7 : Network Management

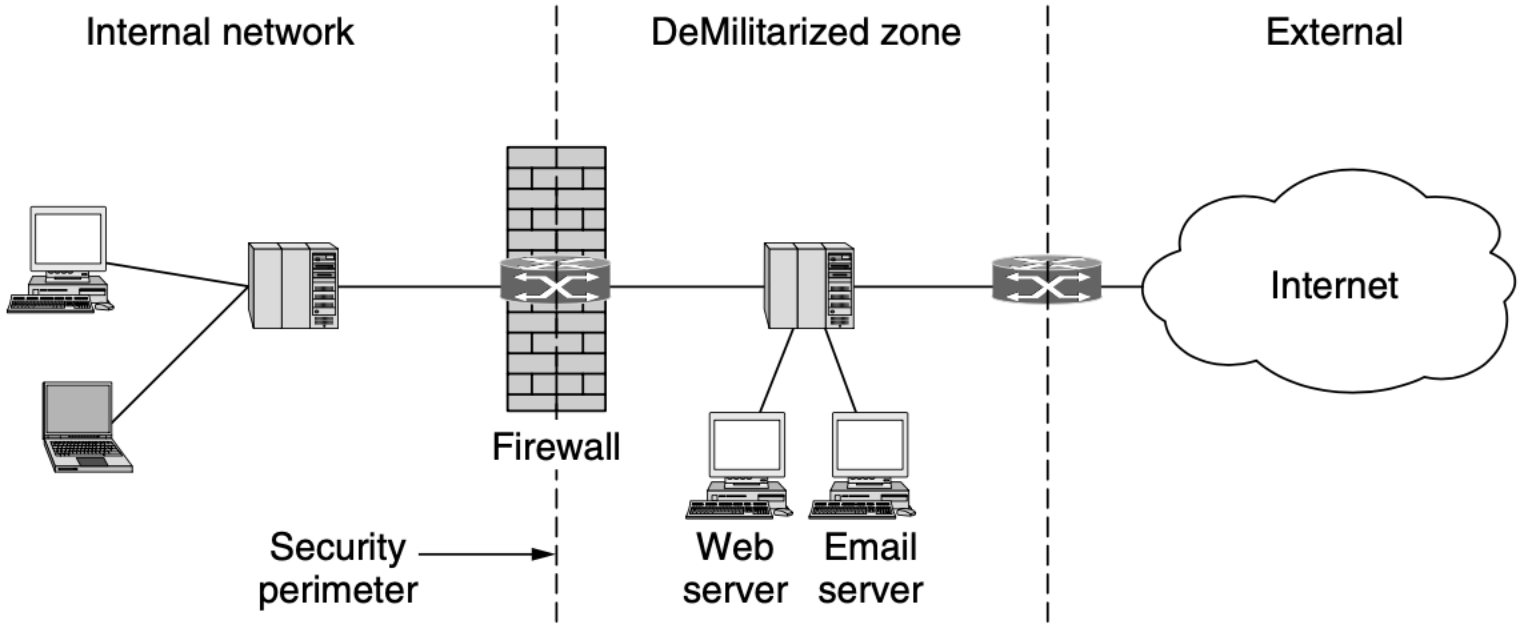
IT 4506 – Computer Networks

Level II - Semester 4

7.1 Firewalls [Ref 01: Section 8.6.2]

- **Firewall** is a perimeter protection device.
- Firewalls are placed in such a way that forces everyone entering or leaving the network to pass over it.
- A Firewall could use different mechanisms to filter traffic mostly rule based.

7.1 Firewalls



7.1 Firewalls

A packet filter:

- Use both whitelisting and blacklisting approaches:
  - Whitelisting: block all and only allow what is acceptable
  - Blacklisting: block what is not accepted and allow others
- The filtering criterion is typically given as rules with a combination of IP addresses and ports.
  - Source IP, Destination IP, source port, destination port
- Ports indicate which service is desired.
  - For example, TCP port 25 is for mail, and TCP port 80 is for HTTP

7.1 Firewalls

DMZ (DeMilitarized Zone) :

- DMZ lies outside of the security perimeter
- DMZ makes sure those who need any services are served outside the perimeter
- There could be specific rules for internal computers to connect to the servers in DMZ for management purposes.

7.1 Firewalls

Stateful Firewalls:

- The firewall keep track of connections between two computers rather than inspecting individual packets.
- This allows the firewall to impose rules more effectively: for example, allowing HTTP traffic to internal network only if the connection request was made by an internal user.

7.1 Firewalls

Application-level gateways:

- Firewall can see application-level protocols to check a particular application's activity.
- With this capability
  - it is possible to distinguish HTTP traffic used for Web browsing from HTTP traffic used for peer-to-peer file sharing
  - Prevent sensitive documents from being emailed outside of the company

7.1 Firewalls

Doesn’t solve all the issues:

- intruder outside the firewall can put in false source addresses to bypass this check
- Only provide a single perimeter of defense thus layered defense mechanisms are required
- May not be able to prevent all the DoS (Denial of Service) or DDoS (Distributed Denial of Service) attacks.

7.2 Virtual Private Networks (VPN)

[**Ref 01: Section 8.6.3**]

- Private Network
  - A network built up from company computers and leased telephone lines is called a private network
  - Intruders have to physically wiretap the lines to break in
  - However, these networks are not scalable and very expensive

- Virtual Private Network
  - VPNs are overlay networks on top of public networks but with most of the proper- ties of private networks
  - Example:
    - VPNs set up by ISP : MPLS
    - VPNs set up by the company itself : IPSec

7.3 Network Management Requirements

- Networks and distributed processing systems are important for most organizations / enterprises
- When the business grows, so as the network and distributed processing systems
- When a network scales:
  - Network become complex
  - Increase of the number of indispensable network resources and applications
  - There are more things that could go wrong
  - Performance of a single component may affect larger segment of the business

7.3 Network Management Requirements

- Managing a large network needs automated network management tools
- The automated network management tools need to be able to:
  - communicate with different devices from multiple vendors
    - Example: A network may have network switches from different vendors such as CISCO, HP, DELL, etc.
  - centralize coordination of network components
    - Example: Monitoring the corporate network using a central dashboard, pushing security updates remotely to devices, etc.

7.3 Network Management Requirements

- ISO Network Management Framework provides a good way of understanding Network Management Requirements.
- It identifies five (5) ISO Management Functional Areas
  - Fault Management
  - Accounting Management
  - Configuration Management
  - Performance Management
  - Security Management

7.3.1 Fault Management

The OSI Management Framework document defines Fault Management as follows:

"Fault management encompasses fault detection, isolation and correction of abnormal operation of the OSI Environment. Faults cause open systems to fail to meet their operational objectives and they may be persistent or transient. Faults manifest themselves as particular events (e.g., errors) in the operation of an open system. Error event detection provides a capability to recognize faults. Fault management includes functions to:

- *maintain and examine error logs;*
- *accept and act upon error detection notifications;*
- *trace and identify faults;*
- *carry out sequences of diagnostic tests;*
- *correct faults*."

7.3.1 Fault Management

- Faults are to be distinguished from errors
  - E.g. CRC errors on communication lines), may occur occasionally and are not normally considered to be faults. However, excessive errors exceeding a certain threshold would indicate a fault.

7.3.1 Fault Management

- User expectation on fault management
  - Reliable problem resolution :
    - *same fault should not be happening again and again*
  - Quality network services delivered on a consistent basis :
    - *attention, taking actions, notifications and reporting, and delivery*
  - Problem to be corrected immediately :
    - *using effective fault tolerance mechanisms*
  - Keep informed of the network status , including both scheduled and unscheduled maintenance
  - Notified of the approximate time that the service will be resumed

7.3.1 Fault Management

Functional requirements of a Network Management System (NMS) with respect to Fault Management

- Detecting and Reporting Faults
  - NMS should provide mechanisms to allow its users to log events and errors
  - NMS should be able to monitor the specified events or errors.
  - NMS should be able to identify faults by analizing errors and/or events
  - NMS should be able to generate event reports and to send them to the NMS users
  - NMS should be able to broadcast or multicast notifications

7.3.1 Fault Management

Functional requirements of a Network Management System (NMS) with respect to Fault Management

- Diagnosis of Faults
  - NMS should allow its users to activate predefined diagnostic and testing procedures
  - NMS users should be able to request fault related data, such as dumps, statistics blocks and status information
  - NMS should provide the capabilities to analyze fault related data (may be limited to certain types depending on the implementations)
  - NMS should provide standard mechanisms to exchange information with other analyzing platforms

7.3.1 Fault Management

Functional requirements of a Network Management System (NMS) with respect to Fault Management

- Correction of Faults
  - NMS should allow its users to change or reset resource attribute values, take components or lines down, put components or lines back in service, or request reconfiguration of all or part of the network.
  - NMS should provide mechanisms to track network operations following fault correction attempts to ensure that the faulty situations are corrected

7.3.1 Fault Management

Functional requirements of a Network Management System (NMS) with respect to Fault Management

- Robust Fault Management
  - NMS should provide the capabilities to have redundant fault manager systems to increase the robustness of the fault management system.

7.3.2 Accounting Management

The OSI Management Framework document defines Accounting Management as follows:

"Accounting management enables charges to be established for the use of resources in the Open System Interconnection Environment (OSIE), and for costs to be identified for the use of those resources. Accounting management includes functions to:

- *inform users of costs incurred or resources consumed;*
- *enable accounting limits to be set and tariff schedules to be associated with the use of resources;*
- *enable costs to be combined where multiple resources are invoked to achieve a given communication objective.*"

7.3.2 Accounting Management

- User expectation on accounting management
  - NMS end users and administrators need to be able to specify the kinds of accounting information to be recorded at various nodes, the desired interval between sending the recorded information to higher level management nodes, and the algorithms to be used in calculating and reporting the accounting information.
  - In order to limit access to accounting information, the NMS must provide the capability to verify user's authorization to access and manipulate that information

7.3.2 Accounting Management

Functional requirements of a Network Management System (NMS) with respect to Accounting Management

- The Ability to Record and Generate Accounting Information
  - The NMS must allow its users to specify the accounting information to be collected as well as the duration of the collection period, or the criteria to be used to determine the duration of the collection period.
  - Mechanisms are needed for the NMS through layer management entities or , the layer entities, to record and/or collect user distinguishable accounting information, and to generate accounting messages.

7.3.2 Accounting Management

Functional requirements of a Network Management System (NMS) with respect to Accounting Management

- The Ability to Control the Storage of and Access to Accounting Information
  - The NMS must provide standard procedures to retrieve and store accounting information
  - Access to accounting information is limited to authorized personnel only

7.3.2 Accounting Management

Functional requirements of a Network Management System (NMS) with respect to Accounting Management

- The Ability to Report Accounting Information
  - The NMS must be capable of reporting degree of resource usage and resource usage charges at an NMS user specified level.
  - Mechanisms are needed to allow NMS users to create and transmit selectively or broadcast accounting news such as network resource billing rate changes or accounting limit changes

7.3.2 Accounting Management

Functional requirements of a Network Management System (NMS) with respect to Accounting Management

- The Ability to Set and Modify Accounting Limits
  - The network manager must be able to read, set and change accounting limits for various groups of users.
  - Mechanisms are needed to allow the network manager to change the priorities assigned to the network users for access to network resources

7.3.2 Accounting Management

Functional requirements of a Network Management System (NMS) with respect to Accounting Management

- The Ability to Define Accounting Metrics
  - Time – minutes, hours, etc.
  - Transmission speed – Gbps, etc.
  - Storage capacity – MB, GB, TB
  - Etc.

7.3.3 Configuration Management

The OSI Management Framework document defines Configuration Management as follows:

"Configuration identifies, exercises control over, collects data from and provides data to open systems for the purpose of preparing for, initializing, starting, providing for the continuous operation of, and terminating interconnection services. Configuration management includes functions to:

- *set the parameters that control the routine operation of the open system;*
- *associate names with managed objects and sets of managed objects;*
- initialise and close down managed objects;
- *collect information on demand about the current condition of the open system;*
- *obtain announcements of significant changes in the condition of the open system;*
- *change the configuration of the open system.*"

7.3.3 Configuration Management

- User expectation on configuration management
  - NMS should provide start and shutdown operations of authorized network devices
  - Network administrator should have the capability to define the desired connectivity between the components that comprise the network
  - Authorized network administrators should be allowed to set / modify default configurations, load predefined configurations, export / save current configurations, etc.
  - Network users often need to be informed of the status of network resources and components in terms of configurations such as the current version of security update and available security patches

7.3.3 Configuration Management

Functional requirements of a Network Management System (NMS) with respect to Configuration Management

- Defining Resources and Attributes
  - Mechanisms are needed to allow the NMS users to specify resources and the attributes associated with a resource
  - The NMS users should be allowed to specify the range and type of values to which the specified resource attribute can be set

7.3.3 Configuration Management

Functional requirements of a Network Management System (NMS) with respect to Configuration Management

- Setting and Modifying Attribute Values
  - Mechanisms are needed to allow the NMS users to set and modify values of resource attributes
    - e.g., activate and deactivate ports
  - The NMS users require mechanisms to load predefined default attribute values

7.3.3 Configuration Management

Functional requirements of a Network Management System (NMS) with respect to Configuration Management

- Defining and Modifying Relationships
  - The NMS users must have the ability to specify relationships among network resources.
    - These relationships can take the form of a topology, a hierarchy, a physical or logical connection or a management domain (management domain is a set of resources that share a set of common attributes or a set of common resources that share the same management authority).
    - Mechanisms are needed to allow the NMS users to add, delete, and modify the relationships among network resources.

7.3.3 Configuration Management

Functional requirements of a Network Management System (NMS) with respect to Configuration Management

- Examining Attribute Values and Relationships
  - Mechanisms are needed to allow the NMS users to examine the attributes associated with the resources and the current values of these attributes
  - NMS must be able to keep track of configuration changes from which the existing network resources and attributes, their status, and relationships can be determined

7.3.3 Configuration Management

Functional requirements of a Network Management System (NMS) with respect to Configuration Management

- Distributing Software Throughout the Network
  - The NMS user needs mechanisms to examine, update and manage different versions of software and routing information

7.3.3 Configuration Management

Functional requirements of a Network Management System (NMS) with respect to Configuration Management

- Initializing and Terminating Network Operations
  - The NMS must provide mechanisms to allow its users to initialize and close down network, or subnetwork, operation.

7.3.3 Configuration Management

Functional requirements of a Network Management System (NMS) with respect to Configuration Management

- Verifying NMS Users' Authorization
  - Mechanisms are required to allow only authorized NMS users to perform various configuration functions.

7.3.3 Configuration Management

Functional requirements of a Network Management System (NMS) with respect to Configuration Management

- Reporting Configuration Status
  - Notification of configuration changes in resources and in relationships among resources must be available to the NMS users.
  - Mechanisms are needed to allow the NMS users to request and obtain configuration reports.

7.3.4 Performance Management

The OSI Management Framework document defines Performance Management as follows:

"Performance management enables the behaviour of resources in the OSIE and the effectiveness of communication activities to be evaluated. Performance management includes functions to:

- *gather statistical information;*
- *maintain and examine logs of system state histories;*
- *determine system performance under natural and artificial conditions;*
- *alter system modes of operation for the purpose of conducting performance management activities.*"

7.3.4 Performance Management

- Performance management deals with the quality and effectiveness of network communications. It involves the processes of quantifying, measuring, and reporting error levels, the responsiveness, availability, and utilization of individual network components and the network as a whole.
- performance management of computer networks includes two broad functional categories
  - **Monitoring** : Monitoring is the performance management function which tracks activities on the network.
  - **Tuning** : Tuning function enables performance management to make adjustments to improve network performance.

7.3.4 Performance Management

- Monitoring
  - Identify a set of resources to be monitored in order to assess performance levels.
  - associate appropriate metrics and their values with relevant network resources as indicators of different levels of performance.
  - For example, how many retransmissions on a Transport connection should be considered a performance problem requiring attention?

7.3.4 Performance Management

- Tuning – Performance control
  - Often this is accomplished by setting the necessary parameters for management of the traffic on the network.
  - Sometimes, however, additional network resources must be allocated or procured to solve the problem
  - If the problem is severe and unexpected, functions developed for fault management may be called to solve the problem.

7.3.4 Performance Management

- User expectation on performance management
  - Users often want to know information such as the average and worst case network response times for their applications, variability in response, and the reliability and availability of network services
  - Network managers need performance statistics to help them plan, manage, and maintain large networks. E.g. recognize potential bottlenecks before they cause problems
  - End users expect network resources to be managed in such a way as to consistently afford their applications minimal response time and minimal delays.
  - Users want to know that the network has adequate capacity to handle their loads under normal and adverse (e.g., heavily loaded) conditions.

7.3.4 Performance Management

Functional requirements of a Network Management System (NMS) with respect to Performance Management

- The Ability to Monitor Performance
  - The NMS needs to be able to monitor performance relevant events, measures and resources. This includes the facilities to allow NMS users to select the events, resources, or measures to be monitored, to specify the starting and stopping times for monitoring, to specify how frequently the monitored events, measures or resources are to be polled and recorded, and to specify the threshold level when a notification of performance abnormality or degradation should be given

7.3.4 Performance Management

Functional requirements of a Network Management System (NMS) with respect to Performance Management

- The Ability to Tune and Control Performance
  - NMS user needs mechanisms to execute predefined performance tests, and to collect test results for the purpose of diagnosing network performance anomalies and determining the appropriate performance tuning strategy.
  - NMS users need to be able to change resource allocation, to modify resource attributes and to set managed object attribute values in order to provide better performance or resolve performance problems

7.3.4 Performance Management

Functional requirements of a Network Management System (NMS) with respect to Performance Management

- The Ability to Evaluate Performance Tuning
  - The NMS users need the ability to keep track of the performance tuning results in terms of user specified measures or criteria.

7.3.4 Performance Management

Functional requirements of a Network Management System (NMS) with respect to Performance Management

- The Ability to Report on Performance Monitoring, Tuning, and Tracking
  - Notification of abnormal performance changes must be able to be spontaneously generated and sent to the NMS users who have previously requested such notification.
  - Mechanisms are needed for NMS users to request and obtain performance reports based on user specified criteria

7.3.4 Performance Management

Functional requirements of a Network Management System (NMS) with respect to Performance Management

- The Ability to Report on Performance Monitoring, Tuning, and Tracking
  - The NMS should have the ability to display routine snapshots of network performance in terms of those user specified measures
  - NMS should have the ability to compute and display statistics of standard metrics such as average, median, maximum, minimum, ratios and standard deviation.

7.3.4 Performance Management

Functional requirements of a Network Management System (NMS) with respect to Performance Management

- The Ability to Test Capacity and Special Conditions
  - In order to assure that capacity margins for network components are sufficient, it may be necessary to run tests to determine the effects of additional network loading under natural or artificial conditions

7.3.5 Security Management

The OSI Management Framework document defines Security Management as follows:

"The purpose of security management is to support the application of security policies by means of functions which include:

- *the creation, deletion and control of security services and mechanisms;*
- *the distribution of security-relevant information;*
- *the reporting of security-relevant events."*

7.3.5 Security Management

- There are three (03) types of management activities required to support security functions:
  - **Administration** : refers to both the gathering (reading) of system security management information and the addition, modification, or deletion (writing) of this system security management information.
  - **Detection** : refers to the auditing of system security operations which compose of four (04) components :
    - audit trail content specification,
    - audit trail analysis,
    - audit reporting, and
    - audit trail archiving.
  - **Recovery** : concerned with recovering from an actual, or suspected security attack.

7.3.5 Security Management

- OSI security goals that security management is intended to keep intact and properly functioning.
  - **Authentication** : The need to prove the identity of security subjects
  - **Access Control** : The need to verify authorization for access to some security object.
  - **Confidentiality** : The need to prevent disclosure of information.
  - **Integrity** : The need to detect various activities such as modification, loss, insertion, replay, or reflection of information.
  - **Non-repudiation** : registration of activity in order to be able to be certain that some activity has indeed occurred.

7.3.5 Security Management

Functional requirements of a Network Management System (NMS) with respect to Security Management

- The Ability to Control Access to Resources
  - NMS should provide the capabilities to grant or restrict access to the entire network or selected critical parts of the network for users or appropriate roles.

7.3.5 Security Management

Functional requirements of a Network Management System (NMS) with respect to Security Management

- The Ability to Archive and Retrieve Security Information
  - NMS should provide the ability to gather appropriate information, store the information and access that information for analysis and control purposes.

7.3.5 Security Management

Functional requirements of a Network Management System (NMS) with respect to Security Management

- The Ability to Manage and Control the Encryption Process
  - NMS should provide the capabilities to encrypt its communications, and facilitate the encryption process including Key management.

7.4 Simple Network Management Protocol (SNMP)

What is SNMP?

- For querying network devices for state and notification (e.g. Data rates, CPU load, Uptime, errors, running processes, etc.)
- Used to set or change device parameters by managers through agents
- Supported by most of the modern network devices
- Communication:
  - SNMP use UDP 161 port for SNMP Managers to communicate with SNMP Agents
  - SNMP use UDP 162 port when agents send unsolicited Traps to the SNMP Manager.

7.4 Simple Network Management Protocol (SNMP)

Protocol Data Units (PDUs):

- Used for the communication between Manager and Agents/Manager
- Each SNMP message contains a protocol data unit (PDU) by which it informs the receiving party the actions that should be taken.

7.4 Simple Network Management Protocol (SNMP)

Protocol Data Units (PDUs):

PDU	From	To	Purpose
GETREQUEST	Manager	Agent	to retrieve one or more requested MIB variables specified in the PDU
GETNEXTREQUEST	Manager	Agent	to retrieve the next MIB variable that is specified in the PDU (used for SNMP walking)
SETREQUEST	Manager	Agent	to set one or more MIB variables specified in the request PDU with the value specified in the request PDU
RESPONSE	Agent	Manager	response to a GETREQUEST, GETNEXTREQUEST, GETBULKREQUEST, INFORMREQUEST, or SETREQUEST PDUs

7.4 Simple Network Management Protocol (SNMP)

Protocol Data Units (PDUs):

PDU	From	To	Purpose
GETBULKREQUEST	Manager	Agent	to retrieve a number of variables up to a limit in a single request
INFORMREQUEST	Manager /Agent	Manager	Similar to trap but improved reliability as a response is required for INFORMREQUEST. Otherwise, the request will be sent multiple times.
TRAP	Agent	Manager	Asynchronous notification from agent to manager with information on a particular event

7.4 Simple Network Management Protocol (SNMP)

MIB (Management Information Base):

- Every Agent maintains the information corresponding to the device variables/parameters: e.g. CPU load, vendor name, etc.
- SNMP manager uses MIB to query a particular device and translate the information as required by the NMS
- This shared information base between agent and manager in an SNMP architecture is called Management Information Base.
- The MIB comprised of managed objects identified by a globally unique Object Identifier (OID)

7.4 Simple Network Management Protocol (SNMP)

OID (Object Identifier) and MIB:

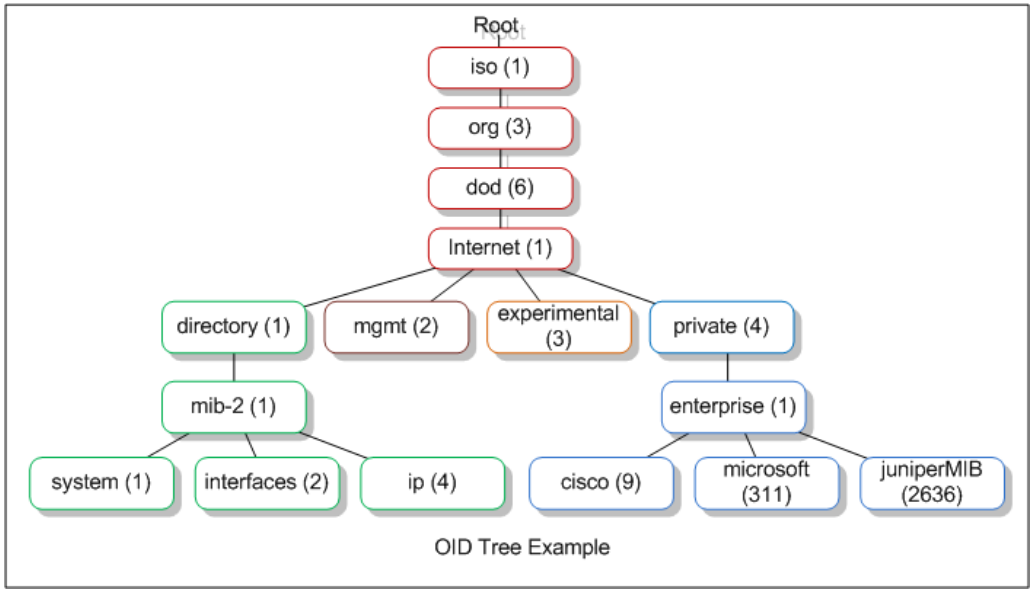


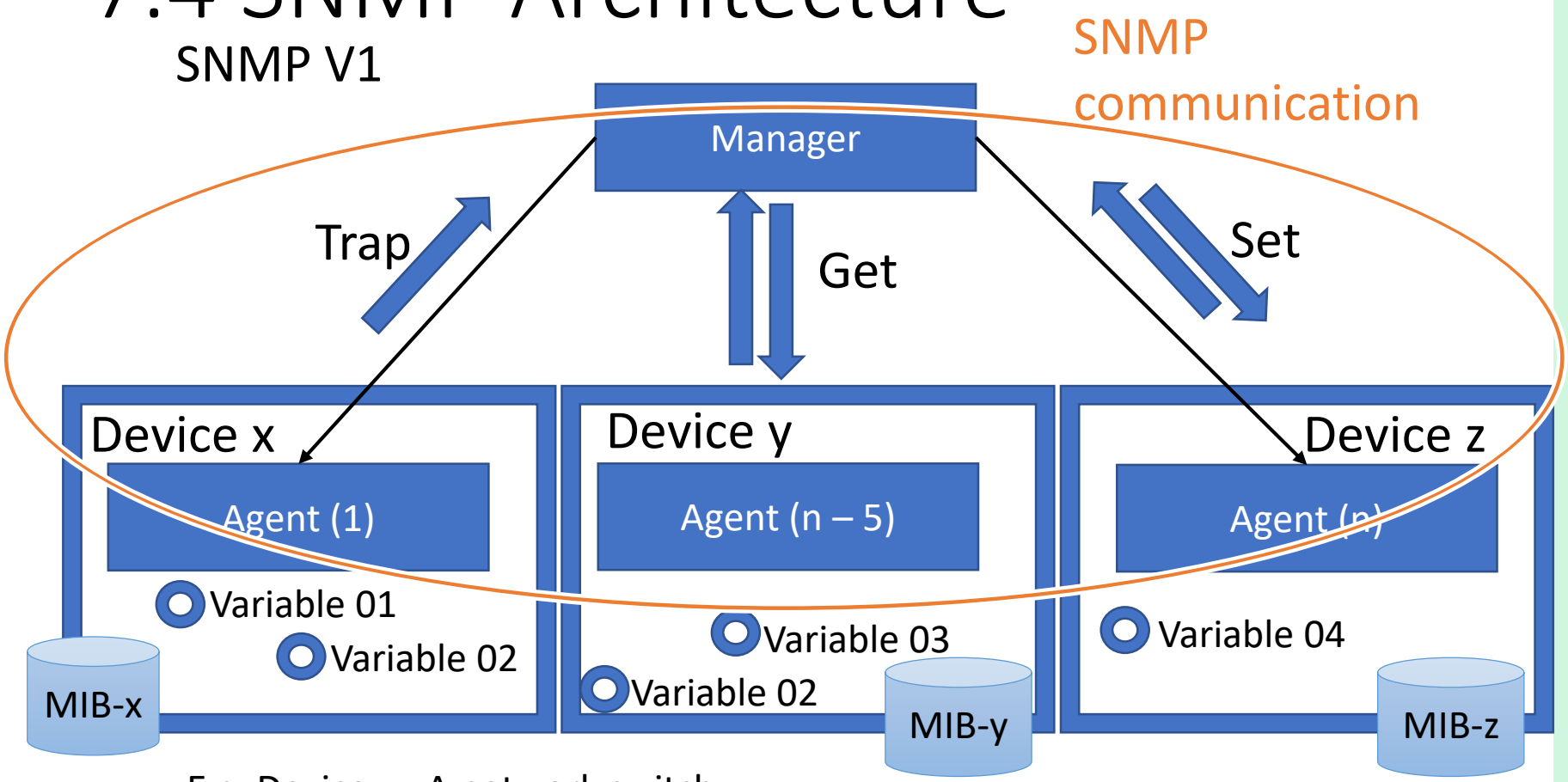
Image ref: Wikipedia

E.g.
The OKD associated with Microsoft is 1.3.6.1.4.1.311
the OID in RFC1213 for "sysDescr" is .1.3.6.1.2.1.1.1

Find a few MIB files for selected vendors to get an idea about an MIB file. Note that you don't need to fully understand MIB files.

7.4 SNMP Architecture

SNMP V1



E.g. Device x : A network switch

E.g. Variable 01 : temprature of the device.

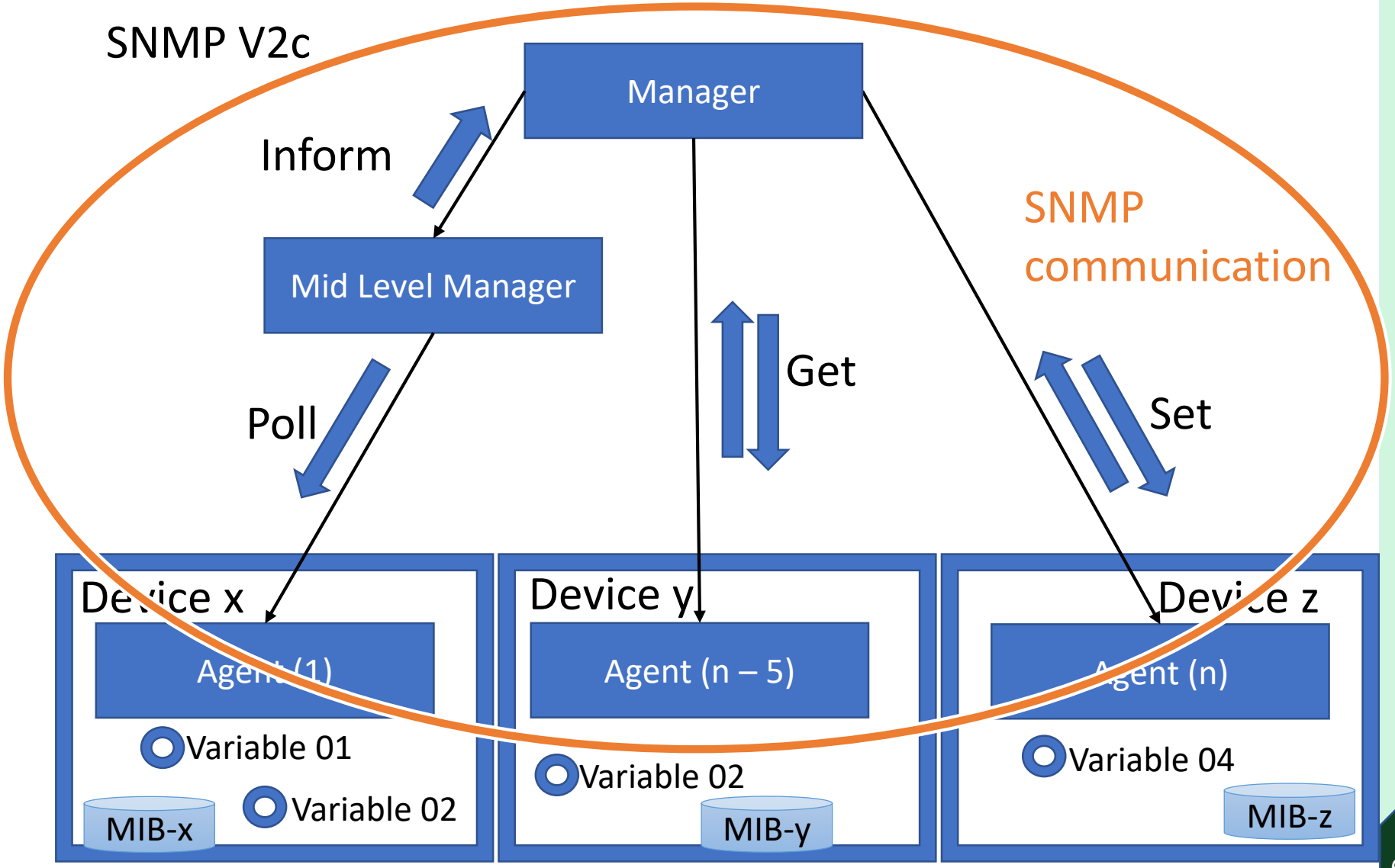
E.g. Manager : A server setup to monitor the network (Network Management System)

7.4 Simple Network Management Protocol (SNMP)

Mainly two types of communications:

- Asynchronous :
  - Trap – Used by agents to notify managers about certain events or errors. Not acknowledged.
  - Informrequest – Similar to Trap but acknowledged asynchronous communication
- Synchronous :
  - Poll – Retrieving MIB variables from device in order to determine faulty behaviour or connection problems. A polling interval can be defined.

7.4 SNMP Architecture



Ref: https://snmp.com/products/mlm.shtml

7.4 Simple Network Management Protocol (SNMP)

SNMP versions 1 and 2c are insecure

SNMPv3 use user based authentication

SNMPv3 provides support for encrypted messages

- Messages can be encrypted using DES, Triple DES, or AES

References

- https://datatracker.ietf.org/doc/html/rfc1157
- https://datatracker.ietf.org/doc/html/rfc3416
- NIST 500 – 175