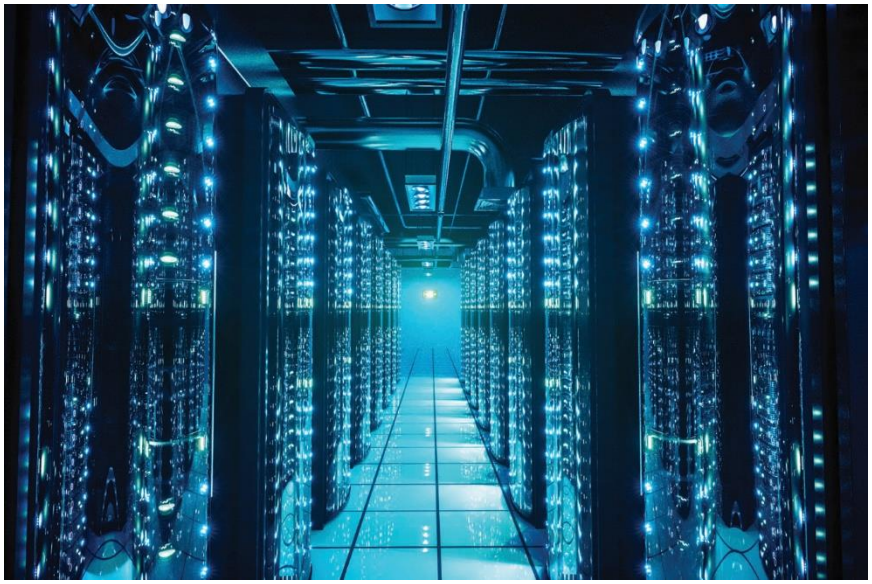
Network Components

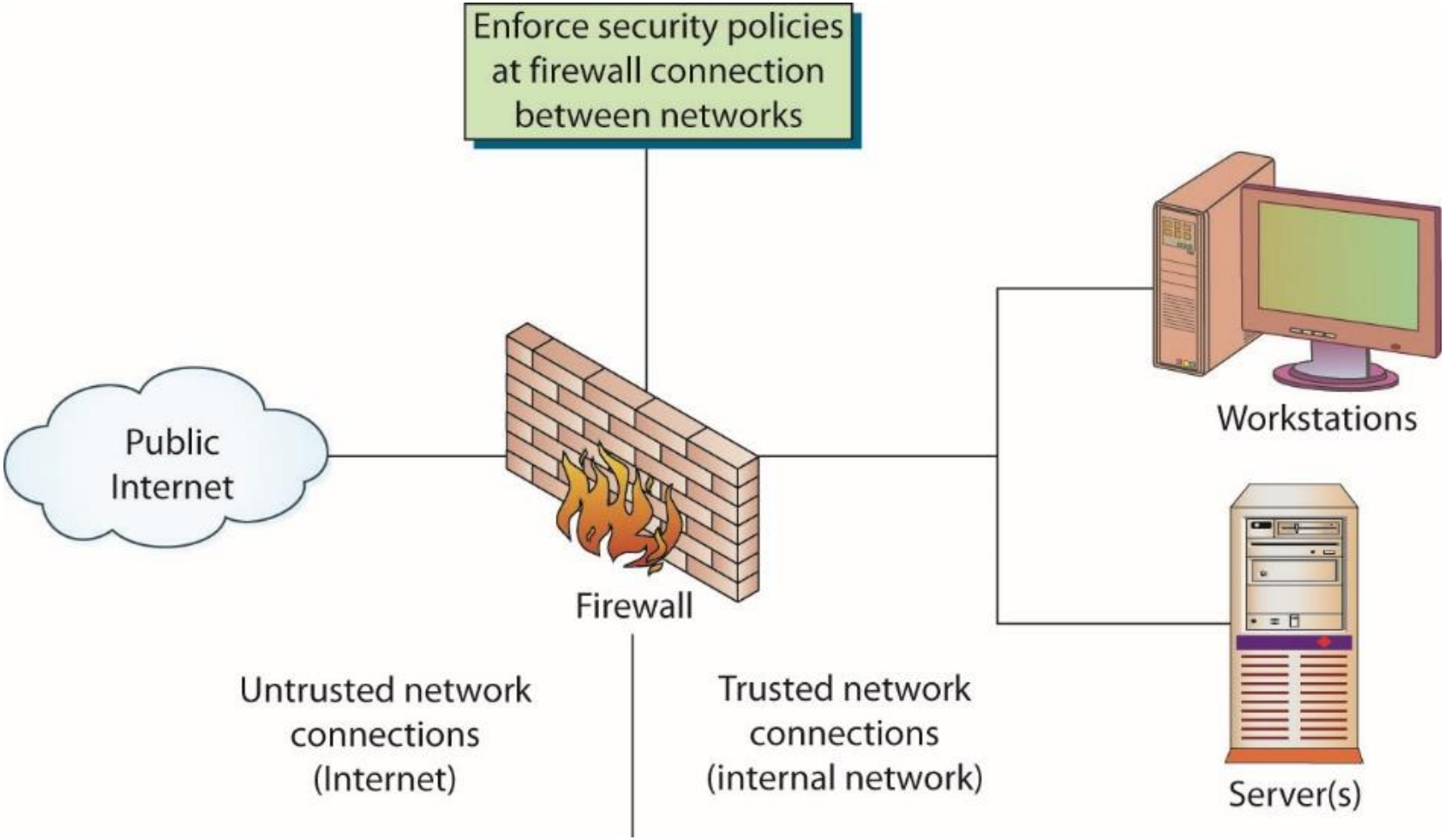


Devices

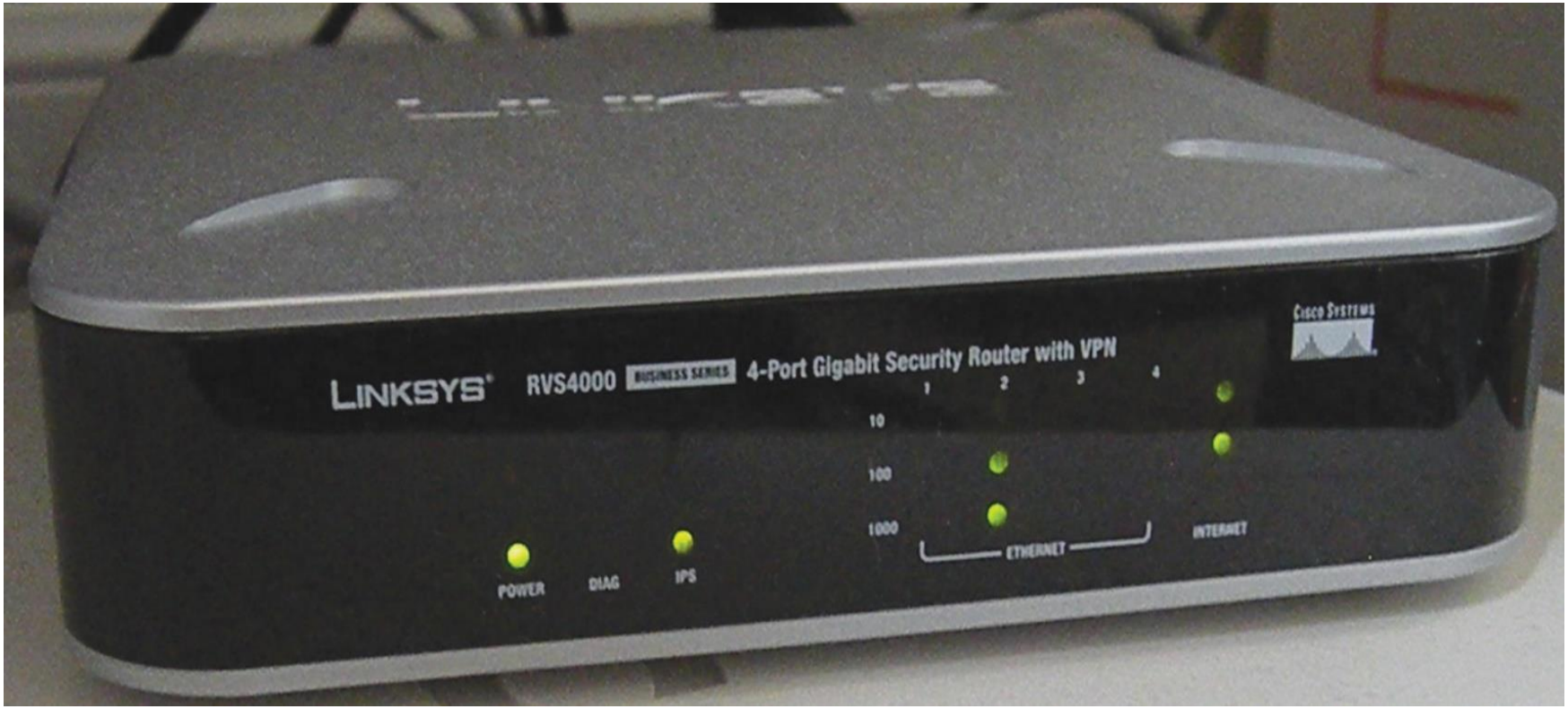
- *Devices* are needed to connect clients and servers and to regulate the traffic between them.
- Devices expand the network beyond simple client computers and servers.
- Devices come in many forms and with many functions.
- Each device has a specific network function and plays a role in maintaining network infrastructure security.

Firewalls

- A **firewall** is a network device—hardware, software, or a combination thereof.
  - Its purpose is to enforce a security policy across its connections by allowing or denying traffic to pass into or out of the network.
- The heart of a firewall is the set of security policies that it enforces.
  - A key to security policies for firewalls is the principle of least access.



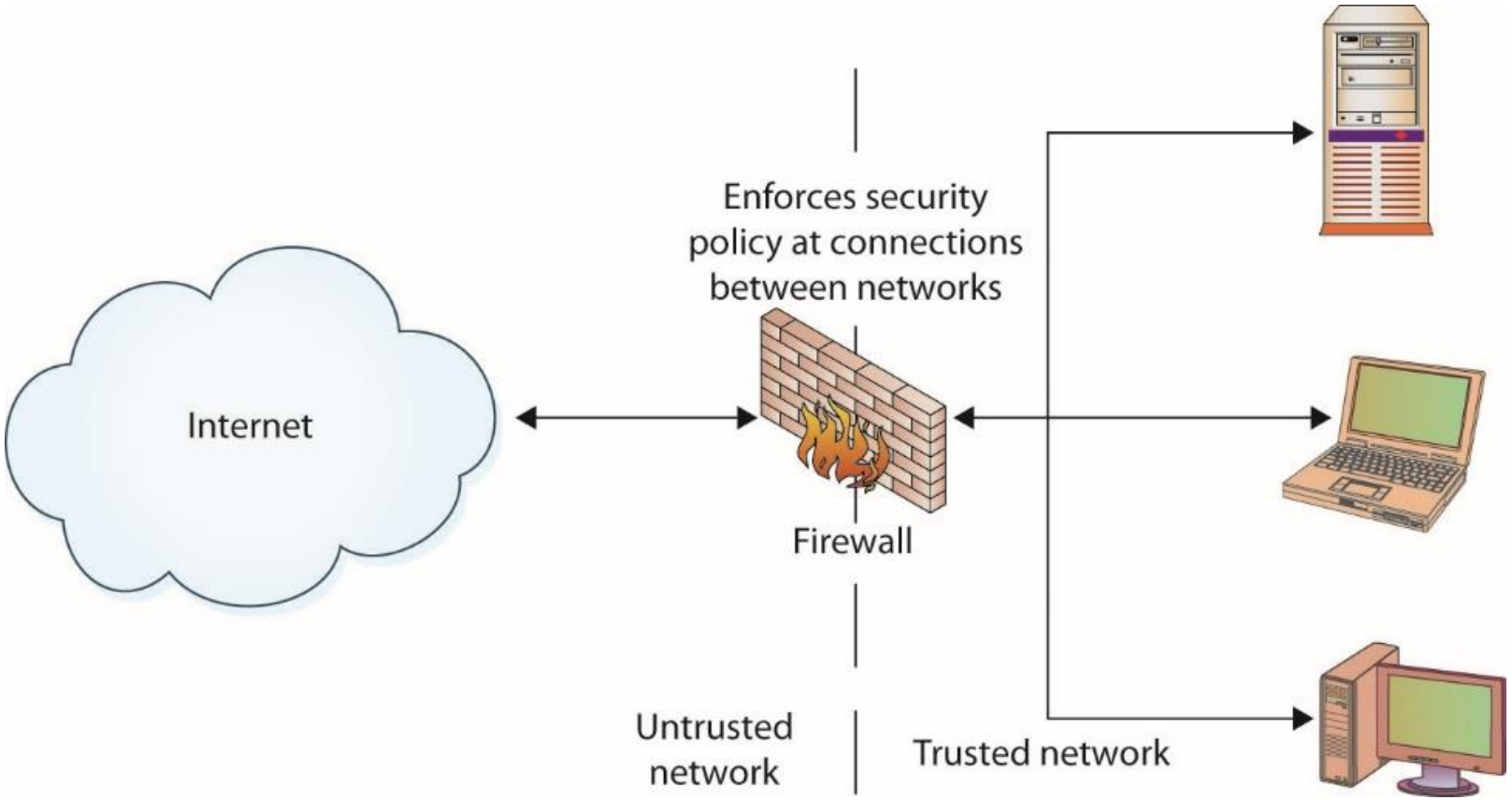
How a firewall works



Linksys SOHO firewall

Firewalls (*continued*)

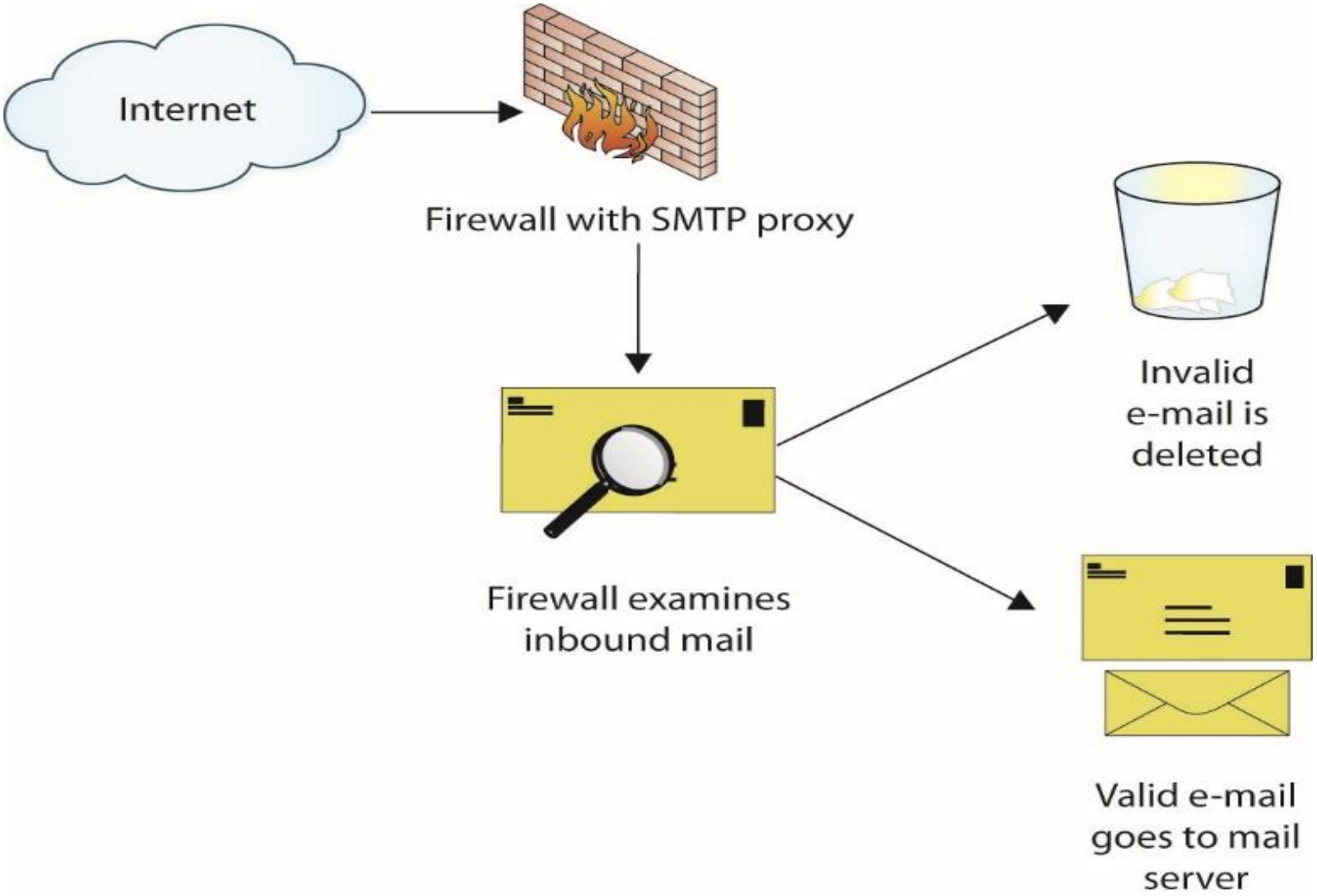
- The security topology determines what network devices are employed at what points in a network.
- The perfect firewall policy is one that the end user never sees and one that never allows even a single unauthorized packet to enter the network.
  - To develop a complete and comprehensive security policy, it is first necessary to have a complete and comprehensive understanding of your network resources and their uses.



Logical depiction of a firewall protecting an organization from the Internet

How Do Firewalls Work?

- Firewalls enforce the established security policies through a variety of mechanisms, including:
  - Network Address Translation (NAT)
  - **Basic packet filtering**
  - Stateful packet filtering
  - Access control lists (ACLs)
  - Application layer proxies
- ACLs are a cornerstone of security in firewalls.
- Firewalls can also act as network traffic regulators.



Firewall with SMTP application layer proxy

Next-Generation Firewalls

- **Next-generation firewalls** are characterized by these features:
  - Deep packet inspection
  - Move beyond port/protocol inspection and blocking
  - Add application-level inspection
  - Add intrusion prevention
  - Bring intelligence from outside the firewall
- Traffic can be managed based on content, not merely site or URL.

Web Application Firewalls vs. Network Firewalls

- A *web application firewall* is the term given to any software package, appliance, or filter that applies a rule set to HTTP/HTTPS traffic.
  - They shape web traffic and filter out SQL injection attacks, malware, cross-site scripting (XSS), and so on.
- A network firewall is a hardware or software package that controls the flow of packets into and out of a network.

VPN Concentrator

- A virtual private network (VPN) is a construct used to provide a secure communication channel between users across public networks such as the Internet.
  - The most common implementation of VPN is via IPsec, a protocol for IP security.
  - IPsec is mandated in IPv6 and is optional in IPv4.
  - IPsec can be implemented in hardware, software, or a combination of both and is used to encrypt all IP traffic.
  - The use of encryption technologies allows either the data in a packet to be encrypted or the entire packet to be encrypted.

Intrusion Detection Systems

- Intrusion detection systems (IDSs) are designed to detect, log, and respond to unauthorized network or host use, both in real time and after the fact.
- These systems are implemented using software.
  - In large networks or systems with significant traffic levels, dedicated hardware is typically required as well.
- IDSs can be divided into two categories:
  - Network-based systems and host-based systems

Routers

- A **router** is a network traffic management device used to connect different network segments.
  - Operate at the network layer (Layer 3) of the OSI model
  - Form the backbone of the Internet
  - Use algorithms and tables to determine where to send the packet
  - Use access control lists (ACLs) as a method of deciding whether a packet is allowed to enter the network
  - Must limit router access and control of internal functions

A cable modem/DSL

Switches

- A **switch** forms the basis for connections in most Ethernet-based LANs.
- Switches have replaced hubs and bridges.
- A switch has separate collision domains for each port.
  - When *full duplex* is employed, collisions are virtually eliminated from the two nodes, host and client.
- A switch is usually a Layer 2 device, but Layer 3 switches incorporate routing functionality.

Switches (*continued*)

- Advantages of switches
  - They improve network performance by filtering traffic.
  - They provide the option to disable a port so that it cannot be used without authorization.
  - They support port security allowing the administrator to control which systems can send data to each of the ports.
  - Switches use the MAC address of the systems to incorporate traffic filtering and port security features.
    - Port address security based on MAC addresses functionality is what allows an 802.1X device to act as an “edge device.”

Switches (*continued*)

- Switch security concerns
  - They are intelligent network devices and are therefore subject to hijacking by hackers.
  - Switches are commonly administered using the Simple Network Management Protocol (SNMP) and Telnet protocol.
    - Both protocols have a serious weakness in that they send passwords across the network in cleartext.
  - Switches are shipped with default passwords.
  - Switches are subject to electronic attacks, such as ARP poisoning and MAC flooding.

Switches (*continued*)

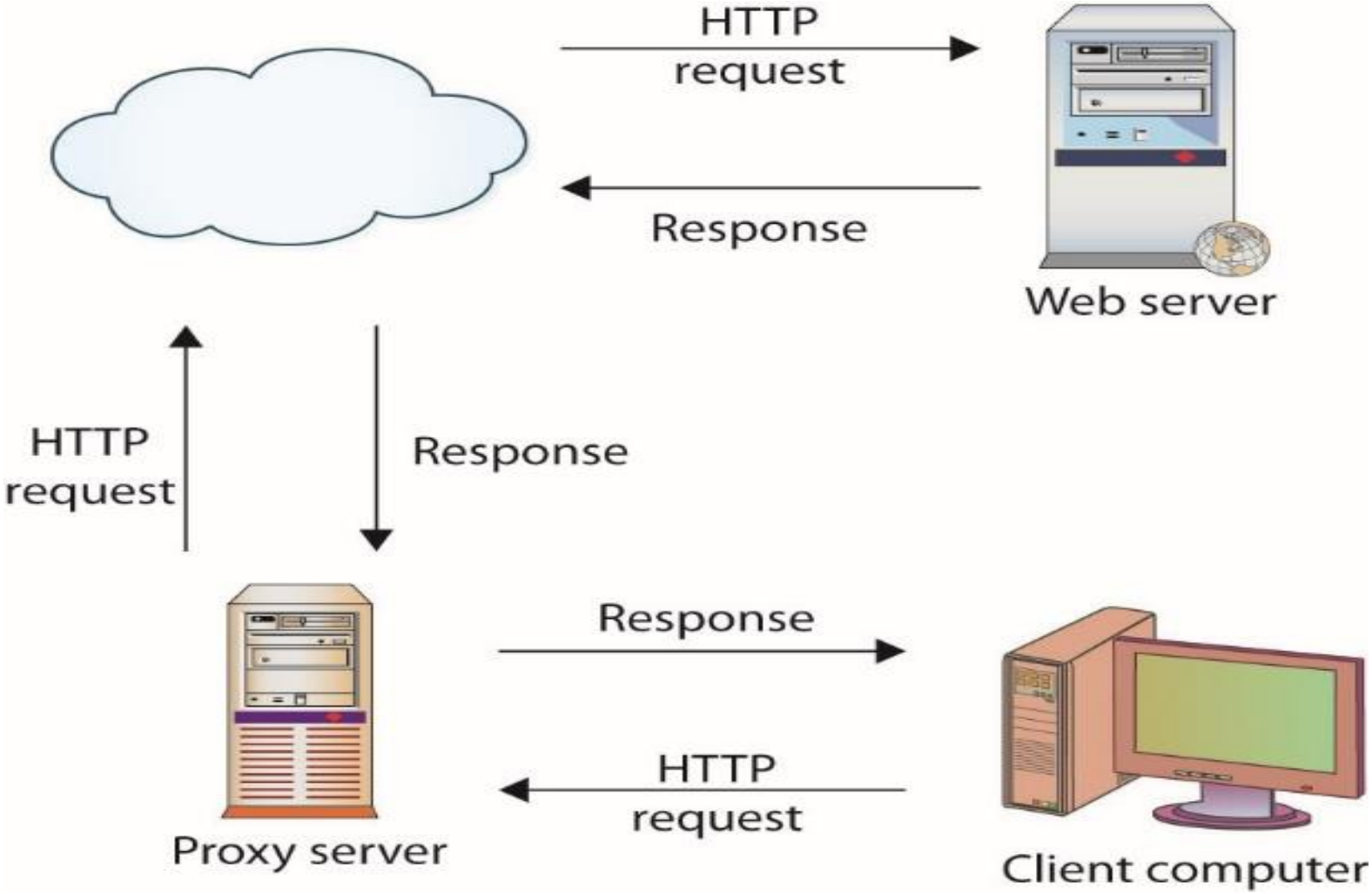
- Loop protection is a concern with switches.
  - Switches operate at Layer 2 so there is no countdown mechanism to kill packets that get caught in loops or on paths that will never resolve.
  - The Layer 2 space acts as a mesh, where potentially the addition of a new device can create loops in the existing device interconnections.
  - Spanning trees technology is employed to prevent loops.
  - The Spanning Tree Protocol (STP) allows for multiple, redundant paths, while breaking loops to ensure a proper broadcast pattern.

Proxies

- A **proxy server** (or simply proxy) can be used to filter out undesirable traffic and prevent employees from accessing potentially hostile web sites.
- Proxy servers can be completely transparent (*gateways* or *tunneling proxies*), or a proxy server can modify the client request before sending it on, or even serve the client's request without needing to contact the destination server.
- Several major categories of proxy servers are in use.

Load Balancers

- **Load balancers** are designed to distribute the processing load over two or more systems.
  - They are used to help improve resource utilization and throughput but also have the added advantage of increasing the fault tolerance of the overall system since a critical process may be split across several systems.
  - Should any one system fail, the others can pick up the processing it was handling.



HTTP proxy handling client requests and web server responses

Bridges

- A **bridge** operates at the data link layer, filtering traffic based on MAC addresses.
- Bridges can reduce collisions by separating pieces of a network into two separate collision domains.
  - This only cuts the collision problem in half.
- A better solution is to use switches for network connections.

Network Interface Cards

- To connect a server or workstation to a network, a device known as a **network interface card (NIC)** is used.
  - A NIC is the physical connection between a computer and the network.
  - Each NIC port is serialized with a unique code, 48 bits long, referred to as a Media Access Control address (MAC address).
  - Unfortunately, these addresses can be changed, or "spoofed," rather easily.

Linksys network interface card (NIC)

Hubs

- A **hub** is networking equipment that connects devices that are using the same protocol at the physical layer of the OSI model.
  - A hub allows multiple machines in an area to be connected together in a star configuration with the hub at the center.
  - All connections on a hub share a single **collision domain,** a small cluster in a network where collisions occur.
  - Increased network traffic can become limited by collisions; this problem has made hubs obsolete in newer networks.
  - Hubs also create a security weakness due to sniffing and eavesdropping issues.

Concentrators

- Network devices called **concentrators** act as traffic management devices, managing flows from multiple points into single streams.
  - Concentrators typically act as endpoints for a particular protocol, such as SSL/TLS or VPN.
  - The use of specialized hardware can enable hardware-based encryption and provide a higher level of specific service than a general-purpose server.
  - This provides both architectural and functional efficiencies.

Wireless Devices

- Wireless devices bring additional security concerns.
  - Radio waves or infrared carry data, which allows anyone within range access to the data.
- The point of entry from a wireless device to a wired network is performed at a device called a **wireless access point**.
  - They can support multiple concurrent devices accessing network resources through the network node they create.
- Several mechanisms can be used to add wireless functionality to a machine.

A typical wireless access point

A typical PCMCIA wireless network card

Modems

- **Modem** is a shortened form of *modulator/demodulator*, converting analog signals to digital and vice versa.
- A DSL modem is a device connected to special digital telephone lines using a direct connection.
- A cable modem is a device connected to cable television lines set up in shared arrangements.
  - DOCSIS includes built-in support for security protocols.
- Both DSL and cable are designed for a continuous connection.

Modern cable modem

Modems (*continued*)

- Security is needed with a cable/DSL connection.
  - The modem equipment provided by the subscription service converts the cable or DSL signal into a standard Ethernet signal that can then be connected to a NIC on the client device.
  - This is still just a direct network connection, with no security device separating the two.
  - The most common security device used in cable/DSL connections is a router that acts as a hardware firewall.
  - The firewall/router needs to be installed between the cable/DSL modem and client computers.

Telephony

- A **private branch exchange (PBX)** is an extension of the public telephone network into a business.
- The following are security concerns:
  - They can be compromised from the outside and used by phone hackers (*phreakers*) to make phone calls at the business's expense.
  - A path exists for a connection to outside data networks and the Internet.
    - A firewall is needed for security on these connections.

Security Devices

- There are a range of security devices that can be employed at the network layer to instantiate security functionality in the network layer.
- Devices can be used for intrusion detection, network access control, and a wide range of other security functions.
- Each device has a specific network function and plays a role in maintaining network infrastructure security.

Network Access Control

- Managing endpoints on a case-by-case basis as they connect is a security methodology known as **network access control**.
- Two main competing methodologies are:
  - **Network Access Protection (NAP)** – Microsoft
    - Measures the health of a host when it connects to the network
  - **Network Admission Control (NAC)** – Cisco
    - Enforces policies chosen by the network administrator
- Both are still in early stages of implementation.

Network Monitoring/Diagnostic

- The **network operations center (NOC)** allows operators to observe and interact with the network, using the self-reporting and, in some cases, self-healing nature of network devices to ensure efficient network operation.
  - Software enables controllers at NOCs to measure the actual performance of network devices and make changes to the configuration and operation of devices remotely.
  - SNMP was developed to perform management, monitoring, and fault resolution across networks.

Web Security Gateways

- Some security vendors combine proxy functions with content-filtering functions to create a product called a **web security gateway.**
  - They are intended to address the security threats and pitfalls unique to web-based traffic.
- Web security gateways capabilities include:
  - Real-time malware protection
  - Content monitoring
  - Productivity monitoring
  - Data protection and compliance

Internet Content Filters

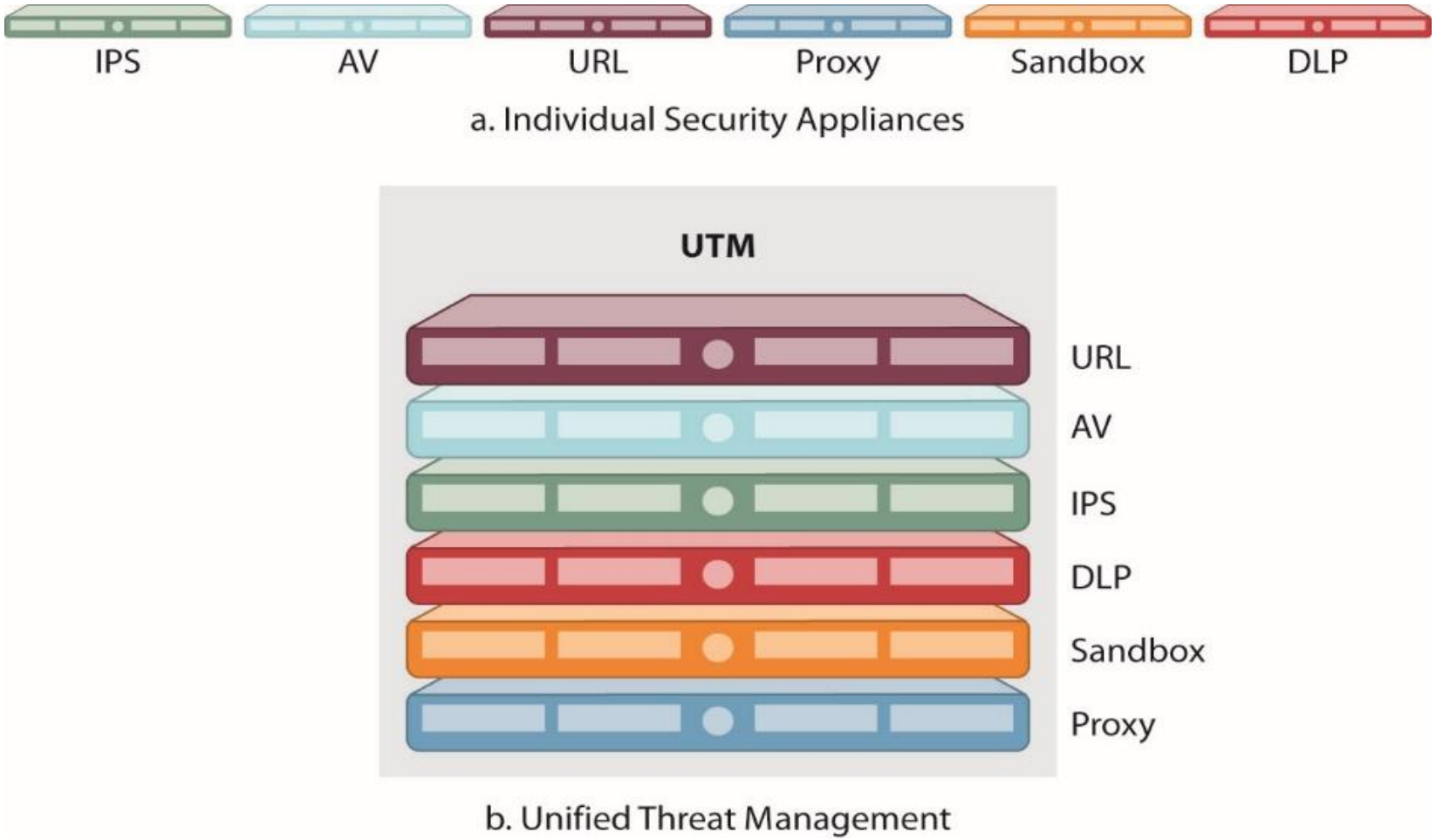
- An **Internet content filter** protects a corporation from employees' viewing of inappropriate or illegal content at the workplace and the subsequent complications that occur when such viewing takes place.
- They filter undesirable content, such as pornography and malicious activity such as browser hijacking attempts or XSS attacks.
- Content-filtering systems face many challenges.

Data Loss Prevention

- **Data loss prevention (DLP)** refers to technology employed to detect and prevent transfers of data across an enterprise.
  - DLP technology can scan packets for specific data patterns.
  - DLP can be tuned to detect account numbers, secrets, specific markers, or files.
  - The primary challenge is the placement of the sensor.
    - The DLP sensor needs to be able observe the data, so if the channel is encrypted, DLP technology can be thwarted.

Unified Threat Management

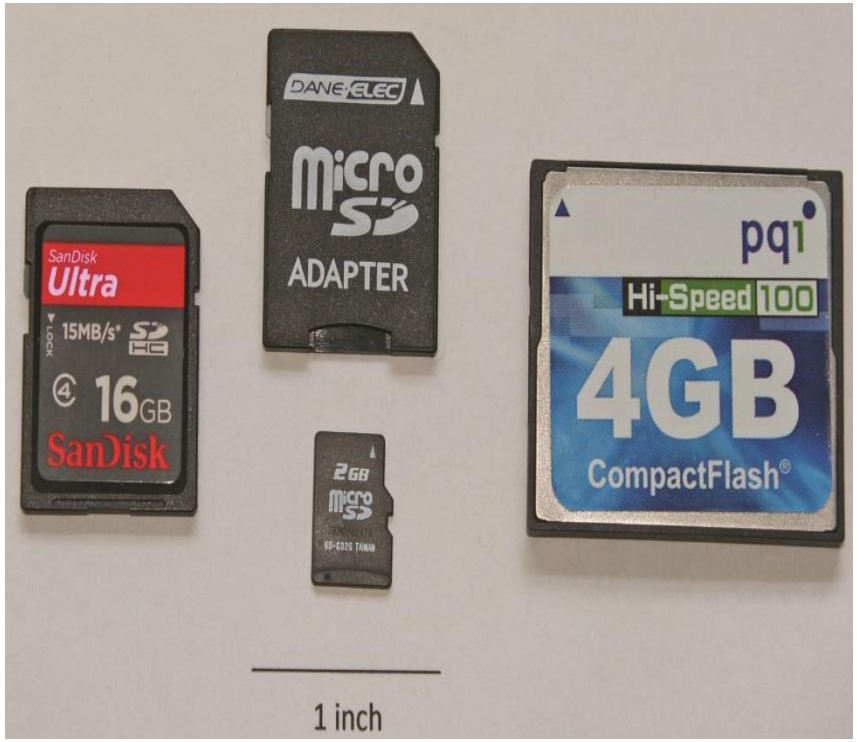
- A **unified threat management (UTM)** appliance refers to the “all-in-one security appliances,” many vendors offer that are devices that combine multiple functions into the same hardware appliance.
  - Most commonly these functions are firewall, IDS/IPS, and antivirus, although all-in-one appliances can include VPN capabilities, antispam, malicious web traffic filtering, antispyware, content filtering, traffic shaping, and so on.
- A UTM simplifies the security activity as a single task, under a common software package for operations.



Unified threat management architecture

Electronic Media

- The latest form of removable media is electronic memory.
  - Static memory which retains data even without power
  - Variety of vendor-specific types:
    - Smart cards, SmartMedia, SD cards, flash cards, memory sticks, and CompactFlash devices
  - Range from small card-like devices to USB sticks
  - Storage size ranges from 256MB to 64GB making them capable of carrying significant quantities of information

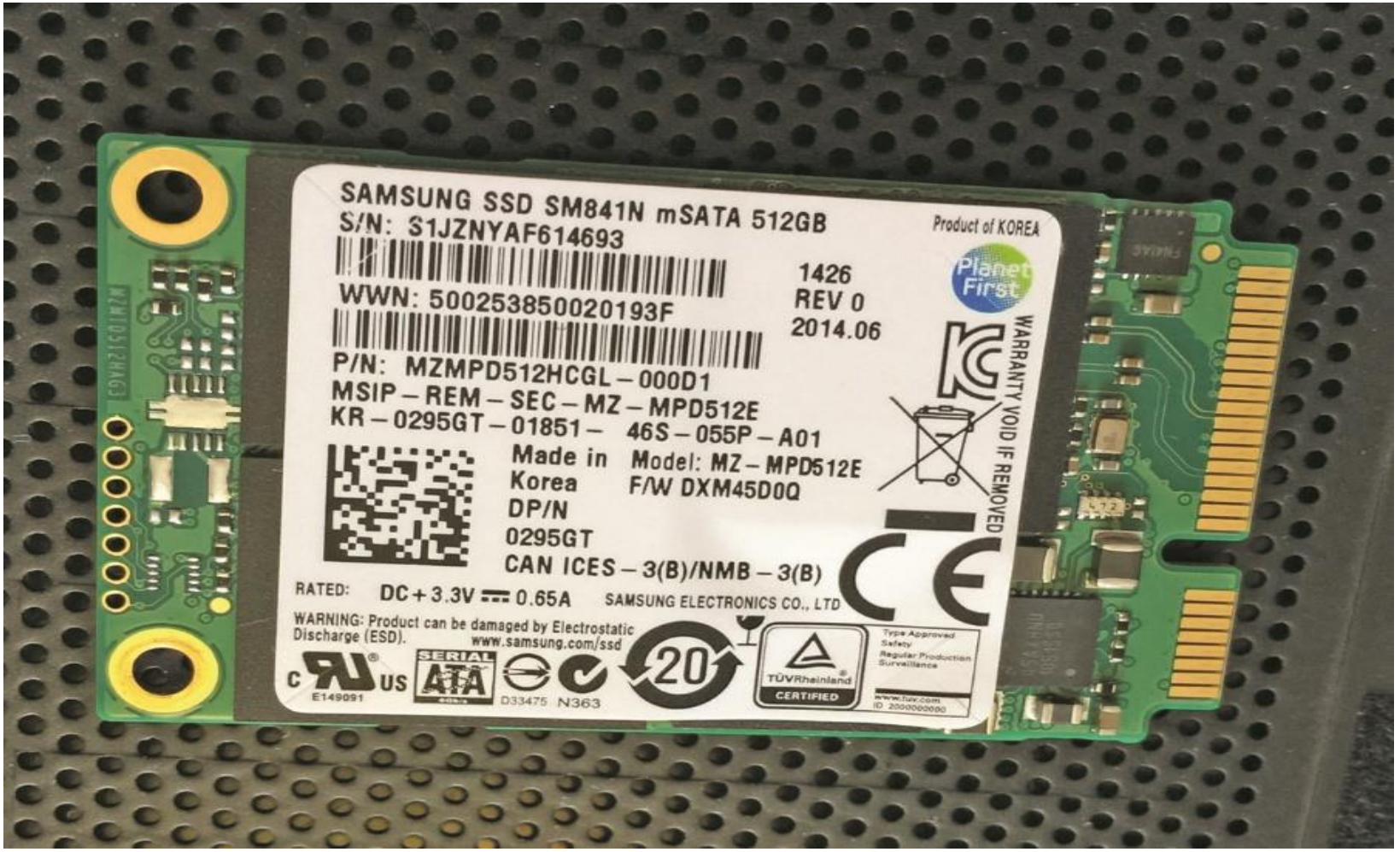


SD, microSD, and CompactFlash cards

128GB USB 3.0 memory stick

Electronic Media (*continued*)

- Solid-state hard drives
  - With the rise of solid-state memory technologies comes a solid-state "hard drive."
  - **Solid-state drives (SSDs)** are moving into mobile devices, desktops, and even servers.
  - Memory densities are significantly beyond physical drives, there are no moving parts to wear out or fail, and SSDs have vastly superior performance specifications.
  - The only factor that has slowed the spread of this technology has been cost, but recent cost reductions have made this form of memory a first choice in many systems.



512GB solid-state half-height minicard

Security Concerns for Transmission Media

- The primary security concern for a system administrator must be preventing physical access to a server by an unauthorized individual.
- One of the administrator's next major concerns should be preventing unfettered access to a network connection.
- Preventing such access is costly, yet the cost of replacing a server because of theft is also costly.