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

Outline

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management
- Conclusion

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

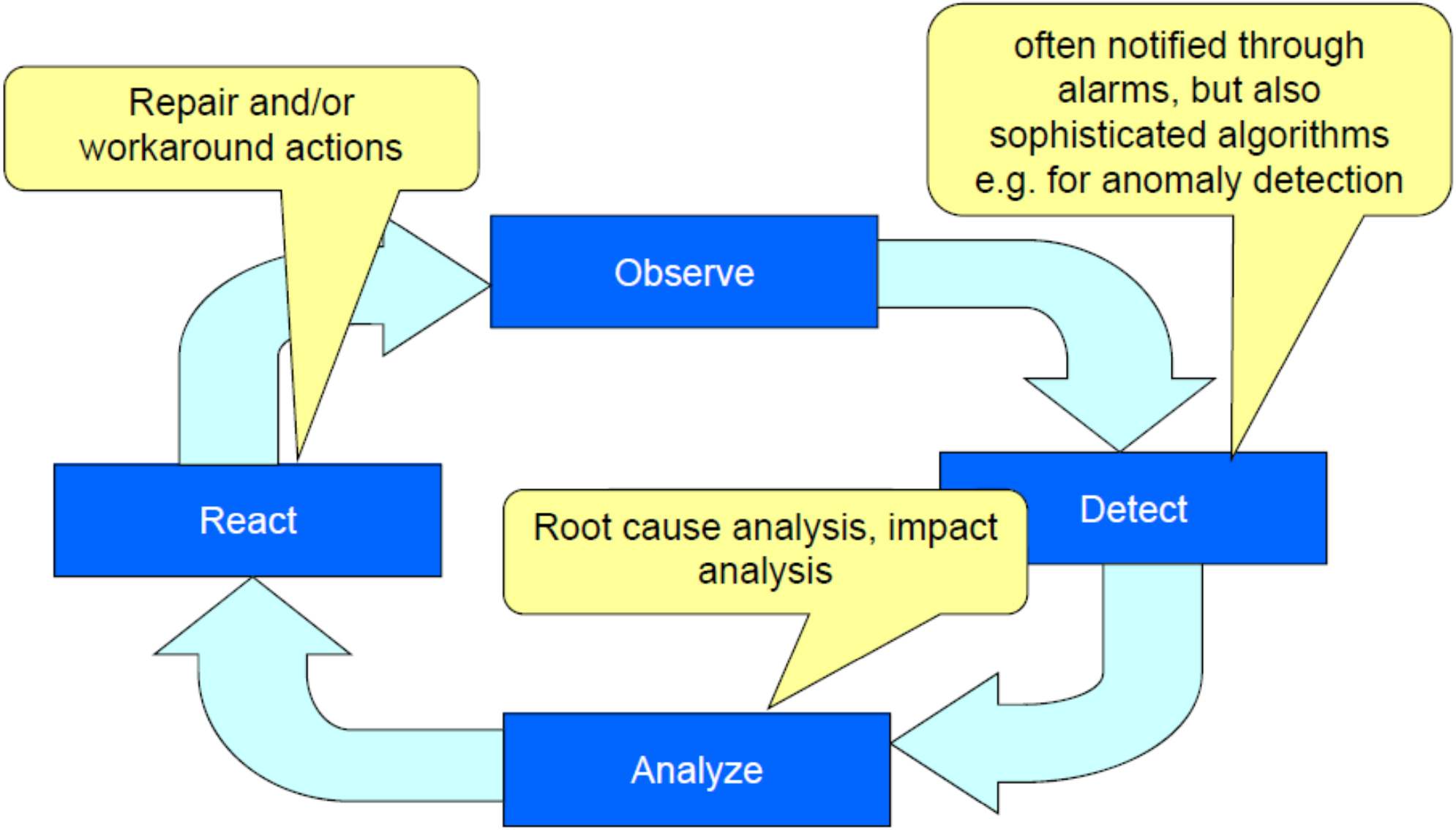
Fault Management

- 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

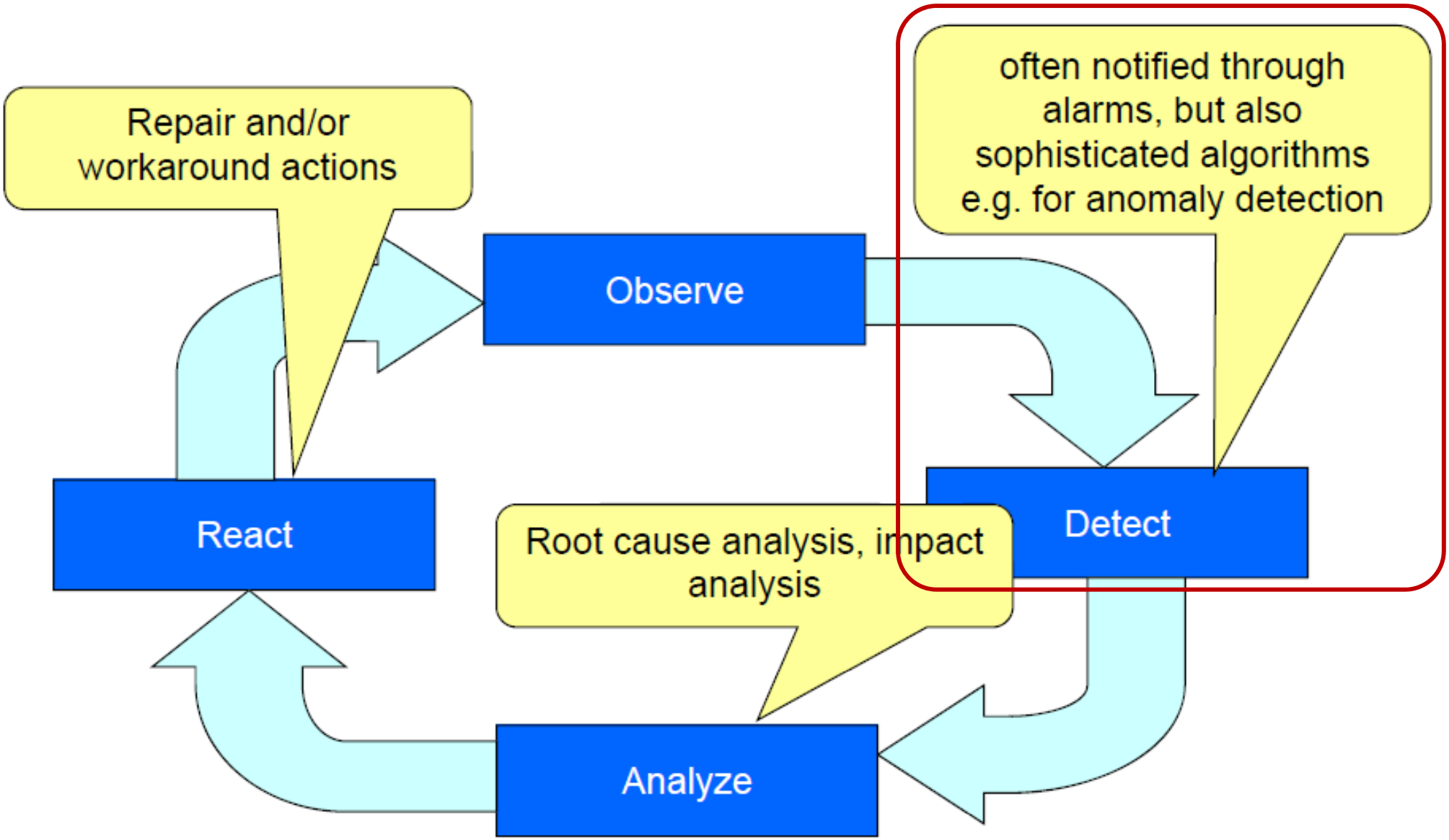
Fault Management Functionalities

- Network monitoring
  - Basic alarm management
    - Advanced alarm processing functions
- Fault diagnosis
  - Root cause analysis
  - Troubleshooting
- Trouble ticketing
- Proactive fault management

Fault Management Steps



Fault Management: Monitoring & Detection



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?

Alarms (cont'd)

- Alarms are associated with specific information
- E.g. X.733: Alarm reporting function

  - Affected system
  - Time of occurrence
  - Correlated alarms

  } part of the additional information transmitted as part of the alarm

  - Severity
  - Probable cause
  - Recommended repair action
  - Additional information

  } part of the alarm definition

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

Fault Management: Alarm Management

- Basic functions
  - Collect alarm information from the network
  - Visualize alarm information
- Advanced alarm preprocessing
  - Filtering
    - Subscription
    - Deduplication
  - Correlation
  - Augmentation

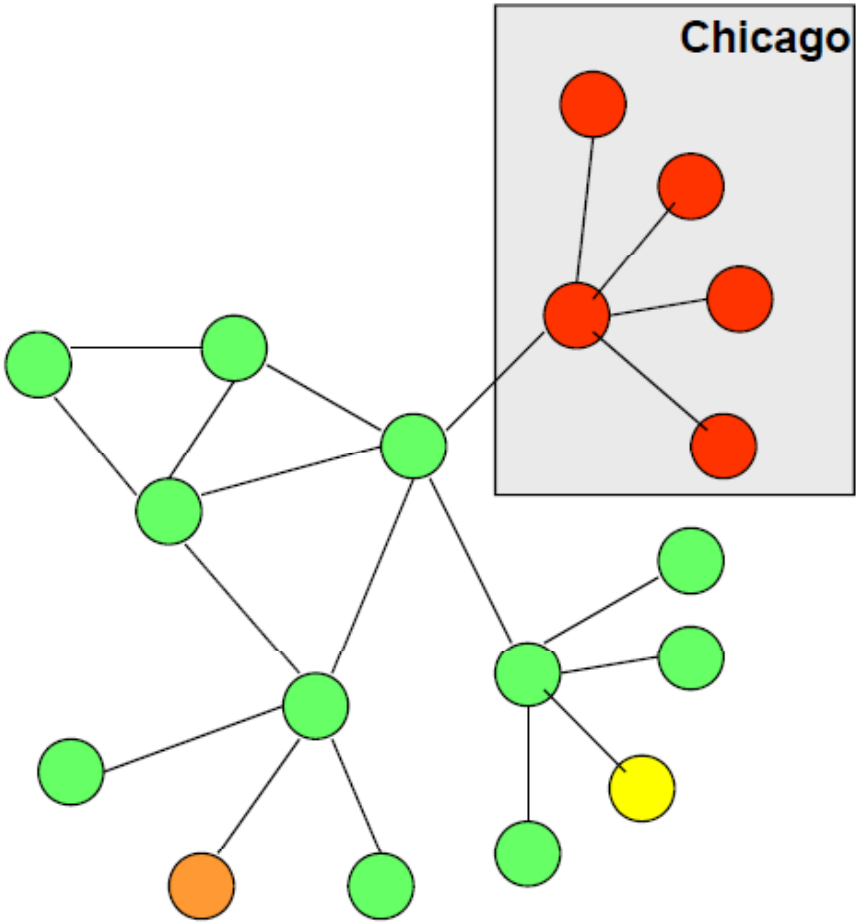
Alarm (event) Collection

- 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

(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	l0exc	....
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	...

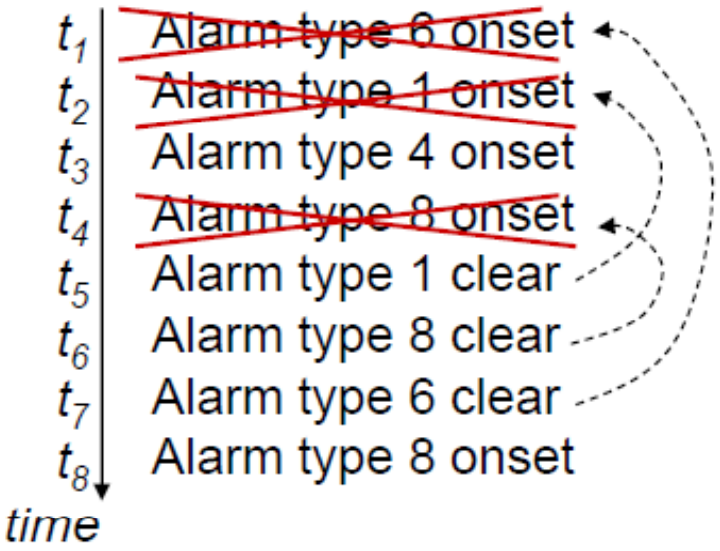
List-based:
current alarm conditions



Topology-based:
current alarm status

Alarm Visualization (cont'd)

- Distinguish list of alarms from list of currently active alarms
- Current alarm state requires correlating alarm onsets with alarm clears



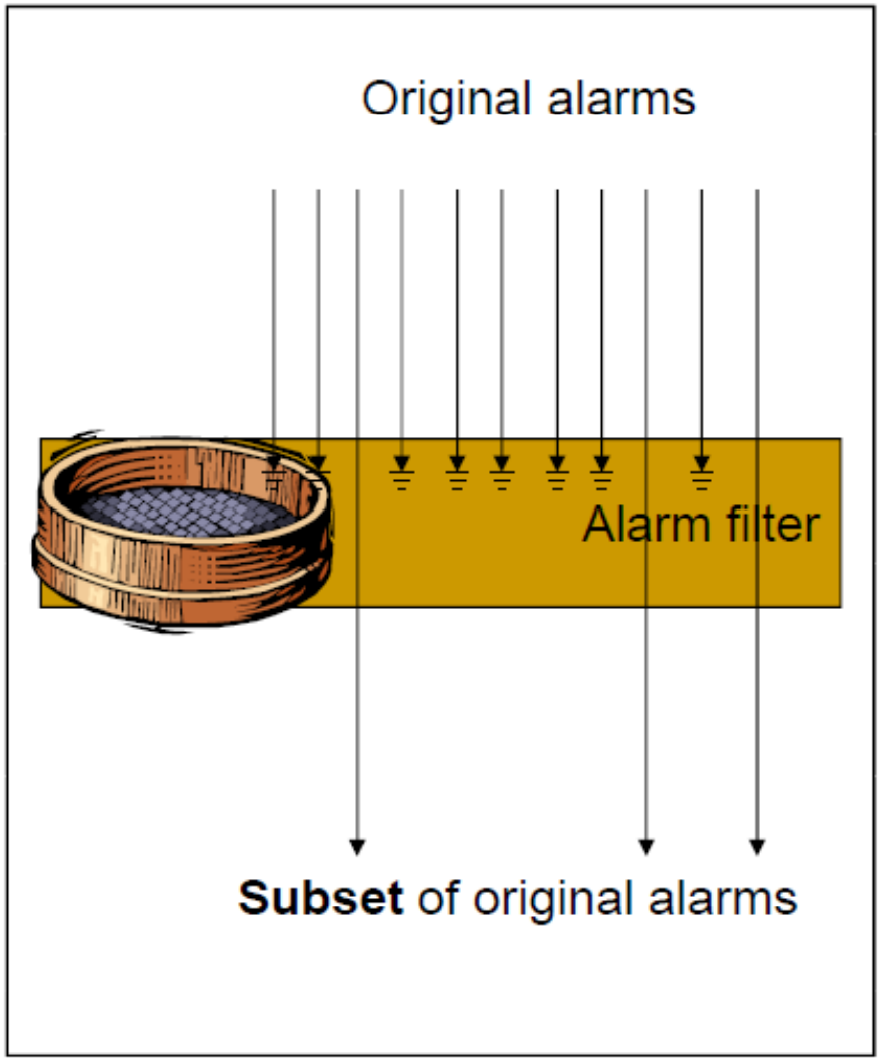
(a) Emission of alarms over time

(b) Corresponding standing alarm conditions (analogous to LED panel)

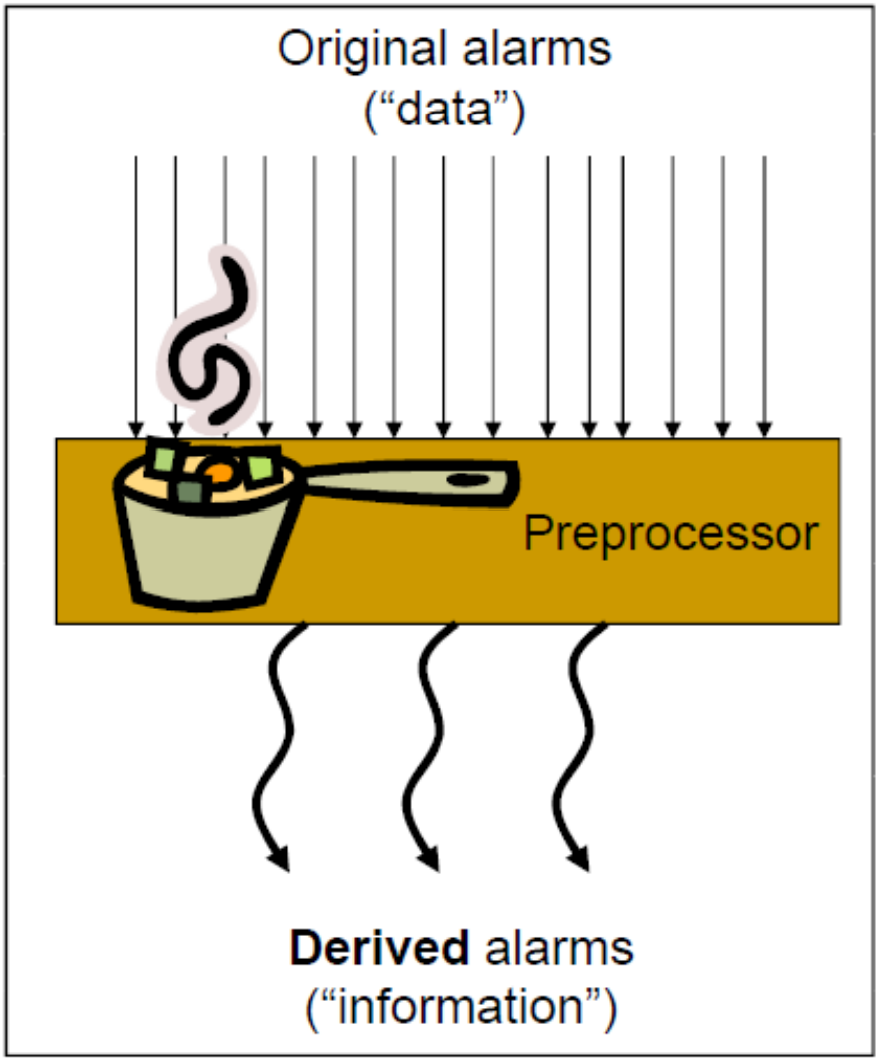
Alarm Processing

- 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)

Alarm Filtering vs. Preprocessing



(a) Alarm filtering



(b) Alarm preprocessing

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

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
- Closely tied to root cause analysis
  - Alarms are correlated in root cause analysis

Alarm (+ Event) Correlation

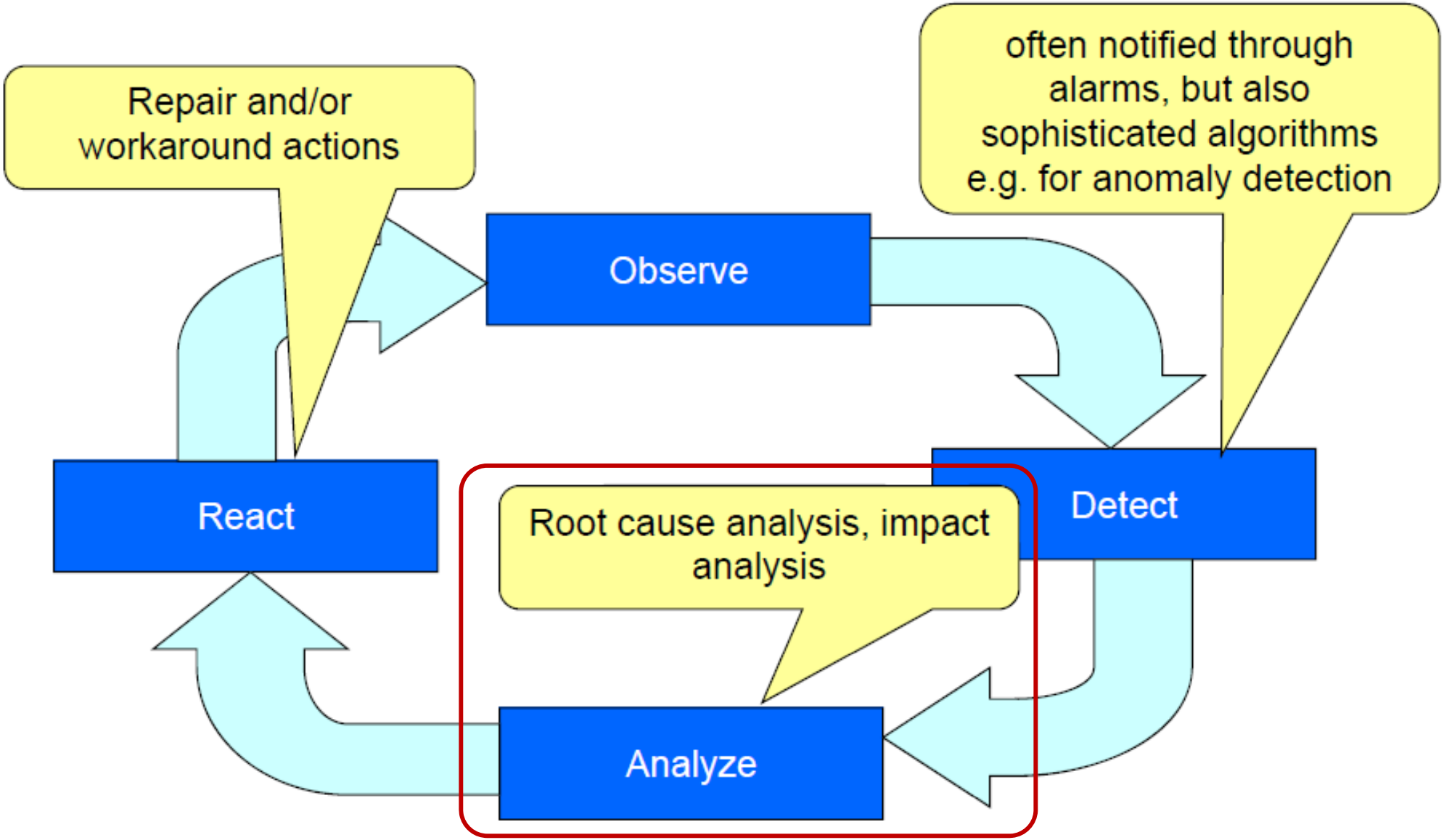
- Alarm correlation typically incurs a time delay
  - Need to wait if other alarms that could be correlated arrive
  - Tradeoff: staleness versus quality of alarm information
- Implementation flavors
  - Original alarms do not get modified but additional alarm gets generated (specifying which other alarms 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)

Alarm Augmentation

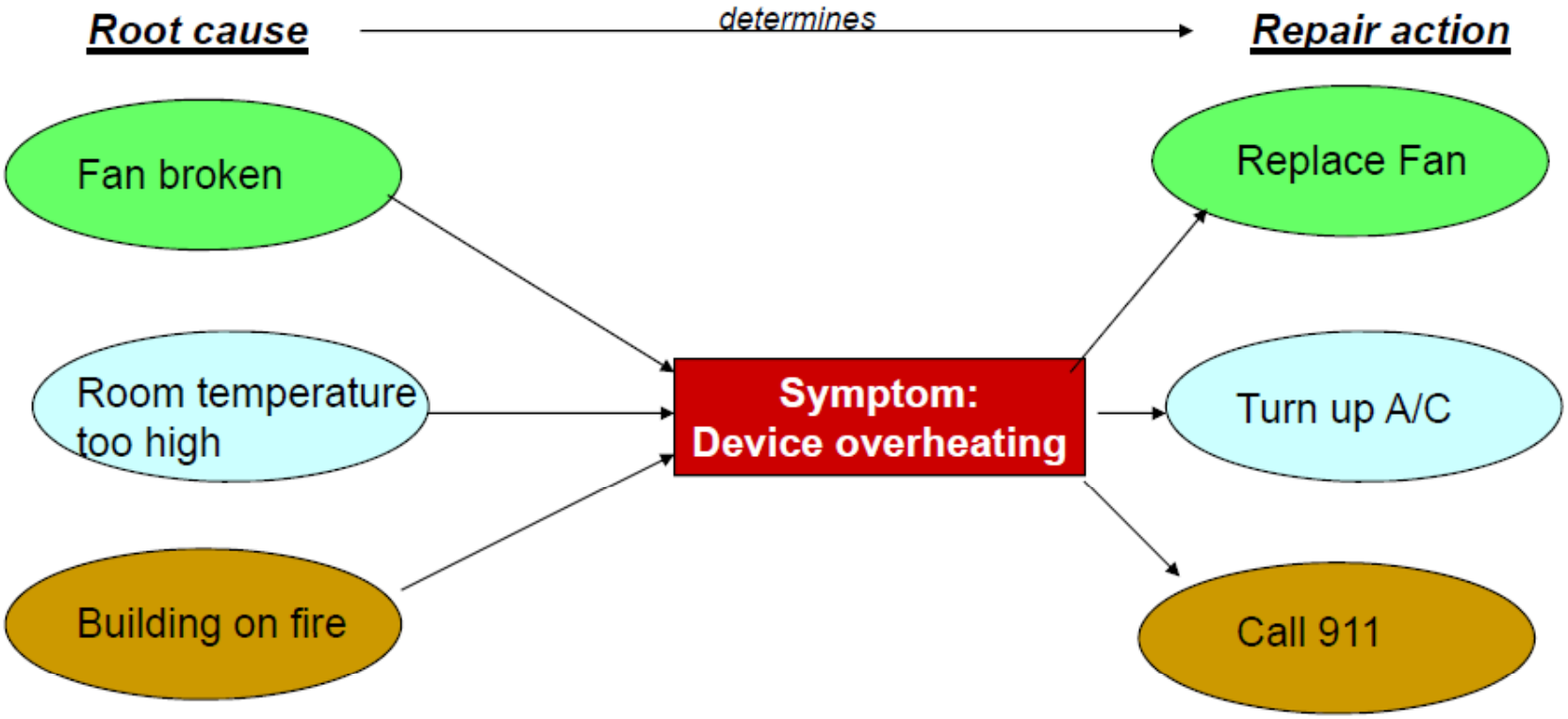
- Alarms do not always have sufficient information
- Alarm augmentation: collect additional information about the alarm context, e.g.
  - Current state
  - Current configuration
  - Self-test / diagnostics
- Anticipate which information a manager would request
  - Save an additional mgmt exchange

    → optimize management pattern
  - Make sure context information is fresh, not stale

Fault Management: Analysis & Diagnosis



Root Cause Analysis Example

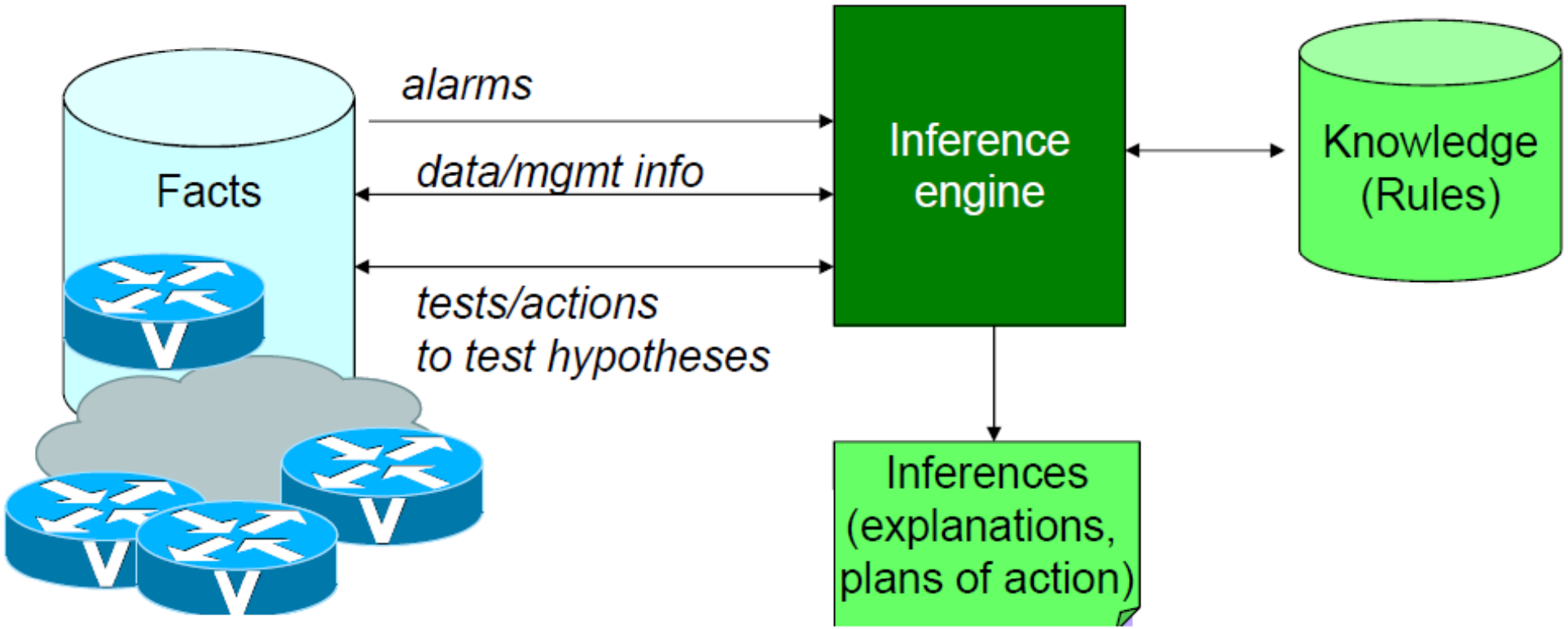


- Techniques to correlate all these events and isolate the root cause of the problem
  - Rule-based systems, Model-based reasoning, Case-based reasoning, State transition graph, …

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

Rule-Based Systems (cont'd)

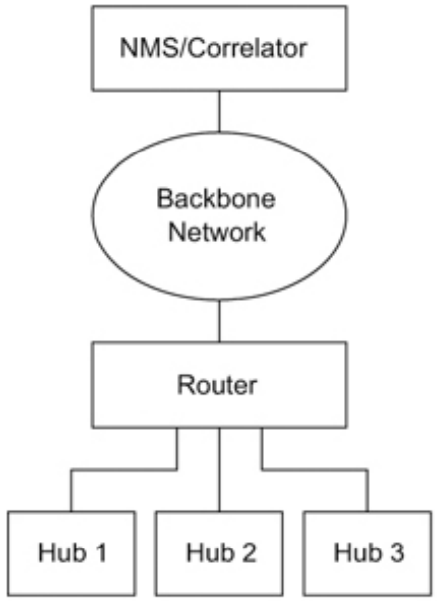


Rule-Based Systems (cont'd)

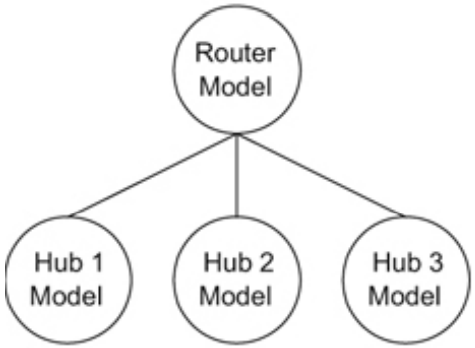
- Knowledge base
  - Rule-based in the form of **if–then** or **condition–action**,
    - Operations are to be performed when the condition occurs
- Inference engine
  - Compares the current state with the rule-base
  - Finds the closest match to output

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



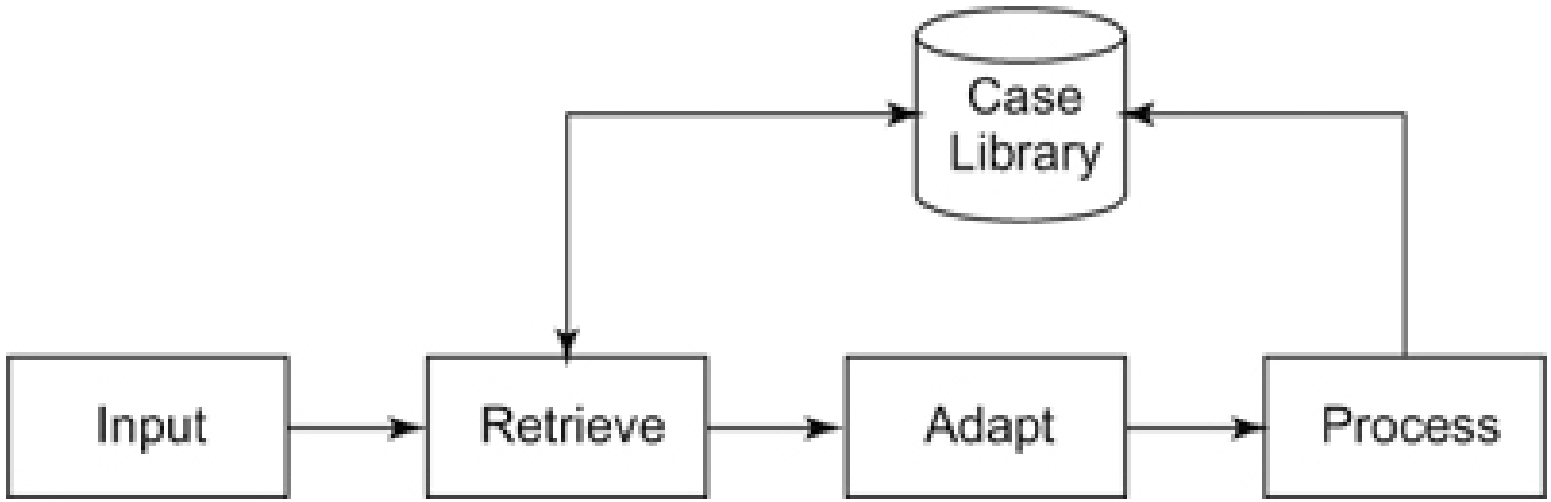
Equivalent Model

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

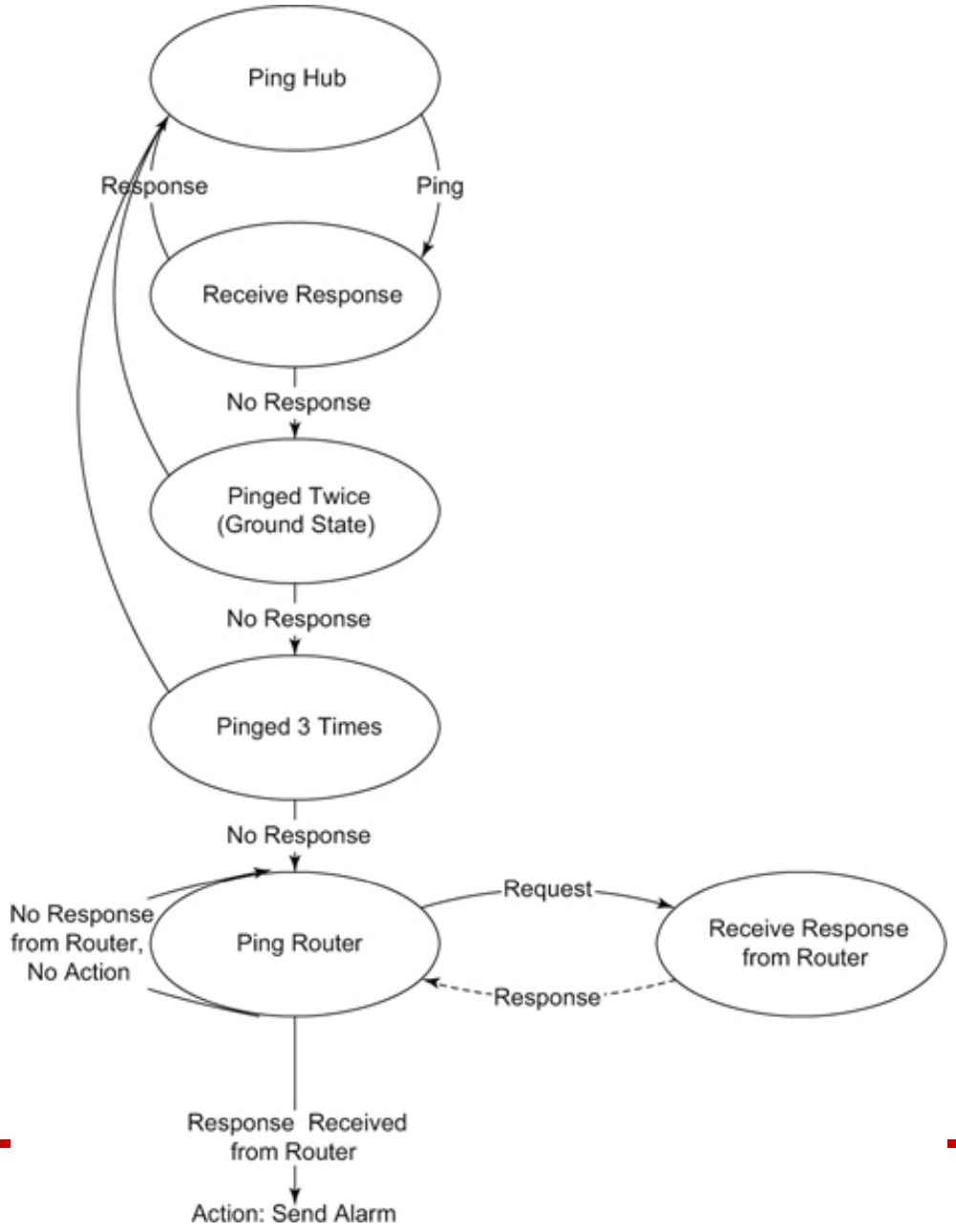
Case Based Systems

- 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



State Transition Graph

- Example



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)

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”

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

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

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

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

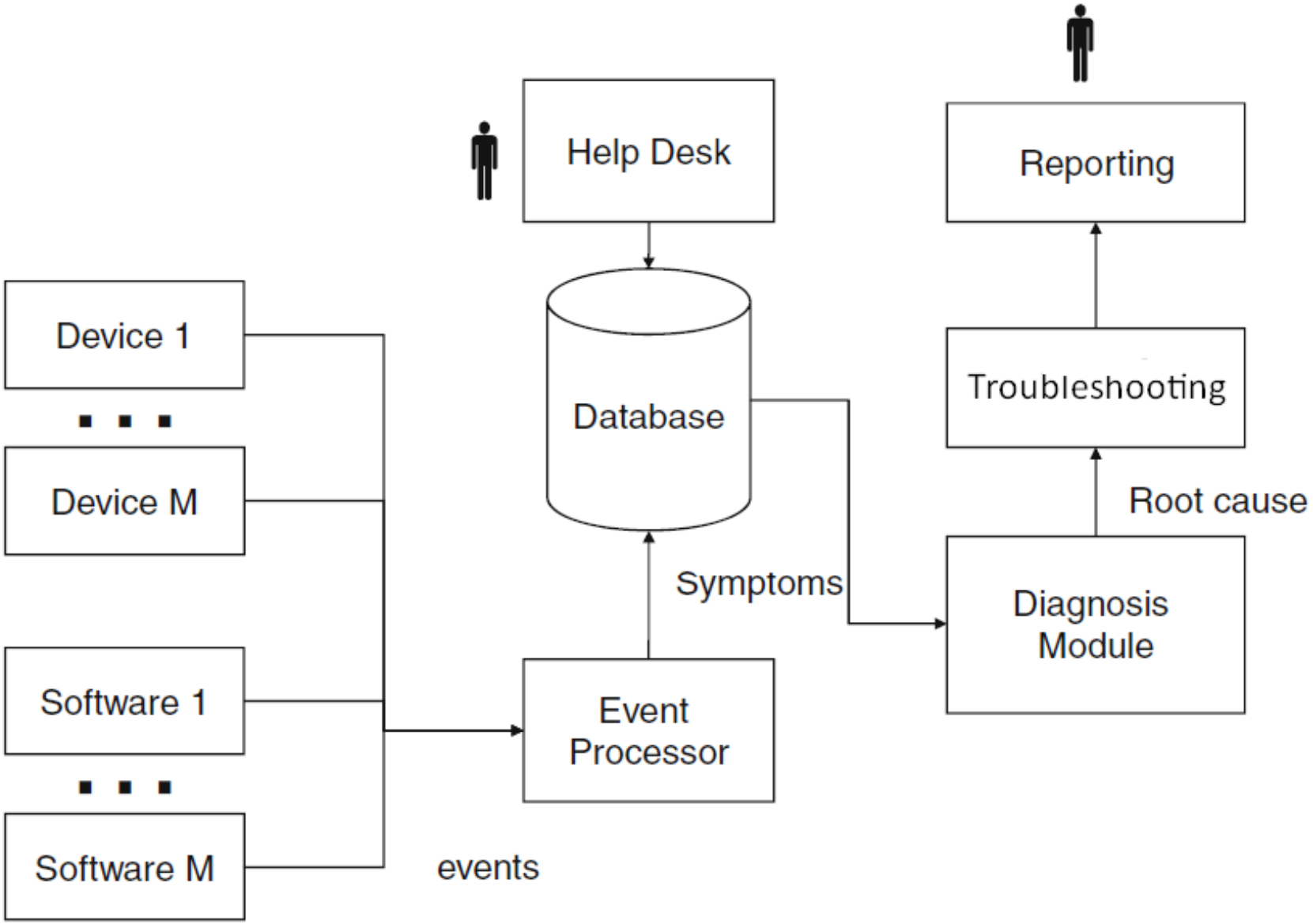
Fault Management Issues

- 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

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)

Fault Management Summary



Outline

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management
- Conclusion

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

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

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

Configuration Management Functions

- (Auto)Discovery & Auditing
- Configuration setting
  - Provisioning
- Synchronization
- Image management
- 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

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, …

CMDB (Configuration Management Database)

- CMDB
  - Contains information about the configuration of devices in the network
  - Relatively static but heterogonous 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

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

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)

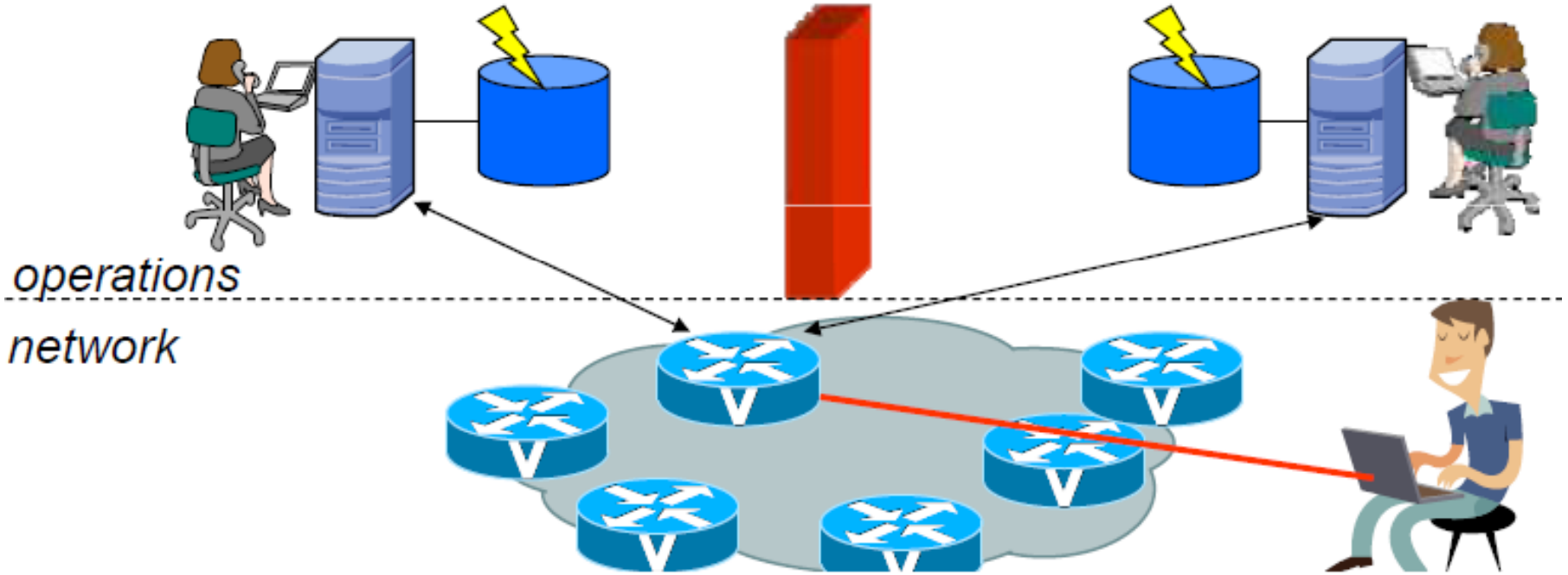
CM: Configuration Setting: Provisioning

- 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

CM: Configuration Synchronization

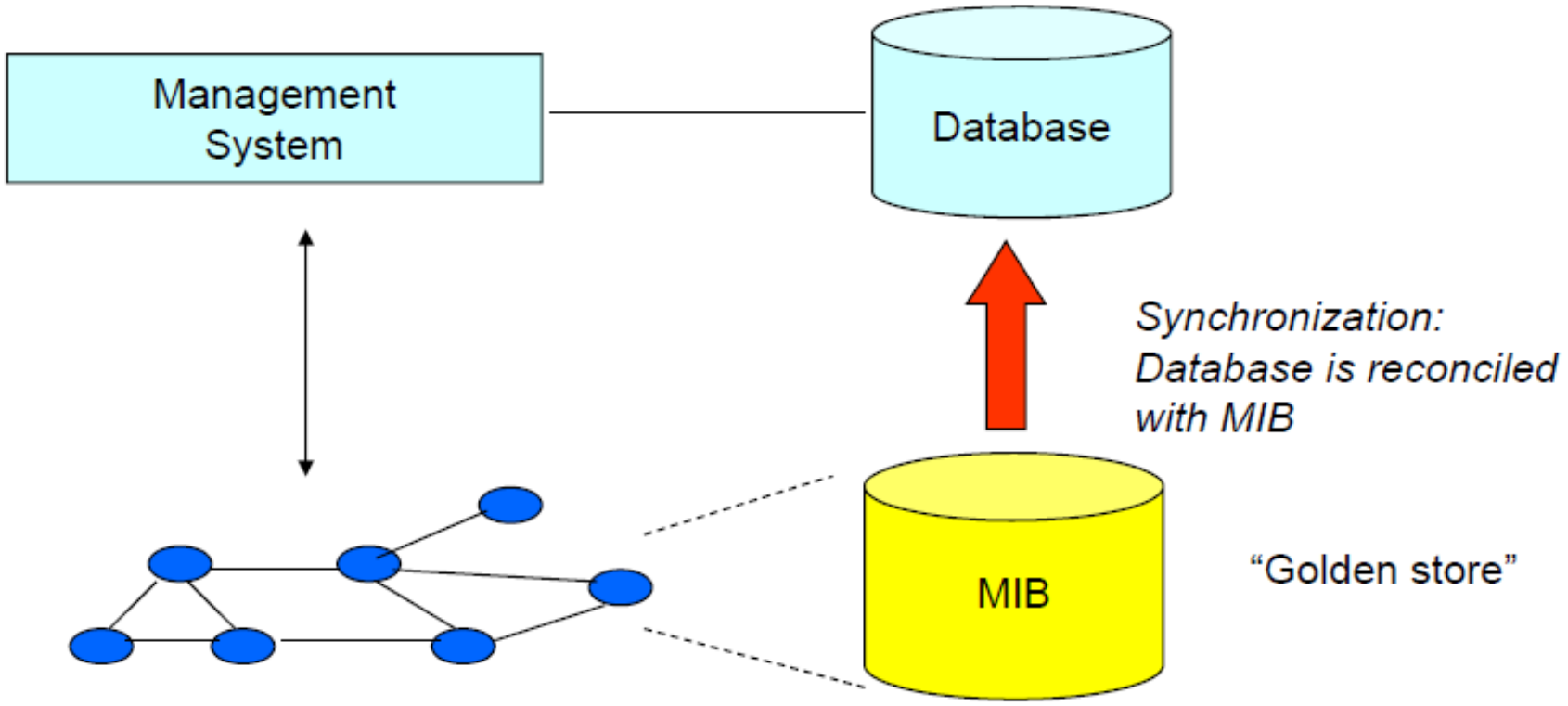
- Management systems (CMDB) keep management databases
  - Cache in the database to avoid repeatedly hitting the network
    - Management database and network need to be "in synch"
- Counterintuitive: why worry about synching
  - Configuration information changes only through management actions
- Network 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

CM: Configuration Synchronization



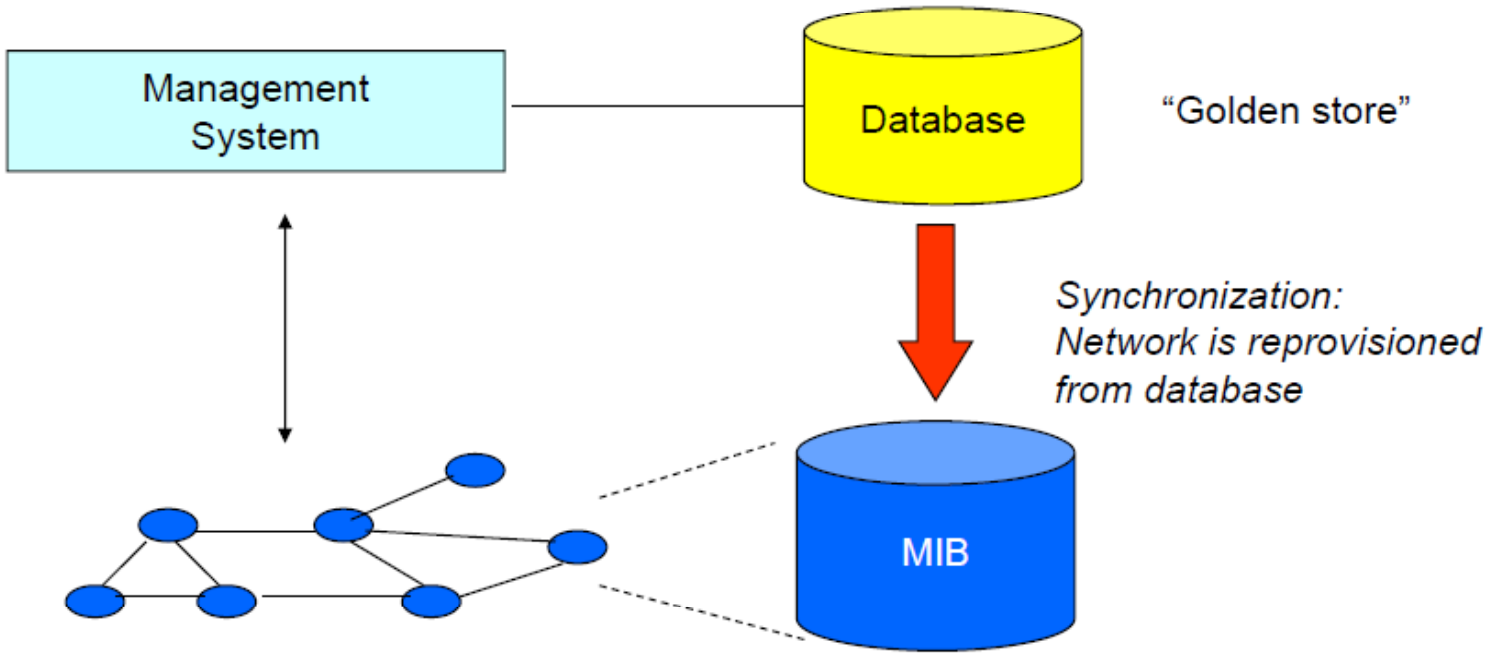
Network as Golden Store

- Most common approach
- Synchronize mgmt database with network
  - Reconciliation or Discrepancy reporting



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



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

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

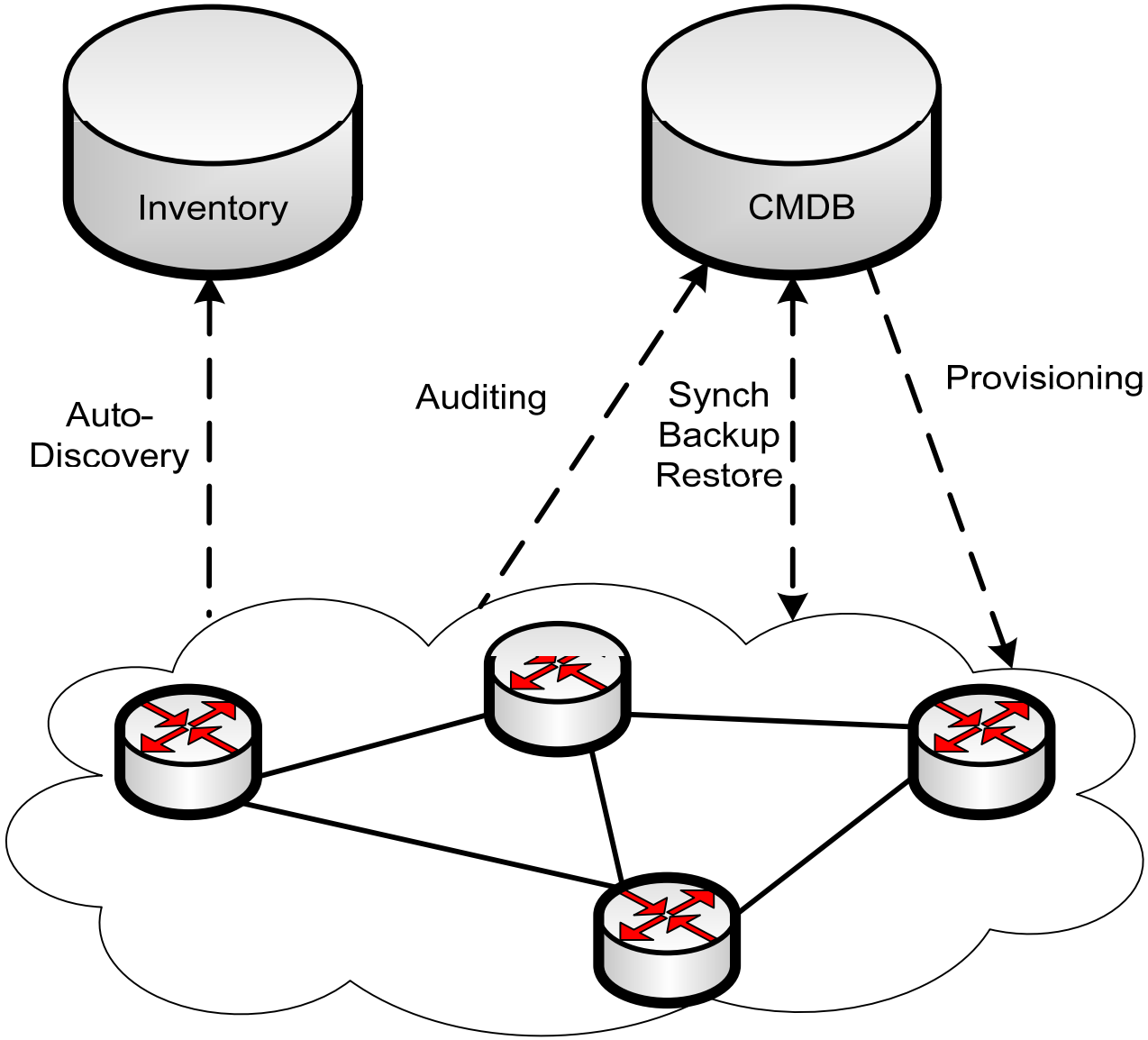
Configuration Management Issues

- 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

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

Configuration Management Summary



Outline

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management
- Conclusion

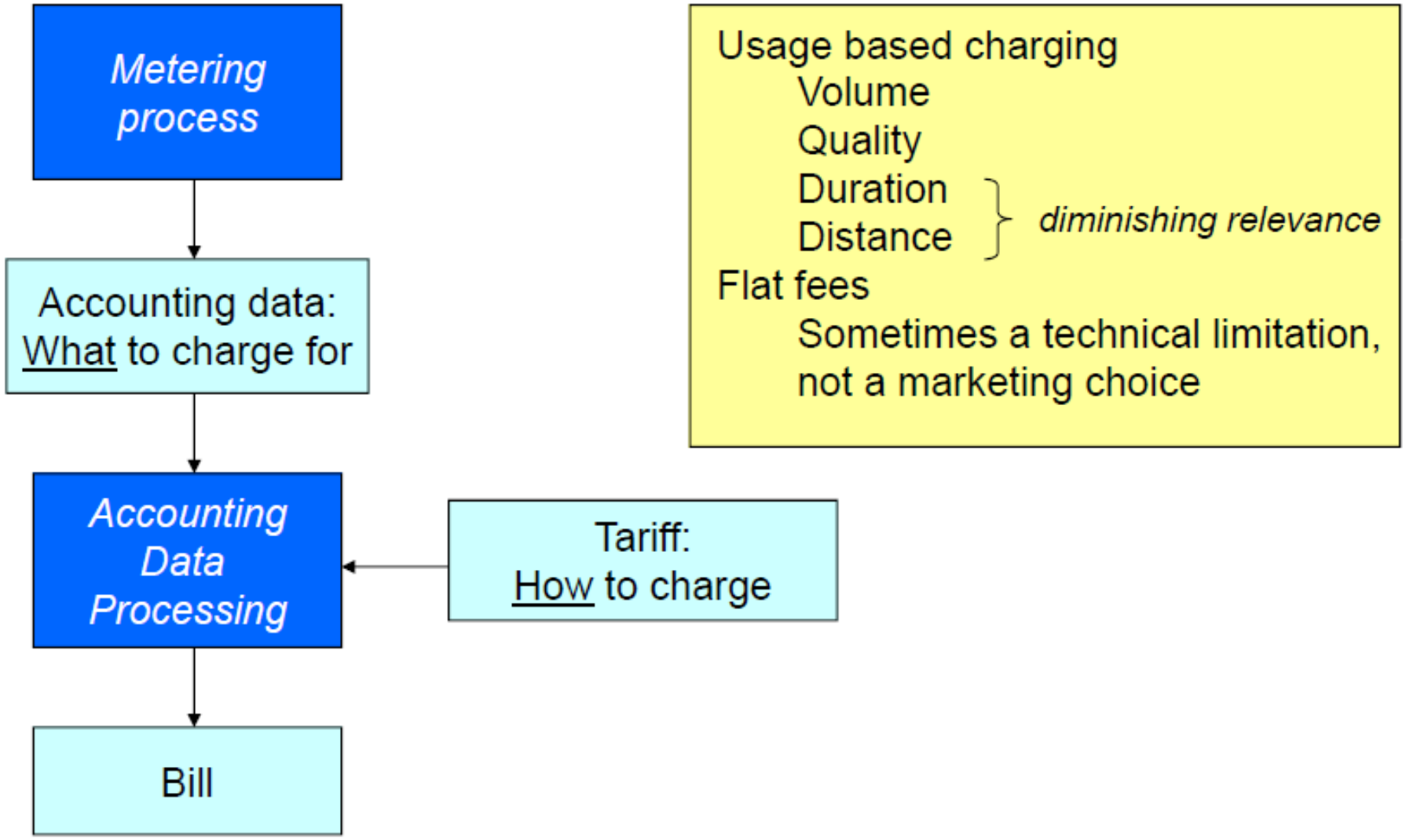
Accounting Management

- 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!

Accounting Management Functions (TMN)

- Usage Measurement
  - How much resources are used?
- Pricing
  - Pricing strategy & Rating usage
- Collections and Finance
  - Administration of customer accounts
  - Informing customers of balances
  - Receiving payments

Accounting and Billing



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

Accounting Data (cont'd)

- 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

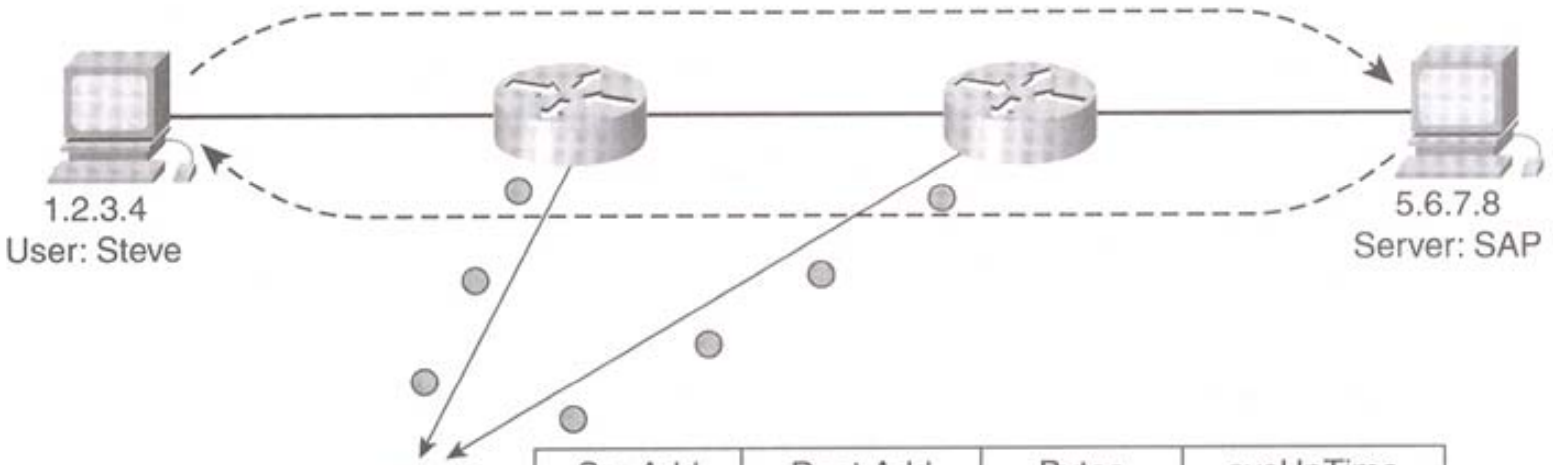
Billing

- 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

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

Billing vs. Accounting



Src Add	Dest Add	Bytes	sysUpTime
1.2.3.4	5.6.7.8	130	710940996
5.6.7.8	1.2.3.4	23977	3600362
1.2.3.4	5.6.7.8	1500	711240891
5.6.7.8	1.2.3.4	64	6033120

User	Resource	Volume	Day&Time	Cost
Steve	SAP	S→D 1630	10-01-2004 8.15 AM	2
		D→S 24107	10-01-2004 9.52 AM	

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
  - …

Outline

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management
- Conclusion

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

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

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

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

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

Performance Management Aspects

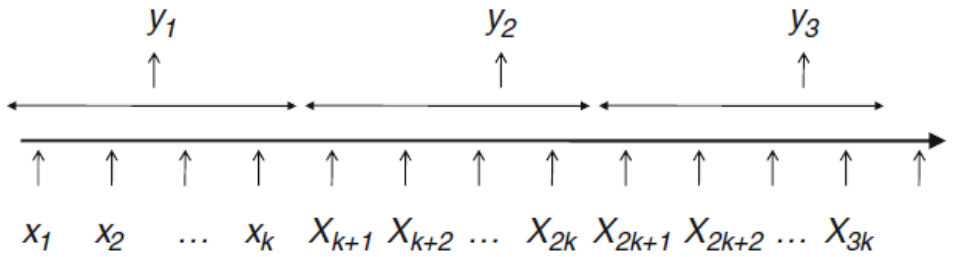
- Proactive
  - Reporting & Monitoring (performance metric history graphs)
  - The value of performance metrics are gathered periodically
  - The data analyzed and reported
  - Capacity planning
- Reactive
  - QoS assurance
  - Define threshold
  - Automatically take action when a threshold is eclipsed
    - Send an email / text message / IM
    - Sound an alarm
    - Call a pager
    - Switch to a back-up circuit
    - …

Performance Management Issues

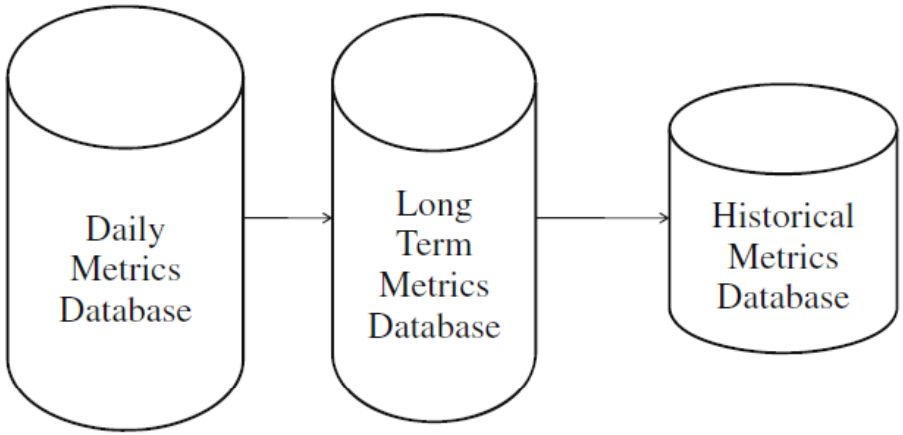
- 1) Effect of performance management on network performance
  - Large volume of performance monitoring data increase network traffic
    - Efficient mechanisms/protocols; e.g., IPFIX or local snapshot
    - Periodic polling
      - Polling rate?!
    - Database design
- 2) SLA management vs. Reporting
  - Performance reporting is typically used for capacity planning
  - SLA should be guaranteed
    - Performance troubleshooting

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



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

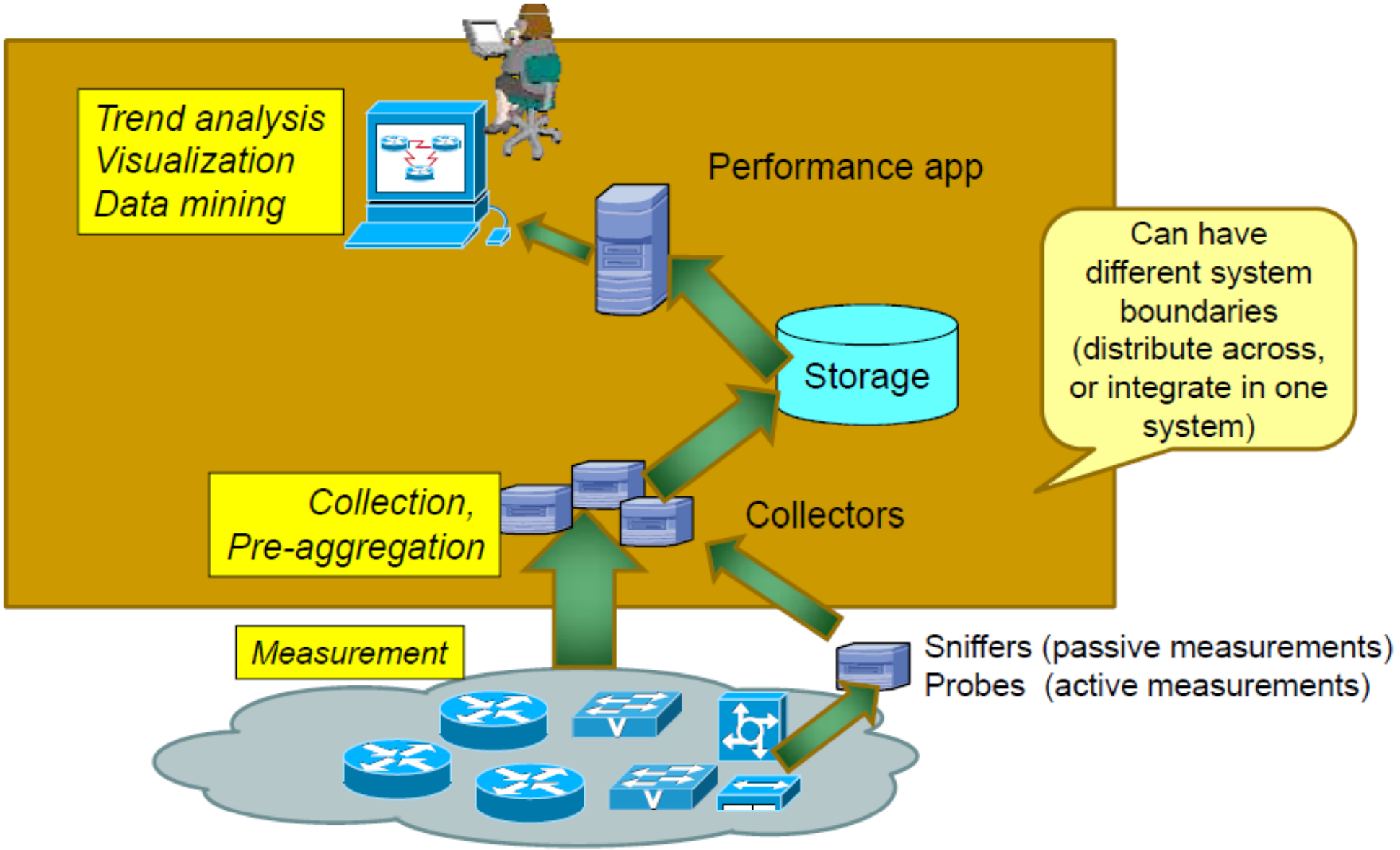
Performance Management Issues (2)

- 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

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

Performance Management Summary

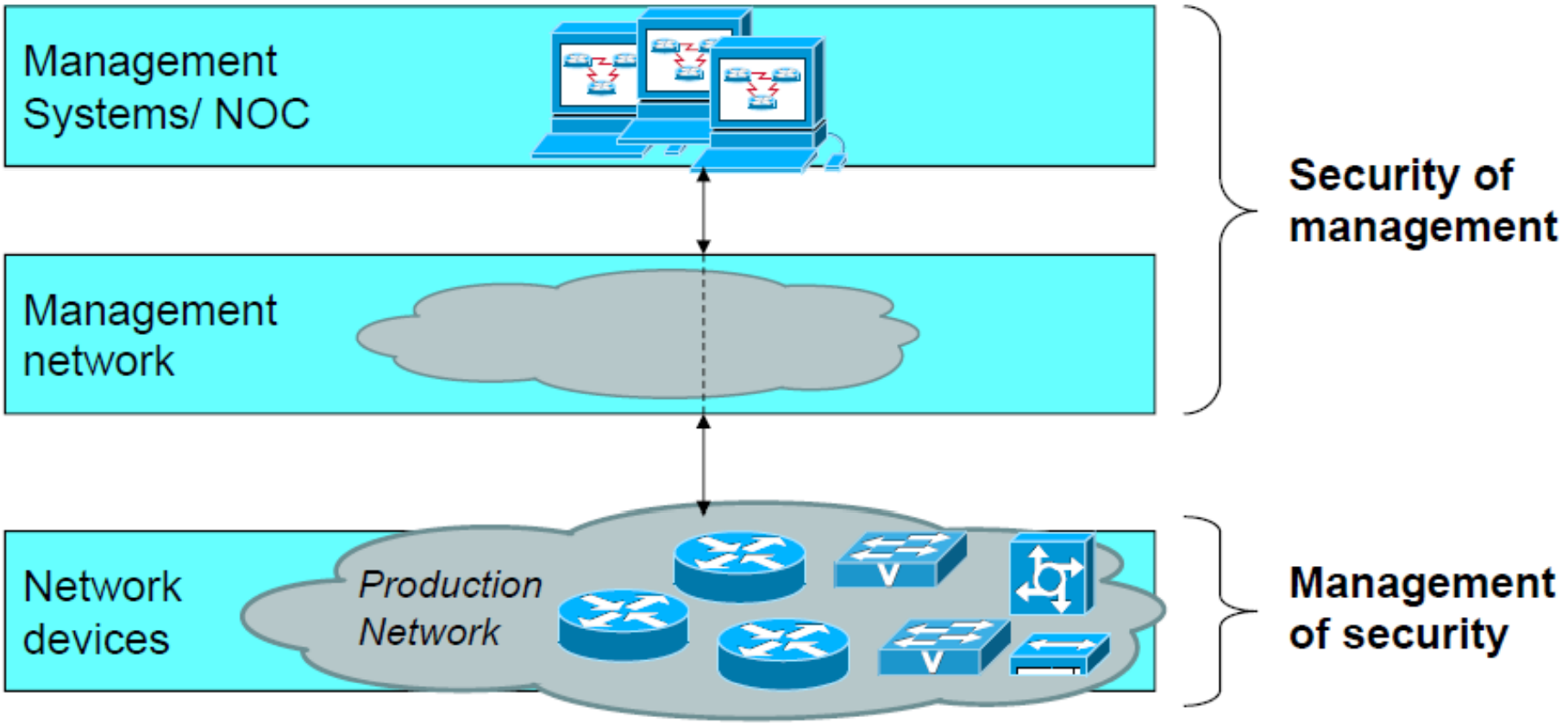


Outline

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management
- Conclusion

Security & Management

- Security of Management
- Management of security



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

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

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

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

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, …

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

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

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, …

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

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).

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

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

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

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

Outline

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management
- Conclusion

Summary

- NOC
  - Configuration management → service provisioning
  - Fault & Performance management → service assurance
  - Accounting management → Billing
- SOC
  - Security of management
  - Management of security (FCAP for security)

References

- Reading Assignment: Chapters 6, 7, 8, and 9 of "Dinesh Chandra Verma, 'Principles of Computer Systems and Network Management', Springer, 2009"
- Reading Assignment: Chapter 5 of "Alexander Clemm, 'Network Management Fundamentals' , Cisco Press, 2007"
- Mani Subramanian, "Network Management: Principles and Practice," Ch. 13
- R. Dssouli, "Advanced Network Management," Concordia Institute for Information Systems Engineering, http://users.encs.concordia.ca/~dssouli/INSE 7120.html
- Nhut Nguyen, "Telecommunications Network Management," University of Texas at Dallas, www.utdallas.edu/~nhutnn/cs6368/
- J. Won-Ki Hong, "Network Management System," PosTech University, dpnm.postech.ac.kr/cs607/
- Raymond A. Hansen, "Enterprise Network Management," Purdue University, netcourses.tech.purdue.edu/cit443
- Woraphon Lilakiatsakun, "Network Management", Mahanakorn University of Technology, http://www.msit2005.mut.ac.th/msit_media/1_2553/ITEC4611/Lecture/