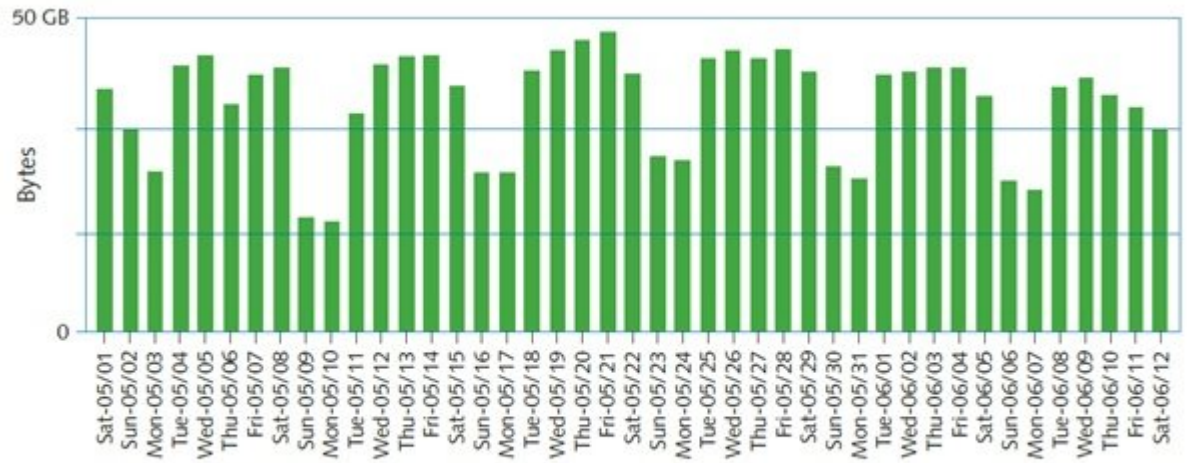
آموزش رایگان دوره نتورک‌پلاس (Network+) (بخش 61)

در شماره گذشته آموزش نتورک‌پلاس با قابلیت‌های ارائه شده از سوی ابزارهای نظارت بر شبکه، گزارش‌گیری و نحوه خواندن گزارش‌ها، نقش پروتکل SNMP در تهیه گزارش‌ها و سرور NMS آشنا شدیم. در این شماره مبحث فوق را ادامه خواهیم داد.

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

معیاری برای ارزیابی عملکرد

برای آن‌که مشخص کنید شبکه در چه زمانی دچار مشکل شده است، ابتدا باید اطلاعاتی در ارتباط با وضعیت عادی شبکه در اختیار داشته باشید. برای این منظور باید یک خط پایه که بیان‌گر وضعیت عادی شبکه است ترسیم کنید. خط پایه متشکل از سنجه‌هایی است که از طریق تحلیل ترافیک شبکه به دست آمده و ممکن است شامل اطلاعاتی درباره نرخ استفاده از شبکه، تعداد کاربرانی که هر روز یا هر ساعت به شبکه وارد می‌شوند، تعداد پروتکل‌هایی که روی شبکه اجرا می‌شوند، آمار مربوط به خطاها (jabbers، runts یا Gaints)، بسامدی که برنامه‌های تحت شبکه از آن استفاده می‌کنند یا اطلاعاتی مربوط به کاربرانی باشد که از پهنای باند بیشتر استفاده می‌کنند. نمودار زیر یک خط پایه ساده برای ترافیک روزانه شبکه در یک بازه شش هفته‌ای را نشان می‌دهد.



معیارهای تعیین شده در خط پایه به شما اجازه می‌دهند در آینده عملکرد شبکه و عواملی که به واسطه تغییرات در شبکه یا اتفاقات مختلف باعث افزایش یا کاهش عملکرد شبکه می‌شوند را با یکدیگر مقایسه کنید. به‌دست آوردن سنجه‌های خط مبنا تنها روشی است که با استناد بر آن می‌توانید مشخص کنید که آیا الگوی استفاده تغییر کرده و به توجه نیاز دارد یا لازم است در آینده یکسری از فاکتورهای شبکه ارتقا پیدا کنند. هر شبکه‌ای رویکرد خاص خود را طلب می‌کند. به عبارت دقیق‌تر برای ارزیابی هر شبکه‌ای باید یک برنامه قابل اعتماد برای ثبت و بررسی خطوط پایه به منظور شناسایی تغییرات غیر منتظره تدوین کنید. به‌طور مثال شما باید به سراغ اندازه‌گیری و نظارت بر عناصری بروید که برای شبکه و کاربران حائز اهمیت است.

الگوهای ترافیک شبکه در طول زمان می‌توانند به‌طور قابل توجهی تغییر کنند که این تغییرات به دو عامل اصلی زیر تقسیم می‌شوند:

• تغییرات عادی در طول روز، هفته، ماه و فصل‌های مختلف. به‌طور مثال، یک شرکت خرده فروشی بزرگ در طول فصل تعطیلات، الگوهای ترافیکی شلوغی دارد و این مسئله برای شبکه چنین شرکتی کاملا طبیعی است.

• تغییراتی که برخواسته از یک اتفاق غیر قابل پیش‌بینی بوده و روی شبکه اثرگذار بوده‌اند. به‌طور مثال، در مثال پاراگراف قبل فرض شده است که کاربران جدید و کاربران قدیمی خرده فروشی عادت‌های یکسانی دارند. اما این احتمال وجود دارد که کاربران جدید مقدار قابل توجهی از ترافیک شبکه را به خود اختصاص دهند.

ابزارهای کاربردی مختلفی وجود دارند که در تهیه خط پایه به شما کمک می‌کنند. قبل از آن‌که به فکر خرید یک نرم‌افزار تجاری یا دانلود یک نرم‌افزار رایگان باشید به این مسئله فکر کنید که قرار است چه کاری با ابزار فوق انجام دهید. پس از آن‌که ابزار خود را انتخاب و داده‌ها را جمع‌آوری کردید، در مرحله بعد باید به فکر تحلیل داده‌ها باشید. از جمله معیارهای عملکردی رایج که برای ارزیابی وضعیت یک شبکه استفاده می‌شوند به موارد زیر می‌توان اشاره کرد:

• مصرف- فاکتور فوق به توان عملیاتی واقعی استفاده شده به عنوان درصدی از پهنای باند موجود در دسترس اشاره دارد. میزان مصرف در هیچ شبکه‌ای نباید به حداکثر ظرفیت خود برسد. شناسایی الگوهای مصرف و حصول اطمینان از اینکه پهنای باند موجود، در دسترس طیف گسترده‌ای از کاربران قرار خواهد گرفت به دقت باید مورد توجه قرار گیرد.

• نرخ خطا- بیت‌هایی هستند که در مدت زمان انتقال به دلایلی همچون وجود میدان‌های الکترومغناطیس یا سایر نویزها آسیب می‌بینند.

• بسته‌های خرد شده- بسته‌هایی که قبل از آن‌که استفاده شوند، آسیب دیده‌اند یا تاریخ اعتبار آن‌ها به اتمام رسیده یا رابط شبکه آن‌ها را رد کرده است. این بسته‌ها باعث ایجاد تاخیر در شبکه می‌شوند، زیرا دستگاه‌ها در انتظار پاسخ یا ارسال دوباره بسته‌ها هستند. آگاهی از این موضوع که چه فعالیتی برای شبکه شما عادی است به شما کمک می‌کند مشکلات را زمانی که نرخ بالای بسته‌های از دست رفته زیاد می‌شود به درستی شناسایی کنید.

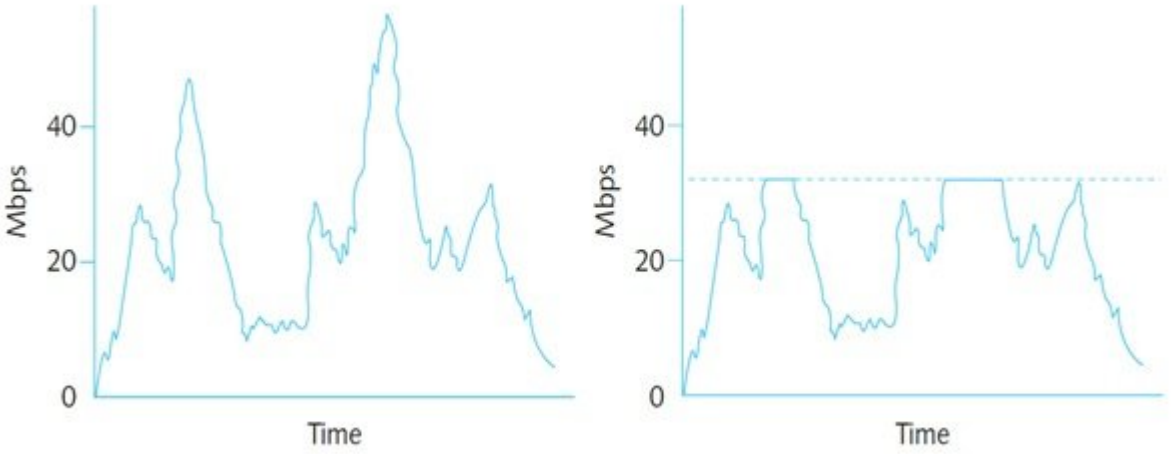
• jitter-همه بسته‌ها همراه با تاخیر به مقصد می‌رسند. هنگامی که بسته‌ها به شکل متوالی تاخیری را تجربه کنند، مشکل زمان انتظار در شبکه بیشتر می‌کنند که نتیجه آن از درست رفتن بسته‌ها بوده و یک تجربه کاربری بد را برای مخاطب رقم می‌زنند. به این مشکل jitter گفته می‌شود که از طریق به‌کارگیری تکنیک‌های مدیریت ترافیک می‌توان آن‌را اصطلاح کرد.

مدیریت ترافیک شبکه

پس از آن‌که داده‌های مرتبط با الگوهای ترافیکی شبکه را جمع‌آوری کرده و خط مبنا را آماده کردید، در مرحله بعد باید وضعیت شبکه را به‌طور مداوم زیر نظر گرفته و تغییراتی که باعث می‌شوند کاربران بهترین تجربه کاربری را داشته باشند پیاده‌سازی کنید. این فرآیند دو عامل مدیریت بر عملکرد (**performance management**) که نظارت و حصول اطمینان از این‌که دستگاه‌ها به درستی به شبکه متصل شده‌اند و مدیریت خطاها (**fault management**) که خطاهای مرتبط با ارسال سیگنال برای دستگاه‌ها را بررسی کرده و مولفه‌هایی که باعث بروز اشکال در این زمینه می‌شوند را شناسایی می‌کند، در بر می‌گیرد

مدیریت ترافیک

زمانی‌که یک شبکه باید حجم بالایی از ترافیک را مدیریت کند، مدیریت بر عملکرد و روش بهینه‌سازی تاثیر قابل توجهی بر ترافیک داشته و اجازه می‌دهد کاربران بدون مشکل از شبکه استفاده کنند. قالب‌بندی ترافیک که برخی مواقع قالب‌بندی بسته نیز نامیده می‌شود، به ویرایش ویژگی‌های خاص بسته‌ها، جریان‌های داده‌ای یا مدیریت ارتباطات، نوع و حجم ترافیکی که باید روی یک شبکه یا رابط در یک لحظه انتقال پیدا کند اشاره دارد. هدف این است که اطمینان حاصل شود ترافیک در زمان به موقع به مقصد خواهد رسید و کاربران کمترین زمان تاخیر را تجربه کنند. شکل‌دهی ترافیک می‌تواند مواردی همچون تاخیر در ترافیک کمتر با اهمیت شبکه، افزایش اولویت ترافیک حائز اهمیت، محدود کردن حجم ترافیك که در يك دوره مشخص باید وارد یا از آن خارج شود، محدودیت‌های مقطعی در ارتباط با نرخ توان عملیاتی برای هر رابط را شامل شود. دو مورد آخر در قالب سیاست‌گذاری ترافیک (**traffic policing**) شهرت دارند. شکل زیر نشان می‌دهد که چگونه حجم ترافیک روی یک رابط که فاقد اعمال محدودیت است به یکباره افزایش پیدا کرده یا برعکس روی مرز مشخصی تنظیم شده است.



اولویت‌بندی ترافیک شبکه به شکل‌های مختلفی می‌تواند انجام شود، اما نکته مهمی که وجود دارد پیاده‌سازی درست این اولویت‌بندی است، زیرا اگر اولویت‌ها به شکل درستی پیاده‌سازی نشوند ممکن است موجبات نارضایتی کاربران را به همراه داشته باشند. این مسئله به ویژه در ارتباط با شرکت‌های ارائه خدمات اینترنتی که اولویت‌بندی خاصی برای پهنای باند در نظر می‌گیرند صدق می‌کند. نرم‌افزار در حال اجرا روی یک روتر، سوئیچ چند لایه، گیت‌وی، سرور یا حتی یک ایستگاه کاری کلاینت می‌تواند به عنوان یک شکل‌دهنده ترافیک استفاده شده و بر مبنای ویژگی‌های پروتکل، نشانی آی‌پی، گروه کاربران، پرچم DiffServ سرنام Differentiated Services در یک بسته IP، برچسب VLAN در فریم لایه پیوند داده و سرویس یا برنامه به اولویت‌بندی ترافیک بپردازد.

بسته به نرم‌افزار اولویت‌بندی، ترافیک ممکن است به کلاس‌های اولویتی همچون بالا، عادی، کند یا آهسته تقسیم شود. به‌طور متناوب، می‌توان ترافیک را از 0 (کمترین اولویت) تا 7 (بالاترین اولویت) رتبه‌بندی کرد. به‌طور مثال، می‌توان برای برنامه‌های VoIP که حساسیت زمانی بالایی دارند اولویت بالایی تعیین کرد، در حالی که برای بازی‌های آنلاین اولویت کم (یا برعکس، بسته به تشیخص شما) را تعیین کرد. اولویت‌بندی ترافیک بیشتر زمانی لازم است که شبکه شلوغ باشد. این رویکرد تضمین می‌کند که در طول زمان استفاده حداکثری، داده‌هایی که حائز اهمیت هستند به سرعت انتقال پیدا می‌کنند، در حالی که داده‌هایی که اهمیت کمتری دارند با کمی تاخیر به مقصد می‌رسند.
همچنین توجه داشته باشید زمانی که شبکه‌ای نه چندان شلوغ در اختیار دارید، اولویت‌بندی ممکن است تاثیرگذاری قابل توجهی نداشته باشد.

تضمین کیفیت سرویس

شما نمی‌خواهید در زمان برقراری یک ارتباط ویدویی آنلاین یا زمانی که در حال تماشای یک فیلم از اینترنت هستید، پیغام در حال بافر شدن است را مشاهده کنید. دقت کنید که انتقال صدا و ویدئو حساس به تأخیر هستند. گاهی اوقات از دست دادن داده‌ها (از جمله فریم‌های ویدئویی)، قابل تحمل است؛ زیرا در زمان انتقال صدا و ویدئو این مشکل عمدتا رخ می‌دهد. گشت و گذار عادی در وب ممکن است به پهنای باند چندان بالایی نیاز نداشته باشد، اما

زمانی که در حال استریم کردن فیلم یا برقراری یک تماس صوتی و تصویری آنلاین هستید یا دستگاه دیگری در حال انجام بازی آنلاین است که همه این دستگاه‌ها به پهنای باند سنگینی نیاز دارند، آن‌گاه باز کردن یک صفحه نیز به سختی امکان‌پذیر است. برای مدیریت درست همه این درخواست‌ها، مدیران شبکه به سراغ تکنیک **QoS** سرنام **Quality of Service** می‌روند. QoS مجموعه‌ای از تکنیک‌هایی است که اجازه می‌دهد برای دستگاه‌های مختلف اولویت‌بندی مشخصی را تنظیم کنید. برای انجام این کار، مدیران شبکه باید در مورد برنامه‌هایی که تحت شبکه اجرا می‌شوند، منجمله پروتکل‌های کاربردی که از آن‌ها استفاده می‌شود و همچنین میزان پهنای باندی که برنامه‌ها استفاده می‌کنند اطلاعاتی داشته باشند. به‌طور مثال، تاخیر متغیر در بسته‌های VoIP منجر به کاهش کیفیت صدا می‌شود. شبکه‌ای که حجم بالایی از ترافیک VoIP را مدیریت می‌کند، باید ترافیک را به درستی اولویت‌بندی کند تا مشکلاتی همچون jitter گریبان‌گیر شبکه نشود.

Differentiated Services

DiffServ سرنام Differentiated Services یک تکنیک ساده است که مشکلات مربوط به QoS را با اولویت‌بندی ترافیک در لایه 3 حل می‌کند. به عبارت دقیق‌تر برای روترها سطح اولویت‌بندی بسته‌هایی که قرار است پردازش شوند را مشخص می‌کند. DiffServ به جای آن‌که تنها سرویس‌های با حساسیت زمانی همچون صدا و ویدیو را بررسی کند انواع مختلفی از ترافیک شبکه را زیر نظر می‌گیرد. به این ترتیب، می‌تواند به استریم‌های صوتی اولویت بالایی تخصیص داده و در همان زمان به استریم‌های داده‌ای غیر ضروری (به‌طور مثال کارمندی که در زمان ناهار در حال وب‌گردی است)، اولویت کمتری را تخصیص دهد. این تکنیک از سرویس‌هایی که حساسیت زمانی بالایی دارند به بهترین شکل محافظت کرده و اولویت درستی به آن‌ها تخصیص می‌دهد. برای اولویت‌بندی ترافیک، DiffServ اطلاعات را درون فیلد DiffServ از یک بسته IPv4 قرار می‌دهد. 6 بیت اول از این فیلد 8 بیتی DSCP سرنام Differentiated Services Code Point) نام دارد. در بسته‌های IPv6 تکنیک DiffServ از یک فیلد مشابه به نام Traffic Class استفاده می‌کند. اطلاعات ارائه شده از سوی این تکنیک در بسته‌های IPv4 و IPv6 به روترهای شبکه نشان می‌دهد چگونه جریان داده‌ها باید منتقل شوند. DiffServ دو نوع فوروارد کردن به شرح زیر را تعریف می‌کند:

•EF سرنام Forwarded Forwarding–این تکنیک تاخیرهایی که باعث می‌شوند سرعت انتقال طبیعی داده‌ها با کندی همراه باشد را به دام انداخته و اجازه می‌دهد داده‌ها به موقع به مقصد برسند.

•AF سرنام Assured Forwarding - سطوح مختلفی از منابع روتر را می‌توان به استریم‌های داده‌ای اختصاص داد. AF مدیریت داده‌ها را اولویت‌بندی کرده، اما تضمین نمی‌دهد در یک شبکه شلوغ پیام‌ها به موقع به مقصد تحویل داده شوند.

Class of Services

کلاس خدمات CoS سرنام Class of Service گاهی به صورت مترادف با QoS شناخته می‌شود، اما یک تمایز مهم در این بین وجود دارد. اصطلاح QoS به تکنیک‌هایی که در لایه‌های مختلف OSI از طریق چندین پروتکل پیاده‌سازی می‌شود اشاره دارد. در مقابل، اصطلاح CoS تنها به تکنیک‌های قابل اجرا در لایه 2 روی فریم‌های اترنت اشاره داشته و یک روش پیاده‌سازی QoS است. CoS اغلب برای کارآمدتر بودن ترافیک اترنت بین VLANها استفاده می‌شود. فریم‌هایی که برچسب‌گذاری شده‌اند (منظور یک VLAN خاص است) شامل یک فیلد 3 بیتی در سرآیند فریم خود هستند که PCP سرنام Priority Code Point نام دارد. CoS با تنظیم این بیت‌ها به یکی از هشت سطح از 0 تا 7 به سوییچ نشان می‌دهد که باید برای پیام یک سطح اولویت مشخص شود، به شریط که پورت در حال دریافت ترافیکی فراتر از آن چیزی باشد که قادر به فوروارد کردن آن در یک لحظه است. پیام‌های در حال انتظار تا وقتی که پورت بتواند به آن‌ها دسترسی پیدا کند ذخیره شده یا از دست می‌روند. فرآیند کش کردن یا حذف بسته‌ها به نوع کلاسی که به فریم تخصیص داده شده است بستگی دارد. دستگاه‌های ارتباطی شبکه و کلاینت‌ها برای آن‌که بتوانند از مزایای QoS استفاده کنند باید از مجموعه پروتکل‌های یکسانی پشتیبانی کنند. البته شبکه‌ها می‌توانند - و اغلب – چند تکنیک QoS را با یکدیگر ترکیب می‌کنند.

دسترس‌پذیری شبکه

در دنیای شبکه‌سازی، دسترس‌پذیری به قابل اعتماد بودن و تداوم یک اتصال، سامانه یا سایر منابع شبکه که می‌توانند در اختیار افراد مجاز قرار بگیرد اشاره دارد. این دسترس‌پذیری اغلب با درصدی در محدوده 98٪ یا 99.5٪ نشان

داده می‌شود. اصطلاح دسترس‌پذیری بالا (HA) سرنام high availability به سیستمی اشاره دارد که به طور قابل اطمینانی تقریبا تمام وقت عمل می‌کند. به‌طور مثال، سروری که به کارکنان اجازه ورود، استفاده از برنامه‌ها و داده‌ها را می‌دهد و سطح دسترس‌پذیری آن به شدت بالا است با ضریب 99.999 درصد توصیف می‌شود، زیرا کارکنان در هر زمانی قادر هستند به شبکه دسترسی داشته باشند.

یکی از راه‌های سنجش دسترس‌پذیری، اندازه‌گیری یک سیستم یا محاسبه میزان زمانی است که یک سرور که قابل روشن شدن است به درستی کار می‌کند. به این فرآیند network uptime گفته شده و مدت زمان یا درصدی که شبکه میان خرابی‌های به شکل عادی کار می‌کند را نشان می‌دهد. شکل زیر نشان می‌دهد، سیستمی که بتواند در 99.999 درصد به درستی کار کند، به‌طور متوسط تنها در 5 دقیقه و 15 ثانیه در سال غیر قابل دسترس است!

Availability	Downtime per day	Downtime per month	Downtime per year
99%	14 minutes, 23 seconds	7 hours, 18 minutes, 17 seconds	87 hours, 39 minutes, 29 seconds
99.9%	1 minute, 26 seconds	43 minutes, 49 seconds	8 hours, 45 minutes, 56 seconds
99.99%	8 seconds	4 minutes, 22 seconds	52 minutes, 35 seconds
99.999%	.4 seconds	26 seconds	5 minutes, 15 seconds

در ویندوز 10 از طریق Task Manager قادر به مشاهده اطلاعات uptime هستید و در لینوکس یا یونیکس باید این اطلاعات را از طریق فرمان uptime به دست آورید.

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

تاریخ انتشار:

22 خرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15535/%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%B4-61