

# Chapter 11:

# Build a Small Network

Introduction to Networks v5.1



# Chapter Outline

11.0 Introduction

11.1 Network Design

11.2 Network Security

11.3 Basic Network Performance

11.4 Summary

# Section 11.1: Network Design

Upon completion of this section, you should be able to:

- Identify the devices used in a small network.
- Identify the protocols used in a small network.
- Explain how a small network serves as the basis of larger networks.

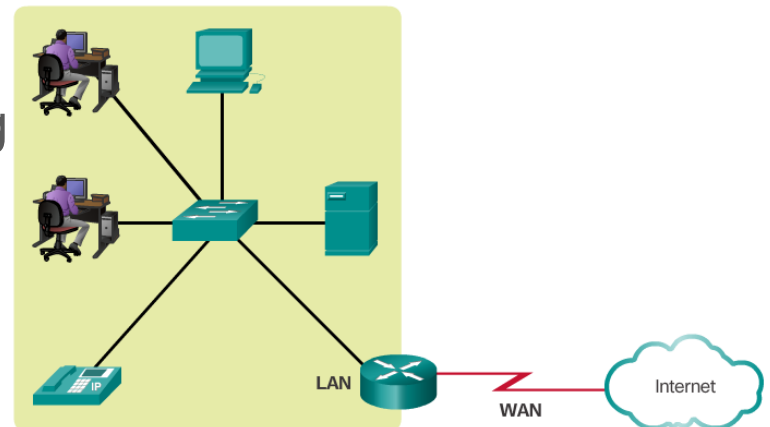
## Topic 11.1.1: Devices in a Small Network



# Small Network Topologies

## Typical Small Business Network

- Small networks have simple designs.
- Only a small number of network devices are needed.
- A small network usually comprises one router, a couple of switches, and the user PCs.
- A connection to the Internet is achieved through a single WAN link (commonly either cable or DSL).
- Most of the managing task is related to maintaining and troubleshooting existing equipment.
- The management of a small network is usually done by an employee of a third party company.



# Device Selection for a Small Network

Factors to consider when choosing a device in addition to those listed in the graphic include OS features:

- Security
- QoS
- VoIP
- L3 switching
- NAT
- DHCP



Cost



Ports



Speed



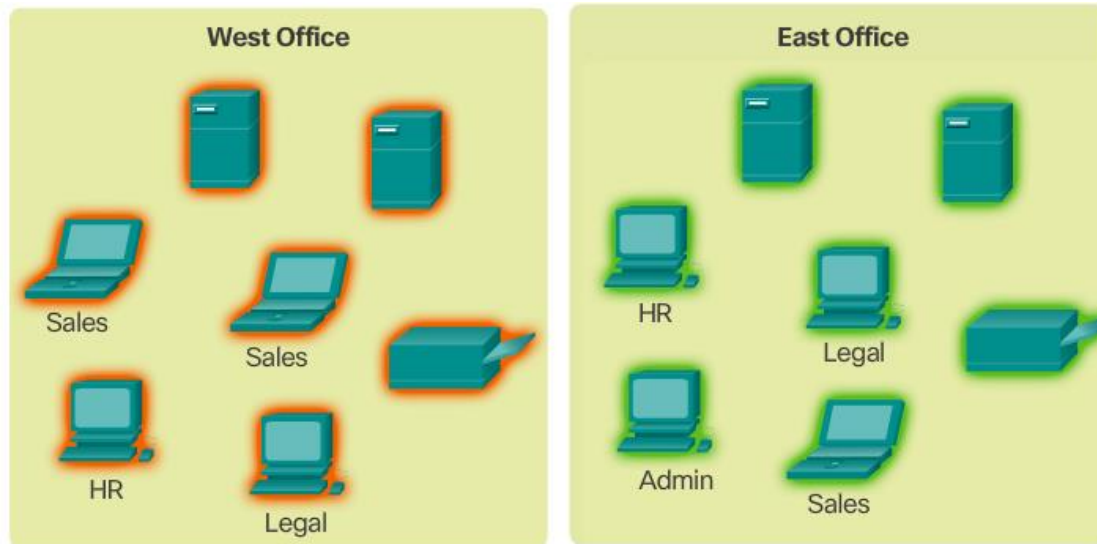
Expandable/Modular



Manageable

# IP Addressing for a Small Network

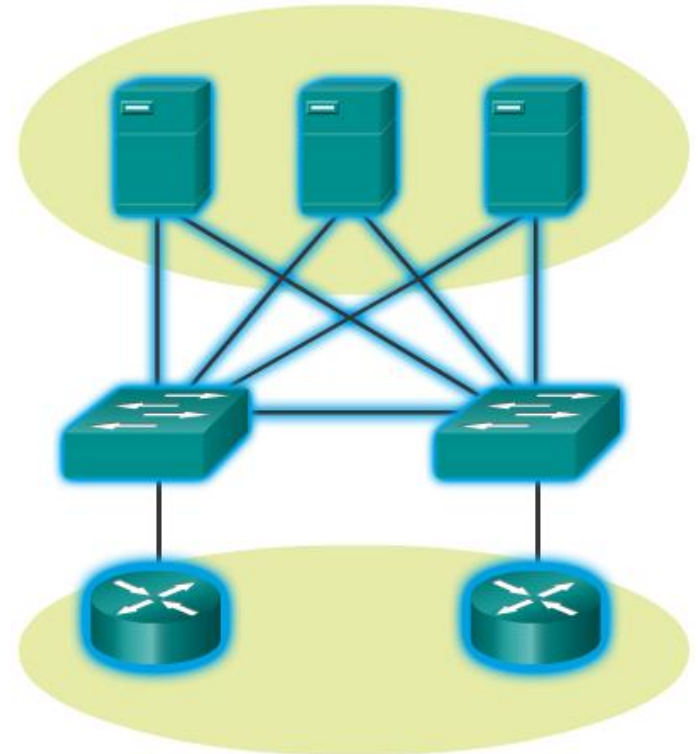
- Address space is a crucial component of a network design.
- All devices connected to the network require an address.
- The address scheme must be planned, documented, and maintained.
- Address space documentation can be very useful for troubleshooting.
- Address documentation is also very important when controlling resource access.



# Redundancy in a Small Network

## Redundancy to a Server Farm

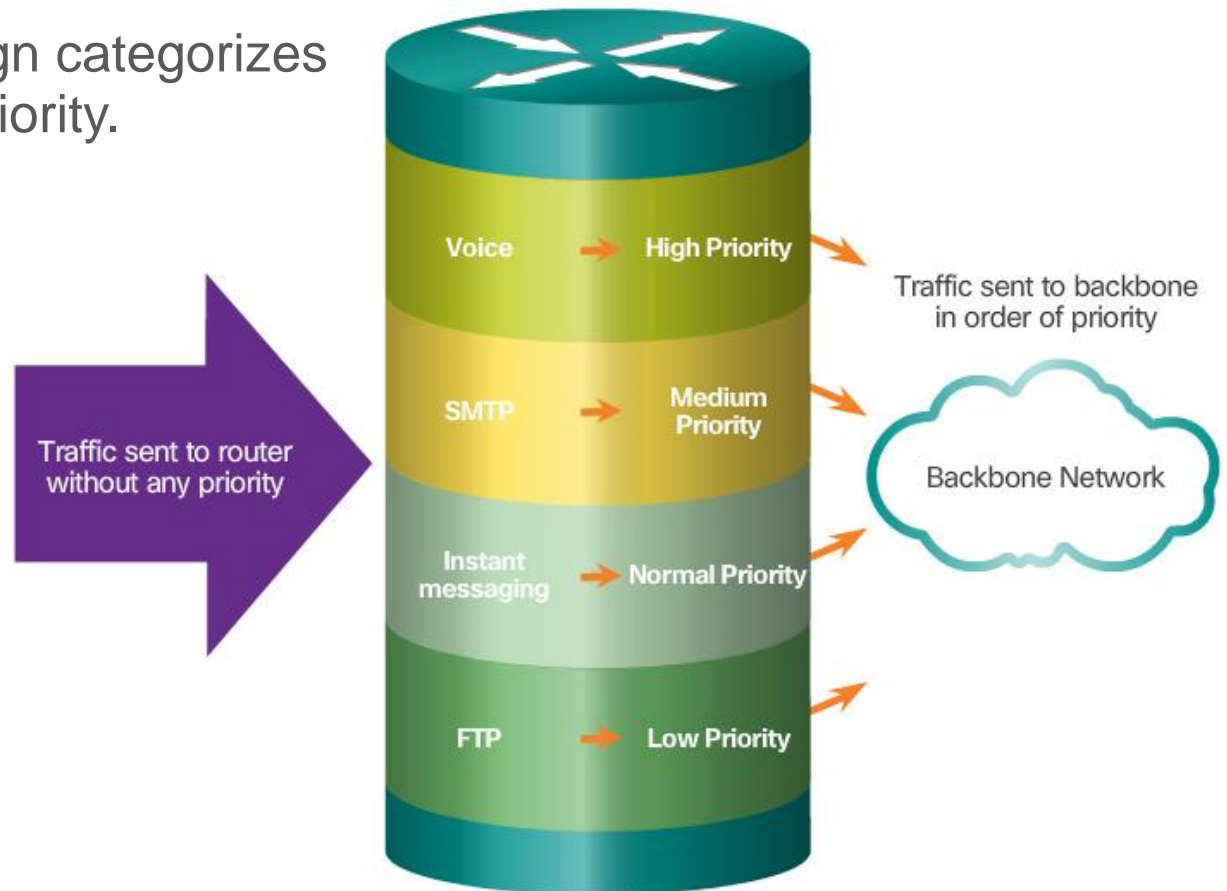
- A network should be reliable by design.
- Network failures are usually very costly.
- Redundancy increases reliability by eliminating single points of failure.
- Network redundancy can be achieved by duplicating network equipment and links.
- A good example is a network's link to the Internet or to a server farm.





# Traffic Management

- Traffic type and patterns are should also be considered when designing a network.
- A good network design categorizes traffic according to priority.



## Topic 11.1.2: Small Network Applications and Protocols



# Common Applications

## Network Applications

- Used to communicate over the network.
- Email clients and web browsers are examples of this type of application.

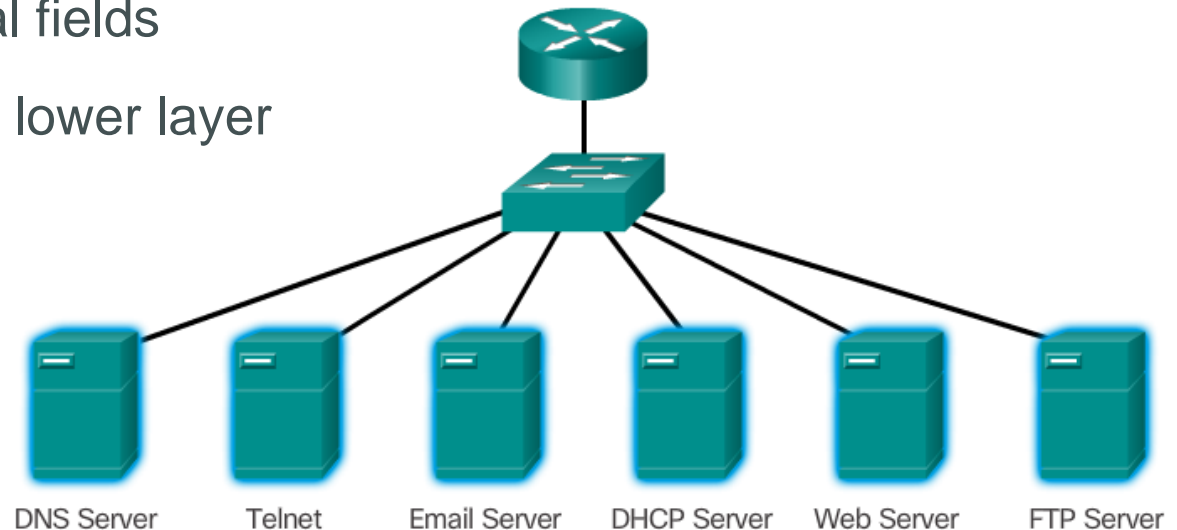
## Application Layer Services

- Programs that interface with the network and prepare the data for transfer.
- Each service uses protocols, which define the standards and data formats to be used.

# Common Protocols

Each of these network protocols define:

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



# Real-Time Applications

Basic components:

- Infrastructure
- VoIP
- IP Telephony
- Real-time Appli



## Topic 11.1.3: Scale to Larger Networks



# Small Network Growth

To scale a network, several elements are required:

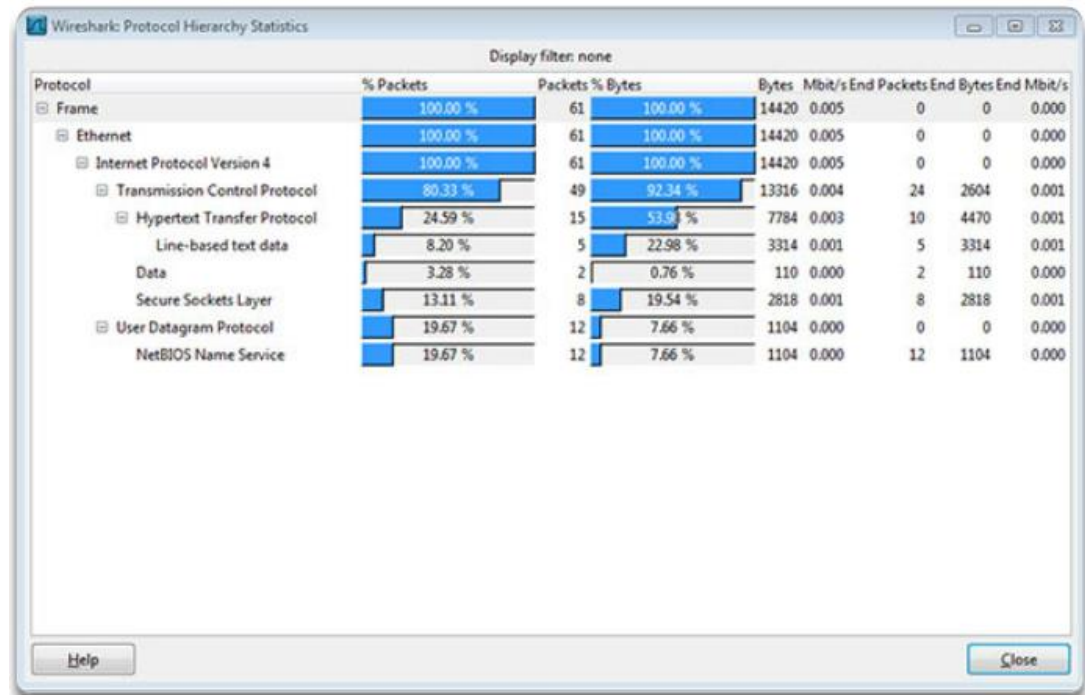
- Network documentation
- Device inventory
- Budget
- Traffic analysis





# Protocol Analysis

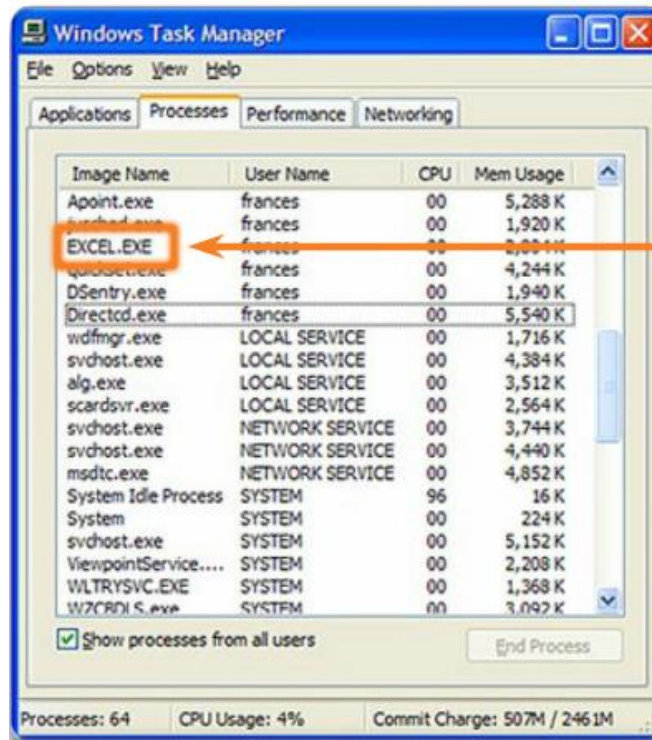
- A network administrator must understand the protocols in use in the network. Protocol analyzers are tools designed to help in that task.
- For a more accurate protocol analysis, it is important to capture traffic in high-utilization times and in different locations of the network.
- The result of the analysis allows for a more efficient way to manage traffic.





# Employee Network Utilization

- It is also important to be aware of how network use is changing.
- A network administrator can create in-person IT “snapshots” of employee application utilization.



Processes are individual software programs running concurrently.

**Processes can be:**

**1** Applications

**2** Services

**3** System operations

**4** One program may be running several times, each in its own process

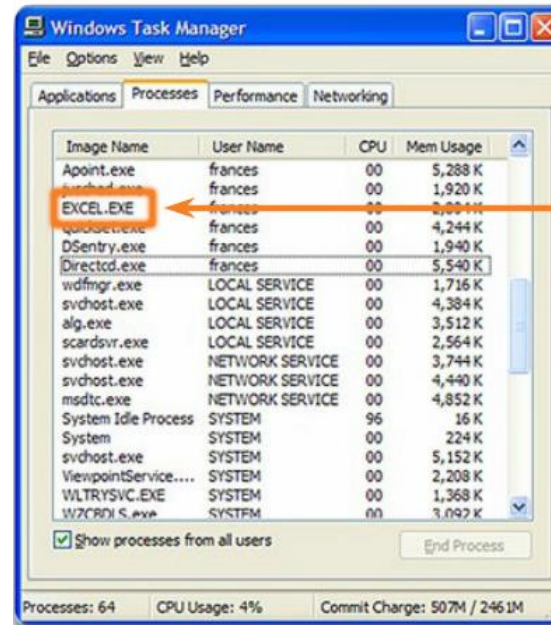
# Employee Network Utilization (cont.)

- These snapshots typically include information such as:

- OS and OS version
- Non-network applications
- Network applications
- CPU utilization
- Drive utilization
- RAM utilization

- Documented employee IT snapshots will go a long way toward informing of evolving protocol requirements.

- A shift in resource utilization may require an adjustment of network resource allocations.



Processes are individual software programs running concurrently.

**Processes can be:**

- 1 Applications
- 2 Services
- 3 System operations
- 4 One program may be running several times, each in its own process

# Section 11.2:

## Network Security

Upon completion of this section, you should be able to:

- Explain why security measures are necessary on network devices.
- Identify security vulnerabilities.
- Identify general mitigation techniques.
- Configure network devices with device hardening features to mitigate security threats.
- Apply the commands to back up and restore an IOS configuration file.

## Topic 11.2.1: Security Threats and Vulnerabilities



# Types of Threats

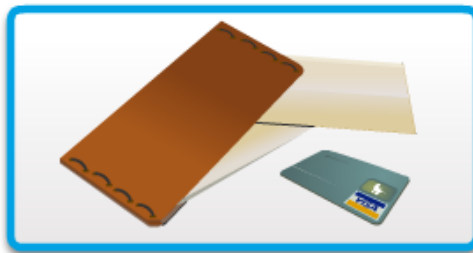
- Digital intrusion can be costly.
- Intruders can gain access through software vulnerabilities, hardware attacks, or stolen credentials.
- Common types of digital threats include those listed in this graphic.



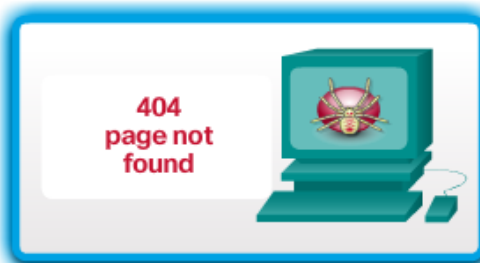
Information Theft



Data Loss and Manipulation



Identity Theft

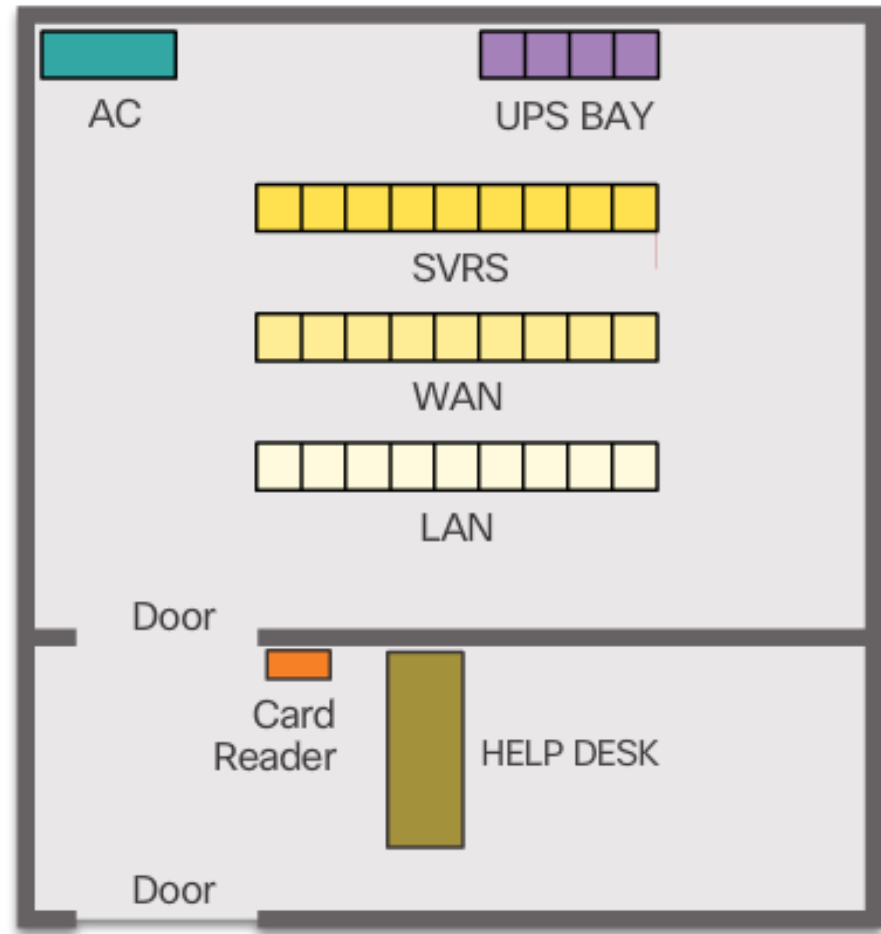


Disruption of Service

# Physical Security

Classes of physical threats:

- Hardware
- Environmental
- Electrical
- Maintenance



Secure computer room floor plan

# Types of Vulnerabilities

- There are three primary vulnerabilities:
  - Technological - Vulnerabilities in protocols, operating systems, and network equipment
  - Configuration - Vulnerabilities created by misconfigured devices, default configuration values, and easily guessed passwords
  - Security policy - Lack of security policy, software and hardware installation is not consistent with security policy, and no disaster or recovery plan
- Typically, the devices under attack are the endpoints, such as servers and desktop computers.
- Any of these three vulnerabilities can be exploited and used in attacks.

## Topic 11.2.2: Network Attacks





# Types of Malware

- Viruses
- Worms
- Trojan Horses



# Reconnaissance Attacks

- The discovery and mapping of systems and services
- Often not considered an attack on its own
- Goal is to acquire enough information on the target system or network to facilitate the search for vulnerabilities.
- Common tools rely mostly on free and public Internet services, such as DNS and Whois.
- Port-scanners and packet sniffers are also commonly used in reconnaissance.



Internet queries



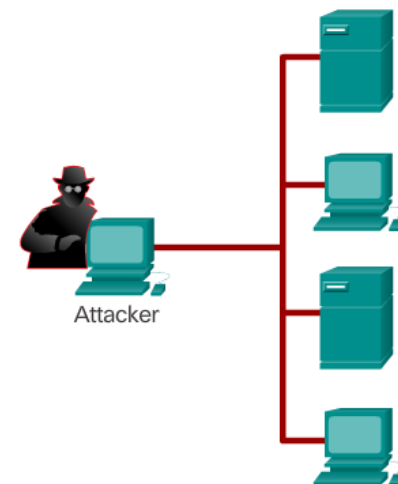
Ping sweeps



Port scans



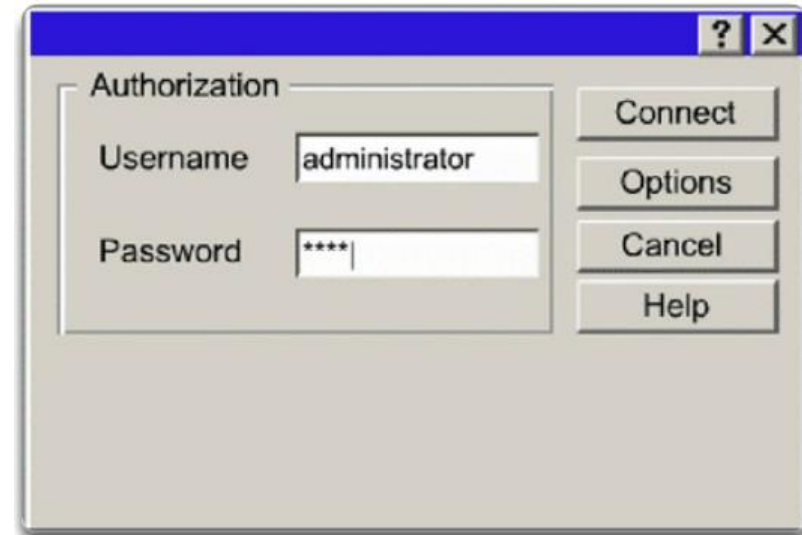
Packet sniffers



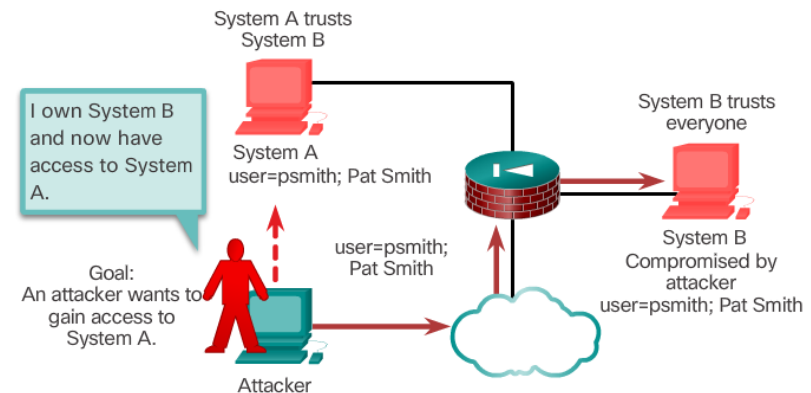
# Access Attacks

- Attacks against known vulnerabilities and services.
- The goal is to gain access to information that they have no right to view.
- Access attacks can be classified into four types:
  - Password Attacks
  - Trust Exploitation
  - Port Redirection
  - Man-in-the-Middle

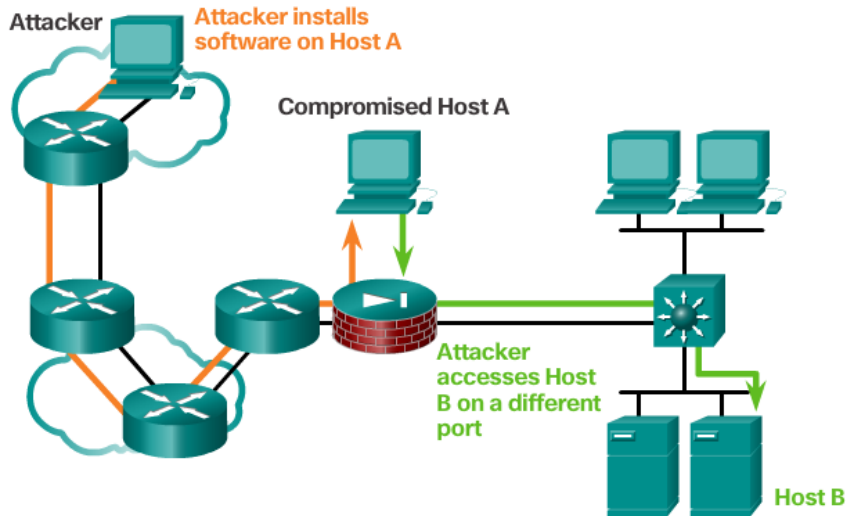
## Password Attack



## Trust Exploitation

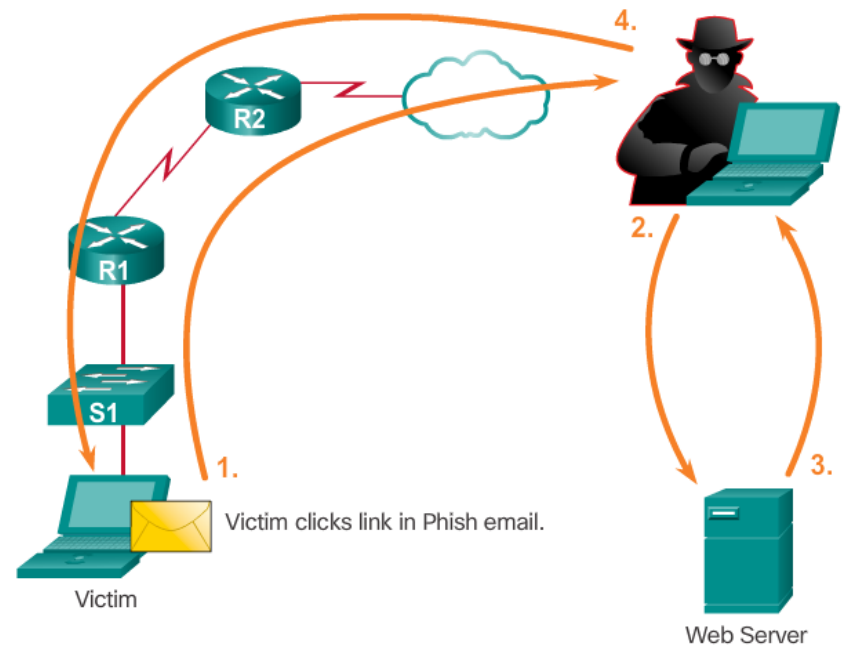


# Access Attacks (cont.)



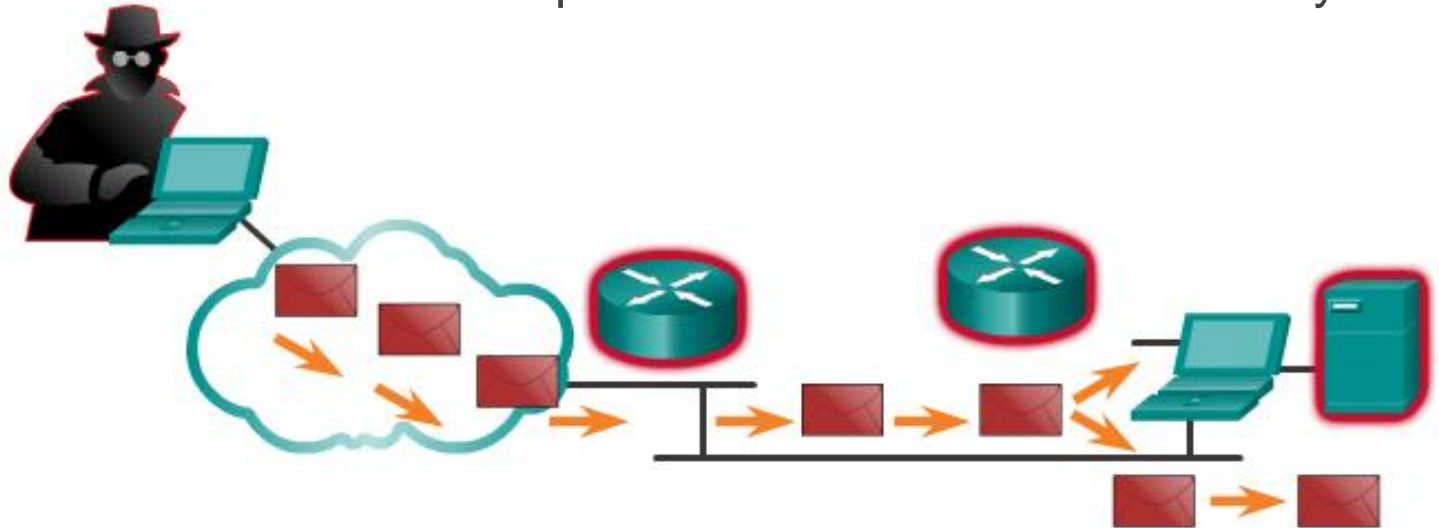
Man-in-the-Middle

## Port Redirection



# Denial of Service Attacks

- Denial of Service (DoS) attacks are difficult to eliminate.
- DoS attacks are regarded as trivial and require little effort to execute.
- Although simple, DoS attacks are still dangerous.
- Ultimately, they prevent authorized people from using a service by consuming system resources.
- To help prevent DoS attacks it is important to have the latest security updates.

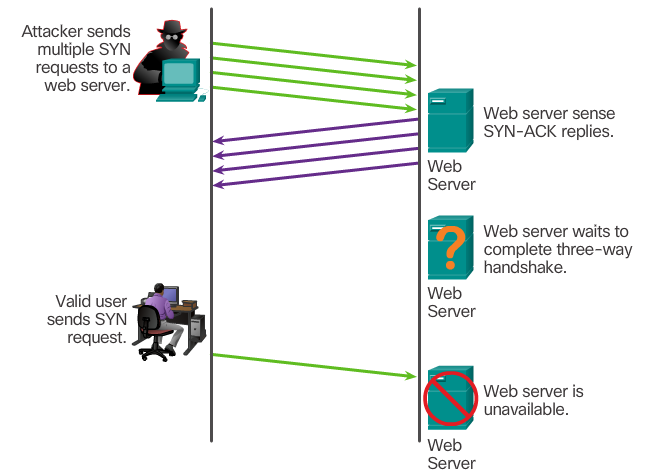


# Denial of Service Attacks (cont.)

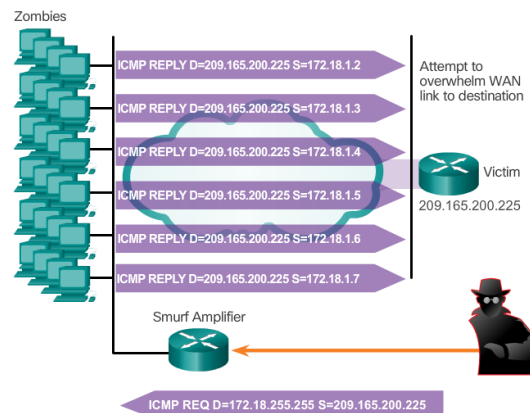
## Common DoS Attacks:

- Ping of Death
- SYN Flood
- DDoS
- Smurf Attack

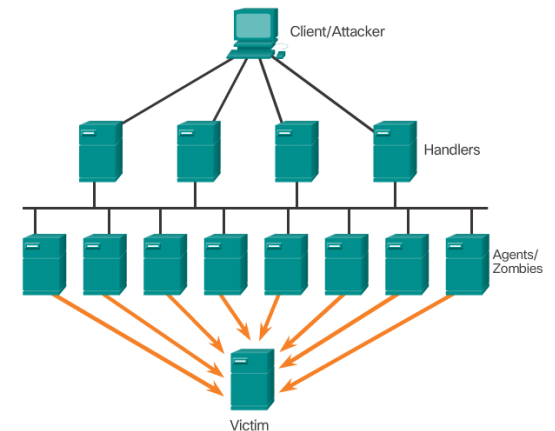
### SYN Flood



### Smurf Attack



### DDoS

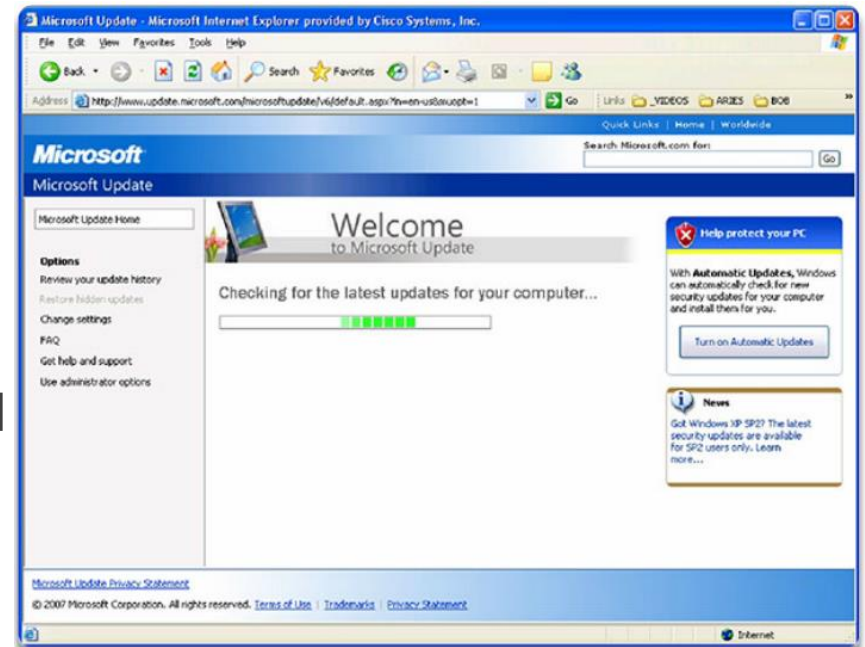


## Topic 11.2.3: Network Attack Mitigation



# Backup, Upgrade, Update, and Patch

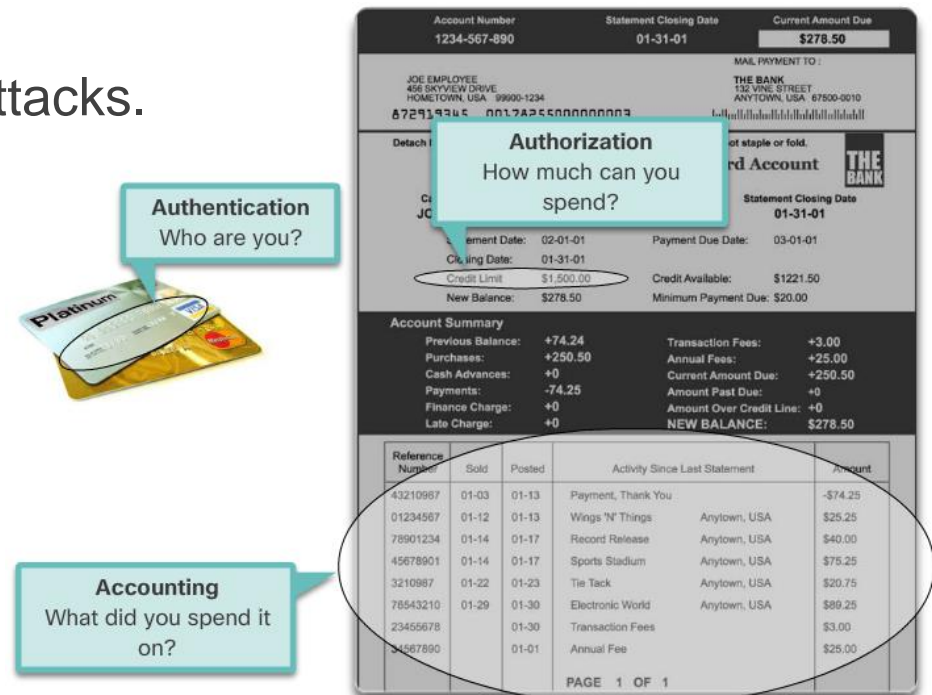
- Keeping up-to-date with the latest developments can lead to a more effective defense against network attacks.
- As new malware is released, enterprises need to keep current with the latest versions of antivirus software.
- To mitigate worm attacks, patches for all known vulnerabilities must be applied.
- A central patch server can be a good solution for managing a large number of servers and systems.
- Any patches that are not applied to a host are automatically downloaded without user intervention.





# Authentication, Authorization, and Accounting

- AAA services provide access control on a network device.
- AAA is a way to control who is permitted to access a resource (authenticate), what they can do while they are there (authorize), and what actions they perform while accessing the resource (accounting).
- The AAA framework can be very helpful when mitigating network attacks.



# Firewalls

- A firewall controls the traffic and helps prevent unauthorized access
- Techniques for determining what is permitted or denied access to a network include:
  - Packet filtering
  - Application filtering
  - URL filtering
  - Stateful packet inspection (SPI)



Cisco Security Appliances



Server-Based Firewall



Linksys Wireless Router with Integrated Firewall



Personal Firewall

# Endpoint Security

- Common endpoints are laptops, desktops, servers, smartphones, and tablets.
- Securing endpoint devices is challenging.
- Employees need to be trained on proper use of the network.
- Policies often include the use of antivirus software and host intrusion prevention.
- More comprehensive endpoint security solutions rely on network access control.

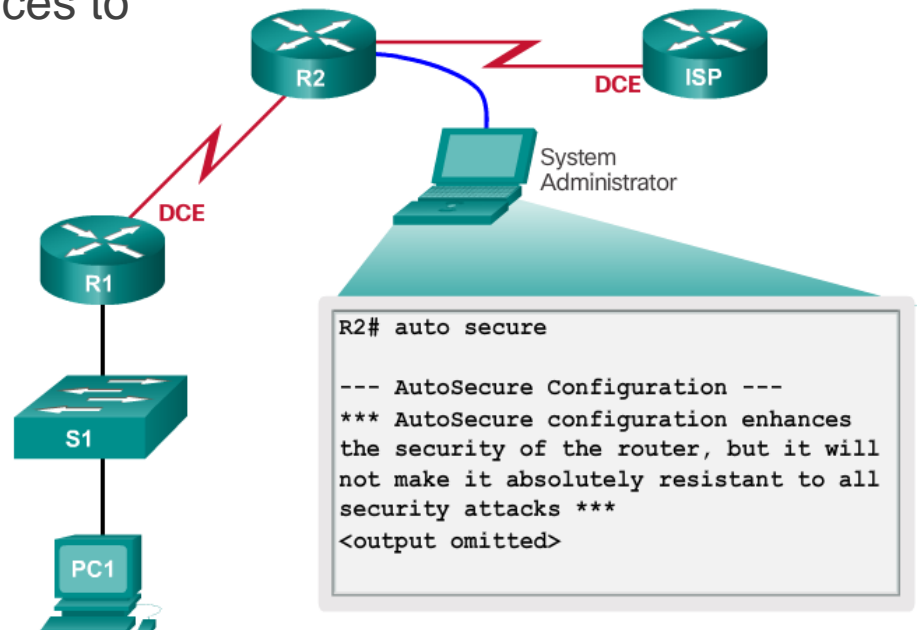


## Topic 11.2.4: Device Security



# Device Security Overview

- Default settings are dangerous because they are well-known.
- Cisco routers have the Cisco AutoSecure feature.
- In addition, the following apply for most systems:
  - Change default usernames and passwords immediately
  - Restrict access to system resources to authorized individuals only.
  - Turn off unnecessary services.
  - Update any software and install any security patches prior to production operation.



# Passwords

- Use strong passwords. A strong password has/is:
  - At least 8 characters, preferably 10 or more
  - A mix of uppercase and lowercase letters, numbers, symbols, and spaces.
  - No repetition, no common dictionary words, no letter or number sequences, no usernames, relative, or pet names, and no other easily identifiable pieces of information
  - Misspelled words
  - Changed often
- Cisco routers support the use of a phrase made of many words, which is called a passphrase.

Weak Password	Why it is weak
secret	Simple dictionary password
smith	Mother's maiden name
toyota	Make of a car
bob1967	Name and birthday of a user
Blueleaf23	Simple words and numbers

Strong Password	Why it is strong
b67n42d39c	Combines alphanumeric characters
12^h u4@1p7	Combines alphanumeric characters, symbols, and also includes a space

# Basic Security Practices

- Strong passwords are only as useful as they are secret.
- The **service password-encryption** command encrypts the passwords in the configuration.
- The **security passwords min-length** command ensures all configured passwords have a minimum specified length.
- Blocking several consecutive login attempts helps minimize password brute-force attacks.
- **login block-for 120 attempts 3 within 60** will block login attempts for 120 seconds if there are three failed login attempts within 60 seconds.
- **Exec Timeout** automatically disconnect idle users on a line

```
Router(config)#service password-encryption
Router(config)#security password min-length 8
Router(config)#login block-for 120 attempts 3 within 60
Router(config)#line vty 0 4
Router(config-vty)#exec-timeout 10
Router(config-vty)#end
Router#show running-config
-more-
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 exec-timeout 10
 login
```

# Enable SSH

- Telnet is not secure.
- It is highly recommended to use SSH for remote shell protocol.
- To configure a Cisco device to support SSH takes four steps:
  - **Step 1.** Ensure that the router has a unique hostname and a IP domain name.
  - **Step 2.** Generate the SSH keys.
  - **Step 3.** Create a local username.
  - **Step 4.** Enable **vtty inbound SSH** sessions.
- The router can now be remotely accessed only by using SSH.



```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Step 1: Configure the IP domain name.  
Step 2: Generate one-way secret keys.  
Step 3: Verify or create a local database entry.  
Step 4: Enable VTY inbound SSH sessions.



## Topic 11.2.5: Backup and Restore Configuration Files



# Router File Systems

- The Cisco IOS File System (IFS) allows for file system read and write operations.
- Use the **show file systems** command lists all of the available file systems
- This course focuses on **tftp**, **flash**, and **nvr** file systems. The bootable IOS image is located in flash.
- The Flash File System
  - Commonly the largest file system in a Cisco router.
  - Commonly stores the IOS image.
  - Use the **dir** command to list the contents of the flash or any other file system.
- The NVRAM File System
  - Commonly used to store the configuration files.
  - It is not common for a IOS to have a large NVRAM.

## File Systems

```
Router#show file systems
File Systems:
```

	Size (b)	Free (b)	Type	Flags	Prefixes
	-	-	opaque	rw	archive:
	-	-	opaque	rw	system:
	-	-	opaque	rw	tmpsys:
	-	-	opaque	rw	null:
	-	-	network	rw	tftp:
*	256487424	183234560	disk	rw	flash0: flash:#
	-	-	disk	rw	flash1:
	262136	254779	nvr	rw	nvr:
	-	-	opaque	wo	syslog:
	-	-	opaque	rw	xmodem:
	-	-	opaque	rw	ymodem:
	-	-	network	rw	rcp:
	-	-	network	rw	http:
	-	-	network	rw	ftp:
	-	-	network	rw	scp:
	-	-	opaque	ro	tar:
	-	-	network	rw	https:
	-	-	opaque	ro	cns:

## Flash

```
Router#dir
Directory of flash0:/

 1 -rw-      2903 Sep 7 2012 06:58:26 +00:00  cpconfig-
 19xx.cfg
 2 -rw-    3000320 Sep 7 2012 06:58:40 +00:00  cpexpress.tar
 3 -rw-      1038 Sep 7 2012 06:58:52 +00:00  home.shtml
 4 -rw-     122880 Sep 7 2012 06:59:02 +00:00  home.tar
 5 -rw-    1697952 Sep 7 2012 06:59:20 +00:00  securedesktop-
 ios-3.1.1.45-k9.pkg
 6 -rw-     415956 Sep 7 2012 06:59:34 +00:00  sslclient-win-
 1.1.4.176.pkg
 7 -rw-    67998028 Sep 26 2012 17:32:14 +00:00 c1900-
 universalk9-
 mz.SPA.152-4.M1.bin

256487424 bytes total (183234560 bytes free)
```

# Switch File Systems

## Cisco 2960 Switch

- Is similar to the router's file system.
- The Cisco 2960 switch flash file system supports configuration files, copy, and archive (upload and download) software images.
- Same command as on the router to view the file systems:  
**show file systems**

```
Switch# show file systems
File Systems:

      Size(b)      Free(b)      Type  Flags  Prefixes
*      32514048      20887552      flash   rw      flash:
      -            -            opaque   rw      vb:
      -            -            opaque   ro      bs:
      -            -            opaque   rw      system:
      -            -            opaque   rw      tmpsys:
      65536         48897         nvram    rw      nvram:
      -            -            opaque   ro      xmodem:
      -            -            opaque   ro      ymodem:
      -            -            opaque   rw      null:
      -            -            opaque   ro      tar:
      -            -            network  rw      tftp:
      -            -            network  rw      rcp:
      -            -            network  rw      http:
      -            -            network  rw      ftp:
      -            -            network  rw      scp:
      -            -            network  rw      https:
      -            -            opaque   ro      cns:
```

# Backing up and Restoring using Text Files

## Backing up the Configuration

- Configuration files can be saved/archived to a text file.
- For Tera Term the steps are:

**Step 1.** On the File menu, click **Log**.

**Step 2.** Choose the location to save the file. Tera Term will begin capturing text.

**Step 3.** Any text displayed in the terminal window will be directed to the chosen file.

**Step 4.** When the capture is complete, select **Close** in the Tera Term: Log window.

**Step 5.** View the file to verify that it was not corrupted.

## Restoring the Configuration

- A configuration can be copied from a file to a device.
- IOS executes any text pasted into a terminal window as a command.
- The device must be set at the global configuration mode.
- For Tera Term, the steps are:

**Step 1.** On the File menu, click **Send file**.

**Step 2.** Locate the file to be copied into the device and click **Open**.

**Step 3.** Tera Term will paste the file into the device. The text in the file will be applied as commands in the CLI and become the running configuration on the device.

# Backing up and Restoring TFTP

## Backup running configuration

**Step 1.** Enter the **copy running-config tftp** command.

**Step 2.** Enter the IP address of the host where the configuration file will be stored.

**Step 3.** Enter the name to assign to the configuration file.

**Step 4.** Press Enter to confirm each choice.

## Restore running configuration

**Step 1.** Enter the **copy tftp running-config** command.

**Step 2.** Enter the IP address of the host where the configuration file is stored.

**Step 3.** Enter the name to assign to the configuration file.

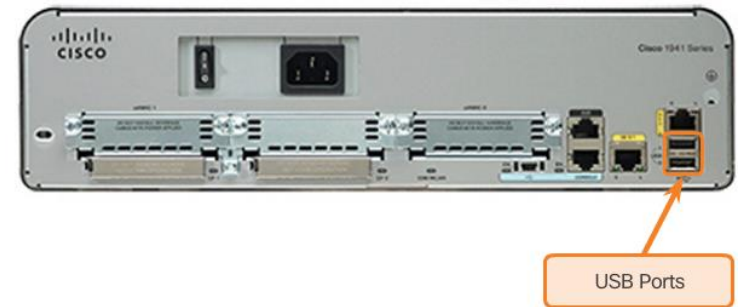
**Step 4.** Press Enter to confirm each choice.

```
Router# copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm]
Writing tokyo.2 !!!!! [OK]
```

# Using USB Ports on a Cisco Router

## Cisco 1941 Router USB Port

- Certain models of Cisco routers support USB flash drives.
- The USB flash feature provides an optional secondary storage capability and an additional boot device.
- It can hold images, configurations, and other files.
- USB flash can hold multiple copies of the Cisco IOS and multiple router configurations.
- Use the **dir** command to view the contents of the USB flash drive, as shown in the figure.



```
Router# dir usbflash0:
Directory of usbflash0:/
1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00
c3825-entservicesk9-mz.123-14.T
63158272 bytes total (33033216 bytes free)
```

# Backup and Restoring using USB

## Backup Configurations with a USB Flash Drive

- Confirm the drive is present with **show file systems**.
- Use the **copy run usbflash0:/** command to copy the configuration file to the USB flash drive.
- The IOS will prompt for the filename.
- Use the **dir** command to see the file on the USB drive.

## Restore Configurations with a USB Flash Drive

- Assuming the file name is **R1-Config**, use the command **copy usbflash0:/R1-Config running-config** to restore a running configuration.

```
R1# show file systems
File Systems:
```

	Size (b)	Free (b)	Type	Flags	Prefixes
	-	-	opaque	rw	archive:
	-	-	opaque	rw	system:
	-	-	opaque	rw	tmpsys:
	-	-	opaque	rw	null:
	-	-	network	rw	tftp:
*	256487424	184819712	disk	rw	flash0: flash:#
	-	-	disk	rw	flash1:
	262136	249270	nvr	rw	nvr
	-	-	opaque	wo	syslog:
	-	-	opaque	rw	xmodem:
	-	-	opaque	rw	ymodem:
	-	-	network	rw	rcp:
	-	-	network	rw	http:
	-	-	network	rw	ftp:
	-	-	network	rw	scp:
	-	-	opaque	ro	tar:
	-	-	network	rw	https:
	-	-	opaque	ro	cns:
	4050042880	3774152704	usbflash	rw	usbflash0:

Shows the USB port and name: "usbflash0:"

# Section 11.3:

## Basic Network Performance

Upon completion of this section, you should be able to:

- Use the output of the ping command to establish relative network performance.
- Use the output of the tracer command to establish relative network performance.
- Use show commands to verify the configuration and status of network devices.
- Use host and IOS commands to acquire information about network devices.



## Topic 11.3.1: The ping Command



# Interpreting Ping Results

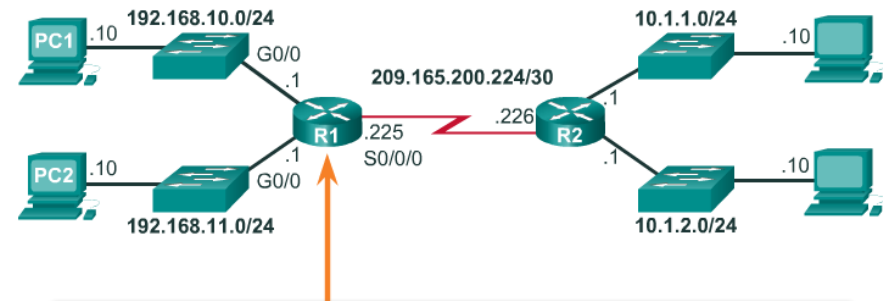
## IOS Ping Indicators

- Using the **ping** command is an effective way to test connectivity.
- Use the Internet Control Message Protocol (ICMP) to verify Layer 3 connectivity.
- The **ping** command can help to identify the source of the problem.
- A ping issued from the IOS will yield one of several indications for each ICMP echo request that was sent. The most common indicators are:
  - **!** - Indicates receipt of an ICMP echo reply message.
  - **.** - Indicates time expired while waiting for an ICMP echo reply message
  - **U** - Indicates that an ICMP unreachable message was received

# Interpreting Ping Results (cont.)

## IOS Ping Indicators

- The "." (period) may indicate that a connectivity problem occurred somewhere along the path. A number of reasons can result in this indicator:
  - A router along the path did not have a route to the destination.
  - The ping was blocked by device security.
  - The ping timed out before another protocol's response was received (ARP, for instance).
- The "U" indicates that a router along the path responded with an ICMP unreachable message. The router either did not have a route to the destination address or the ping request was blocked.



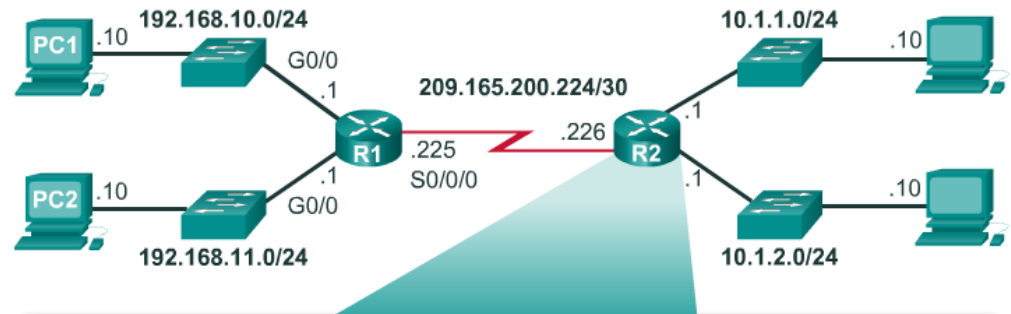
```
R1# ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout
is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
3/3/4 ms

R1#
```

# Extended Ping

- The Cisco IOS offers an "extended" mode of the ping command.
- This mode is entered by typing **ping** in privileged EXEC mode, without a destination IP address.
- A series of prompts are then presented.
- Pressing Enter accepts the indicated default values.



```
R2# ping
Protocol [ip]:
Target IP address: 192.168.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
```

# Network Baseline

- A network baseline is a very important tool.
- An effective network performance baseline is built over a period of time.
- The output derived from network commands can contribute data to the network baseline.
- A baseline can be created by copying and pasting the results from an executed ping, trace, or other relevant commands into a text file.
- These text files can be time stamped for later comparison.
- Among items to consider are error messages and the response times from host to host.
- If there is a considerable increase in response times, there may be a latency issue to address.

FEB 8, 2013 08:14:43

```
C:\>ping 10.66.254.159
```

```
Pinging 10.66.254.159 with 32 bytes of data:
```

```
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 10.66.254.159:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

MAR 17, 2013 14:41:06

```
C:\>ping 10.66.254.159
```

```
Pinging 10.66.254.159 with 32 bytes of data:
```

```
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
```

```
Ping statistics for 10.66.254.159:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 6ms, Average = 6ms
```

## Topic 11.3.2: The traceroute and tracert Command



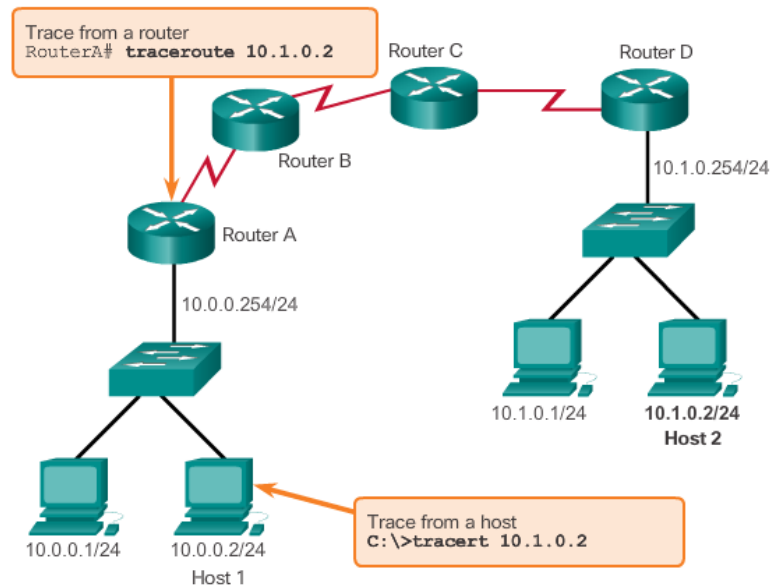
# Interpreting Trace Messages

- A trace returns a list of hops as a packet is routed through a network.
- The form of the command depends on the platform.
- Use **tracert** for Windows-based systems and traceroute for Cisco IOS and UNIX-based systems.

## Tracing the Route from Host 1 to Host 2

### Testing the Path to a Remote Host

```
C:\> tracert 10.1.0.2
Tracing route to 10.1.0.2 over a maximum of 30 hops
 1  2 ms  2 ms  2 ms  10.0.0.254
 2  * * * Request timed out.
 3  * * * Request timed out.
 4  ^C
C:\>
```



## Topic 11.3.3: Show Commands





# Common show Commands Revisited

- The Cisco IOS CLI **show** commands are powerful troubleshoot tools.
- The **show** commands display configuration files, checking the status of device interfaces and processes, and verifying the device operational status.
- The status of nearly every process or function of the router can be displayed using a show command.
- Some of the more popular **show** commands are:
  - **show running-config**
  - **show interfaces**
  - **show arp**
  - **show ip route**
  - **show protocols**
  - **show version**

```
R1# show running-config
<Output omitted>
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$dvdpm6zV10E6tSyLdkR5/
no ip domain lookup
!
interface FastEthernet0/0
description LAN 192.168.1.0 default gateway
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
```

```
!
interface Serial0/0/0
description WAN link to R2
ip address 192.168.2.1 255.255.255.0
encapsulation ppp
clock rate 64000
no fair-queue
!
interface Serial0/0/1
no ip address
shutdown
!
interface Vlan1
no ip address
!
router rip
version 2
network 192.168.1.0
network 192.168.2.0
!
banner motd ^CUnauthorized Access Prohibited^C
!
ip http server
!
```

## Topic 11.3.4: Host and IOS Commands



## ipconfig

# The ipconfig Command

- The **ipconfig** command can be used to display IP information on a Windows-based computer.
- The **ipconfig** command displays the host and its default gateway IP addresses.
- Use the **ipconfig /all** command to view the host's IP configuration in more detail, including its MAC address.
- The **ipconfig /displaydns** command displays all of the cached DNS entries on a Windows-based computer system.




```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254
```

### Legend

-  IP address for this host computer
-  Local network subnet mask
-  Default gateway address for this host computer

## ipconfig /all

```
C:\>ipconfig /all

Ethernet adapter Network Connection:

    Connection-specific DNS Suffix: example.com
    Description . . . . . : Intel(R)
    PRO/Wireless 3945ABG Network Connection
    Physical Address. . . . . : 00-18-DE-C7-F3-FB
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 10.2.3.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.2.3.254
    DHCP Server . . . . . : 10.2.3.69
    DNS Servers . . . . . : 192.168.226.120
    Lease Obtained. . . . . : Thursday, May 03,
                                2007 3:47:51 PM
    Lease Expires . . . . . : Friday, May 04,
                                2007 6:57:11 AM

C:\>
```

# The ipconfig Command (cont.)

ipconfig /displaydns

```
C:\> ipconfig /displaydns
```

```
Windows IP Configuration
```

```
cisco-tags.cisco.com
```

```
-----
```

```
Record Name . . . . . : cisco-tags.cisco.com
```

```
Record Type . . . . . : 1
```

```
Time To Live . . . . . : 44024
```

```
Data Length . . . . . : 4
```

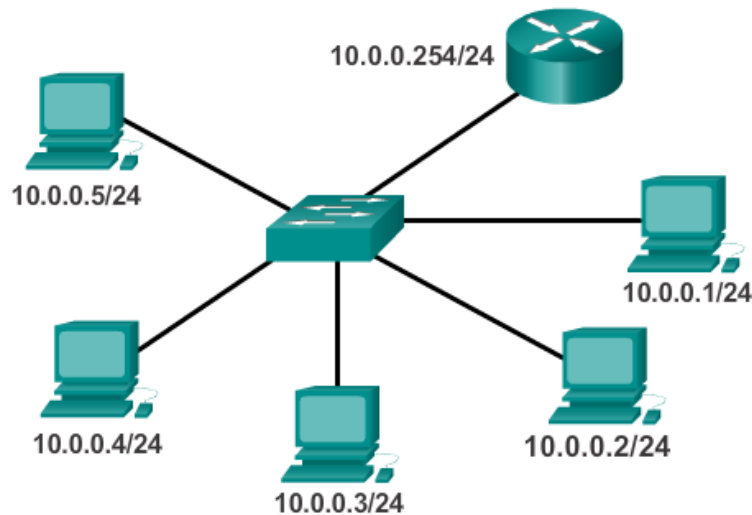
```
Section . . . . . : Answer
```

```
A (Host) Record . . . : 72.163.10.10
```

```
<output omitted>
```

# The arp Command

- The **arp -a** command lists all devices currently in the ARP cache of the host.
- It also includes the IPv4 address, physical address, and the type of addressing (static/dynamic), for each device.
- The cache can be cleared by using the **arp -d** command.



```
c:\>arp -a
```

Internet Address	Physical Address	Type
10.0.0.2	00-08-a3-b6-ce-04	dynamic
10.0.0.3	00-0d-56-09-fb-d1	dynamic
10.0.0.4	00-12-3f-d4-6d-1b	dynamic
10.0.0.254	00-10-7b-e7-fa-ef	dynamic

IP- MAC Address  
Pair

# The show cdp neighbors Command

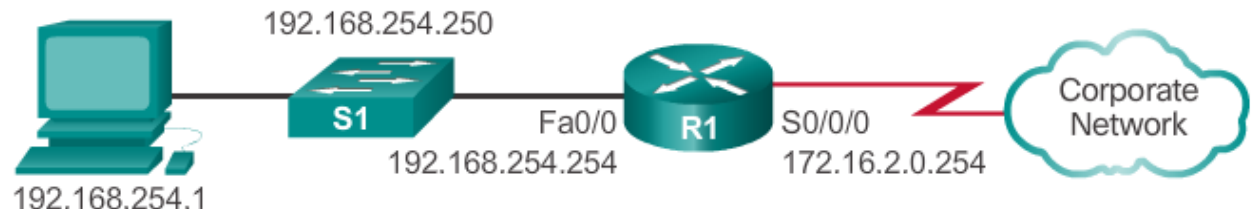
- CDP is a Cisco-proprietary protocol that runs at the data link layer.
- Two or more Cisco network devices can learn about each other even if Layer 3 connectivity does not exist.
- When a Cisco device boots, CDP starts by default.
- CDP exchanges hardware and software device information with its directly connected CDP neighbors.
- CDP provides:
  - Device identifiers
  - Address list
  - Port identifier
  - Capabilities list
  - Platform

## The show cdp neighbors Command (cont.)

- The **show cdp neighbors detail** command reveals the IP address of a neighboring device.
- CDP will reveal the neighbor's IP address regardless of whether you can ping the neighbor.
- The **show cdp neighbors detail** command will help determine if one of the CDP neighbors has an IP configuration error.
- CDP can be a security risk.
- To disable CDP globally, use the global configuration command **no cdp run**.
- To disable CDP on an interface, use the interface command **no cdp enable**.

# The show ip interface brief Command

- The **show ip interface brief** command displays a summary of the key information for all the network interfaces on a router.
- The **show ip interface brief** command can also be used to verify the status of the switch interfaces.



```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.254.254	YES	NVRAM	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
Serial0/0/0	172.16.0.254	YES	NVRAM	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down

```
S1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.254.250	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	up	up



# Section 11.4: Summary

## Chapter Objectives:

- Explain how a small network can scale into a larger network.
- Configure switches and routers with device hardening features to enhance security.
- Use common show commands and utilities to establish a relative performance baseline for the network.
- Explain how a small network of directly connected segments is created, configured, and verifies.

Thank you.



Cisco Networking Academy  
Mind Wide Open