Chapter 16

Advanced Management Topics

Objectives

- Next generation NM requirements
  - ITU-T
  - IETF
- Status of current NM technology
  - ISO Model: FCAPS
  - Product requirements
- Limitations of SNMP management
- Early Web-based development
  - Web interface and Web management
  - WBEM
  - WIMA
- CORBA-based NM technology
- XML-based NM technology
- Comparison of NM technologies
- Recent NM-related standards

Need for New Management Technologies

- Since late ’80s
  - Networks have evolved
  - Management needs have changed
  - Management technologies have evolved

- Mismatch in speed of evolution of networks and management requirements compared to the speed of management technology development

Notes

Evolution of Networks

- In the mid-late ’80s
  - Devices simple, resources constrained
  - Capabilities were limited

- Today
  - Increased functional complexity
  - Increased complexity in configuration
  - Increased intelligence and programmability of devices
  - Networks that provide a wide range of services
  - NGNs: Packet-based networks for all services
  - Providing unfettered (unrestricted) access for users to networks and to competing service providers for services of their choice

a next generation network (NGN) is a packet-based network that can be used for both telephony and data and that supports mobilility.

Notes

NGN Requirements

NGN…Next Generation Networks

Original Requirement	New Requirements
End-to-end transparency	Packet inspection, NAT
Peer-to-peer	NATs/firewalls/servers
Connectionless	MPLS
Best effort	Real-time demands, bandwidth demands
User back-off	QoS guarantees
Network empowerment	User empowerment
No flow state	Flow state
Trust	Hackers everywhere
Static addresses	DHCP, mobility
Fairness	QoS
Terminal-to-host	Mass public residential services, multiterminal, multi QoS
Flat network	Access and core domains
Simple protocol layering	Protocol maze
Research/Defense use	Commercialization, competition, consumer choice

- Inspection= careful examination or scrutiny

Short for Network Address Translation, an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT where the LAN meets the Internet makes all necessary IP address translations.

NAT serves three main purposes:

1. Provides a type of firewall by hiding internal IP addresses
2. Enables a company to use more internal IP addresses. Since they're used internally only, there's no possibility of conflict with IP addresses used by other companies and organizations.
3. Allows a company to combine multiple ISDN connections into a single Internet connection.

Changes in Operator Needs

- Management of large backbone networks requires powerful configuration management
- Move from device management approach to system management
- Service-centric view of network
  - VoIP (residential and business), multimedia streaming, IP TV, fast data connectivity, triple play
- Increased speed of service delivery
- Automation of business processes

Notes

Configuration Management Needs

- Need for concurrent configuration changes to several network devices
- Download bulk configuration changes on many devices
- Schedule configuration operations on devices at particular times
- Roll back support
- Coordinated activation of downloaded configurations

Roll back support
= Return to a previously committed configuration. The software saves the last 50 committed configurations, including the rollback number, date, time, and name of the user who issued the commit configuration command.

Notes

Consequences for Management

- Rethinking management principles – Integration of independent developments
- Management support for delivering quality service
- Changes resulting from “user” focus as opposed to “network” focus
- Importance of developing standardized management software for easy maintenance and extensibility

Notes

Traditional Approaches - Datacomm

- SNMP based
- Aim was to have simple small footprint protocol
- Kept self contained and independent of other network services
- Catered to fault, performance monitoring, and simple configuration management
- Soon after release, shortcomings were exposed
- SNMPv2: Get-Bulk, Inform, SMIv2
- SNMPv3: security

Notes

- DataComm is a privately held company, established in 1984. Building upon a strong foundation, layered with tradition, ethical values, innovation and excellence, DataComm has assembled a dynamic team that fuels our continued growth. As we look towards our bright and promising future, we continue to stay grounded in the past – understanding the challenges of success.

- Technology Solutions include:

    - Network Security
    - Network Management
    - Messaging
    - Consultation
    - IP Telephony
    - Cabling

Drawbacks of SNMP

- Inadequate information modeling – simple data structures and protocol operations
- Object based rather than object oriented
- No inheritance – so no information re-use
- Inadequate primitive for bulk information retrieval
- UDP transport restricts size of data sent
- Limited configuration management support
- Low level semantics

Notes

Overcoming SNMP Shortcomings

- Evolutionary efforts were made to address shortcomings
  - Improving SMI
  - Improving SNMP protocol
  - Enhancing configuration management

Notes

Improving SMI

- Internet Research Task Force (IRTF) and Network Management Research Group (NMRG) developed **SMIng**
  - Allows arbitrarily nested data structures
  - Facilitates re-usability of complex data structures
  - Extensible mechanisms
- IETF was to develop a standards track for above in 2000
  - Phase 1: requirements drawn up
  - Phase 2: two strong proposals emerged
- Efforts to merge these failed, in 2003 group was wound up

Next Generation Structure of Management information

SNMP Protocol Improvement

- Attempt to improve protocol shortcomings
- Efforts to reduce overhead due to OID redundancy
  - Compression
  - Suppression of redundant OID fragments
  - Effect bulk transfer at MIB level instead of OID
- Use of TCP as transport protocol
- Did not meet with success because of industry reluctance to accept new technology

Configuration Management

- COPS-PR (Common Open Policy Service– Policy Provisioning) for improving Configuration Management capability
- Resource Allocation Protocol (RAP)–WG (**working group**) for policy-based configuration and provisioning
- Specification language: Structure of Policy Provisioning Information (SPPI)
- TCP is transport protocol
- Intends to make configuration changes based on PBMS (Policy-Based **Management** (**PBM**))
- Did not meet with market acceptance

OSI NM

- Designed as successor to SNMP OSI-NM
- Comprehensive management technology addressing datacom and telecom arena
- CMIP/ CMISE support many primitives
- Information access is powerful
- Supports bulk and selective retrieval
- Connection-oriented transport included
- Found to be complex and technologically too advanced for deployment in late ‘80s

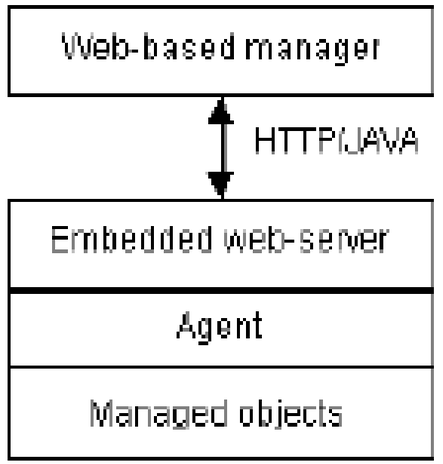
OSI NM

•The OSI Network Management model is a model for Network and System Administrators to understand the major functions of network management systems. In this model, there are 5 areas' of functions which is also known as FCAPS.

•The aim of the model is for Network and System Administrators to understand a number of issues and aspects. These include:

- •Fault management and recovery
- •Configuration and change management
- •Accounting User Management
- •Performance Management
- •Security Management
- •Application support
- •Integration and Migration
- •Planning for growth and acquisitions

Web-based Management



- Early approaches:
  - Embedded Web server in device
  - Browser can connect to the URL of the device and html pages with management information
  - Provides graphical displays of management information
  - Improved configuration facility, detailed device management
- Drawbacks
  - More an EMS (element management system)-like approach – no end-to- end view
  - High level management functions such as map-based view, root cause analysis, trend analysis not supported

Recent Trends

- For efficient service delivery, end-to-end automation of certain processes essential.
    - eTOM map specifies these
- Software architecture of individual applications must cater to seamless integration.
- Service Oriented Architecture holds the promise of meeting this requirement.
- MTOSI and OASIS are two standards getting established in this regard.

Notes

MTOSI

- Multi Technology Operations Systems Interface
- Standard that provides an integration framework for different applications in Service Provider's Operations Centre
- Processes referred to as Operations Systems or OS
  - Management functional areas of an NMS (FCAPS)
  - Root Cause Analysis, Service Impact Analysis, SLA monitoring, etc.
- The objective of MTOSI is to extend MTNM using XML/Web services interface
- Results in integration of the different OS components using SOA and NGOSS design principles
- Initial focus of MTOSI was to develop an OS-to-OS interface that covers the NMS/EMS interface as a special case

Notes

MTOSI-based Architecture

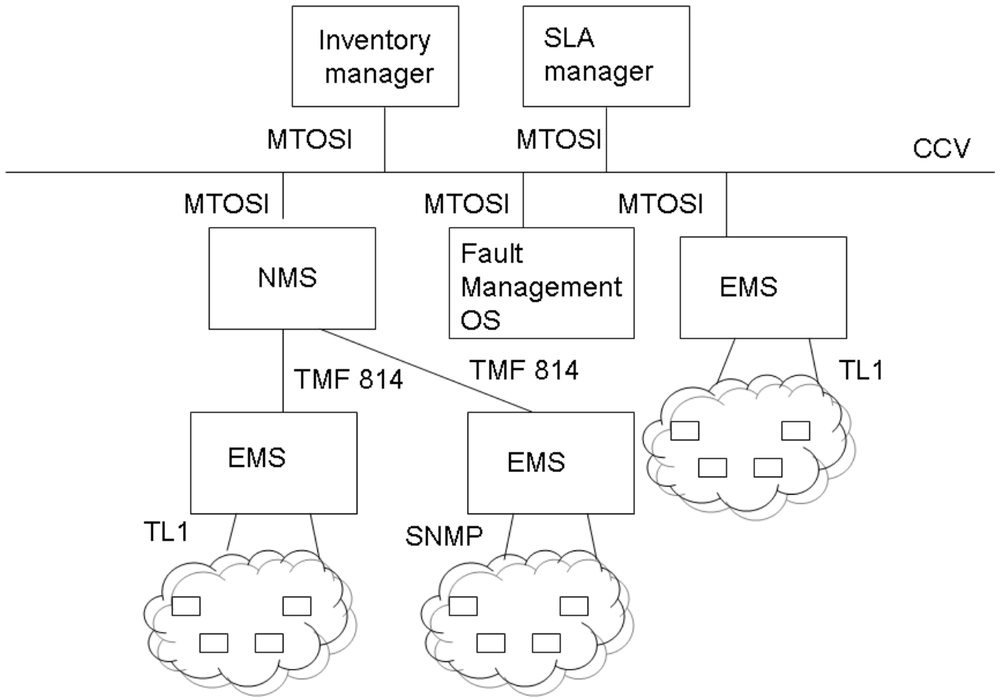


Figure 16.17 MTOSI Architecture

OASIS

"Organization for the Advancement of Structured Information Standards (OASIS) is a not-for-profit consortium that drives the development, convergence, and adoption of open standards for the global information society."

Notes

OASIS Standards

- Web Services Distributed Management (WSDM) [WSD] committee defined the architecture and technology to manage distributed resources using Web services
- Standard particularly applicable to systems management
- The two applicable standards are Management Using Web Services (MUWS) and Management Of Web Services (MOWS).

Notes

MUWS

- Addresses the use of Web services as the foundation of a systems management framework
- Includes the use of Web services for interaction between the managed resources and management applications
- Wire-level specification of how to describe the manageability of a resource using WSDL documents
- Capability for discovery of manageable resources and their manageability capabilities.

Notes

MOWS

- Includes management-specific attributes to expose properties such as lifecycle state and performance of Web services.

- Management operations to monitor/control a Web service itself are specified.

Notes

Summary

- Service Provider's NOC has several loosely coupled applications interacting with managed resources and with each other.
- Network facing interface is low-level, efficient, and fast.
- Application communication via event-driven bus architecture required rather than a request-response model.
- Web services-based management approach appropriate
  - MTOSI, in the telecom IT environment , and WSDM for systems management meet the needs.

Notes