فصلنامه پژوهش در علوم، مهندسی و فناوری
دوره ۴، شماره ۱، بهار ۱۳۹۷
صفحات ۱۴-۲۶
ISSN: 2476-5082
www.uctjournals.com

بررسی مدیریت شبکه بر پایه مدل FCAPS

امین بهاری [۱] و نبی اله کاکایی [۲]

۱ کارشناسی ارشد مهندسی فناوری اطلاعات ، دانشگاه آزاد اسلامی واحد آشتیان Bahari.eng@gmail.com
۲ کارشناسی ارشد مهندسی فناوری اطلاعات ، دانشگاه آزاد اسلامی واحد آشتیان

چکیده

ابزار های مدیریتی که برای مدیریت شبکه وجود دارند مانند مجموعه نرم افزار های مختلف باید جنبه های مختلف استانداردهای FCAPS را رعایت کنند. معمولا مدل های مختلف که ارایه دهنده راهکار برای مدیریت شبکه هستند نمی توانند تمامی جنبه های مدیریتی FCAPS را اجرا کنند. یکی از دلایلی که باعث شده تا این مدل ها نتوانند تمامی بخش های FCAPS را رعایت کنند پر هزینه و زمان بر بودن آن است[1]. البته نرم افزار هایی هم هستند که روی یک جنبه تمرکز دارند که معمولا کارا تر و ارزان تر هم هستند ولی سادگی آن ها سبب قابلیت های کمتر آن ها نیز می شود. برای مثال نرم افزارهایی که بر اساس SNMP کار می کنند فقط جنبه ی Fault Management را رعایت می کنند. استانداردهای FCAPS توسط شرکت ISO ارایه شده است و این استاندارد به طور کلی بر روی شبکه و سیستم های مدیریتی تمرکز دارد[10]. در این مقاله به جنبه های مختلف مدیریت شبکه بر پایه مدل FCAPS پرداخته می شود.

واژه‌های کلیدی: مدل مدیریت شبکه FCAPS، SNMP، سیستم مدیریت شبکه(NMS)، ISO

مقدمه

شبکه‌های ارتباطی، در آغاز از ابعاد کوچک و فناوری‌های محدودی برخوردار بودند و در نتیجه کار نگهداری آن‌ها آسان بود. ولی با رشد ناگهانی شبکه‌ها در دهه ۸۰ میلادی، نظارت بر عملکرد و برنامه‌ریزی توسعه آنها، کاری دشوار و به شدت پرهزینه گردید. در چنین شرایطی نیاز به مکانیسم‌هایی که به خودکارسازی عملیات و ساده‌سازی وظایف اپراتورهای انسانی کمک کنند، به شدت احساس می‌شد و این سرآغاز توسعه سیستم‌های مدیریت شبکه بود. ممکن است تعابیر متعددی از مدیریت شبکه وجود داشته باشد، ولی می‌توان به طور خلاصه آن را چنین تعریف کرد: مجموعه‌ای از عناصر سخت‌افزاری و نرم‌افزاری که به عوامل انسانی امکان نظارت بر عملکرد و حفظ کارآیی شبکه را به شکلی مقرون به صرفه می‌دهند[2].

تعریف شبکه :

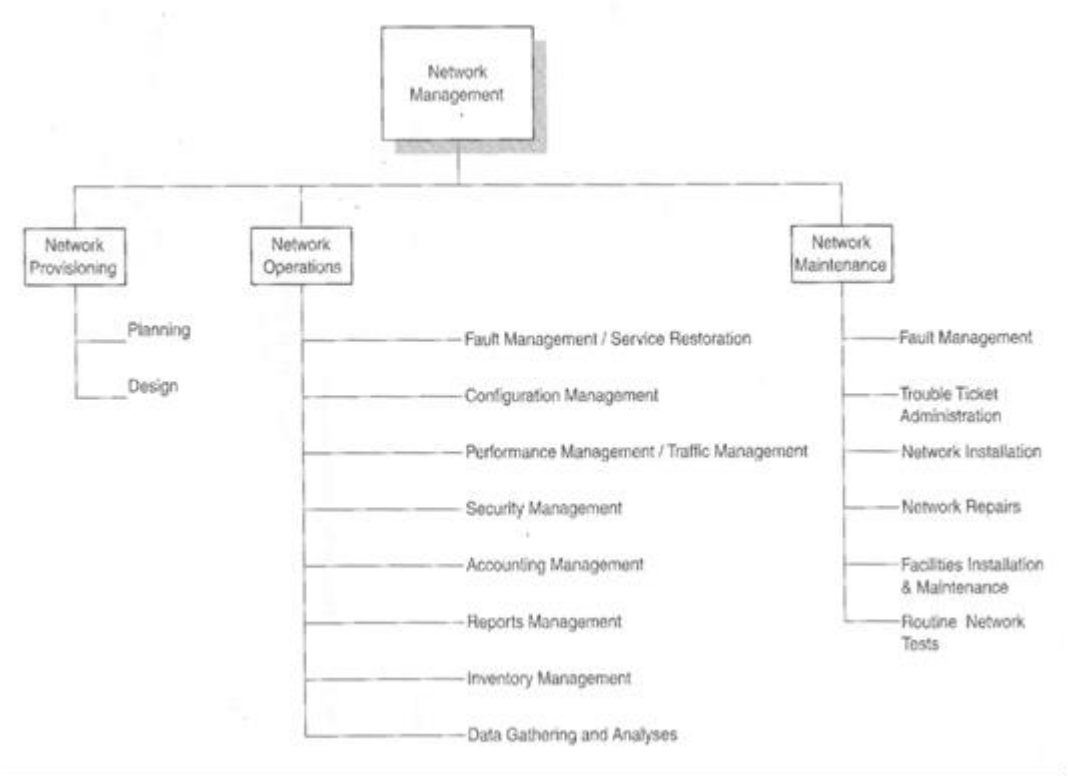
مجموعه ای از دو یا چند کامپیوتر ، پرینتر و ... که به منظور به اشتراک گذاری منابع و اطلاعات با یکدیگر در ارتباطند.در این مجموعه به هر یک از سخت افزار ها و نرم افزار ها یک Source یا منبع می گویند.

شبکه های کامپوتری اغلب به دلایل زیر به وجود می آیند و مورد استفاده قرار می گیرند:

- استفاده از منابع مشترک : استفاده از یک منبع اطلاعاتی یا وسایل جانبی رایانه بدون توجه به موقعیت جغرافیایی آن را استفاده از منابع مشترک می نامند.
- کاهش هزینه : متمرکز نمودن منابع و استفاده مشترک از آن ها باعث کاهش هزینه در یک مجموعه می شود.
- قابلیت اطمینان: در شبکه های کامپوتری با توجه به وجود پشتیبان اطمینان در شبکه بالا می رود به طوری که از اطلاعات موجود بر روی هر سیستم یک نسخه نیز بر روی پشتیبان نگهداری می شود که این موضوع سبب می شود در صورت از کار افتادن یک سیستم اختلالی در شبکه به وجود نیاید.
- کاهش زمان: یکی از اهداف اصلی شبکه های کامپوتری برقراری ارتباط بین اعضا شبکه بدون مرز جغرافیایی است که همین موضوع سبب می شود زمان دسترسی و استفاده از منابع کاهش یابد.
- قابلیت توسعه: شبکه های کامپیوتری قابلیت ورود اجزا جدید به شبکه را دارند که به این شکل می توانند توسعه پیدا کنند.
- ارتباطات: کاربران می توانند بر اساس نوآوری های موجود مانند پست الکترونیکی و یا دیگر سیستم های اطلاع رسانی پیام های خود را منتقل کنند و حتی امکان انتقال فایل نیز وجود دارد[3-2].

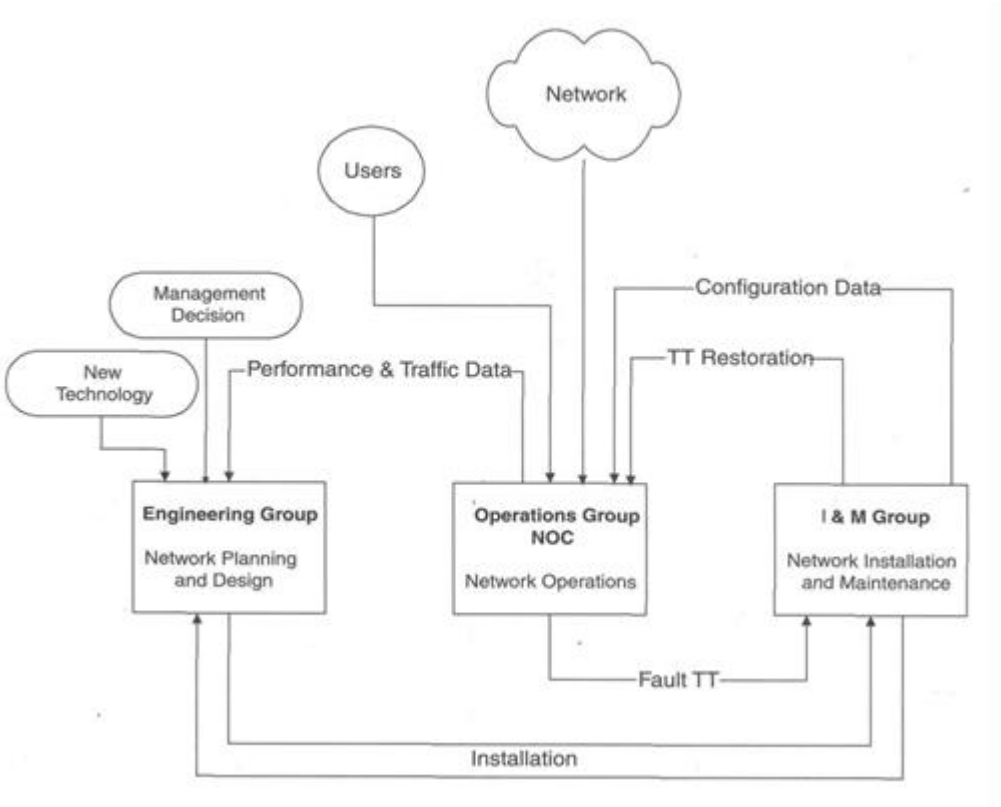
هدف از مدیریت شبکه اطمینان داشتن از کیفیت سرویسهای تکنولوژی اطلاعات مورد انتظار می‌باشد که بعنوان سرویسهای شبکه ارائه می‌شود. در برخورد با این اهداف، مدیریت باید سیاست رسمی و یا غیر رسمی، برای قرارداد توافقات سطوح سرویس با کاربران را بنا نهد. بطور مثال برای سرویسهای بحرانی وقفه‌ای را نمی‌توان در نظر گرفت و آن باید ۲۴ ساعته و در طول ۷ روز هفته باشد که از آن جمله E-mail Server و Web Server می‌باشد در حالی که برای فعالیتهای غیربحرانی می‌توان بفرض ساعت ۸-۵ روزهای دوشنبه و جمعه را در نظر گرفت.

از دیدگاه و نقطه نظر مدیریت اقتصادی، مدیریت شبکه، طرح‌ریزی استراتژی و راهکار برای مهندسی نمودن اعمال و نگهداری شبکه و سرویسهای شبکه است تا با کمترین هزینه نیازمندیهای حال و آینده را پاسخگو باشد. که ایجاد مدیریت خوب، تعامل و ارتباطات مابین گروهها را خوب تعریف می‌کند تا وظایف بنحو احسن اجرا شود.



شکل ۱- وظایف مدیریت شبکه

در شکل ۱ یک دید بالا به پایین از وظایف مدیریت شبکه را نشان می‌دهد که از سه گروه اصلی تشکیل شده است ۱- تدارک و پیش‌بینی نمودن شبکه ۲- عملهای شبکه ۳- نصب و نگهداری شبکه (I&M). این امر مفید است چرا که وظایف در گروهی حاضر قرار گرفته و توانایی پاسخگو شدن را براساس یک ساختار سازمانی فراهم می‌آورد. تهیه و تدارک شبکه اولین گروه پاسخگو برای گروه مهندسی است و I&M اولین گروه پاسخگو برای گروه مستقر کننده وسایل (Facilities) هستند تعادل مابین گروهها در شکل ۲ نشان داده شده است عملهای روزانه معمولی وظیفه گروه عملهای شبکه است که مرکز عملهای شبکه را کنترل و مدیریت می‌کنند و عملهای مدیریت شبکه را تقویت می‌کنند. وظیفه NOC در ابتدا به عملهای شبکه و سپس به پاسخگو بودن به گروههای تدارک و نصب و نگهداری مربوط می‌شود[2].



شکل ۲ – عناصر مدیریت شبکه

با وجود تنوع سیستم‌های مدیریت شبکه یا NMS (Network Management System)، ساختار آنها کمابیش شباهت‌هایی به یکدیگر دارد. در تمامی این سیستم‌ها عناصر مدیریت‌شونده شامل کامپیوترها و سایر تجهیزات شبکه، به صورت دوره‌ای و یا در صورت مشاهده شرایط خاص (مانند خرابی یک بخش) به صورت آنی، پیامی حاوی اطلاعات لازم در مورد رویداد پیش‌آمده و وضعیت فعلی خودشان، برای سیستم مدیریت کننده ارسال می‌کنند. این سیستم نیز با توجه به نوع پیام دریافت شده، عملیاتی همچون تولید آلارم، ثبت رویداد، توقف عملیات و یا سعی در برطرف‌سازی مشکل را به انجام می‌رساند[3].

البته مکانیسم مدیریت‌کننده نیز می‌تواند خود راساً اقدام به بررسی وضعیت عناصر مدیریت‌شونده در شبکه نماید. همان‌طور که در شکل ۱ نشان داده شده است، عناصر مدیریت شونده باید حاوی موجودیتی موسوم به کارگزار مدیریت (Agent) باشند که مسئولیت جمع‌آوری اطلاعات لازم و ارسال آنها را به سیستم مدیریت شبکه بر عهده دارد. در پاره‌ای مواقع این موجودیت نقش واسطی (proxy) را بین سیستم مدیریت شبکه و تعدادی از عناصر دیگر بر عهده دارد. استفاده از واسطه‌ها به کاهش تعداد پیام‌های اضافی در سطح شبکه کمک می‌نماید[3-6].

سیستم مدیریت کننده، نرم‌افزاری متشکل از ماجول‌های مدیریتی می‌باشد که وظایف و توابع گوناگونی را برعهده دارد. ساختار درونی این سیستم می‌تواند به دلخواه طرح شود ولی ارتباط آن با عناصر کارگزار حتماً باید با استفاده از یک پروتکل استاندارد مانندSNMP یا CMIP انجام پذیرد[2].

SNMP پروتکل اصلی جهت تبادل اطلاعات مدیریتی بین عناصر شبکه و سیستم مدیریت می‌باشد که استاندارد بودن آن، امکان کار تجهیزات سازندگان گوناگون با یکدیگر و با نرم‌افزارهای مدیریت شبکه سایر سازندگان را فراهم می‌نماید. جدیدیترین نسخه پروتکلSNMP، نسخه ۳ می‌باشد ولی نسخه‌های اصلی و پرکاربرد آن SNMPv1 و SNMPv2 می‌باشند که نسخه اخیر دارای ایمنی بیشتری در برابر نفوذهای غیر مجاز به ساختار مدیریتی شبکه می‌باشد.

علاوه بر سطوح کنترل کاربر، سطح مدیریت، یکی از سطوح معماری شبکه است که شامل پروتکل های مختلفی می باشد و از استاندارد SNMP می توان به عنوان یک پروتکل در سطح مدیریت نام برد.

طبق استاندارد ISO-8498-2، دو جنبه ایمنی مدیریت در شبکه داریم : امنیت مدیریت و مدیریت در امنیت .بخش امنیت مدیریت در واقع، امنیت بسته های مدیریتی است که در شبکه ارسال می شوند .به عنوان مثال، حفظ امنیت بسته های مدیریتی که در شبکه ارسال و دریافت می شوند به این بخش مربوط میشود .پروتکل هایی همانند ...,IPsec , TLS, SSL در صورتی که از بسته های مدیریتی حمایت کنند، میتوانند جزو این دسته باشند. (البته این پروتکل ها هر نوع ترافیک در شبکه را پشتیبانی می نمایند و فقط مختص ترافیک مدیریتی نیستند و می بایست هر نوع ترافیکی را محافظت نمایند.)

بخش دوم اشاره شده در استاندارد ISO-8498-2، ایجاد مدیریت در ایمنی شبکه و یا مدیریت امنیت می باشد. مدیریت امنیت پشتیبانی هایی است که یک پروتکل مدیریتی همانند SNMP در شبکه انجام می دهد تا ما به یک شبکه امن دست یابیم.[6]

مدیریت شبکه با استفاده از مجموعه ای از ابزارهای کنترلی، به همراه مانیتورینگ شبکه، گزارشی از وضعیت شبکه می دهد و باعث می شود تا سیاست های امنیتی و کنترلی لازم اندیشیده شود. در این بخش پروتکل های کنترلی و مدیریتی وضعیت شبکه را کنترل می نمایند و تعیین می کنند که ترافیک و پیکربندی شبکه چگونه انجام شود.

مدیریت در شبکه، کار پیکر بندی مناسب شبکه را با توجه به کاربرد هر شبکه انجام می دهد و مسولیت نگهداری و پشتیبانی از شبکه، محاسبه مقدار استفاده از منابع و تنظیم سیاست های اجرایی را بر عهده دارد. این تنظیمات افزایش ایمنی شبکه را فراهم می آورند.

مدیریت یک شبکه باید به صورت بلادرنگ و در کنار شبکه ی فعال، انجام پذیرد تا در سرویس دهی شبکه خللی ایجاد نشود و احیانا شبکه کند نشود. ابزارهای مدیریتی شبکه، یک محیط GUI برای مدیر فراهم می نماید و با پیام های مربوطه، خطاهای شبکه را اطلاع می دهد. این ابزار قابلیت بررسی و تست شبکه و ترافیک آن، هم چنین ثبت رویدادهای شبکه را نیز دارند. به کار بردن ابزار های مدیریتی، زمان عیب یابی و راه اندازی سیستم ها را کاهش می دهد[4].

استاندارد SNMP، یک استاندارد مانیتورینگ می باشد که وضعیت شبکه را بررسی کرده و دستورات لازم را ارسال می نماید. سه نسخه از این استاندارد به بازار آمده است. نسخه سوم استاندارد، ابعاد امنیتی احراز هویت، محرمانگی و کنترل دسترسی فیچرهای مدیریتی را پشتیبانی می نماید. پروتکل SNMP مربوط به لایه کاربرد بوده و می تواند بر روی TCP و UDP اجرا شود. البته نسخه یک تنها بر روی UDP قابل پیاده سازی بوده است.

این استاندارد از شماره پورت ۱۶۱ برای ارسال درخواست به عناصر شبکه و شماره پورت ۱۶۲ برای ارسال رویداد ها به ایستگاه مدیریت استفاده می نماید. ایستگاه مدیریتی یا (Management Agent)، کار نظارت و مدیریت را انجام می دهد و سایر عناصر موجود در شبکه تحت نظارت این ایستگاه مدیریتی فعالیت می نمایند. اطلاعات مدیریتی تحت ساختار (Management Information Base) MIB قرار دارند. عناصر(Agent) هایی که در کار مدیریت شبکه شرکت می نمایند، می توانند Bridge ها، مسیریاب ها و یا هاب ها و یا هر عنصر دیگری باشند. مدیریت این عناصر بر عهده ایستگاه مدیریت می باشد که می تواند بیش از یک ایستگاه در نظر گرفته شود. استاندارد SNMP امکان تنظیمات ایستگاه مدیریتی، بازیابی مقادیر MIB و یا اطلاعات از رویدادهایی که در هر Agent رخ می دهد، را با استفاده از دستورات ساده (Get, SET, Trap) به دست می آورد.

پروتکل SNMP ، علاوه بر مدیریت برای ایجاد امنیت شبکه، در ثبت رویدادها و به اصطلاح log management نیز کاربرد دارد. ثبت رویداد ها به منظور آگاهی از رفتار شبکه انجام می پذیرد تا سیاست های مناسب کنترلی برای شبکه بر اساس نوع رویداد ها، تنظیم شود و ما را به سوی داشتن شبکه امن تر رهنمون سازد[5].

بخش های امنیتی پروتکل SNMP

در ادامه معرفی پروتکل مدیریتی SNMP به مکانیزم های امنیتی آن می رسیم.

بخش های امنیتی همانند احراز هویت، محرمانگی و یکپارچگی در نسخه سوم SNMP مورد توجه قرار گرفته است. در زمان انتقال پیام توسط SNMP می توان حالت های دسترسی read-only, read-write, no-access را برای پیام ها تنظیم نمود. در نسخه ۱ و ۲ این پروتکل شنود بسته های ارسال شده قابل انجام بود زیرا رمزنگاری داده در ترافیک شبکه انجام نمی شد.

این پروتکل می تواند بر روی TCP پیاده سازی شود اما در اغلب موارد بر روی UDP پیاده سازی می شود که IP spoofing را در این بخش میسر می نماید و شنود بسته های داده ارسال شده در شبکه را رد لایه IP قابل انجام می نماید.

حملات brute force (شکستن رمز با امتحان تعدادی کلید با توجه به طول کلید الگوریتم رمزنگاری) و dictionary attack از جمله مواردی هستند که تمام نسخه های این پروتکل نسبت به آن ضعف دارند. این ضعف به خاطر عدم پشتیبانی پروتکل از challenge- response handshake می باشد.

علاوه بر جملات بالا، این پروتکل می بایست در مقابل حمله dos نیز مقابله نماید. به این منظور، مقایسه پاسخ های دریافت شده به ازای درخواست های دریافت شده به شبکه در SNMP انجام می پذیرد. هر پاسخی که دریافت می شود می بایست به ازای درخواستی، ارسال شده به شبکه باشد. در غیر این صورت احتمال وجود حمله dos وجود دارد.

در نسخه سوم این پروتکل مدل امنیتی مبتنی بر کاربر با نام ((User-based Security Model(USM)) تعریف شده است. مدل USM در معماری SNMP کاربرد دارد و پروسیجر هایی تولید می کند تا در ایجاد سطوح امنیتی برای پیام های SNMP استفاده شوند. یکسری MIB مدیریتی برای مانیتورینگ و نظارت بر این مدل امنیتی (USM) تعریف شده است. نحوه انجام این تنظیمات در RFC 3414 تشریح شده است.

در بخش احراز هویت از الگوریتم های رمزنگاری HMAC-MD5-96 و HMAC-SHA-96 استفاده می شود و CBC-DES برای محرمانگی در پروتکل SNMP کاربرد دارد. به منظور حفظ محرمانگی، احراز هویت پیام بایستی الزامی باشد. مدل USM پروتکل SNMP امکان استفاده از این الگوریتم ها را در کنار SNMP مهیا نموده است[9].

هر کدام از الگوریتم ها به روشی پیاده سازی می شوند و توضیح نحوه پیاده سازی روش ها و الگورتم های ذکر شده در بالا جزو معرفی SNMP نمی باشد. برای آشنایی با هر کدام از این الگوریتم ها می توانید از شبکه اینترنت استفاده نموده و شرح پیاده سازی آن ها را مطالعه نمایید. روش و مدل USM این الگوریتم ها را به منظور افزایش کارایی و امنیت پروتکل SNMP در کنار هم و به کمک واحد های MIB پیاده سازی نموده است.

پروتکل SNMP امکان پیاده سازی بر روی محیط های متعدد با کاربری در شبکه های وسیع و یا شبکه هایی با کاربرد های محدود و کوچک را دارا می باشد.

پروتکل SNMP برای سیستم های مدیریت در شبکه به منظور مانیتورینگ تجهیزات نصب شده در شبکه کاربرد دارد و شامل یک لایه کاربردی، یک پایگاه داده و بخش داده می باشد.

داده مدیریتی پیکربندی سیستم را توصیف می نماید. داده ها توسط کاربرد های مدیریتی تنظیم و مقدار دهی می شوند. معماری و ساختار SNMP متشکل از مجموعه ای از ایستگاه های مدیریت شبکه و المان های شبکه است. المان های مدیریتی کاربردهای مربوط به مدیریت را اجرا می کنند. این المان ها وظیفه منترل و مانیتورینگ تجهیزات شبکه را بر عهده دارند. SNMP ارتباط بین المان های مدیریتی و المان های شبکه را در لایه کاربرد OSI برقرار می نماید[10-9].

هر سیستم مدیریتی با استفاد از یک بخش نرم افزاری (agent) اطلاعات لازم را از طریق SNMP به سیستم مدیریتی منتقل می نماید. همان طور که قبلا هم اشاره شده است، SNMP پورت ۱۶۱ از UDP را برای agent ها و پورت ۱۶۲ را برای مدیریت استفاده می کند. مدیریت می تواند درخواست ها را از طریق هر پورت مبدا به پورت ۱۶۱ یک agent بفرستد و هر agent پاسخ درخواست مدیریت را به پورت های مبدا می فرستد.

مدیریت پیام های هشدار و اطلاع رسانی را از طریق پورت ۱۶۲ دریافت می نماید، اما یک agent اجازه دارد پیام های هشدار و اطلاع رسانی را از طریق هر پورت در دسترس خود ارسال نماید.

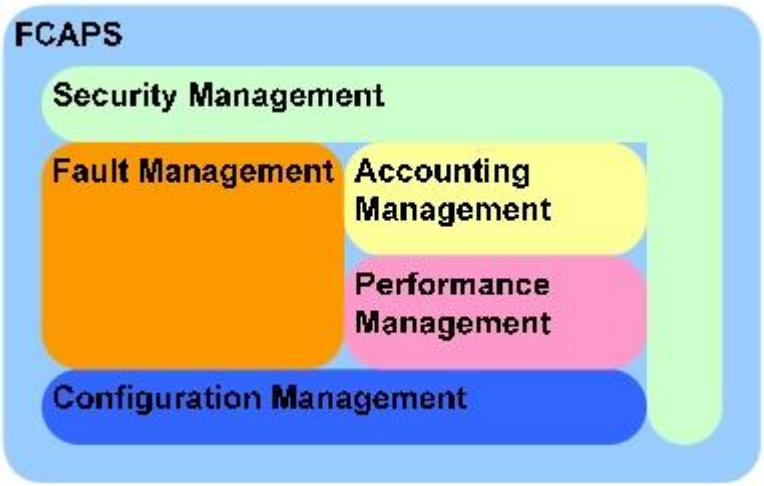
تجهیزات شبکه که از پروتکل SNMP استفاده می نمایند، یک گره مدیریتی در شبکه تشکیل می دهند. این گره ها و تجهیزات مدیریتی، وظیفه جمع آوری و ذخیره اطلاعات مدیریتی و تبدیل آن ها به داده هایی قابل استفاده برای SNMP را بر عهده دارند.

یک agent در واقع یک ماژول نرم افزاری مدیریت شبکه است و در مورد داده های محلی گره شبکه، اطلاعات مدیریتی دارد و آن ها را به فرمت قابل تفسیر SNMP، ترجمه می نماید.

ساختار مدیریتی توسط زیربخشی از SNMP با نام MIB و یا (Management Information Base) تعریف می شود. MIB ساختار مدیریتی یک سیستم را توصیف می کند. هر واحد MIB با نام OID و یا (Object Identifier) نام دارد و متغیری را در بر می گیرد که توسط SNMP قابل خواندن و تفسیر می باشد. هر OID می تواند به لایه ای از OSI مربوط باشد[10].

پروتکل SNMP، دارای یک متعادل کننده بار نیز می باشد. این بخش (dispatcher) وظیفه مدیریت ترافیک بار را در SNMP بر عهده دارد. برای بسته های داده ای که خارج می شوند، یک dispatcher نوع پیام و نوع پردازشی که باید روی آن انجان پذیرد، را مشخص می نماید. سپس پیام را به ماژول مورد نظر راهنمایی می نماید. Dispatcher پیام مربوطه را برای ارسال به لایه انتقال می سپارد.

برای پیام های ورودی، dispatcher پیام ها را از لایه انتقال دریافت می نماید و هر پیام را به ماژول متناظر برای پردازش می دهد و پیام را به کاربرد مورد نظر راهنمایی می نماید.



شکل۳- توابع پنجگانه مدیریت شبکه

توابع اصلی سیستم مدیریت شبکه

سازمان بین‌المللی استانداردها موسوم به ISO مدلی را برای سیستم‌های مدیریت شبکه پیشنهاد نموده که به استانداردی جهت شناخت و مقایسه قابلیت‌های آنها تبدیل گردیده است. این مدل توابع سیستم مدیریت شبکه را در پنج حوزه قرار می‌دهد (شکل ۳) که به طور خلاصه با حروف اول آنها یعنی FCAPS شناخته می‌شوند[11-5-4]:

۱- مدیریت خطا (Fault Management)
۲- مدیریت پیکربندی (Configuration Management)
۳- مدیریت حسابرسی (Accounting Management)
۴- مدیریت کارآیی (Performance Management)
۵- مدیریت امنیت (Security Management)

البته بسیاری از سیستم‌های موجود، در عمل تنها بخشی از توابع پنجگانه فوق را اجرا می‌کنند و همواره نمی‌توان تناظر یک به یک بین قابلیت‌های کاربردی یک سیستم مدیریت شبکه و توابع فوق مشاهده نمود. در ادامه اشاره‌ای مختصر به توابع هر گروه خواهیم داشت.

مدیریت خطا: تشخیص، ثبت، تولید آلارم و درصورت امکان سعی در رفع خطاهای شبکه بر عهده این بخش می‌باشد. خطا می‌تواند اثرات مخربی بر کارکرد شبکه داشته‌باشد و به همین دلیل مدیریت خطا مهمترین عنصر در مدیریت شبکه محسوب می‌گردد و اولین عنصری است که در نرم افزارهای مدیریت شبکه گنجانده می‌شود[5].

مدیریت پیکربندی: هدف این بخش، نظارت و گردآوری اطلاعات مرتبط با پیکربندی سیستم‌های شبکه در یک نقطه، جهت کنترل تاثیر آنها بر عملکرد کلی شبکه می‌باشد، برای مثال پیکربندی یک کامپیوتر شامل اطلاعاتی در مورد نوع سیستم‌عامل و اینترفیس‌های آن با شبکه، پروتکل ارتباطی و... می‌باشد که در پایگاه اطلاعات مدیریت پیکربندی، ذخیره می‌گردند[5].

مدیریت حسابرسی: هدف مدیریت حسابرسی، اندازه‌گیری میزان استفاده کاربران شبکه از منابع آن می‌باشد، به این ترتیب علاوه بر کنترل سطح دسترسی و استفاده از شبکه توسط کاربران، نوعی اعتدال میان منابع و حجم استفاده از آنها پدید می‌آید که به کمک مدیریت کارآیی می‌آید. مدیریت حسابرسی اطلاعات لازم برای محاسبه و صدور صورت حساب کاربران را فراهم می‌نماید[11].

مدیریت کارآیی: این گروه از توابع، اندازه‌گیری و نمایش پارامترهای کارآیی شبکه همچون نرخ عبوری برونداد (Throughput)، زمان پاسخ‌دهی و نرخ بهره‌وری خطوط (Line Utilization) را برعهده دارند که به تلاش برای حفظ این پارامترهای کیفی در سطح مطلوب منجر می‌گردد[5].

فرآیند مدیریت کارآیی معمولاً در سه گام انجام می‌گیرد. ابتدا جمع‌آوری اطلاعات مرتبط با کارآیی، سپس تحلیل این اطلاعات و در نهایت واکنش مناسب در صورت کاهش هر یک از پارامترهای کیفی به کمتر از مقدارهای آستانه که پیشاپیش توسط مدیریت شبکه تعریف گردیده‌اند. بسیاری از سیستم‌های مدیریت شبکه قابلیت پیش‌بینی شرایط ناکارا را به کمک تکنیک‌های شبیه‌سازی دارند. به عبارت دیگر قادر خواهند بود تا پیش از وارد شدن شبکه به شرایط بحرانی، اخطارهای لازم را به گردانندگان آن بدهند[14-11].

مدیریت امنیتی: وظیفه دارد دسترسی به منابع شبکه را کنترل نماید و از دسترسی عوامل خارج از شبکه ممانعت به عمل‌آورد. به این ترتیب امکان بهره‌گیری غیر مجاز (عمدی و یا سهوی) از منابع شبکه وجود نخواهد داشت. مدیریت امنیت می‌تواند منابع یک بخش از شبکه را از دید و استفاده کاربران سایر بخش‌ها، دور کند. البته برای دستیابی به این هدف، شناسایی منابع حساس و ایجاد نوعی تناظر بین کاربران مجاز و این منابع لازم می‌باشد. مدیریت امنیت همچنین سوابق کلیه استفاده‌های نابجا از منابع شبکه را برای استفاده‌های بعدی مدیران امنیتی شبکه، ثبت می‌نماید[11-5].

مدیریت خطا

- تولید، گزینش و اعلان هشدارها
- تشخیص مشکلات
- تصحیح مشکلات
- آزمایش و پذیرش
- بازیابی شبکه

مدیریت پیکربندی

- تنظیمات آغازین سیستم‌ها
- تدارکات شبکه
- تشخیص خودکار
- ذخیره و بازیابی تنظیمات

* مدیریت پایگاه داده

مدیریت حسابرسی

* ثبت میزان استفاده از شبکه
* تولید صورت حساب

مدیریت کارآیی

* جمع آوری اطلاعات مرتبط
* تولید گزارش‌ها
* تحلیل اطلاعات

مدیریت امنیت

* کنترل دسترسی
* ثبت دسترسی
* مدیریت مجوزها

اصولاً با توجه به پیچیدگی و تنوع وظایف یک سیستم مدیریت شبکه، رعایت مدل FCAPS، این اطمینان را ایجاد می‌کند که کلیه اصول پایه رعایت گردیده‌اند. به این ترتیب مدیریت خطا و کارایی اطلاعات لازم برای تشخیص عناصر و لینک‌های ناکارا و رفع معایب شبکه را فراهم می‌کنند. مدیریت پیکربندی، تاثیر تغییراتی که پرسنل شبکه در تنظیمات سیستم‌ها ایجاد کرده‌اند را نشان می‌دهد تا نقش خطاهای انسانی در مشکلات شبکه مشخص‌شود (که معمولاً عامل اصلی ایجاد خطا در شبکه می‌باشد)، مدیریت امنیتی نیز سابقه حملات به شبکه و عکس‌العمل در برابر آنها را برای استفاده‌های آتی ضبط می‌کند.

البته در برخی موارد و برحسب نیاز، دو گروه دیگر از توابع را نیز در زمره توابع سیستم مدیریت شبکه قرار می‌دهند: مدیریت دارایی‌ها (Assessment) و مدیریت برنامه‌ریزی (Planning).

مدیریت دارایی‌ها، یک پایگاه داده از شرایط فعلی تجهیزات شبکه، امکانات آن‌ها و حتی پرسنل ایجاد می‌کند و قادر به تولید گزارش‌های آماری از این پایگاه می‌باشد. مدیریت برنامه‌ریزی نیز به یاری آنالیزهایی که بر روی روند کار شبکه و مشکلات آن دارد، اطلاعاتی را جهت برنامه‌ریزی هر چه بهتر توسعه شبکه، در اختیار قرار می‌دهد[12].

لایه‌های مدیریت شبکه

پیچیدگی و تعدد وظایف سیستم مدیریت شبکه باعث گردیده تا مطابق استاندارد شبکه‌های مدیریت مخابراتی موسوم به TMN، آن‌ها را در چهار لایه جای دهند که بر روی یک لایه فیزیکی متشکل از تجهیزات شبکه، قرار دارند. در این مدل هر لایه تعریف خود را دارد[12]:

لایه عناصر (Element Layer): متشکل از عناصر مدیریت شونده در سراسر شبکه می‌باشد.

لایه مدیریت عناصر (Element Management Layer): متشکل از واحدهای نرم‌افزاری است که هر یک قادر به مدیریت گروه خاصی از عناصر شبکه می‌باشند. هر واحد این لایه به کمک نرم‌افزار کارگزار موجود در گروه تجهیزات مربوط به خود و پروتکل SNMP به گردآوری اطلاعات لازم راجع به عناصر آن گروه اقدام می‌کند و البته دارای دید کاملی از شبکه و همبندی بین عناصر آن نمی‌باشد.

لایه مدیریت شبکه (Network Management Layer): این لایه اطلاعات لازم راجع به عناصر شبکه را از طریق لایه مدیریت عناصر به‌دست می‌آورد و با ایجاد یک تصویر یکدست از کلیت شبکه، کنترل آن را به صورت یک موجودیت واحد در اختیار می‌گیرد.

لایه مدیریت سرویس (Service Management Layer): کنترل سطح کیفی خدماتی مانند شبکه‌های خصوصی مجازی (VPN) و تلفن اینترنتی بر عهده این لایه است. فراهم‌کنندگان خدمات شبکه مجبور به عقد قراردادی با مشتریان خود موسوم

به توافقنامه سطح خدمات یا SLA (Service Level Agreement) می‌باشند، که در آن سطح کیفی خدمات مورد نیاز و جریمه‌های متعلقه در صورت ناتوانی فراهم کننده از ارائه این سطوح مشخص می‌گردد.

لایه مدیریت خدمات، در عمل ابزاری برای گردانندگان شبکه جهت حفظ چارچوب و عمل به تعهدات SLA می‌باشد.

لایه مدیریت تجاری (Business Management Layer): در بالاترین لایه، مدیریت تجاری قرار دارد که موضوعاتی همچون روابط بین شبکه‌ای را به لحاظ موضوعات مالی و تجاری کنترل می‌کند. این لایه با ساختار کلی مدیریت سازمانی فراهم‌کننده و مشتریان بزرگ آن در ارتباط تنگاتنگ می‌باشد و از برخی لحاظ ماهیت متفاوتی نسبت به سایر لایه ها دارد.

مشخصات لازم برای سیستم مدیریت شبکه

شرط اصلی برای دستیابی به اهداف مدیریت شبکه، تأمین کلیه توابع پنجگانه FCAPS می‌باشد. اصولاً یک سیستم مدیریت شبکه موفق واجد خصوصیاتی است که در ادامه به آنها اشاره می‌شود[4]:

قابلیت تحلیل: پالایش، تطبیق و تحلیل اطلاعات گردآوری شده در سیستم مدیریت، در تشخیص میزان پایداری و کارآیی شبکه نقش اصلی را بازی می‌کند. اطلاعات خام بدون یک تحلیل مناسب چندان مفید نخواهند بود. ذکر یک مثال به روشن شدن اهمیت موضوع کمک می‌کند.

به طور معمول پدید آمدن یک خطا یا خرابی در نقطه‌ای از شبکه باعث ارسال همزمان پیام‌های متعدد از جانب تجهیزاتی که در محدوده آن خطا قرار دارند، می‌گردد. حال اگر سیستم مدیریت شبکه فاقد هوشمندی کافی جهت تشخیص منبع اصلی خطا باشد، اپراتورهای شبکه با سیلی از آلارم‌ها روبرو خواهند شد که فرآیند رفع خطا را دشوار می‌گرداند.

گزارش‌گیری: امکان تولید گزارش‌های جامع برای سطوح گوناگون پرسنل فنی و مدیران شبکه، از دیگر مشخصات یک سیستم مدیریت شبکه می‌باشد. این گزارشها می‌بایست علاوه بر تعیین مشکلات و گلوگاه‌ها، همراه با ارائه راهکارهایی جهت رفع آنها باشد.

تشخیص تقدم: تعیین شدت مشکلات و صدماتی که می‌توانند به عملکرد شبکه وارد آورند، از قابلیت‌های پیشرفته یک سیستم‌های مدیریت شبکه می‌باشد که وجود آن به پرسنل نگهداری شبکه اجازه انتخاب ترتیب مقابله با مشکلات را خواهد داد.

ساختار لایه‌ای: شبکه، سیستمی متشکل از تعدادی زیرسیستم می باشد. امکان مدیریت و تولید گزارش در سطوح گوناگون شبکه از یک گره گرفته تا کل آن، از مشخصات لازم برای یک سیستم انعطاف‌پذیر می‌باشد.

استفاده آسان: به کارگیری برخی از سیستم‌های مدیریت شبکه، مترادف طی کردن دوره‌های طولانی آموزش جهت کسب مهارت لازم در کار با آنها می‌باشد. اما رقابت و لزوم کاهش هزینه‌ها، چنین الزاماتی را نمی‌پذیرد. یک سیستم مدیریت شبکه مدرن باید در تمامی مراحل پیاده‌سازی، راه‌اندازی و به کارگیری با استفاده از رابط‌های گرافیکی (GUI) و فرآیندهای استاندارد، نیازهای آموزشی پرسنل را به حداقل برساند.

سکوهای مدیریت شبکه

سیستم‌های مدیریت شبکه، عموماً متشکل از چندین بخش می‌باشند که هر یک اجرای گروهی از توابع را برعهده دارند. در چنین شرایطی، ملاحظات اقتصادی و فنی، پیاده‌سازی عناصر یکسان در میان انواع سیستم‌های مدیریت شبکه را به صورت یک پلتفرم مشترک توصیه می‌کند. پلتفرم مدیریت شبکه یک محصول نرم‌افزاری است که قادر به ارائه توابع اولیه و عمومی مدیریت شبکه برای طیف متنوعی از تجهیزات و سیستم‌ها می‌باشد. برخی از مهمترین این توابع عبارتند از[5-4]:

۱- رابط گرافیکی کاربران (GUI)

۲- نقشه همبندی شبکه (Map Network Topology)

۳- سیستم مدیریت پایگاه داده (DBMS)

۴- مکانیسم استاندارد جمع‌آوری اطلاعات از تجهیزات

۵- منوهای قابل تغییر و سفارشی

۶- مکانیسم ثبت رویدادها (Log)

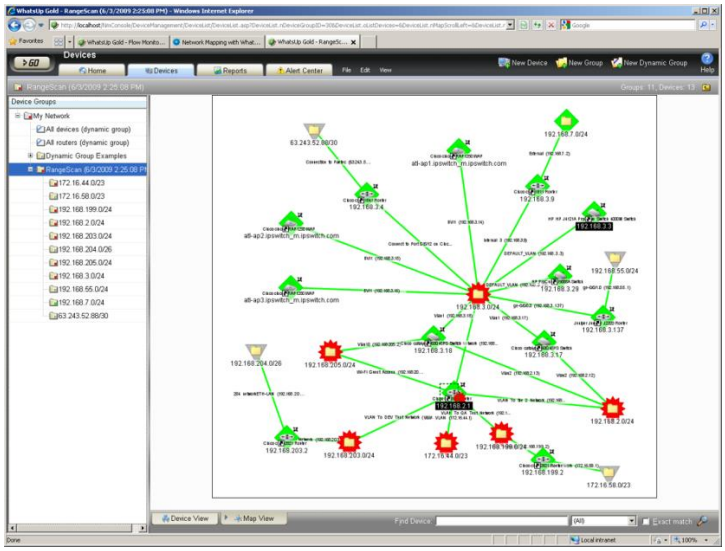
برخی از پلتفرم‌های مدیریت شبکه دارای قابلیت‌های اضافی چون ابزارهای ترسیم گرافیکی، اینترفیس‌های برنامه‌نویسی کاربردی (API) و ماجول‌های امنیتی می‌باشند. اصولاً سه معماری متداول برای پیاده سازی این پلتفرم‌ها وجود دارد:

۱. معماری متمرکز

۲. معماری توزیع شده

۳. معماری سلسله مراتبی

در معماری متمرکز، پلتفرم مدیریت شبکه برروی یک کامپیوتر مرکزی قرار دارد که البته در این صورت وجود یک سیستم پشتیبان برای حفظ استمرار عملیات، الزامی است. مهمترین مزایای معماری فوق امنیت بالا و تمرکز کلیه توابع در یک نقطه می‌باشد. در مقابل به دلیل تمرکز تمامی عملیات در یک نقطه، آسیب پذیری بالا می‌رود و توسعه برای شبکه های بزرگ به دشواری انجام می‌گیرد[13-12].



شکل ۵ - نمایی از نرم افزار مدیریت شبکه What What's up Gold

در معماری سلسله مراتبی، یک سیستم مرکزی و تعدادی زیرسیستم وجود دارد که اطلاعات را پس از پالایش و تحلیل مقدماتی در اختیار سیستم مرکزی قرار می‌دهند. در نتیجه فشار کمتری به سیستم مرکزی وارد می‌گردد. البته در عوض مزایای امنیتی معماری متمرکز از دست می‌رود.

در معماری توزیع‌شده، عملاً شبکه به بخش‌های کوچکتری تقسیم می‌شود که یک سیستم مدیریت شبکه در راس هر یک از آنها قرار دارد. هر بخش به تنهایی قادر به اجرای توابع مدیریت و تولید گزارش می‌باشد. می‌توان با تمرکز اطلاعات در یک نقطه مرکزی، مدیریت سراسری را نیز به طور همزمان اجرا نمود که به این ترتیب تلفیقی از مزایای دو معماری متمرکز و سلسله مراتبی به‌دست می‌آید.

در بازار سکوهای مدیریت شبکه سه عنوان HP OpenView، Sun SunNet Manager و IBM NetView در راس قرار دارند که در میان آنها HP OpenView از جایگاه ممتازی در رده شبکه‌های بزرگ برخوردار است و در عمل به صورت استانداردی برای حفظ سازگاری میان محصولات مدیریت شبکه درآمده است.

بر روی پلتفرم‌های مدیریت شبکه، رده دیگری از نرم‌افزارهای مدیریتی موسوم به کاربردهای مدیریت شبکه قرار دارند که اجرا توابع مکمل را برعهده دارند و معمولاً خاص گروهی از تجهیزات طراحی می‌شوند. به عنوان مثال در این رده می‌توان به نرم‌افزار

CiscoWorks از شرکت Cisco و همچنین Optivity از شرکت Nortel اشاره داشت. اغلب محصولات این گروه توسط شرکت‌های سازنده تجهیزات و به عنوان مکملی برای آنها تهیه می‌گردد.

به عنوان مثالی دیگر، می‌توان از نرم‌افزار What's up Gold نام برد. این برنامه محصول شرکت Ipswitch، یک نرم‌افزار مدیریت شبکه جمع و جور و ارزان قیمت می‌باشد که از قابلیت‌های مناسبی برخوردار است و می‌توان نسخه آزمایشی آن را از نشانی www.ipswitch.com/downloads دریافت نمود.

این نرم افزار به محض پدیدآمدن هر نوع خطا در شبکه با ارسال آلارم پرسنل فنی را مطلع می‌سازد و با تعیین گلوگاه‌ها، علاوه بر کمک به رفع مشکل، طرح توسعه شبکه را ساده‌تر می‌سازد. برخی از قابلیت‌های این نرم افزار به طور خلاصه عبارتند از:

- تشخیص کلیه عناصر دارای آدرس IP در شبکه و ایجاد نقشه توپوگرافیک از شبکه و زیرشبکه‌های آن به صورت کاملاً خودکار
- نظارت بر عملکرد کلیه تجهیزات و سرویس‌های شبکه و راه‌اندازی مجدد سرویس‌ها در صورت نیاز.
- ارسال آلارم‌های هشداردهنده بر روی کنسول‌های مدیریت و یا از طریق SMS،e-Mail و تلفن.
- اجرای خودکار برنامه‌های بازیابی و رفع خطا.
- امکان دسترسی و کنترل نرم‌افزار از هر نقطه بر روی Web
- ثبت تغییرات کارآیی سیستم‌ها و سرویس‌ها و جمع‌آوری آمار استفاده از شبکه.
- تولید خودکار فهرست رویدادها و گزارش‌های آماری از آنها.

نتیجه گیری

موضوع امنیت در شبکه ها آن قدر مهم است که لازم باشد ضمن تأکید مداوم بر آن، هر از گاهی نگاهی دوباره به آن انداخت و با توجه به تحولاتی که در این حوزه روی می دهد، موضوع جدیدی درباره آن نوشت یا موضوعات قبلی را با رویکردهای جدید بازخوانی کرد .از یک شبکه کامپیوتری، عوامل مهمی مانند نوع سیستم عامل، موجودیتها، منابع، برنامه های کاربردی، نوع خدمات و کاربران نقش مهم ومستقیمی در امنیت شبکه دارند. برقراری امنیت بصورت ۱۰۰ ٪ امکان پذیر نیست چرا که بعضی از عوامل از حیطه قوانین سیستمی خارج هستند، بعنوان نمونه کانالهای مخابراتی هدایت ناپذیر (مثل امواج مخابراتی و ارتیاط ماهواره ای) یا کاربران شبکه (که همیشه از آموزشهای امنیتی داده شده استفاده نمی کنند.). بنابراین الگوی امنیتی شبکه یک طرح امنیتی چند لایه و توزیع شده را پیشنهاد می کند ،به نحوی که کلیه بخشهای شبکه اعم از تجهیزات، ارتباطات، اطلاعات و کاربران را در برمی گیرد . در الگوی امنیتی ضمن مشخص کردن سیاست امنیتی شبکه که در اصل در مورد اهداف امنیتی بحث می کند، راهکارهای مهندسی و پیاده ازی امنیت نیز ارئه می گردد و با آموزشهای مختلف امنیتی و نظارت مداوم ، امنیت شبکه بطور مداوم ارزیابی می گردد. هکرها به طور فزاینده ای اقدام به حمله به شبکه ها می کنند. رویکرد سنتی امنیت - یعنی یک فایروال در ترکیب با یک آنتی ویروس- در محافظت از شما در برابر تهدیدهای پیشرفته امروزی ناتوان است. اما شما می توانید با برقرای امنیت شبکه با استفاده از رویکرد لایه بندی شده، دفاع مستحکمی ایجاد کنید. با نصب ابزارهای امنیتی در پنج سطح موجود در شبکه تان می توانید از داده های دیجیتالی خود محافظت کنید و از افشای اطلاعات خود در اثر ایجاد رخنه های مصیبت بار تا حد زیادی بکاهید. اما فراموش نکنید هیچ سیستمی صد در صد امن نخواهد بود.

References

1. Sampson, Andrew T. "The use of FCAPS and ITIL in managing the network of a medium to large public sector organisation."Asian journal of information technology 10(6):240-248,2011
2. Subramanian, Mani. *Network management: principles and practice*. Pearson Education India, 2010.

3. Kitagata, Gen, et al. "Network Management System Based on Activated Knowledge Resource." *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*. IEEE, 2012.
4. Kwiecień, Andrzej, and Karol Opielka. "Management of Industrial Networks Based on the FCAPS Guidelines." *Computer Networks*. Springer Berlin Heidelberg, 2012. 280-288.
5. Iournals, Medwell. "The Use of FCAPS and ITIL in Managing the Network of a Medium to Large Public Sector Organisation." *Asian J. Inform. Techn0l* 10.6 (2011): 240-248.
6. Hu, Zechun, and Furong Li. "Cost-benefit analyses of active distribution network management: investment reduction analysis." *Smart Grid, IEEE Transactions on* 3.3 (2012): 1075-1081.
7. Hassan, Rosilah, et al. "Architecture of network management tools for heterogeneous system." *arXiv preprint arXiv:1001.1967* (2010).
8. Kim, Hyojoon, and Nick Feamster. "Improving network management with software defined networking." *Communications Magazine, IEEE* 51.2 (2013): 114-119.
9. Yang, Jeonghwa, W. Keith Edwards, and David Haslem. "Eden: supporting home network management through interactive visual tools." *Proceedings of the 23nd annual ACM symposium on User interface software and technology*. ACM, 2010.
10. Nuangjamnong, Chompu, Stanislaw P. Maj, and David Veal. "The OSI network management model-capacity and performance management." *Management of Innovation and Technology, 2008. ICMIT 2008. 4th IEEE International Conference on*. IEEE, 2008.
11. Mikkilineni, Rao, and Ian Seyler. "Parallax-A New Operating System Prototype Demonstrating Service Scaling and Service Self-Repair in Multi-core Servers." *Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2011 20th IEEE International Workshops on*. IEEE, 2011.
12. Mearns, Haydn, John Leaney, and Dominique Verchere. "The architectural evolution of telecommunications network management systems." *Engineering of Computer Based Systems (ECBS), 2010 17th IEEE International Conference and Workshops on*. IEEE, 2010.
13. Wuhib, Fetahi, and Rolf Stadler. "Distributed monitoring and resource management for large cloud environments." *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on*. IEEE, 2011.
14. BARBU, Gheorghe. "ITIL&FCAPS-NETWORK MANAGEMENT FUNDAMENTALS." *Defense Resources Management in the 21st Century* (2012).