garantice que hay solamente un trayecto activo entre dos dispositivos de red. El STP se asegura de que el tráfico tome el trayecto más corto posible dentro de la red. El STP puede también volver a permitir automáticamente los trayectos redundantes como trayectorias de reserva si un trayecto activo falla.

Servidor SSL — Secure Sockets Layer (SSL) es un protocolo usado principalmente para la Administración de seguridad en Internet. Utiliza una capa del programa que esté situada entre el HTTP y las capas TCP. Para la autenticación, el SSL utiliza los Certificados que se firman digitalmente y se limitan a la clave pública para identificar al propietario de la clave privada. Esta autenticación ayuda durante la época de la conexión. Con el uso del SSL, los Certificados se intercambian en los bloques durante el proceso de autenticación que están en el formato descrito en ITU-T X.509 estándar. Entonces por las autoridades de certificación que es una autoridad externa, se publican los Certificados X.509 se firman digitalmente que.

Agregación del Syslog — Un servicio de Syslog valida simplemente los mensajes, y los salva en los archivos o los imprime según un archivo de Configuración simple. La agregación del Syslog significa que varios mensajes de Syslog del mismo tipo no aparecerán en la pantalla cada vez que ocurre un caso. Habilitar la agregación del registro permite que usted filtre los mensajes del sistema que usted recibirá por un período de tiempo específico. Recoge algunos mensajes de Syslog del mismo tipo así que no aparecerán cuando ocurren, pero aparecerían bastante en un intervalo especificado.

TACACS+ — El Terminal Access Controller Access Control System (TACACS+) es un protocolo de propietario de Cisco que es utilizado para la implementación de la seguridad mejorada proporcionando a la autenticación y autorización vía el nombre de usuario y contraseña. Para configurar un servidor TACACS+, el usuario debe tener acceso del privilegio 15, que proporciona el acceso del usuario a todas las características de configuración del Switch. Un poco de Switches puede actuar como cliente TACACS+, donde todos los usuarios conectados pueden ser autenticados y ser autorizados en la red vía un servidor correctamente configurado TACACS+. El TACACS+ soporta solamente el IPv4.

Servidor TFTP — Un servidor del Trivial File Transfer Protocol (TFTP) es un servidor se utiliza que transfiere automáticamente la configuración y inicia los archivos entre los dispositivos en un LAN. El protocolo es simple que permite el uso de memoria baja; sin embargo, esta simplicidad también permite que el protocolo sea comprometido fácilmente. Por este motivo, el TFTP se utiliza raramente con Internet.

VLA N — Una red de área local virtual (VLA N) es una red de switch que es dividida en segmentos lógicamente por la función, el área, o la aplicación, sin consideración alguna hacia las ubicaciones físicas de los usuarios. Los VLA N son un grupo de host o los puertos que pueden ser situados dondequiera en una red sino comunicar como si estén en el mismo segmento físico. Los VLA N ayudan a simplificar la Administración de redes dejándole mover un dispositivo a un nuevo VLA N sin el cambio de ningunas conexiones físicas.