Cisco Networking Academy

CCNA R&S: Introduction to Networks

Chapter 11:

It’s a Network

Frank Schneemann

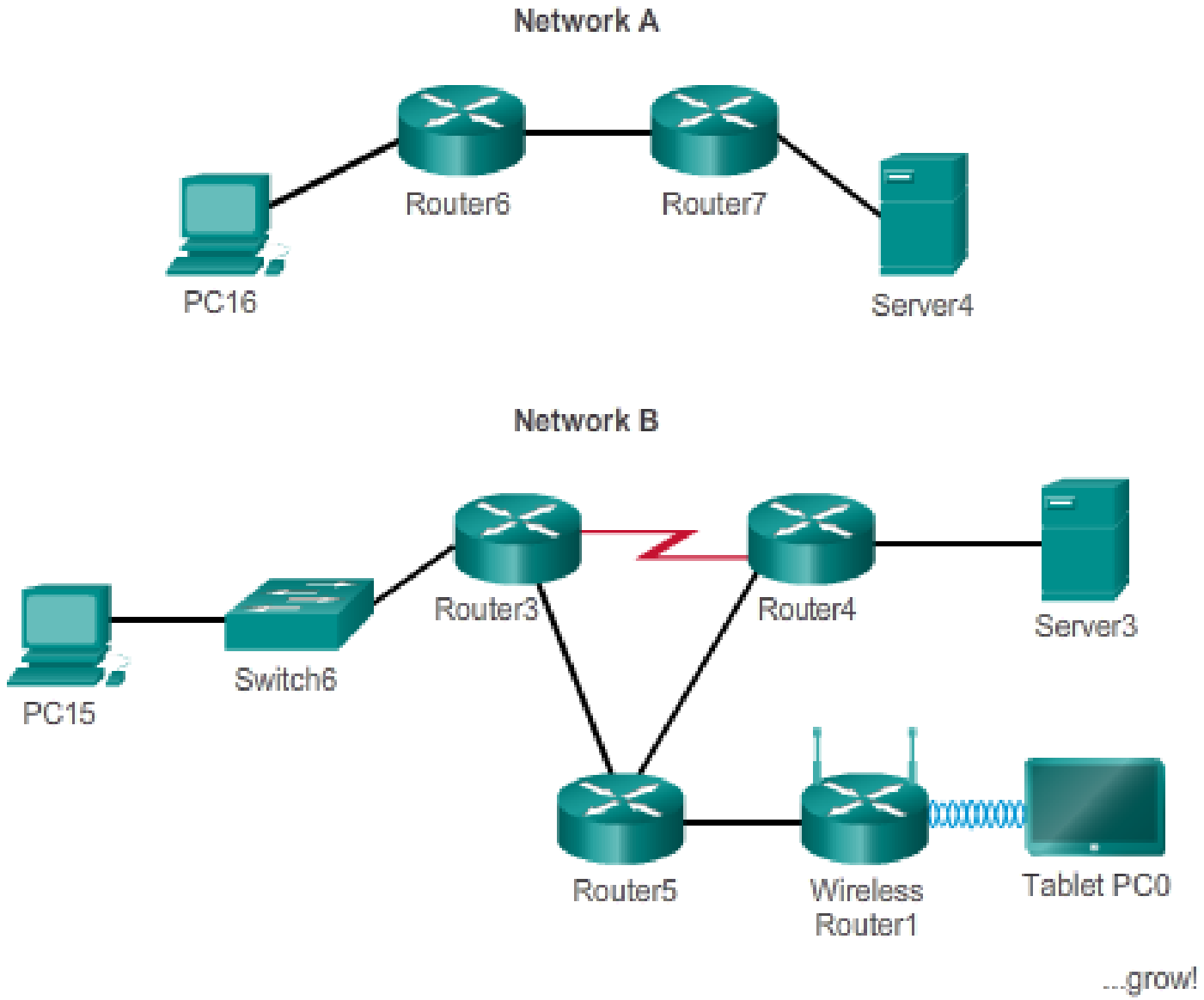
11.0.1.1 Introduction

Upon completion of this chapter you will be able to:

- Identify the devices and protocols used in a small network.
- Explain how a small network serves as the basis of larger networks.
- Describe the need for basic security measures on network devices.
- Identify security vulnerabilities and general mitigation techniques.
- Configure network devices with device hardening features to mitigate security threats.
- Use the output of the **`ping`** and **`tracert`** commands to establish relative network performance.
- Use basic **`show`** commands to verify the configuration and status of a device interface.
- Use the basic host and IOS commands to acquire information about the devices in a network.
- Explain file systems on routers and switches.
- Apply the commands to back up and restore and IOS configuration file.

11.0.1.2 Activity – Did You Notice…?

Create and…

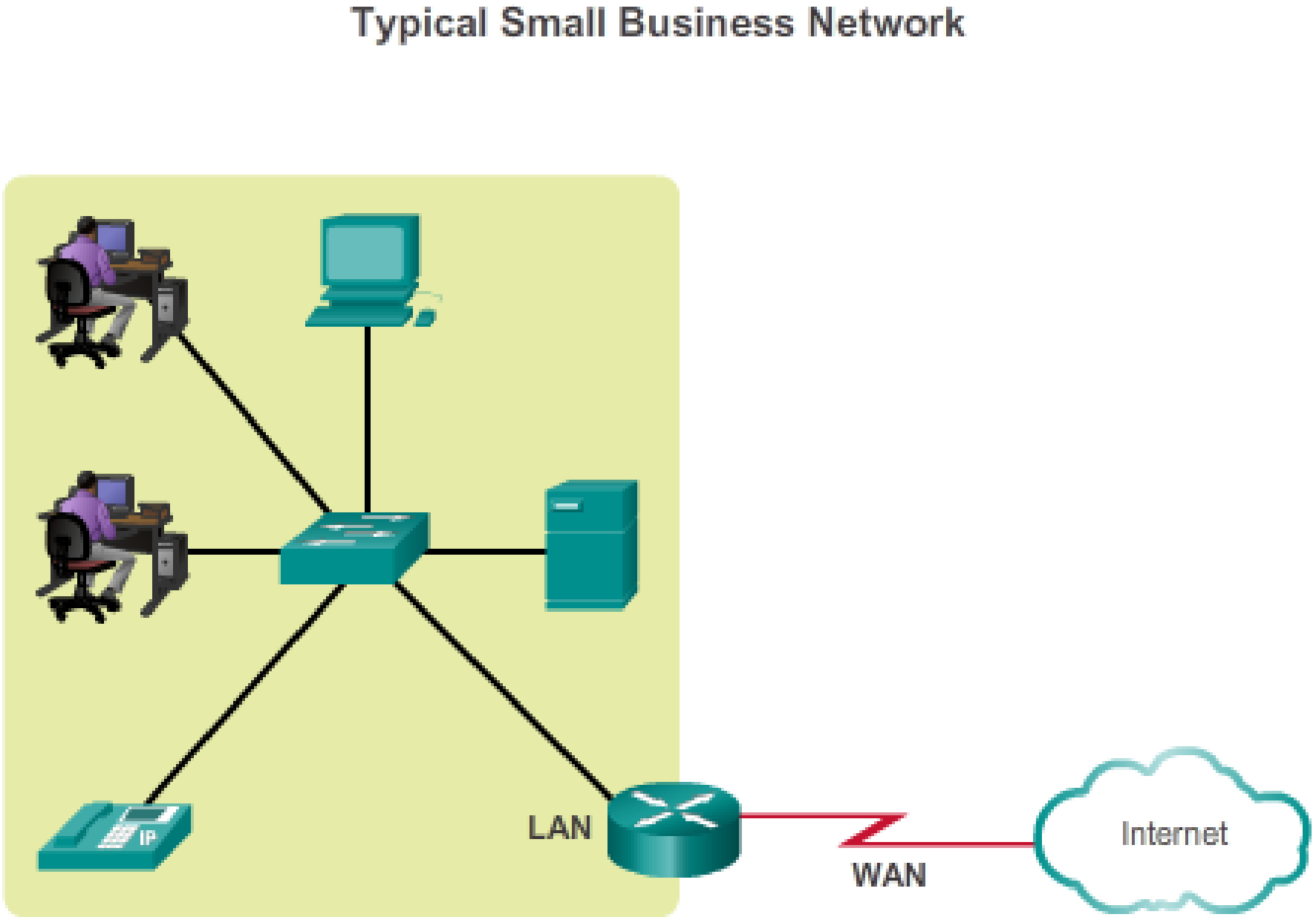


Take a look at the two networks in the diagram. Visually compare and contrast the two networks. Make note of the devices used in each network design. Since the devices are labeled, you already know what types of end devices and intermediate devices are on each network.

But how are the two networks different? Is it just that there are more devices present on Network B than on Network A?

Select the network you would use if you owned a small to medium-sized business. Be able to justify your selected network based on cost, speed, ports, expandability, and manageability.

11.1.1.1 Small Network Topologies



11.1.1.2 Device Selection for a Small Network

Factors to Consider in Choosing a Device

Cost

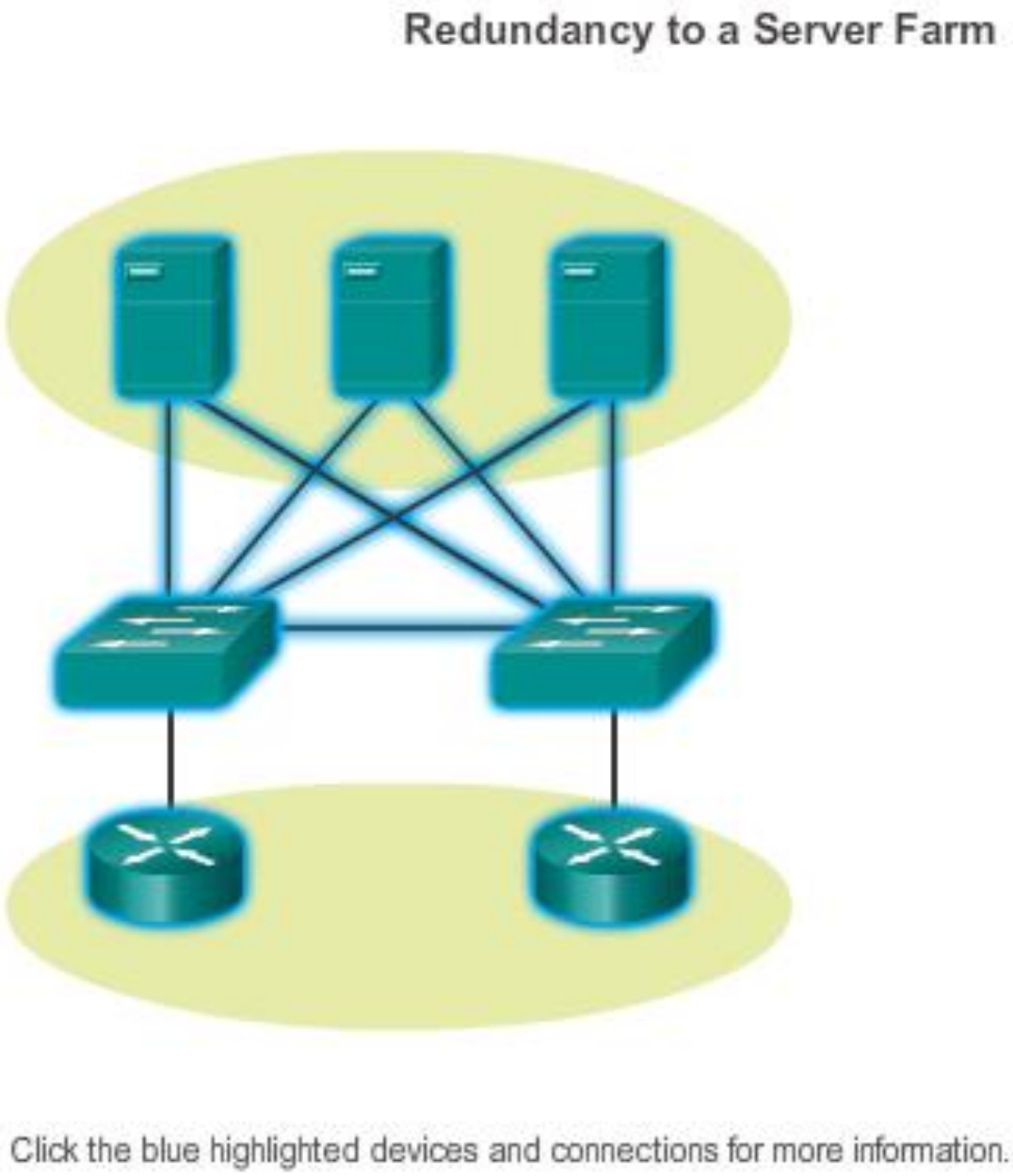
Ports

Speed

Expandable/Modular

Manageable

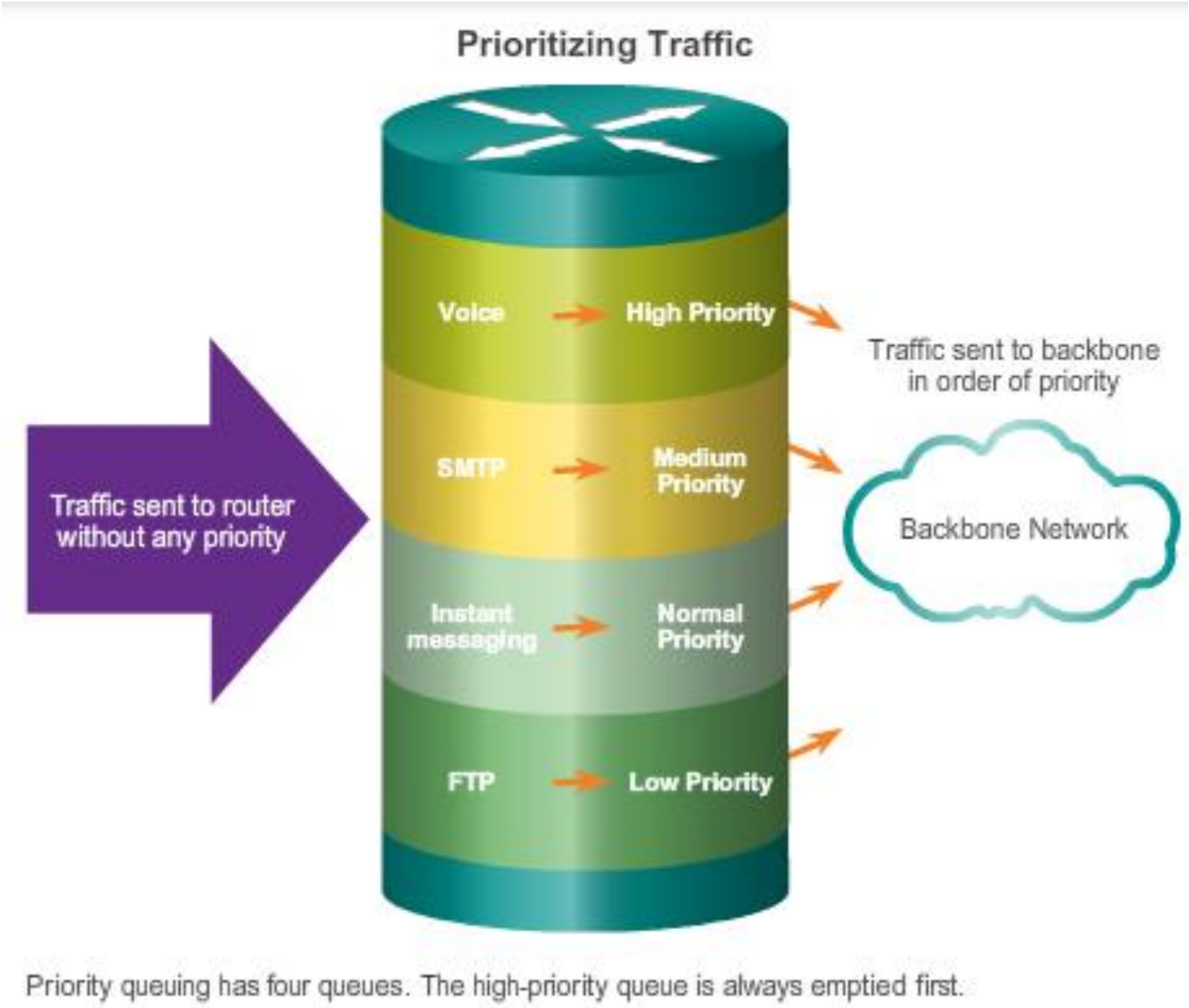
11.1.1.4 Redundancy in a Small Network



The smaller the network, the less the chance that redundancy of equipment will be affordable. Therefore, a common way to introduce redundancy is through the use of redundant switch connections between multiple switches on the network and between switches and routers.

Also, servers often have multiple NIC ports that enable redundant connections to one or more switches. In a small network, servers typically are deployed as web servers, file servers, or email servers.

11.1.1.5 Design Considerations for a Small Network



Priority queuing has four queues. The high-priority queue is always emptied first.

Users expect immediate access to their emails and to the files that they are sharing or updating. To help ensure this availability, the network designer should take the following steps:

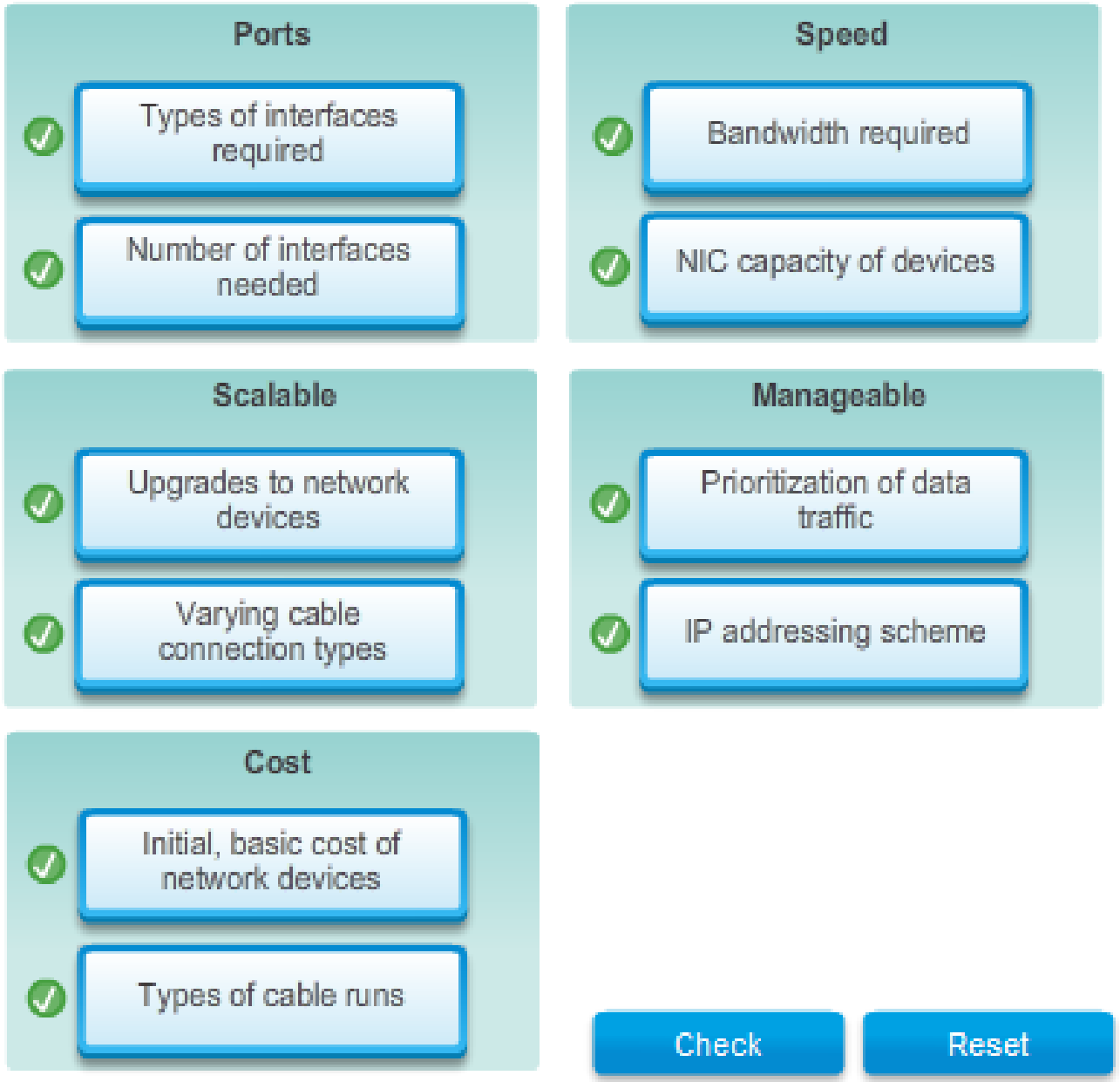
Step 1. Secure file and mail servers in a centralized location.

Step 2. Protect the location from unauthorized access by implementing physical and logical security measures.

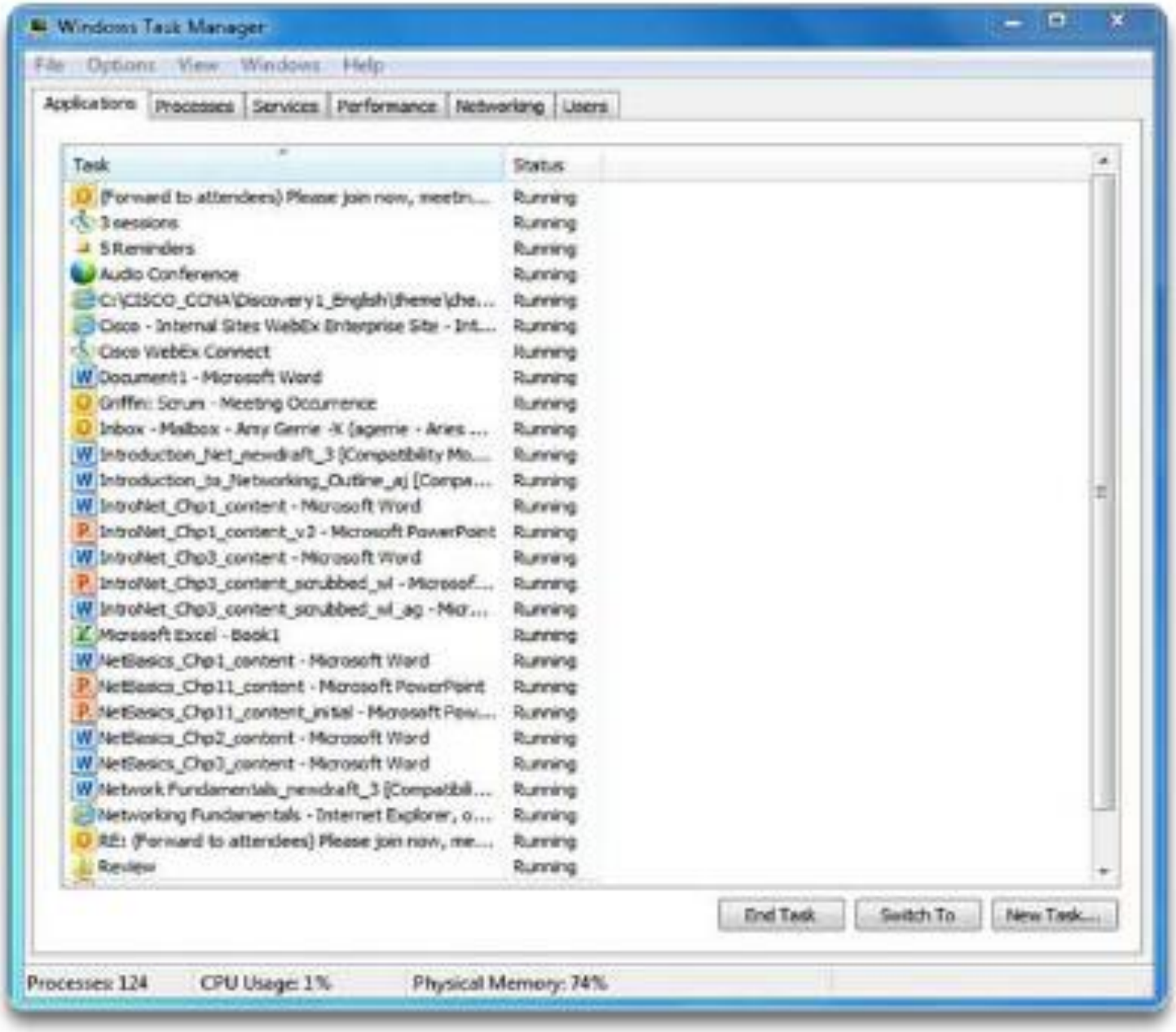
Step 3. Create redundancy in the server farm that ensures if one device fails, files are not lost.

Step 4. Configure redundant paths to the servers.

11.1.1.6 Identifying Network Planning and Design Factors

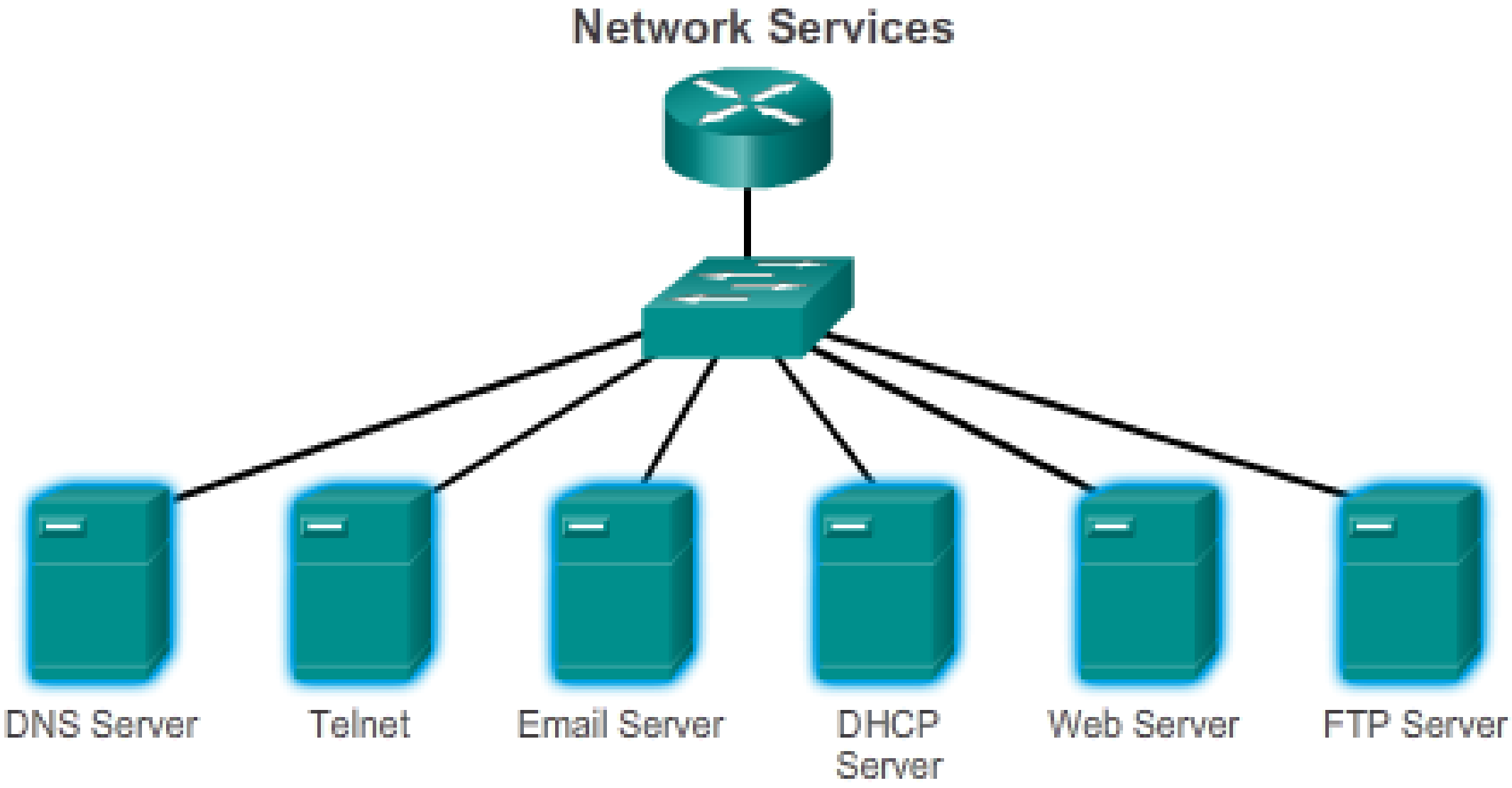


11.1.2.1 Common Applications in a Small Network



The network is only as useful as the applications that are on it. As shown in the figure, within the application layer, there are two forms of software programs or processes that provide access to the network**: network applications and application layer services.**

11.1.2.2 Common Protocols in a Small Network



11.1.2.3 Real-Time Applications for a Small Network

In addition to the common network protocols described previously, modern businesses, even small ones, typically utilize real-time applications for communicating with customers and business partners.

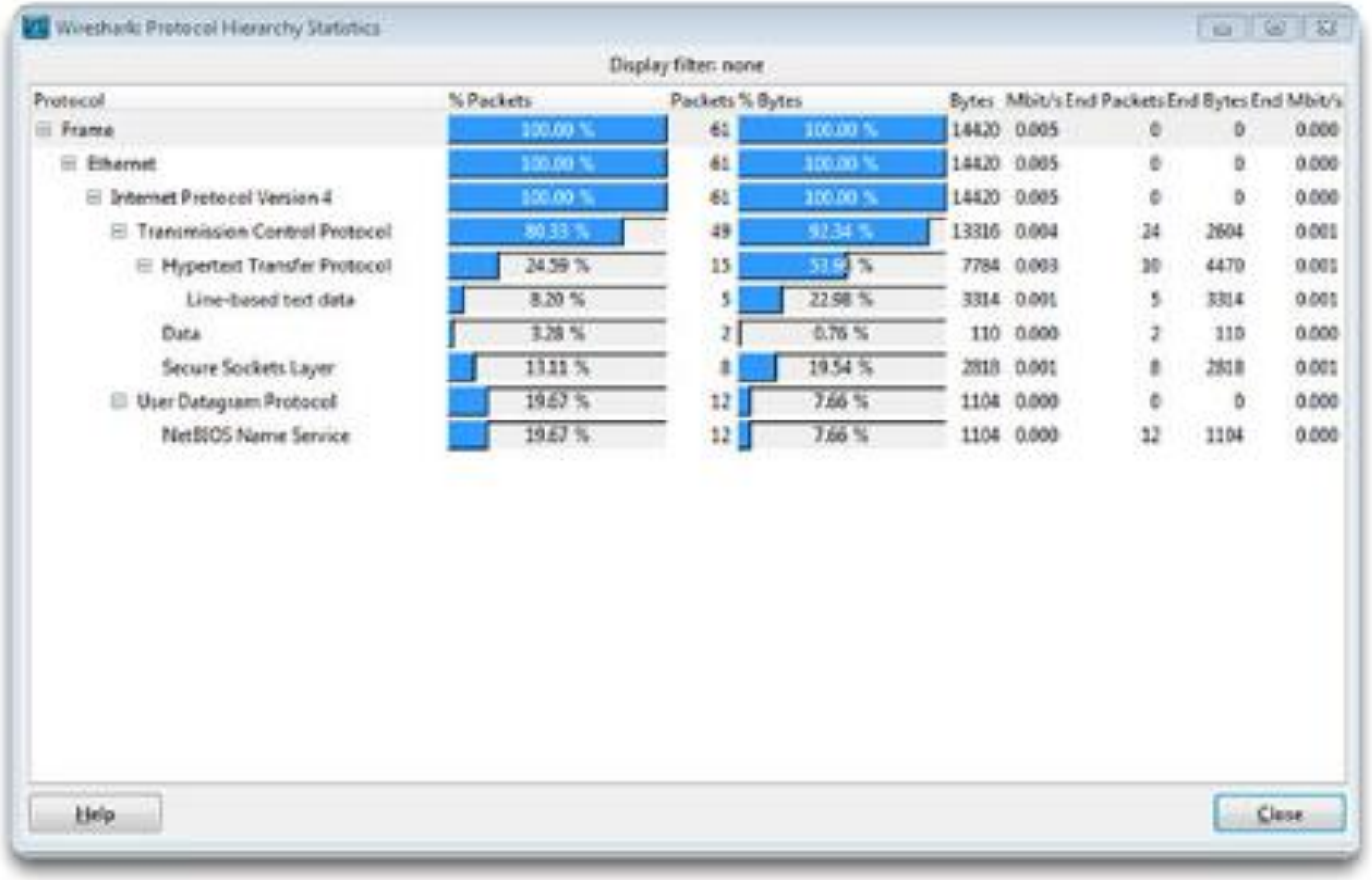
While a small company may not be able to justify the cost of an enterprise Cisco Telepresence solution, there are other real-time applications, as shown in Figure 1, that are affordable and justifiable for small business organizations.

11.1.3.1 Scaling a Small Network

To scale a network, several elements are required:

- Network documentation - physical and logical topology
- Device inventory - list of devices that use or comprise the network
- Budget - itemized IT budget, including fiscal year equipment purchasing budget
- Traffic analysis - protocols, applications, and services and their respective traffic requirements should be documented

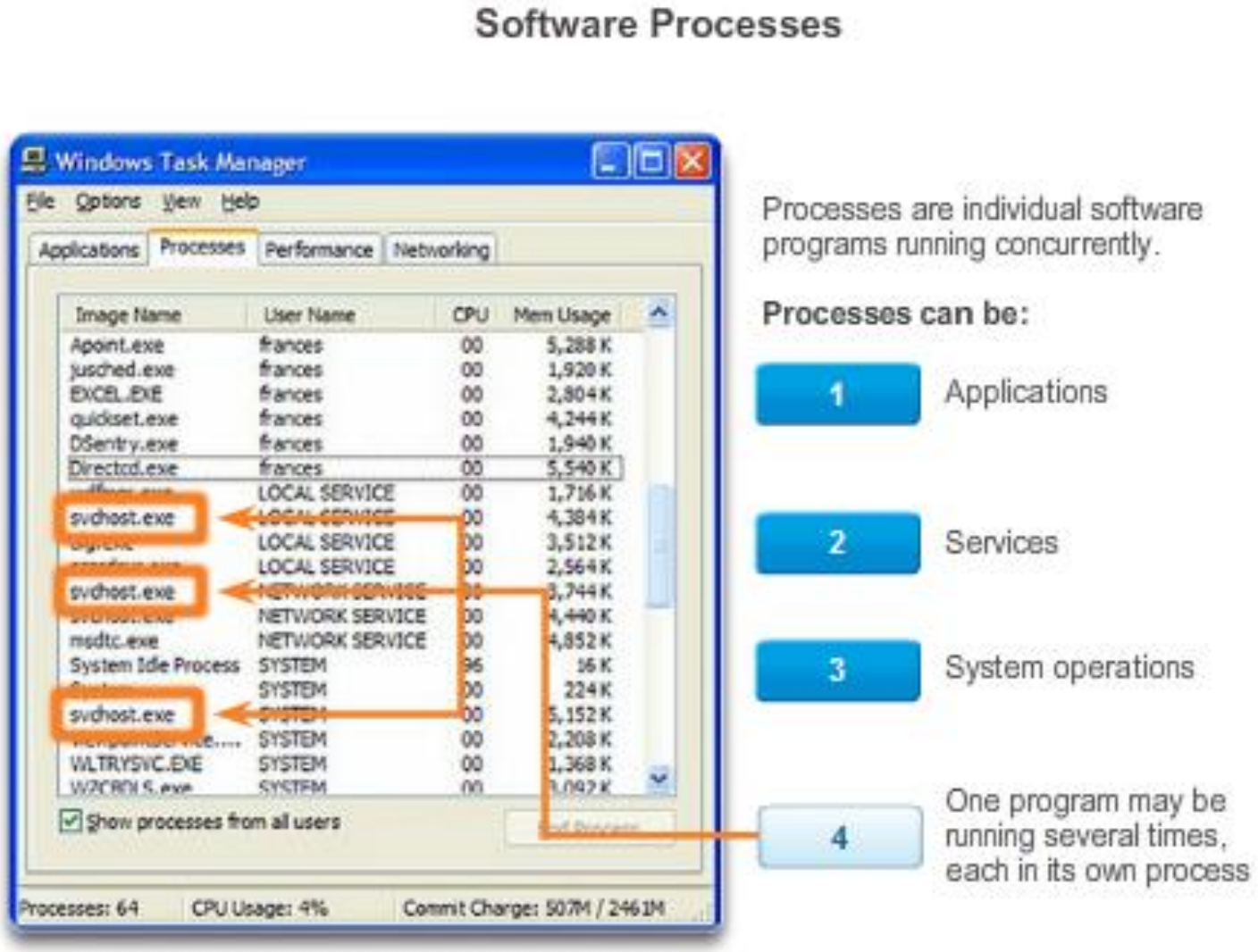
11.1.3.2 Protocol Analysis of a Small Network



Supporting and growing a small network requires being familiar with the protocols and network applications running over the network. While the network administrator will have more time in a small network environment to individually analyze network utilization for each network-enabled device, a more holistic approach with some type of software- or hardware-based protocol analyzer is recommended.

As shown in the figure, protocol analyzers enable a network professional to quickly compile statistical information about traffic flows on a network.

11.1.3.3 Evolving Protocol Requirements



Examples of processes running in the Windows operating system

A network administrator in a small network has the ability to obtain in-person IT "snapshots" of employee application utilization for a significant portion of the employee workforce over time. These snapshots typically include information such as:

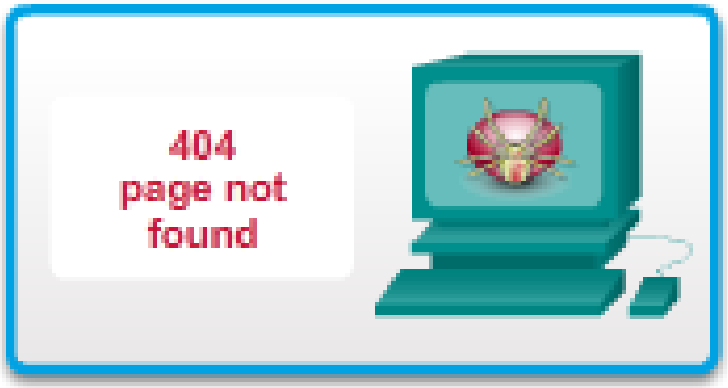
- OS + OS Version
- Non-Network Applications
- Network Applications
- CPU Utilization
- Drive Utilization
- RAM Utilization

11.2.1.1 Categories of Threats to Network Security

Information Theft

Data Loss and Manipulation

Identity Theft



Disruption of Service

After the hacker gains access to the network, four types of threats may arise:

- Information theft
- Identity theft
- Data loss/manipulation
- Disruption of service

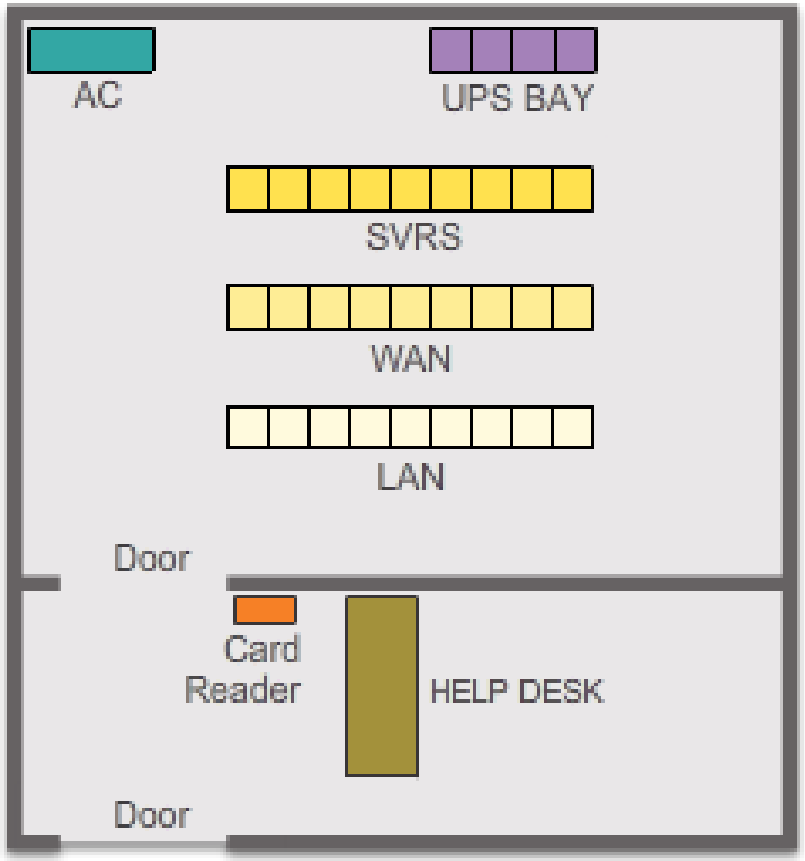
Click the images in the figure to see more information.

11.2.1.2 Physical Security

Physical Security Plan

Plan physical security to limit damage to the equipment:

- Lock up equipment and prevent unauthorized access from the doors, ceiling, raised floor, windows, ducts, and vents.
- Monitor and control closet entry with electronic logs.
- Use security cameras.



Secure computer room floor plan

The 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) or humidity extremes (too wet or too dry)
- Electrical threats - voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss
- Maintenance threats - poor handling of key electrical components (electrostatic discharge), lack of critical spare parts, poor cabling, and poor labeling

11.2.1.3 Types of Security Vulnerabilities

Vulnerabilities - Technology

Network security weaknesses:

TCP/IP protocol weakness
- Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Internet Control Message Protocol (ICMP) are inherently insecure.
- Simple Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP) are related to the inherently insecure structure upon which TCP was designed.

Operating system weakness
- Each operating system has security problems that must be addressed.
- UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8
- They are documented in the Computer Emergency Response Team (CERT) archives at http://www.cert.org.

Network equipment weakness

Various types of network equipment, such as routers, firewalls, and switches have security weaknesses that must be recognized and protected against. Their weaknesses include password protection, lack of authentication, routing protocols, and firewall holes.

Threats are realized by a variety of tools, scripts, and programs to launch attacks against networks and network devices. Typically, the network devices under attack are the endpoints, such as servers and desktop computers.

There are three primary vulnerabilities or weaknesses:

- Technological, as shown in Figure 1
- Configuration, as shown in Figure 2
- Security policy, as shown in Figure 3

11.2.1.3 Types of Security Vulnerabilities

Vulnerabilities - Configuration

Configuration Weakness	How the weakness is exploited
Unsecured user accounts	User account information may be transmitted insecurely across the network, exposing usernames and passwords to snoopers.
System accounts with easily guessed passwords	This common problem is the result of poorly selected and easily guessed user passwords.
Misconfigured Internet services	A common problem is to turn on JavaScript in Web browsers, enabling attacks by way of hostile JavaScript when accessing untrusted sites. IIS, FTP, and Terminal Services also pose problems.
Unsecured default settings within products	Many products have default settings that enable security holes.
Misconfigured network equipment	Misconfigurations of the equipment itself can cause significant security problems. For example, misconfigured access lists, routing protocols, or SNMP community strings can open up large security holes.

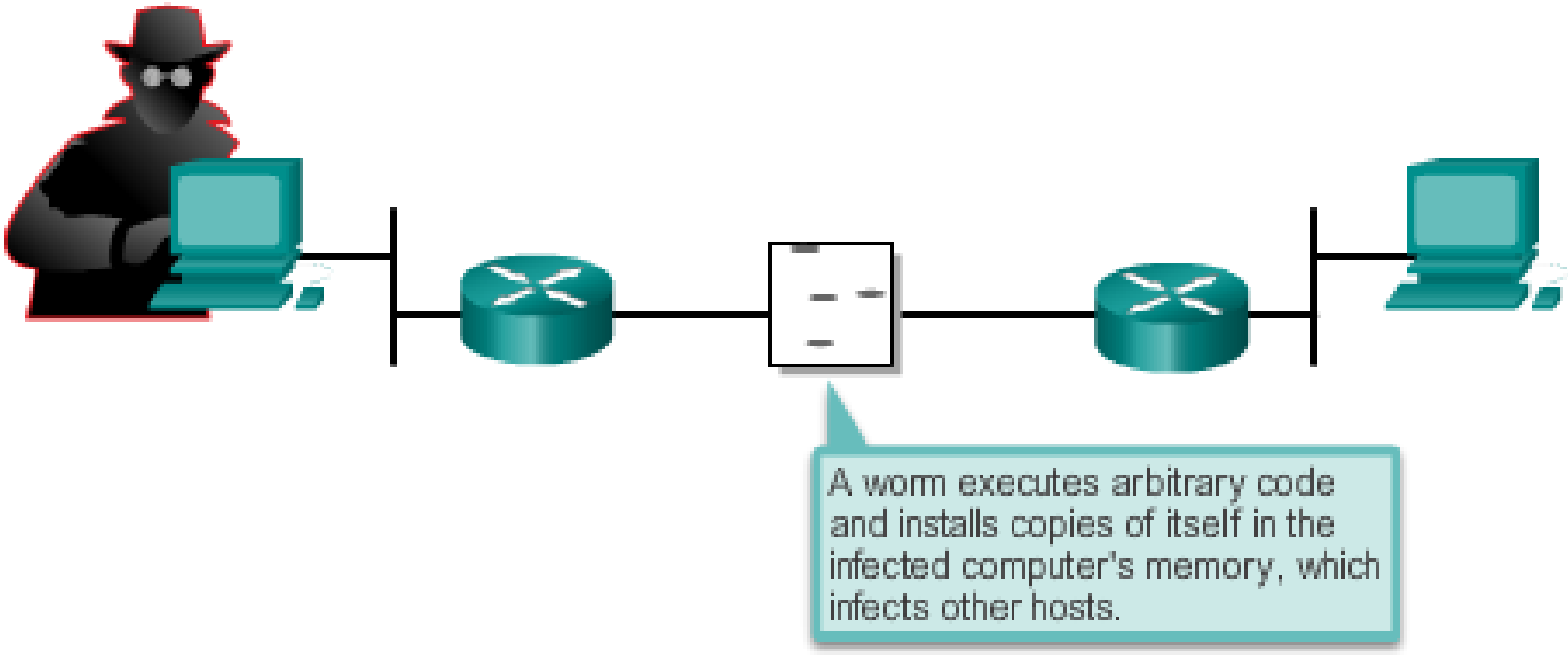
11.2.1.3 Types of Security Vulnerabilities

Vulnerabilities - Policy

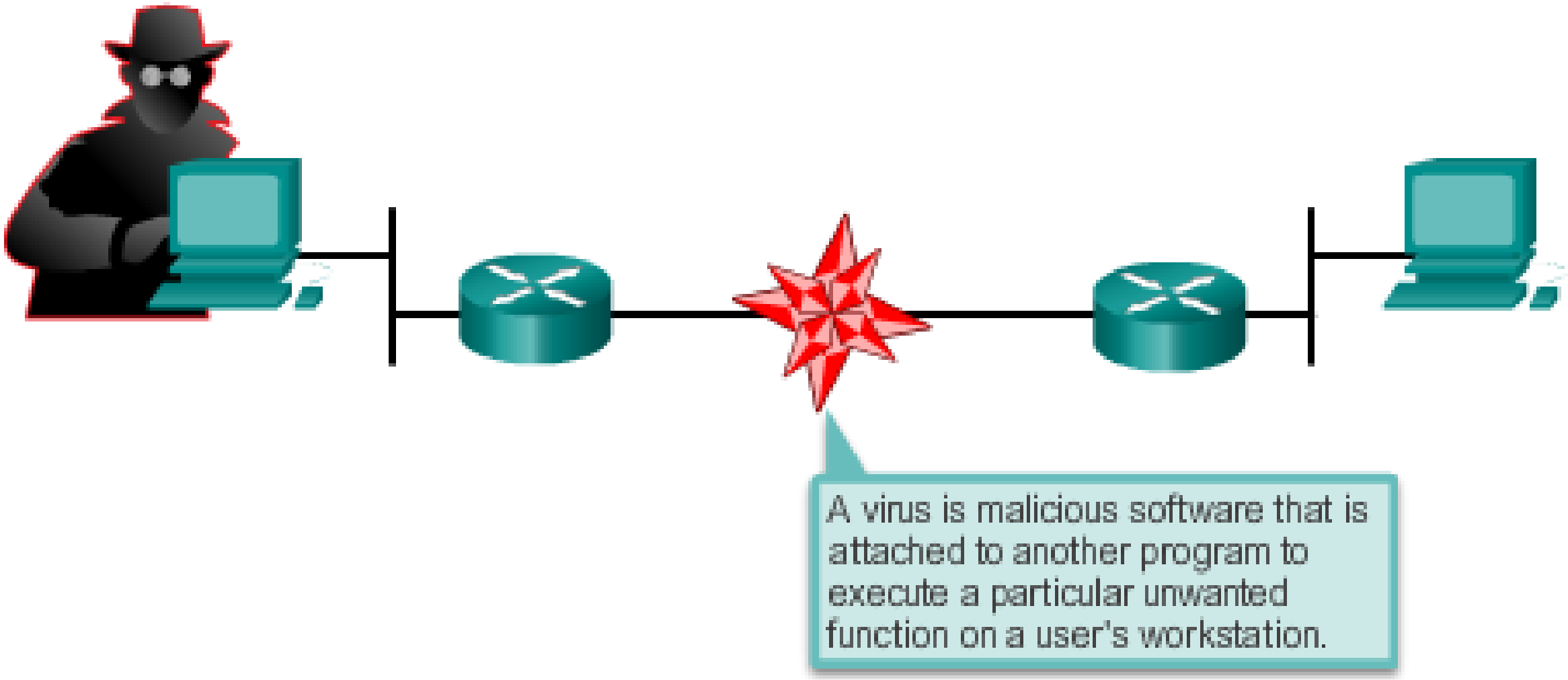
Policy Weakness	How the weakness is exploited
Lack of written security policy	An unwritten policy cannot be consistently applied or enforced.
Politics	Political battles and turf wars can make it difficult to implement a consistent security policy.
Lack of authentication continuity	Poorly chosen, easily cracked, or default passwords can allow unauthorized access to the network.
Logical access controls not applied	Inadequate monitoring and auditing allow attacks and unauthorized use to continue, wasting company resources. This could result in legal action or termination against IT technicians, IT management, or even company leadership that allows these unsafe conditions to persist.
Software and hardware installation and changes do not follow policy	Unauthorized changes to the network topology or installation of unapproved applications create security holes.
Disaster recovery plan is nonexistent	The lack of a disaster recovery plan allows chaos, panic, and confusion to occur when someone attacks the enterprise.

11.2.1.4 Activity – Security Threats and Vulnerabilities

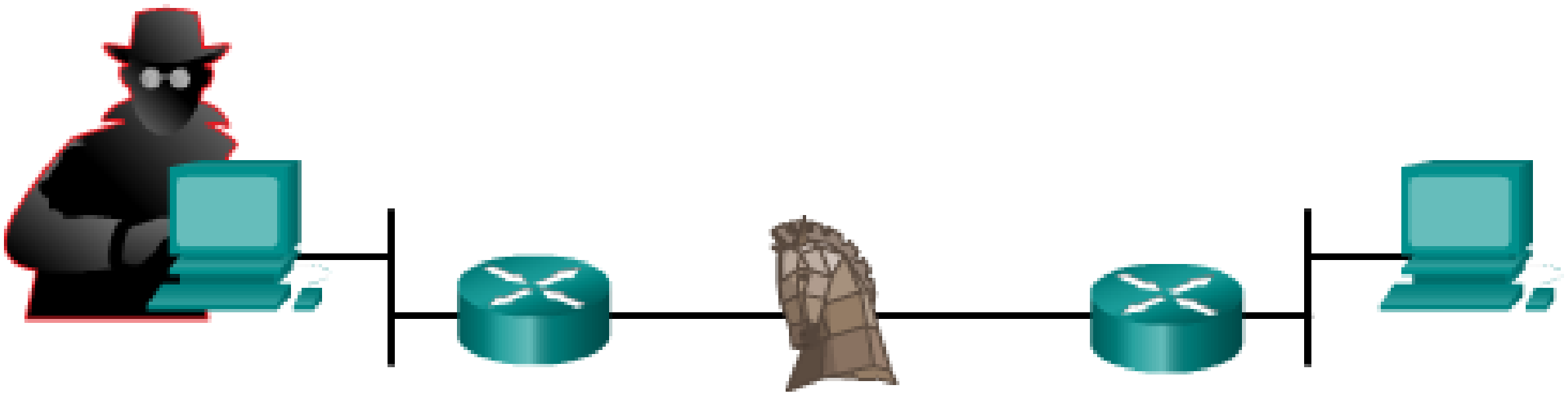
11.2.2.1 Viruses, Worms, and Trojan Horses



11.2.2.1 Viruses, Worms, and Trojan Horses

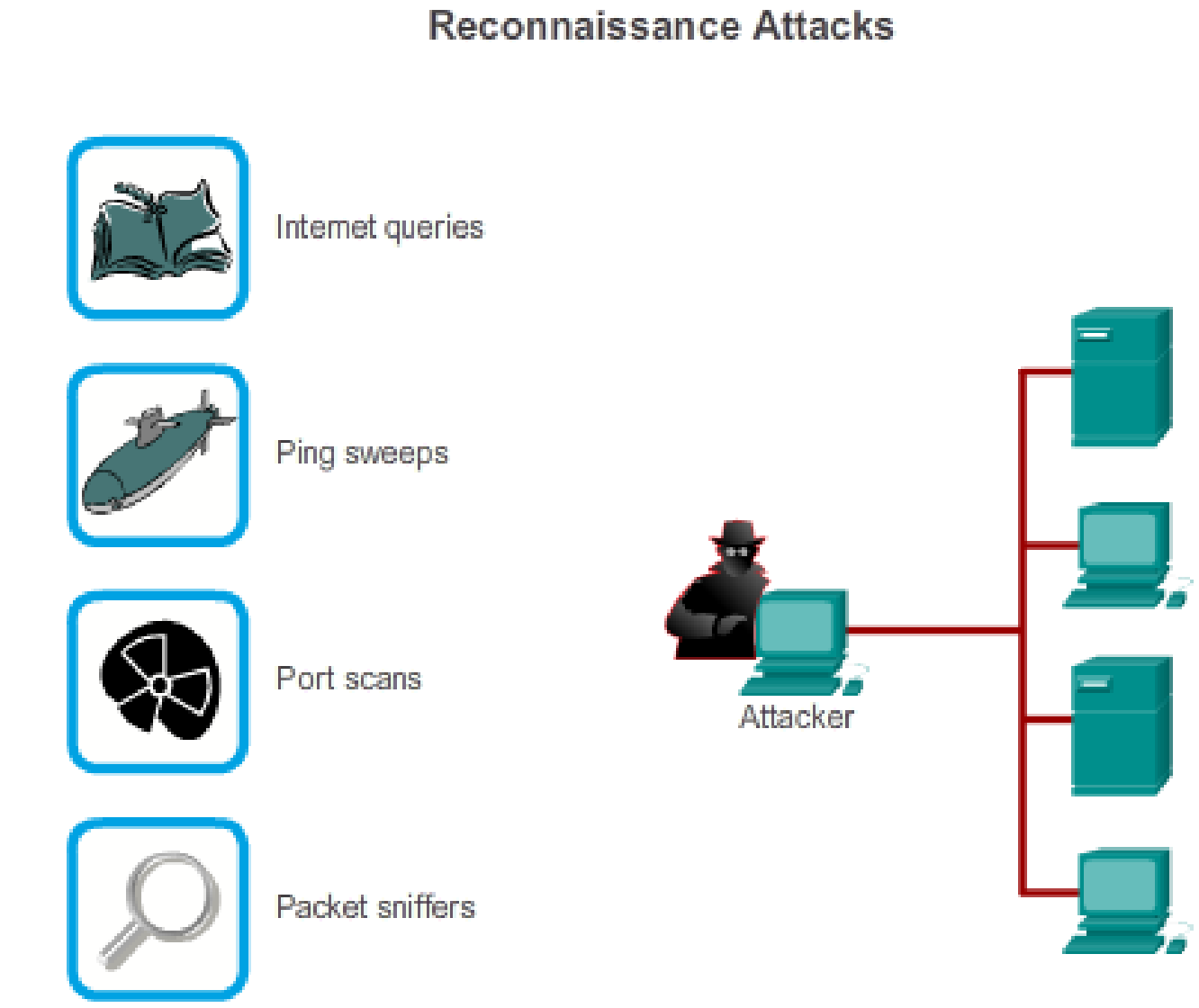


11.2.2.1 Viruses, Worms, and Trojan Horses



A Trojan horse is different only in that the entire application was written to look like something else, when, in fact, it is an attack tool.

11.2.2.2 Reconnaissance Attacks



In addition to malicious code attacks, it is also possible for networks to fall prey to various network attacks. Network attacks can be classified into three major categories:

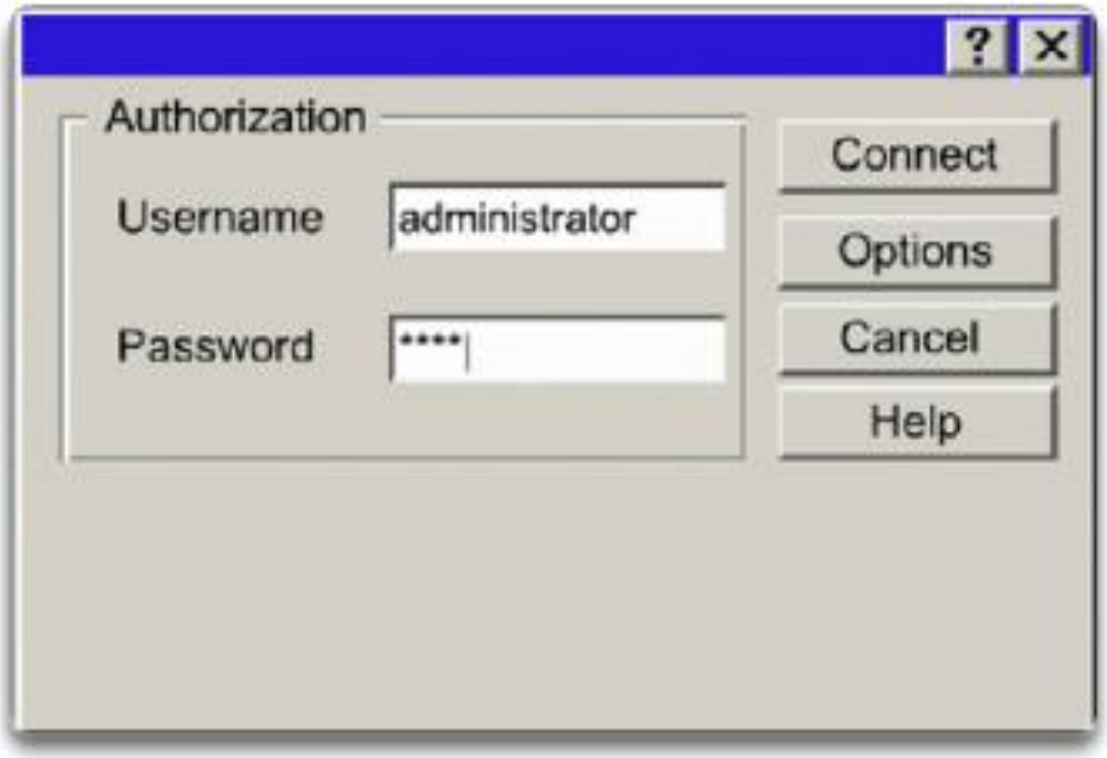
- Reconnaissance attacks - the unauthorized discovery and mapping of systems, services, or vulnerabilities
- Access attacks - the unauthorized manipulation of data, system access, or user privileges
- Denial of service - the disabling or corruption of networks, systems, or services

11.2.2.3 Access Attacks

Password Attack

Attackers can implement password attacks using several different methods:

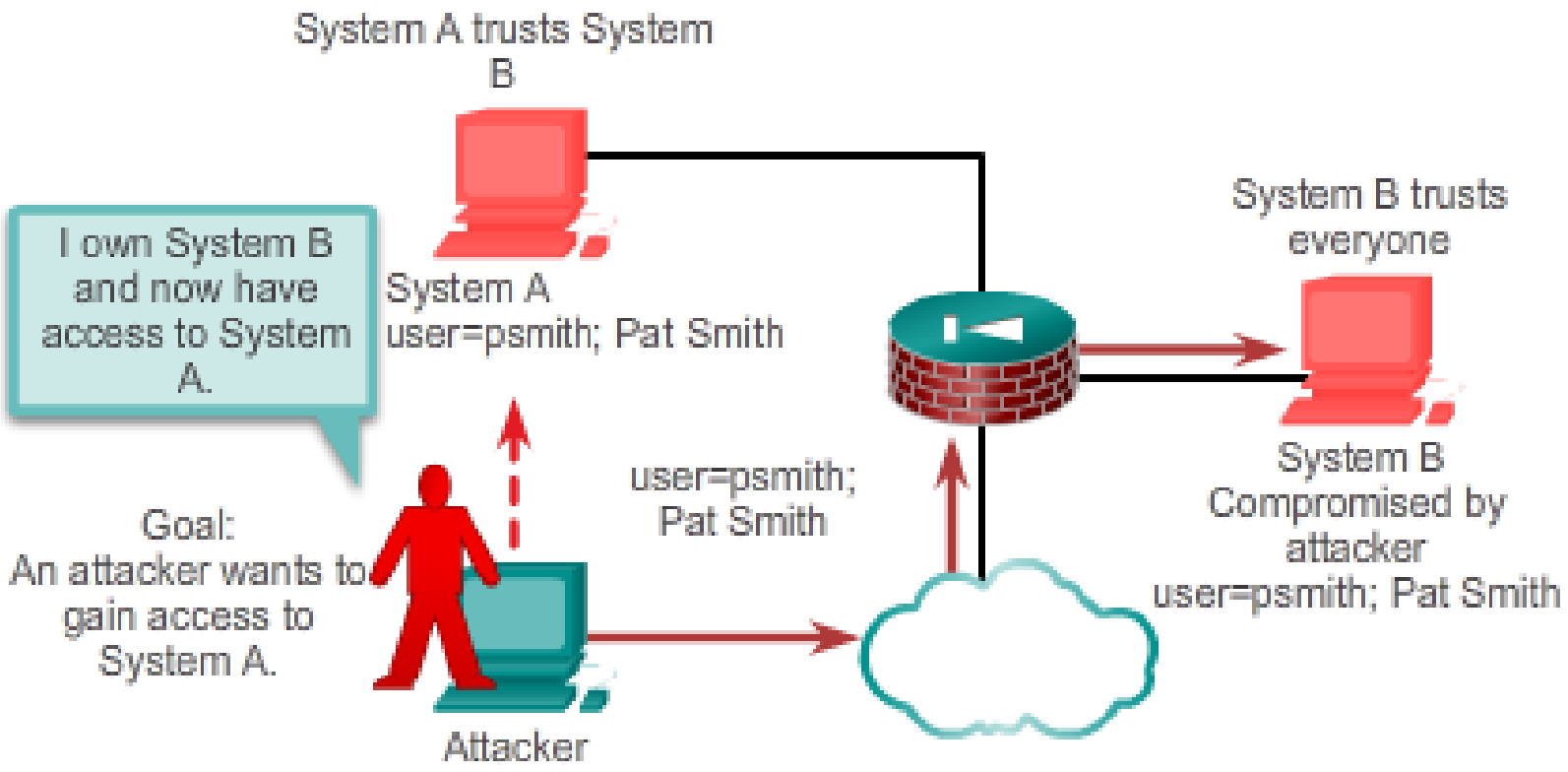
- Brute-force attacks
- Trojan horse programs
- Packet sniffers



11.2.2.3 Access Attacks

Trust Exploitation

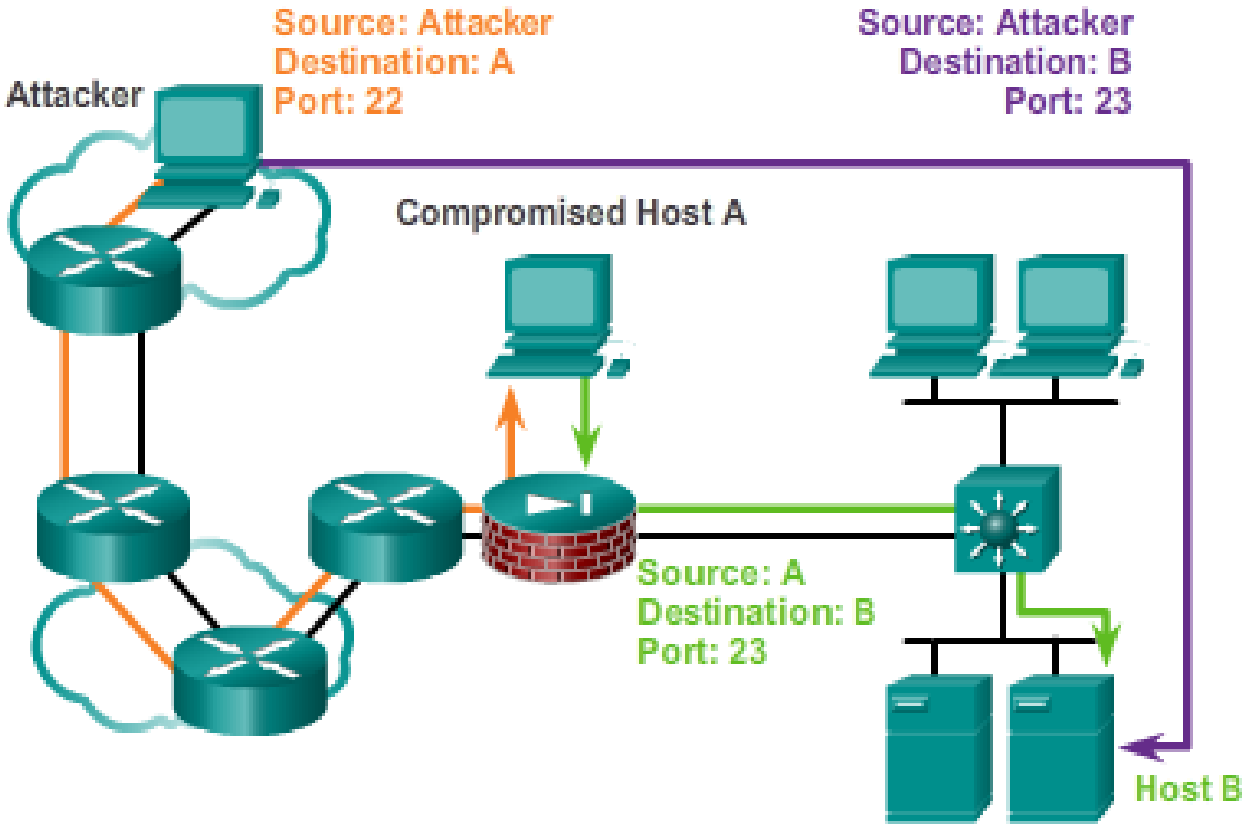
Network OS	Trust Models
Windows	Domains Active Directory (AD)
Linux and UNIX	Network File System (NFS) Network Information Service Plus (NIS+)



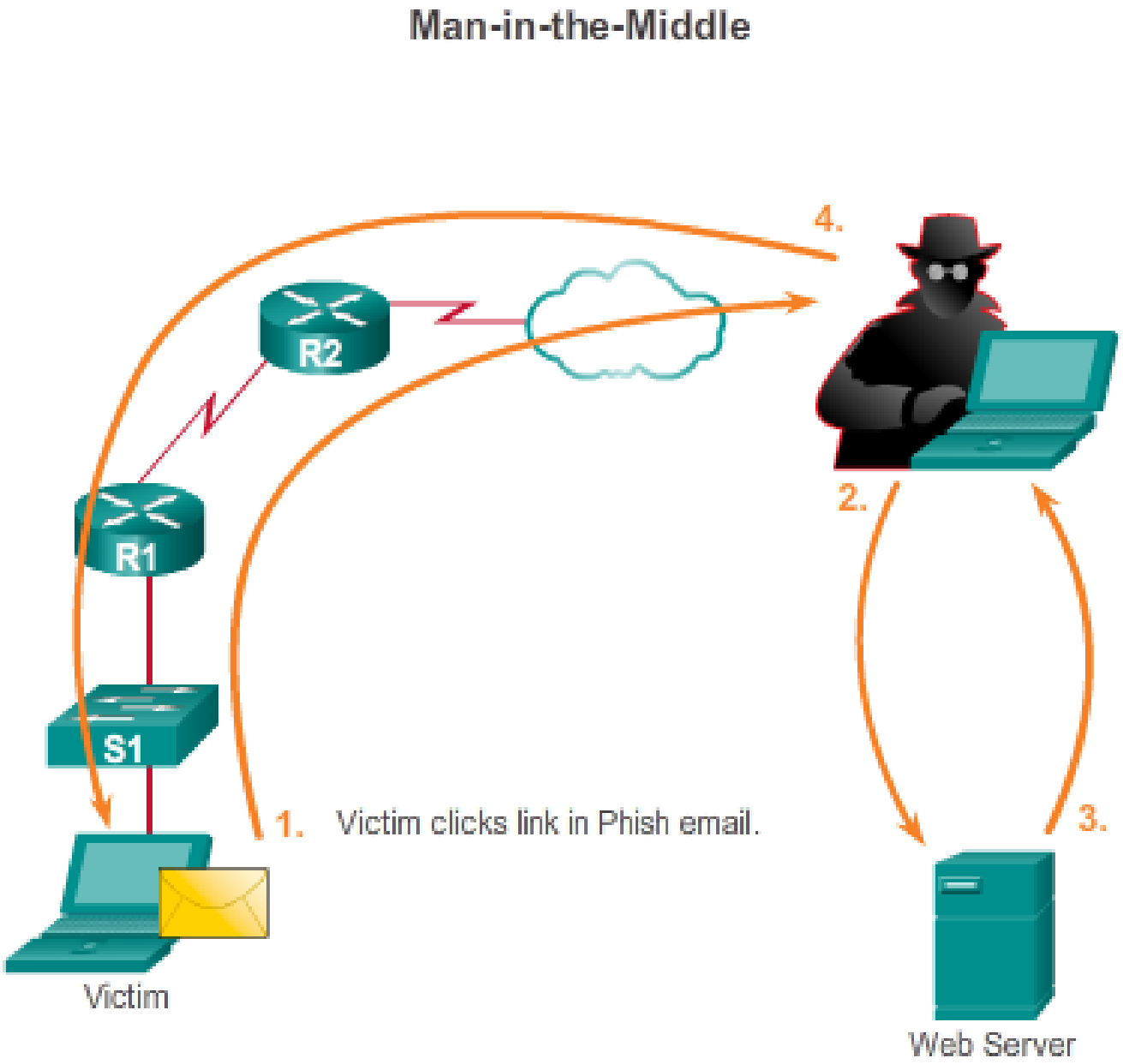
11.2.2.3 Access Attacks

Port Redirection

Port redirection is a type of trust-exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped. It is mitigated primarily through the use of proper trust models. Antivirus software and host-based IDS can help detect and prevent an attacker installing port redirecting utilities on the host.



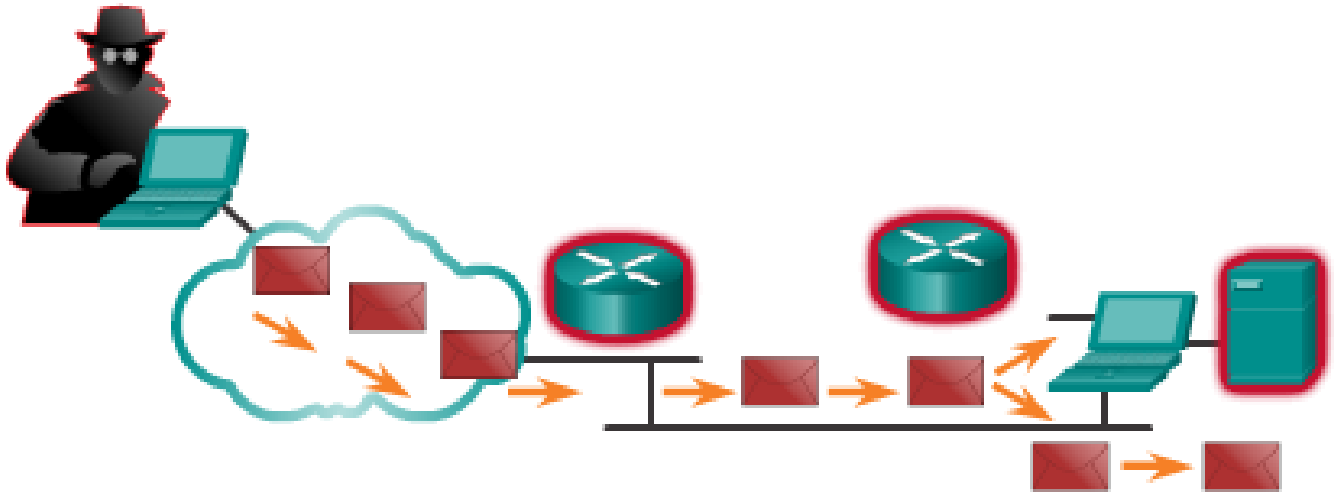
11.2.2.3 Access Attacks



11.2.2.4 DoS Attacks

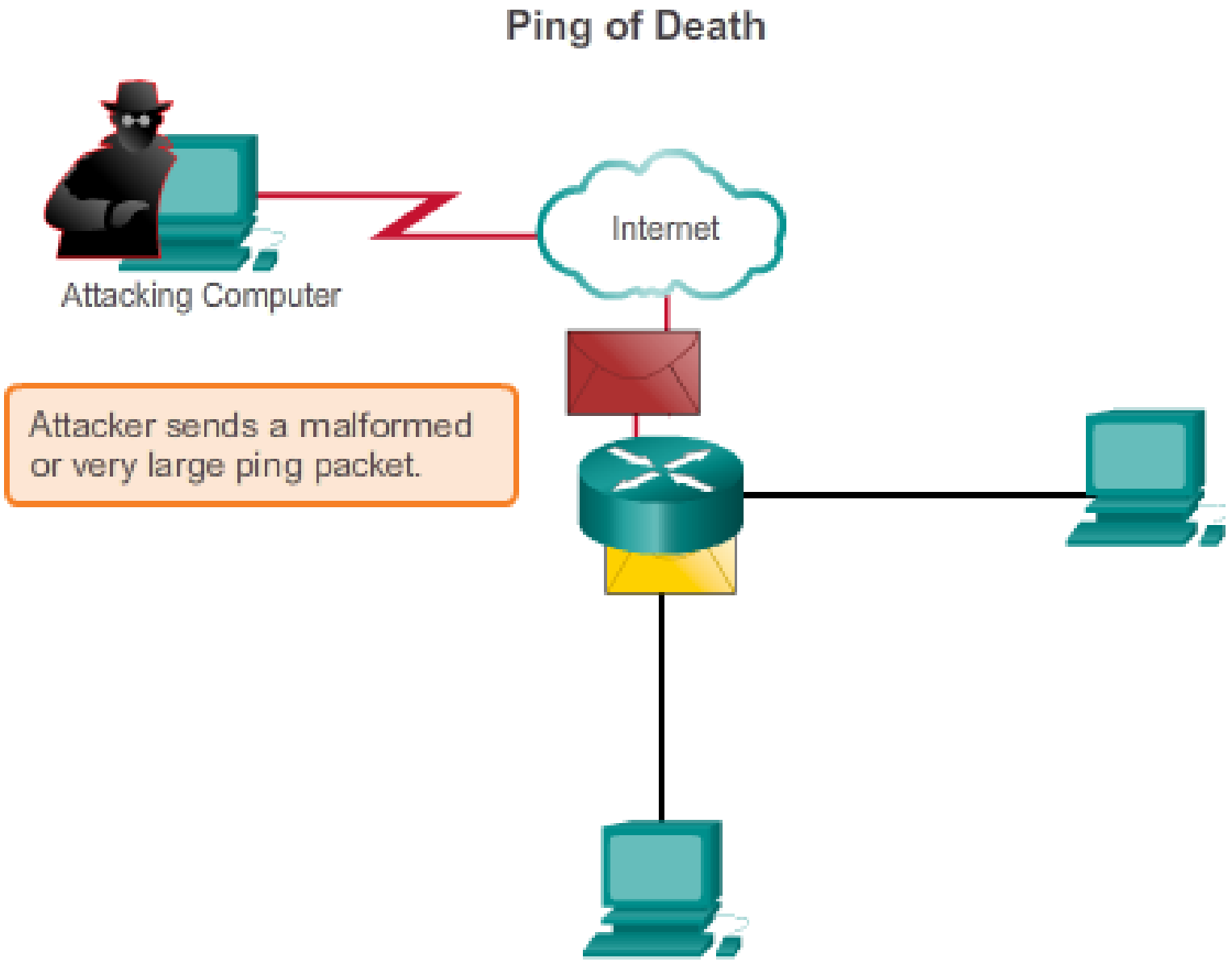
DoS Attack

Resource overloads	Malformed data
Disk space, bandwidth, buffers	Oversized packets such as ping of death
Ping floods such as smurf	Overlapping packet such as winuke
Packet storms such as UDP bombs and fraggle	Unhandled data such as teardrop

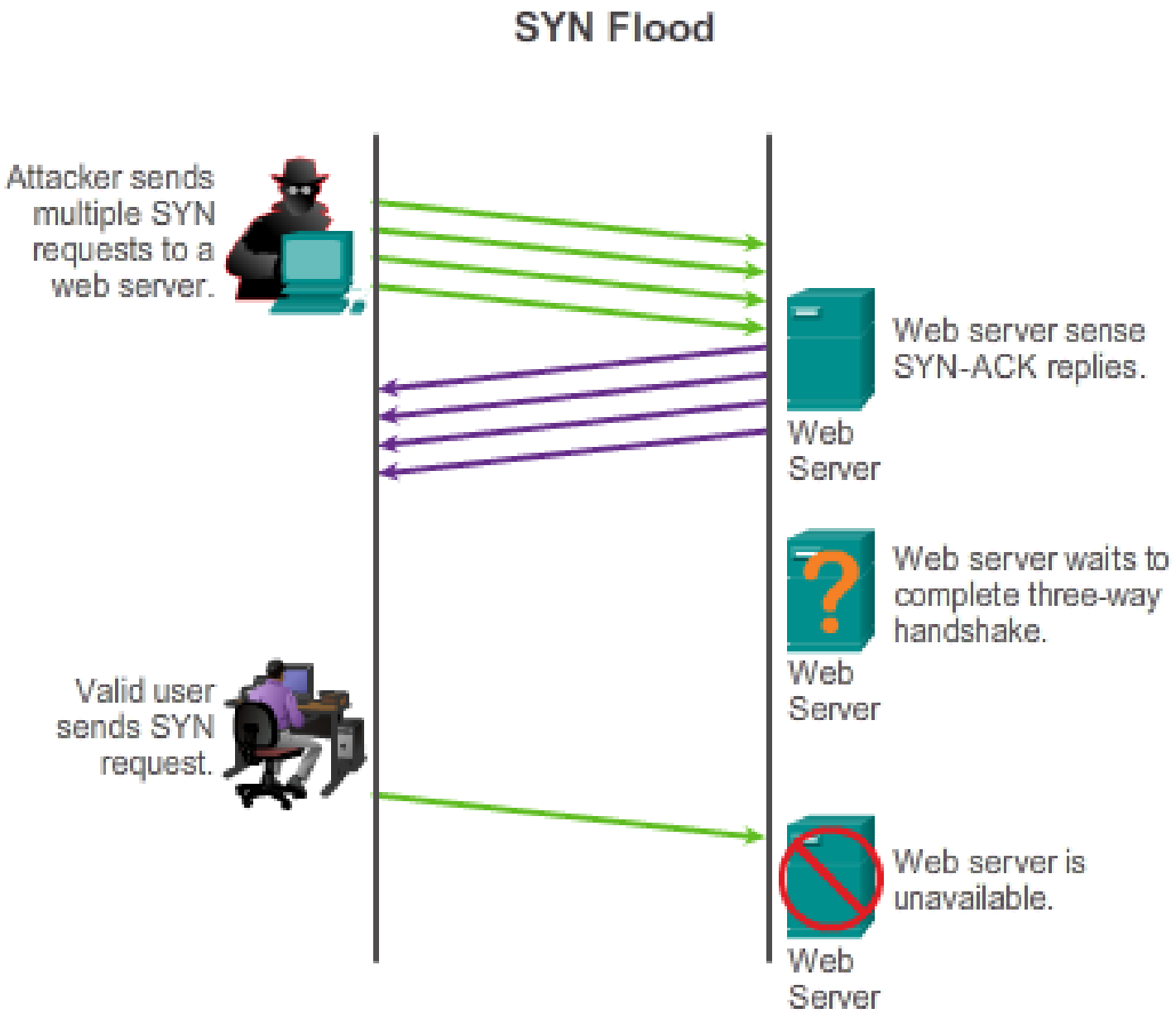


DoS attacks prevent authorized people from using a service by using up system resources.

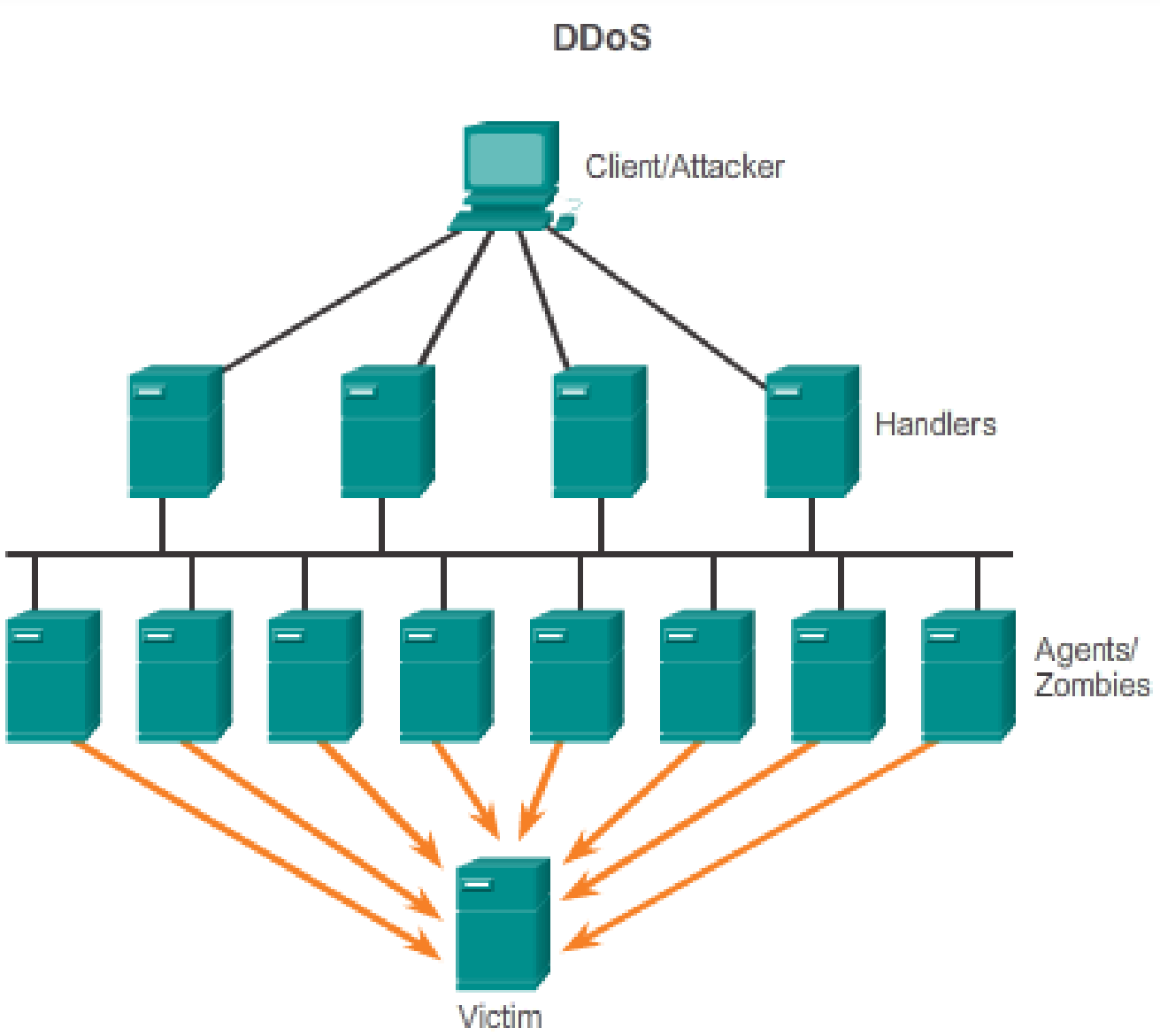
11.2.2.4 DoS Attacks



11.2.2.4 DoS Attacks

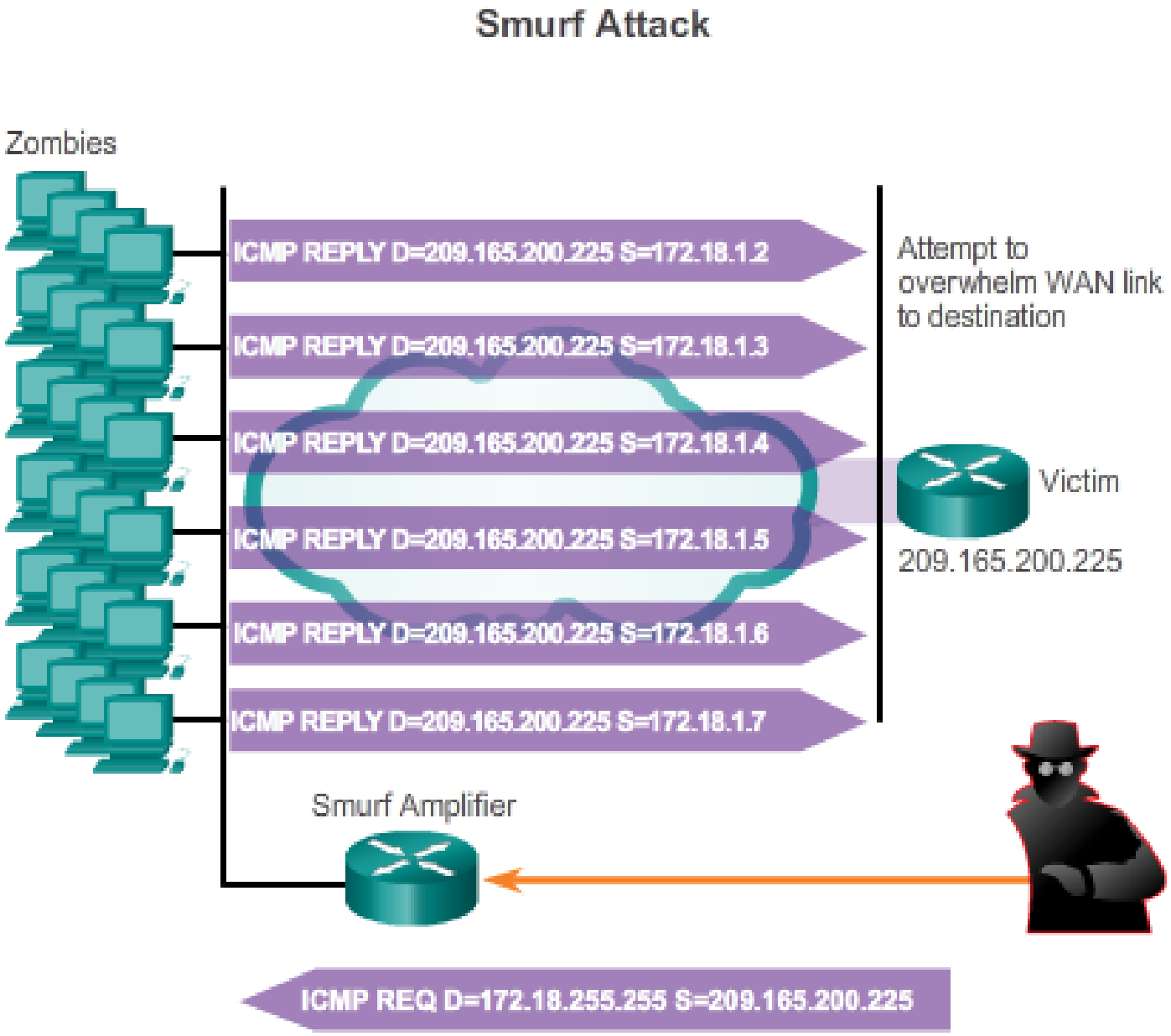


11.2.2.4 DoS Attacks

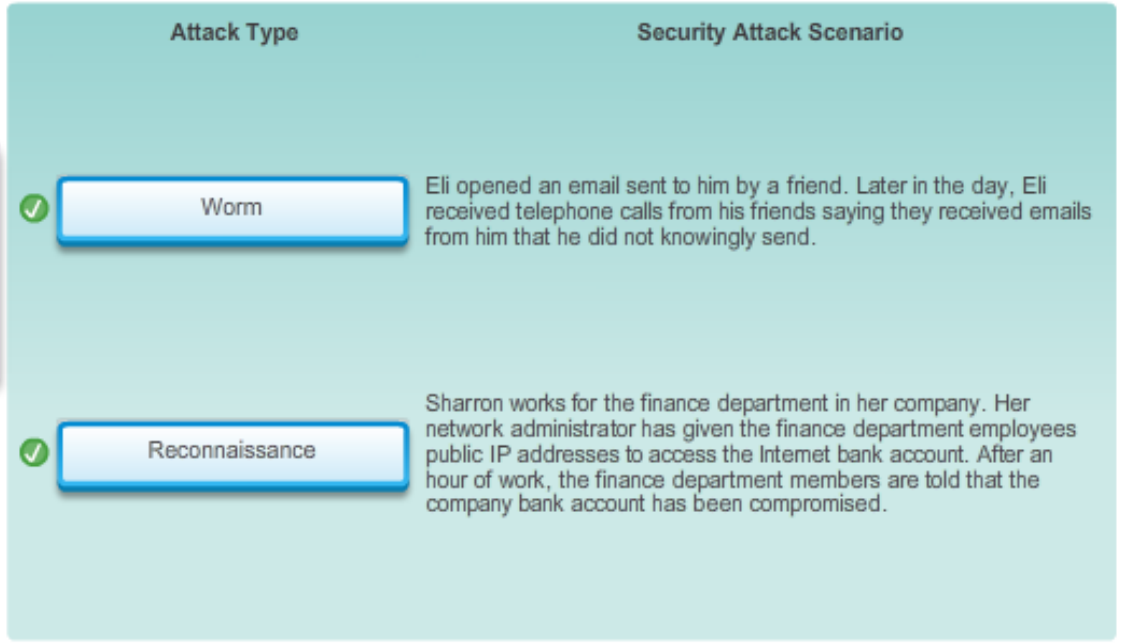


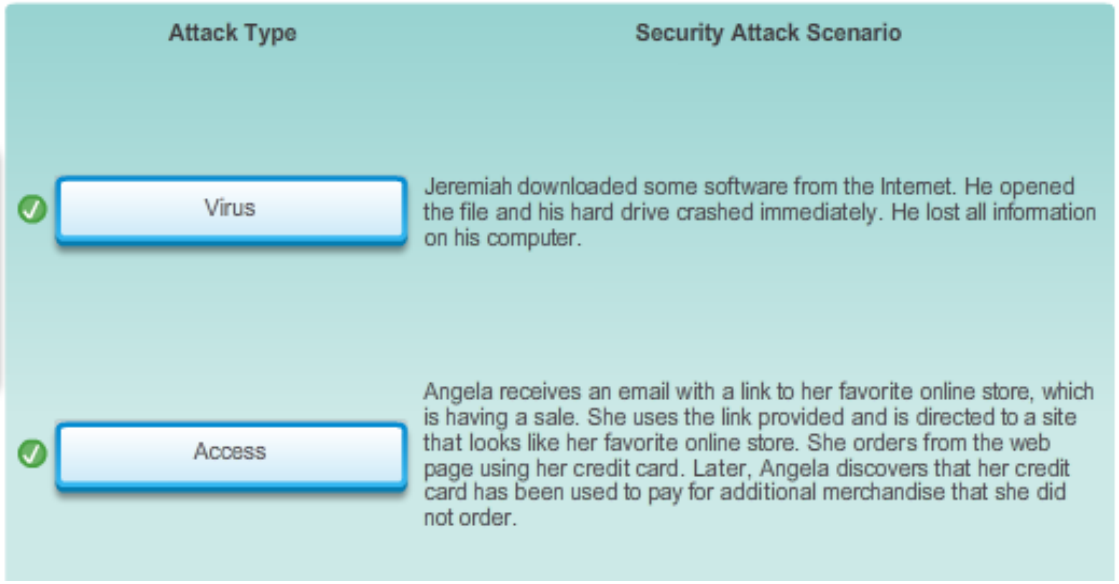
Attacker uses many intermediate hosts, called zombies, to launch the attack.

11.2.2.4 DoS Attacks



11.2.2.5 Activity – Types of Attack





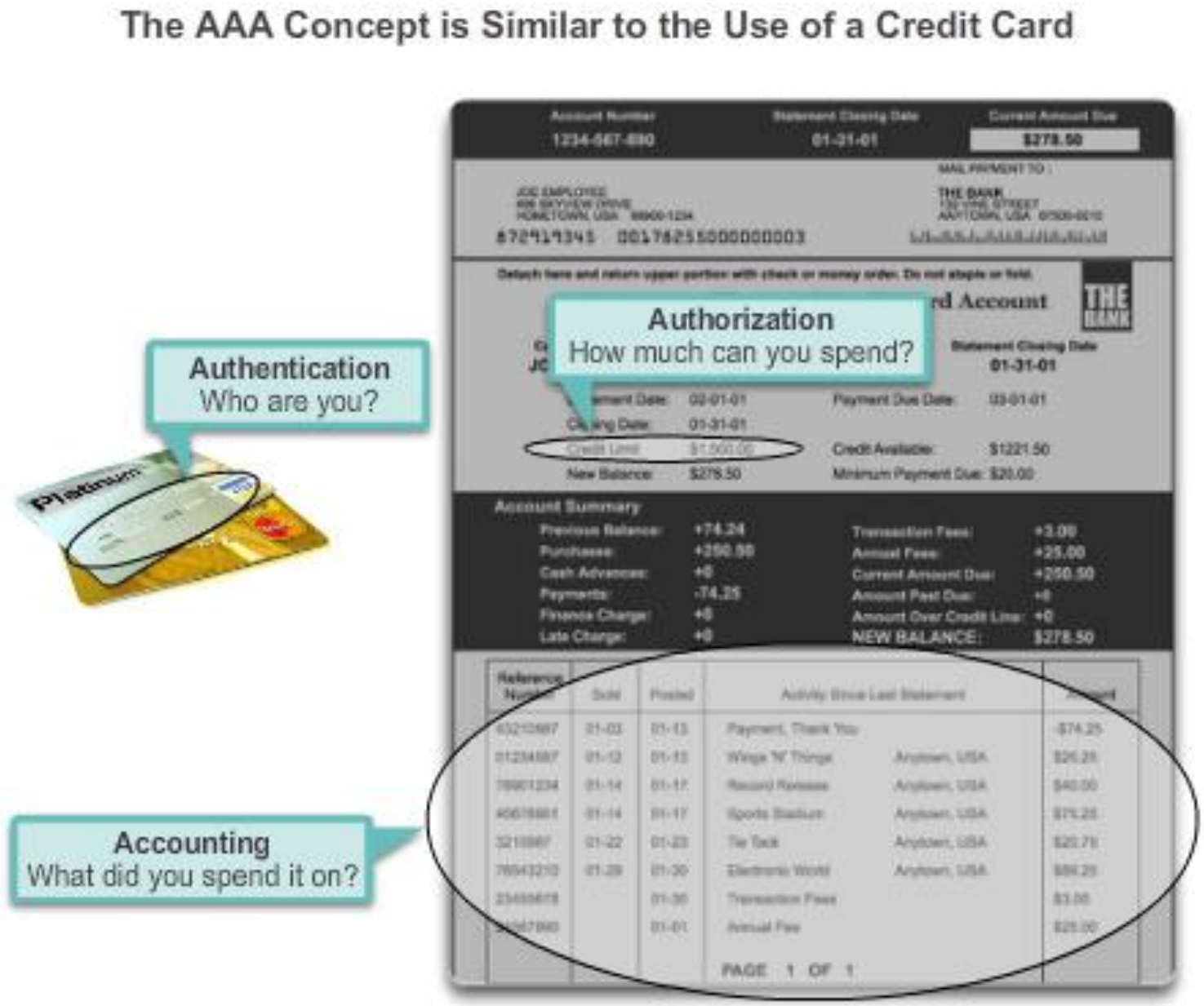
11.2.2.6 Lab - Researching Network Security Threats

11.2.3.1 Backup, Upgrade, Update, and Patch

Worm attack mitigation requires diligence on the part of system and network administration staff. The following are the recommended steps for worm attack mitigation:

- **Containment** - Contain the spread of the worm within the network. Compartmentalize uninfected parts of the network.
- **Inoculation** - Start patching all systems and, if possible, scanning for vulnerable systems.
- **Quarantine** - Track down each infected machine inside the network. Disconnect, remove, or block infected machines from the network.
- **Treatment** - Clean and patch each infected system. Some worms may require complete core system reinstallations to clean the system

11.2.3.2 Authentication, Authorization, and Accounting



For larger networks, a more scalable solution is external authentication. External authentication allows all users to be authenticated through an external network server. The two most popular options for external authentication of users are RADIUS and TACACS+:

- **RADIUS** is an open standard with low use of CPU resources and memory. It is used by a range of network devices, such as switches, routers, and wireless devices.
- **TACACS+** is a security mechanism that enables modular authentication, authorization, and accounting services. It uses a TACACS+ daemon running on a security server.

Thanks for your attention!!