CS7012

NETWORK MANAGEMENT PRINCIPLES REVIEW
THE MANAGED OBJECT

MANAGED OBJECT

OPERATIONS

ATTRIBUTES & BEHAVIOUR

NOTIFICATIONS
Manager / Agent Relationship

Manager

Standard Interface

Agent

Local (proprietary) Interface

Management Operations

Event Reports

Managed Objects

Management Operations & Notifications

Managed System

Managing System
FCAPS

Fault

Security

Configuration

Performance

Accounting
CONFIGURATION MANAGEMENT

• Responsible for:
  – Changes, additions and deletions on the managed object parameter(s)
  – Needs to be co-ordinated with the network management systems personnel (frequently involve some manual work scheduling)
  – Underlies most of the other network management functional areas
Fault Management

• Responsible for:
  – Detection of a problem
  – Fault Isolation
  – Correction to normal operation
  – Uses Polling of managed objects to search for error conditions and/or report alarms/alerts
  – Illustrates the problem detected either as a graphic or in textual format
PERFORMANCE MANAGEMENT

• Responsible for:
  – Optimisation of managed objects e.g. telephone truck line utilisation, bandwidth allocation in ATM network, load balancing on distributed servers
  – Identification of bottlenecks in network and implementation of corrective action.
  – Divides into four main functions: Performance data collection, Data analysis, Problem Reporting, Display & formatting
SECURITY MANAGEMENT

• Responsible for:
  – Administration of access controls on managed objects
  – Issuing of security alarm reports for violations. Several types of violation are possible:
    • Integrity (ensure information not tampered with), operational (deliberate misconfiguration), privacy (information read), physical (damage, loss), time delay (message delay, or replay) etc.
  – Maintenance and security audit trail
ACCOUNTING

- Responsible for:
  - Usually divided into three stages: metering, tariffing and billing.
  - Metering logs a particular usage of the managed object.
  - Tariffing is the means by which a charge can be calculated e.g. Flat rate (e.g. leased line), incremental rate, variable rates etc.
  - Billing is the selection & application of a tariffing mechanism on the metered usage and the composition of the customer bill.
  - Typically ignored in LAN networks where tariffing and billing are irrelevant but VERY important for Telecom Network & Service providers.
DIVERSITY OF MANAGED OBJECTS
KEY QUESTIONS

• What is each protocol designed to manage?

• What is the Management Information in each protocol?
  – How are different MIBs represented?
  – Naming and data types

• What functional features are there in the protocol?
  – Asynchronous communication
  – Schema alteration
WHAT IS EACH PROTOCOL DESIGNED TO MANAGE?

- **SNMP**
  - IP Networks - devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks

- **CMISE/CMIP**
  - CMIP was a key part of the Telecommunications Management Network, and enabled cross-organizational as well as cross-vendor network management. On the Internet, however, most TCP/IP devices support SNMP and not CMIP. This is because of the complexity and resource requirements of CMIP agents and management systems. CMIP is supported mainly by DMFT

- **WBEM**
  - Is intended to manage a wide range of multi-vendor IT infrastructures, and systems and network management including cloud, virtualization, desktop, network, servers and storage.
## WHAT IS EACH PROTOCOL DESIGNED TO MANAGE?

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>SNMP</th>
<th>CMIP</th>
<th>WBEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Model</td>
<td>Object Based</td>
<td>Object Oriented</td>
<td>Object Oriented</td>
</tr>
<tr>
<td>Specification Language</td>
<td>SMI</td>
<td>GDMO</td>
<td>CIM(MOF)</td>
</tr>
<tr>
<td>Operations</td>
<td>GET, SET, TRAP</td>
<td>M-GET, M-SET, M-CREATE, M-DELETE, M-ACTION, M-EVEN REPORT, M-CANCEL-GET</td>
<td>GetClass, EnumerateClasses, GetProperty, EnumerateClassName, GetInstance, EnumerateInstance, EnumerateInstanceNames, SetProperty, CreateInstance, ModifyInstance, DeleteInstance, CreateClass, ModifyClass, DeleteClass, GetQualifier, SetQualifier, DeleteQualifier, EnumerateQualifier, Enumerators, EnumeratorNames, References, ReferenceNames, ExecQuery</td>
</tr>
<tr>
<td>Standard Body</td>
<td>IETF</td>
<td>ITU-T, ISO/OSI</td>
<td>DMTF</td>
</tr>
<tr>
<td>Addressing</td>
<td>MIB with OID at leaves of the Tree</td>
<td>MIB with OID Scoping/Filtering</td>
<td>Name and Association</td>
</tr>
</tbody>
</table>
CS7012

NETWORK MANAGEMENT PAST PAPER
EXAMPLE EXAM QUESTION

• You are responsible for managing the entire network of a University, which must provide a set of services to employees and students to support the defined objectives for teaching, research and information dissemination. The requirements placed on these services will vary, but a general trend is that there is increasing reliance on the underlying network functioning day and night, all year-round. Not only must the network function, but it must also have adequate capacity and acceptable, reliable response time.

• Outline the possible network management architecture and deployment strategy you would suggest for the University based on FCAPS, giving reasons for your answer.

• In your answer identify the appropriate network management protocols and monitoring strategy you would suggest. State any assumptions you make in deciding the configuration of the management infrastructure. Your answer should highlight: strengths and weaknesses, as well as challenges, for your chosen protocol and strategy.

• [15 marks]
• **Underlying Technology/Protocol**
  
  - Things to consider: Type and size of network, capabilities of managed objects, complexity of solution, security of solution, etc.
  
  - Strengths: SNMP is supported by most vendors, communicates using UDP over Ethernet, low processing requirements, flexible and extensible, etc.
  
  - Weaknesses: Not so simple ;) as difficult to implement, not particularly efficient (wasted bandwidth with needless information – SNMP version, use of byte Strings)…still works well enough though 😊

• **Architecture**
  
  - Things to consider - Manager of managers?
    
    • Manager, agent, MIB
      
      - Use of manager resource in manager system, resources in agent, external monitors, proxy agents?
• **Configuration management**
  – Things to consider: Need to be able to get and set properties of both physical resources and logical objects, configure devices on initialization, shutting down devices, reconfiguring devices to address issue related to maintenance e.g. faults, performance, security. Manager should have an overview of all managed objects in the network and maintain an archive of change logs.
  – Challenges: limited operations (get, set, trap, getbulk, inform), does not support actions

• **Fault management**
  – Things to consider: identifying faults in the communication network (routers, cables, etc.), identifying faults in devices (printers, etc.), detection of a problem, fault isolation, correction to normal operation, uses polling of managed objects to search for error conditions and/or report alarms/alerts, illustrates the problem detected either as a graphic or in textual format.
  – Use of SNMP polling and traps.
  – Some challenges: managing the additional bandwidth to support polling of many managed objects – use of logs. Avoiding ‘event storm’ – ensure thresholds are not too low to trigger events.
• **Security management**
  
  – Monitors access to the network and its components. How to handle modification of information, masquerading, message stream modifications. Limited security in SNMPv1 (community name authentication). Authentication, privacy and access control (Encryption) - SNMPv3
  
  – Challenges: private key must be set up outside of SNMPv3 as a configuration function. Avoiding event storms.

• **Accounting management**
  
  – Things to consider: Keeping an overview of traffic load and traffic types. Also evaluates the state of health of network equipment (CPU load, memory use, environmental data, etc.).
  
  – Challenges: Reducing additional bandwidth

• **Performance management**
  
  – Things to consider: See a) – service oriented (availability, response time, accuracy) and efficiency oriented (throughput, utilisation) evaluation answer. Evaluates the performance of the network, including delay, packet loss, and throughput.
  
  – Challenges: Reducing additional bandwidth
(c) What is trap directed polling in SNMP? Indicate how trap directed polling could be utilized in the above problem for distributed fault management. What are the weaknesses in trap directed polling and how could they occur if applied in the above problem.

(5 Marks)
• (b) What is trap directed polling in SNMP? Indicate how trap directed polling could be utilized in the above problem for distributed fault management. What are the weaknesses in trap directed polling and how could they occur if applied in the above problem.

  – impractical for the manager to poll or request information from every object on every device.
  – Trap directed - each agent on the managed device to notify the manager without solicitation. It does this by sending a message known as a trap of the event.
  – manager can then poll the agent directly, or poll other associated device agents to get a better understanding of the event.
  – Trap-directed notification can result in savings of network and agent resources by eliminating the need for frivolous SNMP requests.
  – In addition, a managed device agent cannot send a trap if the device has had a catastrophic outage e.g. if a gateway between two buildings goes down.