Unit 5

Introduction to Network Management

Remote Monitoring Techniques

- **DEFINITION:**

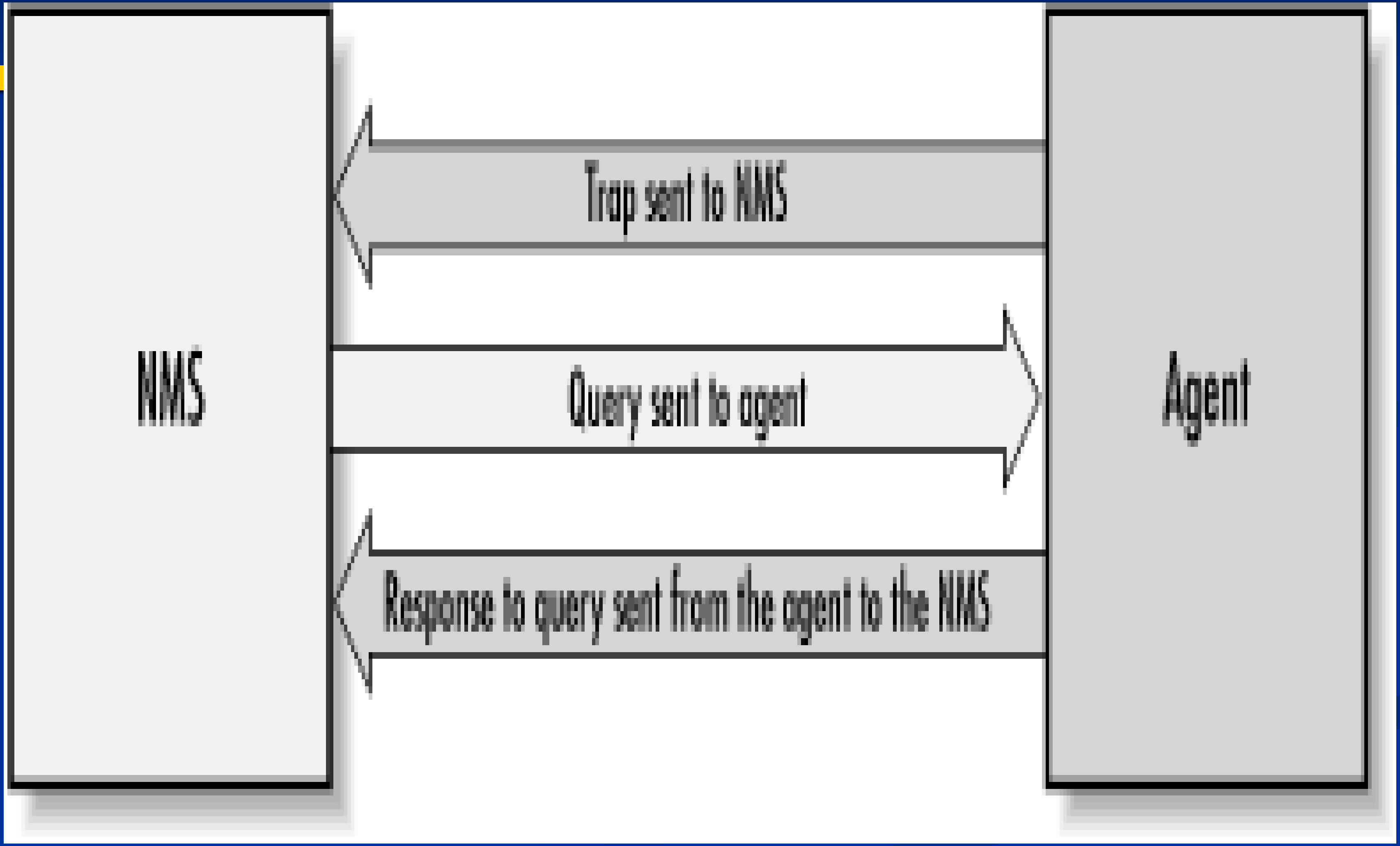
  RMON (Remote Network Monitoring) was developed to help us understand how the network itself is functioning, as well as how individual devices on the network are affecting the network as a whole.

  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 (SNMP)

- 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

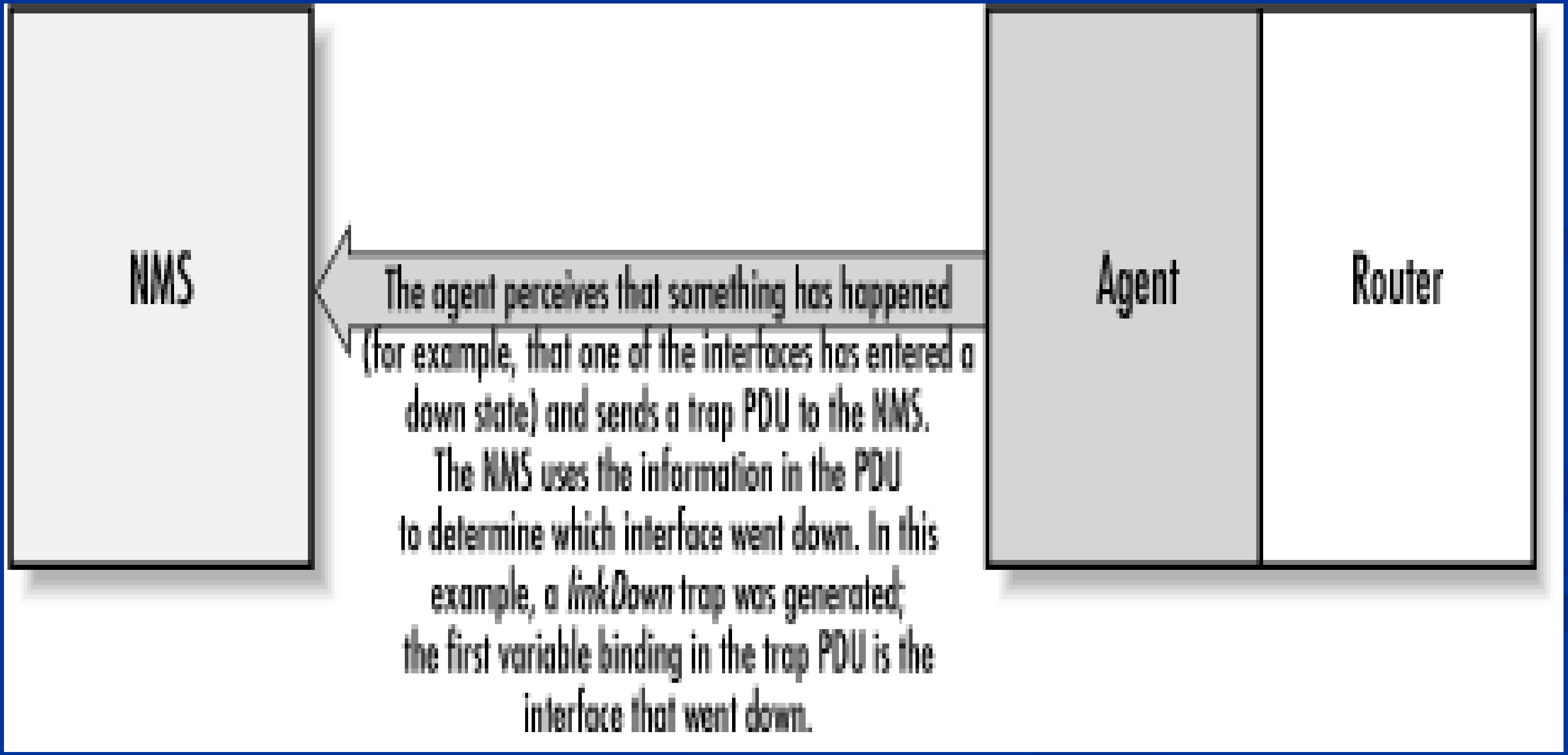
- In the world of SNMP there are two kind of entities: ***managers*** and ***agents.***
- A **manager** is a server running some kind of software system that can handle management tasks for a network. Managers are often referred to as *Network Management Stations* (NMSs).
- An NMS is responsible for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

- 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.



The agent perceives that something has happened (for example, that one of the interfaces has entered a down state) and sends a trap PDU to the NMS. The NMS uses the information in the PDU to determine which interface went down. In this example, a *linkDown* trap was generated; the first variable binding in the trap PDU is the interface that went down.

SNMP Traps cont..

- 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.
- Here are a few situations that a trap might report:
  - 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

- 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?). .

- 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 certain level.

- **TIP:** 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.

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

Proxy Servers

- In computer networks, a proxy server is a server (a computer system or an application program) that acts as an intermediary between for requests from clients seeking resources from the other servers.
- A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server.
- The proxy server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol. If the request is validated by the filter, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client. A proxy server may optionally alter the client's request or the server's response, and sometimes it may serve the request without contacting the specified server.
- In this case, it 'caches‘(i.e. stores) responses from the remote server, and returns subsequent requests for the same content directly.

Proxy server has many potential purposes, including:

- To keep machines behind it anonymous (mainly for security)
- To speed up access to resources (using caching). Web proxies are commonly used to cache or reserve web pages from a web server.
- To apply access policy to network services or content, e.g. to block undesired sites.
- To log / audit usage, i.e. to provide company employee Internet usage reporting.
- To bypass security/ parental controls.
- To scan transmitted content for malware before delivery.
- To scan outbound content, e.g., for data leak protection.
- To circumvent regional restrictions.

Firewalls

- Sits between two networks
  - Used to protect one from the other
  - Places a bottleneck between the networks
    - All communications must pass through the bottleneck – this gives us a single point of control

Protection Methods

- **Packet Filtering**
  - Rejects TCP/IP packets from unauthorized hosts and/or connection attempts bt unauthorized hosts
- **Network Address Translation (NAT)**
  - Translates the addresses of internal hosts so as to hide them from the outside world
  - Also known as IP masquerading
- **Proxy Services**
  - Makes high level application level connections to external hosts on behalf of internal hosts to completely break the network connection between internal and external hosts

Additional services sometimes provided

- **Virus Scanning**
  - Searches incoming data streams for virus signatures so they may be blocked
  - Done by subscription to stay current
    - McAfee / Norton
- **Content Filtering**
  - Allows the blocking of internal users from certain types of content.
    - Usually an add-on to a proxy server
    - Usually a separate subscription service as it is too hard and time consuming to keep current

Packet Filters

- Compare network and transport protocols to a database of rules and then forward only the packets that meet the criteria of the rules
- Implemented in routers and sometimes in the TCP/IP stacks of workstation machines
  - in a router a filter prevents suspicious packets from reaching your network
  - in a TCP/IP stack it prevents that specific machine from responding to suspicious traffic
    - should only be used in addition to a filtered router not instead of a filtered router

Limitations of Packet Filters

- IP addresses of hosts on the protected side of the filter can be readily determined by observing the packet traffic on the unprotected side of the filter
- filters cannot check all of the fragments of higher level protocols (like TCP) as the TCP header information is only available in the first fragment.
  - Modern firewalls reconstruct fragments then checks them
- filters are not sophisticated enough to check the validity of the application level protocols imbedded in the TCP packets

Network Address Translation

- Single host makes requests on behalf of all internal users
  - hides the internal users behind the NAT's IP address
  - internal users can have any IP address
    - should use the reserved ranges of 192.168.n.m or 10.n.m.p to avoid possible conflicts with duplicate external addresses
- Only works at the TCP/IP level
  - doesn't do anything for addresses in the payloads of the packets

Proxies

- Hides internal users from the external network by hiding them behind the IP of the proxy
- Prevents low level network protocols from going through the firewall eliminating some of the problems with NAT
- Restricts traffic to only the application level protocols being proxied
- proxy is a combination of a client and a server; internal users send requests to the server portion of the proxy which then sends the internal users requests out through its client (keeps track of which users requested what, do redirect returned data back to appropriate user)
- Address seen by the external network is the address of the proxy
- Everything possible is done to hide the identity of the internal user
  - e-mail addresses in the http headers are not propagated through the proxy
- Doesn’t have to be actual part of the Firewall, any server sitting between the two networks can be used

Content filtering

- Since an enterprise owns the computing and network facilities used by employees, it is perfectly within it’s rights to attempt to limit internet access to sites that could be somehow related to business
  - Since the proxy server is a natural bottle neck for observing all of the external requests being made from the internal network it is the natural place to check content
  - This is usually done by subscription to a vendor that specializes in categorizing websites into content types based on observation
  - Usually an agent is installed into the proxy server that compares URL requests to a database of URLs to reject
  - All access are then logged and reported, most companies then review the reported access violations and usually a committee reviews and decides whether or not any personnel action should be taken (letter of reprimand, dismissal, ect)
  - Sites that are usually filtered are those containing information about or pertaining to:
    - Gambling
    - Pornography

Effective Border Security

- For an absolute minimum level of Internet security a Firewall must provide all three basic functions
  - Packet filtering
  - Network Address translation
  - High-level application proxying
- Use the Firewall machine just for the firewall
  - Won’t have to worry about problems with vulnerabilities of the application software
    - If possible use one machine per application level server
      - Just because a machine has a lot of capacity don’t just pile things on it.
        - Isolate applications, a side benefit of this is if a server goes down you don’t lose everything
  - If possible make the Firewall as anonymous as possible
    - Hide the product name and version details, esp, from the Internet

Problems Firewalls can't fix

- Many e-mail hacks
  - Remember in CS-328 how easy it is to spoof e-mail
- Vulnerabilities in application protocols you allow
  - Ex. Incoming HTTP requests to an IIS server
- Modems
  - Don't allow users on the internal network to use a modem in their machine to connect to and external ISP (AOL) to connect to the Internet, this exposes everything that user is connected to the external network
  - Many users don't like the restrictions that firewalls place on them and will try to subvert those restrictions

Firewalls Aren’t Perfect?

- Useless against attacks from the inside
  - Evildoer exists on inside
  - Malicious code is executed on an internal machine
- Organizations with greater insider threat
  - Banks and Military
- Protection must exist at each layer
  - Assess risks of threats at every layer
- Cannot protect against transfer of all virus infected programs or files
  - because of huge range of O/S & file types

Network Management

- Network management is the process of controlling a complex data network to maximize its efficiency and productivity.

- The overall goal of network management is to help with the complexity of a data network and to ensure that data can go across it with maximum efficiency and transparency to the users.

Network Management

- The International Organization for Standardization (ISO) Network Management Forum divided network management into five functional areas:
  - Fault Management
  - Configuration Management
  - Security Management
  - Performance Management
  - Accounting Management

Fault Management

- Is the process of locating problems, or faults, on the data network

- It involves the following steps:
  - Discover the problem
  - Isolate the problem
  - Fix the problem (if possible)

Configuration Management

- The configuration of certain network devices controls the behavior of the data network.

- Configuration management is the process of finding and setting up (configuring) these critical devices.

Security Management

- Is the process of controlling access to information on the data network.

- Provides a way to monitor access points and records information on a periodic basis.

- Provides audit trails and sounds alarms for security breaches.

Performance Management

- Involves measuring the performance of the network hardware, software and media
- Example of measured activities are:
  - Overall throughput
  - Percentage utilization
  - Error rates
  - Response time.

Network Management Tasks

- fault management
- configuration management
- performance management
- security management
- inventory management
- accounting management

Our main concern is Performance Management & Security Management.

Performance Management

- What is the level of capacity utilization?
- Is there excessive traffic?
- Has throughput been reduced to unacceptable levels?
- Are there bottlenecks?
- Is response time increasing?
- Indicators: availability, response time, accuracy throughput, utilization
- Service efficiency..

---

network throughput is the average rate of successful message delivery over a communication channel.

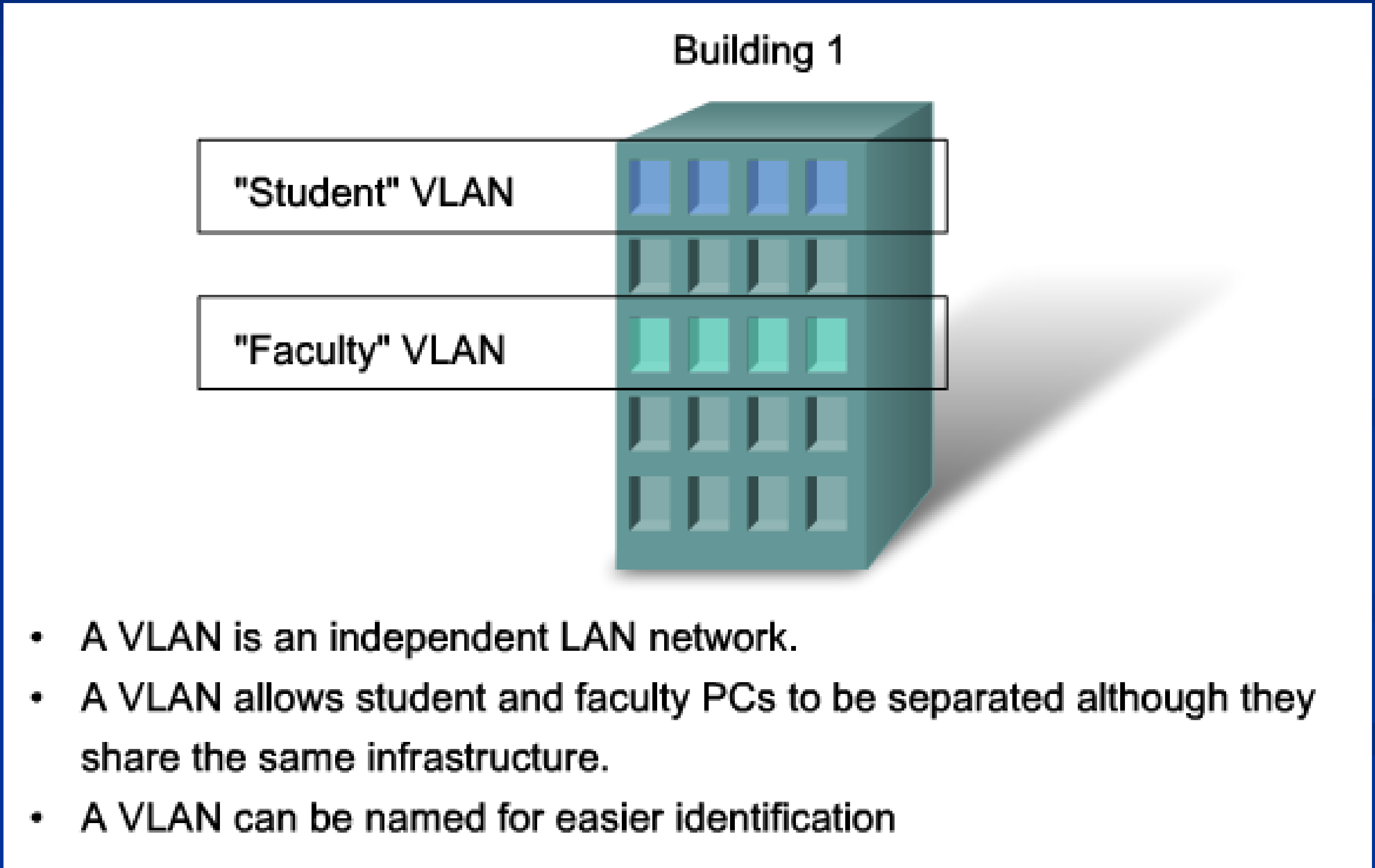
Security Management

- Security management
  - Security services: generating, distributing, storing of encryption keys for services
  - Exception alarm generation, detection of problems
  - Uniform access control to resources
  - Backups, data security
  - Security logging

Virtual LANs

- A VLAN allows a network administrator to create groups of logically networked devices that act as if they are on their own independent network, even if they share a common infrastructure with other VLANs.
- Using VLANs, you can logically segment switched networks based on functions, departments, or project teams.
- You can also use a VLAN to geographically structure your network to support the growing reliance of companies on home-based workers.
- These VLANs allow the network administrator to implement access and security policies to particular groups of users.

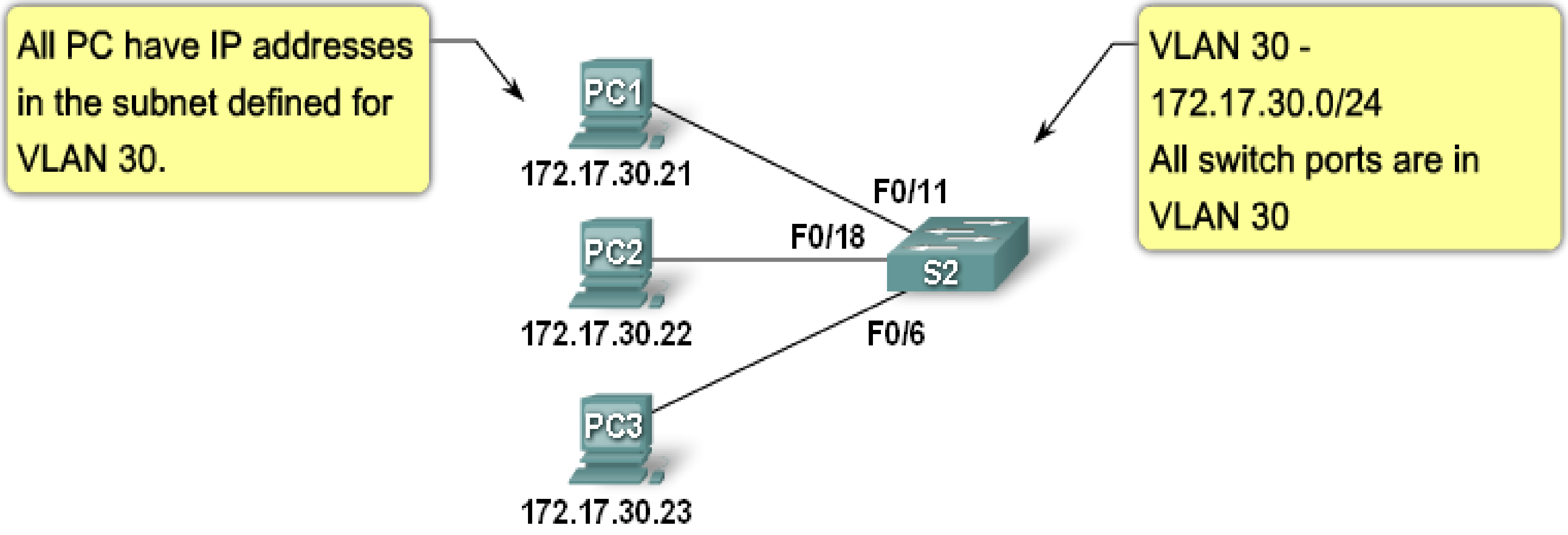
Example



- A VLAN is an independent LAN network.
- A VLAN allows student and faculty PCs to be separated although they share the same infrastructure.
- A VLAN can be named for easier identification

- A VLAN is a logically separate IP subnetwork.
- VLANs allow multiple IP networks and subnets to exist on the same switched network.
- For computers to communicate on the same VLAN, each must have an IP address and a subnet mask that is consistent for that VLAN.
- The switch has to be configured with the VLAN and each port in the VLAN must be assigned to the VLAN.

- A switch port with a singular VLAN configured on it is called an access port.
- Remember, just because two computers are physically connected to the same switch does not mean that they can communicate.
- Devices on two separate networks and subnets must communicate via a router (Layer 3), whether or not VLANs are used.



All PC have IP addresses in the subnet defined for VLAN 30.

VLAN 30 - 172.17.30.0/24
All switch ports are in VLAN 30

- A VLAN = Subnet (in modern switched LANs)
- On the switch
  - Configure the VLAN
  - Assign the port to the VLAN
- On the PC assign an IP address in the VLAN subnet

Benefits of VLAN

- Security - Groups that have sensitive data are separated from the rest of the network, decreasing the chances of confidential information breaches.
  - Faculty computers are on VLAN 10 and completely separated from student and guest data traffic.
- Cost reduction - Cost savings result from less need for expensive network upgrades and more efficient use of existing bandwidth and uplinks.

- Higher performance - Dividing flat Layer 2 networks into multiple logical workgroups (broadcast domains) reduces unnecessary traffic on the network and boosts performance.