Scambia il glossario dei termini

Obiettivo

In questo articolo vengono elencati i termini utilizzati per l'impostazione, la configurazione e la risoluzione dei problemi degli switch Cisco Small Business.

Dispositivi interessati

Serie Sx200

Serie Sx250

Serie Sx300

Serie Sx350

Serie SG300X

Serie Sx500

Serie Sx550X

Elenco di termini

Supplicant 802.1X: uno dei tre ruoli dello standard 802.1X IEEE. Lo standard 802.1X è stato sviluppato per garantire la sicurezza nel layer 2 del modello OSI. È composto dai componenti Supplicant, Authenticator e Authentication Server. Un supplicant è il client o il software che si connette a una rete in modo che possa accedere alle risorse in tale rete. Deve fornire credenziali o certificati per ottenere un indirizzo IP e far parte di tale rete. Un richiedente non può accedere alle risorse della rete finché non è stato autenticato.

ACL: un elenco di controllo di accesso (ACL, Access Control List) è un elenco di filtri del traffico di rete e di azioni correlate utilizzate per migliorare la sicurezza. Blocca o consente agli utenti di accedere a risorse specifiche. Un ACL contiene gli host a cui è consentito o negato l'accesso al dispositivo di rete. Il router o lo switch esamina ciascun pacchetto per stabilire se inoltrarlo o eliminarlo, in base ai criteri specificati negli elenchi degli accessi. I criteri dell'elenco degli accessi possono essere l'indirizzo di origine del traffico, l'indirizzo di destinazione del traffico, il protocollo di livello superiore o altre informazioni.

Snooping IGMP: il protocollo IGMP (Internet Group Management Protocol) funziona sugli switch e consente loro di apprendere dinamicamente il traffico multicast. Lo snooping IGMP è

una funzione che consente a uno switch di rete di ascoltare la conversazione IGMP tra host e router. Lo snooping IGMP esegue un meccanismo di filtro abilitato nel router per inoltrare il traffico multicast di un gruppo solo alle porte che sono state unite al gruppo. Pertanto, con lo snooping IGMP, il traffico sulla rete viene ridotto ed è possibile migliorare le prestazioni degli host dietro il router. I multicast possono essere filtrati dai link che non ne hanno bisogno.

IPv4: IPv4 è un sistema di indirizzamento a 32 bit utilizzato per identificare un dispositivo in una rete. È il sistema di indirizzamento utilizzato nella maggior parte delle reti di computer, incluso Internet.

IPv6 — IPv6 è un sistema di indirizzamento a 128 bit utilizzato per identificare un dispositivo in una rete. È il successore dell'IPv4 e della versione più recente del sistema di indirizzamento utilizzato nelle reti di computer. IPv6 è attualmente in fase di implementazione in tutto il mondo. Un indirizzo IPv6 è rappresentato in otto campi di numeri esadecimali, ognuno contenente 16 bit. Un indirizzo IPv6 è diviso in due parti, ognuna composta da 64 bit. La prima parte è l'indirizzo di rete, la seconda l'indirizzo host.

Link Flap: il link flap è una situazione in cui un'interfaccia fisica sullo switch continua a salire e scendere, tre o più volte al secondo per una durata di almeno 10 secondi. La causa comune è in genere correlata a un cavo non valido, non supportato o non standard, a un SFP (Small Form-Factor Pluggable) o ad altri problemi di sincronizzazione del collegamento. Il link flapping può essere intermittente o permanente.

ACL basato su MAC: l'elenco dei controlli di accesso (ACL) basato su MAC (Media Access Control) è un elenco di indirizzi MAC di origine. Se un pacchetto proviene da un punto di accesso wireless a una porta LAN (Local Area Network) o viceversa, il dispositivo controllerà se l'indirizzo MAC di origine del pacchetto corrisponde a una voce dell'elenco e controllerà le regole ACL in base al contenuto del frame. Utilizza quindi i risultati corrispondenti per autorizzare o negare il pacchetto. Tuttavia, i pacchetti da una porta LAN a una porta LAN non verranno controllati.

MLD Snooping: la tecnica multicast è il livello di rete che trasmette i pacchetti di dati da un host agli host selezionati di un gruppo. Al livello più basso, lo switch trasmette il traffico multicast su tutte le porte, anche se solo un host desidera riceverlo. Lo snooping MLD (Multicast Listener Discovery) viene utilizzato per inoltrare il traffico multicast IPv6 solo agli host desiderati. Quando lo snooping MLD è abilitato sullo switch, rileva i messaggi MLD scambiati tra il router IPv6 e gli host multicast collegati all'interfaccia. Mantiene quindi una tabella che limita il traffico multicast IPv6 e lo inoltra dinamicamente alle porte che lo desiderano ricevere.

MSTP — Multiple Spanning Tree Protocol (MSTP) è un protocollo che crea più spanning tree (istanze) per ciascuna VLAN virtuale (VLAN) su una singola rete fisica. In questo modo, ciascuna VLAN può avere un bridge radice configurato e una topologia di inoltro. In questo modo si riduce il numero di BDPU (Bridge Protocol Data Unit) sulla rete e lo stress sulle CPU (Central Processing Unit) dei dispositivi di rete.

Mirroring della porta/VLAN: il mirroring è un metodo utilizzato per monitorare il traffico di rete. Con il mirroring della porta o della VLAN, le copie dei pacchetti in entrata e in uscita sulle

porte (porte di origine) di un dispositivo di rete vengono inoltrate a un'altra porta (porta di destinazione) dove i pacchetti vengono analizzati. Viene utilizzato come strumento di diagnostica dall'amministratore di rete.

Sicurezza porta: la configurazione della sicurezza della porta è uno dei modi per migliorare la sicurezza della rete. Può essere configurato su una porta specifica o su un gruppo LAG (Link Aggregation Group). Un LAG combina singole interfacce in un unico collegamento logico, che fornisce una larghezza di banda aggregata fino a otto collegamenti fisici. È possibile limitare o consentire l'accesso a utenti diversi su una determinata porta o su un determinato LAG. La funzione di sicurezza delle porte può essere utilizzata anche con indirizzi MAC statici e appresi in modo dinamico per limitare il traffico in entrata su una porta.

VLAN basata sul protocollo: è possibile definire i gruppi basati sul protocollo e collegarli a una porta. Di conseguenza, ogni pacchetto proveniente dai gruppi del protocollo viene assegnato alla VLAN configurata nella pagina. La VLAN basata sul protocollo suddivide la rete fisica in gruppi di VLAN logici per ciascun protocollo richiesto. Nel pacchetto in entrata, il frame viene controllato e l'appartenenza della VLAN può essere determinata in base al tipo di protocollo. Il mapping dei gruppi basati sul protocollo alla VLAN consente di mappare un gruppo di protocolli a una singola porta.

QoS: Quality of Service (QoS) consente di assegnare priorità al traffico per diverse applicazioni, utenti o flussi di dati. e può essere utilizzato anche per garantire prestazioni fino a un determinato livello, con conseguente impatto sulla qualità del servizio del cliente. QoS è generalmente influenzato dai seguenti fattori: jitter, latenza e perdita di pacchetti.

Server RADIUS - RADIUS (Remote Authentication Dial-In User Service) è un meccanismo di autenticazione che consente ai dispositivi di connettersi e utilizzare un servizio di rete. Viene utilizzato per l'autenticazione, l'autorizzazione e la contabilità centralizzate. Un server RADIUS regola l'accesso alla rete verificando l'identità degli utenti tramite le credenziali di accesso immesse. Ad esempio, una rete Wi-Fi pubblica è installata in un campus universitario. Solo gli studenti che dispongono della password possono accedere a queste reti. Il server RADIUS controlla le password immesse dagli utenti e concede o nega l'accesso in base alle esigenze.

RSTP — Rapid Spanning Tree Protocol (RSTP) è un miglioramento di STP. RSTP garantisce una convergenza Spanning Tree più rapida dopo una modifica della topologia. Il processo STP può impiegare da 30 a 50 secondi per rispondere a una modifica della topologia, mentre il processo RSTP risponde entro tre volte il tempo di benvenuto configurato. RSTP è compatibile con STP.

SNMP — Simple Network Management Protocol (SNMP) è uno standard di rete per l'archiviazione e la condivisione di informazioni sui dispositivi di rete. L'SNMP semplifica la gestione, la risoluzione dei problemi e la manutenzione della rete.

Spanning Tree Protocol - Spanning Tree Protocol (STP) è un protocollo di rete utilizzato su una LAN (Local Area Network). Lo scopo di STP è garantire una topologia senza loop per una LAN. L'algoritmo STP rimuove i loop attraverso un algoritmo che garantisce la presenza di un solo percorso attivo tra due dispositivi di rete. Il protocollo STP assicura che il traffico utilizzi il percorso più breve possibile all'interno della rete. STP può inoltre riattivare automaticamente i

percorsi ridondanti come percorsi di backup in caso di errore di un percorso attivo.

Server SSL: il protocollo SSL (Secure Sockets Layer) è utilizzato principalmente per la gestione della sicurezza su Internet. Utilizza un livello di programma situato tra i livelli HTTP e TCP. Per l'autenticazione, SSL utilizza certificati con firma digitale e associati alla chiave pubblica per identificare il proprietario della chiave privata. Questa autenticazione consente di controllare l'operatività durante la connessione. Tramite SSL, i certificati sono scambiati in blocchi durante il processo di autenticazione nel formato descritto nello standard ITU-T X.509. Quindi dall'autorità di certificazione che è un'autorità esterna, vengono rilasciati i certificati X.509 con firma digitale.

Aggregazione syslog: un servizio syslog accetta semplicemente i messaggi e li archivia in file o li stampa in base a un semplice file di configurazione. Aggregazione syslog significa che diversi messaggi syslog dello stesso tipo non verranno visualizzati sullo schermo ogni volta che si verifica un'istanza. L'attivazione dell'aggregazione della registrazione consente di filtrare i messaggi di sistema che verranno ricevuti per un periodo di tempo specifico. Raccoglie alcuni messaggi syslog dello stesso tipo, in modo che non vengano visualizzati quando si verificano, ma vengano visualizzati a intervalli specifici.

TACACS+ — Terminal Access Controller Access Control System (TACACS+) è un protocollo proprietario di Cisco utilizzato per implementare una sicurezza migliorata tramite autenticazione e autorizzazione tramite nome utente e password. Per configurare un server TACACS+, l'utente deve disporre del privilegio di accesso 15, che gli consente di accedere a tutte le funzionalità di configurazione dello switch. Alcuni switch possono funzionare come client TACACS+, in cui tutti gli utenti connessi possono essere autenticati e autorizzati nella rete tramite un server TACACS+ configurato correttamente. TACACS+ supporta solo IPv4.

Server TFTP: un server TFTP (Trivial File Transfer Protocol) è un server utilizzato per trasferire automaticamente i file di configurazione e di avvio tra i dispositivi di una rete LAN. Il protocollo è semplice e consente un utilizzo di memoria ridotto; tuttavia, questa semplicità consente anche di compromettere il protocollo. Per questo motivo, il TFTP viene raramente utilizzato con Internet.

VLAN: una VLAN (Virtual Local Area Network) è una rete commutata segmentata logicamente in base alla funzione, all'area o all'applicazione, indipendentemente dalla posizione fisica degli utenti. Le VLAN sono un gruppo di host o porte che possono essere collocate in qualsiasi punto della rete ma che comunicano come se si trovassero sullo stesso segmento fisico. Le VLAN semplificano la gestione della rete consentendo di spostare un dispositivo su una nuova VLAN senza modificare le connessioni fisiche.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).