Switches Lijst van termen

Doel

Dit artikel bevat de lijst met termen die worden gebruikt bij het instellen, configureren en oplossen van problemen van Cisco Small Business-Switches.

Toepasselijke apparaten

SX200 Series

SX250 Series

Sx300 Series

Sx350 Series

SG300X Series

Sx500 Series

Sx550X Series

Lijst van voorwaarden

802.1X Supplicant — Supplicant is een van de drie rollen in de 802.1X IEEE Standard. De 802.1X is ontwikkeld om beveiliging te bieden in Layer 2 van het OSI-model. Het bestaat uit de volgende componenten: Supplicant, Authenticator, en de Server van de Verificatie. Een Supplicant is de client of software die verbinding maakt met een netwerk, zodat deze toegang heeft tot bronnen op dat netwerk. Het moet referenties of certificaten verstrekken om een IP-adres te verkrijgen en deel uit te maken van dat specifieke netwerk. Een verzoeker kan geen toegang tot de middelen van het netwerk hebben tot het is voor authentiek verklaard.

ACL — Een toegangscontrolelijst (ACL) is een lijst van netwerkverkeersfilters en gecorreleerde acties die worden gebruikt om de beveiliging te verbeteren. Het blokkeert of verleent gebruikers om tot specifieke middelen toegang te hebben. Een ACL bevat de hosts die zijn toegestaan of geweigerd toegang tot het netwerkapparaat. De router of switch onderzoekt elk pakket om te bepalen of om het pakket door:sturen of te laten vallen, op basis van de gespecificeerde criteria binnen de toegangslijsten. De criteria van de toegangslijst zouden het bronadres van het verkeer, het bestemmingsadres van het verkeer, het bovenlaagprotocol, of andere informatie kunnen zijn.

IGMP-controle — Internet Group Management Protocol (IGMP) is een protocol dat werkt op switches waarmee zij dynamisch informatie kunnen verkrijgen over multicast-verkeer. IGMP-spionage is een functie waarmee een switch van het netwerk kan luisteren naar het IGMP-gesprek tussen hosts en routers. IGMP-spionage voert een filtermechanisme uit dat in de router is ingeschakeld om het multicastverkeer van een groep alleen te doorsturen naar de poorten die tot de groep zijn toegetreden. Zodoende wordt met IGMP-spionage het verkeer op het netwerk beperkt en is verbetering van de prestaties van hosts achter de router mogelijk. Multicast kan worden gefilterd uit koppelingen die deze niet nodig hebben.

IPv4 — IPv4 is een 32-bits adresseringssysteem dat wordt gebruikt om een apparaat in een netwerk te identificeren. Het is het adresseringssysteem dat in de meeste computernetwerken wordt gebruikt, inclusief het internet.

IPv6 — IPv6 is een 128-bits adresseringssysteem dat wordt gebruikt om een apparaat in een netwerk te identificeren. Het is de opvolger van IPv4 en de meest recente versie van het adresseringssysteem dat in computernetwerken wordt gebruikt. IPv6 wordt momenteel wereldwijd geïmplementeerd. Een IPv6-adres wordt weergegeven in acht velden met hexadecimale getallen, elk veld bevat 16 bits. Een IPv6-adres wordt in twee delen verdeeld, elk deel bestaat uit 64 bits. Het eerste deel is het netwerkadres en het tweede deel het hostadres.

Link Flap — Link flap is een situatie waarin een fysische interface op de switch continu op en neer gaat, drie of meer keer per seconde voor een periode van ten minste 10 seconden. De veel voorkomende oorzaak is meestal gerelateerd aan slechte, niet-ondersteunde of niet-standaard kabel of Small Form-Factor Pluggable (SFP), of aan andere problemen met linksynchronisatie. De oorzaak van het flappen van de link kan intermitterend of permanent zijn.

Op MAC gebaseerde ACL — op Media Access Control (MAC) gebaseerde toegangscontrolelijst (ACL) is een lijst met MAC-adressen van bronnen. Als een pakket van een draadloos access point naar een Local Area Network (LAN) poort komt of omgekeerd, controleert dit apparaat of het MAC-adres van de bron van het pakket overeenkomt met elk item in deze lijst en controleert het de ACL-regels op de inhoud van het frame. Het gebruikt dan de aangepaste resultaten om dit pakket toe te staan of te ontkennen. Pakketten van LAN naar LAN poort worden echter niet geselecteerd.

MLD Snooping — Multicast is de techniek van de netwerklaag die gegevenspakketten van één host naar de geselecteerde hosts in een groep verzendt. Op de onderste laag zendt de switch het multicastverkeer uit op alle poorten, zelfs als slechts één host het wil ontvangen. Multicast Listener Discovery (MLD) Snooping wordt gebruikt om IPv6-multicast verkeer alleen naar de gewenste host(s) te doorsturen. Wanneer MLD-snuffelen is ingeschakeld op de switch, worden de MLD-berichten gedetecteerd die worden uitgewisseld tussen de IPv6-router en de multicast-hosts die op de interface zijn aangesloten. Vervolgens wordt een tabel bijgehouden die IPv6 multicast-verkeer beperkt en dynamisch doorstuurt naar de poorten die het willen ontvangen.

MSTP — Multiple Spanning Tree Protocol (MSTP) is een protocol dat meerdere omspanningsbomen (instanties) maakt voor elke virtuele LAN (VLAN) op één fysiek netwerk. Dit staat voor elk VLAN toe om een gevormde root-brug te hebben en topologie door:sturen.

Dit vermindert het aantal Bridge Protocol Data Units (BPDU's) over het netwerk en vermindert de druk op de Central Processing Units (CPU's) van de netwerkapparaten.

Port/VLAN-mirroring — Spiegelen is een methode die wordt gebruikt om netwerkverkeer te bewaken. Met Port of VLAN Mirroring worden kopieën van inkomende en uitgaande pakketten via de poorten (bronpoorten) van een netwerkapparaat doorgestuurd naar een andere poort (doelpoort) waar de pakketten worden bestudeerd. Dit wordt door de netwerkbeheerder gebruikt als een diagnostisch gereedschap.

Poortbeveiliging — Het configureren van poortbeveiliging is een manier om de netwerkbeveiliging te verbeteren. Het kan op een specifieke poort of Link Aggregation Group (LAG) worden geconfigureerd. Een LAG combineert individuele interfaces in één enkele logische verbinding, die een gezamenlijke bandbreedte van zelfs acht fysieke verbindingen verstrekt. U kunt de toegang tot verschillende gebruikers op een bepaalde poort/LAG beperken of toestaan. Poortbeveiliging kan ook worden gebruikt met dynamisch aangeleerde en statische MAC-adressen om het toegangsverkeer van een poort te beperken.

Op protocol gebaseerde VLAN — Op protocol gebaseerde groepen kunnen worden gedefinieerd en aan een poort worden gebonden. Daarom wordt elk pakket dat afkomstig is uit de protocolgroepen toegewezen aan het geconfigureerde VLAN op de pagina. Op protocollen gebaseerde VLAN verdeelt het fysieke netwerk in logische VLAN-groepen voor elk vereist protocol. In het inkomende pakket, wordt het kader gecontroleerd en het lidmaatschap van VLAN kan worden bepaald gebaseerd op het protocoltype. De protocolgebaseerde groepen op VLAN-toewijzing helpt een protocolgroep aan één poort in kaart te brengen.

QoS — Quality of Service (QoS) stelt u in staat prioriteit te geven aan verkeer voor verschillende toepassingen, gebruikers of gegevensstromen. Het kan ook worden gebruikt om de prestaties op een bepaald niveau te waarborgen, waardoor de kwaliteit van de dienstverlening van de klant wordt beïnvloed. QoS wordt over het algemeen beïnvloed door de volgende factoren: jitter, latency en pakketverlies.

RADIUS Server — Remote Authentication Dial-In User Service (RADIUS) is een verificatiemechanisme voor apparaten om verbinding te maken met en gebruik te maken van een netwerkservice. Het wordt gebruikt voor gecentraliseerde authentificatie, vergunning, en boekhoudingsdoeleinden. Een RADIUS-server regelt de toegang tot het netwerk door de identiteit van de gebruikers te verifiëren aan de hand van de ingevoerde aanmeldingsgegevens. Op een universiteitscampus is bijvoorbeeld een openbaar Wi-Fi-netwerk geïnstalleerd. Alleen studenten met een wachtwoord hebben toegang tot deze netwerken. De RADIUS-server controleert de wachtwoorden die door de gebruikers zijn ingevoerd en verleent of ontkent, naargelang het geval, toegang.

RSTP — Rapid Spanning Tree Protocol (RSTP) is een uitbreiding van STP. RSTP biedt een snellere overspannende boomconvergentie na een topologiewijziging. STP kan 30 tot 50 seconden vergen om aan een topologieverandering te antwoorden terwijl RSTP binnen drie keer de gevormde hello tijd antwoordt. RSTP is achterwaarts compatibel met STP.

SNMP — Simple Network Management Protocol (SNMP) is een netwerkstandaard voor het opslaan en delen van informatie over netwerkapparaten. SNMP vergemakkelijkt

netwerkbeheer, probleemoplossing en onderhoud.

Spanning Tree — Spanning Tree Protocol (STP) is een netwerkprotocol dat wordt gebruikt op een Local Area Network (LAN). Het doel van STP is een lusvrije topologie voor LAN te verzekeren. STP verwijdert lijnen door een algoritme dat garandeert dat er slechts één actief pad is tussen twee netwerkapparaten. STP zorgt ervoor dat het verkeer binnen het netwerk het kortst mogelijke pad neemt. STP kan ook automatisch redundante paden opnieuw inschakelen als back-uppaden als een actief pad mislukt.

SSL Server — The Secure Sockets Layer (SSL) is een protocol dat voornamelijk wordt gebruikt voor beveiligingsbeheer op internet. Het maakt gebruik van een programmalaag die zich tussen de HTTP- en TCP-lagen bevindt. Voor authenticatie gebruikt SSL certificaten die digitaal zijn ondertekend en begrensd aan de openbare sleutel om de private sleuteleigenaar te identificeren. Deze verificatie helpt tijdens de verbinding. Door het gebruik van SSL worden de certificaten tijdens het authenticatieproces in blokken uitgewisseld in het formaat dat wordt beschreven in ITU-T-norm X.509. Vervolgens worden door de certificeringsinstantie, die een externe instantie is, X.509-certificaten afgegeven die digitaal worden ondertekend.

Syslog Aggregation — Een Syslog-service accepteert alleen berichten en slaat ze op in bestanden of drukt ze af volgens een eenvoudig configuratiebestand. Syslog Aggregation betekent dat meerdere syslog berichten van hetzelfde type niet op het scherm zullen verschijnen telkens als er een instantie optreedt. Door logaggregatie in te schakelen kunt u de systeemberichten filteren die u voor een bepaalde periode ontvangt. Het verzamelt een paar syslog berichten van hetzelfde type zodat ze niet zullen verschijnen wanneer ze voorkomen, maar liever op een bepaald interval verschijnen.

TACACS+ — Terminal Access Controller Access Control System (TACACS+) is een merkgebonden Cisco-protocol dat wordt gebruikt voor de implementatie van verbeterde beveiliging door verificatie en autorisatie via gebruikersnaam en wachtwoord te bieden. Om een TACACS+ server te kunnen configureren moet de gebruiker de bevoegdheid 15 hebben, wat de gebruiker toegang biedt tot alle configuratiefuncties van de switch. Sommige switches kunnen fungeren als een TACACS+ client, waar alle aangesloten gebruikers kunnen worden geverifieerd en geautoriseerd in het netwerk via een correct geconfigureerde TACACS+ server. TACACS+ ondersteunt alleen IPv4.

TFTP Server — Een Trivial File Transfer Protocol (TFTP) Server is een server die wordt gebruikt om automatisch configuratie- en opstartbestanden over te dragen tussen apparaten op een LAN. Het protocol is eenvoudig, waardoor weinig geheugen gebruikt kan worden, maar deze eenvoud zorgt er ook voor dat het protocol gemakkelijk gecompromitteerd kan worden. Om deze reden, wordt TFTP zelden gebruikt met Internet.

VLAN — Een Virtual Local Area Network (VLAN) is een switched netwerk dat logisch gesegmenteerd is per functie, gebied of toepassing, zonder rekening te houden met de fysieke locaties van de gebruikers. VLAN’s zijn een groep hosts of poorten die overal in een netwerk kunnen worden gevestigd, maar communiceren alsof ze op hetzelfde fysieke segment liggen. VLAN’s helpen het netwerkbeheer te vereenvoudigen door u een apparaat naar een nieuw VLAN te laten verplaatsen zonder fysieke verbindingen te wijzigen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.