NERTWORK MONITORING TOOLS

Outcome 1

1.Simple Network Management Protocol

- **Simple Network Management Protocol (SNMP)** is an "Internet-standard protocol for managing devices on IP networks."
- Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more."
- It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention
- In typical SNMP uses, one or more administrative computers, called managers, have the task of monitoring or managing a group of hosts or devices on a computer network.
- Each managed system executes, at all times, a software component called an *agent* which reports information via SNMP to the manager.

HOW SNMP WORKS

- An SNMP-managed network consists of three key components:
  1. Managed device
  2. Agent — software which runs on managed devices
  3. Network management system (NMS) — software which runs on the manager

- A *managed device* is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones,IP video cameras, computer hosts, and printers.

- An *agent* is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP specific form.

- A *network management system* (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

2.MANAGED NODES

- A *node* is a logical grouping of managed servers.
- A node usually corresponds to a logical or physical computer system with a distinct IP host address. Nodes cannot span multiple computers.
- Node names usually are identical to the host name for the computer.
- Nodes in the network deployment topology can be managed or unmanaged. A managed node has a node agent process that manages its configuration and servers. Unmanaged nodes do not have a node agent.
- A managed node has a node agent that manages all servers on a node. The node agent represents the node in the management cell and keeps the configuration up to date.

- You can add managed and unmanaged nodes to a Network Deployment cell in one of the following ways:
- Administrative console
- Command line (managed nodes only)
- Administrative script
- Java program

3. MANAGEMENT STATION

- In terms of the network management model, a **network management station** **(NMS)** is one that executes network management applications (NMAs) that monitor and control network elements (NE) such as hosts, gateways and terminal servers.
- These network elements use a management agent (MA) to perform the network management functions requested by the network management stations.
- The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements.

- The management station agent is a monitoring agent for network storage. After you add an agent, you can configure the management station to:
- Notify users by email when events occur on the enclosures attached to the management station. Use the Email Notification Manager, from the Management Station Configuration console, to add recipients to the email notification list.
- Prevent unauthorized users from connecting to the management station using its built-in security feature. The management station checks the security list user name and password to ensure that only authorized users can log in. Use the Security Manager, from the Management Station Configuration console, to add users to the agent security list.

- The agent monitors and generates events for critical or fatal problems in the enclosure configuration every 5 seconds. These changes include:
- Failed drives
- Failed battery
- Offline or critical logical drives
- Failed controllers
- Enclosure problems
- Non-warranted drives.

PERFORMANCE AND SYSTEM MONITOR

- **System Monitor** (sysmon.exe) is a program in Windows 95, 98 and ME that is used to monitor various activities on a computer such as CPU usage or memory usage. The equivalent of System Monitor on Windows 2000 and XP is called Performance Monitor (perfmon.msc or perfmon.exe). Despite this, the original System Monitor can be run on XP.

- System Monitor can display information as a graph, a bar chart, or numeric values and can update information using a range of time intervals. The categories of information that you can monitor depend on which networking services are installed on your system, but they always include File System, Kernel, and Memory Manager. Other possible categories include Microsoft Network Client, Microsoft Network Server, and protocol categories.

- This application is usually used to determine the cause of problems on a local or remote computer by measuring the performance of hardware, software services, and applications. System Monitor is not installed automatically during Windows setup, it must be installed manually using the Add/Remove Programs applet, located in the Control Panel.

PROTOCOL ANALYZER

- A "Protocol analyzer" is a tool (hardware or software) used to capture and analyze signals and data traffic over a communication channel. Such a channel differs from a local computer bus to a satellite link, that provides a means of communication using a standard communication protocol (networked or point-to-point). Each type of communication protocol has a different tool to collect and analyze signals and data.

What protocol analyzer can detect

- Unexpected traffic
- Unnecessary traffic
- Authorized program use
- Email programs
- Virus detection

INTERPRET THE INFORMATION PROVIDED

- demand overload
- storage capacity overload
- speed reduction
- high percentage of resource users

FAILURES OF IT SYSTEMS

- system operates, but is unacceptably slow
- unacceptable number of internet connection drop-outs
- users have difficulty in accessing data
- users have difficulty running software installed on their own workstations
- users have difficulty running software installed on the server

COMMON CAUSES OF FAILURES OF IT SYSTEMS

- insufficient memory
- operating system cannot cope with user numbers
- poorly distributed load
- speed reduction
- high percentage of users
- excessive e-mail files on system
- modem slow to dial out, causing missed Internet connection

REMEDY TO FAILURES OF IT SYSTEMS TO MEET OPERATIONAL REQUIREMENTS

- re-configure operating system
- b upgrade operating system
- c upgrade system hardware
- d re-configure application software
- e upgrade application software
- f re-distribute load on system hubs

CREATING AND MAINTAINING OPERATIONAL RECORDS.

- It is a good practice to create and maintain operation records.
- they act as reference during future configurations.

TYPICAL CONTENT AND FORMAT OF OPERATIONAL RECORDS, FOR EACH MACHINE (SERVER OR WORKSTATION):

- the type of machine
- serial number
- location of machine
- what disk drives are available in the machine
- adapter card modules fitted to the machine, make, version, configuration (IRQ, I/O address, speed, etc.)
- operating system type and version installed in each machine
- for servers: network operating system and version installed (including configuration)
- other software permanently running in the machine (version, configuration)
- what addresses the machine is using
- if the IP is the address issued by a Dynamic Host Control Protocol (DHCP) server, the
- computer name of the machine details of workgroup/domain membership details of the normal users of the machine
- passwords and authorities in use
- security arrangements (firewalls, anti-virus protection etc)
- fault log
- maintenance log
- upgrade log