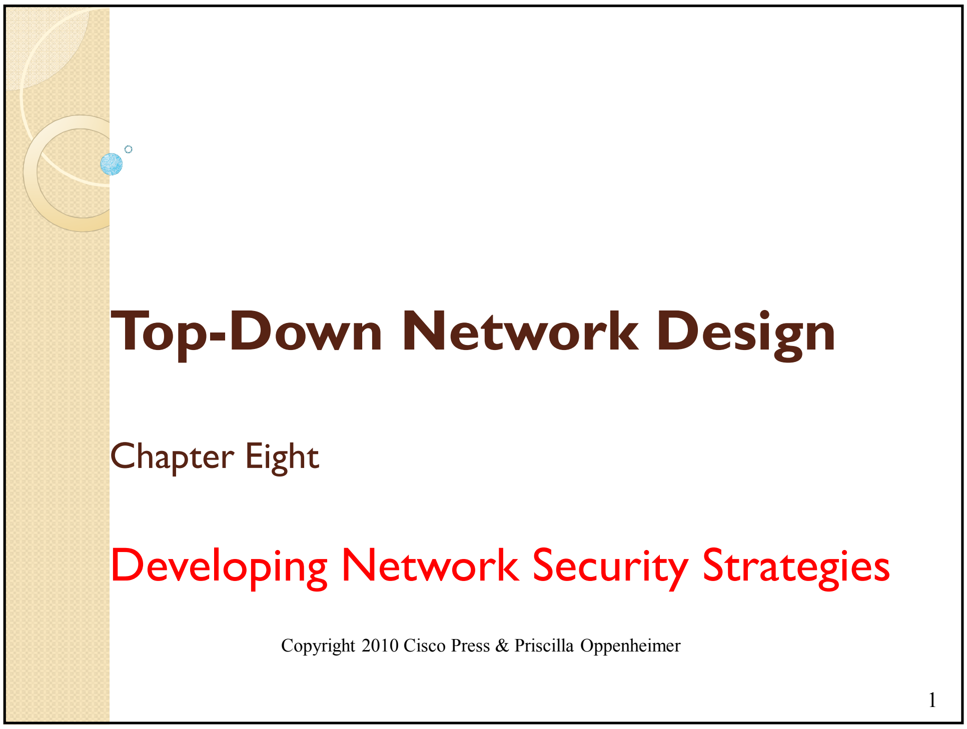
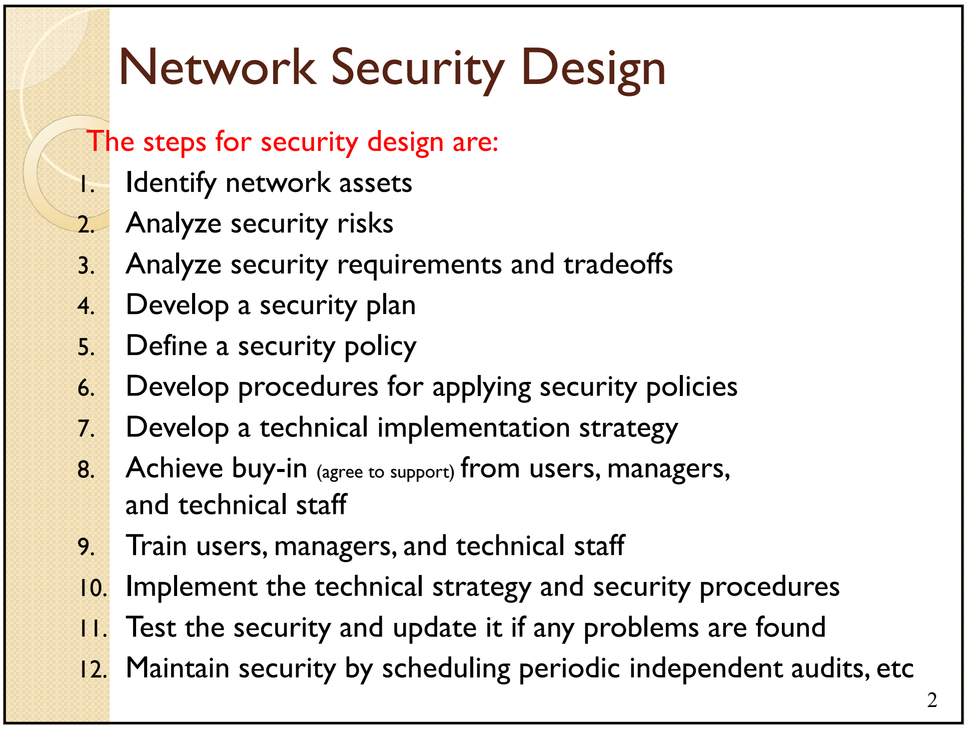


Top-Down Network Design

Chapter Eight

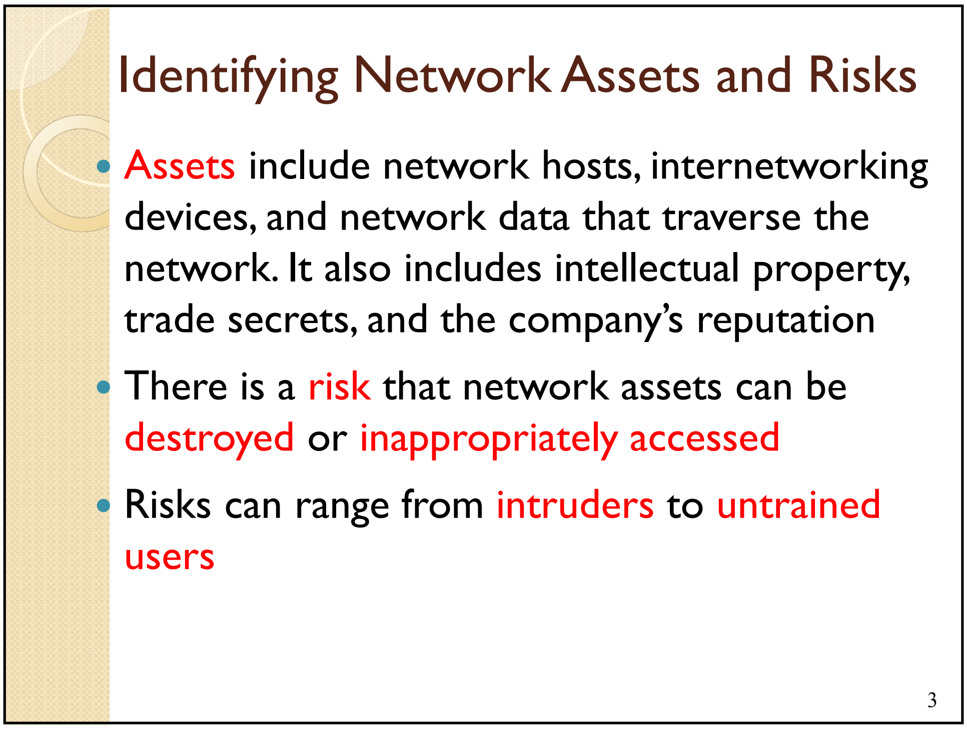
Developing Network Security Strategies



Network Security Design

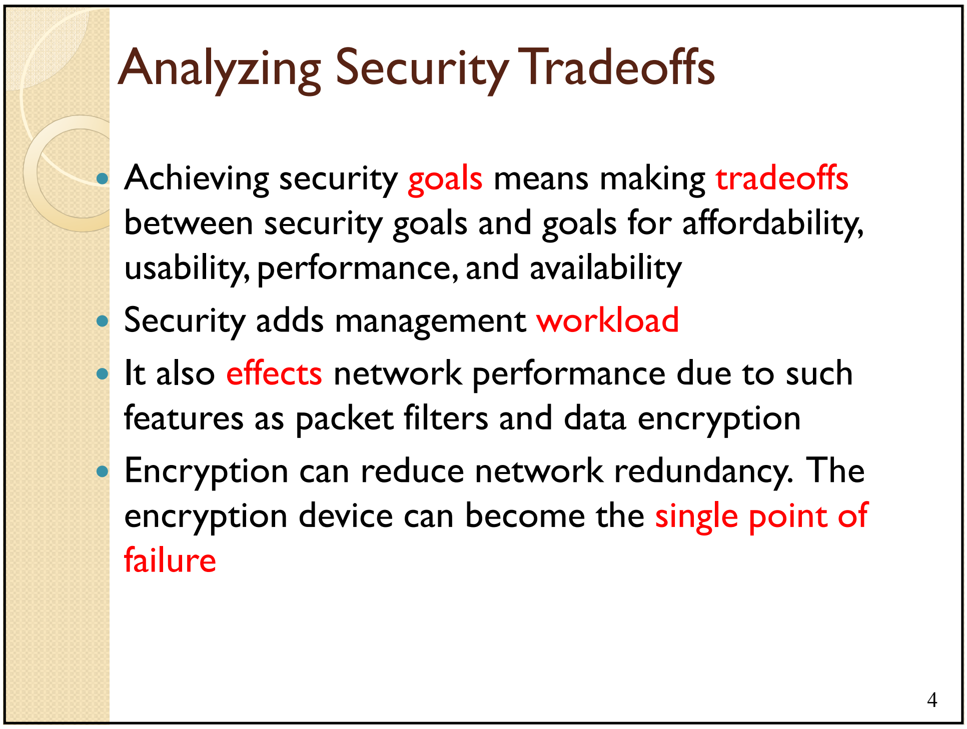
The steps for security design are:

1. Identify network assets
2. Analyze security risks
3. Analyze security requirements and tradeoffs
4. Develop a security plan
5. Define a security policy
6. Develop procedures for applying security policies
7. Develop a technical implementation strategy
8. Achieve buy-in (agree to support) from users, managers, and technical staff
9. Train users, managers, and technical staff
10. Implement the technical strategy and security procedures
11. Test the security and update it if any problems are found
12. Maintain security by scheduling periodic independent audits, etc



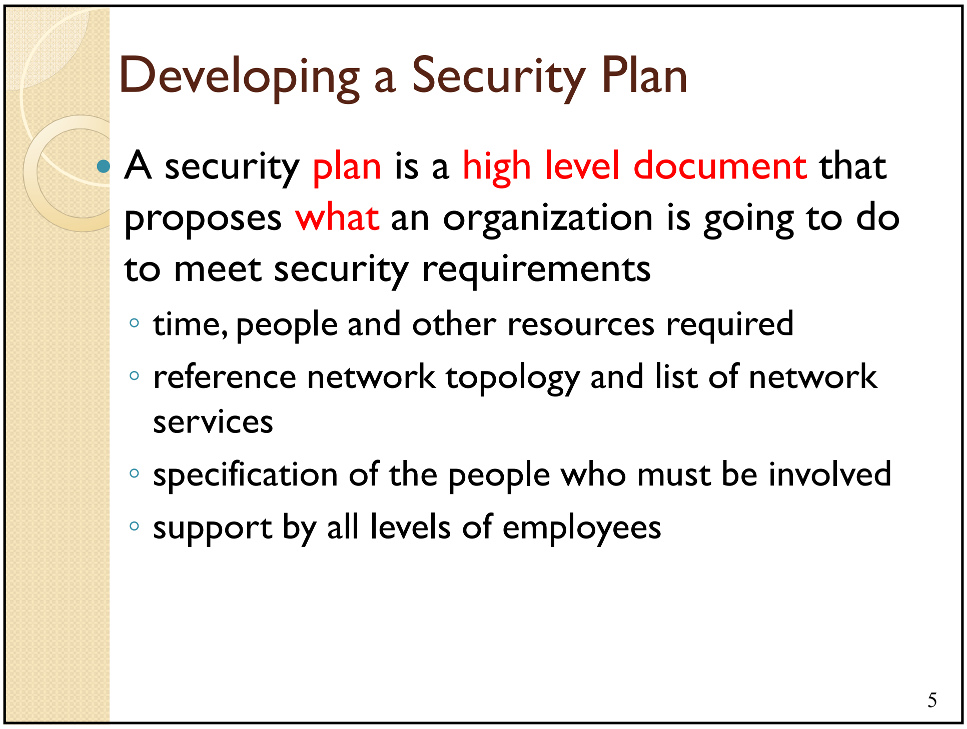
Identifying Network Assets and Risks

- Assets include network hosts, internetworking devices, and network data that traverse the network. It also includes intellectual property, trade secrets, and the company's reputation
- There is a risk that network assets can be destroyed or inappropriately accessed
- Risks can range from intruders to untrained users



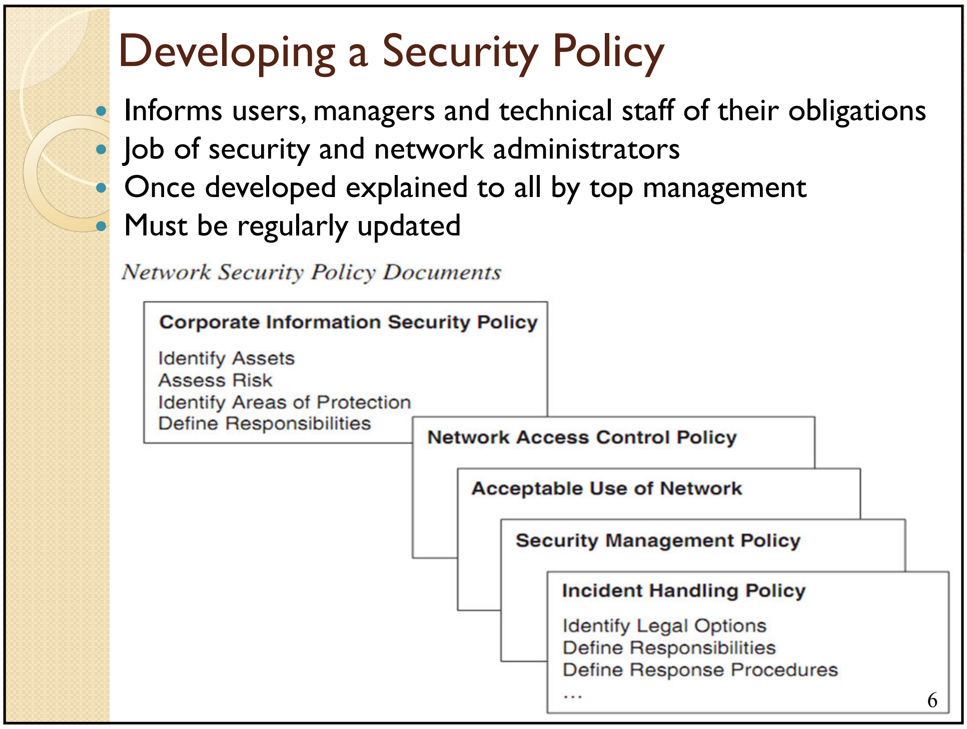
Analyzing Security Tradeoffs

- Achieving security goals means making tradeoffs between security goals and goals for affordability, usability, performance, and availability
- Security adds management workload
- It also effects network performance due to such features as packet filters and data encryption
- Encryption can reduce network redundancy. The encryption device can become the single point of failure



Developing a Security Plan

- A security plan is a high level document that proposes what an organization is going to do to meet security requirements
  - time, people and other resources required
  - reference network topology and list of network services
  - specification of the people who must be involved
  - support by all levels of employees



Developing a Security Policy

- Informs users, managers and technical staff of their obligations
- Job of security and network administrators
- Once developed explained to all by top management
- Must be regularly updated

Network Security Policy Documents

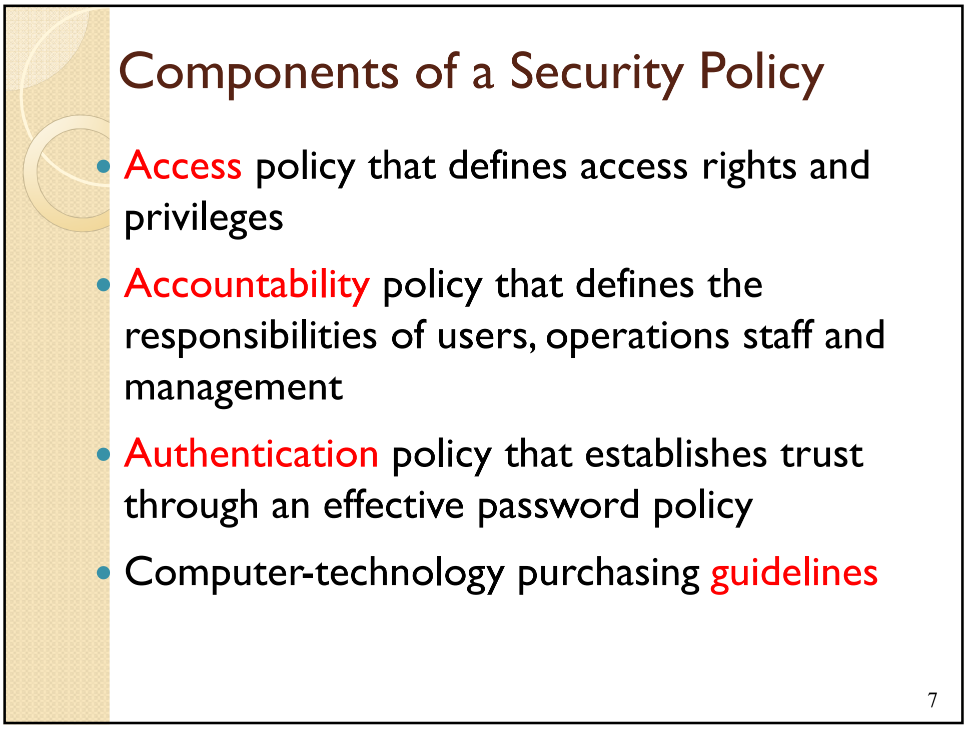
Corporate Information Security Policy
Identify Assets
Assess Risk
Identify Areas of Protection
Define Responsibilities

Network Access Control Policy

Acceptable Use of Network

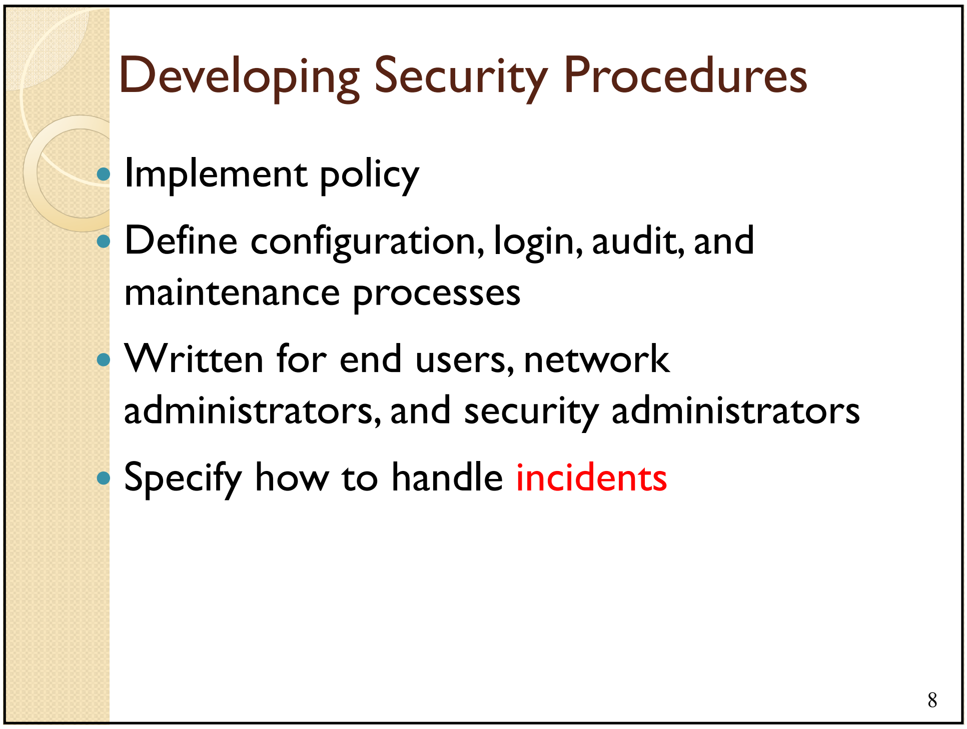
Security Management Policy

Incident Handling Policy
Identify Legal Options
Define Responsibilities
Define Response Procedures
…



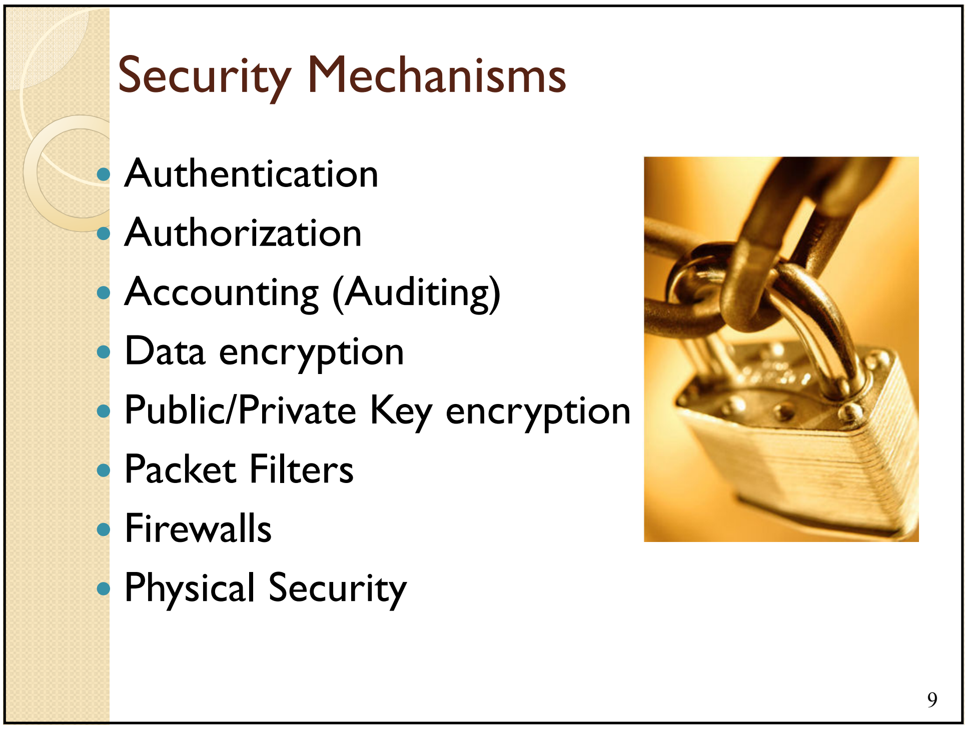
Components of a Security Policy

- Access policy that defines access rights and privileges
- Accountability policy that defines the responsibilities of users, operations staff and management
- Authentication policy that establishes trust through an effective password policy
- Computer-technology purchasing guidelines



Developing Security Procedures

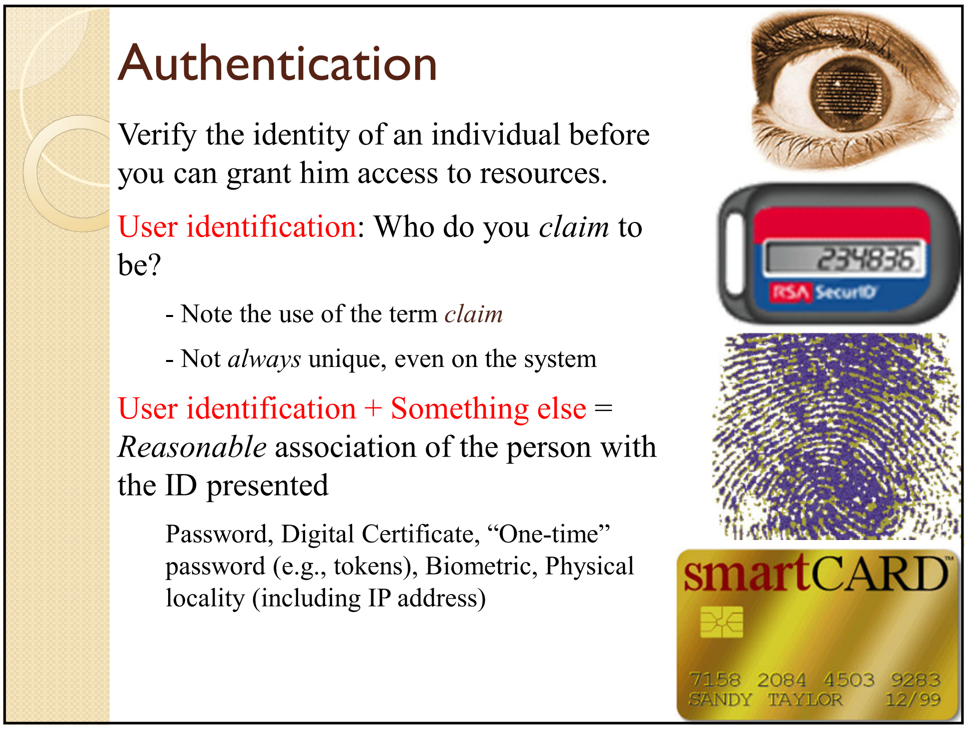
- Implement policy
- Define configuration, login, audit, and maintenance processes
- Written for end users, network administrators, and security administrators
- Specify how to handle incidents



Security Mechanisms

- Authentication
- Authorization
- Accounting (Auditing)
- Data encryption
- Public/Private Key encryption
- Packet Filters
- Firewalls
- Physical Security

9



Authentication

Verify the identity of an individual before you can grant him access to resources.

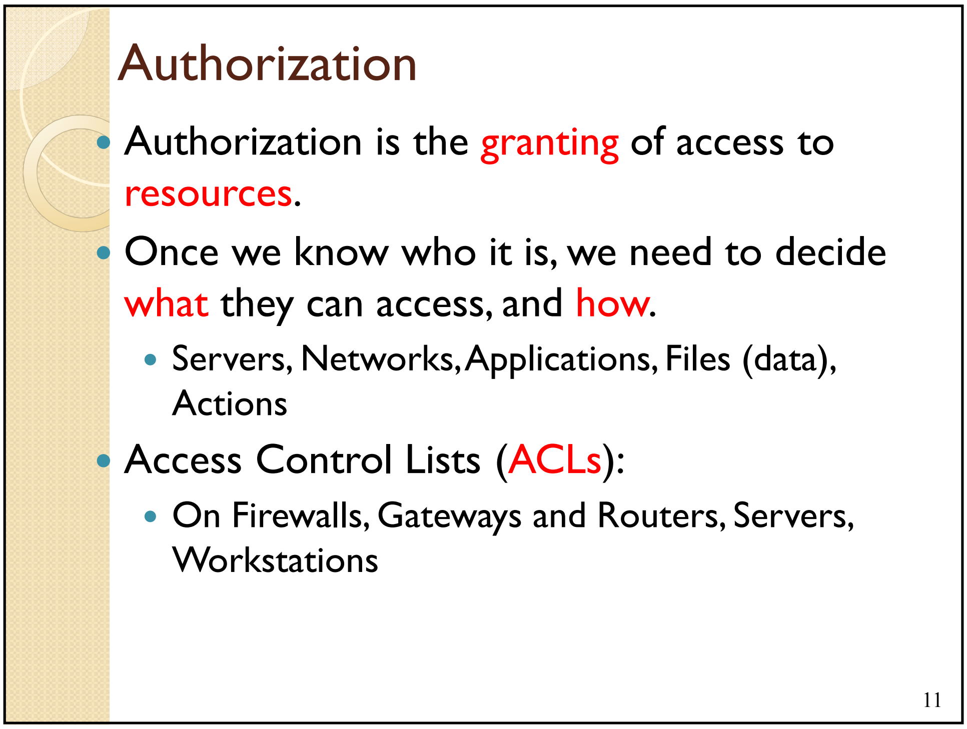
User identification: Who do you *claim* to be?

- Note the use of the term *claim*

- Not *always* unique, even on the system

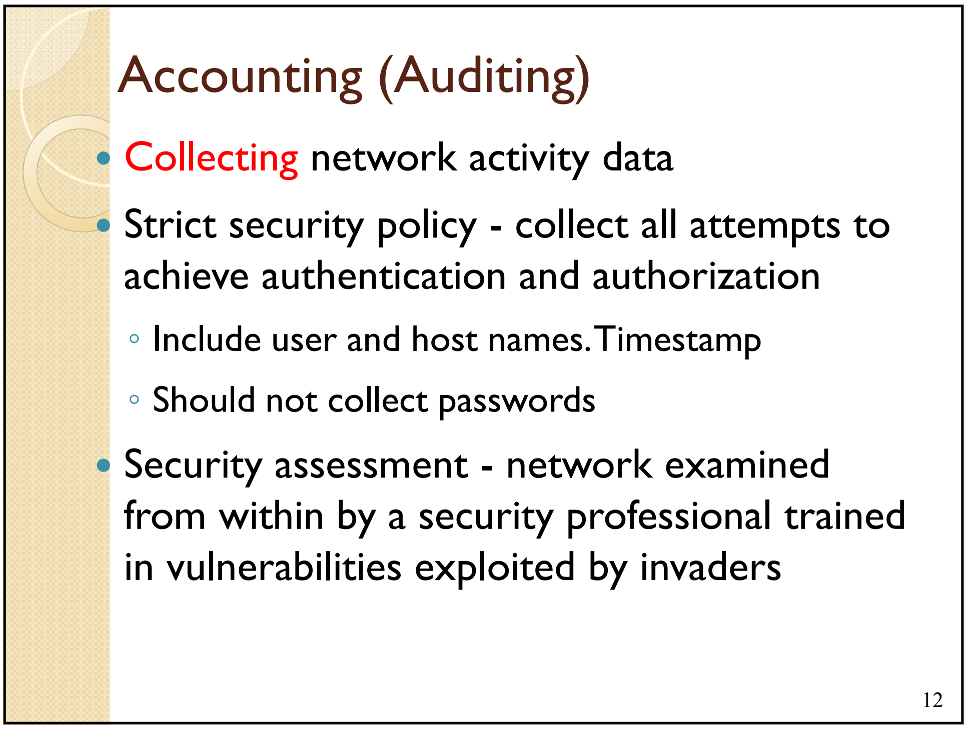
User identification + Something else = *Reasonable* association of the person with the ID presented

Password, Digital Certificate, “One-time” password (e.g., tokens), Biometric, Physical locality (including IP address)



Authorization

- Authorization is the granting of access to resources.
- Once we know who it is, we need to decide what they can access, and how.
  - Servers, Networks, Applications, Files (data), Actions
- Access Control Lists (ACLs):
  - On Firewalls, Gateways and Routers, Servers, Workstations



Accounting (Auditing)

- Collecting network activity data
- Strict security policy - collect all attempts to achieve authentication and authorization
  - Include user and host names. Timestamp
  - Should not collect passwords
- Security assessment - network examined from within by a security professional trained in vulnerabilities exploited by invaders

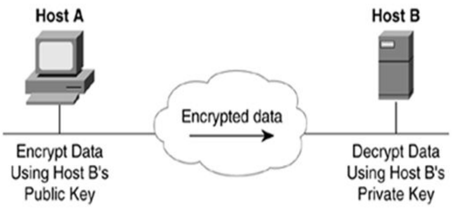
Data Encryption

- Process that scrambles data to protect it from being read by anyone but the intended receiver
- Useful for providing data confidentiality
- Tradeoffs
- Encryption algorithm is a set of instructions to scramble and unscramble data
- Encryption key is a code used by an algorithm to scramble and unscramble data

13

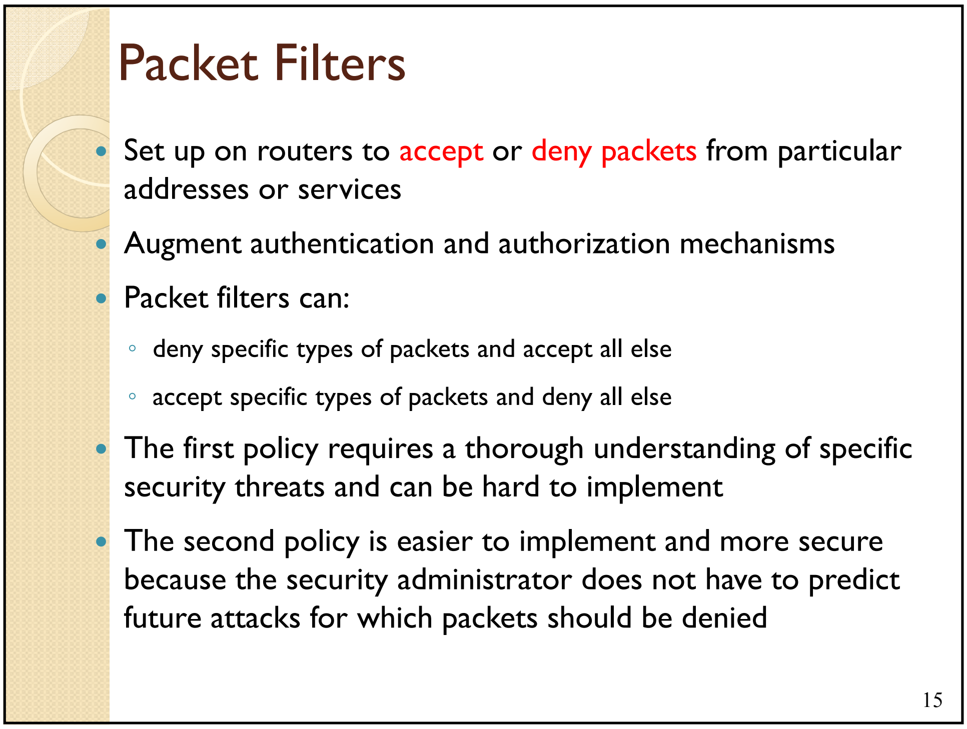
Public/Private Key Encryption

- Best known example of an asymmetric key system
- Each station has a public key that is openly published or easily demanded


Host A
Host B
Encrypted data
Encrypt Data Using Host B's Public Key
Decrypt Data Using Host B's Private Key

- Receiving station decrypts using its own private key. Since no other stations have the key they cannot decrypt
- Public/private key provides both confidentiality & authentication
- The asymmetric keys allow the recipient to verify that a document came from who it said it was
- Encrypting all or part of your document with your private key results in a digital signature

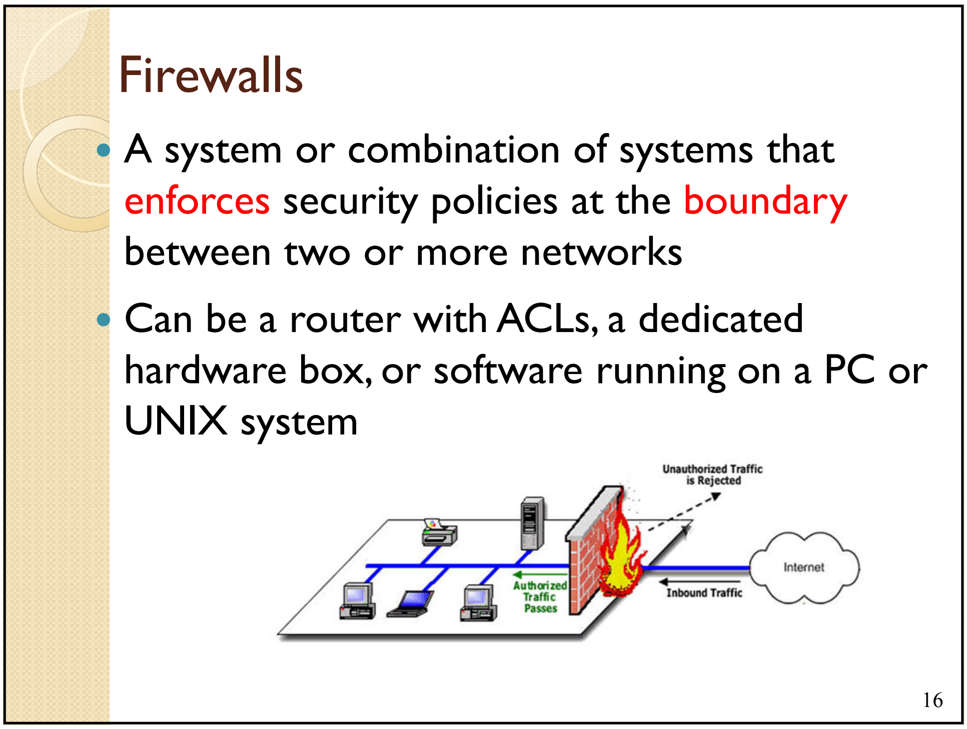
14



Packet Filters

- Set up on routers to accept or deny packets from particular addresses or services
- Augment authentication and authorization mechanisms
- Packet filters can:
  - deny specific types of packets and accept all else
  - accept specific types of packets and deny all else
- The first policy requires a thorough understanding of specific security threats and can be hard to implement
- The second policy is easier to implement and more secure because the security administrator does not have to predict future attacks for which packets should be denied

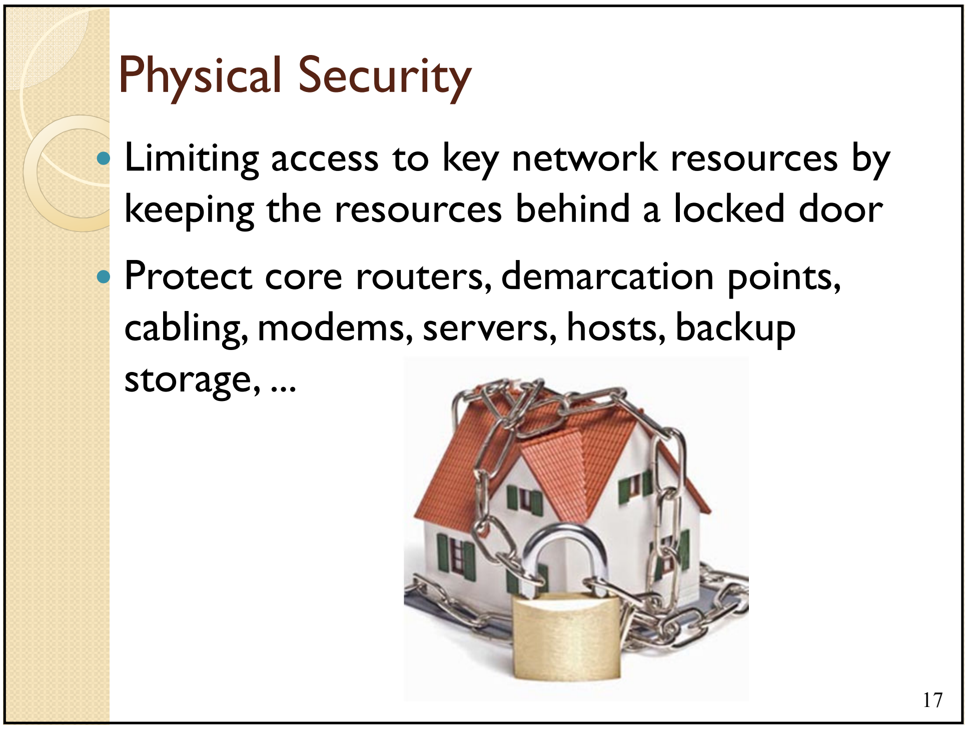
15



Firewalls

- A system or combination of systems that enforces security policies at the boundary between two or more networks
- Can be a router with ACLs, a dedicated hardware box, or software running on a PC or UNIX system

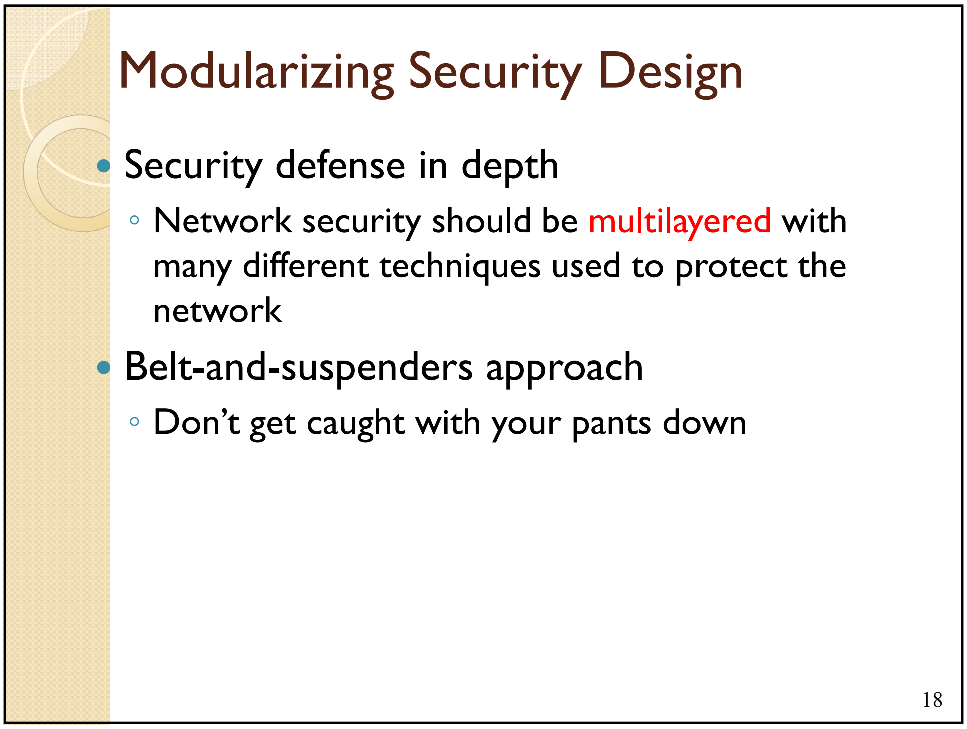
16



Physical Security

- Limiting access to key network resources by keeping the resources behind a locked door
- Protect core routers, demarcation points, cabling, modems, servers, hosts, backup storage, ...

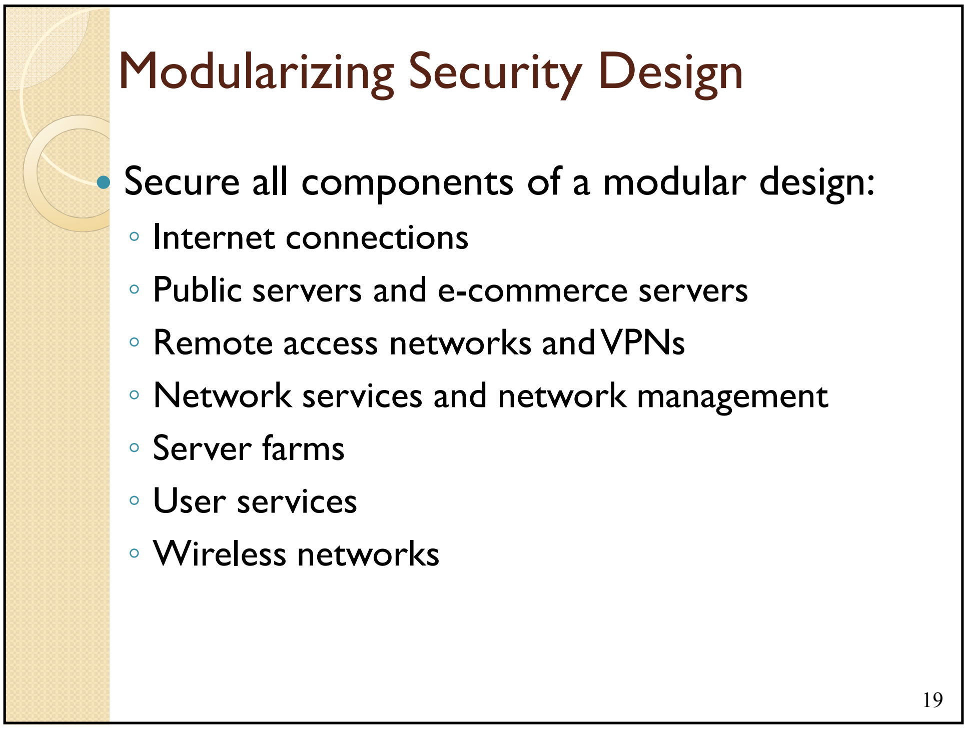
17



Modularizing Security Design

- Security defense in depth
  - Network security should be multilayered with many different techniques used to protect the network
- Belt-and-suspenders approach
  - Don’t get caught with your pants down

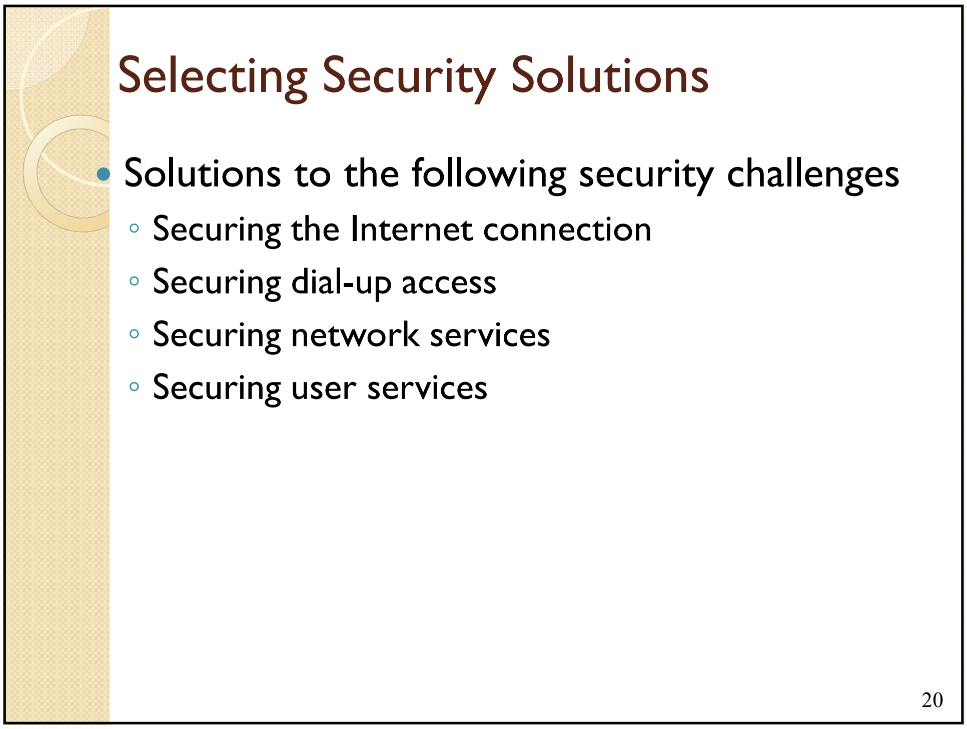
18



Modularizing Security Design

- Secure all components of a modular design:
  - Internet connections
  - Public servers and e-commerce servers
  - Remote access networks and VPNs
  - Network services and network management
  - Server farms
  - User services
  - Wireless networks

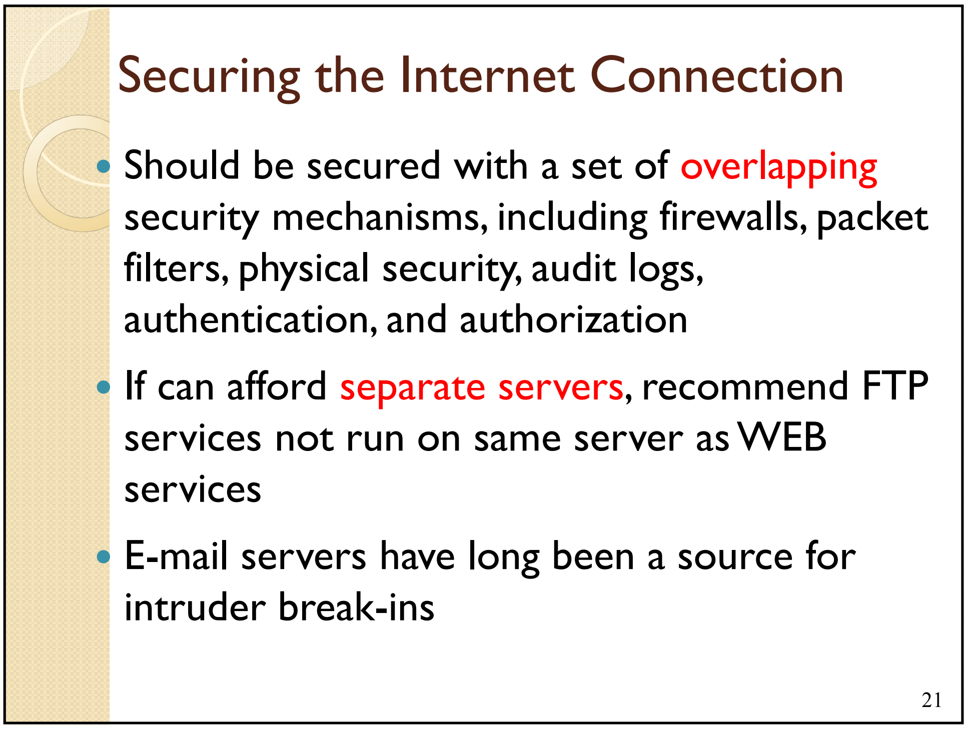
19



Selecting Security Solutions

- Solutions to the following security challenges
  - Securing the Internet connection
  - Securing dial-up access
  - Securing network services
  - Securing user services

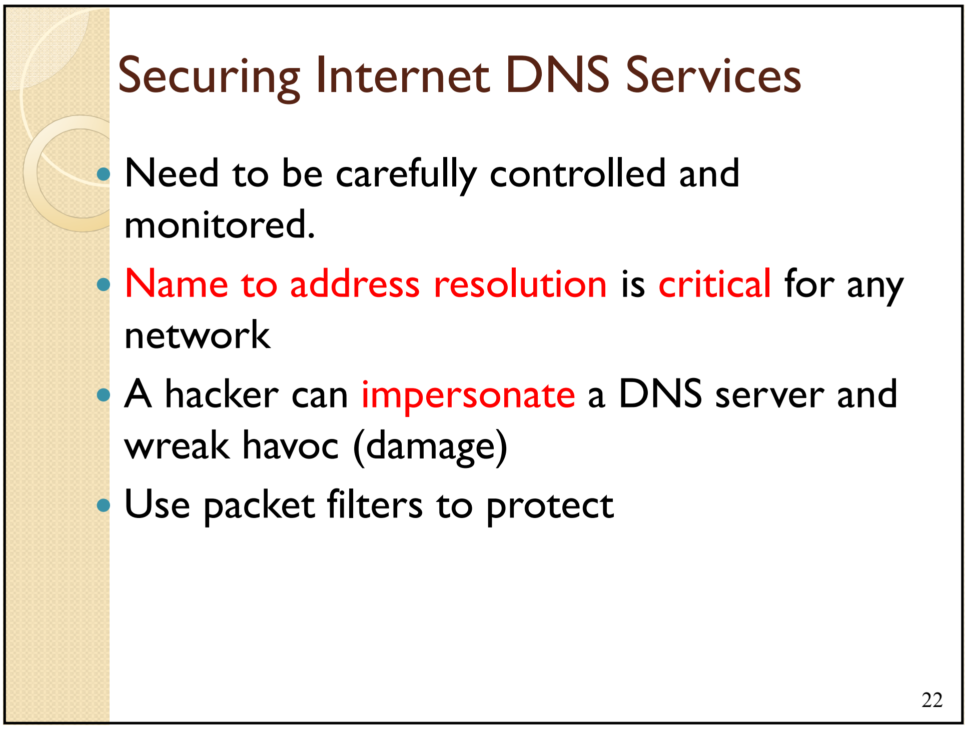
20



Securing the Internet Connection

- Should be secured with a set of overlapping security mechanisms, including firewalls, packet filters, physical security, audit logs, authentication, and authorization
- If can afford separate servers, recommend FTP services not run on same server as WEB services
- E-mail servers have long been a source for intruder break-ins

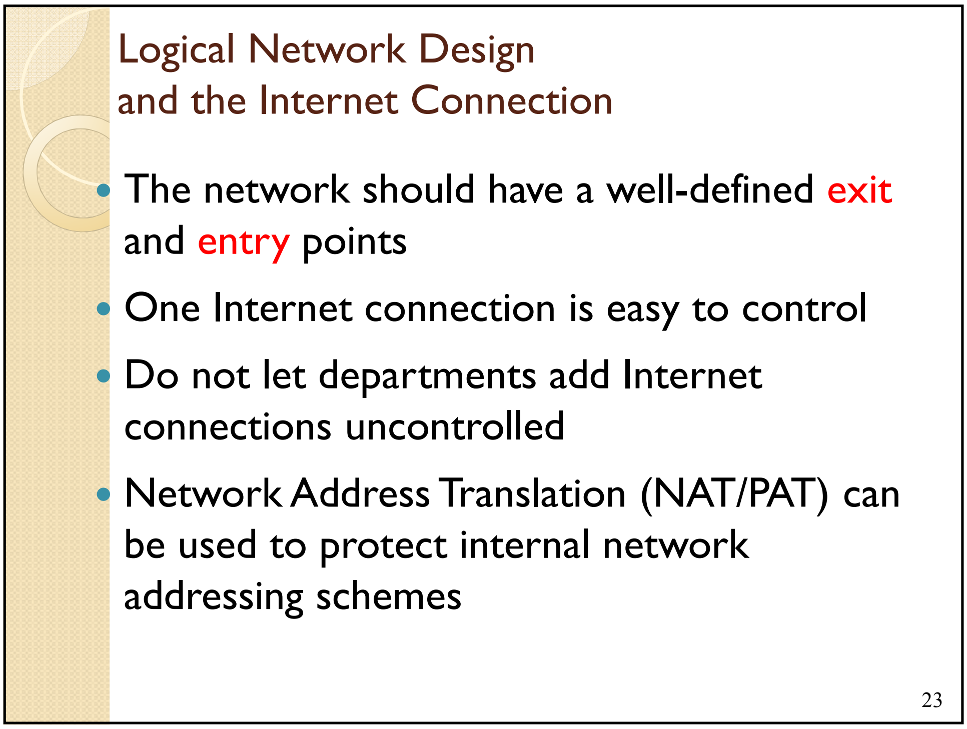
21



Securing Internet DNS Services

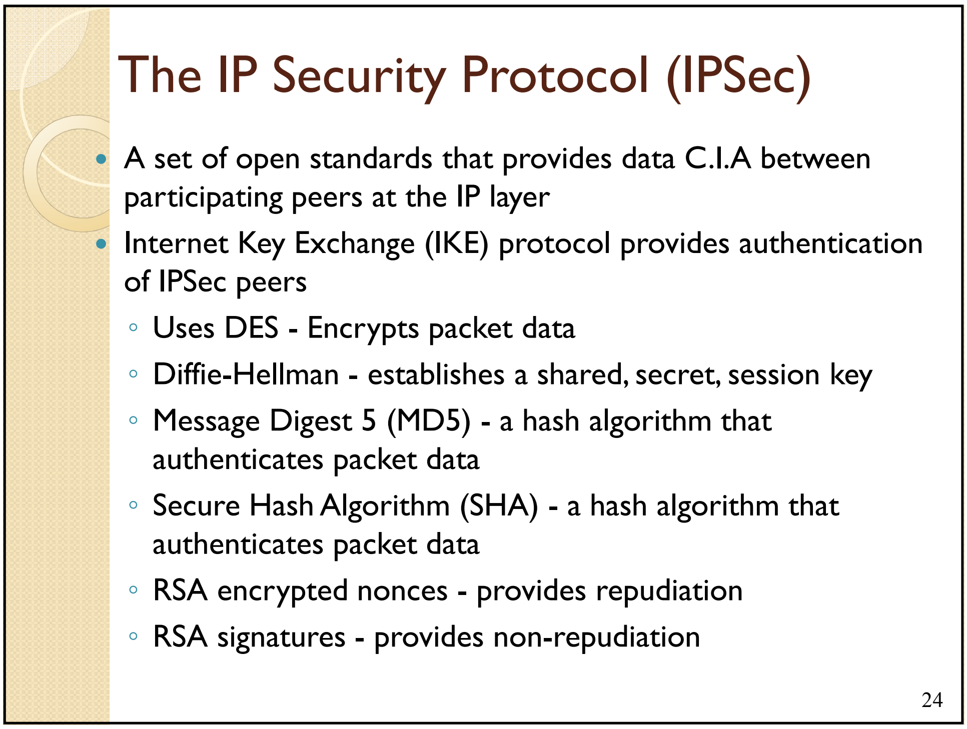
- Need to be carefully controlled and monitored.
- Name to address resolution is critical for any network
- A hacker can impersonate a DNS server and wreak havoc (damage)
- Use packet filters to protect

22



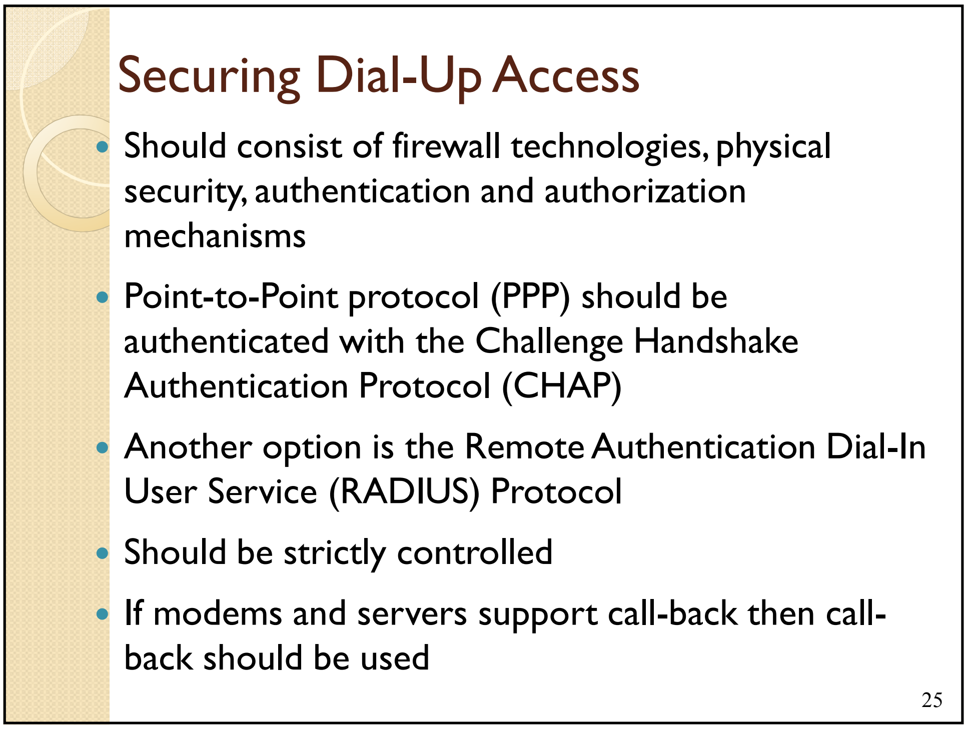
Logical Network Design and the Internet Connection

- The network should have a well-defined exit and entry points
- One Internet connection is easy to control
- Do not let departments add Internet connections uncontrolled
- Network Address Translation (NAT/PAT) can be used to protect internal network addressing schemes



The IP Security Protocol (IPSec)

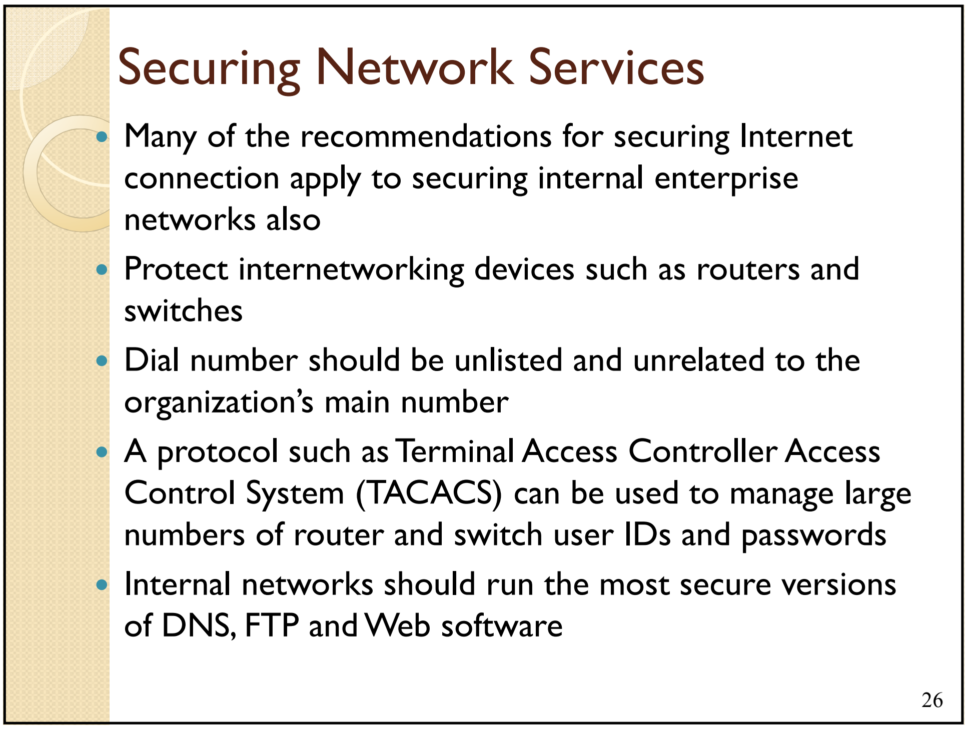
- A set of open standards that provides data C.I.A between participating peers at the IP layer
- Internet Key Exchange (IKE) protocol provides authentication of IPSec peers
  - Uses DES - Encrypts packet data
  - Diffie-Hellman - establishes a shared, secret, session key
  - Message Digest 5 (MD5) - a hash algorithm that authenticates packet data
  - Secure Hash Algorithm (SHA) - a hash algorithm that authenticates packet data
  - RSA encrypted nonces - provides repudiation
  - RSA signatures - provides non-repudiation



Securing Dial-Up Access

- Should consist of firewall technologies, physical security, authentication and authorization mechanisms
- Point-to-Point protocol (PPP) should be authenticated with the Challenge Handshake Authentication Protocol (CHAP)
- Another option is the Remote Authentication Dial-In User Service (RADIUS) Protocol
- Should be strictly controlled
- If modems and servers support call-back then call-back should be used

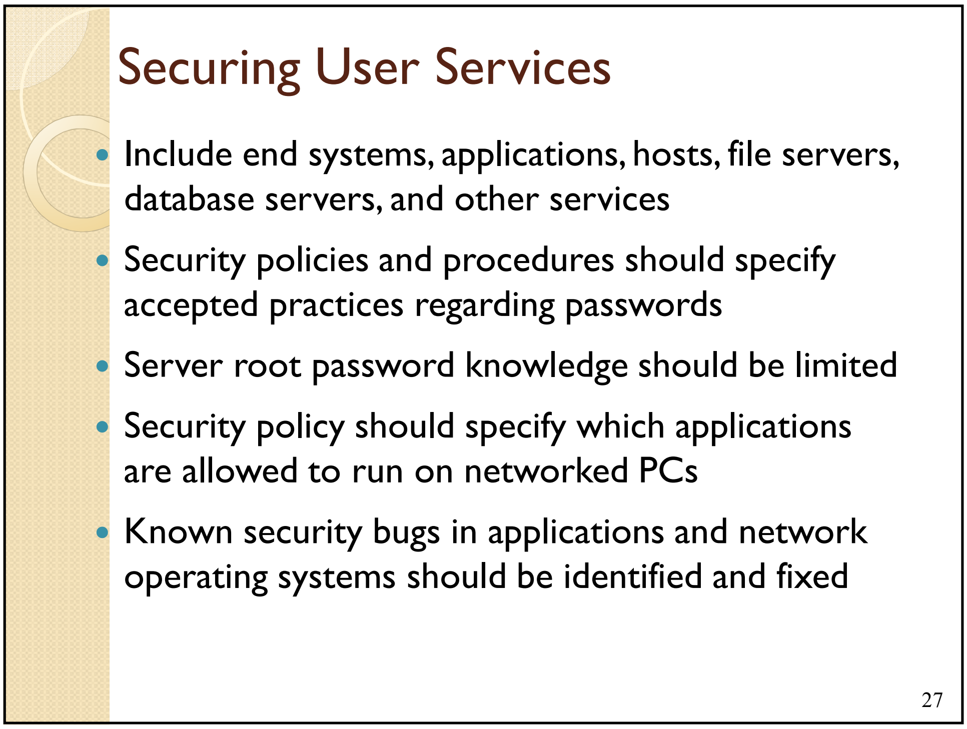
25



Securing Network Services

- Many of the recommendations for securing Internet connection apply to securing internal enterprise networks also
- Protect internetworking devices such as routers and switches
- Dial number should be unlisted and unrelated to the organization’s main number
- A protocol such as Terminal Access Controller Access Control System (TACACS) can be used to manage large numbers of router and switch user IDs and passwords
- Internal networks should run the most secure versions of DNS, FTP and Web software

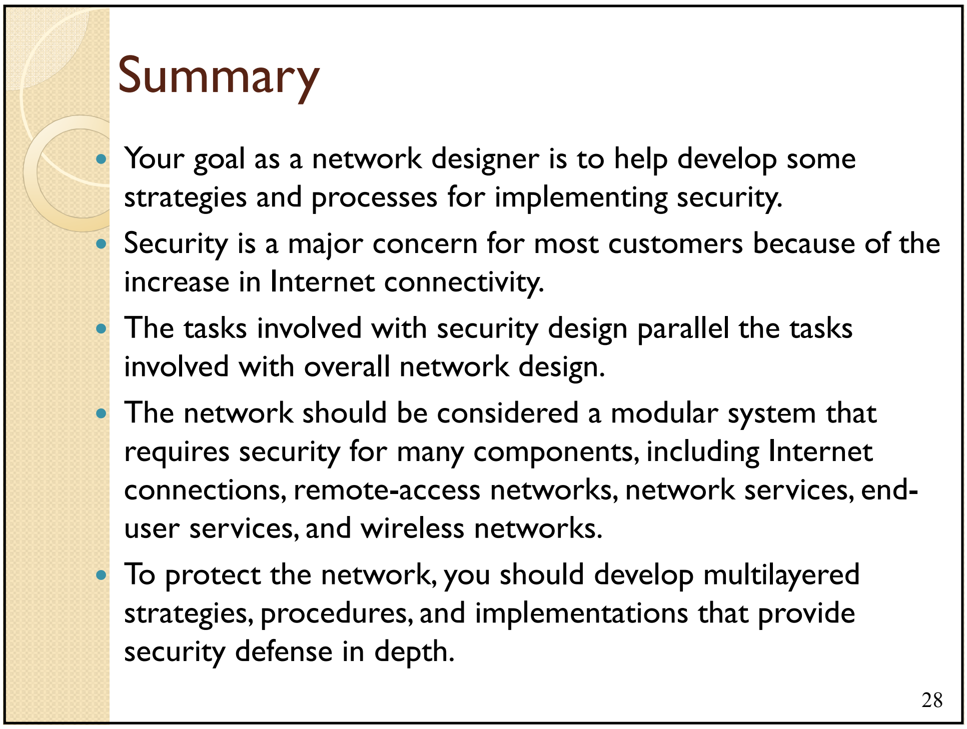
26



Securing User Services

- Include end systems, applications, hosts, file servers, database servers, and other services
- Security policies and procedures should specify accepted practices regarding passwords
- Server root password knowledge should be limited
- Security policy should specify which applications are allowed to run on networked PCs
- Known security bugs in applications and network operating systems should be identified and fixed

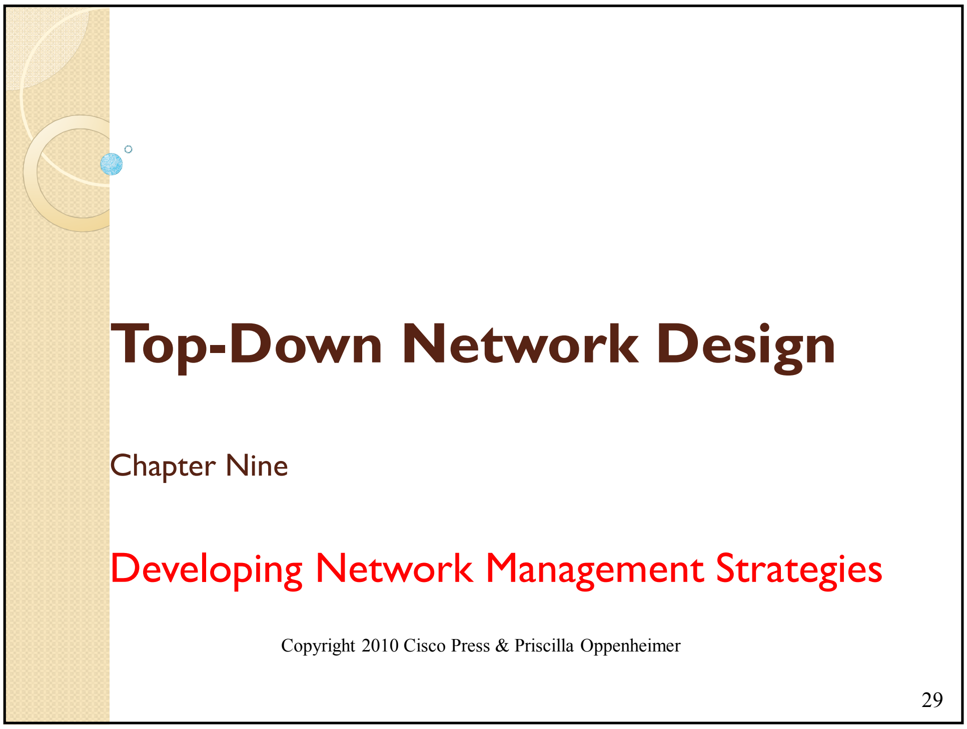
27



Summary

- Your goal as a network designer is to help develop some strategies and processes for implementing security.
- Security is a major concern for most customers because of the increase in Internet connectivity.
- The tasks involved with security design parallel the tasks involved with overall network design.
- The network should be considered a modular system that requires security for many components, including Internet connections, remote-access networks, network services, end-user services, and wireless networks.
- To protect the network, you should develop multilayered strategies, procedures, and implementations that provide security defense in depth.

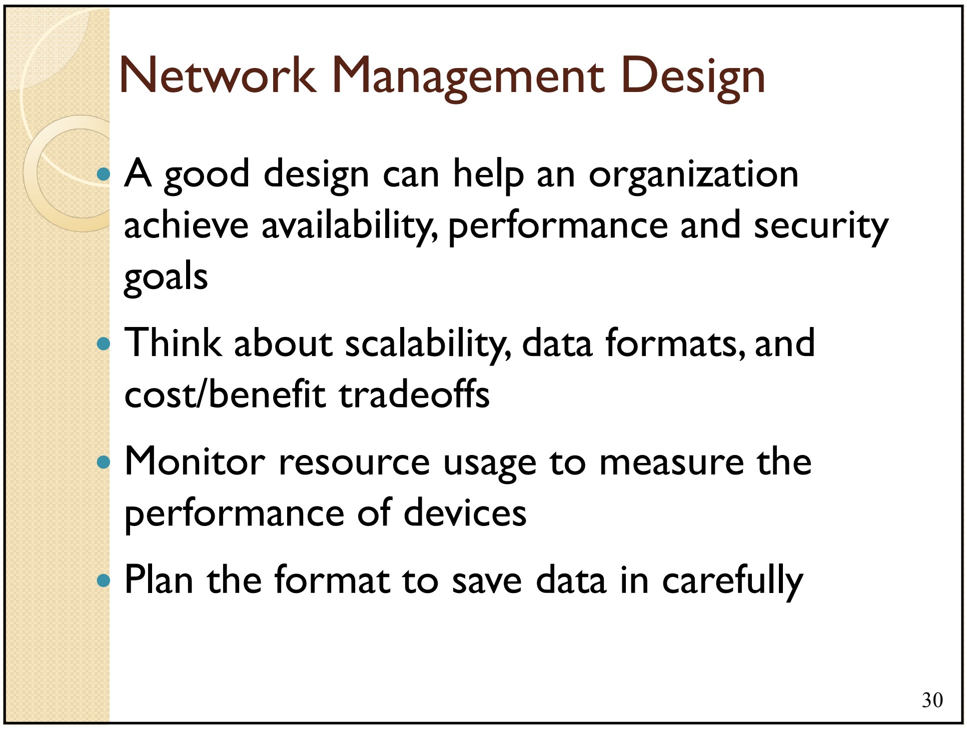
28



Top-Down Network Design

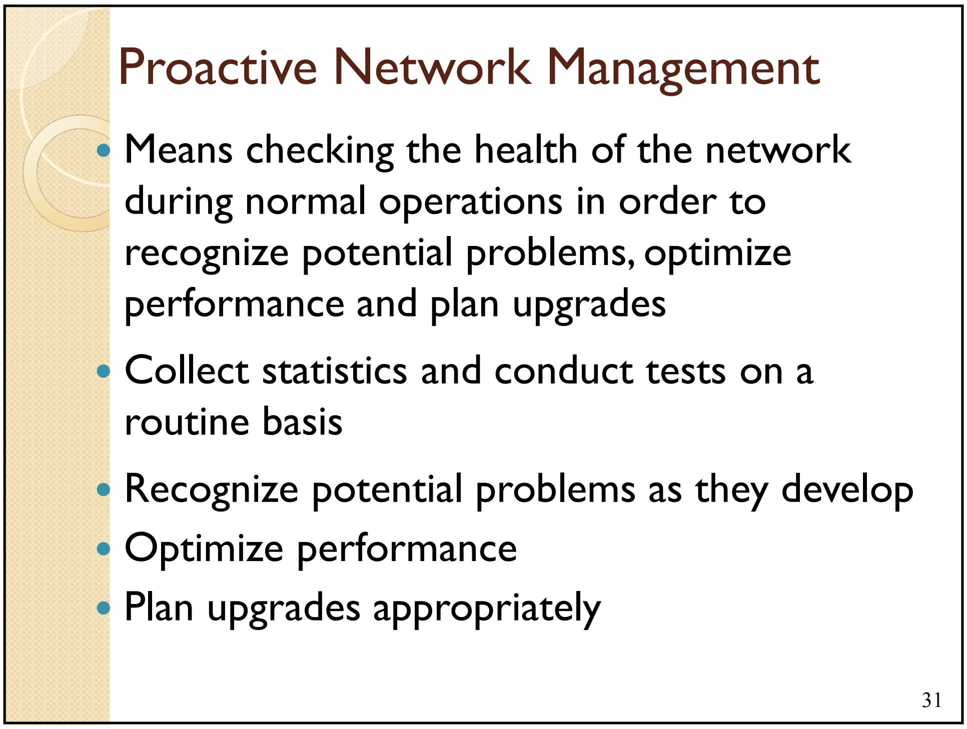
Chapter Nine

Developing Network Management Strategies



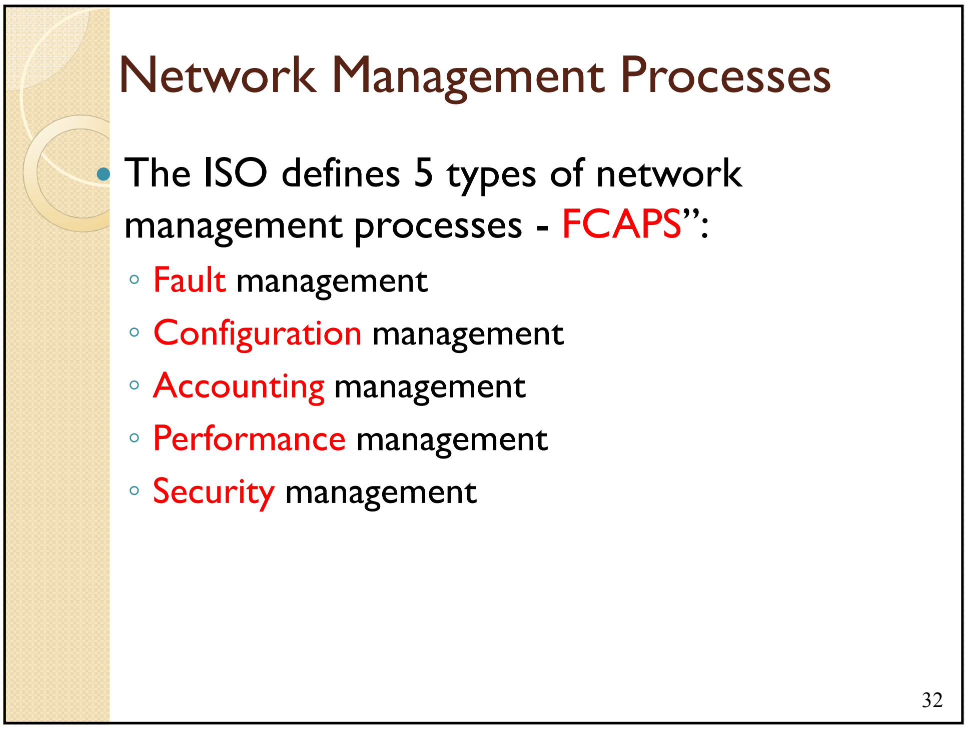
Network Management Design

- A good design can help an organization achieve availability, performance and security goals
- Think about scalability, data formats, and cost/benefit tradeoffs
- Monitor resource usage to measure the performance of devices
- Plan the format to save data in carefully



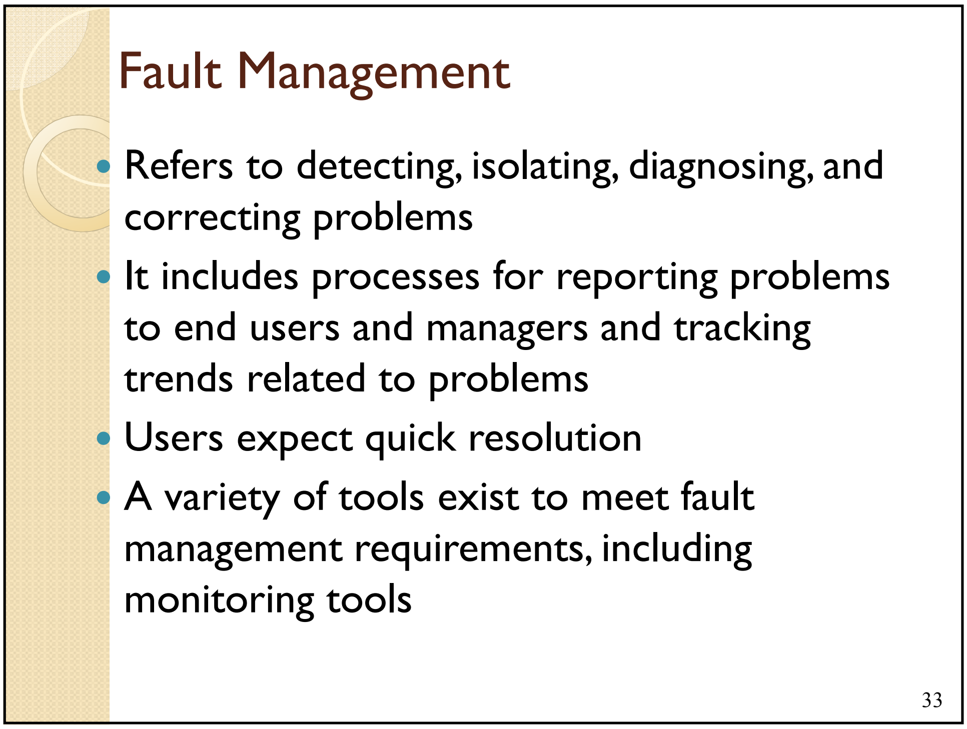
Proactive Network Management

- Means checking the health of the network during normal operations in order to recognize potential problems, optimize performance and plan upgrades
- Collect statistics and conduct tests on a routine basis
- Recognize potential problems as they develop
- Optimize performance
- Plan upgrades appropriately



Network Management Processes

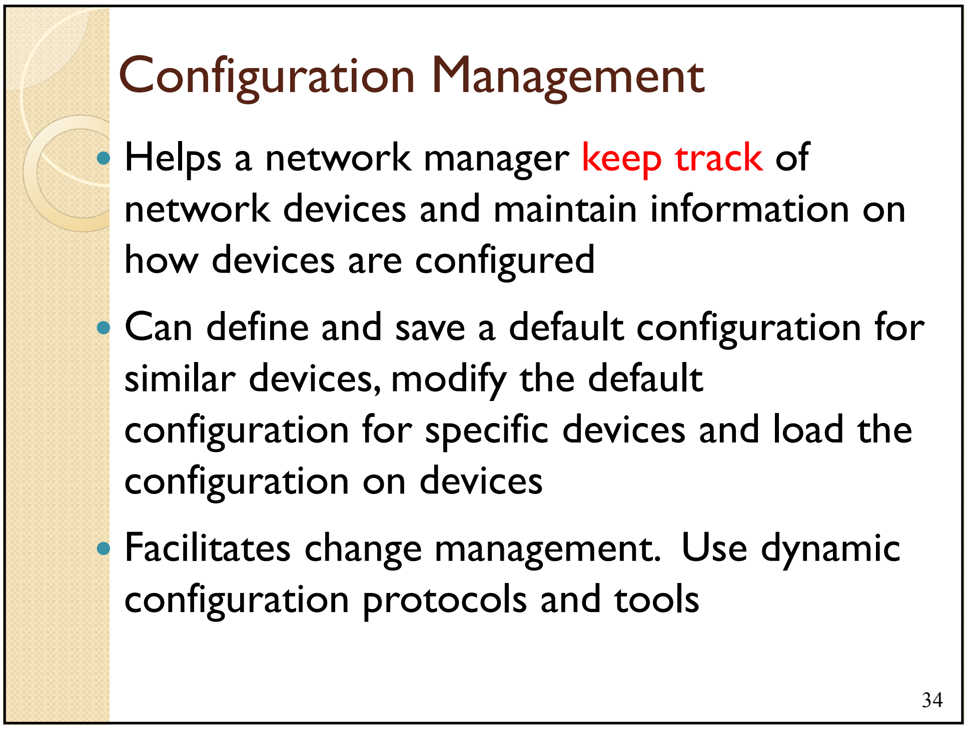
- The ISO defines 5 types of network management processes - FCAPS”:
  - Fault management
  - Configuration management
  - Accounting management
  - Performance management
  - Security management



Fault Management

- Refers to detecting, isolating, diagnosing, and correcting problems
- It includes processes for reporting problems to end users and managers and tracking trends related to problems
- Users expect quick resolution
- A variety of tools exist to meet fault management requirements, including monitoring tools

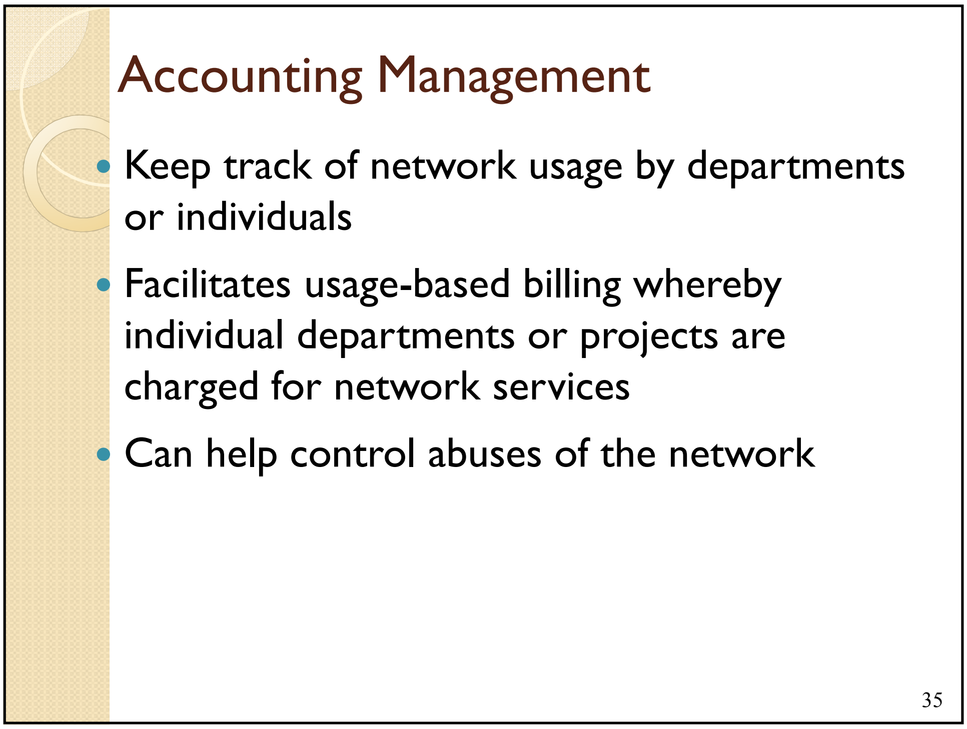
33



Configuration Management

- Helps a network manager keep track of network devices and maintain information on how devices are configured
- Can define and save a default configuration for similar devices, modify the default configuration for specific devices and load the configuration on devices
- Facilitates change management. Use dynamic configuration protocols and tools

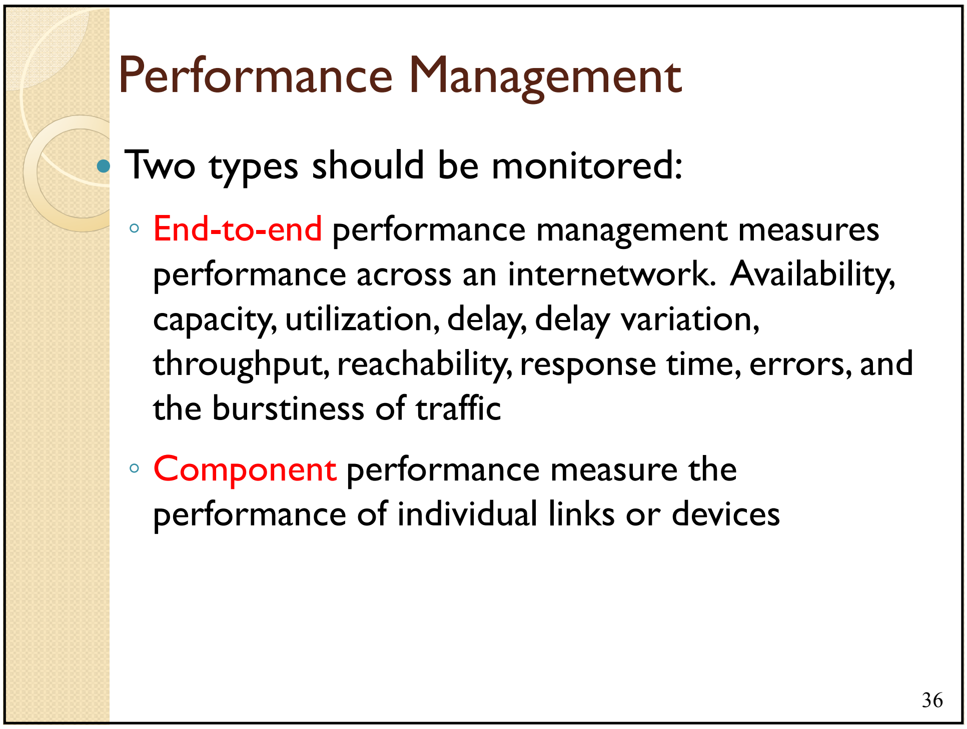
34



Accounting Management

- Keep track of network usage by departments or individuals
- Facilitates usage-based billing whereby individual departments or projects are charged for network services
- Can help control abuses of the network

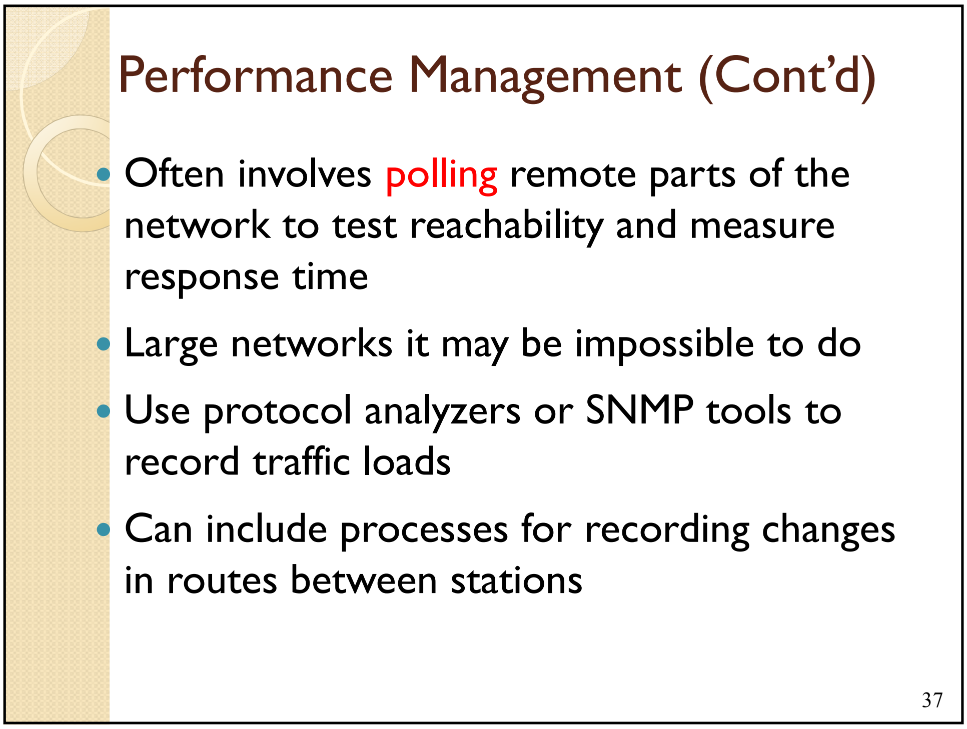
35



Performance Management

- Two types should be monitored:
  - End-to-end performance management measures performance across an internetwork. Availability, capacity, utilization, delay, delay variation, throughput, reachability, response time, errors, and the burstiness of traffic
  - Component performance measure the performance of individual links or devices

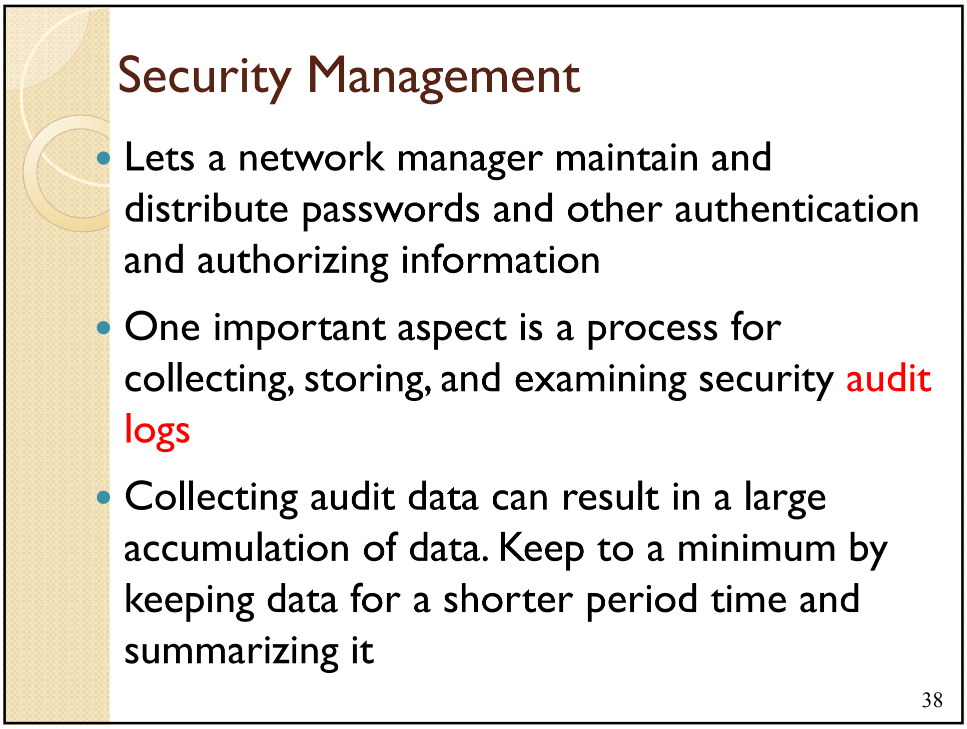
36



Performance Management (Cont'd)

- Often involves polling remote parts of the network to test reachability and measure response time
- Large networks it may be impossible to do
- Use protocol analyzers or SNMP tools to record traffic loads
- Can include processes for recording changes in routes between stations

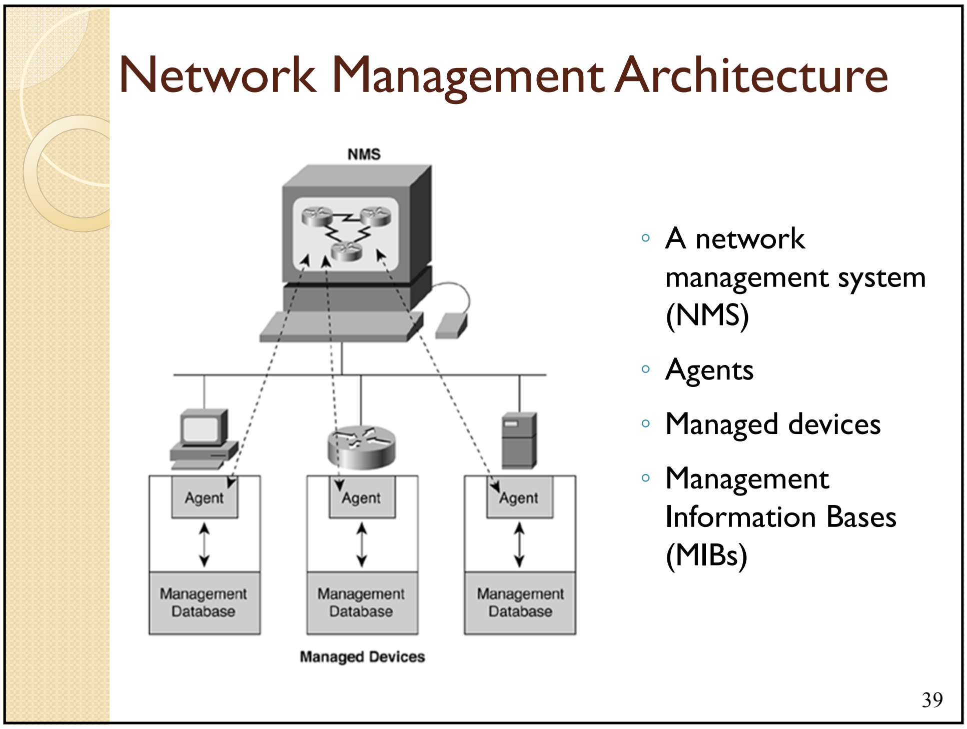
37



Security Management

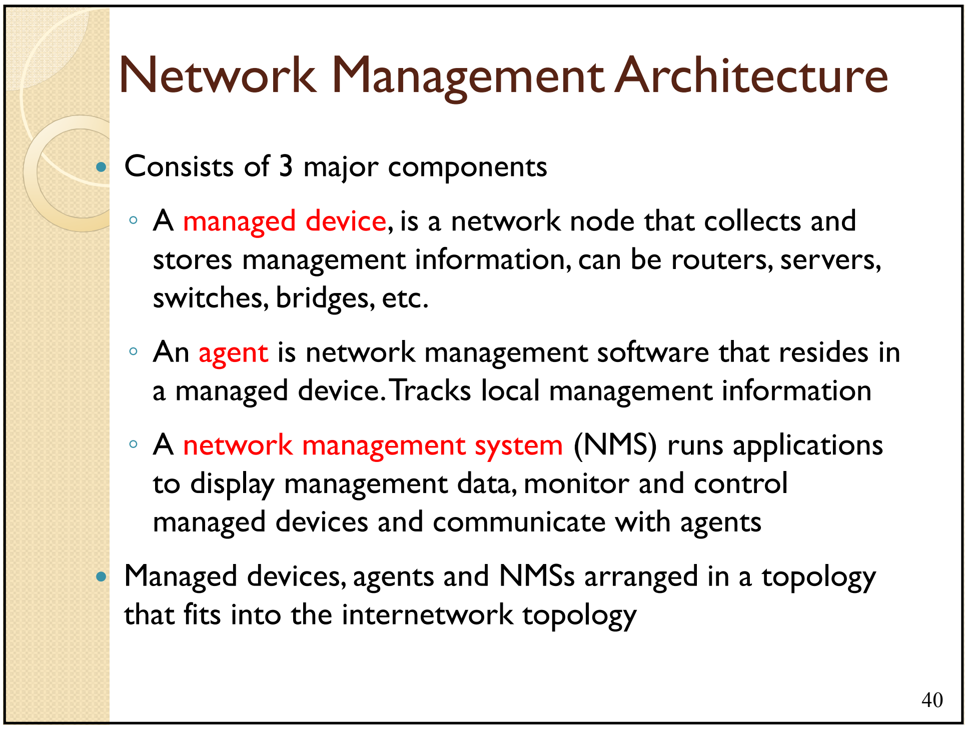
- Lets a network manager maintain and distribute passwords and other authentication and authorizing information
- One important aspect is a process for collecting, storing, and examining security audit logs
- Collecting audit data can result in a large accumulation of data. Keep to a minimum by keeping data for a shorter period time and summarizing it

38



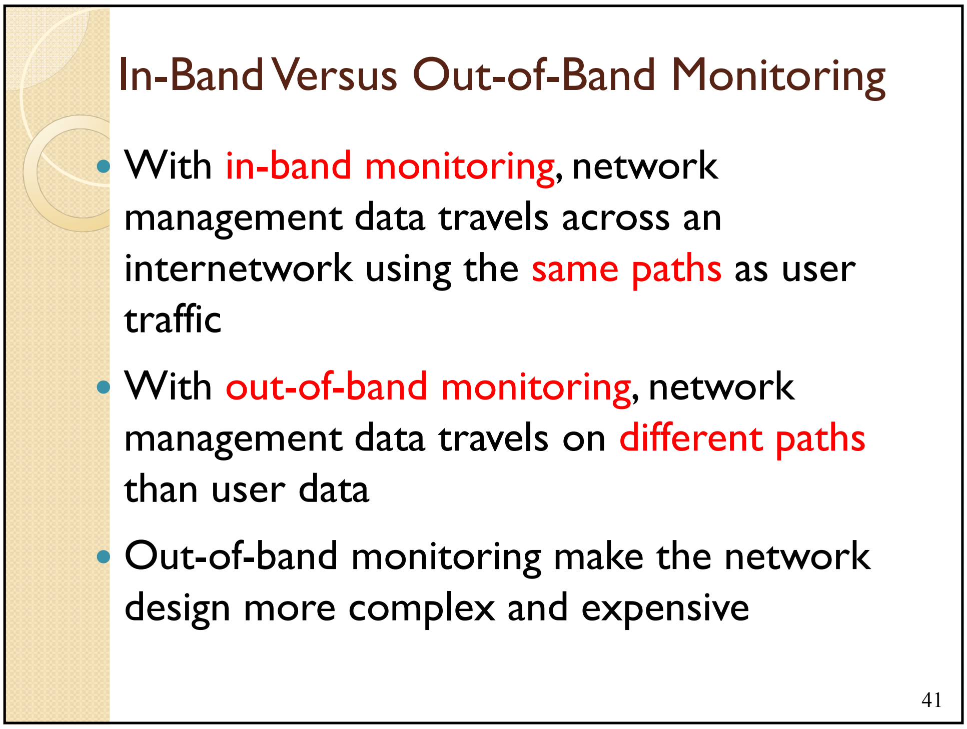
Network Management Architecture

- A network management system (NMS)
- Agents
- Managed devices
- Management Information Bases (MIBs)



Network Management Architecture

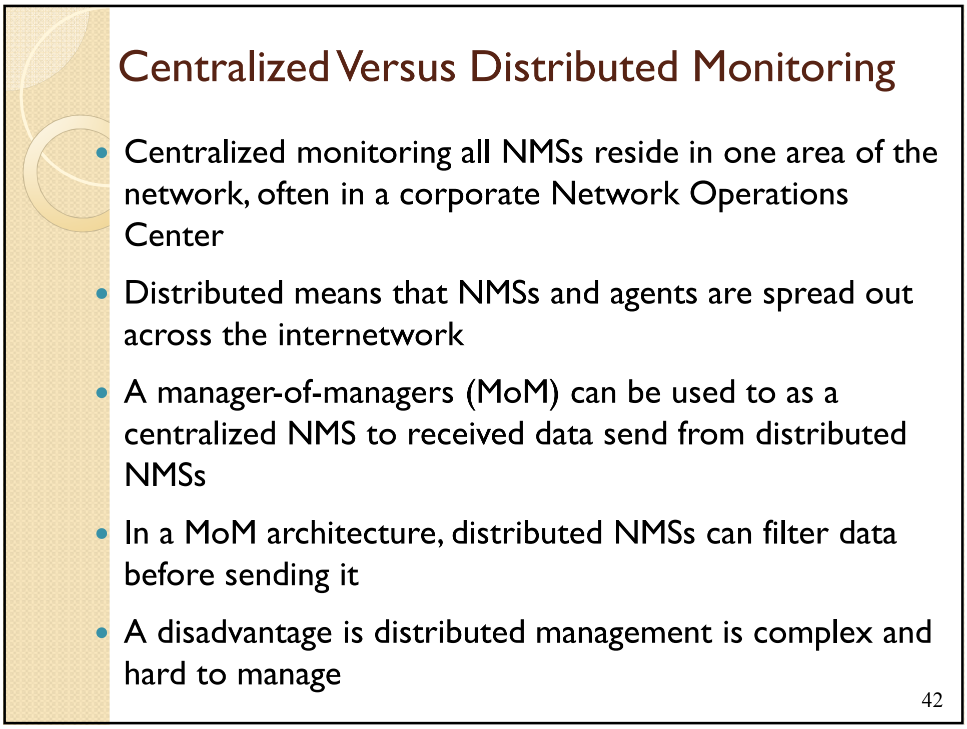
- Consists of 3 major components
  - A managed device, is a network node that collects and stores management information, can be routers, servers, switches, bridges, etc.
  - An agent is network management software that resides in a managed device. Tracks local management information
  - A network management system (NMS) runs applications to display management data, monitor and control managed devices and communicate with agents
- Managed devices, agents and NMSs arranged in a topology that fits into the internetwork topology



In-Band Versus Out-of-Band Monitoring

- With in-band monitoring, network management data travels across an internetwork using the same paths as user traffic
- With out-of-band monitoring, network management data travels on different paths than user data
- Out-of-band monitoring make the network design more complex and expensive

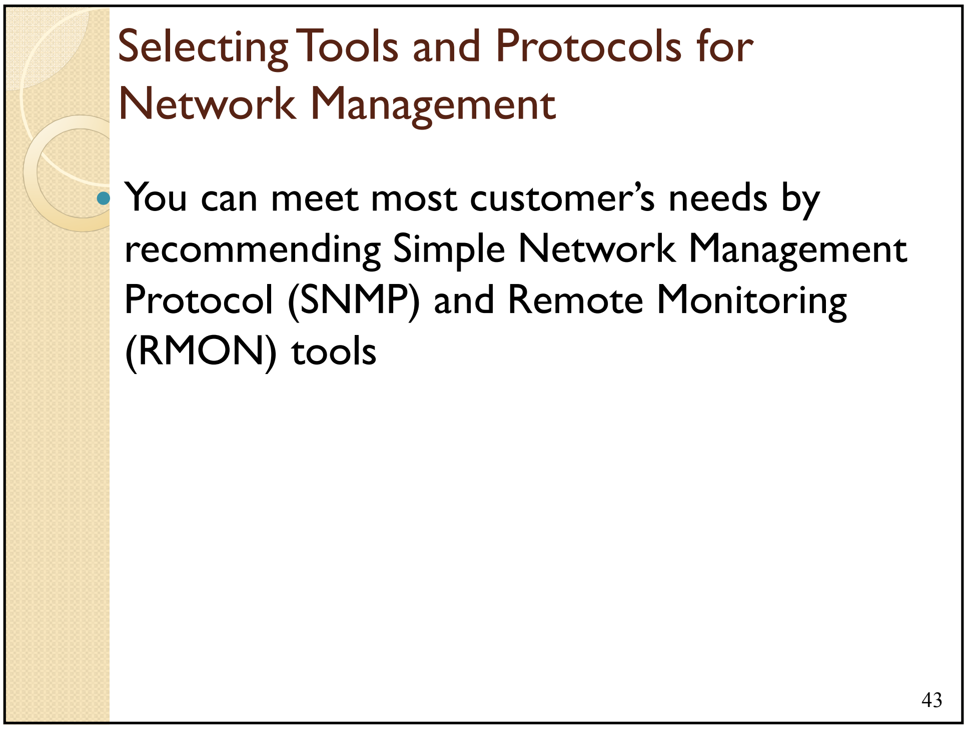
41



Centralized Versus Distributed Monitoring

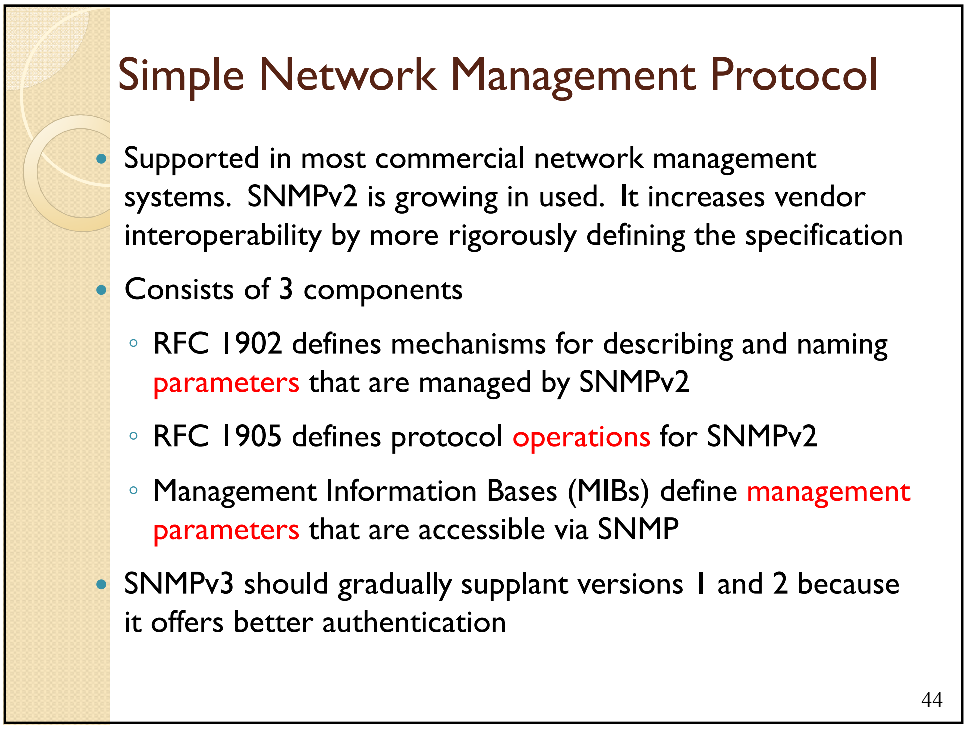
- Centralized monitoring all NMSs reside in one area of the network, often in a corporate Network Operations Center
- Distributed means that NMSs and agents are spread out across the internetwork
- A manager-of-managers (MoM) can be used to as a centralized NMS to received data send from distributed NMSs
- In a MoM architecture, distributed NMSs can filter data before sending it
- A disadvantage is distributed management is complex and hard to manage

42



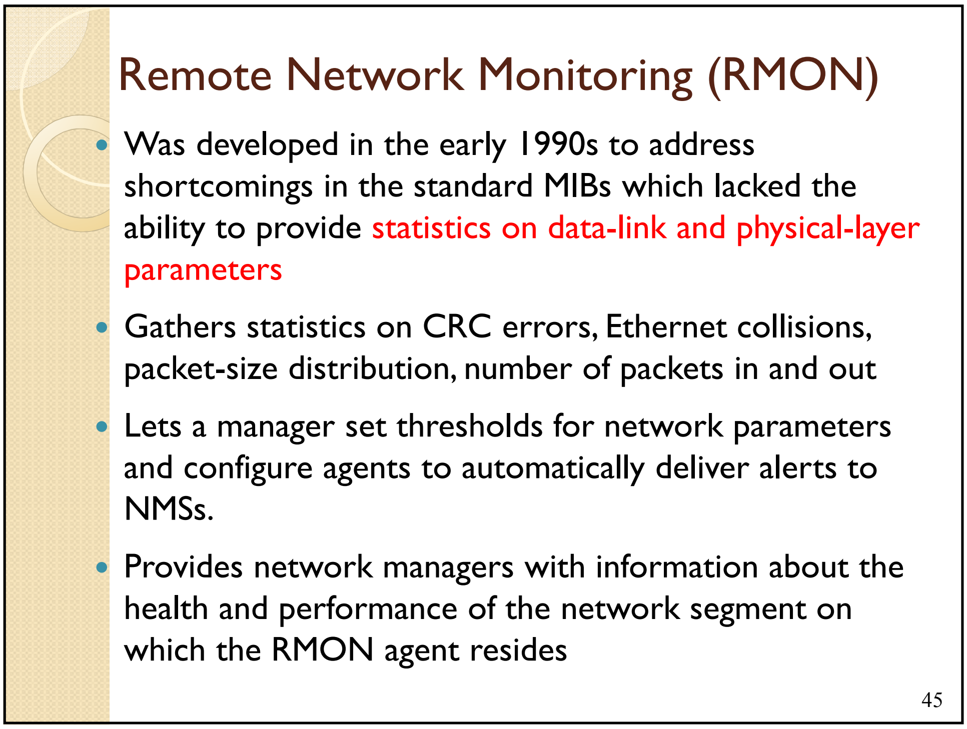
Selecting Tools and Protocols for Network Management

- You can meet most customer's needs by recommending Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON) tools



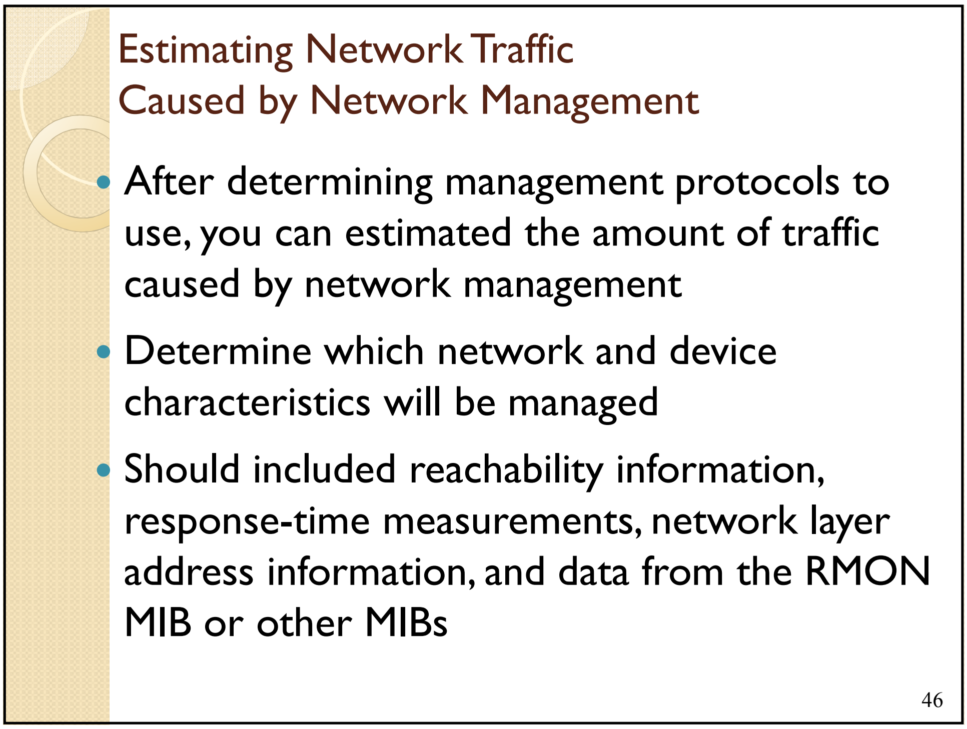
Simple Network Management Protocol

- Supported in most commercial network management systems. SNMPv2 is growing in used. It increases vendor interoperability by more rigorously defining the specification
- Consists of 3 components
  - RFC 1902 defines mechanisms for describing and naming parameters that are managed by SNMPv2
  - RFC 1905 defines protocol operations for SNMPv2
  - Management Information Bases (MIBs) define management parameters that are accessible via SNMP
- SNMPv3 should gradually supplant versions 1 and 2 because it offers better authentication



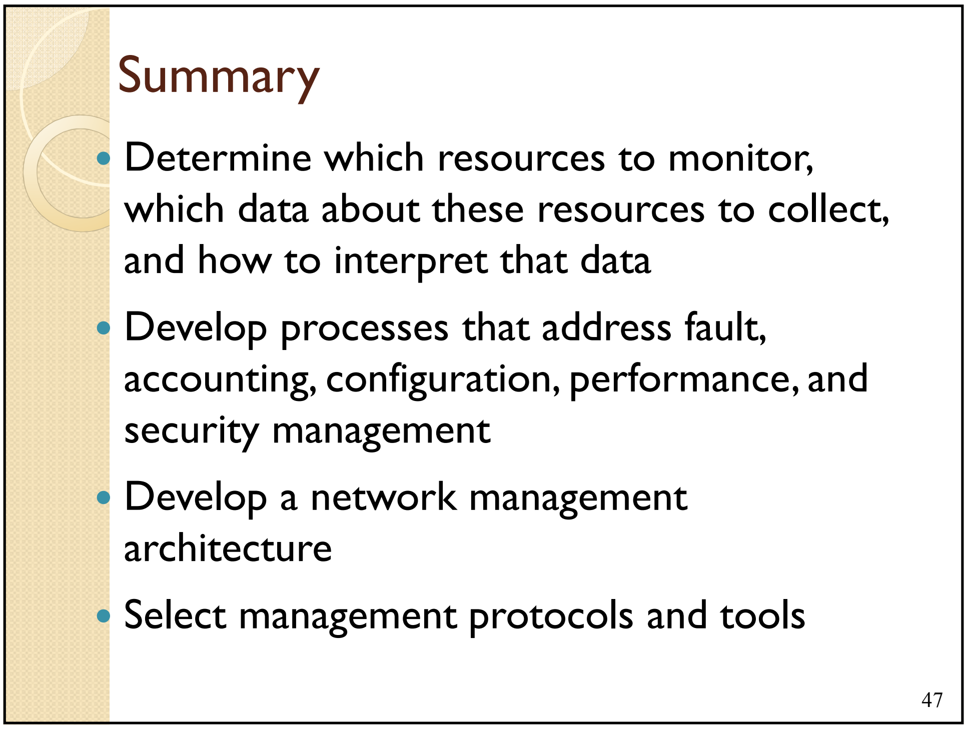
Remote Network Monitoring (RMON)

- Was developed in the early 1990s to address shortcomings in the standard MIBs which lacked the ability to provide statistics on data-link and physical-layer parameters
- Gathers statistics on CRC errors, Ethernet collisions, packet-size distribution, number of packets in and out
- Lets a manager set thresholds for network parameters and configure agents to automatically deliver alerts to NMSs.
- Provides network managers with information about the health and performance of the network segment on which the RMON agent resides



Estimating Network Traffic Caused by Network Management

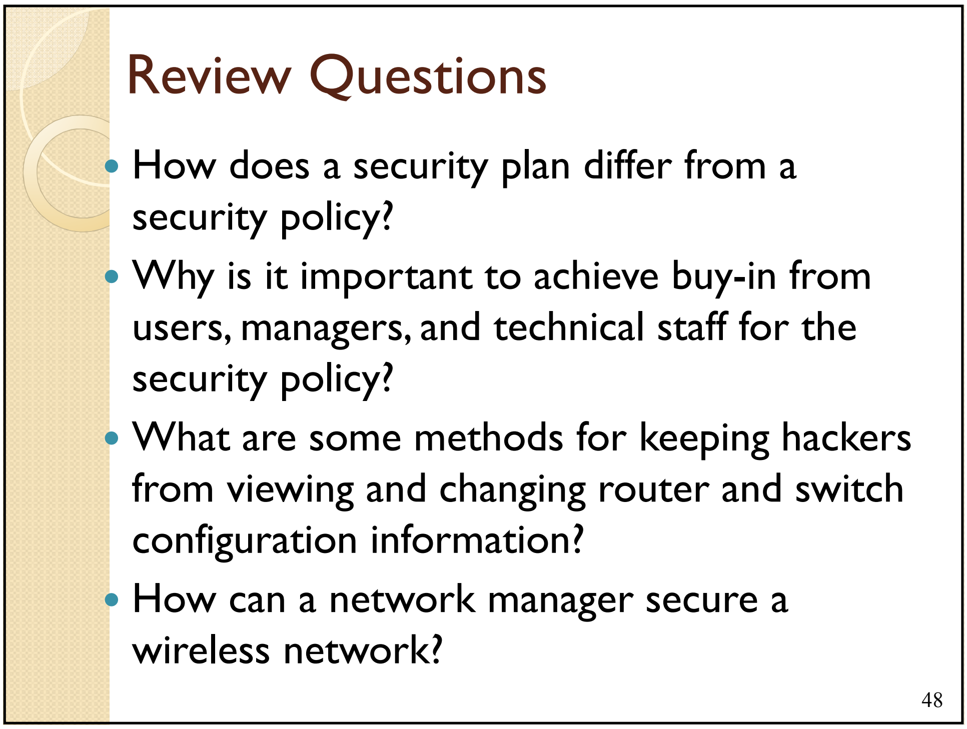
- After determining management protocols to use, you can estimated the amount of traffic caused by network management
- Determine which network and device characteristics will be managed
- Should included reachability information, response-time measurements, network layer address information, and data from the RMON MIB or other MIBs



Summary

- Determine which resources to monitor, which data about these resources to collect, and how to interpret that data
- Develop processes that address fault, accounting, configuration, performance, and security management
- Develop a network management architecture
- Select management protocols and tools

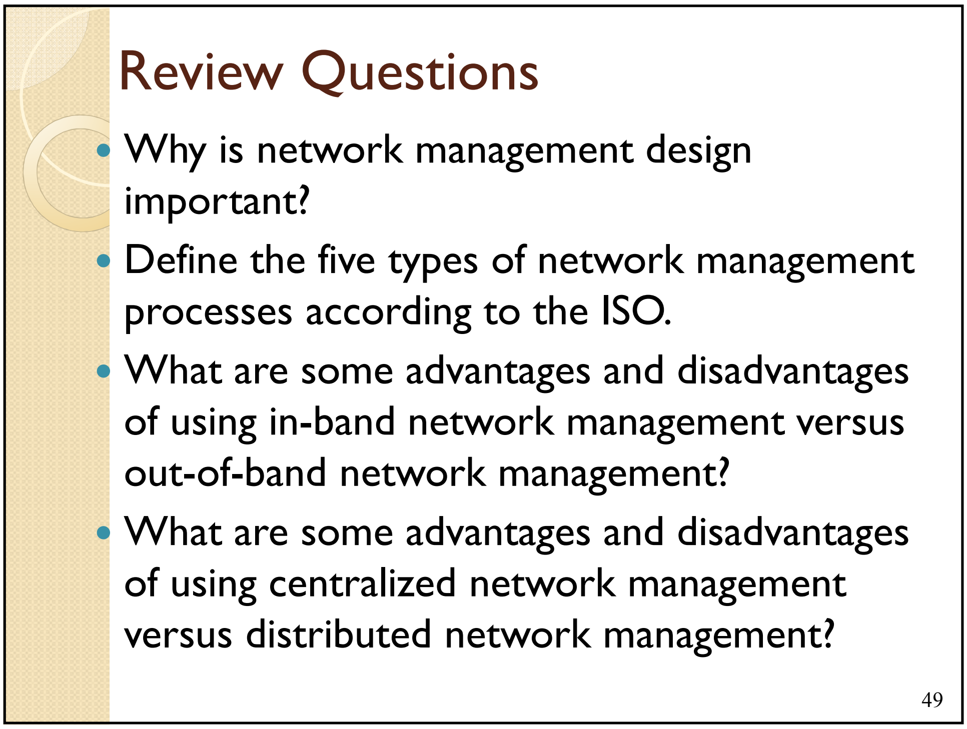
47



Review Questions

- How does a security plan differ from a security policy?
- Why is it important to achieve buy-in from users, managers, and technical staff for the security policy?
- What are some methods for keeping hackers from viewing and changing router and switch configuration information?
- How can a network manager secure a wireless network?

48



Review Questions

- Why is network management design important?
- Define the five types of network management processes according to the ISO.
- What are some advantages and disadvantages of using in-band network management versus out-of-band network management?
- What are some advantages and disadvantages of using centralized network management versus distributed network management?

49