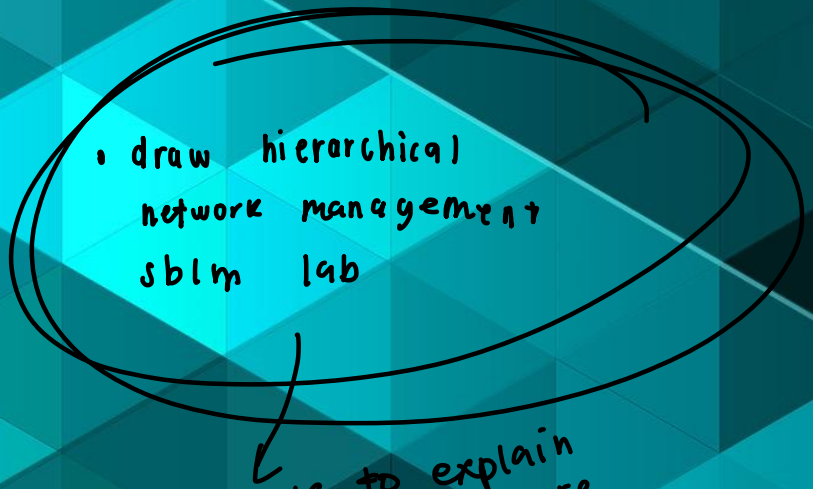
BCN 3023
NETWORK MANAGEMENT



CHAPTER 3
Network Management Reference Model

focus shared & dedicated

Dr. Suraya Abu Bakar
Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang
surayaab@ump.edu.my

NM Reference Model (1)

- It can be used for guidance and helps
  - To check a management system or operations support infrastructure for completeness (most important aspect)
  - Categorize and group different functions
  - To identify scenarios and use cases that need to be collected and to recognize interdependencies and interfaces between different tasks

NM Reference Model (2)

dedicated

- **FCAPS** – Fault, Configuration, Account, Performance, Security

shared

- **OAM&P** – Operation, Administration, Maintenance and Provision
- **TOM** (Telecom Operation Maps) – FAB :Fulfillment – Assurance - Billing

masih wujud

surayaab@ump.edu.my

FCAPS

- **FCAPS** is part of TMN model
  - **F** : Fault management
  - **C** : Configuration management
  - **A** : Accounting management
  - **P** : Performance management
  - **S** : Security management

surayaab@ump.edu.my

(1) Fault Management

Hanya cari masalah
Detect error/issues

+ AI (indirectly assist)

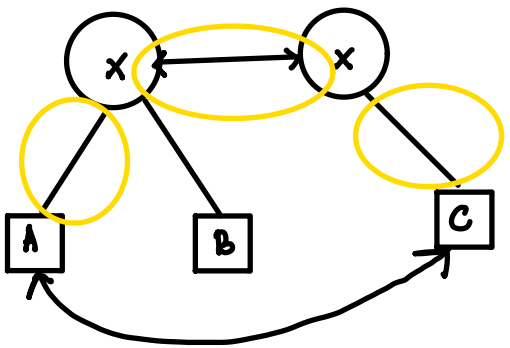
- **Deal with faults that occur** in the network
  - Equipment or software failure
  - Communication services fails to work properly
- Functionality (not limited to)
  - Network monitoring + alarm management + advanced alarm processing function
  - Fault diagnostic/ root cause analysis/ troubleshooting
  - Maintaining historical alarm logs
  - Trouble ticketing
  - Proactive fault management

main point

① Detect error /issues

i) connection
- cable type
- port cable
- ip address

ii) Devices
- default gateway
- pre configuration



② · network security

i) instrution detection
- . bad elimination
- . block mac address intruder

footprint
fingerprint

· shift + delete

③ Reactive vs Proactive

Reactive	Proactive
→ Aft prob. occur	→ Detect, prevent & avoid prob. occur

Fault Management – Network Monitoring

- Allow a network provider organization:
  - To see whether the network is operating as expected
  - To keep track of its current state
  - To visualize the current state
- The most important aspect of network monitoring is alarm management
- Alarm is an unsolicited messages from the network indicate that some unexpected event has occurred
  - Link down
  - Intrusion detected

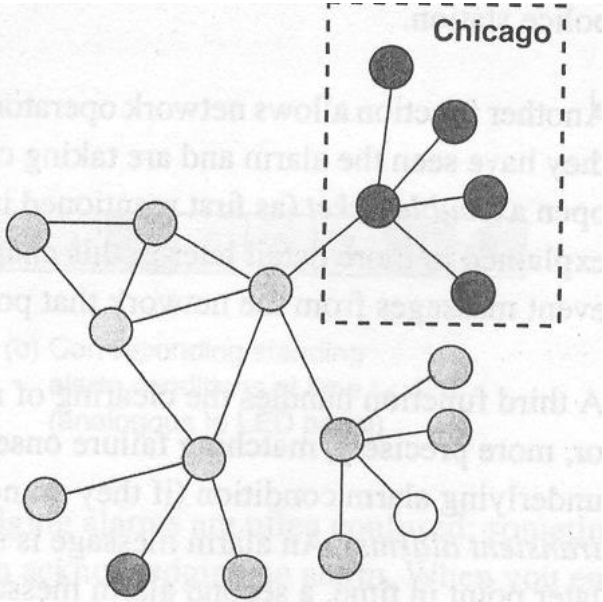
Fault Management – Basic Alarm Management Function

- Alarm management with basic function Ex.
  - Collecting alarms
  - maintaining accurate and current lists of alarms (historical alarm data)
  - Visualizing alarms and network state
- The most important task consists of collecting alarms and making sure that nothing important is missed

Fault Management – Basic Alarm Management Function

Node	Sev	Time	Event	Info
ruby	cr	16:00:42	sysdn	...
ibee	cr	16:00:42	sysdn	...
M3660-sjs	mn	16:00:33	qostc	...
M3660-sjn	mn	16:00:25	l0exc	...
Pep-7600	mj	16:00:20	dropn	...
lxsouth	cr	16:00:05	sysdn	...
blubber	cr	16:00:05	sysdn	...
Hlee-7569	cr	16:00:04	pwrfl	...
snorkel88954	cr	15:59:58	sysdn	...

(a)



(b)

Figure 1: Visualizing Alarm (a) Table List (b) Topology Map

Fault Management – Basic Alarm Management Function

- Historical alarm data can be useful
  - To resolve future problems faster by recognizing patterns and recalling their past resolution
  - To establish trends, to see how alarm rates and types of alarms reported have evolved over time

Fault Management – Proactive Fault Management

- Most fault management is reactive
  - Deal with faults after they have occurred
- Proactive fault management
  - Taking a step to avoid failure conditions before they occur
  - Test network to detect deterioration in the quality of service
  - Alarm analysis that recognizes pattern of alarms caused by minor faults that point to bigger problems

Fault Management – Trouble Ticket

- The trouble ticket system helps keep track of which trouble tickets are still outstanding
- Trouble tickets are assigned to operator who are responsible for resolving the trouble ticket
- Not every alarm results in trouble ticket, only when alarm conditions having impact to deliver services or need human intervention

(2) Configuration Management

- It includes the initial configuration of a device to bring it up as well as ongoing configuration changes
- Configuration management functions:
  - Configuring Managed Resources
  - Auditing the network and discovery what's in it
  - Synchronization management information in the network
  - Backing up network configuration and restoring
  - Managing software images running on network equipment

Configuration management

① auditing

→ update inventory info

Duration : Laptop → 3 y
Desktop → 5 y – 10 y

include → location of desktop
i) IP address
ii) mac address

② Backup & Restoring

→ Restore the previous configuration to real devices

→ Backup configuration
- every 5 → 2 years

→ Backup info need to store 5-7 years.

Configuration Management – Auditing and Discovery

- Auditing - To find out what actually has been configured – read and check
- Reason to do (auto) Discovery
  - Inventory records might not be accurate
  - Changes might not always be recorded
  - More efficient than to enter the information into management app.
  - etc

Configuration Management – Backup and Restore

- In case of some catastrophic event, it helps network operators brings the network back to operation in a short period of time
- For example
  - Save in a file
  - Setup a TFTp server

(3) Accounting Management

- It is at the core of the economics of providing communication services
- Accounting management needs to be highly robust, highest availability and reliability standard apply
- Account management is often associated simply with billing

surayaab@ump.edu.my

Accounting Management

- Account management can serve as an additional feature of the service itself
  - Billing information online

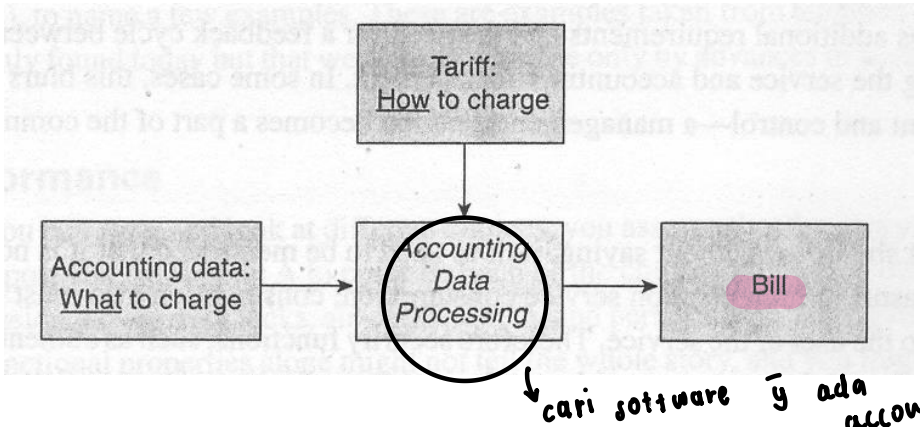


Figure : Accounting vs Billing

(4) Performance Management – Performance metrics

- Throughput – units of communication per unit of time
  - Network layer – packets/sec
  - Application layer – requests/sec
- Delay – unit of time
  - Network layer – time that packet take to reach the destination
- Quality – might different
  - Network layer – percentage of packet dropped
  - Application layer – percentage of request that could not be serviced

① Throughput

② Delay

③ Quality of service

Performance Management – Monitoring and Tuning

- At basic level, to retrieve a snapshot of the current performance
- For a more sophisticated analysis, to observe over time
  - Plot a histogram of some performance values with a new sample taken every 5 minutes

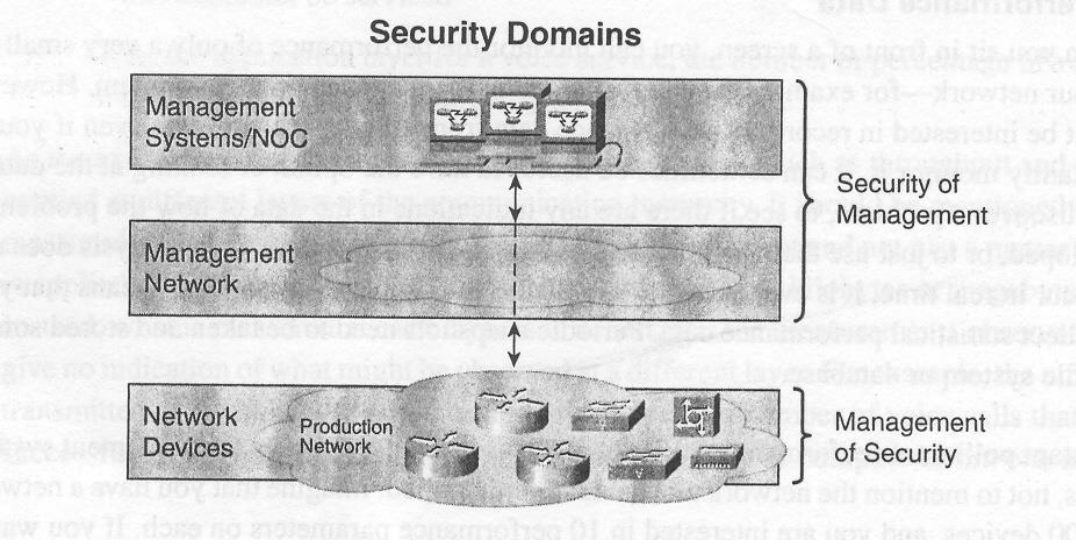
Performance Management – Collecting Data

- Polling – a manager polls to agents
  - Not scale
- Intelligent agent – agents can be set up to do data collection
- Use protocol supported
  - Netflow or IPFIX

(5) Security Management

Security of Management

Management of security



Security Management (1)
-Security of management

- Security of management deals with ensuring that management operations themselves are secured
- Tasks to defend against threat:
  - Assign access privileges
  - Require secure passwords
  - Passwords need to be changed at regular interval
  - Establish audit trail
  - Set up proper facilities for backup and restore

Security Management (1)
-Management of Security

- Common security threat – hacker attack, denial of service (DoS), malware, spam
- Components of security management
  - Intrusion detection system (IDS)
  - Applying policy to limit or allow to only gradually increase amount of traffic
  - Capability to blacklist ports and network addresses at which suspicious traffic patterns
  - Honey pots to gather information about security vulnerability

OAM&P (1)

- Operation, Administration, Maintenance and Provisioning
- Operation – day-to-day running of the network
  - Coordinating activities among administration, maintenance and provisioning
  - Monitoring the network to ensure it runs properly

OAM&P (2)

- Administration – cover the support functions that are required to manage the network and do not involve performing change
  - Designing the network
  - Tracking network usage
  - Assigning addresses
  - Keeping track of network inventory

FLAPS —— DEDICATED

OAMP —— SHARED

OAM&P (3)

- Maintenance – include functionalities ensuring that the network and services operate as they are supposed to
  - Diagnosing, troubleshooting, repairing
- Provisioning – concern with proper setting of configuration parameters on the network

TOM (1)

- **Telecommunication Operation Map**

. focus on building system → Billing → postpaid

- 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

TOM (2)

- Assurance – includes all activities ensuring that a service run 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

related, if at all.

Table 5-1 *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	—	—	—

Table 5-2 *Relationship Between FCAPS and FAB*

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

TO BE CONTINUE...