



## دانشکده کامپیوتر - دانشگاه علم و صنعت تهران

استاد: دکتر حسین غفاریان

درس: مدیریت شبکه

این جزو با کوشش خانم ها و آقایان علی خیر، محسن قادری، شیما رضایی، جعفر مسلم نژاد، مجتبی آیت، نیکوبنی اسدی، معصومه خزایی، حسین کرمی، پویا عباسی، احمد رحمانی، عقیله یزدی، خاطره مقدس زاده، فاطمه کارگر مقدم، زهرا قنبرزاده، امیر علی فیروزمنش و حسن اسدی نگارش و گردآوری شده است و امید است گامی هر چند کوچک، جهت ارتقا سطح علمی دانشجویان عزیزکشور مان باشد.

نیمسال اول 1401-1400

## نکات جلسه اول درس:

مدریت شبکه چند بعدی است و دانش شبکه نیاز دارد و باید منابع و موارد انسانی و همه موارد را بشناسید.

منبع درس: اسلاید های دکتر بهادر بخشی است در Lms آپلود شده .

یکسری موضوع تعیین میشود برای هر نفر به عنوان پژوهش که تا انتهای ترم وقت داریم روی اون موضوع تحقیق کنیم و باید یک ارایه در حد 10 دقیقه بدھیم و باید گزارش کتبی هم از این ارایه تهیه شود و همه چیز(فایل های ارایه دوستان ) هم در کانال واتس آپی به اشتراک گذاشته میشود: (در صورت مشکل به آقای علی خیر پیام دهید [@Alikhayyer](#) ).  
اگر دوستان تجربه مدیریت شبکه دارند و میخواهند ابزار یا تجربه ای را توضیح دهند مشکلی ندارد و باید با استاد هماهنگ باشد و اوکی هست. پیاده سازی هم میشه (باید دید چی هست...)  
کتاب ندارد و منبع فقط همین اسلاید هاست.

## نحوه ارزیابی درس:

دو بخش دارد:

- ۱- امتحان که میتواند شامل پایانterm و میانterm باشد که بحث میشود(تمامی امتحانات تستی هستند) (۱۴-۱۶)
- ۲-بخش ارایه و گزارش یا همون ارایه کتبی است (۴ تا ۶ نمره).  
استاد فرمودند سعی میکنیم میانterm بگیریم و حذفی هم باشد که حجم مطالب کم شود . (این باید حتما پیگیر شویم در کلاس ).

فعالیت ویژه کلاسی هم ممکن است تقدیر شود و تاثیر داده شود!

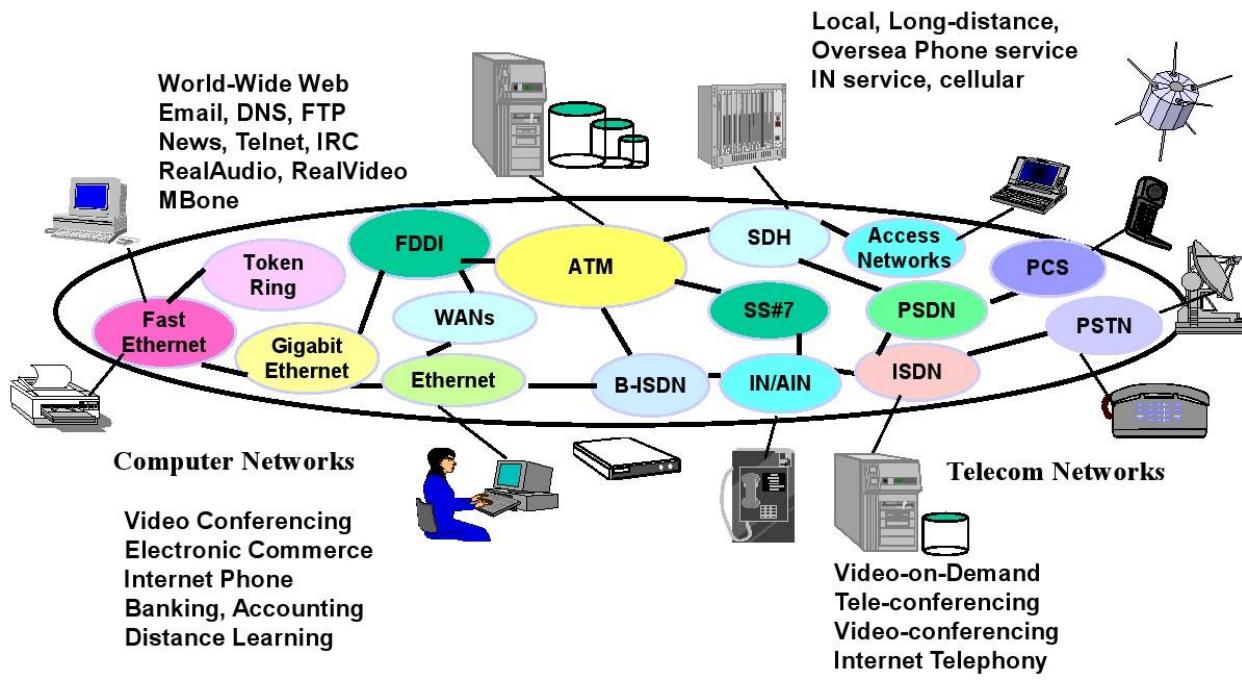
## تدریس جلسه اول:

مدیریت شبکه چیست؟

چه کابردی دارد؟

چی به چیه کی به کیه؟

# Today's Networks



ما وقتی در باره شبکه صحبت میکنیم شبکه های ما دو دسته اند : ۱- مخابراتی ۲- کامپیوتری

جنس این دو یکی نیست . در شبکه کامپیوتری اطلاعات بصورت تکه تکه منتقل میشود و هر تکه جدا جدا مسیر یابی میشود . به صورت پایه تضمینی در این شبکه نیست . اما تلکام یا مخابرات اساس و پایه این است که باید رزرو منبع انجام شود و در طول سرویس هم چک میشود . (Call Setup – انتقال اطلاعات – آزاد سازی منبع). فرق دارد که Atm باز نزدیکتره به شبکه کامپیوتری . اینترنت ترکیبی از همه این هاست و این شبکه ها با هم دارند کار میکنند . ماهواره مثلا با تلفن و پرینتر و ... همه وصل اند به هم.

امروزه کلی سرویس مورد استفاده است که میتواند همزمان هم باشد (کلاس آنلاین و ) من کامپیوتری ام و به شبکه کامپیوتری متصل ام اما معلوم نیست سرور در شبکه کامپیوتری باشد . اصلا هنوز بک بون اینترنت و Sdh Sonet است . کامپیوتر در حال غالب شدن است و اترنوت خیلی سریع است (۱۰ گیگ - ۴۰ گیگ و ۱۰۰۰ گیگ حتی ) و ساده است همه اکثرا بلدن اما شبکه های مخابراتی خیلی سخت است و کمتر کسی بلد است یه Wan Csmaca بود که در همون هم فراموش شد. آینده برای شبکه کامپیوتری است. در کشور های پیشرته تلفن Psdn ندارند یک کابل هم تلویزیون است هم اینترنت هست هم تلفن هست....

از نسل ۳ پکت سوییچینگ وارد کار شد خیلی خوب بود. اما با خاطر وایمکس نابود شد نسل ۳ و نسل ۴ او مد. نسل ۵ هم که Ip و هوش مصنوعی هست. Sonet – Sdh هم داره با خاطر گیگابیت اترنت دار منسوخ میشن. با خاطر پول جلوی Mms گرفته شد.

## What is Network Management?

---

- Computer networks are complex live systems
  - Require a great deal of attention to be kept up & **running**
    - E.g. Failures, Performance tuning, Service Provisioning, accounting, ...
- Network management system:
  - Anything that has to do with running a network
    - Technologies
    - Tools
    - Activities
    - Procedures
    - People



شبکه از نظر مدیریت شبکه یک موجود زندست و پیچددست و باید دایم ترک بشه از لحاظ امنیت – تعمیرس کنیم اگه خراب شد اکانتینگ داشته باشیم و ....

ترکیبی از تکنولوژی ابزار ها فعالیت ها و روال های کاری و مردم است . و اصلا ساده نیست.

## Running a Network: OAM&P

---

### ➤ Operations

- Keep the network running smoothly, monitor for alarms, watch for intrusions and attacks, ...

### ➤ Administration

- Keep track what's in the network, who uses what, housekeeping

### ➤ Maintenance

- Repairs failures and upgrades network

### ➤ Provisioning

- Configure the network to provide services, turn up services for end customers
- 



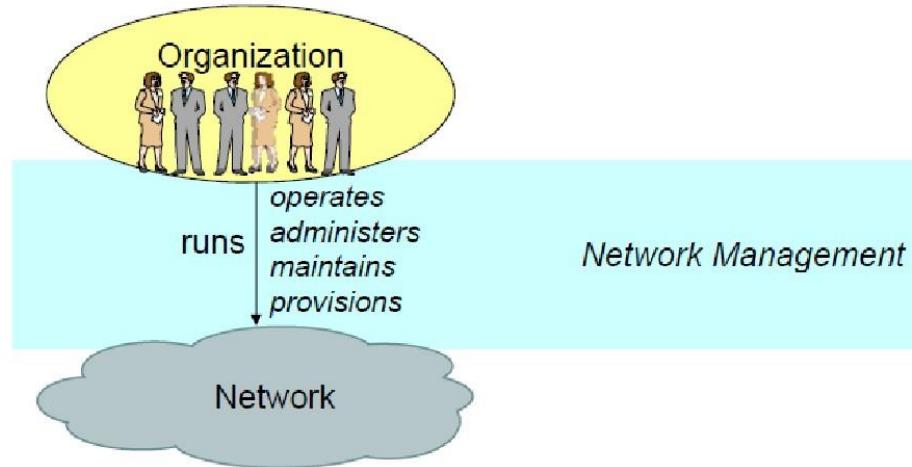
6



مدیریت شبکه چندین مدل دارد . یکی از آنها Oam&P است که مخفف عبارات بالاست  
Operation یعنی چک کن که شبکه من خیلی نرم و روون کار کنه و حواست به همه جاش باشه  
Administration ما باید حواسمنون به یوزر هامون باشه(گند نزنن و سرو صدا الکی نکنن)  
Maintenance نگه داری و آپگرید و رفع خرابی و بروز رسانی شبکه و ...  
Provisioning نظارت روی یک سرویسی که آپ شود. مثلا اینترنت پرسرعت تر راه اندازی کنیم و سرویس  
جدید فعال کنیم پشت پرده سرویس رو اجرا کنیم تا فاصله زمانی و مشکلات کم شود.

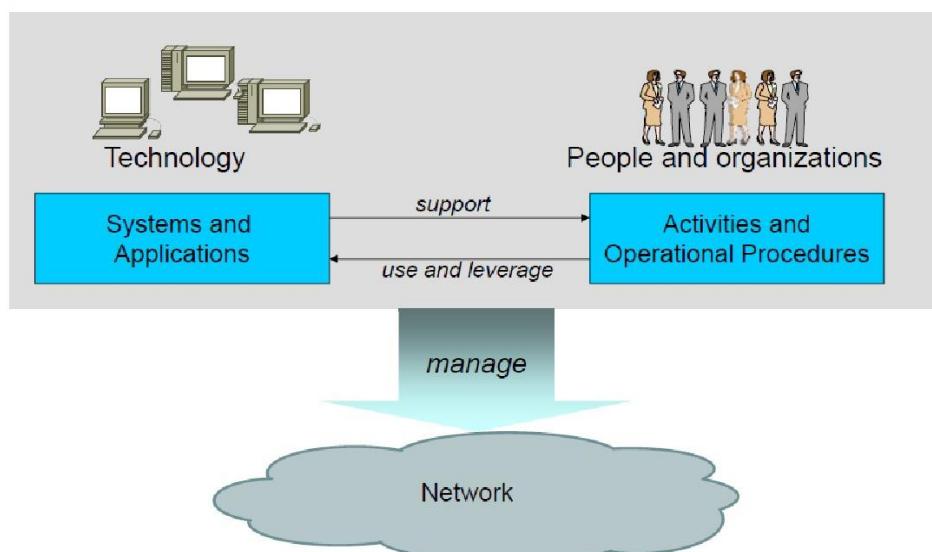
# What is Network Management

- Therefore, network management is the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networks



مدیریت شبکه یعنی شبکه ای داریم با یوز هاش و فعالیت میکنیم بر اساس روال سازمانیشون و ابزار هم دارند کلی ... حالا ما باید ابزار هایی استفاده کنیم شبکه رو فعال نگه داریم مدیریت کنیم و نگه داری کنیم و اگر نیاز باشه Provisioning کنیم و این چتر روی همه ای ابر شبکه است . چه آدم ها چه سیتم ها .

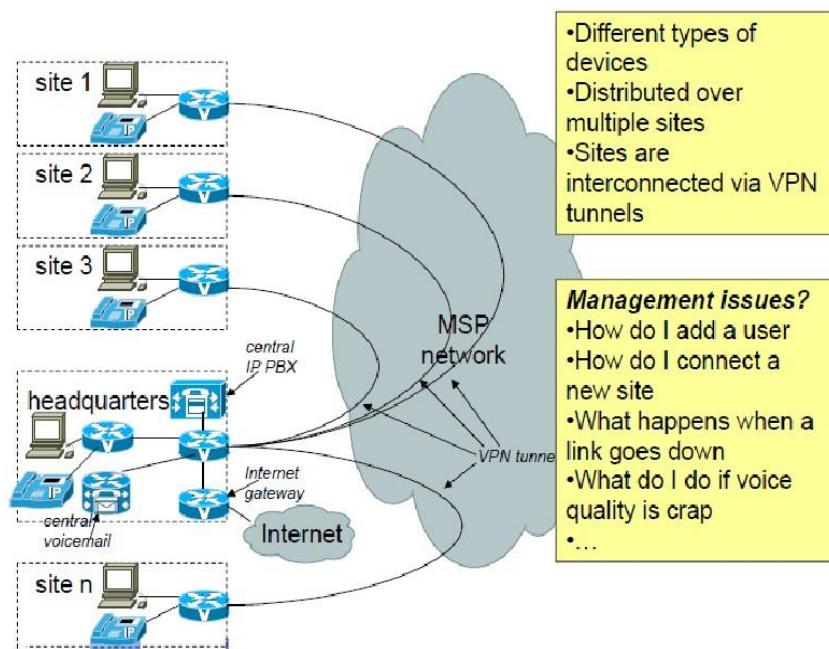
## Network Management System



خود مدیریت شبکه آدم هم هست داخلش و فقط ماشین نیست (ترکیبی از ماشین ها و انسان هاست) و با هم در تعامل اند که نتیجه تعامل اینها مدیریت شبکه است.

## Network Management Examples (1)

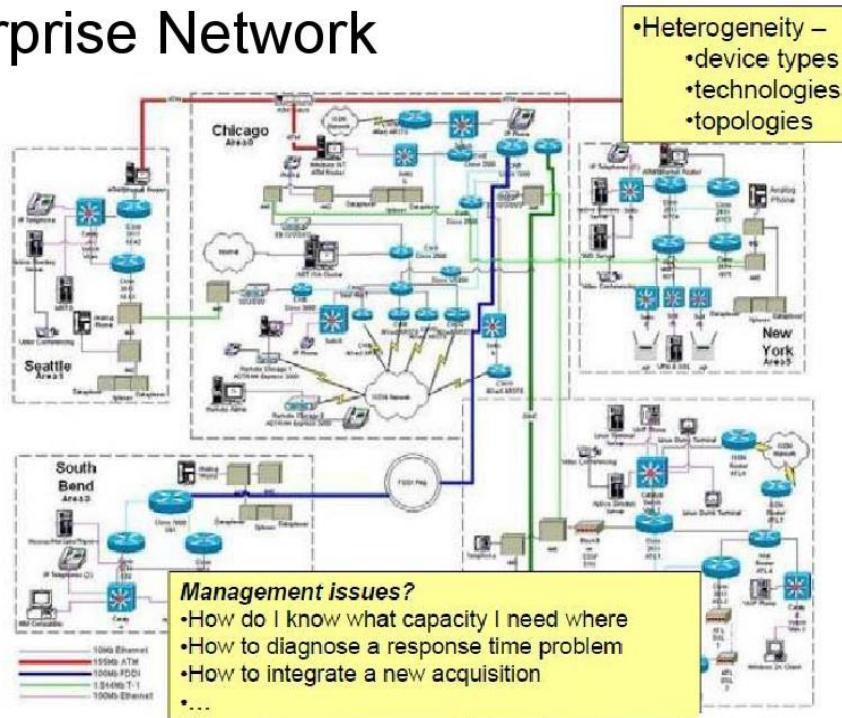
### ➤ Medium-sized business network



اگر ما شعب مختلف داریم مثل بانک که خودش یک مدیریت شبکه است که متوسط تا بزرگ هم هست که باید سایت ها و کامپیوتر های مختلف را به شعبه مرکزی (Headquarter) وصل کند.

# Network Management Examples (2)

## ➤ Enterprise Network



مدیریت اینجا یکم سخت تر است . چون مدیریت روی شبکه های مختلف است و بین شبکه ای است (بحث نوع مختلف دستگاه ها - توضیع شدگی اطلاعات در سایت های مختلف- اتصال سایت های مختلف - Vpn های مطرح است) و کاملاً تخصصی است و موضوع های انسانی مثل افزودن کاربر یا شعبه جدید هم مطرح است . چطوری سرعت را بالا ببریم چطوری گسترش بدیم ....

ما اگر اسلاید بالا را یک شبکه سازمانی در نظر بگیریم بخش های مختلفی دارد و کلی شبکه داریم و ممکن است جنش شبکه ها هم میتوند یکی نباشد (مثلا پالایگاه اصلاً یه قسمت شبکه صنعتی است) و این تفاوت ها در نوع شبکه ها در مدیریت چالش میشود.

از دید کاربر بحث های مدیریتی مثل تخصیص منابع و حرکت به سمت فناوری های نوین و.... هم مطرح هست. چالش ها از دید Enterprice فرق دارد و هر قسمت یک شبکه ای است که برای ماست .

# Other Perspectives

---

- The NM operations & procedures & functionalities can be classified from other perspectives than (traditional) OAM&P
  - Classification based **functionalities**
    - ISO's point of view: FCAPS
  - Classification based on **layers**
    - ITU-T's point of view: TMN
  - Classification based on **business model**
    - TMF's point of view: eTOM
  - Other classifications ...
- 



11



در بحث توابع کاری کلی فانکشن های امنیت و کارایی فانکشن اکانتینگ و فالت تلورنس را داریم.

ما میتوانیم سیستم مدیریت شبکه را از باب فانکشنالیتی یا لایه شبکه و یا بیزینس خود(نیاز های کسب و کار) مورد بررسی قرار دهیم . یعنی در مدیریت شبکه هر چیزی را در نظر بگیریم باز از یک لحظه هایی کمبود هایی دارد. مثلا مدل Lms ما بر حسب کار کرد باشد ایزو Fcaps را ارایه کرده یا بر حسب لایه ها Itut مدل Tmn را ارایه میدهد. یا Tmf ها مدل Etom را پیشنهاد میکنند و این جنبه های خیلی متفاوت هستند . ما که دعوا نداریم !!! تازه اینا مدله ابزار هاش داستان داره....

# FCAPS

---

## ➤ Fault management

- Detecting, isolating, and elimination of failures

## ➤ Configuration management

- Setting management parameters, backup and track changing (hardware & software) configurations

## ➤ Accounting management

- Resource usage monitoring

## ➤ Performance management

- Resource utilization monitoring and management

## ➤ Security management

- Security policies definitions, implementations, monitoring
- 



12



Fcap مخفف عبارات بالاست مدیریت خطا یعنی ابتدا محل خطا را پیدا کنیم سپس آنرا ایزوله کنید و در نهایت آنرا رفع کنیم.

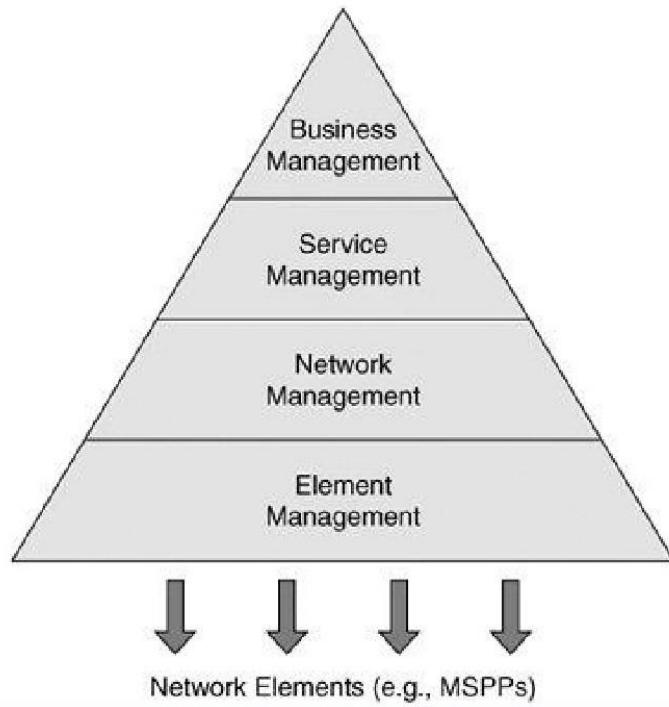
در بحث مدیریت پیکر بندی بحث کانفیک کردن بک آپ گرفتن و ترک کردن و ری استور کردن آنها است.

بحث اکانتینگ مدیریت منابع است و بفهمیم کی از چی داره استفاده میکند . موضوع مهمی است (مثالش محدود کردن حجم اینترنت است ).

مدیریت کارایی یعنی استفاده مناسب از دستگاه ها و تقسیم فشار بین منابع و مدیریت و پایش بهره وری منابع

مدیریت امنیت یعنی فایر وال و Ids فقط ابزار هستند و این بحث امنیت نیست بحث سر تعریف سیاست های امنیتی و پیاده سازی آنهاست و اینکه مانیتور کنیم که نقض نشوند . (مثلا بدون تعریف سیاست نمیتوانیم فایر وال را تنظیم کنیم ) . ( این مدل طرز تفکر ما کامپیوتوری هاست).

# TMN

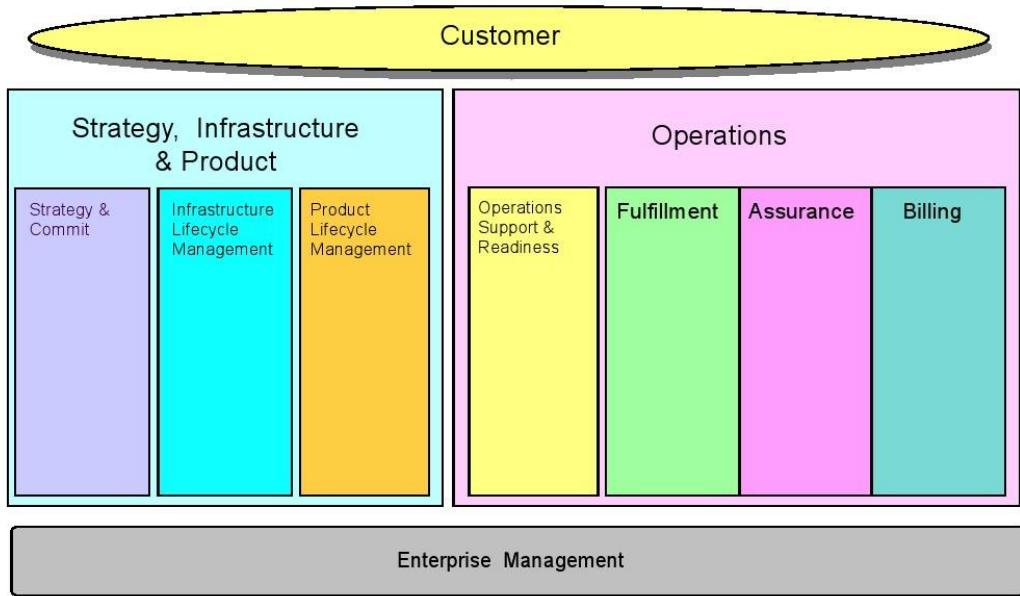


13



این مدل Tm1 است که برای مدیریت در بین مخابراتی ها است و بسیار هم موفق است چون مخابراتی ها خیلی در مدیریت قوی تر اند و از اول مدیریت و تظمین را ارایه دادند. و این حسرت کامپیوترا ها هست و خیلی در حوضه مدیریت شبکه ضعیف هستند مثل مخابراتی ها روی Call drop rate اصلا اهمیت نمیدهند مثلا.

# eTOM



14



این مدل Etom است . برای بیزینس است مدیریت سازمان می گوید من مشتری دارم و میخواهم مشتری راضی باشد چون اعتبار و پول من وابسته به مشتری است . در این حالت مدیر شبکه باید در راستای اهداف من باشد . دو قسمت دارد ۱- سخت افزاری ۲- نرم افزاری سخت افزاری می گوید استرالی و زیر ساخت و محصولات را مدیریت کن .

نرم افزاری می گوید کسب و کار و اطمینان و صورت حساب هایت را مدیریت کن .

ایتم میگوید کسب و کار من این ها است و باید بر طبق این مدیریت کنی که برای من مفید باشد و سود ده شود شبکه برای من و ۴ تا مشتری بیشتر برای ما بیاید .

مدیریت شبکه آشفته بازار است و هزار رنگ اند و هر کسی میتواند نظر دهد و نقد کند و تازه روش های پیاده سازی و ابزر ها هم بسیار زیاد اند و متفاوت اند .

## جلسه دوم:

# Outline

---

- What is Network Management?
  - Why Network Management?
  - Who is Who in Network Management?
  - What is going in Real Network Management Systems?
  - Why is Network Management Challenging?
  - Network Management Evolution
- 



15



چرا مدیریت شبکه؟

شاید در گذشته کمتر این موضوع دیده میشد، ولی امروزه یک واقعیت هست که شبکه به یک کسب و کار تبدیل شده، و عده زیادی از این طریق ارتزاق می کنند.

# Why Network Management?

- Computer/Teleco networking is a **business**
  - Networks are built to make money
- Income (revenue) vs. TOC (Total Ownership Cost)
- Income
  - Service provision for customers with desired QoS
- TOC
  - Cost to **build** up the network and its **operation** cost



وقتی شبکه بعنوان یک کسب و کار در نظر گرفته میشود، درآمدی که مطرح میشه در مقابلش یک هزینه باید پرداخت بکنیم. درواقع، مقابلش ما باید هزینه مالکیت بپردازیم. مثلاً اگه بخواهیم از یک شبکه یا سرویسی استفاده کنیم باید هزینه ش رو بدیم و میدونیم هرچی هزینه بیشتر بدیم منطقاً در اکثر اوقات سرویس بهتری هم میگیریم. درواقع به ازای سرویسی که میخواهیم به مشتری بدهیم بر اساس سطح کیفیت که در نظر گرفته میشود، یک درآمدی خواهیم داشت و از آن طرف یک هزینه مالکیت (TOC) یا هزینه تمام شده سرویس هم وجود داره که باید آن شبکه رو بسازیم، راه اندازی کنیم و در حالت سرویس دهی نگه ش داریم.

این میشود هزینه تمام شده برای آن سرویس که شامل مالیات، بیمه، نیرو انسانی، آب، برق، گاز، تلفن، سفرها، تیم پشتیبانی، بخشی حقوقی، فیبرنوری بسترهای وايرلس ... اینا همه هزینه هست.

به هر حال هزینه مالکیت اولیه وجود دارد و باید روی آن سود دریافت کنیم، پس بحثی که وجود داره بحث مالی و سود و زیان هست.

## Why Network Management? (cont'd)

- Cost (to provide the services)
  - NM to maximize efficiency, thus minimizing cost
- Revenue (realized through the services)
  - NM to ensure services are accounted for and delivered when and where they are needed
- Quality (of the delivered services)
  - NM to maximize the inherent “value” of the managed network and services provided



در دنیای بیزینس و کسب و کار حرف و اول و آخر را مباحثت مالی میزنند، اگر یک سرویس داشته باشیم که نتونه خرج خودش را در بیارورد، بهتره هست جمع آوری شود.

اقتصاد مبتنی بر هزینه هست.

یک سرویس شبکه داریم که در حال کار هست، یک هزینه داریم برای مالکیت و راه اندازیش، یک هزینه هم داریم برای نگهداریش.

## استفاده از NMS هزینه دارد، حالا چرا مدیریت شبکه؟

وقتی مدعی ارایه سرویس با کیفیت هستیم و در نتیجه پول بیشتری طلب میکنیم، خب NMS کمک میکنه سرویس خوبی بدھیم و شبکه رو تا جایی که جا داره efficiency بکنیم تا بتوانیم رو آن شبکه بیشترین سطح سرویس را بدھیم، به این ترتیب هزینه ها تقسیم بشه بر سطح سرویس، در واقع متوسط هزینه به شدت افت میکند. پس NMS باعث افزایش کارایی شبکه و کاهش هزینه متوسط میشود.

پس در بحث هزینه NMS کمک میکند کیفیت را ببرید بالا، متوسط هزینه را کاهش دهد. در بحث سوددهی، NMS تضمین میکند آنقدری که نیاز هست، به مشتری سرویس بدھیم. (یک بخشش Accounting یعنی حسابداری هست و چک میکنه هر کسی اونقدر ک سرویس میگیره، بهش بدیم) وقتی سرویسی میگیریم، قراردادی مینویسیم که در این قرارداد یه اصطلاح هست، بنام "service-level agreement" SLA که مشخص میشه ظرفیت سرویس چقدر، مثل پهنای باند و ترافیک و... که اگر مشتری به این ظرفیت برسد، دیگر پشتیبانی دریافت نمیکند. در مقابلش موضوعی برای سرویس دهنده هست که اگر نتواند سرویس را به درستی ارائه بدهد، باید جریمه بدهد یا قرارداد را مشتری میتواند کنسل کند و از جایی دیگر سرویس بگیرد و مشتری از دست میرود و درواقع این به معنای ضرر سرویس دهنده هست.

دومین بحثی که هست اینه که NMS تضمین میکند که سرویس در آن حدی که لازم است، در زمان و مکان مناسب تحويل افراد بشود و این یعنی اینکه سود آوری دارد.

سومین بحثی که NMS کمک میکند در بحث کیفیت هست. اینجا قسمت ارزش افزوده NMS هست، کمک میکند تا سرویسی مناسب با شرایط رو تحويل بده. اینجایی هست که مدیریت شبکه دست میزاره روش که میگه من سرویس با کیفیت رو تضمین میکنم.

# Why NM: Cost

- CAPEX (Capital Expenses): Equipments, Software, License, Location, ...
- OPEX (Operation Expenses) : People, electricity, maintenance, ...



18



Cost:

هزینه 2 قسمت دارد : Capex و Opex

Capex: هزینه ای هست که بابت تجهیزاتی مثل سوکت، کابل، کارت شبکه و... میدهیم.

(هر کدام از این تجهیزات یه تایم لایفی دارند، مثلاً بین 3 تا 5 سال برآورد میشه)

Opex: بحث Information و اطلاعات هست. اطلاعات فقط تجهیزات نیستند، میتوانند سخت افزاری، نرم افزاری یا حتی انسانی یا روال کاری باشند. قسمت Opex مربوط به استفاده از تجهیزات هست که نیاز به مدیر شبکه هست.

در بحث امنیت اطلاعات ۵۰٪ شامل تجهیزات قوی و حرفه‌ای هست و ۵۰٪ مرتبط با نیروی انسانی هست یعنی نصف حوزه امنیت شبکه مربوط به انسان است. پس انسان‌ها اصلی ترین گزینه برای نفوذ به یک سیستم امنیتی هستند حتی در NMS هم به همین صورت می‌باشد.

بحث maintenance، بحث حفظ و نگهداری که بحث خیلی مهمی هست.

## Why NM: Cost (cont'd)

### ➤ Important fact

*While network equipment and NM software are expensive, but the cost is **amortized** over the lifetime of the network; hence,  
**OPEX >> CAPEX***

### ➤ Attempt to decrease OPEX

➤ Even if it results in increasing in CAPEX

### ➤ Efficient network management system can decrease OPEX significantly, e.g., ...



هر موقع در ابعادی بزرگ، کار انجام می‌شود هزینه‌های Opex به مرتب از هزینه‌های Capex بیشتر هست (یعنی هزینه مدیریت و نگهداری خیلی بیشتر از هزینه تجهیزات هست).

OPEX در حوزه NMS می‌توانه کمک کنه تا هزینه رو کاهش بده البته با هزینه کردن برای Capex بهتر و بیشتر.

# Why NM: Cost (cont'd)

- More efficient troubleshooting and diagnostics
  - Free up operators from routine problems to focus on the hard stuff
  - Reduce amount of expertise required
- Automation of service provisioning, workflows
  - Less operator involvement
  - Increased throughput
  - Less prone to operator error
    - >50% of network & service outages! (impacts cost and quality)
- Planning, bottleneck analysis
  - Deploy resources where they are needed most
  - Optimization of topologies
  - Minimize investment needed for given network goals
- And more



20



اما چجوری هزینه Opex را کاهش میدهد؟

1) در حوزه troubleshooting کارایی سیستم را افزایش میدهد، که هرجا NMS به مشکلی بخورد، مشکل را شناسایی میکند و بصورت یه هشدار مشکل را نشان میدهد که باعث کاهش هزینه عیب یابی میشود و دیگر نیازی به هزینه های انسانی برای عیب یابی نیست.

2) فرآیند service provisioning را اتوماتیک میکند، یعنی کمتر از عوامل انسانی استفاده میشود و سرویس کمتر به مشکل میخورد و سرویس سریعتر آپدیت میشود.

3) در بحث planning و bottleneck analysis نیاز داشته باشه بتونه به راحتی نحوه سرویس دهی در شبکه را مانیتور بکند.

# Why NM: Cost (cont'd)

- More efficient troubleshooting and diagnostics
  - Free up operators from routine problems to focus on the hard stuff
  - Reduce amount of expertise required
- Automation of service provisioning, workflows
  - Less operator involvement
  - Increased throughput
  - Less prone to operator error
    - >50% of network & service outages! (impacts cost and quality)
- Planning, bottleneck analysis
  - Deploy resources where they are needed most
  - Optimization of topologies
  - Minimize investment needed for given network goals
- And more



20



## Revenue:

1) NMS کمک میکنه تا سرویس های accounting و billing فعال بشه و باعث سود دهی بیشتر بشه.

2) NMS کمک میکنه تا سرویس ها بصورت service on demand باشه یعنی بطور مثال اگر مشتری نتونست سرویس رو تمدید کنه مشکلی پیش نمیاد، سرویس پیش ما میمونه تا هر وقت پول داد سرویس رو فعال میکنیم. با این ویژگی NMS دیگه سرویس مشتری از بین نمیره و یک مزیت ویژه میتونه باشه.

3) NMS کمک میکنه تا ریزکارکرد و گزارش از مصرف منابع سرویس رو در اختیار مشتری قرار بدیم.

4) NMS کمک میکنه تا (time until revenue) بازه زمانی رسیدن به سود دهی کاهش پیدا کنه.

# Why NM: Quality

---

- Central term in networking: QoS
  - QoS = managed unfairness (to satisfy service level objectives)
    - In management, QoS is also referred to as “service level”
  - Examples of quality
    - Availability of service, Service response time, Delay, jitter, echo, clipping, Video quality, ...
- While network must be designed for QoS requirements, network operation management is also greatly influence QoS



22



## Quality:

QoS به معنی کیفیت سرویس هست. یعنی یک جوری سرویس بدیم که بی عدالتی اتفاق نیفته که در دیدگاه فنی به کیفیت سرویس service level هم معروف است. که این سرویس دیدگاه های فنی مختلفی داره مثل availability of service , service response time, delay jitter, echo, video quality ...

با automated provisioning سرویس ما سریعتر آپدیت میشه و پیکربندی های اشتباہ کاهش پیدا میکنه و کیفیت سرویس افزایش پیدا میکنه.

با سطح از کیفیت رو برای یک شبکه میتوانیم مشخص کنیم.

با کمک diagnose و help identify میشه محل مشکلات و خطاها رو شناسایی و حتی در حل مشکل، چالش ها رو کمتر کنیم و یک قابلیت reactive به ما میده. درصورتی که مشکلی رو پیدا کنه میتوانه بصورت اتوماتیک مشکل رو حل بکنه.

## Outline

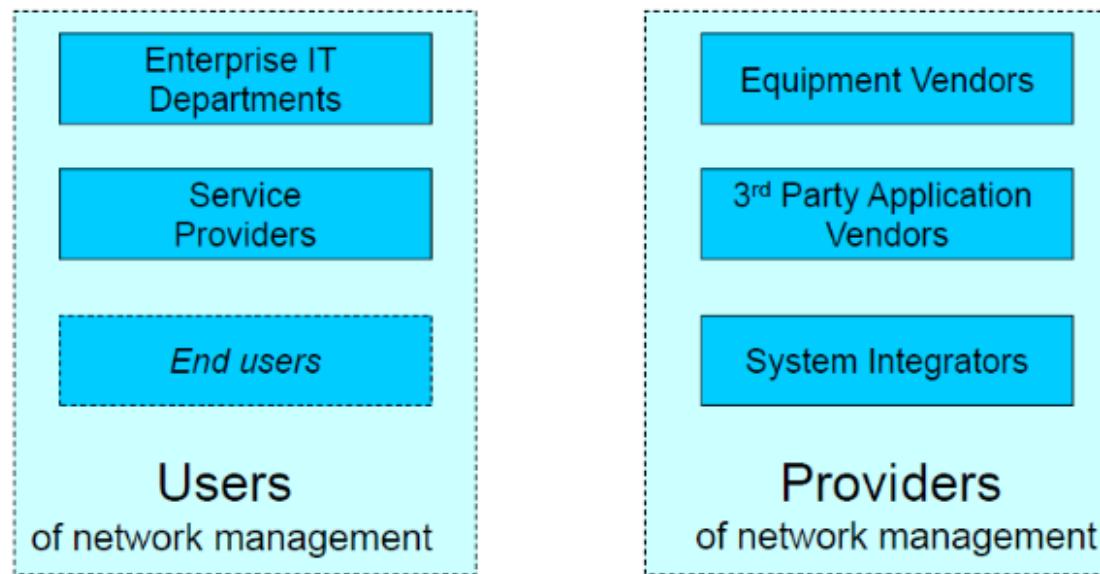
---

- What is Network Management?
  - Why Network Management?
  - Who is Who in Network Management?
  - What is going in Real Network Management Systems?
  - Why is Network Management Challenging?
  - Network Management Evolution
- 



اصولا در هر سیستمی یک سری موجودیت داریم که نقش آفرینی میکنند که Player هستند. حالا این Playerها در شبکه دو دسته هستند یک دسته کاربران استفاده کننده هستند و یک دسته افرادی که ارائه دهنده آن سرویس و بستر هستند.

## Network Management: The Players



- دسته اول، یعنی کاربران سیستم مدیریت شبکه چه کسانی میتوانند باشند؟ اول کاربر معمولی (User)، دوم service providers، سوم Enterprise providers هست.
- دسته دوم، یعنی ارائه دهنده ها یا همان providers چه کسانی میتوانند باشند؟
  - 1) سازنده تجهیزات (equipment vendors) کسایی که تجهیز تولید میکنند مثل سیسکو و ...
  - 2) شرکت های طرف سوم (3rd party) مانند تولید کننده های نرم افزار برای تجهیزات خاص.

های جدیدا خیلی باب شده است، سیستم تجمعی شده رو به اصطلاح system integrators (۳ مدیریت میشه کرد که اغلب به مباحث نرم افزاری، سخت افزاری و اپلیکیشنی پرداخته میشه.

## Service Provider Interest in NM

---

- Service providers sell communication services
  - Many market segments: Long Distance versus Local Exchange Carriers, voice, data, video, ...
- Whereas differentiation in services
  - All running networks is their core business
  - However, many companies offering same services
    - Compare airlines: same air planes, airports, "function"
- Major differentiation: Quality (SLA)



26



### service providers interest in NM

سرویس های ارتباطی معمولاً دو نوع هستند یه بصورت local که داخلی انجام میشه یا بصورت از راه دور (long distance) که سرویس های طولانی و از راه دور هستند. به همین دلیل سرویس پرووایدرها علاقمند به استفاده از NMS هستند.

## Service Provider Interest in NM (cont'd)

---

### ➤ Management-related differentiation

- Turning up new services the fastest
- Running the network at lowest cost
- Fixing problems the most efficiently, or avoid them altogether
- Ability to give service level guarantees, and keep them
- Best customer service
- Who squeezes the most out of network investment



27



### service providers interest in NM (cont'd)

یه جاهایی هست که در حوزه سرویس دهی، پرووایدرها به یه عده ای بصورت فوری سرویس بدهند، یا مثلا میخواهند شبکه را استارت بزنن که با کمترین هزینه باشه، یا اگر به مشکل برخوردند مشکل رو به شکل سریعتری حل بکنند یا اینکه سطح سرویس رو متناسب با نیاز مشتری ارائه بدن.

# Enterprise Interest in NM

---

- Enterprise networks are different from service provider networks:
- Running networks is not the core business
  - Communication services for enterprise operation
  - IT departments are cost centers
- The network has only one customer & the customer has not any alternative options
  - The network is not the primary competitive differentiator



28



## Enterprise interest in NM

سازمانها هم به NMS علاقه دارند، چون سرویس های متفاوتی را ارائه میکنند. سازمانها، تنها کاربر شبکه های خودشان هستند، چون شبکه های داخلی هستند.

## Enterprise Interest in NM (cont'd)

- Since the network is cost, efficient management → minimizing operation costs. E.g.,
  - Ability to tie in suppliers, partners, customers
  - Ability to quickly integrate a new acquisition
  - Imagine one hour outage...
    - at a financial brokerage, at a car manufacturer, ...
- Since network management does not directly determine revenue of enterprise → less investment on NM systems
- It's not just the network, it's also Data Centers, applications, and systems

29



### Enterprise interest in NM (cont'd)

نیازمند یک سیستم مدیریت کارآمد هستیم تا بتوانیم هزینه های عملیاتی را کاهش بدیم تا بتوانیم مشتریان و ارائه دهنده‌گان سرویس و... رو بهم گره بزنیم و هر موقع خدماتی میخواهند، بتوانیم ارائه بدیم. نمیتوانیم مستقیماً بگیم سیستم NMS باعث سودآوری سازمان میشود، بنابراین کمتر بر روی آن سرمایه گذاری میشود.

سیستم NMS فقط منحصر به شبکه نیست، بلکه دیتا سنتر و برنامه‌ها و .... رو هم شامل میشود.

# End Users

---

- Customers of communication services
- Not interested in management unless part of the service (“self service”)
  - Customer care system
  - Trouble ticketing system
  - Service on demand
  - One bill
  - Service statistics online
  - Set up usage policies for kids



30



## End Users

کاربر استفاده کننده از شبکه، مفهوم مدیریت شبکه را نمیداند، اما انتظار ارائه گزارش دارد. گزارشاتی همچون نوع سرویس، زمان، حجم، سرعت و کیفیت سرویس ها، که در اینصورت ارتباط با کاربر میره به سمت سیستم پاسخگویی آنلاین، یا سیستم تیکتینگ که از طریق تیکت به کاربر مشکل یا خطا سرویس اطلاع رسانی میشه، بخش صدور قبض و تک صورتحسابه، سرویس ریزکارکرد و گزارشات آنلاین، سرویس های مبتنی بر شبکه های خاص و محدود مثل ارائه نت رایگان برای اپلیکیشن شاد که فقط در بستر نرم افزار شاد مصرف میشه.

# End Users

---

## ➤ Network managers

- Many roles, for example
  - Network administrators
  - Craft Technicians
  - Device administrators
  - Help desk operators
  - Network planners

## ➤ Network management systems, software, interfaces to support and help them be effective

---



31



میتوانه هر کاربری باشه، میتوانه مدیر شبکه یا عموم مردم باشند. بعنوان استفاده کننده درنظر گرفته میشوند.

# Equipment Vendors Interest in NM

- Make a business out of selling networking and data center equipment
  - Not management systems (application software)
- **Manageability:** Ease with which a vendor's equipment can be managed
  - Support by standard management tools
  - Time & effort to integrate with custom operations support infrastructure
  - Availability of expertise, qualified personnel
  - Required training cost, dependency on support contracts
  - Proneness to operational errors



32



## Equipment Vendors Interest in NM

سازندگان تجهیزات از علاقه مندان NMS هستند. چون برای تولید، تمام تلاششون رو میکنن تا تجهیزاتشون راحت تر مدیریت بشه، فرقی نمیکنه از چه تجهیزاتی باشه میتونه یک شبکه، یک سوئیچ یا یک دیتاسنتر باشه.

تولیدکنندگان تجهیزات، اکثرا بخشی برای آموزش افراد جهت کار با تجهیزات خودشان دارند. به نوعی مدیر شبکه آموزش می دهند.

سازنده تجهیز میاد برای تجهیزش یه سری قابلیت های مدیریتی میزاره. مثلا اینکه فلان ابزارهای استاندارد مدیریت شبکه رو ساپورت میکنن.

## جلسه سوم:

# Equipment Vendors Interest in NM

### ➤ Shift in perception

- Past: network management a necessary **evil**
- Present: network management **competitive differentiator**

### ➤ Relevance to the equipment vendor

- Lower cost of network ownership
- Build brand value: other products work similar to ones already deployed

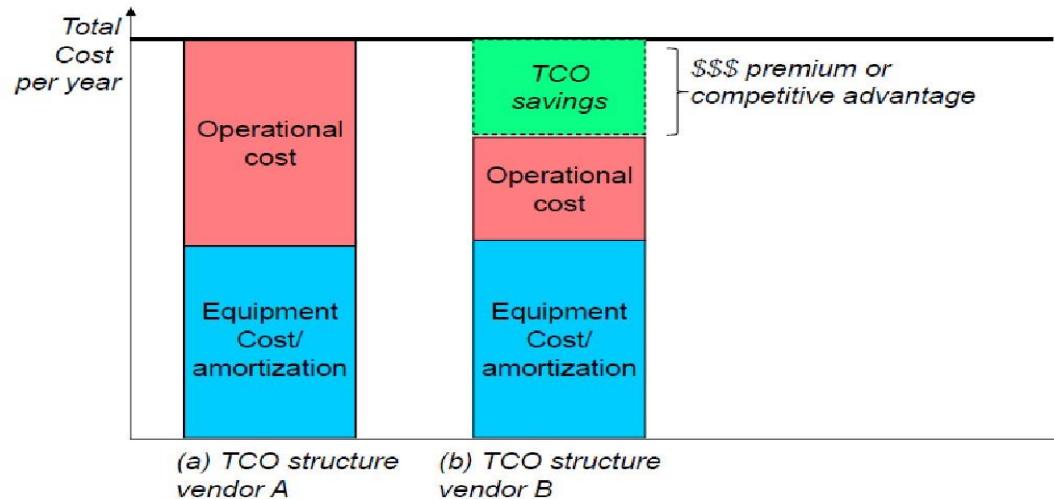
یک دیدگاهی در سازندگان در گذشته وجود داشت که هر کسی استاندارد خودش را داشت و به سیستم مدیریت شبکه دید خوبی نداشتند چون میتوانست اسرار شرکت را افشا کند

اما امروزه میدانیم سیستم های مدیریت شبکه لازم است چون همه چیز استاندارد شده است.

Nms ابزاری برای کاهش هزینه های شبکه است و وقتی شرکتی از تجهیز مدیریت شبکه ای بسازد و برنده یک شرکت مدیریت شبکه استفاده کند برای آن شرکت اعتبار است.

# Equipment Vendors Interest in NM

- If vendor B's equipment is less costly to manage than vendor A's...



ما در بحث هزینه کتس و اتس داشتیم

درکتس به شکل سنتی ما هزینه تجهیزات و هزینه عملیاتی داشتیم حالا با استفاده از تجربیات nms و قابلیت های مفیدی که در اتس nms هست در اتس فضای سبز رنگ فضایی هست که می تواند از هزینه های ما کاسته شود و این بخش همان قسمتی است که توان رقابتی ایجاد می کند و می توان به مشتریان خود اطمینان دهیم که تا این حد میتوانند از هزینه های عملیاتی شرکت کاهش دهند

# NM Application Vendors

- Make a **business** out of developing, selling, servicing network management applications
- Fill the gaps that equipment vendors leave open
  - Multi-vendor support
  - Complete end-to-end NM instead of device management
  - Management functionalities instead of managing devices, e.g., work flow, customer care, ...
- Competitive features
  - Multi-vendor support
  - Customizable
  - High-end management functionalities
  - Easy to use and integrate

یک حوزه سازنده های تجهیزات بود و یک حوزه وندور های خود اپلیکیشن های nms است مثل هر حوزه دیگر برای ساخت یک اپلیکیشن nms ما شرکتهایی رو داریم که از این مسیر به دنبال کسب پول و درآمد هستند و یا نسخه رایگان ارائه می دهند ولی در مجموع این کار یک بیزینس شده است

چرا شده کسب و کار

به این دلیل که سازنده تجهیز درسته به من یک سری از ابزارهای مدیریتی میده و سازنده‌گان امروز سعی می‌کنند استانداردها را رعایت کنند مثلاً استاندارد ip4, igmp, ip6 ...,

اما وقتی بحث پیاده سازی عملی پیش میاد هر کسی از یک گوشه کار میزنه و کامل انجام نمیده و پیاده سازی ها فرق می کنند چون پیاده سازی ها فرق می کند اگر بتوانیم یک nms ارائه کنم که به صورت مولتی وندور ساپورت باشد یعنی بتواند هم با هوایی هم با سیسکو و... با همه این کار کنه یک برگ برنده است و اگر هم چنین ابزاری نداشته باشم باید کلی nms مختلف داشته باشم و هر کدام از این nms ها هر کدام مسئول کار خودش است که خیلی سخته بخاطر هزینه های nms و هزینه های تامین نگهداری

بنابر این اگر nms مولتی وندور باشه خیلی راحت تره و میتونه زبان همه اینها را بفهمند مخصوصاً اگر توانمندی این را داشته باشه که تا حد امکان فرایند کاری رو به صورت end to end مدیریت کنه.

اگه بیاد یک وظیفه خاص شبکه را بحث کنه بیاد به شکل کارکردهای مدیریتی سطح بالا موضوع را ببیند مثلاً یک سیستم customer care که هوای مشتری رو داشته باشه سرویس را بگیره

همه اینها مواردی هستند که یک وندور نمی تونه به اونها ورود کنه چون اصلاً نمیدونه شبکه من چی هست ولی اپلیکیشن وندور ها میتونن

در این nms ها یکسری فیچرها هست که حالت رقابتی ایجاد می کند مثلاً یک فیچر بحث اینکه فلان تجهیز مالتی وندور کار کنه یا customizable باشه یعنی بتونه اونجور که دلمون بخواهد برنامه ریزی بکنیم یا فانکشنالیتی های مدیریتی زیاد باشه و قابلیت های بیشتری به ما بده یا استفاده ازشون راحت باشه همه اینها جزو مواردی هست که در این بیزینس تعیین کننده است که مثلاً تو چه حوزه ای میخواه کار کنه

## System Integrators

- Make a business out of network management
  - How when NM Application providers develop the tools
  - Because of, in real world
    - No one tool or application can do every management tasks*
    - → Multiple applications for different purposes
- These applications manage the same network (from different aspects); hence, should be integrated, because
  - Work on the same databases
  - Used in the same workflow procedure
- While there are many management standard protocols and interfaces, in real world
  - Applications don't work together as easy as it seems
  - NM users need more integrated functionalities

دسته دیگر از این بازیگرانی که در nms برای ما مهم هستند دسته سیستم اینتگریتور ها هستند دسته ای که به دنبال تجمیع هستند.

خیلی علاقه مندی در سازمان ها به وجود آمده که به سمت یک اینتگریشن یا تجمیع نرم افزاری حرکت کنند

یک قسمت خیلی مهم در این فرایند اپلیکیشن های nms است ، ما تجمعیع در حوزه ابزارهای مدیریت شبکه نداریم و هنوز اپلیکیشنی نیومده که تمام ابزارهای مدیریت شبکه را داشته باشد. پس اگر ادمین nms یک شرکت باشیم باید از چند ابزار مدیریتی در کنار هم استفاده کنیم تا بتوانیم شبکه را مدیریت کنیم

آیا کسی به این فکر نکرده که پروتکل های مدیریتی را با هم تجمعیع کنن؟ چرا، خیلی از ابزارهای مدیریت شبکه اینترفیس هایی رو دارند اما موضوع اینجاست که پیاده سازی های متفاوت و ورژن های متفاوتی که وجود داره در عمل این ها را بخواهیم به هم وصل کنیم در نسخه های مختلف مشکل دارند و راحت کار نمی کنند در حالی که کاربر nms نباید لنگ این بماند که چی با چی کار میکنه

## System Integrators

- Fill the niche between COTS (Commercial off-the-shelf) and custom development by network providers
  - Specific operations support infrastructure
    - Management applications to integrate
    - Operational context to integrate: enterprise information systems, ordering, b2b, ...
  - Develop software wrappers, protocol converter/gateways, API customization, ...
- Make a business out of management requirements that are specific only to particular management users

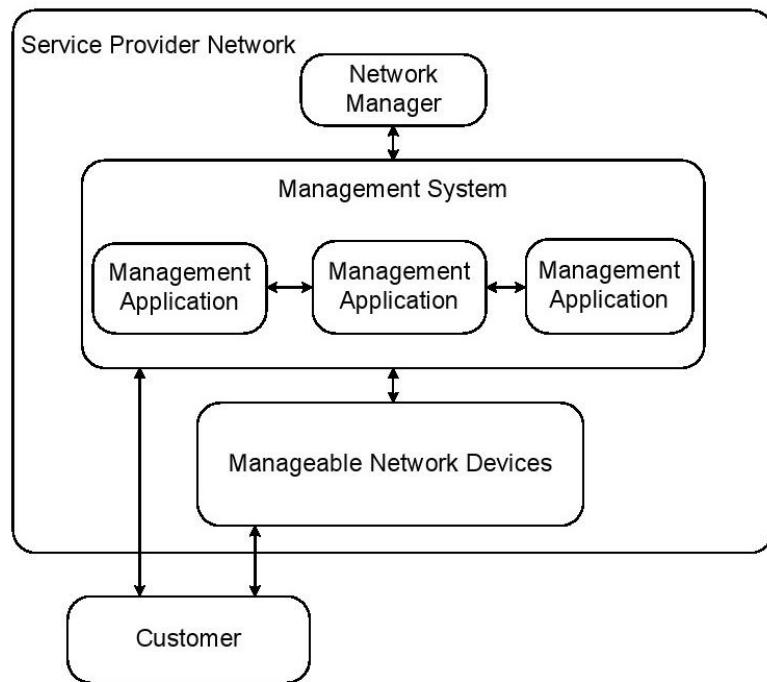
تجمعیع کنندگان سیستم ها بحث های اقتصادی را مطرح می کنند مثلاً میگن ما به شما یک سولوشنی می دهیم که از نظر اقتصادی مقرر رون به صرفه هست یا مثلاً فلان زیرساخت های شبکه میتونی فلان عملیات را مدیریت کنند یا مثلاً می تونه کارهای دیگری را در حاشیه انجام بده مثلاً میتونه تجمعیع بین ابزار مدیریت شبکه و بیزنس اون شرکت باشه یا در حوزه اردرینگ و سفارشاتش در حوزه کسب و کار سازمانی و...

و نکته مهم این که وقتی ما درباره اینتگریشن صحبت می کنیم یعنی من یک بستری را ایجاد کنم که چند تا اپلیکیشن که زبان های متفاوتی دارند به کمک اون بستر بتوان با هم صحبت کنند پس من آن بستری رو می

خوام که وظیفه تبدیل فرمت ها را داشته باشے زبان ها را به هم ترجمه کنه با این اپلیکیشن ها بتونم کار کنم  
یعنی من یک سری api برای این موضوع می خوام.

ایнтگریشن یک نیاز و مدیریتی هست که به وجود آمده که در برخی مناطق خاص برای کاربران خاص  
اینتگریشن یا تجمعی باید مطرح بشود.

## Put Altogether



قسمت پایین شکل مشتری هست و قسمت بالا servis provider یکسری تجهیزات  
قابل مدیریت داره یکسری اپلیکیشن های مدیریتی داره و یک اپلیکیشن مدیریت شبکه داره که همه اینها به  
هم مرتبط هستند و در فرایند کاری سازمان تاثیرگذار هستند.

## Example of Network Management Tools

### ➤ A typical NMS in a NOC



این تصویر مربوط به یک سیستم مدیریت شبکه‌ی بزرگ است که هر فرد جلوی خودش چند تا مانیتور دارد و از جنبه‌های مختلف شبکه را مانیتورینگ می‌کنند و در عین حال چند تا تلویزیون خیلی بزرگ دارند که به صورت لحظه‌ای پارامترهای مختلف را در قالب‌های مختلف رصد می‌کنند یک مرکز ناک یا network center هست که یک شبکه را مدیریت می‌کند

# Network Management Tools

- Management tools: management systems that network managers **interact** with
- User interface of the tools
  - Flow through systems may not have user interface at all
    - Provisioning tasks are done automatically, user never touches it
  - Text-based interfaces: CLI
    - Often preferred by power users
    - More productive, don't be slowed down by mouse clicks and navigation, scripting (automated configuration), ...
  - GUIs
    - Occasional users
    - "Legitimate" GUI uses: Monitoring, Visualization of large quantities of data, Summary reports

حالا می خواهیم ببینیم این ابزارهای مدیریت شبکه کجاست

یک ابزار مدیریتی وقتی میخواود به یوزر سرویس بده باید یک واسطه یا یک قالبی برای ارتباط باید داشته باشد که این قالب می تواند جنبه های مختلف داشته باشد مثلا ممکنه من یک دستگاهی داشته باشم یک اپلیکیشنی نوشته باشم که مثلاً ترافیک را بخواهد برای من جمع کند تقریباً این دستگاه را وقتی من میزارم تو شبکه و روی پورت مدیریتی هم میزنم که همه ترافیک را جمع کنه وقتی می خوام از این استفاده کنند تقریباً میشه گفت که این دستگاه سرخود میشینه کارашو میکنه و اینترفیسی برای من فراهم نمی کنه یا **network provisioning** که زمانی که سرویس های شبکه را دایر می کند خیلی از مباحثت به صورت اتوماتیک انجام میشه و ما به عنوان یک عامل انسانی دخالتی نمی کنیم این یک دسته هست.

دومین دسته اینترفیس هایی هستند که **CLI** هستند کلا تکست هستند کامند لاین هستند یعنی ما میریم تو محیط کامند و کامند می زنیم و جواب می گیریم که به صورت مشخص فقط یک آدم حرفه ای می توان از این کامند استفاده کنند یا آدم های حرفه ای سراغ این موضوع دارند و میگن سرعت نوشتمن ما و اجرای کامند خیلی بیشتر از سرعت یک روش معمولی هست.

دسته سوم اینترفیس گرافیکی هست که غالباً کاربر دوست دارن از این استفاده کنند و در قالب یک محیط گرافیکی اون نتایج مانیتورینگ نتایج مختلف شبکه جمع میشه و نمایش داده میشه.

## NM Tools Examples: Traffic Analyzer

---

- Inspect and “sniff” network traffic
  - Analyze individual packets to understand what’s going on
  - Low-level troubleshooting activities
  - Statistics
    - Per protocol
    - Per host
    - Multicast, Broadcast, Unicast
    - ...
- 

مثلاً ترافیک آنالیزورها، پکت اسنیفرها

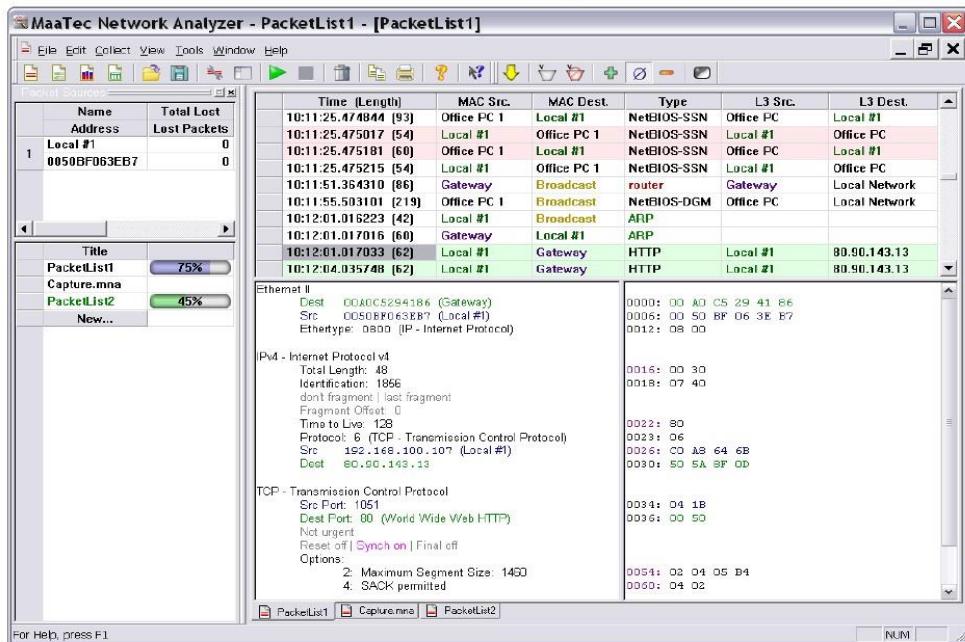
یک پکت اسنیفر میاد میشینه روی شبکه بسته‌هایی که نیاز دارد را جمع میکند و آنالیز می‌کند و جواب میگیرد و نتیجه را بر می‌گرداند و رفتار شبکه را گزارش میده هم بسته میتوانه اطلاعات رو نشون میده و هم کلی میتوانه نشون بده

به چه درد میخوره؟ در خیلی از جاها برای troubleshooting مفید است اگر ما در ک درستی از اینکه چگونه پروتکل‌ها کار می‌کنند داشته باشیم خیلی این موضوع میتوانه مفید باشد.

آنالیز میتوانه اطلاعات آمار جمع کنه و در جنبه‌های مختلف می‌تواند بررسی بشود به ازای پروتکل‌ها میتوانه مطرح بشه به ازای هاست‌ها میتوانه مطرح بشه اینکه آیا ترافیک من multicast, broadcast, unicast من

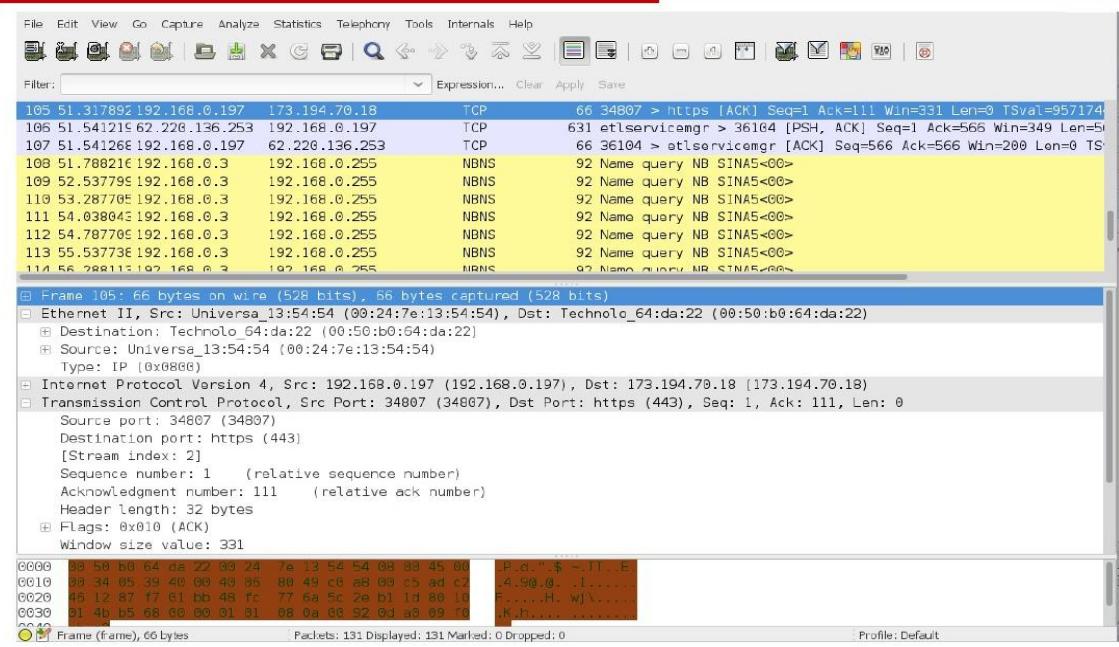
و...

# Network Analyzer: MaaTech



این ماتک هست که یک ابزار برای انالیز است

# Traffic Analyzer: Wireshark



این یک واپرشارک هست که روی کارت شبکه به ما میگه که اسنیف کنیم. هم به درد یک کلاس آموزشی میخوره هم به درد مدیرشبکه میخوره هم به درد یک مهاجم میخورد.

## NM Tools Examples: Device Managers

---

- View and manage individual devices one at a time
  - View statistics
  - View alarms
  - View configuration
  - Change & tune parameters
- Most basic interface: Telnet/SSH sessions, CLI
  - Can do anything on a per-device level
  - Often interface of choice for network administrators
- GUI, Web app more user friendly (easier to operate, but sometimes less productive for “power users”)
- Often specific to a particular vendor and device type

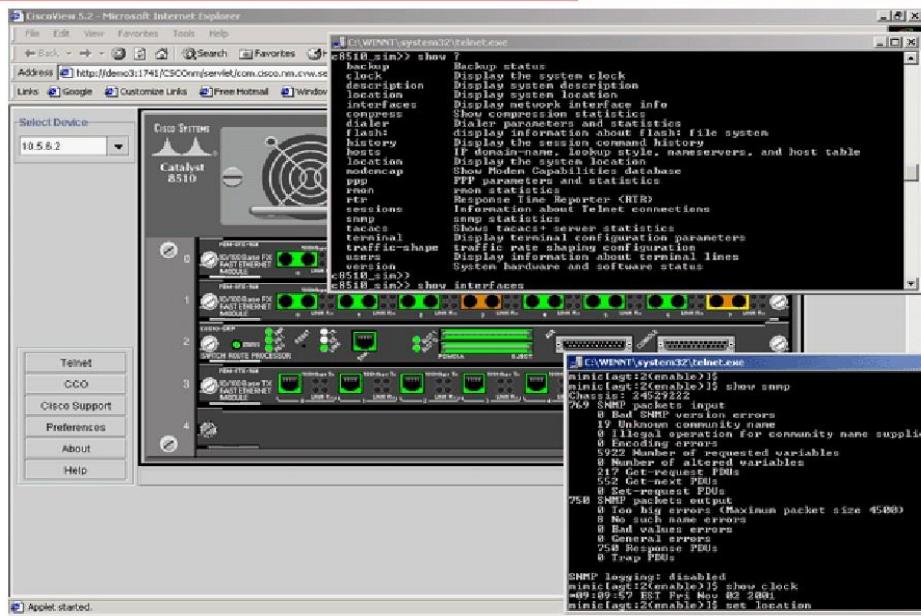
مدیرشبکه میتوانه بیاد از اینها استفاده کنه و آمارها را ببینه آلامرها را ببینه پیکربندی ها را ببینه پارامترها را ببینه و آنها را برای خودش تنظیم کنه.

پس ما می توانیم از پکت اسنیفر برای مدیریت هر دستگاهی به راحتی استفاده کنیم

تجهیزات در محیط های خودشون مثلاً در سشن های تلننت یا SSH از راه دور وصل میشون و بعد با کامند لاین یکسری اطلاعات را میشه گرفت پس اگر ابزار از دسته دیوایس منیجر باشد می توانیم این ها را داشته باشیم .  
مثلًا سیسکو محیط‌های وبی میده و دیگه بصورت کامند نیست

اینترفیس هایی که خود دستگاه به وجود می آید می تواند ابزاری برای مدیریت یک دستگاه باشد مثلاً محیط وبش بیشتر کاربر پسند هست و کمتر خطای داره و میحاط گرافیکی کلا کاربر پسند است.

# Device Manager: CiscoView



سیسکو یک محصولی به اسم Cisco view داره که می تونه از طریق اون وصل به تجهیزات شبکه وصل شد و کارهای آن را انجام داد خیلی گزینه ها را میتواند مدیریت کند

# NM Tools Examples: Element Managers

- View and manage individual devices in a network,  
Similar to device managers; however
- Provides overview of all (or many) devices in a network
- Allow to display devices on a logical topology map
  - Topology often not discovered but edited by an administrator
- Auto-discovers devices on a network
- Maintains state, e.g. database with network elements
- “Northbound interfaces” to interact with other systems
- Often specific to devices of a particular vendor

یک حوزه دیگری از NMS tools ها میتوانیم اسم ببریم بهش المنت منیجر میگیم

المنت منیجر یک چیزی شبیه دیوایس منیجر هست فقط دیوایس منیجر یک جنبه اختصاصی داره ولی المنت منیجر یکمی جنبه عمومی داره و یک فضای بزرگتر را به عنوان تارگت خودش میبینه و یک المنت منیجر میاد و در حوزه توپولوژی منطقی شبکه صحبت میکنه

در این ما به کمک المنت منیجرها دستگاه ها رو شناسایی می کنیم و اطلاعاتش را در یک دیتابیس ذخیره می کنیم و وقتی ذخیره کردیم به مدیر نشون میدیم

ما یکسری اینترفیس داریم مثل اینترفیس northbound که زمانی استفاده میشه که می خواهیم یک تجهیزی ، یک ابزاری، یک دیوایسی را به عناصر سطح بالا وصل کنیم یا به بقیه وصل کنیم.

یک باند جنوبی داره که خودش بره جمع بکنه مثلاً یک تجهیز مدیریت شبکه که از طریق باند جنوبی اطلاعات شبکه را جمع میکنه.

اینترفیس باند شمالی میشه که این اطلاعات را به ابزارها و مدیران دیگر شبکه بده. یک نکته وجود دارد که معمولاً حوزه المنت منیجرها vendor specific هستند چون شکل پیاده سازی در تجهیزات شرکت های مختلف متفاوت است استانداردی هم برآش نداریم

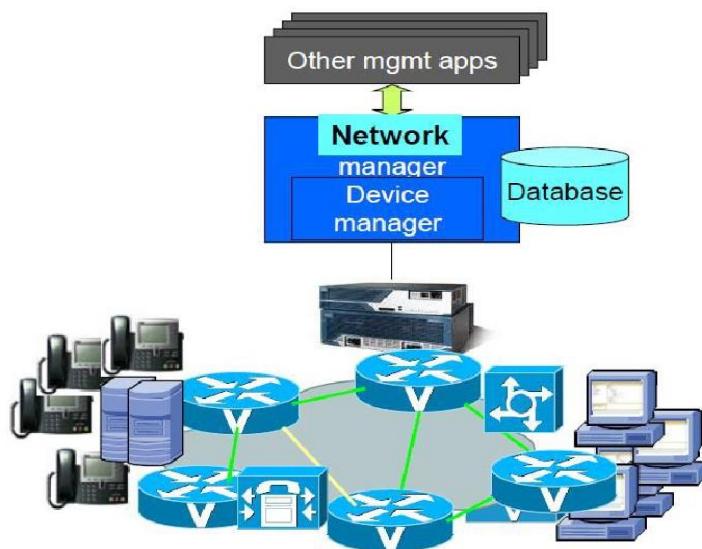
## NM Tools Examples: Network Managers

---

- Additional functions to deal with connectivity
  - Discover logical topology
  - Indicate state of connections
- Wider range of supported devices
  - Integration of multiple devices types from multiple vendors becomes a “must”
- Often built on the basis of vendor-independent management platforms

در سطح بالاتر نتورک منیجر داریم که گزینه های بیشتری را بررسی می کنیم علاوه بر اینکه توپولوژی منطقی تجهیزات را نگاه می کنه، وضعیت کانکشن ها را هم میتوانیم به دست بیاریم که این میشه نتورک منیجمنت که خیلی سطح بالاتر هست. در دیوایس منیجر آنقدر ریز می شدیم که پورت های سیستم رو داشتیم اما در نتورک منیجر معمولاً کلی تر هستند و یک حالت لاجیکال هستند تا فیزیکال به خاطر همین هم معمولاً دیوایس هایی که پشتیبانی می کنند حجم بیشتری دارند و حتی در هر وندور تیپ های مختلفی از آن تجهیزات وندور را دارند و اصولاً این هست که vendor independent است.

## Device/Element/Network Managers



این تصویر شبکه را نشون میده یک نتورک منیجر روی اون نشسته که این نتورک منیجر در دل خودش میتوانه دیوایس منیجر داشته باشه ولی در سطح بالاتر ما بهش میگیم نتورک منیجر و کنارش دیتابیس هست و از طریق اینترفیس شمالی ما می تونیم به بقیه ابزارهای مدیریت شبکه وصل بشیم.

المنت منیجر یک سطح بالاتر از دیوایس منیجر است، **device manager** یعنی ما در کانفیگ یک دستگاه برمی اما المنت منیجر یک سطح بالاتر از اون هست یعنی سعی میکنه توپولوژی منطقی شبکه هم به دست بیاره ولی بین دیوایس منیجر و نتورک منیجر هست چون در نتورک منیجر همه چیز منطقی میشه، دیوایس منیجر همه چیز خیلی خاص و فیزیکی میشه، المنت منیجر وندور اسپسیفیک است سعی میکنه بین منطقی و فیزیکی باشه.

## NM Tools Examples: Performance Analysis Systems

---

- Collect performance statistics
  - Monitor performance tends
  - Detect performance bottlenecks
  - Uses for
    - Service level management
      - Monitor if agreed-to service levels are being kept  
Examples: Delay, jitter, voice quality, ...
    - Proactive fault management
      - Detect problems that are brewing
      - E.g. deteriorating response times
    - Troubleshooting and diagnostics
    - Network planning
- 

مدیریت شبکه جنبه های بسیار متفاوتی دارند مثلاً یک سری از ابزارهای مدیریت شبکه هستند که کارشون اینه که از جنبه کارایی به سیستم نگاه کنند آمارهای گرافیکی را جمع می کنند آمارهای پایه را جمع میکنند، مانیتور می کند. bottleneck های سیستم رو نشون میدن.

فایدش چیه ؟

مثالاً گه ما یک sla بستیم و متناسب با این sla سرویس بدیم، در sla باید مثلاً تاخیر یا جیتر و ... را بدونیم چقدر هست.

در سیستمهای خطایابی فعال، زمانی که بحث سیستم خطایابی میشه یک حوزه ای هست که وقتی یک سیستم به مشکل بر میخوره از منظر کارایی دچار افت کارایی میشه و در واقع میتونه در بحث تشخیص خرابی ها به ویژه قبل از شروع خرابی میتونه مفید باشد. مثلاً یک ماشین را که استارت میزنیم میبینیم که ریپ میزنه که نشون میده که یک جایی یه چیزی مشکل داره و درست کار نمی کنه و می توانیم ببریم تعمیرگاه و درست کنیم یا اینکه می توانیم بگذاریم ببریم یه جایی وسط راه ماشین خراب بشه، سیستمهای تحلیل این حسن رو داره که میتونه به ما کمک کند قبل از اینکه به چالش بر بخوریم به ما اعلام performance

بکنے که در این محدوده فلان کارآمد پارامتر داره افت پیدا میکنے و مشکل داره و این موضوع در حوزه وجود مشکل را به خوبی کشف میکند response times.

بعد از اینکه واقع شد هم میتوانیم استفاده کنیم مثلاً ابزار ساده پینگ شاید 20 خط کدنویسی باشه وقتی پینگ می کنی و جواب نداده یعنی دستگاه خرابه پس در troubleshooting و diagnostics در تشخیص خطا و پیدا کردن موقعیت خطا مفید است. هم قبل از وقوع خرابی میتوانه به ما کمک بکنے که متوجه بشیم هم بعدش میتوانه کمک کنه.

در نتورک پلنینگ وقتی میخواهیم شبکه مان را گسترش بدیم و ببریم در حوزه های دیگه خیلی می تونه برای ما مفید باشد

## Collectors and Probes

---

### ➤ Probes

- Generation of data from the network
- Measurements: e.g. current service levels
- Offload management applications from high-volume routine tasks

### ➤ Collectors

- Collect raw data from the network
  - Traffic statistics
  - Periodic status snapshots
  - Events
- Filing, archiving, compression
- Format normalization
- Sometimes, data pre-aggregation, filtering, searching

چجوری باید آمار جمع کنیم؟ ما برای اینکار دوتا راهکار داریم یکی probes و یکی collectors

probes

در مدارها probes یک سری دستگاه هایی هست که مثلاً میگه ایا این قسمت از دستگاه کار میکنے یا نه. در شبکه probes را میزنیم یک سری اطلاعات را از شبکه جمع می کنیم و مثلا تروپوت دستگاه، تاخیر و... رو به ما میگه. خوبیش اینه که خیلی مزاحم کار شبکه نمیشیم.

کالکشن یعنی یک مجموعه را جمع آوری کنیم در کلکتورها کارشون اینه که میان یک سری داده های خام را از شبکه جمع می کنند بعد آنالیز می کنند و آمار ترافیکی ما رو میگه مثل این که وضعیت ترافیکی ما اینه رویدادهایی که در شبکه ما اتفاق می افته اینه و در قالب یک سری اسنپ شات به ما میده. پس کالکتور بیشتر از یک probes عمل می کند. کالکتور حجم زیادی از ترافیک رو میگیره بعد میتونه فایل درست کنه ، میتونه آرشیو درست کنه . به لحاظ کار فرمتی، فرمت های نرمال رو میشناسه .

تفاوت probes و collectors اینکه probes از اون روش های اکتیو یا فعال هست ولی کالکتور یک روش پسیو هست که میداریم روی شبکه اطلاعات را جمع کنیم و از روی همان اطلاعات با سرچینگ و فیلترینگ به خیلی چیزها می رسیم.

## Other Example Tools

---

- Work order management systems
    - Equipment installation, wiring, repair, replacement
    - Management of truck rolls
    - Interaction with inventory and ordering systems for spares
    - Interaction with workforce planning systems
  
  - Service order management systems
    - Entry of service orders
      - Adding, deleting, modifying a service
    - Orchestration of service order process, e.g.
      - Turning on billing
      - Credit card verification
      - Flow-through systems to provision the service
    - Tracking of service order status
- 

سیستم مدیریت شبکه یک فضای کوچک نیست، مثلا سیستم های مدیریت شبکه داریم که در حوزه work order هستند یعنی مثلاً یک سیستم داریم که همه چیز رو دربارش ثبت میکنیم مثلاً فلان دستگاه را فلان روز در فلان جا نصب کردیم الگوهای تامین نگهداریش مشخصه، این زمان جانشین شد یا مثلا در حوزه work order یا ordering inventory مخصوصات و کلان نقش ها و حوادث رو دارد. نمونه خوب management system ها در هواپیما است.

## Service order management system ها

یکسری فرآیند ما باید داشته باشیم که ببینیم کی سرویس‌ها را انجام بدیم، یعنی یک لیست داشته باشیم که بگیم یک گزینه کی باید add بشه، کی باید delete بشه، کی باید modify بشه، در این موارد ساده‌الارم داده بشه. بحث orchestration سرویس یعنی بحث مدیریت کل مجموعه سرویس، ما وقتی process را میخواهیم شروع بکنیم خصوصاً در حوزه سرویس دهی، همه اینها با هم لازمه مثلاً باید فکر صورتحساب هاش رو بکنیم که چه جوری هزینه هاش تامین میشه، چجوری محاسبه میشه، چه جوری اعتبار طرف از نظر مالی سنجیده میشه، باید اعتبارسنجی بشه و بعد روی فرآیند نظارت کنیم همه اینها جزو فرآیندهایی هست که ما در مدیریت شبکه نیاز داریم.

## Other Example Tools (cont'd)

---

- Address management systems
  - Number assignment and dial plan management systems
  - Helpdesk systems
  - Customer Relationship Management Systems
  - Workflow engines
  - Inventory systems
  - Intrusion detection systems
  - Billing systems
- 

سیستم‌های مدیریت شبکه خیلی وسیع هستند مثلاً ما سیستم‌های مدیریت آدرس داریم، سیستم‌های مدیریت اختصاص شماره داریم، سیستم‌های helpdesk، سیستم dial plan، سیستم CRM، سیستم workflow، سیستم inventory، سیستم IDS، سیستم biling داریم.

# Challenges

---

- Network management is a complicated process
  - Very wide
    - Various functionalities, Different objectives, ...
  - With many details
    - All protocols in networks need to be managed!!!
  - From different perspectives
    - Technical issues, Managerial issues, Human!!
- Challenges
  - Technical challenges
  - Organization and operation challenges
  - Business challenges

اصول سیستم های مدیریت شبکه چالش برانگیز و پیچیده است هستند.

چرا؟

1. خیلی گسترده هست و ما توابع و عملیات های مختلف داریم
2. جزئیات زیادی دارد پروتکل های زیادی دارد
3. از دیدگاه های مختلف و ادم های مختلف بررسی میشه.

# Challenges

- Network management is a complicated process
  - Very wide
    - Various functionalities, Different objectives, ...
  - With many details
    - All protocols in networks need to be managed!!!
  - From different perspectives
    - Technical issues, Managerial issues, Human!!
- Challenges
  - Technical challenges
  - Organization and operation challenges
  - Business challenges



چالش های مدیریت شبکه یکی از مسائلی که در بحث مدیریت شبکه وجود دارد این است که اصولاً یک فرآیند پیچیده‌ای پیش روی ماست که طول عرض خیلی زیادی دارد و هم جزئیات خیلی زیادی، به طور مثال یک ابزار خیلی ساده مانند وایرشارک بیش از ۷۰۰ پروتکل شبکه را می‌شناسد، سیسکو در بحث کیفیت سرویس یک ابزاری دارد که به کمک آن انواع اپلیکیشن‌ها را شناسایی می‌کند ترافیک‌های شبکه را بر اساس نوع شان دسته بندی می‌کند و در کلاس‌های مجزا می‌گذارد و لازمه این کار این است که تمامی پروتکل‌های شبکه را بشناسد به طور مثال TCP یک پروتکل ساده شبکه کلی داستان دارد

موضوع بعدی اینه که ما ببینیم از چه دیدگاهی داریم به سیستم مدیریت شبکه نگاه می‌کنیم

1) از جنبه فنی 2) از جنبه مدیریت شبکه 3) از جنبه کارمندی که در سازمان مشغول کار است

# Challenges Example: Technical

---

- The first and obvious set of challenges
  - NM system is a very big and complex SW, general issues:
    - SW architectural design issues
    - Appropriate technologies
    - Development & documentation
    - Test & troubleshooting
- NM context issues:
  - Application characteristics
  - Scale
  - Technology cross-section
  - Integration



پس ما با یک سیستم بسیار پیچیده با بازیگران گسترده‌ای که سطح درک متنوعی دارند در ارتباط هستیم پس قطعاً چالش داریم که چالش‌ها میتوانه در حوزه فنی و تکنیکی باشد در حوزه فرآیندهای کسب و کار باشد یا در حوزه بیزینس شرکت باشد

به طور مثال در دانشگاه کلاس‌های آموزش مجازی

سیستم مدیریت شبکه یک نرم افزار است، یک نرم افزار بسیار پیچیده که به یک معماری نرم افزاری نیاز دارد و یک سری تکنولوژی‌های متنوع را باید پشتیبانی کند. ۱) معماری نرم افزاری ۲) یک سری تکنولوژی‌های متنوع ۳) قابل توسعه و مستندسازی ۴) قابلیت تست و خطا یابی

این موارد در مورد اپلیکیشن هست. حال ما بعد از تولید نرم افزار باید برروی شبکه اجرا کنیم که با چالش‌های جدیدی برخورد می‌کنیم

به طور مثال مشتری یک سیستم NMS می‌خواهد با این ویژگی‌ها ۱) آیا این ویژگی‌ها در برنامه هست ۲) به یک اپلیکیشن نیاز دارم با scale خاصی ۳) بحث تکنولوژی cross-section (به طور مثال با زبان برنامه نویسی پایتون می‌شه یک نرم افزار سریع نوشته ولی تعداد کاربر زیاد را جواب نمی‌دهد برای کارهای بزرگ به درد نمی‌خورد باید از اسمبلی استفاده کنیم) پس هر تکنولوژی را نمی‌توان استفاده کرد و انتظار داشت خوب جواب دهد ۴) تجمیع ( integration ) سیستم مدیریت شبکه را با بقیه ابزارها ترکیب می‌کنیم اپلیکیشن‌های متفاوت در شبکه با هم تبادل اطلاعات داشته باشند بتوانند با هم کار کنند

# Technical Challenges: Application characteristics

- NM is composed of different functionalities (e.g., FCAPS)
- These functionalities are implemented by specific applications
  - Have own requirements and characteristics from SW engineering point of view
- Some example (common) characteristics
  - Transaction-Based System Characteristics
  - Interrupt-Driven System Characteristics
  - Efficient Data Analysis System Characteristics



59



ویژگی های برنامه (چالش فنی) میخواهیم از منظر ویژگی های اپلیکیشن به NMS نگاه کنیم

به طور مثال FCAPS

از دیدگاه کامپیوتری ها سیستم مدیریت شبکه باید شامل FCAPS باشد، آیا سیستمی که ما می خواهیم باید ۵ حوزه را پوشش دهد ما برای پوشش FCAPS با سیستم خیلی گسترده‌ای در ارتباطیم به طور مثال برای پوشش Fault باید مشخص شود که تا چه محدوده ای را می‌تواند پوشش دهد.

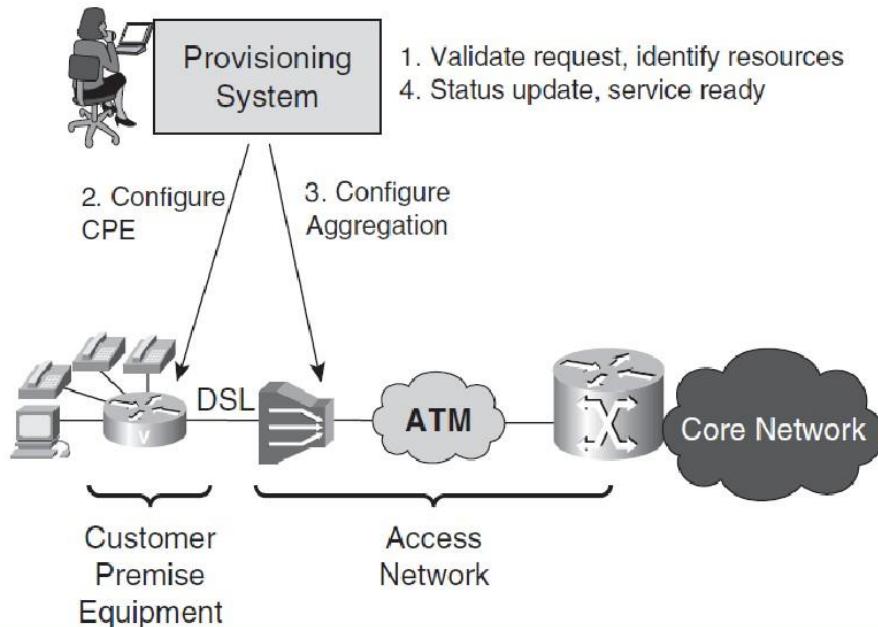
مثال: سیستم مدیریت شبکه باید یکسری آمار رو در بیاورد و در صورتی که مشکلی وجود داشت اعلام کند. جریانی از اطلاعات به یک سیستم تحلیل داده وارد میشود که باید آنها را تحلیل و استنتاج کند

الف) چگونه اطلاعات را جمع آوری کند؟ transaction base کار کند، یعنی هر موقع اتفاقی افتاد یک تراکنش ثبت و ذخیره می شود

ب) وقتی اتفاق مهمی افتاد، یک وقفه رخ میدهد، و بگوید چنین اتفاقی افتاد.

## Transaction-Based Characteristics

- Network configuration for service provisioning
- Rollback in the case of any failure/error

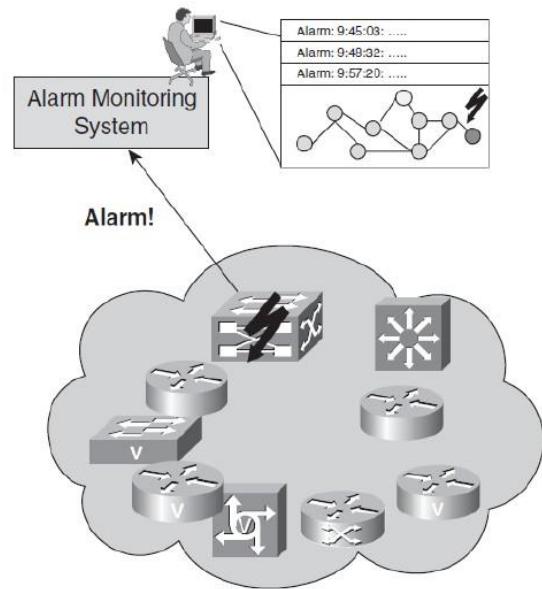


### ویژگی های تراکنشی Transaction

وقتی می گوییم که سیستم دارای ویژگی های تراکنشی باشد، مثل تراکنش های بانکی (هیچ تراکنشی را وسط کار رها نمی کند یا به انتهای می رساند یا بر میگردد به نقطه شروع ، وقتی کانفیگ یک سیستم مدیریت شبکه را می خواهیم بررسی کنیم شبیه یک تراکنش است پس یا باید به طور کامل اجرا شود یا اینکه برگردد به نقطه اول و این الگویی است که در تراکنش ها میبینیم

# Interrupt-Driven Characteristics

- Network health tracking is an objective of NM
  - Devices inform events to manager through alarm message → unsolicited message (interrupt)
- Challenges
  - Real-time processing & response
  - High volume of interrupts
    - E.g., a broken router
      - Multiple physical link failure alarms
      - So many service disruption alarms
      - Unexpected routing updates
      - ....



61



## Interrupt-Driven

مباحثی که در مورد سلامت شبکه هست (Network Health)

سیستمی که سلامت شبکه برایش مهم است، وقتی که یک Fault اتفاق افتاد بلافاصله اطلاع می دهد (درجه اهمیت)

مسائل مهمی مثل خرابی یک سوئیچ خیلی مهم هستند و بلافاصله باید اطلاع رسانی کرد

چرا؟ (چالش ها)

چون اصولاً مسائلی مثل Fault Real-Time-Processing از جنس همون موقع باید بهشون جواب داد.

نکته پس به صورت بالقوه با حجم خیلی زیادی از Interrupt ها مواجه هستیم.

## Efficient Data Analysis System Characteristics

- Operators need to analyze network performance to
  - Identify bottlenecks
  - Guarantee SLA
  - Evaluate utilization of network resources
  - Understand traffic patterns
  - Analyze trends for future network planning/design
- Challenges
  - Gathering large volume of data
  - Processing data
  - Statistical analysis and interference
  - Efficient & complex algorithms



62



### تحلیل داده

تحلیل داده در سیستم مدیریت شبکه از نان شب واجب تر است.

1) تشخیص Bottlenecks

2) تضمین SLA

3) بهینه سازی میزان استفاده از منابع شبکه

4) درک الگوی ترافیکی

## ۵) رفتار سرویس در شبکه

اینها همه مواردی هستند که در آن ها تحلیل داده وجود دارد

چرا تحلیل داده خیلی مهم است (چالش ها)

چون ۱) حجم داده خیلی زیاد است و یک سیستم معمولی نمی تواند به آنها پاسخ دهد ۲) توان پردازشی داده ها ۳) استخراج داده ها

## Technical Challenges: Scale

- Computer networks are large scale systems
  - Scalability is a fundamental requirement in NM
- Scalability needs proper design and technologies
  - NM for ~10 node is completely different from NM for ~1000 node!
- As a general rule scalability is a SW architecture problem rather than HW platforms
  - While hardware performance is increasing, NM processing requirements increase more



ابزار را برای چه شبکه ای می نویسیم به طور مثال تعداد افراد در یک کارخانه با گسترش کارخانه افزایش پیدا میکند و سیستم باید برای این افزایش کاربر پیش بینی های لازم را کرده باشد.

سیستم NMS را جوری باید طراحی کنیم که مقیاس پذیر باشد . بحث مقیاس پذیری را بیشتر در معماری نرم افزاری می بینند تا پلتفرم سخت افزار.

چرا سخت افزار باید رشد کند؟ این مسئله عادی هست ، ارتقاء جنبه های سخت افزاری گسترش جنبه های نرم افزاری را به دنبال دارد.

## Technical Challenges: Technologies

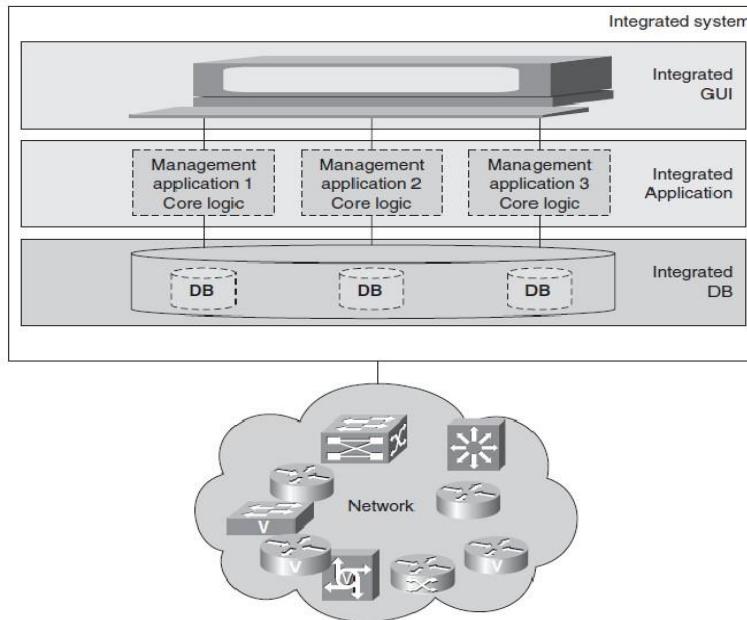
- Many different technologies need to be used to build a NM system → Many technologist with different expertise
- Examples
  - Information modeling
    - How network devices, links, service, management parameters, ... are modeled?
  - Database
    - How to design required NM DBs (devices, links, services, customers, configurations, ...)
  - Distributed computing
    - By definition, NM is distributed computing
      - Moreover, to achieve scalability & reliability, distributed computing is needed
  - Network (L4-L7) protocols
  - User interface
    - Visualization of large volume of data efficiently & user-friendly
    - Support large number of user for customer care software



۱) مدلسازی اطلاعات (۲) بانک اطلاعاتی همه ابزارها با یک دیتابیس کار نمی کند (۳) پردازش توزیع شده (۴) پروتکل های شبکه (۵) رابط های کاربری

# Technical Challenges: Integration

- Make different NM applications as if they were a “NM system”

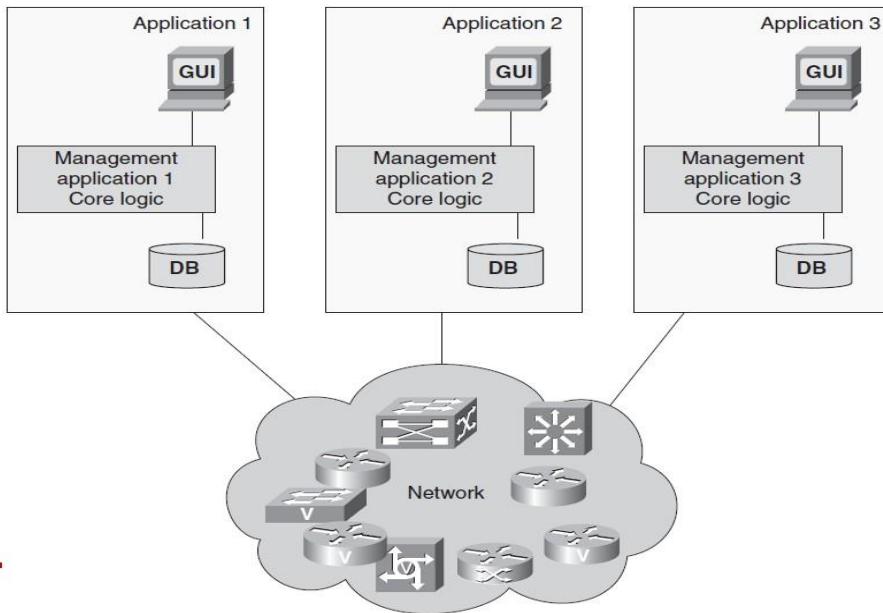


66



# Technical Challenges: Integration

## ➤ Swivel-chair syndrome



تجمعیع

در یک شبکه سیستم ها و اپلیکیشن های مختلفی داریم که ساختار های متفاوتی دارند هر کدام با دیدگاه متفاوتی به جمع آوری اطلاعات می پردازند

# Organization & Operations Challenges

---

- How human are organized for NM is an issue
  - Large enterprises with IT departments
  - Service provider networks (e.g., TIC)
- It is another dimension (rather than technology) for successful network management
- How to divide the tasks of NM?
  - Network planning, deployment, operation, maintenance, ...
  - It is not easy, eTOM tried to answer
- How to organize and manage people to perform tasks
  - Again is not easy, depends on human factors



# Business Challenges

---

- Different player in NM → Different objectives
  - Equipment vendors focus on managing own devices not high-end management functionalities
  - Service providers focus on business success thorough efficient NM
  - Enterprises need cost efficient NM
  - Network operators need user-friendly high-level NMS
  - Customers needs easy-to-use customer care portals
- NM tools providers and Integrator have their own business goal and constraints



68



## چالش سازمان و عملیات های سازمان

یک NMS را در اختیار چه کسی قرار دهیم (۱) فناوری سازمان (۲) service provider  
NMS چه کارهایی انجام میدهد؟ در network planning میتوانیم استفاده کنیم در بحث deployment  
یا پیاده سازی ها می توانیم استفاده کنیم در بحث operation و maintenance و خیلی موارد دیگر...

این سیستم مدیریت شبکه به چه درد میخورد چه کارهایی را میتواند انجام دهد؟ و چه کسانی مخاطب این سیستم هستند؟

# Telecommunications Services Evolution



## تکامل سیستم های مدیریت شبکه

می توانیم به سیستم ها و تکامل شان در حوزه telecommunication بپردازیم، چون همان فضا را برای ماتداعی می کند سیستم های ابتدایی در حوزه تلکام فقط برای انتقال صوت و بعداً صندوق پستی به این سیستم افزوده شد. با آمدن اینترنت سرویس های متنوع تر شد، به طور مثال تله کنفرانس سیستم های پرداخت بانکی و غیره. این حرکت به سمت جلوی سیستم ها فضاهای جدیدتری را در اختیار ما قرار دادند مثل مالتی مедیا text و location based to voice system این فضای متنوعی است و مرتب دارد افزوده می شود و روز به روز پیچیده تر می شود و ما از یک محیط سنتی عبور کردیم.

# Customer & Demand Evolution

## ➤ Traditional networks

- Residential customers & corporate networks
  - Simple process for requesting basic or enhanced services

## ➤ Today

- Business customers
  - Bandwidth and service on demand
  - Electronic interfaces for requesting services or changes, reporting trouble, and billing
  - Quick provisioning time and QoS



## تکامل مشتری و تقاضا

در شبکه های سنتی افراد برای برقراری ارتباطات از تماس صوتی استفاده میکردند که فرآیند های خیلی ساده ای بود، ولی امروزه فرق کرده است و مشتری برای یک سرویس ساده صوتی از بسترها مخابراتی استفاده نمی کند. برای کسب و کاری از این بستر استفاده می کنند که نیازمند یک سری تضمین هست ۱) پهنهای باند ۲) گزارش هایی که می گیرند ۳) هزینه هایی که دارند ۴) بحث کیفیت سرویس

# Management Functionality Evolution

- Traditional (PSTN) networks
- Circuit switching: F > C > A > P > S
  - Fault = service disruption
  - Configuration = service provisioning
  - Per call accounting = Business
  - Ignore performance since resources are reserved
  - No security



## تکامل عملکرد مدیریت

حال برای این شبکه ها میخواهیم سیستم مدیریت شبکه طراحی کنیم با دو تا شبکه روبرو هستیم (الف) شبکه سنتی تلفن (ب) شبکه های امروزی

شبکه های سنتی تلفن (PSTN) اگر بخواهیم FCAPS نگاه کنیم مخابراتی ها به این شکل اعتقاد دارند

F>C>A>P>S

به عبارتی امنیت در شبکه های سنتی اهمیتی نداشت و بی معنی بود ولی بحث Fault خیلی مهم بود که همیشه سرویس برقرار باشد. performance برایشان مهم نبود چون منابع رزرو شده بود. پیکربندی و اکانتینگ برای مخابراتی ها مهم بود چون کسب درآمد میکردند.

# Management Functionality Evolution

## ➤ Next Generation Networks (NGN)

## ➤ Data/Multimedia IP networks:

- S > P > A ~ C ~ F
- Security is the essential requirement
- Efficient resource utilization through Performance management
- Bulk bandwidth or usage based accounting
- Misconfiguration and faults are tolerable in some cases



## تکامل عملکرد مدیریت

کم کم در ابتدای قرن جدید مفهوم NGN مطرح شد (شبکه های هوشمند) مخابراتی ها در تلاش بودند که از دنیا IP عقب نماند چون سرویس های مبتنی بر آی پی خیلی سریع داشتن جانشین می شدند به همین دلیل مخابراتی ها NGN sonnet , NSN SDH را مطرح کردند

(IP رو بر روی شبکه های مخابراتی منتقل میکنند)

از سال 2005 با ورود wimax، و نسل 4 تلفن های همراه (ip back bon ) ضمینه ساز شکست برای مخابراتی ها شد.

در دنیای آی پی FCAPS ، به شکل زیر تغییر کرد

S > P > A ~ C ~ F

در حوزه آی پی مهمترین بحث امنیت و بعد کیفیت سرویس، بحث A , C , F در یک سطح بودند چون منابع ارزان شده بود و بحث اکانتینگ خیلی مهم نبود.

بحث Fault و Misconfiguration در حوزه آی پی خیلی کمرنگ شد چرا؟ به دلیل یک ویژگی خیلی ساده در حوزه آی پی که اگر مسیری را از دست می‌داد و همچنان مسیری به سوی مقصد وجود دارد تضمین می‌کند که ترافیک به سمت مقصد ارسال شود برخلاف شبکه‌های مخابراتی شبکه‌های آی پی fault tolerance هستند.

## Network Management Vision Evolution

### ➤ Traditional management

- Element management
  - Get/Set device management parameters
  - Get alarms from equipments

### ➤ Current trend (vision)

- Service & Business management
- Process & Workflow management
- TeleManagement Forum (TMF) is the driving force behind this vision



## تکامل چشم انداز مدیریت شبکه

در بحث مدیریت شبکه های سنتی یک سری پارامترهای Get, Set داشتیم. یک سری پارامتر ها رو set میگردیم و یک سری alarms میگردیم) به این قالب Element management Get ها رو میگویند،

چون ما با یک شبکه sercet switching در ارتباط هستیم می دانیم که تضمین وجود دارد. ولی در حال حاضر ما بحث ۱) مدیریت Service & Business را داریم ۲) بحث مدیریت Process & Workflow را

داریم ۳) TeleManagement Forum (TMF)

# Basic Concepts

## Network Management

Spring 2013

Bahador Bakhshi

CE & IT Department, Amirkabir University of Technology



*This presentation is based on the slides listed in references.*



# Outline

---

- Introduction
- Managed Devices: Agents and MIBs
- Managing Systems
- Management Network
- Management Support Organization



2



# Introduction

---

## ➤ Until now, we know

- What network management is
- Why it is important
- What Challenges are
- Who major players are

## ➤ What does NM consist of?

---



4



ما در فصل ۲ به یک سری مفاهیم پایه می پردازیم.

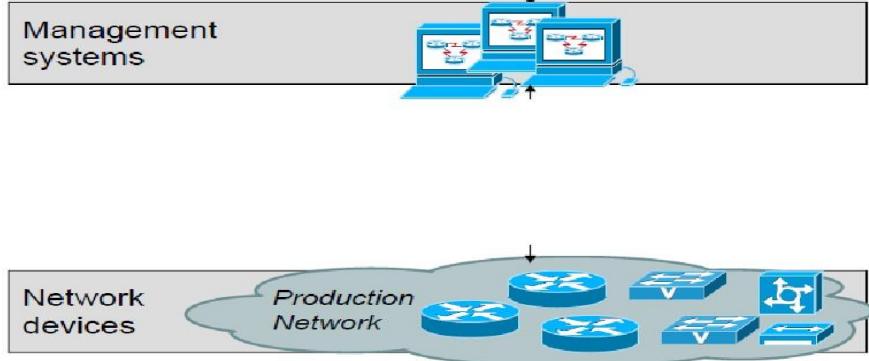
1) سیستم مدیریت شبکه چی هست؟

2) چه چیزی را باید مدیریت کنیم؟

3) چگونه مدیریت کنیم؟

4) چه دستگاه و چه سیستم مدیریت کننده ای استفاده کنیم؟

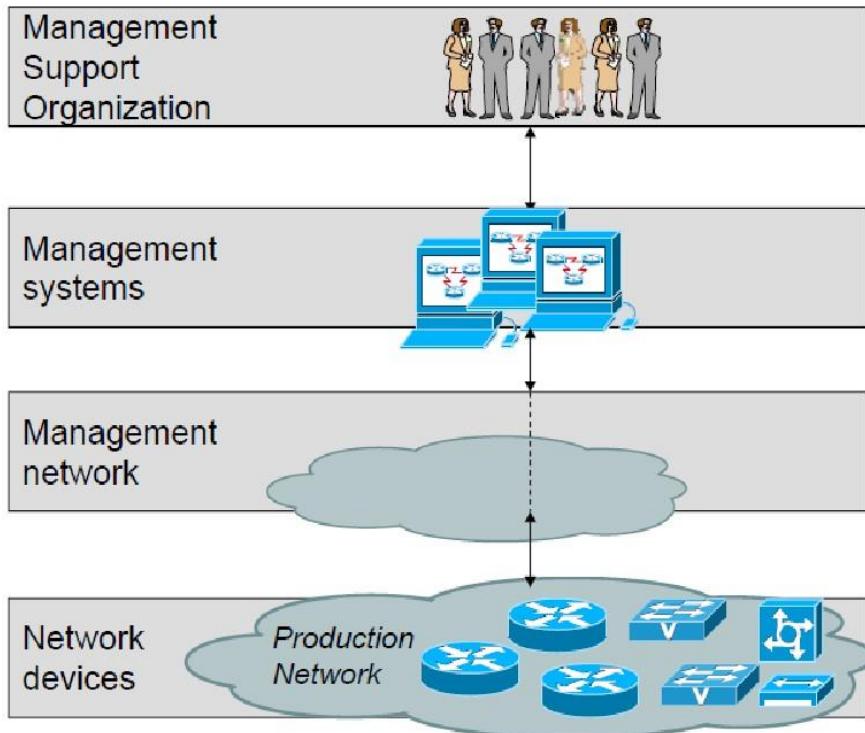
## The Basic Ingredients of Network Management



5

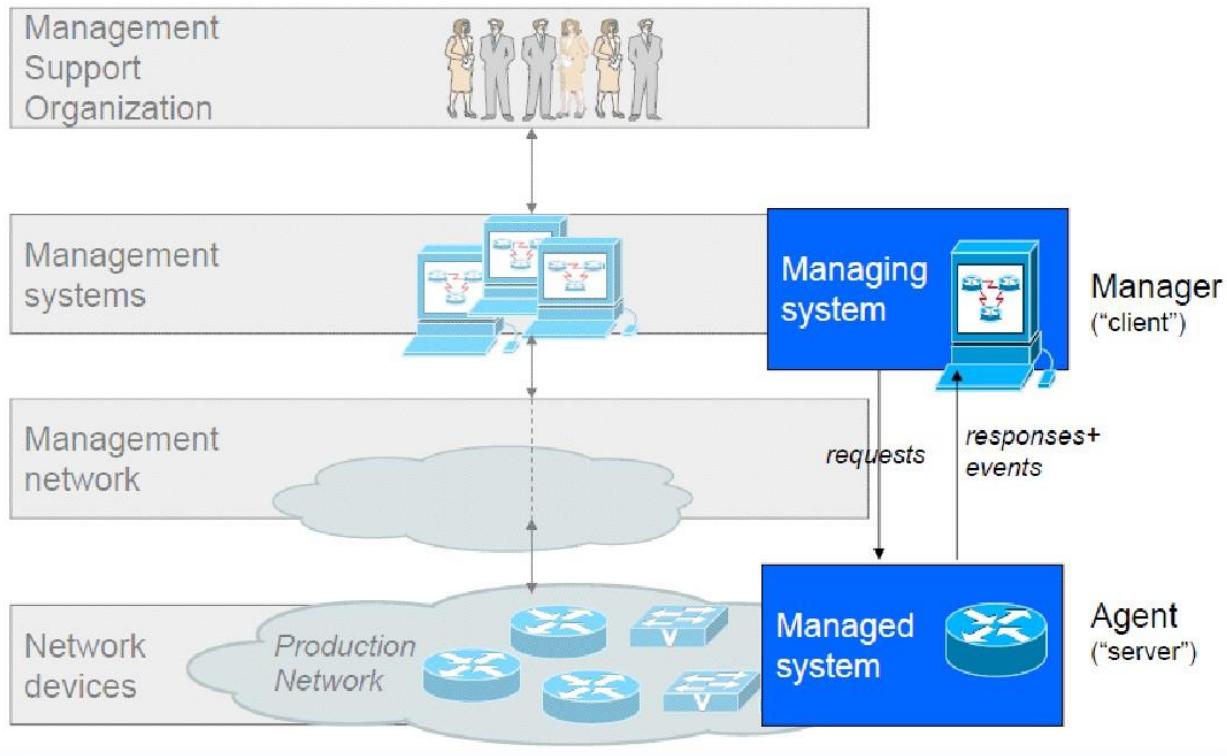
تا الان فهمیدیم که سیستم مدیریت شبکه چی هست چه چالش هایی دارد و مهمترین بازیگرانش چه کسانی هستند حال می خواهیم بدانیم خود سیستم مدیریت شبکه چه چیزهایی دارد در واقع یک شبکه داریم که مخصوص کسب و کار هست و قرار است یک سیستم مدیریت شبکه را بگذاریم که این شبکه را نظارت کند پس نیاز به بستری برای پایش داریم به این بستر management network شبکه مدیریتی گفته می شود.

# The Basic Ingredients of Network Management



یکسری سیستم های مدیریت شبکه داریم یک سری مدیر بالای سر سیستم های مدیر شبکه است که گزارش های سیستم مدیریت شبکه را مشاهده می کند. پس یک سیستم مدیریت شبکه که می خواهد یک سری دستگاه را مدیریت کند. به سیستم مدیریت شبکه (سیستم مدیریت کننده) **managing system** می گوییم. و به دستگاه هایی که مدیریت می شوند (سیستم مدیریت شونده) **managed system** گفته می شود.

# Basic Management Architecture



8

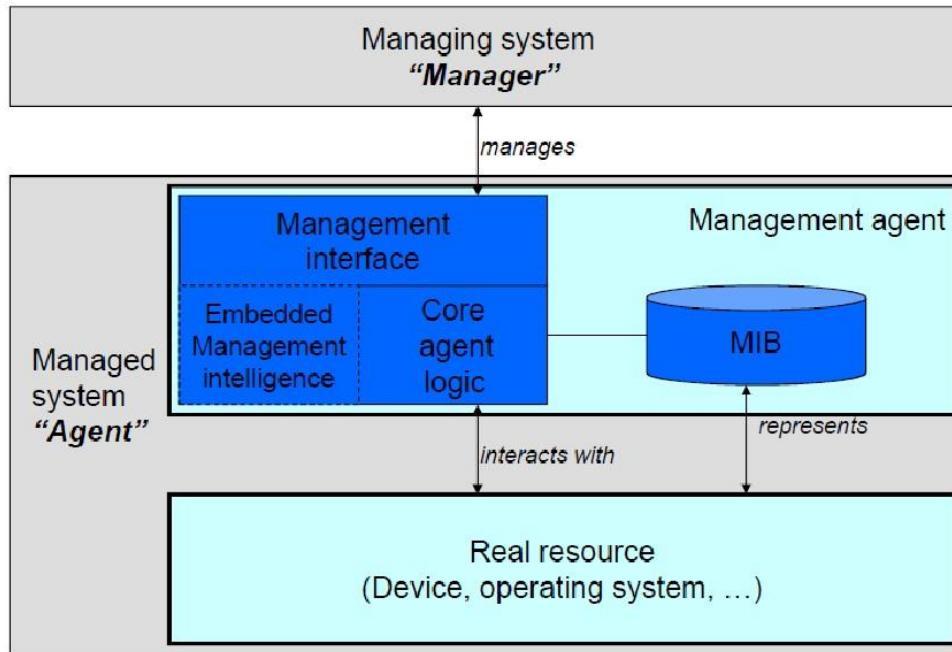


به این نکته توجه کنید که سیستم های مدیریت شده سرور یا Agent می شود گفته می شود

به سیستم مدیریت شبکه manager client یا گفته می شود برعکس اون چیزی که ما فکر میکنیم.

# Managed Devices

## ➤ What's in a managed system



11



Managed devices

در این سیستم یک سری **real resource** داریم (منابع واقعی مثل رم و سی پی یو، فضای ذخیره سازی) و یک سری عناصر هوشمند دارد که سیستم های واقعی رو مدیریت میکنند. یک **core agent logic** دارد که به صورت مستقیم با منابع واقعی کار میکند. سرور در زمان غیر فعال بودن، اطلاعاتی رو که به دست می آورد در یک دیتابیسی به نام **mib** ذخیره میکند. و همه این فضا رو **agent** مدیریت میکند.

### What's in a Managed System

#### ➤ Management interface

- Allows manager to interact with agent
  - CLI, GUI, API, ...
- Typically, is a management **protocol**
  - Application layer protocols with management primitives
    - Report an event, Apply a configuration, Export an accounting detail record, ...
  - Managers use SDK/APIs to hide protocol specifics from application developers
    - Marshalling/unmarshalling parameters



اولین چیز مورد نیاز در مدیریت ، یک اینترفیس میباشد که از طریق آن میتوان به سیستم تحت مدیریت یا API متصل شد اینترفیس می تواند Command Line Interface (CLI) یا از طریق صفحه وب و یا agent باشد . روی اینترفیس باید یک پروتکل مدیریتی اعمال شود این پروتکل از لایه اپلیکیشن می باشد این پروتکل باید رویدادها را گزارش دهد و پیکربندی را تنظیم کند و یک سری از اطلاعات accounting را export کند . با استفاده از برنامه نویسی های component SDK/API و استفاده از معتبر ، میتوان این پروتکل را از دید توسعه دهندهان مخفی نگه داشت .

## What's in a Managed System (cont'd)

- Multiple management interfaces exist, often on the same device
  - Examples: CLI, SNMP, Netconf, syslog, Netflow
  - Some have different purposes
    - Collection of data for accounting purposes
    - Configuration/provisioning of a box
    - Monitoring for alarms and faults
  - Some have overlapping purposes
    - Historical reasons
    - Network manager preferences/ user choice



13



سیستم مدیریت شبکه می تواند همزمان چندین اینترفیس داشته باشد. مثلًا میتوانیم CLI,SNMP,Netconf,syslog,Netflow را همزمان داشته باشیم که هر یک از اینها یک پروتکل جداگانه هستند. هر یک از اینترفیس‌ها ممکن است برای اهداف مختلفی استفاده می‌شود مثلًا یک اینترفیس ممکن است برای configuration و دیگری برای monitoring یا provision یا accounting باشد. مشاهده خطای استفاده شود. بعضی از این اهداف ممکن است با یکدیگر همپوشانی داشته باشد مثلًا ممکن است بحث performance یا امنیت با یکدیگر همپوشانی داشته باشند یا بحث‌های fault و accounting همپوشانی داشته باشد. مثلًا در حملات DDOS که حمله بسیار خطرناک و غیر قابل کنترل است می‌توان با بحث‌های کنترل کیفیت سرویس و محدود کردن load سرور جلوی این حمله را گرفت در واقع موضوع امنیت و کیفیت سرویس با هم همپوشانی دارند. البته این همپوشانی به کاربران و user‌ها هم بستگی دارد.

## What's in a Managed System (cont'd)

- MIB – Management Information Base
  - Conceptual representation of the managed device
  - Management operations are directed against this conceptual view
  - A “model” of the device, or rather an instance of a model
    - Think about configuration parameters, state, performance statistics as entries in a the database
      - Ports of a router are represented as a table
      - Each port is a row in the table
      - Each column is an attribute of port (# of send packets, IP, mask, ...)
  - Don't confuse with a “real” database
    - Data represents real resources (e.g. device registers, hardware state, policies for device behavior)



14



این اطلاعات در (MIB Management Information System) که یک دیتابیس مفهومی است ، ذخیره می شود. MIB یک نمایش مفهومی از دستگاهی که در حال مدیریت شدن است می باشد. در اینجا ما یک مدل از آن دستگاه را بصورت مفهومی می سازیم. این مدل ، یک سری از پارامتر در مورد پیکربندی ، وضعیت ها ، آمارهای ترافیکی و غیره را دارد که این مقادیر در جدول قرار می گیرند . مثلاً این جدول می تواند اطلاعات پورت های روتر را داشته باشد به این صورت که سطر ها پورت های روتر و مقدار ستون های این جدول ، پورت ها شامل IP ، Mask ، حجم ترافیک ارسالی ، سرعت ، میزان بسته ارسالی و غیره باشد . که نسبت یک دیتابیس معمولی ما فضای متفاوتی را تجربه می کنیم .

# MIB

## ➤ An overloaded term

### ➤ Here:

- A conceptual representation of a managed device by a management agent
- The collection of all management information that is exposed by a network element to managing applications (the view of management information)

### ➤ SNMP:

- Management information accessed through an agent
- A specification of a management information model to be implemented by SNMP management agents



15



یک اصطلاح کلی است که برای تمام پروتکل های شبکه کاربرد دارد . یک MIB دیگر وجود دارد که یک اصطلاح خاص است . پس ما یک MIB داریم که واژه مفهومی از اجزای تشکیل دهنده شبکه است و یک MIB داریم که پایگاه داده اختصاصی پروتکل مدیریت شبکه SNMP است . ( مثلاً در جایی می توان گفت API که مفهومی کلی است و در ویندوز هم به صورت اختصاصی API داریم ولی در لینوکس ممکن است اسم دیگری داشته باشد ) . MIB داخل SNMP دقیقاً یک پایگاه داده ای است که مدل مفهومی از دستگاهی که در حال مدیریت آن هستیم برای ما ایجاد می کند و اطلاعات مدیریتی که داخل آن دستگاه است را در MIB می ریزیم و از طریق MIB می توانیم به آن اطلاعات دست پیدا کنیم البته MIB در پروتکل های دیگر ممکن است نام دیگری داشته باشد . زمانی که agent می خواهد اطلاعاتی را بخواند یا بنویسد از این MIB استفاده می کند .

SNMP موجود در MIB مدل خاصی از اطلاعات مدیریتی است که توسط ایجنت های مدیریت کننده MIB مورد استفاده قرار می گیرد .

## What's in a Managed System (cont'd)

### ➤ Core agent logic

- Naming/addressing of management information
  - E.g. Management Information Tree
- Translation between internal and external representations
- Interact with OS to perform management requests
  - Get & Set parameters
  - Get asynchronous notification → Alarm



16



وظیفه agent جمع آوری اطلاعات و مدیریت device یعنی تعریف یک منطق برای agent ، که اطلاعات را از سیستم مدیریت شونده می گیرد و با SNMP سرور ارتباط برقرار می کند و در واقع یک مترجم است که زبان تجهیزات بیرون از خودش را به زبان ماشینی که مدیریت می کند ، ترجمه می کند و برعکس ( چون اینها دو زبان مختلف دارند ) در بحث شبکه ما زبان مخصوص خود را داریم و در داخل OS هم ما زبان و بیان خود را داریم . در درون سیستم ، agent باشد . مثلاً وقتی مقادیر device CPU Temp یا Ram Utilization یا CPU Utilization را بخواهیم drop rate ارتباط برقرار کرده و این اطلاعات را بدست می آوریم که برای اینکار باید Core logic agent را بخواهیم کند و یا اینکه بتواند آنرا handle کند . Get request و Set request همچنین باید معنا و مفهوم اسامی و آدرس هایی که در آن اطلاعات وجود دارد را نیز بفهمد ، مثلاً باید بداند

پورت شماره ۵ اترنست کدام است . ما یک درخت اطلاعات مدیریتی (Management information tree) داریم و این مفاهیم و آدرس ها در آن معنا و مفهوم پیدا می کند

## What's in a Managed System (cont'd)

### ➤ Management intelligence (optional)

- "Value-added" functionality for the purpose of facilitating management
- Automation of certain procedures
- Correlation and filtering of events
- Aggregation and preprocessing of management information
  - e.g. flow information, statistical analysis
- Measurement of service levels
- Anomaly detection, Intrusion detection
- ...



17



علاوه بر مباحث مدیریتی ، برای agent گزینه های optional هم می توان در نظر گرفته شود. مثلاً حوزه پولی و ارزش افزوده (Value added functionality) یا اتوماتیک کردن بعضی از رفتارهای سیستم ، یا تجزیه و تحلیل ارتباط بین رویدادها ، یا بحث های مربوط به آمار و ارقام و اطلاعات را پیش پردازش و مجتمع کرده و آنها را استخراج کنیم و یا بحث تشخیص نفوذ انجام دهیم

## What's in a Managed System (cont'd)

- Manageable resources
  - Hardware components; e.g., NIC
  - Software components; e.g., OSPF daemon
- In addition to their own functionalities, provide manageability facilities
  - Management parameters
    - Subset of the parameters are standard
  - Management interface
    - Usually vendor specific



18



در داخل device مدیریت شونده ما گزینه های دیگری از جمله مدیریت هستند چه نرم افزاری

یا سخت افزاری را داریم، مانند کارت شبکه و یا پروتکل OSPF

و یا توابعی که مخصوص device مدیریت شونده هستند مثل مدیریت پارامترهای مدیریتی و یا واسطه های

مدیریتی (پارامترها سعی شده استاندارد باشند ولی در مورد واسطه ها بسته به نوع وندور متفاوت هستند)

## Agents vs. Resources

- A managed device can contain multiple management agents, each realizing a different management interface
  - Often specialized towards different tasks: configuration, monitoring, accounting...
  - Each management agent offers its own view of underlying resource
    - Example: reference to an interface in a CLI, an API, a URL, an SNMP object
- All the agents manage the same resources

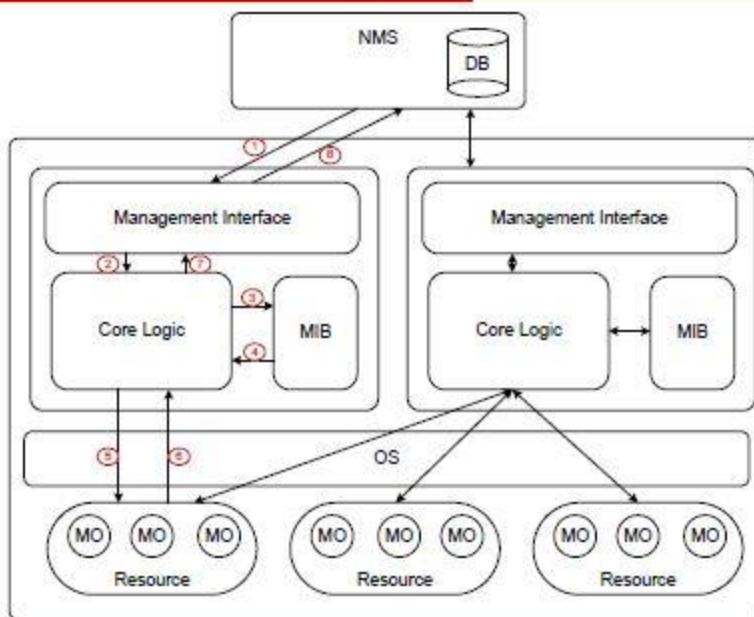


19



در یک device ممکن است یک یا چند agent داشته باشیم چون هر کدام ممکن است کارکردها و وظایف مجزا داشته باشد مثلاً یک configuration agent فقط جنبه monitoring یا جنبه accounting را داشته باشد. هر agent که از دیدگاه خودش subsystem های device خود را نگاه می کند مثلاً در محیط Command API یا URL یا resource خاص وصل شود و تعریف خاص داشته باشیم که مربوط به یکی از دستورات برای SNMP object خاصی است ولی در هر صورت هر agent دیدگاه خاصی دارد. این دستورات برای vendor های مختلف ممکن است مشابه هم باشند (ولی لزوماً یکی نیستند) و این دستورات کارکردهای متنوع و متفاوتی داشته باشند البته چارجوب تمام وندور ها مشابه و یکی است

## Summary



20

در نهایت گروهی از agent‌ها مشغول مدیریت یک سیستم هستند مثلاً در این شکل دو agent متفاوت وجود دارد که به یک NMS و DB آن در ارتباط هستند و از سمت دیگر هر دو با یک OS در ارتباط هستند و هر agent خود را برای خود MIB و core logic interface می‌باشد.

---

## Outline

---

- Introduction
- Managed Devices: Agents and MIBs
- **Managing Systems**
- Management Network
- Management Support Organization



## What's in a Managing System

- Are all the SW applications used for NM
- Software engineering architecture
  - Model-View-Controller a popular design pattern
  - N-tier architectures decouple communication – application – interfaces
  - General concepts of modern software engineering of large **scale** applications apply
    - Distribution
    - SOA: Loose coupling
    - High-availability



22



سیستم مدیریت کننده: یک NMS Server داریم که شبکه را مدیریت می‌کند. معماری این شامل یک کنترلر (view model controller) است و اینکه ما معماری چند سطحی (N-tier) داریم که شامل سطوح communication-application-interface هستند.

چرا ما وارد بحث مهندسی معماری نرم افزار می‌شویم؟ از آنجاییکه این سیستم سریار زیادی را ایجاد می‌کند در عین حال نیاز شدیدی به آن است در این سیستم NMS مسئله مقیاس پذیری (Scaling) که در آن تعداد زیادی Device را بتوانند پشتیبانی کند بسیار مهم است چون معمولاً این حوزه distributed و توزیع شده است و در عین حال High Availability و SOA:loose coupling (معماری مبتنی بر سرویس) است.

( SOA:

# What's in a Managing System

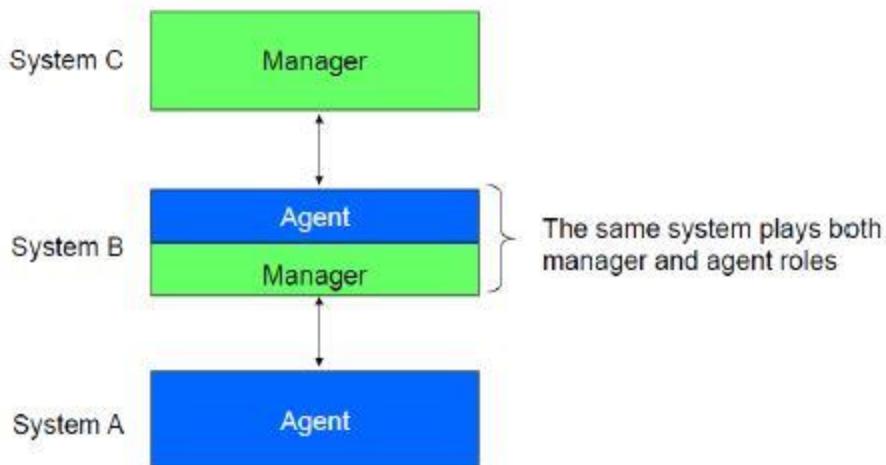
---

- Common components
  - Communication handlers
    - Event handlers
    - Data collectors
    - ...
  - Abstraction layers to normalize interface variations
  - Databases (to store network inventory)
  - Workflow engines
  - GUI components



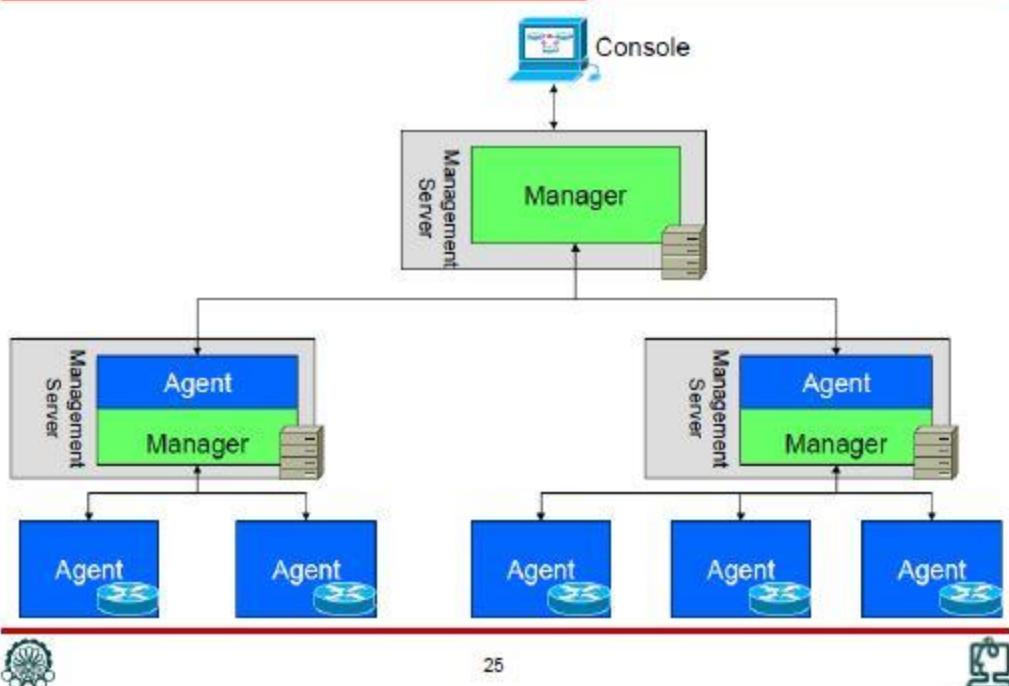
در سیستم مدیریت کننده یکسری handle کننده ارتباط را داریم که ارتباطات event ها و data ها و ... را هندل می کند همچنین در یک سیستم مدیریت کننده می توان از سطوح انتزاعی استفاده نمود تا تغییراتی که در interface های مختلف رخ می دهد را بتوانیم مدیریت کنیم. مثلا می توان یک engine وجود داشته باشد که GUI و دیتا بیس را پردازش نماید

# Management Hierarchies



در اینجا سیستم مدیریت سلسله مراتبی مطرح شده است

## Example: MOM – Manager of Managers



25

در اینجا سیستم مدیریت سلسله مراتبی مطرح شده است . agent ها در پایین نمودار هستند و در قسمت B ما Management Server ها را داریم که در آن می توان با agent ی که در بالای آن قرار دارد به Management Server بزرگتر وصل شد. زمانی که شبکه خیلی بزرگ‌تر شود با یک سیستم نمی توان آن را مدیریت کرد و باید به سراغ سرور بزرگتری برویم و از سیستم مدیریتی چند سطحی و چند لایه استفاده نمود ( MOM:manager of manager)

# Outline

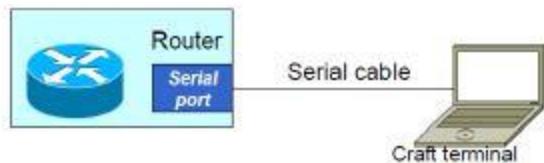
---

- Introduction
- Managed Devices: Agents and MIBs
- Managing Systems
- Management Network
- Management Support Organization



## Manager to Device Connectivity

- Connectivity between managing and managed systems?
- Multiple ways to connect a device to a management station
  - Through a dedicated port (console port)
    - For basic configuration & troubleshooting

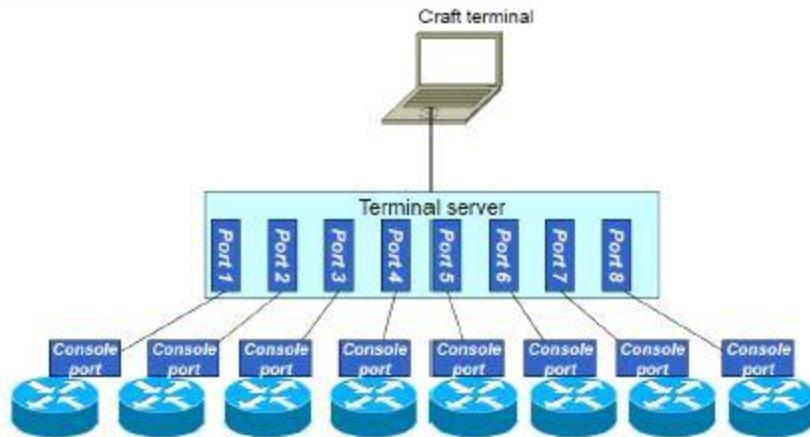


27

چگونه می توان سیستم های مدیریت کننده و مدیریت شونده را به یکدیگر متصل نمود؟

این دو سیستم در واقع دو کامپیوتر هستند و از روش های مختلفی می توان این اتصال را برقرار کرد در روش اول استفاده از پورت اختصاصی جهت مدیریت شبکه است مثلاً استفاده از کابل کنسول سریال که مخصوص اتصال به روتر برای انجام config است که این کابل سریال است.

## Manager to Device Connectivity (cont'd)



- Is not suitable for practical NM
  - Many terminal servers
  - Keep track which route is connected to which port
  - Serial port!!!



28



زمانی که ما مجموعه ای از تجهیزات داخل را در یک شبکه بزرگ داشته باشیم عملاً امکان استفاده از تعداد زیاد

پورت کنسول وجود ندارد و معمولاً Terminal Server دارای تعداد محدودی پورت ( مثل ۸ پورت ) هستند

و در شبکه ای که تعداد زیادی device وجود دارد عملاً استفاده از پورت سریال غیر ممکن است.

## Manager to Device Connectivity (cont'd)

- Connectivity between managing and managed systems?
- Multiple ways to connect a device to a management station
  - Through a dedicated port (console port)
  - Through a dedicated interface, with the device configured such that management traffic is passed through the interface
    - Two port types: Data & Mgt Ethernet interfaces
      - Different route cards: Supervisory engine card (mgt) & Line card (data)
    - Out-of-band management
      - Management traffic is not mixed with data traffic
    - Needs dedicated network for NM, Why??!!!



ایده دوم این است که به جای اینکه ما پورتی مشخصی داشته باشیم ، اینترفیس مشخصی داشته باشیم در این حالت ما دو نوع اینترفیس داریم : اینترفیس داده و اینترفیس مدیریتی که با هم ترکیب نمی شوند و از هم جدا هستند . یعنی اینکه ما شبکه های مجزا برای اینترفیس مدیریتی داریم که این کار معمولاً هزینه بر است لذا برای شبکه ای که اهمیت مدیریت در آن کم است ، ایجاد یک شبکه مجزا غیرمنطقی است

## Manager to Device Connectivity (cont'd)

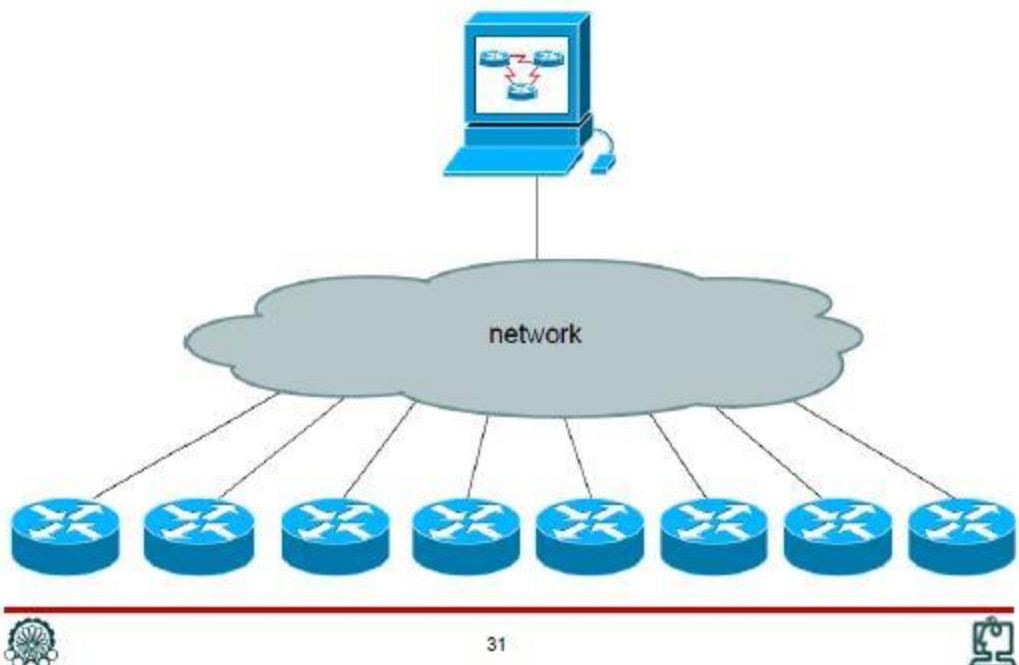
- Connectivity between managing and managed systems?
- Multiple ways to connect a device to a management station
  - Through a dedicated port (console port)
  - Through a dedicated interface, with the device configured such that management traffic is passed through the interface
  - No specific connection at all, data port is used for NM
    - In-band management: NM traffic is part of other traffic
    - Chicken or Egg problem!
      - Data routing need management while management uses data path



در روش سوم، تمام ترافیک اعم از داده و دیتای مدیریتی بر روی یک بستر مشترک ارسال می شود در این حالت in-band به NMS که یک application روی آن است یک شماره پورت اختصاص داده می شود این روش manager می باشد یعنی یک مسیر مشترک برای داده ها و دیتای مدیریتی (outband manager) یعنی یک مسیر مجزا ().

از آن جایی که سیستم مدیریت شبکه را برای مدیریت منابع و غیره می خواهیم اگر این شبکه مشکل پیدا کرد و ما قصد مدیریت آن را داشته باشیم ، چالش در این است که ما ترافیک مدیریتی را روی همین بستن می گذاریم و همین ترافیک مدیریتی در شرایط بحرانی باید مدیریت شود تا به مقصد NMS برسد. لذا در موقع بحرانی به علت مشترک بودن بستر ، ممکن است دیتای مدیریتی با اختلال مواجه گردد.

## Manager to Device Connectivity (cont'd)



31

# The Management Network

- **Production traffic vs. Management traffic**
  - Production traffic carries the customer services
    - Network devices are not destination of it
      - Transient nodes for this kind of traffic
    - Management traffic is management protocols packets
      - Network device is the destination for management traffic, not just a transit station
        - Management traffic hence is addressed at the network device itself, as opposed to a connected end system
  - Out-of-band management: Dedicated physical network for management traffic
  - In-band management: Management network overlayed on top of production network



32

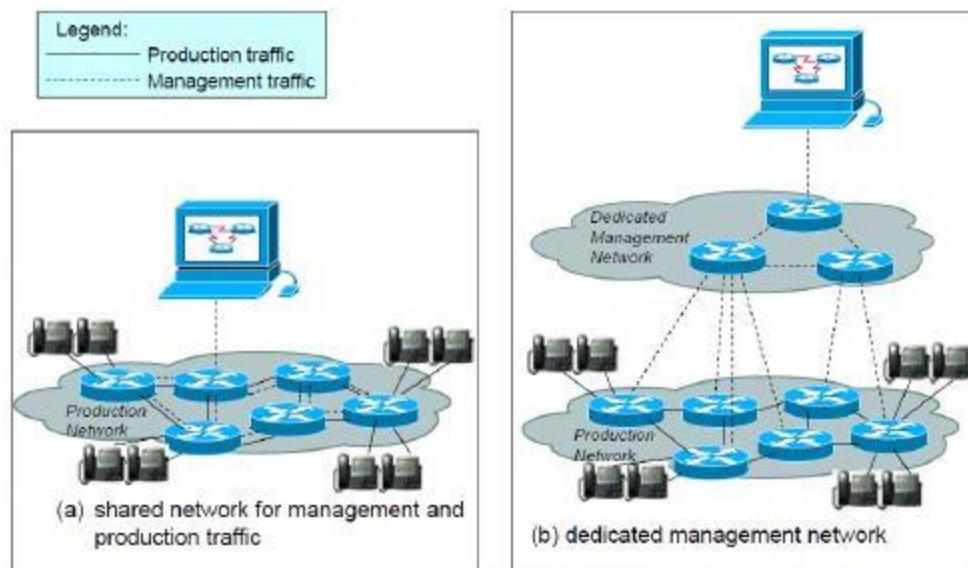


ما یک شبکه داریم که دو تیپ ترافیک در آن رد و بدل می شود تیپ اول ترافیک Production و تیپ دوم . management ترافیک

• ترافیک Production : سرویسی است که کاربر به آن نیاز دارد و بابت آن پول می دهد در این ترافیک ، شبکه پلی است که ترافیک را از مبدا به مقصد هدایت می کند و ترافیک ترانزیتی است و این ترافیک از طریق نودها جابجا می شود.

• ترافیک مدیریتی مربوط به بسته های مدیریتی است و مربوط به تجهیزات شبکه است و این ترافیک ترانزیت نیست و آدرس موجود در آن همان آدرس تجهیزات شبکه می باشد و End system ها همان سوئیچ ها و روتراها می باشند. لذا دو دیدگاه وجود دارد 1- سیستم مدیریت In-Band که هر دو ترافیک همپوشانی دارند و سیستم مدیریت Out-band که هر یک مسیر اختصاصی فیزیکی مجزا دارند.

## The Management Network (cont'd)



33

در شکل a یک شبکه وجود دارد که ترافیک های مدیریتی و دیتا از مسیر مشترک عبور می کنند و در شکل b این دو نوع ترافیک از شبکه های مجزا و مستقل عبور می کنند و از یکدیگر جدا می باشد

# The Management Network (cont'd)

- Pro dedicated management network
  - Reliability
    - No issue "getting through" when network problems occur
  - Interference avoidance
    - No competition with production traffic
  - Ease of network planning
    - No additional category of "service" to take into account
    - But: a separate network needs to be planned
  - Security
    - Users + subscribers never come into contact
    - Easier to secure, less (external) vulnerabilities, e.g., DDoS
- Cost?!
- Management of the management network?!



34



هر یک از این دو راه حل ، مزايا و معایبی دارند. اگر شبکه مدیریتی اختصاصی و جداگانه ایجاد کنیم : 1- این شبکه Reliable و مطمئن است و فقط ترافیک خاص مدیریتی را عبور می‌دهد (مثل شبکه نیروهای مسلح) . 2- اینکه جلوی تداخلات را می‌گیرد ، چون رقابتی بین ترافیک‌های کاربر و مدیریتی وجود ندارد . 3- بحث برنامه ریزی و Planning برای شبکه راحت‌تر می‌شود و مشکل هر کدام از ترافیک‌ها ، جداگانه برطرف می‌شود و نیازی به بررسی کیفیت سرویس بین این دو نوع ترافیک نیست . 4- امنیت در این شبکه بهتر است چون کاربران اینجا نیستند و شبکه جداگانه ای دارند. شناسایی و نفوذ هکرها به این شبکه خیلی مشکل تر است و این شبکه های مدیریتی معمولاً مستقل بوده و به سایر شبکه‌های مدیریتی کاری ندارند و به هم متصل نیستند و دسترسی به آنها محدود است .

در عین حال این نوع راه حل بسیار هزینه بر است و خود این شبکه مدیریتی نیاز به مدیریت دارد .

## The Management Network (cont'd)

- Pro shared management network
  - Cost and overhead
    - Huge price tag! Equipment, space, cabling...
  - Practicality
    - Separate lines sometimes not a practical option
    - Remote sites, customer premises equipment
- In practice, management networks almost always share with production networks
  - Save a few, very rare exceptions with critical service provider infrastructure



35



استفاده از شبکه اشتراکی و Share Network هزینه و Cost کمتری دارد و در این حالت به علت ترافیک مشترک به شبکه فشار می‌آید و overhead بوجود می‌آید، ولی در عین حال این شبکه عملی تر و Practical است. مثلاً اگر فاصله‌ها زیاد باشد ایجاد شبکه مجرزا سخت است.

در این نوع شبکه مجبور هستیم پهنای باند را بین این دو نوع ترافیک تقسیم کنیم. در این روش منابع کمتری را می‌توان رزرو کرد و کمتر می‌توان به استثناهای پرداخت و مجبوریم یکسری فعالیت‌های اضافه تعریف کنیم.

## The Management Network: Consideration

- How do we ensure alarms will not get stuck in traffic?
- How do we ensure network repair actions can reach their intended destination?
- How do we ensure non-essential management traffic does not interfere with production traffic?



- Network planning and engineering applies to management traffic like for other critical network applications (e.g., NM VPN using MPLS)



36



سوال : اگر آلامی در شبکه ایجاد شود ، از کجا میتوان تشخیص داد که این ترافیک بین سایر ترافیک ها گیر نمی کند ؟

سوال : فرض کنیم در شبکه خطایی رخ داده که باید رفع شود ، تا زمانی که برطرف نشده تکلیف ترافیک های پشت این خطا چه میشود ؟

سوال : از کجا مطمئن شویم که ترافیک های مدیریت شبکه ، ترافیک سرویس های با ارزش ما را خراب نمیکند؟  
- اولویت بندی و تعریف کلاس های کیفیت سرویس می تواند راه حلی برای مشکلات بالا باشد ولی خیلی از تجهیزات مفهوم کیفیت سرویس را متوجه نمی شوند .

اگر قرار است از یک بستر مشترک ، ترافیک مدیریتی عبور کند باید بحث های Network Planning و Traffic engineering را مدیریت کنیم . مثلاً با استفاده از VPN یا استفاده از PRN در شبکه MPLS و استفاده

از Tunneling برای عبور ترافیک مدیریتی ، می توان ترافیک مدیریتی را کنترل نمود . (البته همه نودها این استاندارد ها را پشتیبانی نمی کنند )

## Outline

---

- Introduction
- Managed Devices: Agents and MIBs
- Managing Systems
- Management Network
- Management Support Organization



# Management Support Organization

- Purpose of network management technology is ultimately to support the management organization, e.g.,
  - Automate routine tasks
  - Make management tasks less error prone
  - Empower administrators with the proper information
  - Enforce organization processes
    - make sure tasks don't fall through the cracks
  - NMS is also called OSS (Operation Support System)
- Management technology ultimately to be seen in that context
  - How effective does it make the management organization?
  - Success of network management (with this measure)
    - Technical efficiency & productivity
    - +
      - Proper organization architecture



38



هدف از تکنولوژی مدیریت شبکه در سازمان :

- فعالیت‌های روتین سازمان را تا حد امکان اتوماتیک کرد
- مشکلات معمولی را به حداقل رساند
- اطلاعات مورد نیاز مدیران را جمع‌آوری و به آنها ارائه کرد تا سطح کیفیت و توانایی آنها بالا برود
- پروسه‌های اصلی را مطمئن باشیم که هیچگاه down نمی‌شود

برای رسیدن به این اهداف به یک OSS (operation support system) نیاز است و یا به عبارتی دیگر به یک (NOC (network operation system) نیاز است که به سیستم کمک می‌کند تا به اهداف OSS نظر برسد. لذا با اعداد و ارقام باید مفید بودن OSS را اندازه‌گیری کرد و بررسی نمود که وجود چقدر در افزایش کارایی تکنیکی شبکه موثر است.

# Support Organizations Hierarchy

- “Horizontal” partitioning, e.g.
  - Structuring management support organization by analyzing the different tasks and the workflows that they involve
    - Network planning, Network operations, Network administration, Customer management
    - Are not independent, but their interactions are minimized
- “Vertical” partitioning, e.g.
  - Global NOC (Service Provider term)
  - Regional NOCs, e.g. North America/Asia/Europe
- Network architecture based partitioning
  - Access, Distribution, Core, ...
- Hybrid, ...



39



سلسله مراتب مدیریت شبکه در سازمان :

• تقسیم بندی عمودی ( Vertical partitioning ) : یعنی ما محدوده های جغرافیایی ایجاد می کنیم

• در ابتدا Global NOC داریم و در زیر آن NOC های منطقه ای ( مثل بخش آسیایی و اروپایی و ... )

• تقسیم بندی افقی ( Horizontal partitioning ) است که منظور یک سطح پیوسته و flat است و

روی این بستر یکپارچه فعالیت ها در جریان است و یکسری کارها در حال اتفاق افتادن است و برای همه

این مجموعه فعالیتهای

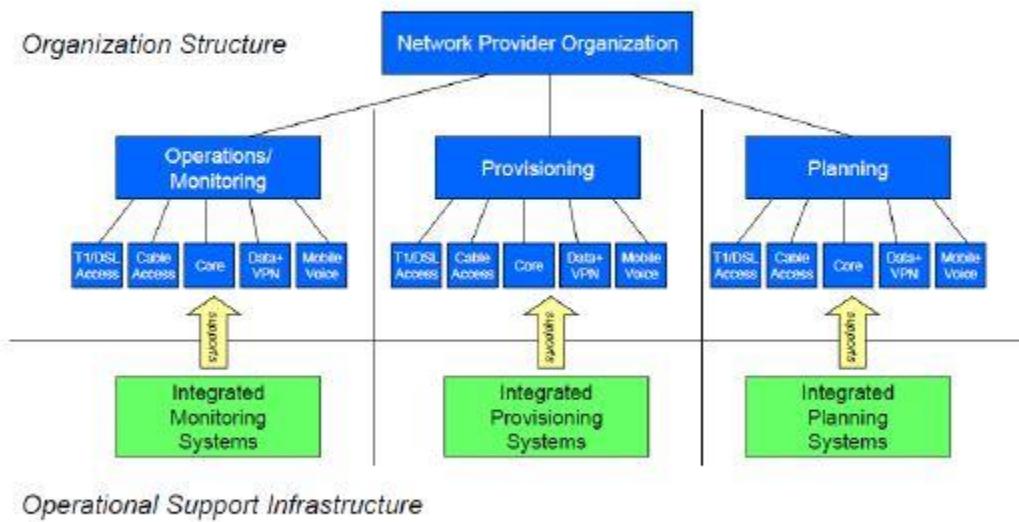
Network planning , network operations , network administrator , customer

management را تعریف می کنیم و جداسازی انجام نمیشود و چیزی مستقل نیست و فقط فعالیتها ریز

می شوند .

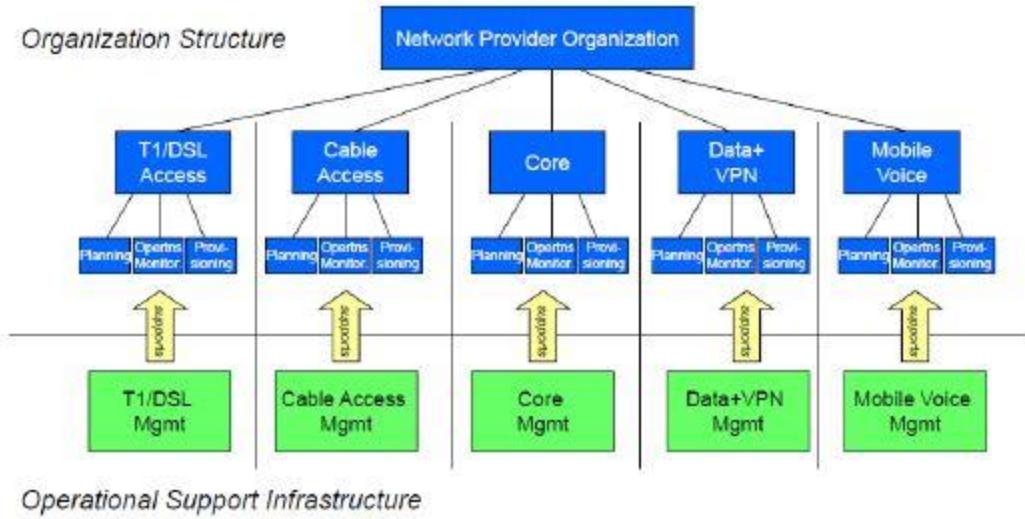
- تقسیم بندی بر مبنای معماری : ساختار شبکه بر مبنای Core,Distribution,Access تقسیم بندی می شود و باید مشخص شود مدیریت در سطح کدام یک از این لایه ها انجام می شود .
- مدیریت Hybrid : ما بصورت ترکیبی از تقسیم بندی های بالا را استفاده می کنیم مثلا مدیریتی در سطح کشور داریم ، بعد از آن NOC استانی و شهرستانی داریم و بعد از آن Distribute های شهری را داریم و بعد یک backbone داریم.

## Examples for Organizational Partitioning



در این مثال تقسیم بندی سازمان را بصورت افقی می توان دید . provider میتواند ابتدا ساختار را بصورت تقسیم بندی کند و سپس هر یک از این حوزه ها کارهای مربوط به خود را برای کل شبکه و سیستمها انجام دهد

## Examples for Organizational Partitioning



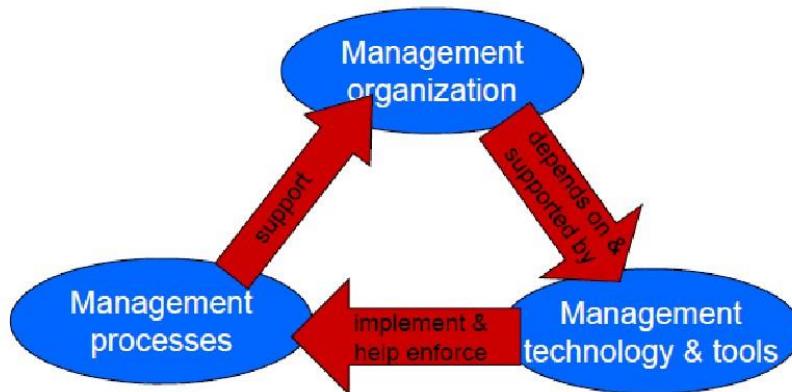
41

در این مثال برای کل شبکه operation/monitoring , provisioning , planning داریم و یعنی مثلاً مدیریت در حوزه T1/DSL یا مدیریت در حوزه Cable Access یا مدیریت در حوزه Core و یا مدیریت در حوزه Mobile Voice وغیره را داریم که مدیریت ها شکسته می شوند و لذا این ساختار مبتنی بر معماری است که جنبه های عملیاتی در سازمان را در نظر می گیرد.

تشخیص اینکه کدام ساختار برای سازمان مفید است امری نسبی است و بستگی به دیدگاه طراحان دارد اگر ابعاد جغرافیایی بزرگ شوند از روش Vertical partitioning استفاده میکنیم و ساختار افقی و سازمانی را روی قسمت های کوچکتر اعمال می کنیم.

# Processes

- Management organization is supported by processes in addition to technology
- Guidelines, workflows to make organizational quality consistent and predictable (not ad-hoc management!)



سیستم مدیریت شبکه ارتباط تنگاتنگی با با حوزه مدیریت آن سازمان دارد. در سازمان سیستم مدیریت داریم و آن ها برای فعالیت های خود یم سری قوانین، سایت و ابزارهایی دارن. حتی ضعیف ترین مدیران هم ترجیح می دهند یک رزومه مثبت از نظر بحث کیفیت و حوزه کاری سازمان به جا بگذارند و سعی می کنند رفتارهایشان حالت Ad-hoc نباشه و یک سری Target داشته باشند و به آن برسند.

Target لزوماً به این معنی نیست که یک پله بالاتر از وضعیت حال داشته باشے ممکنه مدیری تشخیص بده وضعیت سازمان خوبه و باید پایدار باشے. مدیر برای رسیدن به اهداف خود از حوزه ابزارها و تکنولوژی های مدیریتی استفاده می کند.

# Examples for Processes

---

- Documented operational procedures
  - What to do when certain events occur
- Collection of audit trails and network logs
  - Predefined & automated procedures for storing, backing up, consolidating reports
- Network documentation
  - Prerequisite for provisioning, fault isolation, ...
- Backup and restore procedures
  - Lifeline when things go wrong: restore to last working config
- Security processes
  - Audit trails, backup/restore procedures important tools



در بحث مدیریت ابزارها و تکنولوژی می توانند در یک حوزه به مدیر کمک کنند مثلا در سازمان های مختلف یک نقطه اشتراک وجود دارد. این که مستندی برای روال خودشان نمی توانند ارایه کنند به عنوان مثال موضوع یا محتوایی قرار است سینه به سینه حفظ شود ولی بعد از چند سال ماهیت خودش را از دست می دهد و عوض می شود. این در سازمان ها نقطه ضعف بسیار مهمی است در نتیجه نمی دانیم وقتی اتفاقی می افتاد چه کار کنیم در صورتی که اگر مستند باشد می توانیم بگوییم طبق این مستند این اتفاق باید بیفتد. ما کلی ابزار شبکه داریم که در آن ها اتفاقات مختلفی می افتند. Audit و log هایی که تجهیزات شبکه دارن برای ما مهم هستند و

به صورت پیش فرض باید برای ما مطرح شوند. رویه های مربوط به گرفتن گزارش های مختلف می توانند در حوادث مختلف مفید باشند. وقتی من network previsiencing می کنم و یک سرویس رو دایر می کنم باید مستند باشه. در بحث تفکیک خطا، یکی از مواردی که خیلی در کشور خودمان رخ می دهد وقتی خطای رخ می دهد در جایی ثبت نمی شود. وقتی جلوی خطای باید گرفته یشه مستندات آن خطای بسیار مهم است. رویه های بک آپ از جایی که اگر سیستم به مشکل بخوره می توانیم restore کنیم به آخرین نقطه ای که شرایط مناسبی داشته مثلا اختلال در سیستم سوخت رسانی که اتفاق افتاد به دلیل عامل نفوذی بود. سیستمی که بک آپ گیری رو داشته باشه اینجا به درد میخوره. روال های امنیتی مثلا همینه که audit کنیم در پروسه های مختلف و ابزار هایی که این کارها رو می کنن برای ما موضوع مهمی هستن.

## Summary

---

- Network management consists of
  - Manageable devices
    - Management agents, MIB, and MO
  - Management applications
    - SW application for NM functionalities
  - Management network
    - Out-of-band management: dedicated Mgt. network
    - In-band management: overlay Mgt. network
  - Management organization
    - Horizontal/Vertical/... partitioning & NM processes



یک سیستم مدیریت شبکه شامل ابزارهای مدیریت شبکه است که شانل object هایی است که قابل مدیریت هستند. اپلیکشن های مدیریتی به خصوص شبکه مدیریتی که چالش جدی ما این است که شبکه به صورت in bound out of band باشه یا

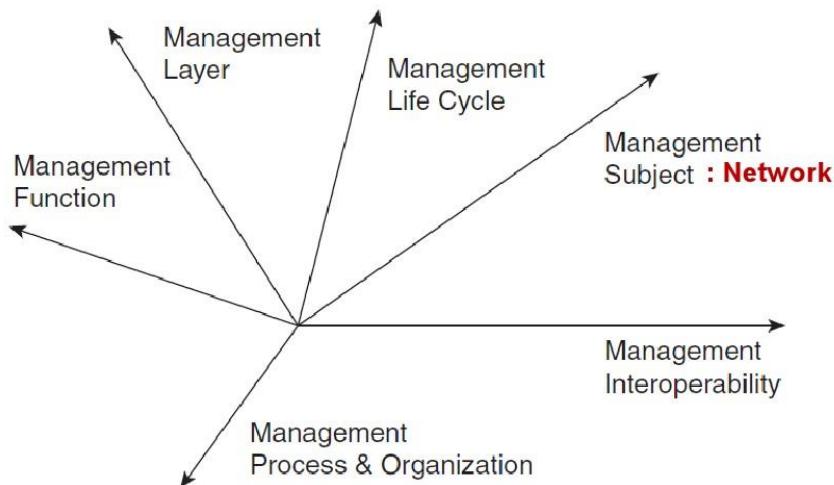
یعنی یک شبکه کاملاً مجزا از شبکه معمولی سازمان باشه اصطلاحاً **dedicated** یا این که یک شبکه تو دل همون شبکه باشه اصطلاحاً میگن **in bound overlay network**. همین یعنی یک ساختار منطقی در ساختار شبکه پیدا کنیم و یک سری اپلیکیشن ها لازمه. مثلاً در کلاسی که برگزار می کنیم من ترافیک رو می فرستم برای سرور و سرور برای شما می فرستم پس علاوه داریم یک **overlay network** ایجاد می کنیم. بحث دیگر مربوط به حوزه سازمانی است که سیستم مدیریت به صورت **horizontal** یا **vertical** باشه و روال های NMS من چطوری اتفاق بیفته.

### :Network Management Dimensions

## Introduction

### ➤ Management dimensions

- Makes it easier to define a systemic approach to solving a network management problem



4



سیستم مدیریت شبکه جنبه های بسیار متنوعی در خودش دارد. علاوه بر جنبه عمومی شبکه می توانیم در مورد مباحث دیگری از جمله **management layer** یا **management life cycle** صحبت کنیم. زیر ساخت های مدیریتی چند لایه است:

Management function

Management process & organization

Management interoperability

## Introduction (cont'd)

---

### ➤ Important fact:

- These dimensions are (almost) orthogonal

### ➤ Examples

- It does not matter which technology is managed
  - The management protocols must be interoperable
- It does not matter which layer is managed
  - The management functionalities are needed



5



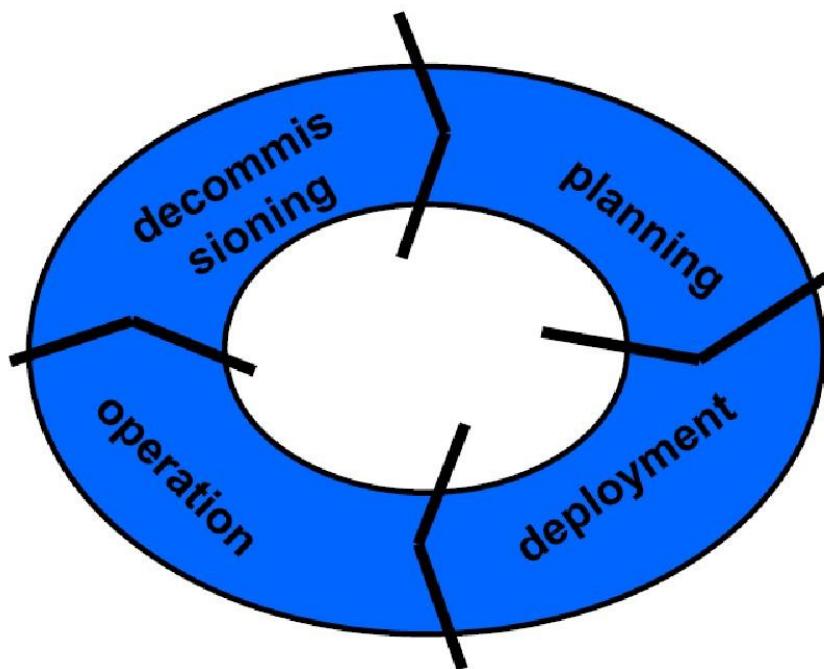
تمام ابعادی که نام بردیم نسبت به همدیگر orthogonal هستند یعنی بر هم عمودند. محور  $X$  و  $Y$  را در نظر بگیرید وقتی روی محور  $Y$  ایستادین از اون جا به محور  $X$  نگاه می کنید محور  $Y$  می شود یک نقطه روی محور  $X$  یا بر عکس.

یعنی به عبارتی ساختارها طوری است که سایه روی هم نمی اندازند. در دنیای انتقال داده به این ها می گوییم عمود بودن ابعادی که در بحث مدیریت سیستم شبکه نام بردیم هر بعدی نسبت به بعد دیگر عمود است یعنی مثلاً این که مدیر سازمان من کی هست و چه کاری می کنه خیلی به فرآیند بک آپ و restore ربط نداره تا

الان یک فکری می کردم الان از این به بعد یک فکر دیگه می کنم من می بینم سازمان پول داره میگی برو  
فلان استوریج رو بخر. یک موقع می بینیم دوتا فلاش و یک هارد اکسترنال بخری کافیه.

موضوع دیگری که وجود دارد این است که من محل مدیریت رو هم باید بدونم مثلا در هر لایه شبکه وظایف  
مدیریتی متفاوتی وجود دارد که مختص به آن لایه است.

## Network Lifecycle



یک سیستم مدیریت شبکه مانند هر سیستم دیگری یک life cycle دارد که شامل 4 مرحله است:

-1 Planning: طرح ریزی برای شناسایی نیازهای سیستم و پیدا کردن سیستم مناسب

-2 Deployment: نیازهارا پیاده سازی کنیم تا بشه اون سیستمی که می خواهیم

-3 اجرای سیستم Operation

-4 Decommissioning زمانی که ببینیم سیستم به درد نمیخوره سیستم رو بازنشست کنیم و

سیستم جدید جایگزین کنیم.

# Network Lifecycle (cont'd)

## ➤ Planning

- Forecast user & service needs, equipment selection, topology planning, ...

## ➤ Deployment

- Equipment installation and turn-up, physical setup, wiring, logical setup and initial configuration

## ➤ Operations

- What is normally associated with network management

## ➤ Decommissioning

- “Opposite” of deployment, early notification of users if affected, graceful shutdown, cutover of traffic, ...



8



در مرحله planning نیازهارو نگاه می کنیم الان چی هست در آینده چه خواهد بود(انتخاب تکنولوژی، انتخاب تجهیز و انتخاب برنامه)

در مرحله دوم چیزهایی که گفتیم رو به صوت فیزیکی اجرا می کنیم.

در مرحله سوم به فاز اجرا می رسیم و در مرحله آخر سیستم جدید جایگزین می کنیم در صورت نیاز

# Network Management Lifecycle

- While the “network management” mainly implies the activities in the operation phase
  - However, each step of network lifecycle needs its own management requirements, E.g.,
    - Network installation & documentation in “Deployment”
    - Migration planning & implementation in “Decommissioning” phase
  - Moreover, every technology & service type has the similar lifecycle in a operational network
- Network management
- To manage the network lifecycle
  - Is evolved in the lifecycle as a part of network



9



وقتی بحث مدیریت شبکه و چرخه حیات را مطرح می کنیم دو دیدگاه به وجود می آید:

1- از ابزار مدیریت شبکه برای مدیریت چرخه حیات در دیگران استفاده می کنیم مثلا من از سیستم مدیریت شبکه در **lifecycle** شبکه و سیستم های مرتبط با آن استفاده می کنم مثلا نیازهارا بشناسیم چالش ها و مشکلات رو شناسایی کنیم و...

2- خود ابزار مدیریت شبکه یک سیستم است و میتوانه چرخه حیات خودش رو داشته باشه مثلا ارزیابی هارو انجام بدم گره و مشکلات را رفع کنم و سه مرحله اول چرخه حیات سیستم رو برash مطرح کنم.

در هر صورت می دانیم در یک شبکه عملیاتی درست مثل هر سیستم دیگری یک چرخه حیات وجود دارد که این چرخه حیات یک سری سرویس ها، تکنولوژی ها و ... استفاده می شود پس سیستم مدیریت شبکه هم به

من کمک می کند تا چرخه حیات رو مدیریت کنم یا خودش بشه جزیی از چرخه حیات شبکه

## Outline

---

- Introduction
  - Lifecycle
  - Interoperability
  - Layers
  - Functions
  - Process & Organization
  - Summary
- 



مرحله interoperability تعامل بین ابزارهاست.

# Management Interoperability

---

- NM is a distributed application, hence
  - A central challenge: How are systems involved in management able to interoperate
    - Managing systems with managed systems
      - Layer 3 connectivity is not sufficient → L7 protocols
    - Management applications with each other
      - Distribute computing issues
- Requires agreed-upon rules for interactions
  - Standard management interfaces and protocols



سیستم مدیریت شبکه ذاتا یک سیستم توزیع شده است. تمامی agent ها در سطح شبکه پخش شدند و ما از طریق سرور ها این اطلاعات را از سطح شبکه جمع آوری می کنیم. اما سوالی که پیش می آید این است نحوه تعامل در این سیستم توزیع شده چگونه می باشد؟ برای این کار نیازمند یک زبان مشترک جهت مدیریت شبکه هستیم این زبان بین یک agent و مدیران شبکه مطرح است.

# Communication Viewpoint (cont'd)

- How do you identify the request you have
  - plus, what parameters are required
- How do you recognize a response to a request
- Is a time stamp required
  - plus, what's the format – there are dozens of them
- How is the message encoded
  - XML? UTF-8?
- What if two messages with the same request are received
  - Execute the same request twice, or ignore?
- Who tears down the management session
- What happens if a response is not received after a certain amount of time



14



انتقال اطلاعات در شبکه به شکل آسنکرون است و وقتی درخواست های مختلف سمت سرور میره در ساعت های مختلفی سمت سرور ارسال میشند مثال هایی از از تباط:

مبحث encoding در متن ها

Session های مدیریتی

نرسیدن پیام بعد از ارسال

# Function Viewpoint

---

- Describes the services a manager can expect from an agent
- Basic services
  - Retrieve a piece of information
  - Modify a configuration
  - Initiate an action
  - Receive an event
- Advanced services (examples)
  - Transaction support: commit and roll back multiple operations as if they were one
  - Event subscription: receive only events of interest
  - Search and filter
- Communication protocol defines the message that are being exchanged to perform the function
  - Advanced functions are implemented through multiple management primitives



15



## از نظر کارکردی:

یک سری سرویس داریم و این سرویس ها ساده نیستند برخی از این سرویس های سرویس های پایه هستند  
مانند: عملیات پیکربندی، دریافت اطلاعات، شروع عملیات و دریافت یک رویداد

اما دسته دوم سرویس های پیشرفته هستند مانند:

مثل تراکنش های پایگاه داده task هایی که یا باید انجام شوند یا انجام نشوند و حد وسط ندارن  
 تشخیص این که کدام اطلاعات باید فرستاده شوند.

Search & filtering

# Information Viewpoint

---

- The context of network management
  - A common terminology between manager and agent
    - Without a common terminology, no management interoperability
  - **Meta model:** the modeling constructs at your disposal to define the model by which the managed system is referred to
    - Object oriented: collection of objects
    - Data oriented, table oriented: entries and columns of tables
    - Command oriented: commands and command parameters
  - **Model:** the actual representation of a type of managed system e.g. a router, a switch, a voicemail application
  - Standards specifies the meta model
  - Model of MOs of an agent is given by vendor
- 



16



رویکرد اطلاعاتی:

یک مشترک بین **agent** و مدیر نیاز است تا اطلاعات منتقل شود.

متا مدل: یک مدل خیلی بزرگ است و چیزی فراتر از مدل هاست و مدل ها بر اساس این متا مدل اسخته می شود. باید استاندارد های این متا مدل نیز مشخص شود.

# The Role of Standards

---

- Goal: align the way in which things are managed
- It's all about interoperability
  - Not an issue if you only manage a single type of thing, but:
    - Different vendors, Different device types, Different OS
  - More easily manage different devices
  - Less time, cost to integrate
- What to standardize
  - Management messages, encoding of information
  - Functions, parameters, return codes
  - Management information (typically, meta-models)



17



قابلیتی است که بتوان با کمک آن دستگاه های مختلف را با هر سیستم عامل یا نوعی **Interoperability** که هستند مدیریت کرد.

موارد مورد نیاز جهت استاندارد سازی:

پیام های مدیریتی همراه با محتوای آن پیام یا **encoding**

توابع، پارامترها و کدهای بازگشته

اطلاعات مدیریتی

# NM Standardization Bodies

---

- Numerous standards bodies, sometimes competing
- Industry consortia
  - Companies serving a common market interest
    - TeleManagement Forum (TMF), DSL Forum, Desktop Management Taskforce (DMTF), ...
- Professional organizations
  - Members are individuals of a profession
    - IEEE, ...
- Government-sanctioned bodies
  - ITU-T, ISO, IETF, W3, ...



18



سازمان های مختلفی هستند که عملیات استانداردسازی را انجام می دهند:

مثل DMTF, TMF (در حوزه صنایع) – IEEE (در حوزه پیشرفته) – ITU/T (در حوزه کشوری)

# TMN: as an example of layering

---

- TMN (Telecommunication Management Network)
    - It is much more then just a network management layering
    - Problem
      - Heterogeneous management systems for heterogeneous technologies
    - Solution
      - Standardized management network with aligned management systems for heterogeneous networks
  - Currently
    - Has little commercial relevance
    - Used as reference model
    - An example of comprehensive management framework
- 



بحث لایه بندی:

از Telecommunication Management Network برای بحث لایه بندی استفاده می شود.

# TMN Layers: Network Element

---

- It is a **manageable** network device
- It means “the management agent”
- It provides agent services, mapping the physical aspects of the equipment into the TMN framework
  - Get management parameters
  - Set management parameters (configuration)
  - Alarm generation
  - ...



دستگاه قابل مدیریت شبکه که بهش Network Element هم میگن و می تونه تو Manage Agent کارهایی مثل گرفتن و تنظیم کردن پارامترها، تولید آلام ر

# TMN Layers: Element Management

---

- Vendor specific management functions
  - Hides these differentiations from the Network Management
- Examples of functions
  - Detection of equipment errors
  - Measuring power consumption & temperature
  - Measuring the resources that are being used
    - Like CPU-time, buffer space, queue length etc.
  - Logging of statistical data
  - Updating firmware
  - ...



23



: شرکت های سازنده اختلاف های خودشون رو در حل یک مشکل از شبکه مخفی می کنند.

# TMN Layers: Network Management

---

- To manage the functions related to the interaction between multiple pieces of equipment
- Involves with keeping the network running as a whole (end-to-end)
- Examples of functions
  - Creation of the complete network view
  - Creation of dedicated paths through the network to support the QoS demands of end users
  - Modification of routing tables
  - Monitoring of link utilization
  - Optimizing network performance
  - Detection of faults
  - ...



ها و پکت ها و تحویل بسته ها و مسیریابی و شبکه به مربوط مباحث Network Management

# TMN Layers: Service Management

---

- Is concerned with management of those aspects that may directly be observed by the users of the network
  - These users may be end users (customers) but also other service providers
- Managing the services that the network provides and ensuring those services are running smoothly
  - Service Provisioning and SLA guarantee
- Examples of functions
  - Quality of Service management (delay, loss, etc.)
  - Accounting
  - Addition and removal of users
  - Address assignment



25



: انجام کارهایی که باعث تسهیل در شبکه می شوند مثلاً ایجاد پرینت سرور در شبکه هم در فاز بروپایی سرویس هم در فاز تضمین SLA فعالیت می کند.

# TMN Layers: Business Management

---

- It is responsible for the management of the whole enterprise
- It can better be related to strategical and tactical management
  - instead of operational management
- Examples of functions
  - Billing and invoicing
  - Help desk management
  - Business forecasting
  - ...



26



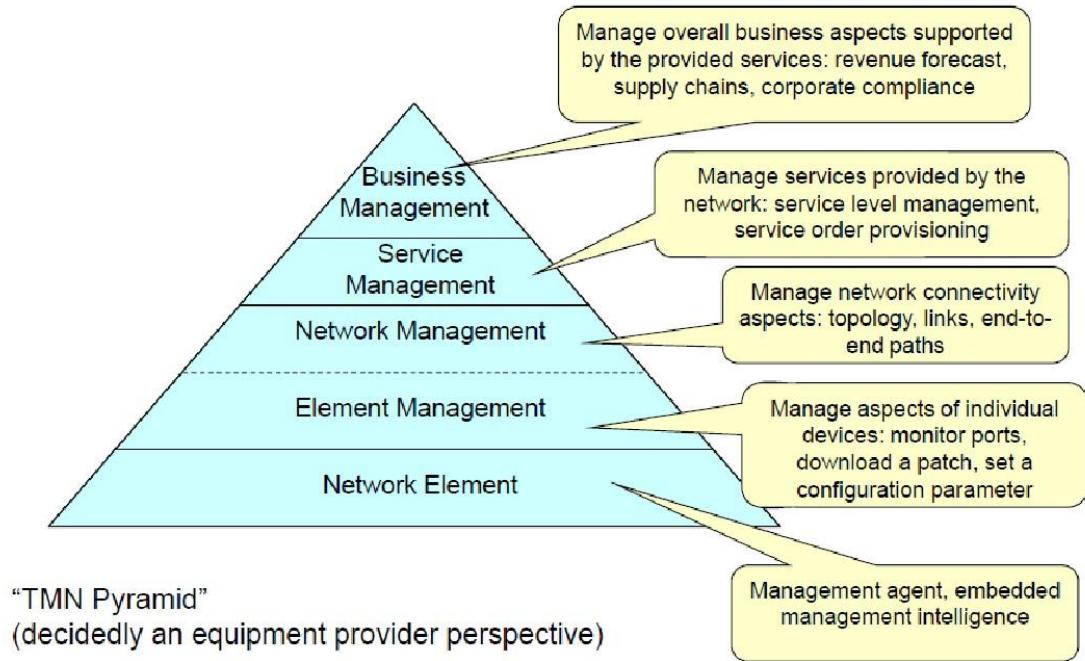
: مواردی که مستقیم به بحث بیزینس سازمان مربوط است مانند:

Billing & Invoicing

Helpdesk Management

Business Forcasting

# TMN Layers



27



از شکل فوق به عنوان هرم TMN یاد می شود.

# Considerations

---

- Different layers are often handled by different organizations; example?
- Technical layering can influence how a business is structured and define its business relationships
  - For example, a transport provider might provide physical lines and transmission equipment
  - Network service providers provide voice or data services, using the transmission services of a transport provider
- The multiple-layer approach is sometimes criticized
  - management solutions consisting of multiple systems each working at a different layer cause an integration difficult, costly system administration



افراد زیادی هستند که در فعالیت تجاری من تاثیر گذار هستند مثلا در حوزه تصمیمات فنی مسیولیت اصلی به عهده ادمین شبکه هستش و بعضی مواقع به عهده مسیول فعالیت تجاری مورد نظر نیز هست مثلا در یک سری از مواقع مدیر بیزینس می خواهد یه تصمیمی در حوزه شبکه گرفته شود که ادمین شبکه آن را نگفته باشد و مواردی از این دست باعث می شود شبکه به آن وضع مطلوبی که مد نظر ماست نرسد.

## جلسه هفتم

# Outline

---

- Introduction
  - Lifecycle
  - Interoperability
  - Layers
  - Functions
  - Process & Organization
  - Summary
- 



29



صحبت کردیم که میتوان از جنبه های مختلف مدیریت شبکه را دید از چرخه حیات صحبت کردیم در مورد اینکه سیستم های مختلف با هم کار میکنند، از جنبه های لایه های مختلف صحبت کردیم از منظر کارکردها بحث کردیم و بعد بحث *process*ها.

امروز از منظر **function** یا کارکرد میخواهیم به این سیستم نگاه کنیم ما وقتی میخواهیم بگوییم کارهایی که در زمینه مدیریت شبکه هست چیا هست این کارها را میتوان در یک سیستم قرار داد. این کارها در دل خودشان ویژگی ها و نیازمندی های مشترک دارند و در حوزه **application** مدیریت شبکه ای به آن میپردازیم وقتی بحث، بحث ساختار مدیریتی سازمان مطرح میشود میتوان گفت این کارکرد مدیریت شبکه ای میتوان گفت این پایه و اساسش است.

# Functional Viewpoint

- Categorization of different management tasks
  - Typically share similar characteristics and requirements
  - Often addressed by management applications
  - Can be basis for structure of management organizations
- Examples of categorization
  - FCAPS (popular in data world)
    - Starting point: Common functions/ purposes of management tools
  - OAM&P (popular in telco world)
    - Starting point: Common structure of organizations running a network
  - Other categorizations are possible
    - E.g. Fulfillment, Assurance, Billing (Telemanagement Forum)
    - E.g. FCAPS + Change Management (former IBM)



30



معرف ترین مدل آن fcaps میباشد که در واقع مدل مشهوری بود که در دنیای شبکه کامپیوترا داریم وقتی به 5 تا فانکشنی که fcaps گرفته نگاه کنیم میتوان گفت fcaps نقطه ای شروعی است از منظر functionality از نظر مدیریتی یا مثلا اگر در دنیای مخابرات oqp یه نقطه شروع هست و مشابه آن زیاد داریم. مثلا ترکیب fcaps یا change management ارائه شده است. یا IBM ارائه شده است. یا telemanagement forum assurance و biling توسط ارائه شده است. پس چیزی که هست کارکردهای پایه ای که از هر دیدگاهی صحبت کنیم یه مدل مدیریت شبکه داریم که میشه پایه های اون سیستم موردنظر ما.

# FCAPS: as an example of functions

- First articulated in ITU-T TMN Reference Model
- Popular in datacomm world
- Fault
- Configuration
- Accounting
- Performance
- Security



31



ما اول مدل مرجع TMN را داشتیم توسط ITU مطرح شده بود که صرفا مدل مخابراتی است و صحبت شده در مورد فضای مخابراتی ها و شبکه ای ها. میشه گفت fcaps براساس تجربیاتی که از TMN گرفته شده بود بنا نهاده شده و امروز تبدیل شده به مدل مرجع در حوزه ای انتقال داده شبکه های کامپیوتری. 5fcaps مخفف تا کلمه است و اینها قبلاً حرف security, performance, accounting, configuration, fault در مورد اینها زدیدم.

# Fault Management

---

- Functions related to dealing with faults in network
  - Monitoring networks and services for faults
  - Reacting to faults when they occur
  - Managing resolution of faults
  - Being proactive about preventing faults before they occur
- Important fault management functions
  - Alarm management
  - Fault diagnosis
  - Trouble ticketing
  - Proactive fault management



32



کارکردها در بحث مدیریت سازمانی تاثیرگذار هست مثلا وقتی میگوییم fault management یا مدیریت خطاهای چگونه خرابی داخل شبکه را هندل میکنیم شامل این میشود که یک سیستم مانیتورینگ داشته باشد که سیستم را مانیتور کنه اگر خطای رخ بدهد در واقع نسبت به آن خطا ری اکشن درست نشان داده شد و آن خطا مدیریت شود و حل شود و نکته مهم اینه اصولا من قبل از شبکه هم دچار خطا و خرابی شود جلوی این اتفاق را بگیرم.

بنابراین 4 تا اصلی تعریف میکنم 1-بحث مدیریت alarm 2-تشخیص خطا 3-trouble function 4-ticketing مدیریت خطاهای به صورت proactive

Proactive یعنی مدیریت خطا به صورت فعال. بعدها در مورد اینها دقیقاً صحبت میکنیم که چه موردی انجام میشود مثلاً مدیریت خطا یا مدیریت آلارام آنقدر مهمه که ممکنه جایی بر سه انقدر خطاها زیاد شه که سیستم من رو از کار بندازه پس همه‌ی اینها خیلی مهمه.

## Configuration Management

- Functions related to dealing with how network, services, devices are configured
  - Physical configuration, e.g.
    - Equipment, line cards, physical connectivity
  - Logical configuration, e.g.
    - Protocol settings, logical interfaces, address assignments, numbering plans, ...
- Important configuration management functions
  - Inventory
  - Auditing, Discovery, Auto-discovery
  - Synchronization
  - Image management
  - Backup and restore



وقتی میگیم مدیریت پیکربندی یا configuration یعنی هرآنچه که مربوط به این باشد که یه شبکه ای رو و یا یک device را config کیم که بتونن کار کنند که شامل 1- physical configuration و 2- logical configuration باشد. 1- شامل اینه که دستگاهام چند تا پورت داشته باشد و چندتا line card باشد، چه امکاناتی داشته باشد چه قسمتهایی از آن daul باشد یا single باشد کلا فیزیکال واقعیت ها فیزیکی هست که از دستگاه میبینیم اما 2 یعنی دستگاهی که من خریدم کلی توانمندی داره که من باید این توانمندیها رو فعال کنم. مثلاً اگر بخواهم urf استفاده کنم مثلًا توی دانشگاه به دردم نمیخورد اما برای vlan مشکل urf در شب بانک مهم میشود مثلاً همین پمپ بنزین که حمله سایبری شد قطعاً logical مهمه.

داشته. این امکانات باید به صورت درست پیاده سازی شود مثل IP PLAN دادن ها(IP PLAN)ها. اگر ما یک الگوی درست داشته باشیم مدیریت راحت تر میشود.

وقتی بحث function های مدیریت مطرح میشود بحث های synchronization, discovery, auditing, inventory داخل شبکه میدارم همون اولش یه image بگیریم که بعدا اگر به هر دلیلی خراب شد بلا فاصله ایمیج رو کپی کنم-بعدی مدیریت restore و backup هست همین دو مورد اول موضوع مهمی هست. Inventory یعنی فهرست اقلامی که دارم باید بدانم چی دارم و چه اتفاقاتی روی چه دستگاهی افتاده و بعدا و بعدا اگر دستگاهی مشکلی داشت در مستندات مشخص میشود تغییرات و مشکل قبلی.

یکی از کارکردهای خیلی مهم مدیریت پیکربندی ثبت config هاست. بحث config رو مطرح نمیکنم بحث مدیریته مثلا در پمپ بنزین بحث ما این بود که برگرده راه بیفته.

## Configuration Management: Provisioning

- Provisioning: The steps required to set up network and system resources to provide, modify, or revoke a network service “Resources”:
  - Bandwidth, CPU, Memory, Port assignments, Address assignments (IP addresses, phone numbers, ...), ...
- Scope:
  - Individual systems (“equipment provisioning”)
    - E.g. set up a firewall
  - Systems across a network (“service provisioning”)
    - Coordinated configuration changes across multiple systems
    - Often required to provide an end-to-end service



یکی از بحث های جدی که در telecom provisioning هم مطرح بحث provisioning میگه یکی از من میخواهد سرویس بگیره من سریع این سرویس و برash setup بکنم سریع منابعی که میخواهد و بهش بدم(ازمش اینه config شبکه رو عوض کنم) منابع شبکه من هم محدوده حالا اینکه کاربر در شبکه ی ما چه میخواهد این داستانش متفاوته. مثلا یک کاربر شبکه در cloud بخواهد cpu بگیره پهنانی باند میخواهد میخواهد memory میخواهد port assignment میخواهد IP میخواهد و غیره پس برای ارائه دادن یه سرویس ساده باید همه ی این موارد در نظر گرفت پس یه provisioning قوی باید داشته باشم که موضوع ساده ای نیست یعنی یه سرویس انتهایی یعنی سیستم ها به صورت individual در نظر گرفته میشود و هم کلی میخواهم ارائه بدهم پس تمام configuration های hob by hob شبکه رو به یه طرف. یه مهندسی سرویس end to end هم باید در بین آن همه سیستم در نظر بگیرند.

## Accounting Management

---

- Account for usage of communication resources and services
    - Metering: Measure what has been consumed by whom at what time
    - Charging: Have the user pay for what has been consumed
  - Often forgotten but arguably the most important function area of all
    - No accounting management, no revenue
    - Even as a user need to know what you pay for
- 



یه مورد دیگه مدیریت accounting هست- سیستم ها دارند از منابع و سرویس ها استفاده میکنند. منابع چی هست: مثلا memory,cpu, پهنانی باند. بحث accounting یعنی کی چقدر از منابع استفاده کند و باهاش

چی کار کند. 2 حوزه مطرح میشند: 1- کی چقدر مصرف کرده؟ متر میخواهم متشرش کنم (معیار و میزانی میخواهم برای میزان استفاده) 2- مناسب با این موارد میگم سرویس میگیری اینقدر پول بده (بحث charging چقدر از حوزه‌ی شارژت باقی مونده هزینه هایش را باهاش حساب کن. این plan خودش را دارد- مثلا همراه اول که برخی اوقات بحث accounting آن مشکل دارد که گاهی اینترنت را آزاد حساب میکند. بحث accounting زمانی مطرح میشود که مثلا همراه اول یا ایرانسل داریم حالا فرض کنیم در دانشگاهیم اینترنت من تموم شد در کلاس زنگ میزنم میگم به G من اضافه کن یا میگم فایل منو دانلود کن و سرو ته آن را هم میارم یعنی بعضی جاها مهمه همه جا مهم نیست.

## Performance Management

### ➤ Performance management tasks

- Monitoring performance and service levels
- Detecting performance trends, degradations
- Tuning network for performance

### ➤ Common support functions

- Performance measurements
  - Accuracy, calibration, sampling considerations as common issues
- Collection of performance data
  - Often, large volumes of data
  - Sampling as a common technique to address scale concerns
- Visualization of large data sets
  - Charts, histograms, etc



بحث مدیریت performance از مباحثی که در شبکه هست این میباشد. ادمین شبکه باید به performance شبکه حساس باشد چون داد افراد درمی‌آید. (مثل الان که کلاسها مجازی شده) درسته شبکه دانشگاه هیچ هزینه‌ای نداره برای کاربر اما در حوزه performance اهمیت بالایی دارد باید پایش بشه و روند آنرا بررسی کرده پس حوزه‌ی ساده‌ای نیست و باید چند گزینه‌ای را بررسی کرد:

1-باید performance measure پارامترهای  $x, y, z$  هست  
 مثلا میزان accuracy یا میزان calibration (در چه بازه زمانی رکورد را حساب میکنم کجاها و کی ها اندازه بگیرم مهمه) و... پس متر خودم را مشخص میکنم. به نظر شما زمانیکه شبکه از همیشه شلوغ تر است کی هست؟ ساعت 9 تا 11 صبح ولی زمانیکه بخواهد log بگیره نصف شب که داره بکاپ میگیره اوج کاری شبکه است این سوال میشه در بحث متر ما. دومین موضوع اینه که من چه جوری باید این اطلاعات رو جمع کنم (چون به صورت مشخصی بحث scability و مقیاس پذیری خیلی مهم میشود) یه سیستم scalable میخواهم که برای من اطلاعات را جمع کند چون حجم زیاده و مورد سوم اینکه چه جوری اینارو present کنم در واقع بصری سازی مجموعه داده بزرگ چه جوری باشد. چارت عددی-نمودار.

## Security Management

---

- Management of security mechanisms, e.g.
- ACL management
  - Consistency between routers on a network
  - Size of ACLs
- Intrusion detection systems
  - Learning of patterns
  - How to protect against hitherto unknown patterns
- System security, anti-virus, ...



مورد بعدی مورد مدیریت فرایندهای امنیتی مثل مدیریت ACL (access control list). چه جوری ACL را مدیریت کنم که ترافیک های مجاز من همواره اجازه ورود داشته باشند و بقیه که در blocklist آنایستند شوند. کافی هست در ACL فایروال یه خط بالا پایین ثبت کنید تا گزینه های امنیتیتان نابود شود. بحث مدیریت acl خیلی بحث مهمیه که نباید لیست شما خیلی بزرگ باشد (چون بزرگ باشد هم به مشکل میخورد)

در حوزه امنیت سیستم تشخیص نفوذهم خیلی مهمه (IDS) ما میدانیم signature ID های امروز signature همه را پیدا میکنند و براساس آنالیز signature های براست میاره. همین signature میگیرند signature همه را کشف کند (الگوی حمله): پس باید الگو را بدانم اگر سیستم من بهترین سیستم باشد signature را کشف کند signature چی هست و در این فاصله IDS دنیا باشداما محدود به این باشد که سازمان ما فقط یه جا بهش بگه signature چی هست و در این فاصله خودم دچار حمله شم نابود میشه. پس مشکل پاسخگویی IDS به حملات ناشناس خودش یه داستانه سیستم های امنیتی دیگر میخواهیم استفاده کنیم یا خیر مثل آنتی ویروس، فایروال و ... تکنیک هایی مثل VLAN و ... میخواهیم استفاده کنیم یا خیر

---

## Time Horizon

---

### ➤ Short-term management

- In the scale of minute, second or even (near) real-time & automated
- Network monitoring
- Fault detection & Performance monitoring

### ➤ Medium-term management

- In the scale of hour(s) & in conjunction with human interaction
- Service provisioning, Fault elimination, Performance reporting

### ➤ Long-term management

- In the scale of weeks or even month, mainly performed by human with software assist
- Enhance management workflows, future (capacity) planning and strategies



کوتاه مدت در حد ثانیه و یا real time اگر دیدگاه مدیریتی در حد Short term هست مباحث fault detection و performance مد نظر هست. (تشخیص خرابی و کارکرد)

در مورد medium term ما در حد چند ساعت یا چند روز وقت داریم و می توانیم اینجا service داریم و گزارش های مدیریتی (مثلا امروز الگوی دانلود فایل ها در شبکه ما اینجوری بوده و ...). چرا میزان الگوی ترافیک عبور یافته را long term نمی گوییم و میگوییم؟ چرا medium performance report را medium می گوییم؟

الگوها را نمی خواهم نقض کنم اما چون حجم ترافیک در شبکه بصورت نمایی رشد می کند و الگوی امسال من با سال گذشته متفاوت می باشد مثلا پارسال من 100 گیگ اینترنت برای خانه و 50 گیگ برای گوشی گرفتم اما همین مقدار را امسال برای یک ماه گرفتم پس الگوی مصرف را باید medium در نظر گرفت.

حالا long term (باشه ای زمانی طولانی مدت ماهها ، سالها، و...) در اینجا عملا کارکردهای انسانی خیلی کمتر می شود و ماشین این کار را انجام می دهد. ما دراز مدت را با این روش پیش بینی می کنیم مانند enhance management workflows ,capacity planing و upgrade کنیم و بگوییم چه عددی لازم هست.

---

# Outline

---

- Introduction
  - Lifecycle
  - Interoperability
  - Layers
  - Functions
  - Process & Organization
  - Summary
- 



39



در مورد process & organization صحبت می کنیم .

# Management Organization & Process

- The nontechnical dimension of network management, including
  - How to organize management
  - The processes that are required to ensure that networks run smoothly and reliably
- The function, life cycle, and management dimensions described earlier can provide guidance for organizing management
- Standard procedures must be established and followed for the network to run smoothly
  - A lack of documented standard operating procedures can cause problems because of: Inconsistent configurations, Troubleshooting problems that arise as a result of inconsistencies, ...



40



یک موضوعی که صحبت کردیم کلمه مدیریت خودش حساس هست. بحث مدیریت شبکه که می کنیم یعنی داریم تعیین تکلیف می کنیم برای فرد ارشد سازمان. حوزه‌ی مدیریت سازمان اثرگذار هست در مدیریت شبکه و بالعکس. هرچه تا الان صحبت کردیم فنی بود اما این موضوع فنی نیست ولی از همه مهمتره به مدیر سازمان می گوییم تو باید از این راه بروی تا موفق شوی پس مدیریت شبکه اثر گذار هست روی مدیریت سازمان البته به شرط آنکه بقبولونیم که اگر شبکه نیاشه هیچ چیز نیست. ( مثل آموزش و پرورش که مجبور شد زیر ساخت خودش را تغییر دهد برای برنامه شاد در دوران کرونا) مدیریت شبکه می گوید باید این اصلاحات را پیذیرد تا شبکه شما reliable و smooth کارکند.

پس تمام این داستانها که تاکنون گفتیم جمع می شود در این نقطه که رئیس سازمان اگر می خواهد سیستم هایشان مدیریت شود باید این کارها را و هزینه‌ها را انجام دهد. آیا اگر پول خرج کند شبکه ما smooth تر خواهد بود؟ خیر. چون فقط هزینه کردن نیست خیلی از جاهای باید روال های مدیریتی استاندارد را پیاده سازی کنیم و پیگیری و نظارت کنیم تا شبکه بصورت قابل قبولی شروع شود تا شبکه بصورت smooth و

به کار خود ادامه دهد. اینجا سیستم های بی در و پیکر نمود پیدا خواهد کرد چون مستندات کافی reliable نداریم که برای بهبود و داشتن زیر ساخت مناسب باید این کارها را انجام داد. برای استارت یک شبکه باید تجهیز مشخص باشد باید configuration مشخص باشد و همه چیز مشخص باشد تا به جواب برسد. اگر در شبکه برویم به سمت configuraqtion ناپایدار و مستندات درستی نداشته باشیم باید کم کم به سمت trouble shooting ناپایدار برویم و شبکه درستی نخواهیم داشت.

---

## TOM & ETOM

# TOM & eTOM

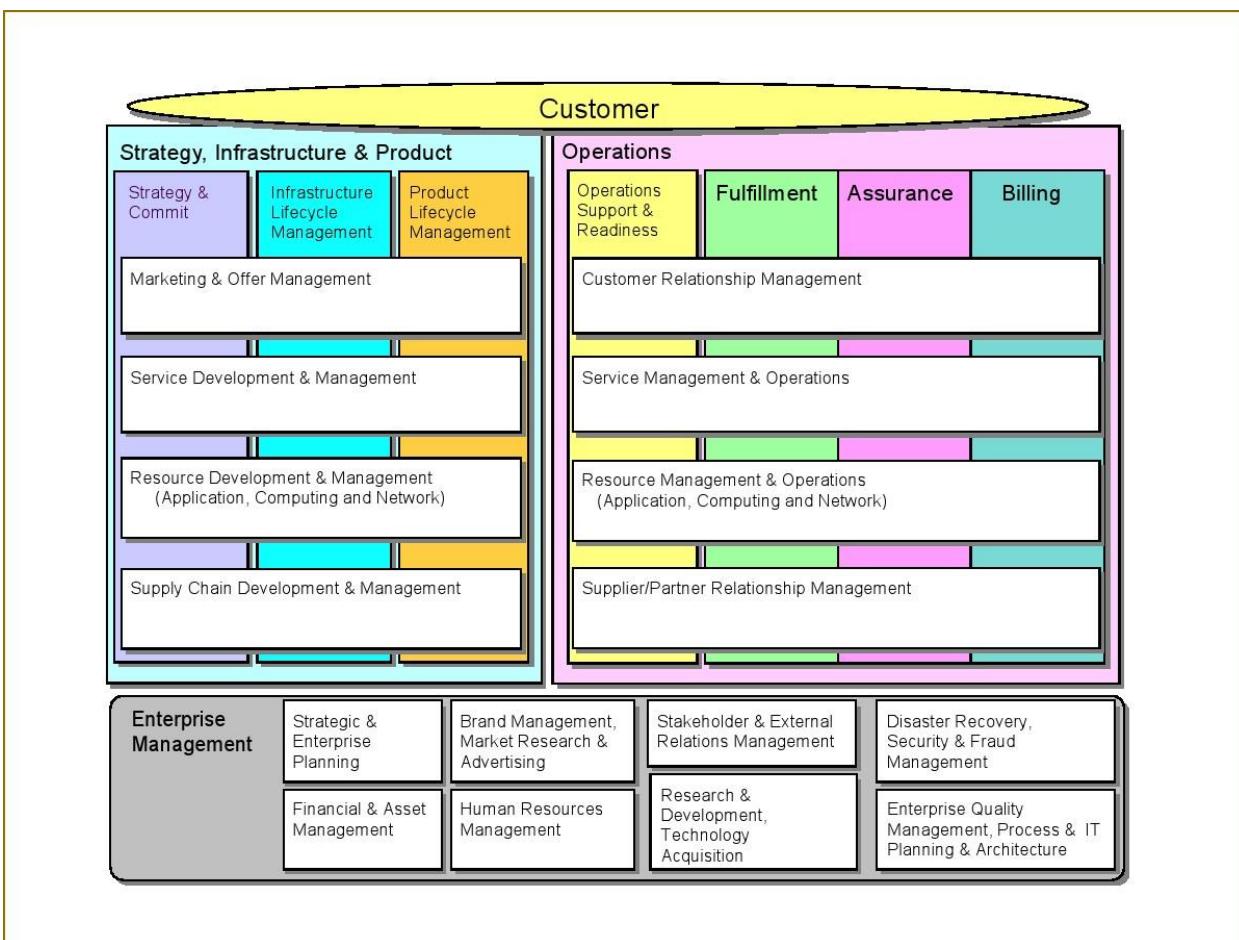
---

- Telecommunication Operation Map
    - Enhanced version: eTOM
  - TOM distinguishes among three life cycle stages – FAB (Fulfillment, Assurance, Billing)
  - Fulfillment ensure that a service order that was received is carried out
    - Turning up any required equipment
    - Performing configuration
    - Reserving resources
  - Assurance – includes all activities ensuring that a service runs smoothly after it has been fulfilled
    - Monitoring service for QoS purposes
    - Diagnosing any faults and repairing
  - Billing – making sure that services provided are accounted properly and can be billed to the user
- 



سیستم مدیریت شبکه یک مدل می باشد به نام TOM و ETOM. که TOM مخفف telecommunication operating map tom هست و نسخه پیشرفته‌ی آن eTOM می باشد. مدل fullfillment ,assurance ,billing stage تا در چرخه‌ی حیات خود دارد؛ می گوید سه

یعنی شما یک سیستمی رو کامل کنید همان فاز fulfillment هست فاز بعدی development هست . یعنی تضمین کنم این سیستم کارش را انجام می دهد. Billing بحث حساب و کتابها را می کند. پس fulfillment اطمینان می دهد که یک سرویسی در واقع اون نیازمندی هایش زل جمع می کنیم و پیکربندی هایش را انجام می دهیم و منابع را رزرو می کنیم و اعمال و سرویس ها شروع می کند به رائمه ای خدمات که تمام مراحل می باشد. assurance تضمین می کند این سرویس بعد از راه افتادن سرویس می دهد. پایش ها را داریم خطاهای را پیدا می کنیم و .... billing میشه حوزه ای که به کاربر می گوید سرویس رو استفاده کردنی پولش رو بد .



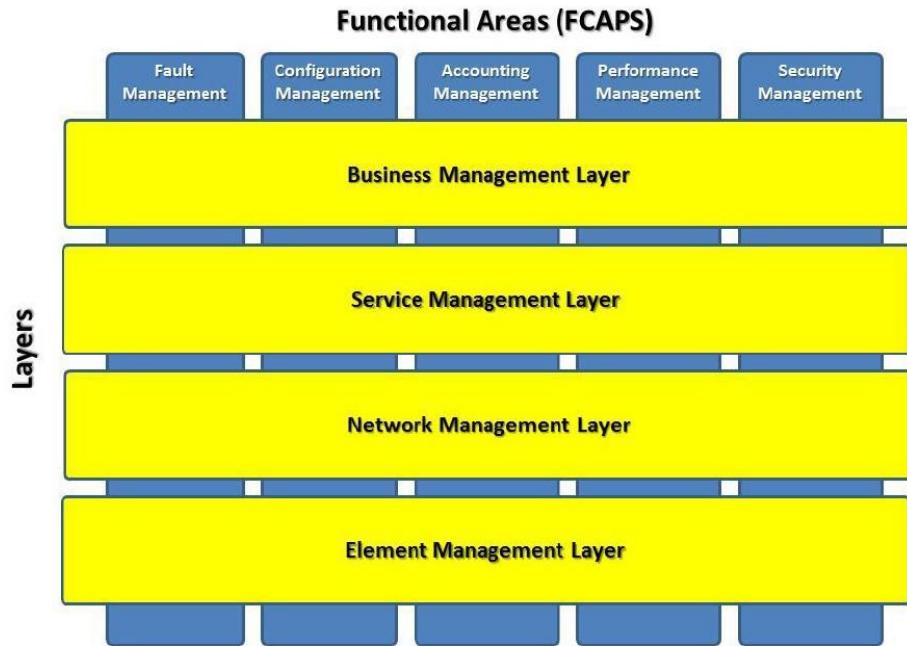
در شکل در operations سیستم این سه مورد را داریم و در کنارشان operation support & readiness داریم که باز هر کدام از این مدل TOM و Etom زیرمجموعه خودشان را دارند که مثلا CRM هست و resource management & operation هست و service management & operation هست و suplier relationship management هست و عناصر اصلی کسب و کار را می گوید .

در واقع مدل etom میگوید من یک سرویس ارتباطی می خواهم بدهم که این سرویس برای تحقق اهداف سازمانی است. چه کسانی مهم هستند؟ مشتریان و سرویس که می خواهم بدهم و منابعی که میخواهم بدهم مهم اند و supplier ها و پارتner هایی که با من کار می کنند مهم است و برای هر کدام از حوزه ها آن سه fulfillment , assurance, billing را مطرح کرده است . و برای استراتژی و محصولات و زیرساخت مورد چه باید کرد و برای هر کدام از مباحث مدیریتی خودشان را دارد و در زیر می گوید آن مشتری که می آید از این فضا استفاده کند می گوید آن زیر enterprise دارد این ها را فراهم کن. کلی مبحث مدیریتی در مبحث مدیریت enterprise یا سازمانی داریم. مثل مباحث مالی و دارایی و استراتژیک سازمانی – برندهینگ – نیروی انسانی – تحقیق و توسعه – روابط با کاربران بیرونی. بحث disaster recovery ( سیل و زلزله آمد چه کنیم؟) بحث معماری سازمانی و کیفیت و.....

اگر من به دنبال مدیریت شبکه هستم این ساله مثل این است که پا کند در کفش مدیران سازمان. اگر به ظاهر می گوییم مدلی مثل FCAPS خیلی پرکاربرد است در شبکه اما تهشیش وقتی بحث کسب و کار سازمانی است وقتی میخواهیم مدیران را قانع کنم که هزینه پرداخت کنند مهم ترین چیز این است که توجیح کنم که من کجای سازمان نشسته ام و جایگاه شبکه کجای سازمان است.

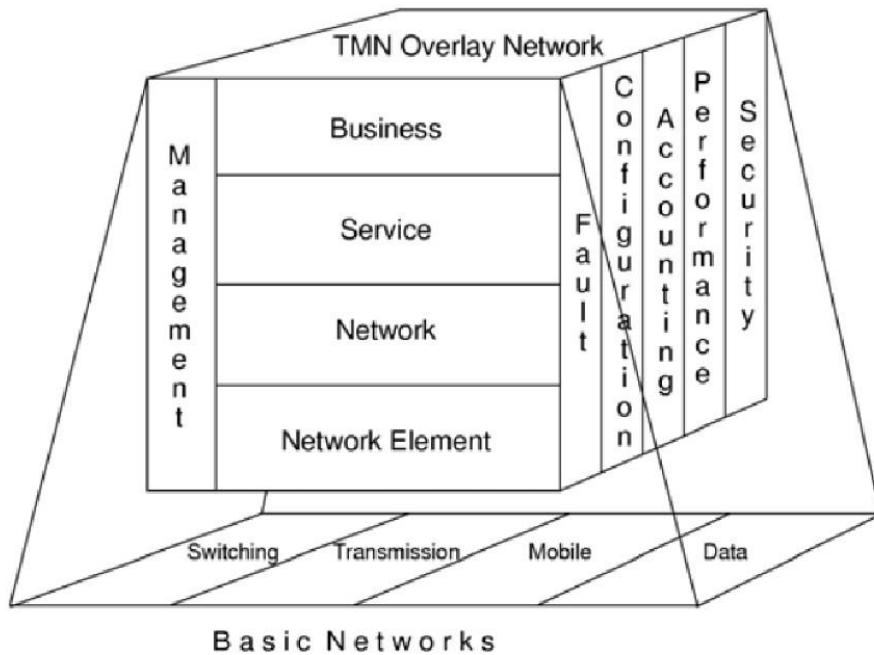
برای اینکه مدیران را قانع کنیم بهتر این است که از این منظرها بحث کنیم، از دیدگاه ارتباط با مشتری و ریسورس و ساپلای منیجمننت و fulfillment , assurance, billing صحبت می کنیم اما اینکه از دیدگاه fcaps ممکن است مدیران بگویند به من چه/ هر جا از جایگاه های فنی صحبت کنیم چون زبان ما با زبان مدیران سازمان یکی نیست با شکست مواجه می شویم. اما با مدل etom و tom زبان ما را بهتر متوجه میشوند .

# Relation Between Models



مدل fcaps که با لایه های مختلف دیگر درگیر می شود .

# Relation Between Functional Models



45



مدل TMN که برای شرکت های مخابراتی است.

# Relation Between Models

*Relationship Between FCAPS and OAM&P*

	F	C	A	P	S
O	(X)	—	—	(X)	—
A	—	—	X	(X)	(X)
M	X	(X)	—	X	X
P	—	X	—	—	—

*Relationship Between FCAPS and FAB*

	F	C	A	P	S
F	—	X	—	—	—
A	X	—	—	X	X
B	—	—	X	—	—

- X: close relation, (X): not close relation, --: very loose relation if at all



46



جدول ارتباطی برای ارتباط عناصر با یکدیگر که oam چه جوری با fcaps ارتباط دارد.

ما تا اینجا نکته مهمی که گفتیم این بود که سیستم مدیریت شبکه یک فضایی هست که هر کسی جرات ورود به آن را ندارد .

چون خیلی از افراد حتی از استادیں الفبای شبکه را بلد نیستند. باید دانش ابعاد شبکه را داشته باشیم و یا تجربه درگیر شدن با مدیران سازمان را داشته باشیم

# Network Management Protocols

---

Network Management

Spring 2013

Bahador Bakhshi

CE & IT Department, Amirkabir University of Technology



*This presentation is based on the slides listed in references.*



تا اینجا در حوزه سیستم های مدیریت شبکه کلیاتی را بحث کردیم. از این حوزه خارج می شویم و به پروتکل های مدیریت شبکه می پردازیم.

# Outline

---

- Network Management Protocol
  - Communication Patterns
  - SNMP
  - CLI
  - syslog
  - Netconf
  - NetFlow/IPFIX
- 



2



الگوهای ارتباطی این پروتکل ها چه جوری است و 5 تا از معروفترین پروتکل های آن چیست **SNMP** و **CLI** . پروتکل **SYSLOG**, **netconf**, **net flow**, **ip fix** 5. شبکه هستند .

# Introduction

---

- Interactions between managers and agents follow certain basic patterns
  - Regardless of the particular management protocol
- The pattern includes
  - Management protocol layering
  - Manager initiated communications
  - Agent initiated communications



4



تا الان درباره ساختار مدیریت شبکه صحبت کردیم (network management system) و گفتیم چه فضا و چه نیازمندی هایی دارد و با چه کسانی درگیرند و .... ولی در مورد agent و سرور و ارتباطشان با هم حرف نزدیم. اینکه سرور و agent چگونه ارتباط برقرار می کنند حرفی نزدیم. مثلا دنیای iOS و اندروید و لینوکس و ویندوز کلی با هم متفاوتند. سوال این است که می خواهم مدیریت کنم سرور هست و یکسری زبان محاوره بین اینها می شود پروتکل مدیریت شبکه.

# Layers of Management Interactions

- Network management is based on protocols stack (the layering)
  - Similar to other networked applications
- Management protocol is an application layer protocol
  - Provides primitives for management applications
    - E.g., Whole web application use HTTP
- To simplify & organize the discussion
  - Layering of network management protocol

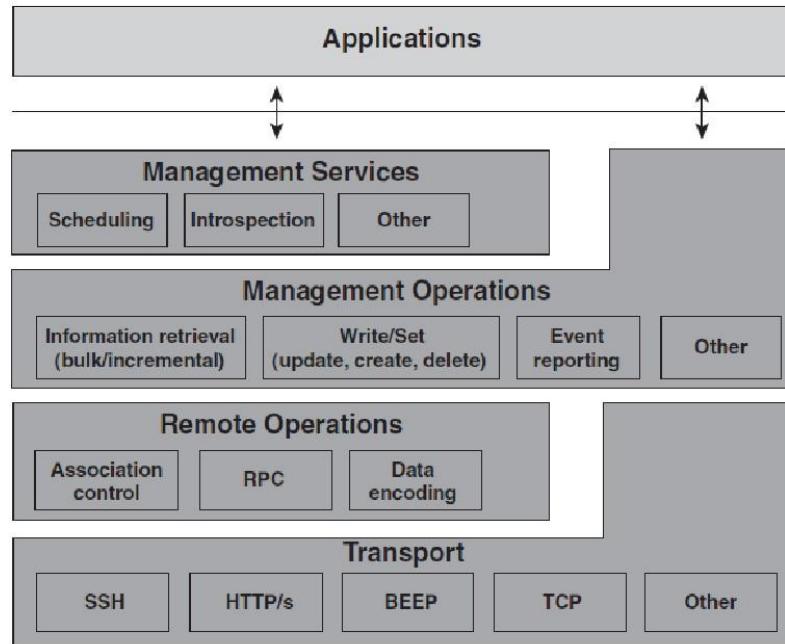


5



پس طراحی پروتکل در چنین فضایی کار راحتی نیست چون زبان ها یکی نیست و شبکه لایه لایه است. و هر کدام در سطح درک و فهم خودشان با یک مکانیزم لایه بندی برای پروتکل مدیریت شبکه می خواهیم و اینکه بدانیم کدام شروع کننده رابطه است SNPM. دنیای خودش را دارد و بسیار وسیع می باشد. مهمترین چالش این است که من پروتکلی که استفاده میکنم، چون همه لایه ها با هم درگیر می شوند باید بگوییم مدیریت شبکه در تمام لایه ها باید دیده شود. در مورد ساختار لایه ای از پروتکل های مختلفی صحبت کردیم.

# Network Management Protocol Layers



6



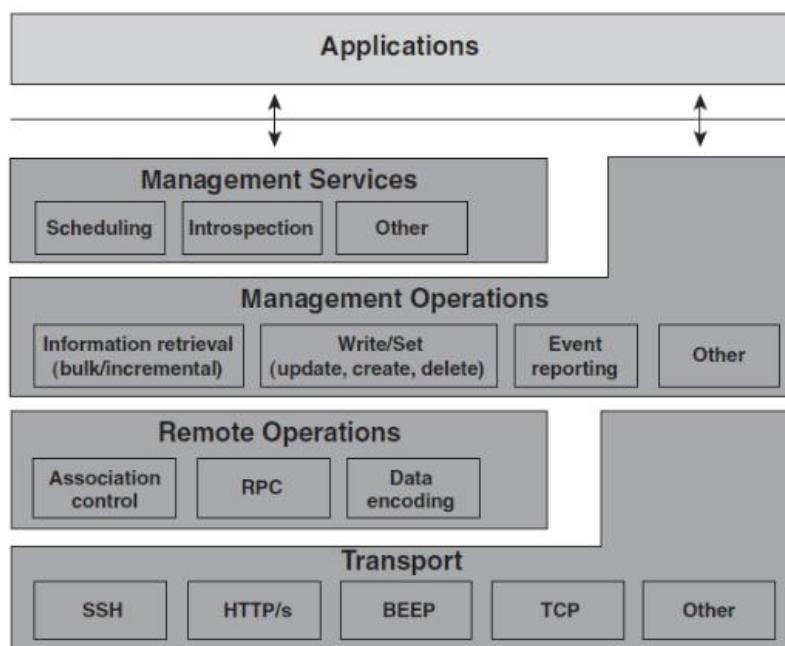
مبخت مدیریت شبکه در لایه application نشسته (لایه 5) از دیدگاه برنامه نویسی، پس من یک مشت پروتکل لایه بندی شده برای 5 لایه tcp میخواهم که توسط یک application لایه application دارد مدیریت می شود. یک ساختار فوق العاده پیچیده در بکگراند دارم که باید انقدر ساده کنم که در یک جمجمه application شود.

## جلسه هشتم

در جلسه گذشته وارد لکچر جدید شدیم و بحث ما تو این لکچر اینه که یسری پروتوكلهای معروف در حوزه مدیریت شبکه رو ببینیم اما قبل اون بذارید ببینم یه پروتوكل مدیریت شبکه چی میخواهد چی نمیخواهد.

و خب گفتیم موضوعات اصلی که مطرحه بحث درواقع لایههای مربوط به خود اون مدیریت شبکه است بحث اینه که چجوری منیجر و ایجنت هم در واقع بخوان ارتباطی رو شکل بدند و خب این بحثاً مباحثی هستن خارج از اینکه چه پروتوكلی داریم استفاده میکنیم.

## Network Management Protocol Layers



او مدمیم جلوتر یه مقدار درمورد مدیریت شبکه صحبت کردیم گفتیم یه پروتکلی لایه اپلیکیشنیه باید تو اون لایه بحث دیده شه خودش باز زیرلایههای مختلفی داره به عنوان اپلیکیشن که باید با قسمت‌ها و اجزای مختلفی

کار بکنه در واقع من یک چارچوب یا همان Framework باید ارائه بکنم که بگم یک پروتکل مدیریت شبکه داره کار می کنه.

که این چارچوب یا Framework را توان اسلامید میبینیم که چهارتا حوزه‌ی جدی دارد یکی سرویس‌های مدیریتی یکی عملیات‌های مدیریتی و یکی عملیات‌های راه دور و عملیات‌های حمل و نقل که مربوط به خود شبکه است.

توی هر کدوم از این موارد هم باز چار جوب‌های خودش هست که جای بحث داره که چی بوده و چی هست و چی خواهد بود.

مثلا در مورد سرویس‌های مدیریتی بحث زمانبندی هست در بحث عملیات‌هاش بحث اینکه من چجوری اطلاعات رو برگردونم اینکه دونه‌دونه برگردونم یا کلی برگردونم، Get باشه Set باشه قابلیت Create، Update و Remote Procedure از Remote Operation رو Report کنم توى Event استفاده کنم، Call Association Control داشته باشم، Data Encoding چیه؟، توى Transport باشه Over https باشه Over ssl باشه tcp باشه dls باشه باشد شبکه مدیریت شبکه باید در کنار هم دیده بشه یعنی خیلی راحت نمیتونم بگم یه پروتکل شبکه دارم او نجا.

## NM Protocol: Transport

- A L4/7 protocol for end-to-end communication
  - In fact, it is a separated independent protocol
- However, NM protocols impose restrictions on transport protocols
  - Make assumptions and depend on it
  - Management interface specifies it
- E.g.,
  - SNMP: UDP
  - NetConf: RPC on SSH on TCP



7



حالا این کجا قرار میگیره؟ پروتکل مدیریت شبکه اصولاً پروتکل لایه‌ی اپلیکیشنیه و کارکردش و اونچه در ظاهر دیده میشه اینه که «انتها به انتها» است یعنی یک طرف قضیه یک Agent ای هست که نشسته روی یک سیستمی در شبکه و یک طرف دیگر یک Manager ای هست که سمتی نشسته و میخواهد این سیستم را مدیریت کنه. یک بستری برای انتقال یک Communication platform این وسط وجود دارد.

ولی میخوام بگم اون چارچوبه همونه و چیز بیشتری از این نداره. خب این یعنی چی؟

یعنی اگه بخوایم از منظر لایه‌های شبکه، من درواقع باید برم دنبال پروتکل‌ها و چارچوب‌هایی بگردم که در سیستم انتهایی هست و ما میدونیم دامنه‌ش اصلاً انتها به انتهاست نه میانه‌ی مسیر و ما میدونیم این میشه موضوع لایه‌ی 4 به بالا در شبکه لایه‌ی شماره‌ی 4 و 5 در مدل TCP/IP و تو مدل 7 لایه میشه لایه‌ی 4 تا 7.

تمام ارتباطات انتها به انتها اونجا در واقع قرار گرفته و روش صحبت میشه.

ما الان شاید دچار یک گفتمان خاص میشیم من دارم میگم پرتوکل لایه‌ی اپلیکیشنیه بعد میام این پایین میگم که آقا از لایه‌ی 4 به بالا شما درگیری چون انتها به انتهای است این یعنی چی؟ این به معنای ساده‌ی کلمه بخواه بگم وقتی من در مورد پروتکل NMS صحبت می‌کنم پروتکل مدیریت شبکه این پروتکل باید از لایه‌های 7 بیاد تو 6 بعد بیاد تو 5 بعد بیاد تو 4 و حالا بره اون سمت از لایه‌ی 4 و 5 و 6 و 7 عبور پیدا کنه.

می‌خواه بگم پروتکل مدیریت شبکه باید از بین یک خروار پروتکل دیگه در واقع عبور کنه و این یعنی این که اون پروتکل‌ها هر کدام اگه محدودیتی دارن این محدودیته به ارث میرسه برای NMS . یعنی اگه فرضی وجود داره در اونها اون فرضه هم باید به این پروتکل منتقل بشه اگه نمیدونم interface خاصی داره این اینجا هست اگه مورد خاصی داره اینجا هست مثلاً اگه TCP رو سوار بیشیم میدونیم که TCP رفتارش از یک sliding window استفاده می‌کنه و وقتی به congestion بر بخوره اندازه پنجره رو نصف می‌کنه و از این داستانا داره.

اگر من TCP بخواه کار بکنم باید بدونم که همچین رفتاری داره در واقع یه جورایی باید بپذیرم که نرخ انتقال اطلاعاتی میتونه بالا پایین بره . خب ولی اگه UDP باشه میدونیم که reliable نیست و خودم باید یه فکری برای Reliability برای اعتماد در سیستم ارسالم داشته باشم. اینا هست دیگه و باید بهش پاسخ داده بشه .

یا مثلاً SNMP میگه من over udp ارسال می‌کنم خب بعد که میری در مورد SNMP بیشتر می‌خونی می‌بینی که خب نه خب حق داشته که میگه من Over udp میفرستم که خیلی فشار نیاد به شبکه. ولی مثلاً در نقطه‌ی SSH مقابله Net Conf هست Net Config میگه نه ! من RPC استفاده میکنم اونم روی SSH باید باشه و هم روی TCP سوار میشه. زمین تا آسمون با SNMP فرق کرد. ما باید ببینیم کی رو برای کجا و چه شرایطی چه ساختاری می‌خوایم.

# NM Protocol: Remote Operation

- Mechanism to implement performing remote operations
  - Are not a separated protocol
  - Are provided by the management protocol
  - May not present in every NM protocol
- Major functionalities
  - Association control
  - Remote operation call/invocation
  - Payload encoding



8



پس من یه مکانیزم میخوام که این مکانیزم بتونه بصورت راه دور کار کنه این باید هست و در عین حال همهی این چیزی که دارم میگم باید تو قالب یک پروتکل باشد سوار بشه یعنی در واقع یک پروتکل مدیریتی باشه که همهی این بحثایی که ما داریم صحبت میکنیم که راه دور بیاد و کاری انجام و بده و اینا همش باشد در یک قالب قرار بگیره و خب واقعیت اینه که نمیشه و ما همچین چیزی نداریم یعنی ما یک پروتکل مدیریت شبکه که واقعا ندارم که بگم این میاد و حتما در این شرایط و با یک چارچوب از این خبرا نیست!

اما این جز نیازها هست اما نداریم ولی باید ما شرایط رو بپذیریم اگه بخوایم نپذیریم باید خودمون همچین چیزی رو پیاده کنیم.

اصلی ترین کار یک پروتکل مدیریت شبکه رو ببینید : وقتی وارد بحث پروتکل مدیریت شبکه میشیم گفتیم بحث من یک بحث انتقال از راه دوره. خب این بحث انتقال راه دور سه تا موضوع جدی تو خودش داره :

اولین این که دو طرف باید بتونن بهم Join بشن اساسا یک مشارکتی رو باید بتونن با هم راهاندازی کنم و باهم سلام علک کنن. که میشه یک Association Control که اینا بتونن باهم Join بشن چون این مدیره میخواهد با کلی سیستم تو شبکه ارتباط برقرار کنه این میشه همون فاز Association Control.

بعد از اینکه این ارتباط ایجاد شد ما invocation و Remote Operation Call رو می خوایم.

یعنی بعد جوین شدن گام بعدی چیه؟ یعنی من چگونه با سمت مقابل تبادل اطلاعات بکنم از یک Remote Operation Call مثلا بگم فلان چیزو برای بخون اون بخود بخونه من باید یه جوری بهش بگم که فلان چیزو بخون یا اون اگه داره برا من یه سری اطلاعات میفرسته من باید بفهمم زبونش چیه چون این نکته خیلی مهمیه که شما فاز پیاده‌سازی که بری اینو میبینید که زبانی که در ویندوز داره استفاده میشه با زبانی که داره در لینوکس استفاده میشه کاملا متفاوته حتی در پایه‌ای ترین چیزها با هم متفاوتن حتی در فرمت ارسال و دریافت. با همون فرمت ارسال و دریافت میشه فهمید سیستم لینوکسی هست یا ویندوزی یکسری سیگنچرهای رفتاری مشخص داره برا خودش.

من میخوام یک NMS بدارم رو شبکم نمیتونم که خر همه رو بگیرم که بگم شما همتون باید لینوکسی یا ویندوزی باشین که سیستم من باید بتونه با همه این‌ها کار بکنه و Encoding اینا رو یک فرمتی بذاره که شما اگه لینوکسی یا ویندوزی هرچی که هستی باید با این فرمت برای من بفرستین. باید برای تکنکشن تعريف کرد که به مشکل بر نخوریم

# NM Protocol: Remote Operation (cont'd)

## ➤ Association control

- How to establish and tear down management sessions
  - It is independent of transport protocol: connection oriented/less
- Mutual understanding between manager and agent that transport protocol is not aware of
  - E.g., to negotiate a particular functional profile to use

## ➤ Remote operation

- Mechanism to delineate management requests and responses in communication exchanges, E.g., RPC
  - Managing Request/Response IDs because of asynchronous communication due to its efficiency

## ➤ Encoding

- How to encode management data in PDU: BER, XML, UTF-8, ...



9



این سه تا مورد رو بیشتر باز بکنیم: اولیش Association Control بود که خب گفتیم یک session مدیریتی میخواهد شکل بگیره خب من باید Session رو Setup کنم یا Handel کنم یا Session رو Tier Down کنم و در انتهای کنم و بگم خدا حافظ رفته دیگه.

خب این میشه رفتاری که وابسته به پروتکل انتقال در شبکه که حالا پروتکل انتقال در شبکه وقتی ؟؟؟ بشه آیا مثلما من باید این Association که درست میکنم و اون Session که درست میکنم یک

؟ Connection Oriented باشه یا Connection Less

وقتی میگیم Connection Less یعنی اینکه من یه چیزی رو میفرستم برای سمت مقابل بدون اینکه حتی سلام علک هم بکنم انشالله که میرسه اما وقتی میگم Connection Oriented یعنی اینکه اولی برم یه ارتباط اولیه برقرار کنم بعد اگه بشه انتقال صورت بگیره. یعنی یک کانکشنی که دارم و روی اون کانکشن setup میشه و رو اون انتقال اطلاعات دارم.

فرق عمدش در حوزه‌ی Transport یا لایه‌ی 4 وقتی صحبت می‌کنیم فرق عمدشون اینه که اگه سیستم انتقال من Connection Less باشه فشار کمتری به Manager من میاد تا زمانی که سیستم انتقال من Connection Oriented باشه. چون Manager من برای کانکشن Connection Oriented باید همیشه یادش باشه که من کی هستم و اتصالش باید حفظ و بشه ولی تو Connection Less نمیخواهد من یه بسته‌ای فرستادم یا یه درخواستی دارم میگیره و جواب میگیره و تموم شد و رفت. خدا حافظ. پس اینکه من یه گزینه‌ی ساده انتخاب بکنم : آیا پروتکلم Connection Oriented باشه یا Connection Less ؟

خیلی راحت بگم بسته به شرایط کاری اگه هر کدام از اینا رو انتخاب کنم Scalability سیستم من به شدت تحت تاثیر قرار میگیره.

SNMP میاد UDP استفاده میکنه وقتی میاد کارکردش رو میبینه که خوبه .UDP

میگه نه من میخوام Config بکنم تجهیزات تو نمیخوایم خطرناکه! برو روی TCP و از SSH استفاده کن، امنیت همه چیزه. بعدش بیاد ما ببینیم چی به چی میشه یعنی در تعریف Netconfig با توجه به اینکه قرار است اطلاعات بسیار خاص منتقل بشه که مربوط به پیکربندی است اونجا میگیم من Scalability نمیخوام امنیت برای من مهمتره نه اینکه نخوام ولی اول بحث امنیتم باید هندل بشه بعدش میریم میچسبیم به اون یکی. پس ببینید میخوام بگم چارچوب‌ها رو باید حواسمنون بپوش باشه. پس این یه بحث هست که Session رو چجوری میخوام مدیریت بکنم. حالا ببینید من رفتم تو لایه Transport و یک Session گذاشتم قبول! بله UDP یا هرچی که هست اینا قبول. خب این چه ربطی به Manger و Agent داره؟ Manager و TCP تو لایه‌ی Application هست اصن کاری به اون پروتکل TCP و UDP ندارن یعنی نمیبینن اصن اگه ما بخوایم بگم که حالا این در لایه‌ی transport کل این مدیریت میشود من جمله تبادل اطلاعات بین Agent و Manager و اینا یک درک متقابلی از همدگیه داشته باشن من باید بگم نه! همچین اتفاقی نمیفته در لایه‌ی Transport ما واقعا درک مشخصی بین مدیر و Agent نداریم اون پایین نشسته خود UDP و TCP دارن مدیریت میکنن. یعنی اینکه یک Profile مدیریتی مجازی برای خودت درست کن اگه بین Agent و Manager میخواد تبادل اطلاعاتی اتفاق بیفته و همدمیگرو بخوان درک بکنن باید برن تو حوزه‌ی در واقع اون Profile برای خودشون درست کن اونا خودشون همدیگرو بخوان درک کن و بفهمن کی چیکار کرده و چی نشده اون موضوع کاملاً مجزا هست و ربطی به لایه‌ی Transport نداره.

یک جا هست که بحث Remote Procedure Call را مطرح میکنم که من میخوام از راه دور یک عملیاتی انجام بدم مثلاً میخوام که یکسری اطلاعات رو Get کنم مثلاً بگم الان دمای CPU چقدر؟ و از این قبیل چیزا.

وقتی میخوام این کارا رو بکنم TCP و UDP این چیزا رو به من نمیده به اینا نمیتونم بگم من چقدر کجا باید برم؟ باید براش یک Remote Procedure Call بنویسم بهش تیکت بدم بگم فلانی RAM Utilization ت چقدر؟ فلانی CPU Utilization ت چقدر؟

پس من یک RPC میخوام که بهش بگم فلانی من الان اینو میخوام ازت برو برام این کارو بکنم. Remote Procedure Call! یک Agent نشسته و اون اونجاست درخواستم پاسخ بده و یه Response برگردونه این حداقلش اینه که یه ID باید داشته باشه بین Manager و Agent باید یک ID داشته باشه که ببینیم این درخواست که برگشته برای کیه؟ کی بود؟ چی بود؟ چی داشت میگفت؟ اصن برای چی اینکارو کرد؟ یعنی یک asynchronous communication میخوایم یک ارتباط ناهمگام و ناهمزمان دارم هیچ موقع Manager من واينميسته تا ابد منتظر درخواست. نه بسیار از اوقات باید بصورت asynchronous مدیریت بکنیم که من یه درخواستی میدم حالا این بره انجام بده فلانی تو هم بگو فلان و Manager هم نشسته کار خودشو میکنه.

فلانی درخواستش اومند! اومند خیلی هم خوش اومند ما بررسی میکنیم. نمیذارم سرورم وايسه منتظر خب حالا فلانی جواب بده من بشینم چیکار بکنم. سیستم مدیریت شبکه میخواد کار بکنه پس باید کار بکنه. یه درخواست که میده بفرسته بره یعنی بشینه کارای دیگش رو بکنه هرموقع که اومند بره دنبال کارش بشینه چکار میخواد بکنه پس این باز یکی از بحثهایی هست که در RPC بهش توجه کنیم.

گزینه‌ی بعدی که وجود داره بحث Encoding هست خب من میخوام یک RPC داشته باشم اینو به چه زبانی بفرستم؟ مثلاً Microsoft در اوایل سال 2000 خیلی تلاش کرد که همه چی رو Over XML منتقل کنه چرا؟ چون XML به فرمت خیلی ساده است.

مثلاً اگه من بخوام فارسی بفرستم Encoding م حتماً باید UTF-16 باشد یا UTF-8 خب نمیتونم بیام بگیم که حالا زبان فارسی رو میفرستیم Over Encoding های قدیمی داده‌های ما و وقتی میرسه به مقصد میشه خرچنگ قورباگه. مثلاً اگه بخوایم Over Ascii بفرستم هم همین میشه اینایی که ما انتخاب میکنیم گزینه‌های تاثیرگذاری هست. مثلاً restful api که شما استفاده میکنی یا JSON این بحثاً اینا همش Encoding های

مشخصی داره برای داده‌ها که داره استفاده میشه و شما وقتی میخوای وقته انتخاب کنی با چه Encoding‌ی دارم اینکار میکنم اینا رو باید مشخص کنی. باید بری رفتار اون XML یا UTF-8 یا .. چیه بعد ارزیابی بشه با توجه به رفتار به کجا ختم میشه؟ یعنی همینجوری نیست که من یه چیزی رو بردارم و بگم از این استفاده کنیم. رفتارش باید بررسی شه نیازمندیش باید بررسی بشه و آیا میخوری به کاری که میخوایم بکنیم؟ مثلا من میخوام یه پرتل مدیریت شبکه داشته باشم آیا این اصلا به درد میخوره و ارزش داره؟ یا نه؟

اینا موضوعات مهمی هستن که به راحتی نمیشه ازشون گذشت.

## NM Protocol: Management Operations

- The core of management protocol stack
  - Management primitives
- Typical operations
  - Read/Get: To read the value of a MO
  - Write/Set: To modify the value of a MO
    - Create or Deletion of a MO
  - Event: To report occurrence of event to manager
  - Action: To perform an operation on agent
  - Some rarely used: subscribe, ...
- Not every protocol provides all operations



من برای بحث مدیریت شبکه باید یک پشته‌ی پروتکل مدیریت در شبکه برای خودم ایجاد کنم یک Stack.

یک Management Protocol Stack میخوام. یک پشته‌ای که کارش توی حوزه‌ی مدیریت پروتکل باشه و این مرکزش میشه اون کارهای پایه و کلیدی و اساسی که در مرکز اون پروتکل وجود داره.

حالا این کارای پایه‌ای چیه؟

مثلا من دستور Read یا get دارم. فلان مقدار رو برای من بخون و بیار این یه کار پایه‌ایه یه سری دستورات هم هستن یا Write مثلا آقا بیا فلان گزینه رو توی حافظه رو بنویس یا فلان محدودیت رو اعمال بکن. دمای آلام CPU رو از 75 درجه بکن 73 این یه نوشته. وقتی Write مطرح میشه میتونه Update هم باشه یا میتونه Config باشه و وقتی شما Delete میکنی خیلی معنا داره میتونه Crash میگه که میخوای بریزه. میتونه در حوزه‌ی Event ها باشه مثلا من سیستمم یه دفعه Crash میکنه بعد Crash میگه که میخوای به مايكروسافت خبر بدم؟ میخوای به این تیم پشتیبانی خبر بدم که اینطوری شده؟ این یه Event هست و Manager شروع نکرده و خودش سعی میکنه به تیم پشتیبانی خبر بده که اینطوری شده این اتفاق افتاده و کرش کرده.

ما یکسری Action هم داریم در سمت Agent وقتی من بهش میگم Get کن یه چیزی به من بده باید بره یه کاری بکنه پس یه Action داره وقتی میگیم Set کن این باید باز بره یه کاری بکنه دیگه یه چیزی رو بنویسه پس این get و Set ها در واقع چارچوبهای خودش رو دارن که باید بهشون پرداخته بشه.

خب حالا این وسط ممکنه برخی Operation های خاص دیگه هم بسته به کار مطرح بشه مثلا Subscribe بشه برای انجام فلان کار اینا رو بذاریم کنار که چه کارکردهای دیگه ای میتونه داشته باشه اصلیاش همینا بود که گفتمیم : get , set , event , action

نکته : ما هیچ پروتکلی نداریم تو دنیای مدیریت شبکه که همه اینا کارها رو باهم بکنه یعنی همه این چیزایی که داریم صحبت میکنیم که فلان چیز خوبه و اینا. هیچ پروتکلی در دنیای شبکه ما نداریم هیچ درواقع هیچ Provider ی نداریم که اصن بتونه همچین پروتکلی رو بسازه و درواقع این سرویس‌ها رو ارائه بکنه برای همه‌چی.

ما در مورد Operation ها صحبت کردیم حالا ببینیم خودمون سرویس مدیریتی رو نگاه بکنیم به هر حال من یه عملیاتی که میخوام انجام بدم این قراره یه سرویسی تو خودش داشته باشه دیگه بیخود که نیست.

## NM Protocol: Management Service

- Additional offering to management applications
- Builds itself on the Management Operations layer
  - Combine the management primitives with additional capabilities
- Examples
  - Subscription to specific events
  - Scheduling management operations
- Actually management services are not really a layer because management operations are still accessible to management applications



خب تو اون سرویس مدیریتی ما میتوانیم بگیم که آقا مثلای این اطلاعات رو بهم بده من فلان سرویس رو هم بهت میدم نمودارشم رسم میکنم و Utilization هم میگم چقده اگه به این قدر رسید بدون آلام بدم و اینا.

وقتی من دارم از سرویس مدیریتی حرف میزنم صرفا این نیست که حالا ما یک حضور یا عدم حضور باشه این داره یک توضیحات اضافه‌ای رو در حوزه‌ی اپلیکیشن‌های مدیریتی میده.

خب الان چی شد؟ من یه سری Operation های پایه عملیاتی داشتم توی اسلاید قبلی الان میگم که الان شما اگه سرویسش رو هم بگین من فلان کارها رو هم برآتون میکنم یعنی یه سری توانمندی‌های اضافی رو هم داره به سیستم اضافه میکنم میگم اینکارا رو هم میتونم برات بکنم پس یه پله میریم جلو! میگیم خب اینکارای بیسیک هست یکسری هم توانمندی هم هست که قولشو داده تو اون سرویسه به من بده. مثلا به من بگه که من

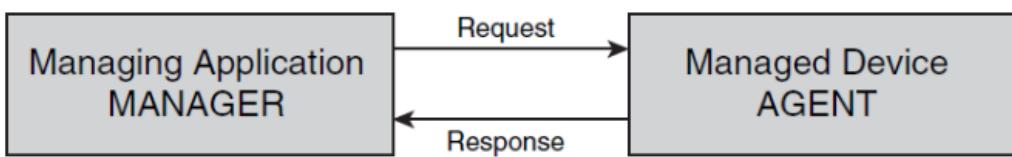
Schedule میکنم رویدادهای مدیریتی تو رو با یک سیستم . کن من حواسم بهش هست. یا مثلاً اگه فلان اتفاق افتاد سریع به من تیکت بده بگو که اینطوری شده.

سرویس‌های مدیریتی هم در یک لایه‌ی مشخصی قرار ندارن چون که در اون عملیات‌های مدیریتشون چون باید از مسیرهای اپلیکیشن‌های مدیریتی مختلف در واقع عبور بکنه و Accessable بشه و قابل اجرا باشه بنابراین من نمیتونم بگم که سرویس مدیریتی توی یک لایه نشسته نه این بسته به عملیات و کارکردها میتوانه در لایه‌ی مختلفی قرار بگیره.

## Manager-Initiated Communications

### ➤ Request-Response paradigm

- A manager makes a request
  - To get/set/create MO or perform action
  - Includes request type, parameters, and headers
- Agent sends a response
  - Includes a return code, result, and headers



یه پله بریم جلوتر یک موضوعی که ما صحبت کردیم گفتیم در یک سیستم مدیریت شبکه باید نگاه بکنیم این است که خب در این دنیای تبادل اطلاعات کی شروع کنه؟ شروع کننده کی باشه؟ شروع کننده‌ی ارتباط.

به صورت پیش‌فرض وقتی ما این حرف رو مطرح کنیم اولین گزینه اینه که خب شروع ارتباط برای من از سمت مدیر خواهد بود و مدیر یک ریکوئست میده به Agent و او پاسخ میده که اینجوریه موضوع.

ریکوئست میتوانه `get` و `set` یا یک در واقع درخواستی باشه که فلان کار رو برای من بکن. پس میتوانه این ریکوئست من خیلی ساده باشه یا خیلی پیچیده و ساده و پیچیده بودنش تو خودش `pipe` های مختلفی داشت مثل انواع `get`, `set` میتوانه انواع مختلف و پارامترهای مختلفی میتوانه داشته باشه. `Header` های متفاوتی میتوانه داشته باشه.

ما به ازاش میره به `Agent` و اون هم با توجه به `Request` کاراش رو انجام میده و پاسخی میده حالا اون جواب چیه؟ ممکنه یه گزارش باشه یا ممکنه یه کد وضعیتی باشه. پس اینکه پاسخ چی باشه یه موضوع مهمیه که بر میگردد به طراحی پروتکل که این `Response` یک کد بازیابی هست یه زمانی هم میشه مسائل بحث `Header` ها.

## Manager-Initiated Communications

### ➤ Information Retrieval: Polling

#### ➤ Basic types

- Requests for Configuration Information
- Requests for Operational Data and State Information

#### ➤ Advanced types

- Bulk Requests and Incremental Operations
- Historical Information

### ➤ Configuration Operations

#### ➤ Main issue: Failure Recovery

### ➤ Actions



یه سوال دیگه : مدیر میخواد یه اطلاعاتی رو بگیره چجوری بره سراغ کلاینتی که این اطلاعات رو بگیره؟

اولین ایده‌ای که به ذهن میرسه polling کردن یعنی سرکشی کردن که انواع مختلف داره اطلاعات پیکربندی رو میتوانه درخواست کنه یا داده‌های عملیاتی مثل داده‌های وضعیتی این رو با polling انجام میدن.

من مدیر هرچیزی رو که لازم دارم به Agent میگم که این اطلاعات رو به من بده این polling هست یعنی سرکشی. این اطلاعات میتوانه یه درخواست ساده باشه یا اینکه این اطلاعات میتوانه به صورت heuristic و بزرگ باشه. مثلا یه سری اطلاعات تاریخچه‌ای من میخوام بدونم log‌های یک سیستم رو بررسی کنم از منظر اینکه آیا مثلا یک کشف مهاجم داشتم یا نه؟ بدرفتاری در سیستم داشتم یا نه؟.

من اگه حجم اطلاعاتم کم باشه با همون اولیا؟؟ میتونم بفرستم ولی یه جاهایی هست که حجم درخواست ما خیلی زیاده و این باعث این میشه که خب وقتی من درخواستام زیاد بشه باعث میشه یه نوع خاصی از پیامهای http رو درخواست کنم که از پیامهای Agent دریافت کنم حالا اگر یکی دوتا باشه مشکل حله اگه زیاد باشن به این شکل نمیشه ما اینجا تعریف میکنیم یه سری Request‌ها داریم به اسم Bulk Request که به صورت انبوه اطلاعات رو ارسال میکنن. خب یه سری هم اطلاعات تاریخی هست که ما داریم حالا دیگه چی میخوایم؟ یه سری درواقع اینکه مدیر شروع کننده باشه میتوانه برای یه سری درخواست‌های پایه باشه یه سری درخواست‌های پیشرفته یا مثلا میتوانه اطلاعات مربوط به پیکربندی باشه.

یه سری عملیات‌های عملیات‌های پیکربندی هستن نکته‌ی مهمش اینه که زمانی رخ میده که من یا اصن سیستم تازه داره وارد شبکه میشه که داره پیکربندی میشه یا اینکه ما میداریم و استفاده کنیمش برای اصلاح خرابی. و خب وقتی مدیر داره از کلاینت یا ایجنت سوال میپرسه به صورت مشخص این کلاینت یا سرور اون کلاینت یا سیستم مورد نظر ماست که باید بیاد و یه کاری رو برای من انجام بده.

## Manager-Initiated: Information Retrieval

- Polling mechanism steps:
- The manager asks the agent for a particular piece, or pieces, of management information
- The agent checks the validity of the request and retrieves the requested information
- The agent then responds,
  - The requested information
  - An error-response code why request could not be fulfilled
- An error message is sent in case the agent
  - Does not understand the request
  - Does not know the type of management information



14



حالا این چیو انجام میده؟ این polling ما مراحل مختلفی داره مثل Manager میاد میگه که یه تیکه از اطلاعات رو بهم بدین خب پس Manager من برای یک محدوده‌ای یا حجمی از اطلاعات درخواست میده.

این درخواست رو میگیره باید چک بکنه که ببینه اصن درخواسته معتبره یا نه؟ مجاز هست یا نه؟ Agent میتونه همچین درخواستی مطرح بشه یا نه؟ که اطلاعات برگرده اگه مجاز بود که میتونه اطلاعات برگرده اگه نه که نمیشه.

پس این یه بحثی هست که مطرح میشه که Agent من باید بررسی کنه که درخواست یک درخواست معتبر بوده حالا بر اساس اون پاسخ بده. و خب Request در واقع بعد از اینکه حالا رو گرفت و دید معتبره باید پاسخ بده برای این پاسخ هم باید بره یک Action را انجام بده و اطلاعات مورد نظری رو بگیره و بیاد بگه خب اطلاعاتی که وجود داره چی هست و به چه شکلی هست. باید بیاد و درواقع از این موضوع استفاده کنه برای اطلاعات درخواستیش رو بپردازه.

یه پله بريم جلوتر وقتی خواست اين اطلاعات درخواست شده رو بفرسته موضوع اينه که ممکنه درخواست من يك درخواست معتبر نباشه اينجا ممکنه به ازاي Request اطلاعاتي که درخواست شده يك گزينه‌ي درخواست بشه که ميدونى چيه اصن درخواست شما مشکل داره درواقع يك Error Code برگردونيم برای اينجا. من دو حالت دارم برای Response يکی اينکه من بگم اون اطلاعات مورد درخواست شما اينه و خدمت شما و دوم اينکه بگيم نه درخواست شما مشکل داره من نميفهممش ايني که من نميفهمم سه حالت داره که يکی اينکه در واقع بگه که نميفهمم چي داري ميگي و حالت دوم اينکه بگه من ميفهمم چي ميگي ولی پارامترهايی که برای من فرستادي مشکل داره من با اين نميتونم جور کنم با اين پارامترهايی که فرستادي مثلا Type اطلاعاتي که خواستي اشتباهه يه بحث ديگه هم ميشه درنظر گرفت مثلا اگه من يه سطح دسترسی به اطلاعات داشته باشم ميتونم درخواست بكنم بگم که سطح دسترسی به اطلاعات رو نداري. مثلا در ابزارهای Cisco که داريد کانفيگ ميکنيد يکسری درخواست ها رو ميتوانيد به صورت ساده درخواست کنيد که ShowConfig رو بهم بده برای يکسری چيزهای خاص ShowIp بگيريد به صورت خيلي معمولی بهتون اطلاعات مدیريتی مиде ولي يه جايی هست که شما ميخوايد بريت توی مدي که پيكردبندی کنيد همون فرایند کاري که تو سيسکو انجام ميدين به شما Error مиде که اول شما برو تو مد Privilage بعد من به شما اجازه‌ي دسترسی بدم اينو به عنوان يه جور پاسخ دارم يا واقعا چيزی که خواسته رو برميگردونه يا پيغام خطأ مиде که اين پيام به اين دليل پاسخی ندارد.

# Polling (cont'd)

- Requests for configuration information
  - Physical or logical configuration information
    - Discovery, Provisioning, Fault, ...
  - Typically infrequent and (maybe) external changes
    - Caching is efficient → Management DBs
- Requests for operational and state information
  - Network monitoring → Fault detection, performance, accounting, ...
  - Manager cannot change the information
  - Typically frequent changes
    - (Typically) no Caching DB; on demand snapshots
- These requests can also be
  - Bulk request: Ask several MO which has the same attributes
  - Historical information: Snapshot of management data in an interval



15



Polling رو ادامه بدیم ببینید گفتم که میشه سرکشی کردن. این میتونه شامل بحثهای مختلفی باشه ولی معمولاً بحث اصلی که وجود داره اینه که درخواستی داشته باشه در حوزه اطلاعات پیکربندی مثلاً بگه که اطلاعات پیکربندی فیزیکی یا منطقی فلان تجهیز رو بهم بده یا این اطلاعات رو ثبت بکن براش که بحث Discovery میتونه باشه که یه سختافزار جدید اضافه شده چه بحث یک Service Provisioning که یک سرویسی درواقع فراهم شده بحث Fault هست که میتونه مطرح بشه. این اطلاعات وجود داره تو بحثاً و میتونه مدنظر قرار بگیره.

یه نکتهای که وجود داره اینه که ما این اطلاعات مربوط به پیکربندی رو اگه بحثمون باشه میدونیم این اطلاعات خیلی خاص هستن نیست که من هر روز صبح که پامیشم پیکربندی دستگاه‌ها عوض کنم این اطلاعات خیلی به ندرت و خیلی کم درواقع تغییر میکنن مگه اینکه یه اتفاق خاصی بیفته یه پورتی اضافه بشه یه غیر فعال و فعال بشه یه چیز اینطوری میتونه تغییرات به وجود بیاره پس راحتترین کار اینه که بگه اگه دنبال اطلاعات پیکربندی هست این اطلاعات رو توی حافظه بذاریم هر موقع خواستن از اونجا برش داریم بدیم. اصن میشه یه

دیتابیس مدیریتی گرفت و اطلاعات رو تو اون گذاشت. در نتیجه خیلی راحت از این جا میشه برای درخواست کننده فرستاد.

دومین دسته از اطلاعاتی که میشه درخواست داد درخواست برای اینه که شما بردید یک عملیاتی رو انجام بدین یا یک State ی رو رصد کنید ببینید چی میشه این وضعیت در واقع چجوری هست مثلا من میخوام یک Network Monitoring بکنم شبکم رو ببینم مثلا ئه اینجا سیستمه رفت الان اینجا 20 درصد utilize شده مثلا 20 درصد از حجمش رو مصرف کرده این 40 گیگ تو این ماه مصرف حافظه داشته خب این بحثهای Network Monitoring Accounting , Performance , fault detection درخواست کنیم که این اطلاعات رو بهم بده. خب این اطلاعات وقتی میاد Manager این اطلاعات رو نمیتونه عوض کنه بر خلاف Configuration. توی Configuration مدیر اگه دسترسی داشته باشه میتونه عوض کنه میتونه get , set کنه ولی اطلاعات Cpu Utilization مثلا Network Monitoring 60 درصده به من چه من چیکار میتونم بکنم؟ عوضش کنم؟ دستوری نیست که بگی که این عدد عوض بشه.

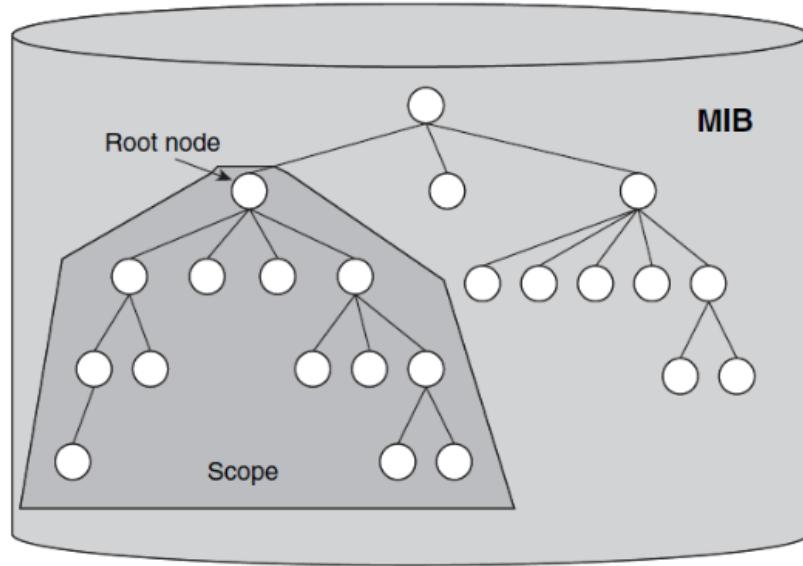
سیستم مدیریت شبکه نمیتونه این اطلاعات رو دستکاری کنه. و نکته اینه که این اطلاعات دائما در حال عوض شدنه اگه Traceroute بگیریم میبینم که تاخیرات لحظه‌ای دائم بالا پایین میشه و هیچ چیز ثابت نیست و داره عوض میشه. این رو باید بگم On-Demand هر موقع خواستیم بهمون بده.

یک نکته‌ای اینجا وجود داره این که وقتی polling اتفاق میفته درخواست‌هایی که میاد تو این حوزه این درخواست‌ها میتونه جنبه Bulk داشته باشه میتونه یه دفعه 7 یا 8 تا درخواست بده میتونه بگه تمام این سیستم شما که او مده به من بگو CPU Utilization و Ram Utilization و ... دمای CPU چقدر و خیلی چیزی دیگه چقدر. همه اینا رو بهم بگو. همه اینا رو در یک درخواست میشه گفت همه اینا رو برو برام بیار.

به این میگیم Bulk Request یعنی توده‌ی انبوه. چندین سوال داره با پارامترهای مشخص و مشابه. و این اطلاعات هم میتونه حالت تاریخچه‌ای باشه مثلا بهم بگه که در این زمان انقد فشار بوده روش بعد انقد شده بعد انقد شده مثلا فشار روی لینک شبکه درخواست بکنیم خب اصن این فشار لینک شبکه Utilization شما انقد بوده اطلاعات آماری هست درواقع. اطلاعات تاریخچه‌ای هست و در بازه‌های زمانی مختلف هم مشخص شده که چقدر است. بصور مشخص Bandwidth روی لینک‌های شبکه که میشه درآوردن اینا اطلاعاتی هست که دائم درخواست میشه. و میشه گفت از الان به مدت 5 دقیقه ثانیه به ثانیه Utilization رو برام گزارش کن.

# Bulk Request

- Bulk request operation when MIB view is a tree



16



حالا نکته‌ای که قبلاً بود به اسم Management information Base گفته‌یم یک پایگاه داده‌ای است که اطلاعات مدیریتی رو تو خودش نگه میداره اتفاقاً در حوزه‌ی SNMP ما پایگاه دادمون اتفاقاً اسمش MIB هست پس من دو تا MIB دارم یکی به مفهوم عام یه پایگاه داده‌ای که یه اطلاعاتی تو ش ثبته و یکی دیگه که به صورت خاص برای SNMP ئه هست پس این رو حواستون باشه.

API من یک مفهومون کلی داره که برای همه‌ی سیستم‌عامل‌ها می‌تونم بگم که Microsoft API هست و یه دونه API هم دارم که برای Linux اینم یعنی دیگه‌ای داره.

توی SNMP MIB یک ساختار درختی داره و شما وقتی می‌خوای یک درخواستی بپرس بدی باید تو این ساختار درختی بری و حالا اون به صورت سلسله مراتب توی Scope‌های مختلف حرکت حرکت می‌کنه و بهتون میده. مثلاً وقتی شما می‌گی تجهیز Cisco را می‌خواهی تجهیز Cisco توی این شاخه هستیم میری توی زیرمجموعه تجهیزات Cisco بعد می‌داد می‌گی که برای این تجهیزات فلان پارامتر رو می‌خواهی توی Router هاش برو دنبال فلان پارامتر. بعد میره تو قسمت Router‌ها یک ساختار درختی داره.

تجهیزات مایکروسافت هم ساختاری درختی خودش را دارد. پس این MIB ئه به حالت درختی داره و محصولات هر شرکت هم جدا میشه و ما در Scope های مختلف میتونیم به عناصر اطلاعاتی دسترسی پیدا کنیم. مثلا وقتی توی SNMP Request میاد مثلا میگه این شاخه رو انتخاب کن و دقیقا مسیر رو بهش میدیم و میگیم این نقطه این نقطه این عدد : 2.2.1.1 بعد میگیم مقدار اینو بهمن بده. همش هم عدد و اون عدد های متولی رو با نقطه جدا شدن اون اعداد رو بهش تو این درخته حرکت میکنه میرسه به اونجا میگه مقداری که میخواستی این مقداره.

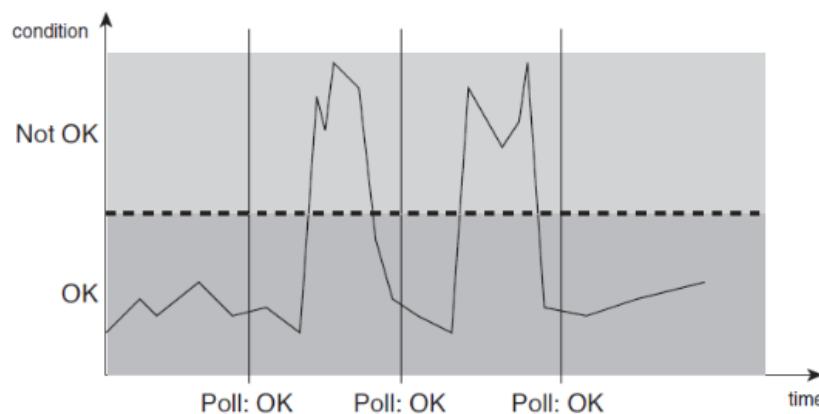
## Polling Disadvantage

### ➤ Frequent polling

- Expensive & High overhead : high management traffic!

### ➤ Infrequent polling

- Miss critical condition
- Long delay to find out critical conditions



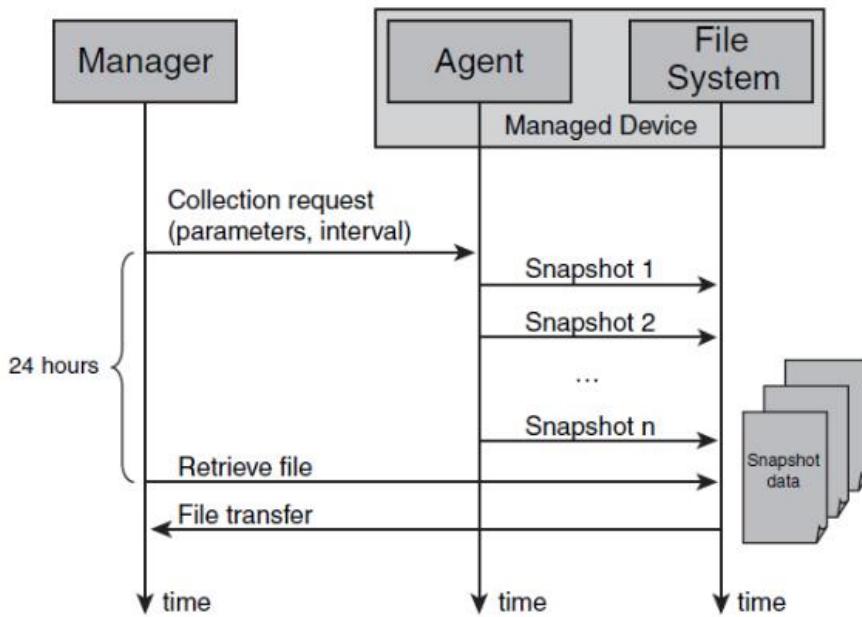
سوال: آیا Polling خوبه؟ یه سری جاها بله خوبه ولی آیا همه جا خوبه؟ نخیر همه جا خوب نیست چرا؟ ببینید توی polling سرور من باید بیاد بگه که فلانی شما چیکار کردی مث معلمی که میخواهد درس بپرسه.

وقتی من یکی یکی بخوام تک تک سوال بپرسم زمان بره و کلی وقت باید صرف بشه که فقط سوال بپرسم میخواهم بگم که اگر من polling م یک فرایند هست خیلی پر تکرار هست این خودش هزینه بره و خودش اصن بار ترافیکی برای من ایجاد میکنه ترافیک مدریتی سنگین ایجاد میکنه که من فقط سوالاتم رو بپرسم. وقتی

من میخوام Trueput شبکه روی لینک اندازه بگیرم مثلا اگه بخوام بگم الان این چقدر Utilize شده مثلا یه اتفاق افتاده من باید Utilization شبکه رو همون لحظه ببینم که این لینکه Dos Attack رفت رو 60 درصد این نباید اینجوری میشد. همون موقع باید من اینو باید ببینم که این Attack مشخص بشه که onfrequent polling باشه میگم خب 5 دقیقه‌ای ئه. یعنی یه شرایط بحرانیه من همون لحظه اگه polling باشه میگم خب 60 تا درخواست بدی یه بار یه Snapshot از شبکه بگیر کافیه یا دقیقه‌ای یه بار نمیخواد ثانیه‌ای بگیری و 60 تا درخواست بدی شکل اسلاید رو ببینید اینجا polling کرده و این اکی کرده تا poll بعدی رفته بالا و Not Ok شده وسط همونا خراب شده و جهش داشته. کاربر زنگ زده گفته گیره ولی شما میگید نیست. کاربر نسبت به شما بدین میشه.

اگر من polling م به صورت infrequent باشه و با نرخ خیلی کم رخ بده اتفاقی که میفته اینه که من شاید خیلی از شرایط بحرانی رو نبینم اصلا و از دست بدم. و چار پارادوکس شدم اگه polling زیاد بشه به شبکه فشار میاد خود دارم فشار میدارم پرخرج و پرهزینه میشه و سرور شبکه من به مشکل برミخوره. اگر هم infrequent نباشه کند پیش برم شرایط بحرانی و حساس رو از دست میدم باید چیکار کرد؟

# Alternative Polling Mechanism



➤ Advantage? When is applicable?



18

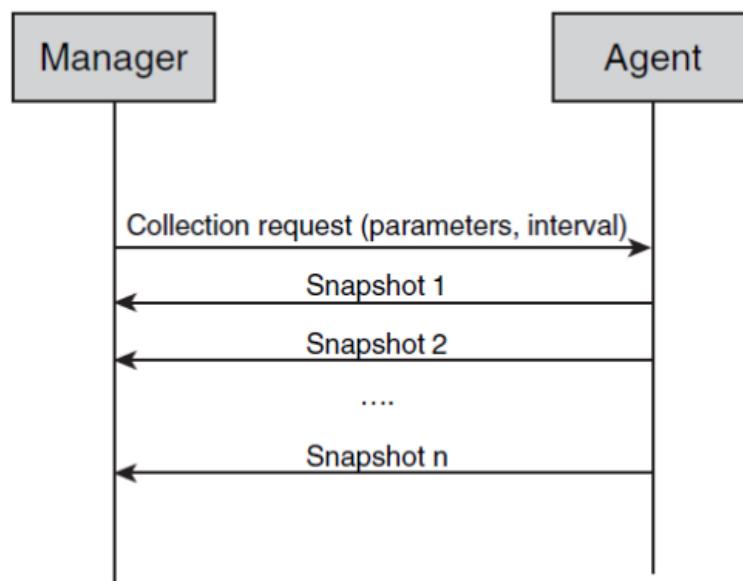


کاری که باید کرد اینه که باید سراغ یک جایگزین رفت برای سیستم polling یک جایگزین فراهم کنم و بگم که حالا به جای اینکاری که میکنی اینجوری به من جواب بده. مثلا : جایگزین اینه مدیر بیاد بگه که جناب سلام من از شما درخواست دارم فلان پارامتر رو به صورت ثانیه‌ای برای من به مدت 24 ساعت مانیتور کنید. من فردا میام اطلاعات رو ازت میگیرم این Agent شروع میکنه مثلا به صورت دقیقه‌ای مانیتور میکنه هارد رو مانیتور میکنه فردا که میشه میگیم جناب Snapshot هاتون رو لطفا به من بدین داده‌هایی که جمع کردین رو به من بدین. اونم فایل‌ها رو برミگردونه. خوبیش اینه که من تو 24 ساعت نرفتم سراغ Agent میدونه که باید این کار رکنه منم میشنیم کارامو میکنم فردا سر فرصت رفتم گرفتم آوردم حالا میتونم تمام اطلاعات 24 ساعت گذشته رو ببینم ولی ببینید من توی 24 ساعت هیچ اطلاعاتی ندارم اینو حواستون باشه!

تا زمان تموم نشه و من نگیرم هیچ اطلاعاتی ندارم باز اون بحث شرایط بحرانیه سرجاشه و میتونه اتفاق بیفته و عملا من گیر کنم ! پس اینو باید حواسمون باشه. ولی خب خوبه وقتی شرایط خیلی عادیه مثلای یک چیزی رو

پایش کنم که شرایط شبکم چطوریه؟ توی شرایط معمولی خیلی خوبه، مثلا آخر شب که شبکه خلوته مدیر Request میده فردا شب آخر شب اطلاعات رو میگیره. برای بحث‌های Planing خیلی خوبه که من این اطلاعات 24 ساعت آماده‌ای صورت گرفته بعد 24 ساعت مهاجم اومنده زده برد و بعدش من خبردار میشم اصلا برای بحث آیا حمله‌ای به دست من نمیخوره. فقط همون بحث‌های Planing و آموزش و اینا خوبه.

## Alternative Polling Mechanism (cont'd)



- Advantage? When is applicable?



19



ایده دیگه میتونه این باشه مدیر میتونه بیاد به Agent بگه که من این اطلاعات رو میخوام و به من بدمش مثلا به من دقیقه‌ای به مدت 100 دقیقه این اطلاعات رو برگدون اونم شروع میکنه اینم یه ایده هستش خوبیش اینه که مدیر من نمیاد 100 تا درخواست بده فقط یک درخواست میده میگه در همین بهم بده و Agent هم میاد این رو بهم پشتسر هم بهم میده. این یه جایگزین دیگست.

# Manager-Initiated: Configuration

- To change configuration information
- Parameter settings to affect agent's behavior
- Some aspects are fundamentally different from information retrieval requests
  - Failure recovery
    - Failure in configuration is much more than information retrieval
    - Configuration is much more sensitive to failures
  - Response
    - Response of configuration requests are typically a success/failure status code not huge data



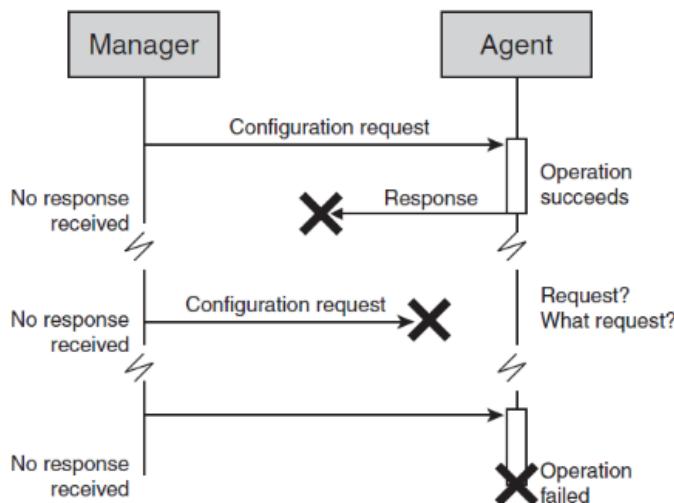
یکسری از درخواست های مدیر درخواست های پیکربندی بود وقتی به اون Configuration ها نگاه میکنیم یک چیزی رو میبینیم که ما وقتی Config را عوض میکنیم مشخصاً روی رفتار Agent میتوانه موثر باشد. و اصلاً تو برخی موارد هستن که اصولاً متفاوت هستن از این بحث های Configuration و این ها.

مثلاً وقتی ما درخواستی میدیم برای اینکه اطلاعاتی به ما داده بشه در حوزه‌ی Failure Recovery وقتی این موضوع مطرح میشه مثلاً من یه Config را میخوام انجام بدم اون Config رو انجام میدم Down هم میکنم اوکی میشه و میره دارم میزنم سیستم رو فعال میکنم بعد میبینه ئه یک مشت خطا دارم میگرم. و من متوجه یک Failur در شبکه میشم تغییر در پیکربندی باعث ایجاد خطا شد و اون خطا باعث شد کلی آلام و اطلاعات دیگه‌ای برای من برگرده پس در این حوزه من باید به این نکنه دقت کنم که وقتی Failure رو مطرح میکنم و تغییر در پیکربندی رو مطرح میکنم این تغییر در پیکربندی میتواند شرایط حساس برایم ایجاد کند و میتواند

خرابی‌ها رو بیشتر کن. وقتی Failure‌ها بیشتر می‌شه اتفاقاً به نسبت یک شرایط معمولی کسب اطلاعات اتفاقاً می‌تونه برای من بیشتر آسیب‌زا بشه و در دسرساز بشه این رو در نظر بگیریم. شاید اگه او نو بپذیریم به نفع‌مون باشه. چرا؟ چون خیلی از وقتاً من Config می‌کنم اطلاعاتی که برمی‌گردید اینه که این Config شما تو سیستم نشست یا ننشست می‌اد کد وضعیتی به ما برمی‌گردونه و همین. این رو باید در نظر داشت که اون تغییر پیکربندی می‌تونه آسیب جدی به سیستم بزنه.

## Configuration Operation: Failure

- It is not easy to handle failures in configuration
  - Different failures
  - Different configuration (behavior effects)



مثلاً مدیر Configuration Request داشته عملیات موفقیت آمیز بوده اما Response‌ی که برمی‌گردد گم می‌شه و به مدیر نمیرسه. حالت دوم: درخواست میره و به Agent نمیرسه و اونم کاری نمی‌کنه

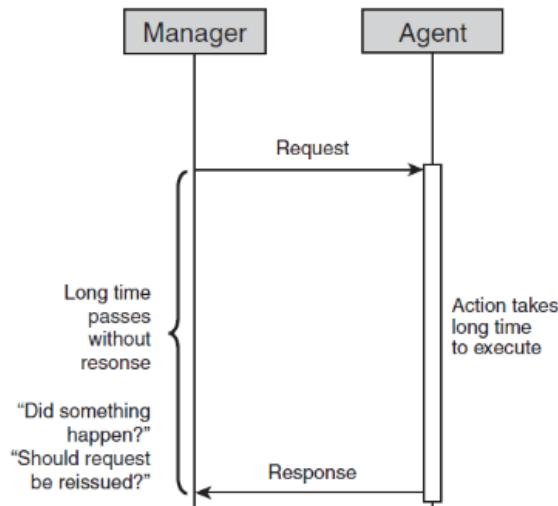
و حالت سوم اینه که درخواست میره و Agent نمیتونه اون عملیات رو Commit بکنه و تایید بکنه و تمومش کنه. من سه تا حالت مختلف دارم که در هر سه تا هم مدیر درکی درمورد موفقیت آمیزبودن یک عملیات نداره.

Commit ها انواع مختلفی دارند و در پی Configuration مختلف رفتارهای مختلفی دارند اولی Failure شده و اتفاق افتاده ولی مدیر متوجه نشده دومی اصن به Agent نرسیده سومی هم رفته و Faild شده وقتی اینطوری شده باید حتما سیستمی داشته باشم که پیکربندی رو بهم زده رو سومی نکته مهم اینکه رفته پیکربندی رو بهم زده و سیستم در شرایط ناپایدار قرار میگیره پس من باید این حتما Roll Back ش کنم به نقطه‌ی Safe قبلی. وقتی تغییری انجام میشه یا باید Commit بشه صدرصد یا به حالت قبل برگرد. حالت سومی بدترین حالته و حتما باید به شرایط قبل برگرد.

پس وقتی پیکربندی عوض میشه حالت‌های مختلف خطا میتونه اتفاق میتونه بیفته و بسته به نوع خطا خیلی اثرگذار هست روی رفتار بعدی شبکه.

## Manager-Initiated: Actions

- To request device to perform certain action: self-test, ping,...
  - Manager requests an action
  - Agent runs the action and sends the output

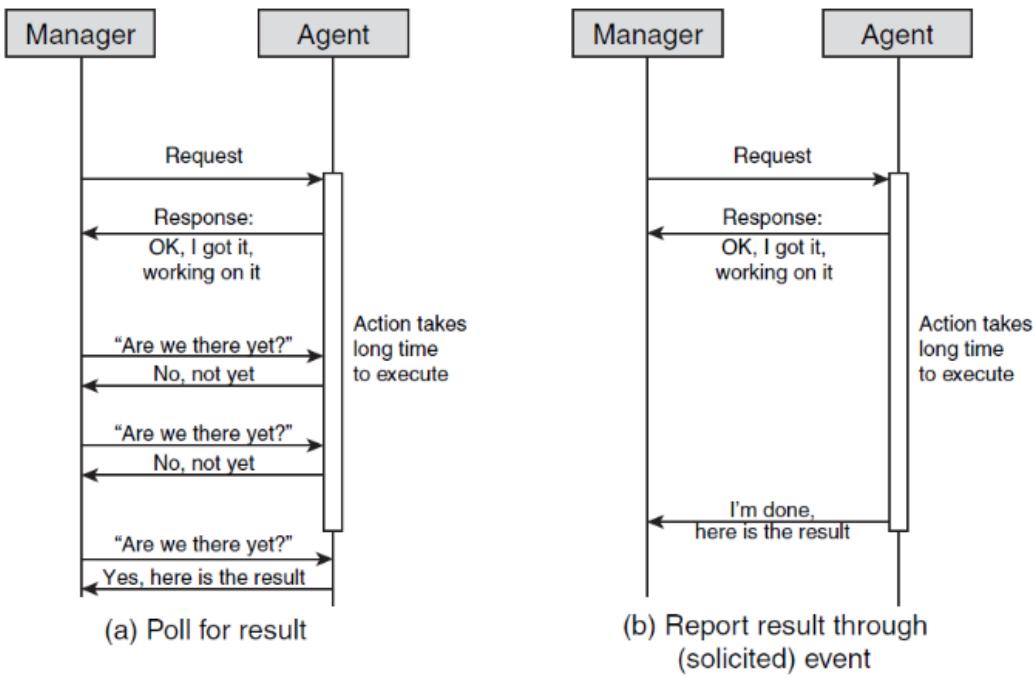


22



یک موضوع دیگه هم هست که باید نگاه بکنیم من وقتی مثلا میگم که Agent برو اینکارو بکن وقتی اینو میگم میخواود اون کاره رو بکنه میره انجامش میده و بعد یه پاسخی برミگردونه اما نکته اینجاست اگه این کاره زود انجام بشه مدیر من میبینه که اوکیه انجام شده رفت اما اگه پاسخ خیلی دیر برگردد اتفاقی که میفته اینه که منیجر ممکنه بگه که این چی شد؟ رفت گم شد.

## Manager-Initiated: Actions (cont'd)



23



پس در مواردی که در واقع Request من انجامش طول میکشه ما با این چالش مواجههیم که چگونه به این پاسخ بدیم. ما یه کاری میتونیم بکنیم بگیم که میدیم این داره انجامش میده مثلًا من تلفن دارم صحبت میکنم خیلی هم طول میکشه بعد میبینی طرف مقابل چیزی جواب نمیده بعد میگی الو! زنده‌ای؟ هستی؟

یه راهش اینه که اون سمت مقابل که داره گوش میکنه بگه که آها آره این یعنی که من هستم تو حرف تو بزن.

که آقا وسط صحبتای طولانی من تو یه سیگنالی بده که بفهمم هستی تو و داری گوش میکنی و در واقع این نیست که همچ در واقع یک طرفه باشه پس یک روش اینه که بگیم Agent داری کار میکنی بگو که بله من هستم و اون وسطا هم مدیر بگه زنده‌ای هستی و ارتباط باشه کلا. وقتی طولانی میشه مدیر باز poll داشته باشه در مورد اینکه کار من چی شد انجام شد به کجا رسید. این یک روش است.

راه دیگه اینه که بگه که اون اولی که میپرسه بگه که دارم روش کار میکنم و زمانی که تمام شد من تمومش کردم خب اینم یک سیستمیه این حداقلش بهتر از اینه که Agent رفته تا پاسخ رو برگردونه طول میکشه پس

حداقلش اینه که یه Request که من میفرستم شما یه تایید بده که داری کار میکنی و من بدونم بہت رسیده.  
پس این در واقع این موضوع باید دیده بشه.

## Agent-Initiated Communications

- Agent sends the manager an **event** (trap) message to bring something to the manager's attention
  - Event messages correspond to **interrupts** that help managers do their jobs better
    - Unsolicited communications
- Categories
  - Alarms: Requires management attention
  - Configuration-change: Inform of a configuration change in the device.
  - Threshold-crossing: Performance-related state variable has exceeded a certain value
    - Might require management attention
  - Logging: Occur regularly in network operation
    - Typically, do not require an operator's attention
    - But need to be logged



تا اینجا ما داشتیم میگفتیم که سرور polling کنه . سرور بخود شروع بکنه غیر polling راهکار دیگه‌ای نداریم برای polling حداقلش اینه که بگیم هر 5 دقیقه به من اینو گزارش کن این poll یا درخواست اولیه رو باید داشته باشیم که کارش رو انجام بده.

بریم سمت مقابل : Agent هم یک جاهایی هم هست که باید درخواست بده دقیقا یک زمانیبی هست که سیستم من به مشکل بر میخوره یک Event یا یک رخدادی اتفاق میفته که Agent میگه باید اینو بلافصله گزارش بکنه چون شرایط خطرناکه و مدیر باید خبردار بشه اینجا که Agent دیگه نمیتونه منتظر باشه که آقای مدیر تورو خدا از من یه poll داشته باش. اینجا خود Event Message یک Agent بلافصله رو برای مدیر

میفرسته که آقای مدیر حواست باشه که این اتفاق افتاده در واقع به جوری مثل یک وقه هست در سیستم‌های کامپیوتری که آقا آقا این اتفاقه افتاده برو یه فکری بکن!

ما یه اصطلاحی داریم به نام unsolicited communication این رو اینجا ببینید در نقطه‌ی مقابل Solicited Event میدارن. یعنی کاری که درخواستی برash وجود داشته! ما اینجا به درخواستی داشتیم و اینم پاسخی برミگردونه که این گزینه پاسخ درخواست شمامست. زمانی که poll میکنیم این وضعیت Event مبنی بر درخواسته ولی پاسخی که به مدیر برミگرده مدیر منتظرشے ولی در زمانی که من یک trap یا دارم این مدیر من نشسته داره کارشو میکنه یکی درو باز کرد او مد وسط اتاقش منتظر نمیشه که بگه.

بدون دعوت میاد. ارتباطاتی که بدون درخواسته برای همین بهش میگیم.

و این یک دسته‌بندی خاص هست که باز خودش زیرمجموعه‌های زیادی داره : آلام میتونه باشه برای تغییرات پیکربندی که اینجا عوض شد مثلا. عبور از حدود آستانه میتونه باشه که آقا دمای cpu از این بیشتر رفت و باید حواسمن باشه یا log میتونه باشه که الان یکی log کرد و log اش هم موفق نبود یا یکی سه بار چار بار تلاش کرده نتوانسته یا یکی داره port scanning میکنه که تو log ها مشخصه کاملا.

در مورد log کردن شاید بشه گفت که یه مقدار اغراق آمیزنه میتونیم log کردن رو در قالب یک trap نبینیم که به سمت مقابل که مدیر باشه اعلام کنیم ولی اشکال نداره به مدیر اعلام نمیکنیم توی log خودت بنویس اما این لزومی نداره که حتما به سمت مقابل اعلام بشه.

یعنی توی این کتگوری که Agent شروع کننده شاید درمورد log ها نیازی نباشه که به مدیر خبری بده شاید لازم داشته باشه که این اتفاق بیفته که این میتونه در قالب آلام یا اون threshold Raising تغییرات پیکربندی اتفاق بیفته. ولی میگم وقتی به logها میرسه معمولاً ما در مورد logها میگیم فلاں اتفاق افتاده و این خیلی مهم نیست ولی ثبتش میکنم تو دفترچم به عنوان Agent نیازی نیست که به مدیر بگیم ولی اگه خیلی مهم بود خبرش میکنم. بعداً مدیر باید هر از گاهی بیاد بگه که log هات رو بده ببینم چه خبره.

# Event Messages

- The included information in event messages:
- The system from which the event originated
  - IP, Name, ID, ...
- A time stamp of when the event occurred
- The type of event that has occurred
  - Security, Fault, ....
- Event detail information



25



که رخ میده شامل یکسری اطلاعات هست : اولا باید بگیم این Event در کدوم سیستم اتفاق افتاده دقیق باید بگیم ip سیستم چیه؟ اسم سیستم چیه؟ ID اون تجهیز چیه؟ اطلاعات کامل در مورد اون مبدا Event رو باید بگیم.

دوم باید زمان رو بگیم Time Stamp میخوایم در فلان روز فلان ساعت فلان دقیقه ثانیه و میلی ثانیه این اتفاق افتاده.

سوم چه خطایی اتفاق افتاده؟ یکسری Type ها داریم خطای امنیتیه خطای خرابیه یا انواع دیگه نوع خط را هم باید بگیم

و چهارم جزئیات خط را هم باید مطرح کنیم.

پس وقتی Event اتفاق میفته شامل چهار جز کلیه که میشه مشخصات سیستم، زمان رخداد، دسته‌بندی خط و جزئیات خط.

# Event: Alarms

- Alarm: unexpected event has occurred that likely requires management attention
- Examples
  - Router line card failure
  - Loss of connectivity
- Alarm: condition that persists over a period of time; two states
  - On: Abnormal condition starts
  - Off: Conditions back to normal case
- Additional information in alarm messages
  - Alarm severity: Critical, Major, Minor, Warning, Cleared
  - Additional information to troubleshoot the alarm



26



ما انواع مختلف داشتیم دیگه از چیزا یکیش Alarm بود و زمانی رخ میداد که یک حادثه غیر مترقبه رخ بده و باید مدیر در جریان باشه مثلا : Fail من Line router card میکنه اینجا بلافاصله باید آلام بدم که اینطوری شده.

یا کانکشن شبکه‌ی من قطع شده بلافاصله باید Alarm بدم که Connection ، Connectivity رو از دست داده.

اینا مواردی هست که باید بلافاصله باید اعلام بشه. معمولا آلام ها شرایط پایدار رو در شبکه دارن در یک بازه زمانی اینطوری نیست مثلا در خراب شدن Line router cord اینطوری نیست که 5 ثانیه بعد برگرده این خراب شده و باید درست بشه.

در طول زمان معمولا ثابت هستن و ممکنه در طول بازه زمانی رفتار نامتعارف خودش رو ادامه بده آلام بده که اینطوری هست ممکنه بعد از يه بازه زمانی هم برگردد. شما کابل شبکه رو که میزني میبیني دوتا LED کوچیک

داره پشت اون کانکتور شبکتون یکی سبزه یکی زرد و قتی زرد چشمک میزنه یعنی مشکل دارید وقتی سبزه میاد یعنی مشکل رفع شده. این درواقع دوتا وضعیتی هست که درمورد آلام هست یا Fault هست شرایط بد ادامه داره یا اینکه نه تموم شد و سیستم به شرایط پایدار برگشت.

ما در مورد آلامها خیلی بحث‌ها داریم ما باید میزان سختی آلام رو باید بگیم که میشه Critical/Cleared .Major/Minor/Warning

Critical میشه خیلی حساس. که Major میشه مهم . Minor میشه ای حالا مهمه ولی درجه کم. میشه Warning یعنی که هشدار و Cleared یعنی حله! ولش کن.

خب پس درجه‌ی سختی رو من باید مشخص بکنم تو اون سلسه مراتب که اون آلام چی هست. چون ببینید بعضی از سیستم‌های مدیریت شبکه اینطوریه که اگه درجه‌ی سختی خیلی Critical باشه پیام صوتی ضبط شده موجوده که زنگ میزنه به گوشی مدیر و دو سه تا شماره هم داره که اگه مدیر هم نبود به فلانی زنگ میزني و یا major بده. توی sms به سه چار نفر همزمان sms بده درجه سختی اینطوری که وجود داره.

و یه نکته‌ی دیگه در Alarm ما نیازمند اطلاعات اضافی هستیم چون من میخوام به Alarm م پاسخ بدم یه خرابی اتفاق افتاد من باید برم و خرابی رو بررسی کنم و برای اینکار من اطلاعات اضافی میخوام که این TroubleShouting در ساعت فلان در زمان فلان شامل این جزئیات اتفاق افتاده. این خیلی کمک میکنه به بحث که مطرحه.

## Event Messages

- The included information in event messages:
- The system from which the event originated
  - IP, Name, ID, ...
- A time stamp of when the event occurred
- The type of event that has occurred
  - Security, Fault, ....
- Event detail information



یا رویداد شامل اطلاعاتی است که باید حواسمن باشه زمانیکه event رخ داد ، کجا رخ داده ، ip و ID سیستم چیه ، چه زمانی اتفاق افتاده (time stamp) ، نوع اون event چیه و آیا مشکل امنیتی داره یا نه .

## Event: Alarms

- Alarm: unexpected event has occurred that likely requires management attention
- Examples
  - Router line card failure
  - Loss of connectivity
- Alarm: condition that persists over a period of time; two states
  - On: Abnormal condition starts
  - Off: Conditions back to normal case
- Additional information in alarm messages
  - Alarm severity: Critical, Major, Minor, Warning, Cleared
  - Additional information to troubleshoot the alarm



Alarm یا هشدار زمانی رخ میده که یک رویداد ناخواسته اتفاق بیفته و باید مدیر اطلاع پیدا کنه و دلیل اتفاقی افتادن هشدار و بررسی کنه. Alarm از اهمیتی بالایی برخورداره.

مثلاً fail شدن یکی از line card های روتر یا قطع شدن connection در شبکه Alarm بسته به شرایط میتونه یک آلام ثابت باشه(مثل : سوختن پاور یک دستگاه) و تا زمانیکه مشکل رفع نشه، آلام ادامه داره اما برخی آلام ها حالت گذرا دارند ؛ یعنی خطایی اتفاق میفته و بعد از یک دوزه زمانی قطع میشه(مثل قطع شدن connction شبکه بدلیل شل بودن پورت)

نکته : آلام ها را نسبت سطح سختیشون دسته بندی میکنیم :

Critical, major, minor, warning, cleared

نکته : برای برخی از آلام ها حد آستانه ای تعريف میکنیم تا اگر به اون حد رسید ، آلام اتفاق بیفته.

مثلاً : اگر بار شبکه به بالای 70 درصد رسید اخطار بده

## Event: Configuration Change

- 1) Many applications need accurate information of network configuration
- 2) Due to infrequent changes, configuration information are cached
- 3) Configuration can be modified externally (not through the NM application), e.g., CLI
- 1 + 2 + 3 → configuration change event
  - To keep update the cache
    - Without wasting bandwidth
    - Without out-of-date cache periods



دسته ای از event ها مربوط به تنظیمات پیکربندی میشوند

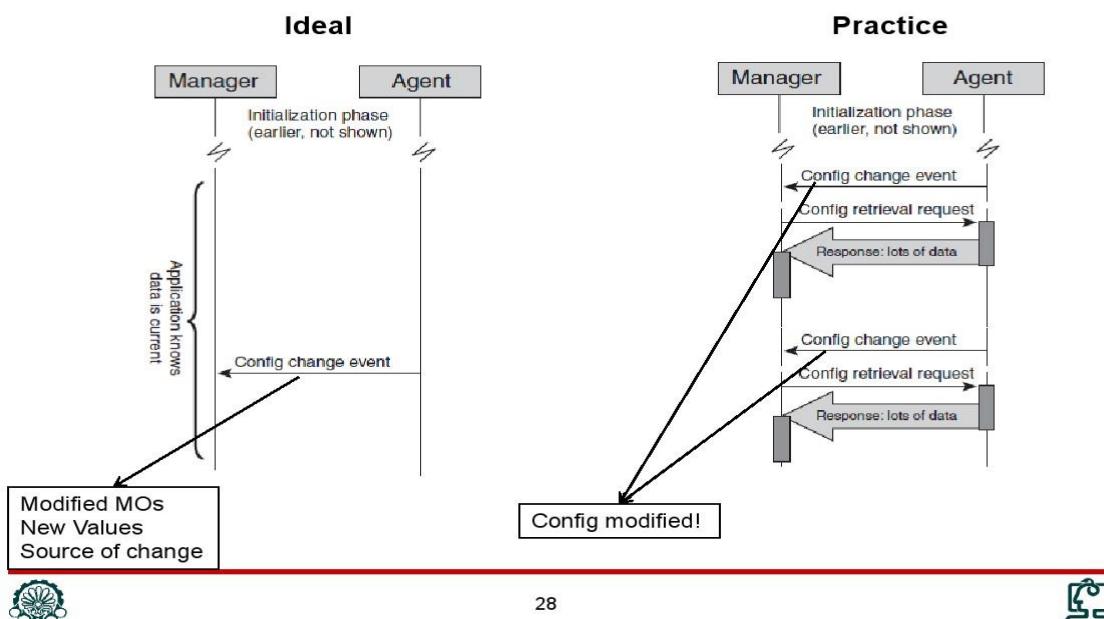
پیکربندی میتونه به شکل های متفاوتی انجام بشه :

آیا سیستم NMS داره پیکربندی و اعمال میکنه(مثل دستور set) که در اینصورت خودش همه چی و ثبت میکنه یا اینکه من از یک مسیر غیر از اپلیکیشن مدیریت شبکه (مثل cmd) دارم config و اعمال میکنم.

اطلاعات configuration در یک حافظه NVRAM)catcher میشینه ؛ چون باید پایدار باشه.

نکته : این حافظه باید همیشه update بشه و آخرین تغییرات config و داشته باشه ؛ بدین منظور یک event باید داشته باشیم تا این تغییرات و اطلاع بده.

## Event: Configuration Change



28



هر کدام دارن کار خودشونو میکنن ؛ Manager و Agent

میگه که تغییراتی در پیکربندی ایجاد شده . manager به agent : Config change event

حال اگر توسط NMS انجام شده باشه ، نیازی به ack نیست؛

اما اگر جای دیگری اتفاق افتاده باشه ؛ manager Config retrieval request میپرسه که چه چیزهایی عوض شده .

: و سپس agent ، موارد تغییر و اعلام میکنه. Respons :lots of data

## Event: Threshold Crossing

- A monitored MIB (MO) has crossed a certain preconfigured value (*threshold*)
- Similar to alarms
  - Two states: on & off
- Information included in this event
  - The name & value of the monitored MIB
  - The value of the threshold
  - Whether the threshold has been crossed or cleared
- Oscillation around the threshold
  - Lot of cross & clear events
  - **Hysteresis** threshold to clear the event



29



نکته: دسته‌ی دیگری از event‌ها هستند که بخارط عبور از حد آستانه رخ میدن.  
مثال: دمای (cpu) و هر زمان از حد آستانه خارج شد، اخطار قطع (off) میشود.

نکته: اطلاعاتی از قبیل نام، مقدار، مقدار حد آستانه، اتفاقاتی که موقع رد شدن حد آستانه رخ میدن و ... در MIB (دیتابس) قرار میگیرن.

توجه: گاهی در سیستم‌ها اتفاق ناخواسته‌ای رخ میدهد که مقداری که برای حد آستانه تعریف کردیم؛ در یک محدوده‌ای مدام نوسان میکند؛ در نتیجه هر بار که از حد عبور میکند، آلام میدهد؛ در این حالت، یک بازه برای حد آستانه (Threshold) تعیین میکنیم.

# Event vs. Polling

- Event-based management is more efficient
  - Less wasteful, more scalable, more responsive
  - Wherever possible, event-based management should be the pattern of choice
- However; event-based is not possible in every case (is not efficient & convenient)
  - Example: Service provisioning
- Event reliability
  - In polling based, initiator wait for response → can detect failures
  - In event based, initiator does not need response
    - Reliable transport protocol
    - Request acknowledge for events



30



مقایسه event و polling

mekanizm polling be einصورت boud ke manager sistem ha ra چک میکرد.

در مقابل ما د مدیریت event میتوانیم مدیریت و پاسخگویی بهتری داشته باشیم

- Polling یک دوره زمانی داره که فقط در اون دوره زمانی سیستم را سرکشی میکنیم اما Event در کمترین زمان ممکن میتوانیم ازش استفاده کنیم .

با این حال event برای هر موردی جوابگو نیست و در برخی موارد بهتره از polling استفاده کنیم.

Mثل service provisioning که باید توسط manager مستقیما مدیریت شود.

قابلیت اعتماد | Reliability

در polling ، مدیر میتوانه منتظر بمونه تا جواب از سمت سیستم برگرده و خطارا detect کنه

اما در event ، پاسخی دریافت نمیشه؛

به همین خاطر امکان عدم استفاده از polling و جایگزینی آن با event در همه بخش ها وجود نداره.

# Outline

---

- Network Management Protocol
  - Communication Patterns
  - SNMP
  - CLI
  - syslog
  - Netconf
  - NetFlow/IPFIX
- 



31



SNMP

# SNMP

---

- Simple Network Management Protocol
  - Widely, successful
  - To retrieve operational data
- Original SNMP: SNMPv1
  - Keep SNMP agent implementations simple
  - User extensible with new management information
- Current version: SNMPv3
  - Not quite as simple, more complex than original one
  - Adds security and scalability to design goals
- SNMPv1, SNMPv2c and SNMPv3 all in use today



32



191

پر تکلی (simple network management protocol) SNMP

پر تکلی است که اطلاعات مورد نظر مارو برمیگردونه.

SNMPv1 : خیلی ساده ارتباط بین manager و agent و برقرار میکنه.

SNMPv3 : پیچیده تر از نسخه اولیه است. ای ورژن در حوضه مسائل امنیتی و مقیاس پذیری تغییرات بسیاری پیدا کرده .

امروزه از SNMPv3 ، SNMPv2c و SNMPv1 استفاده میشه.

## SNMP Standard

---

- SNMP is a series of IETF RFCs:
  - 1) The protocol itself
  - 2) The MIB specification language
    - SMI
    - SMIv2
  - 3) Series of standard MIB definitions
  - 4) The architecture of agent implementations
- 



# SNMP Fundamental Principles

- Separate definition of management information from definition of management protocol
- Management information
  - Specified in MIB modules
  - MIB specification language (SMI, SMIv2)
  - Extensible by users: Enterprises can define their own
  - Standardized MIB modules for commonly used information available
- Management protocol itself
  - Fixed set of basic services that operate on management information
    - Retrieve and modify information, report events
  - Encoding of management information: Basic Encoding Rules (BER)
  - Not extensible by users



34



SNMP تعاریف اطلاعات مدیریتی و از تعاریف پر تکل مدیریتی جدا میکنه.

MIB : ساختار دیتابیسی برای اطلاعات مدیریتی میباشد که بر اساس زبان SMI تعریف شده.

که هر سازمان، با یادگیری این زبان ، میتوانه MIB خودشو توسعه بده.

ماژول هایی که در MIB استفاده شده استاندارد هستند.

از طرفی پر تکل های مدیریتی و داریم که شامل دستوراتی از قبیل get ، set و گزارش خطای میباشند.

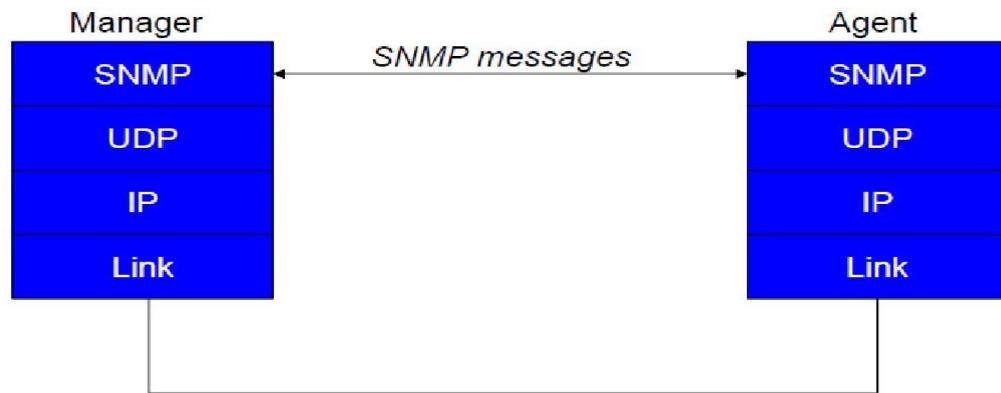
و از آنجایی که سیستم عامل های مخالف ، زبان محاوره ای متفاوتی دارند ؛ باید یک Encoding استانداردی

تعریف کنیم تا در همه ی سیستم عامل ها قابل فهم باشد که به آن (BER)

گویند ؛ که توسط user قابل تغییر نیست. Basic Encoding rules

## SNMP Protocol Stack

---



35



در پرتکل SNMP ، دوتا End system داریک که با هم ارتباط برقرار میکنند.

نکته : SNMP از UDP استفاده میکنه ؛ در نتیجه SNMP یک پرتکل connection less میباشد.

# SNMP Operations

---

## ➤ Get request

- Get value of a MIB object
- Specify one or more **OIDs** of objects to retrieve
- Can request several OIDs in a single request/response

## ➤ Get-next request

- Get value of a MIB object
- Specify one or more OIDs
- Value of closest **lexicographical successor** is returned

## ➤ Set request

- Set a MIB object to a specified valued
  - Can specify one or more OIDs to set
- 



36



دستورات

: این مقدار و از object ای که با OID موردنظر در MIB تعریف شده ، بگیر.

نکته : هر obj یک شناسه OID دارد.

نکته : در یک request میتوان چندین OID را درخواست کرد.

Get-next request : زمانیکه از دستور Get استفاده میکنیم ؛ فقط همون obj با OID مشخص در جواب برگردانده میشه اما در دستور Get-next ، علاوه بر obj مورد نظر ، obj کناری(بعدی) هم برگردانده میشه.

Set request : با این دستور ، برای obj مورد نظر ، مقداری را set(تعیین) میکنیم.

## SNMP Operations (cont'd)

---

### ➤ Get-response

- Really, a request response – sent for get, get-next, set
- The requested OIDs and object values
- Includes request identifier
  - SNMP is connectionless

### ➤ Trap

- Unconfirmed event
- Who emits the trap, what type of trap occurred, when did it occur
- Tuples of OIDs and object values with additional info



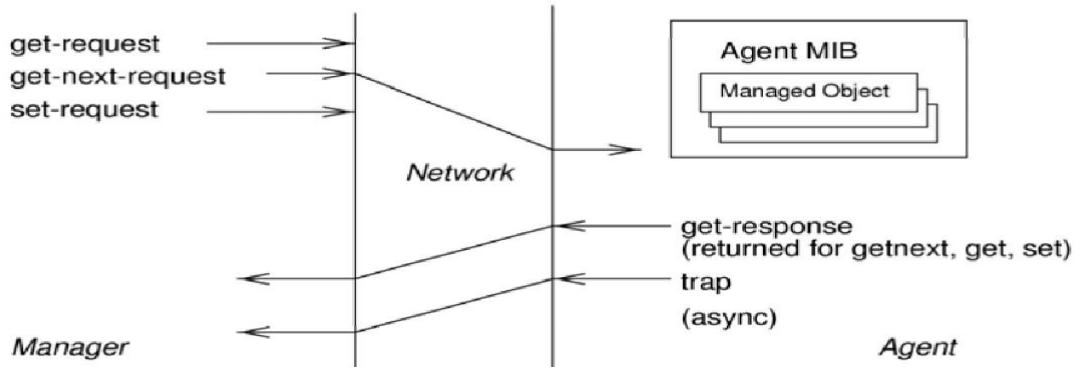
37



پاسخ از سمت مقابل با عنوان get-response شناخته میشے که جواب اطلاعاتی که در request ها خواسته شده را برمیگردونه.

Trap : یک event تایید نشده است که زمانیکه رخ میده ؛ یک اخطار فرستاده میشے تا اطلاع بده رویدادی اتفاق افتاده .

## SNMP Operations (cont'd)



ابتدا از سمت manager درخواست (request) داده میشے ؛ سپس در سمت agent ، اطلاعات مورد نظر از پایگاه داده MIB استخراج میشے و بعد get-response میشے و برミگرده به سمت manager و همچنین یکسری trap نیز از سمت agent به manager ارسال میشے که بدلیل اینکه اطلاعی از زمان ارسالش نداریم و نظم خاصی نداره ؛ آسنکرون هستش.

## Actions in SNMP

---

- SNMP does not provide the ability to invoke an “action”
  - Retrieve or Set management information,
    - But do not cause the device to “do” something
- Work around: model actions as management information
- Action Design Pattern:
  - One MIB object to serve as “action trigger”
    - MIB objects for input parameters, as required
  - One MIB object to contain return code



39



SNMP قابلیت انجام عمل خاصی و نداره و فقط با استفاده از دستورات `get` و `set`، توانایی خواندن و نوشتنداره.

ساختار SNMP نیاز به یک الگوی طراحی عملیات داره؛ با این شکل که یکی از obj های MIB میتوانه بعنوان action trigger (فرمان میدیم که خود obj کاری و انجام) بده فعالیت کنه و سپس پاسخ میده که کار انجام شده یا خیر و جزئیات انجام کار و ارسال میکنه.

# SNMPv1 Evolution

---

- SNMPv1 design goals
    - There's a big "S" in SNMP
    - Focus on easy implementation on agent devices
      - Many vendors were interested to implement it
    - Separation between protocol operations and management information visionary at the time
      - Wide success due to the design choices
  - However, SNMPv1 drawbacks motivated development of newer SNMP versions
    - SNMPv2c, SNMPv3
  - MIBs can be used with newer protocol versions
  - SNMPv1 continues to be widely used
- 



40



SNMPv1 بسیار ساده است.

پر تکل مدیریتی و اطلاعات مدیریتی کاملاً جداست.

بدلیل مشکلات امنیتی در SNMPv1 ، ورژن های بعدی طراحی شدند اما ساختار MIB در تمام ورژن ها ثابت ماند.

## SNMPv2c

---

- Addresses some of the bulk retrieval issues, unreliability issues
- Does not address security issues
  - SNMPv2 tried to but security model broken
  - SNMPv2 used in conjunction with community strings termed SNMPv2c – “SNMPv2 with Community strings”
- Adds two new operations
  - Inform request
  - Get bulk request



41



### SNMPv2c

در ورژن SNMPv2 ، این قابلیت اضافه شد که بجای درخواست تک به تک obj ها ، میتوان مجموعه ای از آنها get bulk request و Inform request دو عملیات Bulk request درخواست کرد. را تحت عملیات Bulk request ارایه شد. اما بدلیل اینکه همچنان مشکلات امنیتی وجود داشت ؛ SNMPv2c ارایه شد.

## SNMPv3

---

- “SNMPv2c plus security”
- No changes to SNMP operations
- Additions
  - SNMP messages can carry proper security parameters
    - This is the most important change
  - Significant expansion of scope
    - Includes standardized and modularized architecture for SNMP agent implementations
    - Does not affect interoperability aspects between agents and managers



42



همان SNMPv2c میباشد که در آن امنیت نقش پررنگ تری پیدا کرد و در آن مکانیزم های امنیتی ای از قبیل رمزنگاری اضافه شد. عملیات ها تغییری ایجاد نشد.

# SNMPv3 Assessment

---

- SNMPv3 is, finally, a secure protocol
  - This means, “sets” are secure
  - Could be used for provisioning and configuration
  - Too late?
    - Management apps developed their workarounds, learned to live with limitations
    - SNMP data models may be awkward for provisioning operations
      - Lack of task orientation
      - Lack of transaction support
    - New, more powerful protocols for configuration (e.g. Netconf)
- It is also far more complex than the original SNMP
- IETF does not pursue further evolution of SNMP



43



تقویت امنیت در SNMPv3، بیشتر از همه زمانی خودشو نشون داد که میخواهیم set request بدیم و تغییراتی ایجاد کنیم.  
این بسیار ورژن برای configuration و Provisioning بسیار مفید است. SNMPv3 پیچیده تر و سنگین تر از نسخه های قبلی شد و به همین دلیل برخی سیستم ها بدلیل عدم توانایی برای پردازش آن، همچنان از SNMPv2c استفاده میکنند.

## Outline

---

- Network Management Protocol
- Communication Patterns
- SNMP
- CLI
- syslog
- Netconf
- NetFlow/IPFIX



44



# CLI

---

- Command Line Interface
  - Administrator interface for networking devices
    - It is for human operator to interact with the device
    - Not intended for (but also used by) electronic applications issues
  - Accessible via Console, Telnet, SSH
  - Very comprehensive and complete
    - Anything you can configure you can do through CLI
    - Most (not all) information can be viewed using CLI
  - Not a standard – different flavors exist but same concepts
    - Different vendors – Cisco, Juniper, Huawei, ...
  - Not fixed set of command, new features add new commands
    - Different from SNMP which has fixed set of primitives
- 



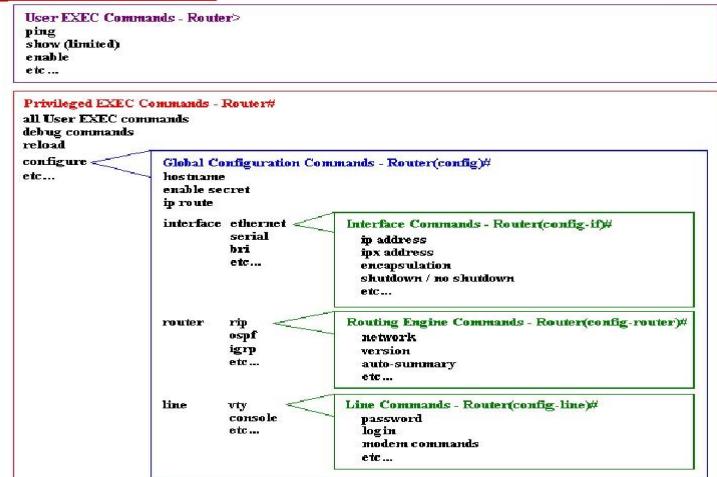
45



یکی از ابزار های دیگر برای مدیریت شبکه (command line interface) CLI است. مدیر شبکه میتوانه با ssh یا telnet زدن به دستگاه مورد نظر و به کمک CLI ، تنظیماتی انجام بده و اطلاعات مورد نظرشو مشاهده و مدیریت کنه. ابزاری بسیار مشکل CLI اینه که ساده و قدرتمند است. استاندارد نشده و در vendor های مختلفی مانند Juniper ، Huawei ، cisco و ... . متفاوت و مخصوص به خودشون برای تنظیم و مدیریت وجود داره.

# Cisco IOS CLI

- Internet Operating System
- OS on the vast majority of Cisco routers and switches
- Different access levels:
  - user EXEC: view information, status, statistics, config
  - privileged EXEC: control the router (e.g. change how it is configured)
  - Switch from user to privileged EXEC using "enable" command



46



محیط CLI سیسکو

## Cisco IOS CLI Example

- Configuration of IP address on an interface

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/4
Router(config-if)# ip address 172.20.52.106 255.255.255.248
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```



47



## Configs in CLI

- Running config
  - The configuration currently in effect
  - Resides in RAM
  - Volatile: lost if device is restarted unless saved to NVRAM
- Startup config
  - The configuration that takes effect when device starts up
  - Resides in NVRAM (non-volatile RAM)
  - Can think of config as a file
    - Contains commands that are executed when the device starts up
    - Subject to back up, restore, FTP, ...
    - Running config is internally not a file, but generates corresponding file when persisted



48



Running config را میشه بكمک CLI ها انجام داد

این اطلاعات در RAM سیستم میشینه

اگر بخواهیم اطلاعات برای همیشه باقی بمونه باید اونارو به حافظه NVRAM انتقال بدیم.

تنظیمات پایه ای هستن که وقتی دستگاه روشن میشه ؛ از حافظه NVRAM خوانده و اجرا میشن. این

اطلاعات در فایلی در حافظه NVRAM قرار میگیره و این اطلاعات میشه کپی گرفت و حتی در صورت نیاز اونارو بازیابی کرد.

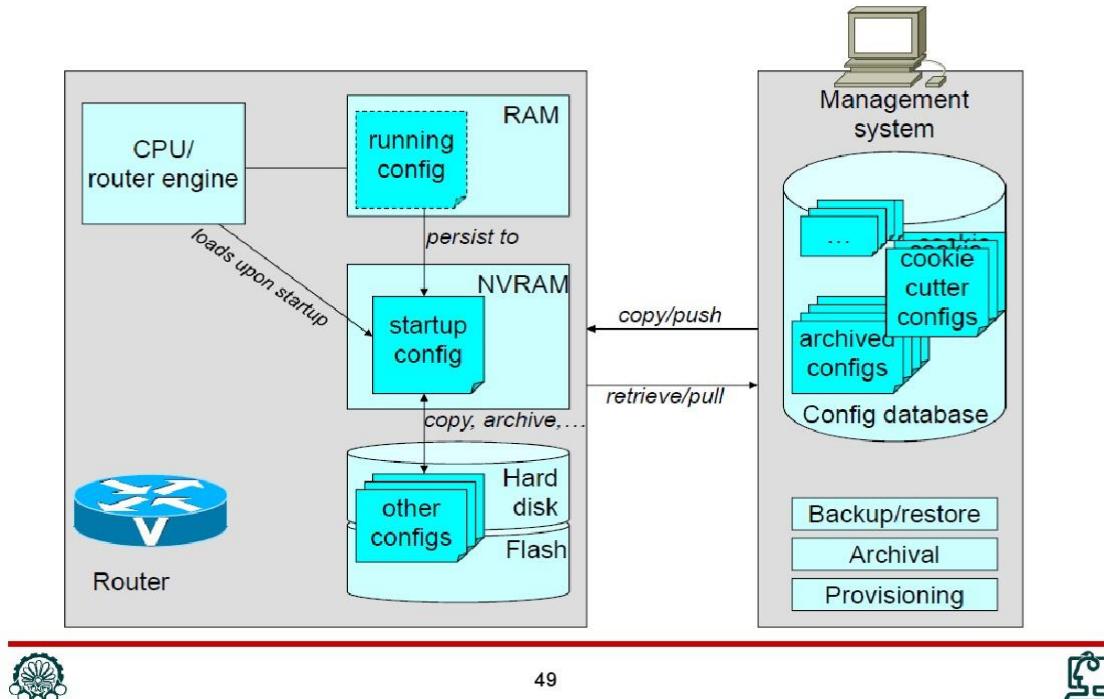
توجه : زمانیکه به یک ip ، interface در حافظه RAM قرار میگیره و وقتی بخوایم این config برای همیشه در سیستم باقی بمانه ، با استفاده از دستور no config این را حفظ کنیم باقی نماند . اونو به حافظه NVRAM انتقال shutdown میدیم.

\*نکته : برای انتقال config ها از RAM به NVRAM از دستورات زیر میتوانیم استفاده کنیم :

```
#copy running-config startup-config
```

```
#write
```

## Configs in CLI & NMS



49



ساختمن یک روترا و ارتباط اون با سیستم مدیریتی

# CLI for Humans

---

- Many features to simplify interactions
  - Help functions, Autocompletion, History, Editing, ...
- Very rich set of functionality
  - Literally, thousands of commands
  - Every new features extends the set
    - New options/ subcommand modes
    - Additional information that can be retrieved
- Commands highly productive for human administrators
  - Large user base, trained work force



# CLI as an Electronic Interface

---

- CLI intended for humans, not management applications
  - So why even consider it
    - Very rich set of functionality
    - Not all features are covered via SNMP or other management interfaces
  - Successfully used with provisioning systems
    - Limited set of commands needed
    - Information flows from NMS to managed device
    - In many cases: management system does not issue command directly but manages configuration files
- 

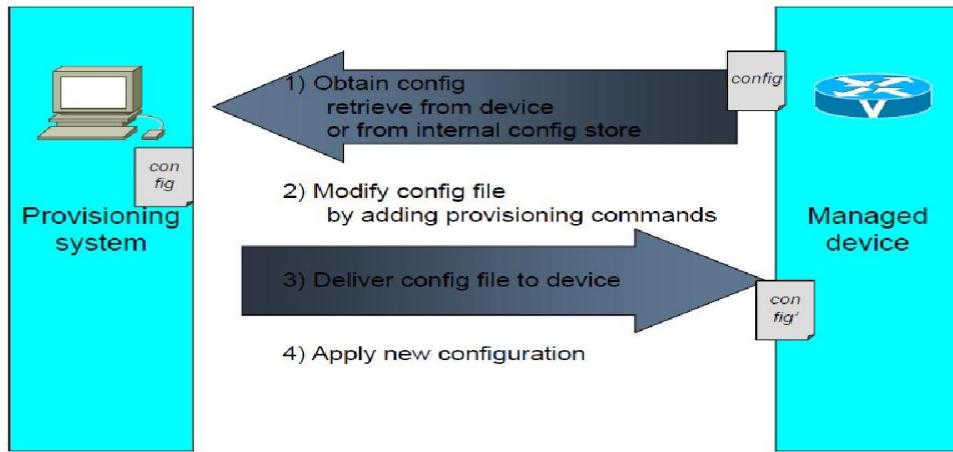


51



CLI یک نرم افزار رابط است و یک سیستم مدیریتی نیست.  
برای سیستم های Provisioning کاملاً قابل استفاده است.

## Example: CLI in Provisioning



52



زمانی که provisioning میکنیم؛ ابتدا اطلاعات configuration اون سیستم و میگیریم و بررسی میکنیم؛ سپس آنارو اصلاح میکنیم و میفرستیم برای سیستم مدیریت شده و config جدید اعمال میشه.

# CLI Issues

- How to process the response
  - Easily interpretable by humans, not so easily by applications
- No consistent grammar
  - Different delimiters
  - Parameter labels: in front, or after, or not at all
  - Horizontal or vertical arrangements (tables)
  - show output is just “printf”
- Techniques
  - Regular expression matching
  - Application of “templates”
- Can deal with on a case-by-case basis, but...
  - Large number commands
  - Variations between vendors, device types, versions



53



## چالش های CLI

- در محیط CLI باید response های که میاد و پروسس کنیم؛ این کار توسط انسان ساده است اما برنامه نویسی آن و انجام این عملیات توسط اپلیکیشن کار پیچیده و سختیست.
- در command ها مسایل گرامری رعایت نمیشه. مثل علایم، جدول ها، فونت و ...
- فقط در همون محیط CLI، نتایج و printf میکنه.
- از نظر تکنیکی: CLI برنامه ایست که command وارد شده توسط admin و چک میکنه و با توجه با غالب ها، اون کار و انجام میده و خروجی و در محیط CLI، به شما نشون میده.
- حتی میتوانیم CLI ای بنویسیم که به حروف بزرگ و کوچک حساس باشه اما اینکار مشکلاتی هم بوجود میاره.

# CLI Issues: Example

```
Router# show interfaces fastethernet 5/4
FastEthernet5/4 is up, line protocol is up
Hardware is Cat6K 100Mb Ethernet, address is 0050.f0ac.3058 (bia 0050.f0ac.3058)
Internet address is 172.20.52.106/29
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s
```

```
Router# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater
```

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
JAB023807H1	Fas 5/3	127	T S	WS-C2948	2/46
JAB023807H1	Fas 5/2	127	T S	WS-C2948	2/45
JAB023807H1	Fas 5/1	127	T S	WS-C2948	2/44
JAB023807H1	Gig 1/2	122	T S	WS-C2948	2/50
JAB023807H1	Gig 1/1	122	T S	WS-C2948	2/49



مثالی از اطلاعاتی که میتوان در محیط CLI ، با استفاده از یک command مشاهده کرد .

- در عکس اول اطلاعات مربوط به یک interface نمایش داده شده .

- در عکس دوم اطلاعات مربوط به همسایه های یک دستگاه نمایش داده شده .

## CLI Concluded

---

- Very rich set of functionality
    - Literally, thousands of commands
    - Every new features extends the set
      - New options/subcommand modes
  - Commands productive for human administrators
    - Large user base, trained work force
  - Not well suited (and never intended) for management applications
    - Retrieval and interpretation of management information has challenges
    - No event reporting (CLI should join with other protocols)
- 



55



با استفاده از CLI ، نمیشه مثل نرم افزار مدیریت شبکه ، روی دادن event ها را مشاهده کرد.

## Outline

---

- Network Management Protocol
  - Communication Patterns
  - SNMP
  - CLI
  - syslog
  - Netconf
  - NetFlow/IPFIX
- 



در ادامه مباحث جلسات قبل پروتکل های مدیریت شبکه را بررسی می کنیم. در جلسات پیش پرتوکل های CLI و SNMP را بررسی کردیم. (البته گفتیم CLI در واقع پرتوکل مدیریت شبکه نیست اما ابزاری را در اختیار ما میگذاره که چارچوب پروتکل ارتباطی را فراهم میکنه)

# syslog

---

- System messages written to a log
  - Provide trail of device activity
    - Each syslog message is an entry in that log
  - Offline analysis of logs by system administrator
  - Not specific to network devices (servers, ...)
- The “message” can be
  - Error messages ... system debug messages
- The “log” can be
  - A local file on filesystem
  - A socket to send log messages directly to remote host



: همانگونه که از اسم این پروتکل پیداست شامل لاغ های سیستم می شود و اتفاقاتی که در یک سیستم رخ می دهد در لاغ فایل هایی رکورد می شود که در صورت بروز هر اتفاق این لاغ فایل ها توسط ادمین مورد بازبینی قرار می گیرد.

لاغ های خطاها و هشدارها از اهمیت بیشتری برخوردار است و به رنگ های مختلف نمایش داده می شود.

این لاغ فایل ها می توانند به دو صورت محلی در خود سیستم و یا بر روی شبکه انتقال داده بشوند.

# syslog (cont'd)

- Used as general event mechanism
  - Very comprehensive coverage of events
  - Management applications as users
  - Near-real time
- Compare with CLI
  - Easy instrumentation
  - Comprehensive coverage
  - Consumption intended for administrators
  - Processed also by management applications
- syslog usage
  - Many syslog messages might never be of any practical use
  - Under certain circumstances, the capability to retrace much of the device's activity trail is invaluable
    - Services degrading severely
    - Suspected network break-ins



58



این لاغ فایل ها event ها و خدادادها را ثب می کند. ورود و خروج کاربر به یک اپلیکشن را می تواند ثبت کند. و به صورت real time و در لحظه داده ها را ثبت میکند.

: CLI در مقایسه با syslog

- Syslog یک پروتکل ساده است.
  - پوشش خیلی خوبی می تونه داشته باشه
  - می تونه یک گزینه خیلی خوب و مطمئن برای مدیران سیستم باشه
  - و حتی برای اپلیکیشن های سیستم این اطلاعات می تونه مفید باشه
- بسیاری از اطلاعات syslog ممکنه هیچ وقت استفاده نشه

# syslog Messages

---

- Each message is a line in the log
  - Header: Prefix of the line
  - Body: Content of message
- Header
  - Minimal but essential information about the message
  - Very structured manner: Time, Host, Severity, Subsystem, Sequence #, ...
- Body
  - The informal content of message
  - Even plain English text
- However there is not one common standard header for all devices



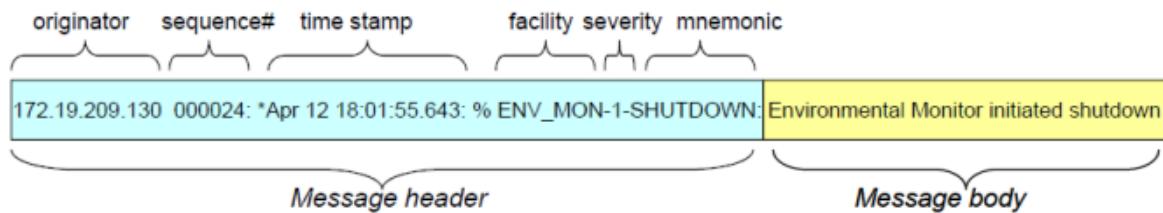
هر message که تولید می شود یکه رکورد ثبت می شود که شامل دو قسمت header و body میشے.

نقطه شروع پیام هست که اطلاعات ضروری مثل زمان رخداد، شماره سیستم، درجه سختی، شماره سریال و ... می باشد.

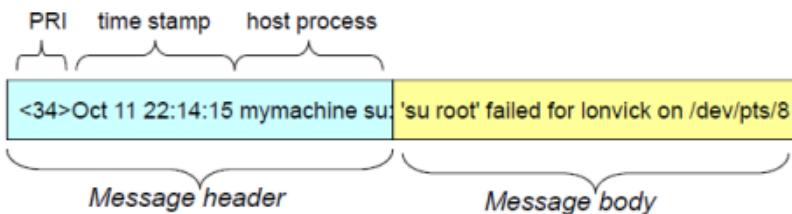
محتوای پیام هست که معمولاً بصورت متن بدون رمز شده و به زبان انگلیسی ثبت می شود. البته این قالب رکورد و هدر استاندارد نیست و در سیستم های مختلف ممکنه متفاوت باشه که چندان اهمیت ندارد و مهم این است که اطلاعات درست و موثق ثبت شده باشد که به ما در خطا یابی و بررسی ها کمک کند.

# syslog Message Examples

Message on IOS:



Message from RFC 3164 (informational RFC, not a standard):



PRI encodes facility and severity according to a numeric formula:

$$\text{facility code} * 8 + \text{severity}$$

here: facility 4 (security), severity 2



60



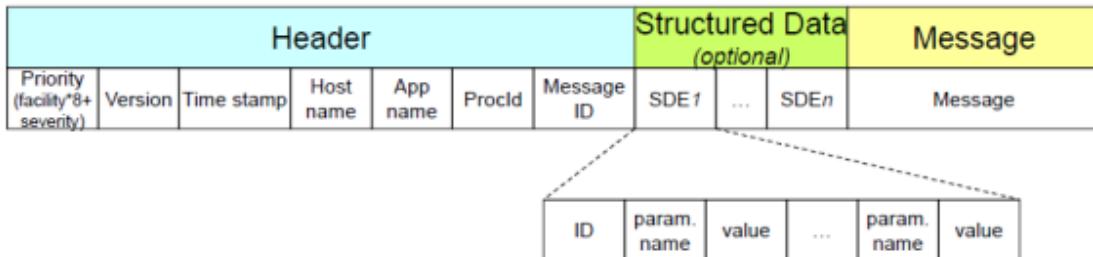
به عنوان مثال نوع لاغ در سیستم IOS سیسکو به این صورت می تواند باشد. که شامل سیستم با آدرس IP شماره سریال، زمان و ساعت وقوع و عنوان(مثلًا سیستم shutDown) که در header قرار دارد و در body که متن پیام ثبت شده.

و در مثال دیگر RFC 3164 پیشنهاد شده است که در header شامل Priority(PRI)، تاریخ و ساعت و سیستم می شود و در body متن پیام ثبت می شود که کد PRI به صورت زیر محاسبه می شود:

Facility code \* 8  
PRI به علاوه درجه سختی (در اینجا 2) می شود کد

$$4 * 8 + 2 = 34$$

# IETF syslog Protocol



- Message text encoding can (but doesn't have to) use UTF-8
- The priority is a combination of a facility and a severity
  - Facility \* 8 + severity
- Timestamps: RFC 3339
- Application name + Process ID → Specify the log source



61



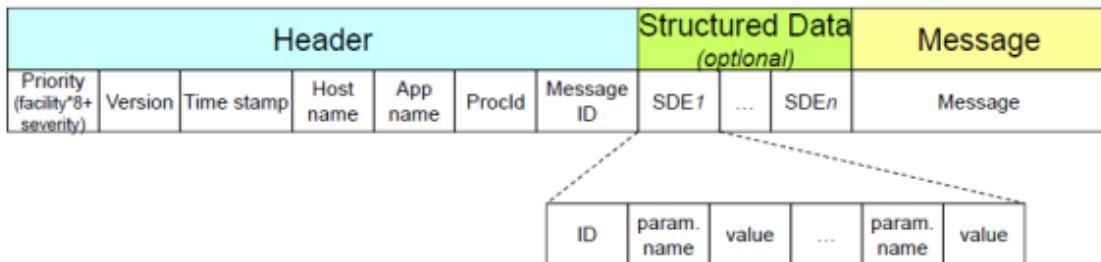
در استاندارد IETF در قسمت هدر syslog، ورژن Priority، تاریخ و زمان (time stamp)، host name، facility و severity (در علاوه درجه سختی)، message ID، procid، App name و App name + Process ID → Specify the log source ضرب 8 محسوبه می شود.

در اینجا داده های ساخت یافته (structure) نیز قابل استفاده است.

در IETF جهت کد گذاری پیام، استفاده از UTF-8 پیشنهاد می کند که امکان ارسال پیام به زبان های دیگر را فراهم می کند.

RFC 3339 نیز time stamp هست.

# IETF syslog Protocol



- Structured Data Element is new staff in IETF syslog
  - ID
  - Set of (name, value) tuples
- Message part is the free format text

```
<165>1 2003-10-11T22:14:15.003Z mymachine.example.com evntslog - ID47  
[exampleSDID@0 iut="3" eventSource="Application" eventID="1011"] An application  
event log entry...
```



62



در اینجا قسمت پایین اسلاید نمونه از پیام syslog در قالب IETF هست که داده ها به تفکیک قابل تشخیص می باشد.

در این مثال Priority 165، ورژن 1، تاریخ و زمان و دیگر اطلاعات قابل مشاهده است.

# syslog Severities

Numerical code	Severity
0	Emergency: system unusable
1	Alert: e action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages



63



جدول تعیین درجه سختی(Severity) (به ترتیب از شرایط بهرانی به نرمال)

کد صفر 0 : اضطراری و سیستم غیر قابل استفاده

کد 1 : هشداری هست که باید بلاfacسله کاری انجام دهید

کد 2 : شرایط بهرانی

کد 3 : Error

کد 4 : هشدار

کد 5 : اعلان notice

کد 6 : پیام اطلاعاتی

کد 7 : کد Debug جهت بررسی خطا

# syslog Facilities

- Priority: facility\*8+severity
- Examples:
  - 191: debug of local7 (23\*8+7)
  - 89: critical msg from FTP daemon
  - 30: informational msg from system daemon

Code	Facility
0	Kernel Messages
1	User-level Messages
2	Mail System
3	System Daemons
4	Security Messages
5	syslogd Messages
6	Line Printer Subsystem
7	Network Subsystem
8	UUCP Subsystem
9	Clock Daemon
10	Security Messages
11	FTP Daemon
12	NTP Daemon
13	Log Audit
14	Log Alert
15	Clock Daemon
16 -- 23	Local (user defined)



64



در اینجا نیز جدول کدهای facilities (ضریب 8) که هر یک مشخص هست و کدهای از 16 تا 23 قابل تعریف برای خود یوز هست تا دسته بندی را مشخص کند.

به عنوان مثال اگر مقدار 191 Priority facility و Severity به صورت زیر محاسبه است:

$$\text{facility} * 8 + \text{Severity} = \text{Priority}$$

$$(23 * 8) + 7 = 191$$

## syslog Deployment: Definitions

---

- A machine that can generate a message will be called a "**device**"
  - A machine that can receive the message and forward it to another machine will be called a "**relay**"
  - A machine that receives the message and does not relay it to any other machines will be called a "**collector**"
    - This has been known as a "**syslog server**"
- 



65



جهت ایجاد توصیه سیستمی و syslog به موارد زیر نیاز داریم:

سیستم تولید کننده پیام ها : Device

سیستم میانی که پیام ها را دریافت می کند و فرward می کند به سمت مقصد مشخصی : Relay

سیستم جمع کننده که همه پیام ها را جمع می کند و به این ماشین syslog server نیز می گوییم : Collector

# syslog Deployment Option 1

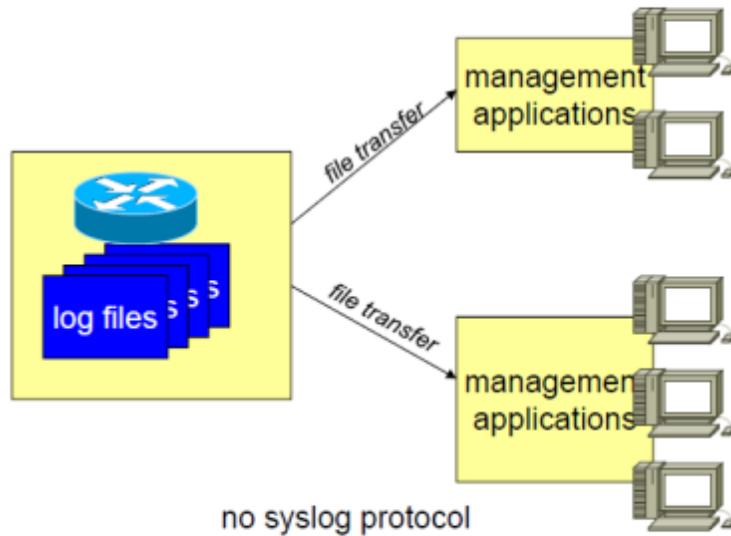
---



## نمونه دیدگاه 1

در این استراتژی **originator** پیام را تولید می کند و ارسال می کند به سیستم **collector** که برنامه مدیریتی ما در این سیستم قرار دارد

## syslog Deployment Option 2



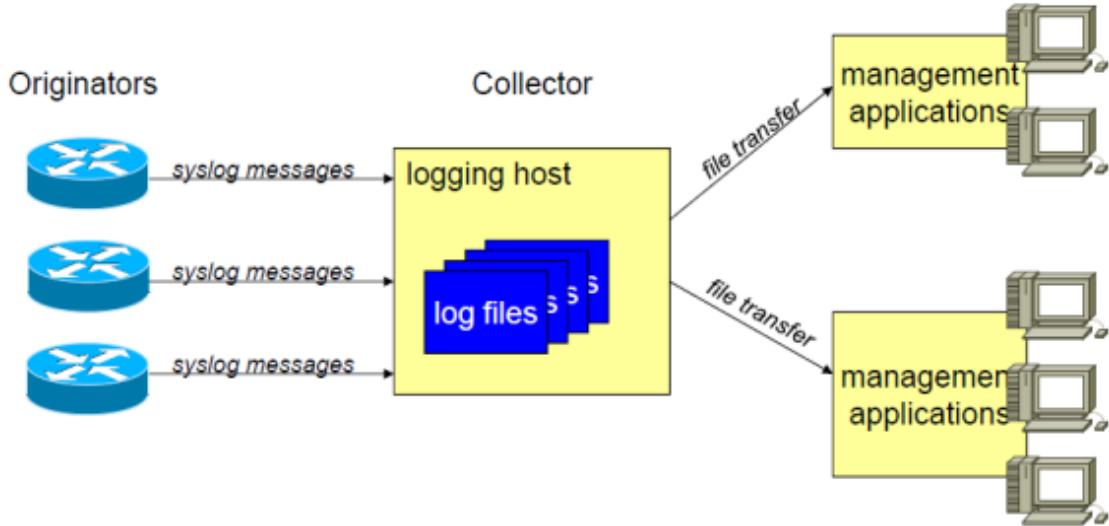
67



### دیدگاه 2

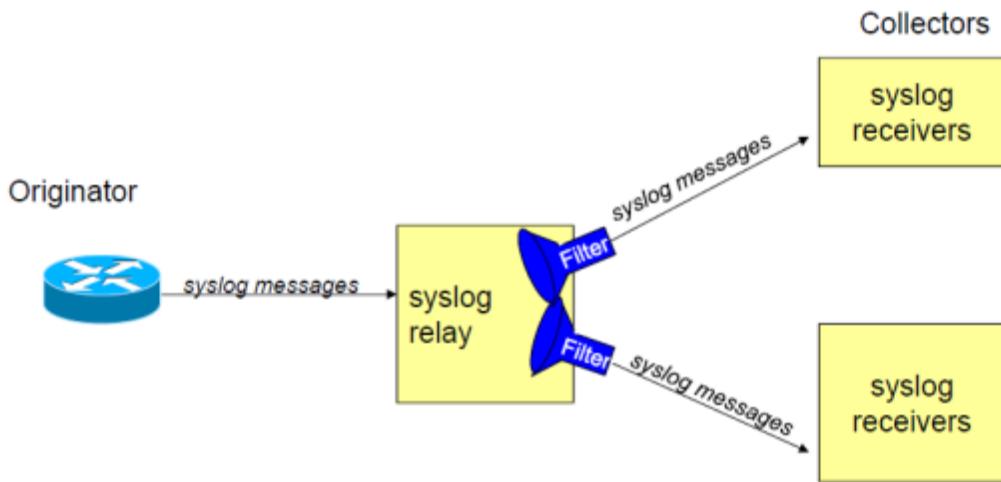
در اینجا یک روتر داریم که log ها را خودش تولید می کنند و هر وقت سیستم های مدیریت شبکه بخواهند فایل ها را دریافت می کنند.

# syslog Deployment Option 3



تعدادی originator داشته باشیم syslog ها را تولید کنند و پیام ها را به سمت collector ارسال و ذخیره کنند و هر وقت سیستم های مدیریت شبکه بخواهند این فایل ها را از collector دریافت می کنند.

# syslog Deployment Option 4



- Example filters:
  - Severity
  - Facility
  - Message ID
  - Regular expression on message body



69

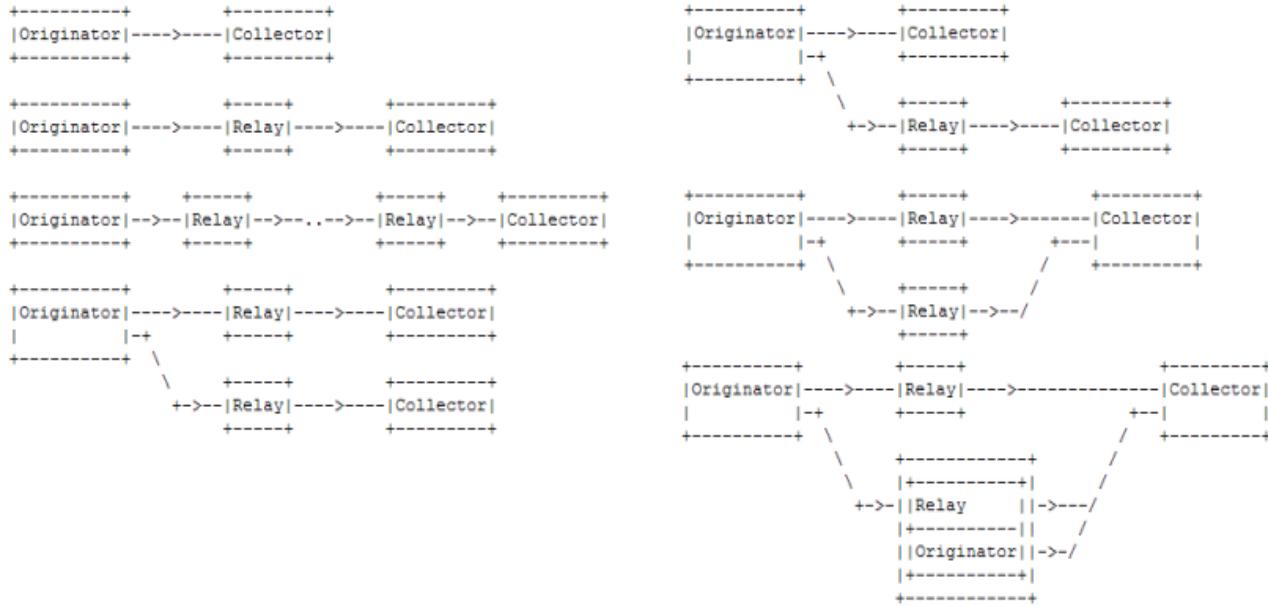


دیدگاه 4

استفاده از relay

پیام ها را می فرستد برای relay و سپس relay پیام ها را به سمت مقصد و collector ها در این مدل به دلیل استفاده از syslog relay امکان فیلتر کردن پیام ها را به ما می دهد. مثلا فیلتر می کنیم که فقط پیام های با درجه سختی خاصی ارسال شوند یا پیام های دستگاه های خاص و غیره.

# syslog Deployment Options: RFC 5424



در RFC 5424 هفت مدل مختلف ترکیب collector و relay و originator را می بینید.

در مدل آخر یک مدل متفاوت داریم که سیستم میانی شامل originator و relay بصورت یکجا را ایفا میکند، مشاهده مکنیم. مانند سیستم های ad-hoc

پیشنهاد استاد: می توانید RFC را به عنوان موضوع ارائه کلاسی انتخاب کنید.

# syslog Deployment: Security & Reliability

- Authentication: No authentication mechanism
    - Misconfigured devices or attacker can send fake logs
  - Integrity: No integrity mechanism
  - Confidentiality: Plain-text protocol
  - Sequenced delivery: No guarantee for ordered delivery
  - Reliable delivery: No acknowledgement
  - If these are major concerns
    - syslog over TCP: RFC 6587
    - syslog over TLS: RFC 5425



## امنیت و قابلیت اطمینان syslog

Syslog از نظر امنیتی مکانیزمی ندارد و هر سیستمی در این پرتوکل می‌تواند با توجه به قالب پیام تولید log فیک کند و سیستم را دچار اختلال شود زیرا احراز هویت (authentication) ندارد، جامعیت (integrity) پیام ندارد، محرمانگی (confidentiality) ندارد،

تحویل مرتب و پشت سر هم (sequence delivery) ندارد هرچند شماره سریال دارد ولی تضمینی وجود ندارد پیام ها مرتب و منظم دریافت شود.

قابلیت اعتماد(reliability) ندارد که پیام ها درست تحویل مقصد داده شود.

راه حل:

در RFC 6587 پیشنهاد استفاده از syslog بر روی TCP هست تا تحويل ها مطمئن تر شود و delivery هم داشته باشد.

در RFC 5425 پنهانهاد استفاده از TLS بر روی syslog هست که integrity authentication و confidentialiy را تامین می کند.

## Outline

---

- Network Management Protocol
  - Communication Patterns
  - SNMP
  - CLI
  - syslog
  - Netconf
  - NetFlow/IPFIX
- 



72



پر تکل بعدی NetConf هست که جهت پیکربندی شبکه استفاده می شود.

# Netconf

---

- SNMP not well suited for configuration management
  - Security concerns (real (v1, v2c) or perceived (v3))
  - Non-task oriented data model or transaction support
- CLI not well suited as programmatic interface
  - Screen scraping
  - Lack of transactionality
  - Lack of programmatic return codes
- As a result, room for a programmatic interface to address configuration management needs



Netconf



73



در جلسات قبلی بررسی کردیم که پرتوکل SNMP تعدادی پیام های get و set داشت که در ورژن 1 و 2 بحث امنیت نداشت و در ورژن 3 به امنیت پرداخته بود و از طرف دیگر فرایند transaction و Task oriented هم نبود و برای configuration SNMP پرتوکل مناسب نبود.

پرتوکل CLI جهت config interface بود که رابط کاربری مناسبی نداشت و در زمینه configuration دچار ضعف بودیم و نیاز به یک پرتوکل خاص در این زمینه احساس می شد تا مدیریت پیکربندی را انجام دهد.

بنابر این پرتوکل NetConf جهت پیکربندی شبکه اینجاد شد.

# Netconf Positioning

---

- For configuration management
  - Manage configurations and sub-configurations
    - edit, copy, transfer, retrieve, merge, delete, ..
  - Might extend into other areas, but not yet!!
    - Operational data
      - Why limit retrieval function just to configuration data
    - Events
      - Events included to notify configuration changes
- Utilizes Web technologies
  - Specifically, XML (but not Web services)



74



همه فرآیند های مربوط به پیکربندی یک مجموع و زیرمجموعه های آن از قبیل copy, edit, ... توسط پرتکل NetConf و ... انجام می شود.

در حوزه های دیگر نیز می شود این پرتکل NetConfig را گسترش داد. مثلا در حوزه Event ها اگر یک تغییری در پیکربندی شد یک Event دهد. یا در زمینه واکشی اطلاعات مربوط پیکربندی نیز استفاده شود.

یک مورد دیگر که در NetConfig خیلی خوب به آن توجه شده است استفاده از آن در حوزه وب و تکنولوژی های آن که پیکربندی توسط webconfig را تسهیل می بخشد.

## Netconf Status

---

- Championed by 2 IETF working groups
    - Netconf – Netconf itself
  - Netconf protocol a standard since early 2008, revised 2011
  - YANG (Netconf's SMIv2) a standard since 2010
  - Netconf implementations by Cisco and Juniper
  - No commercial management applications yet
  - Still young - success yet to be determined – but increasing traction
- 



75



نگاهی به تاریخچه جالب NetConfig

- NetConf itself و دیگری NetConfig دو گروه کاری دارد که یکی NetConfig هست.
  - اولین ارائه NetConfig مربوط به سال 2008 هست و سپس در سال 2011 تجدید نظر شده است.
  - یک استاندارد دارد به نام YANG که مربوط به SMI هست که در سال 2010 ارائه شده است.
  - امروزه در تجهیزات شبکه Cisco و Juniper از NetConfig پشتیبانی می کنند اما در محصولات چینی ها دیده نمی شود.
- پر تکل جدیدی هست که جای رشد دارد هر چند تا به اینجا بسیار موفق بوده است.

# Netconf Datastores

- Document-oriented approach for device configuration
  - Configuration can be considered as **structured** document
    - Can be retrieved or manipulated
  - A filtering mechanism to retrieve/modify a subset of configuration
- Configuration information contained in **datastore**
  - In essence, the Netconf MIB
  - Hierarchical structure: datastore contains other datastores



76



به دلیل کاربرد پر تکل NetConf جهت پیکربندی مشخصا نیاز به Data store جهت ذخیره اطلاعات دارد که برای این موضوع با توجه به دیدگاه Document-oriented اطلاعات پیکربندی هر دستگاه در با ساختار مشخصی در داکیومنت های ویژه خود ثبت شود که باعث می شود دسترسی به اطلاعات آسانتر و قابل فیلتر گذاری باشد.

در مورد MIB قبلا صحبت کردیم که مفهوم MIB عمومی داریم و MIB خصوصی

MIB خصوصی که می شود پایگاه داده SNMP

MIB عمومی که اطلاعات مدیریت شده در آن قرار می گیرد

MIB مربوط به NetConfig را ما می گوییم که یک ساختار سلسه مرتبی دارد که در داخل آن ساختار باز datastore های کوچکتری داریم که از آنها استفاده می شود.

## Netconf Datastores (cont'd)

- Multiple datastores can exist (think configuration files)
  - <running> – like running config
  - <startup> – like startup config
  - <candidate> – a separate datastore to hold a configuration that could be applied at some other point in time
    - Does not need to be supported
    - Availability “negotiated” during connection establishment
- In Netconf terminology, Managing the device means managing its datastore(s)
  - Operations applied against datastores
  - Subtree filtering: apply operation against a particular subset
    - E.g. configuration of a card or subsystem



77



ما datastore های متفاوت داریم که در هریک اطلاعات پیکربندی های متفاوتی ذخیره شده است

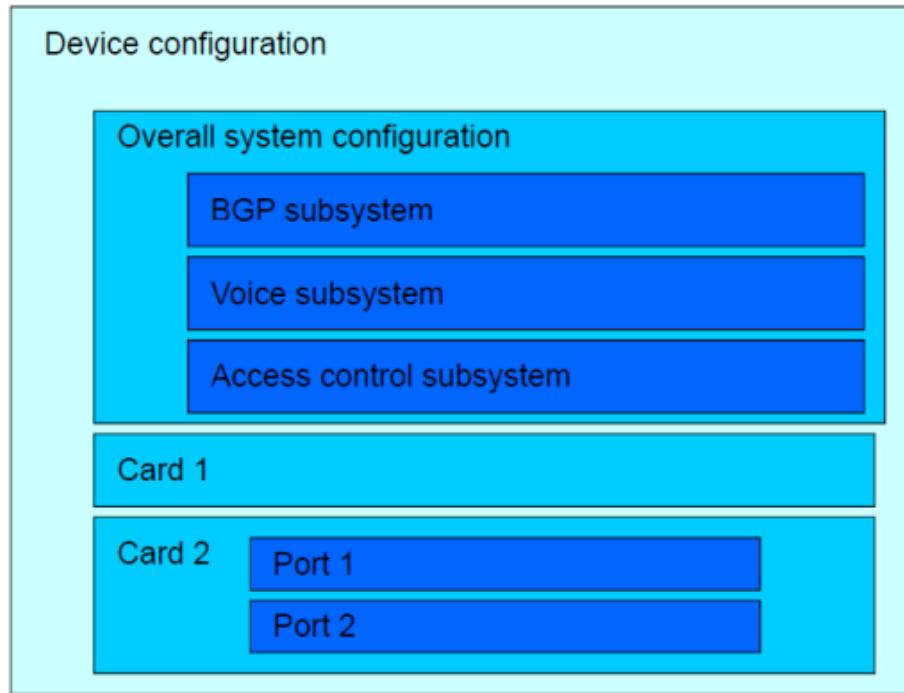
running برای datastore

startup برای datastore

هایی برای پیکربندی هایی که بعدا می توانند اعمال شوند datastore

ما یک واژه شناسی (terminology) در NetConfig هم داریم. مثلا وقتی داریم عملیاتی انجام میدهیم روی datastore بدونیم مکانیزم فیلترینگ زیر درخت ها چجوری هست.

# Hierarchical Datastore Concept



78



در این مثل ساختار سلسله مراتبی یک Device configuration سطح بالا داریم که دسترسی به پیکربندی زیر سیستم ها به صورت سلسله مراتبی مشخص هست.

# Netconf & XML

---

- Every management operation (every request and every response) is encoded as an XML document
  - The requested operation & response
  - The operation parameters
- Configuration information inside a datastore is itself encoded in XML
  - datastore contains tags that divide the configuration information into different portions
  - No predefined tags
- Management information must be “XML-ized”
  - Sophisticated XML document
  - A set of XML tags to delimit a configuration file in its entirety
    - Just a few XML tags for lot of CLI command



79



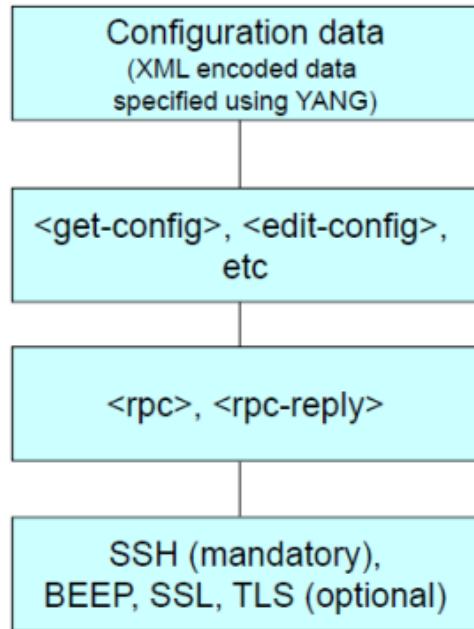
در NetConfig بسیاری از عملیات ها از داکیومنت های XML استفاده می کنند حتی در داخل خود datastore تگ های XML استفاده می شود.

اطلاعات مدیریتی در NetConfig باید به صورت XML-ized شده باشد همه اطلاعات باید بصورت XML باشد حتی اگر داکیومنت پیچیده شده شود.

فقط تعدادی تگ بصورت محدود ایجاد شده است.

# Netconf Architecture

---

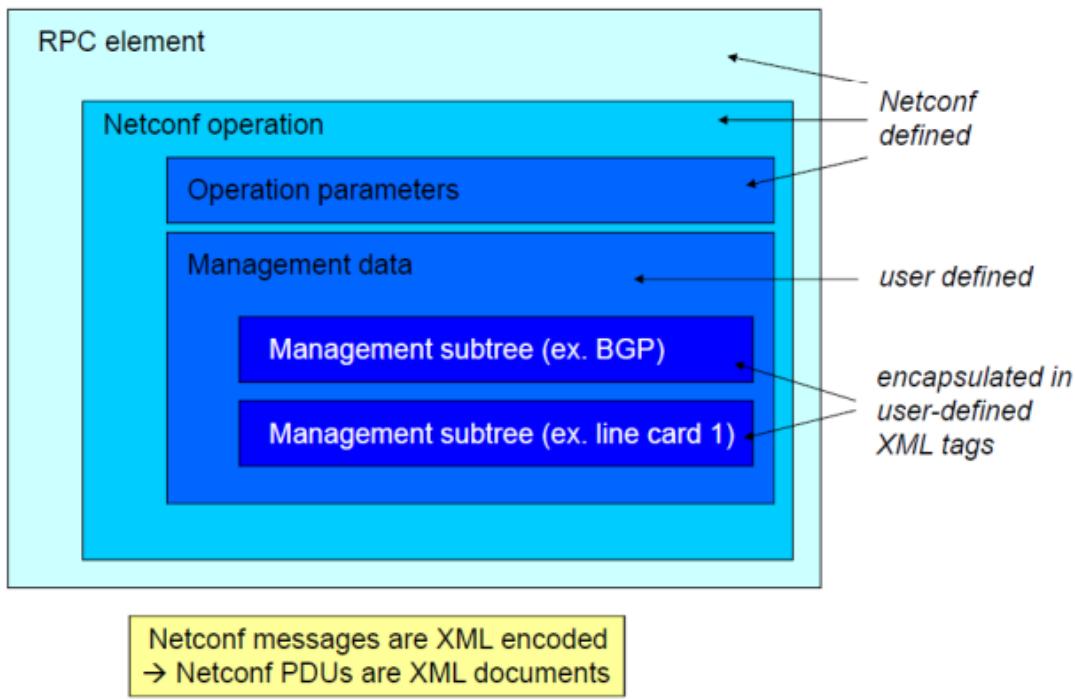


80



در معماری NetConfig ابتدا اطلاعات پیکربندی با استفاده از YANG در قالب XML قرار می‌گیرد. در NetConfig شروع ارتباط باید SSH باشد و بعد از آن می‌توان به صورت اختیاری از SSL یا TLS نیز استفاده کرد.

# Netconf Message Structure



81

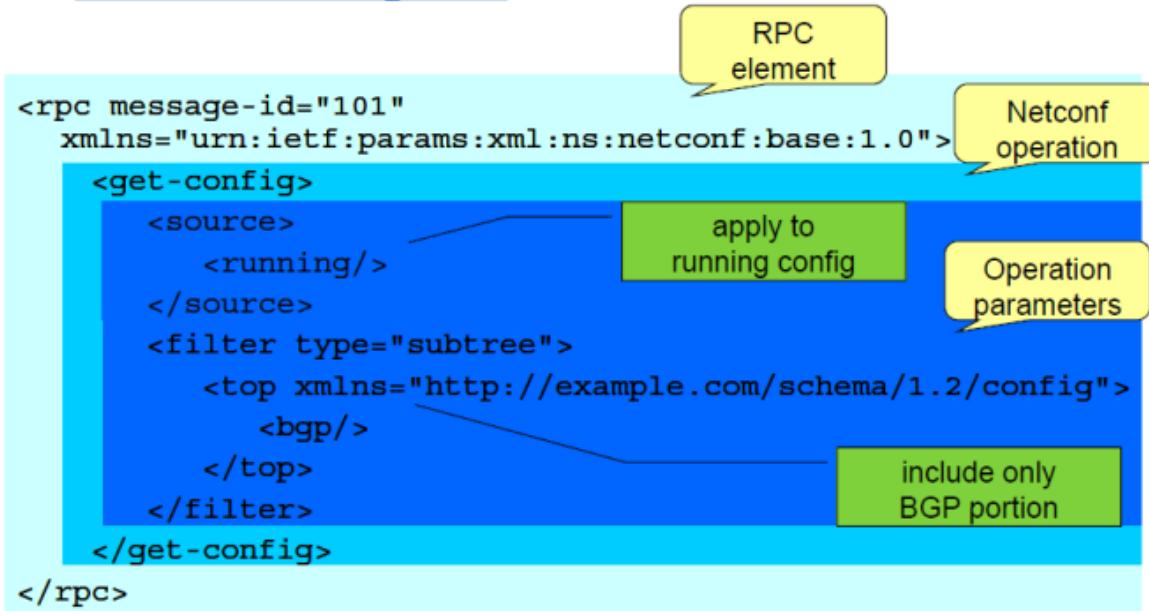


در اینجا یک (remote procedure call) **RPC element** هست به صورت سلسله مراتبی

اطلاعات مدیریتی بصورت تگ های **XML** تعریف شده به وسیله کاربر در زیر درخت ها ذخیره می شود.

تگ های **NetConfig** ، **RPC** تعریف شده به وسیله خود پر تکل هست.

# Netconf Request



82



در این مثال تگ های بیرونی تعریف شده ثابت هست و تگ های داخل کادر آبی داخلی user define هست.

تگ Source از نوع running هست و دیگر جزئیات آن در اسلاید گویا هست.

در XML هر تگی باز می شود در انتهای باید با اسلش `<...>` بسته شود.

# Netconf Reply

---

```
<rpc-reply message-id="101"
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <top xmlns="http://example.com/schema/1.2/config">
      <bgp>
        chunk of BGP data
      </bgp>
    </top>
  </data>
</rpc-reply>
```

skip straight to management data  
no separate operations wrapper



83



در اینجا نیز NetConfig Reply مثال اسلاید قبل هست.

# Netconf Operations

---

## ➤ <edit-config>

- One of 4 operations:
  - Merge (default)
  - Replace (delete any existing configuration in datastore)
  - Create (error if config/subtree exists already)
  - Delete
- Target: which datastore
- Config: the configuration to be applied
- Optionally (not always supported, negotiated up-front):
  - Test-option (validate before applying)
  - Error-option (stop[default] / continue/ rollback on error)



84



Delete .Create .Replace .Merge در فاز عملیاتی به 4 روش انجام می دهد: NetConfig

Create برای ایجاد پیکربندی هست که در صورت موجود بودن خطأ میدهد.

Target همه دستورات datastore هست و روی config که وجود دارد ذخیره می شود.

: optional قسمت های

Test-option برای اینکه قبل از اجرا تست کنیم

Error-option برای زمانی که با خطأ مواجه شدیم چه عملی انجام شود. توقف یا ادامه یا بازگشت

# Netconf Operations (cont'd)

## ➤ <copy-config>

- Copy from a source to a target
- Target is overwritten or created

## ➤ <delete-config>

- Cannot have <running> as target

## ➤ <lock>, <unlock>

- Datastores only available as target as a whole
  - Cannot just lock subtree
- Locks apply beyond scope of Netconf itself
  - Cannot change contents of a datastore through other management interfaces either, e.g., CLI



85



سایر عملیات NetConfig

### <copy-config>

- یک config را از یک مبدا در یک مقصدی در datastore کپی می کند.
- مشخصا در مقصد یا باید جدید ایجاد می شود(Create) یا اینکه overwrite می شود بسته به اینکه کانفیگ وجود داشته باشد یا نه.

### <delete-config>

- کانفیگی که حذف می کنیم نباید در وضعیت running باشد.

### <unlock>,<lock>

- زمانی که تغییری در یک datastore می دهیم کل datastore را lock می کنیم و پس از تغییر درخت مجددا unlock می کنیم.

## Netconf Operations (contd.)

---

### ➤ <get-config>

- source: which datastore
- filter: which portions/ subtree (e.g. specified using xpath)

### ➤ <get>

- Like <get-config>, but can include operational data
- Why a separate operation?
  - Generated very differently: file transfer vs memory dump
  - Retrieving operational data can take a lot more time and resource



86



<get-config>

درخواست اطلاعات بخشی از یک زیردرخت از datastore

<get>

مانند get-config اما get می تواند شامل داده های عملیاتی شود و ساختار ساده تری دارد و مشکلات حافظه ای کمتر دارد

# Netconf Operations (contd.)

---

## ➤ <close-session>

- Graceful session termination

## ➤ <kill-session>

- Abort session

## ➤ Why a separate operation?

- Outstanding requests responded to, or not
- Locks released, or not
- Rollbacks of <edit-config> “in transit” performed, or not



87



<close-session>

➤ برای پایان یک session در بحث کانفیگ

<kill-session>

➤ برای از بین بردن session

➤ در یک شرایط اجبار و غیر نرمال از kill-session استفاده می شود

زمانی که lock کرده باشیم نمی شود close-session استفاده کرد ولی می شود از kill-session استفاده کرد.

اگر در وضعیت `edit-config` باشیم `kill-session` شویم پیکر بندی ما ناقص می شود پس حتما جهت پیشگیری باید `rollback` کنیم تا به نقطه امن قبیل از ویرایش بازگردیم.

## Netconf Operations (contd.)

### ➤ Session establishment

- A handshake of `<hello>` messages at beginning of each session
- Assign a session ID (by the server)
  - Only used to close the session, or indicate certain errors
- Advertise special capabilities (capability exchange)
  - e.g. support for rollback, validation, ....



: Session شروع ارتباط و ایجاد

ابتدا یک پیام `hello` جهت `handshake` منتشر می شود و یک `session ID` از طرف سرور به آن ارتباط اختصاص داده می شود.

برپایی `session` می تواند توانمندی های ویژه مثل امکان `rollback` و اعتبار سنجی را به ما دهد

## Example: <edit-config>

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
    <target>
      <running/>
    </target>
    <error-option> rollback-on-error </error-option>
    <config>
      <top xmlns="http://example.com/schema/1.2/config">
        <interface>
          <name>Ethernet0/0</name>
          <mtu>100000</mtu>
        </interface>
      </top>
    </config>
  </edit-config>
</rpc>
<rpc-reply message-id 101
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```



89



مثالی از Edit-config جهت تغییر پیکربندی در حالت running گفته اگر خطایی رخ داد rollback Error-option برای پورت 0/0 سایز mtu برابر 100000 باشد.

# Netconf Content

- Netconf itself does not specify content, nor how content needs to be described; early days: Vendor-specific
  - Mostly, tagged CLI
  - **CLI blob** legal but arguably constitutes “abuse”
- YANG – Yet Another Next-Generation
  - Data-Definition Language for Netconf
  - Analogous role as SMIv2 for SNMP
    - More powerful and semantically richer
      - Capabilities for reuse, definition of RPCs, support for containment, conditions, constraints
    - No more OIDs
    - Considerably more complex to author
  - Data encoding as XML, not ASN.1 BER



NetConfig محتوای مشخصی ندارد و این محتوا توصیف استانداردی هم ندارد و بیشتر توسط شرکت سازنده مشخص می‌شود.

استاندارد YANG:

- زبان تعریف داده برای NetConfig هست
- چیزی شبیه به SMIv2 در SNMP اما بسیار قدرتمندتر از آن و دارای قابلیت‌های reuse, RPC و ... در آن تعریف شده است که در SMI نیست.
- بجای ASN.1 که در BER برای SNMP اسفاده شد استاندارد YANG برای XML استفاده کرد.

# Outline

---

- Network Management Protocol
  - Communication Patterns
  - SNMP
  - CLI
  - syslog
  - Netconf
  - NetFlow/IPFIX
- 



91



پر تکل آخر مورد بحث در این فصل NetFlow هست که یه همزاد به نام IPFIX دارد.

# Netflow / IPFIX

- Collect network usage data from routers
  - Which type of traffic
  - Between which sources and destinations
  - At which time
- Applications
  - Traffic analysis and monitoring
  - Usage-based billing
  - More detailed questions
    - Who are my top N talkers? Which percentage do they use? HTTP? FTP? SMTP? P2P? DOS attack detection, ...
- 2 flavors:
  - Netflow (in various versions): Cisco-invented, “industry standard”
  - IPFIX (IP Flow Information eXport): IETF standard



92



واژه Netflow جریانات ترافیکی داخل شبکه را شامل می شود  
جمع آوری اطلاعات رد و بدل شده بین روتر ها در شبکه و اینکه نوع ترافیک چیست؟ مبدأ و مقصد ها کجاست

❖ کارکردها

- مانیتور و آنالیز ترافیک
- صدور قبض های مصرفی
- وسیاری از جزئیات بیشتر از ترافیک شبکه مانند:
  - هر پرتکل چقدر از پهنه ای باند شبکه را مصرف کرده
  - کمک در تشخیص حملات

چرا دو اسم Netflow یا IPFIX ؟

توسط Cisco ایجاد شد و سپس IETF آمد IPFIX را با نام Netflow معرفی کرد.

## Applications for Netflow Example: Security Management

Router# show ip cache flow											
SrcIf	SrcIPaddress	SrcP	SrcAS	DstIf	DstIPaddress	DstP	DstAS	Pr	Pkts	B/Pk	
29	192.1.6.69	77	aaa	49	194.20.2.2	1308	bbb	6	1	40	
29	192.1.6.222	1243	aaa	49	194.20.2.2	1774	bbb	6	1	40	
29	192.1.6.108	1076	aaa	49	194.20.2.2	1869	bbb	6	1	40	
29	192.1.6.159	903	aaa	49	194.20.2.2	1050	bbb	6	1	40	
29	192.1.6.54	730	aaa	49	194.20.2.2	2018	bbb	6	1	40	
29	192.1.6.136	559	aaa	49	194.20.2.2	1821	bbb	6	1	40	
29	192.1.6.216	383	aaa	49	194.20.2.2	1516	bbb	6	1	40	
29	192.1.6.111	45	aaa	49	194.20.2.2	1894	bbb	6	1	40	
29	192.1.6.29	1209	aaa	49	194.20.2.2	1600	bbb	6	1	40	

- Typical DoS attacks have the same (similar) entries:
  - Input interface, destination IP, 1 packet per flow, constant bytes per packet (B/Pk)



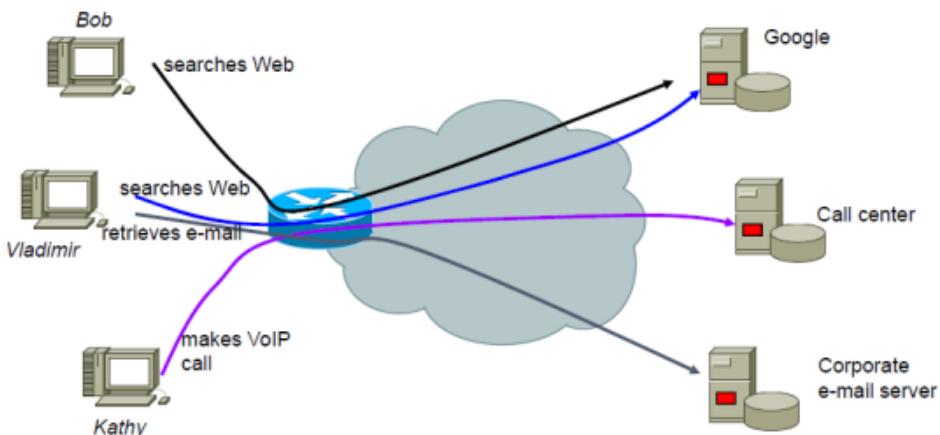
93



در اینجا نمونه ای از cache flow را مشاهده می کنیم که با تحلیل این داده ها حمله distributed DoS را کشف شده است و می توان با استفاده از این تحلیل ها چالش های امنیتی را شناسایی کرد.

# Concept of a Flow

- When a packet goes from one direction in a certain other direction, chances are it's not the only one
- A “flow” is a stream of packets that are likely part of the same association, i.e. that share the same flow key



94



Flow یعنی جریان های پیوسته اطلاعاتی که بین یک مبدأ و مقصد منتقل می شود.

بسته هایی که همگام با هم بین مبدأ و مقصد جریان دارند دارای ویژگی ها و نیازمندی های مشابهی دارند.

# Challenges

---

- How to identify flows
  - IP is connection less protocol
  - Network address are translated
- How to detect start and end of flows
  - No connection establishment / tear down in IP
- So many flows in the network
  - Large volumes of information need to be collected, processed, and transferred



95



❖ چالش ها

▪ چجوری flow ها را شناسایی می کنیم؟

IP هست پس حتما این نیست که بسته بعدی هم از همان مسیر بیاد. و آدرس های شبکه ها ترجمه می شود و مشخص نیست بسته های شبکه از یکه مبدا می آید.

▪ در یک کانکشن خاص به چه طریق تشخیص دهیم یک بسته ip در کجا جریان هست ابتدا یا انتها یا وسط ارتباط؟ با توجه به این مساله که ip کانکشن less هست

▪ جریان های بسیار مختلف در شبکه وجود دارد و حجم بسیار زیاد از اطلاعات داریم

# History

---

- Netflow cache first introduced to improve **routing performance**
  - Cache routing decisions
  - More efficient than route lookup for each packet
- Relevance of cache contents for management not recognized until later
  - Export of cache contents led to definition of Netflow protocol
- Important Netflow versions
  - v1: Original Netflow
  - v5: Most deployed today, includes BGP information
  - v8: Aggregation capability
  - v9: Customization of exported data
  - IPFIX: IETF-standardized version based on v9



96



➤ تایخچه

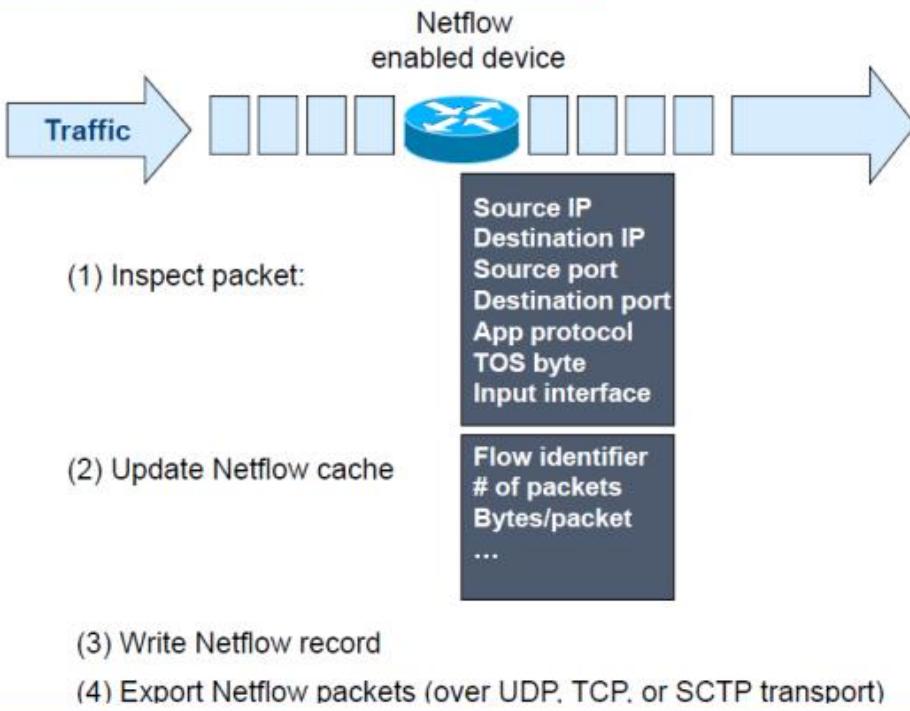
اولین بار جهت بهبود عملیات مسیریابی مورد استفاده قرار گرفت

Netflow شمال 9 ورژن مختلف می شود که مهم ترین آنها به ترتیب زیر می باشد:

- نسخه 1 : اولین ورژن
- نسخه 5 : پر تکلی که بیشترین پیاده سازی را داشته که BGP را در خودش دارد
- نسخه 8 : بحث تجمعی اطلاعات داشت
- نسخه 9 : جهت سفارشی کردن اطلاعات جهت فرستادن به ساختارهای بیرونی

IPFIX که IETF مطرح کرد در واقع معادل Netflow ورژن 9 می شود.

# Netflow Concept



97



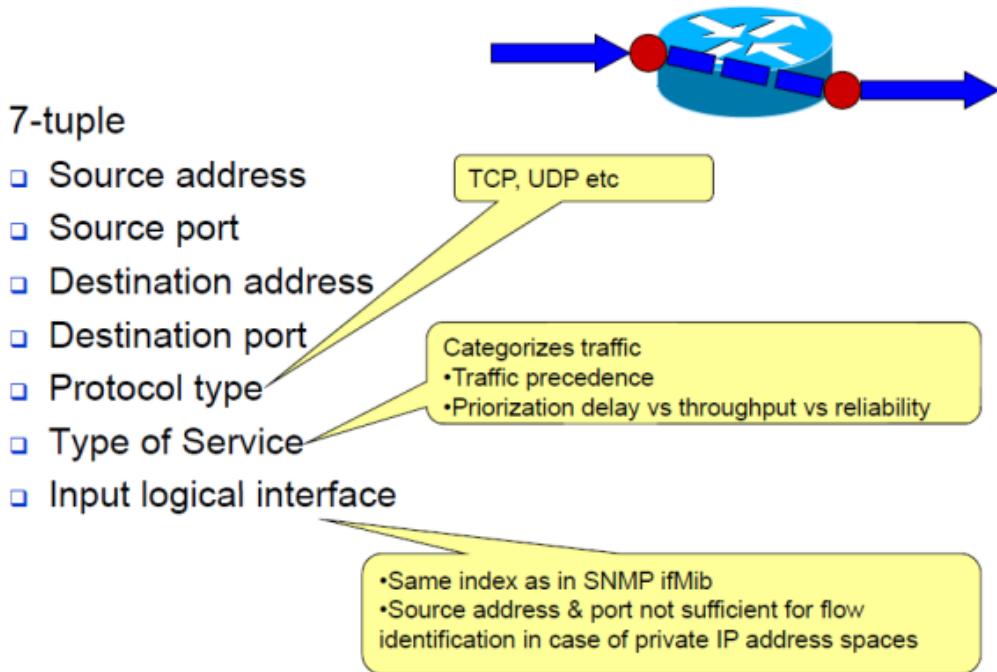
زمانی که ترافیک وارد تجهیزی می شود که هست اون بسته بررسی میشه که در مرحله 1 مشخصات بسته در لایه 3 بررسی و تفکیک میشه

در مرحله 2 این اطلاعات به cach Netflow برده میشه و کش آپدیت می شود.

مرحله 3 اطلاعات در ساختار Netflow ذخیره می کنیم برای همیشه.

4. اطلاعات Netflow می تواند روی TCP ، UDP منتقل شود.

# Challenge 1: Flow Identification



98



❖ چالش 1 ❖

خود Flow به چه صورت مشخص می شود:

- آدرس مبدا
  - پورت مبدا
  - آدرس مقصد
  - پورت مقصد
  - نوع پرتوکل
  - نوع سرویس : اولویت دهی ها، دسته بندی ترافیک، تقدم و تاخر ترافیک
  - شماره پورت ورودی: در بحث vrf, vlan می تواند مفید باشد
- 5 آیتم اول از اهمیت بیشتری جهت شناسایی Flow دارد.

# جلسه 11

اسلايد 2

## Outline

---

- Introduction
- Discovery
- Storing Discovery Data
- Monitoring
- Summary



2

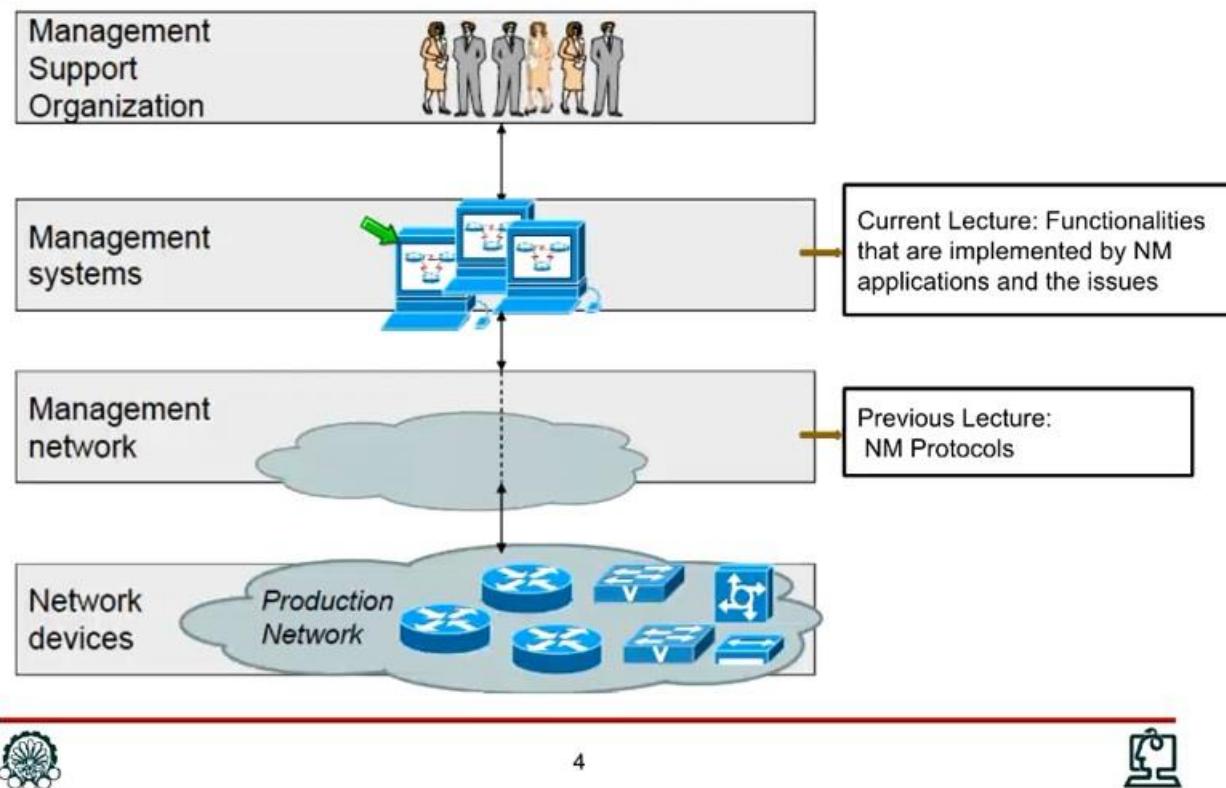


اصل کارهایی که سیستم مدیریت شبکه انجام میدهد

تعريف سیستم مدیریت شبکه : ابزاری که اجازه میدهد اطلاعات شبکه را جمع ، پردازش ، تحلیل و مانیتور کنیم را NMS میگویند.

اسلايد 4

# The Basic Ingredients of Network Management



4



در پایین ترین لایه ، شبکه ای را میبینید که قرار است نظارت شود.

در لایه دوم یک مفهوم منطقی مدیریت شبکه را دارید که به شبکه نظارت میکند ، که این شبکه نظارتی توسط یک سری سیستم های مدیریتی اداره میشوند.

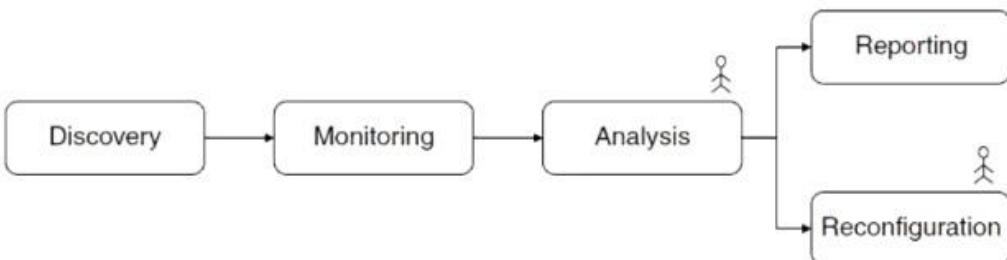
در نهایت مدیران سطح بالا هستند که از نتایج ما استفاده میکنند.

تا امروز راجع به لایه دوم و مدیریت شبکه صحبت شد ؛ الان راجع به لایه های بالاتر بحث خواهد شد

درواقع یک سیستم مدیریت شبکه داریم که میخواهد از مسیره یک سری پروتکل های شبکه اطلاعات را بگیرد ، جمع کند ، تحلیل کند و نمایش دهد.

## NM Functionalities

- Well-known traditional classification of NM functionalities by ITU:  
FCAPS
  - Fault
  - Configuration
  - Accounting
  - Performance
  - Security
- Whereas differences between the functionalities, (almost a) similar activity chain is undertaken to provide them



5



در توضیحات لایه اول و دوم گفتیم یک سری مدل های مدیریت شبکه وجود داشت . مثلا FCAPS که مخفف ،  
Fault , Configuration , Accounting , Performance & Security بود

مدل های دیگری هم مثل TMN بود . این مدل ها یک سری اسم یا کلمه دارند که آن کلمه ها کار کرد ها Functionality یا توابع اصلی آن مدل را در خودشان دارند.

مثلا 5 حوزه FCAPS متفاوت کاری دارد و همه این حوزه ها مرتبط با هم هستند و بر روی همدیگر تاثیر میگذارند . مثلا Fault روی Availability تاثیر گذار میباشد.

فرایندی که میخواهیم را در تصویر مشاهده میکنی : 1-کشف 2-مانیتورینگ 3 - تحلیل

که تحلیل شامل یک خروجی گزارش یا همان report است. که نشان دهد یا آنقدر کار خراب است که نیاز به یک Configuration یا اصلاح مجدد است.

## اسلايد 6

# NM Functions Activities

- Discovery 1
  - Know what the infrastructure is to be managed
    - Devices, Software, Protocols, ...
- Monitoring 2
  - The accurate status of the infrastructure
    - Similar monitoring mechanisms but different data per functionality
- Analysis
  - Processing the raw monitored data and making decisions for reactions
    - The core of each functionality
- Reporting
  - The output of the analysis for external entities
    - Network management documentation process
- Reconfiguration
  - To apply the decisions made by analysis



بنابراین ما نیاز به 5 حوزه جدید داریم که محیط مدیریت شبکه ما باید آن کارها را انجام بدهد.

Discovery -1 : باید در زیرساخت ، اطلاعات را در کشف کنید مثلاً جه اپلیکیشن هایی چه نرم افزار هایی داریم ، پورت های ارتباطی ، پهنهای باند

Monitoring -2 : بعد از کشف اطلاعات باید آنها را مانیتور کرد و متناسب با کسب و کار موارد مورد نیاز را استخراج و مانیتور کرد.

Analaysing -3 : در گام بعد اطلاعات را تحلیل و سپس تصمیم گیری میکنیم.

Report -4 : در این مرحله باید آنها را به شکل گزارش گیری انجام میدهیم که گزارش باید فرمت مشخص داشته باشد چون به مدیران ارائه میشود. و باید بدانیم که مدیران سازمانی جزئی از سیستم مدیریت شبکه نیستند بنابراین گزارش nm طوری تنظیم شود که فردی که توانایی درکش را ندارد هم بفهمد.

ReConfiguration -5 : ممکن است نتایج گزارش باعث اصلاح پیکربندی شبکه یا ReConfiguration بشود

پس باید دارایی جدید را کشف کند-آنها را پایش کند-اطلاعات را تحلیل کند-گزارش دهد - و در صورت نیاز پیکربندی جدید ارائه دهد.

اگر دقت کنید Report و Analaysing و FCAPS هر سه در ReConfiguration مطرح میشوند. فقط باید بدانیم مربوط به کدام حوزه از FCAPS هستند.

اما Monitoring و FCAPS برای "برای FCAPS" هست . یعنی در دل FCAPS این دو مورد را نداریم.

## Outline

---

- Introduction
- Discovery
- Storing Discovery Data
- Monitoring
- Summary



# Discovery Process

- Process of identifying all of the manageable assets
  - Physical assets: Devices, Links, Software, ...
  - Virtual assets: VPNs, Virtual Web Server, ...
- Provides two types of information
  - Inventory of installed physical/virtual assets
  - Interconnection/Topology of HW & SW connection
- Issues
  - How to obtain the information
    - Generic approaches
    - Special case studies
  - How to efficiently store the information



8



وقتی گفته میشود فاز کشف یا Discovery داریم هدف آن است که هر دارایی قابل مدیریتی که در شبکه داریم بدون توجه به نوع دارایی، سیستم باید آنرا کشف کند (دارایی فیزیکی : سویچ، روتر، پورت و... دارایی منطقی : vpn و تونل و VLAN و وب سرویس های مجازی و (...).

بنابراین به دو نوع اطلاعات نیاز داریم :

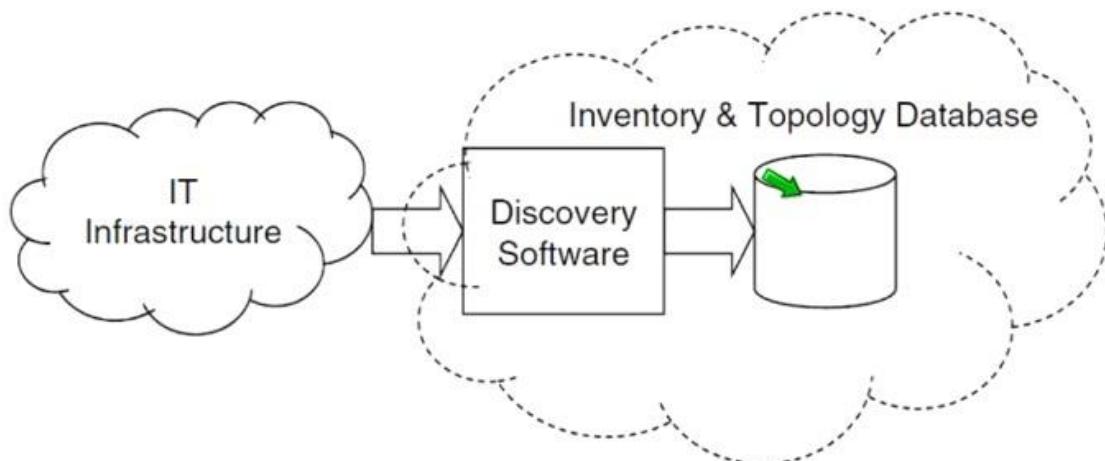
- اطلاعات مربوط به تجهیزات یا assets که نرم افزاری، سخت افزاری یا مجازی و ... میباشد.
- اطلاعاتی که مربوط به اطلاعات آن Asset با دیگران است که درواقع همان تپولوژی شبکه میباشد.

سوال ؟ این اطلاعات را چگونه باید بدست آورد؟ عمومی یا در قالب یک سری اطلاعات مشخص؟

در الواقع قالب ذخیره سازی آنها هم مهم است.

اسلايد 9

# Discovery Process



یک زیرساخت IT در سازمان داریم که یک سری Discovery SoftWare در آن است که کارش تشخیص Asset ها ، ارتباطات و توبولوژی های آنها میباشد و در نهایت اطلاعات تشخیص داده در دیتابیسی در شبکه مدیریتی ذخیره خواهد شد.

# Discovery Approaches

## ➤ Manual

- A team of human in a methodical manner enumerating machines and their attributes
- Disadvantages: Error prone, time consuming, laborious
- Advantages: Reveal turned off or disconnected devices, backup devices, passive devices, ... 
- Usage
  - When automated discovery is not applicable
  - Validate the automated discovery process

## ➤ Directory based

- Used the network information stored in (manual) directory which is basically used for other purpose, e.g., DNS zones



10



سؤال؟ چجوری کشف کنیم؟

یک تیم انسانی وجود دارد که میداند در شبکه چه داریم و چه نداریم و بعد آنچه در شبکه داریم را وارد سیستم مدیریت شبکه میکند. که این ایده خوبی است اما چون عامل انسانی دخیل است عامل اشتباه در آن شایع میباشد. (مثلا ثبت اطلاعات اشتباه – حوصله کاربر سر بوره اتفاف وقت و...)

در مجموع وقتی تمامی فرآیند ها ماشینی است پس فرآیند کشف هم باید به دست ماشین انجام شود.

و تنها زمانی از عامل انسانی کمک میگیریم که یا به ماشین دسترسی نداشته باشیم یا عامل انسانی وظیفه چک کردن درستی کار ماشین را داشته باشد.

معمولًا اطلاعاتی که از دیوایس های مختلف ثبت میشوند یک حالت Directory Base دارند. مانند دایرکتوری ویندوز ، بنابراین برای مدیریت بهتر میتوان یک دایرکتوری ایجاد کرد تا اطلاعات در این Directory ها بصورت manual یا برای استفاده بعدی ثبت بشود.

## Discovery Approaches (cont'd)

### ➤ Self-Advertisement

- Software on devices advertise their presence to a server on the network
  - Broadcast/Multicast on boot-time/periodically
  - Listening (discovery) servers identify the machines

### ➤ Passive Observation

- By watching information flow, discover the presence of devices and software
- E.g., Capture IP packets & inspect L4/7 headers or inspect route advertisement packets



دومین دیدگاه اینست که بجای عامل انسانی یک مکانیزم Self Advertisement داشته باشیم . یعنی وقتی دستگاهی به شبکه وصل شد خودش اعلام حظور کند مثل dhttp که وقتی pc را به شبکه وصل میکنیم دیگر ip را بصورت دستی ست نمیکنیم . در واقع سرویس dhttp به سیستم ip و mask میدهد.

مثلا در شبکه های بی سیم بحث Access Point ما نمیدانیم که اصلا نقطه اتصالی وجود دارد چون بعضی از آنها در box های مخصوص به خود هستند بنابراین خوده Access Point در طول زمان یک سری فریم های weekend میفرستد و به device میگیرد و شبکه ای را پیدا میکند و سعی میکند به آن متصل شود.

باتوجه به این وقتی یک مکانیزم **Self Advertisement** داشته باشیم یک مکانیزم **Listening** هم خواهیم داشت.

که سرور ها هستند که گوش میدهند تا بفهمند در اطراف جه میگذرد.

مثلا در بحث نقاط اتصال گوشی همراه میتواند نقش یک **Listening Server** را داشته باشد.

سؤال؟ آیا تجهیزات باید به شکل فعال روی شبکه باشد و **listen** بکند و جواب دهد؟

مثلا میخواهیم به یک شبکه بی سیم متصل بشویم ، باید فعالانه وارد بشوم یا راه دیگری هم وجود دارد؟

چون در بحث **Self Advertisement** مطرح میشود بنابراین باید یک برنامه یا نرم افزاری باشد تا خودش را معرفی کند

مثلا اطلاعات **flow** ها میخواهیم اطلاعات ترافیکی را دربیاوریم و از روی اطلاعات ترافیکی بفهمیم کی چیکار میکنهو بجای مانیتور کردن آدم در مباحث امنیتی ، مکالمت و تماس هایش را شنود میکنیم.

مثلا در حمله **port scanning** نشان میدهد که یک مهاجم وجود دارد بنابراین با این حمله میتوانیم بگوییم مهاجم چیه یا از کجا میاد (در واقع مهاجم در یک سری فواصل زمانی چک میکند که در شبکه کدام پورت ها باز هستند)

یعنی نوع رفتار آن ، خودش را معرفی میکند که در اینجا مکانیزم **Self Advertisement** به مکانیزم **Passive Observation** تغییر میکند. درواقع با چک کردن جریانات ترافیکی یا **capture** کردن اطلاعات و **packet** ها روی شبکه و تجزیه و تحلیل اطلاعات لایه های مختلف به نتیجه میرسیم. درواقع با شنود شبکه به همه چیز پی میبریم

## 12 اسلاید

# Discovery Approaches (cont'd)

## ➤ Agent-Based

- Discovery agent is installed on all devices
- Collects information about machine resources, and then update the information onto a management server DB

## ➤ Active Probing

- The probing software starts from a set of known machines
- Finds information about the neighbors of the machine, as well as applications installed on the machine
- Repeat this procedure for new found devices



دیدگاه بعدی دیدگاه Agent Base است در واقع یک ایجنت روی هر دستگاهی نصب شود اطلاعات درون دستگاه را جمع میکند و آپدیت میکند و هر زمان لازم به فهمیدن چیزی بود از ایجنت کمک می گیریم

پس آنچه که ذخیره میشود ، اطلاعات جمع آوری شده توسط ایجنت میباشد که در یک دیتابیس در سرور ذخیره میشود.

روش بعدی Active probing میباشد که باید به صورت فعالانه شبکه را بررسی کنیم مثل Ping کردن آدرس های IP .

یعنی این ما هستیم که به دنبال اطلاعات میباشیم و هر زمانی که یک Asset جدیدی وارد شبکه بشود میتوانیم به سراغش برویم و اطلاعاتش را بگیریم.

# Discovery Approaches Examples

## ➤ Discovering servers

- Directory based: DNS zone transfer
  - Find name and IP address of registered machines
  - However, incomplete and out-of-date information
- Passive monitoring: LAN traffic analysis
  - Use IP address to find machines
    - Reverse DNS for machine name
    - TCP/UDP ports and header → Application
- Agent based
  - Active agent: Self-Advertisement based
  - Passive agent: Active probing



موارد مذکور روش های متفاوت داشتن فاز کشف بود.

مثالاً سرور DNS کارش تبدیل URL به آدرس IP است پس DNS باید بفهمد سیستم من به شبکه آمده و این اسم و این IP را دراد

پس اولین قدم در سیستم DNS و فهمیدن اسم و آدرس IP سیستم های داخل شبکه میباشد .

نکته : ممکن است با DNS اطلاعات تاریخ گذشه هم داشته باشیم

dns یک ساختار Directory Base دارد که روی دایرکتوری های مختلف بر اساس آن آدرس URL روی سطوح مختلف میگردد و دنبال سیستم هاست و نکته این است که مبتنی بر دایرکتوری می باشد و اگر دایرکتوری قدیمی باشد به مشکل برمی خوریم سرور DNS خیلی درک درستی نسبت به اضافه کردن تجهیزات جدید ندارد پس سرویس های دایرکتوری بیس از این نظر مشکل دارند که اطلاعاتشان ناکامل هست و بعضاً *.out of date*

پس باید یک سرور دیگر استفاده کنیم ، راهکار این است که سرور باید passive monitoring باشد یعنی با ورود ترافیک اطلاعات را آنالیز کند و ازین طریق پی ببرد که چه سیستم هایی در شبکه هستند چه آدرس آی پی هایی می گیرند و ...

حتی می توانیم بفهمیم که اطلاعات تا کجا گسترد़ه می شود روش دیگر هم Agent Base است یعنی اینجنت فعالی روی دستگاه نصب کنیم تا کار معرفی ما را انجام دهد

سوال؟ آیا سیستم اینجنت باید فعال باشد یا غیر فعال؟

## 14-اسلاید

# Discovery Approaches Examples

## ➤ L3 Network Devices

- Agent-Based + Active probing
  - SNMP MIB provides information of device IP addresses and neighbors
  - Starting from a route, logical & physical topology can be discovered by analysis of route interface IP address and routing tables
  - Other method: Ping neighbors or traceroute

## ➤ L2 Network Devices

- Harder than discovering L3 devices because they are transparent to IP protocol
- Advertisement based specific protocol: Link Layer Discovery Protocol (LLDP)
  - CDP (Cisco), NDP (Nortel)



14



اکثر تجهیزاتی که در دنیای شبکه داریم تجهیزات لایه 3 بی هستند که برای مدیریت و کشف این ها دو راهکار اصلی داریم

1-Agent base

2-Active probing

مثلاً وقتی SNMP استفاده میکنیم میدانیم SNMP اینجنت دارد که اطلاعات مربوط به آدرس IP و همسایه ها و تمامی اطلاعاتی که لازم داریم را برایمان درمیآورد ولی در عین حال در Active Probing، SNMP get کردن ، خودمان اطلاعات را جمع می کنیم.

مثلاً برای تجهیزات لایه ۳ از دستور ping استفاده می کنیم (رنج آدرس های ip را میدهید ، میاد پشت هم پینگ شون میکن) یا دستور trace route مسیر را مشخص می کند

برای تجهیزات لایه دو هم یک پروتکل LLDP داریم Link Layer Discovery Protocol که سیسکو از همین LLDP ابزاری به عنوان CDP ارائه کرده NORTEL هم ابزاری به عنوان NDP ارائه کرده است . که همه اینها بر اساس اطلاعات LLDP هستند.

## Outline

---

- Introduction
- Discovery
- Storing Discovery Data
- Monitoring
- Summary



# Storing Discovered Information

---

- Remark: Two types of information
    - Assets (resources)
    - Relations
  - Relational DB is the common technology
  - Storing assets inventory information in relational DB is straightforward
    - Table for each type of resources
  - Storing relations (hierarchal, point-to-point, partial mesh, LAN, ...) a choice is needed to represent the relationship appropriately in the relational database
- 



16



اطلاعاتی که به دست می آید بعد از کشف در هذ صورت باید ذخیره بشود این اطلاعات شامل دو دسته است ۱-دارایی ها یا منابع

۲- ارتباط بین آن دارایی ها

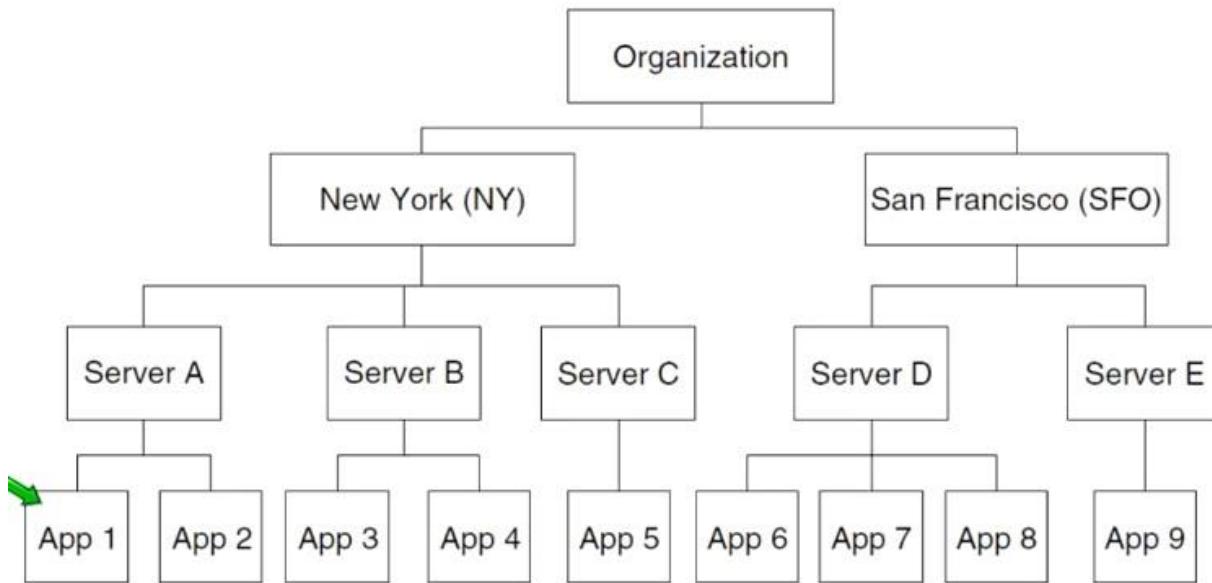
در واقع یک جدول می خواهیم که یک دارایی در آن داشته باشیم و دیگری ارتباط بین تجهیزات که در واقع می شود یک دیتابیس رابطه ای یا همان Relational DataBase را تشکیل داده ازاء هر Asset یک جدول درست می شود.

در بحث ارتباطات جدول باید بگوییم مثلاً از یک دستگاه به دستگاه دیگر به کدام port ارسال انجام بشود ، این LAN به LAN دیگر از کدوم Point باشد یا مثلاً point سلسله مراتبی بود یا wifi بود که در هر حال تمامی این ها برایمان مشخص می شود در واقع لازم داریم بدانیم قالب ارتباطی مان را چطور باید نمایش بدهیم.

اسلاید 17

# Storing Hierarchical Information

---



17



مثلاً یک سازمان هست که دو اداره اصلی دارد؛ در NY و SFC و زیر آن سرور های اصلی هر اداره را نشان می دهد که هر کدام از این سرورها اطلاعات مربوط به خودشان مثلاً Application را دارند که نمایشگر یک ساختار سلسله مرتبی است

## Storing Hierarchical Information (cont'd)

Location	Parent
NY	Org
SFO.	Org

Server	Parent
A	NY
B	NY
C	NY
D	SFO
E	SFO

Application	Parent
1	A
2	A
3	B
4	B
5	C
6	D
7	D
8	D
9	E

- Easy to implement
  - Find parent node
  - Final immediate children
  - Add new node
- Hard to implement
  - Finding all (grand) children of a node



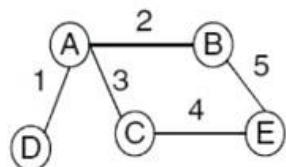
همان شکل قبلی است فقط مدل جدولی آن است که ساختار خیلی ساده ای دارد تا بفهمیم کی به کیه ، کی خانواده کیه، چیز جدید اضافه کنیم ، یا قطع کنیم و تمامی کارها را میشود با یک دیتابیس حل کرد.

## Storing Hierarchical Information (cont'd)



اینجا اندیس داریم که parent کیه ، سمت راست و همسایه ها را هم داریم

## Storing Graphs



Node	Nbr 1	Nbr 2	Nbr 3
A	D	B	C
B	A	E	-
C	A	E	-
D	A	-	-
E	C	B	-

Adjacent node  
up to max limit

Node	Edge	N1	N2
A	1	A	D
B	2	A	B
C	3	A	C
D	4	C	E
E	5	B	E

Separated Edge  
and Node tables

Node	Links	Edge	N1	N2
A	1,2,3	1	A	D
B	2,5	2	A	B
C	3,4	3	A	C
D	1	4	C	E
E	4,5	5	B	E

Edge and Node tables  
With links per node



ساختار چگونگی نمایش گراف مثلاً همسایه های A , B و C و D هستند. B همسایه هایش A و E هستند و باقی هم به همین ترتیب که در جدول (i) نمایش داده شده در جدول (ii) نودها و لبه ها را جدا کرده و در (iii) لبه ها و جداول را در قالب لینک ها میبینید بنابراین ساده ترین ایده در ذخیره سازی استفاده از فرمت جداول رابطه ای است چون جداول رابطه ای را می شناسیم و خیلی راحت می توانیم export کنیم در قالب excel

## Outline

---

- Introduction
- Discovery
- Storing Discovery Data
- Monitoring
- Summary



# Monitoring

- The process of obtaining the **status** and **configuration** information and processing that information
- Issues
  - Type of information to be monitored
  - Monitoring models
    - Generic
    - Special case studies



بعد از کشف و ذخیره سازی دیتا باید اطلاعات راجمع کرد و مانیتور کرد

چه نوع اطلاعاتی را باید جمع کرد؟

پیکربندی یا اطلاعات وضعیتی که وضعیت را نمایش می‌دهد چقدر ترافیک send یا receive شده چه آدرس ip هایی یا شده receive

چالش هایی که وجود دارد: چه نوع اطلاعاتی باید مانیتور بشود؟ string؛ رشته؛ صحیح؟

مدل مانیتورینگ میتواند حالت عمومی داشته باشد یا حالت case study خاص و مشخص باشد

## Monitored Information

- Status information
  - Turned on/off, operational/failed, ...
  - Needed in all FCAPS functions
- Configuration information
  - All attributes than can be modified by an administrator
  - Needed in (almost) all FCAPS functions
- Usage & Performance statistics
  - Information about resource utilization
  - Needed in AP functions
- Error information
  - Information about faults and incorrect operation
  - Needed in FCPS
- Topology information
  - Information about network connectives
  - Needed in (almost) all FCAPS functions



اطلاعات مانیتور شده:

می توانند اطلاعات وضعیتی باشد : دستگاه خاموش / روشن است . عملیاتی در حال انجام است یا نه

اطلاعات وضعیتی در FCAPS خیلی کاربرد داردچون مبتنی بر اطلاعات وضعیتی مانیتور شده است.

در نقطه مقابل اطلاعات پیکربندی هم داریم که فرقش با اطلاعات وضعیتی در این است که اطلاعات وضعیتی همان لحظه را نگاه می کند که الان وضعیت به چه صورت می باشد ، در واقع یک چیز جاری که همیشه قبل محاسبه هست ولی اطلاعات پیکربندی مربوط به پیکربندی دستگاه است که خیلی به ندرت تغییر می کند که آن هم توسط ادمین سیستم انجام می شود که عمدتاً FCAPS

باز هم به اطلاعات پیکربندی احتیاج دارد . مثل Security

اطلاعات دیگر اطلاعات میزان استفاده و بحث های کارایی است. مثلاً استفاده از منابع چقدر است؟

و دیگر اطلاعات آماری از اجزای سیستم که این اطلاعات در Accounting مورد نیاز است و در بحث Performance عمدتاً اطلاعات آماری Performance و Usage و Accounting در حوزه Performance استفاده می شود

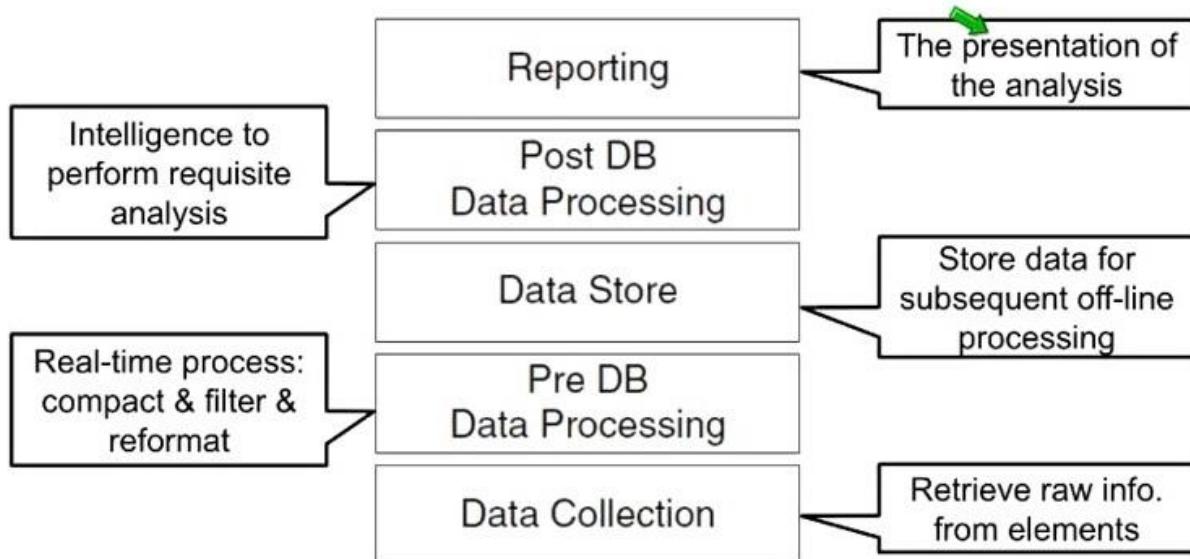
یک سری اطلاعات مربوط به خطاهای هستند درواقع یک Report از اجرای یک کار سیستم که با خطا انجام می شود که در FCAPS فقط در بحث Accounting کارایی ندارد (FCPS)

اطلاعات مربوط به تپولوژی از دیگر اطلاعات جمع آوری شده هستند که شکل همبندی شبکه را توضیح می دهد ابزارهای مختلف شبکه چجوری به هم وصل می شود که در اکثر کارکردهای شبکه میتواند عامل اثر گذاری باشد

## اسلاید ۲۴

# Monitoring Models

## ➤ A generic model



یک داریم در وسط یک Report در بالا و یک Data Collection در پایین

قبل از ذخیره اطلاعات و بعد از بازیابی اطلاعات دوفاز Data Processing هست

که بعد از Data Restore مربوط به Report میباشد یعنی باید اطلاعات ذخیره شده را تحلیل کند تا بتواند گزارش بدهد

اما Pre Data Processing می گوید قبل از نوشتن اطلاعات در Data Base هم باید دیتاهارا تحلیل کرد ، چون log های کاربردی را ذخیره می کند

بنابراین اطلاعاتی که جمع می شود خام هستند و پیش پردازش در همان زمان پردازش انجام می شود در واقع بلافاصله اطلاعات باید فشرده و فیلتر بشود ، شکلش اصلاح بشود و بعد ذخیره کرد.

## Data Collection

### ➤ Major challenges

- Scalability
  - Large number of element (HW + SW) to be monitored
- Heterogeneity
  - Vast variety in type of elements

### ➤ In general data collection can be

- Passive
  - Data collectors observe the monitored system
- Active
  - Data collectors request for information



ما هر وقت حرف از جمع اوری داده می زنیم یک سری چالش های خیلی جدی داریم :

1. Scalability : مقیاس پذیری سیستم جمع اوری اطلاعات:

وقتی من در مورد سیستم جمع آوری اطلاعات صحبت میکنم اون تارگت های من که میخوام مانیتورشون کنم خیلی سریع رشد میکنند مثلا اینم باشه و همینطور اضافه میشه. مثلا اگر قرار باشد ابزاری داشته باشم تا software های توی شبکه را مانیتور کنم ، خیلی سریع این نرم افزارها میتوزن توی شبکه من نصب بشن .

یا میخوام سخت افزار رو مانیتور کنم خیلی راحت تعداد این سخت افزارها در شبکه کم و زیاد میشه . یا بحث (bring your own device(BYOD) یعنی وسیله خود تو بردار بیار، وصل شو به شبکه من ، (مثلا

لپتاپ یا گوشی) خوب خیلی تعداد این ابزارها میتوانه یهو زیاد شه مثلا تو دانشگاه دوهزارتا گوشی یهو وصل میشه.

پس تو شبکه های وايرلس امروز، تعداد اين تارگت ها یهو خيلي زياد ميشه و همه اينها باید مانيتور بشوند. عمدها بحث سистем جمع اوري داده را برای isp ها و carrier های بزرگ مطرح ميکنند که به تعداد خيلي زيادي سرويس ميدهند. پس مانيتور کردن اين همه خيلي سخت است پس مقیاس پذيری موضوع خيلي مهمی است. که مثلا اگر من برای دانشگاه خودم اومدم لايسنس 500 تايی خريدم ولی هزارتا بهش وصل شدن برم راحت بگم لايسنس هزارتايی بهم بدین نه اينکه بیام کل سیستمم بندازم دور و يکی جديد جاش بزارم بلکه مقیاس پذير باشه راحت.

اگر قرار باشد کل سیستمم بنداز بیرون اينطوری کل تاریخچه اطلاعاتی ام ازبين میرود. کل بحث مربوط به configuration و بحث های planning و غيره کلا تحت تاثیر قرار میگيرند. پس بحث مقیاس پذيری يک چالش خيلي جدي در مورد سیستم های جمع اوري داده می باشد.

## 2. Hetrogeneity : تنوعی که در تجهیزات وجود دارد:

ما کلی دیوايس داریم که اصلا جنس هاشون يکی نیستن مثلا يک دیواس سیسکو داریم ، چنتا هواوی هم داریم يه سری سرور لینوکسی و يه سری سرور ویندوزی داریم يه سری کامپیوتر ویندوزی يه سری تبلت و گوشی اندرويدی داریم اينا هیچ کدومشون جنس شون يکی نیست هرکدام تیپ خودشون و دارن حتی در بحث dta type (نوع داده) میتونن فرق کنن. در بحث حجم داده هم میتوونن فرق کنن. در بحث نوع فانکشنی که میخواهد انجام بده، توانمندی های functionality شون میتوانه فرق کنه. اينا بحث ساده ای نیست اين تنوع زياد يا hetrogenity يعني همين و اين خودش يک چالش خيلي جدي برای من بوجود مياره که خوب حالا من چه جوری از اين اطلاعات بگيرم.

حالا فرض که میخوايم داده را جمع اوري کنيم ، حالا active data collection شما است يا passive ؟ يعني بصورت فعال يا غيرفعال میخواي اين کار رو بکنيم؟

وقتی بصورت پسيو است يعني دستگاه مانيتورينگ شما نشسته يه گوشه ای و از ترافيك هایي که رد میشه يه کپی برミداره مثل وايرشارک. مثلا از يک کارت شبکه کل اطلاعات شو کپی میگيره. خوبیش اينه که کسی متوجه نمیشه که ما داریم يه گوشه به شبکه گوش میکنیم.

در حوزه اکتیو، من برای اینکه اطلاعاتی را جمع کنم باید ریکوییست بدم که فلان چیز را به من بده. این ریکوییست دادن خیلی مهمه. حالا که تو داری ریکوییست میدی یعنی داری یه ترافیکی رو وارد شبکه میکنی. اولا که بقیه متوجه میشن و دوما شما داری یه بار ترافیکی روی شبکه ایجاد میکنی ولی خوبیش اینه که شما مطمئنی که اطلاعاتی که میخوای را بدست میاری. مثلا حضور غیاب استاد سر کلاس یک active data است. یعنی باید دونه به شبکه درخواست بده و بپرسه و اطلاعات جمع کنه.

## Data Collection: Passive Monitoring

- Collect information from **regular operation/events/log**
- Application monitoring
  - Log files, e.g., Apache error and access log files
    - Can be collected locally and remotely
  - Proxies to gather operational information
    - Which can be logged (local/remote)
- General purpose computers monitoring
  - Using OS facilities to collect information
    - Agent can save the information locally or send to a remote machine
- Network monitoring
  - Log files, SNMP traps, Routing (other network signaling) protocol inspection



وقتی شما **passive collector** دارین یعنی یه گوشه نشستین و یه سری اطلاعات **log** و **event** و پکت های معمولی و اینارو میتونی بگیری . براساس این اطلاعات میتونین یک تحلیلی بکنین (پیام های خطای اطلاعات داده ای یا عملیاتی که در شبکه منتقل میشوند).

نکته : ابزار مانیتورینگ پسیو مانند وایرشارک باید در محلی نصب شود که سر راه عبور و مرور ترافیک باشد. مثلا اگر میخوای یک مانیتورینگ درست و حسابی داشته باشین باید بین **core switch** را پیدا کنید و یک کامندی میزنین و یک کپی از ترافیک هایی که برای پورتهای شبکه داره ارسال میشه را میفرسته روی

یک پورت خاص . اون پورت خاص میتونه دستگاه مانیتورینگ تون باشه . اینطوری میتونین ترافیک شبکه را تا حد زیادی مانیتور کنین. پس مهمه که سیستم مانیتورینگ رو کجا بزاریم که بیشترین حجم اطلاعات رو بتونیم ببینیم.

سیستم های IDS هم کاملا پسیو مانیتورینگ هستند.

## Data Collection: Active Monitoring

---

- Explicit request for information collecting
- Application monitoring
  - Synthetic traffic/load is used for (performance) monitoring
- General purpose computers monitoring
  - Similar to passive monitoring, agent collect data locally
  - However; agent waits for request from manager
  - Better than passive monitoring
    - No multiple synchronous connection to manager
    - Bulk data is received per-request
- Network monitoring
  - Similar to general purpose computers
  - Protocols: SNMP, Netconf, ...



اکتیو مانیتورینگ مثل همین حضور غیاب استاد هست، مسقیم از طرف میپرسه و اطلاعات میگیره.

این اکتیو مانیتورینگ در کجا کاربرد دارد؟

معمولا در بحث های performance monitoring در app ها. مثلا برای فهمیدن حجم ترافیک یک سیستم باید برم روی خود اون سوییچ یا کامپیوتره ببینم چقدر ولی چون مثلا ازش فاصله دارم از همینجا که نشستم ازش میپرسم که فلانی چقدر cpu utilization داری؟ فلانی روی پورت خروجی اترنت ات چقدر ترافیک ازش میپرسم که packet drop شده؟ چقدر utilize send و receive داری؟ پس اینجا من یک

دارم که داره سوال میپرسه که از اون agent راه دور میگه collector فلانی من منیجر هستم، فلان اطلاعات را به من بده . خوبیش اینه که من میتونم قابلیت های مانیتورینگ بهتری داشته باشم نسبت به پسیو چون دارم مستقیم ازش میپرسم و اینکه از چننا آیتم محدود میپرسم به جای اینکه از همه بپرسم. در ضمن من وقتی میپرسم میتونم کلی اطلاعات درست و درمون دربیارم ازش نه اینکه بشینم یک جا بعد یک ساعت دو تا پکت ازش بگذره و من مانتیور کنم. ممکنه من یک bulk request داشته باشم میتونم از یک سیستم یهו کلی اطلاعات بگیرم. این خیلی مهمه که یهו کلی اطلاعات از یک سیستم بتونم بگیرم.

پروتکل هایی که برای این سیستم مانیتورینگ وجود داره مثل بقیه است همون پروتکل های SNMP و . netconfig

البته روی پسیو مانیتورینگ پروتکل نداریم نشستیم روی شبکه فقط گوش میدیم ولی در اکتیو مانیتورینگ من نیاز دارم یک پروتکل براش تعریف کنم اینم یکی از فرقاشه . چون دارم از راه دور ازش میپرسم پس حتما باید یه پروتکلی باشه تا بر اساس اون پروتکل بتونم اطلاعات رو جذب کنم .

## Pre-DB Data Processing

---

- Objectives of the processing the information before is stored in DB:
- Reducing the volume of information
  - By reducing redundant information
- Cleaning the data
  - By removing erroneous or incomplete data
- Converting the information to a format that information will be stored in the database



حالا من اطلاعات رو جمع کردم میخوام برم ذخیره کنم اما میبینم همه اونایی که او مده به درد من نمیخوره . پس قبل از اینکه برم اطلاعات رو توی دیتابیس ذخیره کنم بهتره برم اطلاعات رو پردازش کنم چون هم حجم اطلاعات و هم اطلاعات افزونه رو کم کنم و هم اطلاعات غلط و هم مشکل دار را پاک کنم هم اینکه ممکنه اطلاعاتم فرمت مناسبی برای ذخیره سازی نداشته باشه.

## Pre-DB Data Processing: Data Reduction

- Large volume of data is generated in operational networks
  - It must be reduced before storing in DB
- This on-the-fly data reduction is different from compressing
  - Which is used for archiving data in off-line manner
- Aggregation method
  - Average of data (either average over time or over elements) is saved instead of multiple pieces of data
- Thresholding method
  - Some information is important (need to be stored) if it exceeds threshold
- Duplicate elimination method
  - Duplicate data is common in networks; e.g., information of the same flow on multiple routers



مثلا net config اطلاعات خیلی بزرگی را تولید میکنه و خیلی از این لاغ ها رو شاید سال تا سال نگاه نکنیم و بدردمون نمیخوره پس چه کاریه که من این لاغ های بدرد نخور رو نگه دارم . چون برای این اطلاعات باید یک دیتا بیسی در نظر بگیرم باید یک هارد یا tape براش بخرم .

ابزار ذخیره سازی میخواهد، بعد یکی باید بیاد اینو نگه داره بعد یکی بعده باید بیاد اینو تحلیل کنه خوب چه کاریه !

بهترین کار اینه که من اینو compress ش کنم همینطور که داره on-the-fly میاد اینو کنم . این یک گزینه است که میخواه تا حد امکان حجم اش رو کم کنم.

خوب برای اینکه حجم داده ها رو کم کنیم به سری چیزها نیاز داریم:

#### :Aggregation method -1

یعنی اینکه داده هامون رو جمع کنیم تو یه سری از دستگاه های تمیز و مرتب در طول زمان و متناسب با عناصر مختلف ، این داده های تجمعی شده رو بتونم به یک حد و حدودی برسونیم.( اینو ما لازم داریم بصورت زمانی بصورت المنت یا عناصر تحت پوشش ، اطلاعات مربوط به یک switch را در یک دسته بندی مشخص بذاریم).

#### :Tresholding method -2

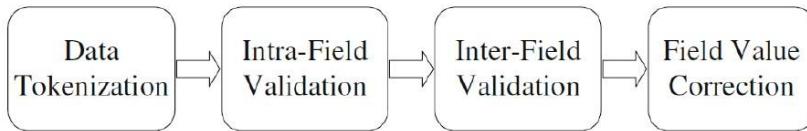
مثلا میگیم اگر دمای cpu زیر 70 درجه بود و لش کن ولی اگر بالای 70 درجه شد به من آلام بد. یا مثلا اگر throughput شبکه زیر 30 درصد شد بیخیال ولی اگر گذردهی بین 40 تا 60 درصد بود به من خبر بده و اگر بالای 70 درصد بود به من آلام جدی بده . چون بالای 70 درصد شرایط شبکه داره ناپایدار میشه و این یک ترشولد هست.

#### :Duplicate elimination method -3

بعضی اوقات برخی اطلاعات تکراری هستند مثلا من میدونم لینک شبکه من که یک ابتدا و انتهایی داره گذردهی این لینک یه عدد مشخصیه و فوقش مثلا 4 تا بسته کم بشه یعنی خراب بشه مثلا 100 تا بسته این طرف میفرستم اون طرف 98 تا بسته میرسه ، 4 تاشم خراب بوده میندازم دور ، 94 تا بسته میرسه. اون کلیت اش مشخصه چرا باید هی تکرارش کنم. این بحث نحوه کاهش داده بوده.

# Pre-DB Data Processing: Data Cleaning

- The process of validating management information being retrieved
  - To reduce the amount of data by eliminating errors
- Why error?
  - Data collection may fail (impartial data)
  - Misconfiguration of devices/agents
  - Implementation bugs
- Data cleaning steps



30



: data cleaning بحث

اینکه چطور داده را تمیز کنم؟ طی یک فرایندی یک سری داده به دست میاد اما ایا همه این داده هایی که بدست اومده داده های منطقی هستند؟

به احتمال زیاد نه. در واقع این اطلاعات باید validate (اعتبارسنجی) بشن. مثلا در یک کلاسی همه نمرات بالا گرفتن ولی یک نفر افتاده پس باید بریم نگاه کنیم شاید اون ۹ که دیدیم ۱۹ بوده و ما اشتباه کردیم.

در هر سیستمی ممکنه یه سری اطلاعات داشته باشیم که این اطلاعات خطأ باشد. در فاز data cleaning من دنبال این هستم که این خطاهای را تا حد امکان از سیستم حذف کنم. مثلا نمره دانشجو که نمیتواند بالای ۲۰ باشد و عدد منفی هم نمیتواند باشد پس وقتی میخواهم اطلاعاتی را ثبت کنم باید به این موضوع بپردازم.

پس هدف از data cleaning این است که تا حد امکان خطاهای داده ای را پاک کنیم. خطاهای داده ای یعنی چی؟

خطا در سیستم دیجیتال شبکه ممکنه به دلایل مختلفی اتفاق بیفته مثل **collector** من که داشته اطلاعات را جمع میکرده یهו خراب میشه. یا شاید **config** اش بد بوده یا اصلا از اول مشکل **bug** داشته. این موارد ممکن است رخ دهد و باعث خطأ شوند.

حالا چطور این خطأ ها را از داده هامون خارج کنیم؟ چه مراحلی دارد؟ این چهار قدم باید طی شود تا به یک **data cleaning** بررسید:

- اول دیتا را **tokenize** کنید
- بعد ارتباطات درون فیلدی را چک کنید
- بعد ارتباطات بین فیلدی را چک کنید
- بعد نهایتاً مقدار خودتون را چک کنید.

## Pre-DB Data Processing: Data Cleaning

- Tokenization
  - Information is divided into record of several values
    - E.g., Temperature trap
      - Low threshold, High threshold, Current value
- Field validation
  - Check data-type and value
    - E.g., all values in the temperature trap must be float numbers in a reasonable rang [-30 ... 90]
- Inter-field validation
  - Check reasonable relationship between fields
    - E.g., Current Value > High threshold or ...
- Correction
  - Drop (common for frequent data) ☺
  - Reuse last valid data
  - Rarely, correction algorithm!



: یعنی من اطلاعات ورودی را میگیرم بعد تکه اش می کنم و در دسته های مختلف قرارشون میدم . مثلا اطلاعات گرمای سنسور را میگیرم و برایش ترشولد میدارم و میگم از

این عدد به پایین سرده از این عدد به بالا گرم و از این عدد به بالا داغه . دمای الان را از سنسور میگرم و در یکی از این سه دسته قرار میدم. پس در اینجا داریم اطلاعات را تفکیک میکنیم.

**Field validation** : اینجا اطلاعات را اعتبارسنجی میکنیم که مثلا data type اش درست باشد و مقادیرش درست باشد و غیره. مثلا نمره دانشجو باید بین 0 تا 20 داشته ایا این نمره بین 0 تا 20 هست؟ یعنی ایا این مقدار معتبر هست یا نه؟

**Inter-field validation** : ارتباط بین فیلدها : برخی از فیلدها با فیلدهای دیگر مرتبط هستند. مثلا اگر میخواهم سیستم سرمايش را روشن کنم اینجا سیستم سرمايش مربوط به دمای هوا میشود. اگر دمای هوا بالا رفت سرمايش را روشن کنم.

**Correction** : فاز اصلاح: در این فاز من میتوانم بگویم این اطلاعات را بریز بیرون چون بدرد نمیخورد. یا این اطلاعات را جانشین کن یا اصلاح کن. این فاز قبل از ذخیره سازی هست. هزینه میکنیم برای اینکه اطلاعات درست بشود.

## Pre-DB Data Processing: Data Format Conversion

- Data should be sorted in DB in common formats
  - Different protocols is used for monitoring
  - Multiple applications use the monitored data
- Straightforward approach
  - Develop a converter SW for each incoming data format
    - To convert the data to desired format
- Technology specific approaches
  - E.g., XSLT for XML transformation
    - If all input data are formatted in XML files using different tags → Appropriate XSLT files create common output



بحث دیگری که مربوط به پیش پردازش هست، بحث فرمت اطلاعات می باشد . قبل از اینکه اطلاعات را در دیتابیس ذخیره کنیم، خیلی اوقات میخواهیم با فرمت خاصی ذخیره شود به دلایل مختلفی مانند بازیگر های مختلف- پروتکل های مختلف – app های مختلف – دستگاه ها و کاربران مختلف در مدیریت شبکه که هر کدام فرمت خاص خودشان را دارن. اما بهتر است یک فرمت به صورت مشخص باشد تا همگی از همان فرمت استفاده کنند.

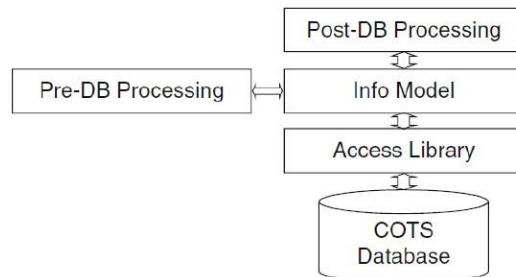
برای تبدیل فرمت دو راه داریم:

-1 - **Straightforward**: روش مستقیم: هر چه اطلاعات امد به طریقی فرمتش را عوض کن و بفرست بره.

-2 - **Technology specific** : مبتنی بر تکنولوژی : مثلا اگر من میخواهم از انتقال xml استفاده بکنم باید xslt هم داشته باشم در غیر این صورت اصلا نمیشه.

# Management DB

- Store management information for further processing and analyses
  - Typically, different DBs for different applications
    - Different schema & DB design
- Consists of
  - DB core
  - Access library
  - Information model library



33



تا الان اطلاعات را جمع کردیم و پردازش کردیم و حالا میخواهیم ذخیره کنیم.  
اطلاعاتی که ذخیره میکنیم برای این است که بعدا ازش استفاده بکنیم یعنی بخوانم و تحلیل کنم و به نتایج بهتری برسم.

برای این کار دیتابیس های مختلفی داریم که متناسب با کار و نیاز و شرایط ازشون استفاده میشود مانند: سیستم ای مدیریت پایگاه اده (DBMS) – دیتابیس های sql دیتابیس های رابطه ای و object oriented و غیره . ولی چیزی که معمولا استفاده میشود دیتابیس رابطه ای است.

از نظر ذخیره سازی اطلاعات روی دیتابیس، type های مختلفی داریم:  
برای کار با یک دیتابیس به این موارد نیاز داریم:

DB core  
Access library  
Information model library

# Management DB Scalability

- Two aspects of scalability
  - Time: To store all information in network lifetime
  - Network size: To store information of all devices
- Design approaches
  - Partitioned DBs: single table of information is split across multiple tables, a key (e.g., hash of network address) is used to select DB
  - Rolling DBs: Partitioning over **time**, suitable in the case of naturally sequential data (e.g., fault)
  - Hierarchical DBs: Partitioning over geographical distribution of information, higher level aggregate lower level DBs



34



برای یک دیتابیس بحث **scalability** مهم هست. عواملی که روی مقیاس پذیری دیتابیس شدیداً تاثیرگذار هستند و انتخاب دیتابیس من و DBMS من باشد:

از نظر **time**: یعنی دوره زمانی که اون حجم از اطلاعات را بتوانه نگه داره براش مهمه چون قرار است کلی اطلاعات مدیریت شبکه را ذخیره کند.

و از نظر **network size** : و خود اندازه شبکه هم مهم هست مثلاً اگر من یک شبکه کوچک داشته باشم با سرور هم جمع میشود ولی یک شبکه خیلی بزرگ دیگه باید برم سراغ oracle و پایگاه داده های بزرگتر.

راه های مختلف برای طراحی دیتابیس:

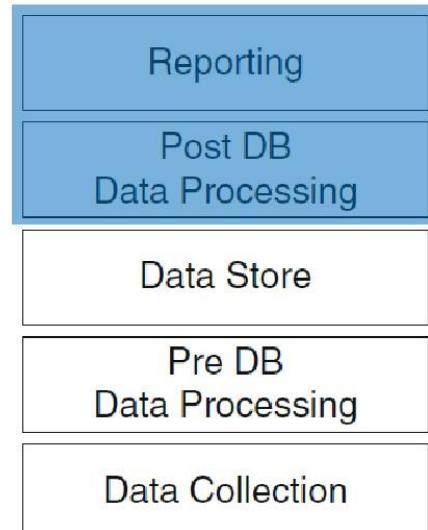
: مثلا دیتابیس من خیلی بزرگ شد میام تقسیم اش میکنم . یه قسمت برای سویچ ها یه قسمت برای روتراها یه قسمت برای لینک ها و غیره. جداول مختلفی برash تعریف میکنم و از کلید خارجی برای ارتباط بین جدولی استفاده میکنم.

علت استفاده از این دیدگاه: به جای استفاده از یک دیتابیس خیلی بزرگ از چندین دیتابیس کوچکتر استفاده میکنم تا بتوان با سیستم های سبک تر و ساده تر مدیریت شون کرد.

: امکان دارد در طول زمان دیتابیس ام را پارتیشن کنم . مثلا بگویم این دیتابیسم ساخته میشود تا جاییکه اندازه دیتابیس ام بشود 10GB اطلاعات. ده گیگ که تمام شد یک ده گیگ دیگر بساز کنارش و الی آخر. یعنی متناسب با زمان و حجم اطلاعات وارد شده هی دیتابیس ام را پارتیشن میکنم. پایگاه داده سلسله مراتبی : تقسیم بندی براساس موقعیت جغرافیایی.

## What is missing?

- Post DB processing and Reporting depends on NM function
  - Post processing is core of each function
  - There are some reporting facilities for all NM functions
    - However, functions use specific dedicate reporting mechanism
- These are the subjects of up coming lectures



زمانی که میخواهیم ریپورت بگیریم باید متناسب با کارمون گزارش گیری کنیم. اما کارمون چیه؟ پس اول باید بفهمم چه ریپورتی باید بگیرم و چون نمیدونم ریپورتم چیه پس اول باید بفهمم چه ریپورتی باید بگیرم و چون نمیدونم ریپورتم چیه. چون براساس ریپورت من خواهد بود.

# FCAPS

---

## Network Management

Spring 2013

Bahador Bakhshi

CE & IT Department, Amirkabir University of Technology



*This presentation is based on the slides listed in references.*



# Outline

---

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management
- Conclusion



2



# Outline

---

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management
- Conclusion



3



# Fault & Root Cause & Symptom

## ➤ Fault

- An event that causes unintended, or unspecified operating conditions in network

## ➤ Root Cause

- Is the occurrence of a specific type of fault
  - E.g., Component failure, Misconfiguration, ...
- Is rarely observed directly

## ➤ Symptom

- Fault messages generated due to occurrence of root cause
- An indication of fault for management system



4



: هر رویدادی که باعث یک واقعه‌ی ناخواسته یا عملیات نامشخص و بی دلیل شود را **Fault** یا **faulty** خطای میگوییم. (رویدادهایی که فرایند معمول را مختل میکنند) به دلایل مختلف اتفاق می‌افتد مثلاً ممکن است یک پورت شبکه بسوزد و دیگر **receive** و **send** انجام نشود. یا مثلاً پیکربندی اشتباه انجام دهیم و غیره.

: وقتی یک خطای خطا میدهد به ندرت ما به صورت مشخص دلیل واقعی آن خطای را میبینیم. بیشتر حواسی آن را میبینیم و دلیل واقعی را کشف نمیکنیم.

: گاهی کلی پیام خطا دریافت میکنیم که این پیام‌ها از جاهای دیگر می‌ایند و اصلاً منبع اش را نمیدانیم فقط بیانگر این است که در شبکه یک خطایی رخ داده.

# Fault Management

## ➤ Fault management

- Monitoring the network to ensure that everything is running smoothly
  - Symptoms collection
- Reacting when this is not the case
  - Analysis symptoms to determine root causes

## ➤ Ultimate objective

- Ensure that users do not experience disruption
- If do → keep it minimum



5



پس وقتی از fault management صحبت میکنم یعنی باید بیام شبکه ام را پایش یا مانیتور کنم و مطمئن بشم همه چی درست مثل ساعت کار میکند خیلی smooth و نرم و روال کار میکند. و وقتی دیدم یه چیزی اونی نیست که باید باشه(یعنی یک خطأ یا خرابی در شبکه) باید بلافصله واکنش نشون بدم.

چرا باید سریع واکنش نشان دهم؟ من fault management را میخواهم تا کاربران من کمترین تجربه‌ی تداخل و بهم ریختگی ان سرویس را داشته باشند.

# Fault Management Functionalities

- Network monitoring
  - Basic **alarm** management
    - Advanced alarm processing functions
- Fault diagnosis
  - Root cause analysis
  - Troubleshooting
- Trouble ticketing
- Proactive fault management



6



چه کارهایی را باید انجام دهد:  
: Network monitoring -1

تصورت پایه یک سیستم مدیریت باید آلامر داشته باشد تا متناسب با خطایی که اتفاق افتاده یک آلامی صادر شود.

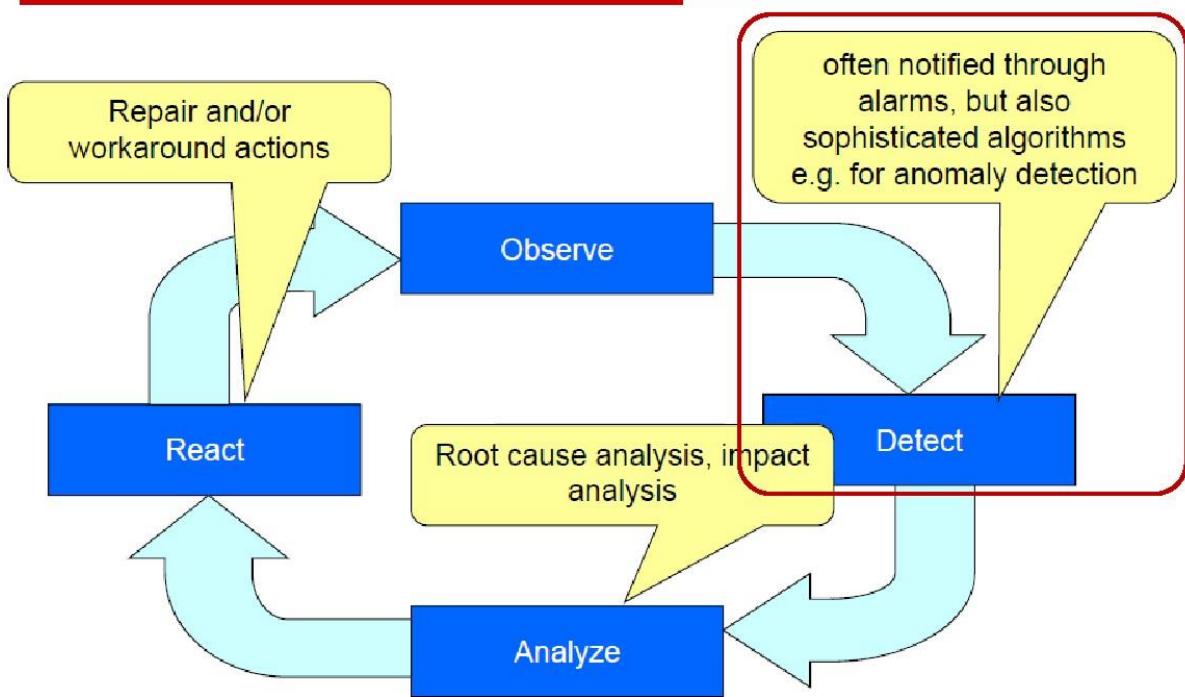
-2 : تشخیص خطا:

وقتی خطایی رخ داد، این سیستم باید ب-tone بره ریشه‌ی خطا را پیدا کند. وقتی ریشه خطا را پیدا کرد میتواند بروд troubleshooting انجام دهد و سعی کند مشکل را حل کند. ( زمانی میتوانیم مشکل را حل کنیم که دلیل خطا را بدانیم).

-3 : یک سری خطاها بوجود میاد که سیستم متوجه نمیشے . راه حل اینه که کاربر بیاد تیکت بده به سیستم fault management که سیستم شما در فلان محل دچار خرابی یا مشکل شده.

-4 : باید به مدیریت خطا بپردازیم پیش از وقوع خطا.

# Fault Management: Monitoring & Detection



8



این چرخه سیستم مدیریت خطا هست که میگوییم اول خطا را کشف میکنیم بعد خطا را آنالیز میکنیم تا دلیل اش را بفهمیم و متناسب با اون خطا واکنش نشان دهیم.

# Fault Indication: Alarms

- Alarm **condition**: an unusual and unplanned for condition that needs management attention
  - Alarm message: Indication of an alarm condition
- Examples
  - Equipment alarms: “A line card went out”
  - Environmental alarms: “Temperature too high”
  - Service level alarms: “Excessive noise on a line”
- Not every event message is an alarm, however, there can be grey lines
  - “A line card was pulled”: Maintenance or unexpected?



9



یک شرایطی پیش میاد که سیستم من آلام میده تا به مدیر شبکه بفهمونه که خطای رخ داده. مثلا این کارت شبکه unplug شده یا این لاین کارت شبکه سوخته یا روی این خط نویز زیاد داریم یا دمای cpu رفته بالا و غیره.

آیا هر پیامی بیاد تحت هر شرایطی باید آلام حسابش کنم و بهش رسیدگی کنم؟؟ نه. فقط برخی آلام ها نیازمند رسیدگی و توجه هستند. آلام ها دسته بندی مختلفی دارند و مثلا من در حال لگین هستم و دوبار رمز ورود را اشتباه زدم و بار سوم درست زدم آیا این چیز مهمی است؟ نه. پس ارسال آلام برای هر اتفاقی صادر نمیشه.

مثلا خود مدیر شبکه در شرایط maintenance (نگهداری) میاد لاین کارت رو درمیاره خوب این یک شرایط غیرمنتظره نیست بلکه خود مدیر این کار را میکنه پس اینجا آلام دادن به مدیر معمول نیست. ولی اگر تو شرایط عادی شبکه یه لاین کارت قطع بشه اینجا حتما باید آلام بده چون اتفاق unexpected (غیرمنتظره) هست.

## Alarms (cont'd)

- Alarms are associated with specific information
- E.g. X.733: Alarm reporting function

- Affected system
  - Time of occurrence
  - Correlated alarms
  - Severity
  - Probable cause
  - Recommended repair action
  - Additional information
- } part of the additional information transmitted as part of the alarm
- } part of the alarm definition



10



استاندارهای مختلفی برای آلام وجود دارد مانند X.733 که قسمت های مختلفی دارد مثل : کدام سیستم آسیب دید – در چه زمانی بود- آلام های مرتبط اش کدام ها هستند- درجه سختی اش چیست – دلیل احتمالی اش چیست – و چه فرایندی برای تعمیر یا repair اش پیشنهاد میشه – و اطلاعات اضافی.

# Alarm Severities

- There are different standards for severities
  - ITU-T X.733 – 6 levels: critical, major, minor, warning, indeterminate, cleared
  - IETF syslog – 8 levels: emergency, alert, critical, error, warning, notice, informational, debug
    - No category for “cleared”
    - Covers any event, not just alarms



11



درجه سختی آلام:

استاندارهای مختلفی برای درجه سختی وجود دارد:

مثلا x.733 که توسط ITU-T معرفی شده، 6 سطح سختی تعريف کرده است:

Critical- major و غیره (در اسلاید هست).

ولی IETF در 8 سطح سختی تعريف کرده است:

Emergency – alert و غیره (در اسلاید هست).

در syslog نداریم بلکه debug ، syslog و چیزهای بیشتری را پوشش داده.

# Fault Management: Alarm Management

## ➤ Basic functions

- Collect alarm information from the network
- Visualize alarm information

## ➤ Advanced alarm preprocessing

- Filtering
  - Subscription
  - Deduplication
- Correlation
- Augmentation



12



مدیریت آلام بخشی از مدیریت fault هست:

یعنی بر مالام های شبکه را جمع کنم و از تو دل اون الام ها یک سری اطلاعات قابل درک و فهم بکشم بیرون یعنی یه جوری اون الام رو مصور(visualize) کنیم.

هدف فقط جمع اوری الام ها نیست بلکه باید اون ها را پردازش هم بکنیم.  
برای پردازش یک سری فرایندهایی لازم است:

-1 Filtering : خطاهای مربوط به حوزه ای که توش خطا رخ داده را فیلتر کنم یعنی جداشون کنم.

-2 Correlation : فهمیدن ارتباط بین خطاهای چون ممکنه یک سری خطاهای بصورت دسته جمعی به یک دلیل اتفاق افتاده باشن. وقتی خطاهای بهم مرتبط رفتارهایشون هم متاثر از یکدیگر هست.  
اینجا اگر بتوانم ارتباط را پیدا کنم میتوانم خطاهای را فیلتر کنم.

-3 Augmentation : افزایش: اگر در محلی اتفاق بیفتد، اون خطا باعث کلی خطای دیگر میشود.

## جلسه سیزدهم

ما در جلسه گذشته درباره `FCAPS` صحبت کردیم و از `fault` شروع کردیم و گفتیم که وقتی بخواهیم `fault` را مدیریت کنیم یک سری توابع پایه و یک سری توابع پیشرفته داریم.

که در توابع پایه ما اطلاعات پایه را از شبکه جمع اوری میکنیم و اون هارو `visualize` میکنیم.

اما در توابع پیشرفته میتوانیم فیلترینگ داشته باشیم که شامل `deduplication` و `subscription` هستند.

در اینجا میتوانیم الارم های تکراری را حذف کنیم، یک سری اطلاعات خاص را از یک سری گزینه های خاص دریافت کنیم، بحث `correlation` یا همبستگی را داشتخت باشیم.

به هر حال توابع زیادی را توی مدیریت `fault` میتوانیم داشته باشیم.

# Alarm (event) Collection

- Typically passive approach for monitoring
  - Event messages
  - Agent-initiated communication
- Manager is waiting
  - Trap server is listening on specified port
- Agent detects failures and sends event message to server; how?
  - Hardware interrupts
  - Local periodic monitoring by agent



13



ما وقتی بحث **fault** را مطرح میکنیم ، آلام های ما اصولاً آلام هایی هستن که نشان بهنده ی وقوع یک شرایط نا متعارف هستش، این شرایط مشخصا در شرایط آلام در سمت مقابل هستش و در سمت کلاینت اون **agent** که روش هستش میاد آلام میده یعنی سروری مثل من شروع کننده ی یک موضوع در بحث آلام نیست و سرور نشسته یه جا داره کار خودشو انجام میده (نشسته ی جا تخمه شو میخوره) و **agent** هستش که اون سمت اگه مشکلی رو ببینه میاد اعلام میکنه .

پس میتونیم بگیم در بحث **collection** یا جمع کردن آلام ها عملاً ما یک دیدگاه **passive** را داریم برای **monitoring** که یک سری مسیج های مختلف میان **agent** و **manager** هستش که شروع کننده ی ارتباطه که مربوط به **event** های مختلف در اون دستگاهی که **agent** روش هست منتشر میشه و ارسال میشه برای ما .

پس میتوانیم بگیم عما **manager** من به صورت **passive** یا غیر فعال هستش و معمولاً من نشسته و منتظره و یکی میاد بهش آلام میده .

پس **agent** هستش که اون جا همه کارس.

حالا **detect** چه جوری **agent** میکنه ؟

توی فرایند های داخلی خودش یک سری وقفه هایی رو تعریف میکنه که وقتی وقفه اتفاق افتاد این **agent** متوجه بشه.

یا برای **agent** تعریف کنیم به صورت دوره ای بره منابع این دستگاه رو بررسی کنه .

مثلاً اگر سخت افزاره به صورت دوره ای بیاد بگه مثلاً **cpu** اینقدر و هارد اونقدر و ... و بعد هم گزارش اعلام کنه و هر وقت به مشکل برخورد بیاد اعلام کنه و از وقفه ها برای اعلام شرایط استفاده کنه یا اینکه کلا خودش بیاد نظارت کنه

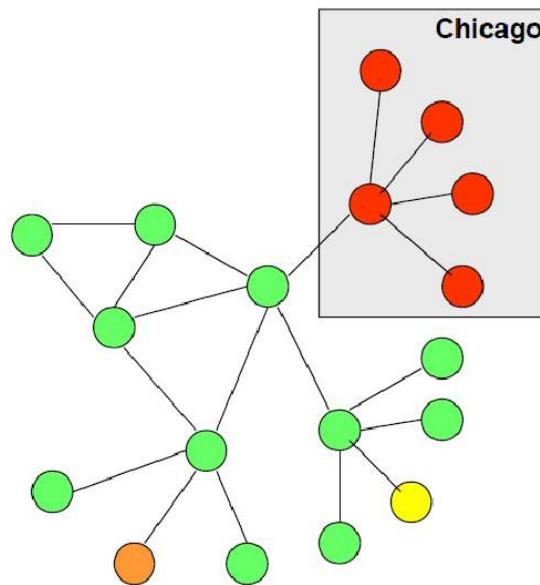
وقفه های سیتمی برای سیستم عامل هستش و برای ایجاد وقفه های سیستمی باید سیستم عامل دستکاری بشه .

سیسکو میاد **ios** خودش رو که میده بعد توی **ios** خودش میاد **agent** رو **mbed** میکنه، رو میذاره تو دل سیستم عامل یا اینکه **agent** از نظر برنامه نویسی یک ساختار **programing** داره یعنی برنامه نویسیش میره تو هسته سیستم عامل .

# (Current) Alarm Visualization

Node	Sev	Time	Event	Info
ruby	cr	16:00:42	sysdn	....
jbee	cr	16:00:42	sysdn	...
M3660-sjs	mn	16:00:33	qostc	.....
M3660-sjn	mn	16:00:25	loexc	.....
Pep-7600	mj	16:00:20	dropn	.....
txsouth	cr	16:00:05	sysdn	....
blubber	cr	16:00:05	sysdn	...
Hlee-7569	cr	16:00:04	pwrfl	...
snorkel88954	cr	15:59:58	sysdn	...

List-based:  
current alarm conditions



Topology-based:  
current alarm status



یه موضوعی که مهم هستش اینکه ما آلام میگیریم اما این آلام گرفتن به خودی خود مهم نیست برای ما بلکه موضوع مهم اینکه ما آلام رو visualize کنیم و بذاریم جلوی چشم ملت

فرض کنید این توبولوژی یه شرکت بزرگه و امتداد اون توی شیکاگو به مشکل برخورده و نود های اون توی اون قسمت همش قرمز شده و بقیه قسمت ها سبز هستش . زرد و نارنجی هم داره .(مثل رنگ بندی کرونا 😊)

یکی ممکنه نود بذاره و اینو نشون بده ، یکی ممکنه لیست بذاره نشون بده هر کسی ممکنه سلیقه ای داشته باشه بالاخره و هر جوری این رو مد نظر قرار بده .

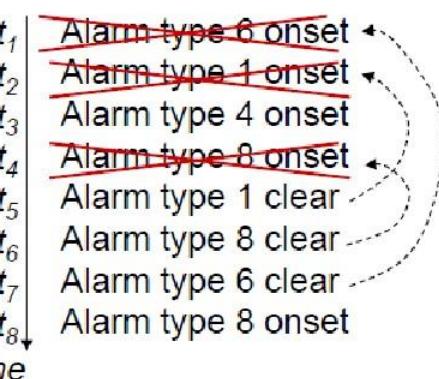
یه موضوعی که این جا مهم هستش و ما چندین بار حرف زدیم اینه که ما در طول زمان لیستی از آلام هارو میگیریم (آلام ها در طول زمان بهمون میرسه)

توی این لیست چیزی که ما میبینیم این که یه اطلاعات وضعیتی وجو داره که ما اون رو نمیبینیم ، بعضی از این الام ها وابسطه هستند به الام های قبلیشون .

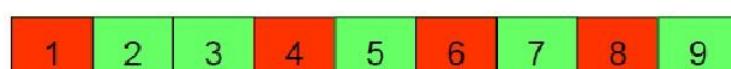
این ارتباطه برای ما مهمه چون اگر ارتباط رو پیدا کیم میتونیم اون لیستمون رو سریعتر مرتب کنیم .

## Alarm Visualization (cont'd)

- Distinguish list of alarms from list of currently active alarms
- Current alarm state requires correlating alarm onsets with alarm clears



(a) Emission of alarms over time



(b) Corresponding standing alarm conditions  
(analogous to LED panel)



مثلا در زمان T2 الارم تایپ 1 اتفاق افتاده است و در زمان T5 این پاک شده .پس این پاک شدنی باید الارم قبلی رو هم پاک بکنه.

پس این اثرات الارم ها رو وقتی میخوایم visual کنیم باید حواسمن باشه که تویی یه تایمی بودن و وقتی از بین رفته ما باید گزینه هامون رو هم غیر فعال کنیم .پس ما نیاز داریم برای آلارم ها یک سری پردازش ها انجام بدیم .اینکه ما ویژال کنیم خوبه ولی خب گاهی اوقات این الارم ها نشون دهنده وقوع یک شرابط دیگه ای هستن یا مثلا گاهی الارم نشون دهنده وقوع یه اتفاقی در اینده هستش.

## Alarm Processing

---

- Alarm collection and visualization are basic required functionalities
- However, in large networks, event information overflows
  - So many alarms + operator → Missed alarms
- Fortunately
  - Not all alarms are the same (alarm filtering)
    - Different severity
  - Usually, alarm are correlated (alarm preprocessing)



اگر ما همه این الارم هارو جمع کنیم توی سرور و زیاد باشه و دچار سر ریز اطلاعاتی بشیم قطعاً یک سری از این الارم ها از بین میره و این برای من میتونه دردرس ساز باشد.

نکته مثبت اینه که الارم ها سطوح مختلفی دارن و اگر ما برمیم تو وضعیت over flow میتونیم خودمون یک سری سطوح رو فیلتر کنیم . مثلاً اگر 50 تا شد اونایی که در حد warning هستش رو بیریزیم دور (اونایی که فیلتر کردیم رو دور نمیزیما فقط نشونمون نمیده )

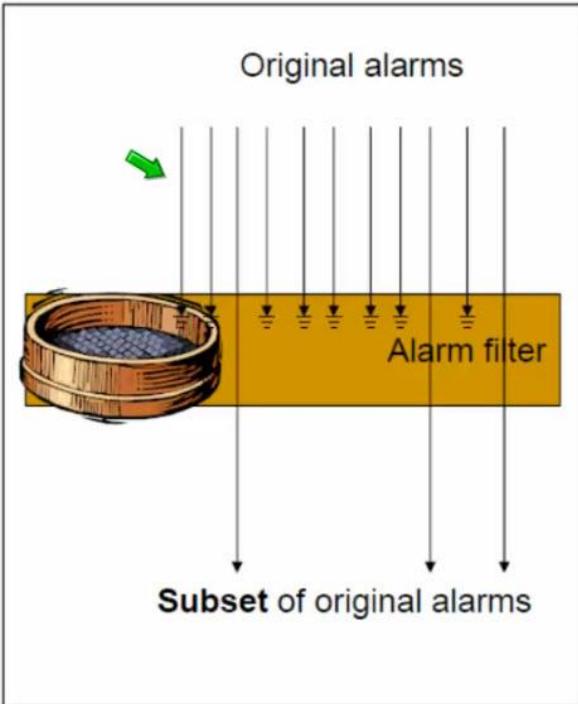
پس الارم هایی که به هم ربط دارن رو بیاییم حذفشون کنیم مثلاً توی یه ساختمون لوله یه واحد در طبقات بالا ترکیده و برای پایین هم مشکل ایجاد میکنه. پس ما بیاییم بالارو لولشو ببنديم تا دیگه برای پایین مشکلی ایجاد نکنه دیگه .

یا مثلاً یه جا تصادف میشه همه وایمیستیم نگاه میکنیم 😅 خب اقا یه عکس بگیر بعد برو کنار و راه ملت رو نگیر

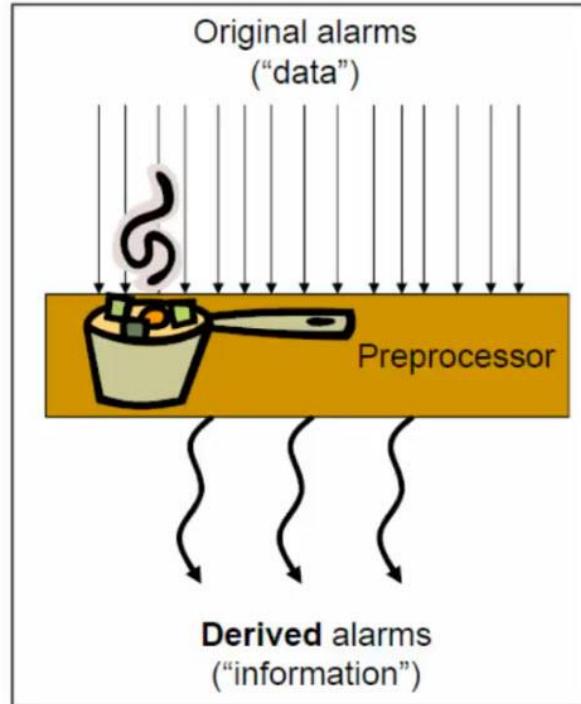
خب اصلاً وایمیستیم که چی بشه ؟ فقط خاله زنک بازیه بعداً میخوای بری تعریف کنی برای بقیه که اقا من اینو دیدم □

پس این الارمی که میگم وابسطس به الارم دیگه وقتی اتفاق بیفته چند تا سیستم دیگه هم دچار مشکل میشن عین تصادفه که تا 2 کیلومتر پشتیش ترافیک میشه ، برید اونو حل کنید مشکل حل میشه .

# Alarm Filtering vs. Preprocessing



(a) *Alarm filtering*



(b) *Alarm preprocessing*

این شکل همین رو نشون میده که یک سری الارم هارو فیلتر میکنیم و نمیخوایم اصلاً ببینیمشون

یک روش دیگه که سمت راست هستش اینه که ما preprocessing کنیم، یعنی تمام الارم هارو بگیریم و روی اجاق گاز تف بدیم و بپزیم و فقط خروجیشو ببینیم .

این preprocessing ایده بدی نیست ولی خب وقت گیره

Alarm هم خوبه ولی خب ما داریم دستی حذف میکنیم و ممکنه اونی که حذف کردیم اتفاقاً مهم باشه ولی خب مجبوریم دیگه چون حجم الارم ها زیاده و بالاخره باید یه کاریش کنیم .

# Alarm (+ Event) Filtering

## ➤ Subscription

- Manager subscribes only for alarm that are really important for him
  - Can be supported as optional features in agent
  - Can be implemented in monitoring software

## ➤ Deduplication

- E.g.,
  - Oscillating alarms
  - Link down alarm from two adjacent routers
- Very simple case of correlated alarms



این فیلترینگ حالا چه جوری اتفاق میفته؟

ما میتوانیم بحث subscription داشته باشیم یعنی یه چیز مشترک بگیریم یعنی مثلاً بگیم توی 6 ماه هیچی روزنامه منتشر میشه یه کپی هم به من بده و پولش رو هم بدیم.

منیجر میاد اون گزینه هایی که برash مهم تر هستن رو رجیستر میکنه و از همونا فقط الارم میگیره. (حتی این طوری هم میتوانیم بگیم که مثلاً فلانی وقتی میخوای تو الارم بدی فقط فلان الارماتو بده)

راهکار دیگه بحث deduplication هستش

میگه اقا مثلا یه لینک قطع شده و این لینک 2 سر داره و بین روتR1 و R2 هستش پس هم قطع میشه هم دیگه

پس 2 تا کپی از الارمش میرسه! خیلی از اوقات این جوریه و یک سری نوسان هایی داریم که الارم هایی که از اون میاد مشترکه و چند بار میادش .

پس میتونیم براش مشخص کنیم که مثلا این 2 تا مال یه سیستم هستش پس اگه یکیش خطدا داد قطعاً اون یکی هم خطدا داده و یکیش رو بدی کافیه .

## Alarm (+ Event) Correlation

- Identify alarms that are related to the same problem
  - Example: alarms from different interfaces on same port
- Idea: Instead of reporting many individual alarms, only a few messages are sent that **summarize** the information from across multiple “raw” events
  - The number of alarm messages is significantly decreased
  - The semantic content of messages is increased

من الارم هایی رو داریم که به خاطر همبستگی میتوانن همون مسئله رو به شکل های مختلف بگن به ما

پس وقتی میدونیم الارم ها corillation دارن میتوانیم اون رو بپزیم و به جای همشون یه خلاصه ای رو نمایش بدیم

اگر این کارو کنیم تعداد الارم هایی که میان و ثبت میشن (چون این کار قبل از ثبت شدنشون انجام میشه ها ولی لزوما هم قبلش نیست یکی ممکنه یه کپی خامشم ثبت بکنه ) کمتر میشه .

اگه استاد هم باشن میگه خلاصش کن چون بار معنایی هم بیشتر میشه (مثل درست کردن رب  ) پس خیلی راحت وقتی میریم دنبال دلیل اصلی مشکل و اینکه بفهمیم چرا الارم داده مهم هستش این خلاصه هه اینجا خیلی اهمیت داره .

# Alarm (+ Event) Correlation

Alarm correlation typically incurs a time delay

- Need to wait if other alarms that could be correlated arrive
- Tradeoff: staleness versus quality of alarm information

Implementation flavors

- Original alarms do not get modified but additional alarm gets generated (specifying which other alarms it correlates)
- Original alarms get modified (add information about correlated alarms)
- Original alarms get replaced with a new, correlated alarm (i.e. correlation coupled with filtering)

مشکل جدی ما در این حوزه اینه که ما میگیم داریم دنبال همبستگی میگردیم پس ما اول باید این وابستگی و دلایلشو پیدا کنیم . پس این رو باید بپذیریم که یه تاخیر زمانی خواهیم داشت (چون باید صبر کنیم الارم ها و دلایلشون برامون مشخص بشه)

خب گاهی اوقات مهمه برامون که سریع جواب بگیریم که در این صورت میشه شرایط staleness که همونalarم رو پردازش کنه و کاری به ادامش نداشته باشه دیگه .

ولی اگر میخوایم stalefull باشه دیگه باید وایستیم و وقت بداریم تا بگذره و بتونیم اون گزارش خوب و باکیفیته رو بگیریم.

این موضوع هستش که باعث تفاوت در پیاده سازی ها شده .

این جا میتوانیم یه فرایند توام filtering و corellaction را داشته باشیم. یعنی اطلاعات پایه را داشته باشیم و هر وقت هم که اطلاعات همبستگی اومد جانشین قبلی کنه.

## Alarm Augmentation

---

- Alarms do not always have sufficient information
- Alarm augmentation: collect additional information about the alarm context, e.g.
  - Current state
  - Current configuration
  - Self-test / diagnostics
- Anticipate which information a manager would request
  - Save an additional mgmt exchange  
→ optimize management pattern
  - Make sure context information is **fresh**, not stale

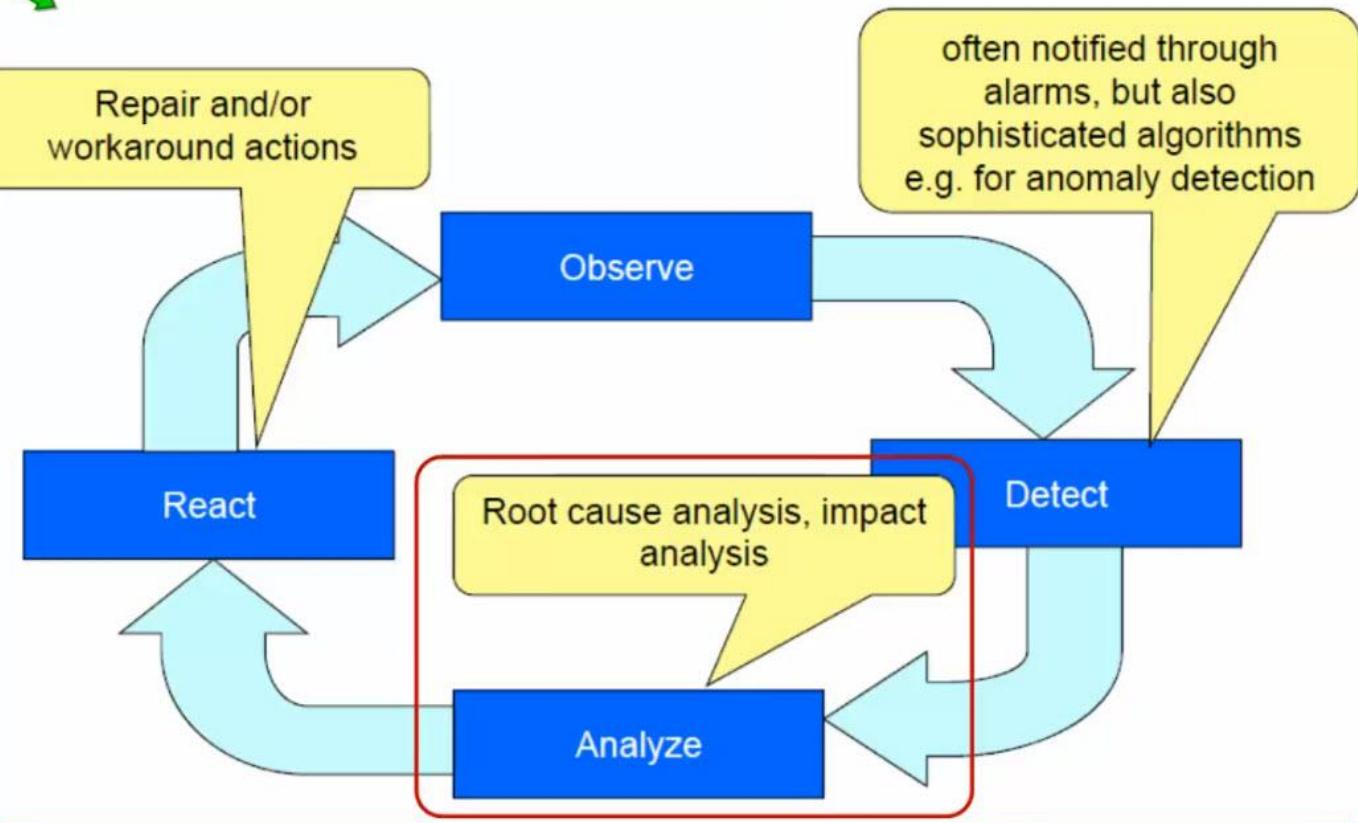


اما نکته جدی اینکه اصلا وقتی ما میاییم و الارمی رو دریافت میکینم یه سری اطلاعات مکانی و زمانی هم داره . ولی الارمی که میخواهد سریع بره قادر اطلاعات اضافه هستش .

وقتی میگیم alarm augmentation به معنی افزایش دادن هستش. پس وقتی الارم رخ میده باید بریم اطلاعات حاشیه ای رو هم جمع اوری کنیم .

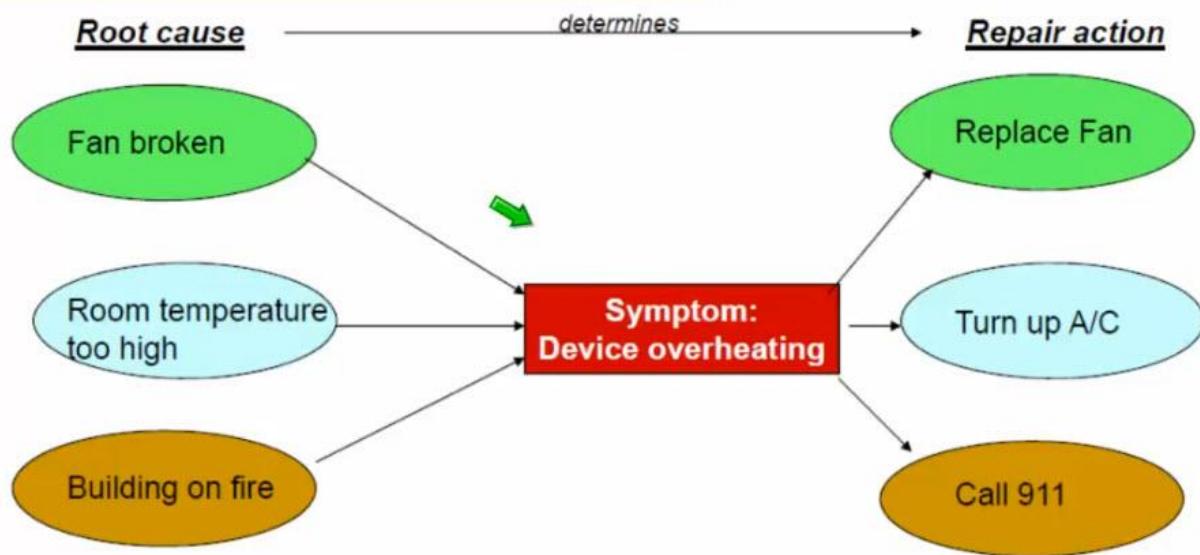
این موضوع مهمی هستش که مدیر یه سری اطلاعات اضافه رو درخواست میکنه برای اینکه بعدا مدریتش رو بهتر انجام بده ها و نسبت به وضعیت اپدیت تر و اگاه تر باشه . اطلاعات مهمه تا ما بتونیم تصمیم گیری بهتری داشته باشیم .

# Fault Management: Analysis & Diagnosis



این شکل همین رو نشون میده که ما نشستیم داریم نگاه میکنیم و اگر مشکلی پیش بیاد متوجه میشیم و میابیم بررسی میکنیم و اتالیز میکنیم و دلایلش رو در بیاریم و تحلیل کنیم و با توجه به تحلیل و تشخیصمون بریم reaction نشون بدیم و حلش کنیم .

# Root Cause Analysis Example



- Techniques to correlate all these events and isolate the root cause of the problem
- Rule-based systems, Model-based reasoning, Case-based reasoning, State transition graph, ...

مثلاً تگاه کنید این جارو اگر یک فن سیستم خراب بشه ، دما زیاد میشه و ممکنه اتیش سوزی بشه این اتیش سوزی دلایل خیلی زیادی میتونه داشته باشه پس بنابه اینکه دلیلش چیه راه حل های خیلی زیادی هم برای رفع این مشکل هستش .

# Rule-Based Systems

---

- Typically, heuristics based
- Codify **human expertise**
  - “If you get a time-out error, see if you can ping the other side”
  - “If that doesn’t work, run IP config to see if your IP is configured”
- Can only assess known conditions
- Don’t need to fully understand inner workings
  - “If you have a headache, take two aspirins”
- Can be built, modified, expanded over time
- Most pragmatic, most commonly used approach
  - E.g., HP OpenView Element Manager



سیستم های rule based معمولاً قوانینی که میارن از سیستم های گذشته هستش و بر اساس تاریخچه ای که داره قوانینی تعریف میشه

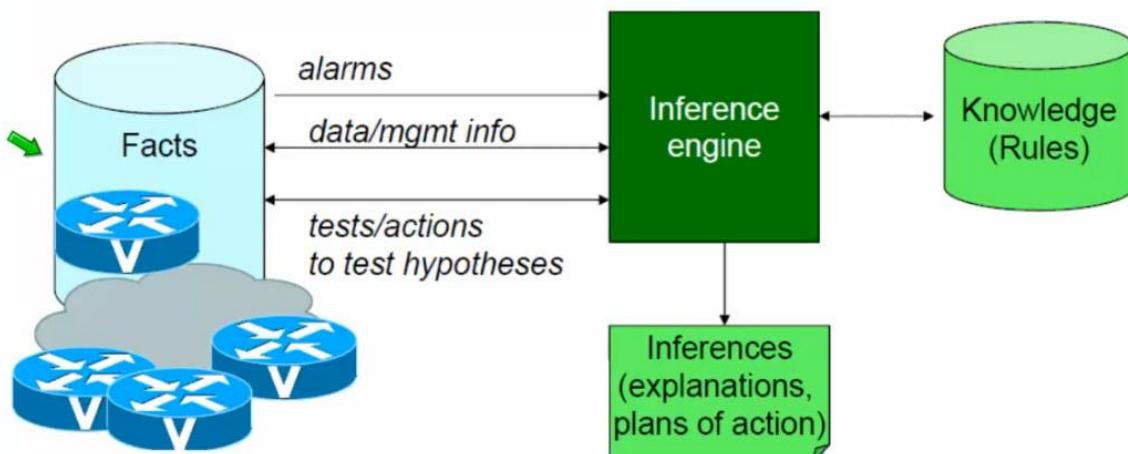
مثلاً یک دیتا سنتر میخوای درست کنی ، چارچوبش این جوری باشه ، سیستم حریقش اون جوری باشه و ....  
یا مثلاً سایت ها میگن هر اینقدر ثانیه سیستم منو پینگ کن و پینگ میفرسته برای سیستم ما تا در دسترس بودنشو چک کنه.

این قوانین رو از کجا اوردیم ؟ تجربس ☺

مشکلش چیه؟ چون بر اساس تجربس اگر چیزی اتفاق افتاده باشه و من قبلًا تجربه نکرده باشم نمیدونم چیکارش کنم .

یا اگر ساختار اون دستگاه رو کامل ندونم نمیتونم مشکل رو حل کنم .پس تجربه باید رشد کنه و اپدیت باشه .

## Rule-Based Systems (cont'd)



ما یه knowledge داریم که این ما حصل یک سری استنباط های قدیمی هستش .

## Rule-Based Systems (cont'd)

---

### ➤ Knowledge base

- Rule-based in the form of **if–then** or **condition–action**,
- Operations are to be performed when the condition occurs

### ➤ Inference engine

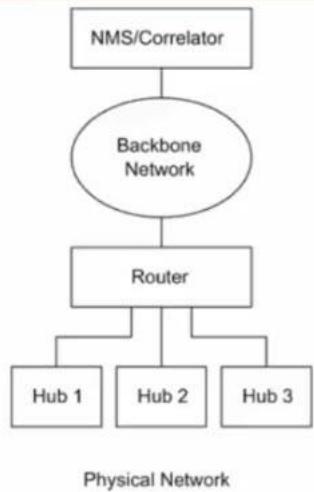
- Compares the current state with the rule-base
- Finds the closest match to output

این قوانین هم حالت شرطی داره دیگه یعنی اگر فلان اتفاق افتاد این کارو بکن.

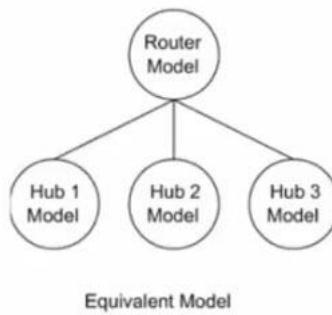
مهم ترین چیزی که هست استنتاجه یعنی بر اساس قوانین باید فکر کنه و بگه بر اساس اسن شرایط نزدیک ترین انطباق برای خروجی چیه .

# Model Based System

- Is built on an object-oriented model associated with each managed network
- Each model checks connectivity to its counterpart object (ping it)
- When connectivity lost
  - Check other node connectivity according to the model
- E.g., Hub 1 model cannot ping its counterpart hub 1
  - Uses the model and checks connectivity of router to its counterpart object
    - If router has lost connectivity → This is router issues, it is not mine



Physical Network



Equivalent Model

27

پس دسته اول rule based هستند و دسته دوم model based هستند.

شکل بالا back bone شبکه رو داره نشون میده.

شکل پایین یک روتیری هستش در بین هاب ها که یه چیزیه شبیه به گراف و connectivity بین اجزا رو بررسی میکنه ، اکثر دستگاه های شبکه این رو دارن و ازش استفاده میکنند . این درواقع مدل object oriented یا شی گرایی هستش .

از بحث شی گرایی استفاده میکنه و یه سری چیزهارو مثل اتصالات چک میکنه .

هر کدام از این مدل ها میتوانن تابع پینگ روشون نصب بشه و تابع پینگ ، پینگ بکنه ببینه متصل هست،  
نیست یا چی

## Case Based Reasoning

---

- Case-based reasoning (CBR) overcomes many of the deficiencies of RBR
- In RBR, the unit of knowledge is a rule
- In CBR, the unit of knowledge is a case
- Idea: **Situations** repeat themselves in the real world
- What was done in one situation is applicable to others in similar, but not necessarily identical, situations

یه مدل دیگه هم case based reasoning است ، یعنی میگه اگر یه کیس خاص رخ بدهد، حالا این گزینه خاص شامل این موارد میشود .

همون روش rule based هستش که قوانین و قواعدی هستش که تعریف میشه ولی مشکلات خودش رو داره .

توی RBR بر اساس قانون حرکت میکردیم ولی این جا در CBR بر اساس case میریم .

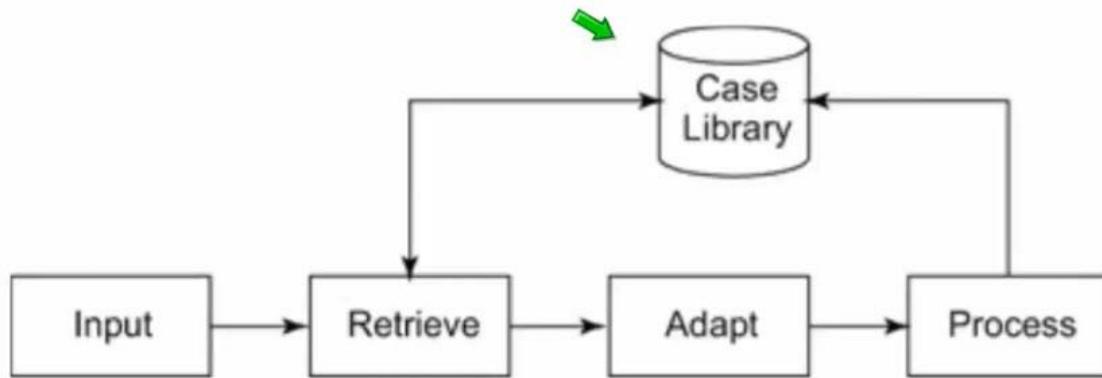
میگیم اگر گزینه خاص یا حالت خاص رخ بدهد آنگاه بیا فلان کارو بکن ، پس قانون نیستا میگیم توی شرایط خاص این کارو کن.

توی دنیای واقعی هم ما همین شرایطو داریم وقتی یه اتفاقی میفته و فلان کارو میکنیم اکی هستش بازم اون شرایط پیش بیاد همون کارو میکنیم دیگه.

مثلا اگر لاستیک ماشین پنچر شد خیلیا میگن ترمز کنیم ! ولی اشتباهه باید اروم اروم سرعت رو کم کنیم . حالا قطعا تویوتا و بنز راه های بهتری داره که پنچر نشه اما حالا اگه شد کیس یکسانه و میتونه ماشین چپ کنه اما شرایط لزوما یکی نیست.

# Case Based Systems

- **Input** module receives current situation
- **Retrieve** compares current scenario with past scenarios
  - If there is a match is it applied
  - Otherwise, **adapt** modules matches closest scenario
- **Process** module takes actions

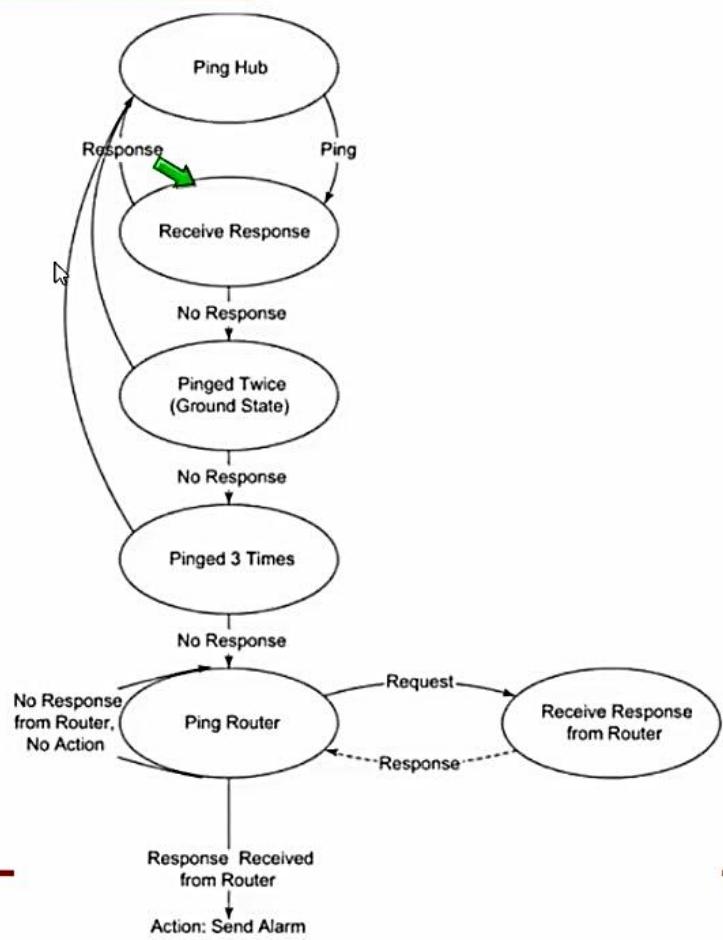


پس ما یه case library میخوایم که وقتی یه اتفاقی میفته بريم مقایسه کنیم با قبلیا و ببینیم قبل چطور بوده و چکار کردیم و چیزی معادل اون شرایط رو پیدا کنیم و راه حل های مشابه رو امتحان کنیم .

مثال دیگه سیستم های پزشکی که مبتنی بر تجربه هستش، یه دکتری مثل واشه چیزی قرصی میده و نتیجه رو میبینه . توی همین جریان کروناهم این قضیه خیلی دیده شدش .

# State Transition Graph

## ➤ Example



مدل دیگه state transition Graph هستش. (گراف تغییر حالت )

میگه اگر پینگ کردی جواب داد که هیچی اگر نداد دوباره و دوباره پینگ کن ولی اگر بیشتر از 3 بار پینگ کردی جواب نداد یعنی یه جای کامیلنگه دیگه .

اصلا شاید روتر رفته رو هوا خب اونو میریم پینگ میکنیم ببینیم چه خبره.

چالشی که وجود داره اینه که ما باید تموم اون state هارو بشناسیم .

پس جریان کار باید قشنگ مدل شده باشه تا بتونیم از این استفاده کنیم .

## Fault Management: Trouble Ticketing

- Purpose: Track proper resolution of problems
  - Collect all information about a problem
  - Ensure proper steps are taken
- Typically addresses end user perspective
  - Keep track of current resolution status
- Alarm vs. Trouble ticket
  - Alarms: bottom-up, notified from the network
    - Related to problems in the network
  - Trouble tickets: top-down, notified by end users
    - Related to problems with a service (provided by network)

یه موضوع دیگه که داریم Trouble Ticketing هستش .

چیزی که هست اینه که یه سری خطا ها توی سیستم هستش که معمولا سیستم اون هارو کشف نمیکنه .

مثلا میخوایم بیاییم سر کلاس ارور میده بعد ما به адمن شبکه میگیم میگه بیا نگاه کن چی میگی تو میره که

/:

یه سری خطا پس هستش که توسط مدیر شبکه دیده نمیشن ، این دسته رو کاربر ها میبینن.

شما به عنوان کاربر این مشکل رو دیدی باید trouble ticketing بدی یعنی بگی فلان کارو کردم و فلان مشکل ایجاد شدش.

معمولًا حالت هایی توی سیستم هست بالاخره چک نشده یه زمان هایی هست یه مشکلی پیش میاد به عقل جنم نمیرسه خب اون جور وقتا تیکت میدیم به ادمین و توضیح میدیم چیکار کردیم و چه اتفاقی افتاد.

پس این مجزا از الارمه ها، الارم یه ساختار بالا به پایینه و خودش میبینه و الارم میده .

ولی اینجا میگیم ای یوزر تو اگر مشکل داری بیا به من اعلام کن.

# Fault Management: Trouble Ticketing

- Boundary between perspectives can be blurred
  - Some alarm management systems generate tickets automatically
  - Some analogous problems apply
    - E.g. trouble ticket correlation
- Trouble ticket systems
  - Workflow engines that manage the workflow related to trouble tickets
  - Interface Customer Help Desk, CRM in the “front”
  - Alarm Management & OSS in the “back”

اینا جای هم دیگه رو نمیگیرنا و نمیگیم کدوم بهتره ها ، هر کدوم کار خودشون رو دارن .

وقتی الام رخ میده میره برای مدیر شبکه پس اون باید ببینه اما وقتی از trouble ticketing صحبت

میکنیم ، من دارم یه پیام میفرستم برای ادمین شبکه پس اون سمت دیگه یه ادم نیست!

پشت قضیه میتونه به هم برسه ها ولی به طور کل این جوریه .

# Proactive Fault Management

---

- Classical fault management: reactive
  - Deals with problems once they occur
- Proactive fault management
  - Deal with problems before they occur
  - Anticipate problems in making and take preemptive action
- Examples
  - Analyze current alarms for precursors of bigger problems
  - Analyze network traffic patterns for impeding problems
    - Trend analysis to recognize deterioration of service levels
  - Inject proactive health tests

ببینید سیستم های مدیریت شبکه ای که ما الان داریم **reactive** هستن. یعنی این سیستم ما داره کارشو میکنه و یکی یهو الارم میده و این پا میشه بره ببینه الارم چی میگه.

حالا کاری که باید کنیم اینه که اصلا قبل از اینکه شبکه دان بشه و مشکلی پیش بیاد براش باید کاری کنیم پس جلوشو باید بگیریم.

سیستم های proactive به دنبال مشکل هستن قبل از اینکه مشکلی پیش بیاد براش.(سیستم های فعال و پیشگیرانه هستن)

خیلی از سیستم های پروакتیو به ما اجازه میده این الارم های کوچولو کوچولو رو جلوگیری کنیم.

پس الارم های کوچولو و **warning** هارو میاد چک میکنه تا جلوشو بگیره و مشکل بزرگ تری پیش نیادش.

## Fault Management Life Cycle

---

### ➤ 1) Detection of faults

- Reporting of **alarms** by failure detection mechanism
  - E.g., SNMP Traps
- Submission of trouble reports by customers
- Reporting of serious degradation or degradation trend by mgmt functions of PM

### ➤ Time to detect fault is an important issue

- Ideally, we need (near) real-time fault detection
  - Penalty for service outage time

اولین چیزی که وجود داره در **fault** تشخیص **fault** هستش

-1- **تشخیص fault** : در تشخیص فالت ما باید الارم هایی که میاد و نشان دهنده مشکل هست رو باید بگیریم و بگیم فلان مشکل رخ داده است .

این جا یه چیزی داریم به نام **trap** که یعنی سیستم یه مشکلی داشته .

یه قسمت هم که **trouble ticketing** هستش که کاربر مشکلات رو میگه .

یه قسمت هم گزارش های دیگه هستش که از قسمت های دیگس و مثلا میگه کارایی کم شده و ..

حالا سوال : وقتی میگیم بالاخره ما کشف میکنیم **fault** هارو یعنی چی؟ یعنی مثلا 2 سال بعد کشفش کنیم هم خوشحالیم ؟

نه از دیدگاه منطقی کشف مشکل باید بلادرنگ باشه . ولی ممکنه یه موقعی هم مدت ها ما شاهد کشفش باشیم.

امن ترین سیستم های دنیا هم گاهی حملاتی رخ میده که سال ها حتی طول میکشه کشف بشن .

# Fault Management Life Cycle (cont'd)

## ➤ 2) Service restoration

- E.g., Built-in redundancy (host-swap) or reinitialize procedures (Restored SW faults temporarily)

## ➤ 3) Fault Isolation & Root Cause Analysis

- Event/Alarm correlation techniques
  - Case-based reasoning, Rule-based reasoning, ...

## ➤ 4) Prioritize

- Not all faults are of the same priority
- Determine which faults to take immediate action on and which to defer



35



دومین بحث ، service restoration هستش

- سرویس **restoration** : در این بحث موضوع اینه که ما سیستم رو میخوایم برگردانیم . پس اون یرویس دهنده‌ی من هر چی که هست باید redundancy داشته باشه . یعنی اگر یه روتی هستش باید یه روتر دومی هم در کنار اون باشه که ما عوض کنیم سریع (hot swap) اینو بر میداریم اونو سریع میداریم جاش.

(تشخیص دلایل ریشه‌ای مشکلات ) **Fault isolation & root cause Analysis -3**

چرا و به چه دلیلی این اتفاق افتاده؟ پس اینم یه موضوعه که وقتی خطایی رخ میده باید بریم دلیل واقعی رو پیدا کنیم

#### -4 Priority يا الويت :

الارم های ما درجه سختی متفاوتی دارند و این الارم ها حتما مشکلی بوده که به وجود اومده . ما میگیم مثلا این دسته از fault هارو بیخیال ولش کن اصلا فقط شرش رو کم کنه بره و بگیم بیا این خسارت

رو بگیر جمع کن برو فقط 😊

اما گاهی خب شرایط حساسه و مثلا کل روتر میره رو هوا و نابود میشه پس بدو بدو باید بره ببینه چیه.

## Fault Management Life Cycle (cont'd)

### 5) Troubleshooting

- Repair, Restore, Replace
  - Depends on failure & affected entities

### 6) Reevaluate

- Test the operation before service delivery

### 7) Fault Reporting

- Why? Speed up future fault management
- What? Cause & Resolution

#### : Trouble shooting -5

يعنى خطایابی کنه و خطارو که پیدا کرد بره سیستم رو restore کنه و برش گردونه .

در واقع 3 تا کار میکنه : restore,repair,replace

repair میشه مثلا بافر سوخته میریم یکی میخریم میذاریم جاش.

Restore یعنی هاردمون ترکید و همه چی پرید و میریم برش میگردونیم  
Replace هم که یعنی جایگزین میکنیم

: Reevaluate -6

خطایی رخ داده و اون 3تا کار بالا هم انجام شده و اسن سیستم میخواهد برگرده خب قبلش باید تستش کنیم و این جوری نباشه ببریمیش و ببینیم ای وای باز خراب شد. این جوری مردمم بیشتر عصبانی میشن.

: Fault Reporting -7

گزارش خطاهای است و در اینجا میگیم کجا بوده؟ کی بود؟ چرا بود؟ و چیکار کردیم؟  
این کار یکی از باید های شبکه هستش ولی خیلی ها انجام نمیدن.  
اگر فردا روزی باز مشکلی پیش اومد میاییم اینجا نگاه میکنیم ببینیم چه خبر بوده.

## Fault Management Issues

- Fault detection: By operator vs. By Customer
  - If customer detected → Service has been violated
- Time to restore service
  - SLA violation penalty depends on this service outage duration
  - Time horizon
    - Real-time: backup/redundant system
      - Most network devices support automated failover
    - Short-term: Alarm detected by admin in NOC
      - Network reconfiguration, ...
    - Long-term: Trouble ticket by customer
- Disaster recovery plan
  - Must be considered in network design phase
  - Plan and procedures must be developed

## چالش هایی که مدیریت شبکه به وجود میان

- 1- کشف فالت: یه زمانی توسط اپراتور کشف میشه یه زمانی توسط مشتری ها کشف میشه اگر توسط اپراتو کشف بشه معمولا در سطح یه سیستم سخت افزار و نرم افزار هست و مشکل جزئیه اما اگر توسط مشتری کشف بشه یعنی سیستم از حالت نرمالی که باید باشه خارج شده .
- 2- چقدر طول میکشه برش گردونیم: به هر حال یه خطای رخ داده و باید برطرف بشه و هر جوری هست دوباره برگردد یعنی **sla** نقض شده پس ما باید خسارت بدیم (اگر توی سازمان خودمون باشه فحش هاشو بهم میدن  خارج از سازمن خودمون باشه که دیگه با ما قرارداد نمیبیندن .
  - زمان هم برای ما مهمه باید سریع برش گردونیم، باید **redundant** داشته باشیم
  - کوتاه مدت به **NOC** میتونه کمک کنه که مثلا دوباره کانفیگ کنه
  - به صورت طولانی مدت میشه **trouble ticketing** در همون لحظه بر طرف نمیشه دراز مدت برطرف میشه.
- 3- یک رویدادی که تاثیرات قابل توجهی رو در سیستم ما بذاره: مثلا اتش سوزی یا زلزله یا سیل مثلا زلزله بیاد ممکنه ساختمان بریزه پایین .  
این جا میگه وقتی داری شبکه جدید طراحی میکنی یه جوری طراحی کن که سیستم بتونه خودش رو برگردونه

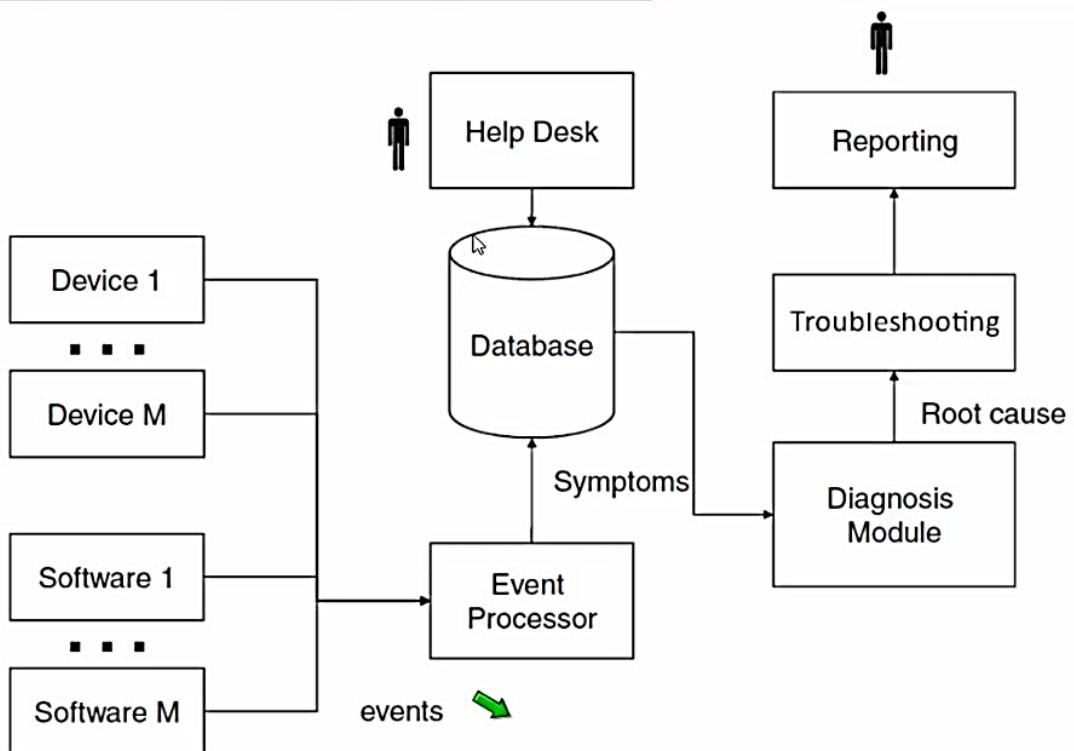
# Technologies in Fault Management

- Automatic fail over
  - Vendor specific in system mechanism
    - Redundant Line Cards in a router
  - Heart beat signaling to check link or equipment
    -
- Alarm notification
  - SNMP trap or property protocols
- Alarm/Event processing
  - Correlation and root cause analysis by “expert systems” (artificial intelligence approaches)
- Customer care
  - Helpdesk systems (24x7 availability)
  - Trouble ticket system (submission and monitoring)

تکنولوژی هایی که در مدیریت fault داریم :

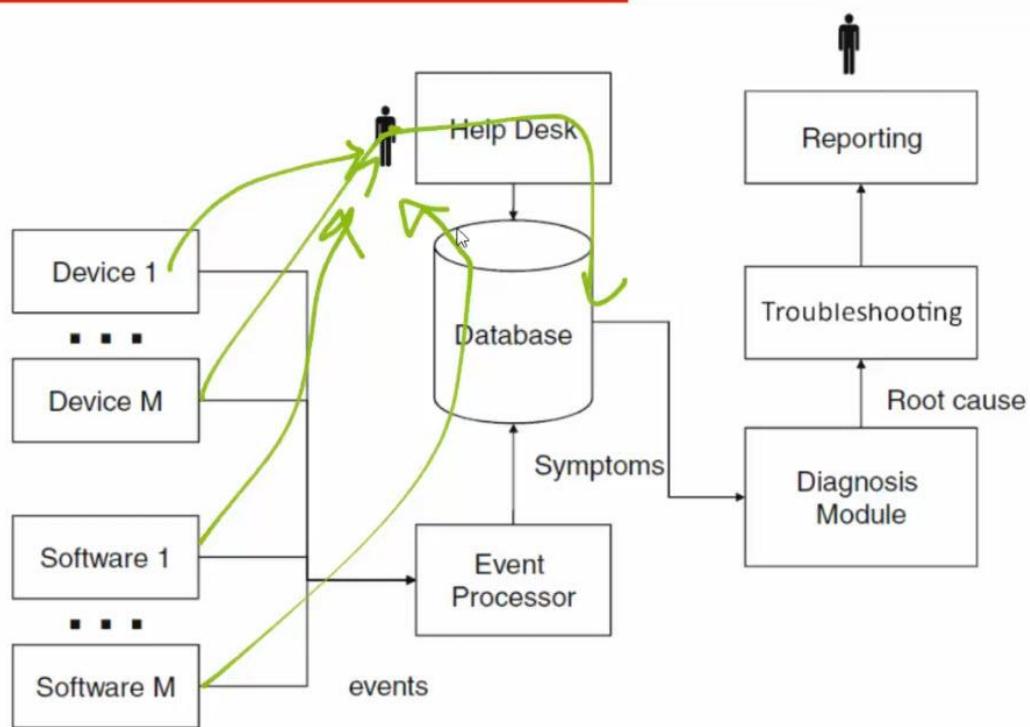
- به صورت اتوماتیک fail over بکنیم : مکانیزم هایی هستش که وندور ها میدارن که وقتی یکیش از کار بیفته اون یکی میاد جاشو میگیره .
- نوتیفیکیشن های الارم : با SNMP و یا سیستم های دیگه نوتیفیکیشن بدیم .
- پردازش الارم ها و رویداد ها : قسمت اصلی همون correlation هستش .
- Customer care : سیستم های 24\*7 که باید در 24 ساعت شبانه روز در دسترس باشن و trouble ticketing میکنن.

# Fault Management Summary



تجهیزات مختلف میاد توی یک event processor و در یک database ثبت میشه و ماژول تشخیص ریشه خطا رو میگه به ما و میریم سراغ trouble shooting و اینکه اینارو برطرف کنیم و گزارش بدیم .

# Fault Management Summary



اینم چرخه کاری مدیریت fault در طول شبکه هستش .

## جلسه چهاردهم

### Configuration Management

---

- What is configuration?
- 1) Description of physical/logical components of a system; e.g.,
  - Network logical & physical topology
  - Physical configuration of routers
- 2) The process of updating parameters of system, e.g., configuring OSPF on routers
- 3) The result of configuration process, e.g., set of management parameters & their values



41



مدیریت پیکربندی چیست؟ سه تا استجواب داره: اول من وقتی درباره پیکربندی صحبت میکنم، شرایط فیزیکی و منطقی سیستم اگر logical یا منطقی باشه کامپوننت های خودشو داره اگر فیزیکی باشه کامپوننت های خودشو داره و یک چیزی بین فیزیکی و منطقی باشه هم باز کامپوننت های خودشو داره ولی در هر صورت از نظر ما configuration کامپوننت ها و اجزایی هست که در اون سیستم وجود داره مثلاً من نیتونم بگم توپولوژی شبکه(چه فیزیکی چه منطقی) یک سیستمه و درباره config اش صحبت بکنم یا در مورد روتر صحبت بکنم

در مورد کانفیگ روتر یا کانفیگ سوییچ در مورد هرکدام از اینها میتونم صحبت بکنم و میتونم یک توصیف رو داشته باشم

بیان دوم یک بیان دیگر از config: یک پروسه یا یک فرایندی که در اون هدف ما آپدیت کردن پارامترهای ospf سیستمی هست مثلاً آپدیت پارامتر الگوریتم مسیریابی

بیان سوم از config: نتایج یک فرایند configuration هست (پارامترهاش و ...)

## Configuration Management (cont'd)

- Functions related to dealing with how network, services, devices are configured
  - Physical configuration, e.g.
    - Equipment, line cards, physical connectivity, ...
  - Logical configuration, e.g.
    - Protocol settings, logical interfaces, address assignments, numbering plans, ...
- Challenges
  - Number of devices/software
  - Diversity of devices/software



ما وقتی میگیم configuration منظور اینکه چگونه یک دستگاهی یک تجهیزی یک دارایی در شبکه باید کانفیگ بشود مثلاً کانفیگ فیزیکی سخت افزاری (مثلاً یک دستگاه رو چگونه کانفیگ بکنم یا این line card یا این پورت نوری چجوری باید کانفیگ بشه connret فیزیک چگونه فعال بشه) یا کانفیگ میتوشه منطقی باشه مثل address plan ها، آدرس ها (ما خیلی وقت ها address plan میخوایم تو شبکه با برای شماره تلفن dial plan میخوایم)

در کانفیگ: تعداد زیادی دستگاه فیزیکی و تعداد زیادی نرم افزار دارم و هر کدام از این دستگاه‌ها تنوع زیادی دارند هم در تعداد و هم در عملکردشون

## Logical Configuration Management

- The process of **obtaining functional data** from each network device, **storing and documenting** that data, and subsequently **utilizing** that data to manage the operations of all network devices
- Includes the **initial configuration** of a device to bring it up, as well as **ongoing** configuration changes
- When to configure
  - System (network & equipment) setup
    - New equipment (hardware)
    - Software upgrades
  - Service provisioning



Logical configuration یعنی توابع و عملیات‌هایی که در حوزه دیتا هستند داده‌های دستگاه‌های شبکه رو بگیرم مرتب بکنم این داده‌ها رو مثلا برای فلان کار استفاده بکنم پس منظور اینکه من با داده‌های دستگاه‌های شبکه کار بکنم (با اون داه‌های عملیاتی کار بکنم) که شامل initial configuration یا پیکربندی‌های اولیه یک دستگاه برای up کردن دستگاه یا یکسری پیکربندی‌های ongoing یا پیکربندی‌های بعدی شبکه

در دو حالت ما logical configuration میکنیم: یک وقتی که میخوایم یک سیستمی رو setup بکنیم

دوم وقتی که من میخوام service provisioning کنم من نیازمند یکسری پیکربندی هستم

# Configuration Management Functions

---

- (Auto)Discovery & Auditing
- Configuration setting
  - Provisioning
- Synchronization
- Image management
- Backup and restore



44



تابع های کانفیگ های مدیریتی چند دسته هستند:

که برای کشف هست Auto discovery

که سرویس جدیدی رو Configuration setting کنم provisioning

همگام سازی در فرایند های دستگاه Synchronization

یکبار کانفیگ میکنیم فقط و برای دستگاه های متعدد image میگیریم ازش image management

و در اخر backup and restore

## CM: (Auto)Discovery & Auditing

- FAPS management areas need current network configuration
- We should be able to query the network to find out what actually has been configured
  - It is called **auditing** (in most cases, it is also called discovery)
- Moreover, we need Auto-discovery
  - Find out the **entities** in network
    - Inventory on the device (licenses, line cards, ...)
- We have already discussed about **discovery techniques and communication patterns for auditing**



45



نیازمند کانفیگ هست ند Faps

ما باید query هایی را بفرستیم که وضعیت شبکه رو ببینیم که در واقع به این میگیم auditing که بیشتر در network discovery مورد بحث قرار میگیره و این discovery ها معمولاً به صورت اتوماتیک هستند entity ها یا فرایند های شبکه کشف بشه حالا این کشف میتوانه در حوزه licence ها باشه یا lincard ها و پورت ها که مربوط به inventory استگاه هست که در discovery میتوانه کشف بشه تا موجودیت هارو در شبکه بتونیم

مدیریت بکنیم

# Configuration Management Inventory

➤ Deals with the actual assets in a network

➤ Equipment

- Type of device, manufacturer, CPU, memory, disk space
- Equipment hierarchies: line cards, which slot, etc.
- Bookkeeping information: when purchased, inventory number, support information, ...

➤ Software

- Software image OS, revision, licenses, ...
- Where & when deployed
- Bookkeeping information: when purchased, inventory number, support information, ...



46



داریم درمورد asset های دارایی های واقعی شبکه بحث میکنیم این دارایی ها یا سخت افزاری هستند یا نرم افزاری مثلا میتوانم بگم نوع تجهیز چیه (سازندش، رم، CPU,...) و یک سلسله مراتب داره مثلا در یک روت، bookkeeping information هاش چیه یا یکسری اطلاعات کلی که اصطلاحا بهش linecard میگیم این دستگاه رو از فلان شرکت در فلان تاریخ خریدیم و پشتیبانیش این شماره تلفن داره، سال ساختش این بوده که برای پشتیبانی دونستن این اطلاعات ضرور هست.

در حوزه نرم افزاری مثلا لاینسنス های نرم افزاری که داریم یا image ها و مهمه که بگیم این لاینسنス ها و این نرم افزارها کی و کجا نصب شدند (کی خریدیم از کجا خریدیم و اطلاعات پشتیبانی و ... داشته باشیم).



## CMDB (Configuration Management Database)

### ➤ CMDB

- Contains information about the configuration of devices in the network
- Relatively **static** but **heterogeneous** information

### ➤ Applications examples

- Network configuration cache to be used in FAPS
- Configuration **validation**
  - Express the constraints the configuration ought to satisfy
    - E.g., IP address in a subnet
    - Automated tools check configuration in CMDB with respect to the constraints
- **What-if analysis**
  - To determine the impact of making configuration change
    - E.g., By creating a simulation model of network using the configurations in CMDB
- Configuration **cloning, backup, and restore**



خیلی مهم هست برای من پس ما یک دیتا بیس نیاز داریم که اون اطلاعات پیکربندی رو تو اون بربیزم که این اطلاعات نسبی و ثابت هم هست و این اطلاعات ناهمگن هستن یعنی از یک جنس نیستند مثلا در مورد کش اینکه بدونیم اطلاعات کش تا کی معتبر هست و یکسری محدودیت های آی پی و ... که این مربوط به بحث های اعتبار سنجی هست

What if analysis یعنی اگر من این اصلاح رو انجام دادم اثراتش چیست که در شبیه ساز ها این نتایج قابل مشاهده هستند و میبینیم این تغییرات اگر اوکی بود در شبکه واقعی میتوانیم پیاده سازی کنیم بعد از اینکه این اثرات دیدیم و config جدید اعمال شد ما باید حتما برایم از اون image استفاده بکنیم و بک آپشن رو نگه داریم که اگر یک زمانی نیاز شد ما از اون بک آپمون در فرایند restore استفاده بکنیم

# CM: Configuration Setting

- (almost) All network devices should be configured properly for the specific network
  - The core of network management
- Element management layer
  - Host name, User, Password, Thresholds, ...
- Network management layer
  - IP address, Netmask, Routing protocol, ...
- Service management layer
  - QoS, VPN, ACLs, ...
  - Called: **Provisioning**



48



برای اینکه بفهمیم دستگاه در کجا مشکل داره باید کلی اطلاعات بگیریم از این مثلا در سطح المنت باید یوزر و پس اون هاست رو بدونید و thresholdهاش چیه و ...

در سطح نتورک باید ... , subnet, mask , ip بدونیم

در سطح service management سطح aceess control list , vpn ، kifiat سرویس ، ... یعنی این اطلاعات رو باید داشته باشم تا بتونم سرویسمو ببرم در جای دیگر شبکه و اون رو دایر بکنم

# Configuration Setting Techniques

- Reusing configuration settings
  - E.g., configuration of OSPF for all routers in the same area →  
All configurations are the same
- Script-Based configuration
  - Approach 1
    - Prepare template script for configuration in general
    - Customize the template per device
    - Apply the customized template via CLI
  - Approach 2
    - Use a high-level script to create configuration files
    - Apply the config file to device via CLI/FTP/...
- Configuration workflow : A sequence of operations to achieve a goal
  - Maintaining a single complex script for whole configuration is difficult
    - Small easy-to-understand script for each module (similar to datastores in Netconf)
    - Invoke the scripts in a specific order → configuration workflow (**automated/manual**)



49



انبوهی از پارامترهای قابل کنترل دارم و برای مدیر شبکه سخت هست که همه‌ی اینها را هر بار چک کنه مثلاً اگر تجهیزات سیسکویی دارم این config‌ها در در دستگاه‌های دیگر هم در شبکه ران بکنم که اصطلاحاً به اون reuse کردن می‌گیم یعنی استفاده مجدد تا بتونیم کمی سرباره‌امون رو کاهش بدیم.

می‌تونیم کانفیگ هامون رو به صورت اسکریپت بنویسیم یعنی بیایم یک اسکریپت تمپلیت درست کنیم و به طور دلخواه بعضی جاهاش رو با کد پایتون تغییر بدیم و بگیم اعمال بشه روی فلان دستگاه و یک روش خیلی خوب هست برای پیکر بندی دستگاه‌ها

یک رو شدیگر این هست که همین اسکریپت رو بنویسیم و بزاریم در یک ftp سروری بعد بگیم دستگاه فلان از روی ftp سرور فلان کانفیگش رو بردار و اعمال کن

یا کانفیگورشن رو می‌تونیم در غالب workflow داشته باشیم یعنی یک فرایند داخل اون اسکریپت طراحی شده باشه یعنی اول باید اینکارو کنم بعد اونکارو کنم و... که مثلاً در حوزه netconf می‌تونه مطرح بشه و این نوع کانفیگ رو می‌تونیم به صورت اتوماتیک یا دستی انجام بدیم.

# CM: Configuration Setting: Provisioning

- Provisioning: The steps required to set up network and system resources to provide, modify, or revoke a network service
  - Bandwidth, Port assignments, Address assignments (IP addresses, phone numbers, ...), ...
- Scope:
  - Individual systems (“equipment provisioning”)
    - E.g. set up a firewall
  - Systems across a network (“service provisioning”)
    - Coordinated configuration across multiple systems
    - Often required to provide an end-to-end service



برای اینکه یکسری سرویس ها دایر کنم نیازمند اینکه یکسری setup ها در شبکه داشته باشم باید یک سری ریسورس ها در شبکه تخصیص بدم یکسری رو حذف بکنم یکسری رو تغییر بدم مثل (پهای باند و port (address assignment, assignment

Scop provisioning کجاست؟ مثلا در حوزه یک سیستم (نصب فایروال و کانفیگ آن) یا در حوزه یک مجموعه از اجزا شبکه یعنی پیکربندی رو در چندین سیستم مختلف اعمال کنم و داشته باشم

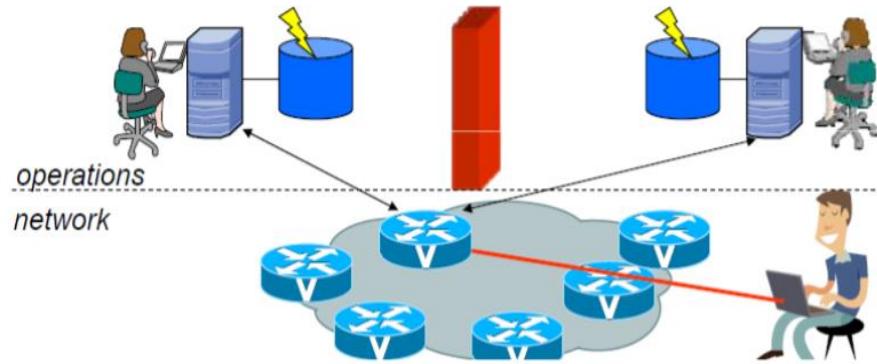
# CM: Configuration Synchronization

- Management systems (CMDB) keep management databases
  - Cache in the database to avoid repeatedly hitting the network
    - Management database and network need to be “*in sync*”
- Counterintuitive: why worry about syncing
  - Configuration information changes **only** through management actions
- Network operations has multiple points of control
  - Provisioning systems for different services
  - Network administrators (operators)
- Configuration **changes** often not reliably indicated
- Synchronization strategy depends on who is the master
  - The network or the management database
  - Fundamental decision in managing a network



هر تغییر در دیتا بیس هم باید ثبت بشه که ما بدونیم که فلان اتفاق افتاده یعنی درواقع **sync** باشه اینکه شبکه دارای اجزا درهم تنیده است نکته مثبت است یا منفی؟ این رو باید بحث کنیم چون تغییرات میتواند در سیستم های مختلف اتفاق بیفتد چیزی نیس که ما هرروز بخوایم بریم کانفیگ رو عوض بکنیم و تغییر پیکربندی میتواند چارچوب های نا مطمئن دیگری برآمون ایجاد بکنه

## CM: Configuration Synchronization

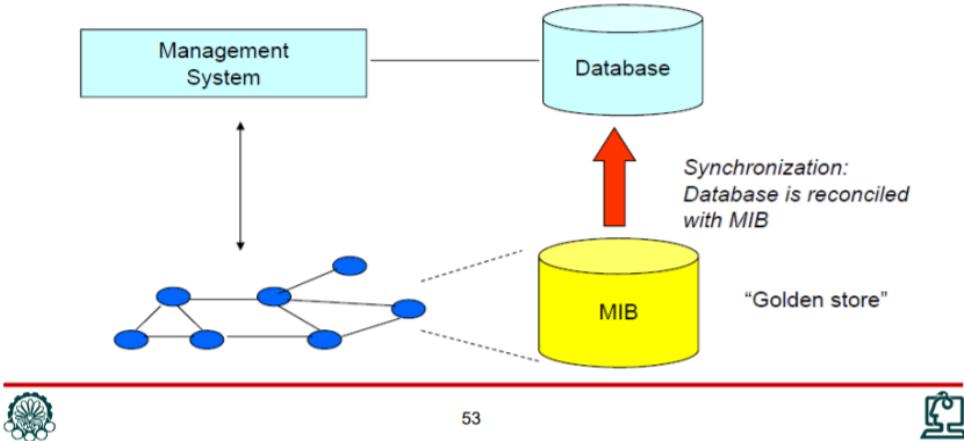


52

برای اینکه سینک باشے باید ببینیم اون نفر بالاسری کی هست و تصمیمات پایه رو کی میگیره که استراتژی syncoranzation خیلی در اون اثر گزار هست.

# Network as Golden Store

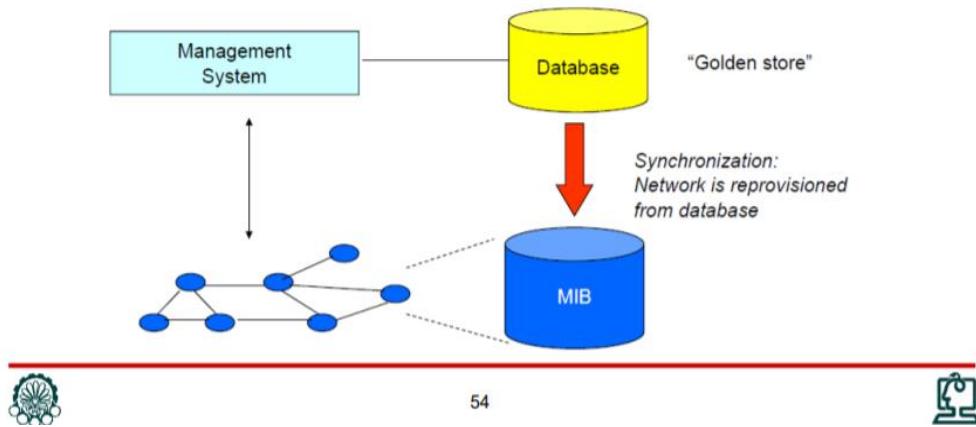
- Most common approach
- Synchronize mgmt database with network
  - Reconciliation or Discrepancy reporting



شبکه مجموعه ای درهم تنیده از سخت افزار و نرم افزاره هر دستگاه ما mib و agent و management system ای که اطلاعات رو تحلیل میکرد میزاشت یعنی داریم در مورد یک فضایی صحبت میکنیم که این فضا پر از دیتابیس و اطلاعاته در طرف دیگر قضیه ما کلی بحث های اصلاحی داریم که اینها همه کار مارو سخت میکنه مثلا اگر یک جاییو درست کنم ممکنه بزنه یک جای دیگر رو خراب بکنه پس در واقعا در دیتا بیس مدیریتی که سینک شده باشه چه اتفاقات مثبت چه گزارش های منفی رو میتوانه نگه داره و بعد در فرایند کاری به من بده

# Management DB as Golden Store

- Common in some service provider environments
  - Very controlled environments
- Discrepancy between network & mgmt indicates that an error occurred in setting up the network
  - Re-provisioning or Discrepancy reporting



به محض اینکه اختلافی در سیستم مدیریتی و شبکه ببینیم یعنی یک جای کار لنگ میزنه و در شبکه یک چیزی تغییر کرده **re provisioning** داشته باشم و دباره برم گزارش خطاهای را ببینیم. زمانی که میخوام اطلاعات جمع آوری کنم فلش از سمت Mib به سمت دیتابیس اما زمانی که میخواهم بحث مدیریت را اعمال بکنم و تجهیزات رو کنترل بکنم فلش رو از دیتابیس به سمت mib میکشه.

## Backup & Restore, Image management

- Backup & restore concerns configuration files
  - Back up working configurations
  - Restoring is quicker, simpler, less error-prone than re-provisioning
- Image management deals with actual software images running on routers
  - Apply upgrades or security patches
- Application challenges mostly related to scale
  - Large deployments can have 10,000's of devices



فرایندهای کاری رو بک آپ بگیرم و در موقع نیاز restore میکنم و هر دستگاه image مخصوص به خودش داره

# Patch Management

## ➤ Patch Identification

- Determination of available upgrades to existing devices that may need to be installed

## ➤ Patch Assessment

- Determining the importance and criticality that any new patch be applied

## ➤ Patch Testing

- Checking whether the installation of the new patches will impact system operation

## ➤ Patch Installation

- Installation of the patches and updating the software of existing applications and devices



56



: اول باید آپگرید کرد تا این نصب ها انجام بشه که میتونه بحث شناسایی داشته باشه Patch identification

چطور این پچ اپلای بشه کجا اپلای بشه اول باید یک نقطه ای تعیین کنم که بگم این نقطه پچ میخواهد به فلان دلیل و اهمیت

این پچ چه بلای سر سیستم میاره و چه کاری میکنه و کارکردش چطوری هست و پرفرمنس سیستم را چه تغییری میدهد

يك installation Patch installation باید کامل باید رخ بده و يك آپدیت نرم افزاری رخ میده و همه چی ختم به خیر میشه

# Configuration Management Issues

- Make sure the inventories be updated
  - Out-of-date inventories (DBs) are useless
  - Autodiscovery mechanism should be used
- Revision control and backup of the inventories
  - Time history of network is needed
  - The configuration management system may fails
- Configuring network equipments
  - Not all configurations are accessible through SNMP
    - Customization needed for each vendor
- Security
  - Configuration process should be secure
  - Insecure configuration → attack



Patch management مشکلات خودش رو هم داره مثلا اینکه شما همیشه باید بدونی که دیتابیس شما در این حوزه دیتا بیس آپدیت شدش و جدیدترین پچ هارو دارید چون اگر بمونه و قدیمی بشه دیگه برد نمیخوره استراتژی کشف خودکار میتونه خیلی مفید باشه برای اینکه دیتا بیسمون آپدیت باشه.

پچ های ما باز هم ورژن دارن در این حوزه باید یک تایم لاین داشته باشم که مثلا این گزینه ها آپدیت شده و تمام وقایع و آپدیت هارو داشته باشم همه تجهیزات شبکه از مسیر snmp کانفیگ نمیشه و یک پیکربندی اشتباه میتونه باعث اختلال در امنیت و منجر به اتک زدن به اون سیستم بشه.

# Configuration Management Technologies

## ➤ SNMP

### ➤ SNMP “Public” Community:

- Gather information about the current network environment, Read-Only

### ➤ SNMP “Private” Community:

- Gather information about the current network environment AND make changes, Read-Write

## ➤ Netconf

### ➤ New protocol by IETF (XML based)

### ➤ Property (vendor specific) commands template to generate appropriate commands for each device



58



Snmp دو تا کامیونیتی داره : public و private که اطلاعاتش رو از کل شبکه میگیره و از شبکه مختص به خودش میگیره

از xml منتقل میشه در موقع استفاده و دستورات و کامندهای مخصوص به خودش رو داره پس یک inventory دارم که میگم چی تو شبکه دارم و یک پایگاه داده پیکر بندی که اطلاعات همه شبکه رو میگیرم میزارم داخلش و این فرایند میتونه برای auditing, provisioning, backup and restore میتونه مناسب باشه

## Accounting Management

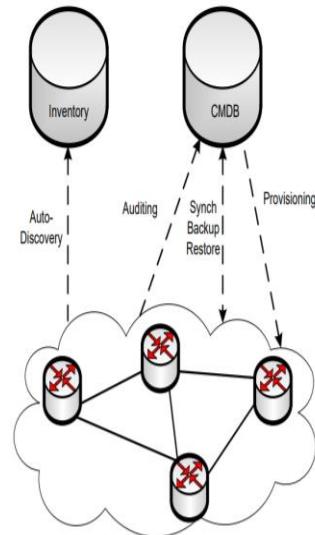
### ➤ Account of the use of network resources

- **Metering:** Measure what has been consumed by whom at what time
- **Charging:** Have the user pay for what has been consumed

### ➤ At the core of the economics of service provider

- Needs to be highly robust, highest availability and reliability
- Otherwise, free service!, lost revenue!

## Configuration Management Summary



61



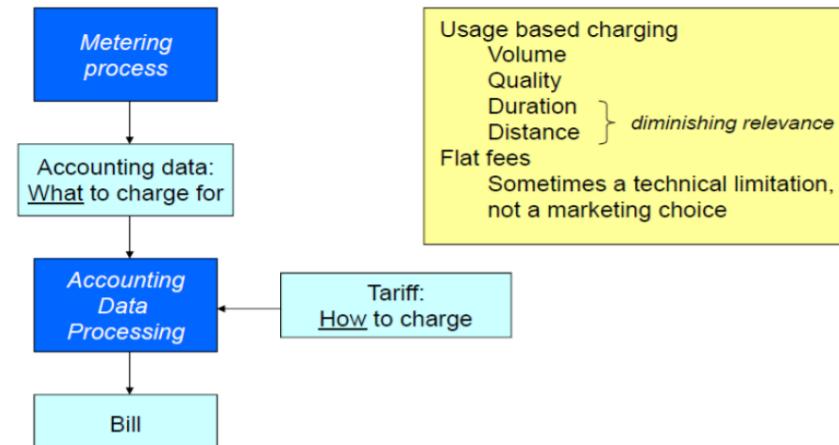
59



اکانتینگ یعنی بیایم حساب کتاب کنیم منابع شبکه چطوری و چقدراستفاده میشه. حالا دو تا موضوع هست اول اینکه من یک متر میخوام که بگه هرکسی در طول بازه زمانی مشخصی بگه چقدر از منابع شبکه استفاده کرده(metering)

و بحث دوم ما معمولاً ب دنبال این هستیم که طرف شارژ کنیم و از طرف پول بگیریم بگیم مثلاً اینقدر صحبت کردی اینقدر قبض تلفن او مده . مثل اپراتورها و .. charging هرچیزی که توجیح اقتصادی نداشته باشه محکوم به فناست در شبکه باید اکانتینگ قوی داشته باشم تا ببینم هر کس چقدر استفاده کرده و متناسب با اون پولشو بگیرم که میتونه highly robust یعنی خیلی قوی و پرفکت و قابل اعتماد و مولادرزش نره باشه (مثال همراه اول)

# Accounting and Billing



63

پس ارزیابی انجام میشے اطلاعات ثبت میشے بعد ترffe ها رو حساب میکنن بعد صورت حساب رو صادرمیکنن

## Accounting Data

- Which data should be measured for accounting?
  - Depends on service type and pricing strategy
- A few examples:
- Call Detail Records (CDRs)
  - Apply to voice service
  - Generated as part of call setup (and teardown) procedures
  - Call statistics upon end of call, or periodically
    - Duration, QoS metrics, etc
- Time based information
  - Duration of IP leases, etc

64



کدوم دیتاهای باید اندازه گیری بشه در بحث اکانتینگ؟ میگیم بستگی داره به چه کلاس سرویسی چه استراتژی قیمتی استفاده میکنید این ها همه تاثیر گزار هست مثلاً یکی میره توشرکت مخابراتی این شماره به این شماره زنگ زده کال ستاپش اینقدر طول کشیده در این بازه زمانی بوده و شروع و خاتمه و مبدأ و مقصد و اطلاعات سرویس رو میگیره و درمورد اینها صحبت میکنه که چی میخاد بشه

اگر بستر آی پی رو اشغال کنه مثلاً رو این آی پی اینقدر ترافیک عبور کرده و در این بازه زمانی و این حجم ترافیک مریوز به شما بوده

## Volume based Data (Volume)

### ➤ Volume based information

- Interface statistics
  - Packets sent & received, etc
- Flow records
  - Records about end-to-end IP traffic
  - Can apply some service level matching
    - E.g. duration of TCP connection: TCP syn / syn-ack, fin / fin-ack exchange
  - More sophisticated: deep packet inspection + service signatures
    - Concerns over privacy, maintainability
    - Can't be applied if encrypted traffic e.g. SSH
    - Or, apply at the servers themselves



محاسبه برآ اساس اطلاعات حجم میزان ترافیک عبوری روی این پورت چندتا پکت سند و رسیو شده

یا در سرویس tcp فرستادن syn , fin ack و syn ack که ترافیکی در این بستر هست و یا سرویس های signature ای

# Billing

---

- Data Collection
  - Measuring the usage data at the device level
    - Performed by accounting
- Data Aggregation & De-duplication
  - Combining multiple records into a single one
- Data Mediation
  - Converting proprietary records into a well known or standard format
- Assigning usernames to IP addresses
  - Performing a DNS lookup and getting additional accounting records from AAA servers



در بحث billing اولین کار اینکه امارهارو جمع بکنم مثلا در بردر شبکه برم ببینم کی چقدر استفاده کرده از سرویس و اکانتینگ بکنیم این اطلاعات رکورد میشه ک و بعد باهم aggregate در چند دسته مشخص و تبدیل میکنیم به یک فرمت مشخص و مثلای میگیم این یوزر اینقدر مصرف داشته و یکسری سرورهای AAA هست که این اطلاعات میره داخل سرویس های AAA و اونجا هم تبدیل به صورت حساب بشه

## Billing (cont'd)

- Calculating call (service) duration
  - In some application, real-time duration is needed
- Charging
  - Tariffs and parameters to be applied
- Invoicing
  - Translating charging information into monetary units and printing a final invoice for the customer



دوره استفاده از سرویس برآمده خیلی مهمه بعضی ها realtime هستند بعضی ها offline هستند مثلاً قبض برای بعضی ها 15 روزه یا یک ماهه یا دو ماہه میاد این دوره استفاده یک چالش جدی هست

بحث دیگه بحث charging هستش تعرفه ها رو حساب میکنیم و صورت حساب و قبض نهایی با احتساب مالیات و ... صادر میکنیم

# Billing Models

## ➤ Postpaid vs. Prepaid

- Postpaid: Off-line charging
  - Needs mechanisms for invoice payment assurance
- Prepaid: On-line charging
  - Complicated, need real time accounting & billing

## ➤ Charging criteria

- Volume based vs. Time based charging
- Best effort vs. QoS based (DiffServ) charging
- Flat fee vs. Application specific
- ...



69



مدل پرداخت خیلی مهمه ، دو مدل پرداخت داریم: **prepaid** یعنی اول پول میدی سرویس رو میخری بعد به اندازه اون سرویس استفاده میکنی

مدل **Postpaid** : یعنی من خرج میکنم بعد سر بر ج برا من قبض میاد اگر پرداخت نکنی سلب اعتبار میشه از اون سیمکارت در این روش پرداخت نیازمن و دیعه از مشتری هستیم تا مطمئن بشیم طرف میاد قبضش رو پرداخت میکنه

مدل های شما برای شارژ کردن چیست؟ **volume based** (مثلا 10 گیگ اینترنت خریدم و استفاده میکنم) و **time basee** (3 دقیقه یا 5 دقیقه یا .. با تلفن صحبت کردم)

کیفیت سرویس معمولا **best effort** یا اگر خیلی دیگه خوب باشه **diffserv** هستش  
ایا سرویس من **flat fee** هست که به صورت یکسان هست سرویس ها یا به صورت **application specific** .  
که مثلا میگه اگر از این 500 تا سرور استفاده کنید نصف بها حساب میکنم .

## Performance Management: Design Phase

- Each system is **designed** for a target level of performance
- The general approaches to guarantee QoS under high load conditions (e.g., congestion)
  - Over provisioning
    - Underutilized network resources in most cases
  - Classification
    - Traffic based, User based, ...
    - Prioritize classes to each other



وقتی میخوایم provisioning کنیم باید ببینم منابع شبکه کشش دارد و دو تا سوال باید پاسخ داده بشه ایا با اوردن این سرویس جدید نیازهاش پاسخ داده میشه و دوم اینکه نیازهای قبلی که پاسخ داده شده تغییر پیدا میکنه؟ مجموع سود و زیان ها رو حساب میکنیم ببینیم میصرفه اینکارو کنم یا نه

---

## Performance Management: Operation Phase

---

- Why PM in operation time?
- Oversimplified assumptions in design phase
  - E.g., Poisson arrival rate, M/M/1, ...
  - Not satisfied by the real workload
- Monitoring the actual performance of network
  - Alert any potential problems in network performance
    - SLA monitoring & guarantee
  - Traffic trend for future planning
    - Capacity planning

---

در بحث عملیاتی مدل  $M/M/1$  ریاضی میتوانیم بر اساس اون یک تخمینی داشته باشیم اما این مدل ها محدودند و نمیتوانند اون **workload** واقعی شبکه رو دربیارند اما بعد از اینکه سرویس رو قبول کردم باید بیام برس کنم و اون موقع **workload** واقعی شبکه دیده نمیشه باید بیام **monitoring** بزارم و پرفرمنس رو به صورت لحظه ای مانیتور میکنم مشکلات بالقوه رو قبل از اینکه بوجود بیاد پیدا میکنم (SLA monitoring&guarantee)

# Performance Management

- Performance Management involves
  - Management of **consistency and quality** of individual and overall network services
    - Monitoring performance and service levels
  - **Optimization** of network performance
    - Need to measure user/application response time
    - Tuning network for performance
  - Allow the network to evolve with the business
    - Traffic trend & capacity planning



در پرفرمنس منیجرمنت من وقتی یک سرویسی میدم به شبکه باید کلا سرویس های مختلفم در یک سری سطوح مشخصی قرار بگیرند به لحاظ سرویس دهی و سرویس گیری و این سطح سرویس باید ثابت باشه و کیفیت لازم هم داشته باشه یعنی دائم باید پرفرمنس و سطوح سرویسم رو مانیتور بکنم دومین گام این هست که آنچه که داریم رو بهتر بکنیم

یعنی اینکه respons time در شبکه رو چطور کاهش بدم برم پارامترهای شبکه رو بگیرم یکی یکی بررسی کنم برای اینکه سطح کارکرد بهتری داشته باشم

# Performance Metrics

- How to measure (define) performance?
- Performance **metrics** differ by layer and service
  - Throughput
    - At link layer: byte / sec
    - At network layer: packet / sec
    - At application layer: request (call) / sec
  - Delay + round trip response time
    - At network layer: RTT for a packet
    - At application layer: Time to response for a request
  - Quality of service metrics
    - Percentage of packets dropped
    - Percentage of dropped calls, etc.
  - Utilization
    - Link and router resource utilization



74



یا معیار چیه؟ در هرجا متفاوته مثل اگر در شبکه صحبت میکنیم در شبکه throughput یا گذردهی یک ملاک مهم هست اگر در لایه لینک باشه میشه byte/sec اگر در لایه شبکه باشه میشه call/sec و اگر در لایه اپلیکیشن باشه packet/sec

یک پارامتر دیگه ای داریم که delay یا تاخیر هست اگر در لایه شبکه باشه میشه RTT برای پکت اگر در لایه اپلیکیشن باشه reponse time برای بسته

ملاک کیفیت سرویس اینکه چقدر از بسته ها drop شده و چقدر باقی مونده و jitter و اینها چقدر هست

در حوزه utilization یا نرخ بهره وری صحبت بکنیم که چقدر منابع شبکه من utilize شده است

# Performance Management Functions

- Document the network management business objectives
- Create detailed and measurable service level objectives
  - Define performance SLAs and Metrics
    - E.g., average/peak volume of traffic, average/maximum delay, availability, ...
- Measure performance metrics
  - Method depends on the metric
  - Charts or graphs that show the success or failure these agreements over time
- When thresholds are exceed, develop documentation on the methodology used to increase network resources
- Have a periodic meeting that reviews the analysis of the baseline and trends



چه function هایی وجود داره برای بحث مدیریت شبکه : اولا ما باید تمام اهداف تجاری کسب و کار یا شبکه مون رو مشخص کنیم بعد که این اهداف مشخص شد جزئیاتش رو مشخص کنیم و بعد بگیم من چجوری میتونم این اهداف رو اندازه گیری بکنم مثلًا متوسز تاخیر یا حداکثرش چقدر به ازا هر پارامتر هم میشه براش نمودار کشید یا خیلی کارهای دیگه هم کرد و زمانی که از threshold عبور پیدا کرد بیا مثلًا فلان کار رو بکن مثلًا اگر منابع اضافه داریم وارد شبکه بشوند و یک بخش از ترافیک رو هندل بکنند

در بحث پرفورمنس منیجرمنت میان به صورت دوره ای review میکنن میان میگن مثلًا کف نیاز ها اینجاست یا چارچوب هارو تعیین میکنند روندها اینجاست یا اهمین اطلاعات رو در سیستم استخراج میکنند و اگر سیستم هوشمند باشه خود سیستم اینکارو میکنه

# Performance Management Aspects

## ➤ Proactive

- Reporting & Monitoring (performance metric history graphs)
- The value of performance metrics are gathered periodically
- The data analyzed and reported
- Capacity planning

## ➤ Reactive

- QoS assurance
- Define threshold
- Automatically take action when a **threshold** is eclipsed
  - Send an email / text message / IM
  - Sound an alarm
  - Call a pager
  - Switch to a back-up circuit
  - ...



76



در بحث پرformance منیجمنت ما دو حوزه کلی داریم : **proactive** : میام گزارش هامو و مانیتورینگمو انجام میدم و مقادیرم رو جکع میکنم به صورت دوره ای و از نتایجی که بدست میارم میتونم برای استفاده بکنم و برای قبل از اینکه به مشکل بر بخوریم هست اما در

: زمانی هست که دچار مشکل میشیم پس پارامتر های کیفیت سرویس هست و اینکه اگر **Reactive** از حد آستانه تجاوز کرد چیکار بکنیم ایمیل بده با **sms** بفرسه یا **circuit** درست کنه و بخشی از ترافیک رو از روی اون منتقل بکنه اگر میخواهیم پرformance منیجمنت داشته باشیم باید تعیین کنیم که یک سیستم **proactive** میخواهیم یا یک سیستم **reactive**

## جلسه پانزدهم

# Performance Management Issues

- 1) Effect of performance management on network performance
  - Large volume of performance monitoring data increase network traffic
    - Efficient mechanisms/protocols; e.g., IPFIX or local snapshot
    - Periodic polling
      - Polling rate?!
    - Database design
- 2) SLA management vs. Reporting
  - Performance reporting is typically used for capacity planning
  - SLA should be guaranteed
    - Performance troubleshooting



در خصوص FCAPS صحبت شد و وارد مبحث Performance شدیم.

وقتی در خصوص مدیریت کارایی (Performance) صحبت می شود یکسری مسائل و چالش ها وجود دارد.

یکی موارد آن تاثیر مدیریت کارایی بر Performance واقعی شبکه می باشد. یک مدیر شبکه باید دائماً ترافیک Backbone اش را مانیتور کند و شرایط شبکه و ازدحام و مسائل دیگر را کشف کنم. می بایست روی شبکه مسائل شبکه را دید

حتی در سازمان متوسط جهم بالای اطلاعات شبکه را داریم که می بایست آن ها را ارزیابی و کنترل کرد. همانطور که قبلاً اشاره شده در مورد مانیتورینگ شبکه ما دو حالت مانیتورینگ داریم. (به صورت Passive و Active

یا ترافیک را بعد از به وجود آمدن آنالیز می کردیم و یا به صورت اکتیو و فعالانه اطلاعات را پراپ کرده و جمع آوری می کردیم.

در حالت عادی اطلاعات مانیتورینگ پسیو به شبکه اضافه می شوند و ما به صورت اکتیو یک ...

در هنگام قرارداد با مشتری جهت سرویس دهی ما در ضمن قرار داد یک SLA یا Service Level Agreement داریم

مثلاً IPFIX به صورت سربار وارد شبکه می شود. سپس چالش های مشخصی صورت می گیرد. اول اینکه پروتکل های حوزه مانیتورینگ باید پروتکل های کارآمدی باشند، یعنی خود آنها باعث دردسر، ازدحام و بد شدن ترافیک نشوند.

دوم این ها اگر بخواهند که بکنند باید حتماً به صورت دوره ای باشند و به صورت دوره ای polling باشند (سرکشی کنند).

سوم اینکه طراحی دیتا بیس باید دید که به چه صورت خواهد بود.

چالش بعدی در خصوص SLA Management می باشد. در هنگام قرارداد با مشتری Reporting جهت سرویس دهی ما در ضمن قرارداد یک SLA یا Service Level Agreement می بینیم.

# Performance Management Issues (1)

## ➤ Data collection & Database design approaches

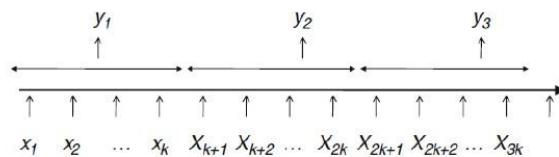
- Performance monitored data is **time-series**

## ➤ Round-robin DB

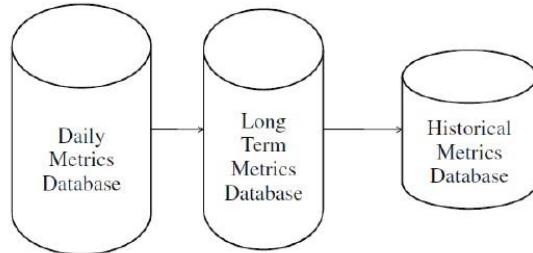
- Time based partitioning of databases

## ➤ Aggregation method

- e.g., average



## ➤ DBs based on time scales



78



78 مسایل مدیریت کارایی

رویکردهای جمع آوری داده و طراحی پایگاه داده

- داده های ناظارت بر عملکرد(سری-زمانی) هستند.

دیتابیس Round-Robin

- پارتیشن بندی بر اساس زمان پایگاه های داده

روش تجمعی

- نظریه میانگین

دیتابیس ها براساس مقیاس های زمانی

در بحث Performance ما گفتیم باید مانیتورینگ فعالانه داشته باشیم. Performance چیزی است که در لحظه می تواند جابجا شود. در traceroute تاخیرهای لحظه ای شبکه را به خوبی میبینیم. پس باید فرآیند مانیتورینگ Data Collection ما به صورت مستمر باشد. این یعنی من چالش جدید در طراحی پایگاه داده پیدا کنم. داده ای که در حوزه Performance دارم میگیرم time series هست یعنی داده های سری زمانی مثلاً اینقدر مگابیت در این ثانیه ( Mb/PS )

پس مانیتورینگ و طراحی پایگاه داده من، به صورت سری زمانی حجم سنگین ترافیک را وارد میکند. بنابراین شاید نتوان با یک پایگاه داده به یک شبکه بزرگ پاسخ دهیم و مجبور شویم یک مجموعه از پایگاه داده طراحی کنیم و بگوئیم گزارشات ثبتی به صورت Round-Robin باشد. این یعنی یکی در زمان مشخصی ثبت شود و در زمان بعدی یکی دیگر ثبت شود. (به صورت نوبتی و چرخشی)

چالش بعدی این است که بعد از گرفتن این داده ها چگونه می توان Performance را حساب کرد؟ باید ترافیک را تجمعی (Aggregate) کرد. و از خیلی از مباحث میانگین گرفت.

مثلاً در این محور روی شکل در بازه زمانی  $y_1, y_2, y_3$  هر کدام کلی ترافیک وجود دارد. و جهت صحبت در این موارد باید میانگین ها را در نظر بگیرید. (پیک ها و مینیمم ها). موارد ذکر شده نیازمند جمع آوری ترافیک و تصمیم گیری در خصوص آنهاست.

یک ترافیک پیوسته زمانی که دائماً در حال دریافت است وجود دارد و بحث Scalability یا مقیاس پذیری در مرکزداده یک چالش ایجاد میکند، پایگاه داده پیوسته ترافیک را در طول زمان دریافت میکند. باید دید دوره زمانی ما به چه صورت است؟ ( ثانیه ای؟ میلی ثانیه ای؟.... )

در مبحث مقیاس زمانی اعمال متدها هم وجود دارد. حتی در بحث ذخیره سازی اعمال مباحث گفته شد وجود دارد.

برای مثال Congestion (ویا حملات در شبکه) یک موضوع کاملاً لحظه ای است . یک موافقی هم هست مثلاً ترافیک مربوط به سرور سلف سرویس دانشگاه در بازه زمانی ظهر و شب ترافیک جمع بعد سرور خاموش میشود.

وقتی نگاه می کنیم یک ساختار سلسله مراتبی در پایگاه داده خودم دارم، بک سری متريک ها هم داریم که در ثانیه و دقیقه و ساعت مطرح می شود و یک سری هفتگی و ماهانه و سالانه صحبت می شود.

یک سری Long term و یک سری Short term می باشند. دوره های زمانی کوتاه، متوسط و بلند داریم.  
پس باید یک ساختار پایگاه داده داشته باشیم که بتوانیم به تمام این موارد پاسخ دهیم.

مخصوصاً وقتی که می خواهیم برای ظرفیت برنامه ریزی کنیم می بایست به صورت Long term بررسی کنیم.  
مثلاً در هفته های مختلف سال، یا ماه های مختلف سال، ترافیک به چه صورت رشد کرده و از مدیر درخواست منابع جهت دیتابیس کنیم و یا جهت افزایش پهنای باند شبکه و تعویض نود ها. در مواردی که به صورت لحظه ای بررسی می شود بحث تضمین SLA ها را داریم.

## Performance Management Issues (2)

- Performance Troubleshooting
  - *Detecting Performance Problems*
- Threshold; e.g.,
  - 80% of maximum acceptable utilization/delay
  - Mean + 3 \* Standard deviation
- Statistical abnormality
  - The time-series data generated by performance metric has statistical properties relatively constant under operating conditions
  - High traffic variance → Traffic fluctuation → More delay jitter
- Help desk reports
  - Problem indication by customer
  - The worst approach



مسائل مربوط به مدیریت کارایی

عیب یابی عملکرد (Performance Troubleshooting)

- تشخیص مشکلات کارائی و عملکرد

آستانه به عنوان مثال:

-  $80\% = \text{حداکثر استفاده} / \text{تاخیر قابل قبول}$

- میانگین  $3^+$  \* انحراف معیار

ناهنجری آماری(شرایط غیر نرمال)

- داده های سری زمانی تولید شده توسط متريک عملکرد

- خواص نسبتا ثابت تحت شرایط عملیاتی

- واریانس ترافیک بالا/ نوسانات ترافیک/تاخیر بیشتر جیتر

گزارش کمک

- نشان دادن مشکل توسط مشتری

- بدترین رویکرد

## Short term Performance Troubleshooting

### Performance

بپردازیم. بلاfacله که به مشکل میخوریم چالش کشف و اعلام می شود. پس اولین قدم این است که مشکل کارائی را در لحظه کشف کنیم. مثلا می توانیم تعریف کنیم اگر **Link Utilization** به درصد خاصی رسید آلام بددهد و برای ما تا چند درصد قابل قبول است. یا برای مثال **Delay** تا چه مقدار قابل قبول است و بعد از آن نیسازمند آلام می باشد. پس می بایست سطح **Threshold** تعریف کرد. و یا گفت که متوسط چقدر باشد و به اضافه سه برابر انحراف معیار برای ما قابل قبول است.

موضوع دیگر این است که دانسته های ما دانش محدودی است و بسیاری از آن مبتنی بر تجربه است که شاید ندانیم در بعضی اوقات چه شرایطی **Abnormal** می باشد و معمولا برای شرایط کنونی شبکه من مناسب نیست. **Threshold** ها را بررسی می کنیم و عیبی را مشاهده نمی کنیم اما در شبکه مشکل داریم. در نتیجه خیلی اوقات است که بر اساس آماری متوجه یک سری رفتار های **Abnormal** می شویم. مخصوصا برای موارد امنیتی ما مجبور به اینکار می شویم.

در سیستم های IDS یک سری حملات هستند که شما یک Signature یا امضا برای حمله پیدا می کنید و یک سری تحلیل آماری که بیان گر این است که نباید در شرایط کنونی به این صورت باشد.

وقتی واریانس ترافیک خیلی زیاد می شود(بالا و پائین ترافیک) یعنی ترافیک یک سری نوسان شدید دارد و نوسان های شدید ترافیکی جیتر شبکه را زیاد می کند و با افزایش جیتر ترافیک های صوتی زیاد می شوند.(مانند ویدیو کنفرانس ها) و این موضوع فقط در خصوص مسائل امنیتی نیست و در خصوص Performance هم میتواند باشد.

کاربران در شرایط کاهش کارایی با Helpdesk ها تماس میگیرند و ما نیازمند یک سیستم Reporting برای Helpdesk ها جهت گزارش گیری هستیم.

و این شرایط بدترین حالت می باشد زیرا کاربر و مشتری اینقدر درگیر آن چالش بوده که زنگ می زندو پیام میدهد و به عنوان مدیر شبکه می بایست ما قبل از کاربران متوجه این شرایط شویم و به رفع آن بپردازیم.

# Performance Management Issues (2)

- Performance Troubleshooting
  - *Correcting performance problems*
- Misconfiguration
  - Incorrect configuration cause slow down device
- System changes
  - Inconsistent configuration for software update
  - Hardware compatibility issues
- Workload growth
  - The congested resource should be upgraded (capacity planning)
- Workload surge
  - Workload increases very rapidly in a very short amount of time
  - Spare resource and traffic shaping can help



80



80

مسائل مربوط به مدیریت کارائی

عیب یابی عملکرد

- تصحیح مشکلات عمرلکرد

پیکربندی نادرست

- پیکربندی نادرست باعث کندی دستگاه می شود.

تغییرات سیستم

- پیکربندی ناسازگار برای بروز رسانی نرم افزار

- مشکلات سازگاری سخت افزاری

## رشد حجم کار

- منابع ازدحام می باشد ارتقا یابد و برنامه ریزی ظرفیت صورت گیرد

## افزایش حجم کار

- حجم کار به سرعت در مدت زمان بسیار کوتاهی افزایش می یابد.

- منابع کمکی و شکل دهی ترافیک میتواند به این مسئله کمک کند.

این اصلاح می تواند در اثر یک **Miss Configuration** رخ داده باشد یعنی در حین تنظیم یک دستگاهی اشتباہی صورت پذیرد و کانفیگ اشتباہ اعمال شود که منجر به کند شدن سرعت دستگاه و کاهش **Utilization** و ترافیک گردد..

یک سری مواردمربوط به تغییرات سیستمی می باشد. سیستم عامل ها و نرم افزارها آپدیت می شوند و سخت افزار می تواند مستعد یک سری تغییرات باشد. بعضی از مشکلات ما می توانند ناشی از آپدیت های سیستمی باشد چه به صورت نرم افزاری و چه به صورت نرم افزاری. برای مثال در سیستمی بعد از آپدیت اشتباہی رخ دهد که بعدا مشخص می گردد آپدیت به درستی کانفیگ نشده است.

بعضی دیگر از مشکلات ناشی از رشد ترافیک و رشد کاری در شبکه می باشد. مثلا یک دستگاهی **Work load** ش رشد کرده و این تجهیز ظرفیت مشخصی دارد مثلا دارای **Core** با ظرفیت یک میلیون کت در ثانیه می باشد. وقتی ظرفیت آن برای پردازش و انتقال این میزان باشد منابع درونی دستگاه دچار ازدحام شده و ممکن است به مشکل بربخورد و ازین رو می باشد برنامه ریزی ظرفیت انجام گیرد و یا دستگاه جمع آوری و یک دستگاه جدید با ظرفیت بالاتر جایگزین آن گردد و یا ترافیک در مسیر های مختلف تقسیم گردد.

گاهی اوقات رشد ترافیکی یا **Work Load** در یک بازه زمانی کوتاه به پیک میرسد و بعد از آن مجدد به سطح نرمال بر میگردد برای مثال وقتی یک سیستم کامپیوتر شخصی را روشن میکنیم بعد از بالا آمدن سیستم عامل تا چند لحظه اول ممکن است سیستم هنگ باشد و بعد از آن شروع به کار روتین خود کند.

تنها راه حل آن استفاده از **Traffic Shaper** و نگهداری ترافیک می باشد. البته می توان راهی پیدا کرد تا ترافیک را پخش کرد و یا منابع **Spare** داشته باشیم که وقتی موج خروشان می آید پاسخگو باشد.

برای مثال اول شب که مردم مصرف برق زیادی دارند فشار زیادی به شبکه های برقی می اید و در اینجا باید یک سری ظرفیت های نیروگاهی از قبل آماده داشته باشیم تا وارد مدار کنیم و موج را کنترل نمائیم.

## Performance Management Tools

- Monitoring network traffic
  - Mostly real-time, Some graphing capabilities
  - Monitor device and link status and utilization
  - E.g., *Intel LANDesk Manager, Farallon Computing Traffic Watch*
- Monitoring network protocols
  - Can capture and decode packets from the network
  - Useful for odd and intermittent network problems
  - Specialty products available
    - *Wildpackets Etherpeek, Ethereal (WireShark), Airopeek*
- Monitoring network equipments
  - Server monitor products
    - Most products include some sort of performance management capabilities
  - Switch, Bridge and Router monitor products
    - Most hardware now includes management modules that provide management capability



### ناظارت بر ترافیک شبکه

- عمدتاً در زمان واقعی و با بهره گیری از برخی از قابلیت های نمودار ناظارت بر وضعیت دستگاه ها و لینک ها و استفاده ها
- ناظارت بر پروتکل های شبکه: می توان بسته ها را از شبکه گرفت و رمزگشائی کرد. برای مشکلات عجیب و غریب و متناوب شبکه ها مفید است. این گونه محصولات تخصصی می باشند.  
ب عنوان مثال:
- ناظارت بر پروتکل های شبکه: می توان بسته ها را از شبکه گرفت و رمزگشائی کرد. برای مشکلات عجیب و غریب و متناوب شبکه ها مفید است. این گونه محصولات تخصصی می باشند.

## مانیتورینگ تجهیزات شبکه

- بیشتر محصولات مانیتورینگ سرورها دارای نوعی قابلیت عملکرد می باشند.
- محصولاتی همچون مانیتور، سوئیچ، پل ، روترا
- اکنون اکثر سخت افزار ها شامل مژول های مدیریتی هستند که قابلیت مدیریت را فراهم می کنند.

ما ابزارهای زیادی در حوزه مدیریت عملکرد داریم که می توانند شرایط مختلفی را بررسی کنند. ابزارهایی داریم که فقط مختص نظارت ترافیک شبکه هستند. ترافیک شبکه یک موضوع Real Time می باشد پس ابزارش هم باید به همین صورت باشد و دارای زمان بندی گرافیکی باشد تا در لحظه وضعیت دستگاه را به نمایش بگذارد.

برای مثال Traffic Watch ، Farallon Computing ، Google Land Desk Manager به صورت لحظه ای می باشند. مثلا واپرشارک وقتی ویندوز در مدیریت سخت عملکرد شبکه می باشد ترافیک لحظه ای را مشاهده می کند. و این همان ترافیک شبکه در سطح لینک یا همان لایه فیزیکال است که Utilization را به ما نشان می دهد.

یک سری ابزارهای مانیتورینگ پروتکل وجود دارد. در شبکه پروتکل های زیادی داریم همانند پروتکل TCP/IP که خود آن دارای پنج لایه می باشد. در واپرشارک که مشاهده می کنیم می توانیم حدود پیج لایه را ببینیم که هر لایه رو جدا نشان میدهد. خوبی ابزارهای آنالیز پروتکل های شبکه این است که به کمک این آنالیز ها می توانیم خیلی از مشکلات شبکه را متوجه شویم.

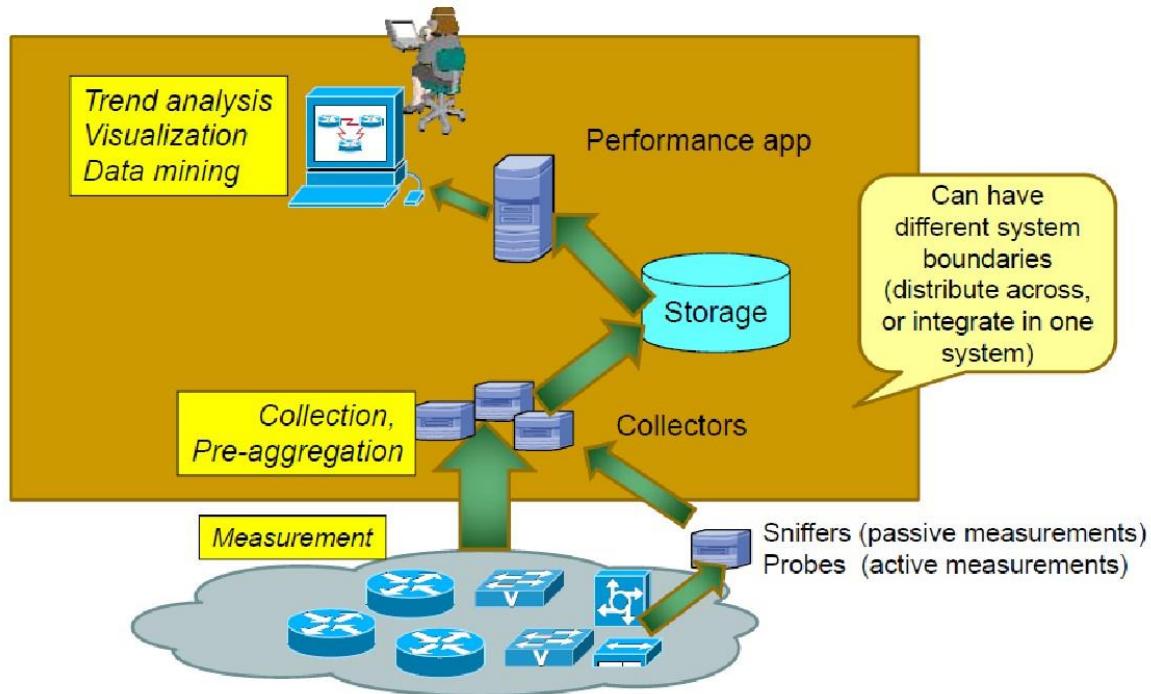
یک سری دیگر از ابزارها جهت مانیتورینگ دستگاه ها می باشند که تجهیزات شبکه مظیر سرور ها و سوئیچ ها و روترا را مانیتور می کنند.

سرورها معمولا سیستم عامل های معروفی دارند و جهت مدیریت عملکرد این سیستم عامل ها ابزار های مخصوصی وجود دارد که خیلی از آن ها ساخت شرکت تولید کننده سیستم عامل یا سخت افزار می باشد.

برای مثال شرکت ماکروسافت روی ویندوز ابزارهایی گذاشته است که دیگر نیاز نیست ابزاری بخریم. در سمت دیگر ابزارهایی مربوط به مانیتورینگ روتراها و سوئیچ ها و... (که معمولا سخت افزاری اند) وجود دارد که دارای مژول های خاص مدیریتی هستند که توانمندی خاص خود را دارند.

در ابزارهای شبکه بسیار نادر است که یک ابزار برای همه استفاده بشه و همه چیز را مانیتور کند.

# Performance Management Summary



82



82

پس ببینید من یک ابر شبکه پر از تجهیزات دارم که باید اطلاعاتشون توسط یک سری Probe یا Sniffer یا ها جمع آوری بشود. اگر Sniff باشد و اگر Probe باشد اکنون است. اطلاعات جمع آوری شده در Collector وارد می شود و در واقع ترافیک ها جمع آوری شده تجمیع می گردد و سپس ذخیره می شود.

مدیر شبکه و یا برنامه های مدیریتی اطلاعات ذخیره شده را استفاده می کنند و به صورت Visual به نمایش می گذارند و موارد Real Time را با نمودار و شکل نشان میدهند و موضوعات میانگین و یا دراز مدت را با عدد نشان میدهد.

فضای مستطیل قهوه ای Storage ، Collector و یا App Performance manager هستند. این موارد موضوعات خاصی هستند که شرایط خاص خودشون رو هم دارند و الگوهای محدودیت های خاصی نیز دارا هستند که ممکن است در سیستم های متفاوتی قرار گیرد.

# Outline

---

- Fault management
- Configuration management
- Accounting management
- Performance management
- **Security management**
- Conclusion



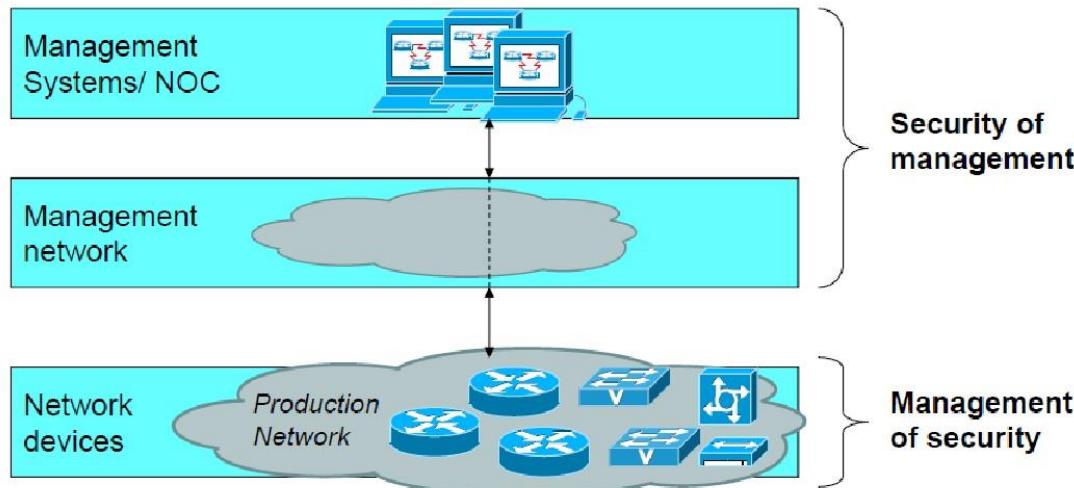
83



83

# Security & Management

- Security of Management
- Management of security



84



و 84

آخرین بحثی که از FCAPS داریم مبحث Security می باشد.

وقتی بحث مدیریت را مطرح می کنیم باید در دو حوزه زیر بررسی کنیم:

Management of Security -  
Security of management -

مدیریت امنیت و امنیتی مدیریت دو موضوع مجزا هستند که هر کدام حوزه خودشان را دارند. وقتی در مورد Element ها یا عناصر شبکه بحث میکنیم می شود مدیریت امنیت، برای مثال فایروال، آنتی ویروس، IDS و ... حوزه های مدیریت امنیت می باشد.

امنیت مدیریت یعنی قسمت های بالایی شکل یعنی یک سری NOC داریم در واقع یک سری تجهیزات مدیریت شبکه داریم و اون ها رو باید امن نگه داریم.

وقتی از FCAPS صحبت میکنیم رابطه مدیریت و امنیت دو سوال را بوجود می آورند:

- آیا میخواهیم مدیریت رو امن کنیم؟
- آیا امنیت را می خواهیم مدیریت کنیم؟

و به عنوان یک مدیر باید هر دو را انجام دهیم و به هر دو بعد قضیه نگاه کنیم.

## Security of Management

- Security of management deals with ensuring that management operations themselves are secured
- Major domains to secure
  - Security of NOC
    - The NMS system must be secured
  - Security of management network
    - The communication for management must be secured
  - Security of management plane of devices
    - The network equipment must be secured



امنیت مدیریت به این معنی است که باید فرآیند مدیریت من امن باشد. یعنی NMS یا NOC امن باشد و شبکه تلکامی که برای مدیریت درست شده است نیز امن باشد. همچنین برنامه های مدیریتی من در دستگاه های مختلف نیز امن باشد که همه اینها می توانند خودشان ابزاری برای نفوذ و ضربه باشند.

برای مثال SNMP ورژن 1 اصلاً امن نبود و حتی در ورژن دوم چالش های زیادی مطرح بود که اصل دستگاه امن نبود و اگر یک نفر از اعضای ارتباطی هک میشد ترافیک ارتباطی در شبکه شنود می شد و ورژن

سوم آمد تا این معایب برطرف شود. در واقع ورژن سوم احراز هویت داشت جامع بود و محترمانگی را رعایت میکرد

## Security of NOC

---

- Firewall
  - To protect NOC from external attacks
- IDS
  - To detect intrusions
- OS update/patch
  - To fix vulnerabilities
- Antivirus/Anti Spam
  - To prevent viruses, Trojans, malwares, ...
- Single-Sign-On
  - To manage password
- Physical security
  - To secure physical access to NOC



وقتی برای امنیت NOC صحبت میکنیم باید حتما در پشت فایروال باشیم زیرا حملات خارج از شبکه بسیار زیادتر اتفاق می افتد

NOC حتما باید دارای IDS باشد و سیستم عامل ها و تجهیزات آن باید حتما دارای آخرین پک های امنیتی باشند. حتما باید دارای Anti Virus و Anti Spam باشند و دارای سیستم امنیتی جهت تشخیص ورود باشد معمولا استفاده از چند روش چند مرحله ای جهت ورود استفاده می شود.

در NOC Physical Security حتما باید رعایت شود و این مسئله خیلی مهم است. باید تردد محدود باشد و افراد احراز شده فقط بتوانند وارد شوند.

Physical Access Noc ها در خیلی خطر ناک هستند و باید این موضوع جدی برخورد شود.

تجربه نشان می دهد بسیاری از ضربات سیستم های امنیتی را نیروی انسانی وارد می کند. در امنیت اطلاعات یک کره می کشند و نصف این کره را ابزار های امنیتی در لایه های مختلف قرار می دهند و نصف دیگه رو نیروی انسانی آن در لایه های مختلف قرار میدهند. یعنی همان قدری که برای تجهیزاتی نظیر فایروال هزینه می شود باید به نیروی انسانی هم توجه کرد و هزینه نمود.

## Security of Management Network

- Out-of-band management
  - Physically separated management network
  - Dedicated VPN for network management
- Integrity and Confidentiality mechanism for network management
  - SNMPv3, HTTPS, SSH, ...
- Firewall and IDS for the management network



اگر سیستم مدیریت شبکه خیلی مهم است یک سیستم Out-of-band management بگذارید . یعنی به صورت منطقی یک vpn بزنید . در کل سیستم ترافیک سیستم مدیریت شبکه را از بقیه ترافیک های شبکه جدا کنید ، ipsec بزنید تا کل ترافیک را رمز کند .

چه شبکه فیزیکی کاملا مجزا و چه شبکه منطقی جدا . بحث های احراز هویت ، جامعیت و رمزگاری را باید نگاه کنید . اون جایی که می گیم SNMP ورژن 3 باید استفاده کنید . اون جایی که میگیم HTTPS استفاده کنید . فایروال و IDS حتما باید روی شبکه استفاده کنیم . این ها همه مباحثی است که در بحث شبکه مدیریتی برای ما جدی است و باید استفاده شود .

## Security of Equipments Management Plane

- Enable password
- Change default passwords
  - SNMP default communities
- Disabled insecure services
  - Telnet
- Limit management traffic
  - Limit the volume of network management traffic
    - Processing of management traffic is CPU intensive
  - Limit the source IP and interface of management traffic
- Enable access control and logging



در مورد پلن های مدیریتی در تجهیزات شبکه وقتی می خواهیم صحبت کنیم ، اولین چیز این است که پسورد گذاشته شود و دیفالت پسورد ها عوض شود . وقتی مدیر شبکه میره اولین کاری باید انجام شود این هست که

تمام پسورد های سیستم های شبکه عوض بشد. جریان اخیری که برای پمپ بنزین ها اتفاق افتاد این بود که شخصی در سیستم بود؛ گذاشت رفت کانادا، از اونجا اطلاعات رو داد ترکوندن.

بک آپ باید داشته باشید و به روز باشد. پسورد ها را باید حتما به صورت دوره ای عوض کنید مثلا هر سه ماه. یک نفر که از سیستم رفت بلا فاصله اصلاح پسورد داشته باشید. ترافیک های مدیریتی را حد امکان محدود کنید چه به لحاظ دامنه انتشار و چه به لحاظ حجم شبکه. اون هایی که تولید می کنند و اون هایی اینترفیس های مدیریتی دارند محدود کنید.

خیلی از حملاتی که در شبکه داریم از مسیر پروتکل های کاملاً معتبر است، حمله DOS یا DDOS عجیب نیستن. با دستور ping شما می توانید DDOS کنید.

پس ترافیک های مدیریت شبکه را هم باید محدود کنید (کی تولید می کنند کی مصرف می کنند کجا به کجا میره، دامنه ای که هستن)

چون خیلی راحت از حوزه ترافیک های مدیریت شبکه میشه به دستگاه ها ضربه زد. در تجهیزات کنترل دسترسی خیلی مهمه و باید log های سیستمی را فعال کنید. برای تجهیزات هر اتفاقی می افتد log شود. یکی از پروتکل های مدیریت شبکه است و اکثر اوقات ما دنبال تحلیل این log ها نمی رویم

# Security Management

- Security management is concept that deals with protection of **data in a network system** against unauthorized access, disclosure, modification, or destruction and **protection of the network system itself (including NOC & management network)** against unauthorized use, modification, or denial of service
- Includes
  - Security policies
  - Implementation of security mechanisms
  - Monitoring, Action & Reporting security event
- We don't discuss about security techniques, e.g., public and private key encryption, confidentiality, integrity, Firewall, IDS, IPS, Honeypot, ...



89



89

حالا میریم سراغ مدیریت امنیت

سیستمی که انتقال دیتا بر روی شبکه من را امن نگه می دارد ، در برابر دسترسی های ناخواسته ، در برابر دسترسی های احراز هویت نشده ، در برابر افشاری اطلاعات ، در برابر اصلاح اطلاعات و در برابر خراب شدن و نابودی اطلاعات

همه چیز در شبکه شامل این ها می شود . مِن جمله خود تجهیزات مدیریت شبکه و NOC . مدیریت امنیت تنها فایروال ، آنتی ویروس ، IDS و هانی پات نیست . این ها بخشی از مدیریت امنیت هستند .

مدیریت امنیت یعنی تعریف :

Security policies -1 یعنی سیاست های امنیتی سازمان را تعریف کنید

سیاست های امنیتی را تبدیل به یک سری قاعده Implementation of security mechanisms -2

و قانون کنم تا قابلیت پیاده سازی در دستگاه های شبکه من را داشته باشد

action نظارت کنم ، اگر اتفاقی افتاد Monitoring, Action & Reporting security event -3

بدم و report تولید کنم

جمله آخر میگه ما در مورد تکنیک های امنیتی مثل public and private key encryption, confidentiality, integrity, Firewall, IDS, IPS, Honeypot نمی خواهیم صحبت کنیم . می خواهیم کلیت را بحث کنیم .

## Security Management Functions (TMN)

### ➤ Security administration

- Planning and administering security policy and managing security related information

### ➤ Prevention

- Security mechanism to prevent intruders

### ➤ Detection

- Detect intrusion

### ➤ Containment and recovery

- Isolate the intruded system and repair it



مدیریت امنیتی (Security administration)	-
برنامه ریزی و مدیریت خط مشی امنیتی و مدیریت اطلاعات مربوط به امنیت	
Prevention	-
مکانیزم امنیتی برای جلوگیری از مزاحمان	
Detection	-
تشخیص نفوذ	
مهار و بازیابی (Containment and recovery)	-
سیستم نفوذی را ایزوله کنیم	

## Security Policies

---

- Overall security guide line and decision in network
- Security policies must be comprehensive
  - Consider all domains in the network
    - Carrier network security (control plane)
    - Service security (data plane)
    - NOC & mgmt network security
- Security policies must provide trade-off between **security** and usability
  - E.g., if security police force at least 20 characters for password → many simple passwords, e.g., 11111111111111111111



اول باید در سازمانم security policy تعریف کنم و guid line یا موارد راهنمای خطا و تصمیم گیری را تعریف کنم . برای اون ها هزینه کنم تبدیل به قاعده و قانون کنم و به جواب برسم .

وقتی policy تعریف می کنم باید بگم اینقدر ارزش و هزینه داره برای من . شما برای تعریف سیاست های امنیتی ریسک منیجر می کنی میگی این ریسک ها وجود داره و اینقدر هزینه می تراشه و اگر برطرف کنم اینقدر باید خرج کنم .

یک جاهایی هم بی معنی است . میگه من میخام امنیت ایجاد کنم ، از همه میخوام طول پسورد شون حداقل 20 کاراکتر باشه . من میام 20 تا کاراکتر رو یک می زنم . ولی بهتره 8 تا بزارید و مجبورشون کنید از اعداد حروف کوچک و بزرگ هم استفاده بشه . همین کافیه

## Prevention

---

- Needs to be covered by security policies
- In service provider networks
  - Attack NOC (to access control on whole network)
  - Attack Network (to disturb the service, to access customer data)
- Prevention mechanism
  - NOC: Firewalls (host & network), SW patches, ...
  - Network: Router hardening, DDoS mitigation, ...



در بحث prevention یا اجتناب  
باید تحت پوشش سیاست های امنیتی قرار گیرد .  
در شبکه های ارائه دهنده خدمات

- حمله به NOC (برای دسترسی به کنترل در کل شبکه)
- حمله به شبکه (برای ایجاد اختلال در سرویس، دسترسی به داده های مشتری)

مکانیزم های اجتنابی

برای (Firewalls (host & network), SW patches ) NOC اپدیت کردن نرم افزارها و فایروال  
ها

(Router hardening, DDoS mitigation) برای شبکه

## Detection & Response

---

- Detection mechanism: IDS, Log analysis, misbehaviors
- Repair & Fix
  - Isolate affected systems & restore service
    - Fault management system can help
  - Recover the affected systems
    - Configuration management system can help
- Report & Document



سیستم هایی مثل IDS و سیستم های تحت log ها جزو الزامات هستند و باید به این ها برسیم. اگر مشکلی وجود دارد این سیستم ها را فیکس کنیم . چه به صورت جداگانه اگر سیستمی تحت تاثیر قرار گرفته و باید restore کنیم برگردانیم و چه خطأ و خرابی داشته باشد ، اون ها رو دست کنیم یک چیز خیلی مهم این هست که چیزهایی که وجود داره حتما باید report بشه .

## AAA (Authentication)

- Authentication is the act of establishing or confirming someone as authentic, that is, that claims made by or about the thing are true
- Authentication is accomplished via the presentation of an identity and its corresponding credentials.
- Examples of types of credentials are passwords, digital certificates, and phone numbers (calling/called).



94



94

AAA یکی از بحث های امنیتی خیلی جدی ما است. هر کی می خواهد بیاد احراز بشه با هر روشی .  
در مورد A اول (Authentication)

احراز هویت عبارت است از اثبات یا تأیید اصالت شخصی، به این معنا که ادعاهای مطرح شده در مورد آن چیز درست است. نمونه هایی از انواع اعتبارنامه ها عبارتند از گذروازه، گواهی های دیجیتال و شماره تلفن. در مناطقی که نیاز به امنیت دارد مثل NOC حتما باید با دو روش احراز هویت کنید .

# AAA (Authorization)

- Authorization is a process to **protect resources** to be used by consumers that have been granted authority to use them
  - aka, access control
- Authorization (deciding whether to grant access) is a separate concept to authentication (verifying identity), and usually dependent on it
- Authorization may be based on restrictions
  - time-of-day restrictions
  - physical location restrictions
  - **restrictions against multiple logins by the same user**



95



95

در مورد A دوم (Authorization) :

من احراز هویت شدم حالا سیستم باید بر اساس جایگاهم در شبکه دسترسی به منابع را تضمین کند.

محدودیت در دسترسی باید برای همه اعمال شود مانند محدودیت در بازه های زمانی در طول شبکه روز

محدودیت در دسترسی بر اساس لوکیشن فیزیکی

محدودیت در تعداد دفعات لاین ناموفق

## AAA (Accounting)

---

- Accounting refers to the **tracking** of the consumption of network resources by users
- Typical information that is gathered in accounting may be:
  - The identity of the user
  - The nature of the service delivered
  - When the service began, and when it ended
- In security domain
  - What does the client do



96



96

در مورد A سوم (Accounting)

هر کسی از منابع شبکه من داره استفاده می کنه باید TRAC ش کنم نگاه کنم چقدر از منابع رو استفاده می کنه .

# AAA Protocols

---

## ➤ RADIUS

- Remote Authentication Dial In User Service
  - Authenticated dial-up and VPN customers

## ➤ TACACS

- Terminal Access Controller Access Control System
- Different protocols and authentication methods
  - TACACS+ is the version by Cisco

## ➤ Diameter

---



97



97

چگونه پروتکل AAA را داشته باشیم

## RADIUS -

برای کاربران VPN از راه دور بوده که از راه دور کانکت میشدن از این استفاده می کردیم . یک شماره تماس می گیری VPN میسازی بعد رادیوس شما را احراز هویت می کند . برای سیستم های قدیمی بوده که کاربران dial-up وصل میشدن

## TACACS -

پروتکلی که بحث کنترل دسترسی سیستم را مطرح می کند . احراز هویت کنید و بگید این سطح دسترسی تون

## Diameter -

# SOC (Security Operation Center)

- Security has become an important issue in networks
- SOC is the center to deal with security issues on organization level and technical level
  - Performs the “FCAP” for security
    - As FM: Detect security problems, security event and alarm processing
    - As CM: Run the security mechanisms in the network
    - As AM: Do auditing, authentication, authorization, accounting
    - As PM: Monitor the status of security mechanism



98



98

برای امنیت باید مرکزی به نام **SOC** داشته باشیم ( مرکز عملیات امنیتی )  
به چالش های امنیتی کل سازمان به صورت تکنیکال می پردازد ( در حوزه **FCAP** )  
**F:** کشف مشکلات امنیتی  
**C:** مکانیزم های امنیتی را اجرایی کنیم  
**A:** بحث های احراز هویت و ...  
**P:** مانیتورینگ وضعیت امنیتی

# Outline

---

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management
- Conclusion



99



100 , 99

# Summary

---

## ➤ NOC

- Configuration management → service provisioning
- Fault & Performance management → service assurance
- Accounting management → Billing

## ➤ SOC

- Security of management
  - Management of security (FCAP for security)
- 



100



اگر می خواهیم یک مدیریت شبکه موفق داشته باشیم حتما باید دو مورد NOC و SOC را داشته باشیم .

پس ما در حوزه امنیت برای FCAP باید این دو تا مرکز را در سازمان مون ایجاد کنیم .

خدایا چنان کن سر انجام کار تو خوشنود باشی و ما رستگار.