MONASH University
Information Technology

FIT3031 INFORMATION & NETWORK SECURITY

MONASH University
Information Technology

FIT3031 INFORMATION & NETWORK SECURITY

Lecture 12
Network Management

Unit Objectives

- ✓ OSI security architecture
  - **common security standards and protocols for network security applications**
  - **common information risks and requirements**
- ✓ operation of private key encryption techniques
- ✓ operation of public encryption techniques
- ✓ concepts and techniques for digital signatures, authentication and non-repudiation
- ✓ security threats of web servers, and their possible countermeasures
- ✓ Wireless Network Security Issues
- ✓ security threats of email systems and their possible countermeasures
- ✓ IP security
- ✓ intrusion detection techniques for security purpose
- ✓ risk of malicious software, virus and worm threats, and countermeasures
- ✓ firewall deployment and configuration to enhance protection of information assets
- ✓ network management protocol for security purpose

Lecture 12 Objective

- **On completion of this session you should:**
  - Understand the need for network management
  - Describe the OSI framework for network management
  - Understand the basic principles of SNMP protocol
  - Be familiar with the operation of SNMPv1.
  - Analyze centralized vs. distributed management
  - Understand the role of proxy agent
  - Be familiar with the operation of SNMPv2.
  - Discuss the lack of security in SNMPv1 and SNMPv2
  - Discuss how security issues have been addressed in SNMPv3

Lecture 12: Outline

- **Network management**
- **Simple Network management Protocol (SNMP)**
  - SNMPv1 protocol
  - SNMPv2 protocol
  - SNMPv1 & v2 security
- **SNMPv3 Security**

Complexity of Large Networks

- **Growing tendency to build larger and more complex networks**
  - organizations can support more and more users and applications
- **But problems are:**
  - managing a network becomes a formidable task as the network grows bigger and bigger
  - more things can go wrong
  - any interruption of the services will decrease productivity
- **Automated network management tools are necessary to manage such complex system**

Why Network Management?

- **Ideally, networks would not need management**
- **However:**
  - Parts break down
    > needs **F**ault management
  - changes are made over time
    > needs **C**onfiguration management
  - Somebody has to pay
    > needs **A**ccounting management
  - Performance needs improvement
    > needs **P**erformance management
  - Security violation occurs
    > needs **S**ecurity management

FCAPS

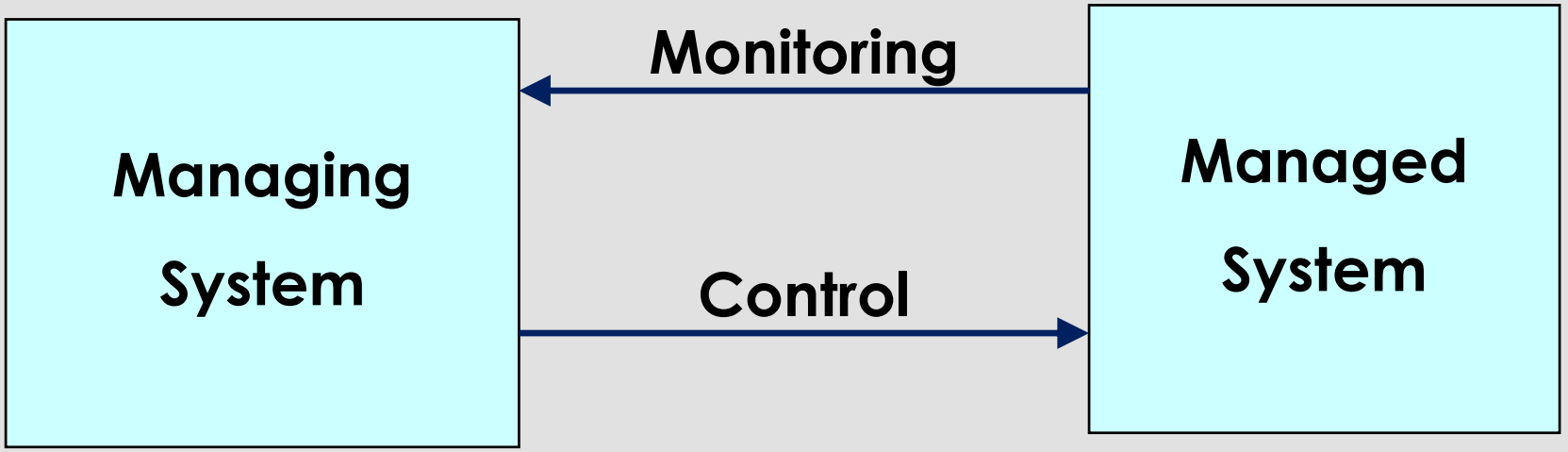
Network Management – OSI FCAPS Model

- **OSI FCAPS model was developed as a framework for network management**
  - Fault management (F): detects, isolates and corrects faults in network operation
  - Configuration management (C): Records and maintains network configuration and updates to ensure normal network operations
  - Accounting management (A): User management, administration, and billing
  - Performance management (P): collects and analyzes traffic data (e.g., link utilization), provides reliable and quality network services
  - Security Management (S): setups and reports various security mechanism via thresholds and alarms; provides protection against all security threats to network resources, its services and data

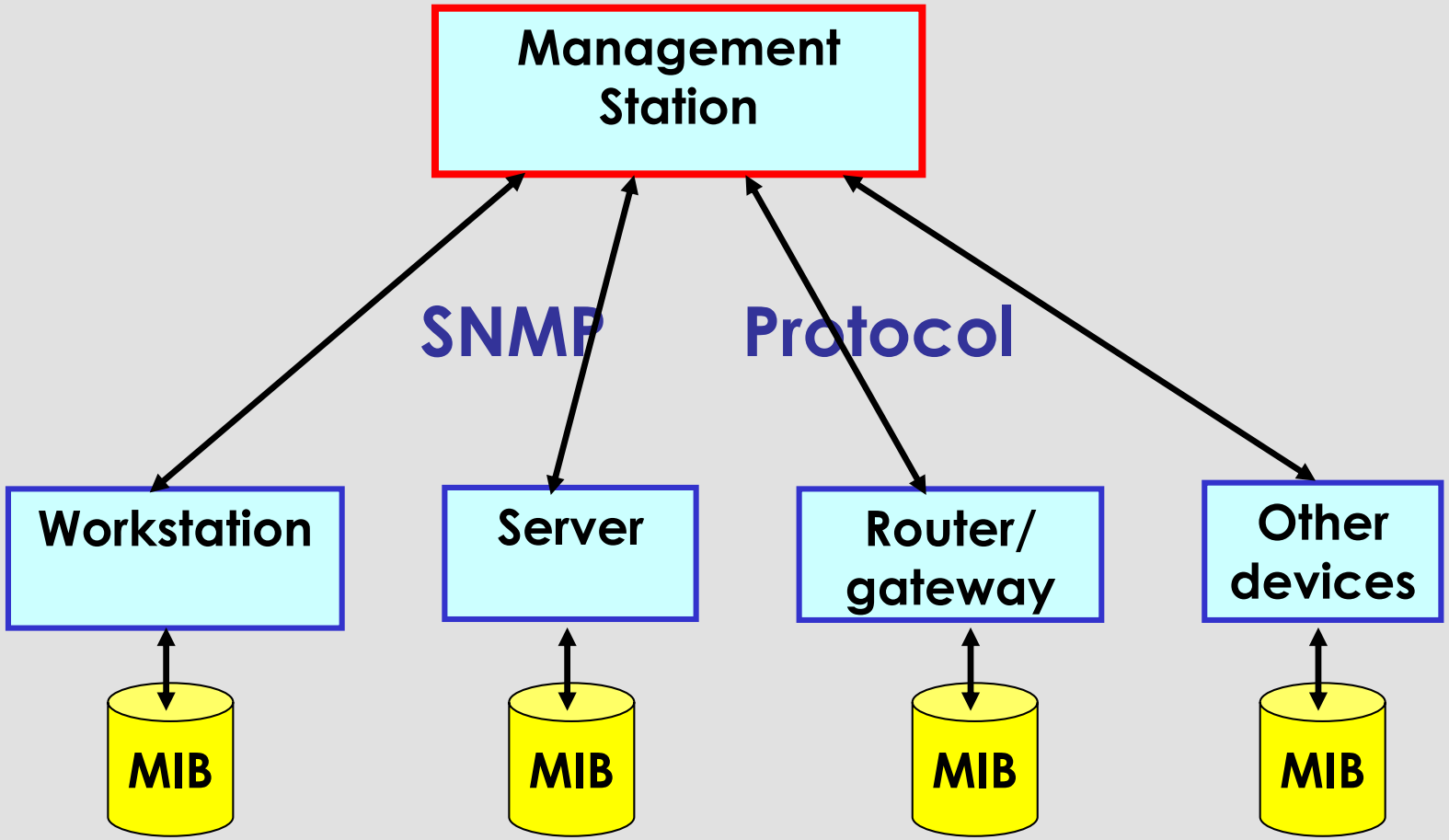
Simple Network Management Protocol (SNMP)

- **FCAPS management architecture was not widely adopted due to slow deployment of OSI protocol suit**
- **Meanwhile Internet Protocol (IP) gained wide acceptance due to the success of the Internet**
- **Simple Network Management Protocol (SNMP) is based on IP**

Management Architecture - Concept

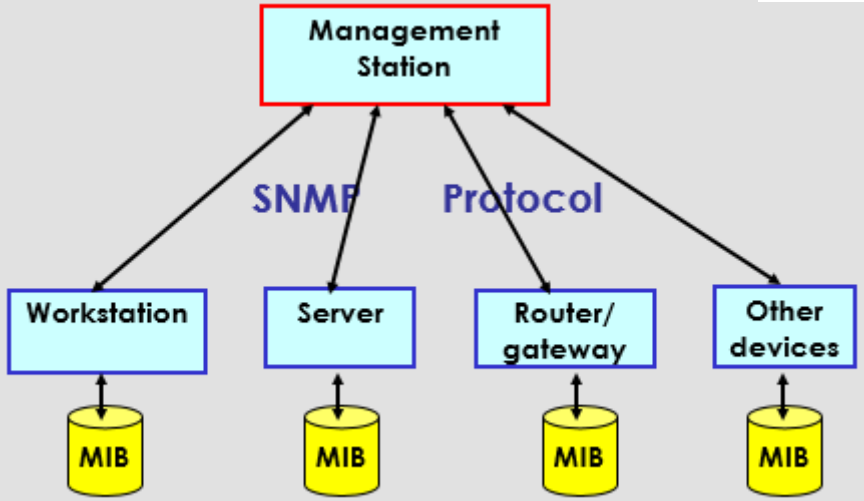


SNMP Architecture



SNMP Protocol …

- **An SNMP architecture has four major components:**
  - Management stations (**manager**)
  - Management agent (**agent**)
  - Management Information Base (**MIB**)
  - Network Management protocol (**SNMP**)
    - > Get, Set, Trap and Notify



SNMP Protocol …

- **Management station (manager)**
  - issues queries and commands to management agents
  - receives and processes their responses
  - serves as an interface for the **human network manager** to **monitor remote devices**
- **Management agents (agents)**
  - these are the devices on the network that are being monitored
  - have the **SNMP agent software** installed
  - respond to manager's query and send alerts

SNMP Protocol …

- **Management Information Base (MIB)**
  - collection of variables that can be examined or altered by manager stations through agents
  - variables represents a set of objects like network address, state information, counters, statistics, etc.
  - management station can change configuration settings of agents by modifying specific objects
- **Network Management protocol**
  - The SNMP protocol for communication between the manager and remote agent

SNMP Commands

- **SNMP has three major types of commands:**
  - **GET**
    - > Management station issues GET command to retrieve information from MIB
    - > Example: server reports number of users currently logged in
  - **SET**
    - > management station issues SET command to alter a variable's value in agent's MIB
  - **TRAP**
    - > agents can issue only trap command
    - > a trap command is an alert sent by an agent to a management station
    - > example: change in the availability status of a communication link, collision rate above a certain threshold

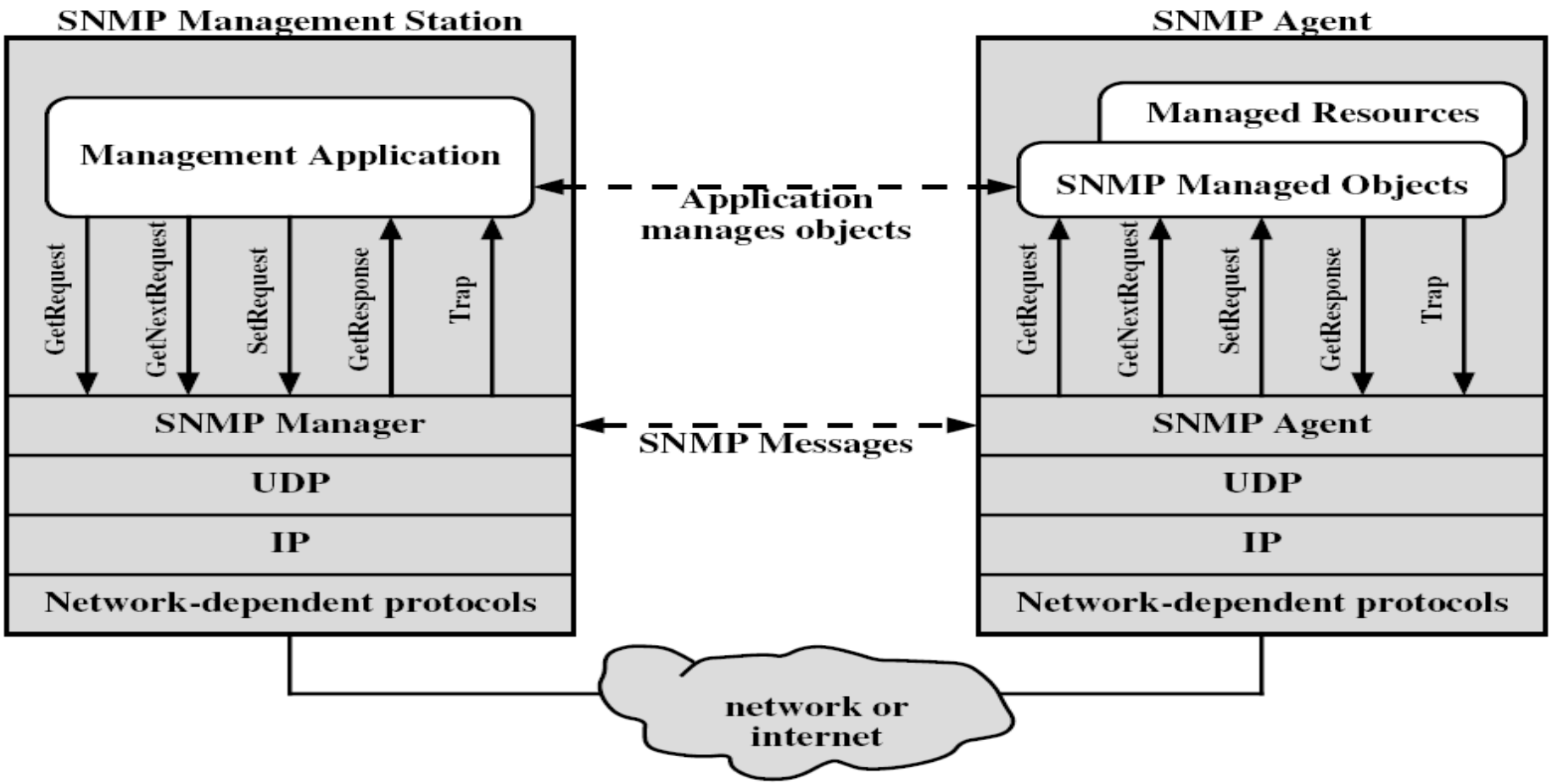
SNMP Protocol

- **SNMP is a connectionless protocol**
  - operates over the **UDP** (User Datagram Protocol in Transport layer of TCP/IP suite)
  - **No ongoing connections** are maintained between a management station and its agents
- **Instead, each exchange is a separate transaction between a management station and an agent**

SNMP v.1

- **Management station and each agent must implement SNMP, UDP and IP**
- **Commands from management station:**
  - **GetRequest** : request to retrieve a specific MIB variable
  - **GetNextRequest** : request to retrieve next variable in the table
  - **SetRequest** : request to alter an MIB variable
- **Response from agent:**
  - **Get-response** : response to get-request or get-next-request
- **Notification:**
  - **Trap** : notification of an event from agent to manager

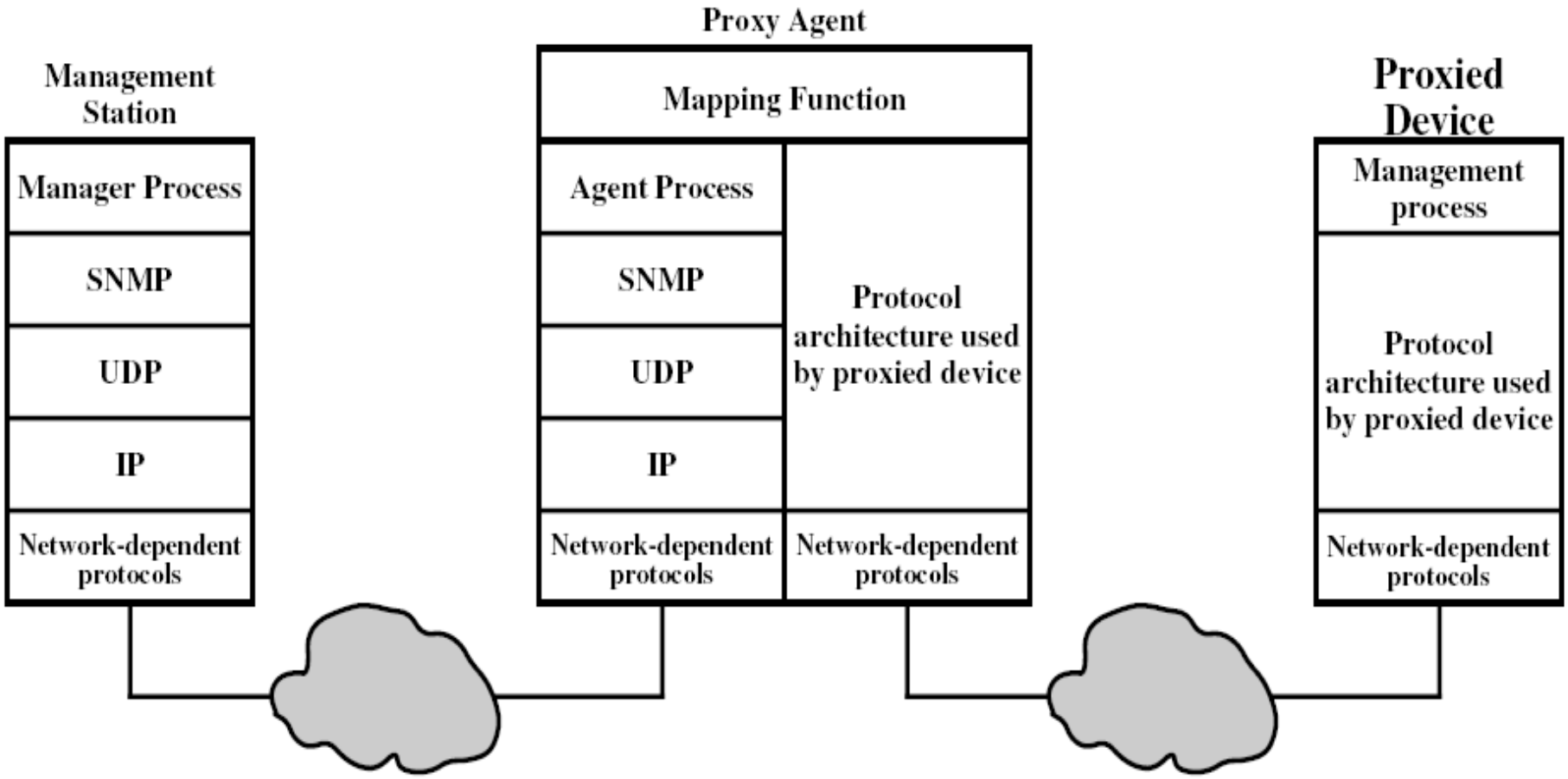
SNMP v.1: Protocol Context



Proxy Agents

- **Problems with SNMP deployment**
  - **not all the devices in the network necessarily implement TCP/IP protocol suite**
    > for example: devices like bridges and modems
  - small system that supports TCP/IP, but may be over burdened with SNMP, agent logic and MIB
- **Solution is to deploy proxy agents**
  - an SNMP agent acts on behave of proxied devices
- **Proxy agent do the followings:**
  - management agent sends query to proxy agent
  - proxy agent converts each query so that it is interpretable by the proxied device
  - proxy agent receives reply from the device, converts it and sends to the management station

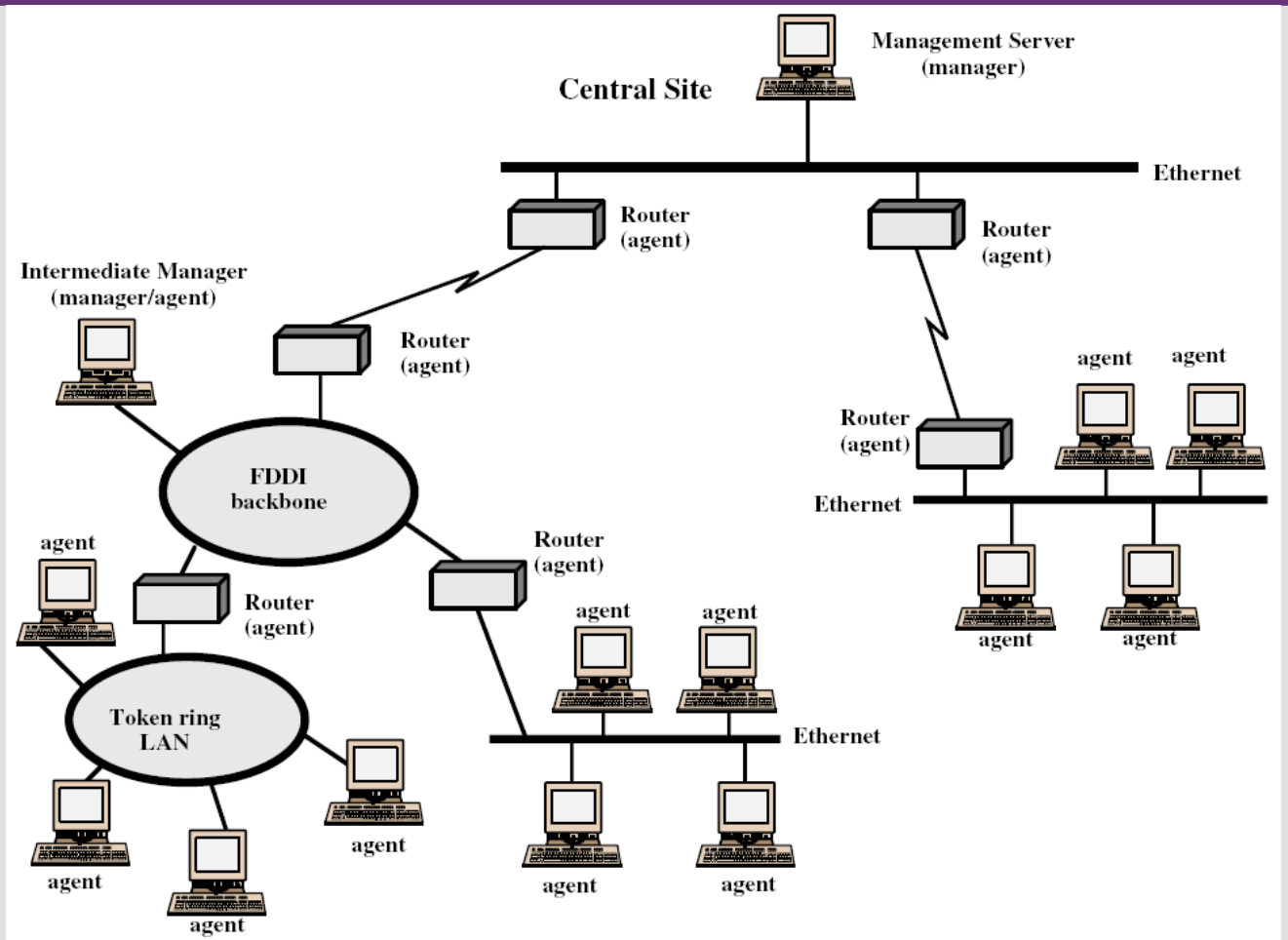
Proxy Agent


Proxy Agent
Management Station
Mapping Function
Proxied Device
Manager Process
Agent Process
Management process
SNMP
SNMP
Protocol architecture used by proxied device
UDP
UDP
Protocol architecture used by proxied device
IP
IP
Network-dependent protocols
Network-dependent protocols
Network-dependent protocols

SNMP v.2

- **SNMPv1 supports only a centralized network management system**
  - one management station and the rest are agents
- **Such a centralized system cannot cope well when the network grows bigger and carries high traffic**
- **The solution is a decentralized scheme**
  - multiple top level management stations (management server)
    > each manages a portion of the total pool of agents
  - some devices play a dual role
    > as an intermediate level manager managing a number of agents
    > as an agent being monitored by a higher level manager
- **SNMPv2 supports either a highly centralized or a distributed network management system**
- **Any device that implements SNMP v.1 but not v.2, can be managed by a proxy that implements SNMPv.2**

Distributed Network Management



SNMP v.2 …

- **To enhance functionality, SNMPv2 uses two additional commands:**
  - **GetBulkRequest :** request to retrieve large block of data at a time from MIB
  - **InformRequest :** notification of event from manager to manager
- **Get command is atomic in SNMPv1 but non-atomic in SNMPv2**
- **SNMPv2 allows the use of TCP for reliable service (UDP is not reliable)**

SNMP v1 and v2

- **Trap – an unsolicited message (reporting an alarm condition)**
- **SNMPv1 is ”connectionless” since it utilizes UDP (rather than TCP) as the transport layer protocol.**
- **SNMPv2 allows the use of TCP for ”reliable, connection-oriented” service.**

SNMP Community

- **SNMP provides only rudimentary security through the concept of community**
- **Each managed agent must be able to control the use of its MIB by a number of distinct management stations**
- **There are three aspects in this control**
  - **Authentication service**: authentication of manager
  - **Access policy**: different privileges to different managers
  - **Proxy service :** implementing the two functions above for the other proxied managed systems
- **SNMP provides only a primitive security through the concept of a community**

Authentication Services: SNMP community

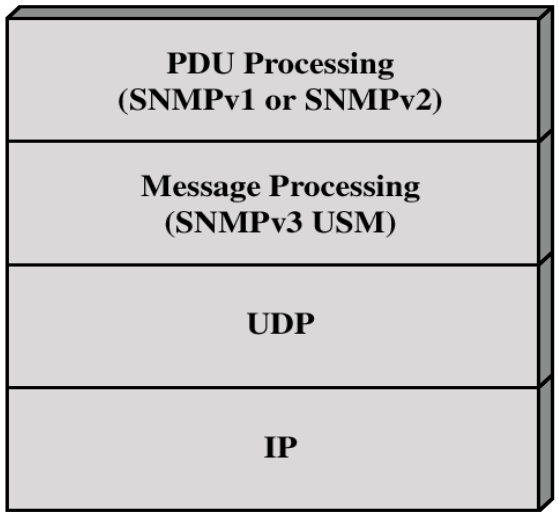
- **SNMP provides for only a trivial scheme for authentication**
- **Every message from a management station includes a community name**
  - It functions like a password
- **With this limited form of authentication, many network managers will be reluctant to allow anything other than network monitoring (GET and TRAP)**
- **Network control by SET command is clearly a more sensitive area**
- **May involve the use of encryption/decryption for more secure authentication functions**

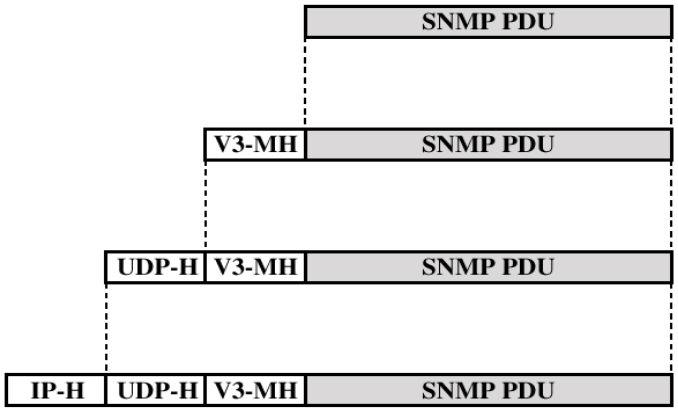
Access Control: SNMP community

- **Two aspects**
  - **SNMP MIB view**: a subset of the objects within an MIB
    - > different MIB views may be defined for each community
    - > Objects in a view need not belong to a single subtree of the MIB
  - **SNMP access mode**: an element of the set {READ-ONLY, READ-WRITE}
    - > an access mode is defined for each community
- **The combination of an MIB view and an access mode is called a community profile**
  - **A community profile** thus consists of a defined subset of the MIB at the agent,
  - plus an **access mode**

SNMPv3

- **SNMPv3 defines a security capability to be used in conjunction with SNMPv1 or v2**





IP-H = IP header
UDP-H = UDP header
V3-MH = SNMPv3 message header
PDU = Protocol data unit

SNMP Manager

- **Command Generator**
  - monitors and manipulates data at remote agents, e.g., issues GET, SET commands
- **Notification Generator/Receiver**
  - Initiates/processes asynchronous messages, like InformRequest, Trap
- **Dispatcher**
  - acts as a traffic manager
  - determines the types of message processing required and sends to the appropriate message processing module
- **Message Processing subsystem**
  - sends and receives message to and from the security subsystem and adds/processes appropriate header
- **Security Subsystem**
  - Performs authentication and encryption functions
  - adds MAC and performs encryption on outgoing message
  - checks MAC and performs decryption on incoming message

SNMP Agent

- **command responder**
  - provide access to management data. These applications respond to incoming requests by retrieving and/or setting managed objects and then issuing a Response PDU
- **notification generator**
  - initiates asynchronous messages; in the case of a traditional agent, the SNMPv2-Trap or SNMPv1 Trap PDU is used for this application
- **Proxy forwarder**
  - forwards messages between entities.
- **Access Control Subsystem – VACM**
  - authorization services to control access to MIBs

SNMPv3 Security

- **SNMPv3 delivers enhancement in three key areas**
  - Security
  - efficiency and
  - scalability
- **Authentication and privacy**
  - User-Based Security Model (USM)
- **Access control**
  - View-Based Access Control Model (VACM)

User Security Model (USM)

- **Designed to secure against:**
  - Modification of information
  - Masquerade
  - Message stream modification
  - Disclosure
- **Not intended to secure against:**
  - Denial of Service (DoS attack)
  - Traffic analysis

View-Based Access Control Model (VACM)

- **VACM determines whether access to a managed object should be allowed**
- **Make use of an MIB that:**
  - Defines the access control policy for this agent.
  - Makes it possible for remote configuration to be used.
- **Granular access control is possible**
  - configure agents to provide different levels of access, e.g.,
    - > only one manager will be able to view and update configuration parameters,
    - > the rest of managers will be able to view only performance relates statistics

Further Reading

- **Study Guide 12**
- **Chapter 12 of the textbook: Network Security Essentials- Application & Standards" by William Stallings 5th Edition, Prentice Hall, 2013**
- **Additional resources for this week**

- **Acknowledgement: part of the materials presented in the slides was developed with the help of Instructor's Manual and other resources made available by the author of the textbook.**