# لجستیک و اهمیت مدیریت شبکه گسترده رایانه‌ای آن

**مهندس علی کریمی**

**عضو هیأت علمی دانشگاه امام حسین (ع)**

**چکیده**

مدیریت شبکه‌های رایانه‌ای جهت کارآمد نمودن بهره‌برداری از قابلیت‌های سیستم‌های ارتباطی و اطلاعاتی به فکر ساختار مشخصی هستند تا توسعه سریع و پایدار، نگهداری ساده و مقرون به صرفه، پیش‌بینی شرایط مختلف و انعطاف‌پذیری در امر مدیریت را فراهم نمایند. هدف نهایی از مدیریت شبکه، داشتن اطمینان از کیفیت و پایداری خدمات ارائه شده در شبکه می‌باشد. سیستم مدیریت شبکه و ابزارهای مربوطه، برای کنترل عملیات شبکه و کاربردهای مدیریتی از قبیل مدیریت خطا، مدیریت امنیت، مدیریت کارآیی شبکه و... مورد استفاده قرار می‌گیرند. اعمال روش‌های مدیریتی علمی و استاندارد، روی شبکه گسترده اختصاصی لجستیک از ضروریات حتمی است و اگر به هر دلیلی امکان مدیریت این شبکه میسر نباشد، سرمایه گذاری برای طراحی و ایجاد شبکه قابل توجیه نخواهد بود.

**۱ـ مقدمه**

مدیریت در حقیقت داشتن ایده برای کارآمد نمودن محیط با ابزارهای در دسترس می‌باشد. مدیریت شبکه نیز با دارابودن نقطه نظرات مختلف و پیاده‌سازی‌های گوناگون، هر روز به صورت مؤثر در این عرصه مدیریتی ظاهر می‌شود.

قرن انفجار اطلاعات، در بستری از ارتباطات با جذابیت ویژه خود معنی شده است. تنوع سرویس‌های مورد درخواست و فعالیت‌های لجستیکی در گستره جغرافیایی وسیع، اهمیت ویژه‌ای به شبکه‌های رایانه‌ای داده است. در این بین نگرش‌های سه گروه از کاربران مورد توجه قرار می‌گیرد. گروه اول کاربران نهایی هستند که در سطح گسترده از این مجموعه امکانات استفاده می‌کنند و تمایل دارند از خدمات متنوع سیستم‌های اطلاعاتی و ارتباطی موردنظر، راحت، مطمئن و ارزان بهره‌مند شوند. گروه دوم متخصصین هستند که پیاده‌سازی، نگهداری و ارائه سرویس‌های گوناگون را عهده‌دار می‌باشند.

این گروه، واسط بین گروه اول و سوم محسوب می‌شوند و به نوعی بستر و تسهیلات لازم جهت استفاده از قابلیت‌های تجهیزات و فناوری‌های مربوطه را فراهم می‌سازند. گروه سوم نیز صاحبان تجهیزات و فناوری‌ها هستند که در واقع بستر عملیاتی را تهیه می‌کنند. این گروه در عین مستقل بودن به لحاظ فنی، به گونه‌ای تحت فشار گروه دوم یعنی متخصصین هستند که آن نیز تأثیرپذیر از گروه اول می‌باشد. لذا تهیه‌کنندگان و عرضه‌کنندگان فناوری ارتباطات و شبکه‌های رایانه‌ای، تحولات مداوم و مستمری را در محصولات خود به وجود می‌آورند و عوامل مختلفی را در مقرون به صرفه شدن محصولات خود مهم می‌دانند. در این بین مقوله مدیریت از جایگاه ویژه‌ای برخوردار می‌شود و در راستای بهره‌برداری اقتصادی از منابع موجود به بهترین نحو مطرح می‌گردد.

با این مقدمه، مدیریت شبکه‌های رایانه‌ای نیز برای کارآمد شدن خود در کنار سایر بحث‌های متنوع، به فکر ساختار مشخصی هستند تا توسعه سریع و پایدار، نگهداری ساده و مقرون به صرفه، پیش‌بینی شرایط مختلف و انعطاف‌پذیری در امر مدیریت را فراهم نماید. این ساختار در حقیقت چارچوب، شرایط و نحوهٔ عمل را نشان می‌دهد که مطابق استاندارد معینی و با توجه به محیط شبکه‌های رایانه‌ای تهیه و تعریف شده و در اختیار متخصصین قرار می‌گیرد تا بدینوسیله بتوانند فناوری‌های مربوطه را با توجه به شرایط خاص خود تعریف و با قاعده‌ای مناسب به کار گیرند.

در این مقاله سعی خواهیم کرد با بیان ساختار مدیریتی شبکه‌های رایانه‌ای، با تکیه بر کاربردهای متنوع سیستم‌های لجستیکی، راهکارهای مدیریت بهینه و قابل اطمینان شبکه‌های رایانه‌ای لجستیکی را تبیین و تشریح نمائیم.

**۲ـ اهداف مدیریت شبکه**

هدف از مدیریت شبکه، داشتن اطمینان از کیفیت سرویس‌ها و خدمات شبکه می‌باشد. در برخورد با این هدف، مدیریت شبکه می‌باید سیاست رسمی یا غیررسمی برای توافقات سطوح مختلف سرویس با کاربران را بنا نهد. به عنوان مثال برای خدمات بحرانی،

وقفه‌ای را نمی‌توان درنظر گرفت و این‌گونه خدمات می‌باید ۲۴ ساعته در طول ۷ روز هفته ادامه یابد که از آن جمله می‌توان به E-mailService و WebService اشاره نمود. بدیهی است برای خدمات و فعالیت‌های غیربحرانی می‌توان به فرض ساعت ۸ الی ۱۲ روزهای دوشنبه و چهارشنبه را در نظر گرفت.

از نقطه نظر مدیریت اقتصادی، مدیریت شبکه طرحریزی استراتژی و راهکار لازم برای مهندسی نمودن فعالیت‌های مربوط به نگهداری شبکه و توسعه خدمات آن می‌باشد تا با حداقل هزینه پاسخگویی به نیازمندی‌های حال و آینده سازمان فراهم شود.

وظایف مدیریت شبکه از سه گروه اصلی زیر تشکیل می‌شود. ۱ـ تدارک و پیش‌بینی کردن شبکه ۲ـ عملیات شبکه ۳ـ نصب و نگهداری شبکه. تهیه و تدارک شبکه، اولین گروه پاسخگو برای گروه مهندسی شبکه است که عهده‌دار طرحریزی و طراحی شبکه هستند.

نصب و نگهداری، اولین گروه پاسخگو برای تیم مستقرکننده تجهیزات می‌باشند. مرکز عملیات شبکه (NOC) [1] در حقیقت عملیات روزانه شبکه را کنترل و مدیریت کرده و عملکرد مدیریتی شبکه را تقویت می‌نماید. وظیفه NOC، در مرحله اول به عملیات شبکه و سپس پاسخگو بودن به گروه‌های تدارک، نصب و نگهداری مربوط می‌شود.

### ۳ـ تدارک و آماده‌سازی شبکه

تدارک شبکه شامل طرحریزی و طراحی شبکه است که باید توانایی پاسخگویی به گروه مهندسی را داشته باشد. گروه مهندسی همیشه یک سلسله از جدیدترین فناوری‌ها را نگه داشته و آنها را معرفی می‌کند.

تغییرات در طرحریزی و طراحی شبکه، ممکن است در تصمیمات مدیریت تأثیر گذارد. بدیهی است طراحی خوب معماری شبکه لجستیک سپاه و استفادهٔ مؤثر از تجهیزات، ما را به مدیریت بهینه برای اصلاح و اعمال تغییرات مورد نیاز در پیکره‌بندی شبکه و افزایش کارآیی آن رهنمون خواهد ساخت.

### ۴ـ مرکز عملیات شبکه (NOC)

وظایف مربوط به عملیات شبکه به وسیله مرکز کنترل عملیات شبکه مدیریت می‌شود. این عملیات به عمل‌های روزانه شبکه و تدارک خدمات آن مربوط می‌شود.

این مرکز کلید عملیات و خدمات شبکه را تحت نظر داشته و تمامی دستورات اجرایی مربوط به سرویس‌های شبکه از طریق این مرکز به مراکز فرعی مدیریت شبکه اعمال می‌شود.

مرکز کنترل عملیات شبکه در حقیقت وظیفه دارد کلیه عملیات، خدمات، خرابی‌ها و سایر عملیات شبکه را کنترل و مدیریت نماید. این وظایف می‌توانند در قالب کنترل پنج نوع ترافیک موجود در شبکه بیان شوند. این ترافیک‌ها عبارتند از:

- ترافیک عملیات شبکه
- ترافیک مدیریت شبکه
- ترافیک مسیریابی شبکه
- ترافیک راهبری سایت‌های شبکه
- ترافیک امنیت سایت‌های شبکه

وظیفه این مرکز در اصل کنترل سطح سرویس این پنج نوع ترافیک می‌باشد. رسیدن به سطح بهینهٔ این ترافیک‌ها این اطمینان را به ما خواهد داد که شبکه‌ای با سطح سرویس دهی بالا، قابل اطمینان، کارآ و با کمترین زمان شکست داشته باشیم.

از لحاظ ساختار فیزیکی، این مرکز مانند یک ساعت می‌باشد، با این تفاوت که علاوه بر سرورها و تجهیزات مورد نیاز کنترل شبکه، تعدادی تجهیزات نمایش وضعیت بخش‌های مختلف مربوط به کنترل عملیات شبکه را نیز دارد. این تجهیزات در سطح استاندارد، معمولاً، ویدئو پروژکتورهایی هستند که اطلاعات و آمار خدمات شبکه را به صورت نمودارها و نقشه‌های مشخص بر روی پرده‌های بزرگی نمایش می‌دهند.

می‌توان گفت که مرکز کنترل عملیات شبکه، با توجه به توسعه شبکه‌ها و پیچیدگی آنها یک بخش ضروری و لازم‌الاجرا جهت رسیدن به یک سطح مطلوب سرویس‌دهی و مدیریت شبکه می‌باشد. این سطح کیفیت می‌تواند به عنوان یک نکته کلیدی برای طراحی و توسعه شبکه‌های گسترده در نظر گرفته شود. نکته دیگری که می‌تواند در مورد این مرکز مورد توجه قرار بگیرد این است که می‌توان تعدادی سرور را جهت گرفتن نسخه‌های پشتیبان از تمامی اطلاعات حیاتی شبکه در این مرکز درنظر گرفت. به این ترتیب، علاوه بر وجود نسخه‌های پشتیبان در سایت‌های فرعی شبکه، یک مرکز پشتیبانی دیگر نیز برای جلوگیری از دست رفتن اطلاعات حیاتی این سایت‌ها وجود خواهد داشت.

سازمان استاندارد جهانی (ISO) [۲] ، پنج کاربرد مدیریت شبکه را تعریف می‌کند که عبارت‌اند از مدیریت خطا، مدیریت پیکره‌بندی، مدیریت کارآیی، مدیریت امنیت و مدیریت محاسبه. مرکز عملیات شبکه جوابگوی جمع‌آوری استراتژی‌ها و تهیه گزارش‌های لازم برای مدیریت، پشتیبانی سیستم و کاربران می‌باشد. سیستم مدیریت شبکه و ابزارهای مربوطه، برای کنترل عملیات شبکه ضروری است که در کاربردهای مدیریتی زیر مورد استفاده قرار می‌گیرد.

**۴ـ۱ـ مدیریت خطا / ترمیم و تجدید سرویس**

هنگامی که یک سرویس در شبکه با شکست مواجه می‌شود،

مرکز کنترل عملیات شبکه باید بتواند مشکل را کشف کرده و سپس جایگزینی سرویس را در حد امکان انجام دهد. اطلاعات مربوط به خطای ایجاد شده در یک پایگاه داده نگهداری می‌شود که این اطلاعات شامل زمان وقوع خطا، نوع خطا، کاربران متأثر از خطا در شبکه و مهندسی برطرف‌کننده خطا می‌باشد. این اطلاعات برای پی‌گیری خطا در شبکه بسیار مهم است و می‌تواند توسط مهندسین مرکز کنترل عملیات شبکه به صورت دستی و یا توسط سیستم مدیریت شبکه (NMS) به صورت خودکار تشخیص و ترمیم شود. کاملاً واضح است که در شبکه گسترده اختصاصی لجستیک سپاه مسأله مدیریت خطا و ترمیم آن از اهمیت ویژه‌ای برخوردار است، چرا که اگر نتوانیم خطاهای ایجاد شده در شبکه را تشخیص دهیم و با ابزارهای مناسبی آنها را ترمیم نمائیم، پایداری شبکه و ارائه خدمات مؤثر در آن دچار خدشه خواهد شد.

**۴ـ۲ـ مدیریت پیکره‌بندی شبکه**

معمولاً سه نوع پیکره‌بندی برای شبکه‌های رایانه‌ای مطرح است. اولین پیکره‌بندی که باید پایدار، استاندارد و دائمی باشد با وضعیت اجرائی فعلی سازمان سازگار نیست. دومین پیکره‌بندی برای یک شبکه، پیکره‌بندی اجرای فعلی و حال حاضر سازمان است.

پیکره‌بندی سوم نیز پیکره‌بندی طرحریزی شده برای آینده است که قطعاً بر اساس نیازمندی‌ها و مقتضیات مدل کلان سیستم‌های جامع آماد و پشتیبانی سپاه، این پیکره‌بندی تنظیم و ایجاد می‌شود. در این شرایط، داده‌های پیکره‌بندی شبکه تغییر می‌یابد و از طریق مرکز عملیات شبکه، می‌توان پیکره‌بندی پویای شبکه را بر اساس اطلاعات جدید اعمال نمود. وضعیت جاری شبکه از قبیل وضعیت ترافیک و کارآیی، توسط سیستم مدیریت شبکه به صورت بلادرنگ نشان داده می‌شود و می‌توان توسط مرکز عملیات شبکه پیکره‌بندی شبکه را به‌گونه‌ای تغییر داد که ترافیک شبکه به حد معمولی رسانده شود. این قابلیت برای مدیریت بهینه نقل و انتقال داده بین رده‌های مختلف در شبکه رایانه‌ای لجستیک سپاه بسیار حیاتی است زیرا در هر لحظه می‌توان وضعیت شبکه را از طریق مرکز عملیات شبکه مشاهده کرده و آن را کنترل و مدیریت نمود.

**۴ـ۳ـ مدیریت امنیت شبکه**

مدیریت امنیت شبکه در سطح وسیعی مطرح است که امنیت فیزیکی را هم شامل می‌شود. برای این منظور باید دسترسی کاربران به امکانات شبکه کاملاً کنترل شده باشد به طوری که صرفاً از طریق ابزارهای مشخص و کاملاً تعریف شده امکان ارتباط با شبکه میسر باشد. البته، کنترل دسترسی کاربران به نرم‌افزارهای کاربردی لجستیکی از اولویت بالاتری برخوردار است که باید از قابلیت‌های نرم‌افزاری و مدیریتی شبکه برای این منظور بهره گرفت. گفتنی است برای رسیدن به اهداف فوق معمولاً از یک پایگاه داده امنیتی استفاده می‌شود و اطلاعات کنترلی شبکه توسط مرکز عملیات شبکه در این پایگاه نگهداری و مورد تجزیه و تحلیل

قرار می‌گیرد. نظر به این که شبکه گسترده اختصاصی لجستیک سپاه در آینده نزدیک حاوی اطلاعات و اخبار مهم لجستیکی، داده‌های سیستم‌های کاربردی مأموریتی از قبیل موجودی انبارها، کالاهای سفارش شده، مبدأ و مقصد جابه‌جایی و توزیع کالا و... خواهد شد، لذا محافظت شبکه از دسترسی کاربران غیرمجاز از اهمیت و حساسیت بالایی برخوردار خواهد بود.

مدیریت امنیت هم از لحاظ فنی و هم از جنبهٔ ملاحظات مدیریتی، به مدیریت داده و اطلاعات، مربوط می‌شود. در حقیقت مدیریت امنیت خواهان آن است که دسترسی به شبکه و اطلاعات موجود در آن امن باشد. مراکز مرتبط به هم در شبکه رایانه‌ای لجستیک سپاه، پیام‌ها و داده‌های مختلفی را به یکدیگر منتقل خواهند کرد که در این میان ممکن است یک مزاحم (کاربر غیرمجاز) به طور زیرکانه به تراکنش‌ها دسترسی پیدا کرده و از آنها سوء استفاده نماید و یا به اطلاعات ارسالی و دریافتی اشخاص صدمه وارد کند. در مقوله امنیت ما نیازمند یک سری سیاست‌ها و رویه‌ها هستیم که برای پیشگیری از ایجاد شکاف‌های امنیتی و محافظت شبکه از حمله نفوذگران (Hakers)، تدوین این سیاست‌ها ضروری می‌باشد. معمولاً تهدیدهای متعارف را می‌توان در قالب دسترسی غیرمجاز به منابع یا اطلاعات شبکه، فاش کردن غیرمجاز اطلاعات و تکذیب و انکار سرویس‌ها تعریف نمود.

تکذیب و عدم پذیرش یک سرویس، از حملات معمول به شبکه محسوب می‌شود.

در این حالت شبکه وضعیتی را پیدا می‌کند که نمی‌تواند داده‌های مشروع کاربران را به طور مناسب حمل کند. معمولاً عمل تکذیب و انکار سرویس می‌تواند با حمله به مسیریاب‌ها یا درگیر نمودن شبکه با ترافیک غیرواقعی انجام گیرد.

**۴ـ۴ـ مدیریت کارآیی شبکه**

مرکز عملیات شبکه، برخی از داده‌های شبکه از قبیل داده‌های مربوط به ترافیک، در دسترس‌بودن و تأخیر شبکه را جمع‌آوری کرده و معمولاً بر اساس تاریخ، آنها را مرتب می‌کند و سپس وظایف خود را برای رسیدن به کارآیی بهینه انجام می‌دهد.

داده‌های ترافیک شبکه بر اساس کاربردهای مختلف مانند پست الکترونیکی، اخبار شبکه و صفحات وب قابل جمع‌آوری و دسته‌بندی هستند و در طرحریزی آینده شبکه مورد استفاده قرار می‌گیرند.

با بهبود کارآیی شبکه می‌توان میزان در دسترس و فعال بودن آن را افزایش داد و با تنظیم پارامترهای شبکه می‌توان قابلیت اطمینان و زمان پاسخ شبکه را بهبود بخشید و اصطلاحاً از تأخیر شبکه جلوگیری نمود. بدیهی است حجم بالای داده‌های لجستیکی و توزیع آن در گسترهٔ شبکه وسیع رایانه‌ای در سطح کشور و انبوه کاربران در سطوح مختلف، لزوم مدیریت بهینه کارآیی شبکه اطلاعاتی لجستیک سپاه را اجتناب‌ناپذیر می‌سازد، چرا که شبکه ناکارآ به هیچ وجه نخواهد توانست رضایت کاربران شبکه را به همراه داشته و هزینه‌های صرف شده را توجیه نماید.

**۵ـ دیواره‌های آتش (Fire Walls)**

هدف اصلی از بکارگیری یک دیواره آتش، محافظت شبکه از حملات خارجی است. دیواره آتش می‌تواند ترافیک را برای درون و برون یک شبکه اختصاصی و سرّی کنترل نماید و معمولاً در یک مسیریاب، درگاه (Ports) یا میزبان (Host) ویژه‌ای پیاده‌سازی می‌شود.

سال‌هاست که پیاده‌سازی دیواره آتش انجام می‌گیرد و خطرات ناشی از دسترسی غیرمجاز به سرورهای اصلی از طریق شبکه‌های خارجی را کاهش می‌دهد. این عمل به وسیله فیلترکردن سرویس‌های داخلی آن و اعمال کنترل برای دسترسی به سرویس‌های داخلی شبکه انجام می‌شود. دیواره‌های آتش با کنترل کاربران خارجی، محافظت شبکه از تهدیدهای خارجی را به طور شفاف و متمرکز انجام می‌دهد. برای مثال سرویسی به نام Finger می‌تواند اطلاعاتی را در مورد کارمندان و کاربران یک شبکه اختصاصی در اختیار بیگانگان و کاربران خارجی قرار دهد و می‌توان با فیلتر کردن این سرویس توسط دیواره آتش، از دسترسی کاربران غیرمجاز خارجی به این گونه اطلاعات جلوگیری کرد.

پرواضح است که اعمال سیاست‌های امنیتی درون سازمانی و محافظت از شبکه اطلاعاتی لجستیک سپاه از دسترسی‌های غیرمجاز، نیازمند پیاده‌سازی و بکارگیری دیواره‌های آتش قابل اطمینان می‌باشد و در این راستا، ایمن‌سازی سایت‌ها، شبکه‌های محلی و نقل و انتقال داده در بستر ارتباطات گسترده در سطح کشور از اهمیت ویژه‌ای برخوردار خواهد بود.

**۶ـ نتیجه‌گیری**

طراحی و ایجاد شبکه گسترده اختصاصی رایانه‌ای با توجه به تنوع و گستردگی فعالیت‌های لجستیکی سپاه کاملاً روشن است. این ضرورت را می‌توان در موارد زیر مطرح نمود:

سرویس دهی بهتر به کاربران: یکی از وظایف اولیه سازمان لجستیک سپاه، ارائه خدمات لجستیکی دقیق و به موقع به کاربران می‌باشد. وجود یک شبکه اختصاصی سراسری، تحقق چنین رسالتی را امکان‌پذیر می‌سازد. از طریق این شبکه سراسری، کاربران می‌توانند به آخرین اطلاعات لجستیکی سپاه در سطح کشور دسترسی داشته باشند.

صرفه‌جویی اقتصادی: وجود یک شبکه گسترده اختصاصی و اطلاع‌رسانی، هزینه‌های حمل‌ونقل و توزیع اطلاعات را کاهش می‌دهد. طراحی و ایجاد سیستم جمع‌آوری و توزیع الکترونیکی اطلاعات روی این شبکه گسترده، تحول عظیمی در کاهش هزینه تبادلات ایجاد خواهد نمود.

در طراحی شبکه گسترده اختصاصی باید دقت نمود که اطلاعات درون سایت، وابسته به یک سیستم عامل خاص یا وابسته به یک سخت‌افزار خاصی نباشد. به طور کلی، شبکه رایانه‌ای به عنوان بستر زیرساختی هر گونه ارتباط بین مراکز و واحدهای مختلف حائز اهمیت است. این بحث و نیز موضوع طرح شبکه گسترده اختصاصی لجستیکی سپاه دنیای جدیدی از ارتباطات بین کاربران در مراکز و واحدهای مختلف به وجود می‌آورد. در این زمینه پارامترهای مهمی از قبیل کیفیت، سرعت، پهنای باند و فناوری بکارگیری شده از اهمیت ویژه‌ای برخوردار خواهد شد.

پرواضح است است که سایت شبکه گسترده به عنوان مهم‌ترین قسمت یک شبکه گسترده اختصاصی مطرح می‌باشد که از آن می‌توان به عنوان مغز متفکر و عمل‌کننده سیستم نام برد و چنانچه این مغز درست عمل نکند، کل سیستم فلج خواهد شد. در طرح یک سایت کارا باید قوانین مربوط به گردش اداری و فنی سایت مشخص شود، سپس ابزارهای لازم برای مدیریت سایت، ارتباط آن با شبکه محلی و گسترده، سرورهای مورد نیاز سایت و امنیت آن تعیین گردد.

**پی‌نوشت‌ها**

1- Network Operation Center

2- International Standard Organization

**منبع**

1 -Halsall F., Modiri N;. An Implementation of on OSI NetWork Management System ,in: Network Magazine ,July 1999