آموزش Security+ مقدمه

امنیت سامانه‌های کامپیوتری، تجهیزات سیار، شبکه‌ها کامپیوتری و گجت‌های اینترنت اشیا و هرگونه دستگاهی که قابلیت اتصال به شبکه را دارد از مباحث روز دنیای فناوری است. به‌طوری که متخصصان این حوزه مورد توجه شرکت‌ها و سازمان‌های مختلف قرار دارند. گسترش شبکه‌های ارتباطی و وابستگی آن‌ها به فناوری باعث شده تا تهدیدات روز افزونی هر روزه سازمان‌ها را با چالش جدی روبرو کند و همین مسئله نیاز به متخصصان حوزه امنیت را دوچندان کرده است. به‌طوری که سرمایه‌گذاری در این مسیر نه تنها اتلاف پول و زمان نیست، بلکه سرمایه‌گذاری روی آینده است.

سکوریتی پلاس چیست؟

برای پاسخ به این نیاز کسب‌وکارها و ترتیب نیروهایی متخصص و کارآزموده، شرکت‌ها اقدام به برگزاری دوره‌های آموزشی تخصصی کردند تا متخصصان به شکل جامع و فراگیر با مباحث مختلف این حوزه آشنا شوند. موسسه کامپتیا (CompTIA) نزدیک به بیست سال است که دوره‌های آموزشی مختلفی را برای علاقه‌مندان به دنیای فناوری ترتیب داده است. یکی از دوره‌های مورد توجه در این زمینه سکوریتی پلاس پلاس است که تا به امروز محبوب‌ترین دوره امنیتی نزد علاقه‌مندان بوده است. سکوریتی پلاس یک گواهینامه جهانی است که مهارت‌های پایه لازم برای انجام وظایف اصلی امنیتی و دنبال کردن حرفه‌ای حوزه امنیت فناوری اطلاعات را تضمین می‌کند. به بیان دقیق‌تر، سکوریتی‌پلاس دری به روی دنیای حرفه‌ای امنیت سایبری باز می‌کند.

چرا سکوریتی پلاس متفاوت از سایر مدارک حوزه امنیت است؟

سکوریتی‌پلاس از جمله گواهینامه‌هایی است که بیش از هر گواهینامه دیگری در بازار کار موردتایید است و مهارت‌های امنیتی پایه آموزش داده شده در این دوره منطبق با DoD 8570 است. به همین دلیل است که شرکت‌های بزرگ و حتا مراکز نظامی این گواهیامه را به رسمیت شناخته‌اند Security+ .مهارت‌های عملی متخصصان را تایید می‌کند، زیرا تنها گواهینامه پایه امنیت سایبری که بر مهارت‌های عملی تأکید دارد و تضمین می‌کند که متخصص امنیتی برای حل مشکلات و طیف گسترده‌تری از مسائل پیچیده امروزی آمادگی لازم را دارد. علاوه بر این، به افراد این شانس را می‌دهد تا برای مشاغل مرتبط با حوزه امنیت درخواست خود را ارسال کنند، زیرا افراد با دانستن مهارت‌های پایه امنیت سایبری به شکل بهتری قادر به محافظت از سیستم‌ها، نرم‌افزار و سخت‌افزارها خواهند بود. سکوریتی‌پلاس با تمرکز بر جدیدترین گرایش‌ها و روندهای حوزه امنیت سعی می‌کند،

مهم‌ترین مهارت‌های فنی در ارزیابی و مدیریت ریسک، پاسخ به حادثه، جرم‌شناسی دیجیتال، محافظت از شبکه‌های سازمانی، عملیات ترکیبی/ابر و کنترل‌های امنیتی را پوشش دهد تا افراد در زمان بروز مشکلات امنیتی یا قبل از آن به محافظت از زیرساخت‌های یک سازمان بپردازند.

مدت زمان برگزاری این دوره و مدت زمان این دوره

به‌طور معمول، دوره سکوریتی پلاس در ایران در یک بازه ۳۰ تا ٤٠ ساعته برگزار می‌شود و اولین نقطه آشنایی متخصصان فناوری اطلاعات با مباحث امنیتی است. به بیان دقیق‌تر اگر به دنبال آن هستید تا شغل مناسبی در دنیای امنیت به دست آورید، در اولین گام باید به فکر یادگیری سکوریتی پلاس باشید. این دوره دانش پایه لازم در ارتباط با مباحث مختلف حوزه امنیت را ارایه می‌کند و عملکردی یکسان با نتورک‌پلاس دارد، با این تفاوت که دوره نتورک‌پلاس روی مباحث پایه‌ای و مهم شبکه متمرکز است، در حالی که سکوریتی‌پلاس روی مباحث پایه‌ای حوزه امنیت متمرکز است. این دوره با تمرکز بر مهارت‌های عملی سعی می‌کند دانش‌پژوهان را برای حل انواع مسائل حوزه امنیت آماده کند. به همین دلیل سرفصل‌های این دوره به نوعی برنامه‌ریزی شده‌اند که بر جدیدترین روندهای و تکنیک‌ها مدیریت ریسک، کاهش خطر، مدیریت تهدید و تشخیص نفوذ تاکید دارد. افرادی که قصد شرکت در این دوره را دارند باید در یک آزمون ۹۰ دقیقه‌ای شرکت کنند و حداقل امتیاز ۷۵۰ از ۹۰۰ را کسب کنند.
در حال حاضر جدیدترین گواهینامه سکوریتی‌پلاس نسخه SY0-601 است که در سراسر جهان آموزش داده می‌شود.

چرا دوره کامپتیا سکوریتی‌پلاس

دوره کامپتیا Security+ پیش‌نیاز بیشتر مدارک بین‌المللی حوزه امنیت است و نقطه شروع مباحث امنیتی است، بنابراین، افراد بدون آگاهی در ارتباط با مباحث امنیتی قادر به شرکت در این دوره هستند، زیرا همه چیز از پایه آموزش داده می‌شود، با این‌حال، برای ورود به این دوره و درک مباحث مطرح شده باید حداقل دانش لازم در ارتباط با مباحث اولیه حوزه فناوری اطلاعات و به ویژه شبکه را داشته باشید. بنابراین پیشنهاد می‌شود ابتدا به فکر دریافت مدرک نتورک‌پلاس باشید و در ادامه به سراغ مدرک سکوریتی‌پلاس بروید. از آن‌جایی که بخش عمده‌ای از منابع این دوره به زبان انگلیسی است، دانشجویان باید توانایی خواندن و درک مطلب مباحث به زبان انگلیسی را داشته باشند.

سایت شبکه چگونه آموزش می‌دهد؟

همان‌گونه که اشاره کردیم، بخش عمده‌ای از مطالب به زبان انگلیسی هستند و علاقه‌مندان باید قادر به درک مباحث به زبان انگلیسی باشند، اما کاری که ما در سایت شبکه انجام می‌دهیم، آموزش این مباحث به زبان پارسی است. علاوه بر این، هر کجایی که برگردانی از مباحث را ارایه کنیم در کنار آن معادل انگلیسی مطالب را نیز قرار می‌دهیم تا همزمان با هر دو اصطلاح آشنا باشید. در این دوره علاقه‌مندان با مفاهیم و اصول اولیه:

- امنیت
- مهارت‌های ویژه برای پیاده‌سازی خدمات امنیتی
- شناسایی انواع تهدیدات امنیتی آشنا می‌شوند

اما علاوه بر این، مباحث پیشرفته‌تری نیز در سایت شبکه مورد توجه قرار می‌گیرد تا علاقه‌مندان فارغ از دوره‌ای که قصد شرکت در آن‌را دارند با مباحث به شکل دقیق‌تری آشنا شوند.

علاقه‌مندان به دوره سکوریتی‌پلاس پس از مطالعه این دوره چه مهارت‌هایی به‌دست می‌آورند؟

به‌طور معمول، هنگامی که تصمیم می‌گیرید در دوره‌ای شرکت کنید یا مباحث دوره‌ای را به مثل سکوریتی‌پلاس را به شکل رایگان بیاموزید، به دنبال افزایش اندوخته‌های فنی خود هستید. از جمله مباحثی که پس از مطالعه این دوره یاد خواهید گرفت باید به آشنایی با اصول و مفاهیم اولیه امنیت، پیاده‌سازی خدمات امنیتی مبتنی بر استانداردها، شناسایی انواع تهدیدات امنیتی، مدیریت ریسک، آشنایی با امنیت شبکه‌های بی‌سیم، موبایل و فضای ابری، آشنایی با مفاهیم رمزنگاری، آشنایی با تایید اعتبار و مجوزها، شناخت استراتژی‌های لازم برای اطمینان از عملکرد صحیح شبکه، تحمل خطا و بازیابی آن در زمان بروز مشکل، پیاده‌سازی معماری‌های ایمن شبکه و.... اشاره کرد.

دوره آموزش Security+ برای چه افرادی مناسب است؟

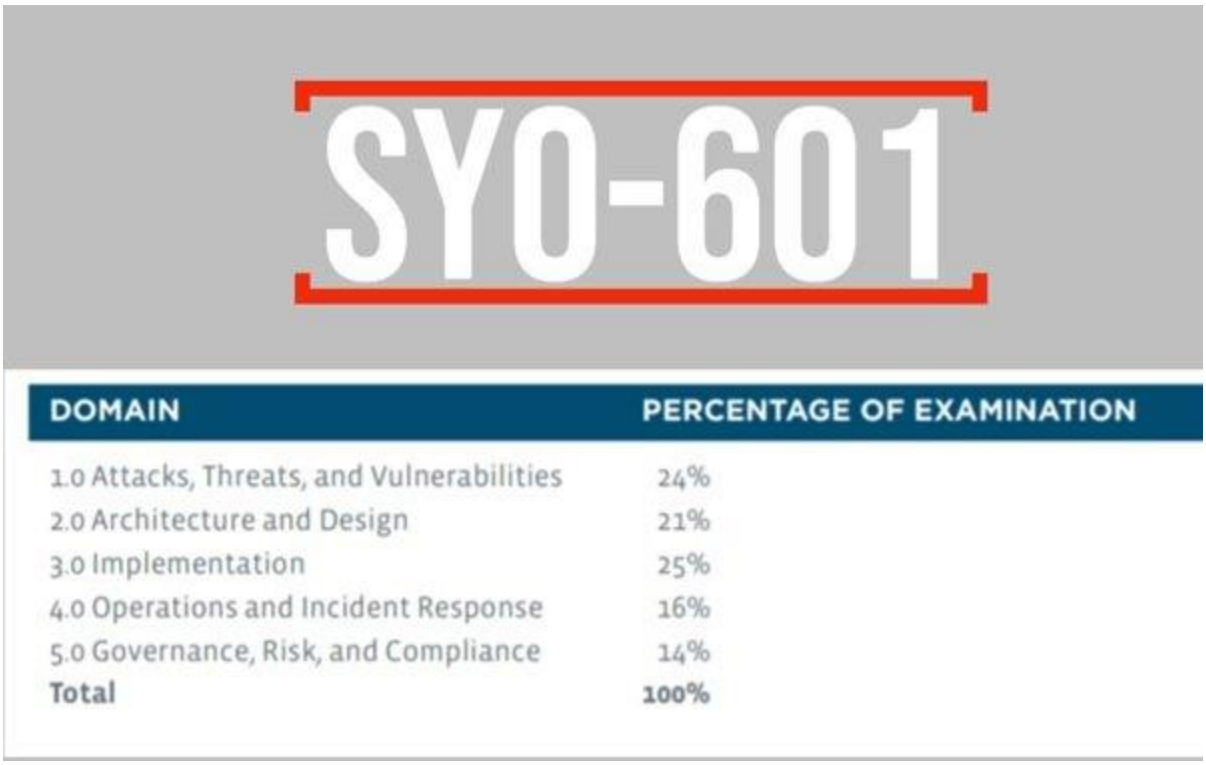
به‌طور معمول، تمامی علاقه‌مندان به مباحث امنیت و شبکه، متخصصان شبکه، کارشناسان مخابرات، مدیران شبکه شرکت‌ها و سازمان‌های دولتی و خصوصی، افرادی که علاقه‌مند به مشاغل حوزه امنیت هستند و افرادی که دوست دارند در ادامه به هکر کلاه سفید تبدیل شده و به سراغ مدارک دیگری مثل CEH و تست نفوذ بروند از مخاطبان اصلی این دوره هستند.

دوره SY0-601 چه تفاوتی با دوره SY0-501 دارد؟

دوره SY0-501 تضمین می‌دهد که داوطلب دانش و مهارت‌های لازم برای نصب و پیکربندی سیستم‌ها با هدف ایمن‌سازی برنامه‌های کاربردی، شبکه‌ها و دستگاه‌ها را به‌دست آورده است.

Domain	% of Examination
1.0 Threats, Attacks and Vulnerabilities	21%
2.0 Technologies and Tools	22%
3.0 Architecture and Design	15%
4.0 Identity and Access Management	16%
5.0 Risk Management	14%
6.0 Cryptography and PKI	12%
Total	**100%**

انجام تجزیه و تحلیل تهدید و پاسخ‌گویی با تکنیک‌های کاهش مناسب از جمله مباحثی است که این دوره به علاقه‌مندان آموزش می‌دهد. آشنایی با خط‌مشی‌های امنیتی، پیاده‌سازی استراتژی‌هایی با هدف کاهش مخاطرات و آگاهی از خط‌مشی‌ها و نحوه مقابله با تهدیدات از جمله مباحث کلی هستند که دوره فوق روی آن‌ها متمرکز است. به بیان ساده، این دوره به افراد آموزش می‌دهد که چگونه اصول سه‌گانه دسترس‌پذیری، یکپارچگی و صحت اطلاعات را حفظ کنند. دوره SY0-601 ضمن حفظ نکاتی که به آن‌ها اشاره شد، به دواطلب دانش و مهارت‌های لازم برای ارزیابی وضعیت امنیتی یک محیط سازمانی و توصیه و اجرای راه‌حل‌های امنیتی را آموزش می‌دهد.



علاوه بر این، روی محیط‌های ترکیبی از جمله ابر، موبایل و اینترنت اشیا و نحوه نظارت و ایمن‌سازی آن‌ها متمرکز است. با آگاهی از قوانین و خط‌مشی‌های قابل اجرا از جمله اصول حاکمیتی، ریسک و انطباق، شناسایی و تجزیه و تحلیل و پاسخگویی به رویدادها و حوادث امنیتی به افراد آموزش می‌دهد که چگونه به مقابله با مخاطرات امنیتی بپردازند.

سرفصل‌های دوره Security+ چه مباحثی را شامل می‌شود؟

به‌طور معمول، کامپتیا در بازه‌های زمانی مختلف بارم‌ها و نمرات هر یک از عناوین این دوره را تغییر می‌دهد. از مهم‌ترین سرفصل‌های این دوره به موارد زیر باید اشاره کرد:

- آشنایی با تهدیدات، حمله‌ها و آسیب‌پذیری‌های(24%)
- معماری و طراحی(21%)
- پیاده‌سازی(25%)
- عملیات و واکنش حوادث(16%)
- حاکمیت، ریسک و انطباق(14%)

در این دوره آموزشی قصد داریم؛ شما را با تعریف امنیت و شناخت انواع مختلف تهدیدات، بررسی اصطلاحات AAA و CIA در امنیت، انواع هکرها، شناخت تهدیدهای امنیت سایبری، انواع مختلف بدافزارها ها و نحوه پیشگیری از آلوده شدن سامانه‌ها به آن‌ها از طریق به‌کارگیری ابزارهای مختلف در سطح سیستم‌عامل‌های ویندوز، لینوکس و نرم‌افزارهای جانبی، پیاده‌سازی امنیت در سطح لایه کاربرد، آشنایی با سامانه‌های تشخیص نفوذ(IDS) ، پیشگیری از نفوذ (IPS) و روش‌های ایمن‌سازی زیرساخت‌های ارتباطی از طریق به‌کارگیری ابزارهای فوق، بررسی مفهوم DLP و انواع آن جهت پیشگیری از خروج اطلاعات، بررسی انواع روش‌های امنیتی در سطح سخت‌افزارها، امنیت در سطح شبکه‌های سیار و بی‌سیم، بررسی مفهوم Hardening در سطح سیستم‌عامل و بستر مجازی‌سازی (جهت پاکسازی سرویس‌ها و برنامه‌ها، بررسی نرم‌افزارهای تحلیل امنیت در سطح یک سیستم یا شبکه، بررسی روش‌های امنیتی در سطح مرورگرها، آشنایی با پروکسی سرور و انواع آن، انواع تهدیدات در سطح برنامه‌نویسی، آشنایی با استانداردOSI ، بررسی دستگاه‌های مختلف و نحوه عملکرد آن‌ها در سطح لایه‌های مختلف، آشنایی با انواع دیوارهای آتش سخت‌افزاری و نرم‌افزاری، بررسی NAC ServerوVLAN ، بررسی انواع تهدیدات پیرامون پروتکل‌ها و نحوه پیشگیری از بروز مخاطرات امنیتی از طریق آن‌ها با استفاده از دیوارآتش یا ابزارهای جانبی، بررسی شبکه DMZ و نحوه راه‌اندازی آن، بررسی انواع دیوارآتش، پروکسی با هدف پیشگیری از نفوذ، بررسیUTM ها و نحوه عملکرد آن‌ها، آشنایی با امنیت در سطح دستگاه‌های مختلف، بررسی انواع پروتکل‌های امنیتی در سطح شبکه‌های بی‌سیم، انواع روش‌های تایید اعتبار کلاینت‌ها در شبکه یا ابر، بررسی پروتکل‌هایKerberos ، LDAP, RADIUSو انواع روش‌های دسترسی به اطلاعات، نحوه تخصیص مجوز دسترسی (Permission) به گروه‌ها و کاربران، بررسی ابزارهای شناسایی تهدیدات در سطح شبکه، بررسی ابزارهای مانیتورینگ و گزارش‌گیری و ممیزی (Auditing) جهت مانیتور و ممیزی کاربران در سطح شبکه، بررسی نرم‌افزارهای جانبی جهت ممیزی کاربران در سطح لینوکس و ویندوز و بررسیSyslog Server ، آشنایی با روش‌های امنیتیPKI ، نحوه عملکردCA Server ، نحوه پیاده‌سازی تحمل خرابی و تقسیم کار در سطح مختلف شبکه مانند سرورها، Storageو غیره آشنا کنیم.

آشنایی با مبانی و اصطلاحات شبکه بخش ۰۱

کارشناسان امنیت با هدف محافظت از سامانه‌ها و زیرساخت‌ها استخدام می‌شوند، بنابراین مهم است که یک کارشناس امنیت با مباحث اولیه شبکه آشنایی داشته باشد. بر همین اساس، در دوره

سکوریتی‌پلاس به شکل فشرده مباحث مهم و زیربنایی شبکه آموزش داده می‌شود. بدیهی است برای تسلط بر مباحث جدی‌تر شبکه باید به سراغ دوره‌های تخصصی‌تری مثل نتورک‌پلاس یا CCNA R&S بروید. از مباحث مهم شبکه که باید بر آن‌ها مسلط شوید باید به آشنایی با تجهیزات شبکه و کابل‌کشی و مباحث مرتبط با TCP/IP اشاره کرد. مباحثی که اجازه می‌دهند به شکل بهتری راه‌حل‌های امنیت شبکه را پیاده‌سازی کنید.

برای آمادگی برای حضور در آزمون گواهینامه سکوریتی‌پلاس به اطلاعات دقیقی در مورد شبکه، تجهیزات شبکه و پروتکل‌ها نیاز دارید. در چند شماره آینده، به بررسی اصول اولیه شبکه خواهیم پرداخت تا اطمینان حاصل کنیم نه تنها با عملکرد دستگاه‌هایی مانند سوئیچ‌ها و روترها آشنا هستید، بلکه اصول اولیه مربوط به پروتکل‌های زیربنایی پروتکل TCP/IP را نیز درک کرده‌اید. همان‌گونه که اشاره کردیم، در این مجموعه آموزش قرار نیست به سراغ مباحث کامل شبکه برویم، زیرا خود به تنهایی یک دوره آموزشی کامل است. بنابراین پیشنهاد می‌کنیم در صورت تمایل دوره آموزش Network+را مطالعه کنید.

آشنایی با دستگاه‌های شبکه و کابل‌کشی

اجازه دهید اصول زیربنایی محیط‌های شبکه را با مروری کلی بر دستگاه‌های شبکه و کابل‌کشی آغاز کنیم. ممکن است در آزمون Security+ به شکل مستقیم پرسش‌هایی در این زمینه را مشاهده نکنید، اما هنگامی که صحبت از امنیت به میان می‌آید باید با مفاهیم امنیتی مرتبط با دستگاه‌ها و کابل‌های شبکه آشنا باشید.

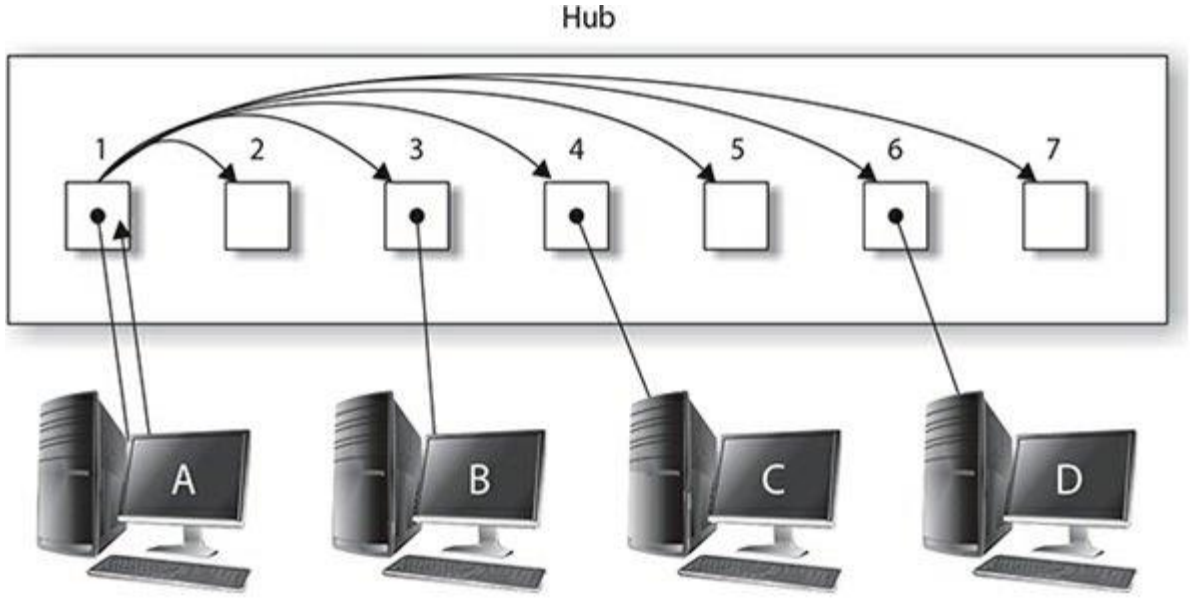
نگاهی به دستگاه‌های شبکه

افرادی که به عنوان کارشناس امنیت جذب سازمان‌ها می‌شوند مجبور هستند برای انجام هرچه بهتر کارهای خود با عملکرد تجهیزات مختلف شبکه آشنا باشند. به‌طور مثال، ممکن است از شما خواسته شود که یک ممیزی امنیتی در یک سازمان انجام دهید که شامل شناسایی دستگاه‌های مورد استفاده در شرکت و ارائه توصیه‌هایی در مورد ایمن‌تر کردن دستگاه‌ها باشد.

هاب(Hub)

هاب شبکه یکی از دستگاه‌های قدیمی است که که برای اتصال همه سیستم‌ها به یکدیگر در یک محیط شبکه استفاده می‌شد. هاب یک دستگاه لایه اول یا همان لایه فیزیکی در مدل مرجع OSI است که به سادگی یک سیگنال را از یک سیستم دریافت می‌کند و سپس سیگنال را به تمام پورت‌های دیگر روی هاب ارسال می‌کند. به‌طور مثال، با نگاهی به شکل زیر مشاهده می‌کنید وقتی کامپیوتر A داده‌ها را

به کامپیوتر C ارسال می‌کند، داده ها در پورت ۱ هاب دریافت می‌شود و سپس به تمام پورت‌های دیگر ارسال می‌شود.

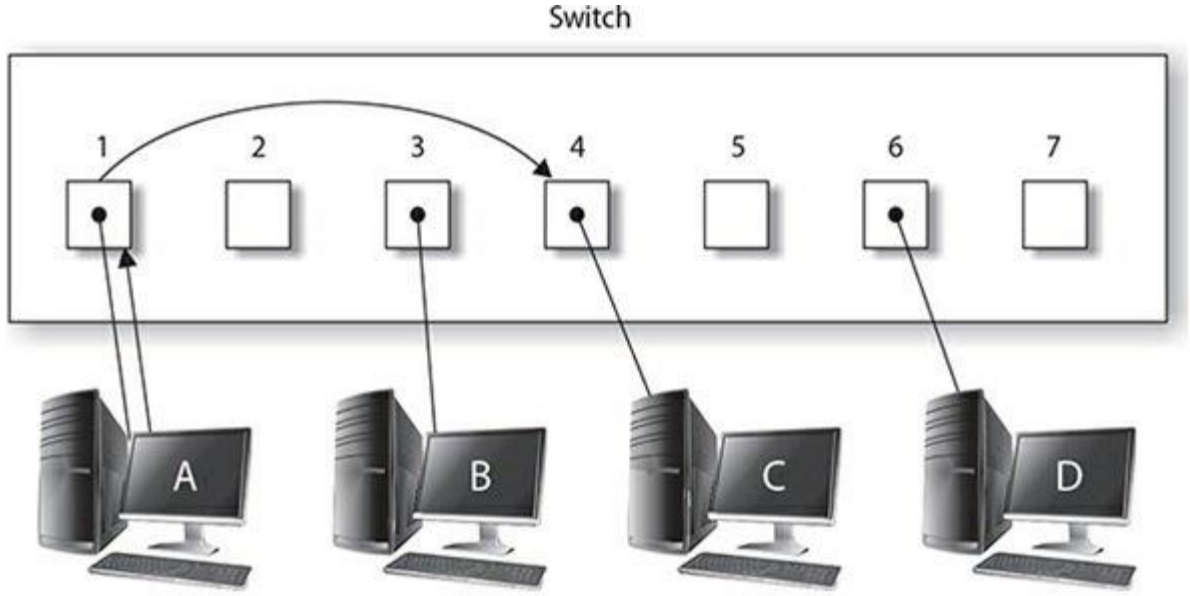


نقطه ضعف هاب این است که با ارسال داده‌ها به هر پورت روی هاب از پهنای باند بدون دلیل استفاده می‌کند. اگر داده‌ها فقط برای رایانه C ارسال شوند، چرا باید کار اضافی انجام شود؟ اشکال دیگر هاب شبکه این است که اگر همه سیستم‌های موجود در شبکه داده‌ها را دریافت کنند، یک مشکل امنیتی جدی به وجود می‌آید، در حالی که این احتمال وجود دارد که سایر گره‌های شبکه داده‌ها را نادیده بگیرد، زیرا برای آن‌ها ارزش یا مفهومی ندارد، اما ممکن است ناخواسته اطلاعات مهمی در دسترس افراد غیر مرتبط قرار بگیرد. در تصویر بالا رایانه‌های B و D می‌توانند تمام ترافیک شبکه را مشاهده کنند زیرا آن ایستگاه‌ها یک کپی از ترافیک را نیز دریافت می‌کنند. این موضوع یک چالش امنیتی بزرگ است و به همین دلیل است که هاب از دنیای فناوری کنار گذاشته شد و جای خود را به دستگاه دیگری به‌نام سوئیچ داد.

سوییچ

سوئیچ شبکه شبیه هاب شبکه است، زیرا برای اتصال همه سیستم‌ها به یکدیگر در یک محیط شبکه استفاده می‌شود، اما یک تفاوت مشهود دارد. در حالت کلی سوئیچ یک دستگاه لایه ۲ است که ترافیک را با مک‌آدرس تجهیزات فیلتر می‌کند و به همنی دلیل در لایه پیوند داده‌ها کار می‌کند. البته سوییچ‌های لایه ۳ نیز وجود دارند که مبتنی بر آدرس آی‌پی هستند و در لایه شبکه کار می‌کنند و قیمت بیشتری نسبت به سوییچ‌های لایه ۲ دارند، با این‌حال، در متون مختلف از سوییچ به عنوان لایه ۲ توصیف می‌شود. نکته‌ای که شاید در آزمون نتورک‌پلاس نیز به شما کمک کند توجه به این نکته است که آدرس لایه ۲ به عنوان آدرس کنترل دسترسی رسانه یا به اختصار مک‌آدرس (MAC) نیز شناخته

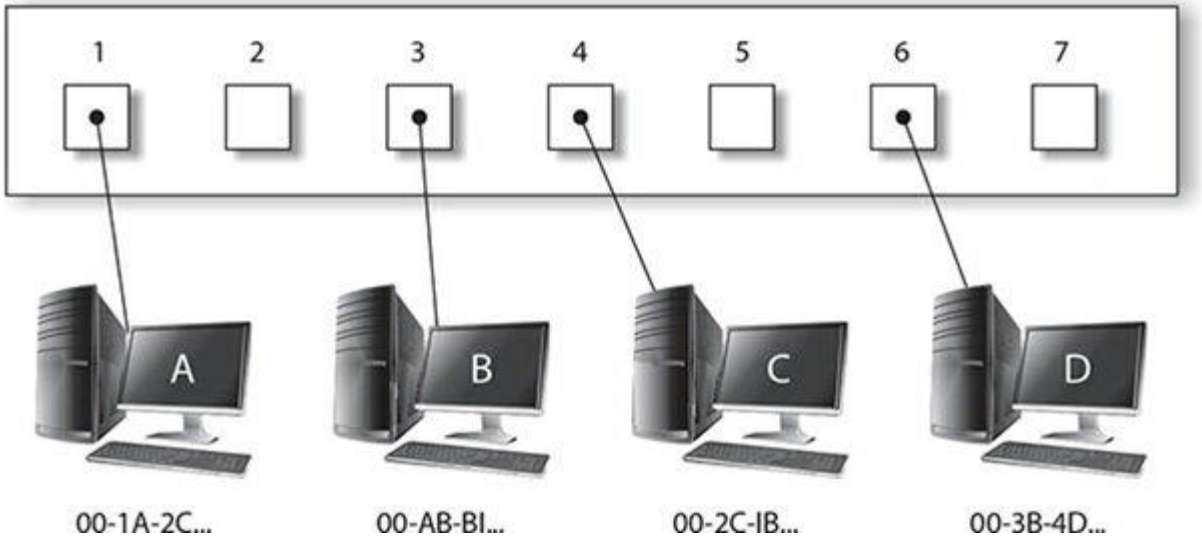
می شود Mac Address .یک آدرس سخت‌افزاری است که توسط سازنده به کارت شبکه اختصاص داده می‌شود و فرمتی شبیه به ۳ C-97-0E-E3-52-5Cدارد.
اجازه دهید به مثال قبل باز گردیم که کامپیوتر A قصد داشت داده‌ها را برای کامپیوتر C ارسال کند. اکنون به جای هاب از یک سوییچ استفاده می‌کنیم. سوییچ به واسطه عملکرد هوشمندانه‌ای که دارد متوجه می‌شود که باید داده‌ها را از رایانه A دریافت کند، بر مبنای مک‌آدرس دستگاه داده‌ها را تنها برای پورت مقصد که در این‌جا شماره ٤ است ارسال کند. شکل زیر عملکرد سوییچ را نشان می‌دهد.



یکی از ویژگی‌های شاخص سوئیچ توانایی در فیلتر کردن ترافیک است، زیرا با نگاه کردن به مک‌آدرس هر دستگاه متصل به سوئیچ و بررسی این موضوع که چه سیستمی به چه پورتی متصل است، اطلاعات مربوط به دستگاه‌ها را درون جدول مک‌آدرس ذخیره‌سازی می‌کند. مک‌آدرس جدولی است که در حافظه سوئیچ ذخیره می‌شود و مسئول پیگیری وضعیت پورت‌هایی است که هر سیستم به آن متصل است. در شکل زیر مشاهده می‌کنید که چگونه سوییچ تناظری میان پورت‌ها و مک‌آدرس‌ها برقرار می‌کند، به‌طوری که می‌داند به هر پورت سوییچ چه دستگاهی با چه مک‌آدرسی متصل شده است.

MAC address table

MAC	Port
00-1A-2C...	1
00-AB-BI...	3
00-2C-IB...	4
00-3B-4D...	6



علاوه بر فیلتر کردن ترافیک با ارسال داده‌ها تنها برای پورتی که سیستم مقصد به آن متصل است، سوئیچ‌های شبکه مزایای زیر را ارائه می‌دهند:

■همان‌گونه که اشاره شد، اصلی‌ترین وظیفه یک سوییچ فیلتر کردن ترافیک است تا همه گره‌های تحت شبکه توانایی مشاهده اطلاعات محرمانه را نداشته باشند.

Port Mirroring Port Mirroring ■که به‌نام ناظر پورت پورت نیز شناخته می‌شود، یکی دیگر از ویژگی‌های برجسته سوئیچ‌ها است که به سرپرست شبکه اجازه می‌دهد ترافیک را از سایر درگاه‌ها به یک درگاه مقصد (معروف به درگاه نظارت) کپی کند. از آن‌جایی که سوئیچ به‌طور پیش‌فرض ترافیک را فیلتر می‌کند، مدیر نمی‌تواند ترافیک شبکه را نظارت کند. بنابراین تولیدکنندگان سوئیچ‌ها باید راهی برای کپی کردن تمام ترافیک در یک پورت ارائه کنند تا مدیر بتواند نظارت دقیقی روی پورت‌ها اعمال کند. به‌طور مثال، از دستورات زیر برای پیکربندی پورت ۱۲ سوییچ برای نظارت بر ترافیک ارسالی یا دریافتی در پورت‌های ۱ تا ۵ استفاده می‌شود:

```
HAL-SW1(config)#interface fastethernet 0/12
HAL-SW1(config-if)#port monitor fastethernet 0/1
HAL-SW1(config-if)#port monitor fastethernet 0/2
HAL-SW1(config-if)#port monitor fastethernet 0/3
HAL-SW1(config-if)#port monitor fastethernet 0/4
HAL-SW1(config-if)#port monitor fastethernet 0/5
```

■یکی از ویژگی‌های خوب سوئیچ شبکه امنیت پورت است که به شما امکان می‌دهد Port Security: یک پورت را برای یک مک‌آدرس خاص پیکربندی کنید. رویکرد فوق به شما در کنترل این موضوع که کدام سیستم‌ها می‌توانند به آن پورت روی سوئیچ متصل شوند کمک می‌کند. هنگامی که یک سیستم غیرمجاز به پورت سوئیچ متصل می‌شود، سوئیچ می‌تواند به طور موقت پورت را غیرفعال کند تا زمانی که سیستم معتبری به سوئیچ وصل شود یا پورت را غیرفعال کند تا زمانی که مدیر شبکه پورت را مجدداً فعال کند. دستورات زیر برای پیکربندی پورت ٦ در سوئیچ Halifax استفاده می‌شود تا اتصالات از یک مک‌آدرس خاص را دریافت کند. در این مثال، مک آدرس aaaa.bbbb.cccc است که می‌توانید آن را با یک مک‌آدرس واقعی جایگزین کنید:

```
HAL-SW1(config)#interface fastethernet 0/12
HAL-SW1(config-if)#port monitor fastethernet 0/1
HAL-SW1(config-if)#port monitor fastethernet 0/2
HAL-SW1(config-if)#port monitor fastethernet 0/3
HAL-SW1(config-if)#port monitor fastethernet 0/4
HAL-SW1(config-if)#port monitor fastethernet 0/5
```

■قابلیت غیرفعال کردن پورت‌ها، اگر پورت‌هایی روی سوئیچ وجود دارند که کاربرد ندارند، ایمن‌ترین روش غیرفعال کردن آن‌ها است. دستورات زیر برای غیرفعال کردن پورت‌های ۷ تا ۱۲ در سوئیچ سیسکو با دستور shutdown استفاده می‌شود:

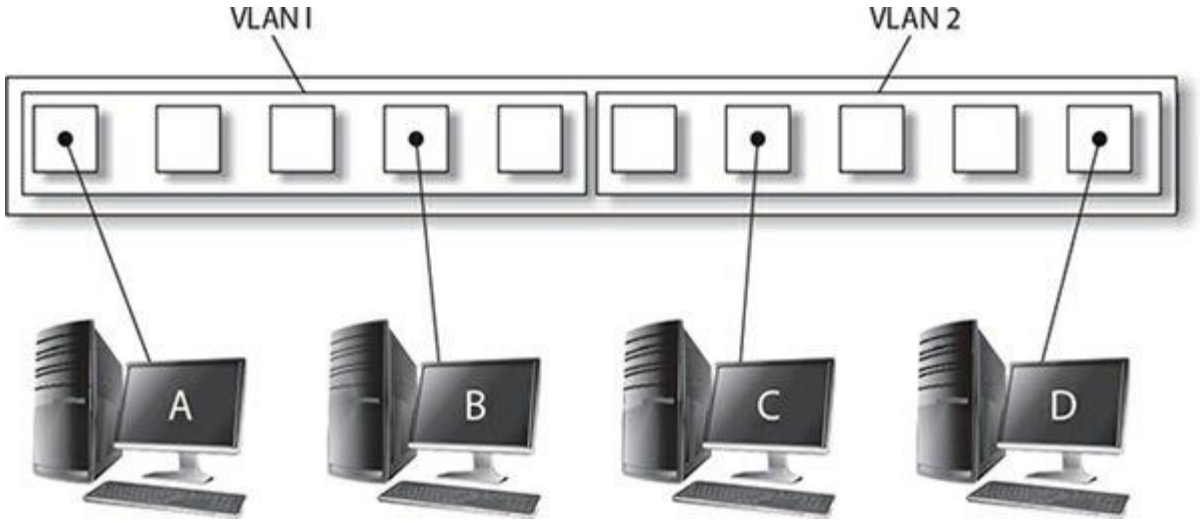
```
HAL-SW1(config)#interface range f0/7–12
HAL-SW1(config-if-range)#shutdown
```

نکته :آزمون Security+ از شما انتظار ندارد تا فرمان‌های پیکربندی امنیتی پورت‌ها یا غیرفعال کردن یک پورت در سوئیچ سیسکو را بدانید، اما انتظار دارد که ویژگی‌های امنیتی سوئیچ‌ها را درک کرده باشید.
دامنه‌های برخورد :(Collision Domains) یکی دیگر از ویژگی‌های مهم سوئیچ دامنه برخورد است که اشاره به گروه‌بندی سامانه‌هایی دارد که همگی به یک بخش یکسان از شبکه تعلق دارند. به بیان دقیق‌تر، دامنه برخورد به حالتی اشاره دارد که تجهیزات عضو آن دامنه ممکن است با مشکل تصادم داده‌های خود روبرو شوند که باعث از دست رفتن داده‌ها می‌شود. به‌طور معمول، پورت‌های یک هاب یک دامنه برخورد واحد دارند، اما هر پورت روی یک سوئیچ یک دامنه برخورد جداگانه دارد. به‌طور مثال،

هنگام استفاده از یک هاب شبکه اگر قرار باشد دو سیستم همزمان داده‌ها را ارسال کنند، بسته‌های اطلاعاتی با یکدیگر برخورد می‌کنند. مشکل فوق به این دلیل به وجود می‌آید که هاب یک بخش شبکه مشترک ایجاد می‌کند که همه سیستم‌ها به آن دسترسی دارند. هنگامی که از یک سوئیچ استفاده می‌کنید، هر پورت روی سوئیچ یک دامنه برخورد مجزا ایجاد می‌کند که سگمنت خاص خود در شبکه را دارد. هنگام اتصال یک سیستم به پورتی روی یک سوئیچ، به دلیل این‌که هیچ سیستم دیگری در سگمنت شبکه به آن پورت متصل نخواهد بود، مشکل برخورد داده‌ها به وجود نخواهد آمد.
نکته :برای آزمون سکوریتی‌پلاس به یاد داشته باشید که سوئیچ‌ها امنیت خوبی را ارائه می‌دهند، زیرا با ارسال ترافیک فقط به پورتی که سیستم مقصد به آن تعلق دارد، ترافیک را فیلتر می‌کند. همچنین باید بتوانید ویژگی‌هایی مانند امنیت پورت، Port Mirroringو قابلیت غیرفعال کردن پورت‌های بدون استفاده را شرح دهید.

شبکه محلی مجازی

امروزه بیشتر سوییچ‌ها از ویژگی معروف شبکه محلی مجازی (VLAN) پشتیبانی می‌کنند. هدف از به‌کارگیری یک VLAN ساخت چند شبکه در یک سوئیچ است. یکی از راه‌های انجام این‌کار، قرار دادن پورت‌های روی سوئیچ در گروه‌های VLAN است. در این حالت هنگامی که یک سیستم به پورت سوئیچ متصل می‌شود، عضوی از VLAN می‌شود که پورت با آن مرتبط است. نکته مهم در این جا این است که وقتی یک سیستم عضو یک VLAN باشد، نمی‌تواند با سیستم‌های عضوVLAN های دیگر ارتباط برقرار کند. به بیان دقیق‌تر، هر VLAN سوئیچ مخصوص به خود را دارد و با سوییچ دیگری مرتبط نیست. شکل زیر سوئیچی را نشان می‌دهد که دو VLAN در آن پیکربندی شده‌اند. در این مثال، کامپیوتر A فقط می‌تواند با کامپیوتر B ارتباط برقرار کند، زیرا آن‌ها تنها سیستم‌های VLAN1 هستند. کامپیوتر A و کامپیوتر B نمی‌توانند با کامپیوتر C و کامپیوتر D ارتباط برقرار کنند، زیرا ارتباط بین VLAN ها بدون روتر ممکن نیست.



قطعه کد زیر نشان می‌دهد که چگونه باید شبکه‌های محلی مجازی را روی سوییچ کاتالیست سیسکو پیکربندی کنید. در مثال فوق دو شبکه محلی مجازی PrivateLAN و WebServers را مشاهده می‌کنید.

```
HAL-SW1>enable
HAL-SW1#config term
HAL-SW1(config)#vlan 2
HAL-SW1(config-vlan)#name PrivateLAN
HAL-SW1(config-vlan)#exit
HAL-SW1(config)#vlan 3
HAL-SW1(config-vlan)#name WebServers
HAL-SW1(config-vlan)#exit
```

هنگامی که شبکه‌های محلی مجازی ساخته می‌شوند، در ادامه می‌توانید پورت‌های مختلفی را به شبکه‌های محلی خاص اختصاص دهید. به‌طور مثال، با استفاده از دستورات زیر می‌توانید پورت‌های ۱۸ تا ۲٤ را به WebServer VLAN اختصاص دهید.

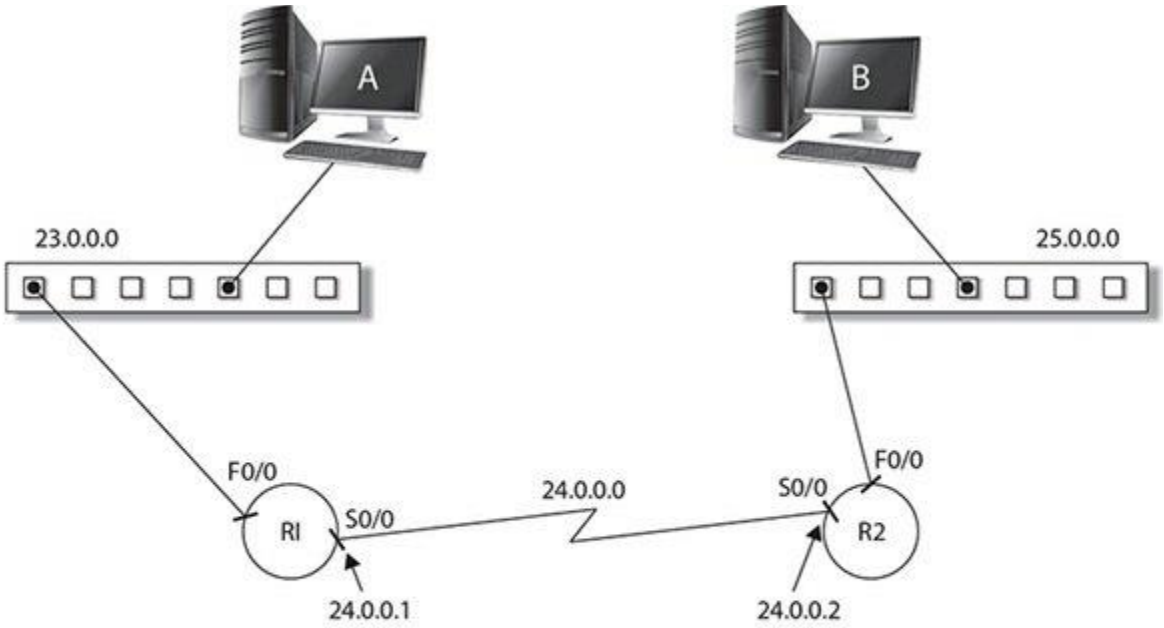
```
HAL-SW1(config-if-range)#interface range f0/18 – 24
HAL-SW1(config-if-range)#switchport access vlan 3
```

لازم به ذکر است که شما می‌توانید چند سوئیچ را به هم متصل کنید و VLAN را در تمام سوئیچ‌ها ایجاد کنید. به عنوان مثال، می‌توانید چند پورت روی هر یک از سوئیچ‌های ۱، ۲ و ۳ که بخشی از WebServers VLANهستند، داشته باشید. پورت uplink که سوئیچ‌ها را به هم متصل می‌کند، ترافیک VLANرا به هر سوییچ منتقل می‌کند.

نکته: برای آزمون، به یاد داشته باشید کهVLAN ها راهی برای ایجاد مرزهای ارتباطی در شبکه هستند. به‌طور پیش‌فرض، سیستم‌های عضو یک VLAN نمی‌توانند با سیستم‌های موجود در VLAN دیگر ارتباط برقرار کنند، مگر با استفاده از روتر.

Router

روتر یک دستگاه لایه ۳ یا همان لایه شبکه است که وظیفه مسیریابی یا ارسال داده‌ها از یک شبکه به شبکه دیگر را بر عهده دارد. روتر از یک جدول مسیریابی که درون حافظه روتر قرار دارد استفاده می‌کند تا شبکه‌هایی را که می‌داند چگونه داده‌ها را برای آن‌ها ارسال کند، تعیین کند. شکل زیر توپولوژی شبکه و جدول مسیریابی روتر را نشان می‌دهد. در شکل زیر برای این‌که روتر R1 داده‌ها را به شبکه ۲۵٫۰٫۰٫۰ ارسال کند، باید داده‌ها را همانطور که در جدول مسیریابی نشان داده شده است به آدرس ۲٤٫۰٫۰٫۲ ارسال کند.



Routing table

Network	Path
23.0.0.0	F0/0
24.0.0.0	S0/0
25.0.0.0	24.0.0.2

فهرست زیر جدول مسیریابی روتر سیسکو را با استفاده از دستور show ip route نمایش می‌دهد. اگر به فهرست مذکور دقت کنید متوجه می‌شوید که سه مسیر وجود دارد. مسیرهای شبکه ۲۳/۰/۰/۰ و ۲٤/۰/۰/۰ شناخته شده هستند زیرا روتر به آن شبکه‌ها متصل است) به C در سمت چپ توجه کنید .(همچنین یک مسیر ثابت) کدS ، در سمت چپ (که مدیر اضافه کرده است، پیکربندی شده است تا داده‌ها را به سیستم ۲٤/۰/۰/۲ ارسال کند تا به شبکه ۲۵/۰/۰/۰ برسد.

```
HAL-R1#show ip route
Codes: C—connected, S—static, I—IGRP, R—RIP, ...
 (Additional codes omitted for briefness)
Gateway of last resort is not set
S   25.0.0.0 [1/0] via 24.0.0.2
C   24.0.0.0/8 is directly connected, Serial0/0/0
C   23.0.0.0/8 is directly connected, FastEthernet0/1
```

روترها از کارآمدترین تجهیزات شبکه هستند، زیرا با ساخت مفهومی که به آن حوزه پخشی (broadcast)گفته می‌شود و در اصل به گروهی از سیستم‌ها اشاره دارد که قادر به دریافت پیام‌های پخشی یکدیگر هستند، مرز شبکه را مشخص کنند. دامنه پخشی (broadcast) به محدوده یا سگمنتی از شبکه گفته می‌شود که اگر یک دستگاه اطلاعات خود را ارسال کند، در آن سگمنت همه دستگاه‌ها قادر به دریافت بسته اطلاعاتی هستند، زیرا همه گره‌ها روی یک شبکه محلی به بسته دسترسی دارند،

اما بسته‌ها از طریق روترها فورورد نمی‌شوند. بنابراین، روترها مرزهای (کرانه‌های) یک دامنه پخشی را تعریف می‌کنند. پیام پخش پیامی است که برای همه سیستم‌ها ارسال می‌شود و روتر به‌شکل راهبردی در شبکه قرار می گیرد تا پیام‌های پخشی را در شبکه نگه دارد. اما همان‌گونه که اشاره شد روتر ترافیک پخشی را انتقال نمی‌دهد.

متعادل کننده بار

متعادل کننده مکانیزیمی است که برای تقسیم بار میان مولفه‌هایی مثل سرورها یا روترها طراحی شده است. تعادل بار مکانیزمی است که با هدف بهبود عملکرد از آن استفاده می‌شود. در این حالت به جای داشتن یک سرور یا دستگاه واحد که همه کارها را انجام می‌دهد، چند سرور یا دستگاه در شبکه قرار می‌گیرد تا حجم کار میان آن‌ها تقسیم شود. این‌کار عملکرد کلی را افزایش می‌دهد، زیرا سیستم‌های بیشتری می‌توانند به‌طور همزمان کار کنند تا به درستی به همه درخواست‌های دریافتی پاسخ داده شده و مدیریت شوند. متعادل‌کننده‌های تنظیمات مختلفی در دسترس سرپرستان شبکه قرار می‌دهند تا به بهترین شکل عملکرد متعادل‌کننده بار را پیکربندی کنند. از جمله این تنظیمات به موارد زیر باید اشاره کرد:

Round-robin ■درخواست یک کلاینت را به ترتیب به هر سرور back-end ارسال می‌کند. متعادل‌کننده بار از طریق فهرستی از سرورها که در اختیار دارد سعی می‌کند درخواست را برای سروری که بار ترافیکی کمتری دارد ارسال کند. بر همین اساس به ترتیب به سراغ سرورها می‌رود.

Affinity Controls ■کنترل می‌کند که آیا تمام درخواست‌های یک کلاینت به همان سرور در بار متعادل کننده می‌رود یا این‌که هر درخواست به‌طور بالقوه می‌تواند به سرور دیگری هدایت شود Affinity . اساساً یک کلاینت را به یک سرور خاص متصل می‌کند.

Persistence ■رویکرد دیگری است که برای مرتبط کردن یک کلاینت با یک سرور خاص درون متعادل‌کننده بار استفاده می‌شود. با استفاده از ویژگی فوق، کوکی فعلی نشست کاربر برای اطمینان از این‌که همان سرور تمام درخواست‌های مشتری را مدیریت می‌کند استفاده می‌شود. این کوکی نشست می‌تواند به خود متعادل‌کننده بار یا برنامه کاربردی مرتبط باشد.

Scheduling Specifies ■مشخص می‌کند که از کدام الگوریتم برای ارسال درخواست به یکی از گره‌ها استفاده شود. زمان‌بندی از سنجه‌ها و پارامترهای پیکربندی مختلفی مثلround-robin ، affinity، و CPU loadاستفاده می‌کند تا مشخص کند درخواست به کدام سرور ارسال شود.

Active/Passive ■در مقابل :Active/Passive دو پیکربندی رایج برای متعادل‌سازی بار وجود دارد. با پیکربندی فعال/غیرفعال، یک سیستم که گره نامیده می‌شود، تمام کارها (گره فعال) را انجام می‌دهد، در حالی که گره دیگر (گره غیرفعال) در حالت آماده‌باش است و در صورت خرابی گره فعال، آماده است تا کنترل را به عهده بگیرد. اگر گره فعال از کار بیفتد، گره غیرفعال به گره فعال تبدیل می شود و تمام حجم کاری را مدیریت می‌کند. با یک پیکربندی فعال/فعال، هر دو گره آنلاین هستند و قادر به رسیدگی به درخواست‌ها هستند و اساسا حجم کار را تقسیم می‌کنند. اگر یک گره از کار بیفتد، گره دیگر تمام

حجم کاری را تا زمانی که گره خراب بازیابی شود، مدیریت می‌کند. با پیکربندی هر دو حالت، می‌توان بیش از دو گره را برای دستیابی به افزونگی اضافی به کار گرفت.
در هر دو حالت، load balancerیک آدرس آی‌پی به‌دست می‌آورد (معروف به آی‌پی مجازی). در این حالت شما می‌توانید همه کلاینت‌ها را برای ارسال درخواست به آی‌پی مجازی اختصاص داده شده به load balancerپیکربندی می‌کنید. هنگامی که متعادل‌کننده بار درخواستی را دریافت می‌کند که به آی‌پی مجازی ارسال می‌شود، در ادامه درخواست را به یک گره فعال در متعادل‌کننده بار ارسال می‌کند.
■ DNS Round-Robin: یکی دیگر از تکنیک‌های متعادل‌سازی بار DNS round-robin نام دارد. راه‌حل متعادل‌کننده بار به سادگی درخواست را به سرور بعدی در فهرست خود ارسال می‌کند. مشکل round-robinاین است که راه‌حل مذکور تضمین نمی‌دهد که آیا سرور واقعاً بدون مشکل راه‌اندازی شده است یا خیر. یک مثال روشن در ارتباط با متعادل‌سازی بار چرخشی استفاده از سامانه نام دامنه (DNS) است. شما می‌توانید چند رکورد DNS با نام یکسان، اما آدرس‌های آی‌پی متفاوت ایجاد کنید و سرور DNSبا هر پاسخ یک آدرس آی‌پی متفاوت را برای کلاینت‌ها ارسال کند. در روش فوق مشکل این است که سرور DNS تأیید نمی‌کند که این آدرس‌های آی‌پی توسط سیستم‌هایی که در حال اجرا هستند استفاده می‌شوند.

آشنایی با مبانی و اصطلاحات شبکه بخش ۰۲

فایروال‌ها و سرورهای پروکسی

در شماره‌های آتی اطلاعات بیشتری در ارتباط با فایروال‌ها و سرورهای پراکسی به‌دست خواهیم آورد، اما در این‌جا توضیح مختصری در ارتباط با این مفاهیم ارایه می‌کنیم. فایروال نرم‌افزار یا سخت‌افزاری که برای کنترل ترافیک شبکه استفاده می‌شود. کاری که فایروال انجام می‌دهد این است که میان ترافیک مجاز ورودی و خروجی شبکه و ترافیکی که باید مسدود شود تمایز قائل می‌شود. فایروال ترافیک را بر اساس خط‌مشی‌های از پیش تعریف شده توسط کارشناسان شبکه یا امنیت فیلتر می‌کند. شما معمولاً با یک قانون deny-all به معنای مسدودسازی همه ترافیک کار را آغاز می‌کنید و در ادامه با تعریف خط‌مشی‌های خاص برای ترافیک، اجازه وارد یا خارج شدن بسته‌های اطلاعاتی را می‌دهید.
پروکسی سرور نرم‌افزار یا سخت‌افزاری است که که همه کلاینت‌ها ترافیک خود را برای آن ارسال می‌کنند و سپس سرور پروکسی درخواست‌های دریافتی از کاربران را برای مقاصد تعریف شده ارسال می‌کند. به‌طور معمول، سرور پروکسی فناوری ترجمه آدرس شبکه (NAT) سرنام Network Address Translationرا نیز پیاده‌سازی می‌کند و به حفظ ساختار شبکه داخلی از دنیای خارج کمک می‌کند. پروکسی‌های transparent نیازی به احراز هویت کاربر ندارند، با این‌حال، محصولات سرور پروکسی نیز وجود دارند که نیاز دارند کلاینت قبل از گشت و گذار در اینترنت احراز هویت شود. رویکرد فوق به کنترل سایت‌هایی که هر کاربر می‌تواند بازدید کند کمک می‌کند و به مدیر پروکسی اجازه می‌دهد تا سایت‌هایی که هر کاربر بازدید می‌کند را ثبت کند. به عنوان آخرین نکته در مورد سرورهای پراکس،

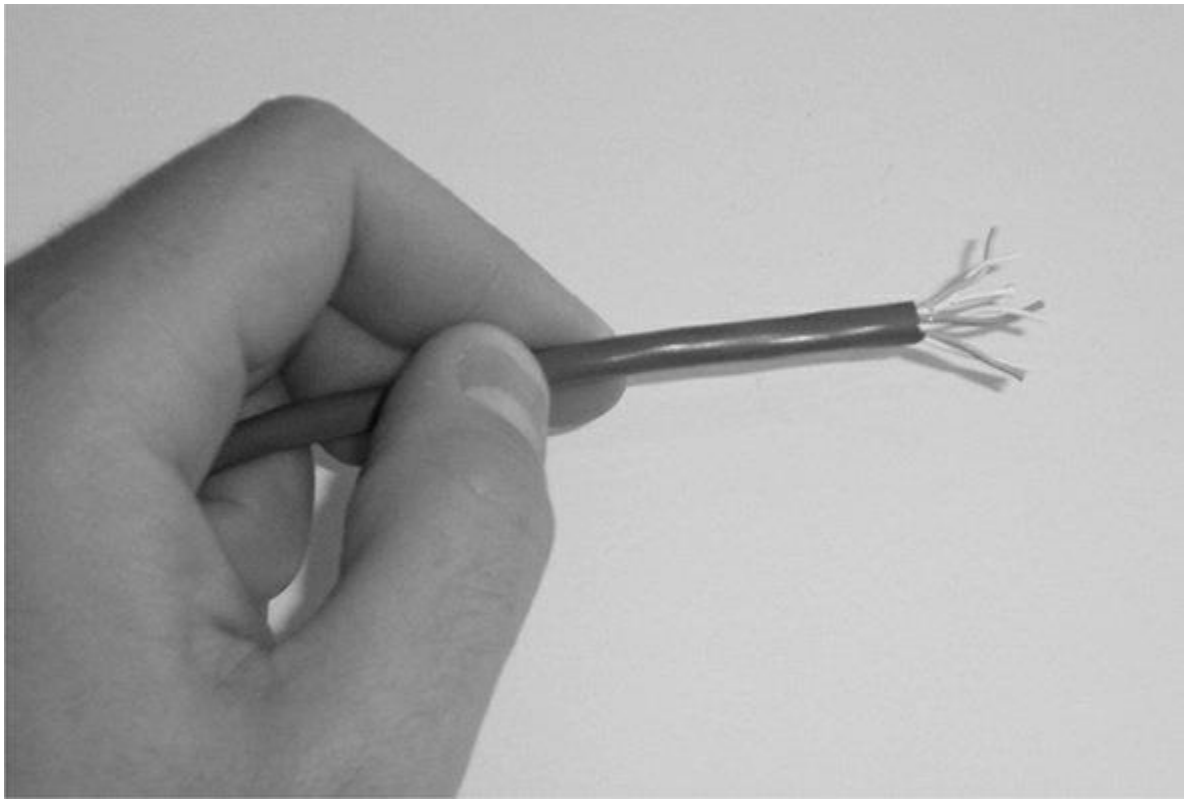
پروکسی‌های معکوس (reverse) وجود دارند که به شما امکان می‌دهند تمام ترافیک ورودی (مانند ترافیک به یک سرور وب) را دریافت کنید، درخواست‌ها را تجزیه و تحلیل کنید و فقط به درخواست‌های ایمن و معتبر اجازه دسترسی به وب سرور را بدهید.

آشنایی با کابل‌کشی شبکه

کابل‌کشی به معنای پیاده‌سازی رسانه انتقال داده‌ها بین میزبان‌ها در شبکه LAN است. سیستم‌های روی شبکه LAN را می‌توان با استفاده از انواع کابل‌هایی مانند جفت تابیده بدون محافظ و فیبر به یکدیگر متصل کرد. هر نوع کابل مزایا و معایب خاص خود را دارد که در این قسمت به بررسی آن‌ها می‌پردازیم.
دو نوع اصلی از رسانه‌های کابلی که می‌توانند برای اتصال سیستم‌ها به یک شبکه استفاده شوند، کابل جفت تابیده و کابل فیبر نوری هستند. نرخ انتقال پشتیبانی شده در هر یک از این رسانه‌های فیزیکی با میلیون‌ها بیت در ثانیه یا مگابیت در ثانیه (Mbps) اندازه‌گیری می‌شود.

کابل جفت درهم تنیده شده

امروزه، کابل‌کشی جفت درهم تنیده شده انتخاب اصلی متخصصان شبکه است. کابل‌های جفت در هم تنیده شده متشکل از چهار جفت سیم هستند که برای کمک به کاهش تداخل یا تداخل دستگاه‌های الکتریکی بیرونی درهم تنیده شده‌اند. یکی از مشکلات پیرامون کابل‌های شبکه هم‌شنوی (Crosstalk) سیم‌های مجاور است که باعث افت کیفیت سیگنال‌ها می‌شود. شکل زیر یک کابل درهم تنیده شده را نشان می‌دهد. دو نوع کابل کواکسیال به‌نام‌های جفت بهم تابیده بدون محافظ (UTP) و جفت بهم‌تابیده شیلددار (STP) وجود دارد.



اگر کابل تلفن را دیده یا با آن کار کرده باشید به خوبی با کابل‌های UTP بدون محافظ آشنا هستید. کابل درهم تنیده شده معمولی برای استفاده در شبکه شامل چهار جفت سیم است. هر یک از جفت سیم‌های موجود در کابل به دور دیگری پیچ خورده‌اند. پیچش سیم‌ها به محافظت در برابر تداخل الکترومغناطیسی کمک می‌کند، با این‌حال حداکثر فاصله مجاز برای کابل UTP در حدود ۱۰۰ متر است. کابل UTP از کانکتورهای پلاستیکی کوچکی استفاده می‌کند که به‌نام جک RJ45 از آن نام برده می‌شود RJ-45 .شبیه کانکتورهای تلفن است، با این تفاوت که به جای چهار سیم شامل هشت سیم است. افراد تازه‌کار دنیای شبکه به راحتی کانکتور RJ-45 را با کانکتور RJ-11 اشتباه می‌گیرند. کانکتور RJ-11یک رابط تلفن است و دارای چهار کانکتور است. از این رو، چهار سیم در کابل تلفن وجود دارد. هنگامی که قصد استفاده از کانکتورهای RJ-45 و RJ-11 را همراه با کابل‌های شبکه دارید برای برقراری تماس بین پین‌های کانکتور و سیم‌های داخل کابل به ابزار خاصی به‌نام آچار سوکت‌زنی شبکه نیاز دارید.

به‌کارگیری کابل UTP راحت‌تر از کواکسیال است زیرا به دلیل انعطاف‌پذیری و اندازه کوچکی که دارد امکان عبور آن از گوشه‌های دیوار وجود دارد. البته اگر میزان خمش بیش از اندازه باشد کابل آسیب می‌بیند. به‌طور معمول، شرکت‌های تولیدکننده کابل روی آن میزان خمش را ذکر می‌کنند. کابل جفت پیچ خورده نسبت به کواکسیال بیشتر مستعد تداخل است و نباید در محیط‌های حاوی وسایل الکتریکی بزرگ استفاده شود.

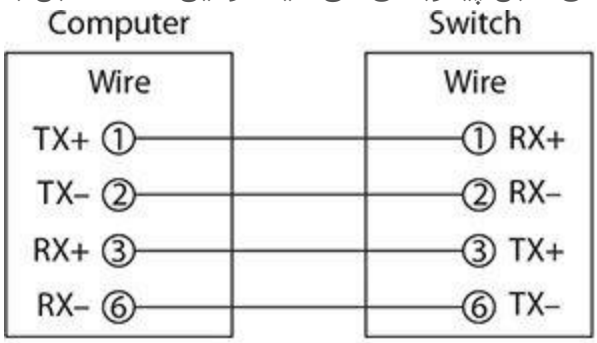
نکته دیگری که باید در مورد کابل‌کشی UTP به آن دقت کنید، طبقه‌بندی استفاده شد است که به‌نام عنوان درجه انتقال یا دسته‌بندی (Categories) شناخته می‌شوند. هر دسته از کابل‌های UTP برای نوع

خاصی از ارتباطات یا انتقال اطلاعات مناسب هستند. جدول زیر طبقه‌بندی‌های مختلف UTP را نشان می‌دهد. امروزه محبوب‌ترین آن‌ها CAT 5e است که دسترسی به سرعت انتقال بیش از ۱۰۰۰ مگابیت در ثانیه یا ۱ گیگابیت در ثانیه (Gbps) را می‌دهد.

UTP Category	Purpose	Transfer Rate
Category 1	Voice only	
Category 2	Data	4 Mbps
Category 3	Data	10 Mbps
Category 4	Data	16 Mbps
Category 5	Data	100 Mbps
Category 5e	Data	1 Gbps (1,000 Mbps)
Category 6	Data	10 Gbps

هنگام کار روی شبکه‌ای که مبتنی بر کابل‌کشی UTP است، با انواع مختلفی از کابل‌ها روبر می‌شوید. به‌طور مثال، گاهی اوقات از کابل مستقیم یا کابل متقاطع استفاده می‌شود.

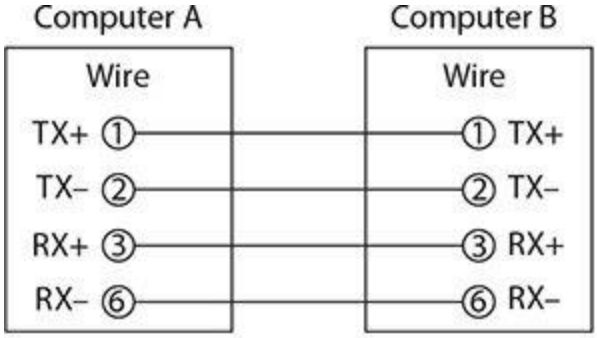
کابل مستقیم :(Straight-Through Cable) کابل‌کشی UTP CAT 5 هنگام ارسال و دریافت اطلاعات در شبکه فقط از چهار سیم استفاده می‌کند. چهار سیم از هشت سیم مورد استفاده، سیم‌های ۱، ۲، ۳ و ٦ هستند. شکل زیر پین‌های ارسال و دریافت روی یک کامپیوتر و پایه‌های روی سوئیچ را نشان می‌دهد که معمولاً کامپیوترها را به هم وصل می‌کند. هنگامی که سیم را روی همان پین در هر دو انتهای کابل پیکربندی می‌کنید در این حالت کابل به‌نام کابل مستقیم شناخته می‌شود.



همان‌گونه که در شکل بالا مشاهده کردید، سیم‌های ۱ و ۲ برای انتقال داده‌ها (TX) از رایانه استفاده می‌شوند، در حالی که سیم‌های ۳ و ٦ برای دریافت اطلاعات (RX) در رایانه استفاده می‌شوند. همچنین متوجه خواهید شد که پین ارسال (TX) روی کامپیوتر از طریق سیم‌های ۱ و ۲ به پین دریافت (RX) روی سوئیچ متصل است. این موضوع مهم است زیرا می‌خواهید مطمئن شوید که داده‌های ارسال شده از کامپیوتر توسط سوئیچ دریافت می‌شوند. همچنین می‌خواهید مطمئن شوید که داده‌های ارسال شده از سوییچ در رایانه دریافت می‌شوند، از این‌رو، پین‌های ارسال (TX) روی سوئیچ از طریق سیم‌های ۳

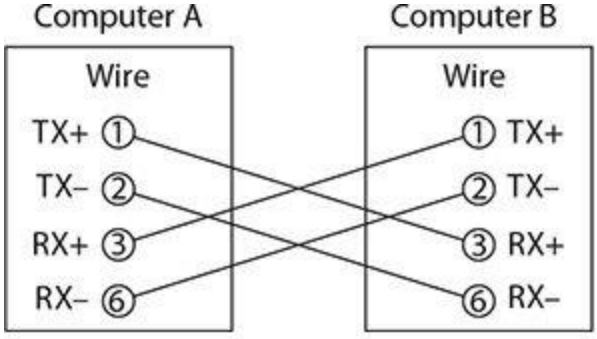
و ٦ به پایه‌های دریافت (RX) روی رایانه متصل می‌شوند. رویکرد فوق به رایانه امکان می‌دهد اطلاعات را از سوییچ دریافت کند. آخرین نکته‌ای که باید در مورد شکل بالا به آن دقت کنید این است که پین ۱ در رایانه به همان سیم به پایه ۱ روی سوئیچ متصل است، به همین دلیل به رویکرد فوق مستقیم می‌گویند، به‌طوری که تمام پین‌ها در شکل فوق مستقیماً به طرف دیگر منطبق شده‌اند.

کابل متقاطع :(Crossover Cable) در برخی مواقع، ممکن است لازم باشد دو سیستم کامپیوتری را مستقیماً بدون استفاده از سوئیچ و از طریق کارت شبکه به یکدیگر متصل کنید یا ممکن است متوجه شوید که باید یک سوئیچ را به سوییچ دیگر وصل کنید. در هر سناریویی که دستگاه‌های مشابه را به یکدیگر متصل می‌کنید، نمی‌توانید از کابل مستقیم استفاده کنید زیرا پایه انتقال در یک طرف به پایه انتقال در انتهای دیگر متصل می‌شود. همان‌گونه که در شکل زیر نشان داده شده است. چگونه یک کامپیوتر می‌تواند داده‌هایی را که به پین‌های دریافتی ارسال نشده‌اند، دریافت کند؟ از آن‌جایی که این کار امکان‌پذیر نیست، باید سیم‌کشی کابل به گونه‌ای تغییر کند که حالت متقاطع داشته باشد.



به بیان دقیق‌تر، استفاده از کابل مستقیم برای اتصال دو کامپیوتر کار نخواهد کرد.

برای اتصال مستقیم دو سیستم به یکدیگر بدون استفاده از سوئیچ، باید کابل متقاطع را با تغییر سیم‌های ۱ و ۲ به سیم‌های ۳ و ٦ در انتهای کابل بسازیم. درست به همان صورتی که در شکل زیر مشاهده می‌کنید. متوجه خواهید شد که پین‌های ارسال در رایانه A به پین‌های دریافت در رایانه B متصل هستند، بنابراین به رایانه A اجازه می‌دهد تا داده‌ها را به رایانه B ارسال کند. همین امر برای رایانه B برای ارسال اطلاعات به رایانه A صادق است. به بیان دقیق‌تر، سیم‌ها به شکل ضربدری به یکدیگر متصل شده‌اند. پین‌های ۱ و ۲ در رایانه B به پین‌های ۳ و ٦ در رایانه A متصل می‌شوند تا رایانه A بتواند داده‌ها را از رایانه B دریافت کند.



نکته :اکثر مدیران شبکه از یک رنگ کابل خاص (مانند زرد) برای نشان دادن کابل‌های متقاطع استفاده می‌کنند و از یک کابل رنگی متفاوت برای نمایش کابل‌های مستقیم استفاده می‌کنند تا کابل‌ها به اشتباه به‌جای یکدیگر استفاده نشوند.
کابل STP محافظدار بسیار شبیه کابل UTP است، اما تفاوت آن با UTP در این است که از لایه‌ای از عایق در پوشش محافظ آن استفاده شده تا کیفیت سیگنال تقویت شود.

کابل فیبر-نوری(Fiber-Optic Cable)

نوع دوم کابل‌کشی مورد بحث، کابل‌کشی فیبر نوری است. کابل‌کشی فیبر نوری بر خلاف جفت تابیده شده است، در حالت اول جفت تابیده از یک سیم مسی برای انتقال سیگنال الکتریکی استفاده می‌شود. کابل‌های فیبر نوری از فیبرهای نوری استفاده می‌کنند که سیگنال‌های داده‌ای دیجیتال را به شکل پالس‌های نور مدوله‌شده حمل می‌کنند. یک فیبر نوری از یک استوانه شیشه‌ای بسیار نازک به‌نام هسته تشکیل شده است که توسط یک لایه شیشه‌ای متحدالمرکز احاطه شده است که به عنوان روکش شناخته می‌شود. دو فیبر در هر کابل وجود دارد - یکی برای انتقال و دیگری برای دریافت. هسته همچنین می‌تواند یک ماده شفاف یا نور باشد و روکش آن می‌تواند از ژل ساخته شود که سیگنال‌ها را به داخل فیبر بازتاب کند تا مانع از دست رفتن سیگنال‌ها شود.
دو نوع کابل فیبر نوری وجود دارد:
■فیبر تک حالته (SMF) از یک پرتو نور، معروف به حالت، برای حمل و انتقال بسته‌ها در فواصل طولانی استفاده می‌کند.
■فیبر چند حالته (MMF) از چندین پرتو نور (حالت‌ها) به‌طور همزمان استفاده می‌کند و از هر پرتو نور در زاویه بازتاب متفاوتی برای انتقال بسته‌ها در فواصل کوتاه استفاده می‌کند.
نکته: برای آزمون فوق به یاد داشته باشید که فیبر نوری نوع کابل ایمن‌تری برای استفاده است زیرا سیگنال الکتریکی را حمل نمی کند، بلکه داده‌ها را به صورت پالس‌های نور حمل می‌کند.
کابل فیبر نوری تا ۱۰۰۰ ایستگاه را پشتیبانی می‌کند و می تواند سیگنال را تا ۲ کیلومتر و بیشتر از آن حمل کند. کابل‌های فیبر نوری همچنین در برابر تداخل خارجی مثل فرستنده‌های رادیویی، جوش‌های قوس الکتریکی، چراغ‌های فلورسنت و سایر منابع نویز الکتریکی بسیار ایمن هستند. از سوی دیگر، کابل‌کشی فیبر نوری تا حد زیادی گران‌قیمت‌تر از روش کابل کشی است و بعید است که یک شبکه کوچک به این ویژگی‌ها نیاز داشته باشد.
کابل‌های فیبر نوری می‌توانند از انواع مختلفی از کانکتورها استفاده کنند، مانند کانکتور مستقیم (ST) سرنامstraight-tip ، کانکتور لوسنت (LC) سرنام Lucent Connector و کانکتور مشترک (SC) سرنام subscriber connector.طراحی کانکتور ST مبتنی بر کانکتور BNC است، اما به جای کابل مسی، یک کابل فیبر نوری دارد. کانکتور SC مربعی شکل است و تا حدودی شبیه به کانکتور RJ-45 است، در حالی که اندازه کانکتور LC نصف کانکتور SC است و برای مناطقی در زیرساخت طراحی شده است که کابل‌های زیادی در آن استفاده می شود، مانند پچ پنل.

صرف نظر از نوع اتصال، کابل فیبر نوری با سرعت یکسانی کار می‌کند که معمولاً ۱۰۰۰ مگابیت در ثانیه یا بیشتر است. تنها نکته‌ای که باید در مورد این دقت کنید تطابق کانکتور با دستگاهی است که باید به آن متصل شود. زیرا این دو نوع کانکتور قابل تعویض نیستند.
نکته :هنگام آماده شدن برای امتحان سکوریت‌پلاس، گاهی اوقات داشتن جدولی که تفاوت‌های بین انواع کابل را فهرست می‌کند مفید است. جدول زیر توضیحی کلی در مورد أنواع مختلف کابل ارایه می‌کند که برای آزمون +Security باید آن‌را بدانید.

Cable	Max Distance	Transfer Rate	Connector Used
CAT 3 (UTP)	100 m	10 Mbps	RJ-45
CAT 5 (UTP)	100 m	100 Mbps	RJ-45
CAT 5e	100 m	1 Gbps	RJ-45
CAT 6	100 m	10 Gbps	RJ-45
Fiber-optic	2 km	1+ Gbps	SC, ST, or LC

در این تمرین، دانش خود در مورد کابل‌های شبکه و دستگاه‌ها را تطابق دادن عبارات با سناریوی مناسب محک بزنید.

Device	Scenario
____ Switch	A. A group of systems that can have their data collide with one another
____ Load balancer	B. A communication boundary
____ UTP	C. A layer-3 device that sends data from one network to another
____ Port security	D. A layer-2 device that filters traffic based on MAC address
____ VLAN	E. A device that is used to split the workload between multiple servers
____ Router	F. A cable type that carries pulses of light
____ Collision domain	G. A type of cable that has copper wires divided into pairs
____ Fiber-optic	H. Controlling which MAC addresses can connect to the switch

آشنایی باTCP/IP

اکنون که تا حدودی با دستگاه‌های زیربنایی مورد استفاده در شبکه‌ها و انواع کابل‌ها آشنا شدیم، اجازه دهید به سراغ پروتکل TCP/IP برویم. به عنوان یک متخصص امنیتی، مهم است که نه تنها با پروتکل TCP/IPآشنایی داشته باشید، بلکه نحوه برقراری ارتباط در یک شبکه TCP/IP را درک کنید.

آدرس IP چیست؟

TCP/IPبرای پیکربندی صحیح سیستم‌ها به کمی دانش نیاز دارد. وقتی TCP/IP را پیکربندی می‌کنید، باید تنظیمات آدرسIP ، ماسک زیر شبکه و گیت‌وی پیش‌فرض را بدانید. آدرس IP یک مقدار ۳۲ بیتی است که به‌طور منحصر به فرد برای شناسایی سیستمی در شبکه یا اینترنت از آن استفاده می‌شود. یک آدرس IP از نظر ظاهری شبیه به ۱۹۲٫۱۶۸٫۱٫۱۵ است. چهار مقدار اعشار در یک آدرس IP با نقطه اعشار از هم جدا می‌شوند. هر مقدار از ۸ بیت (۱ و ۰) تشکیل شده است، بنابراین با چهار مقدار اعشاری، ۸ بیت × ٤ = آدرس ۳۲ بیتی.
از آن‌جایی که هر یک از مقادیر اعشاری از ۸ بیت تشکیل شده‌اند (مثلاً ۱۹۲)، ما به هر یک از مقادیر اعشاری به عنوان یک اکتت (Octet) اشاره می‌کنیم. چهار اکتت در یک آدرس IP هستند. درک این نکته بسیار مهم است که چهار اکتت در یک آدرس IP به دو بخش تقسیم می‌شوند که برای شناسه شبکه و شناسه میزبان از آن استفاده می‌شود. ماسک زیرشبکه تعداد بیت‌هایی که شناسه شبکه را تشکیل می‌دهند و تعداد بیت‌هایی که شناسه میزبان را تشکیل می‌دهند را مشخص می‌کند. اجازه دهید ببینیم این فرایند چگونه کار می‌کند.

ماسک زیر شبکه(Subnet Mask)

هنگامی که به یک ماسک زیر شبکه نگاه می‌کنید، اگر ۲۵۵ در یک اکتت (octet) وجود داشته باشد، اکتت مربوطه در آدرس IP بخشی از شناسه شبکه است. به عنوان مثال، اگر من یک آدرس ۱۹۲٫۱٦۸٫۱٫۱۵ و یک ماسک زیر شبکه ۲۵۵٫۲۵۵٫۲۵۵٫۰ داشته باشم، سه اکتت اول شناسه شبکه را تشکیل می‌دهند و آخرین اکتت شناسه میزبان خواهد بود. شناسه شبکه یک آدرس منحصر به فرد را به خود شبکه اختصاص می‌دهد، در حالی که شناسه میزبان به‌طور منحصر به فرد سیستم را در شبکه شناسایی می‌کند. جدول زیر خلاصه‌ای از این اطلاعات را نشان می‌دهد) شناسایی بخش‌های شناسه شبکه و شناسه میزبان یک آدرس:(IP

	Octet 1	Octet 2	Octet 3	Octet 4
IP address	192	168	1	15
Subnet mask	255	255	255	0
Address portion	N	N	N	H

در جدول بالا مشاهده می کنید که شناسه شبکه) نشان داده شده با 192.168.1 (N است و شناسه میزبان آخرین اکتت با مقدار ۱۵ است. این بدان معنی است که این سیستم در شبکه ۱۹۲٫۱٦۸٫۱ است و هر سیستم دیگری در همان شبکه همان شناسه شبکه را خواهد داشت. اگر ماسک زیر شبکه ۲۵۵٫۰٫۰٫۰ داشته باشید، به این معنی است که اولین اکتت آدرس IP به عنوان بخش شناسه شبکه استفاده می‌شود، در حالی که سه اکتت آخر، بخش شناسه میزبان آدرس IP هستند. بنابراین هدف از زیر شبکه چیست یا بهتر از آن، چرا ماسک زیر شبکه‌ای داریم که آدرس IP را به شناسه شبکه و شناسه میزبان تبدیل می‌کند؟ زیرا هنگامی که سیستمی مانند ۱۹۲٫۱٦۸٫۱٫۱۵ با ماسک زیر شبکه

۲۵۵/۲۵۵/۲۵۵/۰ یک فریم داده‌ای را به ۱۹۲/۱۹۸/۴۵/۱۰ ارسال می‌کند، سیستم ارسال کننده ابتدا باید تعیین کند که آیا رایانه مورد نظر در همان شبکه وجود دارد یا خیر. این کار را با مقایسه شناسه‌های شبکه همانند جدول انجام می‌دهد.

	Octet 1	Octet 2	Octet 3	Octet 4
IP address #1	192	168	1	15
Subnet mask	255	255	255	0
IP address #2	192	198	45	10

اگر شناسه‌های شبکه یکسان باشند، هر دو سیستم در یک شبکه وجود دارند و یک سیستم می‌تواند بدون استفاده از روتر بسته‌های اطلاعاتی را به دیگری ارسال کند. اگر سیستم‌ها در شبکه های مختلف وجود داشته باشند، داده‌ها باید توسط روتر منتقل شوند تا روتر بتواند داده‌ها را به شبکه دیگر ارسال کند.

گیت‌وی پیش‌فرض

هنگامی که سیستم شما می‌خواهد داده‌ها را به سیستم دیگری در شبکه ارسال کند، به شناسه شبکه خود نگاه می‌کند و آن را با آدرس IP سیستم مقصد مقایسه می‌کند. اگر شناسه شبکه یکسانی داشته باشند، داده‌ها مستقیماً از سیستم شما به سیستم مقصد ارسال می‌شود. اگر این دو سیستم در شبکه‌های مختلف باشند، سیستم شما باید داده‌ها را به روتر ارسال کند تا روتر بتواند داده‌ها را به روتر سیستم مقصد ارسال کند. چگونه سیستم شما می‌داند که از کدام روتر استفاده کند؟ پاسخ گیت‌وی پیش‌فرض است. گیت‌وی پیش‌فرض به آدرس IP روتری اشاره دارد که می‌تواند داده‌ها را از شبکه شما ارسال کند.

برای برقراری ارتباط در اینترنت، سیستم شما باید با یک آدرسIP ، یک ماسک زیر شبکه و یک گیت‌وی پیش‌فرض پیکربندی شود. اگر نیاز دارید که فقط با سیستم‌های موجود در شبکه خود ارتباط برقرار کنید، فقط به یک آدرس IP و یک ماسک زیر شبکه نیاز خواهید داشت.

پایان بخش -۲. ادامه دارد.....