Computer Network Unit 4

B.tech (Dr. A.P.J. Abdul Kalam Technical University)

What Is Network Management?

Network management refers to two related concepts. First is the process of configuring, monitoring, and managing the performance of a network. Second is the platform that IT and NetOps teams use to complete these ongoing tasks.

Over the past 10 years, network management systems have evolved to help IT teams operate in more agile ways, incorporating advanced analytics, machine learning, and intelligent automation to continually optimize network performance. As organizations adapt to a more distributed workforce, these network management systems are increasingly deployed in cloud and hosted environments.

Types of Network Infrastructure

While all network infrastructure serves the purpose of ensuring smooth data transfer between computers, users, and sub networks within your organisation, infrastructure falls into different areas. In general, network infrastructure components can be broken down into three major categories:

- **Network hardware**, like routers, switches, and physical servers. These kinds of components are very visible, but they are not the only kind of important infrastructure. Even cables, access points, and network cards are parts of this category.
- **Network software,** which can run on either dedicated hardware or commodity servers. Firewalls can be both hardware and software depending on the configuration. Intrusion detection and other security measures are usually part of this category as well.
- **Network services,** which come in the form of software that runs on servers. A domain name service (DNS) server is a good example of a network service. In general, network software is somewhat standalone and operates on traffic passing through to other parts of the network, while network services use a client-server architecture and only respond to traffic pointed in their direction.

Practically every network, from the simplest home setup to the most complex enterprise deployment, contains components that fall into these three categories. Let’s take a look at each of these categories in more detail.

Network Hardware

Network hardware comes ready to be used from the vendor with designated functionality. While many network hardware components come with configurable software, the software isn't the selling point—it's the dedicated hardware.

In addition to providing the most basic connectivity, network hardware completes specialised tasks fast. As an example, hardware routers and firewalls have discrete components that allow them to process more traffic per second than software running on standard servers.

As the very basis for everything that goes on top, network hardware is the most crucial part of every network. That said, no modern business relies on dedicated network hardware alone. This type of infrastructure must be paired with higher level components as well.

Network Software

While network hardware completes the most basic and performance-critical tasks, network software takes care of more complex and quickly changing tasks. For example, network security appliances (like intrusion detection systems) frequently come in the form of network software.

Network configuration management and privileged access control software, important tools to control and manage your network, also go under the category of network software.

Network Services

On top of the foundation laid by network hardware and software, services provide functionality that endpoint devices and even other non-infrastructure services require. As an example, network-wide authentication services let your employees securely access the systems and data they need to get their work done.

Other specific examples of network services include DNS, Active Directory, and email (especially if it's used to maintain the network itself).

Web servers and other types of services that aren't directly involved in keeping the network running smoothly aren't considered *network* services, although they are still services.

Why Is Network Infrastructure Important?

As your company grows and the amount of data traveling across your corporate network increases, the foundational underpinnings of your network get put under stress. Maintaining your network's reliability—so as to avoid costly downtime incidents or worse, lost data—becomes more and more important. If a disaster were to strike your company, having a reliable and well-supported network will make recovery much easier.

In an age of remote work as a result of the coronavirus pandemic, your company's network is likely under more strain than ever before. Each hour during which your network suffers issues is an hour where your entire business grinds to a halt, so making forward-looking investments into this critical but often forgotten infrastructure pays dividends in the future.

How Does Network Infrastructure Impact Security?

An outsized proportion of your company's network infrastructure serves to protect the network and endpoint devices from attacks. Whether it's your firewall stopping malicious traffic at the edge or a network security appliance detecting and preventing an in-progress malware attack, network hardware, software, and services are all a big part of your company's cybersecurity.

Security-critical network infrastructure devices are frequently strung together to form new integrations. In particular, businesses commonly connect their intrusion detection systems directly to firewalls so that they can stop attacks as soon as they're detected. In a similar vein, logging and management systems can be connected to other infrastructure to provide oversight.

TCP/IP Internet Standard Management Framework Architecture and Protocol Components

TCP/IP network management is based on the Simple Network Management Protocol, abbreviated SNMP. As we saw in the overview topic, however, this term is ambiguous. While it is commonly used to refer to the actual communication protocol used to exchange network management information, the term also refers to the entire set of technologies that enable TCP/IP network management. The technical name for this larger architecture is the *Internet Standard Management Framework*. Again, even though it may seem strange, this term is actually abbreviated in the standards as "SNMP". For simplicity, I abbreviate it as the "SNMP Framework", to differentiate it from the SNMP protocol.

The Internet Standard Management Framework encompasses all of the technologies that comprise the TCP/IP network management solution. The SNMP Framework consists of a number of

architectural components that define how management information is structured, how it is stored, and how it is exchanged using the SNMP protocol. The Framework also describes how the different components fit together, how SNMP is to be implemented in network devices, and how the devices interact.

SNMP Framework Components

As we will explore in more detail later, the Internet Standard Management Framework is entirely *information-oriented*. It includes the following primary components

- **Structure of Management Information (SMI):** To ensure interoperability of various devices, we want to have a consistent way of describing the characteristics of devices to be managed using SNMP. In computer science, a *data description language (DDL)* is the tool for this job. The *Structure of Management Information (SMI)* is a standard that defines the structure, syntax and characteristics of management information in SNMP.

- **Management Information Bases (MIBs):** Each managed device contains a set of variables that is used to manage it. These variables represent information about the operation of the device that is sent to a network management station, and/or parameters sent to the managed device to control it. The *management information base (MIB)* is the full set of these variables that describe the management characteristics of a particular type of device.Each variable in a MIB is called a *MIB object*, and is defined using the SMI data description language. A device may have many objects, corresponding to the different hardware and software elements it contains.

- Initially, a single document defined the MIB for SNMP, but this model was inflexible. To allow new MIB objects to be more easily defined, groups of related MIB objects are now defined in separate RFC standards called *MIB modules*. Over 100 such MIB modules have been defined so far.

- **Simple Network Management Protocol (SNMP):** This is the actual SNMP protocol itself. It defines how information is exchanged between SNMP agents and network management stations. The SNMP *protocol operations* define the various SNMP messages and how they are created and used. SNMP *transport mappings* describe how SNMP can be used over various underlying internetworks, such as TCP/IP, IPX and others.

- **Security and Administration:** To the three main architectural components above, the SNMP Framework adds a number of supporting elements. These provide enhancements to the operation of the SNMP protocol for security, and address issues related to SNMP implementation, version transition and other administrative issues

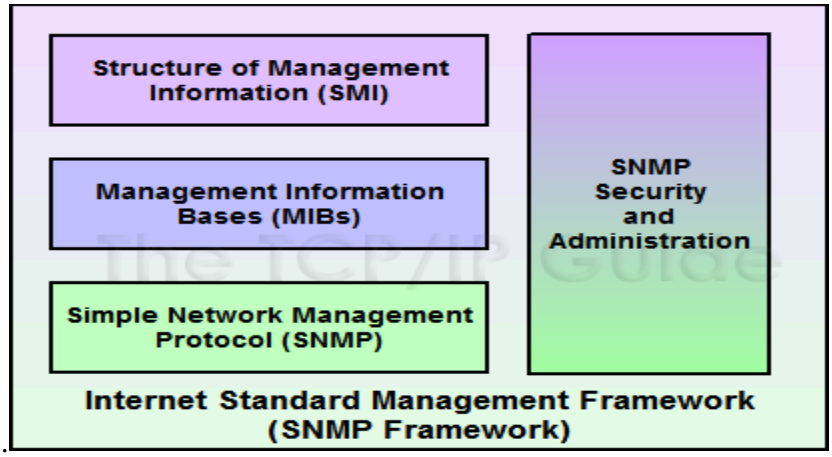

Figure 271: Components of the TCP/IP Internet Standard Management Framework

Simple Network Management Protocol (SNMP)
If an organization has 1000 devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.

Simple Network Management Protocol (SNMP) –
SNMP is an application layer protocol that uses UDP port number 161/162. SNMP is used to monitor the network, detect network faults, and sometimes even used to configure remote devices.
SNMP components –
There are 3 components of SNMP:

1. **SNMP Manager –**
   It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)

2. **SNMP agent –**
   It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.

3. **Management Information Base –**
   MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.

SNMP messages –
Different variables are:

1. **GetRequest –**
   SNMP manager sends this message to request data from the SNMP agent. It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.

2. **GetNextRequest –**
   This message can be sent to discover what data is available on an SNMP agent. The SNMP manager can request data continuously until no more data is left. In this way, the SNMP manager can take knowledge of all the available data on SNMP agents.

3. **GetBulkRequest –**
   This message is used to retrieve large data at once by the SNMP manager from the SNMP agent. It is introduced in SNMPv2c.

4. **SetRequest –**
   It is used by the SNMP manager to set the value of an object instance on the SNMP agent.

5. **Response –**
   It is a message sent from the agent upon a request from the manager. When sent in response to Get messages, it will contain the data requested. When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.

6. **Trap –**
   These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.

7. **InformRequest –**
   It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to send trap message continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn't provide.

SNMP security levels –
It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3. There are 3 security levels namely:

1. **noAuthNoPriv –**
   This (no authentication, no privacy) security level uses a community string for authentication and no encryption for privacy.

2. **authNopriv –** This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.

3. **authPriv –** This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses the DES-56 algorithm.

SNMP versions –
There are 3 versions of SNMP:

1. **SNMPv1 –**
   It uses community strings for authentication and uses UDP only.

2. **SNMPv2c –**
   It uses community strings for authentication. It uses UDP but can be configured to use TCP.

3. **SNMPv3 –**
   It uses Hash-based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. Therefore, the conclusion is the higher the version of SNMP, the more secure it will be.