# SNMP - overview

Based on: W.Stallings – Data and Computer Communications

# Network Management - SNMP

- Simple Network Management Protocol (not so simple …)
- Dominant standardized network management scheme in use today
- More complexity makes failure more likely
- Require automatic network management tools
- Standards required to allow multi-vendor networks
- SNMP set of standards **provides a framework** for the definition of **management information** along with a protocol for the **exchange** of that information
- Covering:
  - Services
  - Protocols
  - Management information base (MIB)

# Network Management Systems

- Collection of tools for network management
- Single operator interface
- Powerful, user friendly command set
- Performing most or all management tasks
- Minimal amount of separate equipment
  - i.e. use existing equipment
- View entire network as unified architecture
- Active elements provide regular feedback

# Key Elements

- Management station or manager
- Agent
- Management information base
- Network management protocol

# Management Station (manager)

- Stand alone system or part of shared system
- Interface for human network manager
- Set of management applications
  - Data analysis
  - Fault recovery
- Interface to monitor and control network
- an entity managing one or more agents from a remote place
- Translate manager's requirements into monitoring and control of remote elements
- Contains Data base of network management information extracted from managed entities
- A management information exchange can be initiated by the manager (via polling) or by the agent (via a trap)

# Agent

- Hosts, bridges, hubs, routers equipped with agent software
- Agent software is a program which communicates with the Manager on one side and with Device or Application on the other side. It is a part of the Device or Application so that it can know everything about the Device or Application regularly
- Allow them to be managed from management station
- Respond to requests for information
- Respond to requests for action
- Asynchronously supply unsolicited information
- UDP ports, 161 and 162- the default ports reserved for SNMP. Agent listens for requests and replies to them over port 161 and reports asynchronous traps on port 162, unless instructed to use different ports
- SNMP accommodates resources that do not implement the SNMP software by means of proxies. A proxy is an SNMP agent that maintains information on behalf of one or more non-SNMP devices.

# Manager – agent Communications

Communications - via SNMP Protocol Data Units (PDUs) that are encapsulated in UDP packets

Kinds of operations permitted between managers and agents:

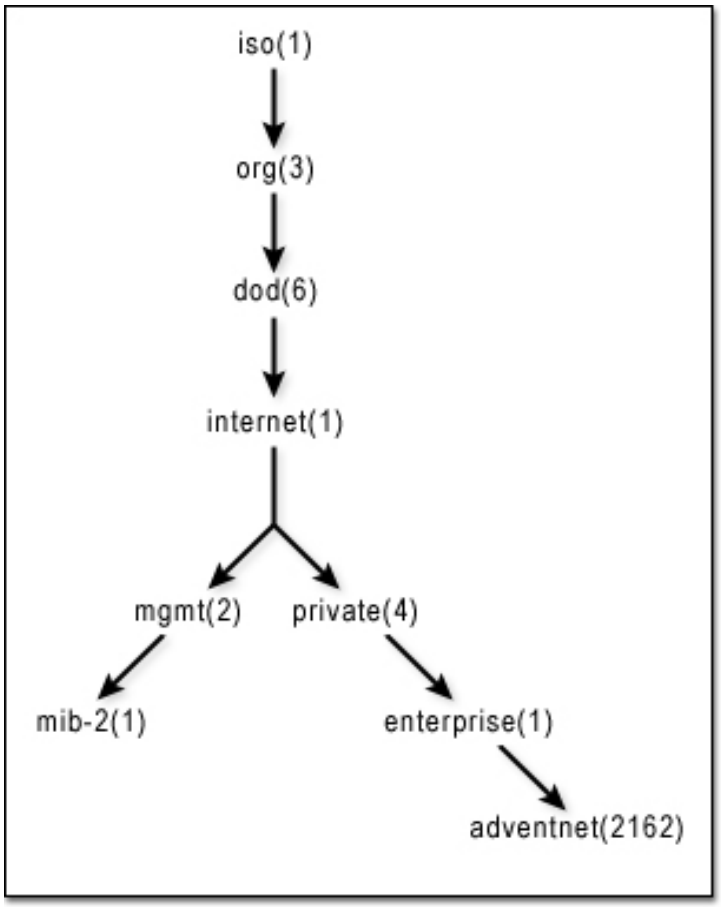
- The manager can perform a **get** (or read) to obtain information from the agent about an attribute of a managed object.
- The manager can perform a get-next to do the same for the next object in the tree of objects on the managed device.
- The manager can perform a get-bulk to obtain information about a group of data from the agent. This is not possible in the case of SNMP V1.
- The manager can perform a **set** (or write) to set the value of an attribute of a managed object.
- The agent can send a **trap**, or asynchronous notification, to the manager telling it about some event on the managed device

# Management Information Base (MIB)

- Representation of network resources as objects
- MIB is a document about the device or the application
- Each object is a variable representing one aspect of managed object
- MIB is collection of access points at agent for management of station
- Objects standardized across class of system
  - Bridge, router etc.

# MIB structure

For any application or device to be remotely managed, need to write a MIB which will have kinds of information, such as: what are the variables that should be published outside (to the Manager), what is the use of each variable, what each value in the variable represents




Each variable is assigned a unique identifier in SNMP that is called an object identifier (OID). Object identifier is a unique ID, maintained all over the world.

Format of OID: a sequence of numbers with dots in between. There are two roots for object identifiers, they are iso (which is .1) and ccit (which starts with .0). Most object identifiers start with .1.3.6.1 (where 1 = iso, 3 = org, 6 = dod, 1 = internet). From internet, there are two branches, mgmt and private.

All standard MIBs (approved by the Internet Activities Board (IAB)) reside under mgmt

MIBs defined unilaterally by equipment and software vendors are initially defined as private MIBs under private.enterprise

# Network Management Protocol

- Link between management station and agent
- TCP/IP uses SNMP
- OSI uses Common Management Information Protocol (CMIP)
- SNMPv2 (enhanced SNMP) for OSI and TCP/IP

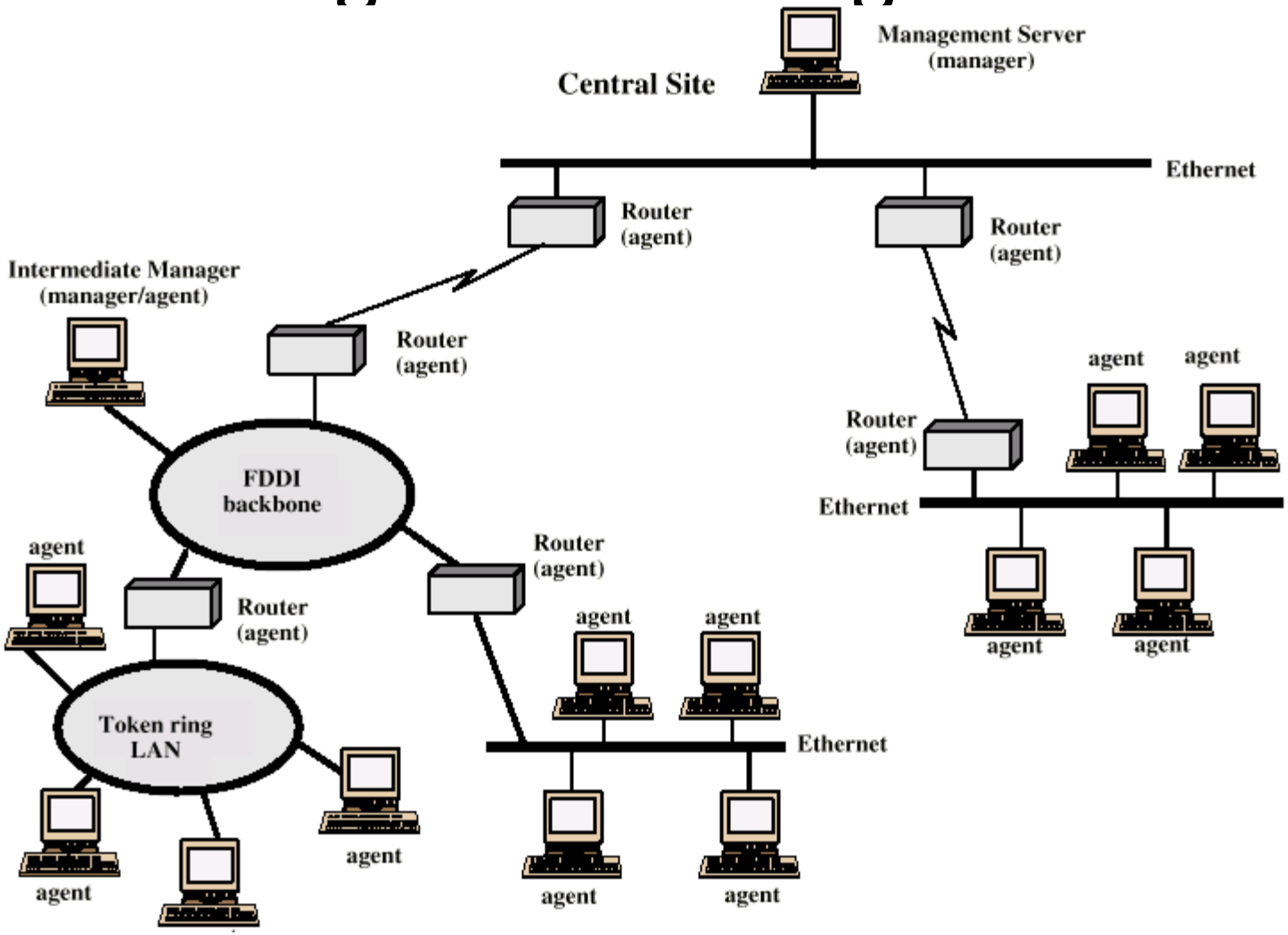
# Protocol Capabilities

- Get
- Set
- Notify (trap notification)

# Management Layout

- May be centralized in simple network
- May be distributed in large, complex network
  - Multiple management servers
  - Each manages pool of agents
  - Management may be delegated to intermediate manager

# Example of Distributed Network Management Configuration



# SNMP v1

- August 1988 SNMP specification issued
- Stand alone management stations and bridges, routers workstations etc supplied with agents
- Defines limited, easily implemented MIB of scalar variables and two dimensional tables
- Streamlined protocol
- Limited functionality
- Lack of security
- SNMP v2 1993, revised 1996
  - RFC 1901-1908

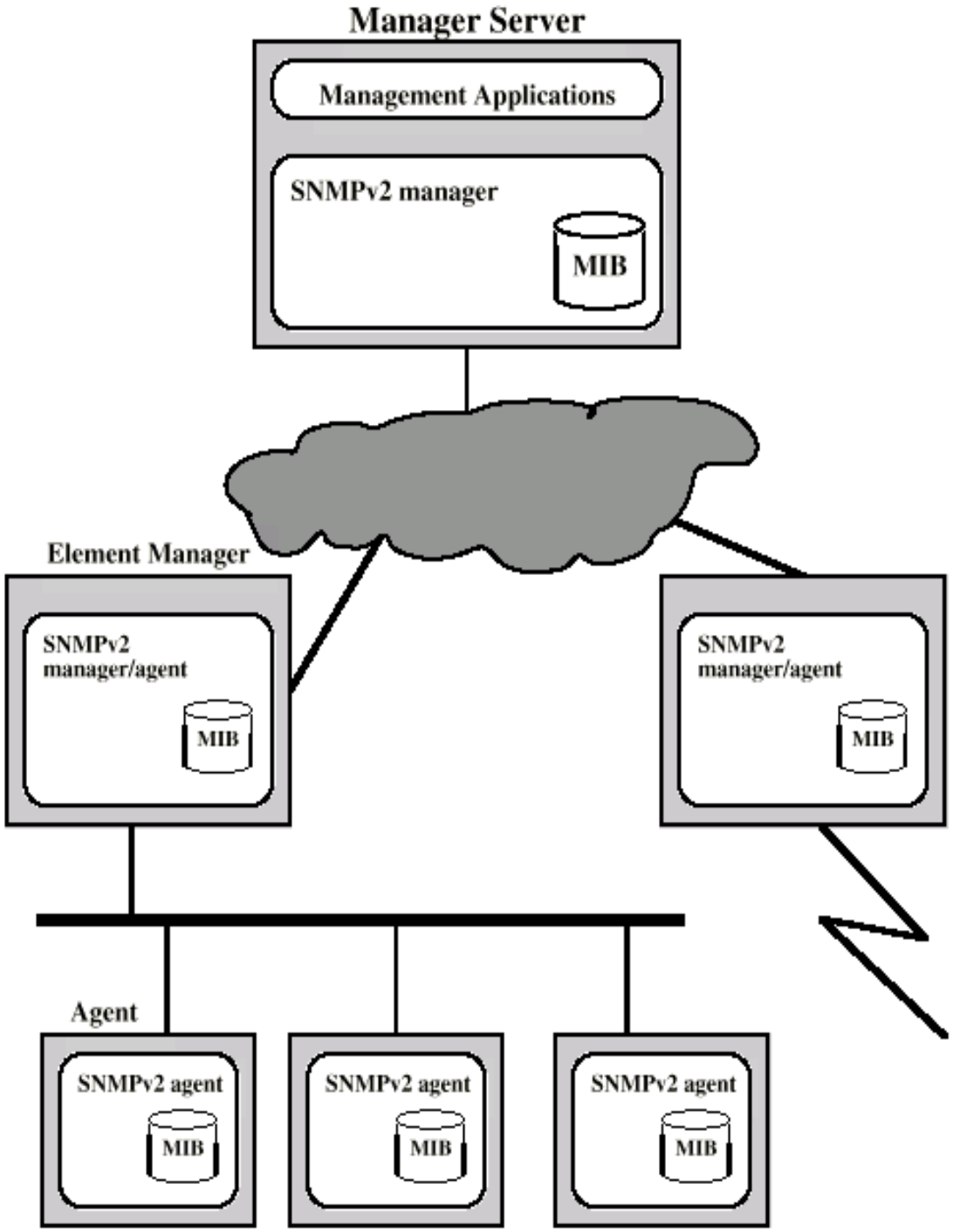
# SNMP v2 (1)

- Framework on which network management applications can be built
  - e.g fault management, performance monitoring, accounting
- Protocol used to exchange management information
- Each player maintains local MIB
  - Structure defined in standard
- At least one system responsible for management
  - Houses management applications

# SNPM v2 (2)

- Support central or distributed management
- In distributes system, some elements operate as manager and agent
- Exchanges use SNMP v2 protocol
  - Simple request/response protocol
  - Typically uses UDP
    - Ongoing reliable connection not required
    - Reduces management overhead

# SNMP v2 Managed Configuration



# Structure of Management Information

- Defines general framework with which MIB defined and constructed
- Identifies data types
- How resources are represented and named
- Encourages simplicity and extensibility
- Scalars and two dimensional arrays of scalars (tables) only

# Protocol Operation

- Exchange of messages
- Outer message header deals with security
- Seven types of PDU

# SNMP v2 PDU Formats

| PDU type | request-id | 0 | 0 | variable-bindings |
|---|---|---|---|---|

(a) GetRequest-PDU, GetNextRequest-PDU, SetRequest-PDU, SNMPv2-Trap-PDU, InformRequest-PDU

| PDU type | request-id | error-status | error-index | variable-bindings |
|---|---|---|---|---|

(b) Response-PDU

| PDU type | request-id | non-repeaters | max-repetitions | variable-bindings |
|---|---|---|---|---|

(c) GetBulkRequest-PDU

| name1 | value1 | name2 | value2 | • • • | name*n* | value*n* |
|---|---|---|---|---|---|---|

(d) variable-bindings

# SNMP v3

- Addresses security issues of SNMP v1/2
- RFC 2570-2575
- Proposed standard January 1998
- Defines overall architecture and security capability
- To be used with SNMP v2

# SNMP v3 Services

- Authentication
  - Part of User-Based Security (UBS)
  - Assures that message:
    - Came from identified source
    - Has not been altered
    - Has not been delayed or replayed
- Privacy
  - Encrypted messages using DES
- Access control
  - Can configure agents to provide a number of levels of access to MIB
  - Access to information
  - Limit operations