تسلط بر مفاهیم پایه شبکه منطبق با استانداردهای بین‌المللی

آموزش رایگان دوره نتورک‌پلاس (Network+) (بخش 59)

در شماره گذشته آموزش نتورک‌پلاس با Kerberos و مباحث مرتبط با آن، احراز هویت و ورود یکپارچه با رویکرد Single Sign-On، احراز هویت کاربر از دور (RADIUS)، کنترل کننده دسترسي ترمینال و سیستم کنترل دسترسي (TACACS+) و امنیت شبکه بی‌سیم آشنا شدیم. در این شماره مبحث فوق را ادامه خواهیم داد.

برای مطالعه بخش پنجاه و هشتم آموزش رایگان و جامع نتورک پلاس (Network+) اینجا کلیک کنید

WPA سرنام Wi-Fi Protected Access

استاندارد 802.11i دارای یک کلید رمزگذاری ساخته و مدیریت شده با پروتکل کلید موقت یکپارچه (TKIP) سرنام Temporal Key Integrity Protocol است که برای بهبود امنیت دستگاه‌های مبتنی بر استاندارد عادی WEP از آن استفاده می‌شود. TKIP برای بهبود امنیت بر سه اصل زیر متمرکز است:

• یکپارچگی پیام - از یک کد یکپارچه پیام که Michael نام دارد برای حصول اطمینان از این‌که بسته‌های وارد شونده درست از همان مبدا مشخص شده ارسال شده‌اند، استفاده می‌کند. این رویکرد، تأیید هویت بسته نیز نامیده می‌شود.

• کلید توزیع شده- هر انتقال کلید اختصاصی خود را دارد.

• رمزگذاری – فرآیند رمزگذاری بر مبنای الگوریتم RC4 سرنام Cipher 4 انجام میشود که اکنون به عنوان یک رمزنگاری غیر ایمن شناخته شده است، هرچند هنوز هم به‌طور گسترده از آن استفاده می‌شود.

در واقع، **TKIP** با هدف ارائه راهکاری سریع برای رفع مشکل رمزگذاری در استاندارد **WEP** ارائه شد تا داده‌ها به شکل ایمن‌تری انتقال پیدا کنند. WPA’s TKIP بر پایه همان مکانیزم رمزگذاری استاندارد WEP کار می‌کرد، اما سعی کرد از الگوریتم‌های بهبود یافته استفاده کند تا مشکلات استاندارد WEP در فرآیند انتقال را بهبود بخشیده و یک مکانیزم انتقال امن‌تر را ارائه کند. با این حال، شما هنوز هم می‌توانید دستگاه‌های شبکه بی‌سیمی را پیدا کنید که برای حفظ سازگاری با دستگاه‌های بی‌سیم قدیمی‌تر استاندارد TKIP را پیشنهاد می‌دهند.

WPA2 سرنام Wi-Fi Protected Access, Version 2

روش‌های حفظ محرمانگی داده‌های مورد استفاده در استاندارد WPA با فناوری‌های قوی‌تر جایگزین شدند و نسخه به‌روز شده‌ای به نام WPA2 را به وجود آورند. حالت ضد رمز به همراه پروتکل کد اعتبارسنجی پیام تغییر بلوک

(CCMP) که سرنام چهار اصطلاح Counter Mode with CBC،Cipher Block Chaining ، Message Authentication Code و Protocol است امنیت دستگاه‌های بی‌سیمی که از WPA2 استفاده می‌کنند را بهبود بخشید. در حالی که TKIP برای حفظ سازگاری با دستگاه‌های قدیمی‌تر ارائه شد، CCMP تمرکزش بر دستگاه‌های آینده است. CCMP با هدف حفظ محرمانگی اطلاعات هر دو رویکرد رمزگذاری و احراز هویت بسته‌ها را به منظور دستیابی به اهداف زیر استفاده می‌کند

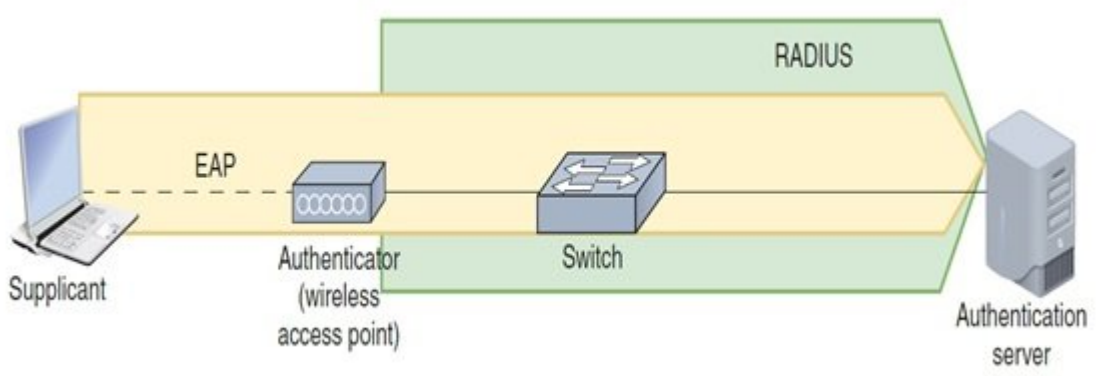
• یکپارچگی پیام - CCMP از CBC-MAC استفاده می‌کند تا مطمئن شود بسته‌های ورودی از منبعی که مشخص شده‌اند دریافت شده‌اند. برای این منظور WPA2 از الگوریتم‌های سایفر AES استفاده می‌کند.

• رمزگذاری- CCMP همچنین از استاندارد رمزگذاری پیشرفته (AES) سرنام Advanced Encryption Standard استفاده می‌کند تا رمزگذاری سریع‌تر و امن‌تر نسبت به TKIP در مدت زمان یک انتقال بی‌سیم فراهم کند.

نکته: دو نوع یکسان از الگوریتم‌های سایفر به نام‌های سایفرهای جریانی و سایفرهای بلوکی وجود دارند. تفاوت اصلی این دو نوع در این است که سایفرهای جریانی در یک زمان یک بایت را رمزگذاری می‌کنند، در حالی که سایفرهای بلوکی حجم گسترده‌تری از اطلاعات را در هر محاسبه رمزگذاری می‌کنند.

شخصی و سازمانی

در بسیاری از روترهای بی‌سیم و اکسس‌پوینت‌ها گزینه‌های WPA-Personal و WPA-Enterprise یا WPA2-Personal و WPA2-Enterprise را مشاهده می‌کنید. نسخه‌های شخصی WPA و WPA2 گاهی اوقات WPA-PSK یا WPA2-PSK نامیده می‌شوند، که PSK سرنام Pre-Shared Key است. در پیکربندی‌های رایج شبکه‌های بی‌سیم خانگی شما باید یک عبارت عبوری یا همان گذرواژه را برای احراز هویت و اتصال به شبکه وارد کنید. گذرواژه و SSID برای محاسبه کلید رمزنگاری منحصربفرد برای هر دستگاه استفاده می‌شود. نسخه‌های سازمانی WPA و WPA2 ملاحظات امنیتی بیشتری را اعمال می‌کنند. در اغلب موارد یک سرور RADIUS در تعامل با یک مکانیزم احراز هویت به نام EAP استفاده می‌شود. پروتکل احراز هویت توسعه پذیر (**EAP**) سرنام **Extensible Authentication Protocol** متفاوت از پروتکل‌های احراز هویتی است که تاکنون به آن‌ها اشاره داشتیم و تنها چارچوبی اعتبارسنجی کلاینت‌ها و سرورها فراهم می‌کند. البته این پروتکل فرآیند رمزگذاری یا احراز هویت را به تنهایی انجام نمی‌دهد. در عوض، در تعامل با سایر برنامه‌ها، رمزنگاری و احراز هویت را برای تأیید اعتبار کاربران و دستگاه‌ها انجام می‌دهد. به‌طور مثال، EAP می‌تواند در کنار RADIUS کار کند، در حالیکه EAP ارتباطات را با دستگاه کلاینت شبکه سازماندهی می‌کند، در طرف دیگر RADIUS احراز هویت واقعی در سرور را مدیریت می‌کند. در این مورد، پیام EAP در داخل پیام‌های RADIUS بین دستگاه‌های شبکه، همچون سوئیچ یا اکسس‌پوینت و سرور RADIUS کپی می‌شود. شکل زیر نشان می‌دهد که چگونه EAP و RADIUS با یکدیگر به تعامل می‌پردازند.



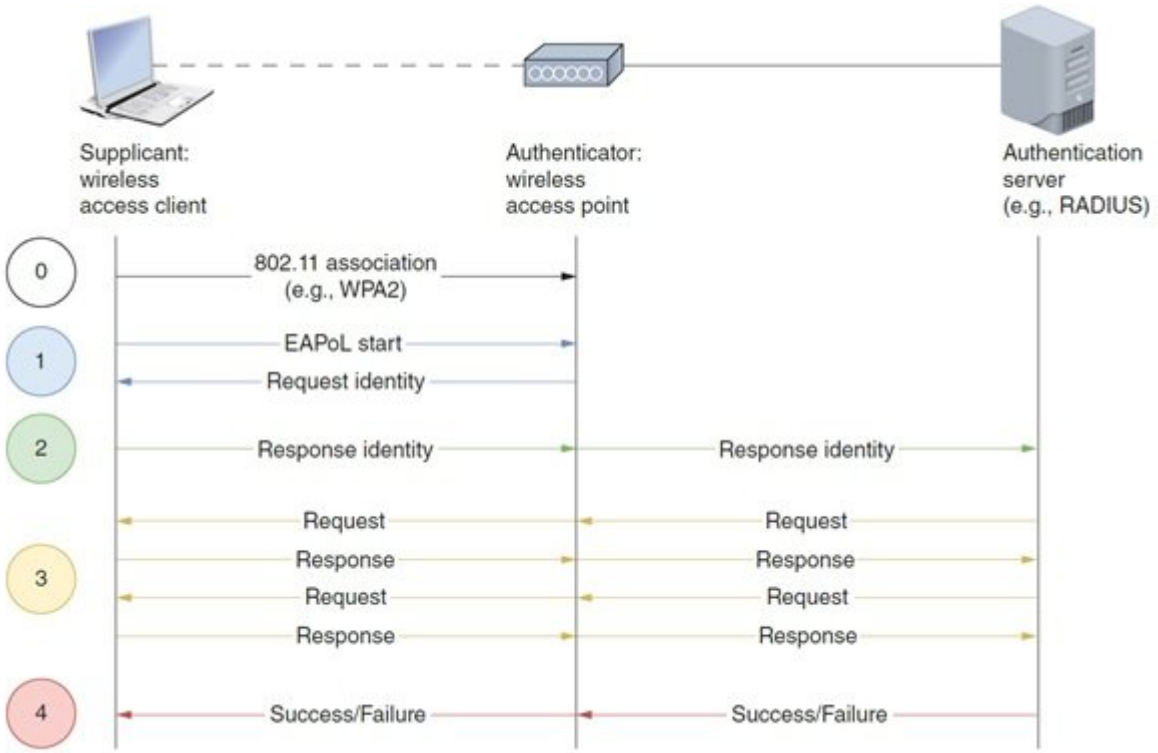
تعریف سه نهاد اصلی EAP به شرح زیر است:

• **supplicant** - دستگاه درخواست‌کننده احراز هویت است. این دستگاه می‌تواند یک گوشی هوشمند یا لپ‌تاپ باشد.

• **authenticator**- تاییدکننده یک دستگاه تحت شبکه همچون یک اکسس پوینت بی‌سیم است که فرآیند تأیید هویت اولیه را انجام می‌دهد.

• **authentication server** -سرور تأیید هویت، فرآیند احراز هویت را انجام می‌دهد

ارتباط میان این نهادها شبیه به دیاگرامی است که شکل زیر نشان می‌دهد.



مراحل نشان داده شده در تصویر بالا به شرح زیر است:

مرحله 0: دستگاه بی‌سیم با اکسس پوینت معمولا از طریق استاندارد WPA2 ارتباط برقرار می‌کند. ما با گام 0 شروع می‌کنیم زیرا در حال حاضر قرار است تنها یک احراز هویت اولیه انجام شود که بخشی از جریان اصلی نیست.

مرحله 1: کلاینت یک درخواست احراز هویت ارسال می‌کند و احراز هویت کننده فرآیند احراز هویت را آغاز می‌کند. این فرآیند با درخواست برقراری ارتباط آغاز می‌شود.

مرحله 2: پس از ارسال درخواست، احراز هویت‌کننده اطلاعات را به سرور احراز هویتی شبیه به یک سرور RADIUS ارسال می‌کند.

مرحله 3: در این مرحله سرور چند پاسخ و درخواست را ارسال کرده و دریافت می‌کند. در اولین درخواست، سرور از احرازهویت کننده درخواست می‌کند تا مشخص کند چه نوع احراز هویتی را نیاز دارد. در درخواست‌های بعدی، سرور اطلاعاتی از احراز هویت‌کننده مبنی بر اصالتش درخواست می‌کند. درخواست کننده به هر یک از درخواست‌های سرور بر مبنای فرمت مشخصی پاسخ می‌دهد.

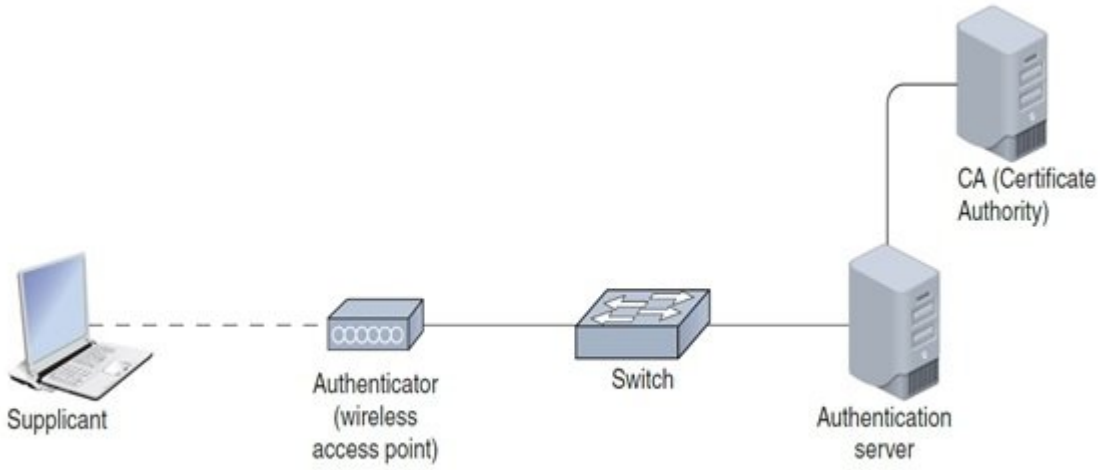
مرحله 4: اگر پاسخ‌ها مورد تایید سرور باشند، اصالت درخواست‌کننده از سوی سرور تأیید می‌شود. در غیر این صورت، احراز هویت ناموفق قملداد می‌شود.

یکی از مزایای EAP انعطاف‌پذیری آن است. این مکانیزم تقریبا از سوی تمام سیستم‌عامل‌های مدرن پشتیبانی می‌شود و می‌تواند با بسیاری از روش‌های احراز هویت مختلف استفاده شود. به‌طور مثال، اگر چه یک احراز هویت معمولی در شبکه یک شناسه کاربری و گذرواژه را درخواست می‌کند، اما می‌تواند با EAP و روش‌های زیستی همچون اسکن شبکیه یا دست ادغام شود. EAP همچنین با فناوری‌های نوین سازگاری دارد. در ابتدا EAP برای کار با

ارتباطات نقطه به نقطه ppp طراحی شده بود، اما توسعه پیدا کرد و اکنون با شبکه‌های سیمی و بی‌سیم بر مبنای استاندارد **802.1X** و **EAPoL** سرنام **EAP over LAN** نیز کار می‌کند. نسخه‌های مختلف و سازگاری با EAP ارائه شده‌اند، اما از رایج‌ترین این نسخه‌ها می‌توان به PEAP، EAP-FAST و EAP-TLS اشاره کرد که برای آزمون **نتورک‌پلاس** باید اطلاعاتی در مورد آن‌ها داشته باشید.

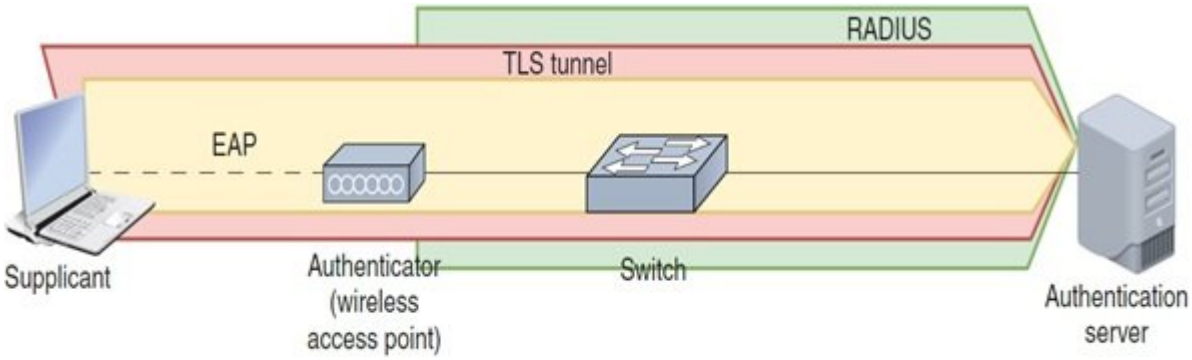
EAP-TLS

همان‌گونه که پروتکل HTTPS از رمزگذاری SSL / TLS برای ایمن‌سازی انتقال روی پروتکل HTTP استفاده می‌کند، EAPTLS از رمزنگاری TLS برای محافظت از ارتباطات استفاده می‌کند. EAP-TLS همچنین از گواهینامه زیرساخت کلید عمومی (PKI) برای تبادل کلیدهای عمومی و احراز هویت در ارتباط با سرور و درخواست‌کننده تایید اعتبار استفاده می‌کند. در حالی که پیکربندی این گواهی‌نامه‌ها چالش خاص خود را دارد، اما اگر به درستی پیاده‌سازی شوند، یک مکانیزم احراز هویت قدرتمند را پیاده‌سازی می‌کنند. شکل زیر نحوه اضافه کردن یک CA سرنام Certificate Authority به شبکه به منظور کمک به مدیریت بهتر گواهی‌نامه‌های موردنیاز EAP-TLS را نشان می‌دهد.



Protected EAP

در حالی که EAP-TLS مبتنی بر گواهی است، PEAP سرنام Protected EAP و EAP-FAST مبتنی بر تونل هستند.PEAP سرنام Protected EAP قبل از آن‌که فرآیند پردازش با EAP را آغاز کند یک تونل TLS رمزگذاری شده بین درخواست کننده و سرور ایجاد می‌کند. همان‌گونه که شکل زیر نشان داده شده است، PEAP ابتدا از یک روش بیرونی استفاده کرده و در ادامه شکل دیگری از EAP که روش درونی نام دارد را استفاده می‌کند که فرآیندی است که درون تونل محافظت شده اجرا می‌شود. رایج‌ترین روش درونی EAP-MSCHAPv2 است که یک نشست MS-CHAPv2 در داخل تونل شاید به سرور RADIUS یا فراتر از Active Directory را پیاده‌سازی می‌کند.



EAP-Flexible Authentication via Secure Tunneling

تأیید هویت انعطاف‌پذیر EAP از طریق تونل زدن امن (EAP-FAST) سرنام EAP-Flexible Authentication via Secure Tunneling شکل دیگری از یک تونل EAP است. این مکانیزم از سوی سیسکو توسعه یافته و شبیه به PEAP کار می‌کند، با این تفاوت که سریع‌تر است. EAP-FAST از گواهی‌نامه‌های دسترسی محافظت شده (PACها) سرنام Protected Access Credentials استفاده می‌کند که تا حدودی شبیه کوکی‌هایی است که وب‌سایت‌ها در کامپیوتر کاربر برای ردیابی فعالیت‌هایش ذخیره می‌کنند. PAC در دستگاه درخواست کننده برای ایجاد سریع‌تر تونل TLS به منظور استفاده در نشست‌های آینده ذخیره می‌شود.

شکل زیر خلاصه‌ای از مباحثی که به آن‌ها اشاره شد را نشان می‌دهد.

Security method	Type	Primary use(s)	Notes
IPsec	Encryption	TCP/IP transmissions	
SSL		TCP/IP transmissions	
TLS			Secure transmission of HTTP sessions
PPP	Connection	Remote access	
SSH	Connection, Authentication, Encryption		
RDP			
VNC			
L2TP	Tunneling	VPN	
GRE		VPN	
OpenVPN			
IKEv2			
VTP			
SHA		Data integrity	
LDAP	Authentication	Directory access	
Kerberos		Client validation	Verify the identity of clients and securely exchange information after a client logs on to a system
RADIUS			Central authentication point for network users, including wireless, mobile, and remote users
TACACS+	AAA (Authentication, Authorization, and Accounting)	Client validation and monitoring	
EAP		Client verification	
802.1X			
AES		Wi-Fi and other uses	

مطالبی که در چند شماره گذشته مشاهده کردید، از مهم‌ترین مباحثی بودند که آزمون **نتورک‌پلاس** از شما انتظار دارد مطالبی در مورد آن‌ها داشته باشید. لازم به توضیح است در ارتباط با مبحث ایمن‌سازی شبکه‌های بی‌سیم شما ابتدا باید در مورد توپولوژی‌های شبکه‌های بی‌سیم اطلاعاتی به دست آورید. بر همین اساس پیشنهاد می‌کنم به مقاله **types-of-wireless-networks** مراجعه کنید که اطلاعات مهمی در اختیارتان قرار می‌دهد.

ما مبحث طراحی امنیت در شبکه‌ها را در همین جا خاتمه می‌دهیم، هرچند پیشنهاد می‌کنیم درباره هر یک از مباحثی که اشاره شد، پژوهش بیشتری انجام دهید. اکنون به سراغ مبحث عملکردها و بازیابی شبکه‌ها خواهیم رفت.

Network Performance and Recovery

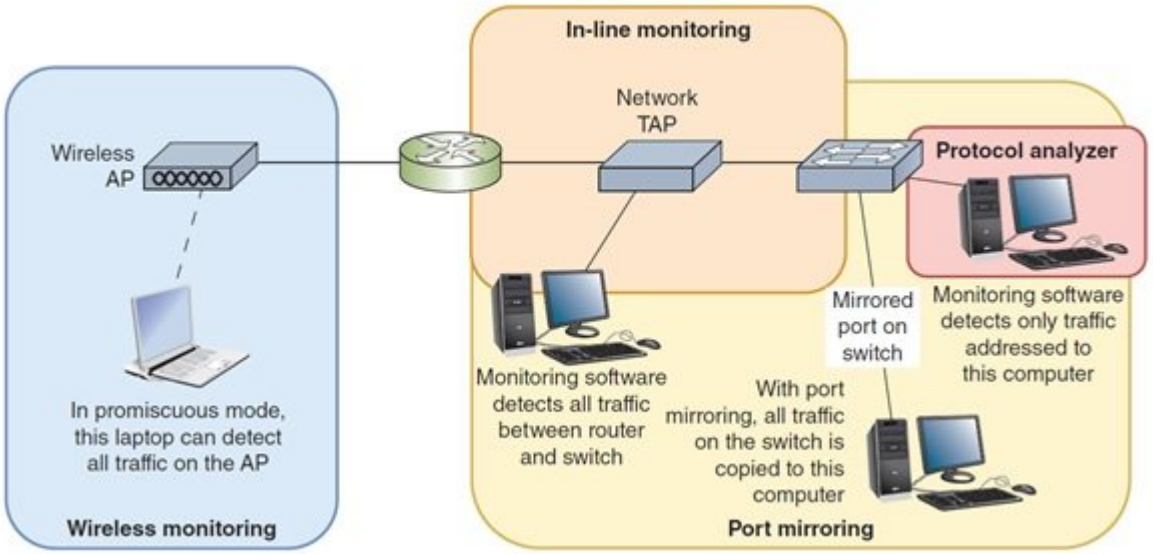
از آنجایی که شبکه‌ها قلب تپنده هر سازمانی هستند در نتیجه مواردی همچون دسترسی ایمن به منابع شبکه و بهینه‌سازی عملکرد شبکه‌ها باید به شکل دقیقی بررسی شود. در چند شماره آتی مطالبی درباره شبکه‌های مقیاس‌پذیر، قابل اعتماد و همچنین انتخاب مناسب‌ترین سخت‌افزار، توپولوژی و خدمات قابل استفاده در شبکه مطالبی را خواهید آموخت.

جمع‌آوری داده‌ها از شبکه

مدیریت شبکه یک اصطلاح عمومی است که فرآیند اداره کردن و رسیدگی به مولفه‌های مختلف در شبکه‌های مختلف را شامل می‌شود. در حالت کلی مدیریت شبکه به ارزیابی، نظارت و نگهداری از تمام ابعاد شبکه اشاره دارد. این مدیریت می‌تواند شامل کنترل دسترسی کاربران به منابع شبکه، نظارت بر عملکرد زیربنایی و اساسی، بررسی خطاهای سخت‌افزاری، اطمینان از کیفیت خدمات (QoS) برای برنامه‌های کاربردی مهم، حفظ سوابق مرتبط با دارایی‌های شبکه و تنظیمات نرم‌افزار و تعیین زمان به‌روزرسانی تجهیزات سخت‌افزاری و نرم‌افزارها اشاره دارد. مدیریت شبکه با هدف جلوگیری از خرابی و کاهش هزینه‌ها انجام می‌شود. ما قبل از اینکه بتوانید مسائل مربوط به صحت و درستی شبکه‌ها را بررسی و پیش‌بینی کنید، ابتدا باید ساختار منطقی و فیزیکی شبکه و نحوه عملکرد آن در شرایط معمولی را درک کنید. برای انجام این کار باید بتوانید اطلاعات مربوط به ترافیک شبکه را جمع‌آوری کنید.

ابزارهای مانیتورینگ

یک ابزار نظارت بر شبکه به‌طور مداوم ترافیک شبکه را تحت بررسی قرار می‌دهد. یک پروتکل تجزیه و تحلیل شبکه یک ابزار شبکه است که می‌تواند ترافیک را برای یک رابط خاص که میان کلاینت و یک شبکه قرار می‌گیرد رصد کند. در عمل، ابزارهای نظارت بر شبکه و پروتکل تحلیل‌گر شبکه زمانی که صحبت از نوع داده‌هایی به میان می‌آید که باید جمع‌آوری شوند تفاوت‌های قابل توجهی با یکدیگر دارند. به‌طور مثال، Spiceworks یک نوع نرم‌افزار نظارت بر شبکه است زیرا می‌توان آن‌را برای نظارت آنی بر چند دستگاه در یک شبکه پیکربندی کرد. Wireshark یک نوع پروتکل تجزیه و تحلیل است، زیرا ترافیک یک رابط که میان یک دستگاه واحد و شبکه قرار دارد را بررسی می‌کند. دقت کنید برنامه‌هایی شبیه به Wireshark یا سایر برنامه‌های نظارتی که به شکل تجمیع شده روی کامپیوتری اجرا می‌شوند که به یک سوئیچ متصل شده است این توانایی را ندارند تا تمام ترافیک شبکه را ببینند؛ بلکه تنها ترافیکی که سوئیچ ارسال می‌کند را مشاهده می‌کنند که شامل ترافیک پخشی و ترافیک خاص یک کامپیوتر است در شکل زیر به کامپیوتری که درون جعبه قرمز سمت راست قرار دارد نگاه کنید.



برای ردیابی بیشتر ترافیک شبکه، شما می‌توانید یکی از این روش‌های نشان داده شده در شکل بالا را استفاده کنید.

• نظارت بی‌سیم - اجرای نرم‌افزار نظارت روی یک کامپیوتر که به شکل بی‌سیم به شبکه متصل شده است. کامپیوتری که شکل بالا در سمت چپ قرار گرفته است. برای اینکه کامپیوتر تمام ترافیک را ببیند، آداپتور شبکه باید از حالت بی‌قاعده (Promiscuous mode) پشتیبانی کند. در حالت بی قاعده، یک دیوایس درایور کارت شبکه تمامی فریم‌های بی‌سیم را به سمت سیستم‌عامل و نرم‌افزار رصد کننده هدایت کند. معمولا حالت فوق در برنامه‌های مانیتورینگ فعال است. اما گاهی اوقات باید ویژگی فوق را روی سیستم‌عامل فعال کنید.

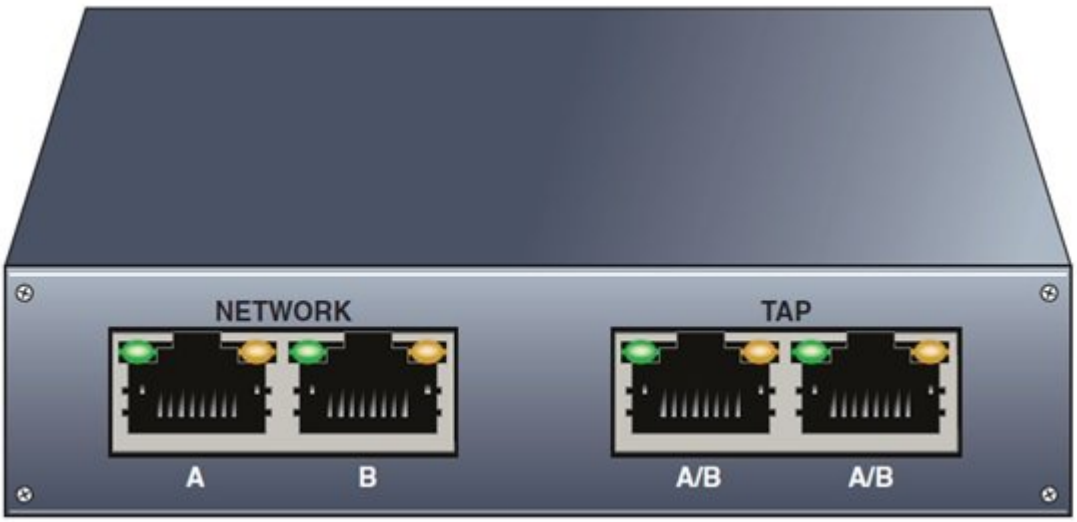
• نظارت بر پورت – از طریق نظارت بر پورت، همه ترافیک روی یک سوییچ برای یک کامپیوتر کپی می‌شود.

• نظارت درون خطی - یک دستگاه که Network TAP یا شنودکننده بسته (sniffer packet) نام دارد به شکل درون خطی نصب شده تا ترافیک شبکه را رصد کند. همان‌گونه که در شکل زیر مشاهده می‌کنید یک چنین دستگاهی چهار پورت دارد.

○ دو پورت همه ترافیک ارسالی میان یک سوییچ و روتر را دریافت می‌کند.

○○ پورت سوم ترافیک را قرینه می‌کند و آن‌را برای یک کامپیوتر که نرم‌افزار نظارتی همچون Wireshark را در وضعیت بی قاعده اجرا می‌کند ارسال می‌کند.

○○ پورت چهارم برای پیکربندی دستگاه استفاده می‌شود.



در شماره آینده آموزش **نتورک‌پلاس** مبحث فوق را ادامه خواهیم داد.

تاریخ انتشار:
18 خرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15495/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3-network-%D8%A8%D8%AE%D8%B4-59