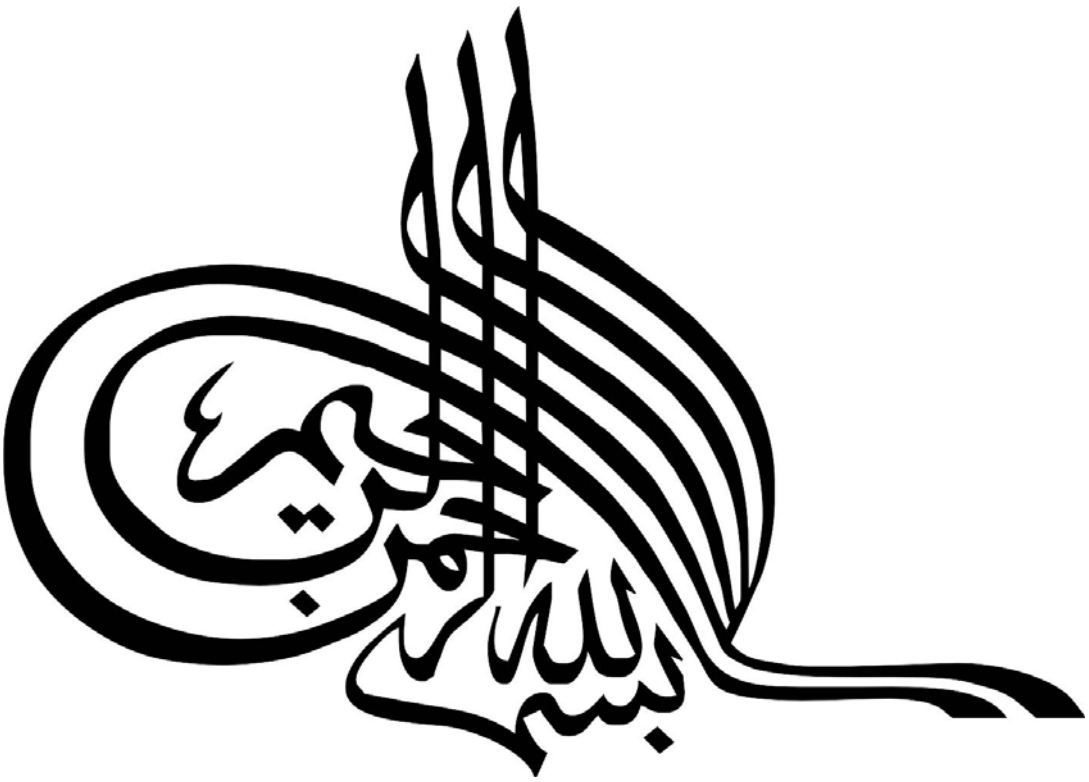
بسم الله الرحمن الرحيم

دانشکده مهندسی برق و کامپیوتر

گروه کامپیوتر

پایان نامه

برای دریافت درجه کارشناسی ارشد

مهندسی فناوری اطلاعات- شبکه های کامپیوتری

بررسی روش های مکان یابی خطا در نقاط حساس شبکه های بزرگ

استاد راهنما: دکتر محمد قاسم زاده

اساتید مشاور: دکتر فضل ا... ادیب نیا، دکتر مهدی آقاصرام

پژوهش و نگارش: مهدی خانی دهنوئی

شهریور ۱۳۸۸

تقدیم به پدر و مادرم

...گرچه می‌دانم این اوراق بی‌بها ذره‌ای از محبتشان را جبران نمی‌کند.

به نام پروردگار بی همتا

در آغاز، برترین سپاس ها و والاترین ستایش ها نثار پروردگار عالمیان باد که تنها او مخصوص چنین ستایشی است و هر آنچه از دانش و غیر آن نصیبمان شد و خواهد شد، همه از الطاف بی پایان اوست و در این الطاف کسی او را شریک نبوده است.

سپس سپاس فراوان و بی پایان، نثار پدر و مادر گرامی ام که بالاترین زحمات را صمیمانه برای رسانیدن من به آنچه هستم، متحمل شده اند.

و پس از آن درود و تشکر من، نثار اساتید محترم اینجانب جناب آقایان دکتر قاسم زاده و دکتر ادیب نیا و دکتر صرام که فراگیری دانش شبکه و در به پایان رسانیدن این پایان نامه مرا یاری نمودند.

و در پایان، از دوستان و بزرگوارانی که به هر نحو مرا در به پایان رسانیدن این مهم یاری نمودند، تشکر و قدردانی می نمایم.

مهدی خانی دهنوئی – شهریور ۸۸

این پایان‌نامه با حمایت‌های مالی

مرکز تحقیقات مخابرات ایران

به انجام رسیده است.

چکیده:

هدف اصلی از ایجاد این پایان نامه، بررسی و ارائه نتایج مربوط به تحقیق و طبقه بندی روشهای مکان یابی خطا در شبکه ها بطور کلی و روشهای مربوط به شبکه های بزرگ و بخصوص قسمت ستون فقرات شبکه ها بصورت جزئی تر می باشد. امروزه افزایش بیش از حد حجم و بزرگی شبکه ها و پیوستگی شبکه های مختلف و اینترنت به یکدیگر و نیز پیچیدگی های حاصل از کاربرد تکنولوژی های جدید در شبکه ها، علاوه بر اینکه مساله بروز خطا را در شبکه ها غیر قابل اجتناب نموده است، نیاز به روش های سازمان یافته و جامع را برای محافظت از شبکه ها و رفع خطا بیش از پیش تقویت کرده است. در این پایان نامه نوعی طبقه بندی برای روش های مکان یابی خطا ارائه شده است که اکثر روش های ارائه شده را در برمی گیرد. در این طبقه بندی، ساز و کار روش های مختلف، به اختصار توضیح داده شده است. مزایا و معایب هر بخش از روش های طبقه بندی شده، تا حد امکان شرح داده شده است. میزان کاربرد این روش ها و جنبه های علمی آنها، پیش نیازهای ریاضی آنها و هزینه های محاسباتی، در صورت لزوم و اهمیت توضیح داده شده اند. همچنین زمینه هایی که نسبت به دیگر بخش های حوزه مکان یابی خطا، میزان تحقیقات کمتری برروی آنها صورت گرفته و علت این نارسایی، تا حد لزوم، توضیح داده شده است. معرفی این بخش ها، برای محققینی که در این زمینه کار می کنند، برای جهت دهی به ایده های جدید، مناسب خواهد بود. دو روش جدید مکان یابی خطا که توسط نویسنده، ایجاد و به جامعه علمی جهانی ارائه شده اند، در دو فصل آخر آورده شده اند. هر دوی این روش ها جدید ترین روش ها در نوع خود هستند و توسط نویسنده ابداع و در اختیار محققین و استفاده کنندگان از دانش شبکه قرار گرفته اند. روش FFL، هرچند دارای پایه علمی کلی و فراگیر است، اما بصورت خاص برای مکان یابی خطا در لایه WDM در شبکه های پشتیبان DWDM مناسب سازی شده است. پس از معرفی این روش و کاربردآن، در فصل هفتم، به معرفی یک سیستم جامع مکان یابی خطا با نام IFMS پرداخته شده است. این سیستم در حقیقت، در بردارنده روشی است که با توجه به لایه های مختلف و بصورت یکپارچه طراحی شده است. در طراحی این سیستم، روش هایی برای استفاده از اطلاعات مهمترین لایه های شبکه اینترنت در نظر گرفته شده و با ایجاد یک مدل یکپارچه برای استفاده از این اطلاعات، سعی شده که به کلیه نیازهای مکان یابی خطا، چه بصورت فیزکی و چه بصورت نرم افزاری و لایه ای پاسخ مناسبی داده شود. از ویژگی های مهم این سیستم جامع، پشتیبانی از مکان یابی خطا در مورد خطاهای مربوط به زیرلایه MPLS و سرویس های VPN موسوم به حفره های سیاه است که کاملاً مورد نیاز ISPها و دیگر مدیران شبکه اینترنت می باشد.

فهرست مطالب

فصل اول

مقدّمه

۱-۱. مقدمه

در جهان امروز، اینترنت، کم کم به مهمترین وسیله ارتباطی تبدیل شده است. تا قبل از دو دهه اخیر، اینترنت بعنوان یک وسیله ارتباطی جانبی و یا تفریحی به حساب می‌آمد که همیشه، تنها برای آسان‌تر کردن یک سری عملیات محدود و صرفاً تحقیقاتی، به عنوان یک انتخاب از میان چند انتخاب به حساب می‌آمد اما امروزه بعلت گسترش روز افزون امکانات سخت افزاری و نرم افزاری، امکان استفاده همگانی از آن، حتی در کشورهای در حال توسعه نیز بوجود آمده است.

واضح است که با بوجود آمدن و گسترش یک وسیله راحت و کم هزینه ارتباطی مانند اینترنت، طبعاً نیاز به این وسیله نیز خود بخود بوجود می‌آید و کم کم به جزئی لاینفک در زندگی مردم بدل می‌گردد. امروزه، اینترنت نه تنها یک وسیله جانبی نیست، بلکه اساس ساختاری بسیاری از امکانات ارتباطی دیگر (مانند انتقال پول بانکها، خرید و فروش از راه دور، مدیریت و کنترل ابزارها از راه دور و ...)نیز به شمار می‌رود و پیش بینی می‌شود که در آینده این روند بیش از پیش نیز ادامه یابد.

اما نهادینه شدن ساختار اینترنت در زندگی مردم و ایجاد امکانات جدید، طبعاً مسائل و مشکلات جدیدی را نیز بوجود می‌آورد. از جمله آنها این است که شبکه اینترنت، هنوز از نظر میزان خطا و قابلیت اعتماد، چه از نظر حفظ ارتباط به طور پیوسته و چه از نظر نگهداری کیفیت ارتباط مناسب، دارای نقص‌های زیادی است. این در حالی است که بعنوان یک ابزار اساسی و پایه بسیاری از امکانات زندگی مدرن امروزی، توقع این است که چنین مسائلی، به حداقل ممکن خود و بسیار پایین تر از حد کنونی برسد.

جهان علمی امروز، این نیاز را درک کرده است و تلاش‌ها و تحقیقاتی را به منظور نیل به این هدف آغاز کرده است. از جمله مهمترین این تحقیقات، مساله رفع خطا در گلوگاه‌های

شبکه‌هاست. این نقاط، حساس ترین نقاط در شبکه‌ها هستند که معمولاً بروز اختلال در آنها منجر به از کار افتادن برخی سرویس‌ها در محدوده گسترده‌ای از نظر تعداد استفاده کنندگان و یا در بعضی موارد، منجر به قطع کامل ارتباط در این محدوده‌ها خواهد شد. این نقاط اصطلاحاً ستون فقرات[1] شبکه‌ها نامیده می‌شوند.

در کشور ما ایران نیز، از زمان بوجود آمدن وزارت ارتباطات و فناوری اطلاعات، بسیاری از زیرساخت‌های ارتباطی در حال تغییرند و شبکه اینترنت رفته رفته به عنوان یک ابزار اساسی برای توسعه در تمام زمینه‌ها جای خود را پیدا می‌کند. امتیاز کشورما و بطور کلی کشورهای در حال توسعه در این زمینه این است که انتقال ساختارهای ارتباطی به شبکه اینترنت، در آنها یک نوآوری جدید و ناشناخته به شمار نمی‌رود و قبلاً تا حدی در کشورهای پیشرفته امتحان شده است و بنابراین نقاط قوت و ضعف آن شناخته شده است. بنابراین می‌توان با استفاده از تجربیات پرهزینه کشورهای پیشرفته، می‌توان بدون پرداخت هزینه‌های اضافی، از نتایج آنها تا حدی که قابل دسترس باشد، استفاده کرد.

ایجاد یک سیستم یکپارچه مدیریت خطا در شبکه‌های کامپیوتری امروزه به دلایل گوناگون، با مشکلات زیادی همراه است. برای مثال گسترش و رشد سریع این شبکه‌ها، موجب شده است که پیوسته به تکنولژی‌های بالاتری برای فراهم کردن امکان این گسترش، مورد نیاز باشد و بنابراین ابزارهای بکار رفته در آنها چه از نظر سخت افزار و چه از نظر نرم افزار و پروتکل‌های بکار رفته، به سرعت پیشرفته تر و پیچیده تر می‌شوند. بنابراین هم توپولژی قسمت‌های مختلف شبکه‌ها و هم ابزارهای ارائه دهنده امکانات، بخصوص در قسمت‌های ستون فقرات شبکه‌ها به صورت پویا در حال تغییراند. این نوع تغییرات مانعی بر سر راه یک طراحی کامل و جامع برای مدیریت خطا در این شبکه‌ها محسوب می‌گردد. چه از این نظر که نحوه خطایابی و رفع خطا در ابزارهای جدید متفاوت است و چه از نظر اینکه تغییرات، ساز و کار سیستم قبلی

[1] Backbone

طراحی شده را به هم می‌ریزد و سیستم طراحی شده، پیوسته نیاز به تغییر و تکمیل خواهد داشت.

دیگر اینکه سرویس‌های جدیدی مانند امکانات صوتی و تصویری (مانند کنفرانس‌های ویدئویی) نیز رفته رفته به کارکردهای شبکه اینترنت، اضافه شده‌اند. اولین نیاز ویژه این سرویس‌ها این است که پهنای باند ثابت و کافی تضمین شده‌ای را در مدت زمان طولانی داشته باشند. این در حالی است که شبکه‌ها اساساً برای هدف بهترین نتیجه ممکن[1] طراحی شده‌اند و بنابراین عموماً تضمینی در کار نیست.

مساله دیگر و شاید مهمترین این مشکلات این است که هیچ گونه سیستم پایه‌ای که بتواند حالت قسمت‌های مختلف شبکه را از نظر میزان سلامتی بطور پیوسته چک کند و نمایش دهد، وجود ندارد. اساساً شبکه‌های امروزی برای ایجاد سرویس‌هایی با این وسعت و حجم استفاده طراحی نشده‌اند و بنابراین از قبل ساختارهای لازم برای مدیریت خطا در آنها در نظر گرفته نشده است.

مجموعه این مشکلات و مانند آنها موجب شده است که شرکت‌های ارائه دهنده امکانات شبکه، برای خطایابی و تضمین کیفت کار خود، هزینه‌های هنگفتی را چه مستقیماً از نظر مالی و چه از نظر بکار گیری نیروی انسانی متخصّص، متحمل شوند. پیش از یافتن راه‌های کاهش این هزینه‌ها باید دانست که این هزینه‌ها از دقیقاً از کجا ناشی می‌شوند. تحقیقات، نشان می‌دهد که بطور متوسط ۸۰ درصد خطاهای ایجاد شده در شبکه‌ها ناشی از اشتباهات نیروی انسانی و یا برنامه‌های نرم افزاری است[۱]. معنای این حرف این است که حتی با داشتن ابزارهای سخت افزاری صد درصد تضمین شده و بدون خطا، ما تقریباً تنها ۲۰ درصد از هزینه مربوط به مدیریت خطا در شبکه‌ها را کاهش داده‌ایم و تازه این در حالی است که تولید ابزارهایی برای رسیدن به میزان تضمین کمتر از این نیز کار بسیار مشکل و پرهزینه‌ای است. طبق تحقیقاتی که در [۱]

[1] Best effort

آورده شده است، رابطه میان میزان پیچیدگی و قابلیت اطمینان به صورت یک مدل حلزونی بیان شده است. بدین معنی که اگر مرکز مارپیچ، نقطه ایده آل باشد، حرکت به سمت این مرکز با پیچیده‌تر کردن قطعات، یک حرکت مارپیچ خواهد بود زیرا پیچیدگی بیشتر ابزارها موجب آسیب پذیر شدن ابزارها نسبت به عوامل جدید ناشی از پیچیگی خواهد شد. بنابراین سرمایه گذاری در این قسمت، برای حل مشکل، چندان مناسب و دارای اولویت بشمار نمی‌رود.

براساس آنچه گفته شد، ریشه مشکل مدیریت خطا، لزوماً به ابزارها برنمی‌گردد و بدین ترتیب در طول زمان پیشرفت تکنولوژی سخت افزاری، لااقل تا آینده نزدیک، چندان تاثیری بر کاهش اهمیت این موضوع نخواهد گذاشت. بنابراین بوجود آوردن روشها و ابزارهای مناسب برای مدیریت خطا در شبکه‌های کامپیوتری در زمان حال و آینده، امری لازم و در خور توجه و سرمایه گذاری بحساب می‌آید.

۱-۲.مدیریت خطا در شبکه‌های بزرگ

تجربه نشان داده است که بروز خطا در شبکه‌های بزرگ، امری اجتناب ناپذیر است. شاید علت این امر این باشد که در شبکه‌های امروزی، بعلت پیچیدگی کار طراحی و پیاده سازی، همکاری تیم‌ها و شرکت‌های مختلف، استفاده از ابزارهای متفاوت با ویژگی‌های خاص خود و بطور کلی بزرگی و پیچیدگی کار طراحی و پیاده سازی این شبکه‌هاست. این مساله موجب شده‌است که حتی با وجود رعایت استانداردهای تعیین شده جهانی در هنگام طراحی و پیاده سازی ابزارها و خود ستون فقرات شبکه‌ها، باز پیچیدگی‌های ناشناخته بسیاری در قسمت‌های مختلف، از دید طراحان و مدیران شبکه، پنهان بماند و موجب بروز خطا در کلیه مراحل گردد.

در نگاه اول، به نظر می‌رسد که چون شبکه‌های کامپیوتری بزرگ، بطور کلی نوعی ابزار پیشرفته به شمار می‌آیند، طبعاً باید روش‌های پیچیده‌ای نیز برای طراحی و پیاده‌سازی آن‌ها بکار

رود. اما با نگاهی دقیق‌تر می‌توان به خوبی دریافت که ابزارهای به کار رفته در شبکه، در برخی موارد بوضوح دارای ناهمخوانی‌ها و نقاط کوری هستند که در طراحی موجب بوجود آمدن خطاهایی می‌شوند که در مراحل اولیه غیرقابل اجتناب‌اند. در بسیاری از موارد حتی در استانداردهای جهانی، با اینکه تلاش زیادی شده است تا هماهنگی و یکپارچگی را در کار طراحی و مدیریت این شبکه‌ها ایجاد کنند، اما نتوانسته‌اند برخی از اصول طراحی، مانند اصل پنهان سازی اطلاعات غیر لازم را از دید مدیران شبکه، و نیز از دید کاربران، بطور کامل در طراحی نرم افزارها و سخت افزارهای شبکه بگنجانند. یک ضرب المثل معروف در زمینه شبکه وجود دارد با این مضمون « در کار شبکه دست بالای دست بسیار است». معنی این جمله آن است که در تکنولوژی شبکه، آن قدر سوراخ و راه‌های گریز و نارسایی در ابزارها و تفاوت در تکنولوژی‌ها و ناهمخوانی و... وجود دارد که هر قدر هم سرمایه گذاری کنید، نمی‌توانید مطمئن باشید که از همه‌لحاظ، شبکه‌شما دارای استحکام کافی و بدون وجود خطا و قابل اعتماد صددرصد می‌باشد.

اما سوال این است که ریشه بروز این مشکل چه بوده است. برخی از متخصصین معتقدند که جهش سریع و در زمان کوتاه، موجب این امر شده است. با نگاهی به روند پیشرفت تکنولوژی در زمینه‌های دیگر، می‌توان دریافت که اولاً بعلت کندی نسبی روند پیشرفت در این تکنولوژی‌ها، زمان کافی برای متصدیان آنها وجود داشته تا بتوانند دیدی کلی نسبت به شرایط نیازهای جهانی و جایگاه ابزارهای مربوطه در آن تکنولوژی بدست آورند. و بدین ترتیب، روند پیشرفت در ابزارها با داشتن زمان کافی انجام گرفته است. این مساله موجب شده است که هماهنگی نسبی در ابزارها و روش‌های طراحی و بکارگیری این تکنولوژی‌ها بوجود آید. ثانیاً بعلت محدود بودن زمینه‌های استفاده از این تکنولوژی‌های جدید، ابزارهای مربوط به آنها با نیازها مطابقت نسبی پیدا کرده‌اند. در حالی که در فناوری شبکه‌ها و بطور کلی، مسائل مربوط به کامپیوترها، چه نرم افزار و چه سخت افزار، هیچ یک از این دو فاکتور وجود ندارند. پیشرفت تکنولژی و رشد نیازهای آن بسیار سریع و برق آسا بوده است و گستردگی استفاده از آن در زمینه‌های مختلف نیز قابل مقایسه با

هیچ یک از تکنولوژی‌های قبلی نیست. این مسائل به اضافه پیچیدگی ذاتی تکنولوژی شبکه‌ها موجب بروز مسائل خاصی در زمینه مدیریت شبکه‌ها شده است. اول این که بعلت رشد سریع این تکنولوژی از همهٔ جنبه‌ها، فرصتی برای هماهنگ و همسان شدن ابزارها و یکسان شدن روند پیشرفت این تکنولوژی در مراکز مختلف وجود نداشته است و دوم اینکه وجود گستردگی استفاده از آن، چه از نظر زمینه‌های مختلف و چه از نظر جغرافیای استفاده و نیز قابلیت تغییر سریع آن، موجب شده است که این تکنولوژی برحسب زمان و مکان و موقعیت، با شرایط خاصی وفق پیدا کند و تغییراتی در آن ایجاد شود. بنابراین استاندارد سازی آن مشکل شده است.

برای مثال در بسیاری از پروتکل‌های بکار رفته در شبکه‌ها، نارسایی‌هایی در زمینه‌های مختلف دیده می‌شود و با کمی تحقیقات، می‌توان آنها را بهبود بخشید. اما مساله اینجاست که بعلت مورد استفاده قرار گرفتن و گسترش سریع، استفاده از آنها بسرعت مصطلح شده است و نرم افزارها و سخت‌افزارهایی براساس استفاده از آنها ساخته شده‌اند و عملاً تغییر دادن آنها در زمان کوتاه به صرفه نیست.

همه این مسائل روی هم رفته نشان می‌دهد که بخش قابل توجهی از پیچیدگی موجود در زمینه طراحی و پیاده‌سازی شبکه‌ها و بخصوص مدیریت خطا در شبکه‌ها بعلت ناهمخوان بودن قسمتهای مختلف نرم افزاری و سخت افزاری این تکنولوژی است و بنابراین امروزه شبکه‌ها بیش از آنچه انتظار می‌رود، مستعد بروز خطا در کلیه قسمت‌ها می‌باشند.

با توجه به آن چه گفته شد، داشتن خطاهای متعدد و از انواع مختلف، با وجود بهترین طراحی‌ها و پیاده‌سازی‌ها در ستون فقرات شبکه‌ها، تا حدی ملموس‌تر می‌شود. برای مثال، اگر در یک مسیریاب بر اثر یک خطای نرم افزاری، اشتباهی درمسیریابی قسمتی از بسته‌ها رخ دهد، پیدا کردن علت بروز خطا و محل آن بصورت معمول، ممکن است ساعت‌ها و یا حتی روزها وقت بگیرد. دقت کنید که یک شبکه ستون فقرات خطی، می‌تواند بیش از ۱۰۰۰ مسیریاب داشته باشد که محصول شرکت‌های مختلف و با ویژگی‌های متفاوت هستند و هر کدام ممکن است مستعد

خطاهای مخصوص به خود باشند.[۱] بنابراین زمان و هزینه بسیار زیادی ممکن است برای یافتن خطا صرف شود.

مساله دیگری که کار خطایابی را پیچیده‌تر و مشکل تر می‌کند، ساختار لایه ای شبکه‌هاست. این ساختار لایه‌ای برای این منظور بوجود آمده که بتواند پیچیدگی بوجود آمده در سخت افزار و نرم افزار شبکه‌ها را طبقه بندی و کار با آن را ممکن سازد. این کار با استفاده از تجرید مفاهیم داخلی مربوط به یک لایه، هنگام کار با لایه دیگر انجام می‌شود. به همان شکلی که در مفاهیم شیء گرایی، تجرید اشیا به مدیریت آنها کمک می‌کرد. اما متاسفانه در مورد مساله خطایابی این نحوه تجرید لایه‌ای، موجب ایجاد خطاهایی می‌شود که در انتقال اطلاعات مابین لایه‌ها رخ می‌دهند و یافتن و رفع آنها مشکل‌تر است.

برای مثال شبکه‌های معمولی که با پروتکل IP کار می‌کنند، می‌توانند از سخت افزار شبکه های نوری استفاده کنند. بنابراین یک ارتباط از طریق IP به تعداد زیادی قطعات نوری مربوط خواهد شد. همچنین بر روی همین سخت افزار ارتباطی، ممکن است یک لایه MPLS میانی نیز وجود داشته باشد که بسته‌های IP از طریق مسیرهای مجازی آن انتقال پیدا کنند. مسیرهای تعریف شده درون لایه MPLS، اصطلاحاً LSP نامیده می‌شوند. چندین LSP ممکن است ممکن است بار مربوط به یک ارتباط IP را باهم به اشتراک بگذارند. علاوه براین، ممکن است مسیرهای مربوط شبکه‌های مجازی VPN نیز بر روی همین شبکه بصورت موازی مشغول به کار باشند که آنها نیز از همان LSPها و حتی ارتباط‌های IP استفاده کنند یا نکنند. حال اگر مثلاً در رساندن بخشی از بسته‌های IP اشکالی رخ دهد، یا مثلاً قسمتی از شبکه VPN به درستی کار نکند، اشکال مربوطه ممکن است مربوط به چندین لایه شود. [۱]

اما در مقابل، تمهیداتی را که برای کنترل خطا عموماً در شبکه‌ها مورد استفاده قرار گرفته‌اند، می‌توان به دو دسته تقسیم کرد.

دسته اول شامل ساختارهایی است که بطور خلاصه موجب ایجاد میزان محدودی از انعطاف پذیری در مقابل خطاهای احتمالی می‌گردد و با عنوان حفاظت در مقابل بروز خطا[1] شناخته می‌شوند. بخشی از خطاهای شبکه‌ها که بیشتر رخ می‌دهند و با استفاده از تجربیات بدست آمده در مورد شبکه‌های مختلف شناسایی شده‌اند، با احتمال خوبی قابل پیش بینی می‌باشند. داشتن این اطلاعات، طراحان شبکه‌ها را قادر ساخته است تا ساختارهایی را برای جلوگیری و یا کاهش اثر این خطاها طراحی کنند. مثلاً برخی پروتکل‌های مسیریابی می‌توانند با اطلاع از قطع شدن یک خط ارتباطی، بسته‌های مربوط به آن خط را از طریق مسیرهای دیگر، ارسال کنند و به مقصد برسانند و یا اینکه نرم افزارهایی وجود دارند که خطاهای مربوط به حمله‌های جلوگیری از سرویس‌دهی[2] را شناسایی می‌کنند و بسته‌های مربوط به آنها را قبل از رسیدن به سرور مربوطه بلاک می‌کنند. این ساختارها عموماً بصورت خودکار عمل می‌کنند و بنابراین تقریباً هزینه‌ای بجز هزینه اولیه را برای متصدیان شبکه، به همراه ندارند. اما میزان کارآیی آنها بسیار محدود است و تنها در کوتاه مدت مفید واقع می‌شوند. با ایجاد یک خطا، احتمال بروز خطاهای دیگر بالا می‌رود و بنابراین خطای ایجاد شده، حتی اگر در کار کلی سیستم خللی وارد نکند، باید به سرعت رفع گردد تا خطاهای احتمالی بعدی موجب از کار افتادن شبکه نشوند.

دسته دوم، تمهیداتی است که توسط مدیر و یا تکنسین‌های شبکه برای شناسایی و تعمیر خطا در شبکه اندیشیده می‌شود و با عنوان بازگرداندن از وضعیت بروز خطا[3] شناخته می‌شوند. مسئولین شبکه، باید بطور پیوسته، پارامترهای مختلف شبکه را چک کنند تا در صورت بروز خطا، در اسرع وقت بتوانند برای رفع خطا اقدام کنند. از زمان بروز یک خطا تا هنگام رفع آن، بخصوص در شبکه‌های ستون فقرات، ممکن است مشتریان زیادی، فقدان تمام یا بخشی از سرویس‌های شبکه را تجربه کنند و این مساله هزینه‌های زیادی را از نظر اقتصادی به متصدیان شبکه تحمیل

---

[1] Network Protection

[2] Denial Of Service (DOS)

[3] Restoration

کند. بنابراین سرعت عمل تیم شناسایی و رفع خطا بسیار مهم و در خور توجه و سرمایه‌گذاری است.

برخی از خطا ها، بصورت مستقیم قابل مشاهده هستند بدین معنی که آنها خودشان هم مشکل (ریشه) و هم نشانه هستند. اما با این وجود انواع زیادی از خطا ها وجود دارند که قابل مشاهده نیستند و این بعلت آن است که اولاً ممکن است طبیعت ذاتی آنها طوری باشد که قابل مشاهده نباشند؛ ثانیاً ممکن است مکانیزم های تصحیح کننده بومی ساخته شده در سیستم مدیریت شواهد مربوط به اتفاق افتادن آن خطا را از بین ببرند و ثالثاً توانایی عملیاتی لازم برای تشخیص وجود برخی از خطاها ممکن است کم باشد.

برخی از خطا ها ممکن است تا حدی قابل مشاهده باشند[1] یعنی اینکه سیستم مدیریت شبکه تشخیص دهد که خطایی رخ داده است اما شواهد برای تشخیص محل خطا کافی نیستند[۲].

از آنجایی که بیشتر خطاها بصورت مستقیم قابل شناسایی نیستند، سیستم مدیریت شبکه مجبور است که وجود آنها را از اطلاعات مربوط به اخطارهای رسیده استنتاج کند. اطلاعات محتوای اخطارهای رسیده می توانند شامل مواردی باشند از قبیل: هویت شیئی که اخطار مربوطه را تولید کرده است، نوع شکست ایجاد شده، مهر زمان، شناسه مشخص کننده اخطار، میزان جدی بودن شکست ایجاد شده، یک توصیف متنی از شکست ایجاد شده و غیره [۴].

در یک شبکه ارتباطی یک خطا ممکن است به چند شکل موجب ایجاد چندین اخطار گردد [۳]:

- چند اخطار ممکن است نتیجه تکرار یک خطا باشند.
- چند اخطار ممکن است نتیجه چند بار فراخوانی یک سرویس توسط قطعه خراب شده باشند.

[1] Partially observable