Chapter 7
Network Management

Introduction

A network consists of *many* complex, interacting pieces of hardware and software - from the links, bridges, routers, hosts and other devices that comprise the physical components of the network to the many protocols that control and coordinate these devices. When hundreds or thousands of such components are cobbled together by an organization to form a network, it is not surprising that components will occasionally malfunction, that network elements will be misconfigured, that network resources will be over utilized, or that network components will simply "break" (e.g., a cable will be cut, a can of soda will be spilled on top of router). The network administrator, whose job it is to keep the network "up and running," must be able to respond to (and better yet, avoid) such mishaps. With potentially thousands of network components spread out over a wide area, the network administrator in a network operations centre (NOC) clearly needs tools to help monitor, manage, and control the network.

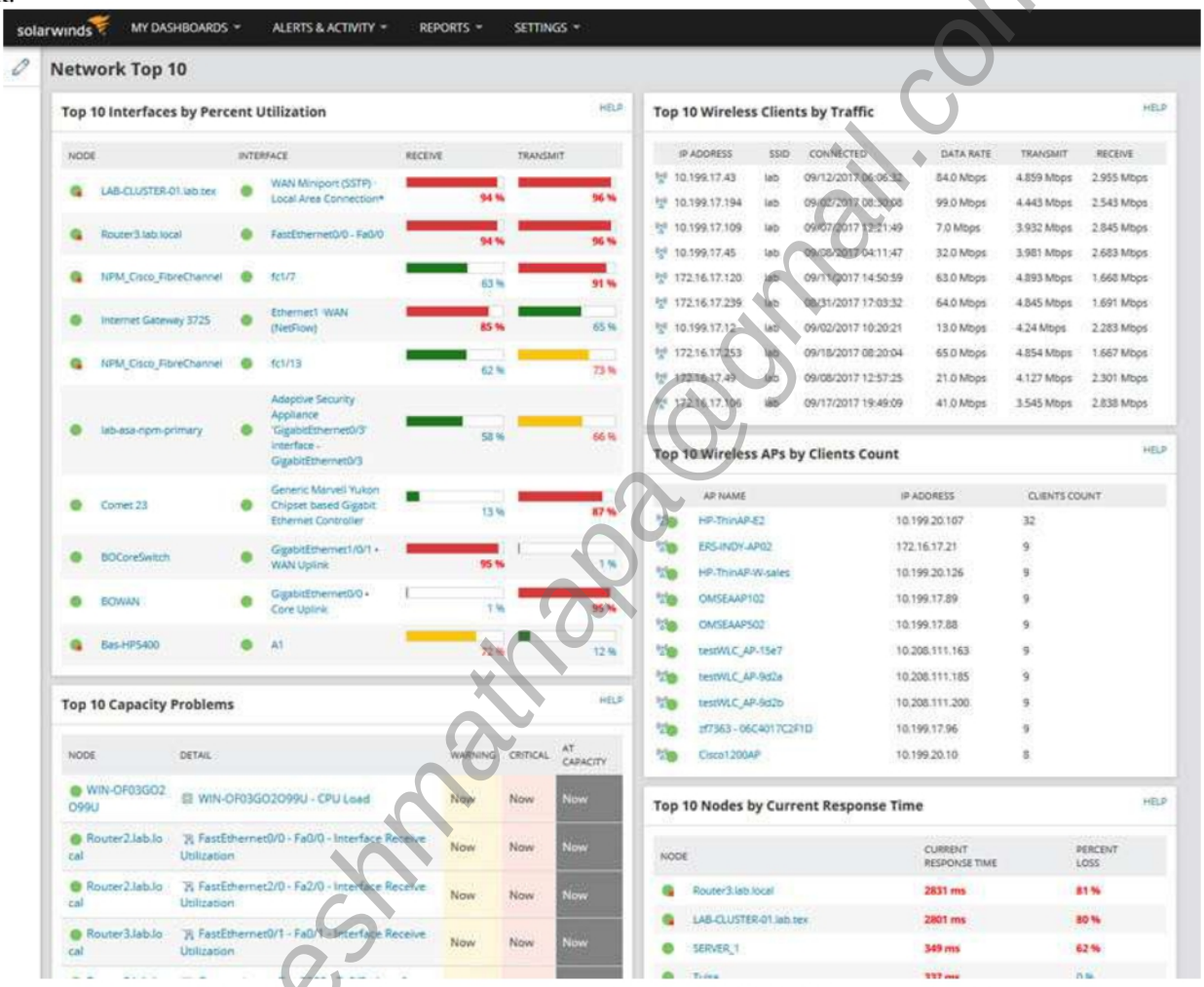

Fig: Network Analysis provided by NMS(Solar winds)

"Network management includes the deployment, integration and coordination of the hardware, software and human elements to monitor, test, poll, configure, analyse, evaluate and control the* Network Management – Introduction *network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost."

Advantage of proper Network Management

1. **Optimizing network availability and performance**

   Network availability can be thought of as how it easy it for one point of the IP infrastructure to reach another. With networks becoming more widely dispersed and supporting more operations than ever before, achieving optimal availability—and fulfilling SLA requirements—requires a top-flight solution.

   Network management software can proactively and automatically gather data about the network, giving administrators information about problems before someone else reports the issue via phone or email. Performance can be analyzed in real time through functionalities that look at packet drops and throughout.

2. **Lowering expenses by improving asset utilization**

   The number of IP-enabled endpoints is rising. Cisco has predicted that mobile and wireless devices will generate more traffic than wired ones by 2016 and account for 55 percent of all activity by 2017. In this context, it is important for administrators to know what's connecting to their networks and whether their infrastructure is equipped to handle major fluctuations, if only to keep costs under control as conditions evolve.

3. **Minimizing risk by providing a secure network that meets compliance guidelines**

   Network operators can no longer worry exclusively about SLAs and customers. They must also be mindful of regulatory requirements. To maintain compliance, organizations need features that keep close tabs on the network. Real-time maps of network topologies, continuous monitoring and secure channels can all help in staying on the right path.

4. **Effective change management**

   Often it is useful to have records of past network configurations in case something needs to be reverted. Network management software enables efficient change management so that users can establish solid baselines for performance.

5. **Achieving service level agreements and documenting performance with reports**

   With the advent of Service Level Agreements (SLA) - contracts that define specific performance metrics and acceptable levels of network provider performance with respect to these metrics These SLAs include service availability (outage), latency, throughput and outage notification requirements. Clearly, if performance criteria are to be part of a service agreement between a network provider and its users, then measuring and managing performance will be of great importance to the network administrator.

6. **Intrusion detection**

   A network administrator may want to be notified when network traffic arrives from, or is destined to, a suspicious source (e.g., host or port number). Similarly, a network administrator may want to detect (and in many cases filter) the existence of certain types of traffic that are known to be characteristic of certain attacks.

Areas of Network Management given by ISO reference model

ISO has created a network management model for placing above scenarios in more structured framework.

1. **Performance management**.

   The goal of performance management is to quantify, measure, report, analyse and control the performance (e.g., utilization, throughput) of different network components.

2. **Fault management**

   The goal of fault management is to log, detect, and respond to fault conditions in the network. We can think of fault management as the immediate handling of transient network failures (e.g., link, host or router hardware or software outages).

3. **Configuration management**

   Configuration management allows a network manager to track which devices are on the managed network and the hardware and software configurations of these devices.

4. **Accounting management.**

   Accounting management allows the network manager to specify, log, and control user and device access to network resources. Usage quotas, usage-based charging, and the allocation of resource access privileges all fall under accounting management.

5. **Security management**

   The goal of security management is to control access to network resources according to some well-defined policy. The use of firewalls to monitor and control external access points to one's network, is one crucial part in security management.

The infrastructure for network management

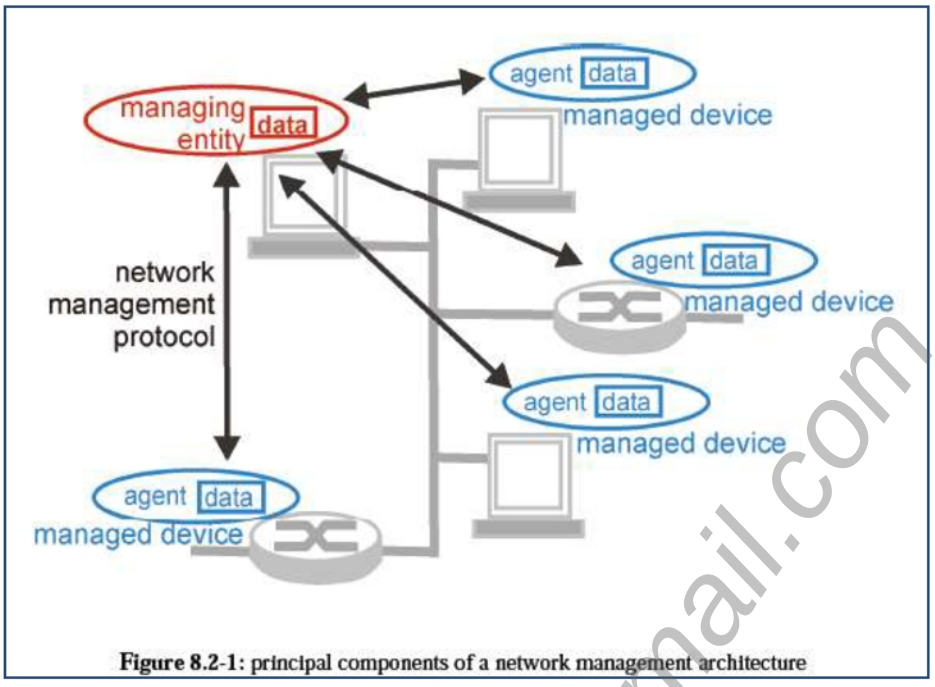

Figure 8.2-1: principal components of a network management architecture

- **The managing entity** is an application, typically with a human-in-the-loop, running in a centralized network management station in the network operations center (NOC). It controls the collection, processing, analysis, and/or display of network management information.

- **A Managed Device** is a piece of network equipment that resides on a managed network. It might be host, router, bridge, hub or printer. Managed Device contains several Managed Objects. These managed objects are the actual pieces of hardware within the managed device (e.g., a network interface card), and the sets of configuration parameters for the pieces of hardware and software (e.g., an intradomain routing protocol such as RIP). Managed Object have Piece of information associated with them that are collected into management information base(MIB). Finally, a network management agent resides in each managed device. An agent is a process running in the managed device that communicates with the managing entity, taking local actions on the managed device under the command and control of the managing entity.

- The third part of network management architecture is **Network management protocol.** Network Management Protocol runs between Managing Entity and Managed Device allowing the managing entity to query the status of managed devices and indirectly effect actions in these devices via its agents. Agents can use the network management protocol (Example: SNMP) to inform the managing entity of exceptional events

Assignment: Write short notes on SNMP