دانشگاه صنعتی امیرکبیر

(پلی‌تکنیک تهران)

دانشکده مهندسی کامپیوتر

پیشنهاد پروژه کارشناسی

پیاده سازی سیستم پایش شبکه‌های کامپیوتری

نگارش

سیدمهدی میرفندرسکی ۹۷۲۳۰۹۳

استاد راهنما

دکتر مسعود صبائی

آبان ۱۴۰۰


بسم الله الرحمن الرحيم

فهرست مطالب

عنوان صفحه

فهرست اشکال

شکل صفحه

فصل اول

مقدمه

پیشرفت روز افزون شبکه‌های کامپیوتری باعث شده است تا مدیریت آن نیز از اهمیت بالایی برخوردار باشد. اگر بخواهیم مروری اجمالی بر مفهوم مدیریت داشته باشیم، این گونه بیان می‌کنیم که مدیریت یک سیستم شامل پایش اجزا و جمع آوری داده، تحلیل داده‌ها و انجام اقدامات برای نزدیک شدن به هدف آن سیستم خواهد بود. به بیان دیگر مدیریت یک فرایند دائمی شامل پایش و نظارت، برنامه ریزی و اقدام است. مدیریت شبکه‌های کامپیوتری نیز به همین اجزا تقسیم بندی می‌شود.

هدف از انجام این پروژه توسعه یک ابزار مدیریتی به منظور پایش و نظارت شبکه‌های کامپیوتری است. به عبارت دیگر در این پروژه نرم افزاری توسعه داده می‌شود که به کمک این نرم افزار امکان پایش و نظارت تجهیزات قابل مدیریت شبکه، فراهم می‌گردد. این امکان از طریق یک رابط مدیریتی که اطلاعات پایش را از تجهیزات دریافت می‌کند و به نحوی قابل فهم برای مدیر شبکه نمایش می‌دهد، فراهم می‌گردد[۲].

با پیاده سازی این ابزار، مدیر شبکه می‌تواند مشکلات شبکه را به موقع متوجه شود. همچنین می‌تواند برنامه ریزی کوتاه مدت و بلند مدت به منظور استفاده بهینه از منابع و جلوگیری از خرابی، انجام دهد.

پس از نگاه دقیق تری به مسئله پایش شبکه، حال ویژگی‌های مختلفی که ابزار پایش باید داشته باشد را بررسی می‌کنیم.

۱-۱ ویژگی‌های ابزار پایش شبکه

۱-۱-۱ انتخاب پروتکل مناسب و نحوه ارتباط

در شبکه‌های کامپیوتری عناصری را می‌توان مدیریت کرد که بتوان اطلاعات مدیریتی را از آن دریافت کرد. به عبارتی عناصر تحت مدیریت، عناصری هستند که عامل مدیریتی بر روی آن‌ها راه اندازی شده باشد. دریافت این اطلاعات مدیریتی از عناصر باید از طریق یک پروتکل صورت بگیرد که به این نوع پروتکل‌ها، پروتکل مدیریتی گفته می‌شود.

اتخاذ یک پروتکل مدیریتی ایمن که مصرف پهنای باند حداقلی را داشته باشد بسیار مهم است.

برای پایش یک شبکه و دستگاه‌های آن، اتخاذ یک پروتکل مدیریتی شبکه امن که مصرف پهنای باند حداقلی را داشته باشد بسیار برای ما مهم است. این پروتکل‌ها می‌توانند مانند SNMP[1]، استاندارد شده باشند. و یا حتی می‌توانند مانند CLI[2] غیر استاندارد باشند. اکثر عناصر تحت مدیریتی از پروتکل‌های SNMP و CLI پشتیبانی می‌کنند. همچنین دستگاه‌های ویندوزی از پروتکل WMI[3] نیز پشتیبانی می‌کنند.

پروتکل SNMP یکی از پروتکل‌های لایه کاربرد برای مدیریت و پایش عناصر شبکه است. درواقع برای ارتباط با سیستم مدیریت شبکه تنها باید پیکربندی و فعال شود. به بیان دیگر نیازی به توسعه برنامه‌ای در سمت عناصر شبکه وجود ندارد[۱]. این پروژه قصد استفاده از پروتکل SNMP را دارد.

۱-۱-۲ کشف شبکه و دستگاه‌های مورد نیاز برای پایش

در پایش شبکه، اولین قدم شناسایی عناصر قابل مدیریت و معیارهای عملکرد مرتبط با هر عنصر است. عناصری مانند رایانه‌های رومیزی و چاپگرها و مواردی از این دست برای ما حائز اهمیت نیستند و اساسا نیازی به پایش مداوم ندارند. از طرفی سرورها، روترها و سوئیچ‌ها وظایفی حیاتی را بر عهده دارند و نیاز به پایش مداوم دارند. ابزار پایش شبکه باید قادر باشد تا عناصر تحت مدیریت را شناسایی کند.

۱-۱-۳ دریافت اطلاعات و تنظیم پارامترهای مختلف

دریافت اطلاعات از عناصر شبکه که قابل مدیریت باشند، به دو روش زیر صورت می‌گیرد:

- ارسال درخواست سیستم مدیریت به عنصر تحت مدیریت و دریافت پاسخ از سمت عنصر تحت مدیریت
- ارسال نوتیفیکیشن[4] بر اساس رخداد و یا رفتار غیر متعارف توسط عنصر تحت مدیریت و دریافت در سمت سیستم مدیریت

[1] Simple Network Management Protocol
[2] command-line interface
[3] Windows Management Instrumentation
[4] Notification

در روش اول، درخواست‌های سیستم مدیریت شبکه به صورت دوره‌ای و متناوب انجام می‌شود. این دوره تناوب توسط مدیر شبکه باید قابل تنظیم باشد. تنظیم نادرست دوره تناوب می‌تواند منجر به استفاده غیر ضروری منابع و مصرف بی اندازه پهنای باند شود.

اما در روش دوم نوتیفیکیشن‌ها بر اساس رخداد و یا رفتار غیر متعارف هستند. این رخداد و رفتار غیر متعارف باید توسط مدیر شبکه قابل تعریف باشد. این کار در سیستم مدیریت شبکه با تعریف حد آستانه‌هایی[1] در سمت عناصر تحت مدیریت صورت می‌گیرد، که این امر نیاز به تنظیم مدیر شبکه دارد. همچنین وجود حد آستانه‌های چند سطحی در شناسایی بهتر عناصر تحت مدیریت کمک می‌کند.

۱-۱-۴ هشدار فوری بر اساس نقض آستانه

با استفاده از حد آستانه‌ها، هشدارهای پایش شبکه را می‌توان تا حدی قبل از رسیدن به شرایط بحرانی هوشمند کرد. به عنوان مثال می‌توان از ارسال ایمیل و یا نمایش در بستر وب بهره برد. بدین صورت که با عبور از هر حد آستانه، به مدیر شبکه از طریق ارسال ایمیل و نمایش بصری در بستر وب اطلاع رسانی شود.

[1] Threshold

فصل دوم

مروری بر پروژه‌ها و سامانه‌های مشابه

از زمانی که دستگاه‌ها در شبکه‌ها به هم متصل می‌شدند، نیاز به نوعی سیستم مدیریت و پایش شبکه وجود داشته است. در سال ۱۹۸۸ بود که SNMP به استاندارد جدید تبدیل شد. هدف پروتکل SNMP این است که زبانی برای انتقال اطلاعات مدیریتی شبکه بین دستگاه‌های مختلف به وجود آورد. امروزه اکثر دستگاه‌های شبکه می‌توانند SNMP را به عنوان یک عامل راه اندازی کنند، به همین جهت اکثر نرم افزارهای پایش شبکه ارتباط از طریق SNMP را در اولویت خود قرار می‌دهند.

۲-۱ مروری بر پروژه‌های موجود

امروزه ابزارهای متنوع و گوناگونی برای پایش شبکه توسعه داده شده‌اند. در ادامه به معرفی ابزارهای سولاروینداز[1]، دیتاداگ[2] و زبیکس[3] می‌پردازیم.

۲-۱-۱ سولاروینداز

این سیستم پایش شبکه از SNMP برای بررسی وضعیت عناصر تحت مدیریت استفاده می‌کند. این ابزار قابلیت کشف عناصر شبکه را داراست به عبارتی دیگر دستگاه‌های موجود در شبکه که برای ما حائز اهمیت هستند را پیدا کرده و توپولوژی شبکه را ترسیم می‌کند. همچنین می‌توان یک توپولوژی مناسب برای کل زیرساخت شبکه طراحی کرد. به علاوه هشدارهای هوشمندی نیز دارد. اما در بحث نصب بر روی سیستم عامل‌های مختلف محدودیت‌هایی وجود دارد، مثلا در بعضی توزیع‌های لینوکس بر پایه دبین[4] قابل نصب نیست. برخی دیگر از ویژگی‌های سولاروینداز عبارتند از:

- قابلیت تجزیه و تحلیل مشکل: با فراهم آوردن دید کاملی از عملکرد زیرساخت شبکه، به هنگام وجود آمدن مشکل، پیدا کردن مبدا آن ساده خواهد بود.
- پایش عملکرد: این امکان را می‌دهد که بتوان بررسی کرد آیا اهداف عملکردی سرویس‌های مختلف برآورده شده‌اند یا خیر. این با پایش عملکرد در سطح برنامه‌های کاربردی، محقق می‌شود.
- سهولت استفاده: رابط کاربری کاربرپسند و ساده‌ای دارد.

[1] SolarWinds
[2] Datadog
[3] Zabbix
[4] Debian

۲-۱-۲ دیتاداگ

دیتاداگ یک ابزار پایش عملکرد شبکه است که مبتنی بر ابر[1] است و این امکان را می‌دهد که ترافیک شبکه بین میزبان‌ها، کانتینرها و سرویس‌ها را در ابر تحلیل کنیم. برخی امکاناتی و تقاط قوتی که دیتاداگ دارد به شرح زیر می‌باشد:

- این برنامه جریان ترافیک شبکه را می‌تواند بین میزبان‌ها، کانتینرها، شبکه‌های مختلف و حتی مفاهیم انتزاعی مانند سرویس‌ها و یا ماژول‌های مختلف نمایش می‌دهد.
- در بحث عیب یابی، داده‌های ترافیک شبکه را با درنظر گرفتن برنامه‌های مربوطه، معیارهای دستگاه‌های مختلف و لاگ‌ها تحلیل می‌کند تا عیب‌یابی را در یک سیستم انجام دهد.
- به صورت بصری جریان ترافیک را نشان می‌دهد تا به شناسایی گلوگاه‌های ترافیکی کمک کند.

۲-۱-۳ زبیکس

زبیکس یک ابزار پایش شبکه متن باز است که برای انواع عناصر تحت مدیریت خدمات ارائه می‌دهد. برخی امکاناتی که زبیکس در اختیار ما قرار می‌دهد به شرح زیر است[۳]:

- جمع آوری داده‌ها انعطاف پذیر است و با تغییر شبکه مشکلی پیش نخواهد آمد.
- توانایی شناسایی دستگاه‌های شبکه به طور خودکار را داراست.
- امکانات مختلفی برای هشدارها ارائه می‌دهد.

[1] Software as a service

۲-۲ ویژگی‌های سامانه

در نهایت بر اساس مطالعاتی که انجام شده و مطالب فصل قبل این سامانه باید قابلیت‌های زیر را داشته باشد:

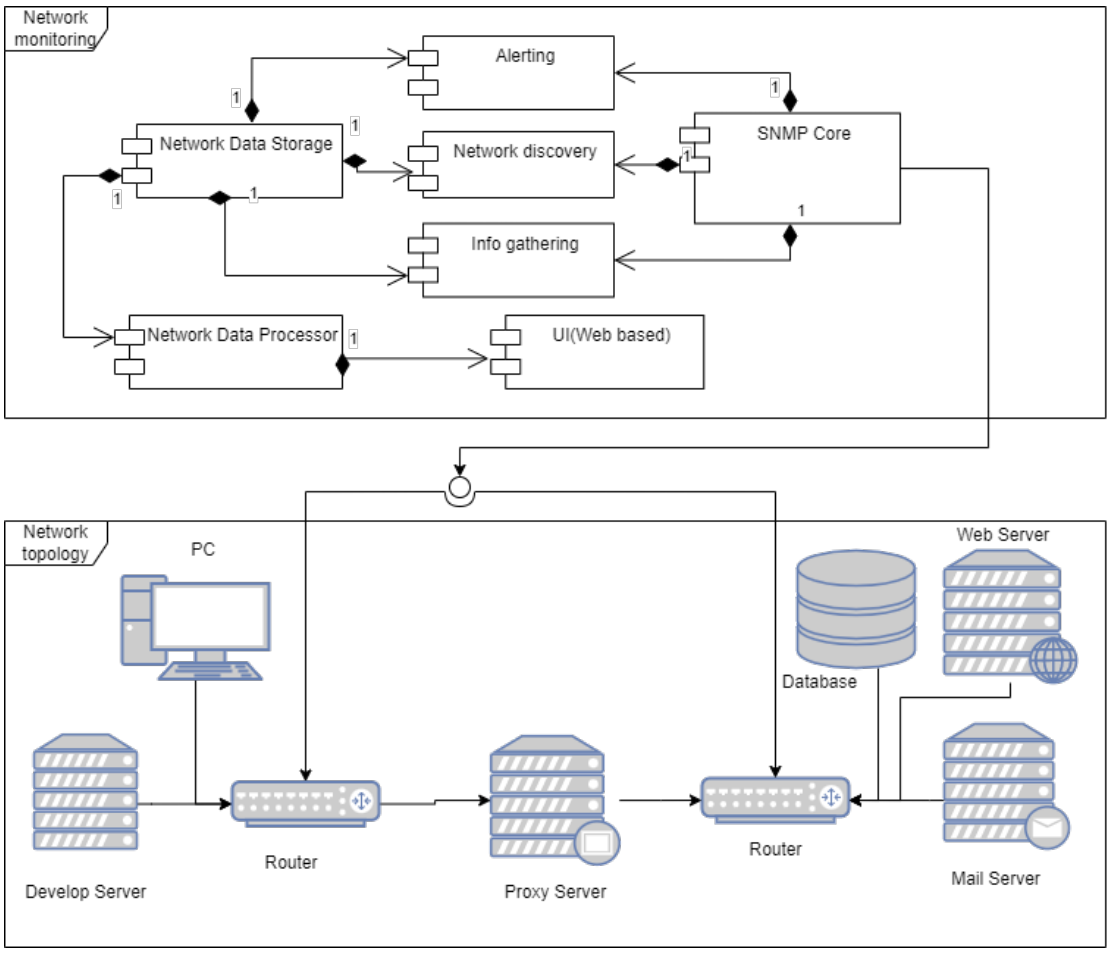
- کشف شبکه و ترسیم بصری آن برای ادراک بهتر توسط مدیر شبکه
- توانایی تنظیم پارامترها از جمله حد آستانه‌های عناصر تحت مدیریت بر اساس رفتار غیرمتعارف توسط مدیر شبکه و دوره تناوب جمع آوری اطلاعات از عناصر
- جمع آوری اطلاعات مدیریتی و پردازش آن‌ها جهت تولید اطلاعات قابل فهم توسط مدیر شبکه
- ایجاد یک رابط بصری مطلوب تحت وب و نمایش اطلاعات قابل فهم
- فراهم آوردن حداقلی امنیت سیستم با استفاده از (SNMPv3 و پروتکل‌های دیگری که ایمن هستند)
- مقیاس پذیری سیستم جهت کارآمد بودن در هنگام افزایش وسعت شبکه
- فراهم آوردن یک مکانیزم هشدار با استفاده از حد آستانه‌های تعریف شده

به طور خلاصه هدف از انجام این پروژه توسعه یک ابزار پایش شبکه با ویژگی‌های پایه‌ای فوق است. به عبارتی هدف، افزودن یک امکان جدید به پروژه‌های موجود و پیاده سازی آن نیست، اما از زبان‌های برنامه نویسی و تکنولوژی‌های بروز در مقایسه با پروژه متن باز زبیکس استفاده خواهد شد. به عبارت دیگر این پروژه از ابتدا بدون استفاده از کدهای متن باز موجود توسعه داده خواهد شد. با انجام این پروژه دید خوبی نسبت به انجام یک پروژه صنعتی بدست خواهد آمد. همچنین چالش‌های مختلفی در ماژول‌ها و ارتباط بین آن‌ها برخورد می‌شود که باید رفع شوند.

فصل سوم

روش انجام پروژه

در این فصل روش انجام پروژه گفته می‌شود. سامانه پایش شبکه‌های کامپیوتری به ماژول‌های زیر تقسیم می‌شودشکل ۳-۱. ابتدا یک ماژول تحت عنوان هسته SNMP در نظر گرفته می‌شود که وظیفه مدیریت پیام‌ها و پیاده‌سازی پروتکل به یک زبان برنامه نویسی خاص است.



شکل ۳-۱: نمودار بلوکی اجزای سامانه

سپس ماژول کشف عناصر تحت مدیریت شبکه را در نظر گرفته می‌شود، که به کمک ماژول هسته وظیفه جمع آوری اطلاعات ساختاری شبکه را بر عهده دارد. بعد از آن ماژول جمع آوری اطلاعات دستگاه‌های مختلف، عملکرد کل شبکه را رصد می‌کند. حال اگر زمانی با توجه به وجود نوتیفیکیشن‌ها نیاز به هشدار وجود داشت، از ماژول هشدار استفاده می‌شود.

نکته حائز اهمیت در رابطه با سه ماژول آخر این است که هر ماژول از ماژول هسته و همچنین ماژول ذخیره‌سازی اطلاعات شبکه تغذیه می‌شود. همچنین اطلاعاتی که هر ماژول بدست می‌آورد تحویل ماژول ذخیره‌سازی اطلاعات شبکه می‌دهد. در ماژول ذخیره سازی اطلاعات شبکه نیز اطلاعات در پایگاه‌های داده ذخیره می‌شوند، تا برای ماژول پردازشگر اطلاعات شبکه قابل بهره برداری باشد.

در پردازشگر اطلاعات شبکه نیز، اطلاعات خام دریافتی از ماژول ذخیره سازی اطلاعات شبکه پردازش می‌شوند تا اطلاعات قابل فهم توسط مدیر استخراج شود. حال باید اطلاعات تولید شده به ماژول رابط کاربری داده شود.

ماژول رابط کاربری نیز در قالب یک وب سایت و فراهم آوردن یک پنل ورودی مدیر شبکه نیز اطلاعات ساختاری شبکه، پایش شبکه و هشدارها را نمایش می‌دهد. همچنین از طریق آن می‌توان پارامترهای مختلف برای عناصر مختلف تنظیم و اقدام به اسکن کل شبکه کرد.

اما نیاز است که یک رابطی بین شبکه و سامانه مذکور باشد. در شکلی که بررسی شد، سامانه به یک شبکه فرضی از طریق روترهای آن متصل است. در واقع جمع آوری اطلاعات از شبکه و دریافت نوتیفیکیشن‌ها از طریق ماژول هسته SNMP امکان پذیر خواهد بود.

فصل چهارم

روش ارزیابی

بعد از پیاده سازی محصول، با توجه به طراحی و پیاده سازی صورت گرفته، بر اساس نیازمندی‌ها سناریوهای تست تعریف و اجرا می‌شوند. برای ارزیابی محصول، دو مرحله زیر در نظر گرفته می‌شود:

- ارزیابی نیازمندی‌های عملکردی محصول

۱. تست یکپارچگی[1]: تست هر ماژول در این قسمت صورت می‌گیرد.

۲. تست سیستم[2]: تست کل سیستم صورت می‌گیرد.

- ارزیابی کیفیت انجام نیازمندی‌های عملکردی

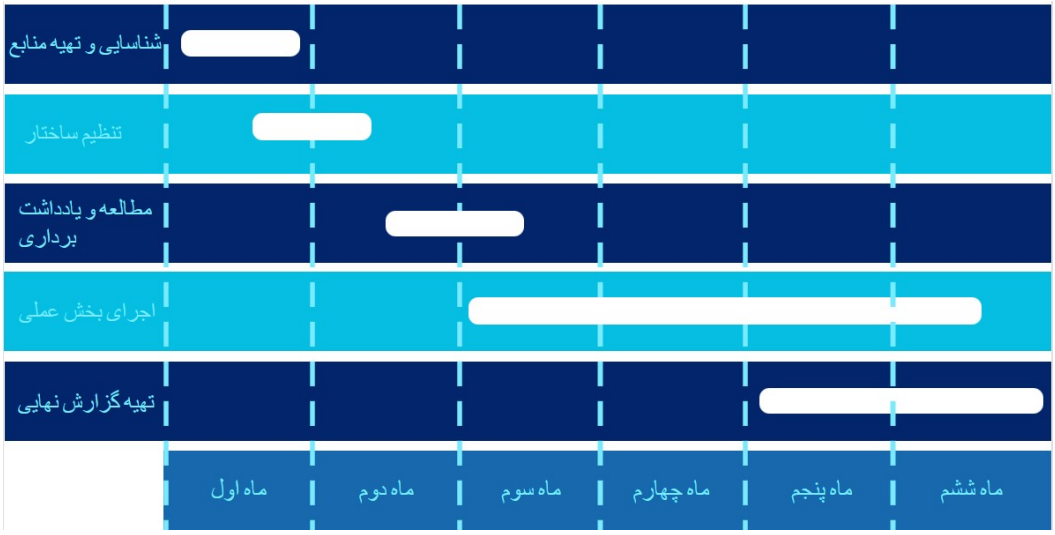
[1] Integration testing

[2] System testing

فصل پنجم

مراحل انجام و زمان‌بندی پروژه

با توجه به ویژگی‌هایی که در فصل قبل برای پروژه ذکر کردیم مسیر زیر را برای پیاده سازی پروژه در نظر می‌گیریم شکل ۵-۱.



شکل ۵-۱: نمودار زمان‌بندی فعالیت‌ها

مطالعه و یادداشت برداری شامل موارد زیر خواهد بود:

- مطالعه کاملی پیرامون مفهوم مدیریت شبکه‌های کامپیوتری و راه‌های انجام آن
- مطالعه کاملی پیرامون پروتکل SNMP و پیاده سازی‌های آن

همچنین اجرای بخش عملی شامل موارد زیر خواهد بود:

- پیاده سازی هسته مدیر SNMP
- پیاده سازی ماژول ذخیره سازی داده‌های شبکه
- پیاده سازی ماژول کشف شبکه
- پیاده سازی ماژول جمع آوری داده از سطح شبکه
- پیاده سازی ماژول هشدار
- پیاده سازی ماژول پردازش داده‌های شبکه
- پیاده سازی یک رابط کاربری در قالب یک وب سایت و ایجاد ارتباط بین ماژول‌های ذکر شده

فصل ششم

امکانات لازم

منابع و امکاناتی که ما نیاز داریم تا این سامانه را پیاده سازی کنیم به شرح زیر می‌باشد:

- اینترنت
- سیستم شخصی جهت توسعه نرم افزار
- تعدادی کتابخانه‌ی عمومی که در دسترس هستند

منابع و مراجع

[1] Hare, Chris. Simple network management protocol (snmp)., 2011.

[2] Mauro, Douglas and Schmidt, Kevin. Essential SNMP: Help for System and Network Administrators. " O'Reilly Media, Inc.", 2005.

[3] Olups, Rihards. Zabbix 1.8 network monitoring. Packt Publishing Ltd, 2010.