Glosario de términos de los switches

Objetivo

Este artículo contiene la lista de términos utilizados en la configuración, configuración y resolución de problemas de los switches Cisco Small Business.

Dispositivos aplicables

Serie Sx200

Serie Sx250

Serie Sx300

Serie Sx350

Serie SG300X

Serie Sx500

Serie Sx550X

Lista de términos

Suplicante 802.1X: Suplicante es una de las tres funciones del estándar IEEE 802.1X. 802.1X se desarrolló para proporcionar seguridad en la capa 2 del modelo OSI. Está compuesto por los siguientes componentes: Suplicante, Autenticador y Servidor de autenticación. Un Suplicante es el cliente o software que se conecta a una red para que pueda acceder a los recursos de esa red. Necesita proporcionar credenciales o certificados para obtener una dirección IP y formar parte de esa red en particular. Un suplicante no puede tener acceso a los recursos de la red hasta que se haya autenticado.

ACL: una lista de control de acceso (ACL) es una lista de filtros de tráfico de red y acciones correlacionadas que se utilizan para mejorar la seguridad. Bloquea o permite a los usuarios acceder a recursos específicos. Una ACL contiene los hosts a los que se les permite o deniega el acceso al dispositivo de red. El router o switch examina cada paquete para determinar si reenvía o descarta el paquete, en base a los criterios especificados en las listas de acceso. Los criterios de la lista de acceso pueden ser la dirección de origen del tráfico, la dirección de destino del tráfico, el protocolo de capa superior u otra información.

Detección de IGMP: el protocolo de administración de grupos de Internet (IGMP) es un

protocolo que funciona en switches que les permite aprender dinámicamente sobre el tráfico de multidifusión. La indagación IGMP es una función que permite que un switch de red escuche la conversación IGMP entre hosts y routers. La indagación IGMP realiza un mecanismo de filtrado que está habilitado en el router para reenviar el tráfico multicast de un grupo solamente a los puertos que se han unido al grupo. Por lo tanto, con la indagación IGMP, se reduce el tráfico en la red y es posible mejorar el rendimiento de los hosts detrás del router. Las multidifusiones pueden filtrarse desde los links que no las necesitan.

IPv4: IPv4 es un sistema de direcciones de 32 bits utilizado para identificar un dispositivo en una red. Es el sistema de direcciones que se utiliza en la mayoría de las redes informáticas, incluida Internet.

IPv6: IPv6 es un sistema de direcciones de 128 bits que se utiliza para identificar un dispositivo en una red. Es el sucesor de IPv4 y la versión más reciente del sistema de direccionamiento utilizado en las redes informáticas. IPv6 se está implementando actualmente en todo el mundo. Una dirección IPv6 se representa en ocho campos de números hexadecimales, cada campo contiene 16 bits. Una dirección IPv6 se divide en dos partes, cada una compuesta por 64 bits. La primera parte es la dirección de red y la segunda, la dirección de host.

Link Flap: La inestabilidad de link es una situación en la que una interfaz física en el switch sube y baja continuamente, tres o más veces por segundo durante al menos 10 segundos. La causa más común suele estar relacionada con un cable o Small Form-Factor Pluggable (SFP) incorrecto, no compatible o no estándar, o con otros problemas de sincronización de enlaces. La causa del aleteo del link puede ser intermitente o permanente.

ACL basada en MAC: la lista de control de acceso (ACL) basada en el control de acceso a los medios (MAC) es una lista de direcciones MAC de origen. Si un paquete proviene de un punto de acceso inalámbrico a un puerto de red de área local (LAN) o viceversa, este dispositivo comprobará si la dirección MAC de origen del paquete coincide con alguna entrada de esta lista y compara las reglas ACL con el contenido de la trama. Luego utiliza los resultados coincidentes para permitir o denegar este paquete. Sin embargo, no se comprobarán los paquetes del puerto LAN al puerto LAN.

Snooping de MLD: la multidifusión es la técnica de capa de red que transmite paquetes de datos desde un host a los hosts seleccionados de un grupo. En la capa inferior, el switch difunde el tráfico multicast en todos los puertos, incluso si sólo un host desea recibirlo. La detección de escucha de multidifusión (MLD) se utiliza para reenviar el tráfico de multidifusión IPv6 sólo a los hosts deseados. Cuando la indagación MLD está habilitada en el switch, detecta los mensajes MLD intercambiados entre el router IPv6 y los hosts multicast conectados en la interfaz. A continuación, mantiene una tabla que restringe el tráfico de multidifusión IPv6 y lo reenvía dinámicamente a los puertos que deseen recibirlo.

MSTP: el protocolo de árbol de extensión múltiple (MSTP) es un protocolo que crea varios árboles de extensión (instancias) para cada LAN virtual (VLAN) en una única red física. Esto permite que cada VLAN tenga una topología de reenvío y un puente raíz configurados. Esto reduce el número de unidades de datos de protocolo de puente (BPDU) en la red y el estrés en las unidades de procesamiento central (CPU) de los dispositivos de red.

Duplicación de puertos/VLAN: la duplicación es un método utilizado para supervisar el tráfico de red. Con la duplicación de puertos o VLAN, las copias de los paquetes entrantes y salientes en los puertos (puertos de origen) de un dispositivo de red se reenvían a otro puerto (puerto de destino) donde se estudian los paquetes. El administrador de la red utiliza esta herramienta de diagnóstico.

Seguridad de puertos: configurar la seguridad de los puertos es una forma de mejorar la seguridad de la red. Se puede configurar en un puerto específico o en un grupo de agregación de enlaces (LAG). Un LAG combina interfaces individuales en un único link lógico, que proporciona un ancho de banda agregado de hasta ocho links físicos. Puede limitar o permitir el acceso a diferentes usuarios en un puerto/LAG determinado. Port Security también se puede utilizar con direcciones MAC estáticas y aprendidas dinámicamente para limitar el tráfico de entrada de un puerto.

VLAN basada en protocolo: los grupos basados en protocolo se pueden definir y enlazar a un puerto; por lo tanto, cada paquete que se origina de los grupos de protocolo se asigna a la VLAN configurada en la página. La VLAN basada en protocolo divide la red física en grupos de VLAN lógicas para cada protocolo requerido. En el paquete entrante, la trama se verifica y la pertenencia a VLAN se puede determinar en función del tipo de protocolo. La asignación de grupos basados en protocolo a VLAN ayuda a asignar un grupo de protocolo a un solo puerto.

QoS: la calidad de servicio (QoS) permite dar prioridad al tráfico de las diferentes aplicaciones, usuarios o flujos de datos. También se puede utilizar para garantizar el rendimiento a un nivel especificado, lo que afecta a la calidad del servicio del cliente. QoS se ve generalmente afectada por los siguientes factores: fluctuación, latencia y pérdida de paquetes.

Servidor RADIUS: el servicio de usuario de acceso telefónico de autenticación remota (RADIUS) es un mecanismo de autenticación para que los dispositivos se conecten y utilicen un servicio de red. Se utiliza con fines de autenticación, autorización y contabilidad centralizados. Un servidor RADIUS regula el acceso a la red mediante la verificación de la identidad de los usuarios a través de las credenciales de inicio de sesión introducidas. Por ejemplo, una red Wi-Fi pública se instala en un campus universitario. Sólo los alumnos que tengan la contraseña pueden acceder a estas redes. El servidor RADIUS comprueba las contraseñas introducidas por los usuarios y concede o deniega el acceso según corresponda.

RSTP: el protocolo de árbol de extensión rápido (RSTP) es una mejora del STP. RSTP proporciona una convergencia de árbol de expansión más rápida después de un cambio de topología. El STP puede tardar de 30 a 50 segundos en responder a un cambio de topología, mientras que el RSTP responde dentro de tres veces el tiempo de saludo configurado. RSTP es compatible con las versiones anteriores de STP.

SNMP: el protocolo simple de administración de red (SNMP) es un estándar de red para almacenar y compartir información sobre los dispositivos de red. SNMP facilita la administración, la resolución de problemas y el mantenimiento de la red.

Spanning Tree: el protocolo de árbol de extensión (STP) es un protocolo de red utilizado en

una red de área local (LAN). El propósito de STP es asegurar una topología sin loops para una LAN. El STP elimina los loops a través de un algoritmo que garantiza que sólo hay una trayectoria activa entre dos dispositivos de red. STP garantiza que el tráfico tome el trayecto más corto posible dentro de la red. STP también puede volver a habilitar automáticamente las trayectorias redundantes como trayectorias de respaldo si falla una trayectoria activa.

Servidor SSL: Secure Sockets Layer (SSL) es un protocolo que se utiliza principalmente para la gestión de la seguridad en Internet. Utiliza una capa de programa que se encuentra entre las capas HTTP y TCP. Para la autenticación, SSL utiliza certificados firmados digitalmente y enlazados a la clave pública para identificar al propietario de la clave privada. Esta autenticación ayuda durante el tiempo de conexión. Mediante el uso de SSL, los certificados se intercambian en bloques durante el proceso de autenticación que están en el formato descrito en el estándar ITU-T X.509. A continuación, la entidad emisora de certificados, que es una entidad externa, emite certificados X.509 firmados digitalmente.

Agregación de Syslog: un servicio de Syslog simplemente acepta mensajes y los almacena en archivos o los imprime de acuerdo con un archivo de configuración simple. La agregación de Syslog significa que varios mensajes de syslog del mismo tipo no aparecerán en la pantalla cada vez que se produzca una instancia. La activación de la agregación de registros permite filtrar los mensajes del sistema que recibirá durante un período de tiempo específico. Recopila algunos mensajes de syslog del mismo tipo para que no aparezcan cuando ocurran, sino en un intervalo especificado.

TACACS+: Terminal Access Controller Access Control System (TACACS+) es un protocolo propiedad de Cisco que se utiliza para la implementación de seguridad mejorada al proporcionar autenticación y autorización mediante nombre de usuario y contraseña. Para configurar un servidor TACACS+, el usuario debe tener acceso con el privilegio 15, que proporciona al usuario acceso a todas las funciones de configuración del switch. Algunos switches pueden actuar como un cliente TACACS+, donde todos los usuarios conectados se pueden autenticar y autorizar en la red a través de un servidor TACACS+ configurado correctamente. TACACS+ solo admite IPv4.

Servidor TFTP: un servidor de protocolo de transferencia de archivos trivial (TFTP) es un servidor que se utiliza para transferir automáticamente archivos de configuración e inicio entre dispositivos en una LAN. El protocolo es simple, lo que permite un bajo uso de memoria; sin embargo, esta simplicidad también permite que el protocolo se vea fácilmente comprometido. Por esta razón, el TFTP rara vez se utiliza con Internet.

VLAN: una red de área local virtual (VLAN) es una red conmutada segmentada de forma lógica por función, área o aplicación, independientemente de las ubicaciones físicas de los usuarios. Las VLAN son un grupo de hosts o puertos que se pueden ubicar en cualquier lugar de una red pero se comunican como si estuvieran en el mismo segmento físico. Las VLAN ayudan a simplificar la administración de la red al permitirle mover un dispositivo a una nueva VLAN sin cambiar ninguna conexión física.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).