# مدیریت شبکه های کامپیوتری
# Network Management

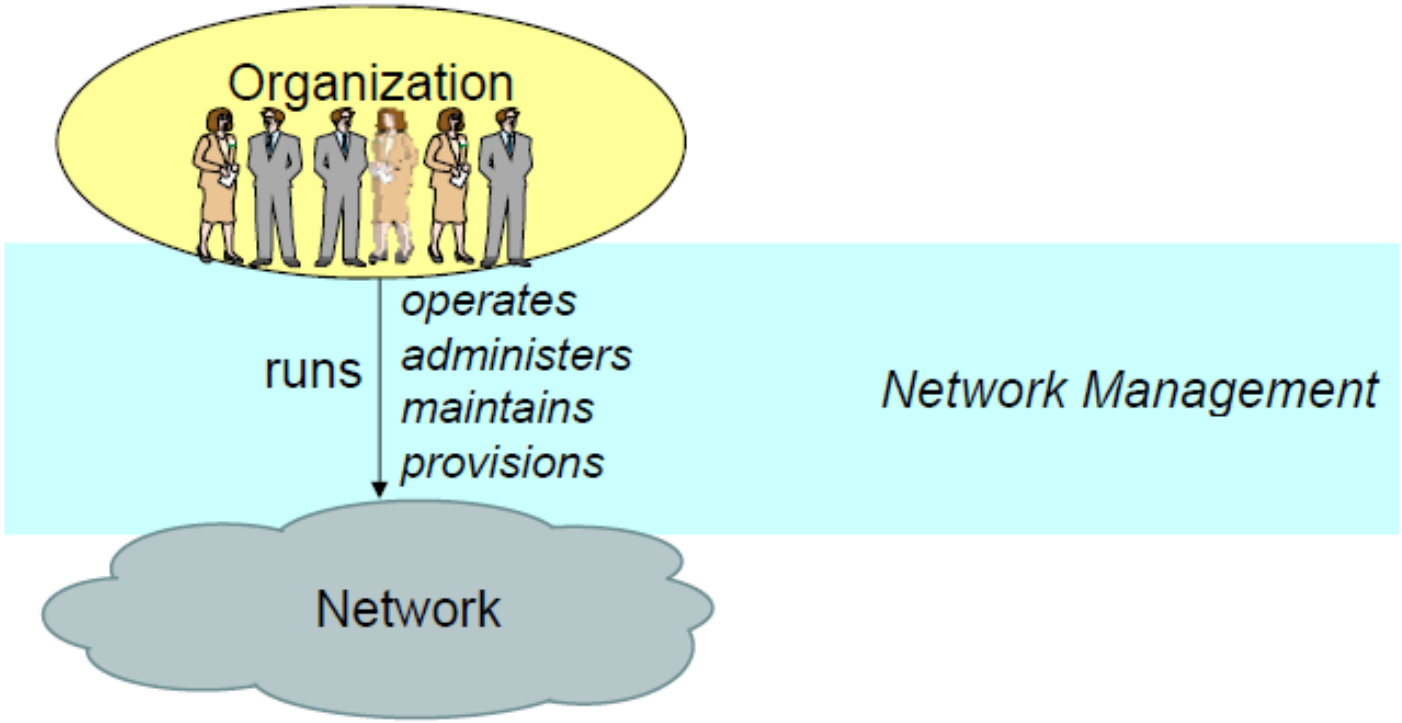
# معیار سلامتی شبکه

استفاده از OAM&P به منظور اطمینان سلامت عملکرد شبکه:

- Operations
  - نگه داشتن شبکه در حالت برقراری پیوسته، مانیتور کردن خطا ها، مشاهده حملات و نفوذ ها و ...
- Administration
  - دنبال کردن عملکرد شبکه، چگونگی استفاده از شبکه و ...
- Maintenance
  - برطرف کردن خطا ها و بروز رسانی های منظم در شبکه
- Provisioning
  - پیکربندی و راه اندازی سرویس مورد نیاز مشتریان

# مدیریت شبکه

- مدیریت شبکه استفاده از فعالیت ها، روش ها، رویه ها و ابزارهایی است که با اندازه گیری و بررسی موارد OAM&P در رابطه است.



# مدل های رایج در مدیریت شبکه

- FCAPS: دسته بندی بر اساس عملکرد
- TMN: دسته بندی لایه ای
- eTOM: دسته بندی بر اساس مدل کسب و کار
- ...

# FCAPS

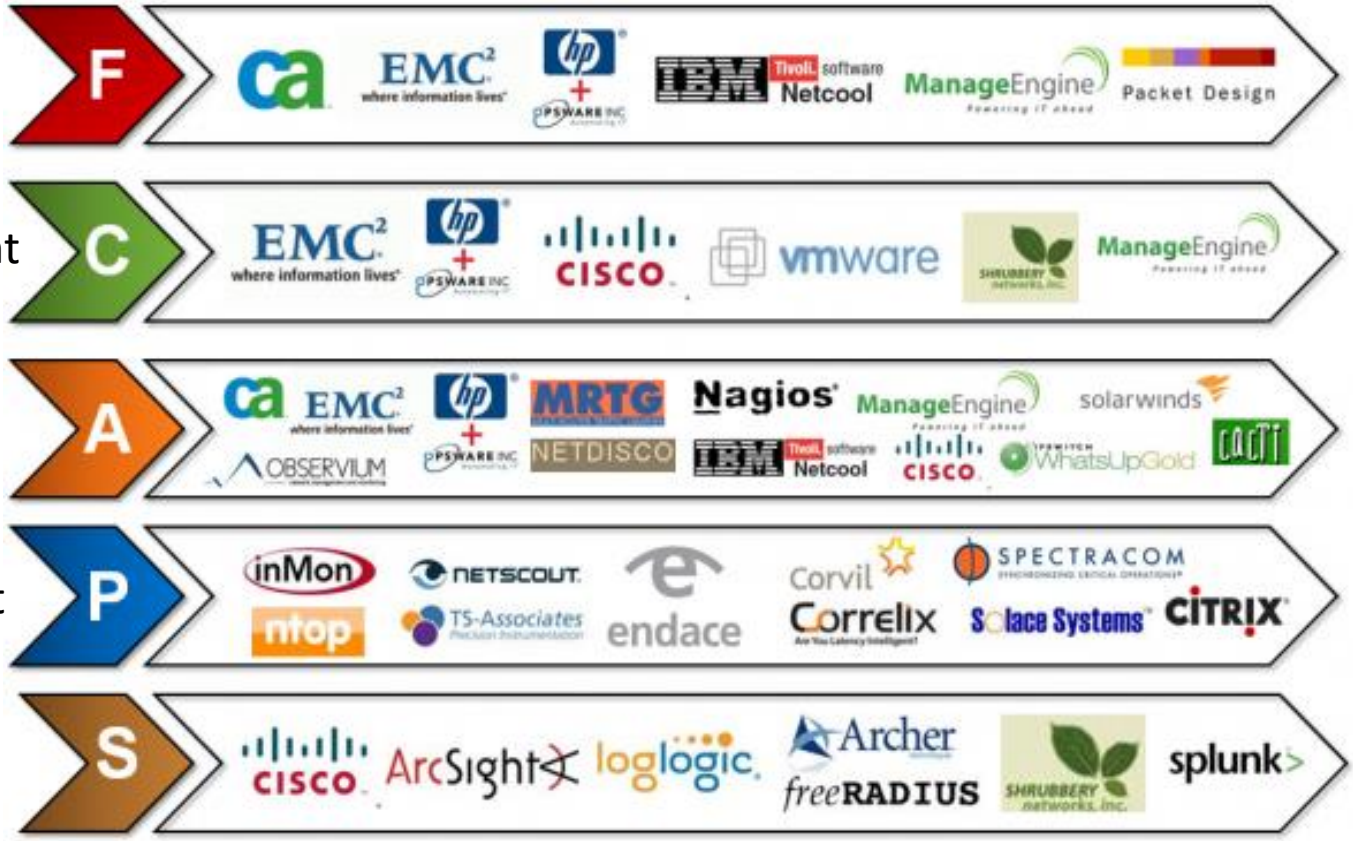
Fault management

Configuration management

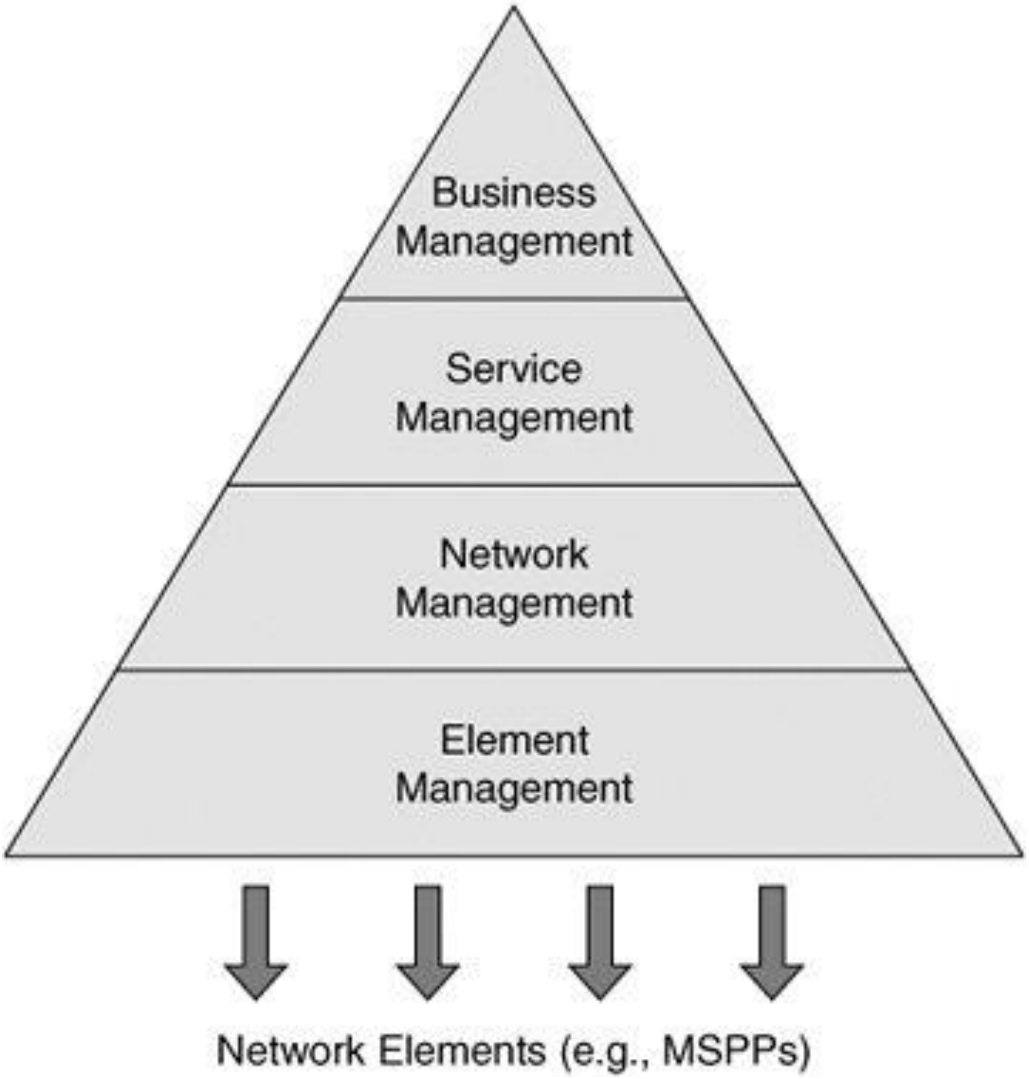
Accounting management

Performance management

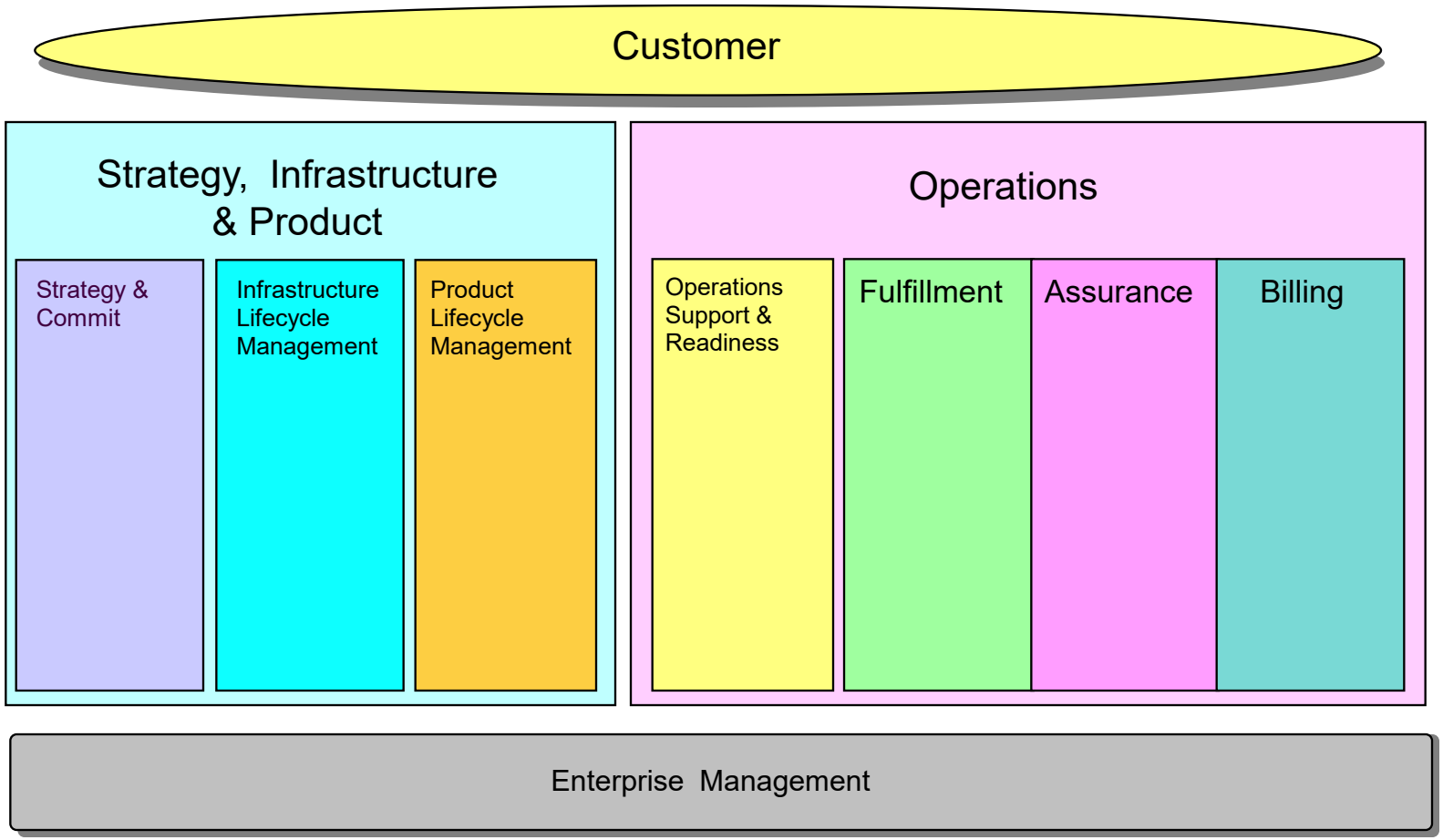
Security management



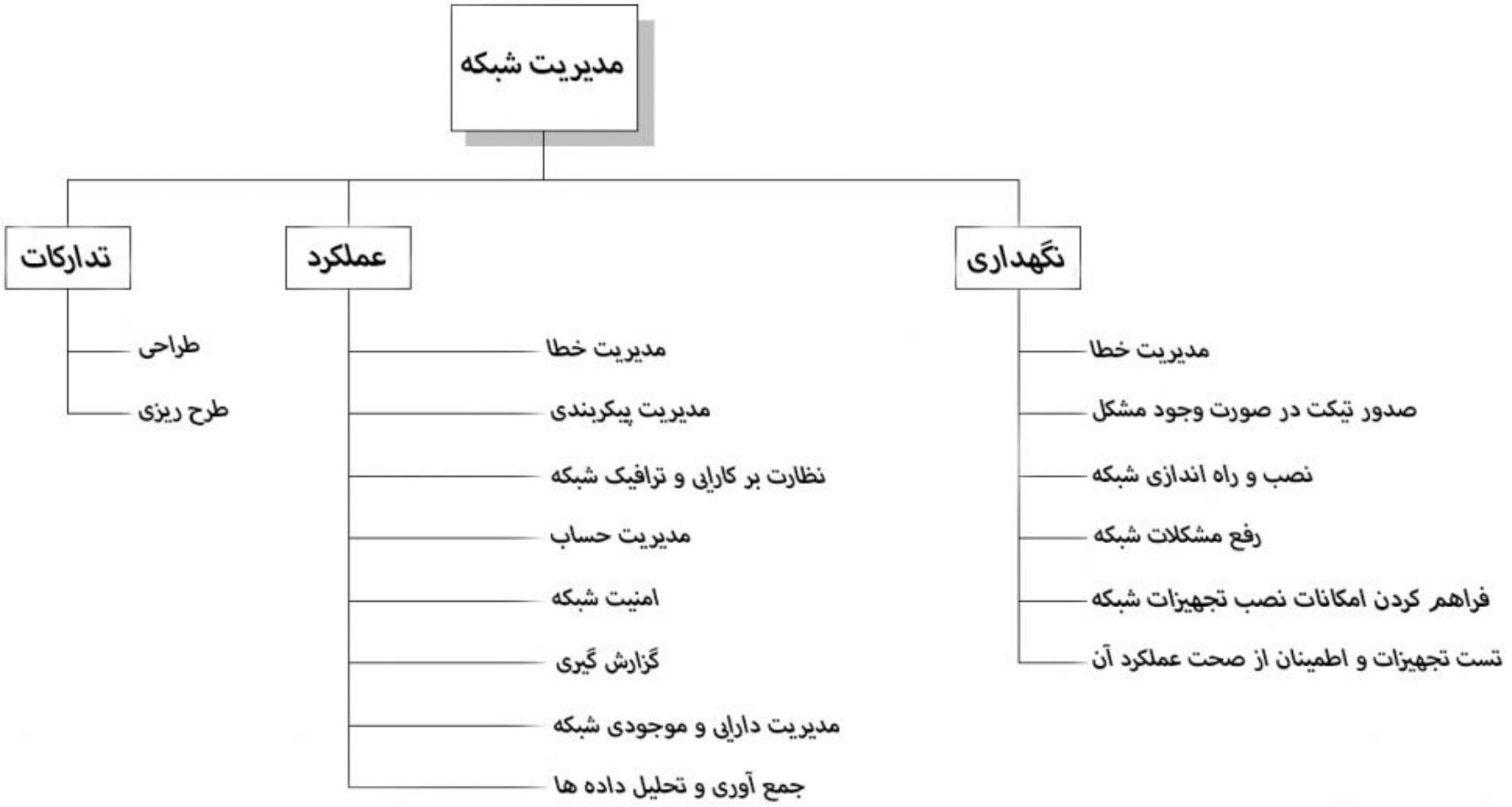
# TMN


Business Management
Service Management
Network Management
Element Management
Network Elements (e.g., MSPPs)

# eTOM


Customer
Strategy, Infrastructure & Product
Strategy & Commit
Infrastructure Lifecycle Management
Product Lifecycle Management
Operations
Operations Support & Readiness
Fulfillment
Assurance
Billing
Enterprise Management

# وظایف مدیریت شبکه



# اهمیت مدیریت شبکه

- **Loss of Connectivity:** قطعی شبکه
- **Duplicate IP Address:** تکراری شدن آدرس IP
- **Intermittent Problems:** برخی مشکلات در طول حیات شبکه به صورت خود به خود بروز کرده و همیشگی نیستند، متناوبا رخ داده و بعد از مدتی نیز به صورت خود به خود رفع می شوند، دلیل این گونه مشکلات مشخص نیست که از آنها با عنوان Intermittent problemsیاد می شود و معنای لغوی آن " اتفاقی است که تکرار می شود" می باشد.
- **Non-Problems:** در مقابل مشکلاتی که در بالا ذکر شد نیز مسائلی وجود دارند که یک بار رخ داده و به صورت خود به خود نیز رفع می شوند ولی هیچ کس متوجه علت آن ها نمی شود.
- **Network Configuration Issue:** مشکلات و مسائلی که بواسطه پیکربندی اشتباه در شبکه رخ داده و به وجود می آیند.
- **Performance Problems:** مشکلات کارایی شبکه، مانند کند بودن شبکه و نارضایتی کاربران شبکه

# سطوح مدیریت شبکه های کامپیوتری

- **مدیریت کسب و کار Business Management**

بالاترین لایه از سطوح مدیریتی است. در این لایه به سراغ سرویس های جدیدی که ارائه شده می رویم و یا اینکه سرویس های قدیمی را از مدار خارج می کنیم. امور مربوط به سرویس دهی کابران از طریق شبکه در این لایه صورت می گیرد.

- **مدیریت سرویس Service Management**

هدف از راه اندازی شبکه، ارائه سرویس به مشتریان است. در لایه های پایین تر با مانیتور کردن وضعیت شبکه سعی داریم از صحت کارکرد آن ها اطمینان حاصل کنیم. به طور مثال، المان ها با چه مشکلات و خطاهایی رو به رو می باشند. همچنین در این لایه به این مسأله می پردازیم که سرویس دهی به مشتریان در چه زمانی و به کدام مشتری باید صورت پذیرد و یا اینکه این سرویس را چه زمانی از مشتری بگیریم. تمامی این موارد در لایه Service Management انجام می گیرد.

# سطوح مدیریت شبکه های کامپیوتری(ادامه)

- **مدیریت شبکه Network Management**

منظور مدیریت شبکه ای با المان های متفاوت می باشد که می تواند از Vendorهای متفاوت باشد.

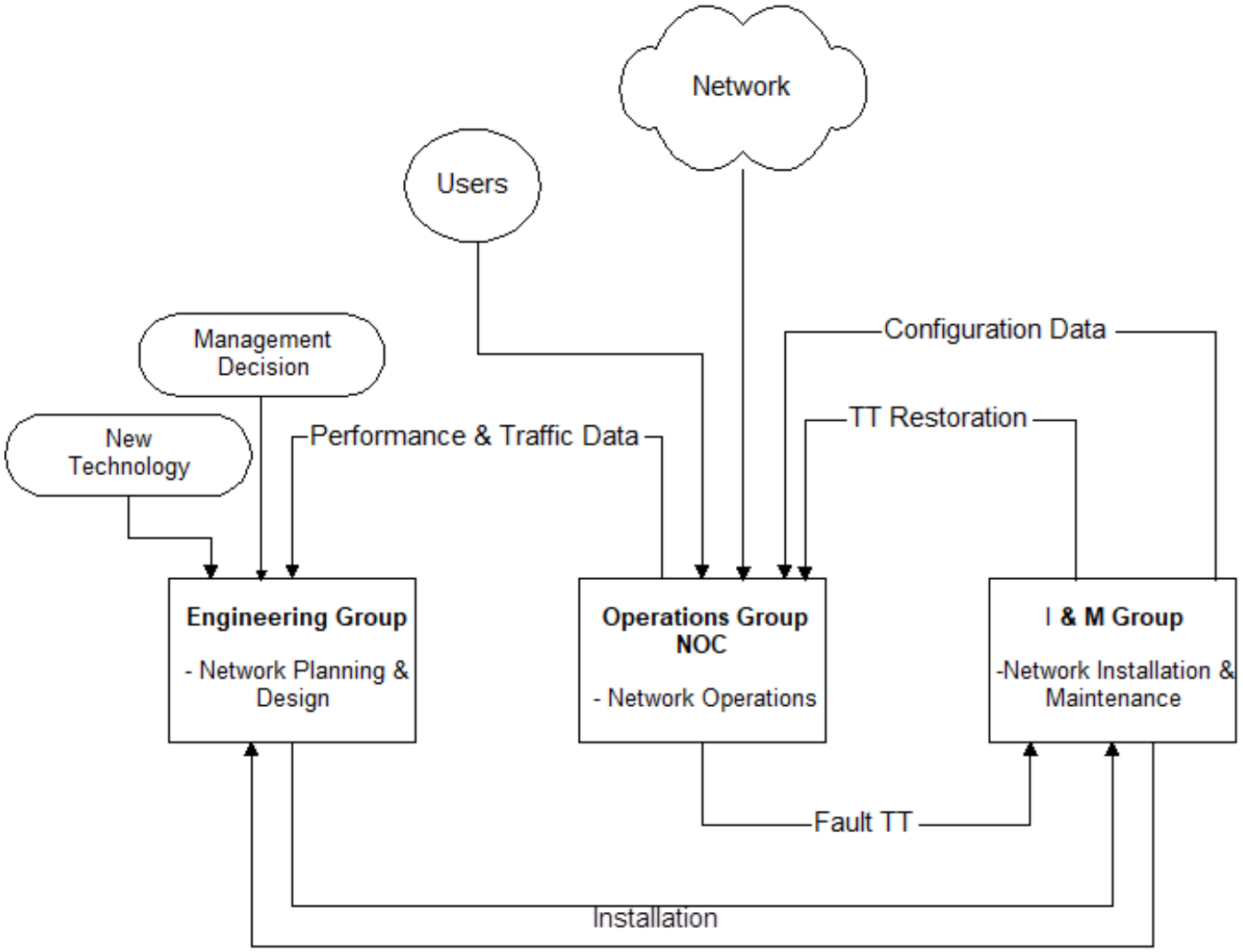
- **مدیریت المان Element Management**

این سطح پایین ترین لایه مدیریت است. در این لایه با یک نوع المان و یا با تعدادی از المان های همسان کار می کنیم که می خواهیم آن ها را مدیریت کنیم. به عنوان مثال المان ها، روتر Cisco3700می باشند.

- **المان شبکه مدیریت شده Managed Network Element**

این لایه جزء سطوح مدیریت نیست. در واقع در اینجا می خواهیم از المانی که در شبکه ی خود داریم اطلاعات گرفته و وضعیت آن را مانیتور کنیم. مانند یک نرم افزار و یا حتی یک Virtual LAN

# عملکرد مدیریت شبکه های کامپیوتری



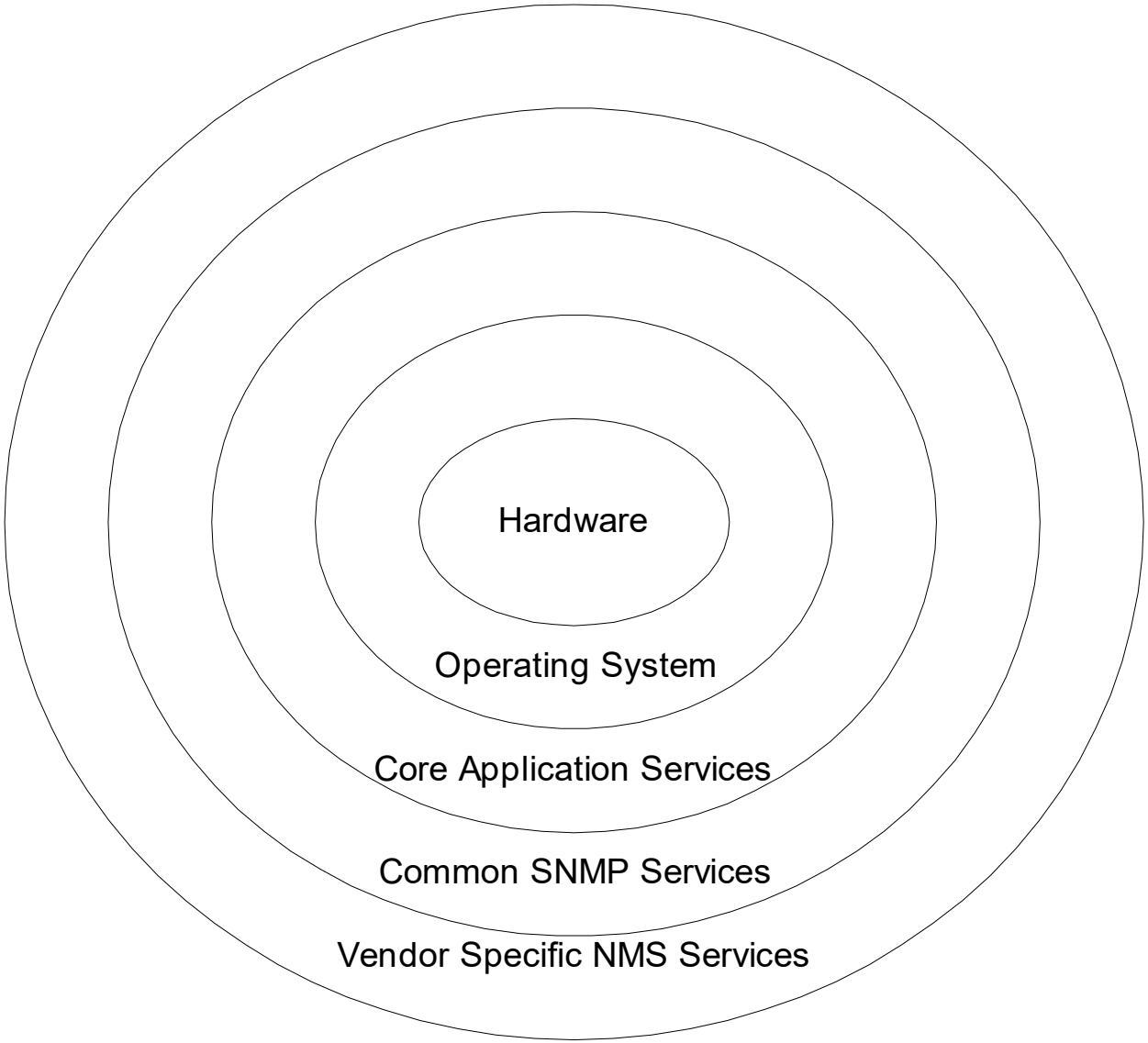
# مدیریت شبکه بصورت موثر

- تهیه یک لسیت موجودی از مهم‌ترین تجهیزات شبکه
- ایجاد تغییر در فرایند کنترل خود تغییر
- آگاهی از استانداردهای انطباق
- نقشه های همراه با آیکون های وضعیت
- توجه به وابستگی‌ها
- راه‌اندازی سیستم هشدار
- تصمیم در مورد استانداردها و سیستم امنیتی دریافت اطلاعات شبکه
- به دنبال گرفتن اطلاعات تکمیلی از همه سیستم‌های مهم و برنامه‌ها
- فراموش نکردن محدوده شبکه
- تعریف سیستم یا فرآیندی برای پیگیری فعالیت های کاربران و تجهیزات شبکه

# نیازمندیهای اساسی در طراحی سیستم مدیریت شبکه

- مقیاس پذیری
- پاسخ دهی بلادرنگ
- پردازش دسته ای
- تنوع کاربران
- سادگی در استفاده
- مدیریت داده ها
- مدیریت محلی و از راه دور
- گستره جغرافیایی
- ناهمگونی
- بار انفجاری
- امنیت

# اجزای سیستم مدیریت شبکه های کامپیوتری



# اجزای سیستم مدیریت شبکه های کامپیوتری (ادامه)

| اجزاء | سرویس | نمونه |
|---|---|---|
| سخت افزار | Processor<br>Monitor<br>Mouse and Keyboard<br>Communications | Sun Sparc<br>HP 9000<br>PC |
| سیستم عامل | OS services | UNIX<br>LINUX / FreeBSD<br>Solaris<br>MS Windows 95 / 98 / NT |
| سرویس های برنامه های اصلی | Display<br>GUI<br>Database<br>Report generation<br>Communication services | OpenView<br>SunNet Manager<br>Solstice Enterprise Manager<br>MS Windows |
| سرویس های متداول SNMP | SNMPv1 messages<br>SNMPv2 messages<br>MIB management<br>Basic SNMP applications<br>3rd party NMS API | SNMPc<br>OpenView Network Node Manager<br>Cabletron Spectrum Enterprise Manager<br>IBM NetView<br>SunNet Manager<br>Solstice Enterprise Manager |
| سرویس های ویژه ی یک سازنده | MIB management<br>SNMP applications<br>Config. management<br>Physical entity display | CiscoWorks<br>Transcend<br>Spectrum Element Manager / Spectrum<br>Portable Management Application |

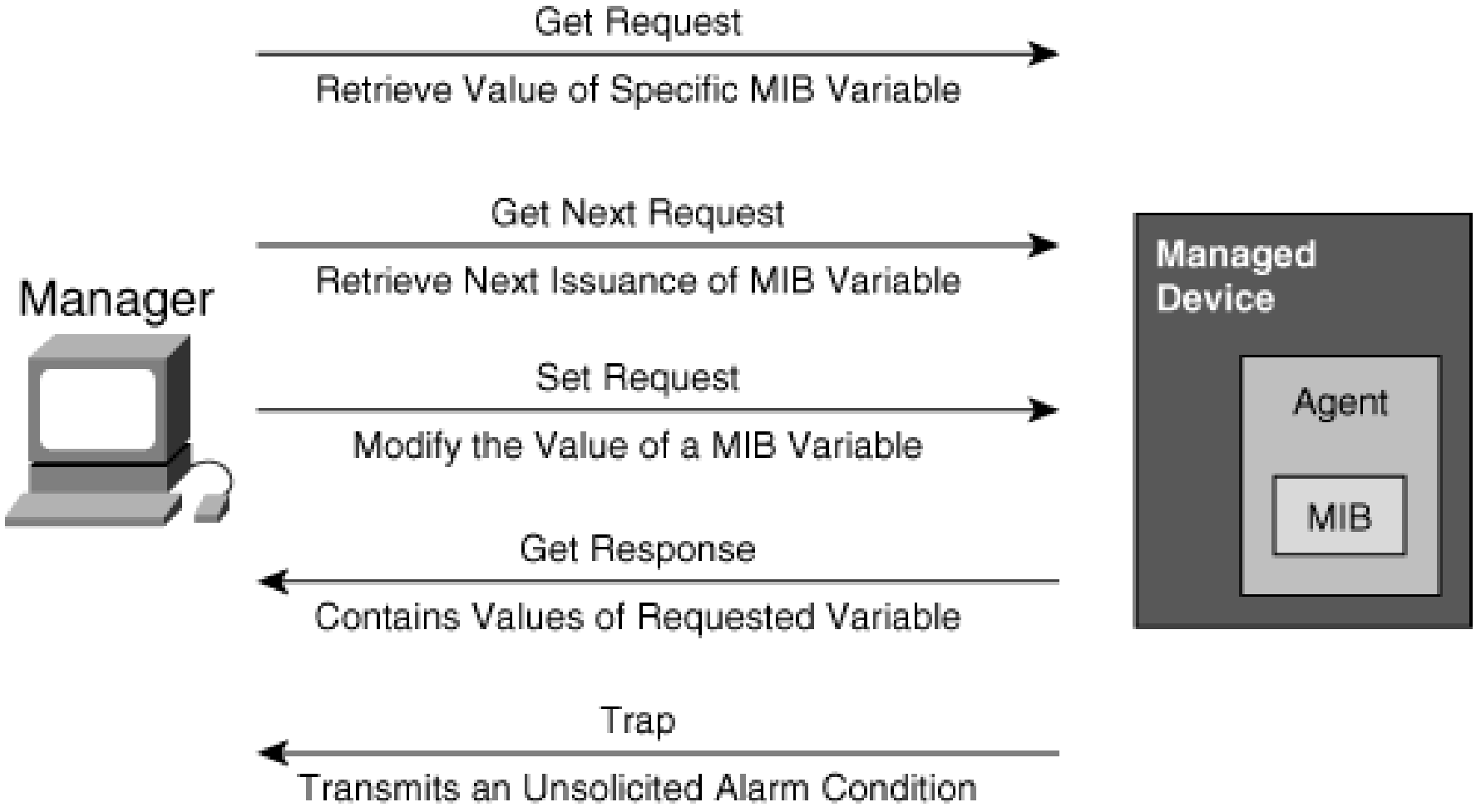
# پروتکل های مدیریت شبکه های کامپیوتری

- SNMP
- MIB
- RMON
- …

# SNMP

- SNMPv1
- SNMPv2
- SNMPv3

# SNMP


Get Request
Retrieve Value of Specific MIB Variable
Get Next Request
Retrieve Next Issuance of MIB Variable
Manager
Set Request
Modify the Value of a MIB Variable
Managed Device
Agent
MIB
Get Response
Contains Values of Requested Variable
Trap
Transmits an Unsolicited Alarm Condition

# SNMP

در شبکه های کامپیوتری که ترکیبی از روترها، سوییچ ها و سرورها هستند، به منظور مدیریت همه ابزارها در شبکه باید کاری انجام شود تا از کارکرد بهینه آنها آگاه شد. اینجاست کهSNMP، پروتکل ساده مدیریت شبکه، می تواند کمک کند.

این پروتکل در سال ۱۹۸۸ معرفی شد تا احتیاجات رشد یافته ای را در یک پروتکل به منظور مدیریت ابزارهایی که بر پایه پروتکل TCP/IPکار می کنند، اعمال کند. هسته اصلی SNMPمجموعه ساده ای از اعمال است که به Administratorها توانایی تغییر در محدوده ابزارهایی که بر پایه این پروتکل کار می کنند را فراهم می‌کند. همچنین امکان اداره کردن، بازبینی و پشتیبانی از شبکه های کامپیوتری دور یا محلی که بر اساس TCP/IPکار می کنند، میسر می شود و در واقع راهی استاندارد به منظور یافتن اطلاعات شبکه ای است.

در مقایسه با SGMPکه تنها برای مدیریت روترهای اینترنت ایجاد شد، SNMPبرای مدیریت Unix ،Windows، پرینترها و غیره به کار می رود. مانیتور کردن شبکه به منظور درک بهتر چگونگی کارکرد شبکه، از دیگر عملکردهای مدیریت شبکه است. در این پروتکل، دو عنصر ارتباطی به نام های عامل ها و مدیران وجود دارند. عامل، اطلاعات شبکه ای را برای برنامه مدیر که روی کامپیوتر دیگر در حال اجراست، تولید می کند. مدیر، یک راه انداز سرور است که بعضی از انواع نرم افزارهای سیستمی که وظایف مدیریتی شبکه را بر عهده دارند، اجرا می کنند. مدیران اغلب با عنوان NMSشناخته می شوند. وظیفه یک NMS، سرشماری و دریافت Trapاز یک عامل در شبکه می باشد. Trapراهی است که یک عامل از طریق آن وقوع چیزی را به NMSخبر می‌دهد.

# SNMP

مدیران و عامل ها از MIBها به صورت مشترک استفاده می کنند که همانند یک پایگاه داده است و متشکل از هر نوع اطلاعات آماری از deviceهای مدیریت شده می باشد و این اطلاعات را به صورت ساختار درختی نمایش می دهد. گروه IETF، پروتکل SNMPرا به عنوان پروتکل استانداردی برای کنترل ترافیک اینترنت معرفی کرده است. همچنین RFCهایی مخصوص پروتکل های موجود در محدوده‌ی پروتکل IPمنتشر کرده است. پروتکل SNMPدر سه نسخه ارائه شده است که اولین نسخه از آن در RFC1157معرفی شده است. امنیت در این نسخه از پروتکل، پایین است و با کلمه عبور می توان با آن ارتباط برقرار کرد. در کل سه نوع ارتباط رشته ای در SNMPv1 وجود داردکه عبارتند از:

Read-only

Write-only

Trap

SNMPv2 بر پایه ارتباط رشته ای کار می کند که از لحاظ فنی SNMPv2cنامیده می شود و در RFC3416، RFC3417و RFC3418معرفی شده است. SNMPv3 آخرین نسخه از SNMP است که مزیت اصلی آن نسبت به نسخ قبلی، در مدیریت شبکه و امنیت است و پشتیبانی هایی به منظور خصوصی کردن ارتباط ها بین موجودیت های مدیریت شده، اضافه می کند. به طور کلی این نسخه از SNMP تحولی از استانداردهای اولیه به استانداردهای نهایی ایجاد کرده است.

# SNMP

با توجه به اینکه SNMPv3یک استاندارد کامل است، ولی تولیدکنندگان به سختی نسخه جدیدی از یک پروتکل را قبول می کنند و اکثر اعمال تولیدکنندگان SNMPبر طبق SNMPv1صورت میگیرد. SNMPv1وSNMPv2از مفاهیم ارتباط های رشته ای به منظور برقراری اطمینان بین مدیران و عامل ها استفاده می کنند. ارتباط های رشته ای که پیشتر نام برده شد، لزوماً کلمه عبور هستند که هر کدام از آنها فعالیت های مختلفی را کنترل می کنند. در ارتباط رشته ای read-only، همانطور که از نام آن مشخص است، امکان خواندن داده را به شما می‌دهد و هر گونه تغییر یا اصلاح در آن غیر ممکن است. به عنوان مثال شما قادر خواهید بود تعداد بسته هایی که به پورت های روتر شما فرستاده می شود را بخوانید، اما صفر کردن شمارنده را غیر ممکن می سازد. ارتباط رشته ایread-write، امکان خواندن و تغییر مقادیر را می دهد. با این ارتباط شما می توانید شمارنده ها را بخوانید، مقادیر آنها را صفر کنید و همچنین واسط ها را صفر کنید یا کارهایی در جهت تغییر تنظیمات روتر انجام دهیم.

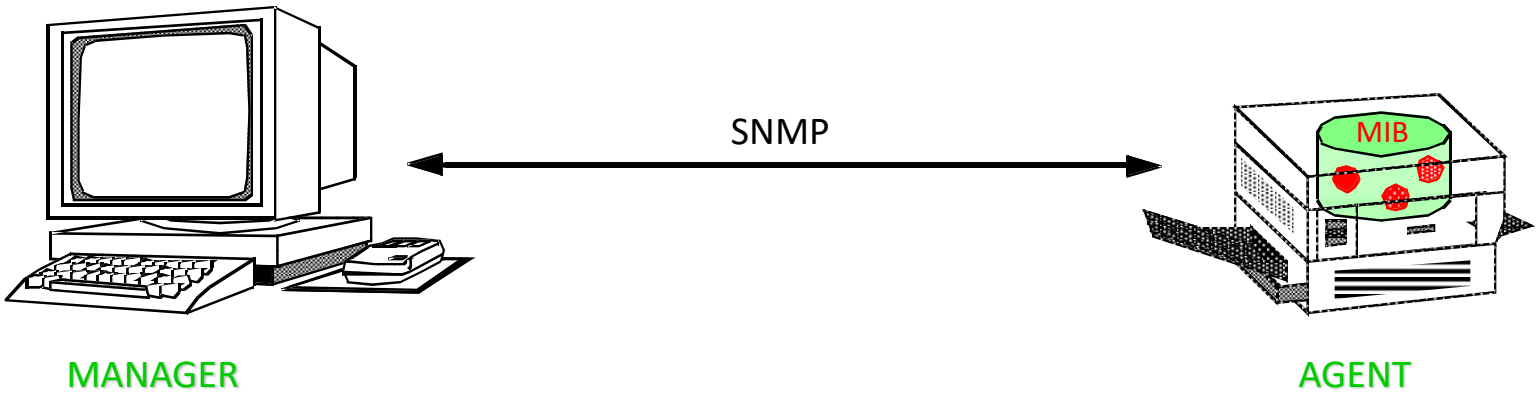
سرانجام ارتباط رشته ای trapامکان دریافت رشته ها از جمله اخطارهای غیر همزمان از عامل را فراهم می کند. بیشتر فروشندگان، تجهیزات خود را با ارتباط رشته ای پیش فرض می فرستند. به طور نمونه از publicبرای ارتباط رشته ای read-onlyو privateبرای ارتباط رشته ای read-writeاستفاده می شود. تغییر این پیش فرض ها پیش از اینکه دستگاه روی شبکه قرار گیرد، مهم است. زمانیکه یک عامل SNMPرا نصب می کنید، مقصد رشته ی آن را تنظیم می کنید. از آن پس هر رشته ای که آن عامل تولید می کند، به این آدرس فرستاده می شود.

برای تفسیر اطلاعاتی که بین مدیر و عامل ردوبدل می شود، اجزا دیگری نیز مورد نیاز است. این اجزا MIBو OID می باشند.

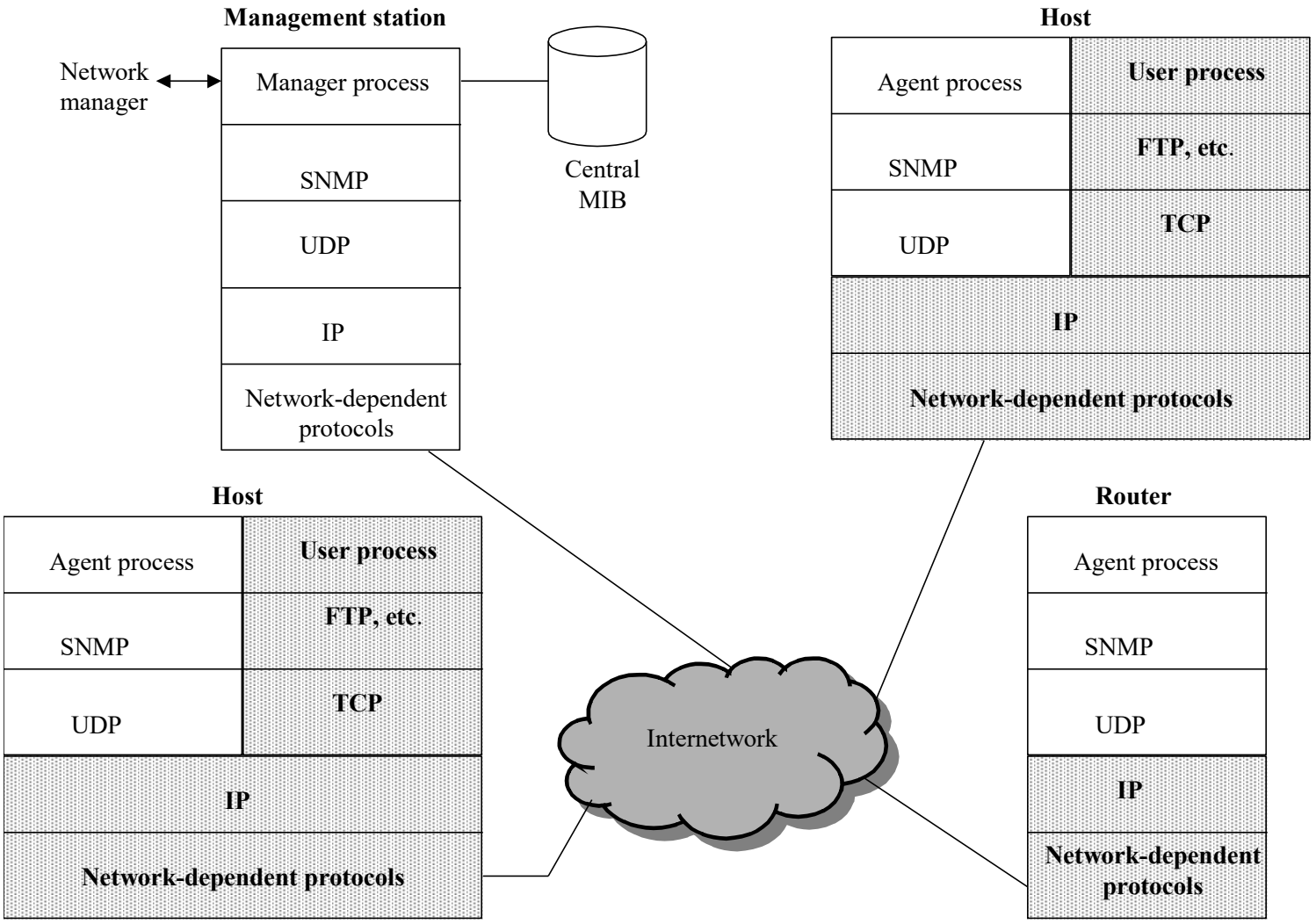
یک MIBدر واقع مخزنی شامل تعاریف شاخص ها و مولفه هایی است که عامل پشتیبانی می کند و توسط پرتکل SNMPقابل دریافت و اندازه گیری می باشد. در MIBموضوعاتی که امکان دریافت اطلاعات آنها وجود دارد معرفی می گردد. هر MIBشامل مجموعه ای OIDها می باشد.

# SNMP

- Manager: به عنوان مدیر و جمع کننده رخداد ها در رابطه SNMP
- Agent: به عنوان بخش های تحت نظارت قرار گرفته



# معماری SNMP


Management station
Network manager
Manager process
SNMP
UDP
IP
Network-dependent protocols
Central MIB
Host
Agent process
User process
SNMP
FTP, etc.
UDP
TCP
IP
Network-dependent protocols
Host
Agent process
User process
SNMP
FTP, etc.
UDP
TCP
IP
Network-dependent protocols
Internetwork
Router
Agent process
SNMP
UDP
IP
Network-dependent protocols

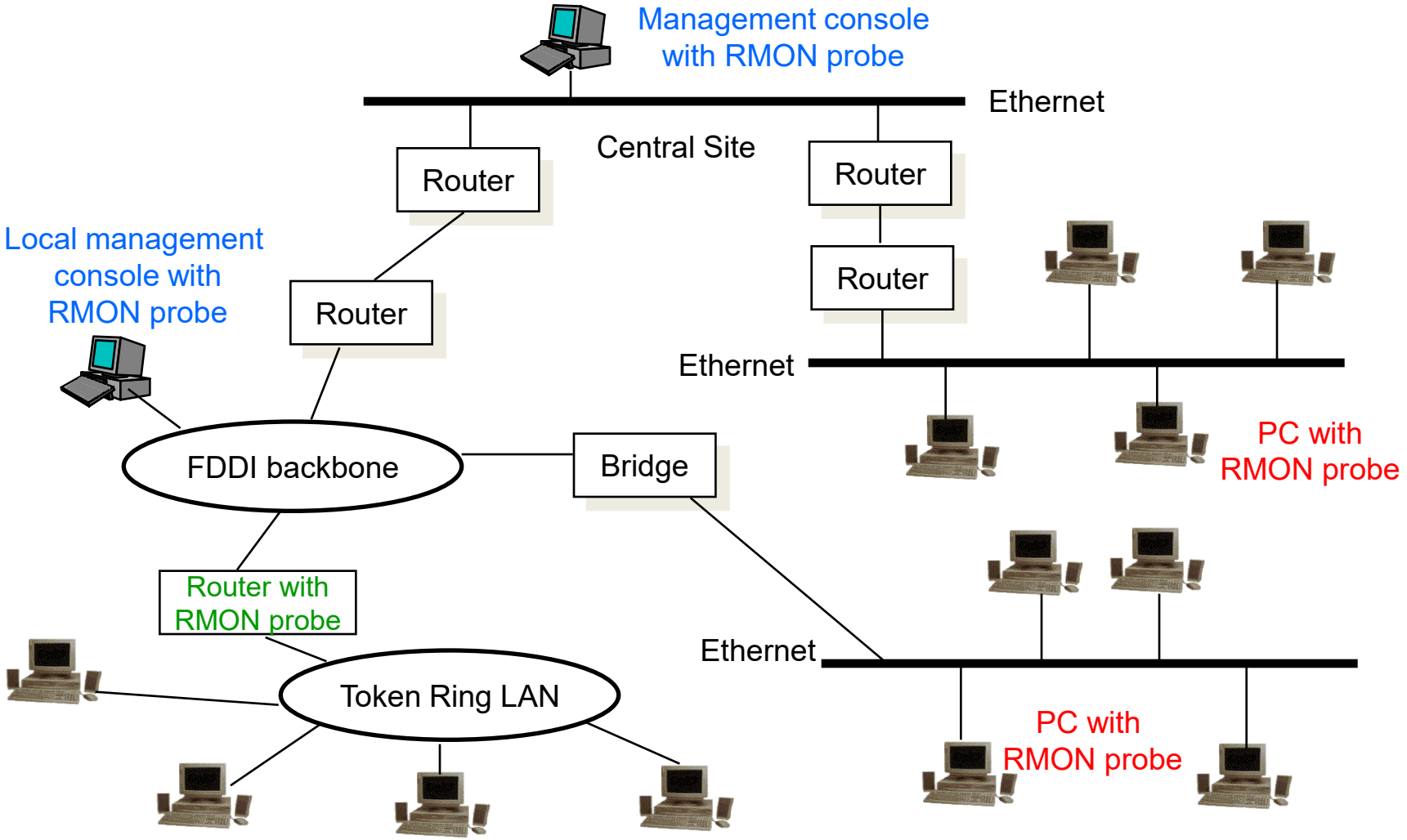
# RMON

RMON یکی از راهکار های Network Monitoring بسیار کاربردی در شبکه های Ciscoاست. در تعریف ، RMON مجموعه ای متشکل از متغیر های مبتنی بر MIBهای استاندارد شده است که شبکه را مانیتور می کند. البته نکته بسیار مهم اینست که تکنولوژی RMON صرفا متعلق به شرکت Cisco نمی باشد و در حال حاضر یک استاندارد است که در IETF شکل گرفته و هدف از ایجاد آن remote monitoringبر اساس RMON MIB می باشد.

چهار مجموعه مختلف از MIBهای استاندارد شده توسط IETF برای استفاده از RMON تاکنون ایجاد شده است:

- RMON 1وRMON2 که شامل remote monitoring با MIBهای نسخه ۱ و ۲ می باشد.
- DSMON که remote monitoringدر مقوله Differentiated Services را شامل می شود.
- SMON که Remote Monioring در شبکه های Switched را پوشش می دهد.
- APM که کابرد آن سنجش کیفیت در سطح Application است.

# شبکه تحت RMON



# مانیتورینگ شبکه های کامپیوتری

مانیتورینگ شبکه های کامپیوتری که معنای لغوی آن نظارت و یا پایش شبکه های کامپیوتری است، در واقع، رصد سیستمهای شبکه در جهت تشخیص هر گونه خرابی به وجود آمده در شبکه، ناشی از نقص در سرورها، سرویسها و یا قطع اتصالات می باشد. سرور و یا سایت شما ممکن است در هر لحظه وضعیت های متفاوتی داشته باشد. فعالیت مانیتورینگ را می توان چشم همیشه بیدار مدیر شبکه نامید. همچنانکه مدیریت خوب، بدون در اختیار داشتن اطلاعات ناب و امکانات پردازشی مناسب میسر نیست، نظارت شبکه های کامپیوتری نیز بدون رصد کردن وضعیت سرویسها امری بسیار پرمخاطره و هزینه بر است. بصورت کلی شما می توانید با داشتن یک سیستم مانیتورینگ قوی در سازمان خود از تمامی اتفاقاتی که در شبکه چه از لحاظ نرم افزاری و چه از لحاظ سخت افزاری رخ می دهد آگاه شوید.

# اهمیت مانیتورینگ شبکه های کامپیوتری

- **بهبود امنیت شبکه**

دلیل اصلی توسعه برنامه های مانیتورینگ شبکه های کامپیوتری ، حفظ داده های حیاتی سازمان هاست. طبق مطالعات انجام شده در سال ۲۰۱۶ توسط موسسه فونمن در حوزه هزینه ناشی از نقص داده ها ( منظور داده های محرمانه ای است که توسط افراد غیر مجاز به سرقت می رود)، میانگین هزینه ی نقص داده ها به ۴ میلیون دلار می رسد.

بدون در نظر گرفتن وسعت کسب و کار، داده ها نیازمند حفاظت و نگهداری می باشند. سیستم های مانیتورینگ شبکه، اطلاعات مهمی از ترافیک شبکه را در اختیار شما قرار می دهند. با نظارت بر ترافیک شبکه قادر خواهید بود تا ترافیک های مشکوک را در شبکه شناسایی کنید. به عنوان مثال، شماره پورت ۴۴۳ در ارتباطات امن مرورگرهای از اهمیت بالایی برخوردار است، مانند انتقال وجه در برخی وب سایت های تجاری، واضح است که داده ها باید هم در سمت مشتری و یا فرستنده و هم در سمت گیرنده حفاظت شوند. در نتیجه مانیتورینگ به شما در شناسایی هر گونه مسئله امنیتی مرتبط با ارسال بسته های داده بر روی این پورت ها کمک خواهد کرد.

- **بازیابی داده ها به هنگام وقوع حوادث طبیعی**

سازمان های فناوری اطلاعات باید برنامه و طرحی برای بازیابی داده های خود به هنگام وقوع حوادثی مانند سیل و زلزله و ... داشته باشند تا بتوانند داده های خود را بازیابی کنند.

# اهمیت مانیتورینگ شبکه های کامپیوتری(ادامه)

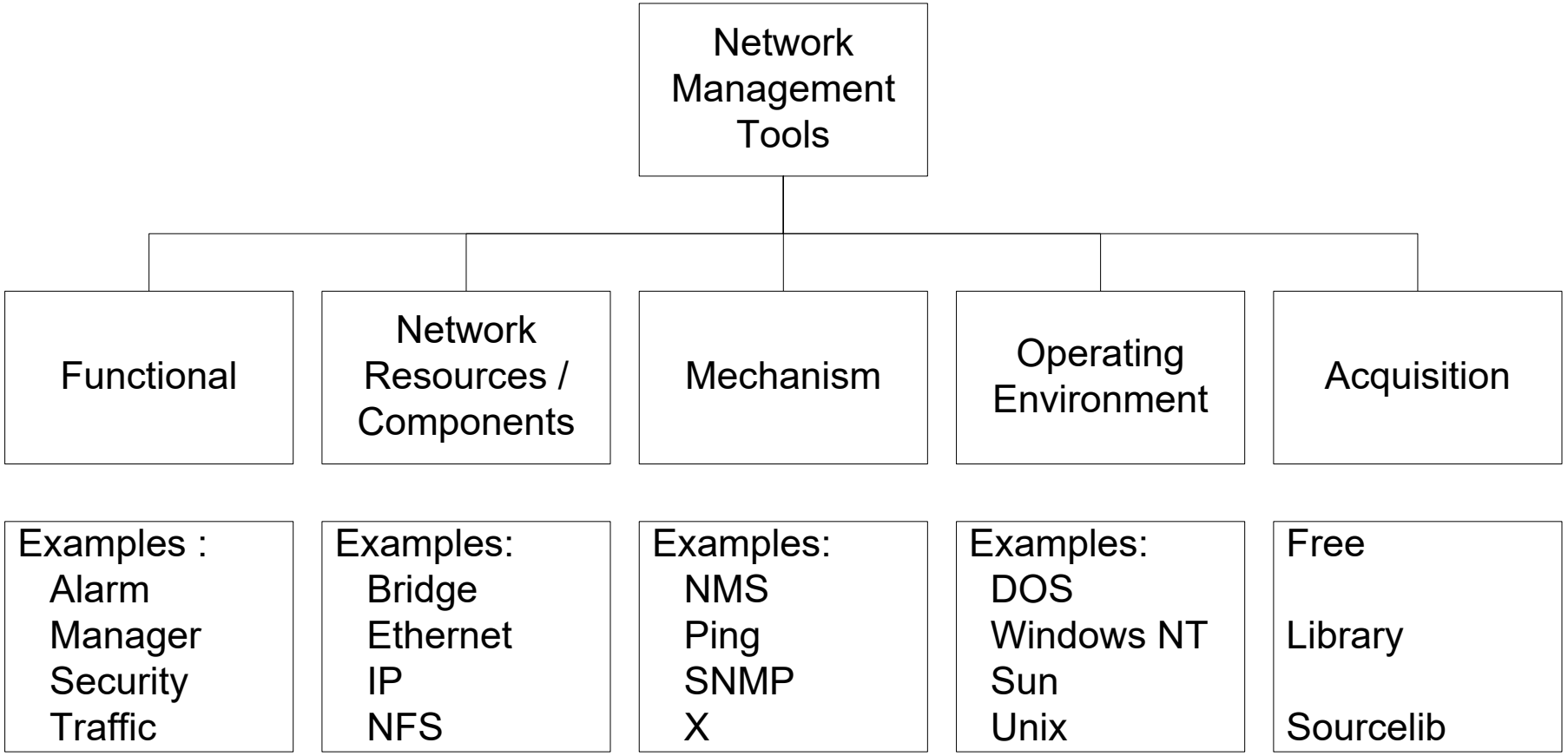
- **شناسایی مخرب ها و تهدیدات امنیتی**

گاهی اوقات در شبکه هایی که داده های پویا و فرار در حال انتقال می باشند (Network Forensic)، با نگاه کردن به نمودارها و الگوهای مانیتورینگ می توان تهدیدات امنیتی را شناسایی کرد. تحقیقات انجام شده نشان می دهد که بسیاری از متخصصان فناوری اطلاعات از راهکارهای Network Forensic برای شناسایی تهدیدات امنیتی خود استفاده می کنند. هنگامی که مشکلات شبکه در ساعات اوج آن اتفاق می افتد، شناسایی مخرب ها، امری دشوار است، سیستم های مانیتورینگ با دنبال کردن Logها مانند Road mapها در تشخیص مخرب های اصلی به ما کمک خواهند کرد.

- **پیکربندی شبکه و برنامه های آتی شبکه**

بسیاری از مشکلات شبکه به هنگام راه اندازی و پیکربندی آن اتفاق می افتد. به عنوان مثال، اگر به هنگام تخصیص شماره IPبه گذرگاه روتر و دستگاه های مسیریابی ، خطایی رخ دهد، بسته های داده ممکن است به مقصد نرسند و یا از مسیر اشتباه عبور کنند. مانیتورینگ شبکه می تواند در زمان هایی که IPهای یکسان به رابط ها در شبکه اختصاص داده اید، با مقایسه مک آدرس مربوط به شماره IPدر روتر، مشکل را شناسایی کند. همچنین سیستم های مانیتورینگ در برنامه های آتی به سازمان ها کمک خواهند تا اگر بخواهند شبکه ی خود را توسعه دهند، منابع خود را راحت تر به روز رسانی کنند و همچنین گلوگاه (Bottleneck) را در شبکه شناسایی کنند.

# ابزار های مدیریت شبکه های کامپیوتری



# تعریف مرکز عملیات شبکه

در یک تعریف مختصر و مفید مرکز عملیات شبکه (Network Operations Center) عبارتست از محلی که مانیتورینگ و مدیریت شبکه‌های کامپیوتری در آن انجام می‌گردد. اگر بخواهیم نگاهی گذرا به تاریخچه آن داشته باشیم، شاید این‌طور باشد که قدیمی‌ترین NOC پیاده سازی شده مربوط به شرکت AT&T در نیویورک می‌باشد که در سال ۱۹۶۲ بازگشایی گردید، البته انتظار نمی‌رفت که NOC راه اندازی شده، قابلیت‌های مانیتورینگ متنوع و متعدد امروزی را در خود داشته باشد اما به هر حال در زمان خود، فکر و نیازی بود که شناسایی شد و مدیریت با ورود نخستین کامپیوترها به عرصه اقتصاد و ساختار اداری و راه اندازی شبکه، تصمیم به پیاده سازی آن گرفت.

# ضرورت راه اندازی مرکز عملیات شبکه

- مانیتور و رصد قسمت‌های مختلف شبکه نظیر سویچ‌ها، پرینترها، سرورها، روترها و ... و رفع مشکلات پیش آمده در کمترین زمان و با کمترین هزینه، همواره مورد نیاز مدیران شبکه (به خصوص شبکه‌های بزرگ) بوده است و این نکته یکی از مهم‌ترین فاکتورهای کلیدی در افزایش و اندازه‌گیری سطح کیفیت سرویس‌های موجود در دیتاسنترها و شبکه‌های کامپیوتری می‌باشد.
- افزایش گسترده شبکه‌های رایانه‌ای و متعاقباً افزایش تعداد تجهیزات سخت افزاری و نرم افزاری و خدمات متنوع شبکه، نیاز به این مراکز را افزایش داده است.
- اطمینان از عملکرد صحیح و پایداری، فعال بودن و سرویس‌دهی منابع و سرویس‌های اطلاعاتی بر اساس SLAهای موجود سازمان.

# اهداف راه اندازی مرکز عملیات شبکه

- پایداری خدمات IT ارائه شده در بستر شبکه
- افزایش سرعت در ارائه خدمات IT
- بهینه‌سازی فرآیندهای IT
- کاهش هزینه ها
- ایجاد ساختار در زیر ساخت شبکه
- بهره‌وری مناسب از منابع سخت افراری و نرم افراری موجود

# وظایف مرکز عملیات شبکه

- شناسایی نقاط آسیب‌پذیر شبکه
- شناسایی به موقع ایرادات سخت افزاری و یا نرم افزاری شبکه
- مانیتورینگ آنلاین ترافیک شبکه و رصد ۲۴ ساعته جهت شناسایی رویدادها یا شرایط خاص در شبکه است که ممکن است کارایی شبکه را کاهش داده باشد برای مثال، مانیتورینگ قطع برق، هشدارهای ارتباطی، سرویس‌ها و مسائل دیگر که می‌تواند در کارایی شبکه تاثیر بسزایی داشته باشند.
- تحلیل بهنگام ایرادات موجود در زیرساخت
- عیب‌زدایی سریع مشکلات پیش آمده در تجهیزات سخت افزاری و یا دارایی‌های دیجیتال بطور مثال زمانی‌که پاور سرور از کار می‌افتد، یا کابل آن قطع می‌شود، NOCفرآیندهای فوری برای ارتباط با تکنسین برای برطرف ساختن آن دارد.
- مدیریت موثر ارتباطات
- مستندسازی اشکالات رخ داده جهت بهره برداری موثر در آینده
- گزارش‌دهی‌های منظم از وضعیت شبکه و زیرساخت
- به روزرسانی‌های منظم نرم افزارها و سخت افزارها
- ارتباط سازنده با مرکز SOCسازمان
- ارتباطات موثر با مراکز CERT

# معرفی ابزار های مدیریت شبکه های کامپیوتری

- SolarWinds
- Cacti
- ManageEngine OpManager
- PRTG Network Monitor
- Nagios
- Zabbix
- Cisco Prime
- …

# SolarWinds


Powerful Products
SolarWinds Orion
Enterprise Operations Console
Orion NPM
NetFlow
IP SLA
Orion IPAM
Orion NCM
Application
Network Performance Monitoring
Network Traffic Analysis
WAN Performance
IP Address Management
Network Configuration Management
Application Performance Monitoring
Orion Scalability Engines
solarwinds

# SolarWinds

شرکت SolarWinds یکی از بزرگترین تولید کنندگان نرم افزارهای مدیریتی در حوزه فناوری اطلاعات می‌باشد. این شرکت که درسال ۱۹۹۹ میلادی تاسیس شده است دارای مشتریان بسیاری دربیش از ۱۷۰ کشور جهان میباشد. شرکت SolarWinds با شعار مشتری مداری توانسته است با رفع موانع موجود، موجب کاهش هزینه و پیچیدگی نرم افزارها شود. این شرکت نرم افزارهای مختلفی را جهت مانیتورینگ بخش‌های متفاوت در حوزه فناوری اطلاعات ارائه کرده است. این محصولات که از معروف ترین محصولات مدیریت و مانیتورینگ شبکه محسوب می گردند شامل مدیریت سرورها و برنامه های کاربردی، مدیریت شبکه، امنیت و لاگ ها، مدیریت سیستم های ذخیره سازی و ساختار مجازی و همینطور مدیریت پهنای باند و کنترل ایستگاه های کاری از راه دور می‌باشند:

- نرم افزار مانیتورینگ عملکرد شبکه Orion Network Performance Monitor یا NPM
- نرم افزار مدیریت پیکربندی شبکه Orion Network Configuration Manager یا NCM
- نرم افزار مانیتورینگ برنامه های کاربردی و سرور Application Performance Monitor یا APM و در نسخه جدیدتر SAM
- نرم افزار آنالیز کننده ترافیک جریان شبکه Orion Netflow Traffic Analyzer یا NTA
- نرم افزار ردیاب دستگاه کاربر User Device Tracker یا UDT
- نرم افزار مدیریت لاگ و رویدادها SolarWinds Log & Event Manager
- نرم افزار مدیریت فضای ذخیره سازی SolarWinds Storage Manager

# Cacti

یکی از نرم افزار های رایگان **مانیتورینگ شبکه** نرم افزار سورس باز **Cacti**می باشد که با نصب آن تمامی مزایای فوق و بسیاری بیشتر از آن فراهم خواهد شد.

**نرم افزار Cacti** توسط پروتکل SNMP به دستگاه های مورد نظر شما متصل و آنها را طی Interval تنظیم شده توسط شما بررسی می کند. این نرم افزار بر پایه PHP/MySQL می باشد که عمدتا بر روی سیستم عامل های لینوکسی نصب و راه اندازی می شود و جهت ارائه گراف های خود از نرم افزار بسیار خوب RRDTool بهره برداری می کند.
همچنین این نرم افزار امکان ارائه پنل مانیتورینگ به مشتریان شما را ارائه می کند. که شما می توانید در این نرم افزار تعیین کنید که مشترک شما پس از لاگین به چه پورت هایی دسترسی داشته باشد.

# PRTG Network Monitor

PRTG Network Monitorنرم افزاری قدرتمند برای نظارت بر شبکه و سیستم های مبتنی بر ویندوز است. این نرم افزار برای شبکه های کوچک، متوسط و بزرگ مناسب است و قادر به نظارت بر شبکه های LAN، WAN، WLANو VPNمی باشد. شما همچنین می توانید وب سایت ها، ایمیل ها و پرونده های سرور، سیستم های لینوکس، ویندوز، روترها و بسیاری دیگر را تحت نظارت داشته باشید. PRTGنظارت بر دسترسی به شبکه و استفاده از پهنای باند، و همچنین پارامترهای مختلف شبکه مانند کیفیت سرویس، بار حافظه و استفاده از CPU، حتی نظارت بر دستگاه های از راه دور می باشد. راه اندازی این نرم افزار بسیار ساده است و نظارت بر شبکه با استفاده از پروتکل های : SNMP،WMI، packet sniffe، IPFIXو..... می باشد. PRTG Network Monitorبه طور مستمر نظارت بر شبکه و در دسترس بودن سیستم های شبکه را ثبت می کند. داده های ثبت شده در یک پایگاه داده داخلی برای تجزیه و تحلیل بعدی ذخیره می شوند.

# Nagios

Nagios یک سیستم مانیتورینگ اپن سورس برای مانیتور کردن شبکه، زیر ساخت ها و نرم افزار ها است. با Nagiosامکان مانیتورینگ سیستم، سرویس ها و شبکه با ارسال پیغام هایی به ایمیل مدیران در زمان های بحرانی وجود دارد. با آن می توانید کل زیر ساخت ها ( Inferastructureها) وجود دارد. در Nagiosاز دو ماشین لینوکسی که یکی به عنوان Nagios Serverعمل می کند و دیگری به عنوان Nagios Clientاستفاده می کنیم. Nagios Serverماشینی است که Nagiosو کنسول آن برویش نصب شده و می توان دیگر ماشین های شبکه را را برای مانیتورینگ متمرکز به آن ( Nagios Server)معرفی کرد. در واقع با استفاده از ماشین Nagios Serverمی توان سرویس ها، زیر ساخت ها (مانند ftp, dns)و وضعیت پردازنده، حافظه، swapبر روی ماشین های راه دور را یکجا مانیتور کرد. به ماشین هایی که به Nagios Serverمعرفی می شوند، Nagios Client گویند.

# Zabbix

**Zabbix** یک نرم افزار قدرتمند در زمینه مانیتورینگ و جمع آوری اطلاعات در شبکه میباشد. با استفاده از این نرم افزار میتوانید بصورت Real-Time بیش از ۱۰ هزار سرور، ماشین مجازی و دیگر سخت افزار های شبکه ای را هم زمان مانیتور کنید. Zabbix در کنار جمع اوری اطلاعات، با استفاده از یک رابط کاربری مناسب انواع Graphها و Mapها را در اختیار شما قرار میدهد تا به بهترین شکل تمامی سخت افزار های مورد نظر را زیر نظر داشته باشید.کارایی بسیار قدرتمند این ابزار در جمع اوری اطلاعات و آنالیز، آن را برای سازمان های بزرگ مناسب میسازد. مانیتورینگ توضیع شده نیز با استفاده از Zabbix Proxies امکانپذیر میباشد.

این نرم افزار با یک رابط کاربری تحت وب ارائه شده است که این محیط برای ورود با اعتبار سنجی امن شده است. در این محیط میتوانید کاربرانی با سطوح دسترسی مختلف ایجاد نمایید. جمع آوری اطلاعات با استفاده از نصب Agentدر سیستم میزبان انجام میشود، البته متد Agent-Less نیز در این نرم افزار فراهم بوده و میتوان بدون Agent نیز سرور و سخت افزار ها را مانیتور کرد. Zabbix میتواند بصورت اتوماتیک تمامی سخت افزار های شبکه را شناسایی کند. با استفاده از امکان Network Discovery میتواند بصورت اتوماتیک تمامی سخت افزار های درون شبکه را شناسایی و در صورت تمایل آن را مانیتور نمایید.

# Zabbix

بعضی از ویژگی های مهم Zabbix عبارتند از:

- مانیتورینگ عملکرد و کارایی شبکه ها، نرم افزارها و منابع ابری
- پشتیبانی از محیط های کوچک تا محیط های بزرگ توزیع شده
- آمادگی برای پشتیبانی از اینترنت اشیاء
- پشتیبانی از گستره ی بزرگی از معماری های گوناگون
- ارسال هشدار و یا اجرای دستورات از راه دور در صورت بروز مشکلات
- قابلیت های منحصربه فرد در زمینه ی Visualization،شخصی سازی داشبورد، نقشه ها و گراف
- قابلیت پیاده سازی مانیتورینگ توزیع شده با استفاده از Proxy Zabbix

# Cisco Prime

کمپانی سیسکو از دیرباز پلتفرمهای مختلفی را از جمله Cisco Works LMS , NCS , WSCو ...( جهت پایش و مدیریت تجهیزات )باسیم و بیسیم و سرویسهای خود ارائه داده است. شرکت مذکور در نهایت تصمیم به تجمیع تمامی آنها در قالب یک محصول واحد تحت عنوان Cisco Prime Infrastructureگرفت. Prime Infrastructureبه اختصار PIآخرین و جامعترین راهکار کمپانی سیسکو برای پایش و مدیریت آسان و خودکار شبکه در بالاترین سطح ممکن است.

این محصول برای عیبیابی و سالم سازی شبکه بسیار کارآمد میباشد. پلتفرم PIبه دو مدل مجازی و فیزیکی در دسترس میباشد که حالت مجازی قابلیت پیاده سازی روی بستر VMwareرا داراست.

# Cisco Prime

**موارد زیر از جمله قابلیتهای Cisco Prime Infrastructure میباشند:**

- چرخه پایش و مدیریت دائمی شبکه های بیسیم و با سیم Lifecycle.
- امکان بررسی کارایی و کیفیت سرویسدهی نرم افزارهای موجود در شبکه Assurance.
- مقایسه پیکربندی تجهیزات، با راهنماها تعریف شده و یا سایر مراجع منتخب از سوی شرکت سیسکو، برای افزایش کارائی و امنیت Compliance.
- مشاهده و بررسی مقدار مصرف پهنای باند.
- قابلیت یکپارچه سازی با محصولات دیگر شرکت سیسکو از قبیل ISEو MSEبه منظور پایش و مدیریت دقیق تمامی پایانه های کاری باسیم و بیسیم و نیز پشتیبانی از فناوری BYOD.
- امکان تنظیم خودکار تجهیزات خام براساس پیش فرضهای تعریف شده.
- ارائه انواع متنوع گزارشات لحظهای و دورهای از کارکرد شبکه.
- (High Availability)دسترس پذیری بالا.
- قابلیت تعریف کاربران وگروه های مختلف برای مدیریت بخشهای مختلف شبکه.
- قابلیت ارتباط مستقیم با وب سایت سیسکو جهت رفع ایرادات Bugsموجود روی تجهیزات و دریافت آخرین نسخه از سیستم عامل آنها.
- قابلیت یکپارچگی با WLCبرای مدیریت Access Pointها.