Ch 11: Build a Small Network

Computer Networks Course

BY

Dr. Essam Halim Houssein

Cisco | Networking Academy®
Mind Wide Open™

Chapter 11: Build a Small Network

Up to this point in the course, we have considered the services that a data network can provide to the human network, examined the features of each layer of the OSI model and the operations of TCP/IP protocols, and looked in detail at Ethernet, a universal LAN technology. The next step is to learn how to assemble these elements together in a functioning network that can be maintained.

Did You Notice…?

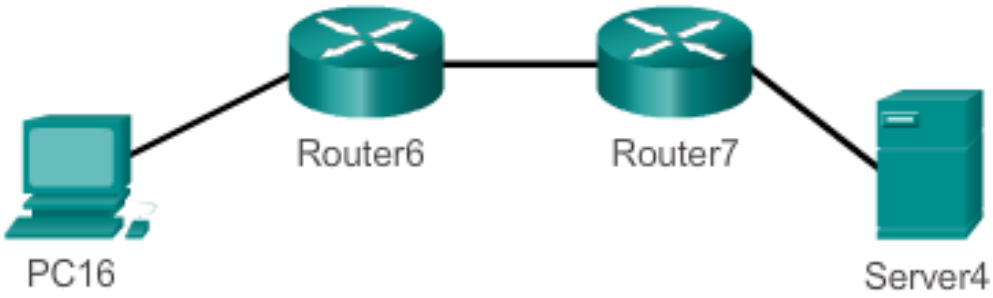
Note: Students can work singularly, in pairs, or the full classroom can complete this activity together.

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.

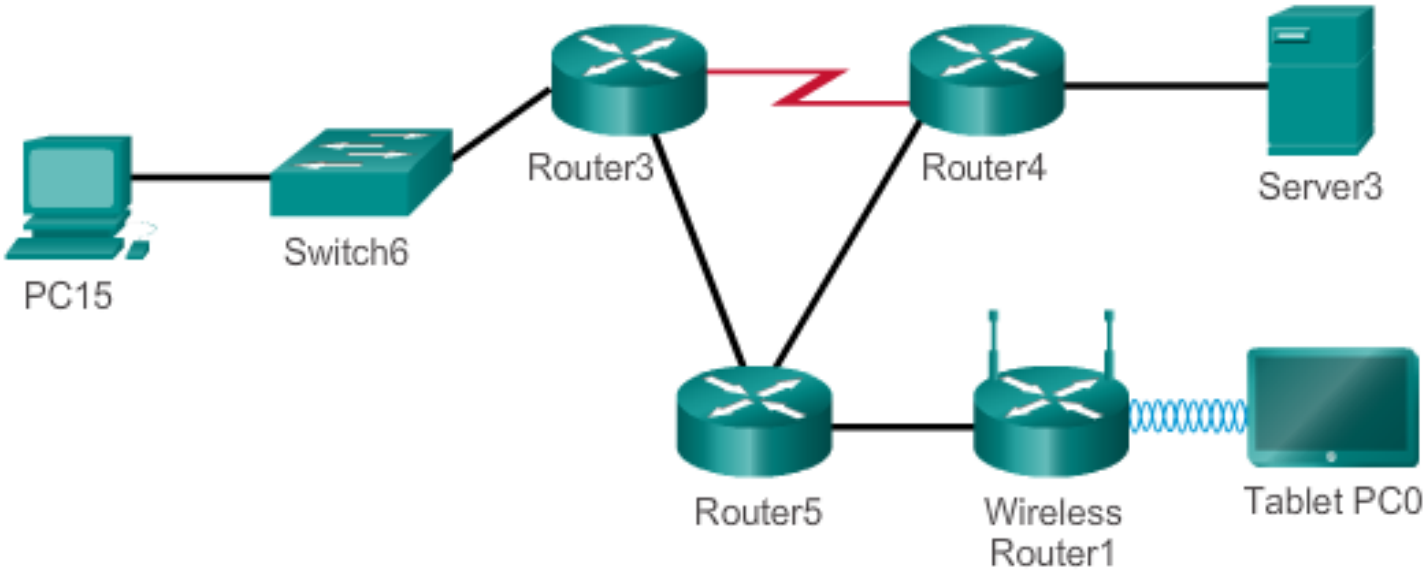
How are the two networks different? Is it just that there are more devices present on Network B than on Network A?

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.

Network A



Network B



Device Selection for a Small Network

In order to meet user requirements, even small networks require planning and design. Planning ensures that all requirements, cost factors, and deployment options are given due consideration.

Cost

The cost of a switch or router is determined by its capacity and features. Other factors that impact the cost are network management capabilities, embedded security technologies, and optional advanced switching technologies.

Speed and Types of Ports/Interfaces

Choosing the number and type of ports on a router or switch is a critical decision. While it is more expensive, choosing Layer 2 devices that can accommodate increased speeds allows the network to evolve without replacing central devices.

Expandability

Networking devices come in both fixed and modular physical configurations. Switches are available with additional ports for high-speed uplinks. Routers can be used to connect different types of networks. Care must be taken to select the appropriate modules and interfaces for the specific media.

Operating System Features and Services

Depending on the version of the operating system, a network device can support certain features and services, such as:

- Security
- Quality of Service (QoS)
- Voice over IP (VoIP)
- Layer 3 switching
- Network Address Translation (NAT)
- Dynamic Host Configuration Protocol (DHCP)

IP Addressing for a Small Network

When implementing a small network, it is necessary to plan the IP addressing space. All hosts within an internetwork must have a unique address. The IP addressing scheme should be planned, documented and maintained based on the type of device receiving the address.

Examples of different types of devices that will factor into the IP design are:

End devices for users

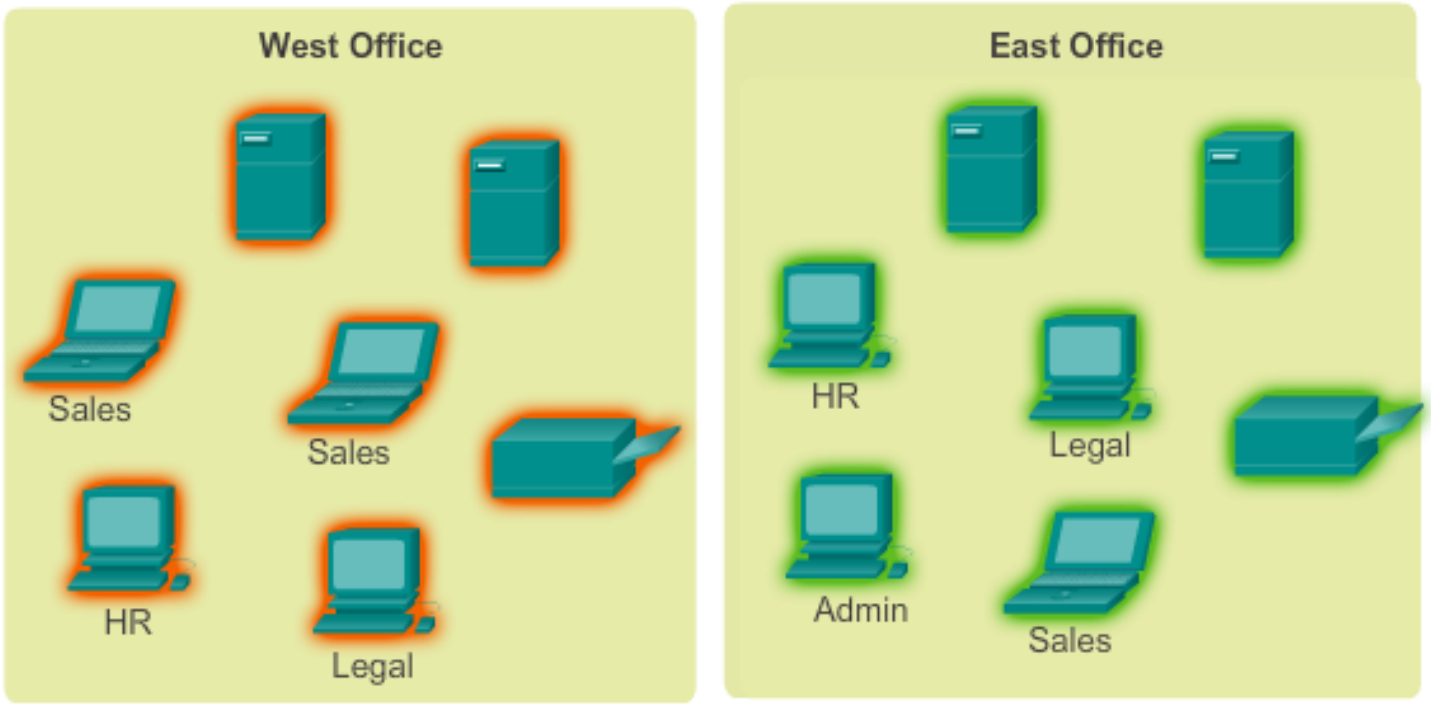
Servers and peripherals

Hosts that are accessible from the Internet

Intermediary devices

Planning and documenting the IP addressing scheme helps the administrator track device types.

IPv4 Address Planning and Assignment



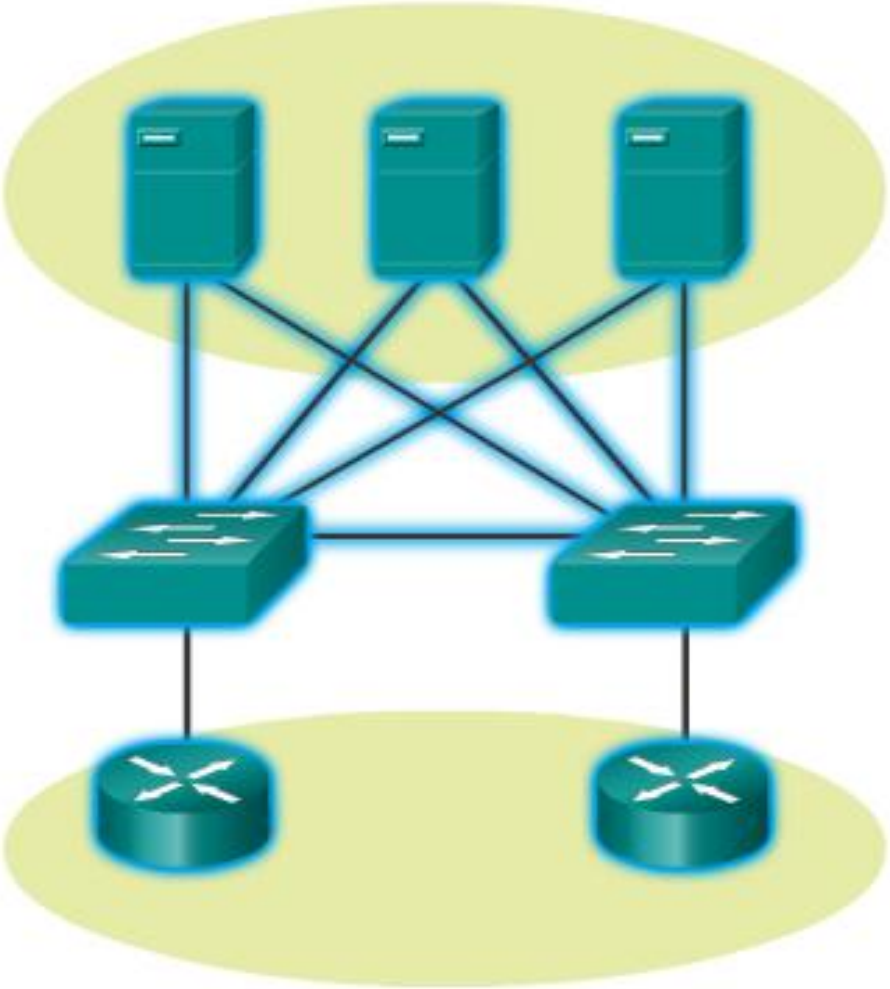
Location

Department	Sales	HR	Legal
Device	Printer	Server	Computer

Redundancy in a Small Network

Another important part of network design is reliability. Even small businesses often rely heavily on their network for business operation. A failure of the network can be very costly. In order to maintain a high degree of reliability, redundancy is required in the network design. Redundancy helps to eliminate single points of failure. There are many ways to accomplish redundancy in a network. Redundancy can be accomplished by installing duplicate equipment, but it can also be accomplished by supplying duplicate network links for critical areas.

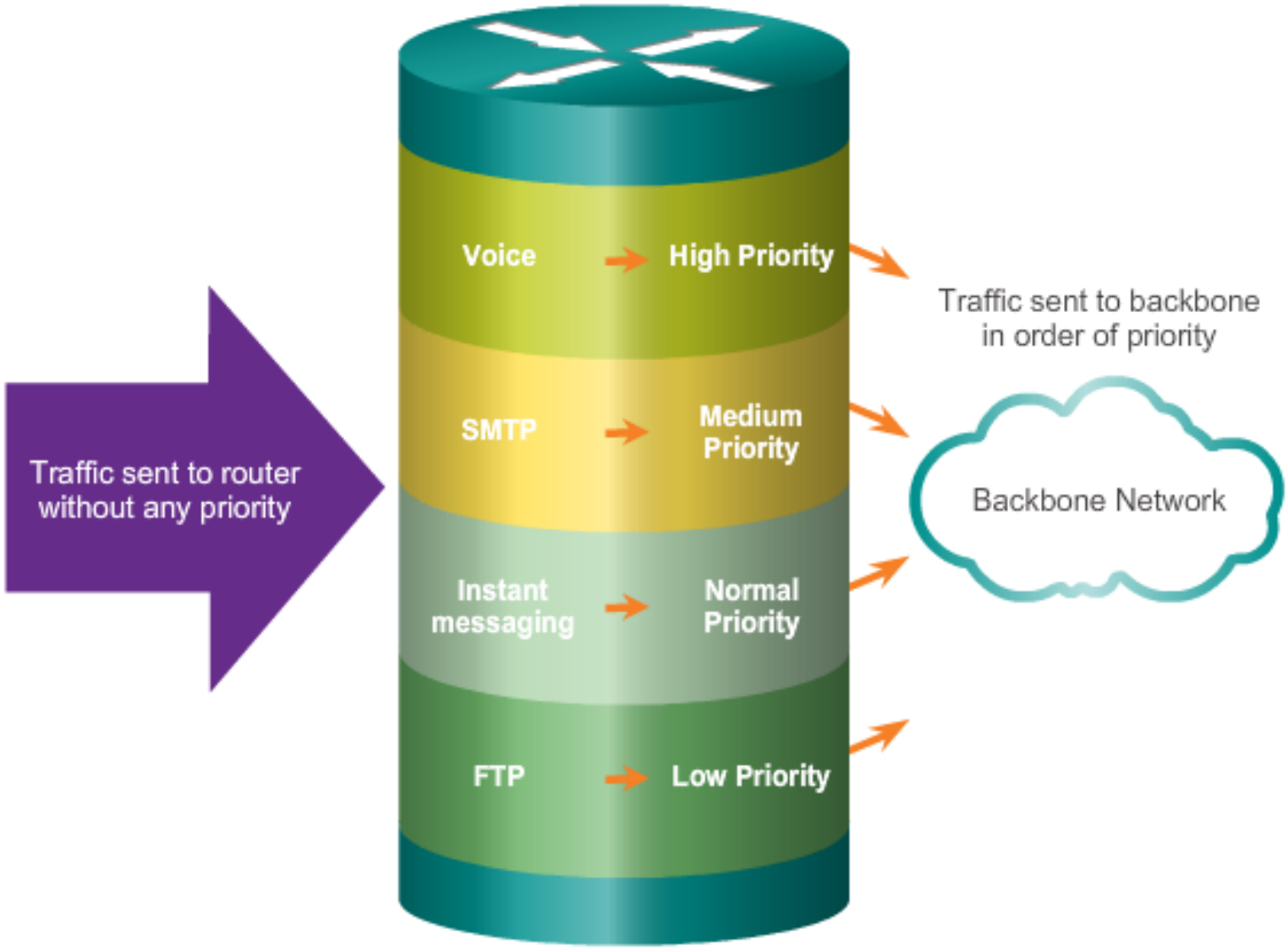
Redundancy to a Server Farm



Traffic Management

The network administrator should consider the various types of traffic and their treatment in the network design. The routers and switches in a small network should be configured to support real-time traffic, such as voice and video, in a distinct manner relative to other data traffic. In fact, a good network design will classify traffic carefully according to priority. In the end, the goal for a good network design, even for a small network, is to enhance the productivity of the employees and minimize network downtime.

Prioritizing Traffic



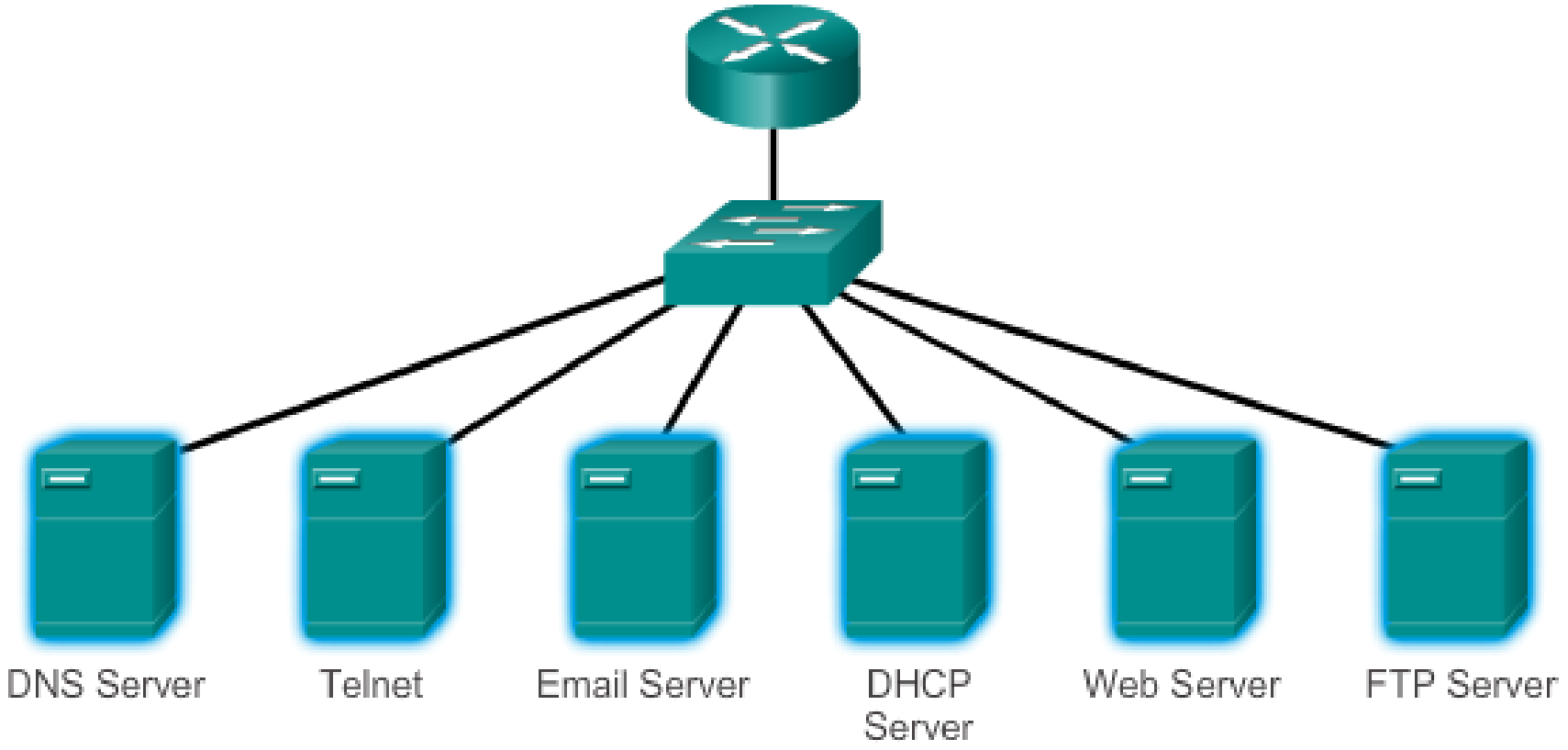
Common Protocols

Network protocols support the applications and services used by employees in a small network.

These network protocols comprise the fundamental toolset of a network professional. Each of these network protocols define:

1. Processes on either end of a communication session
2. Types of messages
3. Syntax of the messages
4. Meaning of informational fields
5. How messages are sent and the expected response
6. Interaction with the next lower layer
7. Many companies have established a policy of using secure versions of these protocols whenever possible. These protocols are HTTPS, SFTP, and SSH.

Network Services



Types of Threats

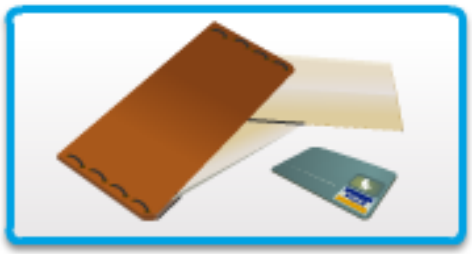
Whether wired or wireless, computer networks are essential to everyday activities. Individuals and organizations alike depend on their computers and networks. Intrusion by an unauthorized person can result in costly network outages and loss of work. Attacks on a network can be devastating and can result in a loss of time and money due to damage or theft of important information or assets.

Intruders can gain access to a network through software vulnerabilities, hardware attacks or through guessing someone's username and password. Intruders who gain access by modifying software or exploiting software vulnerabilities are often called hackers.

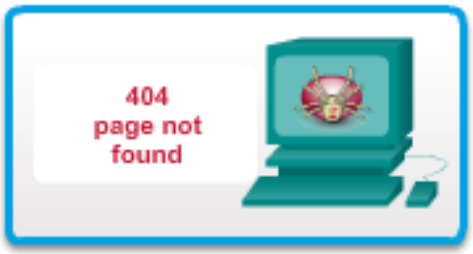
After the hacker gains access to the network, four types of threats may arise, as shown in the figure. Click each image for more information.

Information Theft

Data Loss and Manipulation



Identity Theft



Disruption of Service

Information Theft

This is breaking into a computer to obtain confidential information. Information can be used or sold for various purposes. Example: stealing an organization's proprietary information, such as research and development information.

Physical Security

An equally important vulnerability is the physical security of devices. An attacker can deny the use of network resources if those resources can be physically compromised.

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)

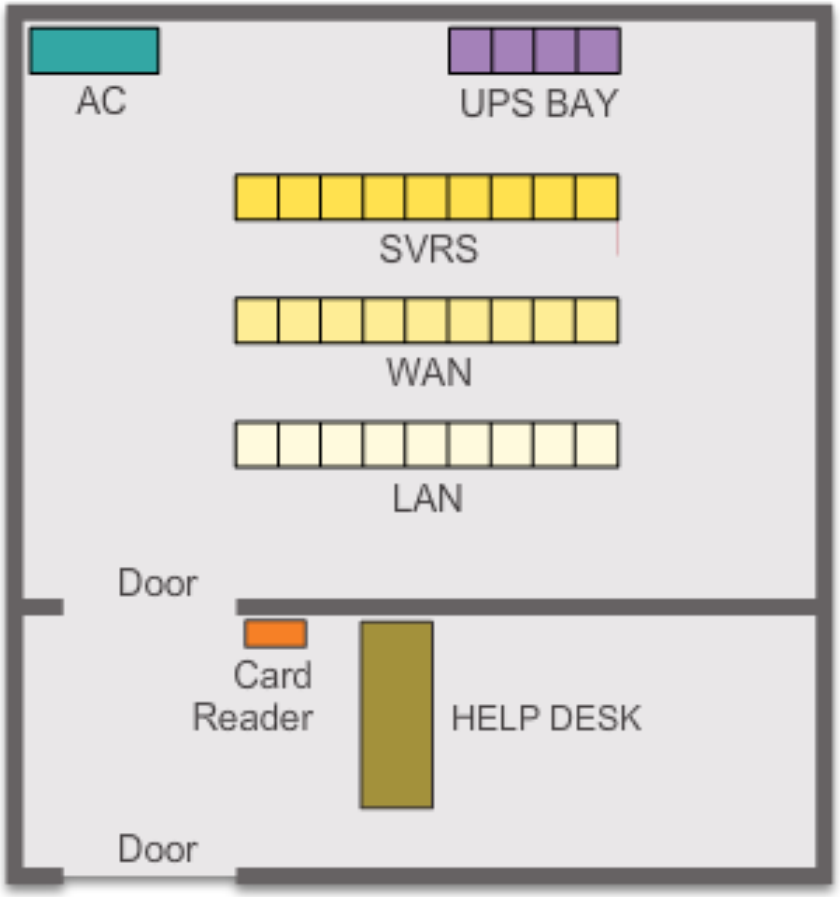
Electrical threats - voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss

Maintenance threats - poor handling of key electrical components (electrostatic discharge), lack of critical spare parts, poor cabling, and poor labeling.

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

Types of Vulnerabilities

Vulnerability is the degree of weakness which is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices. Typically, the network devices under attack are the endpoints, such as servers and desktop computers.

There are three primary vulnerabilities or weaknesses:

Technological,

Configuration,

Security policy,

All three of these vulnerabilities or weaknesses can lead to various attacks, including malicious code attacks and network attacks.

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.

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.

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.

Types of Malware

Malware or malicious code (malcode) is short for malicious software. It is code or software that is specifically designed to damage, disrupt, steal, or inflict “bad” or illegitimate action on data, hosts, or networks. Viruses, worms, and Trojan horses are types of malware.

Viruses

A computer virus is a type of malware that propagates by inserting a copy of itself into, and becoming part of, another program. It spreads from one computer to another, leaving infections as it travels. Viruses can range in severity from causing mildly annoying effects to damaging data or software and causing denial-of-service (DoS) conditions. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program. When the host code is executed, the viral code is executed as well. Normally, the host program keeps functioning after it is infected by the virus. However, some viruses overwrite other programs with copies of themselves, which destroys the host program altogether. Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected e-mail attachments.

Worms

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. A worm does not need to attach to a program to infect a host and enter a computer through a vulnerability in the system. Worms take advantage of system features to travel through the network unaided.

Trojan Horses

A Trojan horse is another type of malware named after the wooden horse the Greeks used to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojan horses are also known to create back doors to give malicious users access to the system.

Unlike viruses and worms, Trojan horses do not reproduce by infecting other files, nor do they self-replicate. Trojan horses must spread through user interaction such as opening an e-mail attachment or downloading and running a file from the Internet.

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:

Access attacks - the unauthorized manipulation of data, system access, or user privileges

Denial of service - the disabling or corruption of networks, systems, or services

For reconnaissance attacks, external attackers can use Internet tools, such as the nslookup and whois utilities, to easily determine the IP address space assigned to a given corporation or entity. After the IP address space is determined, an attacker can then ping the publicly available IP addresses to identify the addresses that are active. To help automate this step, an attacker may use a ping sweep tool, such as *fping* or *gping*, which systematically pings all network addresses in a given range or subnet. This is similar to going through a section of a telephone book and calling each number to see who answers.

Click each type of reconnaissance attack tool to see an animation of the attack.

Access Attacks

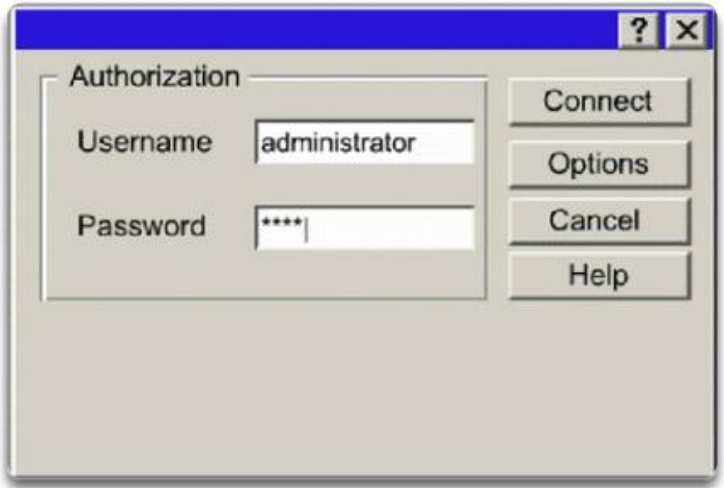
Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information. An access attack allows an individual to gain unauthorized access to information that they have no right to view. Access attacks can be classified into four types:

1. Password attacks
2. Trust Exploitation
3. Port Redirection
4. Man-in-the-Middle

Password Attack

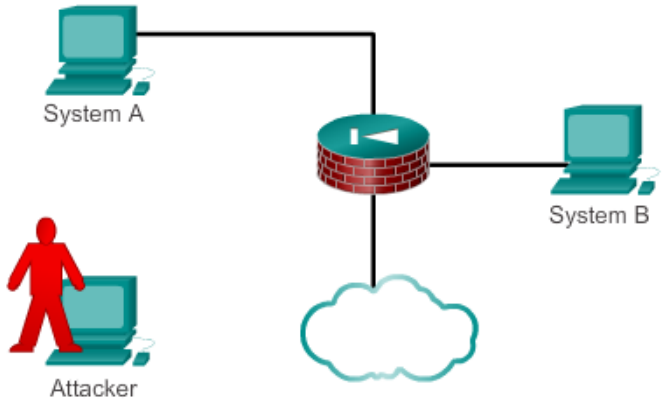
Attackers can implement password attacks using several different methods:

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

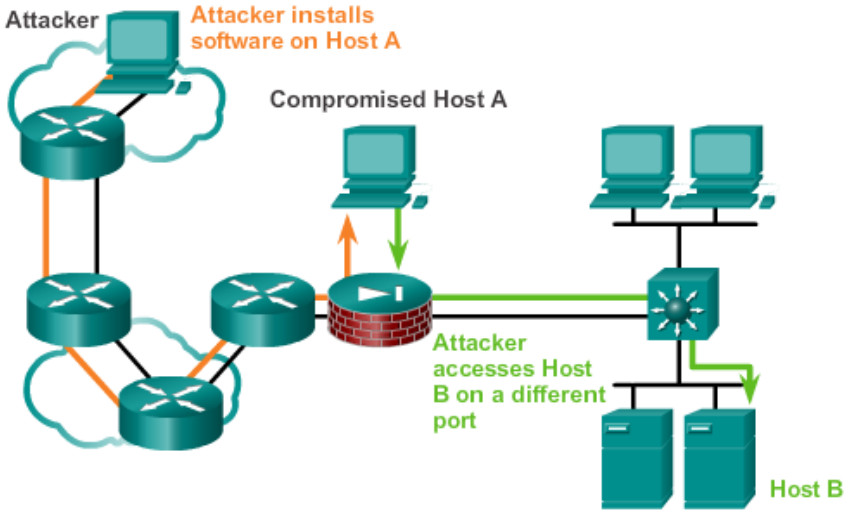


Trust Exploitation

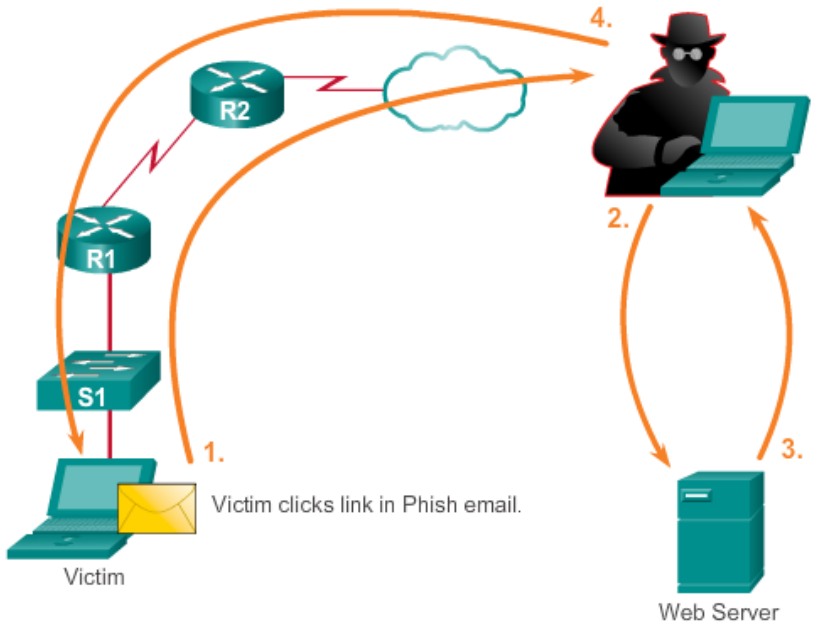
Network OS	Trust Models
Windows	Domains Active Directory (AD)
Linux and UNIX	Network File System (NFS) Network Information Service Plus (NIS+)



Port Redirection



Man-in-the-Middle



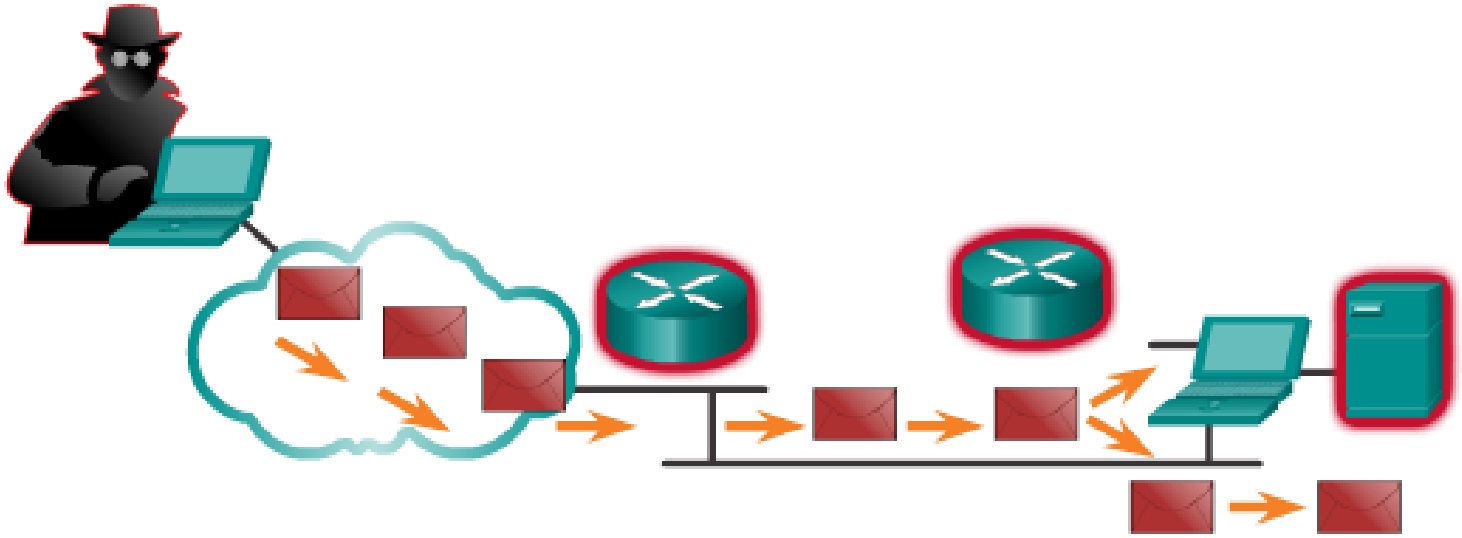
Denial of Service Attacks

Denial of Service (DoS) attacks are the most publicized form of attack and also among the most difficult to eliminate. Even within the attacker community, DoS attacks are regarded as trivial and considered bad form because they require so little effort to execute. But because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators.

DoS attacks take many forms. Ultimately, they prevent authorized people from using a service by consuming system resources.

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



Authentication, Authorization, and Accounting

Authentication, authorization, and accounting (AAA, or “triple A”) network security services provide the primary framework to set up access control on a network device. AAA is a way to control who is permitted to access a network (authenticate), what they can do while they are there (authorize), and what actions they perform while accessing the network (accounting).

The concept of AAA is similar to the use of a credit card. The credit card identifies who can use it, how much that user can spend, and keeps account of what items the user spent money on.

The AAA Concept is Similar to the Use of a Credit Card

Authentication
Who are you?

Authorization
How much can you spend?

Accounting
What did you spend it on?

Account Number	Statement Closing Date	Current Amount Due
1234-567-890	01-31-01	$278.50

MAIL PAYMENT TO:
THE BANK
132 VINE STREET
ANYTOWN, USA 67500-0010

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA 99000-1234

872919345 00178255000000003

Detach here and return upper portion with check or money order. Do not staple or fold.

rd Account

THE BANK

Statement Closing Date
01-31-01

ement Date:	02-01-01	Payment Due Date:	03-01-01
ng Date:	01-31-01		
Credit Limit	$1,500.00	Credit Available:	$1221.50
New Balance:	$278.50	Minimum Payment Due:	$20.00

Account Summary

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	$278.50

Reference Number	Sold	Posted	Activity Since Last Statement		Amount
43210987	01-03	01-13	Payment, Thank You		-$74.25
01234567	01-12	01-13	Wings 'N' Things	Anytown, USA	$25.25
78901234	01-14	01-17	Record Release	Anytown, USA	$40.00
45678901	01-14	01-17	Sports Stadium	Anytown, USA	$75.25
3210987	01-22	01-23	Tie Tack	Anytown, USA	$20.75
76543210	01-29	01-30	Electronic World	Anytown, USA	$89.25
23456678		01-30	Transaction Fees		$3.00
34567890		01-01	Annual Fee		$25.00

PAGE 1 OF 1

Firewalls

A firewall is one of the most effective security tools available for protecting users from external threats. Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access. Host-based firewalls or personal firewalls are installed on end systems. Firewall products use various techniques for determining what is permitted or denied access to a network. These techniques are:

Packet filtering - Prevents or allows access based on IP or MAC addresses

Application filtering - Prevents or allows access by specific application types based on port numbers

URL filtering - Prevents or allows access to websites based on specific URLs or keywords

Stateful packet inspection (SPI) - Incoming packets must be legitimate responses to requests from internal hosts. Unsolicited packets are blocked unless permitted specifically. SPI can also include the capability to recognize and filter out specific types of attacks, such as denial of service (DoS)

Firewall products may support one or more of these filtering capabilities.

Cisco Security Appliances

Server-Based Firewall

Cisco WRP500 Wireless Broadband Router

Personal Firewall

Cisco Security Appliances

Dedicated firewall devices are specialized computers that do not have peripherals or hard drives. Appliance-based firewalls can inspect traffic faster and are less prone to failure.

Endpoint Security

An endpoint, or host, is an individual computer system or device that acts as a network client. Common endpoints, as shown in the figure, are laptops, desktops, servers, smartphones, and tablets. Securing endpoint devices is one of the most challenging jobs of a network administrator because it involves human nature. A company must have well-documented policies in place and employees must be aware of these rules. 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.

Passwords

To protect network devices, it is important to use strong passwords. Here are standard guidelines to follow:

Use a password length of at least 8 characters, preferably 10 or more characters. A longer password is a better password.

Make passwords complex. Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces, if allowed.

Avoid passwords based on repetition, common dictionary words, letter or number sequences, usernames, relative or pet names, biographical information, such as birthdates, ID numbers, ancestor names, or other easily identifiable pieces of information.

Do not write passwords down and leave them in obvious places such as on the desk or monitor.

Basic Security Practices

Additional Password Security

Strong passwords are only as useful as they are secret. There are several steps that can be taken to help ensure that passwords remain secret.

Using the global configuration command **service password-encryption** prevents unauthorized individuals from viewing passwords in plain text in the configuration file, as shown in the figure. This command causes the encryption of all passwords that are unencrypted.

Additionally, to ensure that all configured passwords are a minimum of a specified length, use the **security passwords min-length**c ommand in global configuration mode.

Another way hackers learn passwords is simply by brute-force attacks, trying multiple passwords until one works. It is possible to prevent this type of attack by blocking login

Attempts to the device if a set number of failures occur within a specific amount of time.

Router(config)# **login block-for 120 attempts 3 within 60**

This command will block login attempts for 120 seconds if there are three failed login attempts within 60 seconds.

Exec Timeout

Another recommendation is setting executive timeouts. By setting the exec timeout, you are telling the Cisco device to automatically disconnect users on a line after they have been idle for the duration of the exec timeout value. Exec timeouts can be configured on console, VTY, and aux ports using the **exec-timeout** command in line configuration mode.

Router(config)# **line vty 0 4**

Router(config-line)# **exec-timeout 10**

This command configures the device to disconnect idle users after 10 minutes.

```
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-line)#exec-timeout 10
Router(config-line)#end
Router#show running-config
-more-
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 exec-timeout 10
 login
```

Enable SSH

Telnet is not secure. Data contained within a Telnet packet is transmitted unencrypted. For this reason, it is highly recommended to enable SSH on devices for secure remote access. It is possible to configure a Cisco device to support SSH using four steps, as shown in the figure.

Step 1. Ensure that the router has a unique hostname, and then configure the IP domain name of the network using the **ip domain-name** command in global configuration mode.

Step 2. One-way secret keys must be generated for a router to encrypt SSH traffic. To generate the SSH key, use the **crypto key generate rsa general-keys** command in global configuration mode. The specific meaning of the various parts of this command are complex and out of scope for this course. Just note that the modulus determines the size of the key and can be configured from 360 bits to 2048 bits. The larger the modulus, the more secure the key, but the longer it takes to encrypt and decrypt information. The minimum recommended modulus length is 1024 bits.

Step 3. Create a local database username entry using the **username** global configuration command.

Step 4. Enable inbound SSH sessions using the line vty commands **login local** and **transport input ssh**.

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.

Router File Systems

The Cisco IOS File System (IFS) allows the administrator to navigate to different directories and list the files in a directory, and to create subdirectories in flash memory or on a disk. The directories available depend on the device.

The **show file systems** command, which lists all of the available file systems on a Cisco 1941 router. This command provides useful information such as the amount of available and free memory, the type of file system, and its permissions. Permissions include read only (ro), write only (wo), and read and write (rw), shown in the Flags column of the command output.

Although there are several file systems listed, of interest to us will be the tftp, flash, and nvram file systems.

The Flash File System

The **dir** command. Because flash is the default file system, the **dir** command lists the contents of flash. Several files are located in flash, but of specific interest is the last listing. This is the name of the current Cisco IOS file image that is running in RAM.

The NVRAM File System

To view the contents of NVRAM, you must change the current default file system using the **cd** (change directory) command. The **pwd** (present working directory) command verifies that we are viewing the NVRAM directory. Finally, the **dir** (directory) command lists the contents of NVRAM. Although there are several configuration files listed, of specific interest is the startup-configuration file.

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     nvram     rw   nvram:
             -             -    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)
```

NVRAM

```
Router# cd nvram:
Router# pwd
nvram:/
Router# dir
Directory of nvram:/

  253  -rw-        1156      <no date>  startup-config
  254  ----           5      <no date>  private-config
  255  -rw-        1156      <no date>  underlying-config
    1  -rw-        2945      <no date>  cwmp_inventory
    4  ----          58      <no date>  persistent-data
    5  -rw-          17      <no date>  ecfm_ieee_mib
    6  -rw-         559      <no date>  IOS-Self-Sig#1.cer

262136 bytes total (254779 bytes free)
```

Switch File Systems

With the Cisco 2960 switch flash file system, you can copy configuration files, and archive (upload and download) software images.

The command to view the file systems on a Catalyst switch is the same as on a Cisco router: **show file systems**.

Backing Up and Restoring Using Text Files

Backup Configurations with Text Capture (Tera Term)

Configuration files can be saved/archived to a text file using Tera Term.

As shown in the figure, 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. After capture has been started, execute the **show running-config** or **show startup-config** command at the privileged EXEC prompt. 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 Text Configurations

A configuration can be copied from a file to a device. When copied from a text file and pasted into a terminal window, the IOS executes each line of the configuration text as a command. This means that the file will require editing to ensure that encrypted passwords are in plain text and that non-command text such as "--More--" and IOS messages are removed. This process is discussed in the lab.

Further, at the CLI, the device must be set at the global configuration mode to receive the commands from the text file being pasted into the terminal window.

When using Tera Term, the steps are:

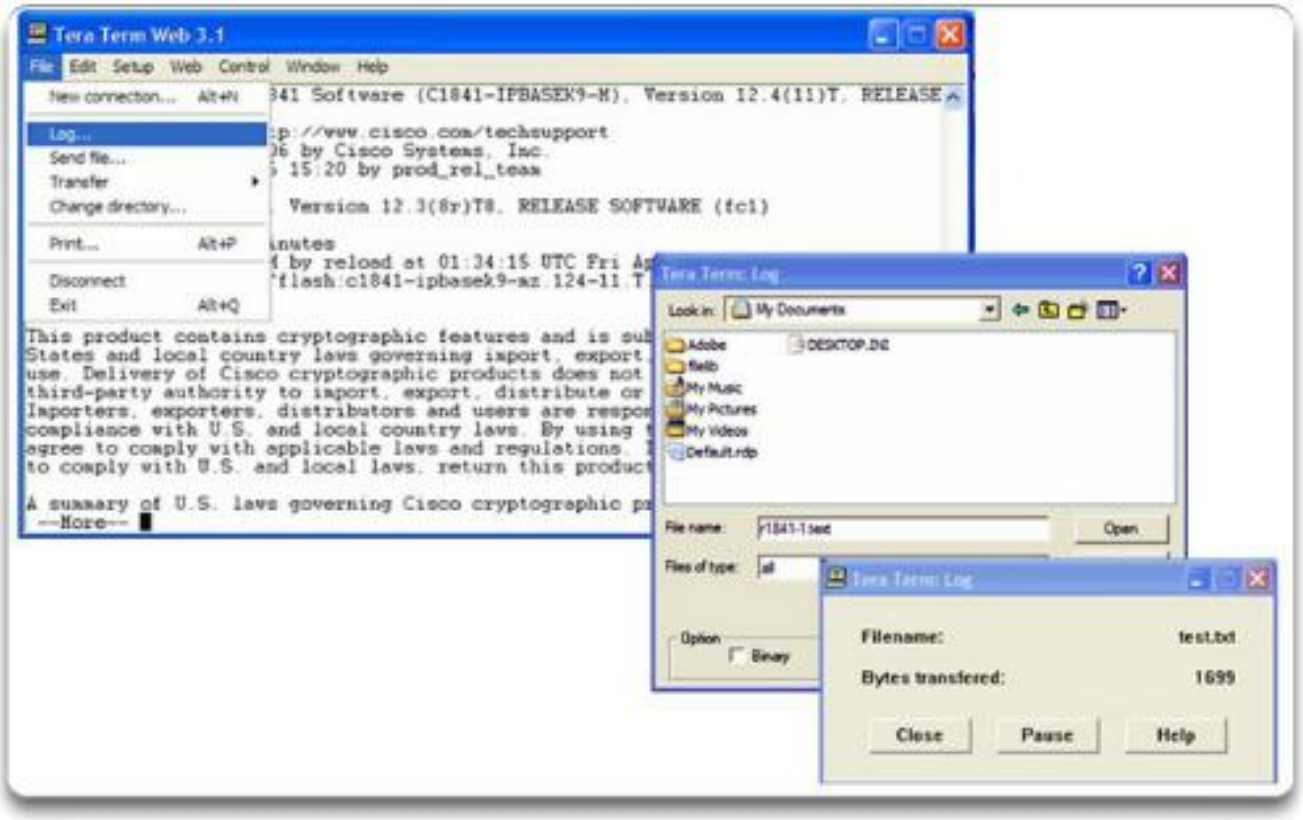
Step 1. On the File menu, click **Send** file.

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. This is a convenient method for manually configuring a router.

Saving to a Text File in Tera Term



1. Start the log process.
2. Issue a **`show running-config`** command.
3. Close the log.

Backing up and Restoring TFTP

Backup Configurations with TFTP

Copies of configuration files should be stored as backup files in the event of a problem. Configuration files can be stored on a Trivial File Transfer Protocol (TFTP) server or a USB drive. A configuration file should also be included in the network documentation.

To save the running configuration or the startup configuration to a TFTP server, use either the**copy running-config tftp** or **copy startup-config tftp** command as shown in the figure. Follow these steps to backup the running configuration to a TFTP server:

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.

Restoring Configurations with TFTP

To restore the running configuration or the startup configuration from a TFTP server, use either the **copy tftp running-config** or **copy tftp startup-config** command. Use these steps to restore the running configuration from a TFTP server:

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.

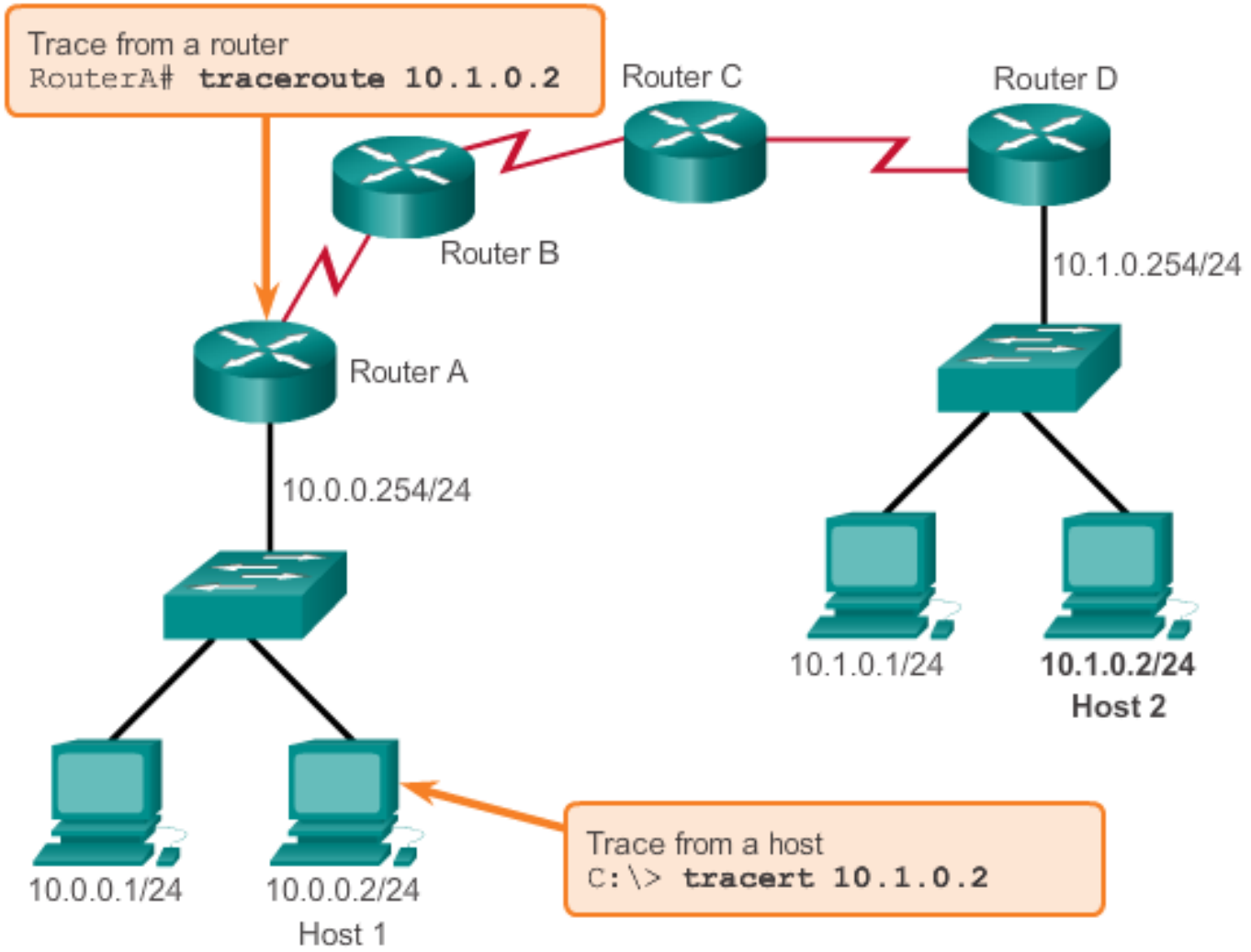
Interpreting Trace Messages

When performing the trace from a Windows computer, use **tracert**.

When performing the trace from a router CLI, **use traceroute**.

The tracert command entered on Host 1 to trace the route to Host 2. The only successful response was from the gateway on Router A. Trace requests to the next hop timed out, meaning that the next hop router did not respond. The trace results indicate that there is either a failure in the internetwork beyond the LAN or that these routers have been configured not to respond to echo requests used in the trace.

Testing the Path to a Remote Host



Tracing the Route from Host 1 to Host 2

```
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:\>
```

Common show Commands Revisited

The Cisco IOS CLI **show** commands display relevant information about the configuration and operation of the device.

Network technicians use **show** commands extensively for viewing configuration files, checking the status of device interfaces and processes, and verifying the device operational status. The **show** commands are available whether the device was configured using the CLI or Cisco Configuration Professional.

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

Show running-config

```
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$dvdpVM6zV10E6tSyLdkR5/
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
```

Show interfaces

```
R1# show interfaces
<Output omitted>
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.5325.256e
  (bia 001b.5325.256e)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:17, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes);
  Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     196 packets input, 31850 bytes
     Received 181 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
```

Show arp

```
R1# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.17.0.1             -   001b.5325.256e  ARPA
FastEthernet0/0
Internet  172.17.0.2            12   000b.db04.a5cd  ARPA
FastEthernet0/0
```

Show ip route

```
R1# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
```

Show protocols

```
R1# show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24
FastEthernet0/1 is administratively down, line protocol is down
FastEthernet0/1/0 is up, line protocol is down
FastEthernet0/1/1 is up, line protocol is down
FastEthernet0/1/2 is up, line protocol is down
FastEthernet0/1/3 is up, line protocol is down
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.2.1/24
Serial0/0/1 is administratively down, line protocol is down
Vlan1 is up, line protocol is down
```

Show version

```
R1# show version
<Output omitted>
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M),
Version 12.4(10b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
R1 uptime is 43 minutes
System returned to ROM by reload at 22:05:12 UTC Sat Jan 5 2008
System image file is "flash:c1841-advipservicesk9-mz.124-10b.bin"

Cisco 1841 (revision 6.0) with 174080K/22528K bytes of memory.
Processor board ID FTX1111W0QF
6 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

```
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
```

The ipconfig Command

The IP address of the default gateway of a host can be viewed by issuing the **ipconfig** command at the command line of a Windows computer.

The **ipconfig /all** command to view the MAC address as well as a number of details regarding the Layer 3 addressing of the device.

The DNS Client service on Windows PCs optimizes the performance of DNS name resolution by storing previously resolved names in memory, as well.

The **ipconfig /displaydns** command displays all of the cached DNS entries on a Windows computer system.

ipconfig

```
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

Sample **ipconfig** output showing default gateway address

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:\>
```

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>
```

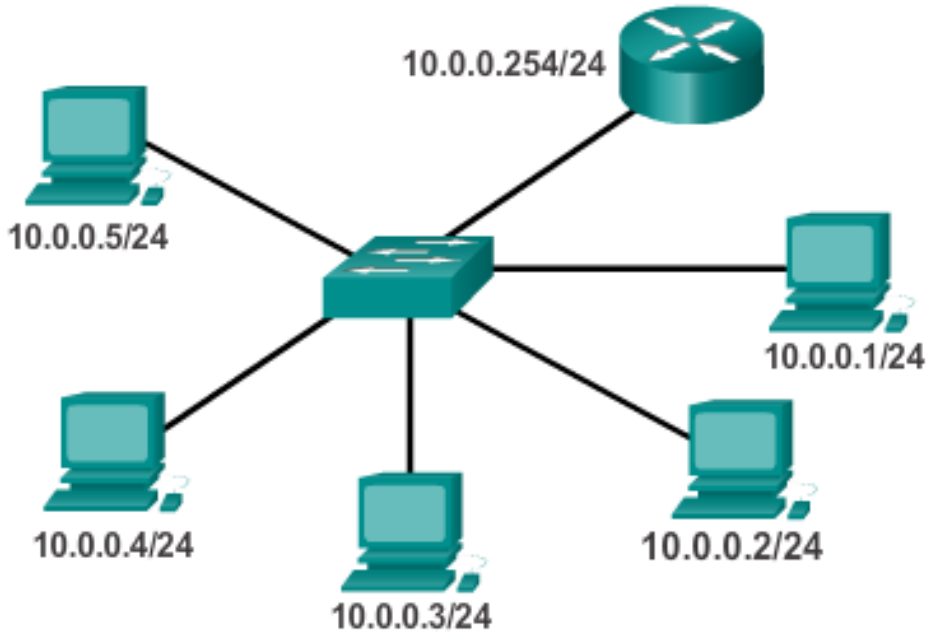
The arp Command

The **arp** command is executed from the Windows command prompt, as shown in the figure. The **arp –a** command lists all devices currently in the ARP cache of the host, which 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 in the event the network administrator wants to repopulate the cache with updated information.

Note: The ARP cache only contains information from devices that have been recently accessed. To ensure that the ARP cache is populated, ping a device so that it will have an entry in the ARP table.

Learning About the Nodes on the Network




```
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

Summary

In order to meet user requirements, even small networks require planning and design. Planning ensures that all requirements, cost factors, and deployment options are given due consideration. An important part of network design is reliability, scalability, and availability.

Supporting and growing a small network requires being familiar with the protocols and network applications running over the network. Protocol analyzers enable a network professional to quickly compile statistical information about traffic flows on a network. Information gathered by the protocol analyzer is evaluated based on the source and destination of the traffic as well as the type of traffic being sent. This analysis can be used by a network technician to make decisions on how to manage the traffic more efficiently. Common network protocols include DNS, Telnet, SMTP, POP, DHCP, HTTP, and FTP.

It is a necessity to consider security threats and vulnerabilities when planning a network implementation. All network devices must be secured. This includes routers, switches, end-user devices, and even security devices. Networks need to be protected from malicious software such as viruses, Trojan horses, and worms. Antivirus software can detect most viruses and many Trojan horse applications and prevent them from spreading in the network. The most effective way to mitigate a worm attack is to download security updates from the operating system vendor and patch all vulnerable systems.

Networks must also be protected from network attacks. Network attacks can be classified into three major categories: reconnaissance, access attacks, and denial of service. There are several ways to protect a network from attacks.

Authentication, authorization, and accounting (AAA, or “triple A”) network security services provide the primary framework to set up access control on a network device. AAA is a way to control who is permitted to access a network (authenticate), what they can do while they are there (authorize), and to watch the actions they perform while accessing the network (accounting).

A firewall is one of the most effective security tools available for protecting internal network users from external threats. A firewall resides between two or more networks and controls the traffic between them and also helps prevent unauthorized access.

To protect network devices, it is important to use strong passwords. Also, when accessing network devices remotely, it is highly recommended to enable SSH instead of the unsecured telnet.

After the network has been implemented, a network administrator must be able to monitor and maintain network connectivity. There are several commands available toward this end. For testing network connectivity to local and remote destinations, commands such as **ping**,**telnet**, and **traceroute** are commonly used.

On Cisco IOS devices, the **show version**command can be used to verify and troubleshoot some of the basic hardware and software components used during the boot process. To view information for all network interfaces on a router, the **show ip interface**command is used. The **show ip interface brief**can also be used to view a more abbreviated output than the **show ip interface** command. Cisco Discovery Protocol (CDP) is a Cisco-proprietary protocol that runs at the data link layer. Because CDP operates at the data link layer, two or more Cisco network devices, such as routers that support different network layer protocols, can learn about each other even if Layer 3 connectivity does not exist.

Cisco IOS configuration files such as startup-config or running-config should be archived. These files can be saved to a text file or stored on a TFTP server. Some models of routers also have a USB port, and a file can be backed up to a USB drive. If needed, these files can be copied to the router and or switch from the TFTP server or USB drive.