Chapter 11: It's a Network

Network Basics

Chapter 11

Chapter 11: Objectives

Upon completion of this chapter, you will be able to:

- Identify the devices and protocols used in a small network.

- Explain how a small network serves as the basis of larger networks.

- Explain the need for basic security measures on network devices.

- Identify security vulnerabilities and general mitigation techniques.

- Use the output of `ping` and `tracert` commands to establish relative network performance.

- Use basic show commands to verify the configuration and status of a device interface.

Chapter 11: Objectives (Cont.)

- Use the basic **host** commands to acquire information about the devices in a network.

- Explain the file systems on Routers and Switches.

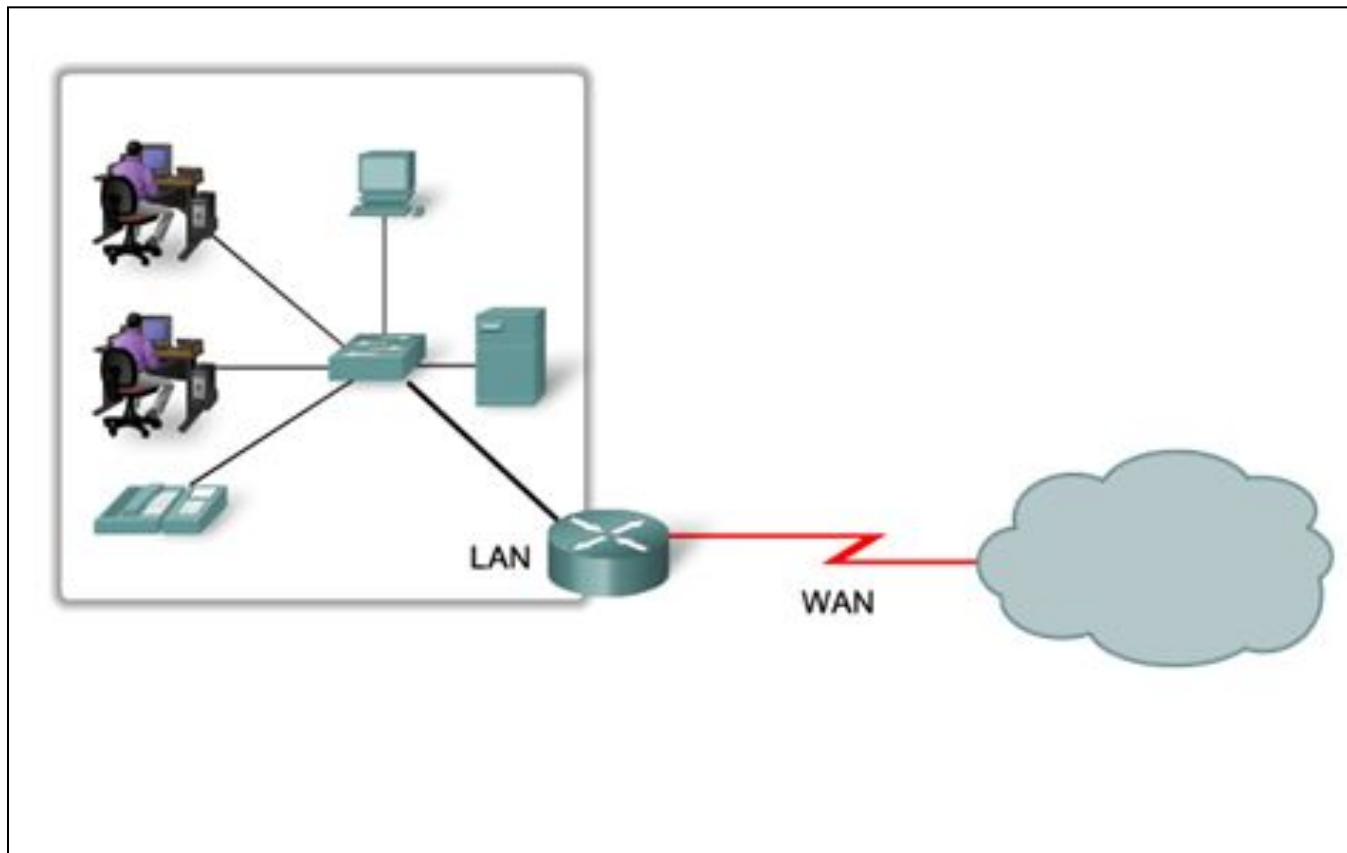- Apply the commands to back up and restore an IOS configuration file.

11.1 Create and Grow

Small Network Topologies

Typical, Small Network Topology

6

Device Selection for a Small Network

Factors to be considered when selecting intermediate devices.

COST

PORTS

SPEED

EXPANDABLE/ MODULAR

MANAGEABLE

Addressing for a Small Network

- IP addressing scheme should be planned, documented, and maintained based on the type of devices receiving the address.

- Examples of devices that should be part of the IP design:
  - End devices for users
  - Servers and peripherals
  - Hosts that are accessible from the Internet
  - Intermediary devices

- Planned IP schemes help the administrator:
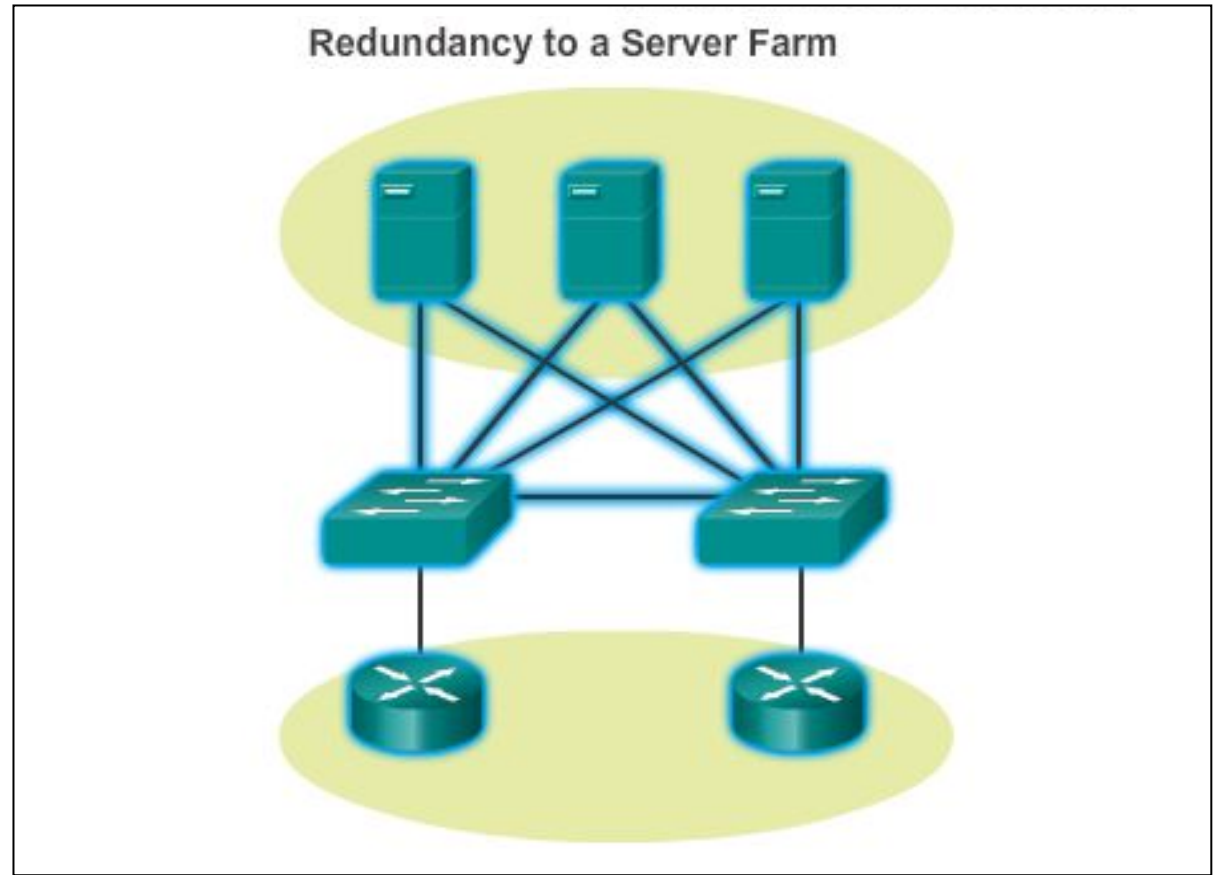 - Track devices and troubleshoot
  - Control access to resources

Redundancy in a Small Network

- Redundancy helps to eliminate single points of failure.
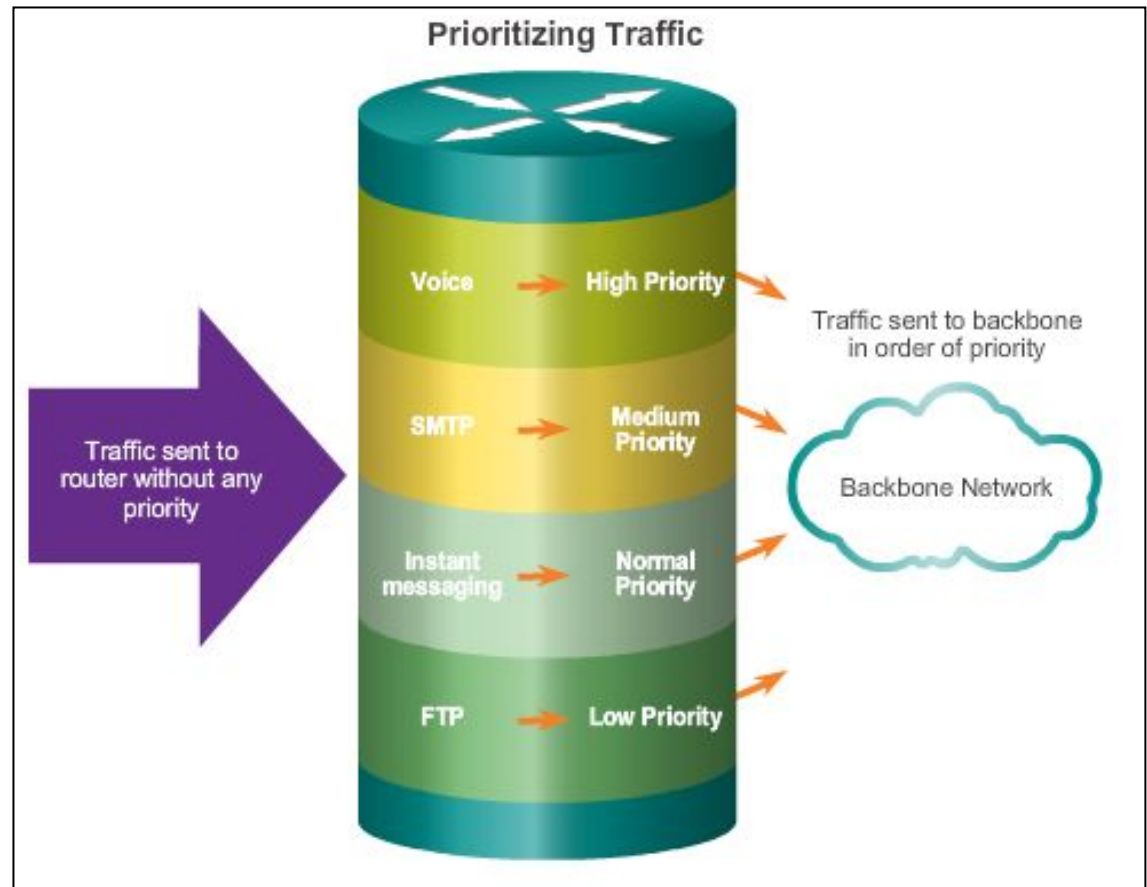
- Improves the reliability of the network.

Redundancy to a Server Farm

Design Considerations for a Small Network

- The following should be included in the network design:

  - Secure file and mail servers in a centralized location.

  - Protect the location by physical and logical security measures.

  - Create redundancy in the server farm.

  - Configure redundant paths to the servers.

Prioritizing Traffic

Traffic sent to router without any priority

Voice → High Priority

SMTP → Medium Priority

Instant messaging → Normal Priority

FTP → Low Priority

Traffic sent to backbone in order of priority

Backbone Network

Common Applications in a Small Network

- **Network-Aware Applications** – Software programs used to communicate over the network.

- **Application Layer Services** – Programs that interface with the network and prepare the data for transfer.
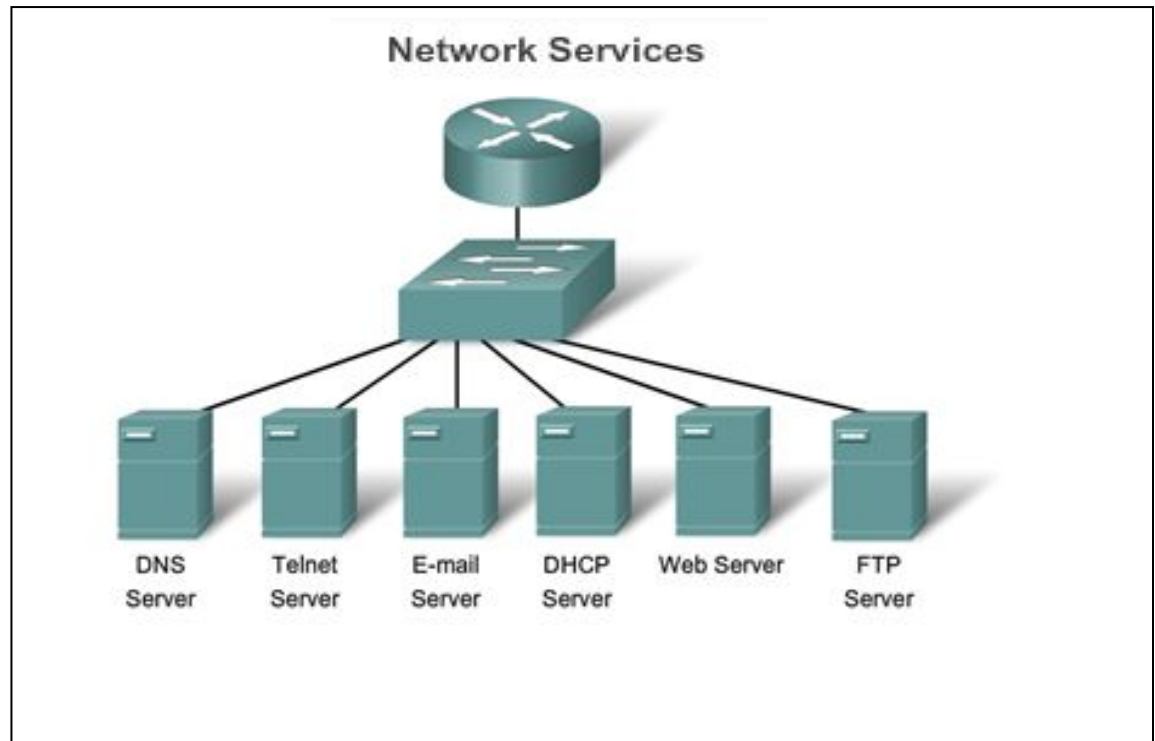
Common Protocols in a Small Network

Network protocols define:

- Processes on either end of a communication session

- Types of messages

- Syntax of the messages

- Meaning of informational fields

- How messages are sent and the expected response

- Interaction with the next lower layer

Network Services

DNS Server Telnet Server E-mail Server DHCP Server Web Server FTP Server

Real-Time Applications for a Small Network

- **Infrastructure** – Should be evaluated to ensure it supports proposed real-time applications.

- **VoIP** – Is implemented in organizations that still use traditional telephones.

- **IP telephony** – The IP phone performs voice-to-IP conversions.

- **Real-time video protocols** – Use the Time Transport Protocol (RTP) and the Real-Time Transport Control Protocol (RTCP).

Scaling a Small Network

Important considerations when growing to a larger 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, services, and their respective traffic requirements should be documented.

Protocol Analysis of a Small Network

Information gathered by protocol analysis can be used to make decisions on how to manage traffic more efficiently.
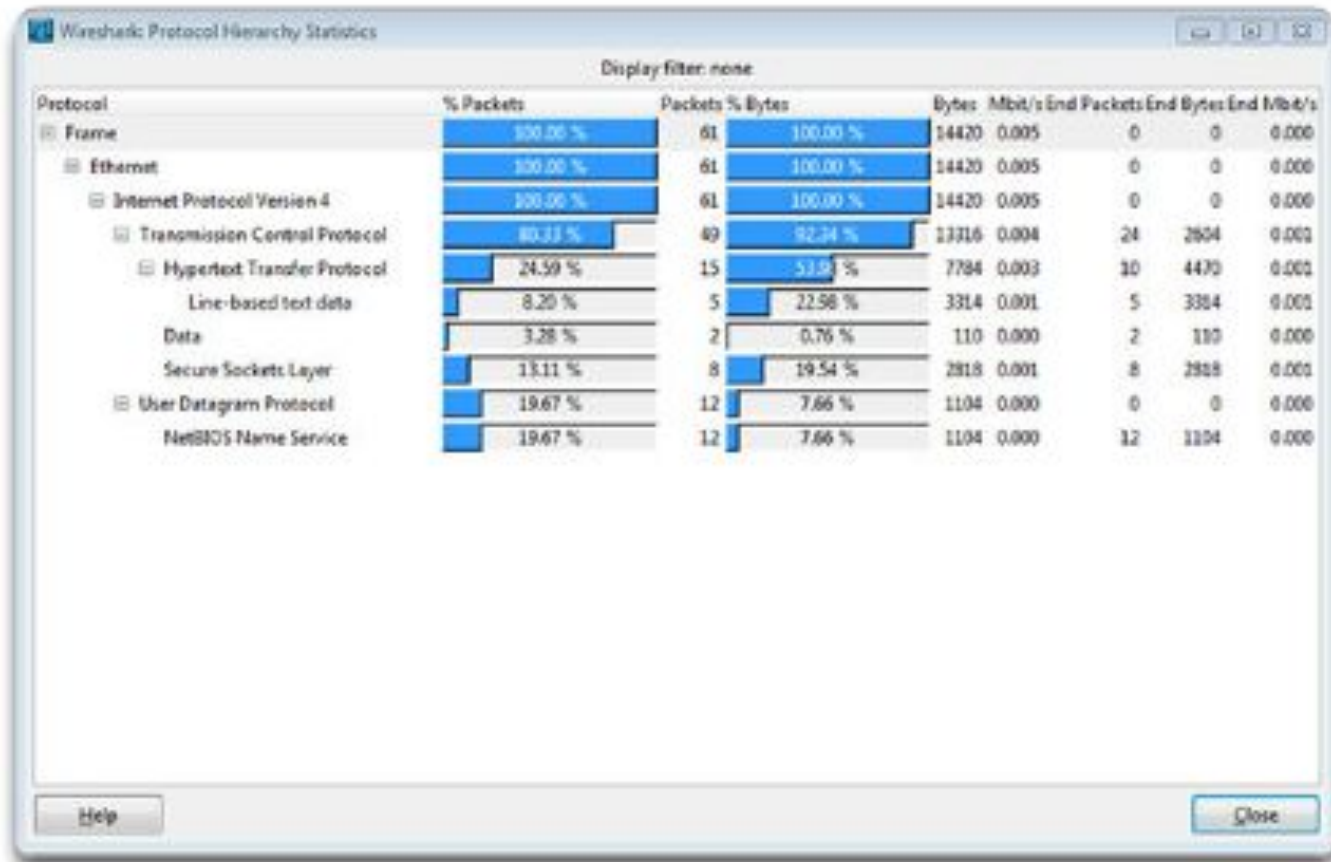
Evolving Protocol Requirements

- Network administrator can obtain IT "snapshots" of employee application utilization.

- Snapshots track network utilization and traffic flow requirements.

- Snapshots help inform network modifications needed to optimize employee productivity.

11.2 Keeping the Network Safe

Categories of Threats to Network Security

Categories of Threats to Network Security

Information Theft

Data Loss and Manipulation

Identity Theft

Disruption of Service

Physical Security

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.

Types of Security Vulnerabilities

Vulnerabilities - Technology

Types of Security Weaknesses:

- Technological

- Configuration

- Security policy

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.

Viruses, Worms, and Trojan Horses

- **Virus** – Malicious software that is attached to another program to execute a particular unwanted function on a workstation.

- **Trojan horse** – An entire application written to look like something else, when in fact it is an attack tool.

- **Worms** – Worms are self-contained programs that attack a system and try to exploit a specific vulnerability in the target. The worm copies its program from the attacking host to the newly exploited system to begin the cycle again.

Reconnaissance Attacks
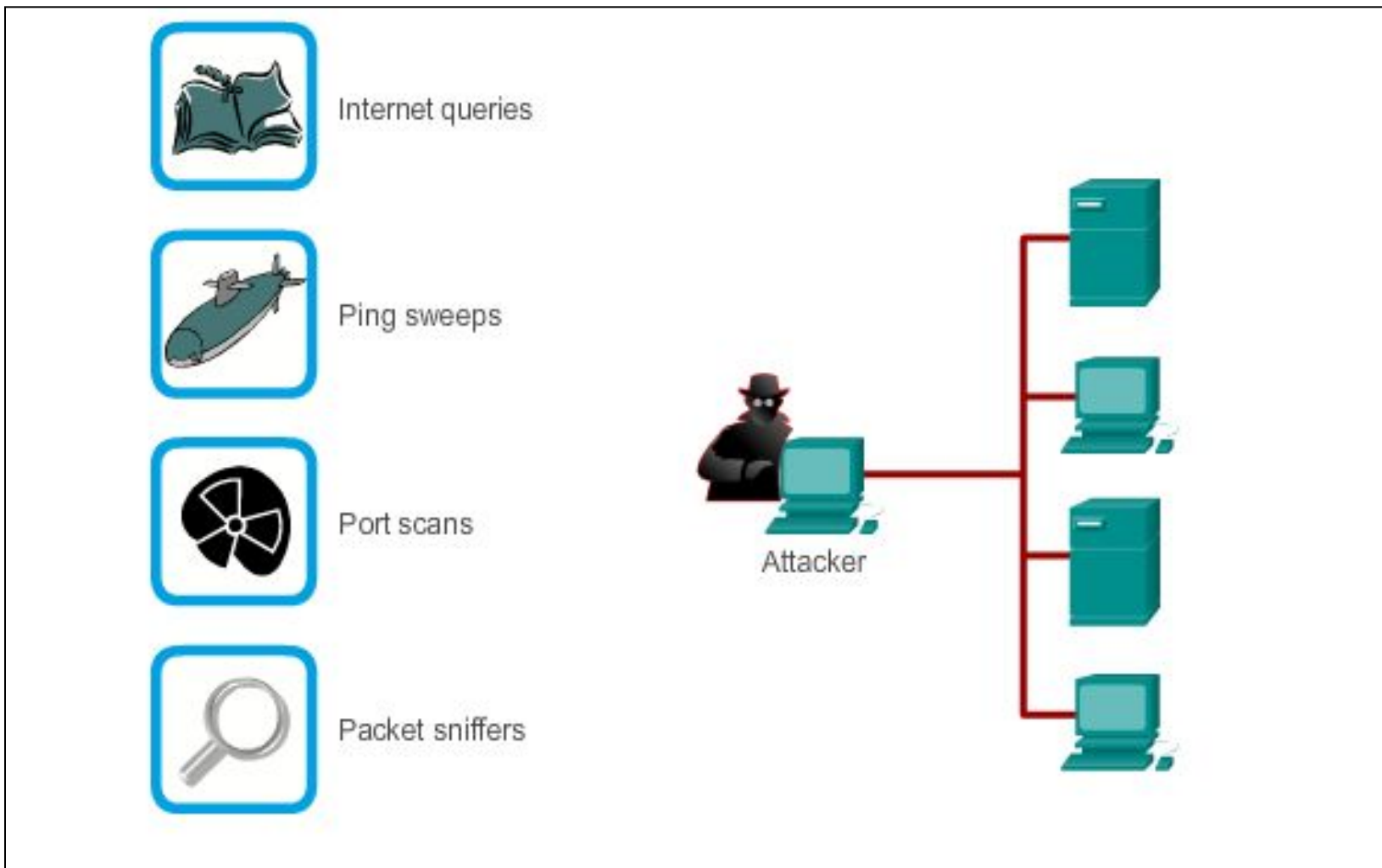
Access Attacks

Access Attacks (Cont.)

Port Redirection

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

Source: Attacker
Destination: A
Port: 22

Source: Attacker
Destination: B
Port: 23

Attacker

Compromised Host A

Source: A
Destination: B
Port: 23

Host B
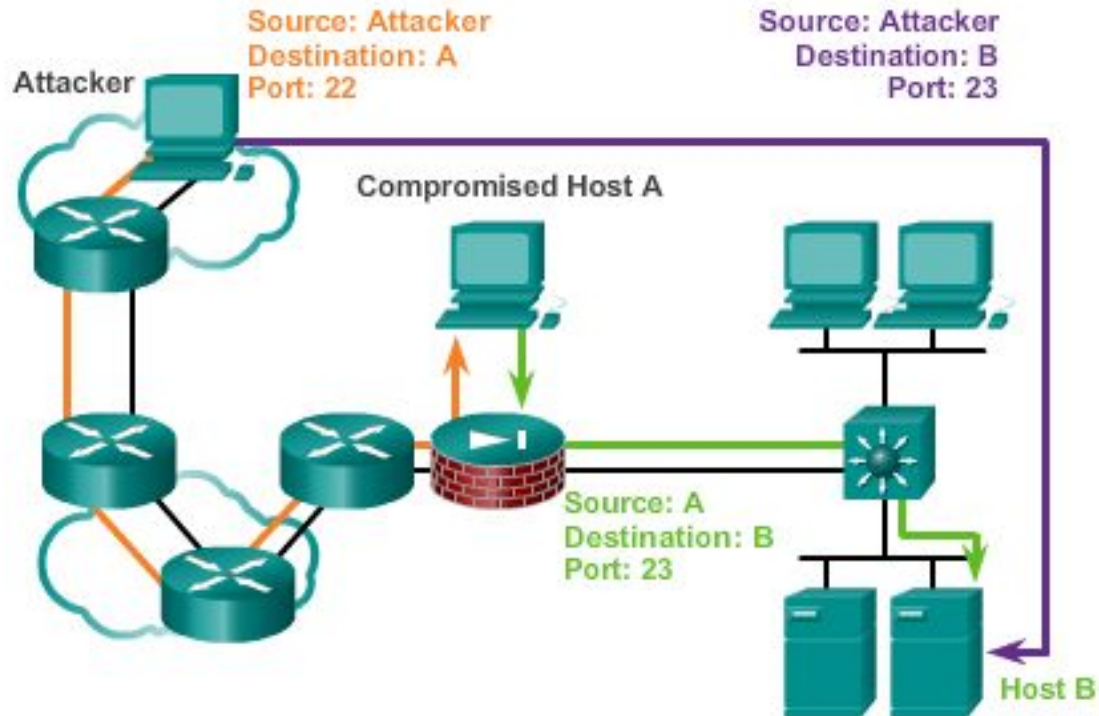
Denial of Service (DoS) Attacks
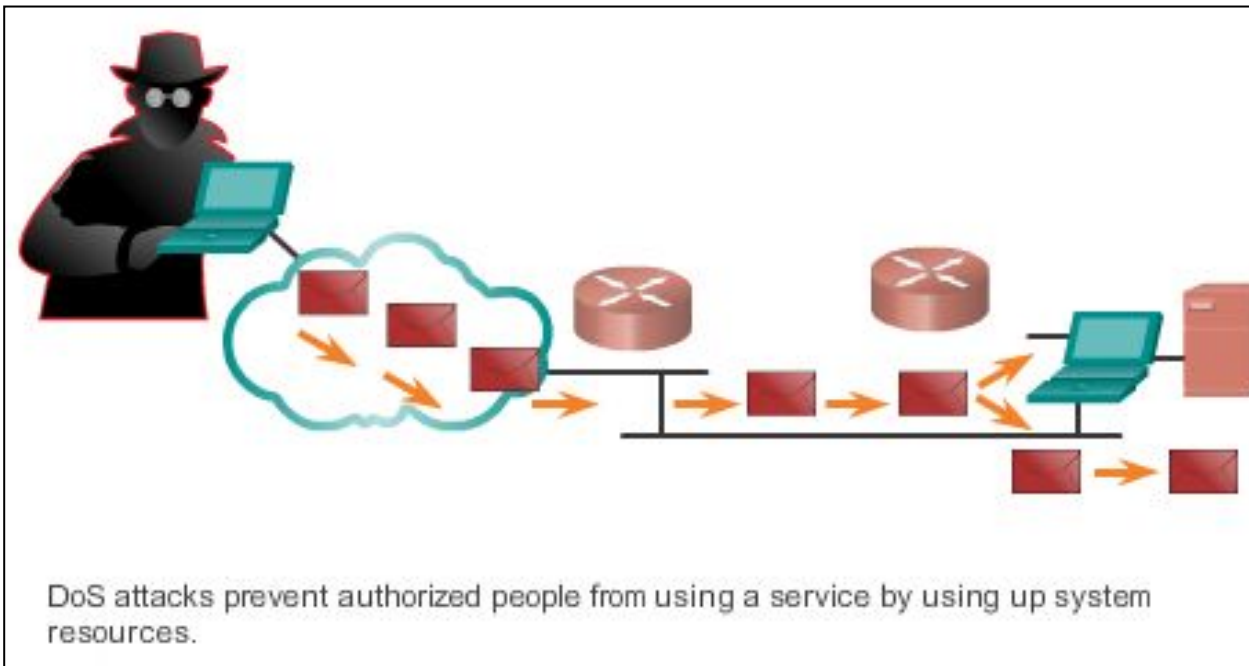
DoS attacks prevent authorized people from using a service by using up system resources.

Backup, Upgrade, Update, and Patch

Antivirus software can detect most viruses and many Trojan horse applications and prevent them from spreading in the network.

- Keep current with the latest versions of antivirus software.

- Install updated security patches.

Install OS Patches

Authentication, Authorization, and Accounting

Authentication, Authorization, and Accounting (AAA, or "triple A")

- **Authentication** – Users and administrators must prove their identity. Authentication can be established using username and password combinations, challenge and response questions, token cards, and other methods.

- **Authorization** – Determines which resources the user can access and the operations that the user is allowed to perform.

- **Accounting** – Records what the user accessed, the amount of time the resource is accessed, and any changes made.

Firewalls

A Firewall resides between two or more networks. It controls traffic and helps prevent unauthorized access. Methods used are:

- Packet Filtering

- Application Filtering

- URL Filtering

- Stateful Packet Inspection (SPI) – Incoming packets must be legitimate responses to requests from internal hosts

Firewalls

Cisco Security Appliances

Server-Based Firewall

Linksys Wireless Router with Integrated Firewall

Personal Firewall

Endpoint Security

- Common endpoints are laptops, desktops, servers, smart phones, and tablets.

- Employees must follow the companies documented security policies to secure their devices.

- Policies often include the use of anti-virus software and host intrusion prevention.

Common Endpoint Devices

Introduction to Securing Devices

- Part of network security is securing devices, including end devices and intermediate devices.

- Default usernames and passwords should be changed immediately.

- Access to system resources should be restricted to only the individuals that are authorized to use those resources.

- Any unnecessary services and applications should be turned off and uninstalled, when possible.

- Update with security patches as they become available.

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

Basic Security Practices

Securing Devices

- Encrypt passwords.

- Require minimum length passwords.

- Block brute force attacks.

- Use Banner Message.

- Set EXEC timeout.

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

Enabling SSH

Enabling 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.

11.3 Basic Network Performance

Interpreting ICMP Messages

- **!** – indicates receipt of an ICMP echo reply message

- **.** – indicates a time expired while waiting for an ICMP echo reply message

- **U** – an ICMP unreachable message was received

Testing Local TCP/IP Stack

Pinging the local host confirms that TCP/IP is installed and working on the local network adapter.

C:\>ping 127.0.0.1

Pinging 127.0.0.1 causes a device to ping itself.

Local Area Connection Properties

General | Authentication | Advanced

Connect using:

VIA Rhine II Fast Ethernet Adapter   Configure...

This connection uses the following items:

☑ QoS Packet Scheduler
☑ Network Monitor Driver
☑ Internet Protocol (TCP/IP)

Install...   Uninstall   Properties

Description

Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

OK   Cancel

Leveraging Extended Ping

The Cisco IOS offers an "extended" mode of the `ping` command:

- 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]:

Network Baseline

Baseline with `ping`

Network Baseline (Cont.)

Router Ping Capture - Saving to a text file

In the terminal session:

1. Start the text capture process.
2. Issue a **ping** `<ip address>` command.
3. Stop the capture process.
4. Save the text file.

Interpreting Tracert Messages
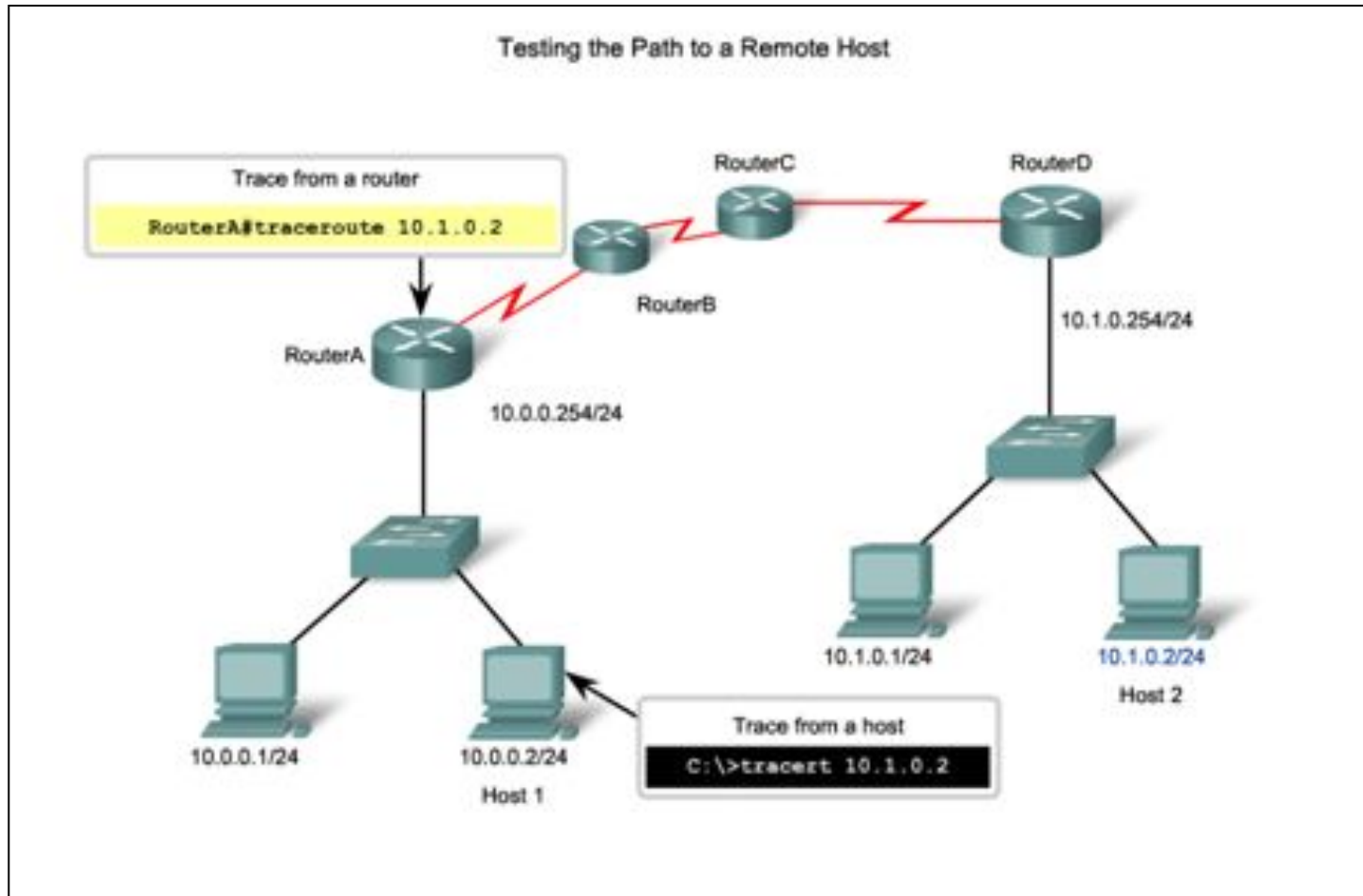
Common Show Commands Revisited

The status of nearly every process or function of the router can be displayed using a `show` command.

Frequently used show commands:

- **`show running-config`**
- **`show interfaces`**
- **`show arp`**
- **`show ip route`**
- **`show protocols`**
- **`show version`**

Viewing Router Settings With Show Version

Cisco IOS Version

System Bootstrap

Cisco IOS Image

CPU and RAM

Number and Type of Physical Interfaces

Amount of NVRAM

Amount of Flash

Configuration Register

```
Router#show version
Cisco Internetwork Operating System Software
IOS(tm)2500 Software (C2500-I-L),Version 12.0(17a),RELEASE
SOFTWARE (fc1)
Copyright (c)1986-2002 by cisco Systems,Inc.
Compiled Mon 11-Feb-02 05:55 by kellythw
image text-base:0x00001000
ROM:system Bootstrap,Version 11.0(10c),SOFTWARE
BOOTFLASH :3000 Bootstrap Software (IGS-BOOT-R),Version
11.0(10c),RELEASE SOFTWARE(fc1)
System image file is "flash:c2500-i-l.120-17a.bin"
cisco 2500 (68030 processor(revision N) With 2048K/2048K
bytes of memory.
processor bord ID 08860060,with hardware revision 00000000
Bridging software.
X.25 software,version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)

32K bytes of non-volatile Configuration memory.

8192K bytes of processor board system flash (Read ONLY)

Configuration register is 0x2102
Router#_
```

Viewing Switch Settings with Show Version

show version Command

```
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)SEE2,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 04:33 by yenanh
Image text-base: 0x00003000, data-base: 0x00AA2F34

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)SEE1, RELEASE
SOFTWARE (fc1)

Switch uptime is 2 minutes
System returned to ROM by power-on
System image file is "flash:c2960-lanbase-mz.122-25.SEE2/c2960-lanbase-
mz.122-25.SEE2.bin"

cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 61440K/4088K
bytes of memory.
Processor board ID FOC1107Z9ZN
Last reset from power-on
1 Virtual Ethernet interface
```

`ipconfig` Command Options

- **`ipconfig`** – Displays ip address, subnet mask, default gateway.

- **`ipconfig /all`** – Also displays MAC address.

- **`ipconfig /displaydns`** – Displays all cached dns entries in a Windows 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
```

`arp` Command Options

`arp` Command Options

```
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
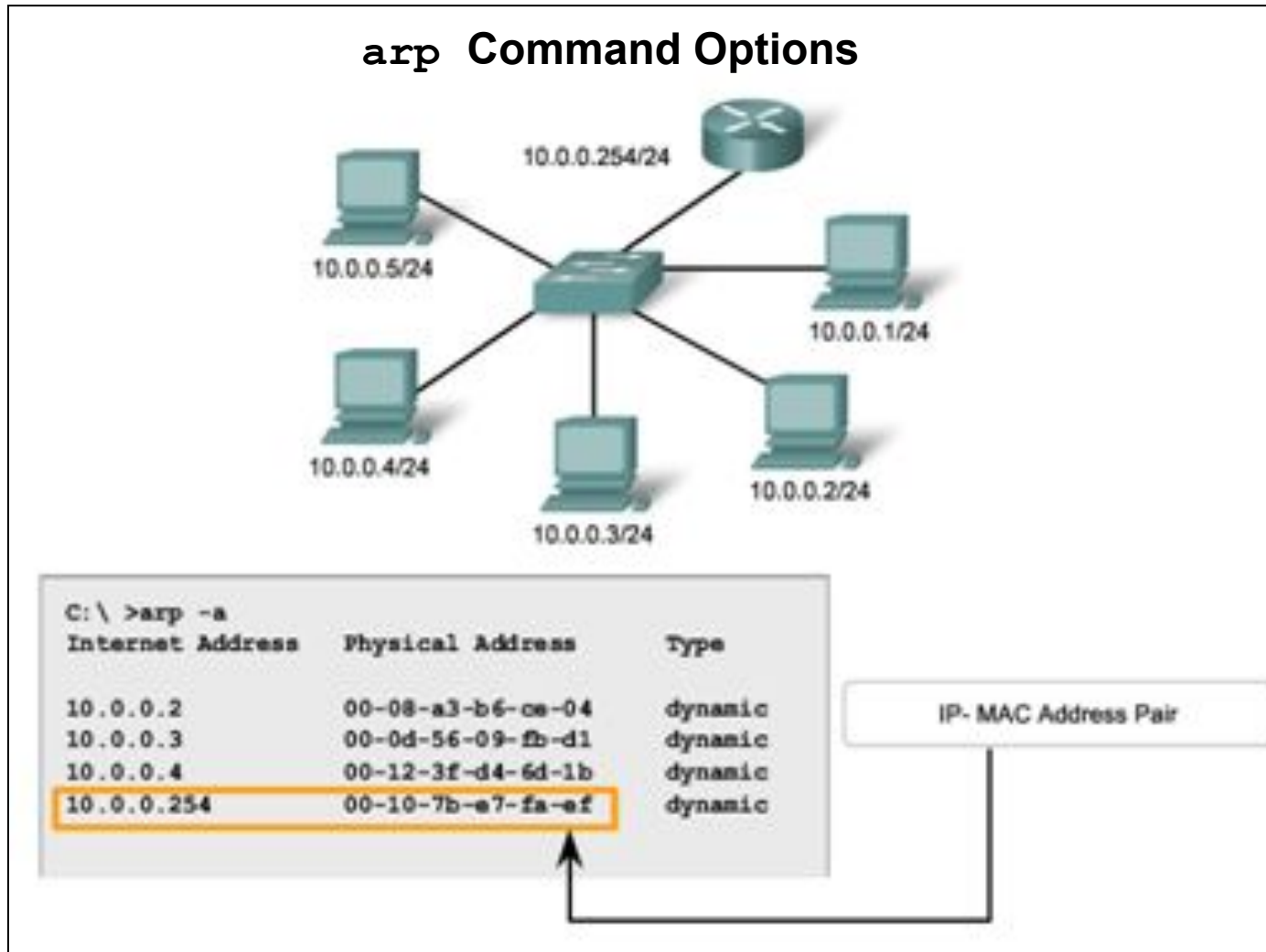
`show cdp neighbors` Command Options

`show cdp neighbors` command provides information about each directly connected CDP neighbor device.

```
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 :
```

Host and IOS Commands
Using the `show ip interface brief` Command

The **show ip interface brief** command verifies the status of all network interfaces on a router or a switch.

```
Router1#show ip interface brief
Interface          IP-Address        OK?  Method  Status                 Protocol
FastEthernet0/0    192.168.254.254   YES  NVRAM   up                     up
FastEthernet0/1/0  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

Router1#ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Router1#traceroute 192.168.0.1
Type escape sequence to abort.
Tracing the route to 192.168.0.1
  1 172.16.0.253 8 msec 4 msec 8 msec
  2 10.0.0.254 16 msec 16 msec 8 msec
  3 192.168.0.1 16 msec * 20 msec
```

11.4 Managing IOS Configuration Files

Router File Systems

`show file systems` command – Lists all of the available file systems on a Cisco 1941 route.

The asterisk (*) indicates this is the current default file system.

```
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:
```

Switch File Systems

The **show file systems** command lists all of the available file systems on a Catalyst 2960 switch.

```
Switch#show file systems
File Systems:

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

Backup and Restore Using Text Files

Saving to a Text File in TeraTerm

In the terminal session:
1. Start the log process
2. Issue a **show running-config** command
3. Close the log

Backup and Restore Using TFTP

- Configuration files can be stored on a Trivial File Transfer Protocol (TFTP) server.

- **copy running-config tftp** – Saves the running configuration to a TFTP server.

- **copy startup-config tftp** – Saves the startup configuration to a TFTP server.

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

Using USB Interfaces on a Cisco Router

- USB flash drive must be formatted in a FAT16 format.

- Can hold multiple copies of the Cisco IOS and multiple router configurations.

- Allows administrator to easily move configurations from router to router.

USB Ports

Backup and Restore Using USB

Backup to USB Drive

```
R1#copy running-config usbflash0:/   ()
Destination filename [running-config]? R1-Config
5024 bytes copied in 0.736 secs (6826 bytes/sec)
```

Copying to USB flash drive, and no file pre-exists

```
R1#copy running-config usbflash0:/
Destination filename [running-config]? R1-Config
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
5024 bytes copied in 1.796 secs (2797 bytes/sec)
```

Copying to USB flash drive, and the same configuration file already exists on the drive.

11.5 Summary

Chapter 11: Summary

In this chapter, you learned:

- Good network design incorporates reliability, scalability, and availability.

- Networks must be secured from viruses, Trojan horses, worms and network attacks.

- Document Basic Network Performance.

- Test network connectivity using `ping` and `traceroute`.

- Use IOS commands to monitor and view information about the network and network devices.

- Back up configuration files using TFTP or USB.