اصطلاحات فنی و کاربردی سوئیچ های شبکه

31 فروردین 1404

سرور لینوکس

آشنایی با اصطلاحات فنی و کاربردی سوئیچ های شبکه برای هر فردی که در زمینه فناوری اطلاعات، مدیریت سرورها یا حتی توسعه وب فعالیت می‌کند، یک ضرورت به‌حساب می‌آید.
سوئیچ‌ها به‌عنوان یکی از اصلی‌ترین تجهیزات در زیرساخت شبکه، نقش مهمی در انتقال داده ها، تقسیم‌بندی شبکه و بهینه‌سازی ترافیک ایفا می‌کنند.
درک مفاهیمی مانند Switching Capacity، Full Duplex، PoE، VLAN و MAC Address Table به ما این امکان را می‌دهد تا درک عمیق‌تری از نحوه عملکرد شبکه ها داشته باشیم و هنگام کانفیگ سوئیچ یا رفع مشکل، سریع‌تر و دقیق‌تر عمل کنیم.

از طرف دیگر، در دنیای سئو و توسعه وب‌سایت، اگرچه سوئیچ‌های شبکه به طور مستقیم دیده نمی‌شوند، اما تاثیر غیرمستقیم آن‌ها بر سرعت، پایداری و امنیت ارتباطات بین سرورها و کاربران نهایی کاملا محسوس است.
به‌عنوان مثال، یک تنظیم اشتباه در سوئیچ می‌تواند باعث ایجاد تاخیر در پاسخ دهی سایت یا حتی قطعی موقت شود که مستقیما بر تجربه کاربری و رتبه‌بندی موتورهای جست‌وجو اثر منفی می‌گذارد. بنابراین شناخت اصولی و کاربردی از تجهیزات شبکه، به‌ویژه سوئیچ‌ها، برای هر متخصص IT، سئوکار و توسعه‌دهنده وب، یک مزیت رقابتی جدی محسوب می‌شود.

در این پست به مخفف و عبارت تخصصی مرتبط با سوئیچ‌های شبکه سیسکو اشاره شده است که به بررسی کوتاه و مختصر هر کدام می پردازیم:

اصطلاحات فنی و کاربردی سوئیچ

VLAN (Virtual Local Area Network)

VLAN (Virtual Local Area Network) یک تکنولوژی است که به مدیران شبکه این امکان را می‌دهد که شبکه های منطقی مختلف را در یک شبکه فیزیکی واحد ایجاد کنند. به عبارت دیگر، VLAN به گروه‌بندی پورت‌های سوئیچ به‌صورت منطقی بر اساس نیازهای شبکه کمک می‌کند تا دستگاه ها با وجود آن که در نقاط فیزیکی مختلفی قرار دارند، همچنان قادر به برقراری ارتباط با یکدیگر باشند. این گروه‌بندی به بهبود عملکرد شبکه، امنیت و مدیریت منابع کمک می‌کند.

هر VLAN دارای شناسه منحصر به فرد (ID) است و با استفاده از برچسب‌گذاری بسته های داده، دستگاه ها می‌توانند به شبکه های مختلف دسترسی داشته باشند.

یکی از مزایای اصلی استفاده از VLAN، امکان جداسازی ترافیک‌های شبکه است که باعث کاهش broadcast domainها و بهبود عملکرد شبکه می‌شود.

به‌طور مثال، می‌توان VLANهای جداگانه‌ای برای کاربران اداری، بخش مالی یا شبکه مهمان ایجاد کرد تا از تداخل داده ها جلوگیری شود. این تفکیک همچنین امنیت شبکه را افزایش می‌دهد، زیرا هر VLAN به‌طور مستقل از VLANهای دیگر عمل می‌کند و می‌تواند از دسترسی‌های غیرمجاز جلوگیری کند. تنظیم VLANها معمولا از طریق سوئیچ‌ها و با استفاده از پروتکل‌هایی مانند IEEE 802.1Q انجام می‌شود.

PoE (Power over Ethernet)

PoE (Power over Ethernet) یک تکنولوژی است که اجازه می‌دهد تا برق و داده ها از طریق یک کابل اترنت مشترک به دستگاه های مختلف منتقل شوند به عبارت دیگر، به جای استفاده از دو کابل مجزا برای انتقال داده ها و برق، PoE این امکان را فراهم می‌کند که هر دو به طور همزمان از یک کابل اترنت (Ethernet) عبور کنند.

این تکنولوژی به ویژه برای دستگاه هایی که نیاز به برق دارند، مانند تلفن‌های IP، دوربین‌های مداربسته، نقاط دسترسی بی‌سیم (Access Points) و دستگاه های مشابه، مفید است. با استفاده از PoE، می‌توان از نیاز به تاسیسات برق اضافی در کنار هر دستگاه جلوگیری کرد.

PoE به چند نوع تقسیم می‌شود: PoE (IEEE 802.3af)، PoE+ (IEEE 802.3at) و PoE++ (IEEE 802.3bt). مدل‌های مختلف PoE توان‌های متفاوتی برای تامین برق دارند.

به‌طور معمول، PoE می‌تواند تا 15.4 وات برق به دستگاه ها تامین کند، در حالی که PoE+ می‌تواند تا 25.5 وات و PoE++ تا 60 وات یا بیشتر برق منتقل کند. این قابلیت برای محیط‌هایی که نیاز به نصب دستگاه های متعدد در موقعیت‌های دور از منبع برق دارند، مانند محیط های تجاری و سازمانی، بسیار مناسب است و به کاهش هزینه ها و پیچیدگی‌های مربوط به تاسیسات برق کمک می‌کند.

PoE+ (Power over Ethernet Plus)

PoE+ (Power over Ethernet Plus) نسخه پیشرفته تر تکنولوژی PoE است که به ویژه برای دستگاه هایی با نیاز به توان بالاتر طراحی شده است. این تکنولوژی بر اساس استاندارد IEEE 802.3at عمل می‌کند و به جای 15.4 وات که توسط PoE تامین می‌شود، می‌تواند تا 25.5 وات برق به دستگاه ها منتقل کند.

این قابلیت امکان تامین انرژی برای دستگاه های پیچیده‌تر مانند دوربین‌های IP با کیفیت بالا، تلفن‌های VoIP پیشرفته، نقاط دسترسی بی‌سیم (Access Points) و دیگر دستگاه های شبکه‌ای که نیاز به توان بیشتر دارند، فراهم می‌آورد.

PoE+ از یک کابل اترنت برای ارسال همزمان داده ها و برق استفاده می‌کند، که موجب کاهش نیاز به کابل‌کشی اضافی و افزایش سهولت در نصب و مدیریت شبکه می‌شود.

این تکنولوژی به ویژه در محیط‌های تجاری و سازمانی که نیاز به نصب تجهیزات شبکه در مکان‌های مختلف دارند، بسیار مفید است. استفاده از PoE+ می‌تواند به صرفه‌جویی در هزینه های نصب و تاسیسات کمک کند، زیرا نیازی به کشیدن کابل برق جداگانه به دستگاه ها نیست.

همچنین، دستگاه هایی که از PoE+ پشتیبانی می‌کنند، می‌توانند از برق ایمن و با کارایی بالا برای عملکرد بهتر بهره‌مند شوند.

PoE++ (Power over Ethernet Plus Plus)

PoE++ (Power over Ethernet Plus Plus) نسل پیشرفته‌تر تکنولوژی‌های PoE و PoE+ است که توان بیشتری را از طریق کابل شبکه اترنت به دستگاه های متصل منتقل می‌کند.

این تکنولوژی بر اساس استاندارد IEEE 802.3bt توسعه یافته و در دو نوع اصلی ارائه می‌شود: Type 3 که تا 60 وات برق را منتقل می‌کند و Type 4 که توان را تا 90 یا حتی 100 وات افزایش می‌دهد.

این میزان از توان انتقالی، امکان پشتیبانی از دستگاه های قدرتمندتری مانند نمایشگرهای بزرگ دیجیتال، تجهیزات کنفرانس تصویری، لپ‌تاپ‌ها و حتی برخی تجهیزات صنعتی را فراهم می‌سازد.

PoE++ از همه چهار جفت سیم موجود در کابل اترنت استفاده می‌کند برخلاف PoE و PoE+ که فقط از دو جفت سیم استفاده می‌کنند و همین موضوع باعث افزایش ظرفیت انتقال توان می‌شود.

این ویژگی به طراحان شبکه اجازه می‌دهد تا از یک بستر ساده و مجتمع برای انتقال برق و داده به‌طور همزمان استفاده کنند، بدون نیاز به منبع تغذیه جداگانه در محل نصب تجهیزات. در کاربردهای مدرن مانند دفاتر هوشمند، ساختمان‌های اتوماسیون‌شده و پروژه های PoE، IoT++ نقش مهمی در ساده‌سازی زیرساخت و کاهش هزینه ها ایفا می‌کند.

CLI (Command Line Interface)

CLI (Command Line Interface) یا رابط خط فرمان ، یک روش تعامل با دستگاه ها و سیستم‌های شبکه‌ای از جمله سوئیچ‌ها، روترها و فایروال‌ها است که به کاربر اجازه می‌دهد تا دستورات متنی را به‌طور مستقیم وارد کرده و تنظیمات، پیکربندی‌ها و عملیات مدیریتی را انجام دهد.

در محیط‌های سیسکو، CLI رایج‌ترین و قدرتمندترین ابزار برای مدیریت تجهیزات شبکه محسوب می‌شود. کاربران از طریق CLI می‌توانند با وارد کردن دستوراتی مشخص، تنظیمات مربوط به پورت‌ها، VLANها، پروتکل‌های مسیریابی، امنیت و بسیاری دیگر از قابلیت‌های دستگاه را کنترل کنند.

CLI معمولا نسبت به واسط‌های گرافیکی (GUI) پیچیده‌تر و نیازمند دانش فنی بیشتری است، اما در عوض سرعت، دقت و انعطاف بالاتری در مدیریت شبکه فراهم می‌کند.

این رابط برای مدیران شبکه حرفه‌ای بسیار حیاتی است، به ویژه در محیط هایی که نیاز به تنظیمات سفارشی یا اسکریپت نویسی برای پیکربندی سریع تعداد زیادی از تجهیزات وجود دارد.

CLI همچنین امکان مانیتورینگ بلادرنگ وضعیت شبکه، ثبت رویدادها (Logs) و عیب‌یابی سریع را در اختیار کاربران قرار می‌دهد، که در بسیاری از سناریوهای عملیاتی حیاتی است.

SNMP (Simple Network Management Protocol)

(Simple Network Management Protocol) SNMP یا **پروتکل ساده مدیریت شبکه** یک پروتکل استاندارد و رایج در مدیریت و نظارت بر تجهیزات شبکه‌ای نظیر سوئیچ‌ها، روترها، سرورها و پرینترها است. این پروتکل به مدیران شبکه اجازه می‌دهد تا اطلاعات مربوط به وضعیت عملکرد دستگاه ها را جمع آوری کرده، آن‌ها را مانیتور کرده و در صورت نیاز، تنظیمات خاصی را از راه دور اعمال کنند.

SNMP از یک ساختار ساده اما موثر برای تبادل اطلاعات میان یک مدیر (manager) و یک یا چند عامل (agent) استفاده می‌کند. این عوامل در دستگاه ها تعبیه شده‌اند و اطلاعات را به مدیر SNMP گزارش می‌دهند.

SNMP به ویژه در محیط‌های شبکه گسترده و سازمانی بسیار مفید است، زیرا نظارت بر سلامت و کارایی زیرساخت شبکه را به‌صورت متمرکز و خودکار امکان‌پذیر می‌سازد. این پروتکل معمولا با نرم‌افزارهای مانیتورینگ مانند Nagios، Zabbix یا PRTG استفاده می‌شود و می‌تواند شاخص‌هایی مانند پهنای باند، دمای دستگاه، تعداد پکت‌ها وضعیت منابع سخت‌افزاری و بسیاری داده های دیگر را به‌صورت دوره‌ای گزارش دهد. نسخه های مختلف SNMP شامل SNMPv1، SNMPv2c و SNMPv3 هستند که نسخه سوم با بهبودهایی در امنیت و رمزنگاری ارتباطات همراه است.

RPS (Redundant Power Supply)

(Redundant Power Supply) RPS یا **منبع تغذیه پشتیبان**، یک ویژگی سخت‌افزاری در تجهیزات شبکه‌ای مانند سوئیچ‌ها و روترهای حرفه‌ای است که برای افزایش قابلیت اطمینان و پایداری در تامین برق دستگاه ها طراحی شده است.

در صورت بروز خرابی در منبع تغذیه اصلی، سیستم به‌طور خودکار به RPS سوئیچ می‌کند تا از خاموشی یا از کار افتادن دستگاه جلوگیری شود. این قابلیت به‌ویژه در محیط‌های حیاتی و حساس شبکه که قطع برق می‌تواند منجر به اختلال‌های جدی در سرویس‌ها شود، بسیار اهمیت دارد.

RPS معمولا به‌صورت یک ماژول یا یونیت خارجی به سوئیچ یا دستگاه متصل می‌شود و به‌صورت دائم آماده به‌کار باقی می‌ماند، بدون اینکه در حالت عادی در فرآیند تامین انرژی دخالتی داشته باشد. برخی مدل‌های سوئیچ سیسکو دارای پورت یا اسلات ویژه‌ای برای اتصال به RPS هستند و از این قابلیت به‌عنوان بخشی از استراتژی افزایش افزونگی (redundancy) استفاده می‌کنند. استفاده از RPS، همراه با منابع تغذیه دوگانه و سیستم‌های مدیریت انرژی، یکی از رویکردهای اصلی در طراحی شبکه های پایدار و بدون نقطه ضعف تکی است.

StackWise

StackWise یک فناوری اختصاصی شرکت سیسکو است که برای اتصال چندین سوئیچ به یکدیگر به‌صورت فیزیکی و منطقی طراحی شده تا مانند یک سوئیچ واحد عمل کنند. این تکنولوژی امکان می‌دهد چند سوئیچ با استفاده از کابل‌های مخصوص StackWise به‌صورت یکپارچه در قالب یک استک واحد پیکربندی، مدیریت و کنترل شوند.

StackWise قابلیت افزایش ظرفیت، ساده‌سازی مدیریت و ارتقای قابلیت اطمینان را فراهم می‌کند؛ به‌طوری که با وجود چندین سوئیچ در استک، تنها یک آدرس IP برای مدیریت کل مجموعه مورد نیاز است و عملیات fail over به‌صورت خودکار انجام می‌شود.

در این ساختار، یکی از سوئیچ‌ها به‌عنوان Active (Master) و سایر سوئیچ‌ها به‌عنوان Standby یا Member عمل می‌کنند اما همگی بخشی از یک سیستم متحد محسوب می‌شوند.
StackWise باعث افزایش پهنای باند بین سوئیچ‌ها شده و حلقه‌ای از اتصال پرسرعت را فراهم می‌کند، که معمولا دارای پهنای باند 64Gbps، 32Gbps یا بیشتر بسته به مدل سوئیچ است.

استفاده از StackWise در شبکه های متوسط تا بزرگ به‌ویژه در مراکز داده، دفاتر اصلی سازمان‌ها یا مراکز آموزشی، به پایداری و مقیاس‌پذیری بهتر شبکه کمک شایانی می‌کند.

FlexStack

FlexStack یک فناوری اتصال و استک‌سازی اختصاصی شرکت سیسکو است که برای مدل‌های خاصی از سوئیچ‌های سری Catalyst، به‌ویژه سری‌های پایین‌تر مانند S-2960 و X-2960 طراحی شده است.

این تکنولوژی به مدیران شبکه اجازه می‌دهد تا چند سوئیچ مستقل را از طریق ماژول و کابل مخصوص به یکدیگر متصل کرده و آن‌ها را به‌صورت یک سوئیچ منطقی واحد مدیریت کنند.

FlexStack باعث ساده‌سازی مدیریت شبکه می‌شود، زیرا تمام سوئیچ‌های موجود در استک به‌طور متمرکز و از طریق یک آدرس IP و یک نقطه کنترلی قابل پیکربندی هستند.

FlexStack از نظر کارکرد مشابه فناوری StackWise عمل می‌کند اما با پهنای باند و قابلیت‌های فنی محدودتر و بیشتر برای محیط‌هایی با اندازه کوچک تا متوسط مناسب است. به‌طور معمول، FlexStack پهنای باندی در حدود 20 تا 40 گیگابیت بر ثانیه بین سوئیچ‌ها فراهم می‌کند و حداکثر تا 4 سوئیچ را می‌توان به یکدیگر متصل کرد.

همچنین نسخه‌ای به نام FlexStack-Plus وجود دارد که در برخی مدل‌های جدیدتر پشتیبانی شده و قابلیت استک‌سازی سریع‌تر و پشتیبانی از تعداد سوئیچ‌های بیشتر را فراهم می‌کند. این تکنولوژی به سازمان‌ها کمک می‌کند تا بدون پیچیدگی زیاد، شبکه‌ای مقیاس‌پذیر، پایدار و قابل مدیریت ایجاد کنند.

StackWise-160

StackWise-160 یک فناوری استک‌سازی پیشرفته از شرکت سیسکو است که در سوئیچ‌های سری‌های Catalyst 3650 و Catalyst 9200 به‌کار می‌رود.

این فناوری امکان اتصال حداکثر ۹ سوئیچ را به‌صورت فیزیکی و منطقی فراهم می‌کند تا مانند یک سوئیچ واحد عمل کنند با استفاده از StackWise-160، تمام سوئیچ‌های موجود در استک به‌طور متمرکز و از طریق یک آدرس IP و یک نقطه کنترلی قابل پیکربندی هستند.

از نظر فنی، StackWise-160 از چهار حلقه داخلی برای انتقال داده استفاده می‌کند که هر حلقه توان انتقال داده تا ۴۰ گیگابیت بر ثانیه را دارد در مجموع، این ساختار پهنای باندی تا ۸۰

گیگابیت بر ثانیه را برای هر سوئیچ فراهم می‌کند و با استفاده از پروتکل Spatial Reuse Protocol (SRP)، این مقدار می‌تواند تا ۱۶۰ گیگابیت بر ثانیه افزایش یابد.

یکی از ویژگی‌های کلیدی StackWise-160، پشتیبانی از Stateful Switchover (SSO) است که در صورت بروز خرابی در سوئیچ فعال، به‌طور خودکار کنترل به سوئیچ پشتیبان منتقل می‌شود، بدون اینکه اختلالی در عملکرد شبکه ایجاد شود.

برای بهره‌برداری از StackWise-160، نیاز به ماژول و کابل‌های مخصوص استک‌سازی است که به‌صورت جداگانه ارائه می‌شوند. این فناوری به‌ویژه برای محیط‌هایی که نیاز به پایداری بالا، مقیاس‌پذیری و مدیریت متمرکز دارند، مانند مراکز داده و شبکه های سازمانی، بسیار مناسب است.

OSPF (Open Shortest Path First)

OSPF (Open Shortest Path First) یک **پروتکل مسیریابی پویا** از نوع Link-State است که در شبکه های مبتنی بر IP برای یافتن بهترین مسیر به مقصد مورد نظر استفاده می‌شود. این پروتکل توسط سازمان IETF طراحی شده و در دسته پروتکل‌های IGP (Interior Gateway Protocol) قرار دارد، به این معنا که برای مسیریابی درون یک سیستم خودمختار (AS) به کار می‌رود. OSPF برخلاف پروتکل‌های Distance Vector مانند RIP، دید کاملی از توپولوژی شبکه دارد و با استفاده از الگوریتم Dijkstra (Shortest Path First)، سریع‌ترین و بهینه‌ترین مسیر ممکن را برای انتقال داده ها محاسبه می‌کند.

یکی از ویژگی‌های مهم OSPF این است که به نواحی (Areas) تقسیم می‌شود تا بتواند در شبکه های بزرگ مقیاس‌پذیری و کارایی بالایی ارائه دهد. معمولا شبکه با یک ناحیه مرکزی به نام Area 0 (Backbone) شروع می‌شود و سایر نواحی به آن متصل می‌گردند. OSPF از مفاهیم پیشرفته‌ای مانند LSA (Link-State Advertisement)، Hello Packets و DR/BDR (Designated Router / Backup Designated Router) استفاده می‌کند تا اطلاعات مسیر را بین روترها مبادله کرده و وضعیت لینک‌ها را بررسی و بروزرسانی کند. این پروتکل برای محیط‌های سازمانی متوسط تا بزرگ با نیاز به مسیریابی سریع، پایدار و قابل اعتماد، انتخاب بسیار مناسبی است.

EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP (Enhanced Interior Gateway Routing Protocol) یک پروتکل مسیریابی پویا است که توسط شرکت سیسکو طراحی و توسعه یافته و به‌عنوان نسخه بهبودیافته‌ای از IGRP ارائه شده است. این پروتکل در دسته‌بندی hybrid routing protocols قرار دارد، زیرا ترکیبی از ویژگی‌های پروتکل‌های Distance Vector و Link-State را داراست. EIGRP از الگوریتم DUAL (Diffusing Update Algorithm) برای محاسبه سریع و بدون loop بهترین مسیر استفاده می‌کند و یکی از سریع‌ترین پروتکل‌های مسیریابی برای بازیابی پس از قطع لینک محسوب می‌شود.

EIGRP به‌طور خودکار فقط اطلاعات تغییر یافته را و نه کل جدول مسیر ، به سایر روترها ارسال می‌کند که باعث کاهش مصرف پهنای باند شبکه می‌شود. این پروتکل از مقادیر متریک چندگانه مانند پهنای باند، تاخیر، قابلیت اطمینان و بار برای تعیین بهترین مسیر استفاده می‌کند.

در گذشته، EIGRP یک پروتکل اختصاصی سیسکو بود اما از نسخه 15 سیستم‌عامل IOS، به‌صورت نسبی باز شد و دیگر فقط محدود به تجهیزات سیسکو نیست. با این حال، هنوز هم بیشترین کاربرد آن در شبکه هایی است که به‌طور کامل از تجهیزات سیسکو استفاده می‌کنند و به مسیریابی سریع، کارآمد و پایدار نیاز دارند.

BGP (Border Gateway Protocol)

BGP (Border Gateway Protocol) یک پروتکل مسیریابی خارجی (EGP) و ستون فقرات اینترنت جهانی است که برای مسیریابی بین سیستم‌های خودمختار (Autonomous Systems یا AS) مورد استفاده قرار می‌گیرد.

BGP به‌طور خاص برای محیط‌های بزرگ، مانند ISPها، دیتاسنترها و شبکه های بین‌المللی طراحی شده و برخلاف پروتکل‌های داخلی مانند OSPF یا EIGRP وظیفه مدیریت مسیرهای بین‌المللی و کنترل جریان ترافیک اینترنت را بر عهده دارد. نسخه رایج آن BGPv4 است که از پروتکل TCP (پورت 179) برای برقراری ارتباطات پایدار بین روترها استفاده می‌کند.

یکی از ویژگی‌های کلیدی BGP انعطاف‌پذیری بالا در کنترل سیاست‌های مسیریابی است.

در BGP مسیرها نه بر اساس سرعت یا کوتاه‌ترین فاصله، بلکه بر اساس سیاست‌ها (Policies) و پارامترهای مدیریتی انتخاب می‌شوند.

این پروتکل از جداول بزرگ مسیریابی پشتیبانی می‌کند و توانایی کنترل دقیق مسیرهای ورودی و خروجی ترافیک بین شبکه ها را دارد. به‌دلیل ساختار پیچیده و حساس آن، پیاده‌سازی BGP نیازمند دقت، تجربه و پیکربندی اصولی است، زیرا اشتباه در تنظیمات آن می‌تواند منجر به اختلالات گسترده در شبکه های جهانی شود.

MACsec (Media Access Control Security)

MACsec (Media Access Control Security) یک پروتکل امنیتی است که برای محافظت از داده ها در لایه لینک داده در شبکه های محلی (LAN) طراحی شده است.

این پروتکل به‌ویژه برای شبکه های اترنت استفاده می‌شود و از طریق رمزگذاری داده های اترنت (Ethernet frames) مانع از دسترسی غیرمجاز و حملات مختلف مانند دستکاری داده ها، شنود (sniffing) و تزریق بسته های مخرب می‌شود.

MACsec بر اساس استاندارد IEEE 802.1AE عمل می‌کند و تمام داده ها و ترافیک بین دستگاه ها را در سطح لایه 2 (لایه لینک داده) رمزگذاری می‌کند.

MACsec از AES (Advanced Encryption Standard) برای رمزگذاری داده ها استفاده می‌کند که امنیت بالایی فراهم می‌آورد. این پروتکل قابلیت‌های مهمی مانند Integrity Check Value (ICV) برای اطمینان از یکپارچگی داده ها و Replay Protection برای جلوگیری از حملات تکراری را دارد.

با استفاده از MACsec، شبکه ها می‌توانند از تهدیدات مختلف جلوگیری کرده و اطلاعات حساس را از دسترسی‌های غیرمجاز محافظت کنند، که به‌ویژه در محیط‌های با داده های حساس یا در اتصالات بین‌دستگاهی در شبکه های گسترده مانند مراکز داده یا محیط‌های بانکی بسیار مفید است.

TrustSec

TrustSec یک فناوری امنیتی سیسکو است که برای مدیریت دسترسی و کنترل ترافیک شبکه بر اساس هویت و سیاست‌های امنیتی طراحی شده است.

این فناوری امکان می‌دهد تا سیاست‌های امنیتی به‌طور متمرکز و بر اساس هویت کاربران یا دستگاه ها، به‌جای موقعیت فیزیکی یا آدرس IP، اعمال شود. TrustSec با استفاده از IEEE 802.1X برای احراز هویت و MACsec برای رمزگذاری داده ها، سطح بالایی از امنیت را در شبکه فراهم می‌کند.

TrustSec از Security Group Tags (SGT) برای تخصیص و اعمال سیاست‌های امنیتی استفاده می‌کند. SGT به هر کاربر یا دستگاه در شبکه یک برچسب امنیتی اختصاص می‌دهد که براساس آن، سیاست‌های مختلف دسترسی و کنترل ترافیک اعمال می‌شود. این ویژگی امکان ایجاد سیاست‌های دسترسی دقیق‌تر، بر اساس هویت و نوع ترافیک، را فراهم می‌آورد و همچنین از حملات مبتنی بر IP spoofing و سایر تهدیدات مرتبط با تغییرات آدرس‌های IP جلوگیری می‌کند.

TrustSec به‌ویژه در شبکه های سازمانی، مراکز داده و محیط‌های دارای ترافیک حساس کاربرد دارد، زیرا امکان کنترل دقیق‌تر و مقیاس‌پذیری بالایی در برابر تهدیدات امنیتی فراهم می‌آورد.

NetFlow

NetFlow یک پروتکل تجزیه و تحلیل ترافیک شبکه است که توسط شرکت سیسکو توسعه یافته و برای جمع‌آوری و گزارش داده های مربوط به جریان‌های ترافیکی (flows) در شبکه ها استفاده می‌شود.

NetFlow به مدیران شبکه این امکان را می‌دهد که با تجزیه و تحلیل این داده ها، الگوهای ترافیک شبکه را شناسایی کرده، عملکرد شبکه را نظارت کرده و مسائل احتمالی مانند حملات DDoS، استفاده غیرمجاز از پهنای باند یا مشکلات پیکربندی را تشخیص دهند. هر جریان (flow) شامل اطلاعاتی مانند آدرس‌های IP مبدا و مقصد، پورت‌های TCP/UDP، نوع پروتکل و مدت زمان ارتباط است.

NetFlow از طریق NetFlow Exporters که معمولا روترها و سوئیچ‌ها هستند، اطلاعات مربوط به جریان‌ها را جمع‌آوری کرده و به NetFlow Collectors ارسال می‌کند، که این داده ها را پردازش و ذخیره می‌کنند. این اطلاعات می‌تواند برای گزارش‌های تجزیه و تحلیل پیشرفته، شبیه‌سازی ترافیک، مدیریت پهنای باند و تشخیص تهدیدات امنیتی استفاده شود.

نسخه های مختلف NetFlow مانند v5، v9 و v10 (IPFIX) ویژگی‌های متنوعی دارند و به مدیران شبکه این امکان را می‌دهند که اطلاعات دقیق‌تری را جمع‌آوری کنند. NetFlow به‌ویژه در شبکه های بزرگ و پیچیده برای پایش و بهینه‌سازی عملکرد شبکه بسیار مفید است.

PoE Budget

PoE Budget به مقدار توان یا برق مجاز و قابل تامین توسط یک دستگاه برای دستگاه های متصل به فناوری Power over Ethernet (PoE) اشاره دارد. این بودجه معمولا به‌طور مستقیم به قدرت تامین‌شده توسط سوئیچ PoE یا دستگاه تامین‌کننده PoE بستگی دارد و به میزان توان مصرفی مورد نیاز برای تامین برق به دستگاه هایی مانند تلفن‌های IP، دوربین‌های امنیتی، نقطه های دسترسی وای‌فای (Access Points) و سایر دستگاه های PoE متصل می‌شود.

به عبارت دیگر، PoE Budget نشان‌دهنده حداکثر توان قابل توزیع برای دستگاه های متصل به یک سوئیچ PoE است که باید به‌طور کارآمد و متوازن بین دستگاه ها توزیع شود. برای مثال، یک سوئیچ PoE ممکن است دارای یک PoE Budget 375 وات باشد، که به این معنی است که سوئیچ می‌تواند مجموعا تا 375 وات برق برای دستگاه های مختلف متصل تامین کند.

هنگام انتخاب سوئیچ‌های PoE، مدیران شبکه باید مطمئن شوند که PoE Budget کافی برای تامین نیازهای تمامی دستگاه های متصل به شبکه وجود داشته باشد تا از بروز مشکلاتی مانند قطعی برق یا عملکرد ضعیف دستگاه ها جلوگیری شود.

SFP (Small Form-factor Pluggable)

SFP (Small Form-factor Pluggable) یک ماژول انتقال نوری یا الکتریکی کوچک و قابل تعویض است که در تجهیزات شبکه مانند سوئیچ‌ها، روترها و سرورها برای اتصال به شبکه های فیبر نوری یا کابل‌های مسی استفاده می‌شود. این ماژول‌ها به‌طور معمول برای فراهم کردن اتصال‌های شبکه با سرعت‌های مختلف (مانند 1Gbps، 10Gbps و حتی بالاتر) و مسافت‌های متفاوت (محلی یا مسافت‌های طولانی) استفاده می‌شوند و به کاربران اجازه می‌دهند تا تجهیزات خود را با توجه به نیازهای شبکه به راحتی ارتقاء دهند.

SFP به‌عنوان یک استاندارد ماژول، می‌تواند انواع مختلفی از اتصالات را پشتیبانی کند، از جمله اتصال‌های فیبر نوری با طول موج‌های مختلف و یا کابل‌های مسی اترنت. یکی از مزایای اصلی SFP این است که این ماژول‌ها می‌توانند به راحتی تعویض شوند (hot-swappable) بدون نیاز به خاموش کردن دستگاه، که این ویژگی موجب تسهیل در مدیریت و ارتقاء شبکه ها می‌شود. همچنین، SFPها در مقایسه با سایر ماژول‌ها مانند GBIC (Gigabit Interface Converter) از ابعاد کوچکتری برخوردارند، بنابراین فضای کمتری در دستگاه اشغال می‌کنند.

SFP+ (Small Form-factor Pluggable Plus)

SFP+ (Small Form-factor Pluggable Plus) یک نسخه پیشرفته‌تر از SFP است که برای انتقال داده با سرعت‌های بالاتر، معمولا تا 10 گیگابیت بر ثانیه (10Gbps) طراحی شده است.

مانند SFP، SFP+ یک ماژول کوچک و قابل تعویض است که در تجهیزات شبکه مانند سوئیچ‌ها، روترها و سرورها برای اتصال به شبکه های فیبر نوری یا کابل‌های مسی استفاده می‌شود.

SFP+ از فناوری‌های مشابهی با SFP استفاده می‌کند، اما از نظر ظرفیت پهنای باند و سرعت بهینه‌تر است و به‌ویژه برای نیازهای شبکه های با پهنای باند بالا و ارتباطات سریعتر مناسب است.

SFP+ به‌طور عمده برای پشتیبانی از اتصالات 10GbE (10 Gigabit Ethernet) به‌کار می‌رود و به‌ویژه در محیط‌های شبکه‌ای با حجم داده های زیاد مانند دیتاسنترها و شبکه های اترنت سریع کاربرد دارد. این ماژول‌ها معمولا از انواع مختلفی از کابل‌ها و اتصالات پشتیبانی می‌کنند، از جمله کابل‌های فیبر نوری برای مسافت‌های طولانی و کابل‌های مسی برای مسافت‌های کوتاه‌تر. به دلیل طراحی جمع و جور و امکان تعویض آن بدون نیاز به خاموش کردن دستگاه، SFP+ به یک گزینه محبوب در محیط‌های شبکه‌ای با نیاز به سرعت بالا و مقیاس‌پذیری تبدیل شده است.

10GbE (10 Gigabit Ethernet)

10GbE (10 Gigabit Ethernet) یک فناوری شبکه است که سرعت انتقال داده را تا 10 گیگابیت بر ثانیه فراهم می‌کند. این استاندارد در واقع نسخه پیشرفته‌تری از Ethernet است که برای پشتیبانی از نیازهای شبکه های با حجم ترافیک بالا طراحی شده است. 10GbE معمولا در دیتاسنترها، شبکه های سازمانی بزرگ و محیط‌هایی که نیاز به انتقال سریع حجم زیادی از داده ها دارند، مورد استفاده قرار می‌گیرد.

10GbE از انواع مختلفی از رسانه ها برای انتقال داده ها استفاده می‌کند، از جمله فیبر نوری (برای مسافت‌های طولانی) و کابل‌های مسی (مانند Cat 6a یا Cat 7 برای مسافت‌های کوتاه‌تر). این تکنولوژی از پروتکل‌های استاندارد IEEE 802.3ae و IEEE 802.3aq پشتیبانی می‌کند و به‌ویژه برای محیط‌های شبکه‌ای با نیاز به سرعت بالا، مانند انتقال داده های ویدیویی، پایگاه های داده و پردازش‌های ابری، بسیار مناسب است. همچنین، 10GbE به‌عنوان یکی از پیش‌نیازهای مهم برای شبکه های اترنت سریع و مقیاس‌پذیر در نظر گرفته می‌شود.

40GbE (40 Gigabit Ethernet)

40GbE (40 Gigabit Ethernet) یک استاندارد شبکه است که سرعت انتقال داده را به 40 گیگابیت بر ثانیه افزایش می‌دهد. این فناوری معمولا در شبکه های بزرگ، دیتاسنترها و شبکه های اترنت با ظرفیت بالا به‌کار می‌رود، جایی که نیاز به پهنای باند وسیع برای انتقال حجم عظیمی از داده ها و پاسخگویی به درخواست‌های سریع شبکه وجود دارد.

40GbE به‌ویژه برای محیط‌های با حجم ترافیک بسیار زیاد و کاربردهای حساس به تاخیر مانند پردازش‌های ابری، ذخیره‌سازی داده های بزرگ و انتقال داده های ویدیویی با کیفیت بالا ضروری است.

40GbE از چند نوع رسانه برای انتقال داده ها استفاده می‌کند، از جمله کابل‌های فیبر نوری برای مسافت‌های طولانی و کابل‌های مسی برای مسافت‌های کوتاه‌تر. این استاندارد از چندین پروتکل و فناوری مختلف برای انتقال داده استفاده می‌کند، از جمله QSFP (Quad Small Form-factor Pluggable) برای ارتباطات 40 گیگابیت، که امکان ارائه ارتباطات سریع و مقیاس‌پذیر را فراهم می‌آورد. 40GbE به دلیل پشتیبانی از پهنای باند بالا، به شبکه ها امکان می‌دهد تا با حجم داده های بیشتر به‌طور موثرتر و با تاخیر کمتری عمل کنند.

Fast Ethernet

Fast Ethernet یک استاندارد شبکه است که سرعت انتقال داده ها را به 100 مگابیت بر ثانیه (Mbps) افزایش می‌دهد. این فناوری به‌عنوان یک نسخه پیشرفته‌تر از 10BASE-T Ethernet شناخته می‌شود که سرعت کمتری داشت.

Fast Ethernet معمولا برای شبکه های محلی (LAN) و کاربردهای عمومی مانند اتصال کامپیوترها به شبکه، اتصال پرینترها و سایر دستگاه های مصرفی در سازمان‌ها استفاده می‌شود. این فناوری عمدتا از کابل‌های Cat 5 یا Cat 5e برای اتصال دستگاه ها به سوئیچ‌ها و روترها استفاده می‌کند.

Fast Ethernet به‌دلیل هزینه های پایین و پشتیبانی از سرعت قابل‌قبول در مقایسه با شبکه های 10 مگابیتی، در شبکه های کوچک تا متوسط بسیار محبوب بود. با این حال، در دنیای امروز که نیاز به سرعت‌های بالاتر مانند Gigabit Ethernet (1GbE) یا 10GbE وجود دارد، Fast Ethernet به‌طور کامل از سوی فناوری‌های جدیدتر کنار گذاشته شده است، اما هنوز هم در برخی شبکه های قدیمی‌تر یا کاربردهایی که به سرعت‌های بسیار بالا نیاز ندارند، مورد استفاده قرار می‌گیرد.

Gigabit Ethernet

Gigabit Ethernet یک استاندارد شبکه است که سرعت انتقال داده ها را به 1 گیگابیت بر ثانیه (Gbps) افزایش می‌دهد.

این فناوری، که به‌طور گسترده در شبکه های محلی (LAN) و محیط‌های تجاری استفاده می‌شود، جایگزینی برای Fast Ethernet (100 Mbps) است و سرعت بالاتری را برای کاربردهایی مانند انتقال داده های بزرگ ویدئو کنفرانس و استفاده از اپلیکیشن‌های با مصرف پهنای باند بالا فراهم می‌کند.

Gigabit Ethernet به‌ویژه با استفاده از کابل‌های Cat 5e و Cat 6 در شبکه ها نصب می‌شود و امکان ارتباطات سریع‌تر و موثرتر را نسبت به نسخه های قبلی می‌دهد.

علاوه بر این، این استاندارد برای استفاده در مسافت‌های طولانی‌تر با استفاده از کابل‌های فیبر نوری نیز مناسب است. Gigabit Ethernet اکنون به‌عنوان استاندارد غالب در شبکه های خانگی و اداری در نظر گرفته می‌شود و به دلیل سرعت بالا و تطبیق‌پذیری آن، برای اکثر نیازهای روزمره شبکه های تجاری و خانگی بسیار مناسب است.

10/100/1000

10/100/1000 به سرعت‌های مختلف انتقال داده در شبکه های اترنت اشاره دارد که به‌طور معمول به‌عنوان Multi-Speed Ethernet یا Gigabit Ethernet شناخته می‌شود. این عبارت نشان‌دهنده سه سرعت مختلف است که یک پورت شبکه می‌تواند از آن‌ها پشتیبانی کند:

- 10 Mbps: سرعت اولیه اترنت که به‌طور معمول در 10BASE-T استفاده می‌شود.
- 100 Mbps: سرعت ارتقا یافته‌ای که در Fast Ethernet استفاده می‌شود.
- 1000 Mbps (1 Gbps): سرعتی که در Gigabit Ethernet برای انتقال داده ها استفاده می‌شود.

این پورت‌ها معمولا به‌صورت auto-negotiating عمل می‌کنند، به این معنا که بسته به نوع کابل و دستگاه های متصل، پورت به طور خودکار سرعت مناسب‌ترین را انتخاب می‌کند.

این ویژگی امکان اتصال دستگاه هایی با سرعت‌های مختلف را در یک شبکه فراهم می‌کند و از آن‌جا که این پورت‌ها توانایی پشتیبانی از هر سه سرعت را دارند، در اکثر سوئیچ‌ها و روترهای مدرن به‌عنوان یک ویژگی استاندارد به‌کار می‌روند.

Stacking

Stacking در شبکه های کامپیوتری به فرآیند اتصال چندین سوئیچ شبکه به یکدیگر برای تشکیل یک سوئیچ واحد مجازی اشاره دارد.

این ویژگی به مدیران شبکه این امکان را می‌دهد که چندین سوئیچ فیزیکی را به‌طور منطقی به یک سوئیچ واحد تبدیل کنند، که به افزایش مقیاس‌پذیری، عملکرد و قابلیت مدیریت شبکه کمک می‌کند. در هنگام استفاده از stacking، هر سوئیچ عضو در پیکربندی استک به‌طور مشترک یک IP واحد و تنظیمات مشابهی دارد و از یک رابط مدیریتی واحد برای کنترل و نظارت استفاده می‌شود.

یکی از مزایای اصلی stacking، قابلیت افزونگی (redundancy) و تحمل خطاست.

اگر یکی از سوئیچ‌های عضو استک دچار مشکل شود، دیگر سوئیچ‌ها می‌توانند به‌طور خودکار جایگزین آن شوند و از قطع شدن شبکه جلوگیری کنند.

همچنین، stacking به مدیران شبکه این امکان را می‌دهد که ترافیک را بین سوئیچ‌ها به‌طور بهینه توزیع کنند و از مصرف منابع به‌طور کارآمدتر استفاده کنند. این ویژگی معمولا در شبکه های بزرگ و پیچیده‌ای که نیاز به مدیریت آسان و افزایش ظرفیت دارند، به‌ویژه در دیتا سنترها و شبکه های سازمانی، کاربرد دارد.

Layer 2

Layer 2 یا لایه دوم در مدل OSI (مدل مرجع تعامل سیستم‌های باز) به لایه لینک داده اشاره دارد.

این لایه مسئول ارسال داده ها از یک دستگاه به دستگاه دیگر در همان شبکه محلی (LAN) است و عملیات‌های مختلفی مانند آدرس‌دهی MAC (Media Access Control)، کنترل خطا و تنظیمات ارتباطی بین دستگاه های شبکه را انجام می‌دهد. در لایه دوم، داده ها به صورت فریم (frames) ارسال می‌شوند که شامل اطلاعات آدرس‌دهی MAC منبع و مقصد، داده های واقعی و همچنین اطلاعات کنترل خطا هستند.

یکی از وظایف اصلی لایه دوم، مدیریت و هدایت داده ها از طریق رسانه های شبکه (مثل کابل‌های مسی یا فیبر نوری) به دستگاه های مختلف است.

دستگاه هایی مانند سوئیچ‌ها (Switches) و بریج‌ها (Bridges) در این لایه عمل می‌کنند و با استفاده از آدرس‌های MAC، ترافیک را بین دستگاه های مختلف در شبکه محلی هدایت می‌کنند. لایه دوم در مقایسه با لایه اول (لایه فیزیکی) وظایف پیچیده‌تری دارد، زیرا به کنترل جریان داده ها و جلوگیری از برخورد بسته ها نیز می‌پردازد. L2 همچنین به دلیل عدم نیاز به آدرس‌دهی IP، عملکرد سریع‌تری را در شبکه های محلی فراهم می‌آورد.

Layer 3

Layer 3 یا لایه سوم در مدل OSI به لایه شبکه اشاره دارد.

این لایه مسئول **هدایت و مسیریابی داده ها** بین دستگاه های مختلف در شبکه های گسترده (WAN) و شبکه های مختلف است. یکی از اصلی‌ترین وظایف لایه سوم، مسیریابی بسته های داده از یک شبکه به شبکه دیگر با استفاده از آدرس‌دهی IP (Internet Protocol) است.

این لایه همچنین شامل اطلاعات مربوط به مسیرها و انتخاب بهترین مسیر برای ارسال داده ها از مبدا به مقصد است.

در لایه سوم، دستگاه هایی مانند روترها (Routers) عمل می‌کنند که با استفاده از آدرس‌های IP، بسته ها را از یک شبکه به شبکه دیگر هدایت می‌کنند. این فرآیند به این صورت است که بسته ها با توجه به اطلاعات موجود در جدول مسیریابی روتر، به مقصد نهایی خود ارسال می‌شوند.

لایه سوم همچنین مسئول **تقسیم‌بندی شبکه ها به زیرشبکه ها** و مدیریت آدرس‌دهی و زیرشبکه ها از طریق subnetting است. این لایه علاوه بر مسیریابی، برای کنترل جریان و بازبینی آدرس‌های IP نیز به‌کار می‌رود. برخلاف لایه دوم که محدود به شبکه های محلی است، لایه سوم امکان ارتباط بین شبکه های مختلف و حتی شبکه های جهانی مانند اینترنت را فراهم می‌آورد.

Static Routing

Static Routing به مسیریابی اشاره دارد که در آن مدیر شبکه به‌طور دستی و ثابت، مسیرهای خاصی را برای هدایت بسته های داده در شبکه تعریف می‌کند.

در این روش، مسیرهای شبکه به‌صورت دستی به دستگاه های مسیریاب (روترها) اضافه می‌شوند و تغییرات در جدول مسیریابی باید توسط مدیر شبکه انجام شود. این نوع مسیریابی معمولا در شبکه های ساده یا شبکه هایی که تغییرات کمتری در توپولوژی دارند، استفاده می‌شود.

مزایای اصلی Static Routing شامل **سادگی در پیاده‌سازی، مصرف کم منابع سیستمی** و **امنیت بیشتر** به دلیل عدم وابستگی به پروتکل‌های مسیریابی پویا است.

از آنجا که مسیرها به‌صورت دستی وارد می‌شوند، هیچ‌گونه تبادل اطلاعات مسیریابی با سایر روترها انجام نمی‌شود، بنابراین کمتر احتمال دارد که مسیرهای اشتباه به دلیل مشکلات پروتکل‌های مسیریابی رخ دهند. با این حال، Static Routing به تغییرات شبکه حساس است و در صورت تغییر توپولوژی یا وقوع خرابی در مسیرها، نیاز به بروزرسانی دستی دارد، که این می‌تواند در شبکه های بزرگ یا پیچیده چالش‌برانگیز باشد.

Dynamic Routing

Dynamic Routing به فرآیند مسیریابی اشاره دارد که در آن روترها به‌طور خودکار و به‌وسیله پروتکل‌های مسیریابی، مسیرهای شبکه را شناسایی و به‌روز می‌کنند.

برخلاف Static Routing که مسیرها به‌صورت دستی پیکربندی می‌شوند، در Dynamic Routing پروتکل‌های مسیریابی مانند OSPF (Open Shortest Path First)، RIP (Routing Information Protocol)، EIGRP (Enhanced Interior Gateway Routing Protocol) و BGP (Border Gateway Protocol) برای تبادل اطلاعات مسیریابی بین روترها استفاده می‌شوند.

این پروتکل‌ها به روترها اجازه می‌دهند تا تغییرات در شبکه (مانند افزودن یا حذف دستگاه ها، تغییر مسیرها و خرابی لینک‌ها) را شناسایی کنند و به‌طور خودکار جداول مسیریابی خود را به‌روزرسانی کنند.

مزیت اصلی Dynamic Routing این است که این روش خودکار است و به شبکه امکان می‌دهد که به‌صورت پویا با تغییرات مختلف سازگار شود.

به‌عنوان مثال، در صورت بروز مشکل یا خرابی در یک لینک، روترها می‌توانند به‌طور خودکار مسیرهای جایگزین را پیدا کرده و ترافیک را هدایت کنند.

این ویژگی باعث می‌شود که Dynamic Routing برای شبکه های بزرگ و پیچیده بسیار مناسب باشد، جایی که نیاز به مدیریت دستی مسیرها در زمان تغییرات مستمر، غیرعملی است. با این حال، به دلیل تبادل اطلاعات بین روترها و استفاده از منابع بیشتر، مصرف پهنای باند و بار پردازشی در این نوع مسیریابی بیشتر از روش‌های ایستا است.

IEEE 802.1Q (VLAN Tagging Protocol)

IEEE 802.1Q یک پروتکل استاندارد برای VLAN Tagging است که به سوئیچ‌ها و دستگاه های شبکه اجازه می‌دهد تا ترافیک شبکه های مجازی (VLANها) را شناسایی کرده و آن را به‌طور صحیح مدیریت کنند.

این پروتکل، که به‌طور گسترده در شبکه های مبتنی بر Ethernet استفاده می‌شود، به هر فریم Ethernet یک Tag خاص اضافه می‌کند که شامل اطلاعات مربوط به VLAN است که آن فریم به آن تعلق دارد.

این اطلاعات معمولا شامل یک شناسه VLAN (VLAN ID) است که به سوئیچ‌ها و دستگاه ها کمک می‌کند تا ترافیک مربوط به VLANهای مختلف را از یکدیگر تفکیک کنند و مسیر مناسب را برای آن ارسال کنند.

IEEE 802.1Q به ویژه در شبکه های پیچیده‌ای که چندین VLAN برای تفکیک ترافیک مورد استفاده قرار می‌گیرد، بسیار مفید است. این پروتکل به مدیران شبکه این امکان را می‌دهد که از یک لینک فیزیکی برای انتقال داده ها از چندین VLAN به‌طور همزمان استفاده کنند، به‌طوری که ترافیک هر VLAN به‌صورت مستقل از دیگران به مقصد خود منتقل می‌شود.

این ویژگی به بهبود مقیاس‌پذیری، بهره‌وری و امنیت شبکه کمک می‌کند و اجازه می‌دهد تا چندین شبکه منطقی به‌طور همزمان روی زیرساخت فیزیکی مشترک اجرا شوند.

Trunking

Trunking در شبکه های کامپیوتری به **فرآیند انتقال ترافیک** از چندین VLAN (شبکه محلی مجازی) از طریق یک لینک فیزیکی واحد اشاره دارد.

این فرآیند به سوئیچ‌ها و دستگاه ها این امکان را می‌دهد که ترافیک مربوط به VLANهای مختلف را از طریق یک اتصال فیزیکی مشترک ارسال و دریافت کنند، بدون اینکه هر VLAN نیاز به لینک فیزیکی جداگانه داشته باشد.

معمولا برای این منظور از پروتکل IEEE 802.1Q (VLAN Tagging) استفاده می‌شود، که به هر فریم شبکه یک VLAN Tag اضافه می‌کند تا ترافیک هر VLAN به‌طور جداگانه در مسیر خود هدایت شود.

Trunking به‌ویژه در محیط‌های شبکه‌ای با تعداد زیادی VLAN ضروری است، زیرا از طریق آن می‌توان چندین VLAN را از طریق یک لینک فیزیکی انتقال داد، که باعث کاهش نیاز به کابل‌های اضافی و سادگی در مدیریت شبکه می‌شود.

معمولا سوئیچ‌ها و روترها از trunking برای ارتباط بین سوئیچ‌های مختلف یا بین سوئیچ و روتر استفاده می‌کنند. این روش همچنین به افزایش مقیاس‌پذیری شبکه کمک می‌کند و امکان مدیریت ترافیک چندین VLAN را با حداقل استفاده از منابع فراهم می‌آورد.

DHCP Snooping

DHCP Snooping یک ویژگی امنیتی در شبکه های سوئیچ است که برای نظارت و کنترل درخواست‌ها و پاسخ‌های DHCP (Dynamic Host Configuration Protocol) در شبکه های محلی (LAN) طراحی شده است. این ویژگی به سوئیچ‌ها اجازه می‌دهد تا فقط دستگاه های معتبر را به عنوان سرور DHCP شناسایی کنند و از ارسال درخواست‌های DHCP از سوی دستگاه های غیرمجاز جلوگیری کنند. DHCP Snooping با ایجاد یک جدول DHCP Snooping که شامل آدرس‌های IP، MAC و پورت‌هایی که از آن‌ها درخواست DHCP صادر شده است، عمل می‌کند.

مزیت اصلی DHCP Snooping افزایش امنیت شبکه است. به‌طور خاص، این ویژگی از حملات DHCP Spoofing جلوگیری می‌کند، که در آن یک مهاجم با ارسال پاسخ‌های DHCP جعلی، تلاش می‌کند آدرس IPها را برای دستگاه های دیگر اختصاص دهد و این ممکن است به حملات Man-in-the-Middle یا حملات DDoS منجر شود.

با فعال کردن DHCP Snooping، تنها درخواست‌هایی که از پورت‌های معتبر مانند پورت‌هایی که به سرور DHCP متصل هستند عبور می‌کنند، پاسخ داده می‌شوند، در حالی که درخواست های غیر معتبر از پورت‌های غیرمجاز مسدود می‌شوند. این ویژگی به‌ویژه در شبکه های بزرگ و پیچیده که در آن تعداد زیادی دستگاه به‌طور دینامیک به شبکه متصل می‌شوند، بسیار مهم است.

Port Security

Port Security یک ویژگی امنیتی در سوئیچ‌های شبکه است که به مدیران شبکه این امکان را می‌دهد که دسترسی به پورت‌های سوئیچ را کنترل و محدود کنند.

این ویژگی به‌ویژه برای جلوگیری از دسترسی غیرمجاز به شبکه و محافظت از پورت‌های فیزیکی سوئیچ در برابر حملات نظیر MAC Address Spoofing استفاده می‌شود. با فعال کردن Port Security، مدیران می‌توانند تنظیم کنند که هر پورت سوئیچ فقط به یک یا چند آدرس MAC خاص پاسخ دهد و از اتصال دستگاه های جدید یا ناشناخته جلوگیری کنند.

از جمله قابلیت‌های Port Security می‌توان به مواردی همچون محدود کردن تعداد آدرس‌های MAC که می‌توانند به هر پورت متصل شوند، فعال کردن عملکرد Sticky MAC (که به سوئیچ این امکان را می‌دهد که به طور خودکار آدرس‌های MAC دستگاه های متصل به پورت‌ها را یاد بگیرد و ذخیره کند) و فعال‌سازی اقدامات امنیتی مانند Shutdown (غیرفعال‌سازی پورت) یا Restrict (محدود کردن ترافیک به پورت) در صورت شناسایی آدرس‌های MAC غیرمجاز اشاره کرد.

Port Security به‌ویژه در شبکه های بزرگ و محیط‌های حساس امنیتی مفید است، زیرا با محدود کردن دسترسی به پورت‌ها می‌توان از اتصال دستگاه های غیرمجاز یا حملات احتمالی جلوگیری کرد. این ویژگی به مدیریت بهتر و امنیت بیشتر شبکه کمک می‌کند و باعث جلوگیری از سو استفاده از پورت‌ها و تهدیدات امنیتی ناشی از دستگاه های ناشناس می‌شود.

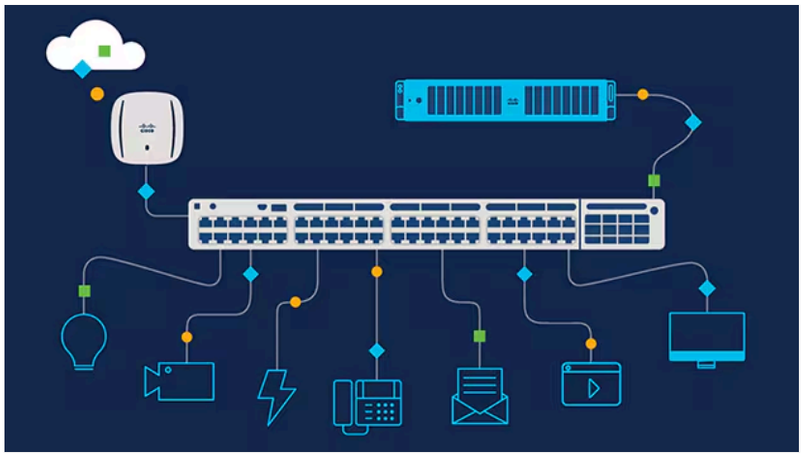
MAC Address Table

MAC Address Table که به آن Forwarding Table یا Content Addressable Memory (CAM) Table نیز گفته می‌شود، یک ساختار داده‌ای در سوئیچ‌های شبکه است که اطلاعات مربوط به آدرس‌های MAC دستگاه های متصل به پورت‌های مختلف سوئیچ را ذخیره می‌کند.

هر بار که یک فریم Ethernet وارد سوئیچ می‌شود، سوئیچ آدرس MAC مبدا فریم را در جدول MAC خود ذخیره کرده و از آن برای هدایت فریم‌های دریافتی به پورت صحیح استفاده می‌کند. این جدول به سوئیچ کمک می‌کند که فریم‌ها را به‌طور کارآمد و بدون نیاز به پخش آن‌ها به تمامی پورت‌ها، فقط به مقصد مناسب ارسال کند.

با توجه به اینکه سوئیچ‌ها از آدرس‌های MAC برای تصمیم‌گیری در مورد نحوه هدایت ترافیک استفاده می‌کنند، جدول MAC یک بخش اساسی از عملکرد سوئیچ است. هنگامی که سوئیچ یک فریم دریافتی را دریافت می‌کند، ابتدا بررسی می‌کند که آیا آدرس MAC مقصد در جدول موجود است یا خیر.

اگر آدرس MAC مقصد در جدول وجود داشته باشد، سوئیچ فریم را به پورت مناسب ارسال می‌کند. در غیر این صورت، سوئیچ فریم را به تمام پورت‌ها ارسال می‌کند تا دستگاه مقصد بتواند پاسخ دهد و آدرس MAC آن در جدول ذخیره شود. این فرآیند باعث بهبود کارایی شبکه و جلوگیری از پخش ترافیک غیرضروری می‌شود.



در این پست از پارس وب سرور با تعداد از اصطلاحات و مفاهیم مورد استفاده در سوئیچ شبکه آشنا شدیم.

از اینکه با ما همراه بودیم سپاسگزاریم.

به اشتراک بگذارید :

4.8/5 - (10 امتیاز)

اصطلاحات فنی سوئیچ کانفیگ سرور

منتظر نظرات ارزشمند شما هستیم. از شنیدن و خواندن دیدگاه شما خوشحال می‌شویم

نظر شما درباره این پست ...

نام *

ایمیل *

ارسال نظر

© - تمامی حقوق مادی و معنوی این وب سایت متعلق به پارس وب سرور می باشد. 2025