

Chapter 11: Build a Small Network

CCNA Routing and Switching

Introduction to Networks v6.0



Chapter 11 - Sections & Objectives

- 11.1 Network Design
 - Explain how a small network of directly connected segments is created, configured, and verified.
 - 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.
- 11.2 Network Security
 - Configure switches and routers with device hardening features to enhance security.
 - Explain why basic 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.

Chapter 11 - Sections & Objectives (Cont.)

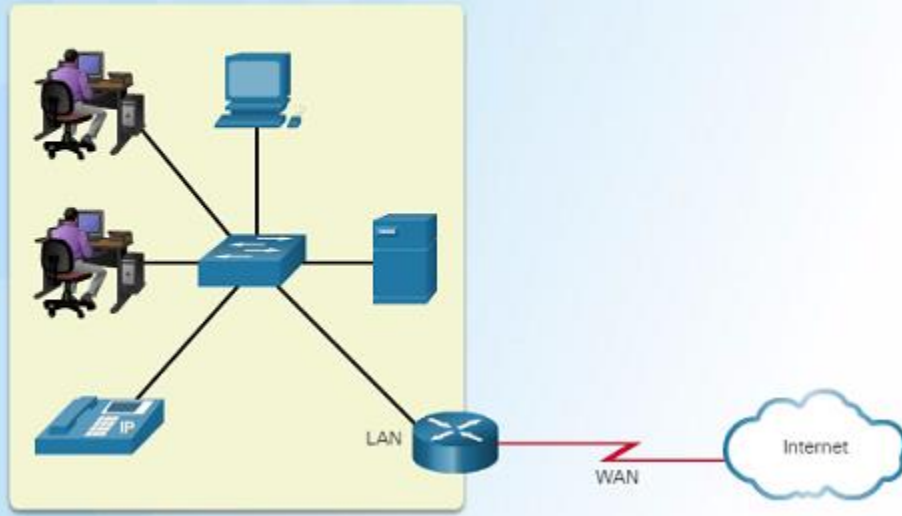
- 11.3 Basic Network Performance
 - Use common show commands and utilities to establish relative performance baseline for the network.
 - Use the output of the ping command to establish relative network performance.
 - Use the output of the traceroute command to establish relative network performance.
 - Use show commands to verify the configuration and status of network devices.
 - Use host and IOS commands to acquire information about the devices in a network.
- 11.4 Network Troubleshooting
 - Troubleshoot a network.
 - Describe common network troubleshooting methodologies.
 - Troubleshoot cable issues and interface issues.
 - Troubleshoot issues with devices in the network.

11.1 Network Design

Devices in a Small Network

Small Network Topologies

Typical Small Business Network



- The majority of businesses are small and typically require small networks consisting of a single router with one or more switches and possibly one or more wireless access points. The business might also have IP phones.
 - For the Internet connection, the router will normally have a single WAN connection using DSL, cable, or an Ethernet connection.
- Managing a small network is similar to managing a large network:
 - Maintenance and troubleshooting of existing equipment
 - Securing devices and information on the network

Device Selection for a Small Network

Factors to Consider in Choosing a Device



Cost



Ports



Speed



Expandable/Modular



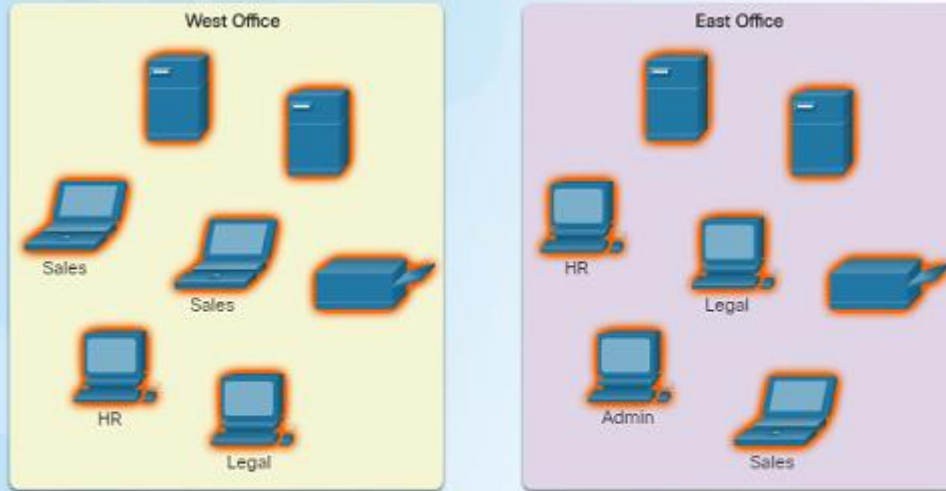
Manageable

- Regardless of the size, all networks require planning and design to ensure that all requirements, cost factors, and deployment options are considered:
 - Cost – The cost of a switch or router is determined by its capacity and features.
 - Speed and Types of Ports/Interfaces – Choosing the number and types of ports on a router or switch is an important decision.
 - Expandability – Networking devices come in both fixed and modular physical configurations for expandability and flexibility.
 - Operating System Features and Services – Features and services should be considered including: security, QoS, VoIP, Layer 3 switching, NAT and DHCP.

Devices in a Small Network

IP Addressing for a Small Network

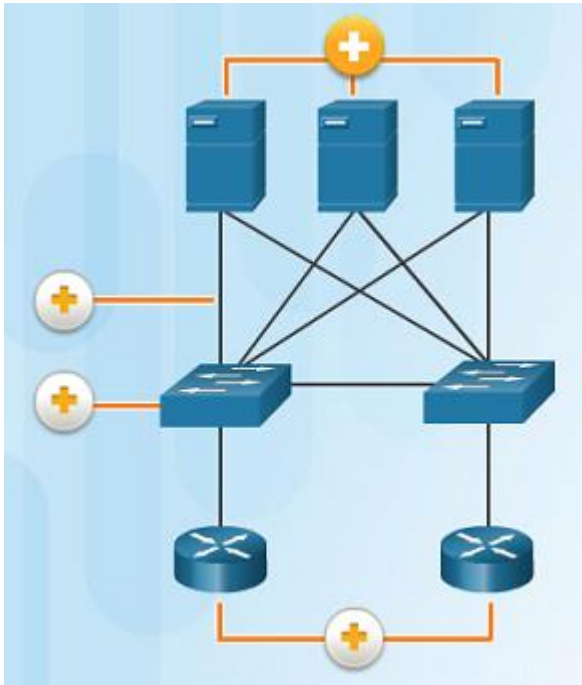
IPv4 Address Planning and Assignment



	Location		
Department	Sales	HR	Legal
Device	Printer	Server	Computer

- IP addressing space must be planned when implementing a small network.
- All hosts within an internetwork must have a unique address.
- Different types of devices will factor into the IP design including:
 - End devices for users
 - Servers and peripherals
 - Hosts that are accessible from the Internet
 - Intermediary devices
- Planning and documenting the IP addressing scheme helps administrators track device types. For example, if all servers are assigned a host address in the range of 50-100, it will be easier to identify server traffic by their IP address.

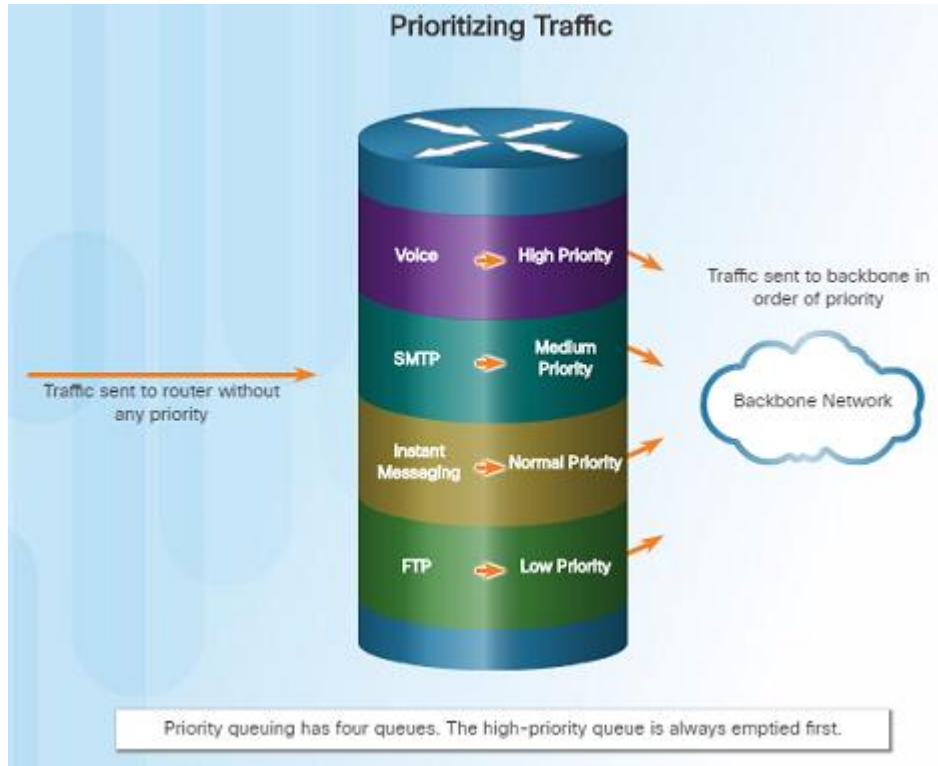
Redundancy in a Small Network



- Reliability is another important element of network design - a network failure can be costly
- The figure to the left represents a Data Center network.
- There are 4 types of redundancy in this figure:
 - Redundant servers
 - Redundant links
 - Redundant switches
 - Redundant routers
- A server, link, switch, or router could fail and the network would continue to function.

Devices in a Small Network

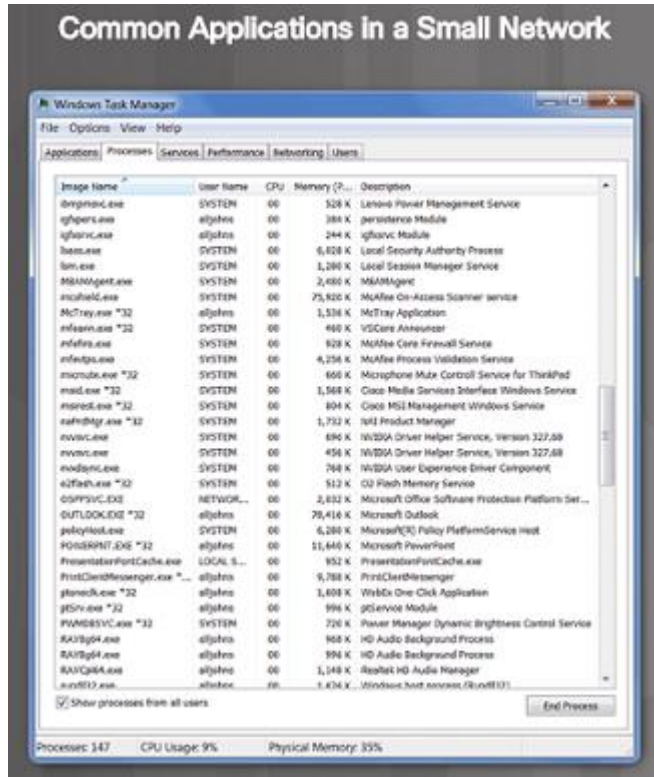
Traffic Management



- The types of traffic and how they should be handled should be considered and prioritized in the network design.
- Routers and Switches in a small network should be configured to support real-time traffic such as voice and video. For example:
 - Voice → High Priority
 - Video → High Priority
 - SMTP → Medium Priority
 - Instant Messaging → Normal Priority
 - FTP → Low Priority
- Network traffic should be classified according to priority in order to enhance productivity of employees and minimize network downtime.

Small Network Applications and Protocols

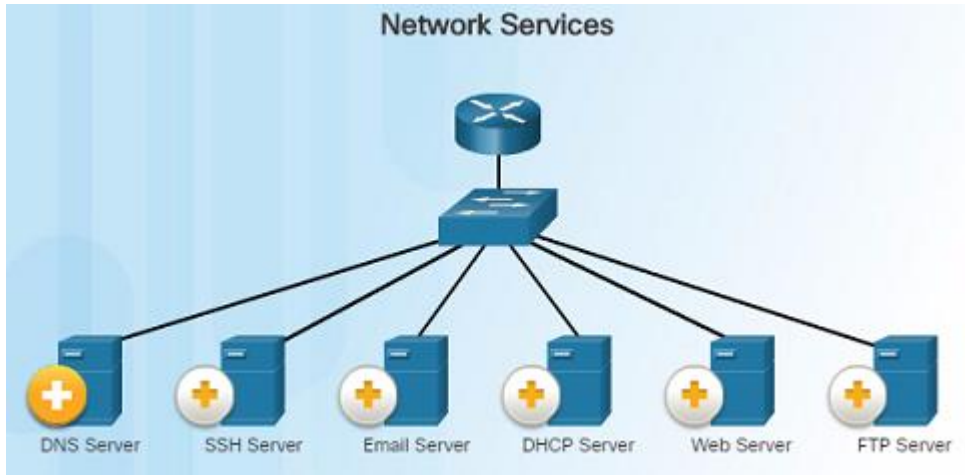
Common Applications



- There are two forms of software programs or processes that provide access to the network:
 - Network Applications – The software programs used to communicate over the network. Some end-user applications are network aware, and are able to communicate directly with the lower layers of the protocol stack. Examples include email clients and web browsers.
 - Application Layer Services – Other programs need the assistance of application layer services to use network resources such as fire transfer or network print spooling.
- Each application or network service uses protocols, which define the standards and data formats to be used to format and direct data.

Small Network Applications and Protocols

Common Protocols



- *DNS – Service that provides the IP address of a website or domain name so a host can connect to it without using the numerical IP address.*
- *DHCP Server – Service that assigns an IP address, subnet mask, default gateway and other information to clients so they don't have to enter them manually.*

- Most network professionals work with network protocols which support the applications and services used by employees in a network.
- The figure on the left lists some common network protocols that are used in most networks – including small networks.
- Each of these network protocols define:
 - Processes on either end of a communication session.
 - Types of messages
 - Syntax of the messages
 - Meaning of information fields
 - How messages are sent and the expected response
 - Interaction with the next lower layer

Small Network Applications and Protocols

Voice and Video Applications



- Businesses today are increasingly using IP telephony and streaming media to communicate with customers and business partners.
- A network administrator must ensure that the network can support these applications and services including a supporting infrastructure with appropriate switches and cabling.
- VoIP devices convert analog signals into digital IP packets. After the signals are converted into IP packets, the router sends those packets between corresponding locations.

Small Network Applications and Protocols

Voice and Video Applications (Cont.)



- In IP Telephony, the IP phone itself performs the voice-to-IP conversion. Voice-enabled routers are not required within a network with an integrated IP telephony solution. IP Phones use a dedicated server for call control and signaling.
- Real-time Applications – the network must be able to support applications that require delay-sensitive delivery. Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP) are two protocols that support this requirement.

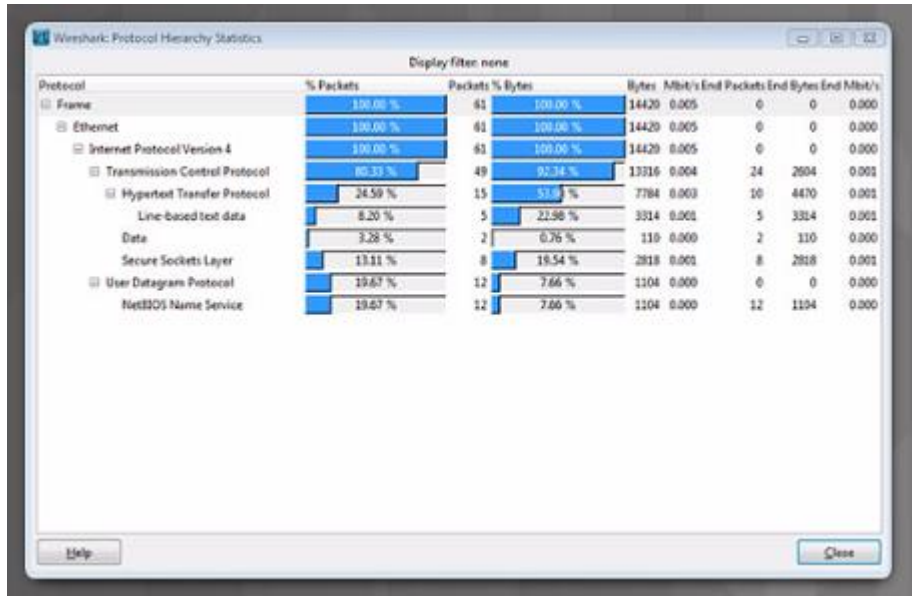
Small Network Growth



- The network administrator must allow for growth for small businesses and their networks.
- Ideally, the network administrator has enough lead time to allow the network to grow in-line with the growth of the company.
- To scale a network, the following are required:
 - Network documentation – physical and logical topology
 - Device inventory – list of devices that use or comprise the network
 - Budget – itemized IT budget, including fiscal year equipment purchasing budget
 - Traffic analysis – protocols, applications, and services along with their traffic requirements should be documented

Scale to Larger Networks

Protocol Analysis



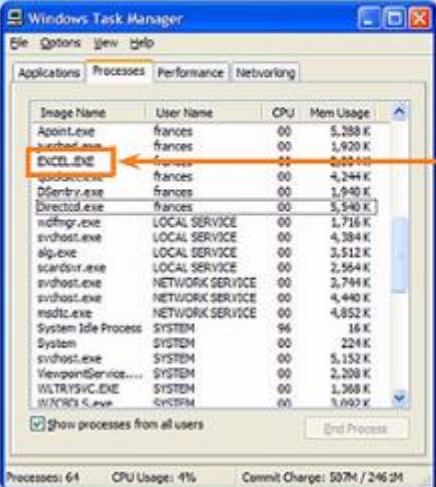
- As a network grows, it is very important to understand the type of traffic that is crossing the network as well as the traffic flow.
- A protocol analyzer is the primary tool used for this. It can also help identify any unknown traffic and its source.
- To determine traffic flow patterns:
 - Capture traffic during peak utilization times.
 - Perform the capture on different network segments since some traffic will be local to particular segments.
- The analysis of traffic patterns can be used to help make decisions on how to manage the traffic for efficiency.

Scale to Larger Networks

Employee Network Utilization

- Examples of processes running in the Windows operating system

Software Processes



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

Image Name	User Name	CPU	Mem Usage
Acrobat.exe	frances	00	5,288 K
Acrobat.exe	frances	00	1,820 K
EXCEL.EXE	frances	00	2,000 K
EXCEL.EXE	frances	00	4,244 K
EXCEL.EXE	frances	00	1,940 K
Directx.exe	frances	00	5,540 K
rdmfrg.exe	LOCAL SERVICE	00	1,716 K
svchost.exe	LOCAL SERVICE	00	4,384 K
alg.exe	LOCAL SERVICE	00	3,512 K
scardprv.exe	LOCAL SERVICE	00	2,564 K
svchost.exe	NETWORK SERVICE	00	3,744 K
svchost.exe	NETWORK SERVICE	00	4,440 K
msdtc.exe	NETWORK SERVICE	00	4,852 K
System Idle Process	SYSTEM	96	16 K
System	SYSTEM	00	224 K
svchost.exe	SYSTEM	00	5,152 K
ViewpointService...	SYSTEM	00	2,208 K
WALTRYSVC.EXE	SYSTEM	00	1,368 K
WALTRYSVC.EXE	SYSTEM	00	3,092 K

- In addition to understanding changing traffic trends, a network administrator must also be aware of how network use is changing.
- A network administrator has the ability to obtain in-person IT “snapshots” of employee application utilization over time. This information can help the network administrator adjust network resources as necessary. These snapshots typically include:
 - OS and OS Version
 - Non-Network Applications
 - Network Applications
 - CPU Utilization
 - Drive Utilization
 - RAM Utilization

11.2 Network Security

Security Threats and Vulnerabilities

Types of Threats



- Computer networks are essential to everyday activities. Individuals and organizations depend on their computers and networks.
- An 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.
- Intruders can gain access to a network through software vulnerabilities, hardware attacks, or something as simple as password guessing – these intruders are called hackers.

Security Threats and Vulnerabilities

Types of Threats (Cont.)



- Four types of threats might occur:
 - Information Theft – Occurs when someone breaks into a computer for the purpose of stealing confidential information.
 - Data Loss and Manipulation – This is breaking into a computer to destroy or alter data records. An example of data loss: a virus that reformats a person’s hard drive. An example of data manipulation: breaking into a system to change the price of an item.
 - Identity Theft – This is a form of information theft where personal information is stolen for the purpose of stealing someone’s identity.
 - Disruption of Service – This is preventing legitimate users from accessing services to which they should be entitled.

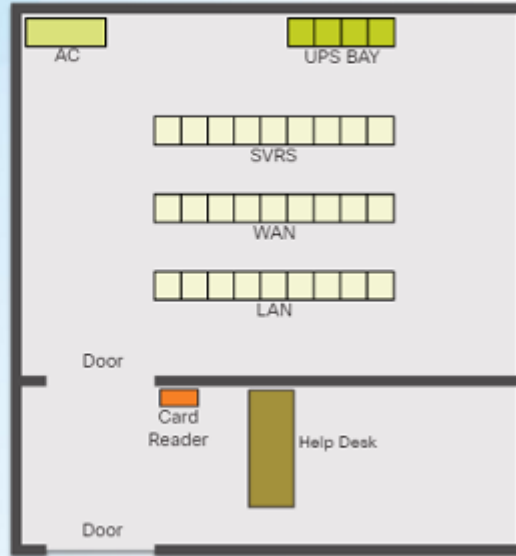
Security Threats and Vulnerabilities

Physical Security

Physical Security Plan

Plan Physical Security to Limit Damage to the Equipment

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



Secure Computer Room Floor Plan

- The physical security of network devices is an equally important security vulnerability to manage.
- There are four classes of physical threats that must be dealt with:
 - Hardware threats – physical damage to servers, routers, switches, cabling plant, and workstations
 - Environmental threats – temperature extremes (too hot or cold) or humidity extremes
 - Electrical threats – voltage spikes, insufficient supply voltage (brownouts), unconditioned power and power outages.
 - Maintenance threats - poor handling of key electrical components (electrostatic discharge), lock of critical spare parts, and poor labeling.

Security Threats and Vulnerabilities

Types of Vulnerabilities

Vulnerabilities - Technology

Network Security Weaknesses

TCP/IP Protocol Weakness

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

Operating System Weakness

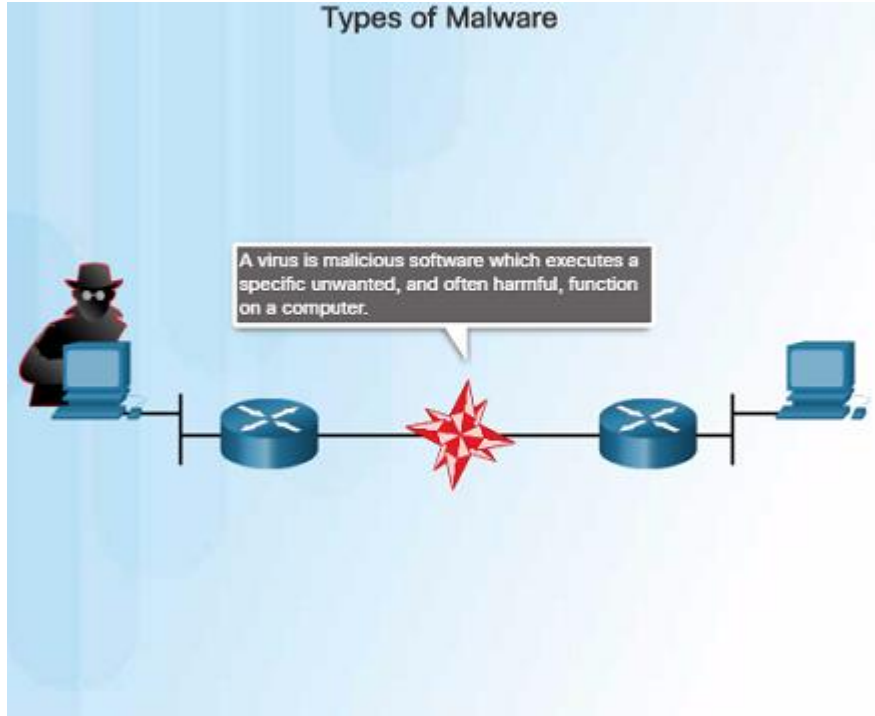
- Each operating system has security problems that must be addressed.
- UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8
- They are documented in the Computer Emergency Response Team (CERT) archives at <http://www.cert.org>

Network Equipment Weakness

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

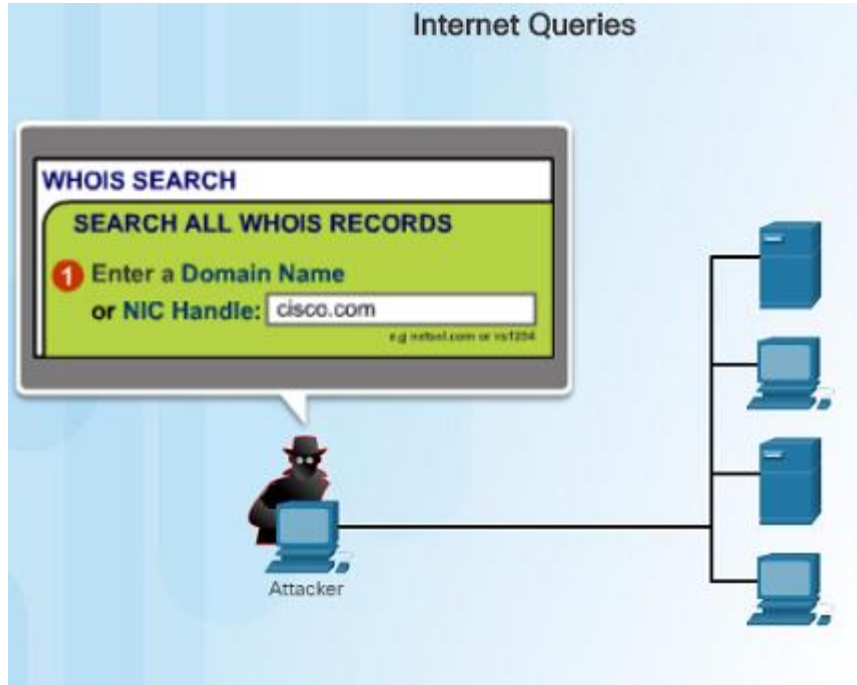
- Vulnerability is the degree of weakness which is inherent in every network and device and includes: routers, switches, desktops, servers, and security devices.
- Typically, servers and desktop computers are the devices under attack.
- There are three primary vulnerabilities that can lead to various attacks. Here are some examples
 - Technological – Weaknesses within insecure protocols, Operating System and network equipment weaknesses.
 - Configuration – Unsecured user accounts, system accounts with easily guessable passwords, misconfigured network equipment.
 - Security policy – Lack of a written security policy, inadequate monitoring and auditing of the network and resources.

Types of Malware



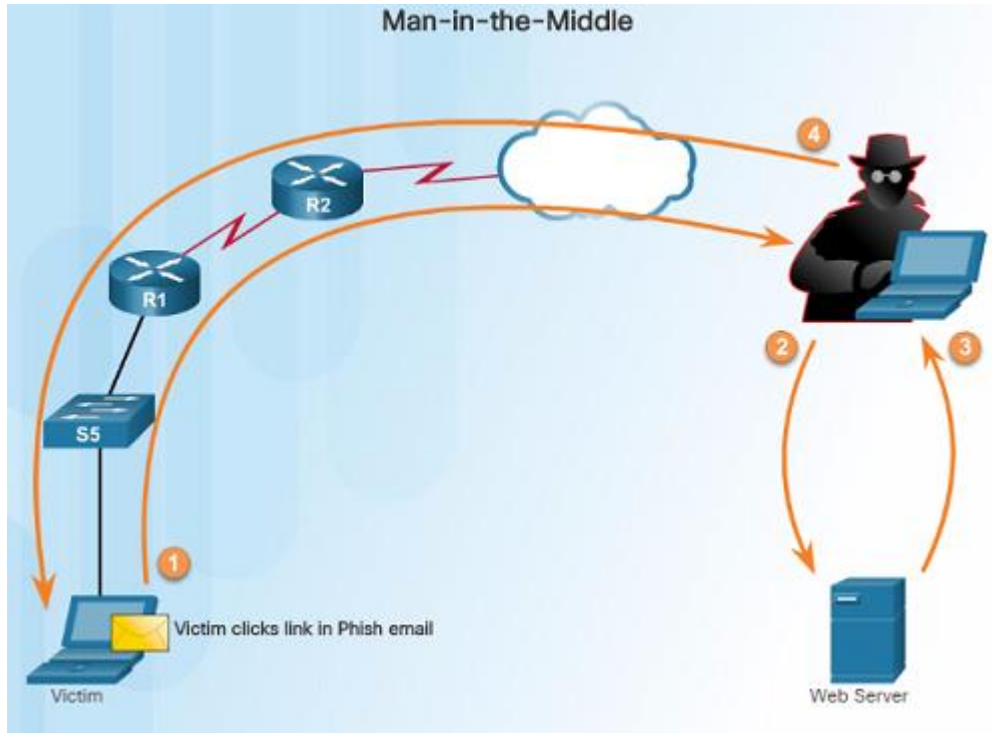
- Malware or malcode is short for malicious software – software or code that is designed to damage, disrupt, steal, or inflict damage on data, hosts, or networks.
- Viruses, worms, and Trojan horses are examples of malware.
 - Viruses – Type of malware (executable file) that is propagated by inserting a copy of itself into and becoming a part of another program. It spreads from computer to computer.
 - Worms – Very similar to viruses, but do not require a host program. Worms are standalone software programs that take advantage of system features to travel through the network.
 - Trojan horses – Users are typically tricked into loading and executing this malware on their systems. They usually create back doors to give malicious users access to the system.

Reconnaissance Attacks



- In addition to malicious code attacks, networks can also fall prey to various network attacks. There are three major categories of network attacks:
 - Reconnaissance attacks – the discovery and mapping of systems, services, or vulnerabilities
 - Access attacks – the unauthorized manipulation of data, system access, or user privileges
 - Denial of Service – the disabling or corruption of networks, systems, or services
- In a Reconnaissance attack, a hacker could use either **nslookup** or **whois** to determine the IP addresses assigned to an entity. Once they have the IP address, they can use **fping** to ping a range of IP addresses to see who is responding. Once they know what IP addresses are responding, they could use **nmap** to see which ports are listening.

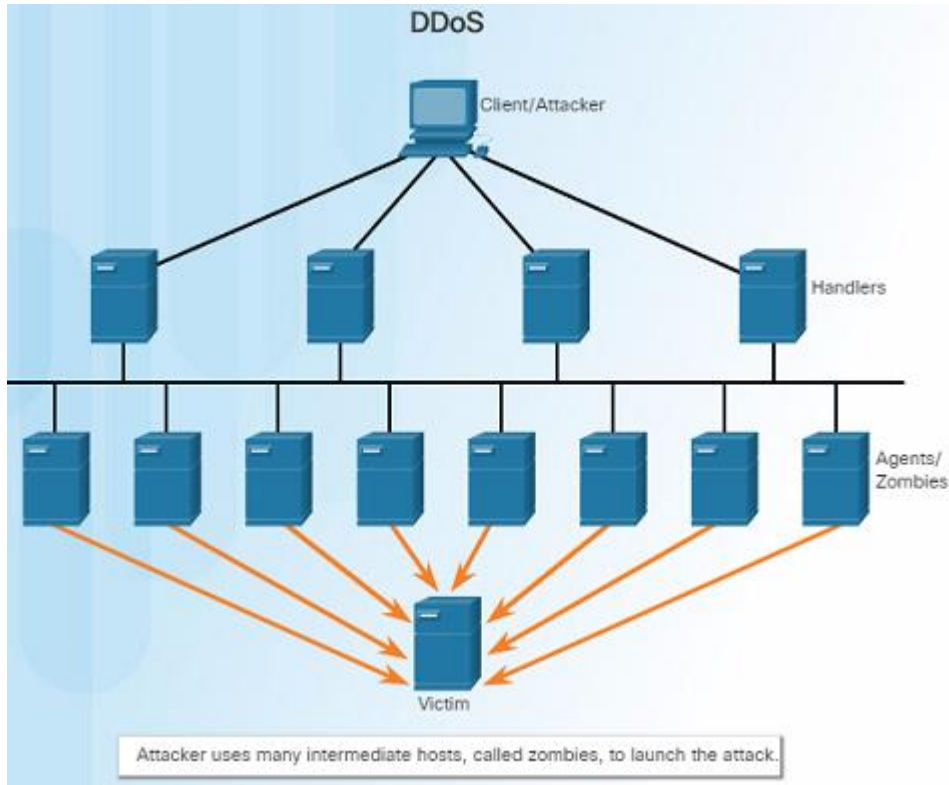
Access Attacks



- Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, or access other resources. There are four classes of access attacks:

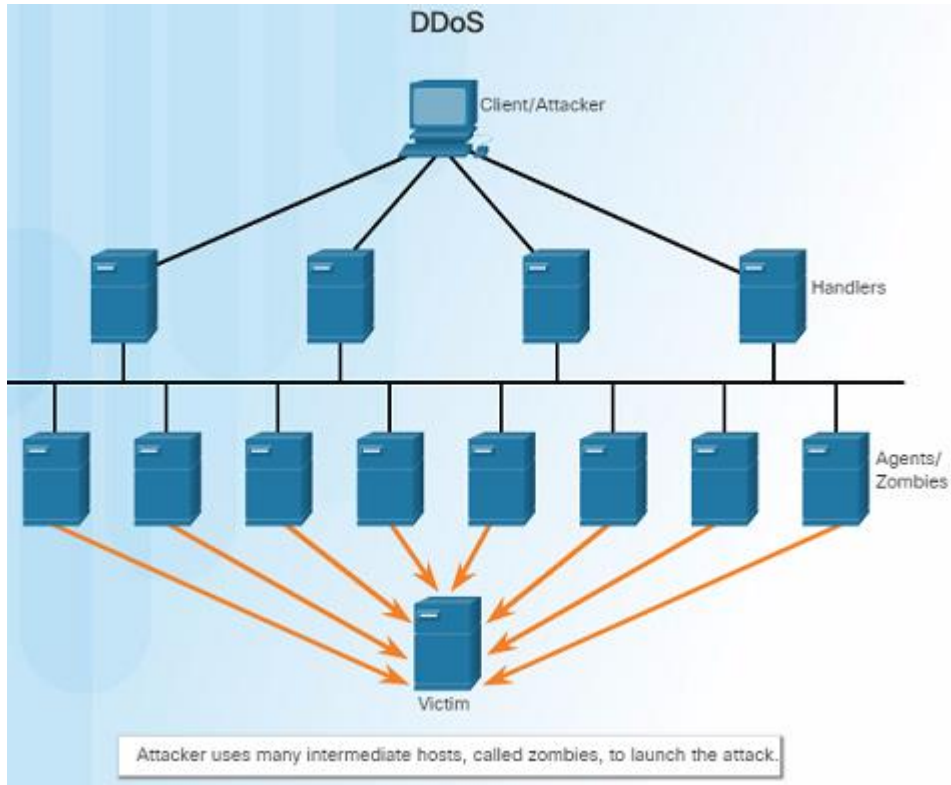
- Password attacks – Hackers can use several methods including: brute-force attacks, Trojan horse programs, and packet sniffers.
- Trust Exploitation – An attacker can access a target system by taking advantage of a trust relationship between the target system and one that is compromised.
- Port Redirection – A hacker installs software on an compromised host and uses that host to access a target host on a different port.
- Man-in-the-middle – An attacker inserts himself in the middle of a conversation. A common type is a Phish email that a victim clicks a link on in their email.

Denial of Service Attacks



- Denial of Service (DoS) attacks prevent authorized people from using a service by using up system resources such as disk space, bandwidth, and buffers. The attack can be caused by resource overload or malformed data.
- DoS attacks are the most publicized and the most difficult to eliminate. Here are some examples of DoS attacks:
 - Ping of Death – An attacker sends a malformed or a very large ping packet.
 - SYN Flood – An attacker sends multiple SYN requests to a web server. The web server waits to complete the TCP three-way handshake. A valid user tries to send a SYN request to the web server, but the web server is unavailable

Denial of Service Attacks (Cont.)



- DDoS – an Attacker uses many intermediate hosts, called zombies, to launch an attack on the victim host or server. The intermediate hosts used to launch the attack are usually infected with malware giving control to the attacker.
- Smurf attack – an ICMP-based attack where an attacker broadcasts a large number of ICMP packets using the victim's source IP address. The zombie hosts reply to the target victim in an attempt to overwhelm the WAN link to the destination.

Network Attack Mitigation

Backup, Upgrade, Update, and Patch



- Keeping up-to-date with the latest developments is a critical part of network security and defending against network attacks.
- As new malware is released, enterprises need to keep current with the latest versions of antivirus software.
- The most effective way to mitigate worm or other attacks is to download security updates from the operating system vendor and install patches on all vulnerable systems.
- The use of a central patch server to install critical patches automatically is a very useful solution to this issue.

Network Attack Mitigation

Authentication, Authorization, and Accounting

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: 1234-567-890 Statement Closing Date: 01-31-01 Current Amount Due: \$278.50

JOE EMPLOYEE
686 SYLVIA DRIVE
HOMERIDGE, CA, USA 94608-1234
6782111345 00176255000000003

MAIL PAYMENT TO:
THE BANK
100 MAIN STREET
ANYTOWN, USA 07502-0010

Statement Closing Date: 01-31-01

Interest Cycle: 02-01-01 Payment Due Date: 03-01-01
Billing Date: 01-31-01

Credit Limit: \$1,000.00 Credit Available: \$721.50
New Balance: \$278.50 Minimum Payment Due: \$20.00

Account Summary

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.90	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+256.50
Payments:	-74.25	Amount Paid Due:	+0
Finance Charge:	+0	Amount Over Credit Limit:	+0
Late Charge:	+0	NEW BALANCE:	\$278.50

Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43270807	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	Taxi Sub. Anytown, USA	\$20.75
76543210	01-25	01-30	Electronic Work Anytown, USA	\$89.25
2345678		01-30	Transaction Fees	\$3.00
9876543		01-01	Annual Fee	\$25.00

PAGE 1 OF 1

- Authentication, authorization, and accounting (AAA) network security services provide the framework to set up access control on a network device.
- AAA is used to control who is permitted to access a network (authentication), what they can do while they are there (authorize), and what did they do when they were accessing the network (accounting).

Network Attack Mitigation

Firewalls



- Firewalls are 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.
- Firewalls use various techniques for determining what is permitted or denied:
 - 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 external hosts. Traffic coming in through the firewall from the outside must originate from the inside network unless specifically permitted.

Network Attack Mitigation

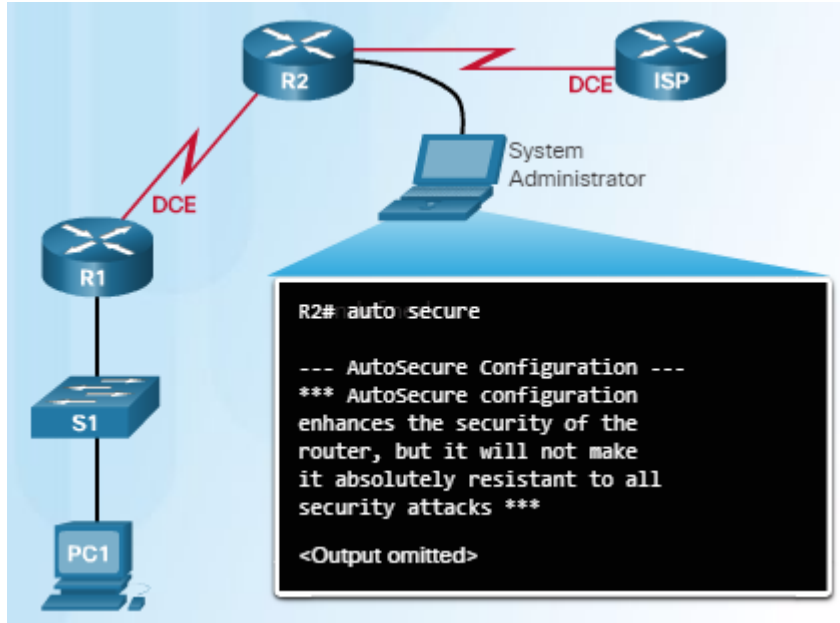
Endpoint Security



- An endpoint, or host is an individual computer system or device that acts as a network client.
- Common endpoints include: laptops, desktops, servers, smartphones, and tablets.
- A company must have a well-documented policy in place that employees must follow since securing endpoint devices is one of the most challenging jobs of a network administrator.
- The policy should include the use of antivirus software and host intrusion prevention.

Device Security Overview

- Locking down your router:



- When a new operating system is installed on a device, the security settings are set to the default values.
- This usually leads to a security threats and the default settings including passwords should be changed.
- System updates and security patches should be installed.
- For Cisco routers, the Cisco AutoSecure feature can be used to assist in securing the system.
- Here are some simple steps that should be taken to most operating systems:
 - Default usernames and passwords should be changed immediately.
 - Access to system resources should be restricted to only those who need those resources.
 - Unnecessary services and applications should be turned off, disabled, and uninstalled if possible.

Device Security

Passwords

Weak and Strong Passwords

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

- Strong passwords are critical in protecting network devices.
- Here are some password guidelines to follow:
 - Use a password of at least 8 to 10 characters – preferably 10 or more. The longer the better.
 - Password should be complex. Include a mix of uppercase, lowercase, numbers, symbols, and spaces if allowed.
 - Do not use passwords based on repetition, common dictionary words, letter or number sequences, usernames, relative or pet names, biographical information or any easily identifiable information.
 - Deliberately misspell words in your passwords.
 - Change your passwords often.
 - Never write down your passwords and leave where anyone can find them.
 - Use passphrases when possible.

Basic Security Practices

- Use the global configuration command **service password-encryption** to encrypt passwords in the configuration file and prevent unauthorized individuals from viewing plain text passwords.

```
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
```

- In order to ensure that all configured passwords are a minimum length, use the **security passwords min-length** command in global configuration mode.
- Hackers frequently use a brute-force attack to decrypt encrypted passwords. Block excessive login attempts to a device if a set number of failures occur within a specific amount of time using the command **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
- Setting the exec timeout on a router will automatically disconnect users if they have been idle for the duration of the timeout value.

Device Security

Enable SSH

- When a



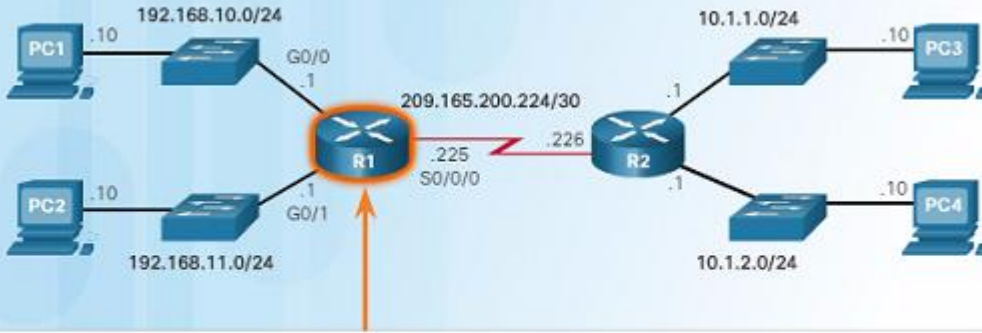
```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: 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
```

11.3 Basic Network Performance

The ping Command

Interpreting Ping Results

IOS Ping Indicators



```
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#
```

- The use of the **ping** command is a very effective method to test for network connectivity to a particular host, server, or device – it is an important first step in troubleshooting a network failure.
- The **ping** command uses the Internet Control Message Protocol and verifies layer 3 connectivity.
- A ping issued from the IOS, such as a Cisco router, will yield several indicators. The most common are:
 - ! – indicates receipt of an ICMP echo message. This is what you want to see.
 - . – indicates a time expired while waiting for an ICMP echo reply message
 - U – an ICMP unreachable message with received

The ping Command

Extended Ping



```
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:
```

- The Cisco IOS offers an “extended” mode of the ping command which will give you more options as shown in the figure to the left.
- This mode is entered by typing **ping** in privileged EXEC mode, without a destination IP address – just type **ping** and press ENTER.
- The example in the figure to the left demonstrates how to force or change the source IP address. This is very useful when troubleshooting.

The ping Command

Network Baseline

Run the Same Test

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:
```

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
```

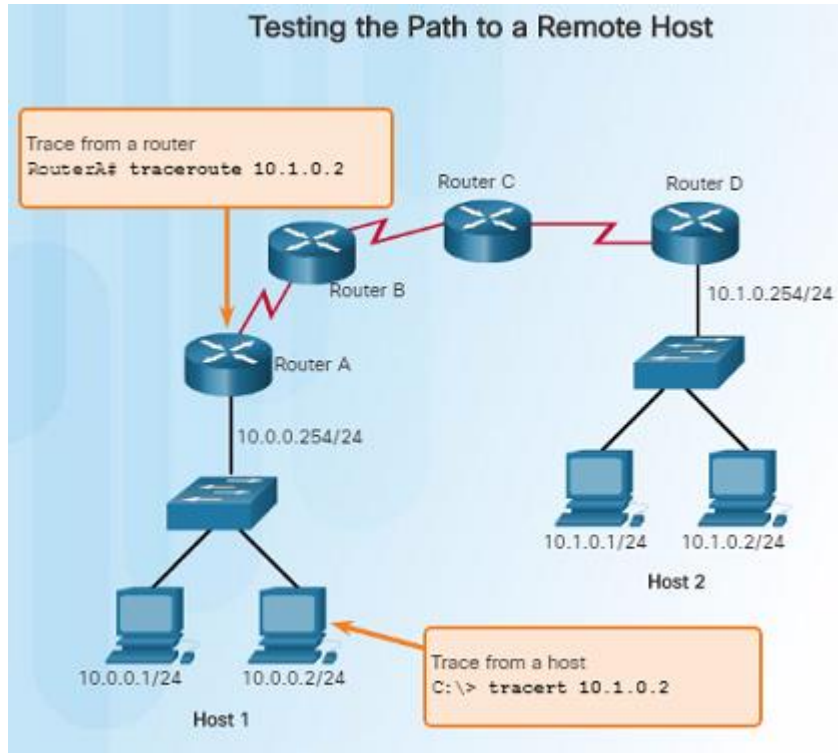
```
Ping statistics for 10.66.254.159:
```

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

- Establishing a network baseline is one of the most effective tools for monitoring and troubleshooting network performance.
- Creating an effective baseline is accomplished by measuring performance at various times over a period of time.
- One method that can be used is to copy and paste the results from a **ping**, **trace**, or other relevant commands into a text file with a time stamp.
- Corporate networks should have extensive baseline statistics using professional-grade software tools

The traceroute and tracert Command

Interpreting Trace Messages



- A trace returns a list of hops as a packet is routed through a network. Each router is a hop.
- When using windows, use the **tracert** command.
- When performing a trace from a router CLI, use the **traceroute** command.
- A “Request timed out” response indicates that the router did not respond. It is possible that there is a network failure, or the routers were configured to not respond to echo requests used in the trace.

The traceroute and tracert Command

Extended Traceroute

Extended traceroute Options

Option	Description
Protocol [ip]:	Prompts for a supported protocol. The default is IPv4.
Target IP address:	You must enter a host name or an IPv4 address. There is no default.
Source address:	The interface or IPv4 address of the router to use as a source address for the probes. The router normally picks the IPv4 address of the outbound interface to use.
Numeric display [n]:	The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display.
Timeout in seconds [3]:	The number of seconds to wait for a response to a probe packet. The default is 3 seconds.
Probe count [3]:	The number of probes to be sent at each TTL level. The default count is 3.
Minimum Time to Live [1]:	The TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.
Maximum Time to Live [30]:	The largest TTL value that can be used. The default is 30. The traceroute command terminates when the destination is reached or when this value is reached.
Port Number [33434]:	The destination port used by the UDP probe messages. The default is 33434.
Loose, Strict, Record, Timestamp, Verbose [none]:	IP header options. You can specify any combination. The traceroute command issues prompts for the required fields. Note that the traceroute command will place the requested options in each probe; however, there is no guarantee that all routers (or end nodes) will process the options.

- The extended traceroute command is a variation that will allow the network administrator to adjust parameters related to the command.
- This command is very useful when troubleshooting routing loops, determining the exact next-hop router, or determining where packets are getting dropped by a router, or denied by a firewall.
- The extended traceroute command can be useful in locating the problem. To use the command, type **traceroute** and press ENTER.
- While **ping** sends icmp packets, **traceroute** sends IP packets with a TTL value (30 by default).

Common show Commands Revisited

```
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
```

- Network technicians use show commands extensively for verifying the configuration and operation of a device or for troubleshooting purposes.
- Common show commands include:
 - show running-config
 - show interfaces
 - show arp
 - show ip route
 - show protocols
 - show version

The ipconfig Command

```
ipconfig /all

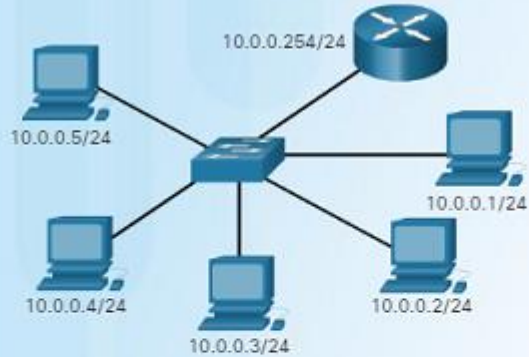
C:\>ipconfig /all
Ethernet adapter Network Connection:
    Connection-specific DNS Suffix: example.com
    Description . . . . . : Intel(R)
    PRO/Wireless 3945ABG Network Connection
    Physical Address. . . . . : 00-18-DE-C7-F3-F8
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : 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:\>
```

- On a Windows computer, the IP address of the default gateway can be viewed by using the **ipconfig** command.
- The **ipconfig /all** command can be used to view the MAC address as well as other important details regarding the Layer 3 addressing of the device.
- The **ipconfig /displaydns** command displays all of the cached DNS entries on a Windows computer system.

The arp Command

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

- On a Windows computer, the **arp -a** command lists all devices currently stored in the ARP cache of a particular host.
- The IPv4 address, physical address, and the type of addressing (static/dynamic) is displayed for each device.
- The arp cache can be cleared using the command **arp-d**

The show cdp neighbors Command

```
R3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge,
                  B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP,
                  r - Repeater, P - Phone

Device ID  Local Intrfce  Holdtme  Capability  Platform  Port ID
S3         Fas 0/0        151      S I         WS-C2950  Fas 0/6
R2         Ser 0/0/1      125      R           1841      Ser 0/0/1
```

```
R3#show cdp neighbors detail
```

```
Device ID: R2
Entry address(es):
  IP address : 192.168.1.2
Platform: Cisco 1841, Capabilities: Router Switch IGMP
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec
```

```
Version :
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
```

```
advertisement version: 2
```

- The Cisco Discovery Protocol (CDP) is a Cisco-proprietary protocol that runs at the data link layer that allows adjacent Cisco devices to learn about each other – even without Layer 3 connectivity.
- When a Cisco device boots up, CDP starts by default. CDP automatically discovers neighboring devices running CDP.
- CDP provides the following information about each CDP neighbor: device identifiers, address list, port identifier, capabilities list, and platform.
- The **show cdp neighbors detail** command will show you the IP address of a neighboring device.

The show ip interface brief Command

```
Interface Testing

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
```

- One of the most frequently used commands to verify interface configuration and status of all interfaces is the **show ip interface brief** command.
- This command provides a more abbreviated output than the **show ip interface** command and provides a summary of the key information for all of the network interfaces on a router.
- The command displays various information including the IP address assigned to each interface and the operational status of the interface.

The debug Command

Output for the debug ip icmp Command

```
R1# debug ip icmp
ICMP packet debugging is on
R1# ping 10.0.0.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
*Nov 13 12:56:08.147: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
R1# undebug all
All possible debugging has been turned off
R1#
```

- IOS processes, protocols, mechanisms and events generate messages to communicate their status.
- These messages can provide valuable information when troubleshooting or verifying system operations.
- The IOS **debug** command, entered in privileged EXEC mode, allows the administrator to display these message in real-time for analysis.
- It is possible to narrow the output of the **debug** command to include only the relevant feature or sub-feature that is needed.

The terminal monitor Command

Issue the command to allow log messages to be sent to your remote session.

```
R1# terminal monitor
```

```
R1#
```

Issue the following troubleshooting commands:

- Issue the debug command that will monitor the status of ICMP messages on R1.
- Ping a device with an IP address of 10.0.0.10.
- Turn off all debugging.

```
R1#
```

- Connections to grant access to the IOS command line interface can be established locally or remotely.
 - Local connections require physical access to the router or switch using a cable.
 - Remote connections using SSH or Telnet are made using the network and require a network protocol such as IP to be configured.
- Debugging long messages are sent to the console by default and not to virtual lines.
- To display log messages on a terminal or virtual console, use the privileged EXEC command: **terminal monitor** and **terminal no monitor** to turn it off.

11.4 Network Troubleshooting

Basic Troubleshooting Approaches

Six Steps of the Troubleshooting Methodology

Step	Title	Description
1	Identify the Problem	The first step in the troubleshooting process is to identify the problem. While tools can be used in this step, a conversation with the user is often very helpful.
2	Establish a Theory of Probable Causes	After you have talked to the user and identified the problem, you can try and establish a theory of probable causes. This step often yields more than a few probable causes to the problem.
3	Test the Theory to Determine Cause	Based on the probable causes, test your theories to determine which one is the cause of the problem. A technician will often apply a quick procedure to test and see if it solves the problem. If a quick procedure does not correct the problem, you might need to research the problem further to establish the exact cause.
4	Establish a Plan of Action to Resolve the Problem and Implement the Solution	After you have determined the exact cause of the problem, establish a plan of action to resolve the problem and implement the solution.
5	Verify Full System Functionality and Implement Preventive Measures	After you have corrected the problem, verify full functionality and, if applicable, implement preventive measures.
6	Document Findings, Actions, and Outcomes	In the final step of the troubleshooting process, document your findings, actions, and outcomes. This is very important for future reference.

- Technicians must be able to analyze the cause of the network problem before they can resolve the issue.
- This process is called troubleshooting.
- A common and efficient method is based on the scientific method and can be broken down into six steps shown in the figure to the left.
- How many devices on the network are experiencing the problem?
 - If it's one device, start troubleshooting at that device.
 - If it's all devices, start troubleshooting at the device where all of those devices are connected.

Troubleshooting Methodologies

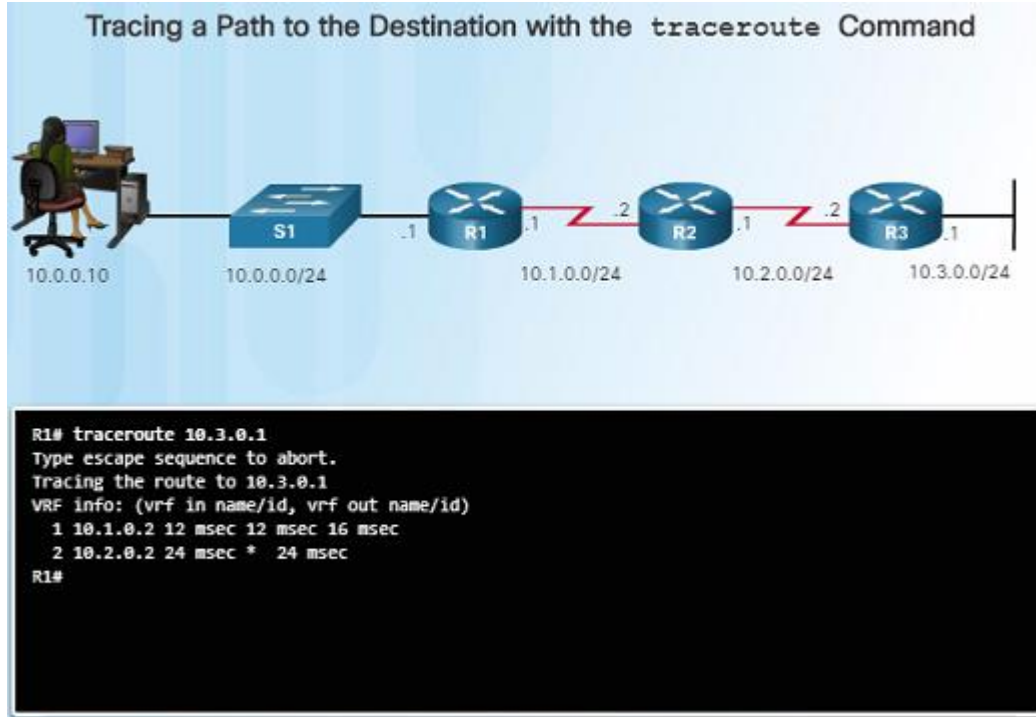
Resolve or Escalate?



- In some cases, it may not be possible to resolve the network problem immediately and may need to be escalated if it requires a manager's decision.
- For example, after troubleshooting, the technician discovers that a router module needs to be replaced. This problem should be escalated for the manager's approval since it might require a financial commitment.

Troubleshooting Methodologies

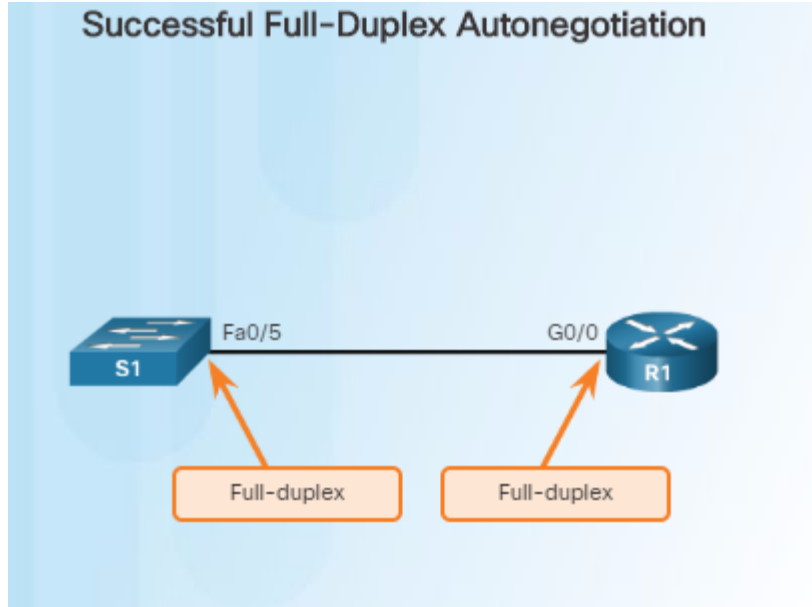
Verify and Monitor Solution



- The Cisco IOS includes powerful tools to help with troubleshooting and verification such as:
- **ping** – can be used to verify successful network connectivity
- **traceroute** – displays the path that packets are using to reach a destination and may show where the packet stopped along the way
- Show commands including **show ip int brief** which will show a summarized view of the interfaces on a device

Troubleshoot Cables and Interfaces

Duplex Operation



- In data communications, duplex refers to the direction of the data transmission between two devices such as a router and a switch.
 - Half-duplex – the data is restricted to one direction at a time
 - Full duplex – the data can go both directions at the same time
- For the best communication performance, two connected Ethernet network interfaces must have matching duplex configurations.
 - They must both be set to full or half.
 - Ethernet autonegotiation was designed to help with this configuration, but could lead to problems if one side is set to auto and the other is not.

Troubleshoot Cables and Interfaces

Duplex Mismatch

Duplex Mismatch Topology



```
S1#
*Mar 1 01:01:03.858: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
FastEthernet0/5 (not half duplex), with R1 GigabitEthernet0/0 (half duplex).
*Mar 1 01:01:04.856: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
FastEthernet0/5 (not half duplex), with R1 GigabitEthernet0/0 (half duplex).
*Mar 1 01:01:05.855: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
FastEthernet0/5 (not half duplex), with R1 GigabitEthernet0/0 (half duplex).
S1#
```

- Duplex mismatch issues are difficult to troubleshoot since the communication between devices still occurs, but is usually much slower.
 - **ping** might not detect the problem.
 - A ping could be successful even though there is a mismatch
- The Cisco Discovery Protocol (CDP) can detect a duplex mismatch between two Cisco devices as shown in the figure to the left.
- These log messages are only displayed on a console or on a remote connection if the **terminal monitor** command is enabled.

Troubleshooting Scenarios

IP Addressing Issues on IOS Devices

The show ip interface Command



```
R1# show ip interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 10.0.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
<output omitted>
```

- IP address-related problems will likely cause connectivity issues.
- Since IP addresses are hierarchical, any IP addresses assigned to a network device must conform to that network's range of addresses.
- Two common causes of incorrect IPv4 assignments are: manual misconfiguration or DHCP-related issues.
- If a mistake is made during the assignment, communication issues with the device will likely occur.
- Use the command **show ip interface brief** to verify what IPv4 addresses are assigned to network interfaces.

Troubleshooting Scenarios

IP Addressing Issues on End Devices

The ipconfig Command



```
C:\> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::fd4c:6609:6733:c5cc%11
    IPv4 Address. . . . . : 10.0.0.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.1

C:\>
```

- On a Windows-based machine, when the device can't contact a DHCP server, Windows will automatically assign the device to the 169.254.0.0/16 range to allow it to communicate within the local network.
- Normally, this is an indication of a problem, and a device assigned with this address/range will not be able to communicate with other devices in the network.
- Most end devices are configured with DHCP for automatic IPv4 address assignment.
- Use the **ipconfig** command to verify the IP address assigned to a Windows-based computer.

Troubleshooting Scenarios

Default Gateway Issues

Verify Router Default Route



```
R1# show ip route
<output omitted>

Gateway of last resort is 10.1.0.2 to network 0.0.0.0
```

```
S* 0.0.0.0/0 [1/0] via 10.1.0.2
   10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C   10.0.0.0/24 is directly connected, GigabitEthernet0/0
L   10.0.0.1/32 is directly connected, GigabitEthernet0/0
C   10.1.0.0/24 is directly connected, Serial0/0/0
L   10.1.0.1/32 is directly connected, Serial0/0/0
R1#
```

- The default gateway for an end device is the closest networking device that can forward traffic to other networks – usually a router.
- Without a valid default-gateway address, a host will not be able to communicate with devices outside of its local network.
 - The default gateway for a host should belong to the same network as the end device.
 - The default gateway can be set manually or obtained from a DHCP server.
- Use the **ipconfig** command to verify the default gateway on a Windows-based computer.
- Use the **show ip route** command to verify that the default route has been set.

Troubleshooting DNS Issues

- Use **ipconfig /all** to obtain DNS Server Information on a Windows PC

```
C:\> ipconfig /all

Ethernet adapter Local Area Connection:
<some output omitted>
Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : F0-4D-A2-DD-A7-B2
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::449f:c2:de06:ebad%10(Preferred)
IPv4 Address. . . . . : 10.0.0.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, November 09, 2015 7:49:48 PM
Lease Expires . . . . . : Thursday, November 19, 2015 7:49:51 AM
Default Gateway . . . . . : 10.0.0.1
DHCP Server . . . . . : 10.0.0.1
DNS Servers . . . . . : 8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled
```

- Domain Name Service (DNS) is used to match names, such as, www.cisco.com, with numerical IP addresses.
- This allows a user to enter www.cisco.com on their web browser instead of entering Cisco's IP address for their web server.
- If DNS is down, it may appear to some users that the “network is down”, when in reality, it might just be that the DNS server is unreachable.
- DNS server addresses can be manually entered or automatically assigned using DHCP.

11.5 Summary

Chapter 11: Build a Small Network

- Explain the features and functions of Cisco IOS Software.
- Configure initial settings on a network device using the Cisco IOS software.
- Given an IP addressing scheme, configure IP address parameters on end devices to provide end-to-end connectivity in a small to medium-sized business network.

