SNMP Network Management Concepts

Chu-Sing Yang

Department of Electrical Engineering
National Cheng Kung University
Outline

- Background
- Basic Concepts
- Summary
The Origins of TCP/IP

- Starts at 1969, and founded by U.S. DoD
- Advanced Research Projects Agency
  - Developed ARPANET
  - Was the one of the first packet-switching networks
  - As ARPANET evolved, interoperability became a major issue
- TCP/IP protocol suite was developed at late of 1970s
  - Standardized as official Internet Architecture Board (IAB) standards issued as request for comments (RFC)
  - Issued as military standards
  - TCP/IP grows rapidly in nonmilitary applications
    - International standards
    - Is a mature protocols
    - Provides interoperability
    - Offers a high level of functionality
The Origins of TCP/IP Network Management

- As TCP/IP was being developed, little thought was given to NM management problems was left to protocol experts
  - Control network with the use of some basic tools
  - There were no management protocols through the late 1970s
  - Internet Control Message Protocol (ICMP) was effectively used for management
    - Provides a means for transferring control messages from routers and other hosts to a host
    - Provides feedback about problems in the environment
    - Is available on all devices that support IP
    - Echo/echo-reply message pair provide a mechanism for testing that communication is possible between entities
      - Recipient returns the contents of that message in an echo-reply message
    - Time stamp/time stamp reply provide a mechanism for sampling the delay characteristics of the network
The Origins of TCP/IP Network Management

- ICMP + IP header options to develop simple but powerful management tools
  - Source routing
  - Record route
- PING (Packet Internet Groper)
  - ICMP + interval between requests and # times to send a request
    - Determines if a physical network device is addressed
    - Verifies a network is addressed
    - Verifies the operation of a server on a host
  - Used to observe variations in round-trip time and in packet loss rate
    - Helps to isolate areas of congestion and points of failure
The Origins of TCP/IP Network Management

- With the number of hosts on the network and the number of individual networks have grown explosively
  - A standardized protocol with more functionality is required
  - Simple Gateway Monitoring Protocol (SGMP)
    - Issued in Nov. 1987
    - Provided a straightforward means for monitoring gateways
      - To minimize the complexity of software needed for gateway management and the number of commands to which gateway agents would have to respond
      - "get" and "set" (change) a value of a variable
General-purpose Network Management Approach

- **High-Level Entity Management System (HEMS)**
  - Was a generalization of Host monitoring Protocol (HMP)
  - HMP was the first NM protocol used in the Internet

- **Simple Network Management Protocol (SNMP)**
  - Was an enhanced version of SGMP

- **CMIP over TCP/IP (CMOT)**
  - Incorporates the CMIP, services, and database structure
  - Standardized by ISO for NM
  - CMIP (Common Management Information Protocol)
Common Management Information Protocol (CMIP)

- Has **Eleven** management commands
- Provides more detailed representation of MIB objects, the ability to create objects, and objects that inherit the properties of other objects
- Define the scope of object filtering according to attributes leads to much greater control of its Get operation
- Upon request from the management application, CMIP creates the protocol data unit and maps it to a Remote Operations Service Element (ROSE) protocol that supports communications between all distributed applications in the OSI environment
The Difference Between CMIP and SNMP

- CMIP has **Eleven** management operations
- SNMP are five management commands
- CMIP runs on OSI model
- SNMP runs on TCP/IP model
- The SNMP motto: "Keep it Simple"
The Similarity Between CMOT and SNMP

- Both protocols use the same database of managed objects.
- Both protocols use the same set of monitoring and control variables, in the same formats, within any host, router, bridge, or other managed device.
  - A single structure of management information (SMI)
    - The basic format for objects
  - A single management information base (MIB)
    - The structure or schema of the database
Evolution of Network Management

- 1968  ARPA funds develop packet switching networks
- 1974  TCP/IP concept proposed
- 1976  Ethernet developed
- 1978  OSI Ref. Model development initiated
- 1983  OSI Ref. Model becomes international standard
- 1987  SGMP development started ASN.1 developed
- 1988  IAB initiates study of SGMP and CMIP
SNMPv1 become Draft Standard
Network Management Framework (SMI)
Draft Standard MIB I developed
Evolution of Network Management

- 1989  CMOT approach abandoned
SNMP becomes the defacto standard
for TCP/IP management

- 1990  SNMPv1 becomes recommended
standard

- 1991  MIB II
RMON

- 1993  SNMPv2 Proposed
SNMPv2 Security
SNMPv2 MIB
SNMPv2 SMI
Evolution of Network Management

- 1995  RMONI
- 1997  RMONII
- 1998  Desktop Management Interface (DMI) Specification v2.0s
- 1999  SNMPv2 Management Frameworks
- 2002  SNMP Management Frameworks
- 2002  SNMPv3 Security
- 2002  SNMP VACM (view-based Access control model)
- 2002  SNMP MIB
SNMP-Related Standards

- Structure and Identification on Management Information for TCP/IP-based networks
  - RFC 1155
  - Describes the managed objects contained in the MIB

- Management Information base for Network Management of TCP/IP-based Internets: MIB-II
  - RFC 1213
  - Describes the managed objects contained in the MIB

- Simple Network Management Protocol
  - RFC 1157
  - Defines the protocol used to manage these objects
Outline

- Background
- Basic Concepts
- Summary
Network Management Architecture

TCP/IP network management model
- Management station
- Management agent
- Management information base
- Network management protocol
Management Station

- Is a stand-alone device
- A set of management applications for data analysis, fault recovery
- An interface by which network manager monitors and controls the network
- A database of information extracted from the MIBs of all the managed entities in the network
- Performs the monitoring function by retrieving the value of MIB objects
- Cause an action to take place at an agent
- Changes the configuration settings at an agent by modifying the value of specific variables
Management Agent

- Equipped on key platforms
  - Hosts, bridges, routers, and hubs
- Managed from a management station
- Responds to requests for information
  - Action from the management station
  - Asynchronously provides the management station with important but unsolicited information
Management Information Base

- **Object**
  - Represented the managed resources in the network
  - Is a data variable that represents one aspect of managed agent

- **MIB**
  - The collection of objects
  - Functions as a collection of access points at the agent for the management station
    - Objects are standardized across systems of a particular class
      - Used for the management of routers
Network Management Protocol

- Linked the management station and agents
- Simple Network Management Protocol (SNMP)
  - Used for the management of TCP/IP networks
  - Key capabilities
    - Get
      - Enables the management station to retrieve the value of objects at the agent
    - Set
      - Enables the management station to set the value of objects at the agent
    - Trap
      - Enables an agent to notify the management station of significant events
Network Management Protocol

Architecture

- Designed to be an application-level protocol that is part of the TCP/IP protocol suite
  - Operates over UDP

Management station

- Manager process
  - Controls access to a central MIB at the management station
  - Provides an interface to the network manager
  - Achieves network management by using SNMP
    - Implemented on top of UDP. IP, and the relevant network-dependent protocols

Managed devices

- Agent
  - Implements SNMP, UDP, IP
  - Interprets the SNMP messages and controls the agent’s MIB
Configuration of SNMP

**FIGURE 4.1** Configuration of SNMP
Network Management Example

- A management application of NMS calls for the service of the management process
- The management process calls the SNMP manager
- The SNMP manager constructs a request packet and sends it to SNMP agent
- The SNMP agent passes the packet to the agent process
- The agent process accesses the values of the requested variable and passes it to the SNMP agent
Network Management Example

- The SNMP agent constructs the response packet and sends it to the SNMP manager.
- The SNMP manager receives the response packet and passes it to the management process.
- The management process either passes the requested values to the application program that displays it, perhaps using a Graphical User Interface (GUI), or stores it in memory for later retrieval.
SNMP Protocol

- SNMP management station
  - getRequest
  - getNextRequest
  - setRequest

- SNMP agent
  - GetResponse
    - The form of acknowledged message by the agent
    - Passed up to the management application
  - Trap
    - Issues by agent to response an event that effects the MIB and the underlying managed resources
The Role of SNMP

[Diagram showing the relationship between SNMP management station and SNMP agent]
If the number of managed agents is large, and if each agent maintains a large number of objects, the management station becomes impractical regularly to poll all agents for all object data.

At initialization time, and at infrequent intervals, the management station poll all of the agents for some key information:
- Interface characteristics
- Baseline performance statistics
- Packet count
Trap-Directed Polling (Cont’)

- Once baseline is established
  - Management station refrains from polling
  - Each agent notifies the management station of any unusual event -- traps
    - Agent crashes and is rebooted
    - Link fails
    - Overload condition as defined by the packet load crosses some threshold
Trap-Directed Polling (Cont’)

- Management station may choose to take some action
  - Is alerted to an exception condition
  - May directly poll to the agent reporting the event and to some nearby agents to diagnose any problem
  - Gain more specific information about the exception condition

- Results in substantial savings of network capacity and agent processing time
Overhead of Network Management System

- The number of CPU cycles
  - Management application program
  - SNMP protocol
    - constructs a request packet
    - the number of control bytes supplied by the protocol stack layers

- Large storage for management stations and management agents

- The amount of traffic generated by network management packets
Proxies

- SNMP
  - Requires all agents, management stations to support UDP and IP

- Proxy configuration
  - Excludes devices that do not support UDP and IP
  - Devices do not implement SNMP
  - **Proxy agent** converts each query into the management protocol that the device is using
  - Agent receives a reply to a query, it passes that reply back to the management station
Outline

- Background
- Basic Concepts
- Summary
Summary

- Simple Network Management Protocol
  - Was designed to be an easily implemented, basic NM tool
  - Becomes the dominant standardized NM scheme

- Manager
  - Is a software module in a NMS responsible for managing part or all of the configuration on behalf of NM applications and users

- Agent
  - Is a software module in a managed device responsible for maintaining local management information and delivering that information to a manager via SNMP

- Management information exchange can be initiated by the manager (via polling) or by the agent (via a trap)

- A proxy is an SNMP agent that maintains information on behalf of one or more non-SNMP devices