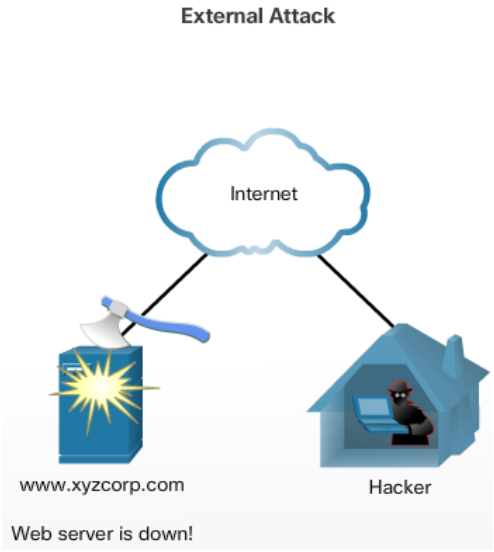
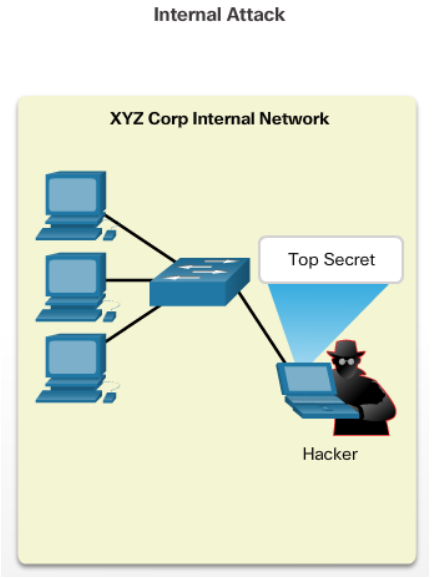
Am I at Risk?

LESSON 4: Basic Network security- Hackers and Intruders

- What Do They Want?
- When the hacker gains access to the network, four types of threat may arise: Information theft, Identity theft, Data loss / manipulation, and Disruption of service



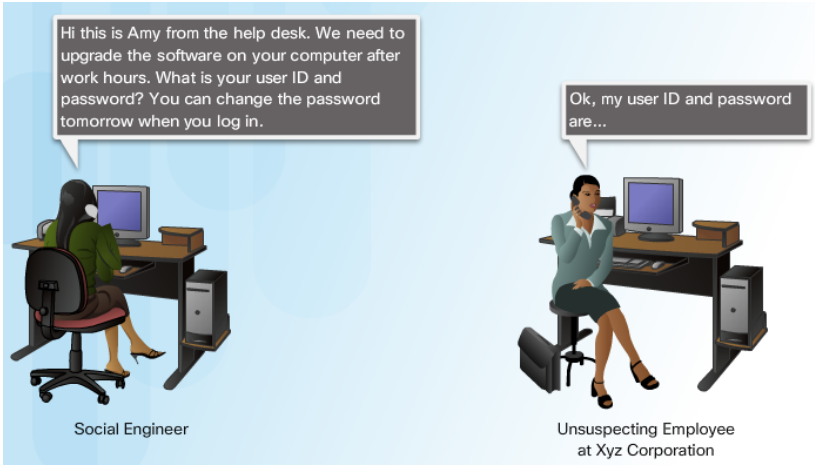
- Where Do They Come From?
- External threats arise from individuals working outside of an organization.
- Internal threats occur when someone has authorized access to the network through a user account or has physical access to the network equipment.



Am I at Risk?

Social Engineering Attacks

- Social Engineering
  - In the context of computer and network security, social engineering refers to a collection of techniques used to deceive internal users into performing specific actions or revealing confidential information.

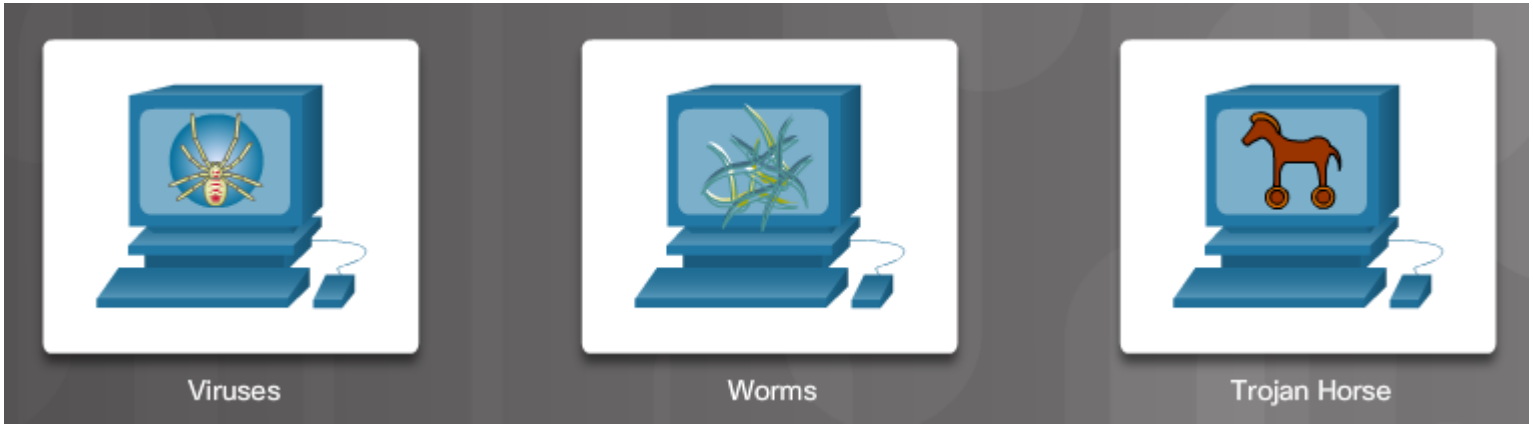


- Types of Social Engineering
- Three of the most common methods hackers use to obtain information directly from authorized users go by unusual names: pretexting, phishing, and vishing.

Am I at Risk?

Virus, Worms, and Trojan Horses

- Other Types of Attacks
  - Malicious software can damage a system, destroy data, as well as deny access to networks, systems, or services. They can also forward data and personal details from unsuspecting PC users to criminals.



A virus is a program that spreads by modifying other programs or files.

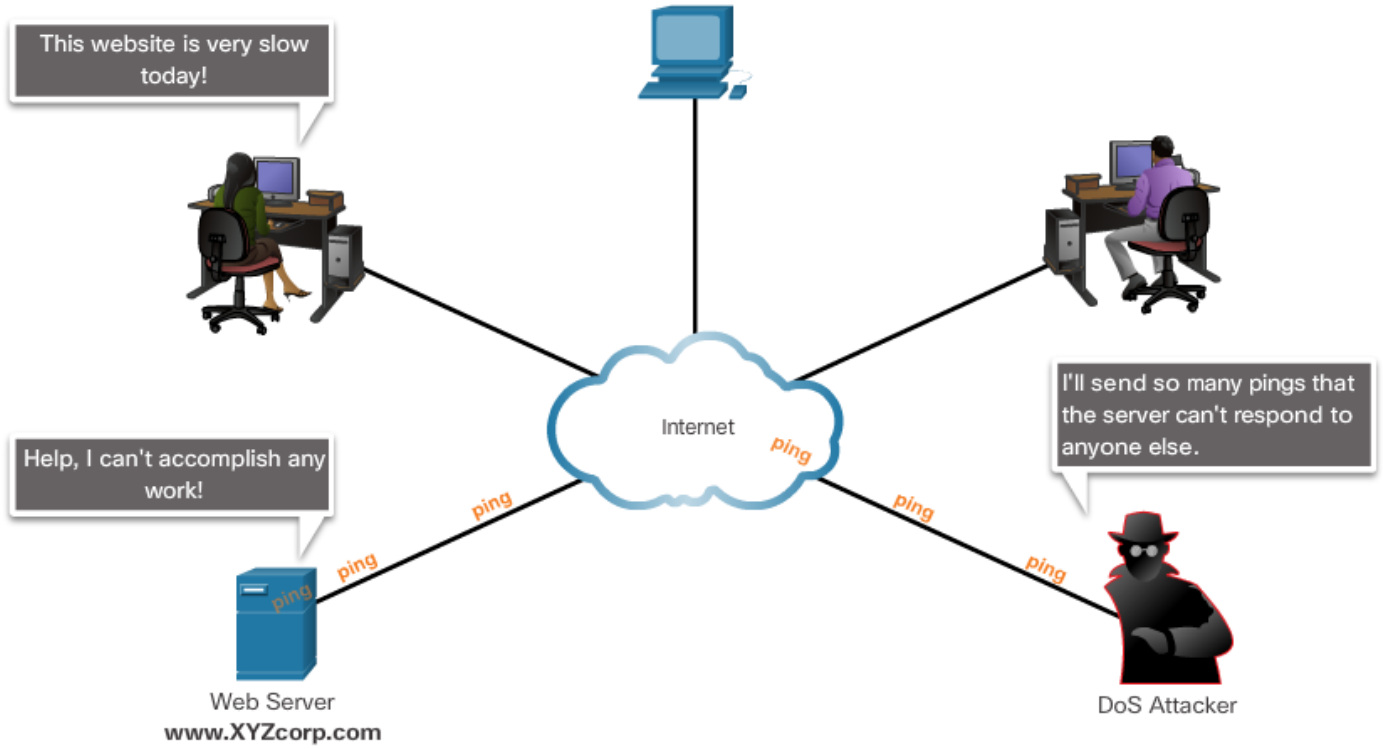
A worm is similar to a virus, but unlike a virus does not need to attach itself to an existing program.

A Trojan horse is program that is written to appear like a legitimate program, when in fact it is an attack tool.

Methods of Attack

Denial of Service and Brute Force Attacks

- An attacker uses a DoS attack to perform these functions:
  - Flood a system or network with traffic to prevent legitimate network traffic from flowing
  - Disrupt connections between a client and server to prevent access to a service



Methods of Attack

Denial of Service and Brute Force Attacks (Cont.)

- DDoS
  - DDoS is a more sophisticated and potentially damaging form of the DoS attack. It is designed to saturate and overwhelm network links with useless data.

- Brute Force
  - With brute force attacks, a fast computer is used to try to guess passwords or to decipher an encryption code. The attacker tries a large number of possibilities in rapid succession to gain access or crack the code.

Methods of Attack

Other Types of Malware

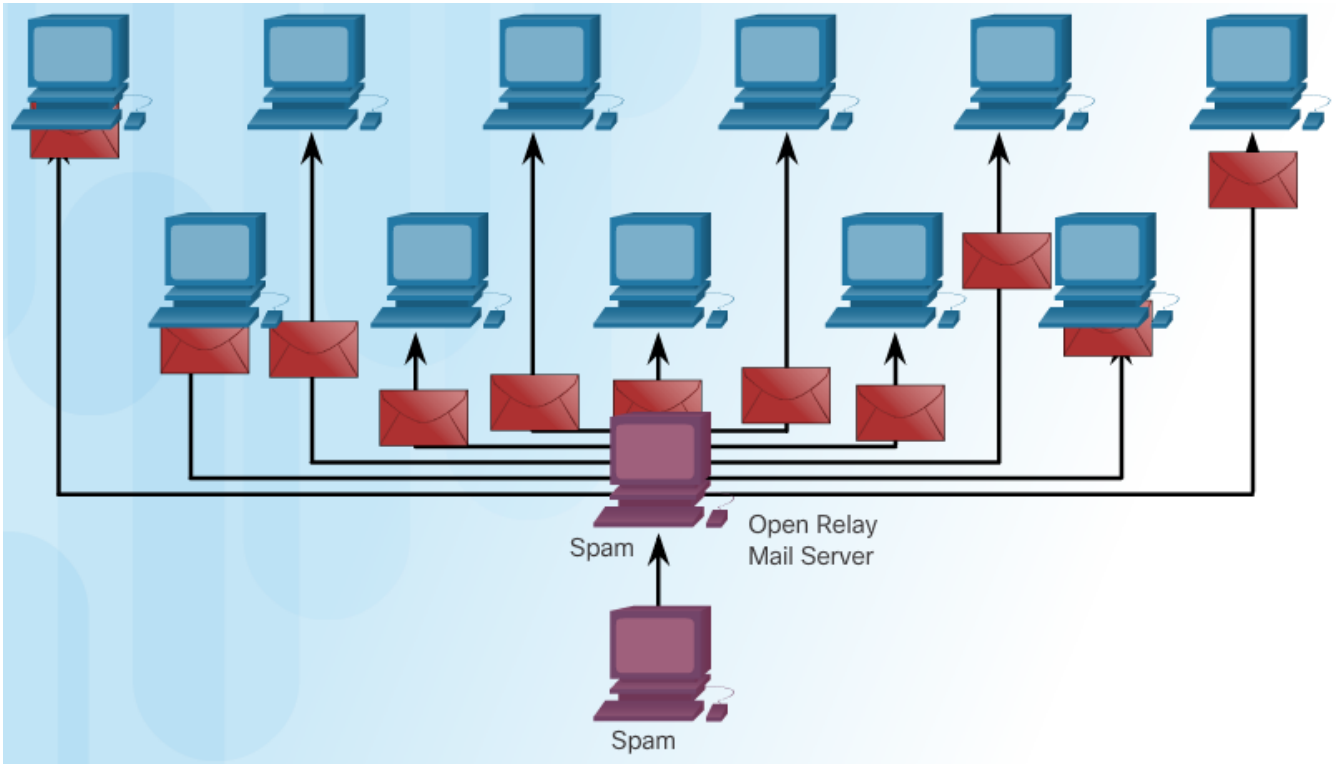
- Spyware
  - Spyware is any program that gathers personal information from your computer without your permission or knowledge. This information is sent to advertisers or others on the Internet and can include passwords and account numbers.

- Adware
  - Adware is a form of spyware used to collect information about a user based on websites the user visits. That information is then used for targeted advertising.

Methods of Attack

Other Types of Malware (Cont.)

- Botnets and Zombies
  - When infected, the “zombie” computer contacts servers managed by the botnet creator. These servers act as a command and control (C&C) center for an entire network of compromised devices, or "botnet."



How Can I Protect My Network?

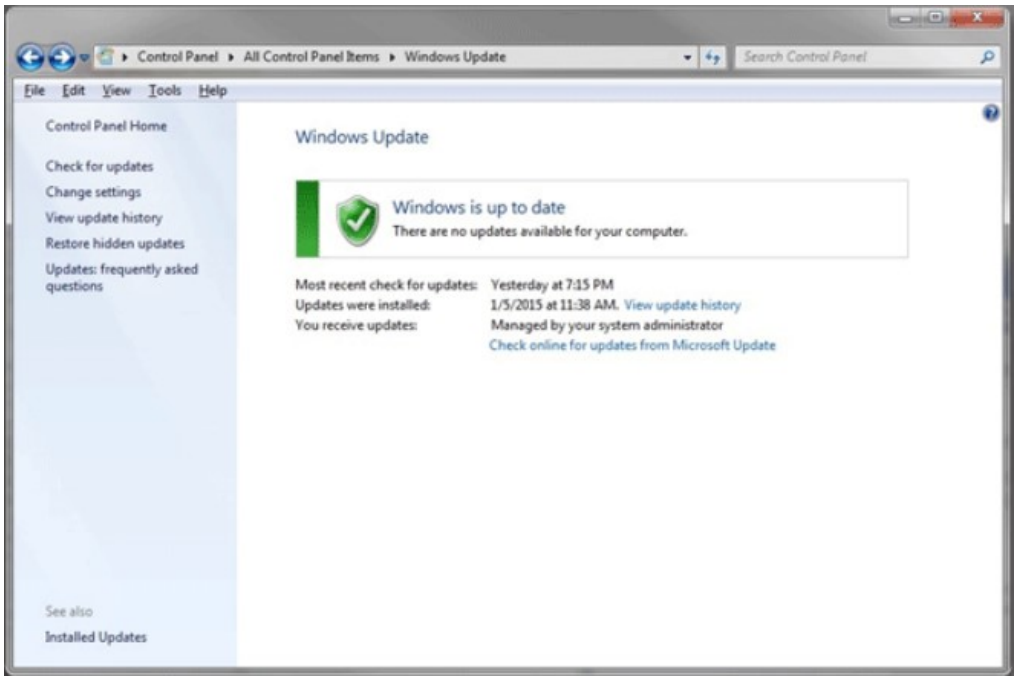
Security Tools

- Security Practices
  - Security procedures can range from simple, inexpensive tasks such as maintaining up-to-date software releases, to complex implementations of firewalls and intrusion detection systems.
- Security Tools
  - Many tools are available to network users to protect the devices from attacks and to help remove malicious software from infected machines.

How Can I Protect My Network?

Security Tools (Cont.)

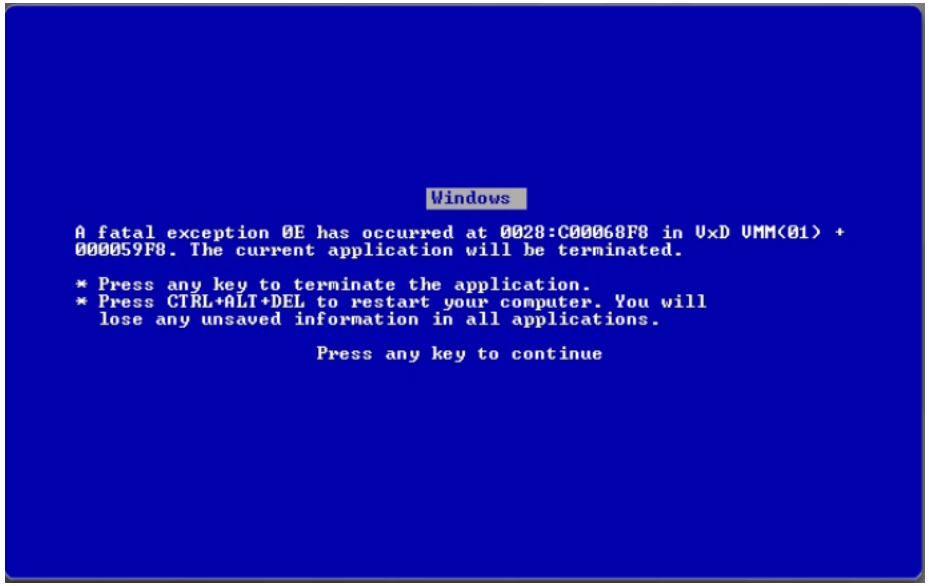
- Patches and Updates
  - A patch is a small piece of code that fixes a specific problem. An update, on the other hand, may include additional functionality to the software package as well as patches for specific issues.



How Can I Protect My Network?

Antivirus Software

- Infection Detection
  - Any device that is connected to a network is susceptible to viruses, worms and Trojan horses. So how do you know if your computer has been infected?



- Computer starts acting abnormally
- Program does not respond to mouse and keystrokes
- Programs starting or shutting down on their own
- Email program begins sending out large quantities of email
- CPU usage is very high
- There are unidentifiable, or a large number of processes running
- Computer slows down significantly or crashes

How Can I Protect My Network?

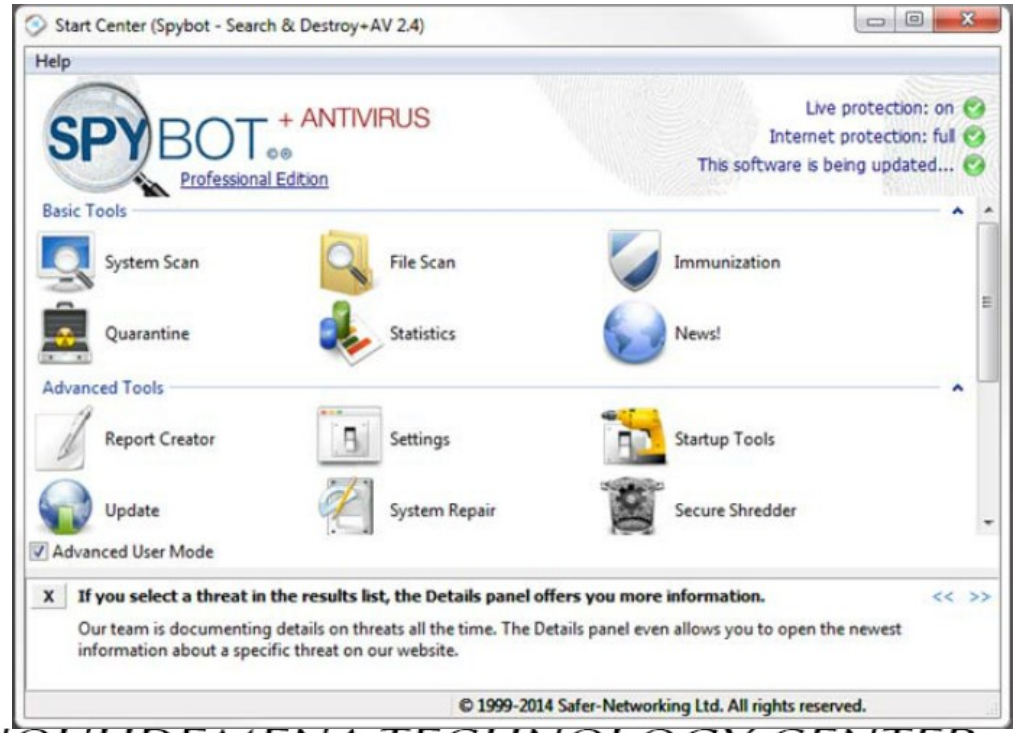
Antivirus Software (Cont.)

- Antivirus Software
  - Antivirus software relies on known “virus signatures” in order to find and prevent new viruses from infecting the computer.
- Antispam Software
  - Protects hosts by identifying spam and performing an action, such as placing it into a junk folder or deleting it.
- Additional Safeguards
  - Before forwarding virus warning emails, check a trusted source to see if the virus is a hoax.

How Can I Protect My Network?

Removing Spyware

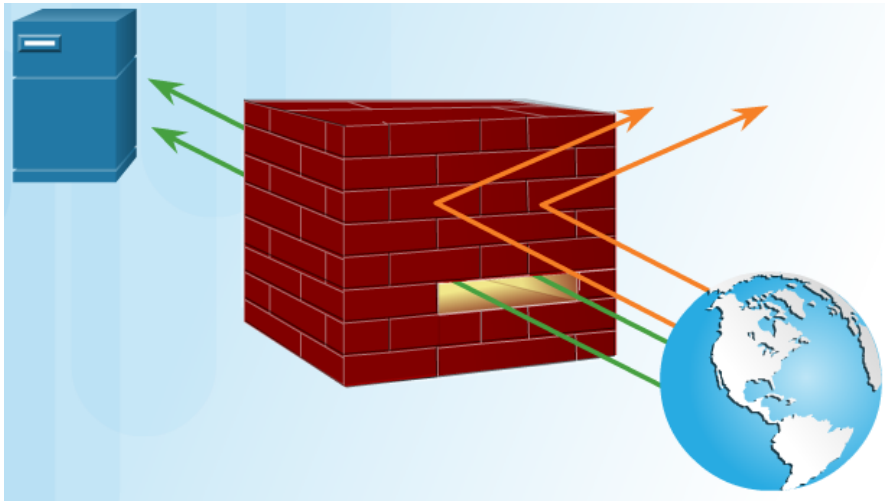
- Antispyware, Adware, and Popup Blockers
  - Antispyware detects and deletes spyware applications. Many antispyware applications also include detection and deletion of cookies and adware. Popup blocking software can be installed to prevent popups and pop-unders.



How Do Firewalls Protect Networks?

Firewall Basics

- What is a Firewall?
  - A firewall prevents undesirable traffic from entering protected areas of the network. A firewall is usually installed between two or more networks and controls the traffic between them as well as helps prevent unauthorized access.
  - Firewalls can be implemented in software. Firewalls may also be hardware devices.
  - A hardware firewall is a freestanding unit.
  - Firewalls often perform Network Address Translation.



How Do Firewalls Protect Networks?

Firewall Basics (Cont.)

- DMZ
  - In computer networking, a DMZ refers to an area of the network that is accessible to both internal and external users.
  - With the wireless router, a simple DMZ can be set up that allows an internal server to be accessible by outside hosts.
  - The wireless router isolates traffic destined to the IP address specified. This traffic is then forwarded only to the switch port where the server is connected.

Cisco LAN Devices

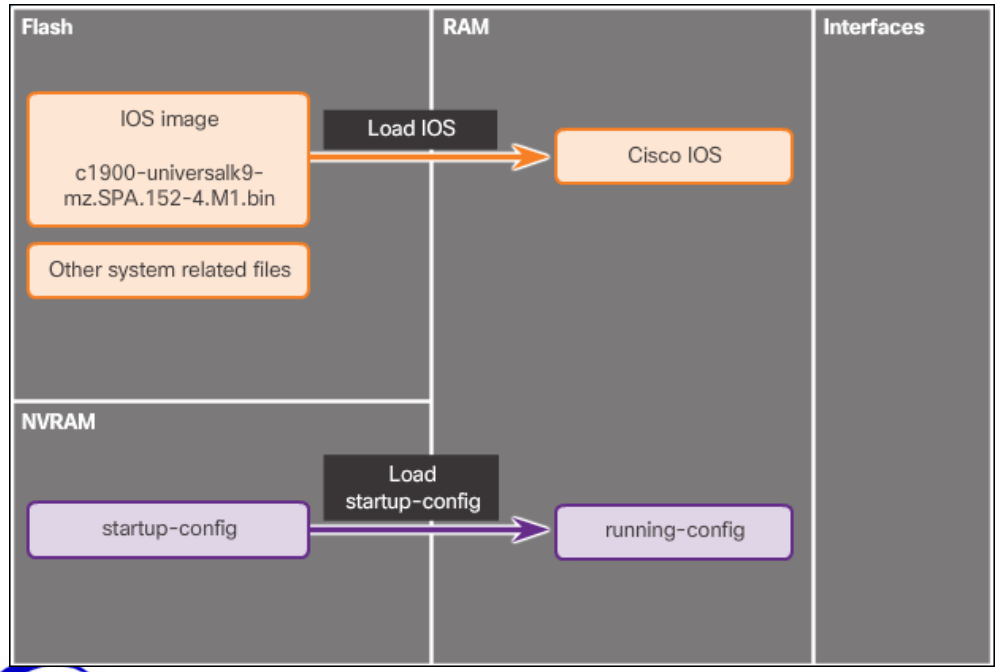
LAN Switches and Wireless Devices

- A switch is used to connect devices on the same network. A router is used to connect multiple networks to each other.
- When choosing a switch for a particular LAN, there are a number of factors to consider: types and number of ports, the speed required, expandability and manageability.
- Cisco Catalyst 2960 Series Ethernet switches are suitable for small and medium sized networks. They provide 10/100 Fast Ethernet and 10/100/1000 Gigabit Ethernet LAN connectivity.

Cisco LAN Devices

Connecting to the Switch

- When the switch is on, the power-on self-test (POST) begins. During POST, the LEDs blink while a series of tests determine that the switch is functioning properly. POST is completed when the SYST LED rapidly blinks green. If the switch fails POST, the SYST LED turns amber.
- Out-of-band management requires a computer to be directly connected to the console port of the network device that is being configured. Use in-band management to monitor and make configuration changes to a network device over a network connection.

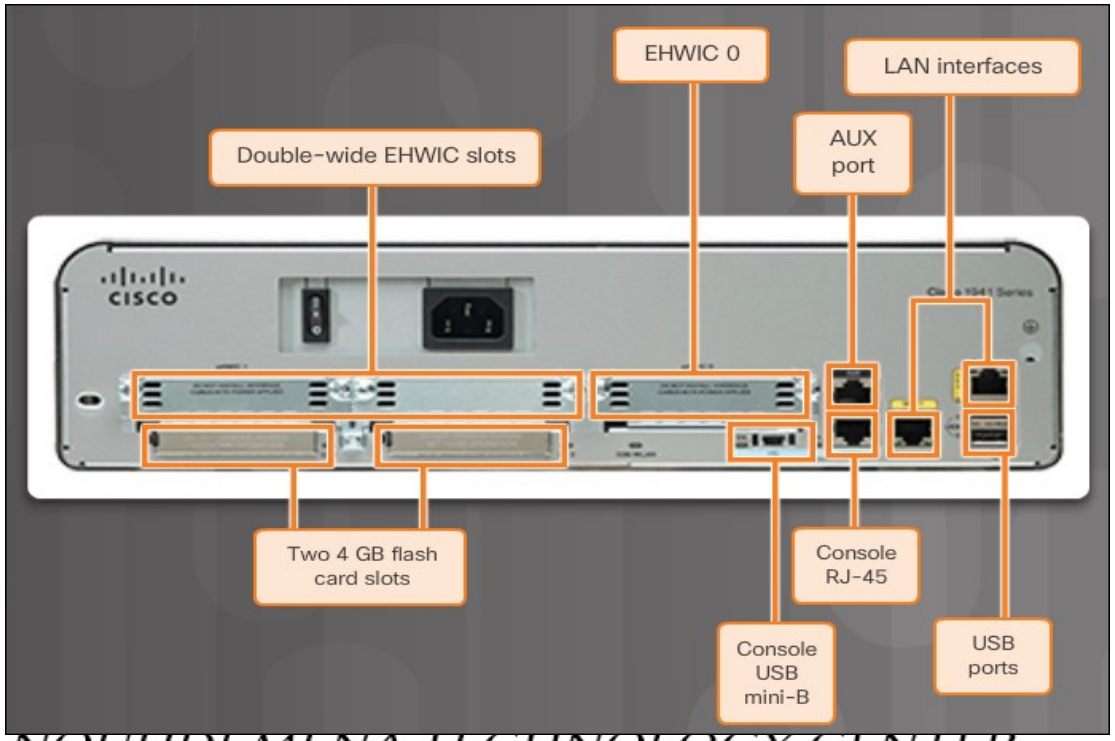


- A Cisco device loads the following two files into RAM when it is booted:
  - IOS Image file
  - Startup configuration file

Internetworking Devices

Cisco Routers

- All routers are essentially computers. Just like computers, routers require: operating systems (OS), central processing units (CPU), random-access memory (RAM), read-only memory (ROM), and nonvolatile random-access memory (NVRAM).
- Every Cisco router has the same general hardware components, and these connections: console ports, 2 LAN interfaces, and enhanced high-speed WAN interface card (EHWIC) slots.

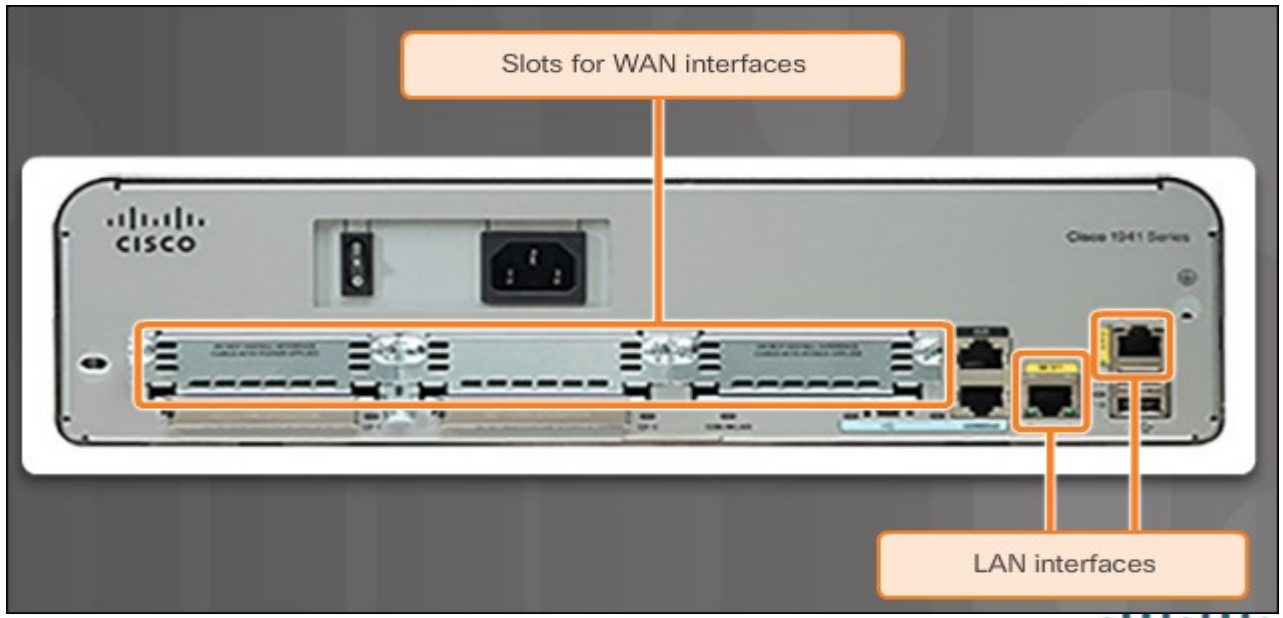


Internetworking Devices

Setting Up the Router

- Follow these steps to power up a Cisco router:
  1. Mount and ground the device chassis.
  2. Seat the external compact flash card.
  3. Connect the power cable.
  4. Configure the terminal emulation software on the PC and connect the PC to the console port.
  5. Turn on the router.
  6. Observe the startup messages on the PC as the router boots up.

- The two most common methods to access the command line interface are console and SSH.



Exploring the Cisco IOS

Navigate the IOS

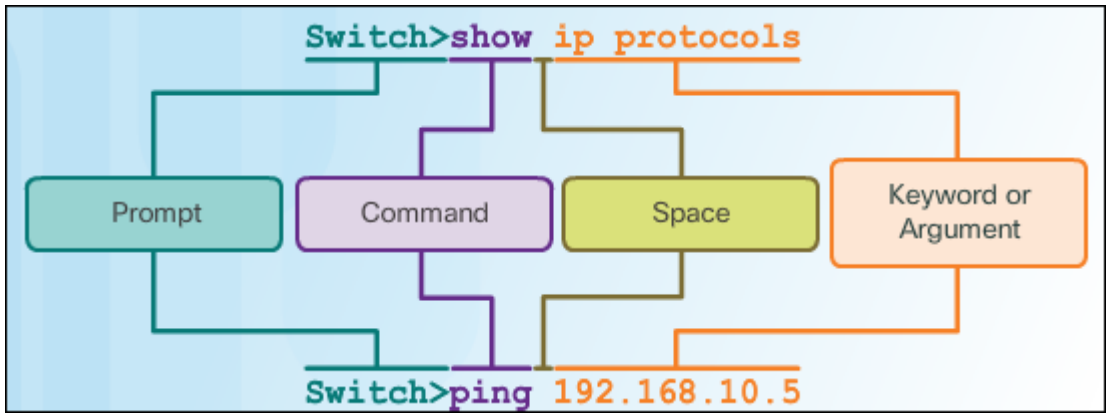
- The Cisco IOS command line interface (CLI) is a text-based program that enables entering and executing Cisco IOS commands to configure, monitor, and maintain Cisco devices.
- To initially configure a Cisco device, a console connection must be established.
- As a security feature, the Cisco IOS software separates management access into the following two command modes: user EXEC mode and privileged EXEC mode.
- Global configuration mode is identified by a prompt that ends with (config)# after the device name, such as **Switch(config)#**.

Command Mode	Description	Default Device Prompt
User Exec Mode	• Mode allows access to only a limited number of basic monitoring commands. • It is often referred to as "view-only" mode.	`Switch>` `Router>`
Privileged EXEC Mode	• Mode allows access to all commands and features. • The user can use any monitoring commands and execute configuration and management commands.	`Switch#` `Router#`

Exploring the Cisco IOS

The Command Structure

- The general syntax for a command is the command followed by any appropriate keywords and arguments:
  - **Keyword** - a specific parameter defined in the operating system (in the figure, ip protocols)
  - **Argument** - not predefined; a value or variable defined by the user (in the figure, 192.168.10.5)



- **ping** *ip-address* - The command is ping and the user-defined argument is the ip-address of the destination device.
- **traceroute** *ip-address* - The command is traceroute and the user-defined argument is the ip-address of the destination device.
- The Cisco IOS has both context sensitive help and command syntax check.
- Commands and keywords can be shortened to the minimum number of characters that identify a unique selection.

Using Show Commands

Viewing Device Information

- To verify and troubleshoot network operation, examine the operation of the devices using the **show** command:
  - **show running-config**
  - **show interfaces**
  - **show arp**
  - **show ip route**
  - **show protocols**
  - **show version**

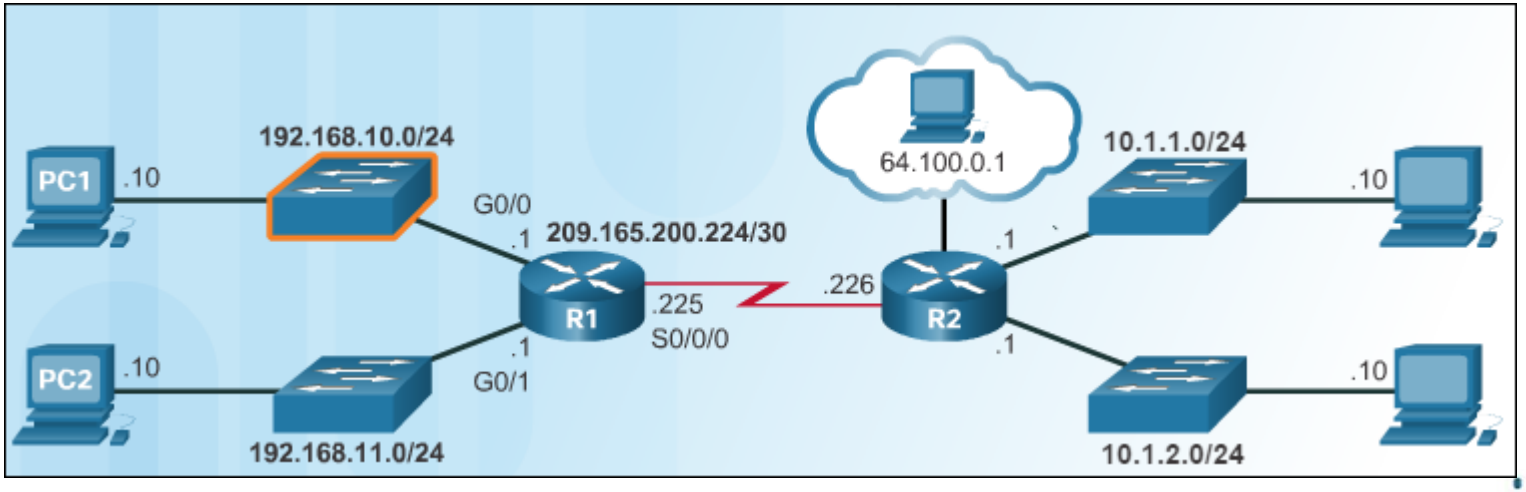
```
R1# show running-config

Building configuration...
Current configuration : 1063 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
enable secret 5 $1$i6w9$dvdpVM6zV10E6tSyLdkR5/
no ip domain lookup
```

- If you are logged into a router or switch remotely, the **show version** command is an excellent means of quickly finding useful summary information about the particular device to which you are connected.

Configuring a Cisco Network

Basic Switch Configuration

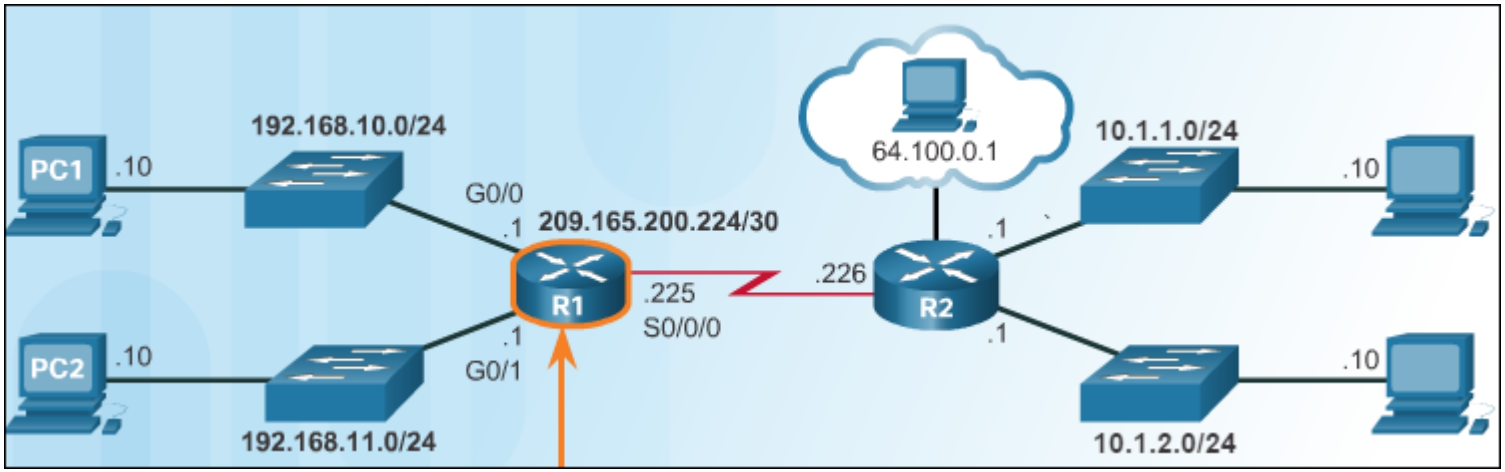
1. Configure the device name.
2. Secure the user EXEC mode.
3. Secure privileged EXEC mode.
4. Secure all passwords in the config file.
5. Provide legal notification.
6. Save the configuration.



Configuring a Cisco Network

Basic Router Configuration

1. Configure the device name.
2. Secure the user EXEC mode.
3. Secure privileged EXEC mode.
4. Secure all passwords in the config file.
5. Provide legal notification.
6. Save the configuration.



Configuring a Cisco Network

Basic Router Configuration (Cont.)

- Configure the interface:
  - **interface** *type-and-number*
  - **description** *description-text*
  - **ip address** *ipv4-address subnet-mask*
  - **no shutdown**
- One of the most useful commands for verifying interface configuration is the **show ip interface brief** command. The output displays all interfaces, their IPv4 address, and their current status. The configured and connected interfaces should display a Status of “up” and Protocol of “up”.

- Other interface verification commands include:
- **show ip route** - Displays the contents of the IPv4 routing table stored in RAM.
- **show interfaces** - Displays statistics for all interfaces on the device.
- **show ip interface** - Displays the IPv4 statistics for all interfaces on a router.

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     192.168.10.1    YES manual up                    up
GigabitEthernet0/1     192.168.11.1    YES manual up                    up
Serial0/0/0            209.165.200.225 YES manual up                    up
Serial0/0/1            unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES NVRAM  administratively down down
R1#
R1#ping 209.165.200.226
```

Configuring a Cisco Network

Connecting the Switch to the Router

- The default gateway address is generally the router interface address attached to the local network of the host. The IP address of the host device and the router interface address must be in the same network.
- To configure a default gateway on a switch, use the **ip default-gateway** global configuration command. The IP address configured is that of the router interface of the connected switch.