NETWORK MANAGEMENT

INTRODUCTION

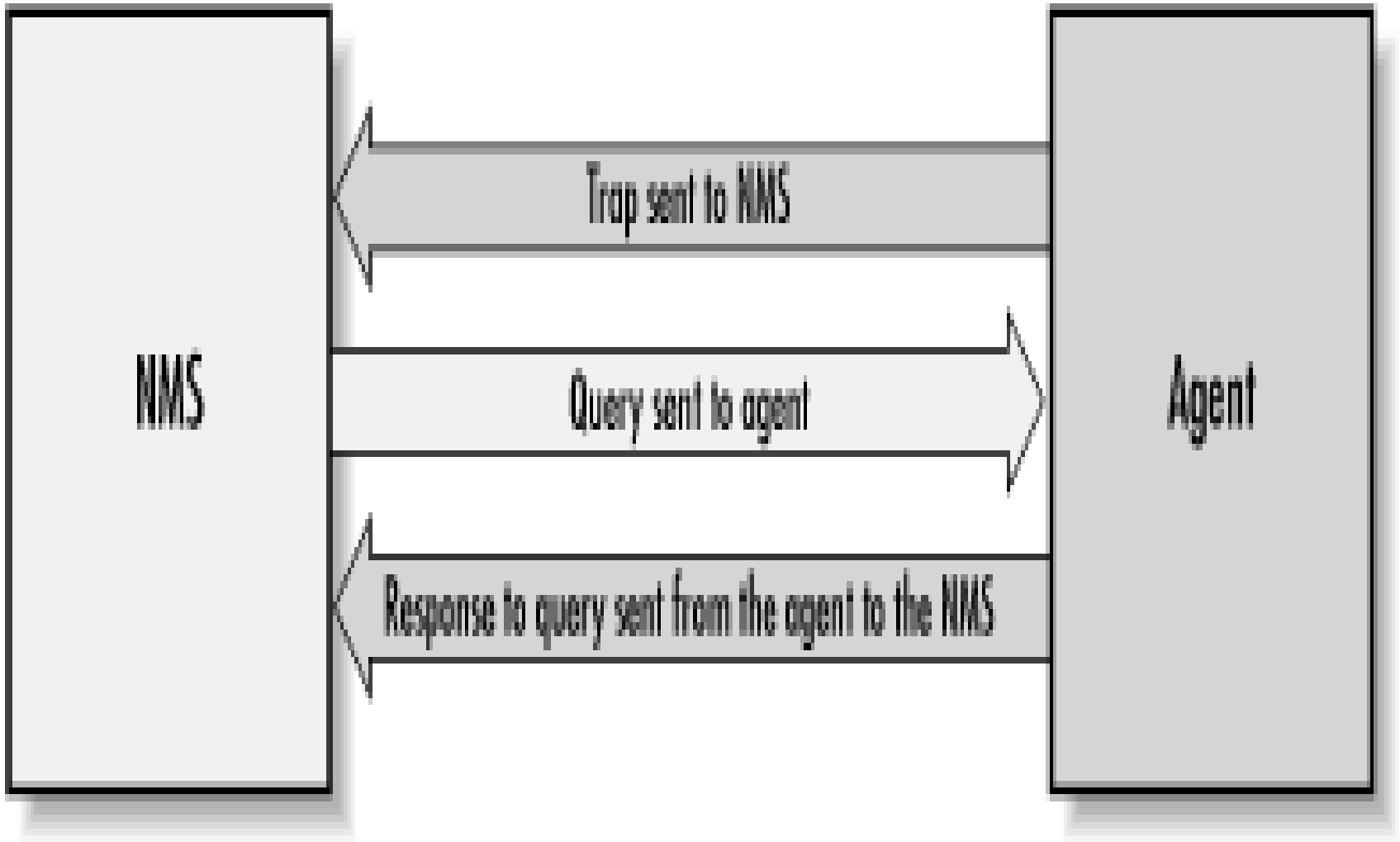
- Different techniques used for Network Management will be discussed here:
  - Remote Monitoring Techniques
  - Traps
  - Polling
  - Firewalls
  - Proxy Servers
  - VLANs

Remote Monitoring Techniques

- RMON (Remote Network Monitoring) was developed to help us understand how the network itself is functioning, as well as how individual devices on the network are affecting the network as a whole.
- It can be used to monitor not only LAN traffic, but WAN interfaces as well.
- In today's complex network of routers, switches, and servers, it can seem like a daunting task to manage all the devices on your network and make sure they're not only up and running but performing optimally.
- This is where the *Simple Network Management Protocol* (SNMP) can help.

Simple Network Management Protocol

- It is a UDP-based network protocol. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.
- SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF).
- It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects


NMS
Trap sent to NMS
Query sent to agent
Response to query sent from the agent to the NMS
Agent

Managers in SNMP

- In the world of SNMP there are two kind of entities: ***managers*** and ***agents*****.**
  - A **manager** is a server running some kind of software system that can handle management tasks for a network. Managers are often referred to as *Network Management Stations* (NMSs).
  - An NMS is responsible for polling and receiving traps from agents in the network.

Pollng & Traps

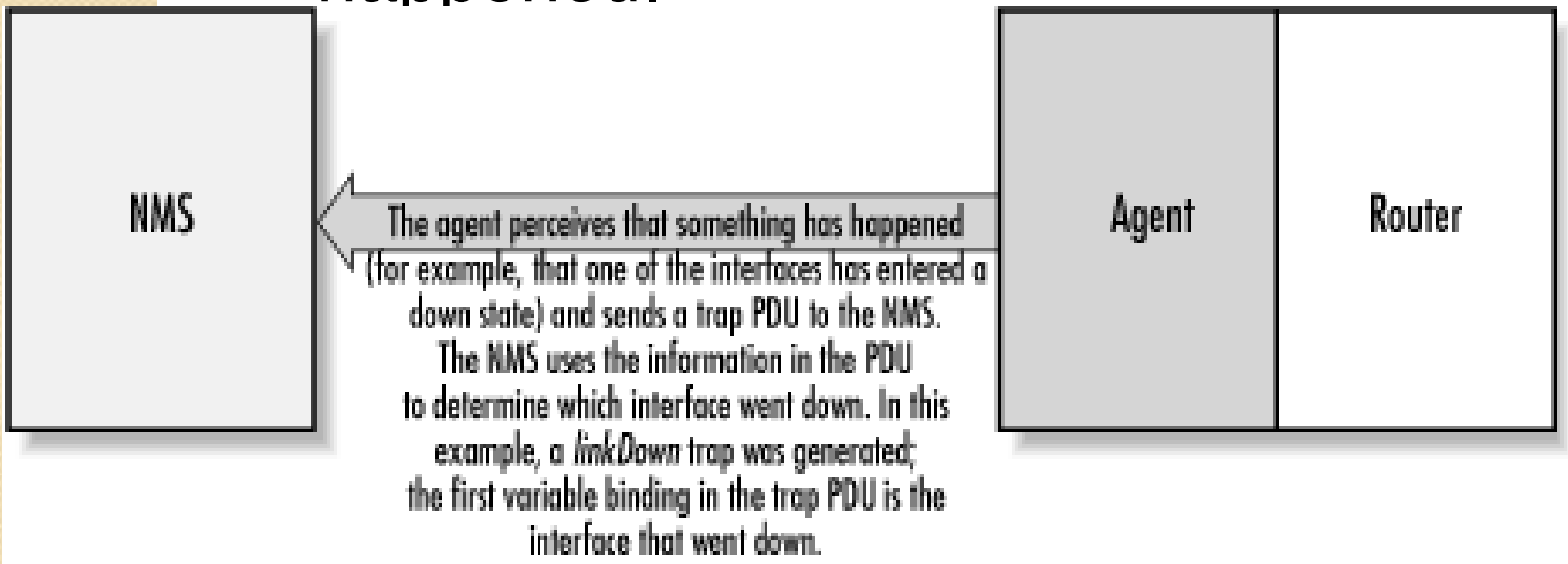
- A ***poll***, in the context of network management, is the act of querying an agent (router, switch, Unix server, etc.) for some piece of information.
- A ***trap*** is a way for the agent to tell the NMS that something has happened. Traps are sent asynchronously, not in response to queries from the NMS.
- The NMS is further responsible for performing an action based upon the information it receives from the agent.

Agents in SNMP

- The second entity, the ***agent*****,** is a piece of software that runs on the network devices you are managing.
- It can be a separate program (a daemon, in Unix language), or it can be incorporated into the operating system.
- The agent provides management information to the NMS by keeping track of various operational aspects of the device.
  - For example, the agent on a router is able to keep track of the state of each of its interfaces: which ones are up, which ones are down, etc.
- It's important to keep in mind that polls and traps can happen at the same time. There are no restrictions on when the NMS can query the agent or when the agent can send a trap.

SNMP Traps

- A trap is a way for an agent to tell the NMS that something bad has happened.



SNMP Traps

- Since traps are designed to report problems with your network, traps are especially prone to getting lost and not making it to their destinations.
- However, the fact that traps can get lost doesn't make them any less useful; in a well-planned environment, they are an integral part of network management.
- It's better for your equipment to try to tell you that something is wrong, even if the message may never reach you, than simply to give up and let you guess what happened.

SNMP Traps: Example

- A network interface on the device (where the agent is running) has gone down.
- A network interface on the device (where the agent is running) has come back up.
- An incoming call to a modem rack was unable to establish a connection to a modem.
- The fan on a switch or router has failed.

SNMP Polling

- SNMP gives you the ability to poll your devices regularly, collecting their management information.
- Furthermore, you can tell the NMS that there are certain thresholds that, if crossed, require some sort of action.
- For example, you might want to be notified if the traffic at an interface jumps to an extremely high (or low) value; that event might signal a problem with the interface, or insufficient capacity, or even a hostile attack on your network. When such a condition occurs, the NMS can forward an alarm to an event-correlation engine

SNMP Polling

- Polling is like checking the oil in a car; this analogy may help you to think about appropriate polling strategies.
- Three distinct items concern us when checking the oil:
  - the physical process (opening the hood, pulling out the dipstick (measuring stick), and putting it back in);
  - the preset gauge that tells us if we have a problem (is the level too high, too low, or just right?);
  - and the frequency with which we check it (once an hour, week, month, or year?). .

SNMP Polling Interval

- Once you determine your monitoring needs, you can specify at what interval you would like to poll a device or set of devices.
- This is typically referred to as the *poll interval*, and can be as granular as you like (e.g., every second, every hour, etc.).
- The threshold value at which you take action doesn't need to be binary: you might decide that something's obviously wrong if the number of packets leaving your Internet connection falls below a

SNMP Polling Interval

- Whenever you are figuring out how often to poll a device, remember to keep three things in mind:
  - the device's agent/CPU,
  - bandwidth consumption,
  - and the types of values you are requesting. Some values you receive may be 10-minute averages.
- If this is the case, it is a waste to poll every few seconds. Review the MIBs surrounding the data for which you are polling. Preference should be given to start polling fairly often. Once We see the trends and peak values, We generally back off. This can add congestion to the network but ensures that We didn't missed any important information.

MIB

- The *Management Information Base* (MIB) can be thought of as a database of managed objects that the agent tracks. Any sort of status or statistical information that can be accessed by the NMS is defined in a MIB

Applications

- Remote monitoring of various nodes in your network
- Performance measurement for Network
- Congestion control in private networks
- Failure Management
- Risk Management

Scope of Research

- Network Management softwares

Assignment

- Differentiate between Pooling and Traps.