



آستانه تحمل خطای شبکه، افزونگی،
افزونگی پیوندها، پشتیبان‌گیری از
داده‌ها، پروتکل مسیریاب اضافه مجازی،
پروتکل آدرس اضافه مشترک

در شماره گذشته آموزش نتورک پلاس با مبحث تعیین معیار برای ارزیابی عملکرد شبکه و ضرورت ایجاد آن، مدیریت ترافیک، تضمین کیفیت سرویس، Differentiated Services، Class of Services و دسترس‌پذیری شبکه آشنا شدیم. در این شماره به سراغ مبحث خطا و آستانه تحمل خطا در شبکه خواهیم رفت.

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

آستانه تحمل خطا

یک عامل کلیدی در حفظ دسترسی به منابع شبکه، تحمل خطا یا ظرفیت یک سیستم برای ادامه کار تا زمانی است که ناسازگاری غیرمنتظره سخت‌افزاری یا نرم‌افزاری به وجود آمده است. بهترین راهکاری که اجازه می‌دهد یک شبکه آستانه تحمل خطای بالایی در برابر مشکلات داشته باشد، ایجاد مسیرهای متعدد است که برای انتقال داده‌ها از یک نقطه به نقطه دیگر استفاده می‌شوند. در این حالت اگر یک اتصال یا یک مولفه موفق نشود از یک مسیر داده‌ها را به درستی انتقال دهد، سایر مسیرها می‌توانند جایگزین این مسیر شوند. برای درک بهتر مسائل مربوط به آستانه تحمل خطا، ابتدا باید ببینیم چه تفاوتی میان شکست/خرابی و عیب وجود دارد و هر یک از این واژگان چه نقشی در شبکه بازی می‌کنند.

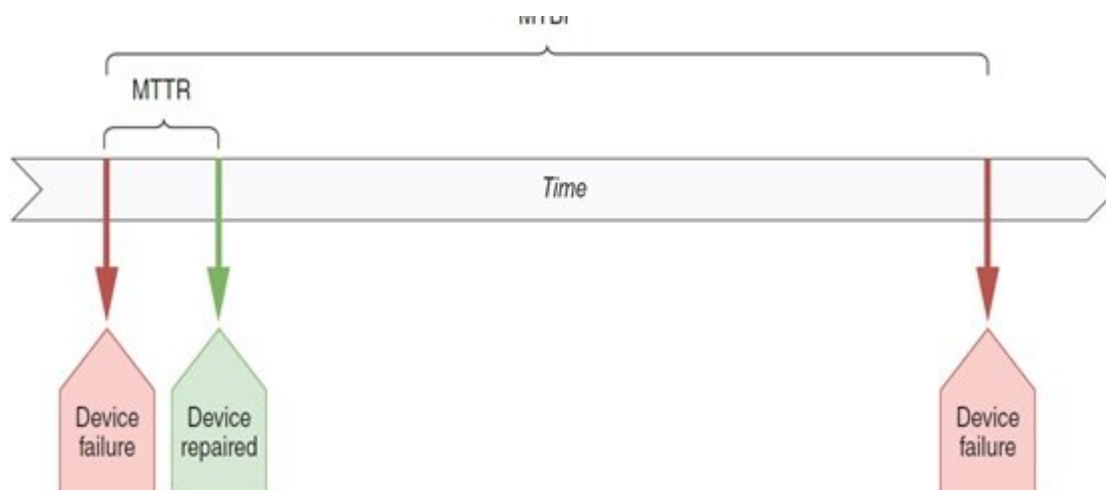
• خرابی/شکست (**failure**) - به انحراف از یک سطح مشخص شده از عملکرد سیستم اشاره دارد که برای یک دوره زمانی خاص رخ می‌دهد. به عبارت دیگر، خرابی زمانی رخ می‌دهد که مولفه‌ای نتواند بر مبنای برنامه‌ریزی از پیش تعیین شده کار کند. به طور مثال، اگر ماشین شما در بزرگراه خراب شود، شما این مسئله را می‌توانید یک خطا یا شکست تصور کنید.

• عیب/خطا (**fault**) - به سوء عملکرد یک مولفه در یک سیستم اشاره دارد. عیب می‌تواند منجر به شکست شود. به طور مثال، عیبی درون واتر پمپ ماشین‌تان که باعث نشستی و از کار افتادن ماشین‌تان در بزرگراه شده در نهایت به خرابی منجر شده است. هدف از پیاده‌سازی یک سامانه آستانه تحمل خطا این است که مانع از آن شوند که عیب‌ها منجر به شکست و خرابی کامل یک شبکه شوند.

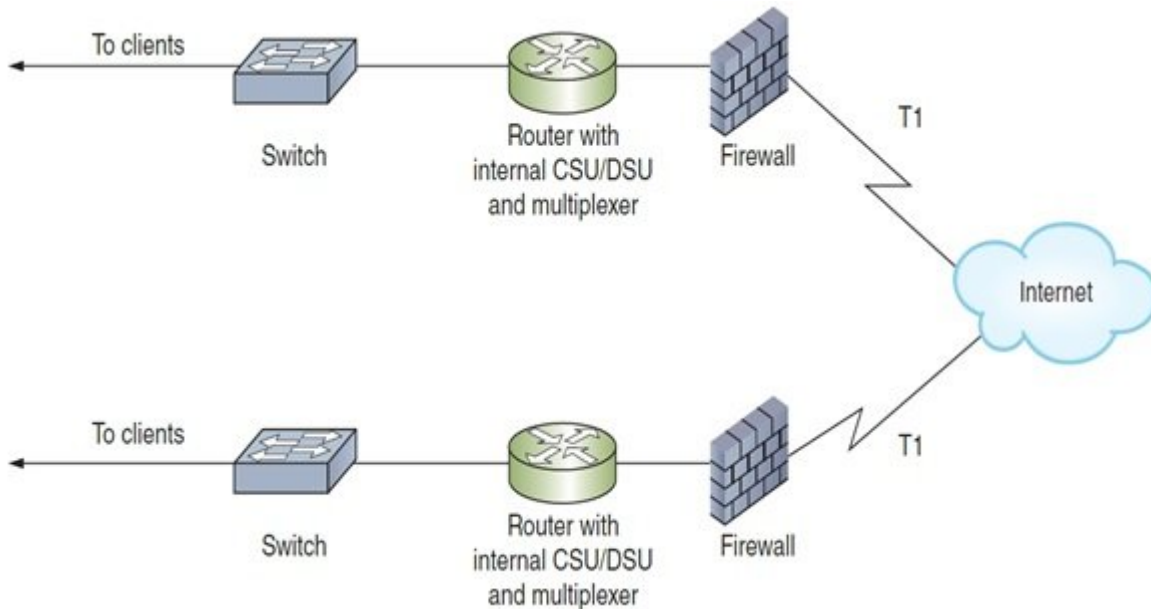
افزونگی

برای دستگاه‌های تحت شبکه، به‌طور معمول، مدت زمان میانگین بین خطاهای سیستم (**MTBF**) سرنام mean time between failures محاسبه می‌شود. این مقدار میانگین، مدت زمانی را نشان می‌دهد که دستگاه‌ها پیش از آن‌که

شکست بعدی را تجربه کنند به کار خود ادامه می‌دهند. هر دستگاهی ممکن است دیر یا زود یک شکست را تجربه کند، بر همین اساس فروشندگان سعی می‌کنند برای فروش بهتر محصول خود روی مقدار نشان داده با MTBF مانور دهند و تکنسین‌ها نیز بر مبنای این مقدار بودجه لازم برای خرید تجهیزات یا تعمیر آن‌ها را در نظر می‌گیرند. هنگامی که یک دستگاه با شکست روبرو شود، مقدار میانگین زمانی که برای تعمیر یک دستگاه سپری می‌شود نیز محاسبه می‌شود. به این مقدار محاسبه شده، میانگین زمان تعمیر (MTTR) سرنام mean time to repair گفته می‌شود. دقت کنید مقدار فوق نیز باید در کنار MTBF به عنوان هزینه خرید محصول در نظر گرفته شود. شکل زیر نشان می‌دهد که چگونه این مفاهیم با یکدیگر مرتبط هستند.

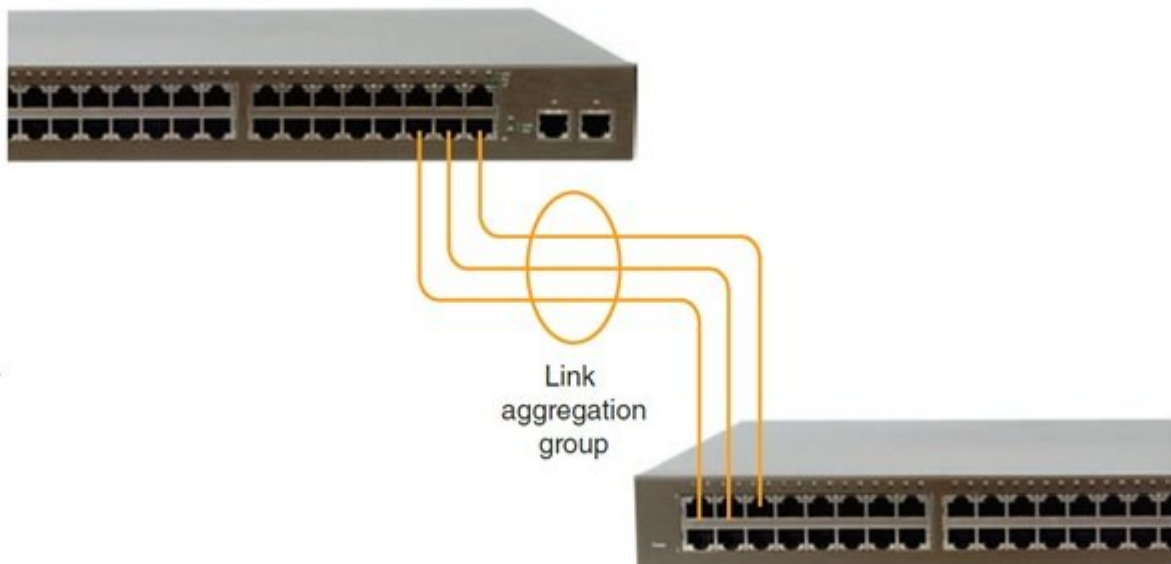


MTBF، MTTR و مفاهیم مربوطه در ارتباط با سرویس‌ها یا سامانه‌ها نیز قابل استفاده هستند. به‌طور مثال یک ISP برای تبلیغ سرویس خود در اساسنامه SLA ممکن است به MTBF و MTTR اشاره کرده باشد. به‌طور مثال، هر زمان اتصال WAN شما قطع می‌شود، ISP ممکن است تضمین داده باشد که طرف دو تا چهار ساعت مشکل را برطرف می‌کند. برای مقابله با پیشامدهایی همچون خرابی‌ها و شکست‌ها در زمان طراحی شبکه‌ها اغلب دو یا چند مورد یکسان از مولفه‌ها، سرویس‌ها یا ارتباطات پیاده‌سازی می‌شوند. اگر یک بخش، سرویس یا اتصال نتواند به درستی کار خود را انجام دهد، نمونه دیگر این فرآیند را متقبل می‌شود. به این مسئله افزونگی (**redundancy**) گفته شده و اشاره به پیاده‌سازی بیش از یک مولفه دارد که درون شبکه نصب شده و آماده است تا برای ذخیره‌سازی، پردازش یا انتقال داده‌ها به کار گرفته شود. افزونگی با هدف برطرف کردن مشکل شکست یا خرابی در یک نقطه خاص که حادثه‌خیز است استفاده می‌شود. به‌طور مثال نصب هارددیسک‌های اضافی برای رفع مشکل خرابی احتمالی هارددیسک‌هایی که در حال استفاده هستند باعث می‌شود تا اصل دسترس‌پذیری به شبکه با بهترین کیفیت حفظ شود. شما باید اطمینان حاصل کنید که برای عناصر مهم شبکه همچون ارتباط با اینترنت یا هارد دیسک سرور جایگزین‌های چندگانه‌ای را در نظر گرفته‌اید تا مشکل خرابی باعث بروز مشکل جدی نشود. وجود منابع تامین برق اضافی برای ساختمان یکی دیگر از مباحث مهمی است که باید به آن رسیدگی شود که البته هزینه قابل توجهی نیز می‌طلبد. همان‌گونه که مشاهده می‌کنید بزرگ‌ترین عیب افزونگی در افزایش هزینه‌ها است، زیرا شما ممکن است برای مدت زمان طولانی از یک مولفه اضافی استفاده نکنید، اما مجبور هستید آن مولفه را برای جلوگیری از بروز یک پیشامد جدی در اختیار داشته باشید. شکل زیر نمونه‌ای از یک پیاده‌سازی اتصال به اینترنت که افزونگی کامل درون آن قرار دارد را نشان می‌دهد که با وجود هزینه بالایی که به همراه دارد، مانع از آن می‌شود که ارتباط شبکه با اینترنت قطع شود.



افزونگی پیوندها (پیوندهای مفرط)

علاوه بر به‌کارگیری مضاعف دستگاه‌ها، شما می‌توانید از اتصالات یا پیوندهای مضاعف میان دستگاه‌های مختلف استفاده کنید. تجمع لینک، ترکیبی یکپارچه از رابط‌های شبکه یا پورت‌های چندگانه است که به عنوان یک رابط منطقی عمل می‌کند و می‌تواند به حل مشکلاتی مانند بروز تنگناها در شبکه کمک کند. این پیاده‌سازی با اصطلاحات دیگری همچون تجمع پورت در دستگاه‌های سیسکو، کارت شبکه در دستگاه‌های ویندوزی یا EtherChannel سیسکو شناخته می‌شود. تجمع پیوند باعث می‌شود دو یا چند کارت شبکه به صورت پشت سرهم یا جفت‌جفت در کنار یکدیگر کار کنند تا ترافیک را میان دو یا چند دستگاه همچون سوئیچ‌ها و سرورها مدیریت می‌کنند. همه پیوندهای فیزیکی که در ساخت یک پیوند منطقی به کار گرفته شده‌اند گروه تجمع لینک (LAG) سرنام link aggregation group نام دارند. شکل زیر پیاده‌سازی چنین ترکیبی را نشان می‌دهد.

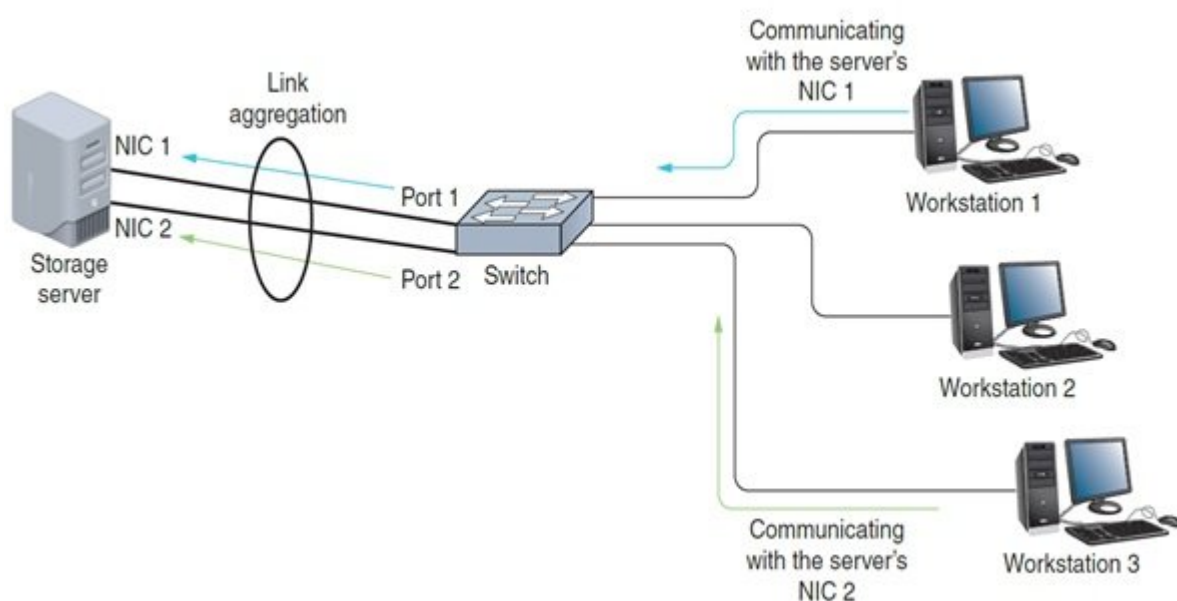


این پیکربندی سه مزیت عمده زیر را دارد:

- افزایش کل توان عملیاتی شبکه
- خودکارسازی غلبه بر خرابی میان کارت‌های شبکه تجمع شده

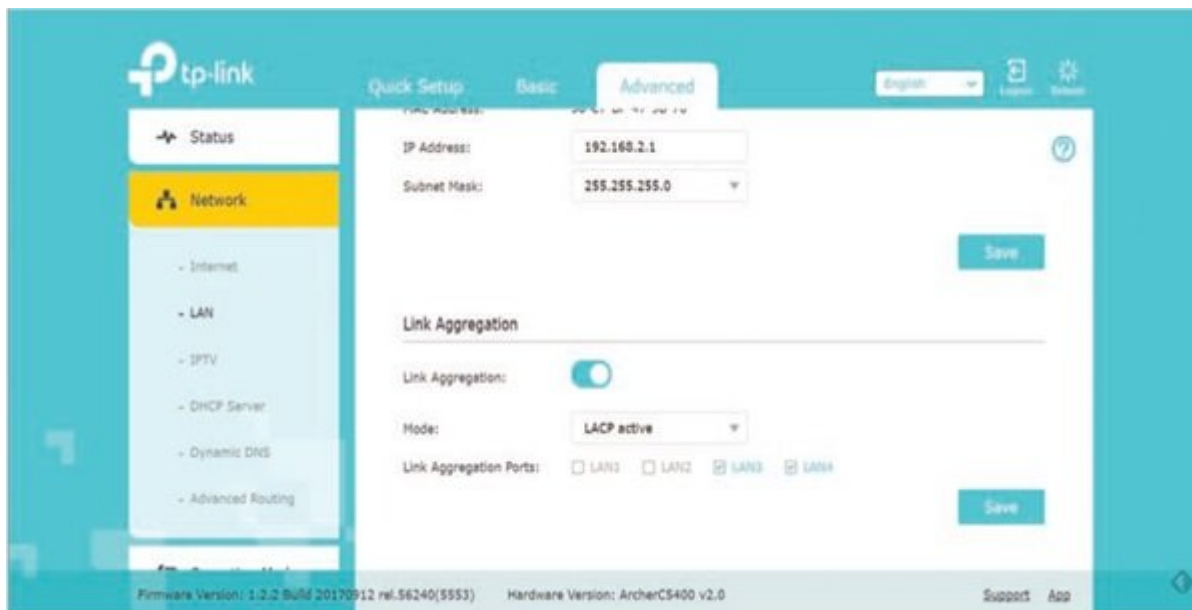
• تعادل‌سازی بار که برای بهینه‌سازی عملکرد و بهبود آستانه تحمل خطا ترافیک روی بیش از چند مولفه یا پیوند توزیع می‌کند.

تجمع پیوند به جای آن‌که در ارتباط با سرعت باشد بیشتر در ارتباط با پهنای باند یا کل ترافیک شبکه و مدیریت هر چه بهتر این مسئله است. تجمع لینک به ویژه در ارتباط با شبکه‌های شلوغ کارایی بالایی دارد. به‌طور مثال، در یک نشست واحد تجمع ارتباطات باعث نمی‌شود تا سرعت آن نشست افزایش پیدا کند. با این حال اگر دو نشست همزمان در حال انتقال داده‌ها هستند، یک نشست می‌تواند یکی از پیوندهای تجمع شده را استفاده کرده و نشست دیگر نیز از پیوند دیگری در همان زمان استفاده کند. در این حالت هیچ‌یک از این دو نشست در حالت انتظار قرار نخواهند گرفت. شکل زیر این مسئله را نشان می‌دهد.

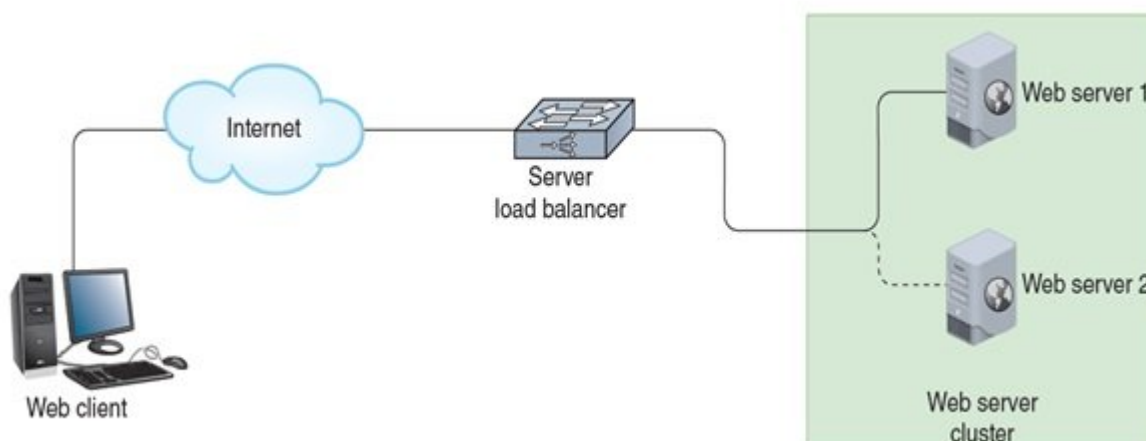


برای آن‌که کارت‌های شبکه یا پورت‌های مختلف بتوانند از قابلیت تجمع لینک استفاده کنند باید به درستی در سیستم عامل پیکربندی شوند. به‌طور مثال، تمام رابط‌های درگیر باید به شکل دو طرفه (full duplex) پیکربندی شوند و سرعت و تنظیمات VLAN و MTU یکسانی داشته باشند. در حال حاضر بسیاری از تولیدکنندگان از پروتکل کنترل تجمع لینک (LACP) سرنام Link Aggregation Control Protocol استفاده می‌کنند که ابتدا در قالب 802.3ad و به تازگی در قالب استاندارد 802.1AX تعریف شده است. LACP به‌طور پویا ارتباطات بین میزبان‌ها روی اتصالات تجمع شده را هماهنگ می‌کند، تقریباً شبیه به کاری که DHCP برای آدرس‌دهی آی‌پی انجام می‌دهد. اکثر این دستگاه‌ها گزینه‌های پیکربندی مشابهی همانند موارد زیر دارند:

- پیکربندی ایستا - هر دو میزبان به صورت دستی پیکربندی می‌شوند تا فرآیند مدیریت تقسیم کار میان لینک‌های مضاعف مطابق با قواعد انجام شوند.
- حالت غیرفعال - پورت به‌طور غیرمستقیم به درخواست‌های تجمع لینک مبتنی بر LACP گوش داده، اما درخواست را مقداردهی اولیه نمی‌کند.
- حالت فعال - پورت به‌طور خودکار و فعال با استفاده از LACP به محاوره با لینک‌ها می‌پردازد. این رویکرد آستانه تحمل خرابی برای یک یا چند پیوند را امکان‌پذیر ساخته و به LACP اجازه می‌دهد برای جبران لینک‌های از دست رفته به‌طور خودکار به تنظیم مجدد لینک‌های فعال بپردازد. در واقع، رویکرد فوق رایج‌ترین پیکربندی برای تمام پورت‌های مرتبط با تجمع لینک‌ها بوده و بیشترین حفاظت در مقابل ناسازگاری‌ها یا خرابی لینک‌ها را فراهم می‌کند. شکل زیر گزینه‌های تجمع لینک در روتر SOHO را نشان می‌دهد.



سرورها می‌توانند از یک دستگاه اختصاصی که وظیفه توزیع هوشمندانه ترافیک میان چند کامپیوتر را بر عهده دارد، استفاده کنند. این دستگاه توازن‌کننده بار نام دارد و تقریباً روی بیشتر سرورها قابل استفاده است. دستگاه فوق می‌تواند تعیین کند که کدام یک از سرورها قبل از فرستادن درخواست برای سرور دیگر بیشترین ترافیک را داشته و کدام سرور ترافیک کمتری داشته است. این استخر سرور (server pool) ممکن است به صورت یک خوشه (کلاستر) پیکربندی شده باشد. خوشه‌بندی به روش دسته‌بندی چندین دستگاه اشاره دارد، به طوری که آن‌ها به صورت یکسان و شبیه به یک دستگاه منفرد در شبکه ظاهر شوند. خوشه‌بندی را می‌توان با گروهی از سرور، روترها یا برنامه‌ها پیکربندی کرد. اگرچه این رویکرد عمدتاً با متعادل‌سازی بار همراه است، اما لزوماً این‌گونه نیست. اجازه دهید به مثالی نگاه کنیم که نشان می‌دهد چگونه خوشه‌بندی و توازن بار ممکن است کار کنند. شکل زیر این مسئله را نشان می‌دهد.



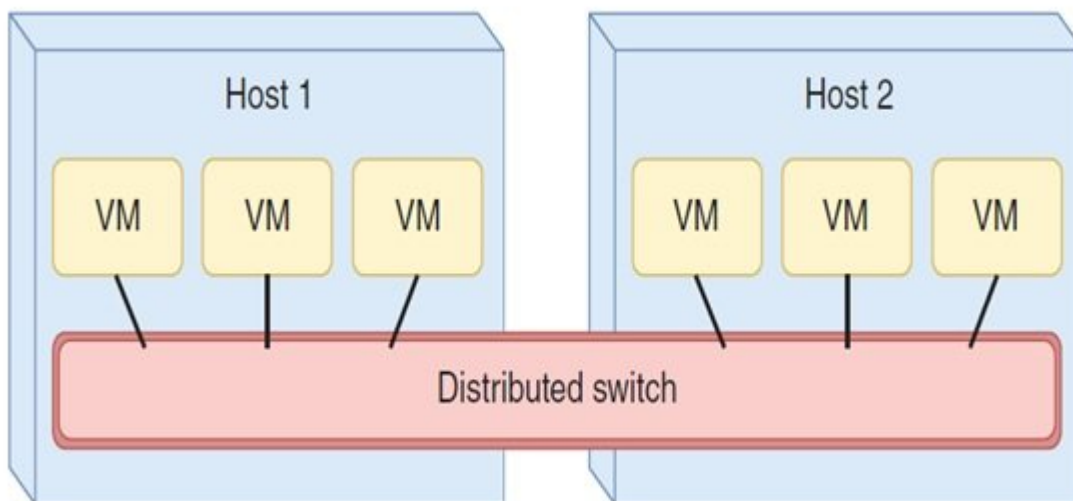
برای دسترسی به یک وب‌سایت، کلاینت‌های وب به‌طور مستقیم یک آدرس آی‌پی مجازی (VIP) را درخواست می‌کنند که نشان‌دهنده یک خوشه کامل است. برای کلاینت، خوشه چیزی شبیه به یک سرور وب منفرد است. یک سامانه تعادل‌کننده بار، ترافیک را به‌طور مساوی بین وب‌سرورها هدایت کرده و هر دو سرور به تمام اطلاعاتی که برای پاسخگویی به صفحات وب درخواستی کلاینت‌ها نیاز دارند دسترسی دارند. با این حال، کلاینت‌ها نمی‌دانند که دو ماشین فیزیکی در حال کار هستند. تا آنجایی که به کلاینت‌ها مربوط می‌شود، آن‌ها می‌دانند که در حال برقراری ارتباط با یک سرور هستند.

در برخی موارد، ممکن است مجموعه‌ای از آدرس‌های آی‌پی را میان چند میزبان به اشتراک قرار دهید. به‌طور مثال، اگر چند روتر دارید که از چند رابط پشتیبانی می‌کنند و می‌خواهید این روترها را به عنوان یک خوشه تحمل خطا با

یکدیگر ترکیب کنید، شما می‌توانید فهرستی از چند آدرس آی‌پی را که به خوشه به عنوان یک گروه اشاره می‌کنند تنظیم کنید. این کار از طریق به‌کارگیری پروتکل آدرس اضافه مشترک (CARP) سرنام Common Address Redundancy Protocol انجام می‌شود که اجازه می‌دهد مجموعه‌ای از رایانه‌ها یا رابط‌ها یک یا چند آدرس آی‌پی را به اشتراک قرار دهند. این مجموعه به عنوان یک گروه افزونگی یا کارگروه افزونگی شناخته می‌شود. هنگام به‌کارگیری پروتکل CARP، یک دستگاه به عنوان رهبر گروه کار کرده، درخواست‌ها را برای یک آدرس IP دریافت کرده و سپس درخواست‌ها را به یکی از چند دستگاه در گروه ارسال می‌کند.

نکته امتحانی: CARP جایگزینی رایگان برای پروتکل مسیریاب اضافه مجازی (VRRP) سرنام Virtual Router Redundancy Protocol یا پروتکل اختصاصی سیسکو موسوم به پروتکل مسیریابی آماده به کار (HSRP) سرنام Hot Standby Routing Protocol است. اگر چه VRRP و HSRP تا حدی عملکردی متفاوت از CARP دارند و فقط برای روترها استفاده می‌شوند، اما ایده کلی این پروتکل‌ها یکسان است.

خوشه‌بندی سرورها به روش‌های مختلفی به منظور گردآوری منابع شبکه و نشان دادن آن‌ها در یک قالب نهاد واحد و همچنین ارائه افزونگی به عنوان راهکاری برای بهبود آستانه تحمل خطا در شبکه استفاده می‌شود. سناریو دیگر به‌کارگیری خوشه‌بندی زمانی است که سرورهایی که ماشین‌های مجازی را میزبانی می‌کنند در یک نهاد به ظاهر واحد جمع‌آوری می‌شوند. در این حالت اگر سرور دچار خرابی شود، به دلیل آن‌که آستانه تحمل خطا افزایش پیدا کرده ماشین‌های مجازی بدون مشکل قابل استفاده خواهند بود. اگر به خاطر داشته باشید به شما گفتیم که ماشین‌های مجازی از طریق یک سویچ مجازی vSwitch که درون هایپرویزور میزبان وجود دارد، به یک شبکه متصل می‌شوند. در یک خوشه سرور، یک سویچ مجازی توزیع شده قادر است به ماشین‌های مجازی که روی میزبان‌های مختلف قرار دارند سرویس‌دهی کند. شکل زیر این موضوع را نشان می‌دهد.



این رویکرد به نام سویچ‌سازی توزیع شده شهرت دارد. از جمله محصولاتی که سویچ توزیع شده را ارائه می‌کنند به VDS شرکت VMware موسوم به vSphere Distributed Switch که به صورت بومی برای پلتفرم itsvSphere ارائه شده و محصولات دیگری همچون Cisco's Nexus 1000v اشاره کرد.

ذخیره‌سازی و پشتیبان‌گیری از داده‌ها

نسخه پشتیبان یک کپی از داده‌ها یا فایل‌های برنامه‌های کاربردی است که به شکل آرشیو شده در مکانی ایمن نگهداری می‌شوند. نگهداری درست از نسخه‌های پشتیبان باعث می‌شود تا قابلیت اطمینان شبکه و آستانه تحمل خرابی شبکه افزایش پیدا کند. اما در هنگام طراحی و پیکربندی سیستم پشتیبان به دو اصل زیر دقت کنید:

اصل 1: ابتدا مشخص کنید قرار است از چه چیزی نسخه پشتیبان تهیه شود. علاوه بر پوشه‌های مشخص که برای نگهداری داده‌ها و برنامه‌های کاربردی استفاده می‌شود، شما ممکن است از پوشه پروفایل کاربران و پوشه‌هایی که فایل‌های پیکربندی برنامه‌ها، سرویس‌ها، روترها، سویچ‌ها، نقاط دسترسی، گیت‌وی‌ها و دیوارهای آتش درون آن‌ها

نگهداری می‌شود پشتیبان بگیرید.

اصل 2: روش‌های تهیه نسخه پشتیبان را انتخاب کنید. پشتیبان‌گیری ابری را بررسی کنید، در حالی که محصولات سخت‌افزاری و نرم‌افزاری ارائه شده از سوی سازندگان ثالث را نیز بررسی می‌کنید. به طور کلی، پشتیبان‌گیری ابری گران‌تر و قابل اطمینان‌تر از سایر روش‌ها است. از آنجایی که پشتیبان‌گیری ابری در فضای محلی شما ذخیره نمی‌شود، شما همواره به نسخه‌ای قابل اعتماد حتی در زمان خرابی تجهیزات محلی و از دست رفتن کلی داده‌ها دسترسی خواهید داشت. البته دقت کنید که باید فروشنده قابل اطمینانی را پیدا کنید. برای یک سامانه پشتیبان‌گیری نباید به سراغ جدیدترین و آخرین فناوری‌های روز بروید، زیرا فناوری‌هایی که تازه به بازار ارائه شده‌اند امتحان خود را پس نداده‌اند.

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

تاریخ انتشار:
25 خرداد 1398

نشانی منبع:

<https://www.shabakeh-mag.com/networking-technology/15552/%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%B4-62>