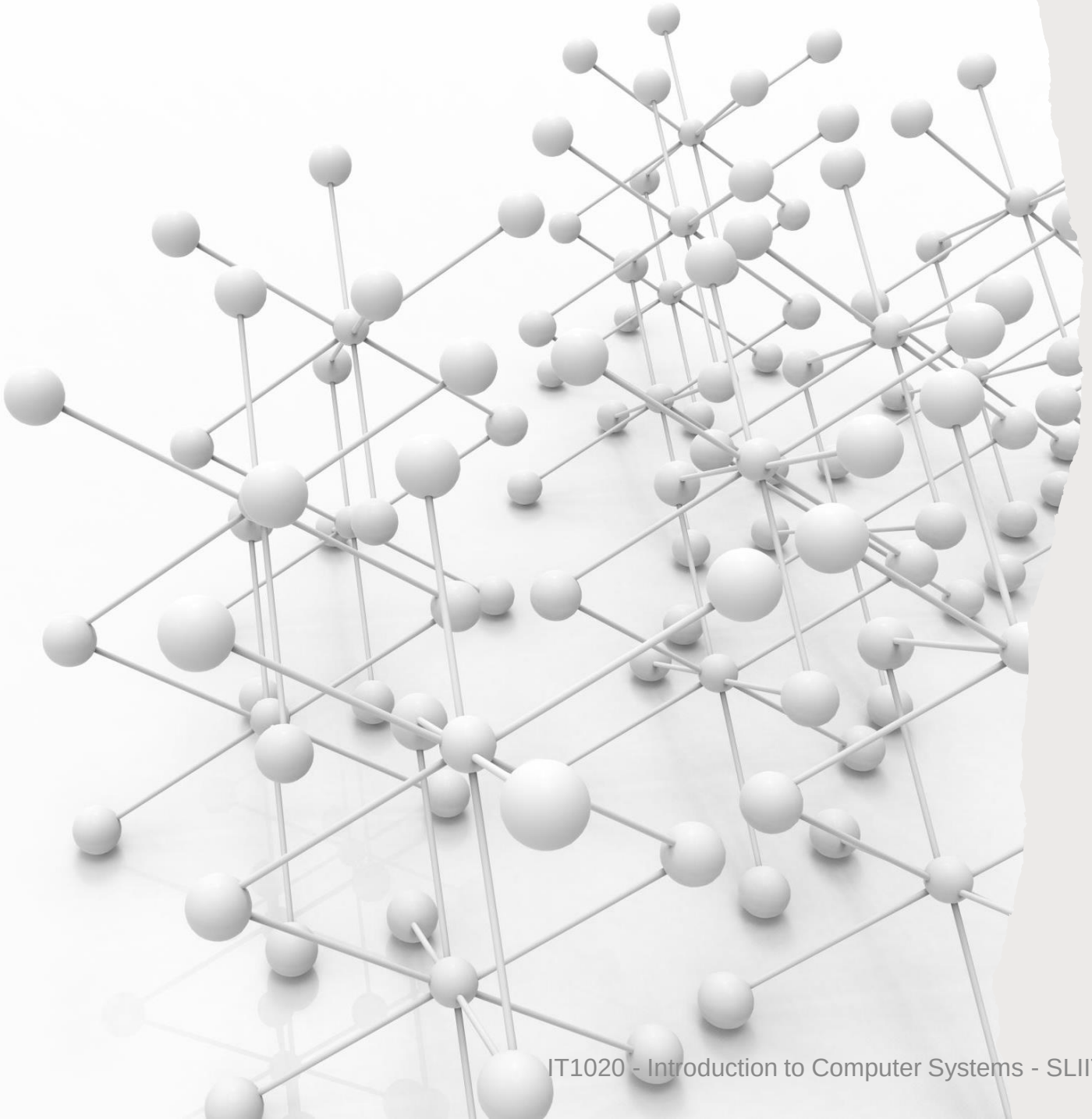
Introduction to Computer Systems

Computer networks



Lecture 11

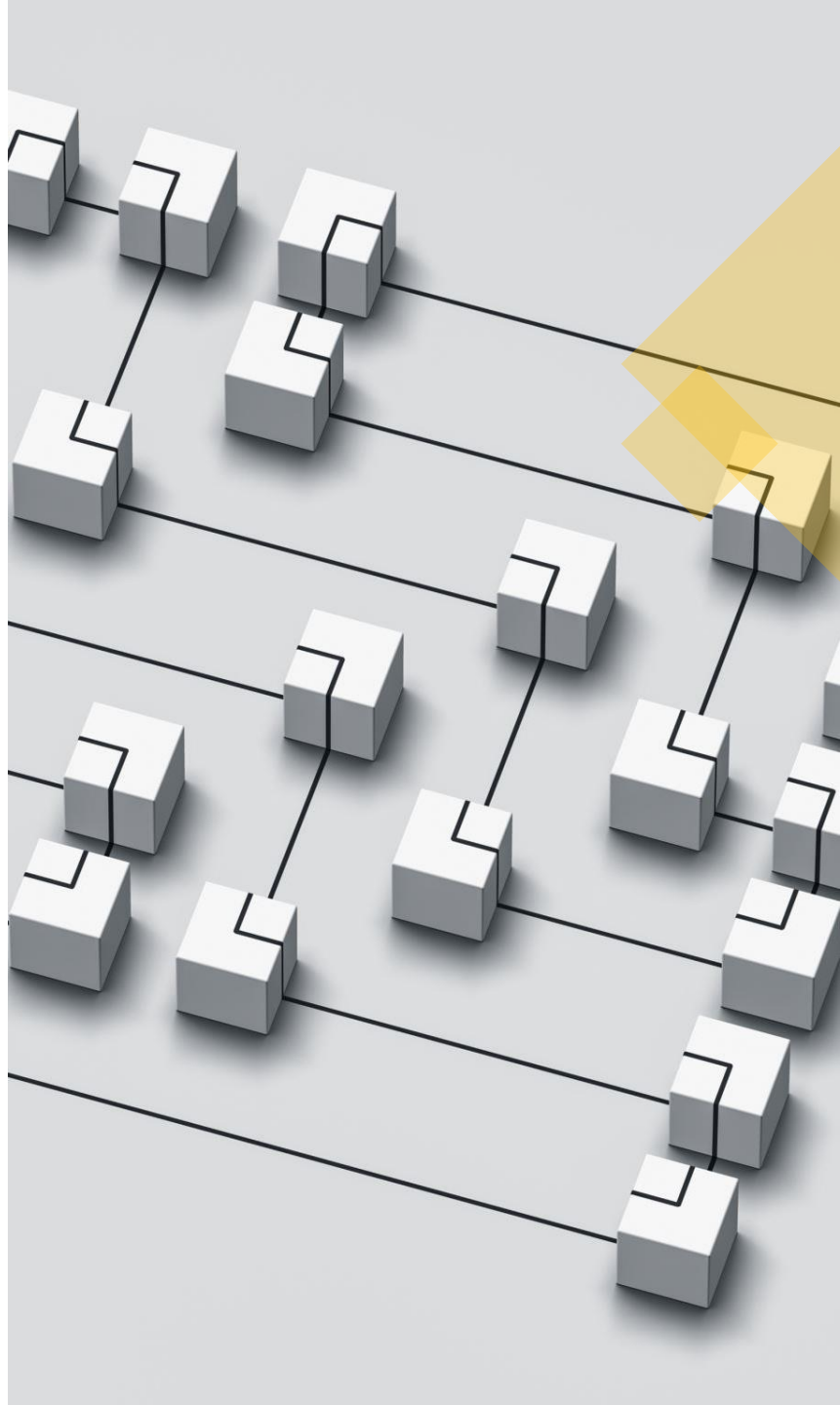
Design a Network

Lecture Outline

- Design Considerations for a Small Network
- Scale to a Large Network
- Threats to the Network
- Keeping the Network Safe

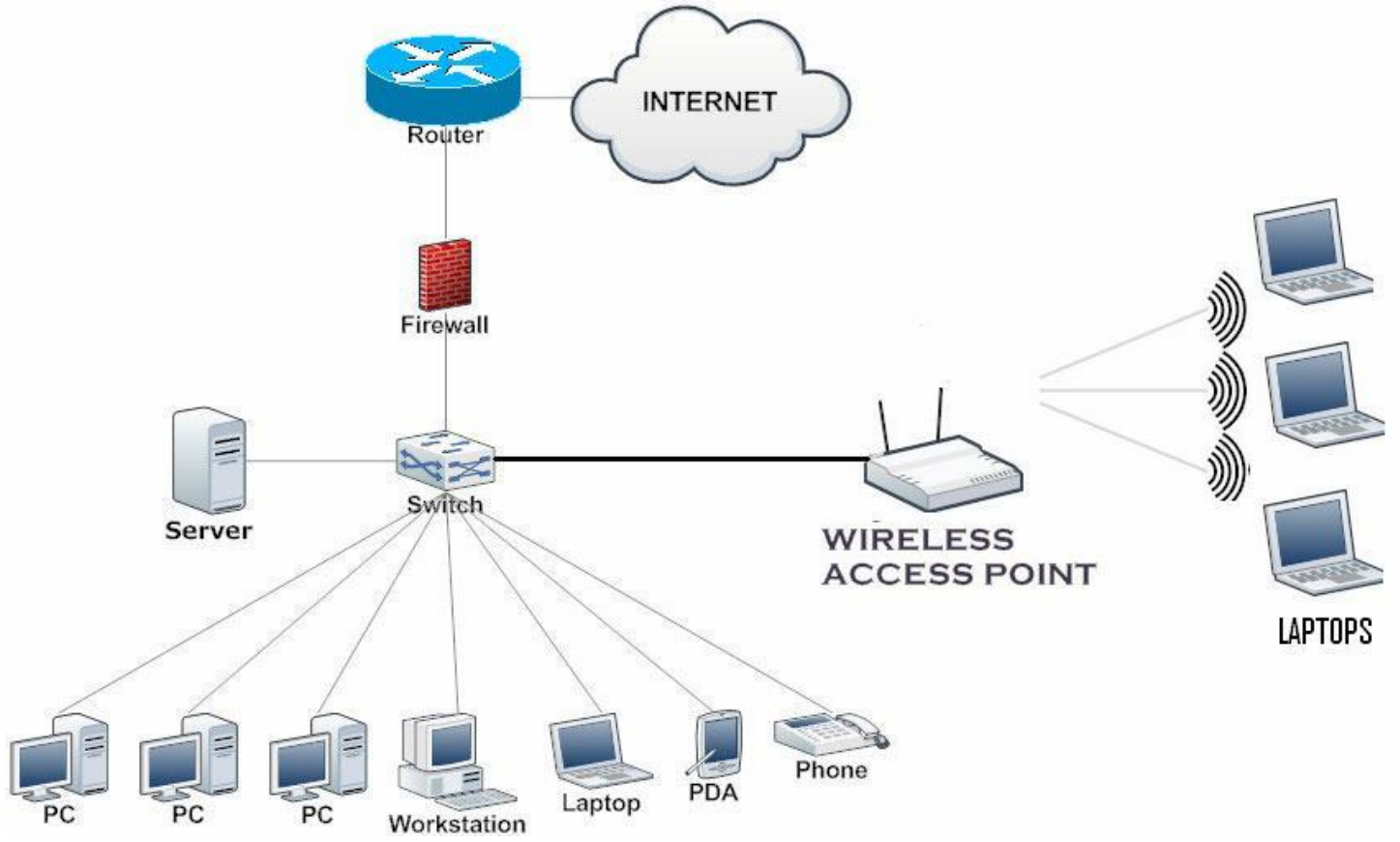
Design and Create a Small Network

- ✓Topologies
- ✓Device selection
- ✓IP addressing
- ✓Redundancy
- ✓Design considerations
- ✓Common applications
- ✓Common protocols
- ✓Real time applications
- ✓Scaling the small network
- ✓Protocol analysis



Topologies

Typical Small Network Topology



Device Selection

Factors to be considered when selecting intermediate devices.

COST

PORTS

SPEED

EXPANDABLE/ MODULAR

MANAGEABLE

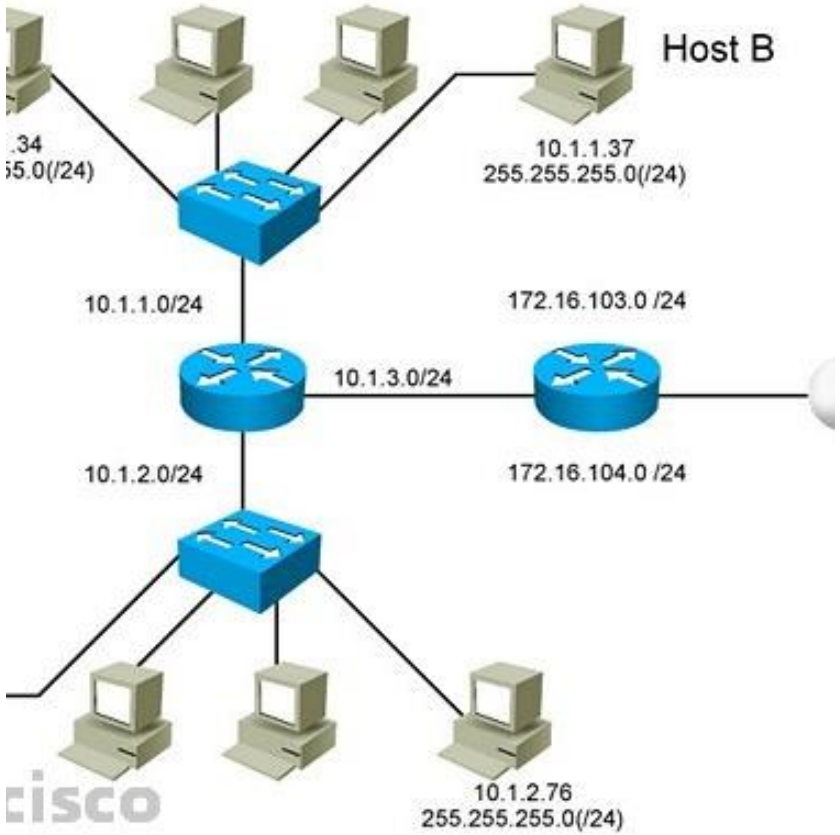
IP Addressing

- IP addressing scheme should be planned, documented and maintained based on the type of devices receiving the address.

- Examples of devices that will be part of the IP design:
  - End devices for users
  - Servers and peripherals
  - Hosts that are accessible from the Internet
  - Intermediary devices

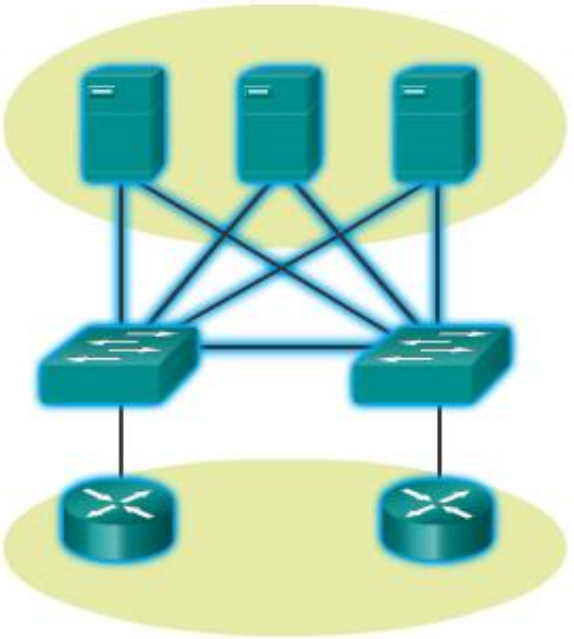
IP Addressing cont.

- Planned IP schemes help the administrator:
  - Track devices and troubleshoot
  - Control access to resources



Redundancy

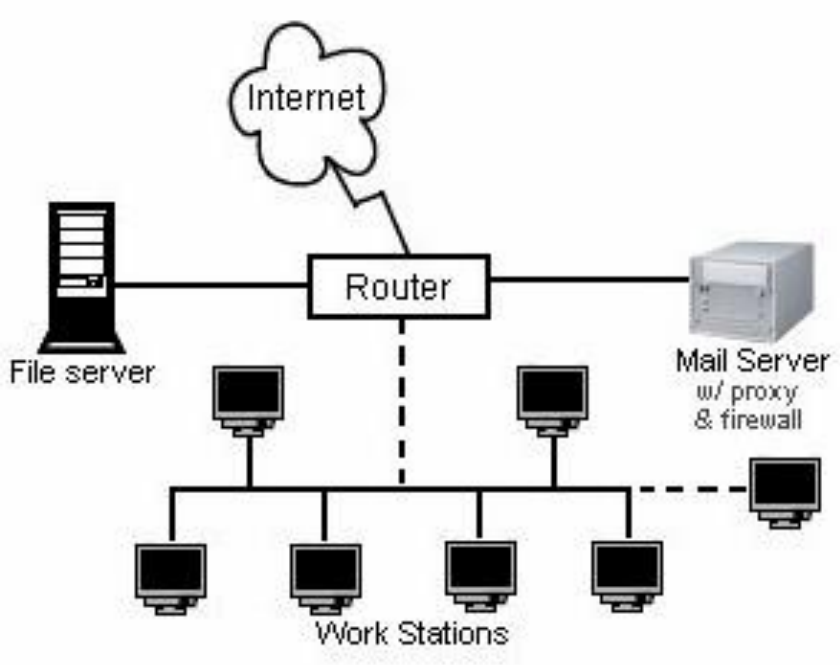
- Redundancy helps to eliminate single points of failure.
- Improves the reliability of the network.

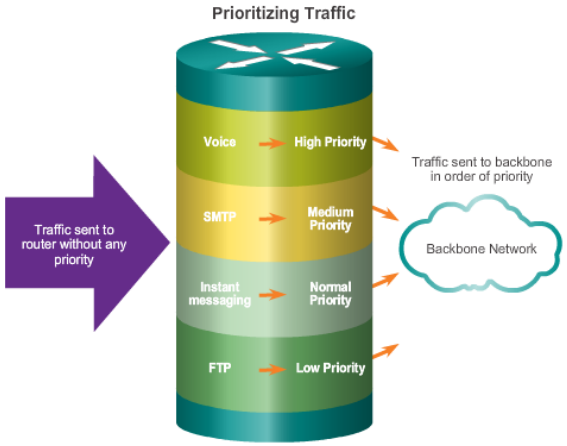


Redundancy to a Server Farm

Design Considerations

- The following should be included in the network design:
  - Secure file and mail servers in a centralized location.
  - Protect the location by physical and logical security measures.
  - Create redundancy in the server farm.





Common Applications

✓ **Network-Aware Applications**

Software programs that are used to communicate over the network.

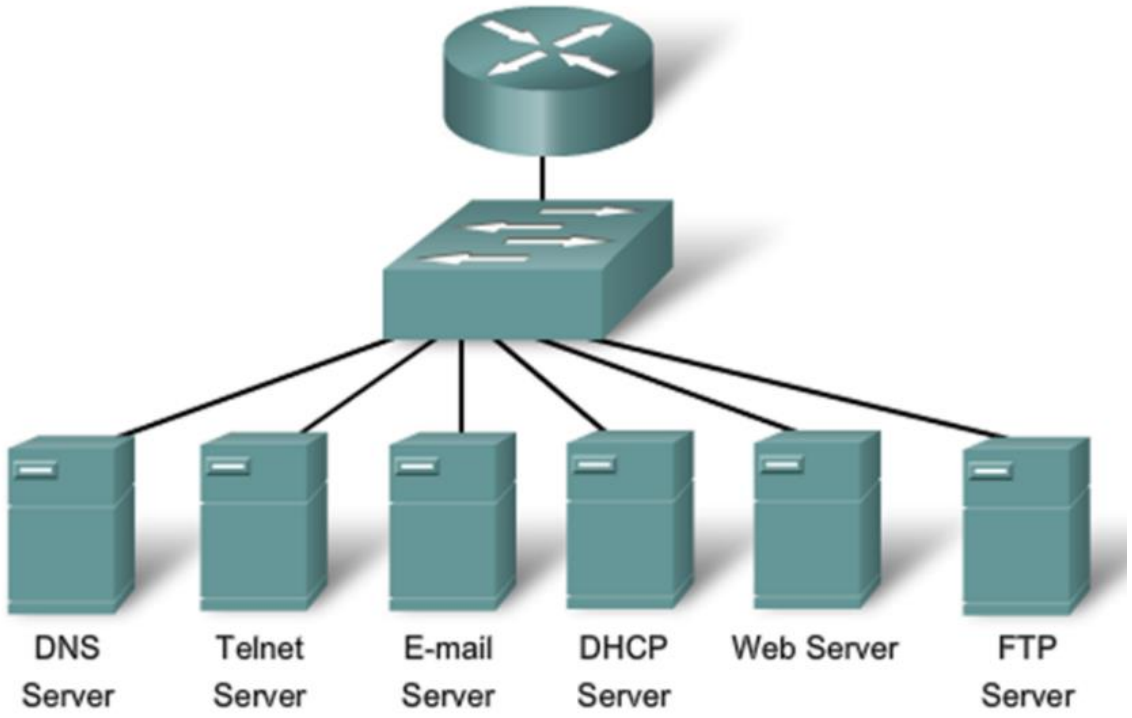
✓ **Application Layer Services**

Programs that interface with the network and prepare the data for transfer.

Common Protocols

Network Protocols Define:

- Processes on either end of a communication session.
- Types of messages.
- Syntax of the messages.
- Meaning of informational fields.
- How messages are sent and the expected response.
- Interaction with the next lower layer.



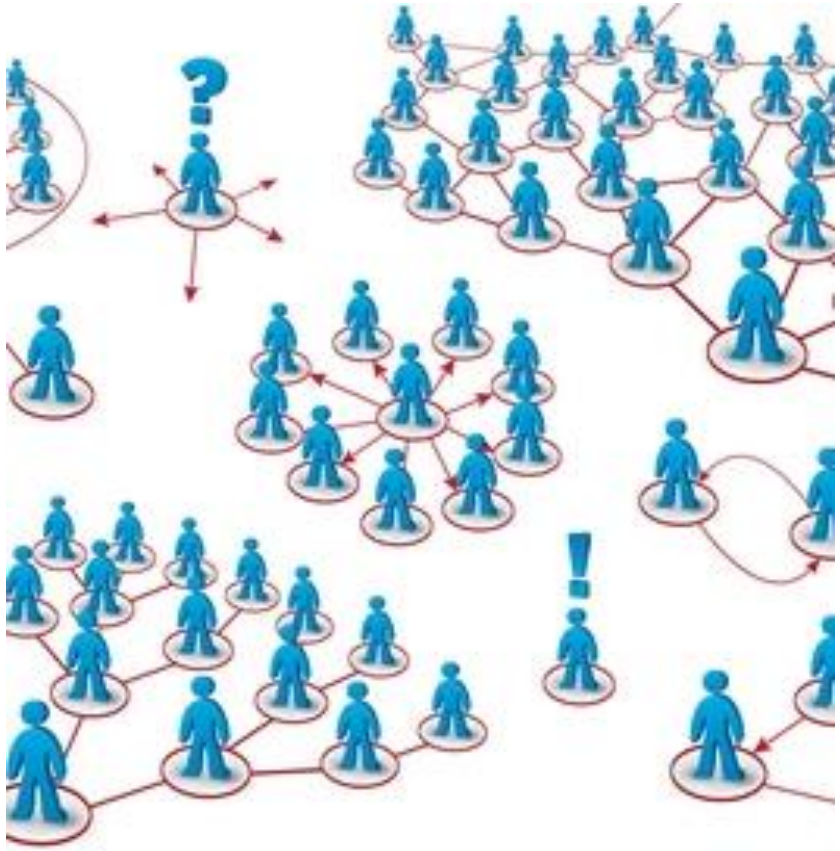
Real-Time Applications

- Real-time applications require planning and dedicated services to ensure priority delivery of voice and video traffic.
  - ✓ **Infrastructure** – Needs to be evaluated to ensure it will support proposed real time applications.
  - ✓ **VoIP** – Is implemented in organizations that still use traditional telephones.
  - ✓ **IP telephony** – The IP phone itself performs voice-to-IP conversion**.**
  - ✓ **Real-time Video Protocols** – Use Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP).

Scaling a Small Network

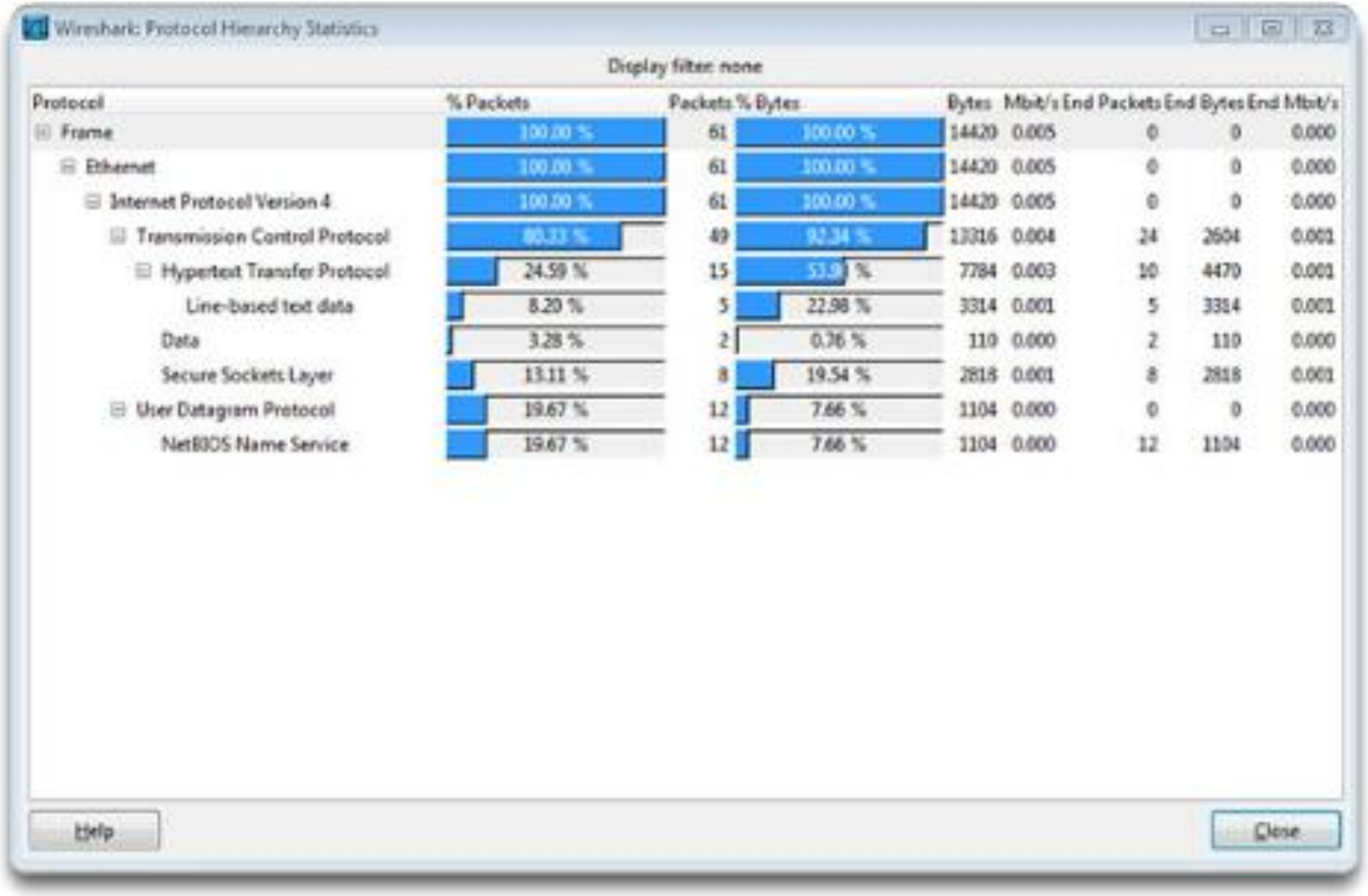
Important considerations when growing to a larger network:

- **Documentation** –Physical and logical topology.
- **Device inventory** – List of devices that use or comprise the network.
- **Budget** – Itemized IT expense items, including the amount of money allocated to equipment purchase for that fiscal year.
- **Traffic Analysis** – Protocols, applications, and services and their respective traffic requirements should be documented.



Protocol Analysis

- Information gathered by protocol analysis can be used to make decisions on how to manage traffic more efficiently.



Keeping the Network Safe

- Threats to Network Security
- Physical Security
- Security Vulnerabilities
- Malware
- Network Attacks
- Mitigating Network Attacks

Threats to Network Security

- Categories of Threats to Network Security

Information Theft

Data Loss and Manipulation

Identity Theft

Disruption of Service

Physical Security

Four classes of physical threats are:

- **Hardware threats**
  - ✓Physical damage to servers, routers, switches, cabling plant, and workstations

- **Environmental threats**
  - ✓Temperature extremes (too hot or too cold)
  - ✓humidity extremes (too wet or too dry)

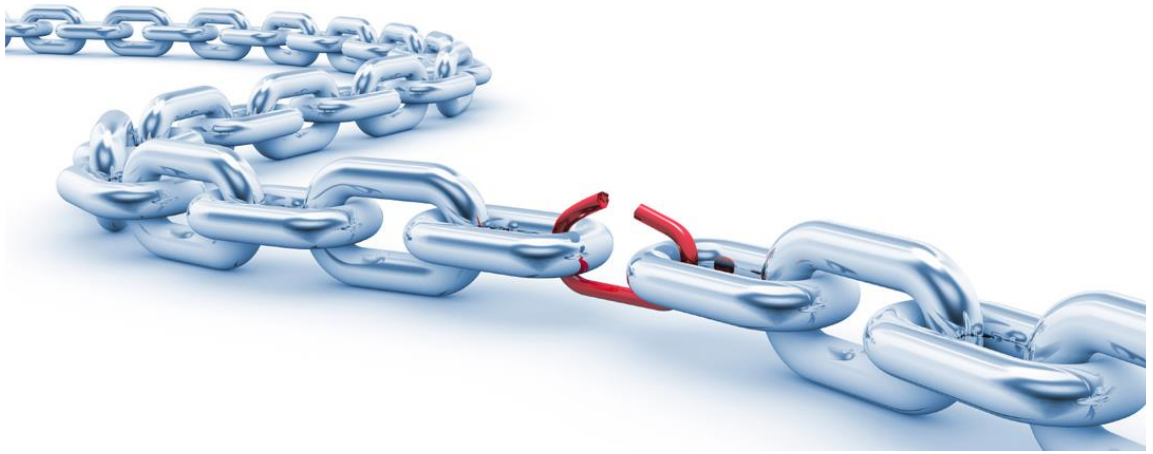
Physical Security Cont.

- **Electrical threats**
  - ✓voltage spikes
  - ✓insufficient supply voltage (brownouts)
  - ✓unconditioned power (noise)
  - ✓total power loss

- **Maintenance threats**
  - ✓Poor handling of key electrical components (electrostatic discharge)
  - ✓lack of critical spare parts
  - ✓poor cabling
  - ✓poor labeling

Types of Security Vulnerabilities

- ✓ Technological
- ✓ Configuration
- ✓ Security policy



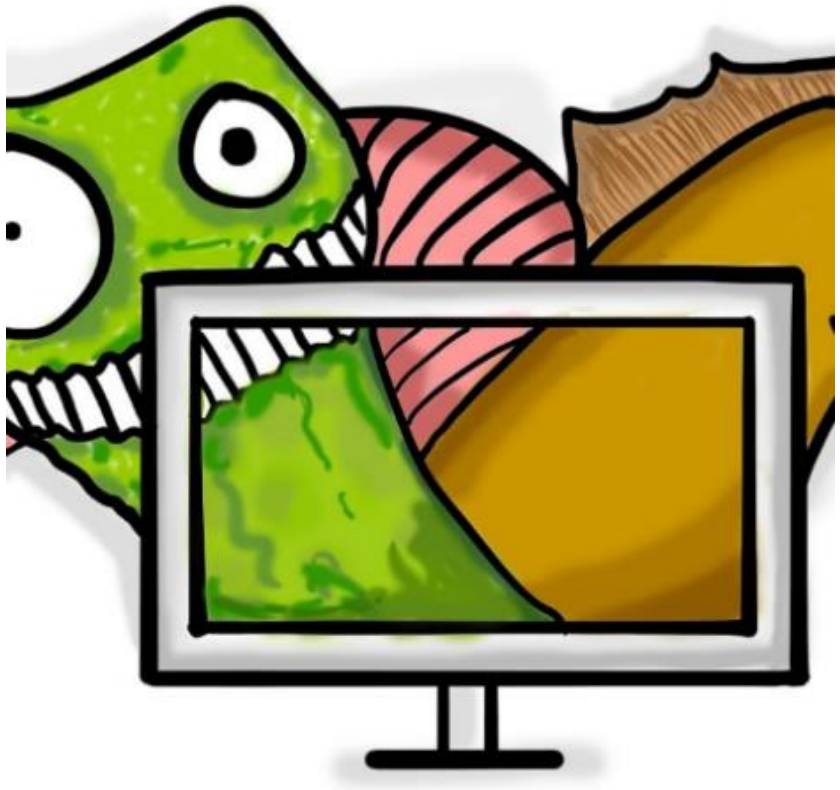
Malware

Virus

- ✓Malicious software that is attached to another program to execute a particular unwanted function on a workstation.

Trojan horse

- ✓An entire application written to look like something else, when in fact it is an attack tool.



Malware cont.

Worms

- ✓Worms are self-contained programs that attack a system and try to exploit a specific vulnerability in the target.
- ✓The worm copies its program from the attacking host to the newly exploited system to begin the cycle again.

Network Attacks

- Malware is a means to get a payload delivered.
- When it is delivered and installed, the payload can be used to cause a variety of network related attacks.

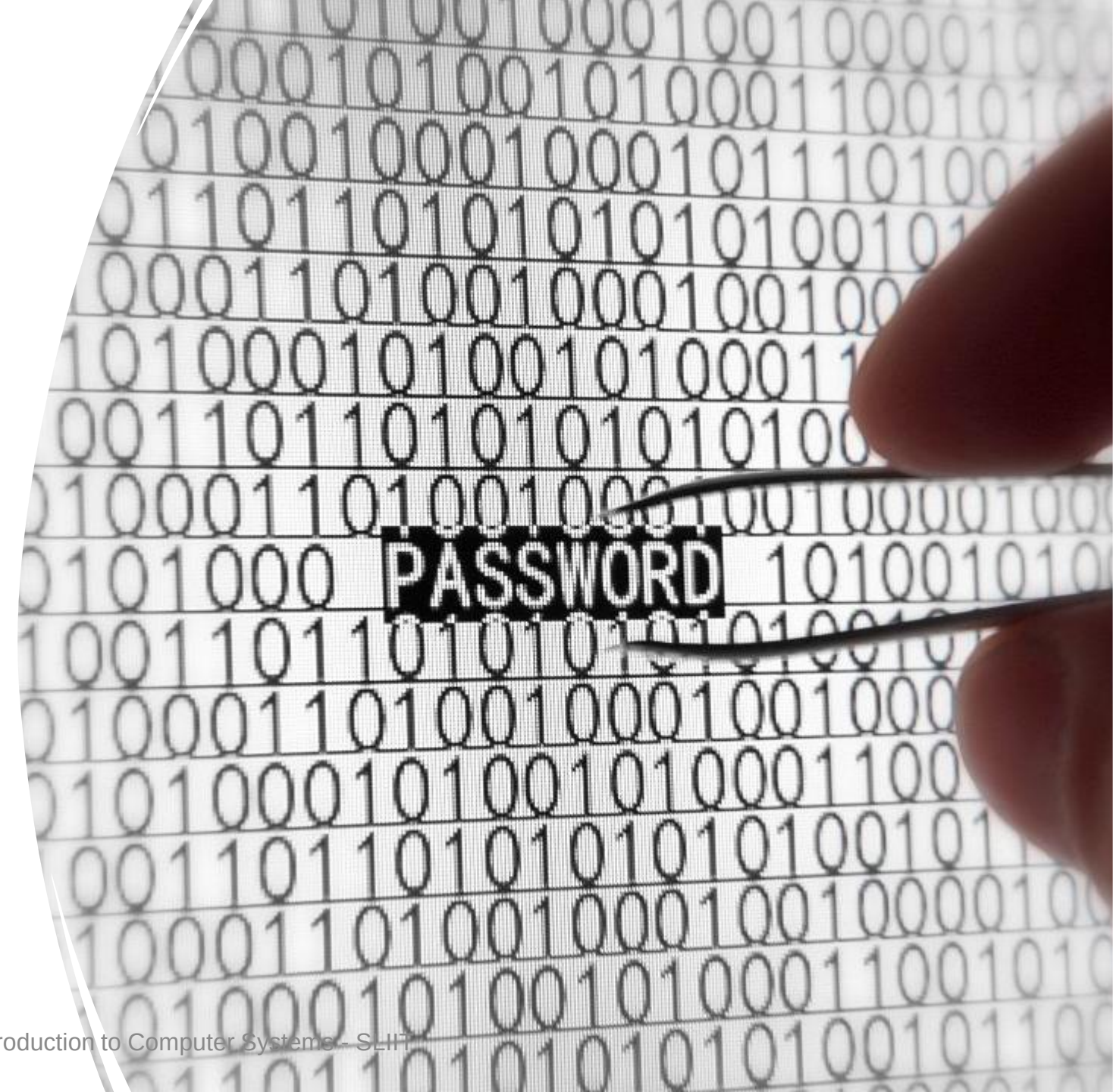
- **Categories of network attacks:**
  - Reconnaissance Attacks
  - Access Attacks
  - Social Engineering Attacks
  - DoS Attacks

Reconnaissance Attacks

- Known as information gathering.
- Analogous to a thief surveying a neighborhood by going door-to-door pretending to sell something.
- Eg:
  - Perform an information query of a target
  - Initiate a port scan of active IP addresses
  - Run Vulnerability Scanners

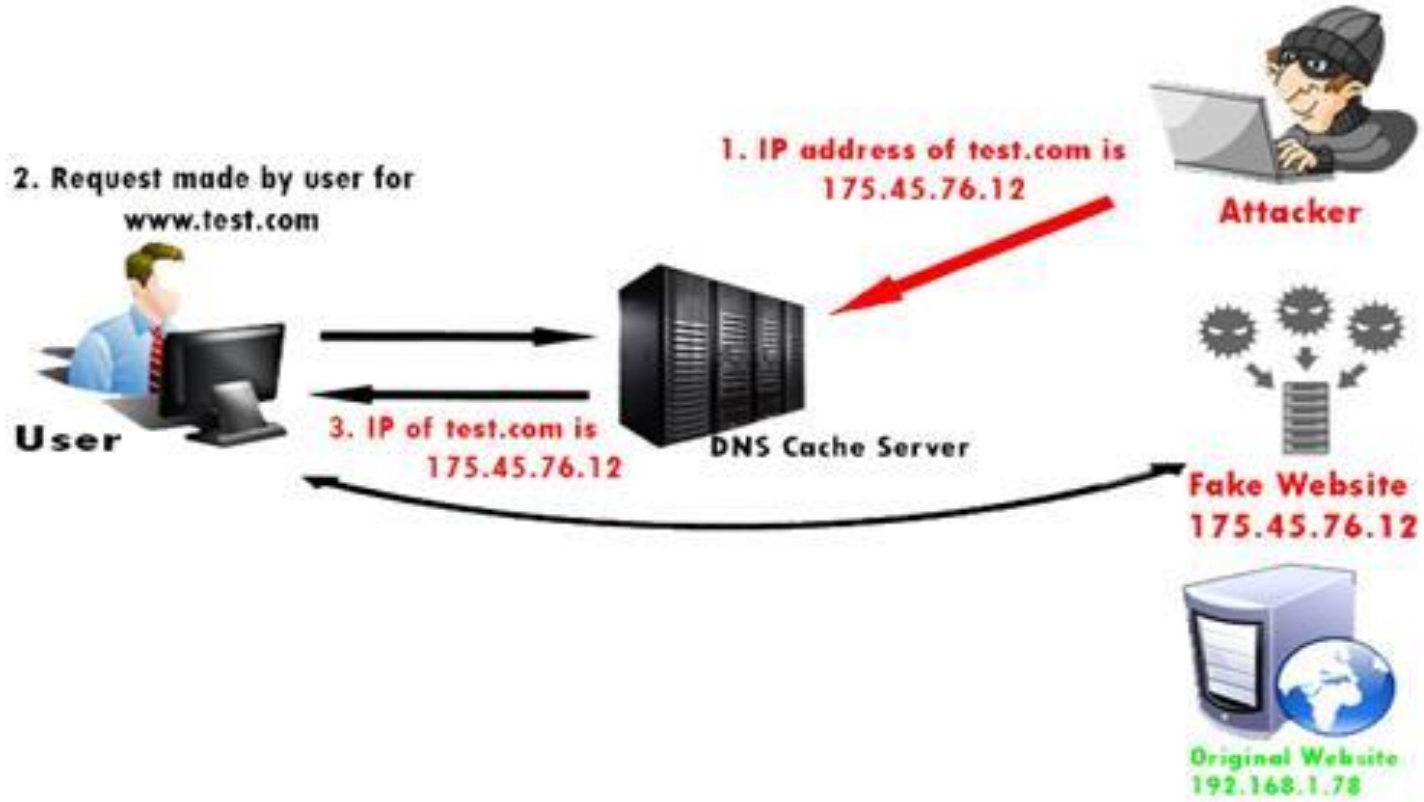
Access Attacks

- **Password Attacks**
  - Brute-force attack
  - Dictionary attack



Port Re-direction

ACCESS ATTACKS CONT.

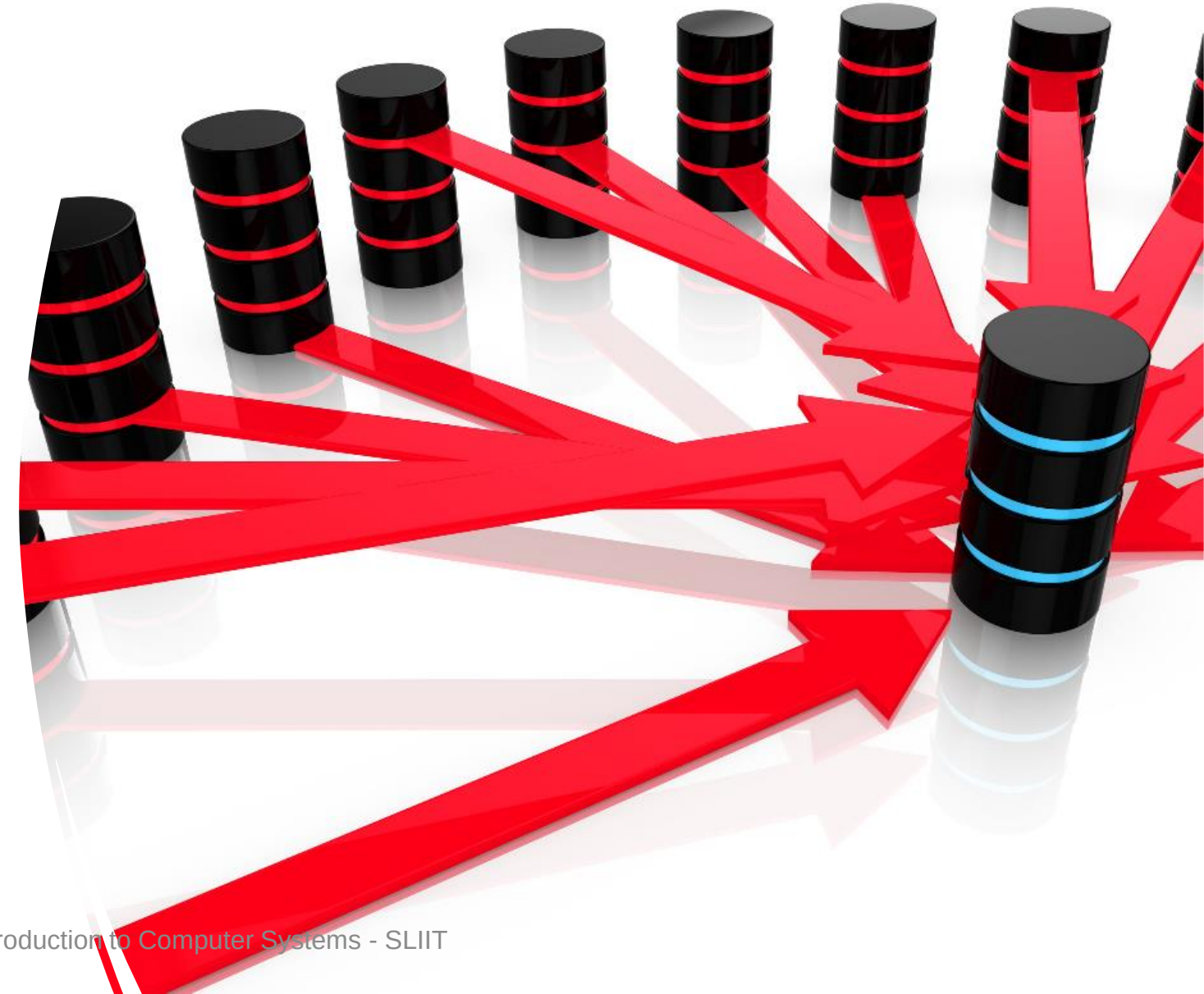


Social Engineering

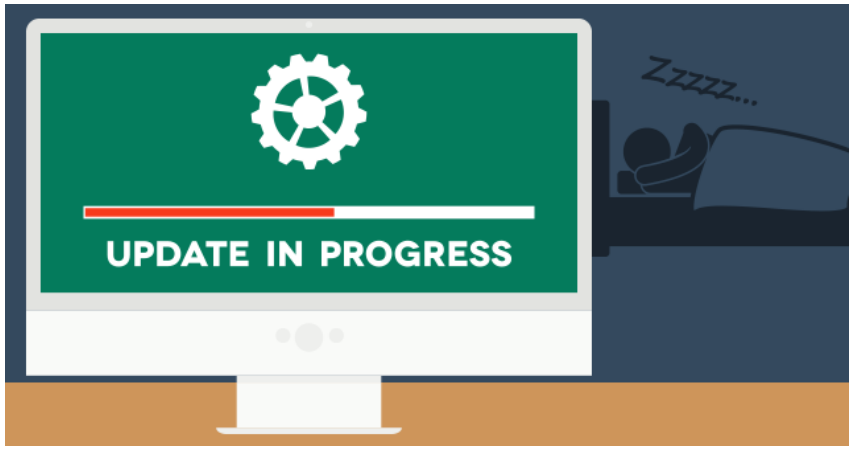
- Attempts to manipulate individuals into performing actions or divulging confidential information.

Denial of Service Attacks (DoS)

- Attacker floods servers, systems or networks with traffic in order to overwhelm the victim resources and make it difficult or impossible for legitimate users to use them.



Mitigating Network Attacks



Backup, Upgrade, Update, and Patch

- Antivirus software can detect most viruses and many Trojan horse applications and prevent them from spreading in the network.
- Keep current with the latest versions of antivirus software.
- Install updated security patches.

Mitigating Network Attacks

Authentication, Authorization, and Accounting (AAA)

Authentication

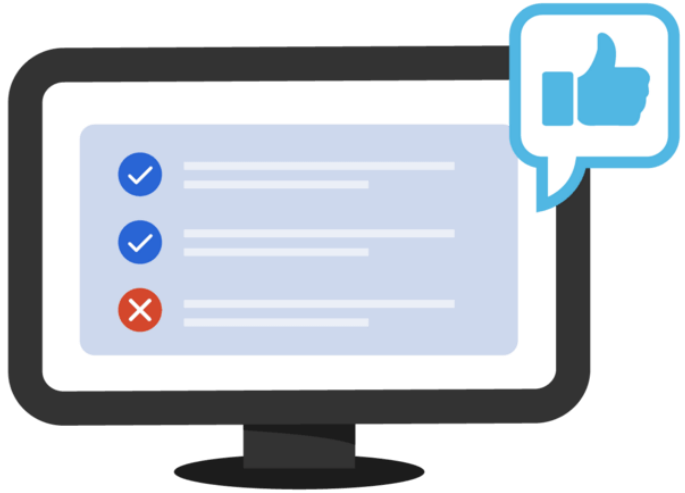
- Users and administrators must prove their identity.
  - ✓Username and password combinations
  - ✓Challenge and response questions
  - ✓Token cards

Mitigating Network Attacks

Authentication, Authorization, and Accounting (AAA)

Authorization

- Determines which resources the user can access and the operations that the user is allowed to perform.



Gives users permission to access a resource.

Mitigating Network Attacks

Authentication, Authorization, and Accounting (AAA)

Accounting

- Records what the user accessed, the amount of time the resource is accessed, and any changes made.

Mitigating Network Attacks

Firewalls

- A Firewall resides between two or more networks.
- It controls traffic and helps prevent unauthorized access.

Mitigating Network Attacks

Firewalls Cont.

- Methods used are:
  - Packet Filtering
  - Application Filtering
  - URL Filtering
  - Stateful Packet Inspection (SPI) – Incoming packets must be legitimate responses to requests from internal hosts.

MITIGATING NETWORK ATTACKS CONT.

Endpoint Security

- Common endpoints: laptops, desktops, servers, smart phones, and tablets.
- Employees must follow the companies documented security policies to secure their devices.
- Policies include the use of anti-virus software and host intrusion prevention.

THANK YOU!