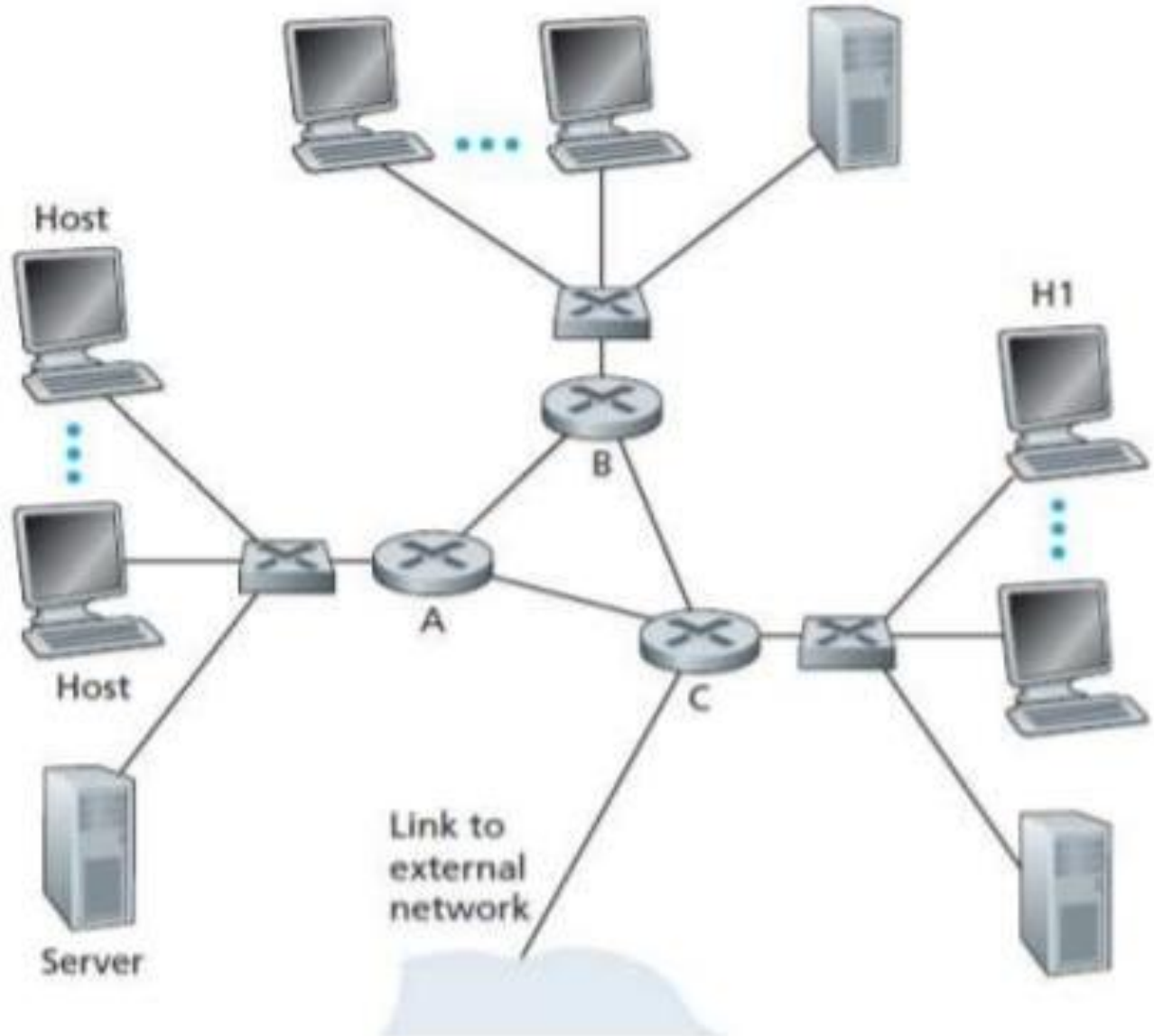
Introduction to network management

“What is network management?”

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

- The network administrator will actively monitor, manage, and control the system with which she or he is entrusted.

- As the public internets and private intranets have expanded into vast global networks, managing the large number of hardware and software components has become increasingly important.


Host
Host
Server
A
B
C
H1
Link to
external
network

- Figure illustrates a small network consisting of three routers and a number of hosts and serve.
- Even in a simple network, network administrators can greatly benefit from using proper network management tools:
- Detecting failure of an interface card at a host or a router:

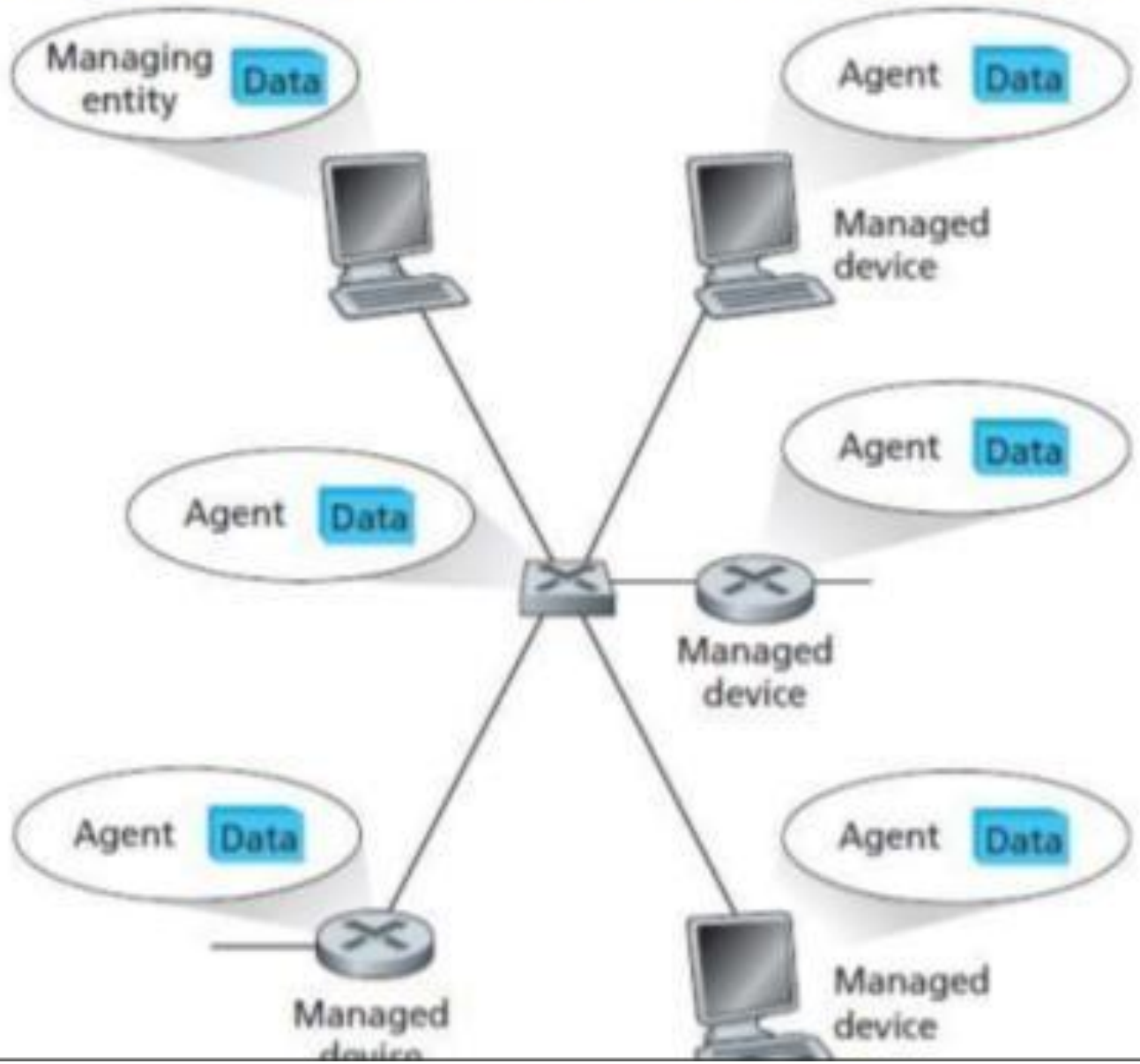
With appropriate network management tools, a network entity (for example, router A) may report to the network administrator that one of its interfaces has gone down.

- Host monitoring:A network administrator can periodically check if all hosts are operational and proactively address issues like a host being down before users report them, which can leave a positive impression.
- Monitoring traffic to aid in resource deployment:A network administrator might monitor source-to-destination traffic patterns and link usage.For example, moving servers between LAN segments may reduce cross-LAN traffic, improving efficiency without extra costs. Monitoring can also reveal overloaded LAN segments or external links.

Five areas of Network Management

- Performance management:The goal of performance management is to quantify, measure, report, analyze, and control the performance of different network components.Simple Network Management Protocol (SNMP) play a central role in Internet performance management.
- Fault management:The goal of fault management is to log, detect, and respond to fault conditions in the network.The line between fault management and performance management is rather blurred.
- 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.
- Accounting management:Accounting management allows the network manager to specify, log, and control user and device access to network resources.
- Security management:The goal of security management is to control access to network resources according to some well-defined policy.

The Infrastructure for Network Management



- There are three principal components of a network management architecture:
- a managing entity
- the managed devices
- network management protocol.

- The **managing entity** is a centralized application, running in network management and often with human loop . It handles data collection, analysis, display, and initiates actions to control the network and the human network administrator interacts with the network devices.
- A **managed device** is network equipment like a router or printer, containing managed objects such as hardware components and configuration settings. These objects store data in a Management Information Base (MIB). A network management agent within the device communicates with the managing entity and executes its commands.
- The **network management protocol** enables communication between the managing entity and managed devices. It allows status queries, remote actions, and alerts for issues. While it doesn’t manage the network directly, it supports administrators in monitoring and controlling the network.

- The Simple Network Management protocol (SNMP)is an application-layer protocol that facilitates the exchange of management information between network devices.
- It is part of the Transmission Control Protocol/ Internet Protocol (TCP/IP) protocol suite.
- SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Some uses of SNMP are:

- Monitoring traffic flowing through the device
- Detecting and notifying faults encountered on network devices
- Collecting device performance data over long periods and identifying
- Remotely configuring network devices
- Remotely accessing and controlling network devices

- SNMP Basic Components:-
- An SNMP managed network consists of three key components:

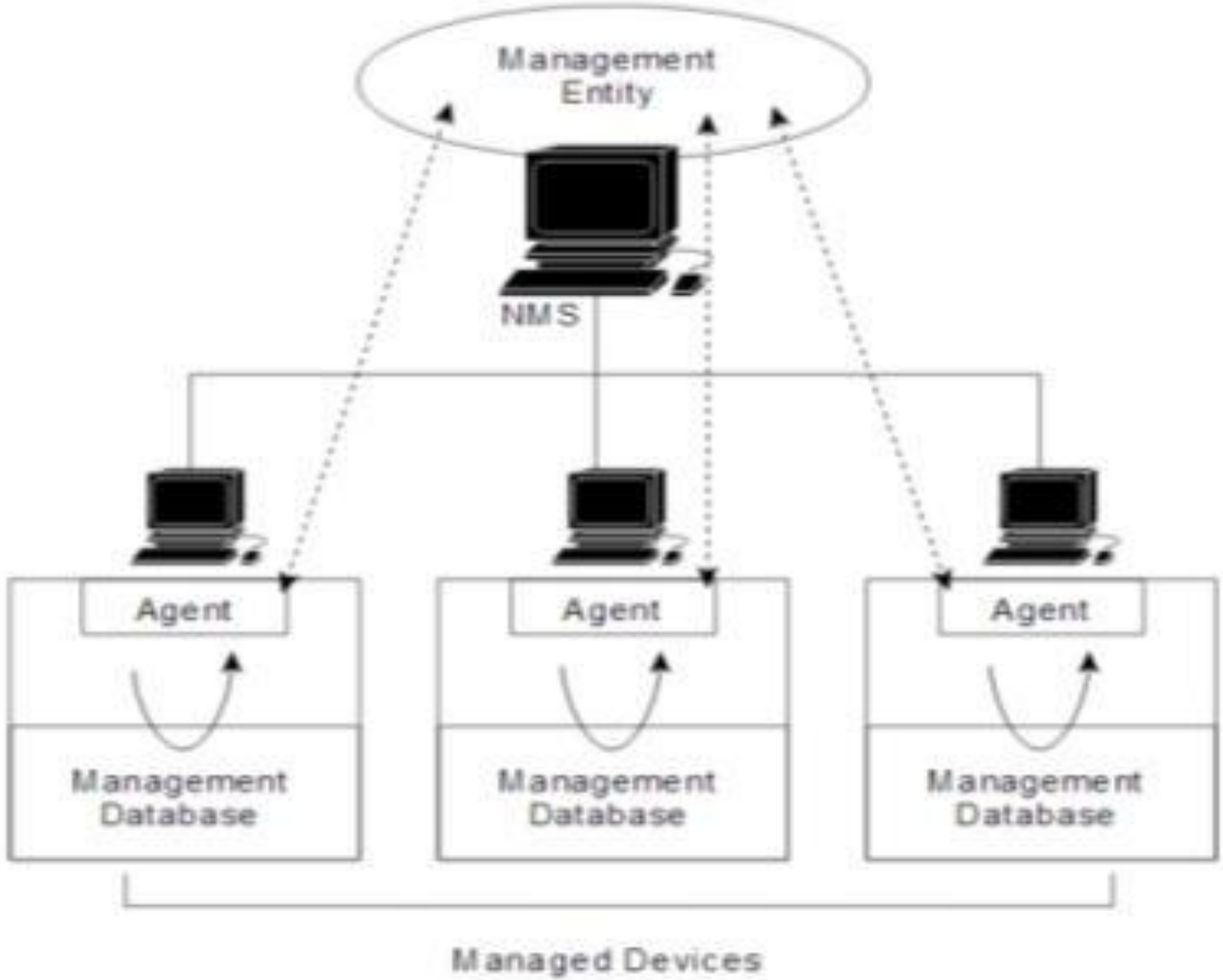
1.Managed devices

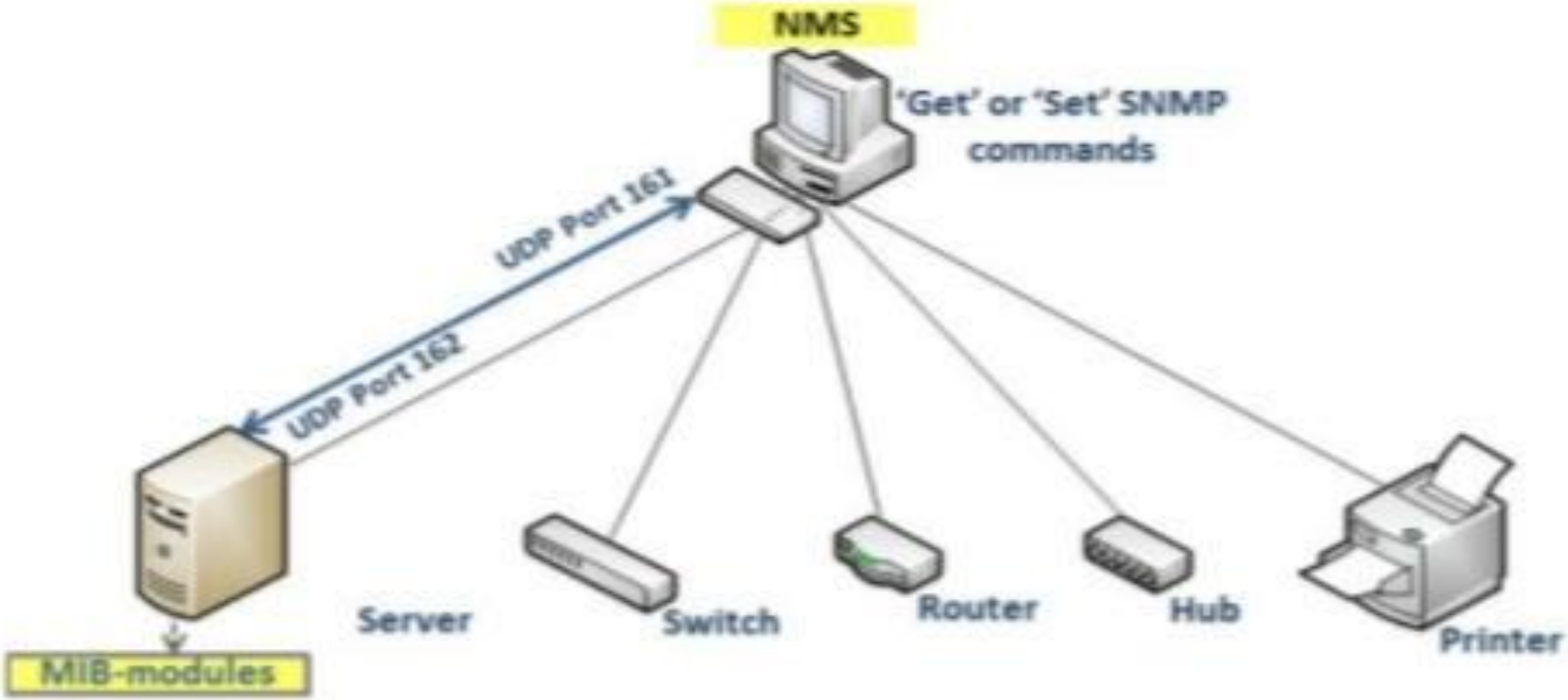
2.Agents

3.Network-management systems(NMSs)

- A managed device is a network node that contains an SNMP agent and resides on a managed network.Managed devices collect and store management information and make this information available to NMS using SNMP. Managed devices, sometimes called network elements,can be routers and access servers, switches and bridges, hubs, computer hosts, or printers.
- An agent is a network-management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.
- An 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 must exist on any managed network.

An SNMP managed network consists of managed devices, agents, and NMSs.





SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. Each managed component has a corresponding subagent and MIBs. SNMP-compliant devices listen for PDUs on port 162 and return the data stored in the MIB to the SNMP requesters via port 161. A network can have multiple SNMP managers.

- **SNMP Versions**
- There are three SNMP messaging protocols: SNMPv1, SNMPv2 and SNMPv3.

- Implementing SNMP helps to monitor and be alerted on the status of device hardware components


Thank
you!