CCNA 1 (network Fundamentals)

1

Outline

- 1 Networking Today
- 2 Basic Switch and End Device Configuration
- 3 Protocols and Models
- 4 Physical Layer
- 5 Number Systems
- 6 Data Link Layer
- 7 Ethernet Switching
- 8 Network Layer
- 9 Address Resolution
- 10 Basic Router Configuration
- 11 IPv4 Addressing
- 12 IPv6 Addressing
- 13 ICMP
- 14 Transport Layer
- 15 Application Layer
- 16 Network Security Fundamentals
- 17 Build a Small Network

2

Module 1: Networking Today

Instructor Materials

Introduction to Networks v7.0 (ITN)

3

Module 1: Networking Today

Introduction to Networks v7.0 (ITN)

16

Module Objectives

Module Title: Networking Today

Module Objective: Explain the advances in modern technologies.

Topic Title	Topic Objective
Networks Affect our Lives	Explain how networks affect our daily lives.
Network Components	Explain how host and network devices are used.
Network Representations and Topologies	Explain network representations and how they are used in network topologies.
Common Types of Networks	Compare the characteristics of common types of networks.
Internet Connections	Explain how LANs and WANs interconnect to the internet.
Reliable Networks	Describe the four basic requirements of a reliable network.
Network Trends	Explain how trends such as BYOD, online collaboration, video, and cloud computing are changing the way we interact.
Network Security	Identify some basic security threats and solution for all networks.
The IT Professional	Explain employment opportunities in the networking field.

 17

17

1.1 Networks Affect Our Lives

 18

18

Networking Today

Networks Connect Us

Communication is almost as important to us as our reliance on air, water, food, and shelter. In today's world, through the use of networks, we are connected like never before.

 19

19

Networking Today

Video – The Cisco Networking Academy Learning Experience

Cisco Networking Academy: learn how we use technology to make the world a better place.

 20

20

Networking Today

No Boundaries

- World without boundaries
- Global communities
- Human network

21

1.2 Network Components

22

Network Components

Host Roles

Every computer on a network is called a host or end device.

Servers are computers that provide information to end devices:

- email servers
- web servers
- file server

Clients are computers that send requests to the servers to retrieve information:

- web page from a web server
- email from an email server

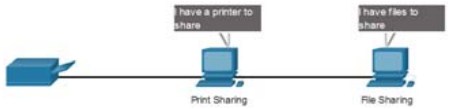
Server Type	Description
Email	Email server runs email server software. Clients use client software to access email.
Web	Web server runs web server software. Clients use browser software to access web pages.
File	File server stores corporate and user files. The client devices access these files.

23

Network Components

Peer-to-Peer

It is possible to have a device be a client and a server in a Peer-to-Peer Network. This type of network design is only recommended for very small networks.



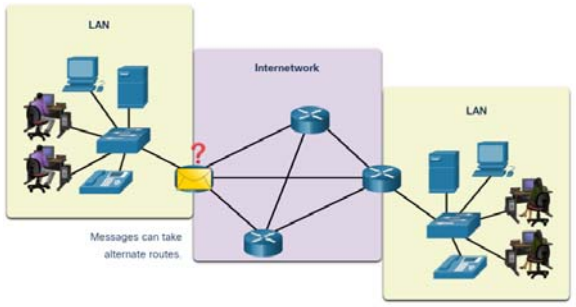
Advantages	Disadvantages
Easy to set up	No centralized administration
Less complex	Not as secure
Lower cost	Not scalable
Used for simple tasks: transferring files and sharing printers	Slower performance

24

Network Components

End Devices

An end device is where a message originates from or where it is received. Data originates with an end device, flows through the network, and arrives at an end device.



25

Network Components

Intermediary Network Devices

An intermediary device interconnects end devices. Examples include switches, wireless access points, routers, and firewalls.

Management of data as it flows through a network is also the role of an intermediary device, including:

- Regenerate and retransmit data signals.
- Maintain information about what pathways exist in the network.
- Notify other devices of errors and communication failures.

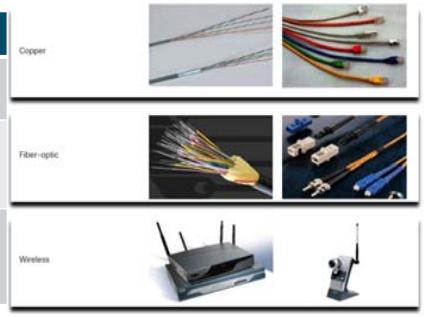
26

Network Components

Network Media

Communication across a network is carried through a medium which allows a message to travel from source to destination.

Media Types	Description
Metal wires within cables	Uses electrical impulses
Glass or plastic fibers within cables (fiber-optic cable)	Uses pulses of light.
Wireless transmission	Uses modulation of specific frequencies of electromagnetic waves.



27

1.3 Network Representations and Topologies

28

Network Representations and Topologies

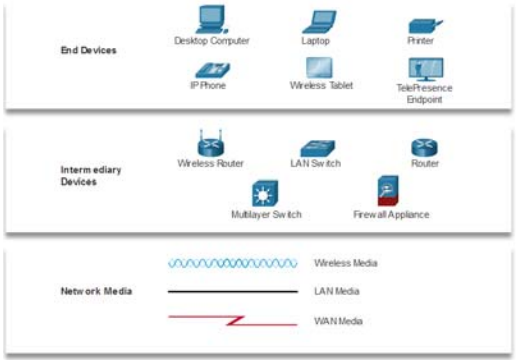
Network Representations

Network diagrams, often called topology diagrams, use symbols to represent devices within the network.

Important terms to know include:

- Network Interface Card (NIC)
- Physical Port
- Interface

Note: Often, the terms port and interface are used interchangeably



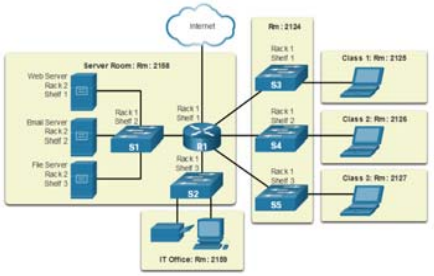
29

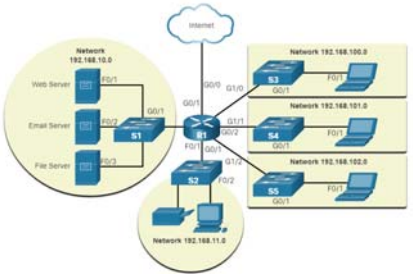
Network Representations and Topologies

Topology Diagrams

Physical topology diagrams illustrate the physical location of intermediary devices and cable installation.

Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network.





30

1.4 Common Types of Networks

31

Common Types of Networks

Networks of Many Sizes

Small Home

SOHO

Medium/Large

World Wide

- Small Home Networks – connect a few computers to each other and the Internet
- Small Office/Home Office – enables computer within a home or remote office to connect to a corporate network
- Medium to Large Networks – many locations with hundreds or thousands of interconnected computers
- World Wide Networks – connects hundreds of millions of computers world-wide – such as the internet

32

Common Types of Networks

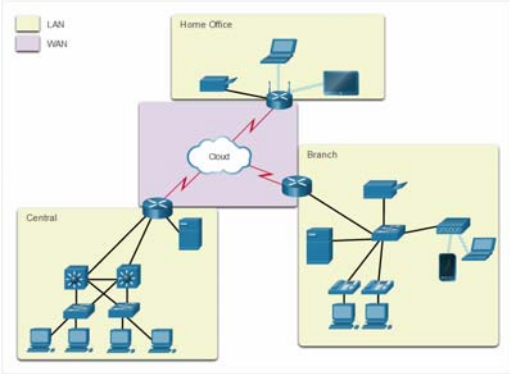
LANs and WANs

Network infrastructures vary greatly in terms of:

- Size of the area covered
- Number of users connected
- Number and types of services available
- Area of responsibility

Two most common types of networks:

- Local Area Network (LAN)
- Wide Area Network (WAN).

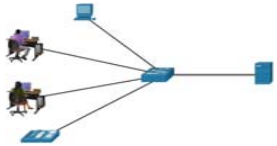


33

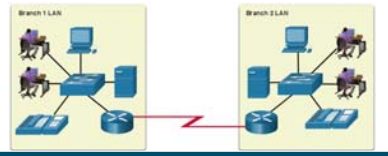
Common Types of Networks

LANs and WANs (cont.)

A LAN is a network infrastructure that spans a small geographical area.



A WAN is a network infrastructure that spans a wide geographical area.



LAN	WAN
Interconnect end devices in a limited area.	Interconnect LANs over wide geographical areas.
Administered by a single organization or individual.	Typically administered by one or more service providers.
Provide high-speed bandwidth to internal devices.	Typically provide slower speed links between LANs.

34

Common Types of Networks

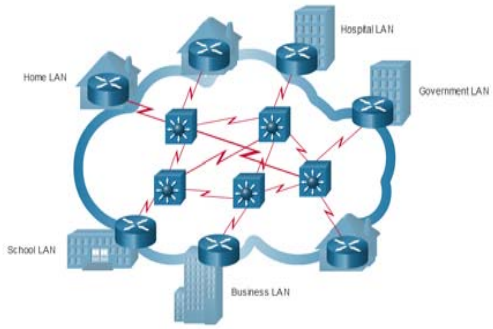
The Internet

The internet is a worldwide collection of interconnected LANs and WANs.

- LANs are connected to each other using WANs.
- WANs may use copper wires, fiber optic cables, and wireless transmissions.

The internet is not owned by any individual or group. The following groups were developed to help maintain structure on the internet:

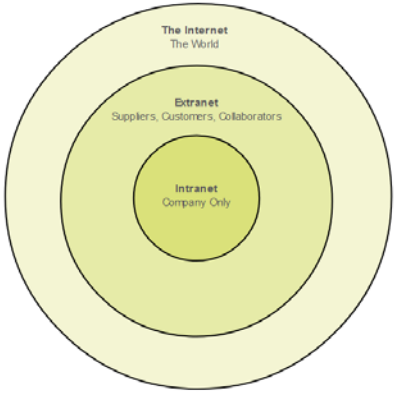
- IETF
- ICANN
- IAB



35

Common Types of Networks

Intranets and Extranets



An intranet is a private collection of LANs and WANs internal to an organization that is meant to be accessible only to the organizations members or others with authorization.

An organization might use an extranet to provide secure access to their network for individuals who work for a different organization that need access to their data on their network.

36

1.5 Internet Connections

37

Internet Connections

Internet Access Technologies

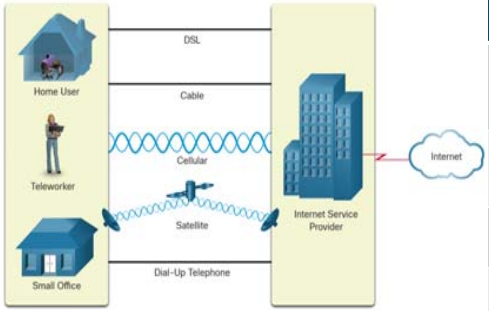
There are many ways to connect users and organizations to the internet:

- Popular services for home users and small offices include broadband cable, broadband digital subscriber line (DSL), wireless WANs, and mobile services.
- Organizations need faster connections to support IP phones, video conferencing and data center storage.
- Business-class interconnections are usually provided by service providers (SP) and may include: business DSL, leased lines, and Metro Ethernet.

38

Internet Connections

Home and Small Office Internet Connections



Connection	Description
Cable	high bandwidth, always on, internet offered by cable television service providers.
DSL	high bandwidth, always on, internet connection that runs over a telephone line.
Cellular	uses a cell phone network to connect to the internet.
Satellite	major benefit to rural areas without Internet Service Providers.
Dial-up telephone	an inexpensive, low bandwidth option using a modem.

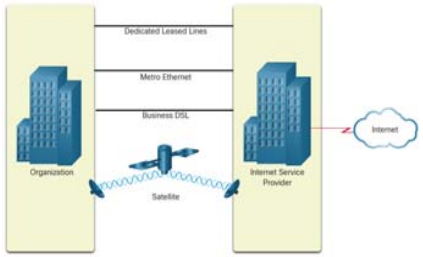
39

Internet Connections

Businesses Internet Connections

Corporate business connections may require:

- higher bandwidth
- dedicated connections
- managed services



Type of Connection	Description
Dedicated Leased Line	These are reserved circuits within the service provider's network that connect distant offices with private voice and/or data networking.
Ethernet WAN	This extends LAN access technology into the WAN.
DSL	Business DSL is available in various formats including Symmetric Digital Subscriber Lines (SDSL).
Satellite	This can provide a connection when a wired solution is not available.

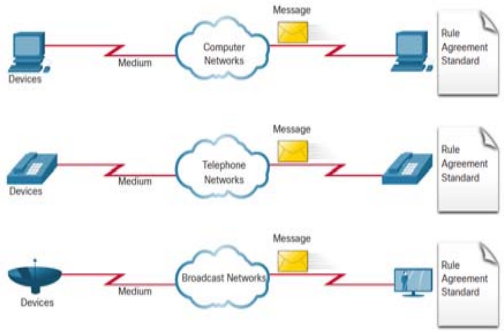
40

Internet Connections

The Converging Network

Before converged networks, an organization would have been separately cabled for telephone, video, and data. Each of these networks would use different technologies to carry the signal.

Each of these technologies would use a different set of rules and standards.



41

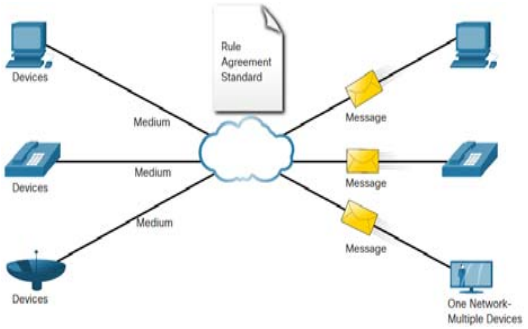
Internet Connections

The Converging Network (Cont.)

Converged data networks carry multiple services on one link including:

- data
- voice
- video

Converged networks can deliver data, voice, and video over the same network infrastructure. The network infrastructure uses the same set of rules and standards.



42

Internet Connections

Video – Download and Install Packet Tracer

This video will demonstrate the download and install process of Packet Tracer.

43

Internet Connections

Video – Getting Started in Cisco Packet Tracer

This video will cover the following:

- Navigate the Packet Tracer interface
- Customize the Packet Tracer Interface

44

Internet Connections

Packet Tracer – Network Representation

In this Packet tracer you will do the following:

- The network model in this activity incorporates many of the technologies that you will master in your CCNA studies.

Note: It is not important that you understand everything you see and do in this activity.

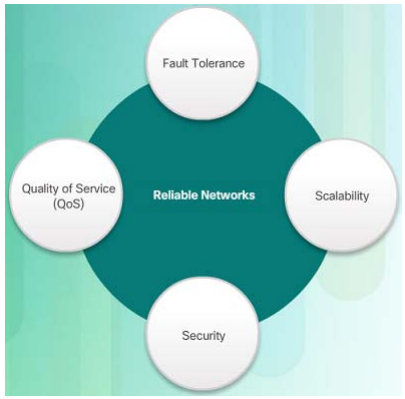
45

1.6 Reliable Networks

46

Reliable Network

Network Architecture



Network Architecture refers to the technologies that support the infrastructure that moves data across the network.

There are four basic characteristics that the underlying architectures need to address to meet user expectations:

- Fault Tolerance
- Scalability
- Quality of Service (QoS)
- Security

47

Reliable Network

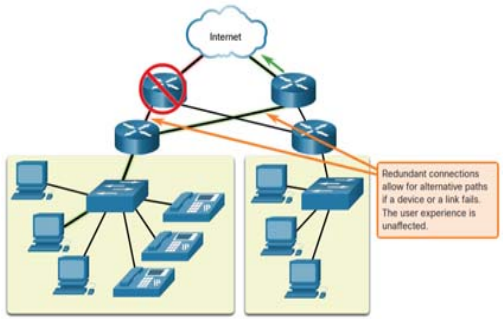
Fault Tolerance

A fault tolerant network limits the impact of a failure by limiting the number of affected devices. Multiple paths are required for fault tolerance.

Reliable networks provide redundancy by implementing a packet switched network:

- Packet switching splits traffic into packets that are routed over a network.
- Each packet could theoretically take a different path to the destination.

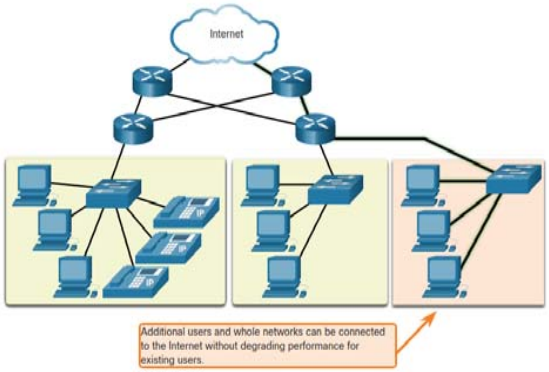
This is not possible with circuit-switched networks which establish dedicated circuits.



48

Reliable Network

Scalability



A scalable network can expand quickly and easily to support new users and applications without impacting the performance of services to existing users.

Network designers follow accepted standards and protocols in order to make the networks scalable.

49

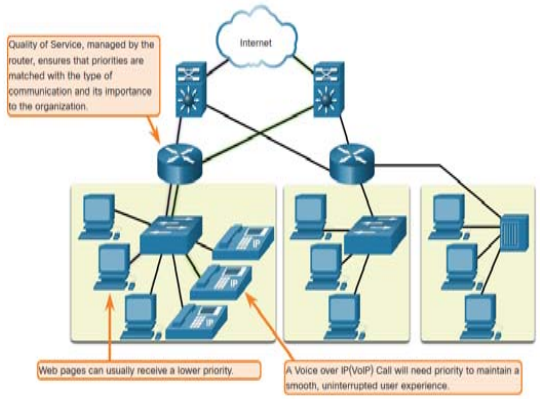
Reliable Network

Quality of Service

Voice and live video transmissions require higher expectations for those services being delivered.

Have you ever watched a live video with constant breaks and pauses? This is caused when there is a higher demand for bandwidth than available – and QoS isn't configured.

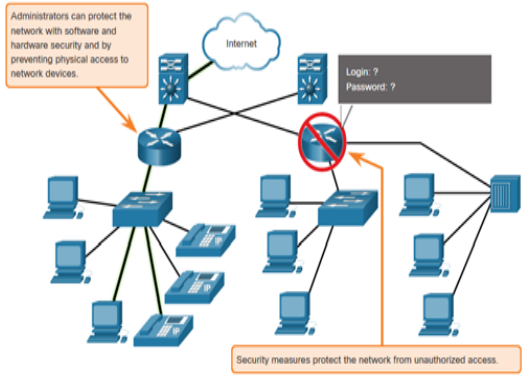
- Quality of Service (QoS) is the primary mechanism used to ensure reliable delivery of content for all users.
- With a QoS policy in place, the router can more easily manage the flow of data and voice traffic.



50

Reliable Network

Network Security



There are two main types of network security that must be addressed:

- Network infrastructure security
  - Physical security of network devices
  - Preventing unauthorized access to the devices
- Information Security
  - Protection of the information or data transmitted over the network

Three goals of network security:

- Confidentiality – only intended recipients can read the data
- Integrity – assurance that the data has not be altered with during transmission
- Availability – assurance of timely and reliable access to data for authorized users

51

1.7 Network Trends

52

Network Trends

Recent Trends

The role of the network must adjust and continually transform in order to be able to keep up with new technologies and end user devices as they constantly come to the market.

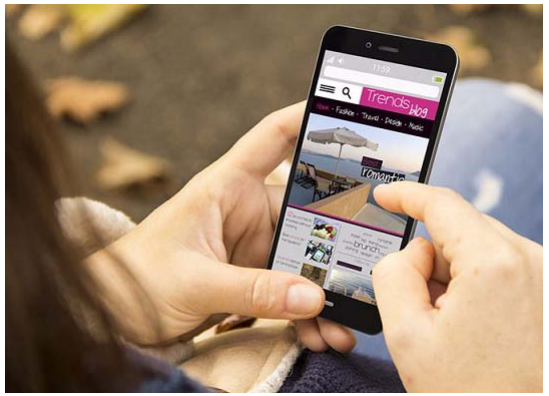
Several new networking trends that effect organizations and consumers:

- Bring Your Own Device (BYOD)
- Online collaboration
- Video communications
- Cloud computing

53

Network Trends

Bring Your Own Device



Bring Your Own Device (BYOD) allows users to use their own devices giving them more opportunities and greater flexibility.

BYOD allows end users to have the freedom to use personal tools to access information and communicate using their:

- Laptops
- Netbooks
- Tablets
- Smartphones
- E-readers

BYOD means any device, with any ownership, used anywhere.

54

Network Trends

Online Collaboration

- Collaborate and work with others over the network on joint projects.
- Collaboration tools including Cisco WebEx (shown in the figure) gives users a way to instantly connect and interact.
- Collaboration is a very high priority for businesses and in education.
- Cisco Webex Teams is a multifunctional collaboration tool.
  - send instant messages
  - post images
  - post videos and links

55

Network Trends

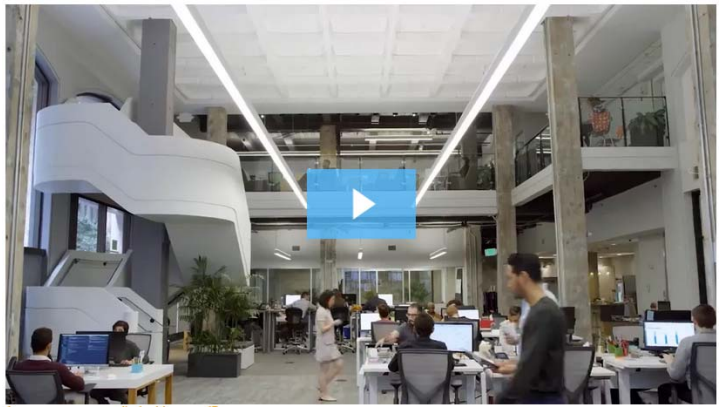
Video Communication

- Video calls are made to anyone, regardless of where they are located.
- Video conferencing is a powerful tool for communicating with others.
- Video is becoming a critical requirement for effective collaboration.
- Cisco TelePresence powers is one way of working where everyone, everywhere.

56

Network Trends

Video – Cisco WebEx for Huddles



57

Network Trends

Cloud Computing

Cloud computing allows us to store personal files or backup our data on servers over the internet.

- Applications can also be accessed using the Cloud.
- Allows businesses to deliver to any device anywhere in the world.

Cloud computing is made possible by data centers.

- Smaller companies that can't afford their own data centers, lease server and storage services from larger data center organizations in the Cloud.

58

Network Trends

Cloud Computing (Cont.)

Four types of Clouds:

- Public Clouds
  - Available to the general public through a pay-per-use model or for free.
- Private Clouds
  - Intended for a specific organization or entity such as the government.
- Hybrid Clouds
  - Made up of two or more Cloud types – for example, part custom and part public.
  - Each part remains a distinctive object but both are connected using the same architecture.
- Custom Clouds
  - Built to meet the needs of a specific industry, such as healthcare or media.
  - Can be private or public.

59

Network Trends

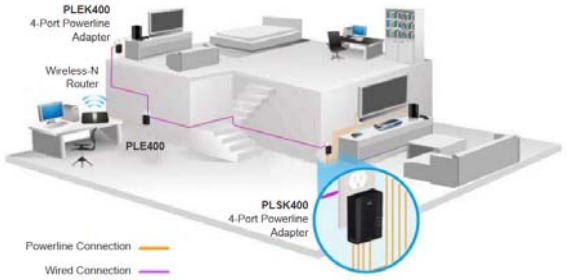
Technology Trends in the Home

- Smart home technology is a growing trend that allows technology to be integrated into every-day appliances which allows them to interconnect with other devices.
- Ovens might know what time to cook a meal for you by communicating with your calendar on what time you are scheduled to be home.
- Smart home technology is currently being developed for all rooms within a house.

60

Network Trends

Powerline Networking



- Powerline networking can allow devices to connect to a LAN where data network cables or wireless communications are not a viable option.
- Using a standard powerline adapter, devices can connect to the LAN wherever there is an electrical outlet by sending data on certain frequencies.
- Powerline networking is especially useful when wireless access points cannot reach all the devices in the home.

61

Network Trends

Wireless Broadband

In addition to DSL and cable, wireless is another option used to connect homes and small businesses to the internet.

- More commonly found in rural environments, a Wireless Internet Service Provider (WISP) is an ISP that connects subscribers to designated access points or hotspots.
- Wireless broadband is another solution for the home and small businesses.
  - Uses the same cellular technology used by a smart phone.
  - An antenna is installed outside the house providing wireless or wired connectivity for devices in the home.

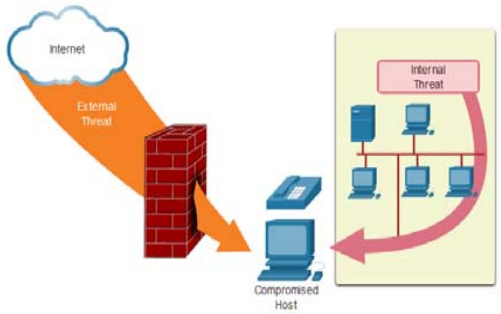
62

1.8 Network Security

63

Network Security

Security Threats

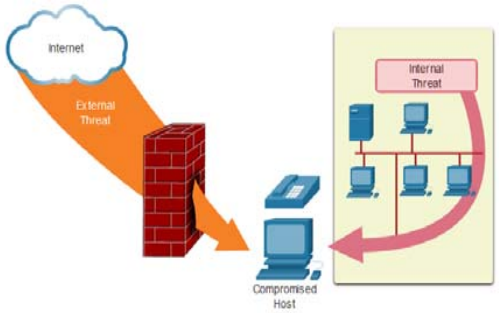


- Network security is an integral part of networking regardless of the size of the network.
- The network security that is implemented must take into account the environment while securing the data, but still allowing for quality of service that is expected of the network.
- Securing a network involves many protocols, technologies, devices, tools, and techniques in order to secure data and mitigate threats.
- Threat vectors might be external or internal.

64

Network Security

Security Threats (Cont.)



External Threats:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks
- Threat Actor attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

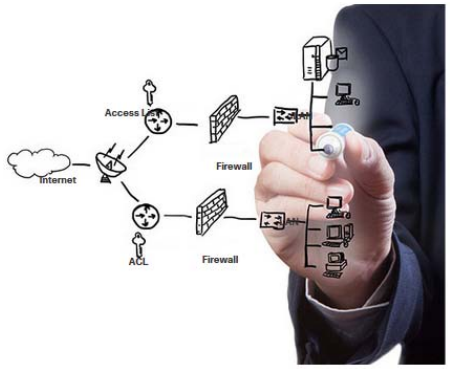
Internal Threats:

- lost or stolen devices
- accidental misuse by employees
- malicious employees

65

Network Security

Security Solutions



Security must be implemented in multiple layers using more than one security solution.

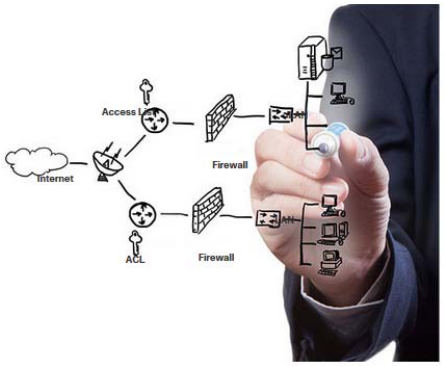
Network security components for home or small office network:

- Antivirus and antispyware software should be installed on end devices.
- Firewall filtering used to block unauthorized access to the network.

66

Network Security

Security Solutions (Cont.)



Larger networks have additional security requirements:

- Dedicated firewall system
- Access control lists (ACL)
- Intrusion prevention systems (IPS)
- Virtual private networks (VPN)

The study of network security starts with a clear understanding of the underlying switching and routing infrastructure.

67

1.9 The IT Professional

68

The IT Professional

CCNA

The Cisco Certified Network Associate (CCNA) certification:

- demonstrates that you have a knowledge of foundational technologies
- ensures you stay relevant with skills needed for the adoption of next-generation technologies.

The new CCNA focus:

- IP foundation and security topics
- Wireless, virtualization, automation, and network programmability.

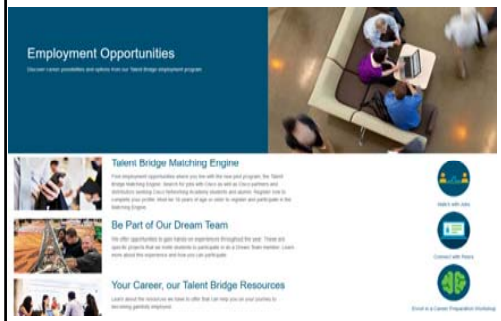
New DevNet certifications at the associate, specialist and professional levels, to validate your software development skills.

Specialist certification validate your skills in line with your job role and interests.

69

The IT Professional

Networking Jobs



At www.netacad.com you can click the Careers menu and then select Employment opportunities.

- Find employment opportunities by using the Talent Bridge Matching Engine.
- Search for jobs with Cisco, Cisco partners and distributors seeking Cisco Networking Academy students and alumni.

70

The IT Professional

Lab – Researching IT and Networking Job Opportunities

In this lab, you will complete the following objectives:

- Research Job Opportunities
- Reflect on Research

71

1.10 Module Practice and Quiz

72

Module Practice and Quiz

What did I learn in this module?

- Through the use of networks, we are connected like never before.
- All computers that are connected to a network and participate directly in network communication are classified as hosts.
- Diagrams of networks often use symbols to represent the different devices and connections that make up a network.
- A diagram provides an easy way to understand how devices connect in a large network.
- The two types of network infrastructures are Local Area Networks (LANs), and Wide Area Networks (WANs).
- SOHO internet connections include cable, DSL, Cellular, Satellite, and Dial-up telephone.
- Business internet connections include Dedicated Leased Line, Metro Ethernet, Business DSL, and Satellite.

73

Module Practice and Quiz

What did I learn in this module? (Cont.)

- Network architecture refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move data across the network.
- There are four basic characteristics of network architecture: Fault Tolerance, Scalability, Quality of Service (QoS), and Security.
- Recent networking trends that affect organizations and consumers: Bring Your Own Device (BYOD), online collaboration, video communications, and cloud computing.
- There are several common external and internal threats to networks.
- Larger networks and corporate networks use antivirus, antispyware, and firewall filtering, but they also have other security requirements: Dedicated firewall systems, Access control lists (ACL), Intrusion prevention systems (IPS), and Virtual private networks (VPN)
- The Cisco Certified Network Associate (CCNA) certification demonstrates your knowledge of foundational technologies.

74

Module 1

New Terms and Commands

- Peer-to-Peer File Sharing
- Small Office/Home Office or SOHO
- Medium to large network
- Server
- Client
- Peer-to-Peer network
- End device
- Intermediary device
- Medium
- Network Interface Card (NIC)
- Physical Port
- Interface
- Physical topology diagram
- Logical topology diagram
- Local Area Network (LAN)
- Wide Area Network (WAN)
- Internet
- Intranet
- Extranet
- Internet Service Provider (ISP)
- Converged networks
- Network architecture
- Fault tolerant network
- Packet-switched network
- Circuit-switched network
- Scalable network
- Quality of Service (Qos)
- Network bandwidth
- Bring Your Own Device (BYOD)
- Collaboration
- Cloud computing
- Private clouds
- Hybrid clouds
- Public clouds
- Custom clouds
- Data center
- Smart home technology
- Powerline networking
- Wireless Internet Service Provider (WISP)
- Network architecture

75

Module 2: Basic Switch and End Device Configuration

Instructor Materials

Introduction to Networks v7.0 (ITN)

76

What to Expect in this Module

- To facilitate learning, the following features within the GUI may be included in this module:

Feature	Description
Animations	Expose learners to new skills and concepts.
Videos	Expose learners to new skills and concepts.
Check Your Understanding(CYU)	Per topic online quiz to help learners gauge content understanding.
Interactive Activities	A variety of formats to help learners gauge content understanding.
Syntax Checker	Small simulations that expose learners to Cisco command line to practice configuration skills.
PT Activity	Simulation and modeling activities designed to explore, acquire, reinforce, and expand skills.

78

What to Expect in this Module (Cont.)

- To facilitate learning, the following features may be included in this module:

Feature	Description
Packet Tracer Physical Mode Activity	These activities are completed using Packet Tracer in Physical Mode.
Hands-On Labs	Labs designed for working with physical equipment.
Class Activities	These are found on the Instructor Resources page. Class Activities are designed to facilitate learning, class discussion, and collaboration.
Module Quizzes	Self-assessments that integrate concepts and skills learned throughout the series of topics presented in the module.
Module Summary	Briefly recaps module content.

79

Module 2: Basic Switch and End Device Configuration

Introductions to Networks v7.0 (ITN)

89

Module Objectives

Module Title: Basic Switch and End Device Configuration

Module Objective: Implement initial settings including passwords, IP addressing, and default gateway parameters on a network switch and end devices.

Topic Title	Topic Objective
Cisco IOS Access	Explain how to access a Cisco IOS device for configuration purposes.
IOS Navigation	Explain how to navigate Cisco IOS to configure network devices.
The Command Structure	Describe the command structure of Cisco IOS software.
Basic Device Configuration	Configure a Cisco IOS device using CLI.
Save Configurations	Use IOS commands to save the running configuration.
Ports and Addresses	Explain how devices communicate across network media.
Configure IP Addressing	Configure a host device with an IP address.
Verify Connectivity	Verify connectivity between two end devices.

90

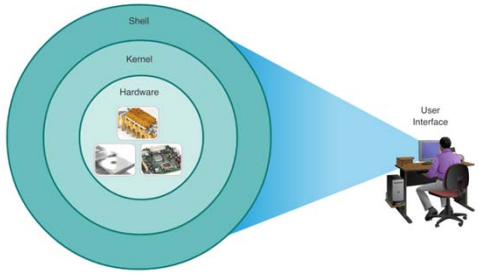
2.1 Cisco IOS Access

91

Cisco IOS Access

Operating Systems

- **Shell** - The user interface that allows users to request specific tasks from the computer. These requests can be made either through the CLI or GUI interfaces.
- **Kernel** - Communicates between the hardware and software of a computer and manages how hardware resources are used to meet software requirements.
- **Hardware** - The physical part of a computer including underlying electronics.



92

Cisco IOS Access

GUI

- A GUI allows the user to interact with the system using an environment of graphical icons, menus, and windows.
- A GUI is more user-friendly and requires less knowledge of the underlying command structure that controls the system.
- Examples of these are: Windows, macOS, Linux KDE, Apple iOS and Android.
- GUIs can fail, crash, or simply not operate as specified. For these reasons, network devices are typically accessed through a CLI.

93

Cisco IOS Access

Purpose of an OS

PC operating system enables a user to do the following:

- Use a mouse to make selections and run programs
- Enter text and text-based commands

CLI-based network operating system enables a network technician to do the following:

- Use a keyboard to run CLI-based network programs
- Use a keyboard to enter text and text-based commands
- View output on a monitor

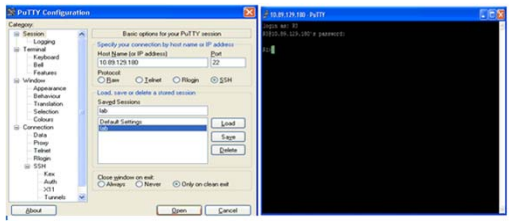
```
analyst@secOps ~]$ ls
Desktop  Downloads  lab.support.files  second_drive
[analyst@secOps ~]$
```


94

Cisco IOS Access

Access Methods

- **Console** – A physical management port used to access a device in order to provide maintenance, such as performing the initial configurations.
- **Secure Shell (SSH)** – Establishes a secure remote CLI connection to a device, through a virtual interface, over a network. (Note: This is the recommended method for remotely connecting to a device.)
- **Telnet** – Establishes an insecure remote CLI connection to a device over the network. (Note: User authentication, passwords and commands are sent over the network in plaintext.)

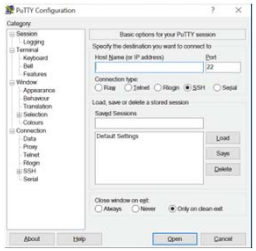


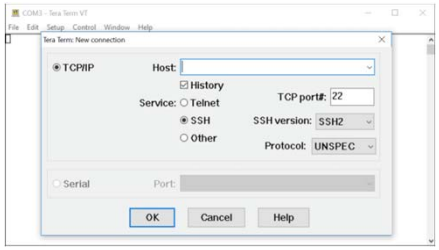
95

Cisco IOS Access

Terminal Emulation Programs

- Terminal emulation programs are used to connect to a network device by either a console port or by an SSH/Telnet connection.
- There are several terminal emulation programs to chose from such as PuTTY, Tera Term and SecureCRT.





96

2.2 IOS Navigation

97

IOS Navigation

Primary Command Modes

User EXEC Mode:

- Allows access to only a limited number of basic monitoring commands
- Identified by the CLI prompt that ends with the > symbol

```
Router>

Switch>
```

Privileged EXEC Mode:

- Allows access to all commands and features
- Identified by the CLI prompt that ends with the # symbol

```
Router#

Switch#
```


98

IOS Navigation

Configuration Mode and Subconfiguration Modes

Global Configuration Mode:

- Used to access configuration options on the device

```
Switch(config)#
```

Line Configuration Mode:

- Used to configure console, SSH, Telnet or AUX access

```
Switch(config-line)#
```

Interface Configuration Mode:

- Used to configure a switch port or router interface

```
Switch(config-if)#
```


99

IOS Navigation

Video – IOS CLI Primary Command Modes

This video will cover the following:

- User EXEC mode
- Privilege EXEC mode
- Global Config mode

100

IOS Navigation

Navigation Between IOS Modes

- **Privileged EXEC Mode:**
  - To move from user EXEC mode to privilege EXEC mode, use the **enabled** command.

```
Switch> enable
Switch#
```

- **Global Configuration Mode:**
  - To move in and out of global configuration mode, use the **configure terminal** command. To return to privilege EXEC mode, use the **exit** command.

```
Switch(config)#
Switch(config)#exit
Switch#
```

- **Line Configuration Mode:**
  - To move in and out of line configuration mode, use the **line** command followed by the management line type. To return to global configuration mode, use the **exit** command.

```
Switch(config)#line console 0
Switch(config-line)#exit
Switch(config)#
```


101

IOS Navigation

Navigation Between IOS Modes (Cont.)

Subconfiguration Modes:

- To move out of any subconfiguration mode to get back to global configuration mode, use the **exit** command. To return to privilege EXEC mode, use the **end** command or key combination **Ctrl +Z**.

```
Switch(config)#line console 0
Switch(config-line)#end
Switch#
```

- To move directly from one subconfiguration mode to another, type in the desired subconfiguration mode command. In the example, the command prompt changes from **(config-line)#** to **(config-if)#**.

```
Switch(config-line)#interface FastEthernet 0/1
Switch(config-if)#
```


102

IOS Navigation

Video – Navigation Between IOS Modes

This video will cover the following:

- enable
- disable
- configure terminal
- exit
- end
- Control + Z on keyboard
- Other commands to enter sub configuration modes

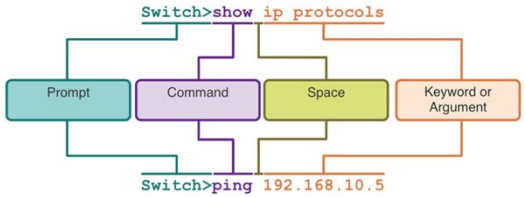
103

2.3 The Command Structure

104

The Command Structure

Basic IOS Command Structure



- **Keyword** – This is a specific parameter defined in the operating system (in the figure, **ip protocols**).
- **Argument** - This is not predefined; it is a value or variable defined by the user (in the figure, **192.168.10.5**).

105

The Command Structure

IOS Command Syntax Check

A command might require one or more arguments. To determine the keywords and arguments required for a command, refer to the command syntax.

- Boldface text indicates commands and keywords that are entered as shown.
- Italic text indicates an argument for which the user provides the value.

Convention	Description
boldface	Boldface text indicates commands and keywords that you enter literally as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets indicate an optional element (keyword or argument).
{x}	Braces indicate a required element (keyword or argument).
[x {y | z }]	Braces and vertical lines within square brackets indicate a required choice within an optional element. Spaces are used to clearly delineate parts of the command.

106

The Command Structure

IOS Command Syntax Check (Cont.)

- The command syntax provides the pattern, or format, that must be used when entering a command.
- The command is **ping** and the user-defined argument is the *ip-address* of the destination device. For example, **ping 10.10.10.5**.

```
ping ip-address
```

- The command is **traceroute** and the user-defined argument is the *ip-address* of the destination device. For example, **traceroute 192.168.254.254**.

```
traceroute ip-address
```

- If a command is complex with multiple arguments, you may see it represented like this:

```
Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}}
```


107

The Command Structure

IOS Help Features

The IOS has two forms of help available: context-sensitive help and command syntax check.

- Context-sensitive help enables you to quickly find answers to these questions:
  - Which commands are available in each command mode?
  - Which commands start with specific characters or group of characters?
  - Which arguments and keywords are available to particular commands?

```
Router#ping ?
  WORD  Ping destination address or hostname
  ip    IP echo
  ipv6  IPv6 echo
```

- Command syntax check verifies that a valid command was entered by the user.
  - If the interpreter cannot understand the command being entered, it will provide feedback describing what is wrong with the command.

```
Switch#interface fastEthernet 0/1
                           ^
% Invalid input detected at '^' marker.
```


108

The Command Structure

Video – Context Sensitive Help and Command Syntax Checker

This video will cover the following:

- Use the help command in user EXEC, privileged EXEC, and global config mode
- Finish commands and arguments with the help command
- Use the command syntax checker to fix syntax errors and incomplete commands

109

The Command Structure

Hot Keys and Shortcuts

- The IOS CLI provides hot keys and shortcuts that make configuring, monitoring, and troubleshooting easier.
- Commands and keywords can be shortened to the minimum number of characters that identify a unique selection. For example, the **configure** command can be shortened to **conf** because **configure** is the only command that begins with **conf**.

```
Router#con
% Ambiguous command: "con"
Router#con?
configure  connect
```

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```


110

The Command Structure

Hot Keys and Shortcuts (Cont.)

- The table below is a brief list of keystrokes to enhance command line editing.

Keystroke	Description
Tab	Completes a partial command name entry.
Backspace	Erases the character to the left of the cursor.
Left Arrow or **Ctrl+B**	Moves the cursor one character to the left.
Right Arrow or **Ctrl+F**	Moves the cursor one character to the right.
Up Arrow or **Ctrl+P**	Recalls the commands in the history buffer, beginning with the most recent commands.

 111

111

The Command Structure

Hot Keys and Shortcuts (Cont.)

- When a command output produces more text than can be displayed in a terminal window, the IOS will display a **"--More--"** prompt. The table below describes the keystrokes that can be used when this prompt is displayed.

Keystroke	Description
Enter Key	Displays the next line.
Space Bar	Displays the next screen.
Any other key	Ends the display string, returning to privileged EXEC mode.

- The table below lists commands that can be used to exit out of an operation.

Keystroke	Description
Ctrl-C	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
Ctrl-Z	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
Ctrl-Shift-6	All-purpose break sequence used to abort DNS lookups, traceroutes, pings, etc.

Note: To see more hot keys and shortcuts refer to 2.3.5.

 112

112

The Command Structure

Video – Hot Keys and Shortcuts

This video will cover the following:

- Tab key (tab completion)
- Command shortening
- Up and down arrow key
- CTRL + C
- CTRL + Z
- CTRL + Shift + 6
- CTRL + R

 113

113

The Command Structure

Packet Tracer – Navigate the IOS

In this Packet Tracer, you will do the following:

- Establish Basic Connections, Access the CLI, and Explore Help
- Explore EXEC Modes
- Set the Clock

 114

114

The Command Structure

Packet Tracer - Navigate the IOS by Using Tera Term for Console Connectivity – Physical Mode
Lab - Navigate the IOS by Using Tera Term for Console Connectivity

In both the Packet Tracer Physical Mode activity and in the Lab, you will complete the following objectives:

- Access a Cisco Switch through the Serial Console Port
- Display and Configure Basic Device Settings
- Access a Cisco Router Using a Mini-USB Console Cable (Note: This objective is optional in the Lab.)

115

2.4 Basic Device Configuration

116

Basic Device Configuration

Device Names

- The first configuration command on any device should be to give it a unique hostname.
- By default, all devices are assigned a factory default name. For example, a Cisco IOS switch is "Switch."
- Guideline for naming devices:
  - Start with a letter
  - Contain no spaces
  - End with a letter or digit
  - Use only letters, digits, and dashes
  - Be less than 64 characters in length

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

Note: To return the switch to the default prompt, use the **no hostname** global config command.

117

Basic Device Configuration

Password Guidelines

- The use of weak or easily guessed passwords are a security concern.
- All networking devices should limit administrative access by securing privileged EXEC, user EXEC, and remote Telnet access with passwords. In addition, all passwords should be encrypted and legal notifications provided.
- Password Guidelines:
  - Use passwords that are more than eight characters in length.
  - Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.
  - Avoid using the same password for all devices.
  - Do not use common words because they are easily guessed.

Note: Most of the labs in this course use simple passwords such as **cisco** or **class**. These passwords are considered weak and easily guessable and should be avoided in production environments.

118

Basic Device Configuration

Configure Passwords

Securing user EXEC mode access:

- First enter line console configuration mode using the **line console 0** command in global configuration mode.
- Next, specify the user EXEC mode password using the **password** *password* command.
- Finally, enable user EXEC access using the **login** command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Securing privileged EXEC mode access:

- First enter global configuration mode.
- Next, use the **enable secret** *password* command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```


119

Basic Device Configuration

Configure Passwords (Cont.)

Securing VTY line access:

- First enter line VTY configuration mode using the **line vty 0 15** command in global configuration mode.
- Next, specify the VTY password using the **password** *password* command.
- Finally, enable VTY access using the **login** command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

- Note: VTY lines enable remote access using Telnet or SSH to the device. Many Cisco switches support up to 16 VTY lines that are numbered 0 to 15.

120

Basic Device Configuration

Encrypt Passwords

- The startup-config and running-config files display most passwords in plaintext.
- To encrypt all plaintext passwords, use the **service password-encryption** global config command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

- Use the **show running-config** command to verify that the passwords on the device are now encrypted.

```
Sw-Floor-1# show running-config
!
!
line con 0
password 7 094F471A1A0A
login
!
Line vty 0 4
Password 7 03095A0F034F38435B49150A1819
Login
!
!
end
```


121

Basic Device Configuration

Banner Messages

- A banner message is important to warn unauthorized personnel from attempting to access the device.
- To create a banner message of the day on a network device, use the **banner motd #** *the message of the day* **#** global config command.

Note: The "#" in the command syntax is called the delimiting character. It is entered before and after the message.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only!#
```

The banner will be displayed on attempts to access the device.

```
Press RETURN to get started.


Authorized Access Only!

User Access Verification

Password:
```


122

Basic Device Configuration

Video – Secure Administrative Access to a Switch

This video will cover the following:

- Access the command line to secure the switch
- Secure access to the console port
- Secure virtual terminal access for remote access
- Encrypt passwords on the switch
- Configure the banner message
- Verify security changes

123

2.5 Save Configurations

124

Save Configurations

Configuration Files

- There are two system files that store the device configuration:
  - **startup-config** - This is the saved configuration file that is stored in NVRAM. It contains all the commands that will be used by the device upon startup or reboot. Flash does not lose its contents when the device is powered off.
  - **running-config** - This is stored in Random Access Memory (RAM). It reflects the current configuration. Modifying a running configuration affects the operation of a Cisco device immediately. RAM is volatile memory. It loses all of its content when the device is powered off or restarted.
  - To save changes made to the running configuration to the startup configuration file, use the **copy running-config startup-config** privileged EXEC mode command.

```
Router#show startup-config
Using 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

```
Router#show running-config
Building configuration...

Current configuration : 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```


125

Save Configurations

Alter the Running Configurations

If changes made to the running config do not have the desired effect and the running-config has not yet been saved, you can restore the device to its previous configuration. To do this you can:

- Remove the changed commands individually.
- Reload the device using the **reload** command in privilege EXEC mode. *Note: This will cause the device to briefly go offline, leading to network downtime.*

```
Router# reload
Proceed with reload? [confirm]
Initializing Hardware ...
```

If the undesired changes were saved to the startup-config, it may be necessary to clear all the configurations using the **erase startup-config** command in privilege EXEC mode.

- After erasing the startup-config, reload the device to clear the running-config file from RAM.

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```


126

Save Configurations

Video – Alter the Running Configuration

This video will cover the following:

- Copy the running-config file to the startup-config file
- Show the files in the flash or NVRAM directory
- Use command shortening
- Erase the startup-config file
- Copy the start-config file to the running-config file

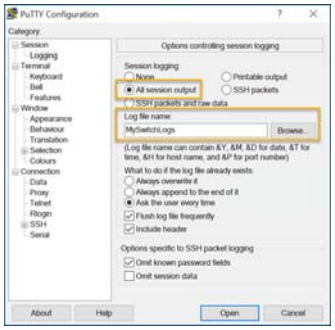
127

Save Configurations

Capture Configuration to a Text File

Configuration files can also be saved and archived to a text document.

- **Step 1.** Open terminal emulation software, such as PuTTY or Tera Term, that is already connected to a switch.
- **Step 2.** Enable logging in to the terminal software and assign a name and file location to save the log file. The figure displays that **All session output** will be captured to the file specified (i.e., MySwitchLogs).



128

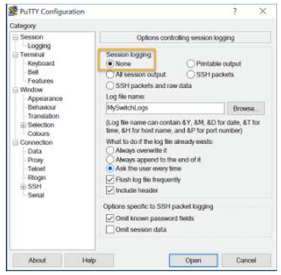
Save Configurations

Capture Configuration to a Text File (Cont.)

- **Step 3.** Execute the **show running-config** or **show startup-config** command at the privileged EXEC prompt. Text displayed in the terminal window will be placed into the chosen file.
- **Step 4.** Disable logging in the terminal software. The figure shows how to disable logging by choosing the **None** session logging option

Note: The text file created can be used as a record of how the device is currently implemented. The file could require editing before being used to restore a saved configuration to a device.

```
Switch# show running-config
Building configuration...
```



129

Save Configurations

Packet Tracer – Configure Initial Switch Settings

In this Packet Tracer, you will do the following:

- Verify the Default Switch Configuration
- Configure a Basic Switch Configuration
- Configure a MOTD Banner
- Save Configuration Files to NVRAM
- Configure a second Switch

130

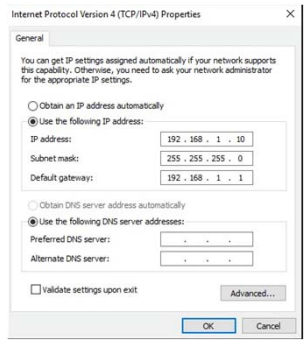
2.6 Ports and Addresses

131

Ports and Addresses

IP Addresses

- The use of IP addresses is the primary means of enabling devices to locate one another and establish end-to-end communication on the internet.
- The structure of an IPv4 address is called dotted decimal notation and is represented by four decimal numbers between 0 and 255.
- An IPv4 subnet mask is a 32-bit value that differentiates the network portion of the address from the host portion. Coupled with the IPv4 address, the subnet mask determines to which subnet the device is a member.
- The default gateway address is the IP address of the router that the host will use to access remote networks, including the internet.



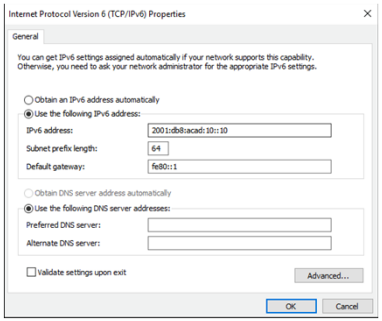
132

Ports and Addresses

IP Addresses (Cont.)

- IPv6 addresses are 128 bits in length and written as a string of hexadecimal values. Every four bits is represented by a single hexadecimal digit; for a total of 32 hexadecimal values. Groups of four hexadecimal digits are separated by a colon ":".
- IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.

Note: IP in this course refers to both the IPv4 and IPv6 protocols. IPv6 is the most recent version of IP and is replacing the more common IPv4.

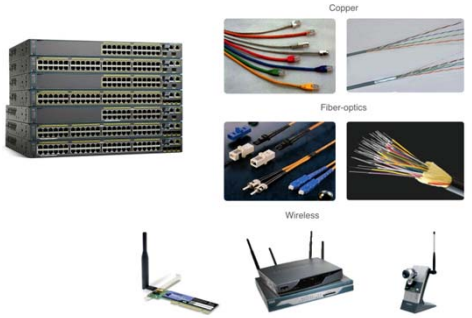


133

Ports and Addresses

Interfaces and Ports

- Network communications depend on end user device interfaces, networking device interfaces, and the cables that connect them.
- Types of network media include twisted-pair copper cables, fiber-optic cables, coaxial cables, or wireless.
- Different types of network media have different features and benefits. Some of the differences between various types of media include:
  - Distance the media can successfully carry a signal
  - Environment in which the media is to be installed
  - Amount of data and the speed at which it must be transmitted
  - Cost of the media and installation



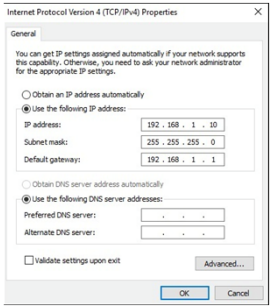
134

2.7 Configure IP Addressing

Configure IP Addressing

Manual IP Address Configuration for End Devices

- End devices on the network need an IP address in order to communicate with other devices on the network.
- IPv4 address information can be entered into end devices manually, or automatically using Dynamic Host Configuration Protocol (DHCP).
  - To manually configure an IPv4 address on a Windows PC, open the **Control Panel > Network Sharing Center > Change adapter settings** and choose the adapter. Next right-click and select **Properties** to display the **Local Area Connection Properties**.
  - Next, click **Properties** to open the **Internet Protocol Version 4 (TCP/IPv4) Properties** window. Then configure the IPv4 address and subnet mask information, and default gateway.

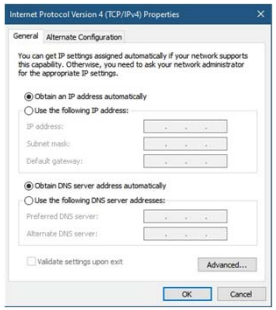


Note: IPv6 addressing and configuration options are similar to IPv4.

Configure IP Addressing

Automatic IP Address Configuration for End Devices

- DHCP enables automatic IPv4 address configuration for every end device that is DHCP-enabled.
- End devices are typically by default using DHCP for automatic IPv4 address configuration.
  - To configure DHCP on a Windows PC, open the **Control Panel > Network Sharing Center > Change adapter settings** and choose the adapter. Next right-click and select **Properties** to display the **Local Area Connection Properties**.
  - Next, click **Properties** to open the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, then select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



Note: IPv6 uses DHCPv6 and SLAAC (Stateless Address Autoconfiguration) for dynamic address allocation.

Configure IP Addressing

Switch Virtual Interface Configuration

To access the switch remotely, an IP address and a subnet mask must be configured on the SVI.

To configure an SVI on a switch:

- Enter the **interface vlan 1** command in global configuration mode.
- Next assign an IPv4 address using the **ip address** *ip-address subnet-mask command.*
- Finally, enable the virtual interface using the **no shutdown** command.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.20 255.255.255.0
Switch(config-if)# no shutdown
```

Configure IP Addressing

Packet Tracer – Implement Basic Connectivity

In this Packet Tracer, you will do the following:

- Perform a Basic Configuration on two switches
- Configure the PCs
- Configure the Switch Management Interface

139

2.8 Verify Connectivity

140

Verify Connectivity

Video – Test the Interface Assignment

This video will cover the following:

- Connect a console cable from the PC to the switch
- Use the terminal emulation program and accept the defaults to bring you to the command line
- Use enable to enter privileged EXEC mode
- Use the global configuration mode and the interface configuration mode to enter the no shutdown command

141

Verify Connectivity

Video – Test End-to-End Connectivity

This video will cover the use of the ping command to test connectivity on both switches and both PCs.

142

2.9 Module Practice and Quiz

143

Module Practice and Quiz

Packet Tracer – Basic Switch and End Device Configuration

In this Packet Tracer, you will do the following:

- Configure hostnames and IP addresses on two switches
- Use Cisco IOS commands to specify or limit access to the device configurations
- Use IOS commands to save the running configuration
- Configure two host devices with IP addresses
- Verify connectivity between the two PC end devices

144

Module Practice and Quiz

Packet Tracer - Basic Switch and End Device Configuration – Physical Mode
Lab – Basic Switch and End Device Configuration

In both the Packet Tracer Physical Mode activity and in the Lab, you will complete the following objectives:

- Set Up the Network Topology
- Configure PC Hosts
- Configure and Verify Basic Switch Settings

145

Module Practice and Quiz

What did I learn in this module?

- All end devices and network devices require an operating system (OS).
- Cisco IOS software separates management access into the following two command modes: User EXEC Mode and Privileged EXEC Mode.
- Global configuration mode is accessed before other specific configuration modes. From global config mode, the user can enter different subconfiguration modes.
- Each IOS command has a specific format or syntax and can only be executed in the appropriate mode.
- Basic device configurations- hostname, password, encrypt passwords and banner.
- There are two system files that store the device configuration: startup-config and running-config.
- IP addresses enable devices to locate one another and establish end-to-end communication on the internet. Each end device on a network must be configured with an IP address.

146

Module 2 : Basic Switch and End Device Configuration

New Terms and Commands

• operating system (OS)	• line configuration mode	• **console**
• CLI	• interface configuration mode	• **enable secret**
• GUI	• Enable	• **VTY line**
• shell	• **configure terminal**	• **show running-config**
• kernel	• **exit**	• **banner motd**
• hardware	• **end**	• **startup-config**
• console	• argument	• **running-config**
• Secure Shell (SSH)	• keyword	• **reload**
• Telnet	• command syntax	• **erase startup-config**
• terminal emulation programs	• **ping**	• DHCP
• user EXEC mode	• **traceroute**	• switch virtual interface (SVI)
• privileged EXEC mode	• help command "?"	• **ipconfig**
	• hot keys	• **show ip int brief**
	• **hostname**	

147

Module 3: Protocols and Models

Instructor Materials

Introduction to Networks v7.0
(ITN)

148

Module 3: Protocols and Models

Introduction to Networks 7.0
(ITN)

159

Module Objectives

Module Title: Protocols and Models

Module Objective: Explain how network protocols enable devices to access local and remote network resources.

Topic Title	Topic Objective
The Rules	Describe the types of rules that are necessary to successfully communicate.
Protocols	Explain why protocols are necessary in network communication.
Protocol Suites	Explain the purpose of adhering to a protocol suite.
Standards Organizations	Explain the role of standards organizations in establishing protocols for network interoperability.
Reference Models	Explain how the TCP/IP model and the OSI model are used to facilitate standardization in the communication process.
Data Encapsulation	Explain how data encapsulation allows data to be transported across the network.
Data Access	Explain how local hosts access local resources on a network.

160

Class Activity – Design a Communications System

Design a Communications System

Objectives:

- Explain the role of protocols and standards organizations in facilitating interoperability in network communications.

3.1 The Rules

The Rules
Video – Devices in a Bubble

This video will explain the protocols that devices use to see their place in the network and communicate with other devices.

The Rules
Communications Fundamentals

Networks can vary in size and complexity. It is not enough to have a connection, devices must agree on “how” to communicate.

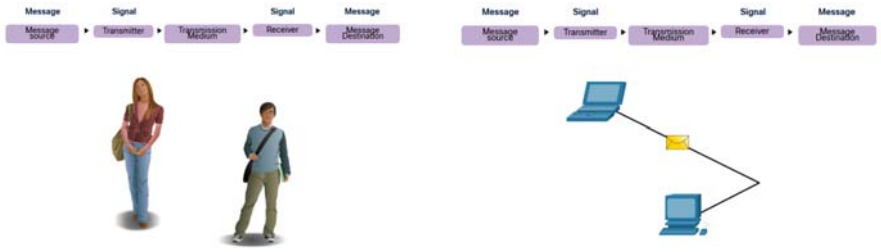
There are three elements to any communication:

- There will be a source (sender).
- There will be a destination (receiver).
- There will be a channel (media) that provides for the path of communications to occur.

The Rules

Communications Protocols

- All communications are governed by protocols.
- Protocols are the rules that communications will follow.
- These rules will vary depending on the protocol.



The Rules

Rule Establishment

- Individuals must use established rules or agreements to govern the conversation.
- The first message is difficult to read because it is not formatted properly. The second shows the message properly formatted

humans communication between govern rules. It is verydifficult tounderstand messages that are not correctly formatted and donot follow the established rules and protocols. A estrutura da gramatica, da lingua, da pontuacao e do sentence faz a configuracao humana compreensivel por muitos individuos diferentes.

Rules govern communication between humans. It is very difficult to understand messages that are not correctly formatted and do not follow the established rules and protocols. The structure of the grammar, the language, the punctuation and the sentence make the configuration humanly understandable for many different individuals.

The Rules

Rule Establishment (Cont.)

Protocols must account for the following requirements:

- An identified sender and receiver
- Common language and grammar
- Speed and timing of delivery
- Confirmation or acknowledgment requirements

The Rules

Network Protocol Requirements

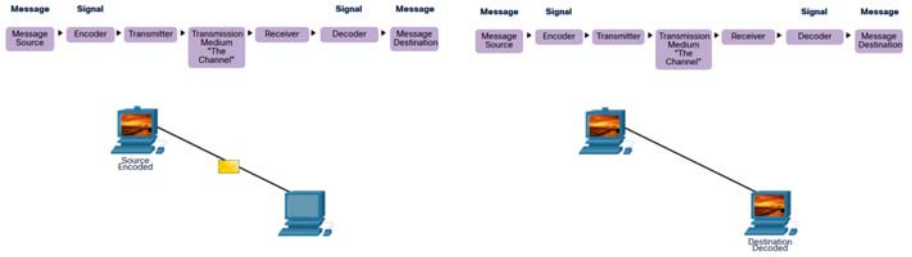
Common computer protocols must be in agreement and include the following requirements:

- Message encoding
- Message formatting and encapsulation
- Message size
- Message timing
- Message delivery options

The Rules

Message Encoding

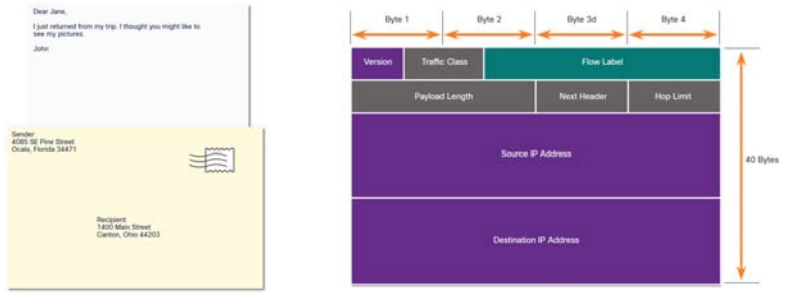
- Encoding is the process of converting information into another acceptable form for transmission.
- Decoding reverses this process to interpret the information.



The Rules

Message Formatting and Encapsulation

- When a message is sent, it must use a specific format or structure.
- Message formats depend on the type of message and the channel that is used to deliver the message.



The Rules

Message Size

Encoding between hosts must be in an appropriate format for the medium.

- Messages sent across the network are converted to bits
- The bits are encoded into a pattern of light, sound, or electrical impulses.
- The destination host must decode the signals to interpret the message.

The Rules

Message Timing

Message timing includes the following:

Flow Control – Manages the rate of data transmission and defines how much information can be sent and the speed at which it can be delivered.

Response Timeout – Manages how long a device waits when it does not hear a reply from the destination.

Access method - Determines when someone can send a message.

- There may be various rules governing issues like “collisions”. This is when more than one device sends traffic at the same time and the messages become corrupt.
- Some protocols are proactive and attempt to prevent collisions; other protocols are reactive and establish a recovery method after the collision occurs.

The Rules

Message Delivery Options

Message delivery may one of the following methods:

- **Unicast –** one to one communication
- **Multicast –** one to many, typically not all
- **Broadcast** – one to all

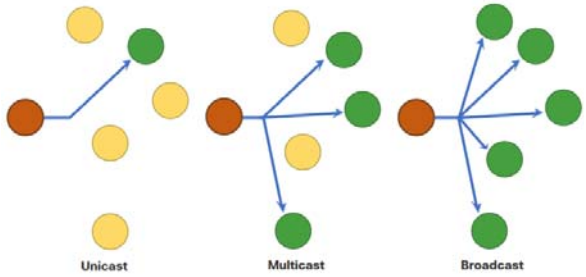
Note: Broadcasts are used in IPv4 networks, but are not an option for IPv6. Later we will also see "Anycast" as an additional delivery option for IPv6.

173

The Rules

A Note About the Node Icon

- Documents may use the node icon , typically a circle, to represent all devices.
- The figure illustrates the use of the node icon for delivery options.



174

3.2 Protocols

175

Protocols

Network Protocol Overview

Network protocols define a common set of rules.

- Can be implemented on devices in:
  - Software
  - Hardware
  - Both
- Protocols have their own:
  - Function
  - Format
  - Rules

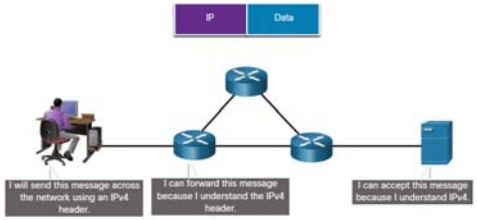
Protocol Type	Description
Network Communications	enable two or more devices to communicate over one or more networks
Network Security	secure data to provide authentication, data integrity, and data encryption
Routing	enable routers to exchange route information, compare path information, and select best path
Service Discovery	used for the automatic detection of devices or services

176

Protocols

Network Protocol Functions

- Devices use agreed-upon protocols to communicate .
- Protocols may have may have one or functions.



Function	Description
Addressing	Identifies sender and receiver
Reliability	Provides guaranteed delivery
Flow Control	Ensures data flows at an efficient rate
Sequencing	Uniquely labels each transmitted segment of data
Error Detection	Determines if data became corrupted during transmission
Application Interface	Process-to-process communications between network applications

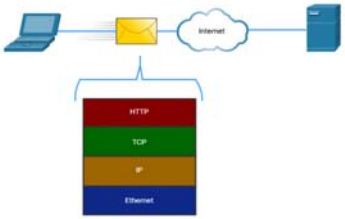
 177

177

Protocols

Protocol Interaction

- Networks require the use of several protocols.
- Each protocol has its own function and format.



Protocol	Function
Hypertext Transfer Protocol (HTTP)	▪ Governs the way a web server and a web client interact ▪ Defines content and format
Transmission Control Protocol (TCP)	▪ Manages the individual conversations ▪ Provides guaranteed delivery ▪ Manages flow control
Internet Protocol (IP)	Delivers messages globally from the sender to the receiver
Ethernet	Delivers messages from one NIC to another NIC on the same Ethernet Local Area Network (LAN)

 178

178

3.3 Protocol Suites

 179

179

Protocol Suites

Network Protocol Suites

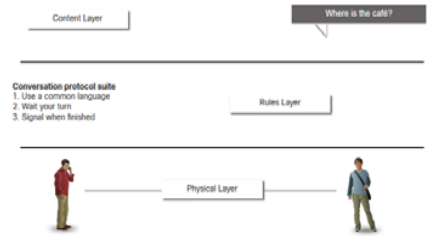
Protocols must be able to work with other protocols.

Protocol suite:

- A group of inter-related protocols necessary to perform a communication function
- Sets of rules that work together to help solve a problem

The protocols are viewed in terms of layers:

- Higher Layers
- Lower Layers- concerned with moving data and provide services to upper layers



Protocol suites are sets of rules that work together to help solve a problem.

 180

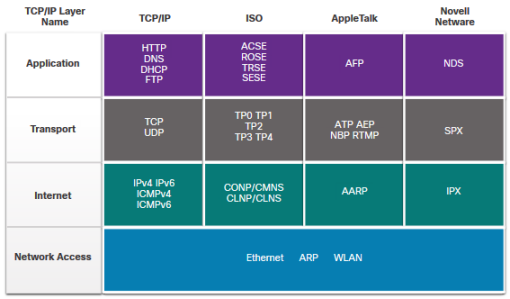
180

Protocol Suites

Evolution of Protocol Suites

There are several protocol suites.

- **Internet Protocol Suite or TCP/IP-** The most common protocol suite and maintained by the Internet Engineering Task Force (IETF)
- **Open Systems Interconnection (OSI) protocols-** Developed by the International Organization for Standardization (ISO) and the International Telecommunications Union (ITU)
- **AppleTalk-** Proprietary suite release by Apple Inc.
- **Novell NetWare-** Proprietary suite developed by Novell Inc.

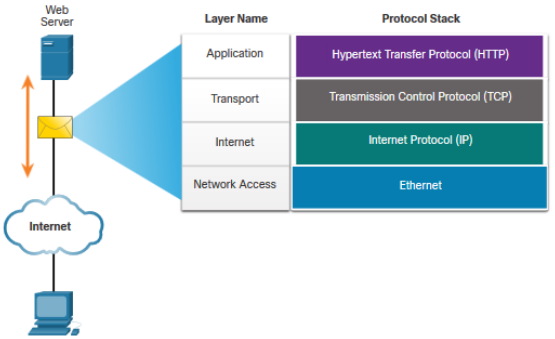


181

Protocol Suites

TCP/IP Protocol Example

- TCP/IP protocols operate at the application, transport, and internet layers.
- The most common network access layer LAN protocols are Ethernet and WLAN (wireless LAN).

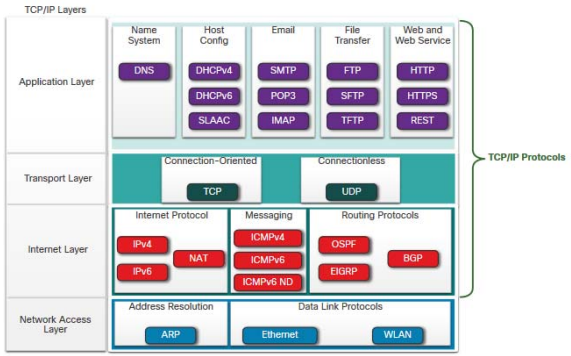


182

Protocol Suites

TCP/IP Protocol Suite

- TCP/IP is the protocol suite used by the internet and includes many protocols.
- TCP/IP is:
  - An open standard protocol suite that is freely available to the public and can be used by any vendor
  - A standards-based protocol suite that is endorsed by the networking industry and approved by a standards organization to ensure interoperability

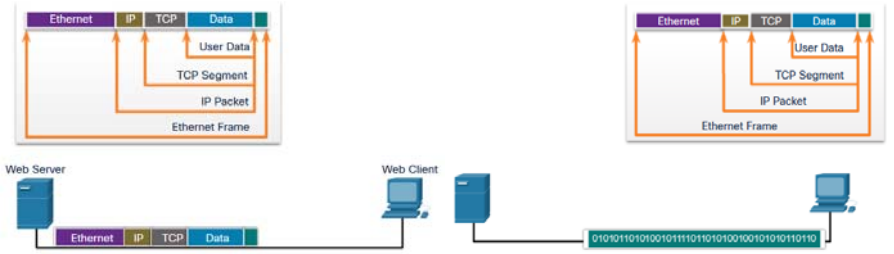


183

Protocol Suites

TCP/IP Communication Process

- A web server encapsulating and sending a web page to a client.
- A client de-encapsulating the web page for the web browser



184

3.4 Standards Organizations

185

Standards Organizations
Open Standards

Open standards encourage:

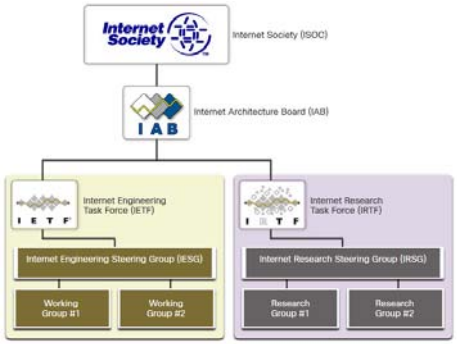
- interoperability
- competition
- innovation

Standards organizations are:

- vendor-neutral
- non-profit organizations
- established to develop and promote the concept of open standards.

186

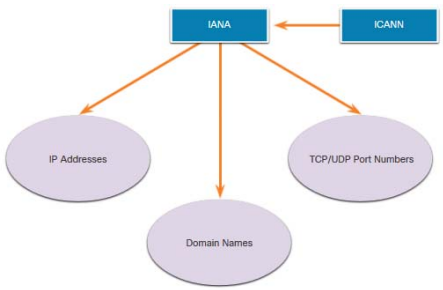
Standards Organizations
Internet Standards



- **Internet Society (ISOC)** - Promotes the open development and evolution of internet
- **Internet Architecture Board (IAB)** - Responsible for management and development of internet standards
- **Internet Engineering Task Force (IETF)** - Develops, updates, and maintains internet and TCP/IP technologies
- **Internet Research Task Force (IRTF)** - Focused on long-term research related to internet and TCP/IP protocols

187

Standards Organizations
Internet Standards (Cont.)



Standards organizations involved with the development and support of TCP/IP

- **Internet Corporation for Assigned Names and Numbers (ICANN)** - Coordinates IP address allocation, the management of domain names, and assignment of other information
- **Internet Assigned Numbers Authority (IANA)** - Oversees and manages IP address allocation, domain name management, and protocol identifiers for ICANN

188

Standards Organizations

Electronic and Communications Standards

- **Institute of Electrical and Electronics Engineers** (**IEEE**, pronounced “I-triple-E”) - dedicated to creating standards in power and energy, healthcare, telecommunications, and networking
- **Electronic Industries Alliance (EIA)** - develops standards relating to electrical wiring, connectors, and the 19-inch racks used to mount networking equipment
- **Telecommunications Industry Association (TIA)** - develops communication standards in radio equipment, cellular towers, Voice over IP (VoIP) devices, satellite communications, and more
- **International Telecommunications Union-Telecommunication Standardization Sector (ITU-T**) - defines standards for video compression, Internet Protocol Television (IPTV), and broadband communications, such as a digital subscriber line (DSL)

 189

189

Standards Organizations

Lab – Researching Networking Standards

In this lab, you will do the following:

- Part 1: Research Networking Standards Organizations
- Part 2: Reflect on Internet and Computer Networking Experience

 190

190

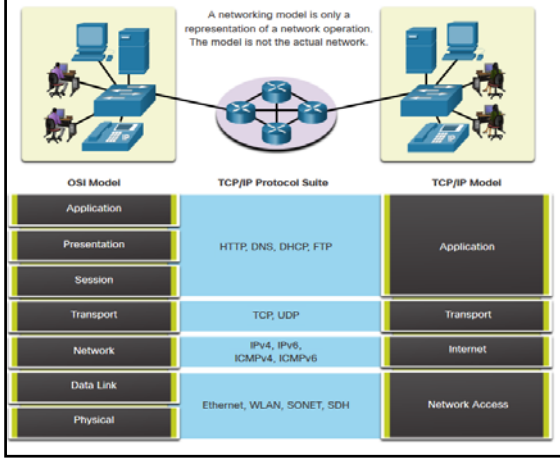
3.5 Reference Models

 191

191

Reference Models

The Benefits of Using a Layered Model



Complex concepts such as how a network operates can be difficult to explain and understand. For this reason, a layered model is used.

Two layered models describe network operations:

- Open System Interconnection (OSI) Reference Model
- TCP/IP Reference Model

 192

192

Reference Models

The Benefits of Using a Layered Model (Cont.)

These are the benefits of using a layered model:

- Assist in protocol design because protocols that operate at a specific layer have defined information that they act upon and a defined interface to the layers above and below
- Foster competition because products from different vendors can work together
- Prevent technology or capability changes in one layer from affecting other layers above and below
- Provide a common language to describe networking functions and capabilities

193

Reference Models

The OSI Reference Model

OSI Model Layer	Description
7 - Application	Contains protocols used for process-to-process communications.
6 - Presentation	Provides for common representation of the data transferred between application layer services.
5 - Session	Provides services to the presentation layer and to manage data exchange.
4 - Transport	Defines services to segment, transfer, and reassemble the data for individual communications.
3 - Network	Provides services to exchange the individual pieces of data over the network.
2 - Data Link	Describes methods for exchanging data frames over a common media.
1 - Physical	Describes the means to activate, maintain, and de-activate physical connections.

194

Reference Models

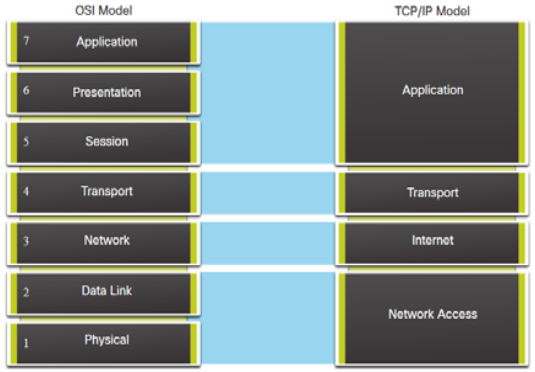
The TCP/IP Reference Model

TCP/IP Model Layer	Description
Application	Represents data to the user, plus encoding and dialog control.
Transport	Supports communication between various devices across diverse networks.
Internet	Determines the best path through the network.
Network Access	Controls the hardware devices and media that make up the network.

195

Reference Models

OSI and TCP/IP Model Comparison



- The OSI model divides the network access layer and the application layer of the TCP/IP model into multiple layers.
- The TCP/IP protocol suite does not specify which protocols to use when transmitting over a physical medium.
- OSI Layers 1 and 2 discuss the necessary procedures to access the media and the physical means to send data over a network.

196

Reference Models

Packet Tracer – Investigate the TCP/IP and OSI Models in Action

This simulation activity is intended to provide a foundation for understanding the TCP/IP protocol suite and the relationship to the OSI model. Simulation mode allows you to view the data contents being sent across the network at each layer.

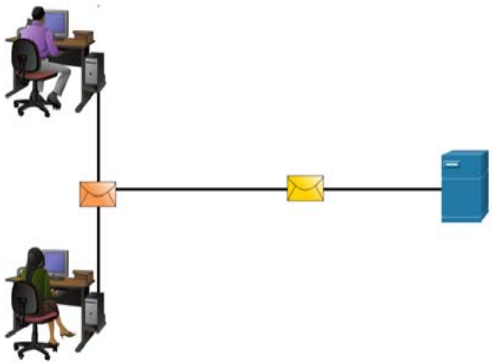
In this Packet Tracer, you will:

- Part 1: Examine HTTP Web Traffic
- Part 2: Display Elements of the TCP/IP Protocol Suite

3.6 Data Encapsulation

Data Encapsulation

Segmenting Messages



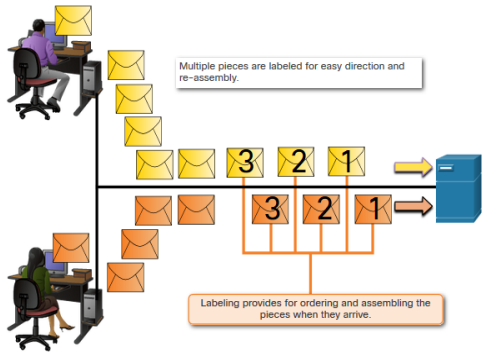
Segmenting is the process of breaking up messages into smaller units. Multiplexing is the processes of taking multiple streams of segmented data and interleaving them together.

Segmenting messages has two primary benefits:

- **Increases speed** - Large amounts of data can be sent over the network without tying up a communications link.
- **Increases efficiency** - Only segments which fail to reach the destination need to be retransmitted, not the entire data stream.

Data Encapsulation

Sequencing

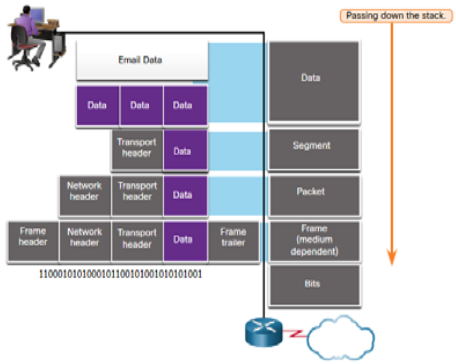


Sequencing messages is the process of numbering the segments so that the message may be reassembled at the destination.

TCP is responsible for sequencing the individual segments.

Data Encapsulation

Protocol Data Units



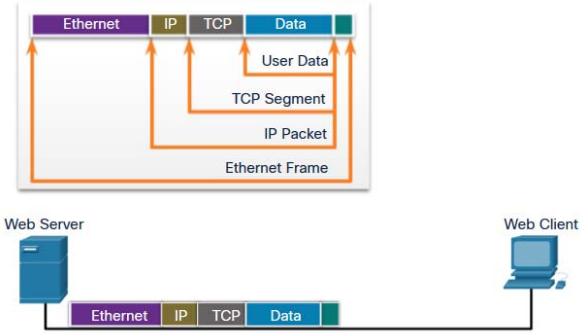
Encapsulation is the process where protocols add their information to the data.

- At each stage of the process, a PDU has a different name to reflect its new functions.
- There is no universal naming convention for PDUs, in this course, the PDUs are named according to the protocols of the TCP/IP suite.
- PDUs passing down the stack are as follows:
  1. Data (Data Stream)
  2. Segment
  3. Packet
  4. Frame
  5. Bits (Bit Stream)

Data Encapsulation

Encapsulation Example

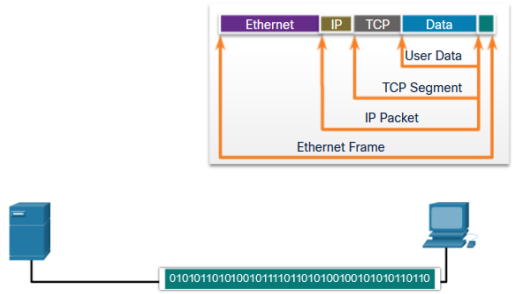
- Encapsulation is a top down process.
- The level above does its process and then passes it down to the next level of the model. This process is repeated by each layer until it is sent out as a bit stream.



Data Encapsulation

De-encapsulation Example

- Data is de-encapsulated as it moves up the stack.
- When a layer completes its process, that layer strips off its header and passes it up to the next level to be processed. This is repeated at each layer until it is a data stream that the application can process.
  1. Received as Bits (Bit Stream)
  2. Frame
  3. Packet
  4. Segment
  5. Data (Data Stream)



3.7 Data Access

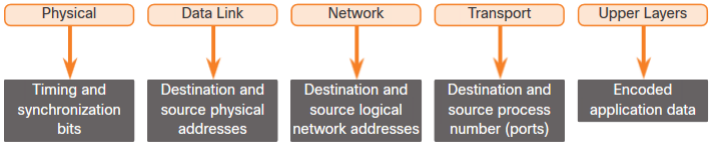
Data Access

Addresses

Both the data link and network layers use addressing to deliver data from source to destination.

Network layer source and destination addresses - Responsible for delivering the IP packet from original source to the final destination.

Data link layer source and destination addresses – Responsible for delivering the data link frame from one network interface card (NIC) to another NIC on the same network.



205

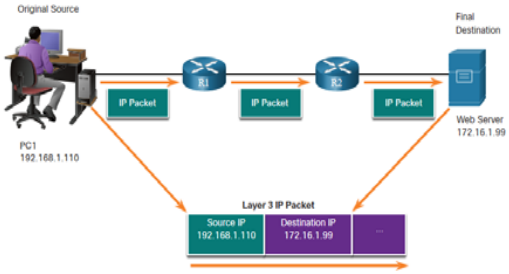
Data Access

Layer 3 Logical Address

The IP packet contains two IP addresses:

- **Source IP address** - The IP address of the sending device, original source of the packet.
- **Destination IP address** - The IP address of the receiving device, final destination of the packet.

These addresses may be on the same link or remote.



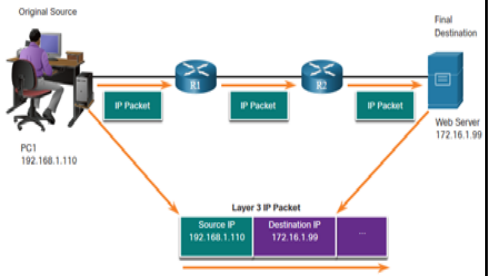
206

Data Access

Layer 3 Logical Address (Cont.)

An IP address contains two parts:

- **Network portion (IPv4) or Prefix (IPv6)**
  - The left-most part of the address indicates the network group which the IP address is a member.
  - Each LAN or WAN will have the same network portion.
- **Host portion (IPv4) or Interface ID (IPv6)**
  - The remaining part of the address identifies a specific device within the group.
  - This portion is unique for each device on the network.



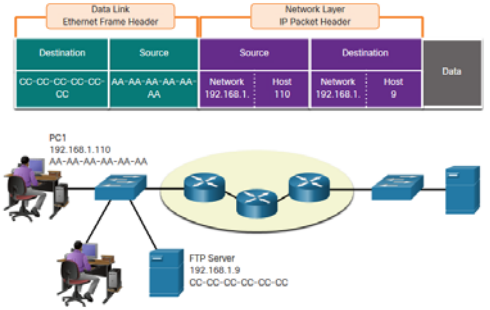
207

Data Access

Devices on the Same Network

When devices are on the same network the source and destination will have the same number in network portion of the address.

- PC1 – 192.168.1.110
- FTP Server – 192.168.1.9



208

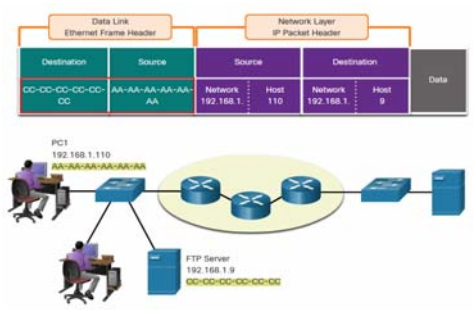
Data Access

Role of the Data Link Layer Addresses: Same IP Network

When devices are on the same Ethernet network the data link frame will use the actual MAC address of the destination NIC.

MAC addresses are physically embedded into the Ethernet NIC and are local addressing.

- The Source MAC address will be that of the originator on the link.
- The Destination MAC address will always be on the same link as the source, even if the ultimate destination is remote.

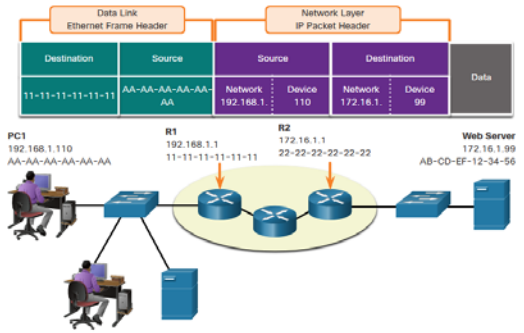


209

Data Access

Devices on a Remote Network

- What happens when the actual (ultimate) destination is not on the same LAN and is remote?
- What happens when PC1 tries to reach the Web Server?
- Does this impact the network and data link layers?



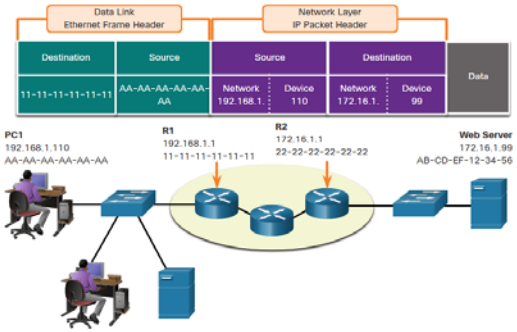
210

Data Access

Role of the Network Layer Addresses

When the source and destination have a different network portion, this means they are on different networks.

- PC1 – 192.168.1
- Web Server – 172.16.1



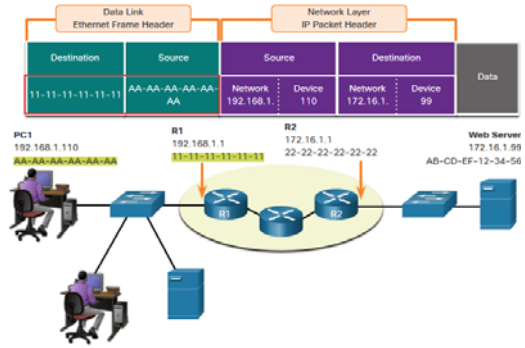
211

Data Access

Role of the Data Link Layer Addresses: Different IP Networks

When the final destination is remote, Layer 3 will provide Layer 2 with the local default gateway IP address, also known as the router address.

- The default gateway (DGW) is the router interface IP address that is part of this LAN and will be the “door” or “gateway” to all other remote locations.
- All devices on the LAN must be told about this address or their traffic will be confined to the LAN only.
- Once Layer 2 on PC1 forwards to the default gateway (Router), the router then can start the routing process of getting the information to actual destination.



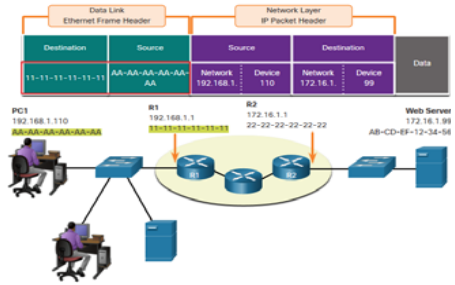
212

Data Access

Role of the Data Link Layer Addresses: Different IP Networks (Cont.)

- The data link addressing is local addressing so it will have a source and destination for each link.
- The MAC addressing for the first segment is :
  - Source – AA-AA-AA-AA-AA-AA (PC1) Sends the frame.
  - Destination – 11-11-11-11-11-11 (R1-Default Gateway MAC) Receives the frame.

Note: While the L2 local addressing will change from link to link or hop to hop, the L3 addressing remains the same.

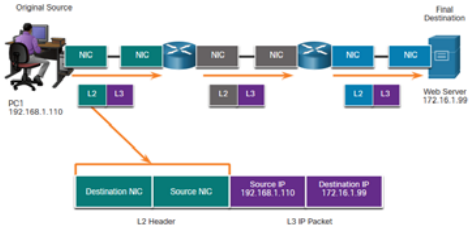


213

Data Access

Data Link Addresses

- Since data link addressing is local addressing, it will have a source and destination for each segment or hop of the journey to the destination.
- The MAC addressing for the first segment is:
  - Source – (PC1 NIC) sends frame
  - Destination – (First Router- DGW interface) receives frame



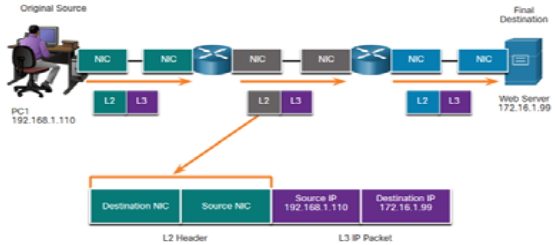
214

Data Access

Data Link Addresses (Cont.)

The MAC addressing for the second hop is:

- Source – (First Router- exit interface) sends frame
- Destination – (Second Router) receives frame



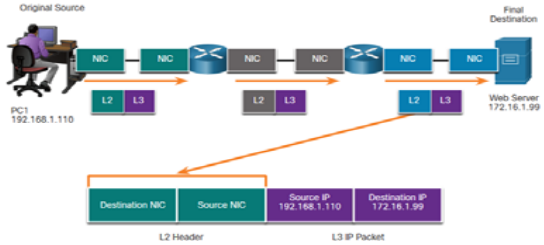
215

Data Access

Data Link Addresses (Cont.)

The MAC addressing for the last segment is:

- Source – (Second Router- exit interface) sends frame
- Destination – (Web Server NIC) receives frame

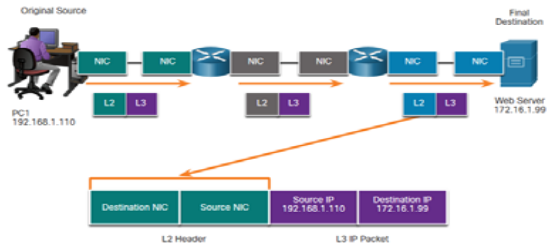


216

Data Access

Data Link Addresses (Cont.)

- Notice that the packet is not modified, but the frame is changed, therefore the L3 IP addressing does not change from segment to segment like the L2 MAC addressing.
- The L3 addressing remains the same since it is global and the ultimate destination is still the Web Server.



217

Data Access

Lab – Install Wireshark

In this lab you will do the following:

- Download and Install Wireshark

218

Data Access

Lab – Use Wireshark to View Network Traffic

In this lab, you will do the following:

- Part 1: Capture and Analyze Local ICMP Data in Wireshark
- Part 2: Capture and Analyze Remote ICMP Data in Wireshark

219

3.8 Module Practice and Quiz

220

Module Practice and Quiz

What did I learn in this module?

The Rules

- Protocols must have a sender and a receiver.
- Common computer protocols include these requirements: message encoding, formatting and encapsulation, size, timing, and delivery options.

Protocols

- To send a message across the network requires the use of several protocols.
- Each network protocol has its own function, format, and rules for communications.

Protocol Suites

- A protocol suite is a group of inter-related protocols.
- TCP/IP protocol suite are the protocols used today.

Standards Organizations

- Open standards encourage interoperability, competition, and innovation.

 221

221

Module Practice and Quiz

What did I learn in this module? (Cont.)

Reference Models

- The two models used in networking are the TCP/IP and the OSI model.
- The TCP/IP model has 4 layers and the OSI model has 7 layers.

Data Encapsulation

- The form that a piece of data takes at any layer is called a *protocol data unit (PDU)*.
- There are five different PDUs used in the data encapsulation process: data, segment, packet, frame, and bits

Data Access

- The Network and Data Link layers are going to provide addressing to move data through the network.
- Layer 3 will provide IP addressing and layer 2 will provide MAC addressing.
- The way these layers handle addressing will depend on whether the source and the destination are on the same network or if the destination is on a different network from the source.

 222

222

New Terms and Commands

- encoding
- protocol
- channel
- flow control
- response timeout
- acknowledgement
- unicast
- multicast
- broadcast
- protocol suite
- Ethernet
- standard
- proprietary protocol
- 802.3 (Ethernet)
- 802.11 (wireless Ethernet)
- segmentation
- default gateway
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol (POP)
- Transmission Control Protocol (TCP)
- transport
- data link
- network access
- Advanced Research Projects Agency Network (ARPANET)

223

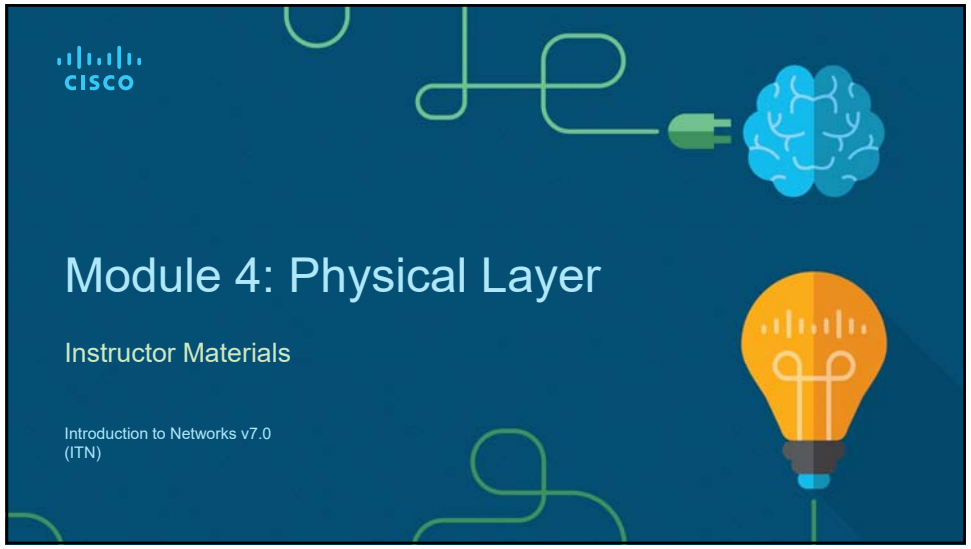
223

New Terms and Commands (Cont.)

- Internet Message Access Protocol (IMAP)
- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- User Datagram Protocol (UDP)
- Network Address Translation (NAT)
- Internet Control Messaging Protocol (ICMP)
- Open Shortest Path First (OSPF)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Address Resolution Protocol (ARP)
- Dynamic Host Configuration (DHCP)
- encapsulation
- de-encapsulation
- protocol data unit (PDU)
- segment
- packet
- frame

 224

224



225

What to Expect in this Module

To facilitate learning, the following features within the GUI may be included in this module:

Feature	Description
Animations	Expose learners to new skills and concepts.
Videos	Expose learners to new skills and concepts.
Check Your Understanding(CYU)	Per topic online quiz to help learners gauge content understanding.
Interactive Activities	A variety of formats to help learners gauge content understanding.
Syntax Checker	Small simulations that expose learners to Cisco command line to practice configuration skills.
PT Activity	Simulation and modeling activities designed to explore, acquire, reinforce, and expand skills.

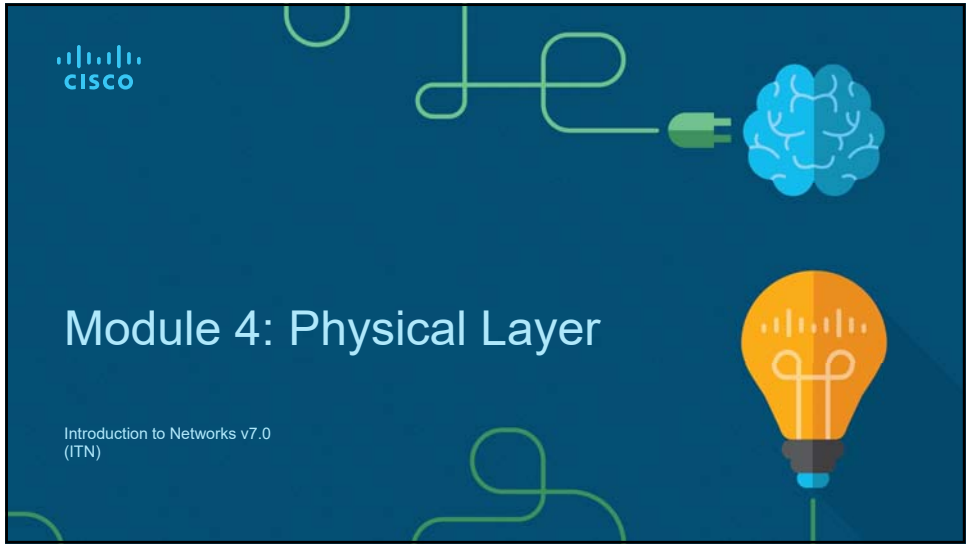
227

What to Expect in this Module (Cont.)

- To facilitate learning, the following features may be included in this module:

Feature	Description
Packet Tracer Physical Mode Activity	These activities are completed using Packet Tracer in Physical Mode.
Hands-On Labs	Labs designed for working with physical equipment.
Class Activities	These are found on the Instructor Resources page. Class Activities are designed to facilitate learning, class discussion, and collaboration.
Module Quizzes	Self-assessments that integrate concepts and skills learned throughout the series of topics presented in the module.
Module Summary	Briefly recaps module content.

228



235

Module Objectives

Module Title: Physical Layer

Module Objective: Explain how physical layer protocols, services, and network media support communications across data networks.

Topic Title	Topic Objective
Purpose of the Physical Layer	Describe the purpose and functions of the physical layer in the network.
Physical Layer Characteristics	Describe characteristics of the physical layer.
Copper Cabling	Identify the basic characteristics of copper cabling.
UTP Cabling	Explain how UTP cable is used in Ethernet networks.
Fiber-Optic Cabling	Describe fiber optic cabling and its main advantages over other media.
Wireless Media	Connect devices using wired and wireless media.

4.1 Purpose of the Physical Layer

Purpose of the Physical Layer

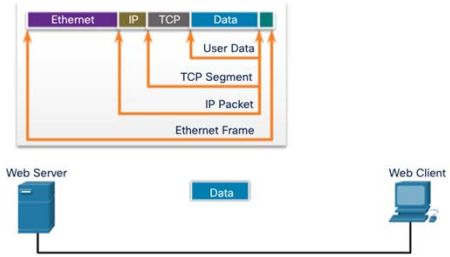
The Physical Connection

- Before any network communications can occur, a physical connection to a local network must be established.
- This connection could be wired or wireless, depending on the setup of the network.
- This generally applies whether you are considering a corporate office or a home.
- A Network Interface Card (NIC) connects a device to the network.
- Some devices may have just one NIC, while others may have multiple NICs (Wired and/or Wireless, for example).
- Not all physical connections offer the same level of performance.

Purpose of the Physical Layer

The Physical Layer

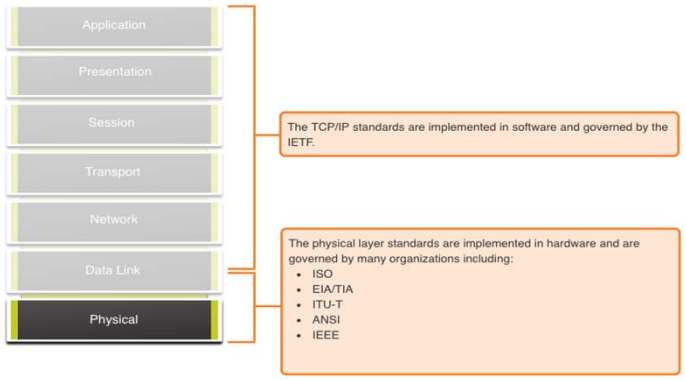
- Transports bits across the network media
- Accepts a complete frame from the Data Link Layer and encodes it as a series of signals that are transmitted to the local media
- This is the last step in the encapsulation process.
- The next device in the path to the destination receives the bits and re-encapsulates the frame, then decides what to do with it.



4.2 Physical Layer Characteristics

240

Physical Layer Characteristics
Physical Layer Standards



241

Physical Layer Characteristics
Physical Components

Physical Layer Standards address three functional areas:

- Physical Components
- Encoding
- Signaling

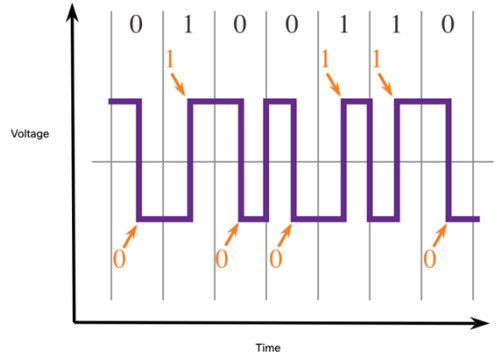
The Physical Components are the hardware devices, media, and other connectors that transmit the signals that represent the bits.

- Hardware components like NICs, interfaces and connectors, cable materials, and cable designs are all specified in standards associated with the physical layer.

242

Physical Layer Characteristics
Encoding

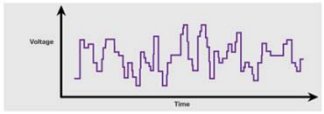
- Encoding converts the stream of bits into a format recognizable by the next device in the network path.
- This 'coding' provides predictable patterns that can be recognized by the next device.
- Examples of encoding methods include Manchester (shown in the figure), 4B/5B, and 8B/10B.



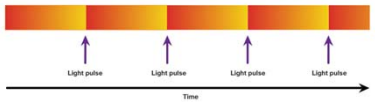
243

Physical Layer Characteristics
Signaling

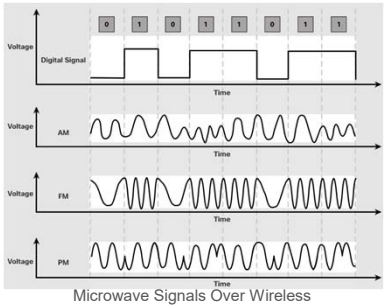
- The signaling method is how the bit values, “1” and “0” are represented on the physical medium.
- The method of signaling will vary based on the type of medium being used.



Electrical Signals Over Copper Cable



Light Pulses Over Fiber-Optic Cable



Microwave Signals Over Wireless

244

Physical Layer Characteristics
Bandwidth

- Bandwidth is the capacity at which a medium can carry data.
- Digital bandwidth measures the amount of data that can flow from one place to another in a given amount of time; how many bits can be transmitted in a second.
- Physical media properties, current technologies, and the laws of physics play a role in determining available bandwidth.

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	Kbps	1 Kbps = 1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps – 1,000,000,000 bps = 10^9 bps
Terabits per second	Tbps	1 Tbps = 1,000,000,000,000 bps = 10^{12} bps

245

Physical Layer Characteristics
Bandwidth Terminology

Latency
- Amount of time, including delays, for data to travel from one given point to another

Throughput
- The measure of the transfer of bits across the media over a given period of time

Goodput
- The measure of usable data transferred over a given period of time
- Goodput = Throughput - traffic overhead

246

4.3 Copper Cabling

247

Copper Cabling
Characteristics of Copper Cabling

Copper cabling is the most common type of cabling used in networks today. It is inexpensive, easy to install, and has low resistance to electrical current flow.

Limitations:

- Attenuation – the longer the electrical signals have to travel, the weaker they get.
- The electrical signal is susceptible to interference from two sources, which can distort and corrupt the data signals (Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI) and Crosstalk).

Mitigation:

- Strict adherence to cable length limits will mitigate attenuation.
- Some kinds of copper cable mitigate EMI and RFI by using metallic shielding and grounding.
- Some kinds of copper cable mitigate crosstalk by twisting opposing circuit pair wires together.

248

Copper Cabling
Types of Copper Cabling

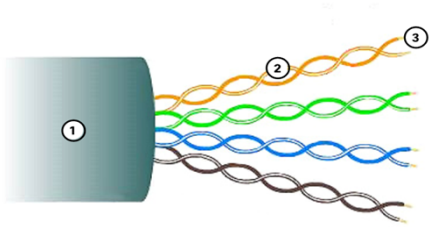
Unshielded Twisted-Pair (UTP) Cable

Shielded Twisted-Pair (STP) Cable

Coaxial Cable

249

Copper Cabling
Unshielded Twisted Pair (UTP)



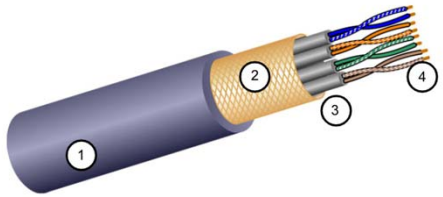
- UTP is the most common networking media.
- Terminated with RJ-45 connectors
- Interconnects hosts with intermediary network devices.

Key Characteristics of UTP

1. The outer jacket protects the copper wires from physical damage.
2. Twisted pairs protect the signal from interference.
3. Color-coded plastic insulation electrically isolates the wires from each other and identifies each pair.

250

Copper Cabling
Shielded Twisted Pair (STP)



- Better noise protection than UTP
- More expensive than UTP
- Harder to install than UTP
- Terminated with RJ-45 connectors
- Interconnects hosts with intermediary network devices

Key Characteristics of STP

1. The outer jacket protects the copper wires from physical damage
2. Braided or foil shield provides EMI/RFI protection
3. Foil shield for each pair of wires provides EMI/RFI protection
4. Color-coded plastic insulation electrically isolates the wires from each other and identifies each pair

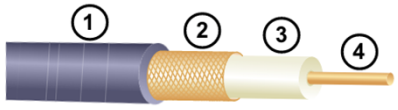
251

Copper Cabling
Coaxial Cable

Consists of the following:
1. Outer cable jacket to prevent minor physical damage
2. A woven copper braid, or metallic foil, acts as the second wire in the circuit and as a shield for the inner conductor.
3. A layer of flexible plastic insulation
4. A copper conductor is used to transmit the electronic signals.

There are different types of connectors used with coax cable.

Commonly used in the following situations:
- Wireless installations - attach antennas to wireless devices
- Cable internet installations - customer premises wiring



252

4.4 UTP Cabling

253

UTP Cabling
Properties of UTP Cabling

UTP has four pairs of color-coded copper wires twisted together and encased in a flexible plastic sheath. No shielding is used. UTP relies on the following properties to limit crosstalk:

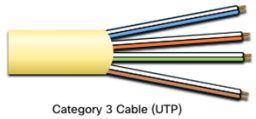
- Cancellation - Each wire in a pair of wires uses opposite polarity. One wire is negative, the other wire is positive. They are twisted together and the magnetic fields effectively cancel each other and outside EMI/RFI.
- Variation in twists per foot in each wire - Each wire is twisted a different amount, which helps prevent crosstalk amongst the wires in the cable.

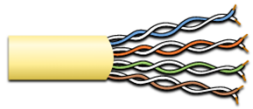
254

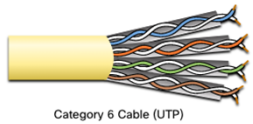
UTP Cabling
UTP Cabling Standards and Connectors

Standards for UTP are established by the TIA/EIA. TIA/EIA-568 standardizes elements like:
- Cable Types
- Cable Lengths
- Connectors
- Cable Termination
- Testing Methods

Electrical standards for copper cabling are established by the IEEE, which rates cable according to its performance. Examples include:
- Category 3
- Category 5 and 5e
- Category 6


Category 3 Cable (UTP)


Category 5 and 5e Cable (UTP)


Category 6 Cable (UTP)

255

UTP Cabling

UTP Cabling Standards and Connectors (Cont.)

RJ-45 Connector

Poorly terminated UTP cable

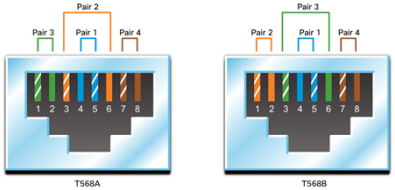
RJ-45 Socket

Properly terminated UTP cable

256

UTP Cabling

Straight-through and Crossover UTP Cables



Cable Type	Standard	Application
Ethernet Straight-through	Both ends T568A or T568B	Host to Network Device
Ethernet Crossover *	One end T568A, other end T568B	Host-to-Host, Switch-to-Switch, Router-to-Router
* Considered Legacy due to most NICs using Auto-MDIX to sense cable type and complete connection		
Rollover	Cisco Proprietary	Host serial port to Router or Switch Console Port, using an adapter

257

4.5 Fiber-Optic Cabling

258

Fiber-Optic Cabling

Properties of Fiber-Optic Cabling

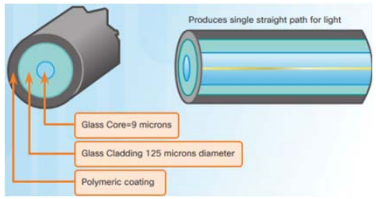
- Not as common as UTP because of the expense involved
- Ideal for some networking scenarios
- Transmits data over longer distances at higher bandwidth than any other networking media
- Less susceptible to attenuation, and completely immune to EMI/RFI
- Made of flexible, extremely thin strands of very pure glass
- Uses a laser or LED to encode bits as pulses of light
- The fiber-optic cable acts as a wave guide to transmit light between the two ends with minimal signal loss

259

Fiber-Optic Cabling

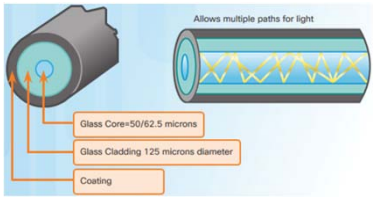
Types of Fiber Media

Single-Mode Fiber



- Very small core
- Uses expensive lasers
- Long-distance applications

Multimode Fiber



- Larger core
- Uses less expensive LEDs
- LEDs transmit at different angles
- Up to 10 Gbps over 550 meters

Dispersion refers to the spreading out of a light pulse over time. Increased dispersion means increased loss of signal strength. MMF has greater dispersion than SMF, with a the maximum cable distance for MMF is 550 meters.

Fiber-Optic Cabling

Fiber-Optic Cabling Usage

Fiber-optic cabling is now being used in four types of industry:

1. **Enterprise Networks -** Used for backbone cabling applications and interconnecting infrastructure devices
2. **Fiber-to-the-Home (FTTH) -** Used to provide always-on broadband services to homes and small businesses
3. **Long-Haul Networks -** Used by service providers to connect countries and cities
4. **Submarine Cable Networks -** Used to provide reliable high-speed, high-capacity solutions capable of surviving in harsh undersea environments at up to transoceanic distances.

Our focus in this course is the use of fiber within the enterprise.

Fiber-Optic Cabling

Fiber-Optic Connectors

Straight-Tip (ST) Connectors

Lucent Connector (LC) Simplex Connectors

Subscriber Connector (SC) Connectors

Duplex Multimode LC Connectors

Fiber-Optic Cabling

Fiber Patch Cords

SC-SC MM Patch Cord

LC-LC SM Patch Cord

ST-LC MM Patch Cord

ST-SC SM Patch Cord

A yellow jacket is for single-mode fiber cables and orange (or aqua) for multimode fiber cables.

Fiber-Optic Cabling

Fiber versus Copper

Optical fiber is primarily used as backbone cabling for high-traffic, point-to-point connections between data distribution facilities and for the interconnection of buildings in multi-building campuses.

Implementation Issues	UTP Cabling	Fiber-Optic Cabling
Bandwidth supported	10 Mb/s - 10 Gb/s	10 Mb/s - 100 Gb/s
Distance	Relatively short (1 - 100 meters)	Relatively long (1 - 100,000 meters)
Immunity to EMI and RFI	Low	High (Completely immune)
Immunity to electrical hazards	Low	High (Completely immune)
Media and connector costs	Lowest	Highest
Installation skills required	Lowest	Highest
Safety precautions	Lowest	Highest

264

4.6 Wireless Media

265

Wireless Media

Properties of Wireless Media

It carries electromagnetic signals representing binary digits using radio or microwave frequencies. This provides the greatest mobility option. Wireless connection numbers continue to increase.

Some of the limitations of wireless:

- **Coverage area** - Effective coverage can be significantly impacted by the physical characteristics of the deployment location.
- **Interference** - Wireless is susceptible to interference and can be disrupted by many common devices.
- **Security** - Wireless communication coverage requires no access to a physical strand of media, so anyone can gain access to the transmission.
- **Shared medium** - WLANs operate in half-duplex, which means only one device can send or receive at a time. Many users accessing the WLAN simultaneously results in reduced bandwidth for each user.

266

Wireless Media

Types of Wireless Media

The IEEE and telecommunications industry standards for wireless data communications cover both the data link and physical layers. In each of these standards, physical layer specifications dictate:

- Data to radio signal encoding methods
- Frequency and power of transmission
- Signal reception and decoding requirements
- Antenna design and construction

Wireless Standards:

- **Wi-Fi (IEEE 802.11)** - Wireless LAN (WLAN) technology
- **Bluetooth (IEEE 802.15)** - Wireless Personal Area network (WPAN) standard
- **WiMAX (IEEE 802.16)** - Uses a point-to-multipoint topology to provide broadband wireless access
- **Zigbee (IEEE 802.15.4)** - Low data-rate, low power-consumption communications, primarily for Internet of Things (IoT) applications

267

Wireless Media
Wireless LAN

In general, a Wireless LAN (WLAN) requires the following devices:

- **Wireless Access Point (AP)** - Concentrate wireless signals from users and connect to the existing copper-based network infrastructure
- **Wireless NIC Adapters** - Provide wireless communications capability to network hosts

There are a number of WLAN standards. When purchasing WLAN equipment, ensure compatibility, and interoperability.

Network Administrators must develop and apply stringent security policies and processes to protect WLANs from unauthorized access and damage.

 268

268

Wireless Media
Packet Tracer – Connect a Wired and Wireless LAN

In this Packet Tracer, you will do the following:

- Connect to the Cloud
- Connect a Router
- Connect Remaining Devices
- Verify Connections
- Examine the Physical Topology

 269

269

Wireless Media
Lab – View Wired and Wireless NIC Information

In this lab, you will complete the following objectives:

- Identify and Work with PC NICs
- Identify and Use the System Tray Network Icons

 270

270

4.7 Module Practice and Quiz

 271

271

Module Practice and Quiz

Packet Tracer – Physical Layer Exploration– Physical Mode

In this Packet Tracer Physical Mode (PTPM) activity, you will complete the following:

- Examine Local IP Addressing Information
- Trace the Path Between Source and Destination

 272

272

Module Practice and Quiz

Packet Tracer – Connect the Physical Layer

In this Packet Tracer, you will do the following:

- Identify Physical Characteristics of Internetworking Devices
- Select Correct Modules for Connectivity
- Connect Devices
- Check Connectivity

 273

273

Module Practice and Quiz

What did I learn in this module?

- Before any network communications can occur, a physical connection to a local network, either wired or wireless, must be established.
- The physical layer consists of electronic circuitry, media, and connectors developed by engineers.
- The physical layer standards address three functional areas: physical components, encoding, and signaling.
- Three types of copper cabling are: UTP, STP, and coaxial cable (coax).
- UTP cabling conforms to the standards established jointly by the TIA/EIA. The electrical characteristics of copper cabling are defined by the Institute of Electrical and Electronics Engineers (IEEE).
- The main cable types that are obtained by using specific wiring conventions are Ethernet Straight-through and Ethernet Crossover.

 274

274

Module Practice and Quiz

What did I learn in this module (Cont.)?

- Optical fiber cable transmits data over longer distances and at higher bandwidths than any other networking media.
- There are four types of fiber-optic connectors: ST, SC, LC, and duplex multimode LC.
- Fiber-optic patch cords include SC-SC multimode, LC-LC single-mode, ST-LC multimode, and SC-ST single-mode.
- Wireless media carry electromagnetic signals that represent the binary digits of data communications using radio or microwave frequencies. Wireless does have some limitations, including coverage area, interference, security, and the problems that occur with any shared medium.
- Wireless standards include the following: Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15), WiMAX (IEEE 802.16), and Zigbee (IEEE 802.15.4).
- Wireless LAN (WLAN) requires a wireless AP and wireless NIC adapters.

 275

275

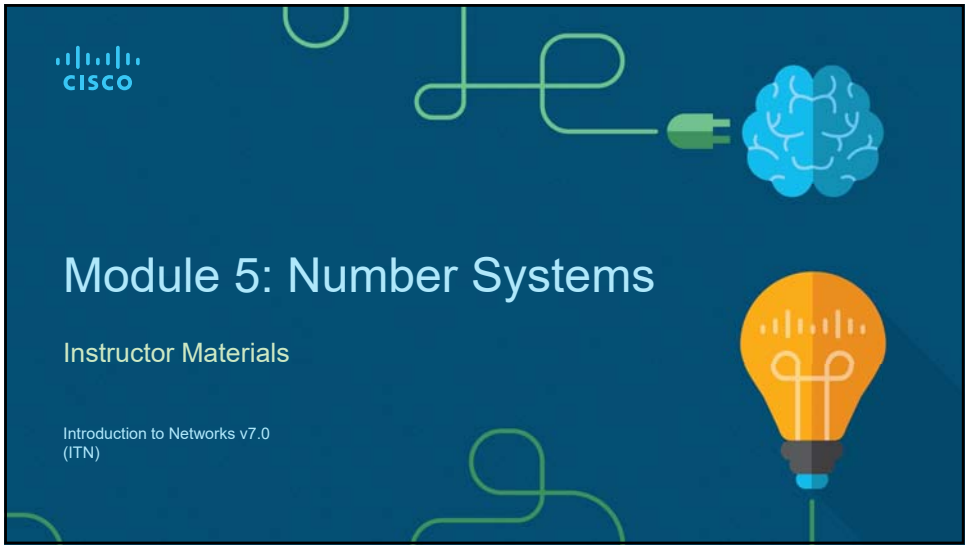
Module 4: Physical Layer

New Terms and Commands

- Telecommunications Industry Association/Electronic Industries Association (TIA/EIA)
- latency
- throughput
- goodput
- Electromagnetic interference (EMI)
- Radio frequency interference (RFI)
- Crosstalk
- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)
- Coaxial cable
- RJ-45
- Cancellation
- TIA/EIA-568
- Ethernet Straight-through
- Ethernet crossover
- Rollover
- Single-Mode Fiber (SMF)
- Multimode (MMF)
- Straight-tip (ST) Connectors
- Subscriber Connector (SC) Connectors
- Lucent Connector (LC) Simplex Connectors
- Duplex Multimode LC Connectors
- Bluetooth (IEEE 802.15)
- WiMAX (IEEE 802.16)
- Zigbee (IEEE 802.15.4)
- Wireless Access Point (AP)

 276

276



277

What to Expect in this Module

- To facilitate learning, the following features within the GUI may be included in this module:

Feature	Description
Animations	Expose learners to new skills and concepts.
Videos	Expose learners to new skills and concepts.
Check Your Understanding(CYU)	Per topic online quiz to help learners gauge content understanding.
Interactive Activities	A variety of formats to help learners gauge content understanding.
Syntax Checker	Small simulations that expose learners to Cisco command line to practice configuration skills.
PT Activity	Simulation and modeling activities designed to explore, acquire, reinforce, and expand skills.

 279

279

What to Expect in this Module (Cont.)

- To facilitate learning, the following features may be included in this module:

Feature	Description
Hands-On Labs	Labs designed for working with physical equipment.
Class Activities	These are found on the Instructor Resources page. Class Activities are designed to facilitate learning, class discussion, and collaboration.
Module Quizzes	Self-assessments that integrate concepts and skills learned throughout the series of topics presented in the module.
Module Summary	Briefly recaps module content.

 280

280

Module 5: Number Systems

Introduction to Networks v7.0
(ITN)

284

Module Objectives

Module Title: Number Systems

Module Objective: Calculate numbers between decimal, binary, and hexadecimal systems.

Topic Title	Topic Objective
Binary Number System	Calculate numbers between decimal and binary systems.
Hexadecimal Number System	Calculate numbers between decimal and hexadecimal systems.

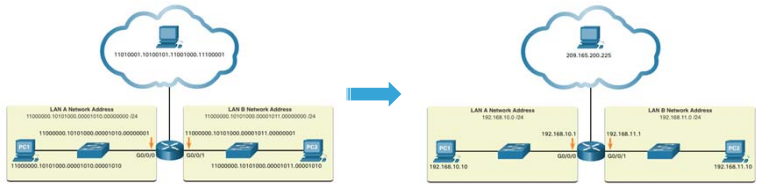
285

5.1 Binary Number System

286

Binary Number System
Binary and IPv4 Addresses

- Binary numbering system consists of 1s and 0s, called bits
- Decimal numbering system consists of digits 0 through 9
- Hosts, servers, and network equipment using binary addressing to identify each other.
- Each address is made up of a string of 32 bits, divided into four sections called octets.
- Each octet contains 8 bits (or 1 byte) separated by a dot.
- For ease of use by people, this dotted notation is converted to dotted decimal.



287

Binary Number System

Video – Convert Between Binary and Decimal Numbering Systems

This video will cover the following:

- Positional notation review
- Powers of 10 review
- Decimal – base 10 numbering review
- Binary – base 2 numbering review
- Convert an P address in binary to decimal numbering

288

Binary Number System

Binary Positional Notation

- Positional notation means that a digit represents different values depending on the "position" the digit occupies in the sequence of numbers.
- The decimal positional notation system operates as shown in the tables below.

Radix	10	10	10	10
Position in Number	3	2	1	0
Calculate	(10^3)	(10^2)	(10^1)	(10^0)
Position Value	1000	100	10	1

	Thousands	Hundreds	Tens	Ones
Positional Value	1000	100	10	1
Decimal Number (1234)	1	2	3	4
Calculate	1 x 1000	2 x 100	3 x 10	4 x 1
Add them up…	1000	+ 200	+ 30	+ 4
Result	1,234			

289

Binary Number System

Binary Positional Notation (Cont.)

The binary positional notation system operates as shown in the tables below.

Radix	2	2	2	2	2	2	2	2
Position in Number	7	6	5	4	3	2	1	0
Calculate	(2^7)	(2^6)	(2^5)	(2^4)	(2^3)	(2^2)	(2^1)	(2^0)
Position Value	128	64	32	16	8	4	2	1

Positional Value	128	64	32	16	8	4	2	1
Binary Number (11000000)	1	1	0	0	0	0	0	0
Calculate	1x128	1x64	0x32	0x16	0x8	0x4	0x2	0x1
Add Them Up…	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Result	192							

290

Binary Number System

Convert Binary to Decimal

Convert 11000000.10101000.00001011.00001010 to decimal.

Positional Value	128	64	32	16	8	4	2	1	
Binary Number (11000000)	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	
Calculate	1x128	1x64	0x32	0x16	0x8	0x4	0x2	0x1	
Add Them Up…	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0	→ 192
Binary Number (10101000)	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	
Calculate	1x128	0x64	1x32	0x16	1x8	0x4	0x2	0x1	
Add Them Up…	128	+ 0	+ 32	+ 0	+ 8	+ 0	+ 0	+ 0	→ 168
Binary Number (00001011)	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**1**	
Calculate	0x128	0x64	0x32	0x16	1x8	0x4	1x2	1x1	
Add Them Up…	0	+ 0	+ 0	+ 0	+ 8	+ 0	+ 2	+ 1	→ 11
Binary Number (00001010)	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	
Calculate	0x128	0x64	0x32	0x16	1x8	0x4	1x2	0x1	
Add Them Up…	0	+ 0	+ 0	+ 0	+ 8	+ 0	+ 2	+ 0	→ 10

192.168.11.10

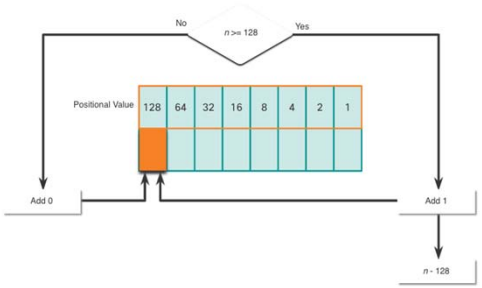
291

Binary Number System

Decimal to Binary Conversion

The binary positional value table is useful in converting a dotted decimal IPv4 address to binary.

- Start in the 128 position (the most significant bit). Is the decimal number of the octet (n) equal to or greater than 128?
- If no, record a binary 0 in the 128 positional value and move to the 64 positional value.
- If yes, record a binary 1 in the 128 positional value, subtract 128 from the decimal number, and move to the 64 positional value.
- Repeat these steps through the 1 positional value.



292

Binary Number System

Decimal to Binary Conversion Example

- Convert decimal 168 to binary

Is 168 > 128?
- Yes, enter 1 in 128 position and subtract 128 (168-128=40)

Is 40 > 64?
- No, enter 0 in 64 position and move on

Is 40 > 32?
- Yes, enter 1 in 32 position and subtract 32 (40-32=8)

Is 8 > 16?
- No, enter 0 in 16 position and move on

Is 8 > 8?
- Equal. Enter 1 in 8 position and subtract 8 (8-8=0)

No values left. Enter 0 in remaining binary positions

128	64	32	16	8	4	2	1
1	0	1	0	1	0	0	0

Decimal 168 is written as 10101000 in binary

293

Binary Number System

IPv4 Addresses

- Routers and computers only understand binary, while humans work in decimal. It is important for you to gain a thorough understanding of these two numbering systems and how they are used in networking.

294

5.2 Hexadecimal Number System

295

Hexadecimal Number System

Hexadecimal and IPv6 Addresses

- To understand IPv6 addresses, you must be able to convert hexadecimal to decimal and vice versa.
- Hexadecimal is a base sixteen numbering system, using the digits 0 through 9 and letters A to F.
- It is easier to express a value as a single hexadecimal digit than as four binary bit.
- Hexadecimal is used to represent IPv6 addresses and MAC addresses.

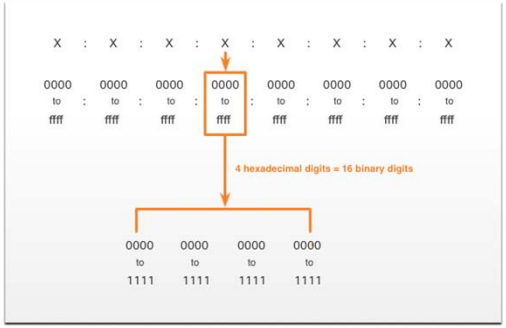
Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

296

Hexadecimal Number System

Hexadecimal and IPv6 Addresses (Cont.)

- IPv6 addresses are 128 bits in length. Every 4 bits is represented by a single hexadecimal digit. That makes the IPv6 address a total of 32 hexadecimal values.
- The figure shows the preferred method of writing out an IPv6 address, with each X representing four hexadecimal values.
- Each four hexadecimal character group is referred to as a hextet.



297

Hexadecimal Number System

Video – Converting Between Hexadecimal and Decimal Numbering Systems

This video will cover the following:

- Characteristics of the Hexadecimal System
- Convert from Hexadecimal to Decimal
- Convert from Decimal to Hexadecimal

298

Hexadecimal Number System

Decimal to Hexadecimal Conversions

Follow the steps listed to convert decimal numbers to hexadecimal values:

- Convert the decimal number to 8-bit binary strings.
- Divide the binary strings in groups of four starting from the rightmost position.
- Convert each four binary numbers into their equivalent hexadecimal digit.

For example, 168 converted into hex using the three-step process.

- 168 in binary is 10101000.
- 10101000 in two groups of four binary digits is 1010 and 1000.
- 1010 is hex A and 1000 is hex 8, so 168 is A8 in hexadecimal.

299

Hexadecimal Number System

Hexadecimal to Decimal Conversions

Follow the steps listed to convert hexadecimal numbers to decimal values:

- Convert the hexadecimal number to 4-bit binary strings.
- Create 8-bit binary grouping starting from the rightmost position.
- Convert each 8-bit binary grouping into their equivalent decimal digit.

For example, D2 converted into decimal using the three-step process:

- D2 in 4-bit binary strings is 1101 and 0010.
- 1101 and 0010 is 11010010 in an 8-bit grouping.
- 11010010 in binary is equivalent to 210 in decimal, so D2 is 210 is decimal

300

5.3 Module Practice and Quiz

301

Module Practice and Quiz

What did I learn in this module?

- Binary is a base two numbering system that consists of the numbers 0 and 1, called bits.
- Decimal is a base ten numbering system that consists of the numbers 0 through 9.
- Binary is what hosts, servers, and networking equipment uses to identify each other.
- Hexadecimal is a base sixteen numbering system that consists of the numbers 0 through 9 and the letters A to F.
- Hexadecimal is used to represent IPv6 addresses and MAC addresses.
- IPv6 addresses are 128 bits long, and every 4 bits is represented by a hexadecimal digit for a total of 32 hexadecimal digits.
- To convert hexadecimal to decimal, you must first convert the hexadecimal to binary, then convert the binary to decimal.
- To convert decimal to hexadecimal, you must first convert the decimal to binary and then the binary to hexadecimal.

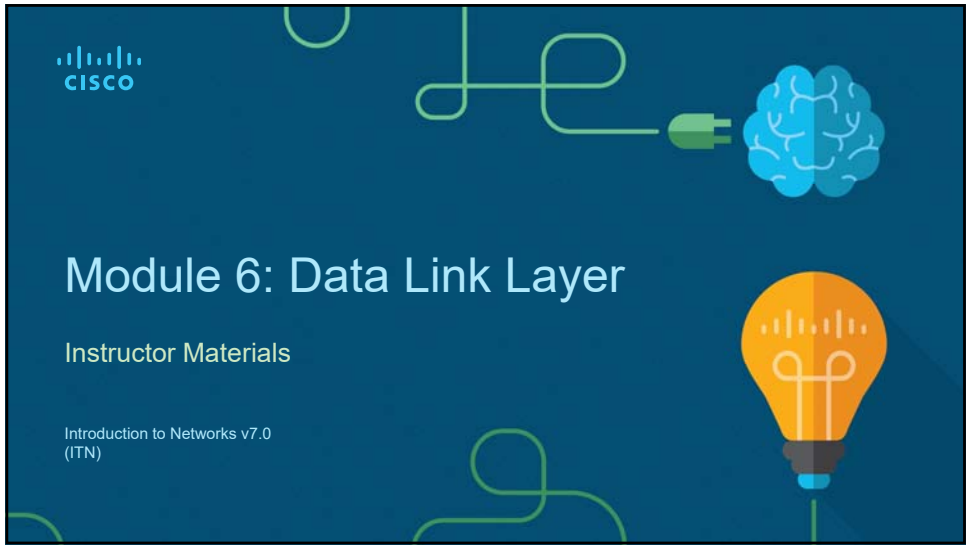
302

Module 5: Number Systems

New Terms and Commands

- dotted decimal notation
- positional notation
- base 10
- base 16
- radix
- octet
- hextet

303



304

What to Expect in this Module

- To facilitate learning, the following features within the GUI may be included in this module:

Feature	Description
Animations	Expose learners to new skills and concepts.
Videos	Expose learners to new skills and concepts.
Check Your Understanding(CYU)	Per topic online quiz to help learners gauge content understanding.
Interactive Activities	A variety of formats to help learners gauge content understanding.
Syntax Checker	Small simulations that expose learners to Cisco command line to practice configuration skills.
PT Activity	Simulation and modeling activities designed to explore, acquire, reinforce, and expand skills.

306

What to Expect in this Module (Cont.)

- To facilitate learning, the following features may be included in this module:

Feature	Description
Hands-On Labs	Labs designed for working with physical equipment.
Class Activities	These are found on the Instructor Resources page. Class Activities are designed to facilitate learning, class discussion, and collaboration.
Module Quizzes	Self-assessments that integrate concepts and skills learned throughout the series of topics presented in the module.
Module Summary	Briefly recaps module content.

307

312

Module Objectives

Module Title: Data Link Layer

Module Objective: Explain how media access control in the data link layer supports communication across networks.

Topic Title	Topic Objective
Purpose of the Data Link Layer	Describe the purpose and function of the data link layer in preparing communication for transmission on specific media.
Topologies	Compare the characteristics of media access control methods on WAN and LAN topologies.
Data Link Frame	Describe the characteristics and functions of the data link frame.

313

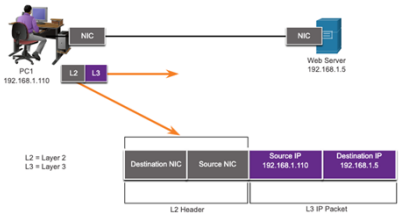
6.1 Purpose of the Data Link Layer

314

Purpose of the Data Link Layer

The Data Link Layer

- The Data Link layer is responsible for communications between end-device network interface cards.
- It allows upper layer protocols to access the physical layer media and encapsulates Layer 3 packets (IPv4 and IPv6) into Layer 2 Frames.
- It also performs error detection and rejects corrupts frames.



315

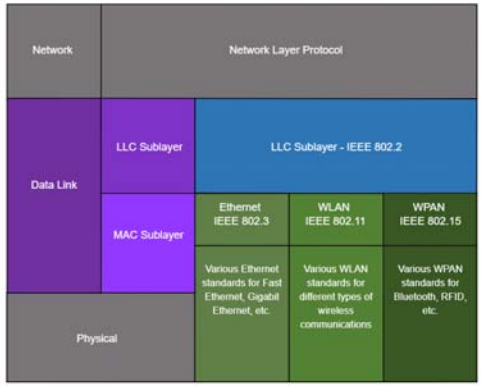
Purpose of the Data Link Layer

IEEE 802 LAN/MAN Data Link Sublayers

IEEE 802 LAN/MAN standards are specific to the type of network (Ethernet, WLAN, WPAN, etc).

The Data Link Layer consists of two sublayers. **Logical Link Control (LLC)** and **Media Access Control (MAC).**

- The LLC sublayer communicates between the networking software at the upper layers and the device hardware at the lower layers.
- The MAC sublayer is responsible for data encapsulation and media access control.



316

Purpose of the Data Link Layer

Providing Access to Media

Packets exchanged between nodes may experience numerous data link layers and media transitions.

At each hop along the path, a router performs four basic Layer 2 functions:

- Accepts a frame from the network medium.
- De-encapsulates the frame to expose the encapsulated packet.
- Re-encapsulates the packet into a new frame.
- Forwards the new frame on the medium of the next network segment.

317

Purpose of the Data Link Layer

Data Link Layer Standards

Data link layer protocols are defined by engineering organizations:

- Institute for Electrical and Electronic Engineers (IEEE).
- International Telecommunications Union (ITU).
- International Organizations for Standardization (ISO).
- American National Standards Institute (ANSI).

318

6.2 Topologies

319

Topologies

Physical and Logical Topologies

The topology of a network is the arrangement and relationship of the network devices and the interconnections between them.

There are two types of topologies used when describing networks:

- **Physical topology** – shows physical connections and how devices are interconnected.
- **Logical topology** – identifies the virtual connections between devices using device interfaces and IP addressing schemes.

320

Topologies
WAN Topologies

There are three common physical WAN topologies:

- **Point-to-point** – the simplest and most common WAN topology. Consists of a permanent link between two endpoints.
- **Hub and spoke** – similar to a star topology where a central site interconnects branch sites through point-to-point links.
- **Mesh** – provides high availability but requires every end system to be connected to every other end system.

 321

321

Topologies
Point-to-Point WAN Topology

- Physical point-to-point topologies directly connect two nodes.
- The nodes may not share the media with other hosts.
- Because all frames on the media can only travel to or from the two nodes, Point-to-Point WAN protocols can be very simple.

 322

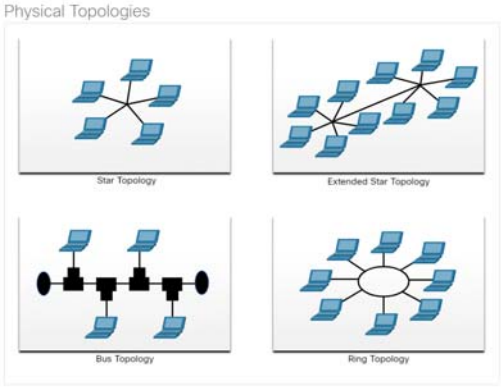
322

Topologies
LAN Topologies

End devices on LANs are typically interconnected using a star or extended star topology. Star and extended star topologies are easy to install, very scalable and easy to troubleshoot.

Early Ethernet and Legacy Token Ring technologies provide two additional topologies:

- **Bus** – All end systems chained together and terminated on each end.
- **Ring** – Each end system is connected to its respective neighbors to form a ring.



 323

323

Topologies
Half and Full Duplex Communication

Half-duplex communication

- Only allows one device to send or receive at a time on a shared medium.
- Used on WLANs and legacy bus topologies with Ethernet hubs.

Full-duplex communication

- Allows both devices to simultaneously transmit and receive on a shared medium.
- Ethernet switches operate in full-duplex mode.

 324

324

Topologies
Access Control Methods

Contention-based access

All nodes operating in half-duplex, competing for use of the medium. Examples are:

- Carrier sense multiple access with collision detection (CSMA/CD) as used on legacy bus-topology Ethernet.
- Carrier sense multiple access with collision avoidance (CSMA/CA) as used on Wireless LANs.

Controlled access

- Deterministic access where each node has its own time on the medium.
- Used on legacy networks such as Token Ring and ARCNET.

325

Topologies
Contention-Based Access – CSMA/CD

CSMA/CD

- Used by legacy Ethernet LANs.
- Operates in half-duplex mode where only one device sends or receives at a time.
- Uses a collision detection process to govern when a device can send and what happens if multiple devices send at the same time.

CSMA/CD collision detection process:

- Devices transmitting simultaneously will result in a signal collision on the shared media.
- Devices detect the collision.
- Devices wait a random period of time and retransmit data.

326

Topologies
Contention-Based Access – CSMA/CA

CSMA/CA

- Used by IEEE 802.11 WLANs.
- Operates in half-duplex mode where only one device sends or receives at a time.
- Uses a collision avoidance process to govern when a device can send and what happens if multiple devices send at the same time.

CSMA/CA collision avoidance process:

- When transmitting, devices also include the time duration needed for the transmission.
- Other devices on the shared medium receive the time duration information and know how long the medium will be unavailable.

327

6.3 Data Link Frame

328

Data Link Frame
The Frame

Data is encapsulated by the data link layer with a header and a trailer to form a frame.

A data link frame has three parts:

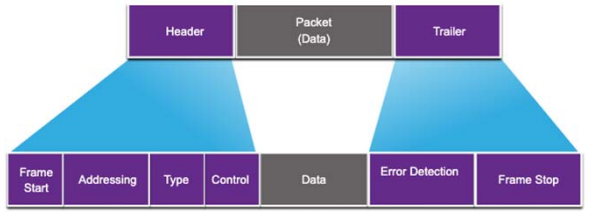
- Header
- Data
- Trailer

The fields of the header and trailer vary according to data link layer protocol.

The amount of control information carried with in the frame varies according to access control information and logical topology.

329

Data Link Frame
Frame Fields

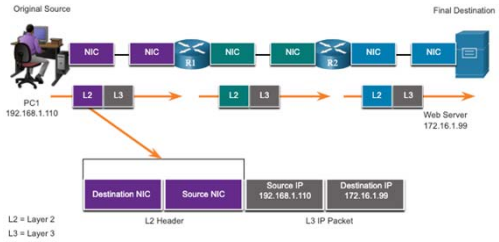


Field	Description
Frame Start and Stop	Identifies beginning and end of frame
Addressing	Indicates source and destination nodes
Type	Identifies encapsulated Layer 3 protocol
Control	Identifies flow control services
Data	Contains the frame payload
Error Detection	Used for determine transmission errors

330

Data Link Frame
Layer 2 Addresses

- Also referred to as a physical address.
- Contained in the frame header.
- Used only for local delivery of a frame on the link.
- Updated by each device that forwards the frame.



331

Data Link Frame
LAN and WAN Frames

The logical topology and physical media determine the data link protocol used:

- Ethernet
- 802.11 Wireless
- Point-to-Point (PPP)
- High-Level Data Link Control (HDLC)
- Frame-Relay

Each protocol performs media access control for specified logical topologies.

332

6.4 Module Practice and Quiz

333

Module Practice and Quiz

What did I learn in this module?

- The data link layer of the OSI model (Layer 2) prepares network data for the physical network.
- The data link layer is responsible for network interface card (NIC) to network interface card communications.
- The IEEE 802 LAN/MAN data link layer consists of the following two sublayers: LLC and MAC.
- The two types of topologies used in LAN and WAN networks are physical and logical.
- Three common types of physical WAN topologies are: point-to-point, hub and spoke, and mesh.
- Half-duplex communications exchange data in one direction at a time. Full-duplex sends and receives data simultaneously.
- In contention-based multi-access networks, all nodes are operating in half-duplex.
- Examples of contention-based access methods include: CSMA/CD for bus-topology Ethernet LANs and CSMA/CA for WLANs.
- The data link frame has three basic parts: header, data, and trailer.
- Frame fields include: frame start and stop indicator flags, addressing, type, control, data, and error detection.
- Data link addresses are also known as physical addresses.
- Data link addresses are only used for link local delivery of frames.

334

Module 6: Data Link Layer

New Terms and Commands

- Logical Link Control (LLC)
- Medial Access Control (MAC)
- Institute of Electrical and Electronic Engineers (IEEE)
- International Telecommunications Union (ITU)
- International Organization for Standardization (ISO)
- American National Standards Institute (ANSI)
- Physical Topology
- Logical Topology
- Half-duplex
- Full-duplex
- CSMA/CD
- CSMA/CA
- Cyclic Redundancy Check (CRC)
- Contention-based access
- Controlled access

335

Module 7: Ethernet Switching

Instructor Materials

Introduction to Networks v7.0 (ITN)

336

What to Expect in this Module

- To facilitate learning, the following features within the GUI may be included in this module:

Feature	Description
Animations	Expose learners to new skills and concepts.
Videos	Expose learners to new skills and concepts.
Check Your Understanding(CYU)	Per topic online quiz to help learners gauge content understanding.
Interactive Activities	A variety of formats to help learners gauge content understanding.
Syntax Checker	Small simulations that expose learners to Cisco command line to practice configuration skills.
PT Activity	Simulation and modeling activities designed to explore, acquire, reinforce, and expand skills.

338

What to Expect in this Module (Cont.)

- To facilitate learning, the following features may be included in this module:

Feature	Description
Hands-On Labs	Labs designed for working with physical equipment.
Class Activities	These are found on the Instructor Resources page. Class Activities are designed to facilitate learning, class discussion, and collaboration.
Module Quizzes	Self-assessments that integrate concepts and skills learned throughout the series of topics presented in the module.
Module Summary	Briefly recaps module content.

339

344

Module Objectives

Module Title: Ethernet Switching

Module Objective: Explain how Ethernet works in a switched network.

Topic Title	Topic Objective
Ethernet Frame	Explain how the Ethernet sublayers are related to the frame fields.
Ethernet MAC Address	Describe the Ethernet MAC address.
The MAC Address Table	Explain how a switch builds its MAC address table and forwards frames.
Switch Speeds and Forwarding Methods	Describe switch forwarding methods and port settings available on Layer 2 switch ports.

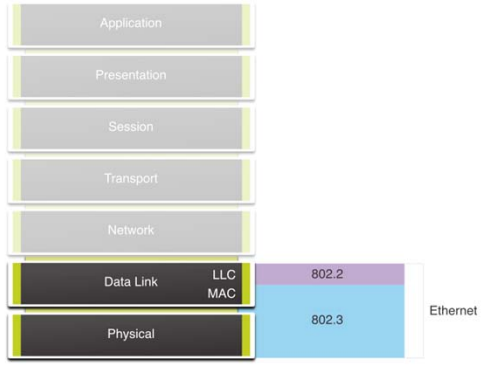
345

7.1 Ethernet Frames

346

Ethernet Frames
Ethernet Encapsulation

- Ethernet operates in the data link layer and the physical layer.
- It is a family of networking technologies defined in the IEEE 802.2 and 802.3 standards.

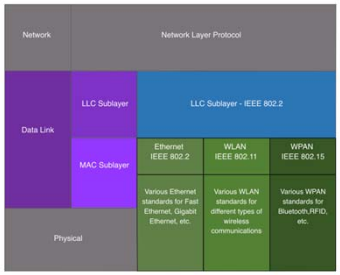


347

Ethernet Frames
Data Link Sublayers

The 802 LAN/MAN standards, including Ethernet, use two separate sublayers of the data link layer to operate:

- **LLC Sublayer**: (IEEE 802.2) Places information in the frame to identify which network layer protocol is used for the frame.
- **MAC Sublayer**: (IEEE 802.3, 802.11, or 802.15) Responsible for data encapsulation and media access control, and provides data link layer addressing.



348

Ethernet Frames
MAC Sublayer

The MAC sublayer is responsible for data encapsulation and accessing the media.

Data Encapsulation

IEEE 802.3 data encapsulation includes the following:

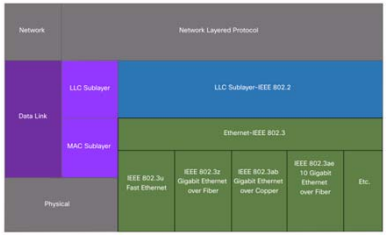
1. **Ethernet frame** - This is the internal structure of the Ethernet frame.
2. **Ethernet Addressing** - The Ethernet frame includes both a source and destination MAC address to deliver the Ethernet frame from Ethernet NIC to Ethernet NIC on the same LAN.
3. **Ethernet Error detection** - The Ethernet frame includes a frame check sequence (FCS) trailer used for error detection.

349

Ethernet Frames
MAC Sublayer

Media Access

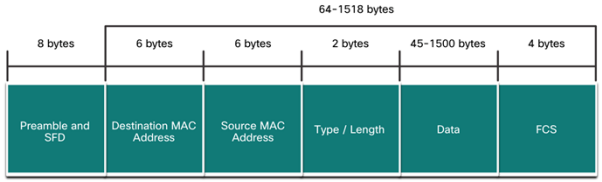
- The IEEE 802.3 MAC sublayer includes the specifications for different Ethernet communications standards over various types of media including copper and fiber.
- Legacy Ethernet using a bus topology or hubs, is a shared, half-duplex medium. Ethernet over a half-duplex medium uses a contention-based access method, carrier sense multiple access/collision detection (CSMA/CD).
- Ethernet LANs of today use switches that operate in full-duplex. Full-duplex communications with Ethernet switches do not require access control through CSMA/CD.



350

Ethernet Frames
Ethernet Frame Fields

- The minimum Ethernet frame size is 64 bytes and the maximum is 1518 bytes. The preamble field is not included when describing the size of the frame.
- Any frame less than 64 bytes in length is considered a “collision fragment” or “runt frame” and is automatically discarded. Frames with more than 1500 bytes of data are considered “jumbo” or “baby giant frames”.
- If the size of a transmitted frame is less than the minimum, or greater than the maximum, the receiving device drops the frame. Dropped frames are likely to be the result of collisions or other unwanted signals. They are considered invalid. Jumbo frames are usually supported by most Fast Ethernet and Gigabit Ethernet switches and NICs.



351

Ethernet Frames
Lab – Use Wireshark to Examine Ethernet Frames

In this lab, you will complete the following objectives:

- Part 1: Examine the Header Fields in an Ethernet II Frame
- Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

352

7.2 Ethernet MAC Address

353

Ethernet MAC Addresses

MAC Address and Hexadecimal

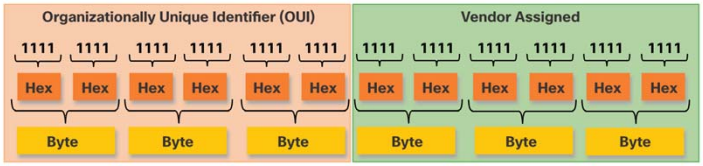
- An Ethernet MAC address consists of a 48-bit binary value, expressed using 12 hexadecimal values.
- Given that 8 bits (one byte) is a common binary grouping, binary 00000000 to 11111111 can be represented in hexadecimal as the range 00 to FF,
- When using hexadecimal, leading zeroes are always displayed to complete the 8-bit representation. For example the binary value 0000 1010 is represented in hexadecimal as 0A.
- Hexadecimal numbers are often represented by the value preceded by **0x** (e.g., 0x73) to distinguish between decimal and hexadecimal values in documentation.
- Hexadecimal may also be represented by a subscript 16, or the hex number followed by an H (e.g., 73H).

354

Ethernet MAC Addresses

Ethernet MAC Address

- In an Ethernet LAN, every network device is connected to the same, shared media. MAC addressing provides a method for device identification at the data link layer of the OSI model.
- An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits. Because a byte equals 8 bits, we can also say that a MAC address is 6 bytes in length.
- All MAC addresses must be unique to the Ethernet device or Ethernet interface. To ensure this, all vendors that sell Ethernet devices must register with the IEEE to obtain a unique 6 hexadecimal (i.e., 24-bit or 3-byte) code called the organizationally unique identifier (OUI).
- An Ethernet MAC address consists of a 6 hexadecimal vendor OUI code followed by a 6 hexadecimal vendor-assigned value.



355

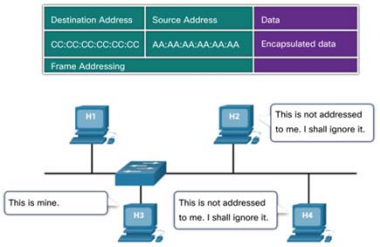
Ethernet MAC Addresses

Frame Processing

- When a device is forwarding a message to an Ethernet network, the Ethernet header include a Source MAC address and a Destination MAC address.
- When a NIC receives an Ethernet frame, it examines the destination MAC address to see if it matches the physical MAC address that is stored in RAM. If there is no match, the device discards the frame. If there is a match, it passes the frame up the OSI layers, where the de-encapsulation process takes place.

Note: Ethernet NICs will also accept frames if the destination MAC address is a broadcast or a multicast group of which the host is a member.

- Any device that is the source or destination of an Ethernet frame, will have an Ethernet NIC and therefore, a MAC address. This includes workstations, servers, printers, mobile devices, and routers.



356

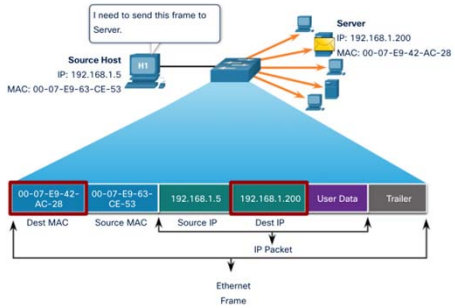
Ethernet MAC Addresses

Unicast MAC Address

In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

- A unicast MAC address is the unique address that is used when a frame is sent from a single transmitting device to a single destination device.
- The process that a source host uses to determine the destination MAC address associated with an IPv4 address is known as Address Resolution Protocol (ARP). The process that a source host uses to determine the destination MAC address associated with an IPv6 address is known as Neighbor Discovery (ND).

Note: The source MAC address must always be a unicast.



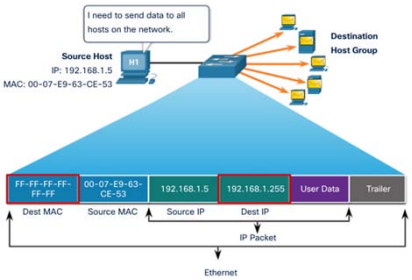
357

Ethernet MAC Addresses

Broadcast MAC Address

An Ethernet broadcast frame is received and processed by every device on the Ethernet LAN. The features of an Ethernet broadcast are as follows:

- It has a destination MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).
- It is flooded out all Ethernet switch ports except the incoming port. It is not forwarded by a router.
- If the encapsulated data is an IPv4 broadcast packet, this means the packet contains a destination IPv4 address that has all ones (1s) in the host portion. This numbering in the address means that all hosts on that local network (broadcast domain) will receive and process the packet.



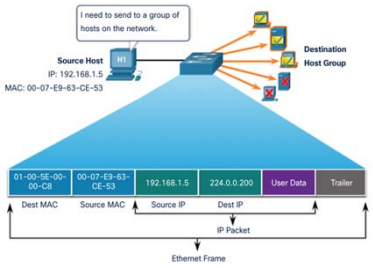
358

Ethernet MAC Addresses

Multicast MAC Address

An Ethernet multicast frame is received and processed by a group of devices that belong to the same multicast group.

- There is a destination MAC address of 01-00-5E when the encapsulated data is an IPv4 multicast packet and a destination MAC address of 33-33 when the encapsulated data is an IPv6 multicast packet.
- There are other reserved multicast destination MAC addresses for when the encapsulated data is not IP, such as Spanning Tree Protocol (STP).
- It is flooded out all Ethernet switch ports except the incoming port, unless the switch is configured for multicast snooping. It is not forwarded by a router, unless the router is configured to route multicast packets.
- Because multicast addresses represent a group of addresses (sometimes called a host group), they can only be used as the destination of a packet. The source will always be a unicast address.
- As with the unicast and broadcast addresses, the multicast IP address requires a corresponding multicast MAC address.



359

Ethernet MAC Addresses

Lab – View Network Device MAC Addresses

In this lab, you will complete the following objectives:

- Part 1: Set Up the Topology and Initialize Devices
- Part 2: Configure Devices and Verify Connectivity
- Part 3: Display, Describe, and Analyze Ethernet MAC Addresses

360

7.3 The MAC Address Table

361

The MAC Address Table

Switch Fundamentals

- A Layer 2 Ethernet switch uses Layer 2 MAC addresses to make forwarding decisions. It is completely unaware of the data (protocol) being carried in the data portion of the frame, such as an IPv4 packet, an ARP message, or an IPv6 ND packet. The switch makes its forwarding decisions based solely on the Layer 2 Ethernet MAC addresses.
- An Ethernet switch examines its MAC address table to make a forwarding decision for each frame, unlike legacy Ethernet hubs that repeat bits out all ports except the incoming port.
- When a switch is turned on, the MAC address table is empty

Note: The MAC address table is sometimes referred to as a content addressable memory (CAM) table.

362

The MAC Address Table

Switch Learning and Forwarding

Examine the Source MAC Address (Learn)

Every frame that enters a switch is checked for new information to learn. It does this by examining the source MAC address of the frame and the port number where the frame entered the switch. If the source MAC address does not exist, it is added to the table along with the incoming port number. If the source MAC address does exist, the switch updates the refresh timer for that entry. By default, most Ethernet switches keep an entry in the table for 5 minutes.

Note: If the source MAC address does exist in the table but on a different port, the switch treats this as a new entry. The entry is replaced using the same MAC address but with the more current port number.

363

The MAC Address Table

Switch Learning and Forwarding (Contd.)

Find the Destination MAC Address (Forward)

If the destination MAC address is a unicast address, the switch will look for a match between the destination MAC address of the frame and an entry in its MAC address table. If the destination MAC address is in the table, it will forward the frame out the specified port. If the destination MAC address is not in the table, the switch will forward the frame out all ports except the incoming port. This is called an unknown unicast.

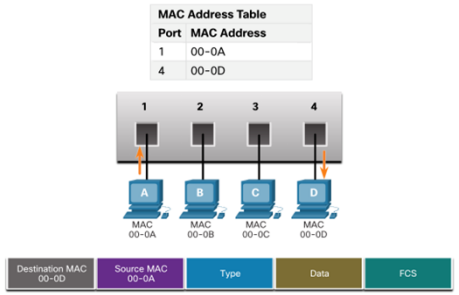
Note: If the destination MAC address is a broadcast or a multicast, the frame is also flooded out all ports except the incoming port.

364

The MAC Address Table

Filtering Frames

As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of every frame. When the MAC address table of the switch contains the destination MAC address, it is able to filter the frame and forward out a single port.



365

The MAC Address Table

Video – MAC Address Tables on Connected Switches

This video will cover the following:

- How switches build MAC address tables
- How switches forward frames base on the content of their MAC address tables

366

The MAC Address Table

Video – Sending the Frame to the Default Gateway

This video will cover the following:

- What a switch does when the destination MAC address is not listed in the switch's MAC address table.
- What a switch does when the source MAC address is not listed in the switch's MAC address table

367

The MAC Address Table

Lab – View the Switch MAC Address Table

In this lab, you will complete the following objectives:

- Part 1: Build and Configure the Network
- Part 2: Examine the Switch MAC Address Table

368

7.4 Switch Speeds and Forwarding Methods

369

Switch Speeds and Forwarding Methods

Frame Forwarding Methods on Cisco Switches

Switches use one of the following forwarding methods for switching data between network ports:

- **Store-and-forward switching** - This frame forwarding method receives the entire frame and computes the CRC. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. Then the frame is forwarded out of the correct port.
- **Cut-through switching** - This frame forwarding method forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

- A big advantage of store-and-forward switching is that it determines if a frame has errors before propagating the frame. When an error is detected in a frame, the switch discards the frame. Discarding frames with errors reduces the amount of bandwidth consumed by corrupt data.
- Store-and-forward switching is required for quality of service (QoS) analysis on converged networks where frame classification for traffic prioritization is necessary. For example, voice over IP (VoIP) data streams need to have priority over web-browsing traffic.

 370

370

Switch Speeds and Forwarding Methods

Cut-Through Switching

In cut-through switching, the switch acts upon the data as soon as it is received, even if the transmission is not complete. The switch buffers just enough of the frame to read the destination MAC address so that it can determine to which port it should forward out the data. The switch does not perform any error checking on the frame.

There are two variants of cut-through switching:

- **Fast-forward switching -** Offers the lowest level of latency by immediately forwarding a packet after reading the destination address. Because fast-forward switching starts forwarding before the entire packet has been received, there may be times when packets are relayed with errors. The destination NIC discards the faulty packet upon receipt. Fast-forward switching is the typical cut-through method of switching.
- **Fragment-free switching -** A compromise between the high latency and high integrity of store-and-forward switching and the low latency and reduced integrity of fast-forward switching, the switch stores and performs an error check on the first 64 bytes of the frame before forwarding. Because most network errors and collisions occur during the first 64 bytes, this ensures that a collision has not occurred before forwarding the frame.

 371

371

Switch Speeds and Forwarding Methods

Memory Buffering on Switches

An Ethernet switch may use a buffering technique to store frames before forwarding them or when the destination port is busy because of congestion.

Method	Description
Port-based memory	•Frames are stored in queues that are linked to specific incoming and outgoing ports. •A frame is transmitted to the outgoing port only when all the frames ahead in the queue have been successfully transmitted. •It is possible for a single frame to delay the transmission of all the frames in memory because of a busy destination port. •This delay occurs even if the other frames could be transmitted to open destination ports.
Shared memory	•Deposits all frames into a common memory buffer shared by all switch ports and the amount of buffer memory required by a port is dynamically allocated. •The frames in the buffer are dynamically linked to the destination port enabling a packet to be received on one port and then transmitted on another port, without moving it to a different queue.

- Shared memory buffering also results in larger frames that can be transmitted with fewer dropped frames. This is important with asymmetric switching which allows for different data rates on different ports. Therefore, more bandwidth can be dedicated to certain ports (e.g., server port).

 372

372

Switch Speeds and Forwarding Methods

Duplex and Speed Settings

Two of the most basic settings on a switch are the bandwidth (“speed”) and duplex settings for each individual switch port. It is critical that the duplex and bandwidth settings match between the switch port and the connected devices.

There are two types of duplex settings used for communications on an Ethernet network:

- **Full-duplex** - Both ends of the connection can send and receive simultaneously.
- **Half-duplex** - Only one end of the connection can send at a time.

Autonegotiation is an optional function found on most Ethernet switches and NICs. It enables two devices to automatically negotiate the best speed and duplex capabilities.

Note: Gigabit Ethernet ports only operate in full-duplex.

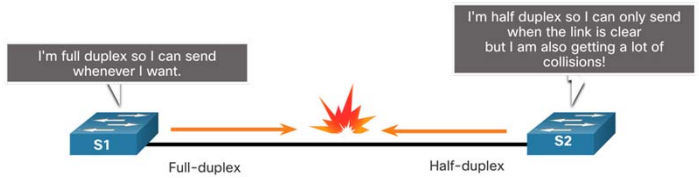
 373

373

Switch Speeds and Forwarding Methods

Duplex and Speed Settings

- Duplex mismatch is one of the most common causes of performance issues on 10/100 Mbps Ethernet links. It occurs when one port on the link operates at half-duplex while the other port operates at full-duplex.
- This can occur when one or both ports on a link are reset, and the autonegotiation process does not result in both link partners having the same configuration.
- It also can occur when users reconfigure one side of a link and forget to reconfigure the other. Both sides of a link should have autonegotiation on, or both sides should have it off. Best practice is to configure both Ethernet switch ports as full-duplex.



374

Switch Speeds and Forwarding Methods

Auto-MDIX

Connections between devices once required the use of either a crossover or straight-through cable. The type of cable required depended on the type of interconnecting devices.

Note: A direct connection between a router and a host requires a cross-over connection.

- Most switch devices now support the automatic medium-dependent interface crossover (auto-MDIX) feature. When enabled, the switch automatically detects the type of cable attached to the port and configures the interfaces accordingly.
- The auto-MDIX feature is enabled by default on switches running Cisco IOS Release 12.2(18)SE or later. However, the feature could be disabled. For this reason, you should always use the correct cable type and not rely on the auto-MDIX feature.
- Auto-MDIX can be re-enabled using the **mdix auto** interface configuration command.

375

7.5 Module Practice and Quiz

376

Module Practice and Quiz

What did I learn in this module?

- Ethernet operates in the data link layer and the physical layer. Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.
- Ethernet uses the LLC and MAC sublayers of the data link layer to operate.
- The Ethernet frame fields are: preamble and start frame delimiter, destination MAC address, source MAC address, EtherType, data, and FCS.
- MAC addressing provides a method for device identification at the data link layer of the OSI model.
- An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits, or 6 bytes.
- When a device is forwarding a message to an Ethernet network, the Ethernet header includes the source and destination MAC addresses. In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

377

Module Practice and Quiz

What did I learn in this module? (Contd.)

- A Layer 2 Ethernet switch makes its forwarding decisions based solely on the Layer 2 Ethernet MAC addresses.
- The switch dynamically builds the MAC address table by examining the source MAC address of the frames received on a port.
- The switch forwards frames by searching for a match between the destination MAC address in the frame and an entry in the MAC address table.
- Switches use one of the following forwarding methods for switching data between network ports: store-and-forward switching or cut-through switching. Two variants of cut-through switching are fast-forward and fragment-free.
- Two methods of memory buffering are port-based memory and shared memory.
- There are two types of duplex settings used for communications on an Ethernet network: full-duplex and half-duplex.

Module 7: Ethernet Switching

New Terms and Commands

- Store-and-Forward Switching
- Cut-through Switching
- Fast-Forward Switching
- Fragment-free Switching
- OUI (Organizationally Unique Identifier)
- ARP (Address Resolution Protocol)
- ND (Neighbor Discovery)
- Port-based memory
- Shared memory
- Auto-MDIX

Module 8: Network Layer

Instructor Materials

Introduction to Networks v7.0 (ITN)

What to Expect in this Module

- To facilitate learning, the following features within the GUI may be included in this module:

Feature	Description
Animations	Expose learners to new skills and concepts.
Videos	Expose learners to new skills and concepts.
Check Your Understanding(CYU)	Per topic online quiz to help learners gauge content understanding.
Interactive Activities	A variety of formats to help learners gauge content understanding.
Syntax Checker	Small simulations that expose learners to Cisco command line to practice configuration skills.
PT Activity	Simulation and modeling activities designed to explore, acquire, reinforce, and expand skills.

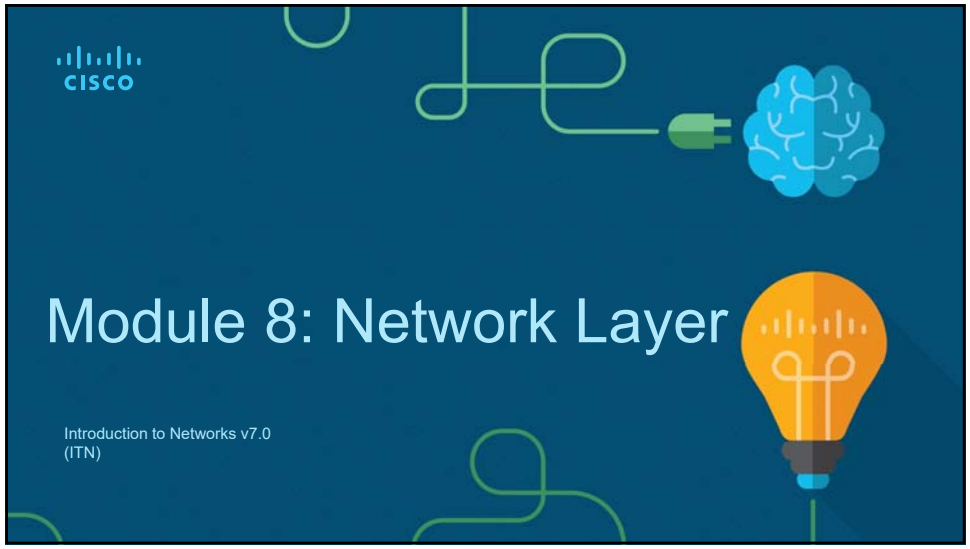
What to Expect in this Module (Cont.)

- To facilitate learning, the following features may be included in this module:

Feature	Description
Hands-On Labs	Labs designed for working with physical equipment.
Class Activities	These are found on the Instructor Resources page. Class Activities are designed to facilitate learning, class discussion, and collaboration.
Module Quizzes	Self-assessments that integrate concepts and skills learned throughout the series of topics presented in the module.
Module Summary	Briefly recaps module content.

 383

383



389

Module 8: Topics

What will I learn to do in this module?

Topic Title	Topic Objective
Network Layer Characteristics	Explain how the network layer uses IP protocols for reliable communications.
IPv4 Packet	Explain the role of the major header fields in the IPv4 packet.
IPv6 Packet	Explain the role of the major header fields in the IPv6 packet.
How a Host Routes	Explain how network devices use routing tables to direct packets to a destination network.
Router Routing Tables	Explain the function of fields in the routing table of a router.

 390

390

8.1 Network Layer Characteristics

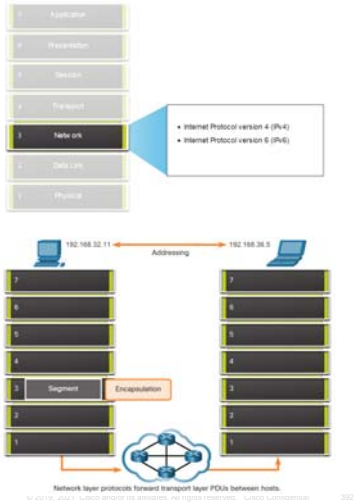
 391

391

Network Layer Characteristics

The Network Layer

- Provides services to allow end devices to exchange data
- IP version 4 (IPv4) and IP version 6 (IPv6) are the principle network layer communication protocols.
- The network layer performs four basic operations:
  - Addressing end devices
  - Encapsulation
  - Routing
  - De-encapsulation



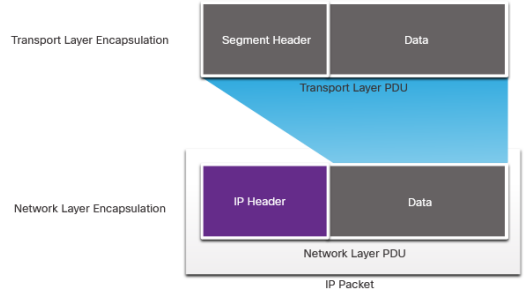
392

Network Layer Characteristics

IP Encapsulation

- IP encapsulates the transport layer segment.
- IP can use either an IPv4 or IPv6 packet and not impact the layer 4 segment.
- IP packet will be examined by all layer 3 devices as it traverses the network.
- The IP addressing does not change from source to destination.

Note: NAT will change addressing, but will be discussed in a later module.



393

Network Layer Characteristics

Characteristics of IP

IP is meant to have low overhead and may be described as:

- Connectionless
- Best Effort
- Media Independent

394

Network Layer Characteristics

Connectionless

IP is Connectionless

- IP does not establish a connection with the destination before sending the packet.
- There is no control information needed (synchronizations, acknowledgments, etc.).
- The destination will receive the packet when it arrives, but no pre-notifications are sent by IP.
- If there is a need for connection-oriented traffic, then another protocol will handle this (typically TCP at the transport layer).

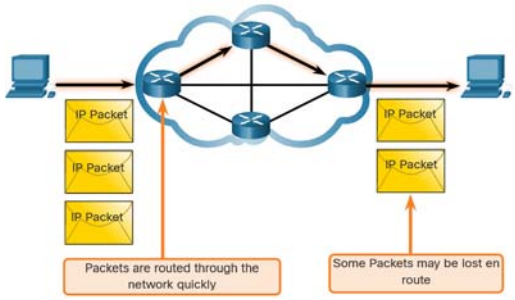
395

Network Layer Characteristics

Best Effort

IP is Best Effort

- IP will not guarantee delivery of the packet.
- IP has reduced overhead since there is no mechanism to resend data that is not received.
- IP does not expect acknowledgments.
- IP does not know if the other device is operational or if it received the packet.



396

Network Layer Characteristics

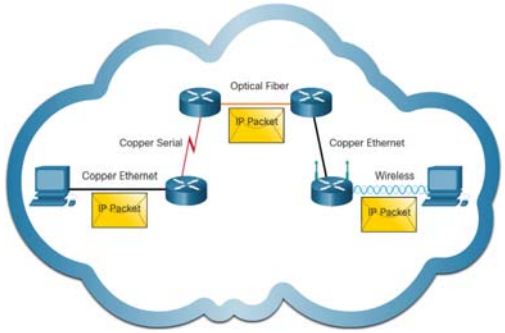
Media Independent

IP is unreliable:

- It cannot manage or fix undelivered or corrupt packets.
- IP cannot retransmit after an error.
- IP cannot realign out of sequence packets.
- IP must rely on other protocols for these functions.

IP is media Independent:

- IP does not concern itself with the type of frame required at the data link layer or the media type at the physical layer.
- IP can be sent over any media type: copper, fiber, or wireless.



397

Network Layer Characteristics

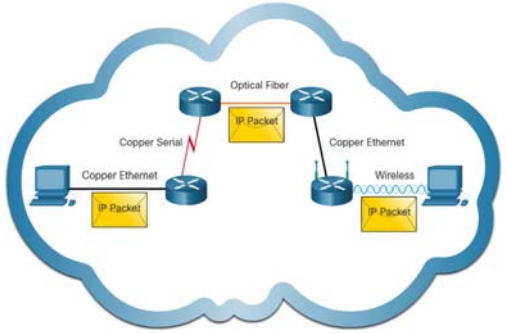
Media Independent (Contd.)

The network layer will establish the Maximum Transmission Unit (MTU).

- Network layer receives this from control information sent by the data link layer.
- The network then establishes the MTU size.

Fragmentation is when Layer 3 splits the IPv4 packet into smaller units.

- Fragmenting causes latency.
- IPv6 does not fragment packets.
- Example: Router goes from Ethernet to a slow WAN with a smaller MTU



398

8.2 IPv4 Packet

399

IPv4 Packet

IPv4 Packet Header

IPv4 is the primary communication protocol for the network layer.

The network header has many purposes:

- It ensures the packet is sent in the correct direction (to the destination).
- It contains information for network layer processing in various fields.
- The information in the header is used by all layer 3 devices that handle the packet

400

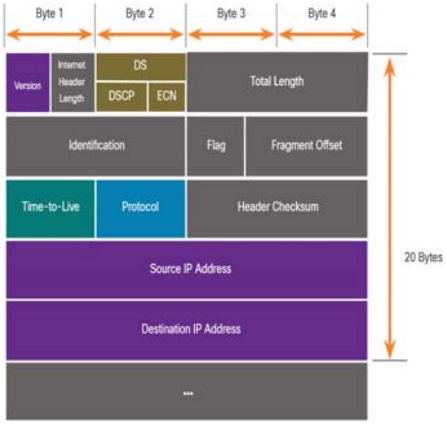
IPv4 Packet

IPv4 Packet Header Fields

The IPv4 network header characteristics:

- It is in binary.
- Contains several fields of information
- Diagram is read from left to right, 4 bytes per line
- The two most important fields are the source and destination.

Protocols may have may have one or more functions.



401

IPv4 Packet

IPv4 Packet Header Fields

Significant fields in the IPv4 header:

Function	Description
Version	This will be for v4, as opposed to v6, a 4 bit field= 0100
Differentiated Services	Used for QoS: DiffServ – DS field or the older IntServ – ToS or Type of Service
Header Checksum	Detect corruption in the IPv4 header
Time to Live (TTL)	Layer 3 hop count. When it becomes zero the router will discard the packet.
Protocol	I.D.s next level protocol: ICMP, TCP, UDP, etc.
Source IPv4 Address	32 bit source address
Destination IPV4 Address	32 bit destination address

402

IPv4 Packet

Video – Sample IPv4 Headers in Wireshark

This video will cover the following:

- IPv4 Ethernet packets in Wireshark
- The control information
- The difference between packets

403

8.3 IPv6 Packets

404

IPv6 Packets

Limitations of IPv4

IPv4 has three major limitations:

- IPv4 address depletion – We have basically run out of IPv4 addressing.
- Lack of end-to-end connectivity – To make IPv4 survive this long, private addressing and NAT were created. This ended direct communications with public addressing.
- Increased network complexity – NAT was meant as temporary solution and creates issues on the network as a side effect of manipulating the network headers addressing. NAT causes latency and troubleshooting issues.

405

IPv6 Packets

IPv6 Overview

- IPv6 was developed by Internet Engineering Task Force (IETF).
- IPv6 overcomes the limitations of IPv4.
- Improvements that IPv6 provides:
  - **Increased address space** – based on 128 bit address, not 32 bits
  - **Improved packet handling** – simplified header with fewer fields
  - **Eliminates the need for NAT** – since there is a huge amount of addressing, there is no need to use private addressing internally and be mapped to a shared public address

IPv4 and IPv6 Address Space Comparison

Number Name	Scientific Notation	Number of Zeros
1 Thousand	10^{3}	1,000
1 Million	10^{6}	1,000,000
1 Billion	10^{9}	1,000,000,000
1 Trillion	10^{12}	1,000,000,000,000
1 Quadrillion	10^{15}	1,000,000,000,000,000
1 Quintillion	10^{18}	1,000,000,000,000,000,000
1 Sextillion	10^{21}	1,000,000,000,000,000,000,000
1 Septillion	10^{24}	1,000,000,000,000,000,000,000,000
1 Octillion	10^{27}	1,000,000,000,000,000,000,000,000,000
1 Nonillion	10^{30}	1,000,000,000,000,000,000,000,000,000,000
1 Decillion	10^{33}	1,000,000,000,000,000,000,000,000,000,000,000
1 Undecillion	10^{36}	1,000,000,000,000,000,000,000,000,000,000,000,000

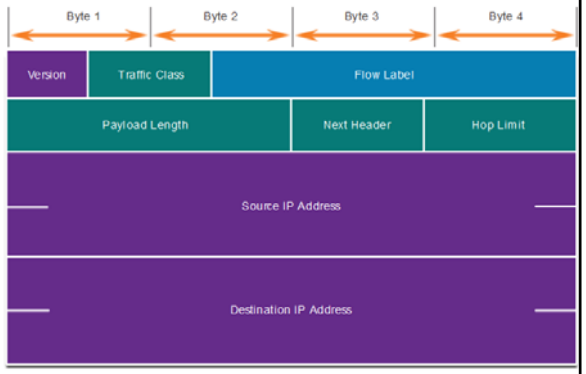
Legend
There are 4 billion IPv4 addresses
There are 340 undecillion IPv6 addresses

406

IPv6 Packets

IPv4 Packet Header Fields in the IPv6 Packet Header

- The IPv6 header is simplified, but not smaller.
- The header is fixed at 40 Bytes or octets long.
- Several IPv4 fields were removed to improve performance.
- Some IPv4 fields were removed to improve performance:
  - Flag
  - Fragment Offset
  - Header Checksum



407

IPv6 Packets

IPv6 Packet Header

Significant fields in the IPv6 header:

Function	Description
Version	This will be for v6, as opposed to v4, a 4 bit field= 0110
Traffic Class	Used for QoS: Equivalent to DiffServ – DS field
Flow Label	Informs device to handle identical flow labels the same way, 20 bit field
Payload Length	This 16-bit field indicates the length of the data portion or payload of the IPv6 packet
Next Header	I.D.s next level protocol: ICMP, TCP, UDP, etc.
Hop Limit	Replaces TTL field Layer 3 hop count
Source IPv6 Address	128 bit source address
Destination IPV6 Address	128 bit destination address

408

IPv6 Packets

IPv6 Packet Header (Cont.)

IPv6 packet may also contain extension headers (EH).

EH headers characteristics:

- provide optional network layer information
- are optional
- are placed between IPv6 header and the payload
- may be used for fragmentation, security, mobility support, etc.

Note: Unlike IPv4, routers do not fragment IPv6 packets.

409

IPv6 Packets

Video – Sample IPv6 Headers in Wireshark

This video will cover the following:

- IPv6 Ethernet packets in Wireshark
- The control information
- The difference between packets

410

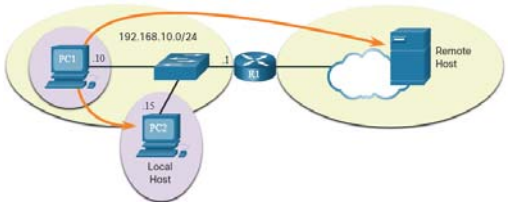
8.4 How a Host Routes

411

How a Host Routes

Host Forwarding Decision

- Packets are always created at the source.
- Each host devices creates their own routing table.
- A host can send packets to the following:
  - Itself – 127.0.0.1 (IPv4), ::1 (IPv6)
  - Local Hosts – destination is on the same LAN
  - Remote Hosts – devices are not on the same LAN

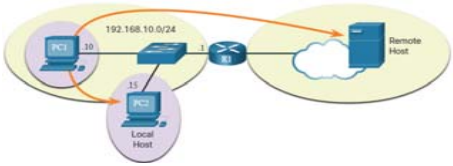


412

How a Host Routes

Host Forwarding Decision (Cont.)

- The Source device determines whether the destination is local or remote
- Method of determination:
  - IPv4 – Source uses its own IP address and Subnet mask, along with the destination IP address
  - IPv6 – Source uses the network address and prefix advertised by the local router
- Local traffic is dumped out the host interface to be handled by an intermediary device.
- Remote traffic is forwarded directly to the default gateway on the LAN.



413

How a Host Routes

Default Gateway

A router or layer 3 switch can be a default-gateway.

Features of a default gateway (DGW):

- It must have an IP address in the same range as the rest of the LAN.
- It can accept data from the LAN and is capable of forwarding traffic off of the LAN.
- It can route to other networks.

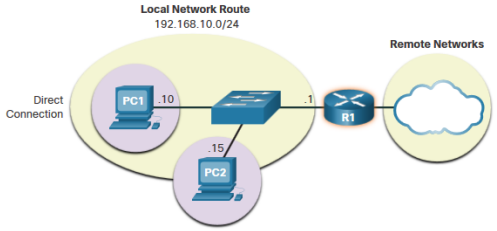
If a device has no default gateway or a bad default gateway, its traffic will not be able to leave the LAN.

414

How a Host Routes

A Host Routes to the Default Gateway

- The host will know the default gateway (DGW) either statically or through DHCP in IPv4.
- IPv6 sends the DGW through a router solicitation (RS) or can be configured manually.
- A DGW is static route which will be a last resort route in the routing table.
- All device on the LAN will need the DGW of the router if they intend to send traffic remotely.



415

How a Host Routes

Host Routing Tables

- On Windows, route print or netstat -r to display the PC routing table
- Three sections displayed by these two commands:
  - Interface List – all potential interfaces and MAC addressing
  - IPv4 Routing Table
  - IPv6 Routing Table

IPv4 Routing Table for PC1

```
C:\Users\PC1> netstat -r

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10      25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     306
      192.168.10.0    255.255.255.0         On-link    192.168.10.10     281
     192.168.10.10  255.255.255.255         On-link    192.168.10.10     281
    192.168.10.255  255.255.255.255         On-link    192.168.10.10     281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1     306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10     281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10     281
```


416

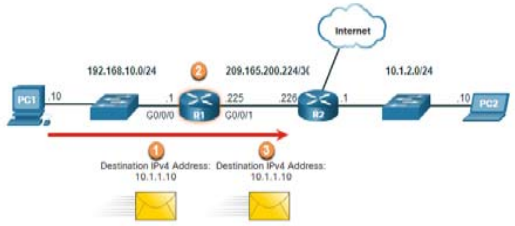
8.5 Introduction to Routing

417

Introduction to Routing

Router Packet Forwarding Decision

What happens when the router receives the frame from the host device?



1. Packet arrives on the Gigabit Ethernet 0/0/0 interface of router R1. R1 de-encapsulates the Layer 2 Ethernet header and trailer.
2. Router R1 examines the destination IPv4 address of the packet and searches for the best match in its IPv4 routing table. The route entry indicates that this packet is to be forwarded to router R2.
3. Router R1 encapsulates the packet into a new Ethernet header and trailer, and forwards the packet to the next hop router R2.

R1 Routing Table

Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	**via R2**
Default Route 0.0.0.0/0	via R2

418

Introduction to Routing

IP Router Routing Table

There three types of routes in a router's routing table:

- **Directly Connected** – These routes are automatically added by the router, provided the interface is active and has addressing.
- **Remote** – These are the routes the router does not have a direct connection and may be learned:
  - Manually – with a static route
  - Dynamically – by using a routing protocol to have the routers share their information with each other
- **Default Route** – this forwards all traffic to a specific direction when there is not a match in the routing table

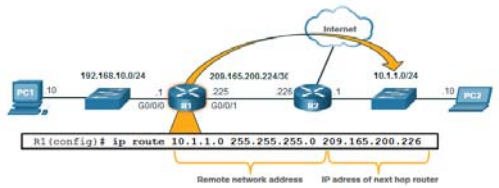
419

Introduction to Routing

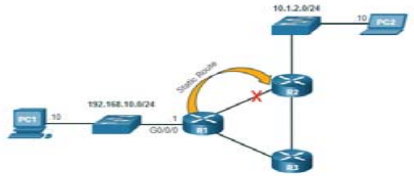
Static Routing

Static Route Characteristics:

- Must be configured manually
- Must be adjusted manually by the administrator when there is a change in the topology
- Good for small non-redundant networks
- Often used in conjunction with a dynamic routing protocol for configuring a default route



R1 is manually configured with a static route to reach the 10.1.1.0/24 network. If this path changes, R1 will require a new static route.



If the route from R1 via R2 is no longer available, a new static route via R3 would need to be configured. A static route does not automatically adjust for topology changes.

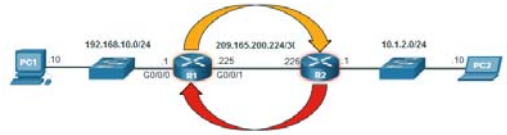
Introduction to Routing

Dynamic Routing

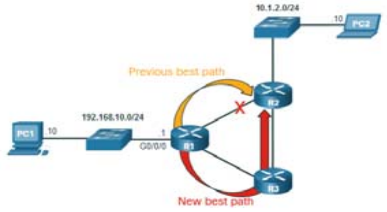
Dynamic Routes Automatically:

- Discover remote networks
- Maintain up-to-date information
- Choose the best path to the destination
- Find new best paths when there is a topology change

Dynamic routing can also share static default routes with the other routers.



- R1 is using the routing protocol OSPF to let R2 know about the 192.168.10.0/24 network.
- R2 is using the routing protocol OSPF to let R1 know about the 10.1.1.0/24 network.



R1, R2, and R3 are using the dynamic routing protocol OSPF. If there is a network topology change, they can automatically adjust to find a new best path.

Introduction to Routing

Video – IPv4 Router Routing Tables

This video will explain the information in the IPv4 router routing table.

Introduction to Routing

Introduction to an IPv4 Routing Table

The **show ip route** command shows the following route sources:

- **L** - Directly connected local interface IP address
- **C** – Directly connected network
- **S** – Static route was manually configured by an administrator
- **O** – OSPF
- **D** – EIGRP

This command shows types of routes:

- Directly Connected – C and L
- Remote Routes – O, D, etc.
- Default Routes – S*


```
R1# show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```


8.6 Module Practice and Quiz

424

Module Practice and Quiz

What did I learn in this module?

- IP is connectionless, best effort, and media independent.
- IP does not guarantee packet delivery.
- IPv4 packet header consists of fields containing information about the packet.
- IPv6 overcomes IPv4 lack of end-to-end connectivity and increased network complexity.
- A device will determine if a destination is itself, another local host, and a remote host.
- A default gateway is router that is part of the LAN and will be used as a door to other networks.
- The routing table contains a list of all known network addresses (prefixes) and where to forward the packet.
- The router uses longest subnet mask or prefix match.
- The routing table has three types of route entries: directly connected networks, remote networks, and a default route.

425

Network Layer

New Terms and Commands

- Encapsulation
- Routing
- De-encapsulation
- Data payload
- Packet
- Internet Protocol Version 4 (IPv4)
- Internet Protocol Version 6 (IPv6)
- Network Layer PDU = IP Packet
- IP Header

- Best effort delivery
- Media independent
- Connectionless
- Unreliable
- Maximum Transmission Unit (MTU)
- Version
- Differentiated Services (DS)
- Time-to-Live (TTL)
- Internet Control Message Protocol (ICMP)

- Identification, Flags, Fragment Offset fields
- Network Address Translation (NAT)
- Traffic Class
- Flow Label
- Payload Length
- Next Header
- Hop Limit
- Extension Headers
- Local host
- Remote host
- Default Gateway

426

Network Layer

New Terms and Commands

- netstat –r
- route print
- interface list
- IPv4 Route Table
- IPv6 Route Table
- directly-connected routes
- remote routes
- default route
- **show ip route**
- route source
- destination network
- outgoing interface
- administrative distance
- metric

- next-hop
- route timestamp

427

428

What to Expect in this Module

- To facilitate learning, the following features within the GUI may be included in this module:

Feature	Description
Animations	Expose learners to new skills and concepts.
Videos	Expose learners to new skills and concepts.
Check Your Understanding(CYU)	Per topic online quiz to help learners gauge content understanding.
Interactive Activities	A variety of formats to help learners gauge content understanding.
Syntax Checker	Small simulations that expose learners to Cisco command line to practice configuration skills.
PT Activity	Simulation and modeling activities designed to explore, acquire, reinforce, and expand skills.

430

What to Expect in this Module (Cont.)

- To facilitate learning, the following features may be included in this module:

Feature	Description
Hands-On Labs	Labs designed for working with physical equipment.
Class Activities	These are found on the Instructor Resources page. Class Activities are designed to facilitate learning, class discussion, and collaboration.
Module Quizzes	Self-assessments that integrate concepts and skills learned throughout the series of topics presented in the module.
Module Summary	Briefly recaps module content.

431

436

Module Objectives

Module Title: Address Resolution

Module Objective: Explain how ARP and ND enable communication on a network.

Topic Title	Topic Objective
MAC and IP	Compare the roles of the MAC address and the IP address.
ARP	Describe the purpose of ARP.
Neighbor Discovery	Describe the operation of IPv6 neighbor discovery.

437

9.1 MAC and IP

438

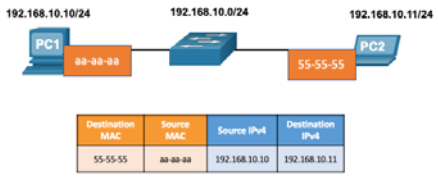
MAC and IP

Destination on Same Network

There are two primary addresses assigned to a device on an Ethernet LAN:

- **Layer 2 physical address (the MAC address)** – Used for NIC to NIC communications on the same Ethernet network.
- **Layer 3 logical address (the IP address)** – Used to send the packet from the source device to the destination device.

Layer 2 addresses are used to deliver frames from one NIC to another NIC on the same network. If a destination IP address is on the same network, the destination MAC address will be that of the destination device.



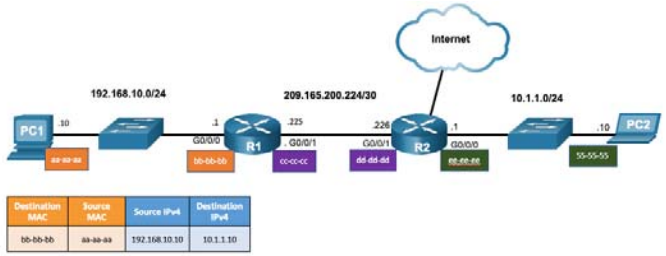
439

MAC and IP

Destination on Remote Network

When the destination IP address is on a remote network, the destination MAC address is that of the default gateway.

- ARP is used by IPv4 to associate the IPv4 address of a device with the MAC address of the device NIC.
- ICMPv6 is used by IPv6 to associate the IPv6 address of a device with the MAC address of the device NIC.



440

MAC and IP
Packet Tracer – Identify MAC and IP Addresses

In this Packet Tracer, you will complete the following objectives:

- Gather PDU Information for Local Network Communication
- Gather PDU Information for Remote Network Communication

441

9.2 ARP

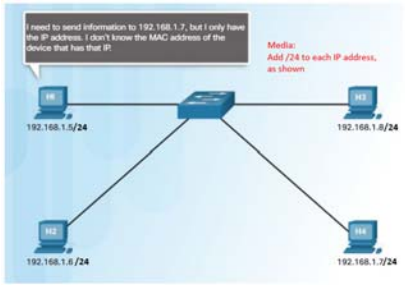
442

ARP
ARP Overview

A device uses ARP to determine the destination MAC address of a local device when it knows its IPv4 address.

ARP provides two basic functions:

- Resolving IPv4 addresses to MAC addresses
- Maintaining an ARP table of IPv4 to MAC address mappings



443

ARP
ARP Functions

To send a frame, a device will search its ARP table for a destination IPv4 address and a corresponding MAC address.

- If the packet's destination IPv4 address is on the same network, the device will search the ARP table for the destination IPv4 address.
- If the destination IPv4 address is on a different network, the device will search the ARP table for the IPv4 address of the default gateway.
- If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame.
- If there is no ARP table entry is found, then the device sends an ARP request.

444

ARP
Video - ARP Request

This video will cover an ARP request for a MAC address.

445

ARP
Video – ARP Operation - ARP Reply

This video will cover an ARP reply in response to an ARP request.

446

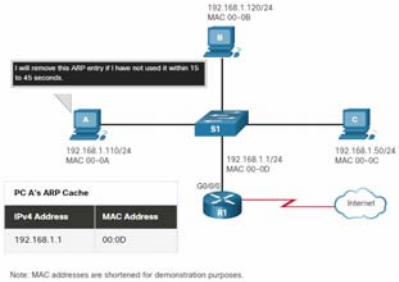
ARP
Video - ARP Role in Remote Communications

This video will cover how an ARP request will provide a host the MAC address of the default gateway.

447

ARP
Removing Entries from an ARP Table

- Entries in the ARP table are not permanent and are removed when an ARP cache timer expires after a specified period of time.
- The duration of the ARP cache timer differs depending on the operating system.
- ARP table entries can also be removed manually by the administrator.



448

ARP
ARP Tables on Networking Devices

- The **show ip arp** command displays the ARP table on a Cisco router.
- The **arp –a** command displays the ARP table on a Windows 10 PC.

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1           -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
```

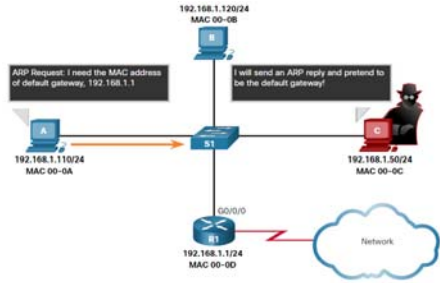
```
C:\Users\PC> arp -a

Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
```


449

ARP
ARP Issues – ARP Broadcasting and ARP Spoofing

- ARP requests are received and processed by every device on the local network.
- Excessive ARP broadcasts can cause some reduction in performance.
- ARP replies can be spoofed by a threat actor to perform an ARP poisoning attack.
- Enterprise level switches include mitigation techniques to protect against ARP attacks.



Note: MAC addresses are shortened for demonstration purposes.

450

ARP
Packet Tracer – Examine the ARP Table

In this Packet Tracer, you will complete the following objectives:

- Examine an ARP Request
- Examine a Switch MAC Address Table
- Examine the ARP Process in Remote Communications

451

9.3 IPv6 Neighbor Discovery

452

IPv6 Neighbor Discovery

Video – IPv6 Neighbor Discovery

This video will explain the process of how IPv6 performs address resolution using ICMPv6 neighbor solicitation and neighbor advertisement messages.

453

IPv6 Neighbor Discovery

IPv6 Neighbor Discovery Messages

IPv6 Neighbor Discovery (ND) protocol provides:

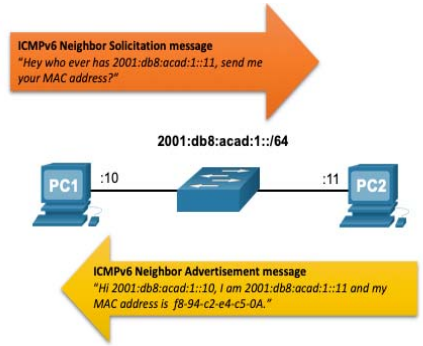
- Address resolution
- Router discovery
- Redirection services

- ICMPv6 Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages are used for device-to-device messaging such as address resolution.
- ICMTPv6 Router Solicitation (RS) and Router Advertisement (RA) messages are used for messaging between devices and routers for router discovery.
- ICMPv6 redirect messages are used by routers for better next-hop selection.

454

IPv6 Neighbor Discovery

IPv6 Neighbor Discovery – Address Resolution



- IPv6 devices use ND to resolve the MAC address of a known IPv6 address.
- ICMPv6 Neighbor Solicitation messages are sent using special Ethernet and IPv6 multicast addresses.

455

IPv6 Neighbor Discovery

Packet Tracer – IPv6 Neighbor Discovery

In this Packet Tracer, you will complete the following objectives:

- Part 1: IPv6 Neighbor Discovery Local Network
- Part 2: IPv6 Neighbor discovery Remote Network

456

9.4 Module Practice and Quiz

457

Module Practice and Quiz

What did I learn in this module?

- Layer 2 physical addresses (i.e., Ethernet MAC addresses) are used to deliver the data link frame with the encapsulated IP packet from one NIC to another NIC on the same network.
- If the destination IP address is on the same network, the destination MAC address will be that of the destination device.
- When the destination IP address (IPv4 or IPv6) is on a remote network, the destination MAC address will be the address of the host default gateway (i.e., the router interface).
- An IPv4 device uses ARP to determine the destination MAC address of a local device when it knows its IPv4 address.
- ARP provides two basic functions: resolving IPv4 addresses to MAC addresses and maintaining a table of IPv4 to MAC address mappings.
- After the ARP reply is received, the device will add the IPv4 address and the corresponding MAC address to its ARP table.
- For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time.
- IPv6 does not use ARP, it uses the ND protocol to resolve MAC addresses.
- An IPv6 device uses ICMPv6 Neighbor Discovery to determine the destination MAC address of a local device when it knows its IPv6 address.

458

Module 9: Address Resolution

New Terms and Commands

- Address Resolution Protocol (ARP)
- ARP table
- show ip arp
- arpr -a
- ICMPv6 Neighbor Discovery protocol (ND)
- ICMPv6 Neighbor Solicitation (NS) message
- ICMPv6 Neighbor Advertisement (NA) message
- ICMPv6 Router Solicitation (RS) message
- ICMPv6 Router Advertisement (RA) message
- ICMPv6 Redirect Message

459

Module 10: Basic Router Configuration

Instructor Materials

Introduction to Networks v7.0 (ITN)

460

Module 10: Basic Router Configuration

Introduction to Networks v7.0 (ITN)

469

Module Objectives

Module Title: Basic Router Configuration

Module Objective: Implement initial settings on a router and end devices.

Topic Title	Topic Objective
Configure Initial Router Settings	Configure initial settings on an IOS Cisco router.
Configure Interfaces	Configure two active interfaces on a Cisco IOS router.
Configure the Default Gateway	Configure devices to use the default gateway.

470

10.1 Configure Initial Router Settings

471

Configure Initial Router Settings
Basic Router Configuration Steps

- Configure the device name.
- Secure privileged EXEC mode.
- Secure user EXEC mode.
- Secure remote Telnet / SSH access.
- Encrypt all plaintext passwords.
- Provide legal notification and save the configuration.

```
Router(config)# hostname hostname
```

```
Router(config)# enable secret password
```

```
Router(config)# line console 0
Router(config-line)# password password
Router(config-line)# login
```

```
Router(config)# line vty 0 4
Router(config-line)# password password
Router(config-line)# login
Router(config-line)# transport input {ssh | telnet}
```

```
Router(config)# service password encryption
```

```
Router(config)# banner motd # message #
Router(config)# end
Router# copy running-config startup-config
```


472

Configure Initial Router Settings

Basic Router Configuration Example

- Commands for basic router configuration on R1.
- Configuration is saved to NVRAM.

```
R1(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)# service password encryption
R1(config)# banner motd #
Enter TEXT message. End with a new line and the #
*****************************************
WARNING: Unauthorized access is prohibited!
*****************************************
R1(config)# exit
R1# copy running-config startup-config
```


Configure Initial Router Settings

Packet Tracer – Configure Initial Router Settings

In this Packet Tracer, you will do the following:

- Verify the default router configuration.
- Configure and verify the initial router configuration.
- Save the running configuration file.

10.2 Configure Interfaces

Configure Interfaces

Configure Router Interfaces

Configuring a router interface includes issuing the following commands:

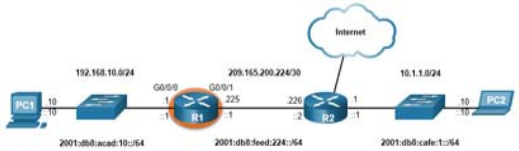
```
Router(config)# interface type-and-number
Router(config-if)# description description-text
Router(config-if)# ip address ipv4-address subnet-mask
Router(config-if)# ipv6 address ipv6-address/prefix-length
Router(config-if)# no shutdown
```

- It is a good practice to use the **description** command to add information about the network connected to the interface.
- The **no shutdown** command activates the interface.

Configure Interfaces

Configure Router Interfaces Example

The commands to configure interface G0/0/0 on R1 are shown here:

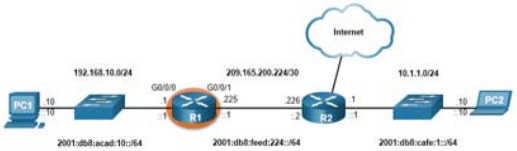



```
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# description Link to LAN
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:10::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug  1 01:43:53.435: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Aug  1 01:43:56.447: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Aug  1 01:43:57.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
```


Configure Interfaces

Configure Router Interfaces Example (Cont.)

The commands to configure interface G0/0/1 on R1 are shown here:




```
R1(config)# interface gigabitEthernet 0/0/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:feed:224::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug  1 01:46:29.170: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down
*Aug  1 01:46:32.171: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up
*Aug  1 01:46:33.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
```


Configure Interfaces

Verify Interface Configuration

To verify interface configuration use the **show ip interface brief** and **show ipv6 interface brief** commands shown here:

```
R1#  show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   209.165.200.225 YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

```
R1#  show ipv6 interface brief
GigabitEthernet0/0/0       [up/up]
    FE80::201:C9FF:FE89:4501
    2001:DB8:ACAD:10::1
GigabitEthernet0/0/1       [up/up]
    FE80::201:C9FF:FE89:4502
    2001:DB8:FEED:224::1
Vlan1                      [administratively down/down]
    unassigned
R1#
```


Configure Interfaces

Configure Verification Commands

The table summarizes show commands used to verify interface configuration.

Commands	Description
`show ip interface brief` `show ipv6 interface brief`	Displays all interfaces, their IP addresses, and their current status.
`show ip route` `show ipv6 route`	Displays the contents of the IP routing tables stored in RAM.
`show interfaces`	Displays statistics for all interfaces on the device. Only displays the IPv4 addressing information.
`show ip interfaces`	Displays the IPv4 statistics for all interfaces on a router.
`show ipv6 interfaces`	Displays the IPv6 statistics for all interfaces on a router.

Configure Interfaces

Configure Verification Commands (Cont.)

View status of all interfaces with the **show ip interface brief** and **show ipv6 interface brief** commands, shown here:

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   209.165.200.225 YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

```
R1# show ipv6 interface brief
GigabitEthernet0/0/0       [up/up]
    FE80::201:C9FF:FE89:4501
    2001:DB8:ACAD:10::1
GigabitEthernet0/0/1       [up/up]
    FE80::201:C9FF:FE89:4502
    2001:DB8:FEED:224::1
Vlan1                      [administratively down/down]
    unassigned
R1#
```


481

Configure Interfaces

Configure Verification Commands (Cont.)

Display the contents of the IP routing tables with the **show ip route** and **show ipv6 route** commands as shown here:

```
R1# show ip route
< output omitted>
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

```
R1# show ipv6 route
<output omitted>
C   2001:DB8:ACAD:10::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:10::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:FEED:224::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:FEED:224::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```


482

Configure Interfaces

Configure Verification Commands (Cont.)

Display statistics for all interfaces with the **show interfaces** command, as shown here:

```
R1# show interfaces gig0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4321-2x1GE, address is a0e0.af0d.e140 (bia  a0e0.af0d.e140)
  Description: Link to LAN
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 100Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:35, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (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
     1180 packets input, 109486 bytes, 0 no buffer
     Received 84 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles

<output omitted>

R1#
```


483

Configure Interfaces

Configure Verification Commands (Cont.)

Display IPv4 statistics for router interfaces with the **show ip interface** command, as shown here:

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  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 Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP Flow switching is disabled

<output omitted>

R1#
```

484

Configure Interfaces
Configure Verification Commands (Cont.)

Display IPv6 statistics for router interfaces with the **show ipv6 interface** command shown here:

```
R1# show ipv6 interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::868A:8DFF:FE44:49B0
  No Virtual link-local address(es):
  Description: Link to LAN
  Global unicast address(es):
    2001:DB8:ACAD:10::1, subnet is 2001:DB8:ACAD:10::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FF44:49B0
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds

R1#
```

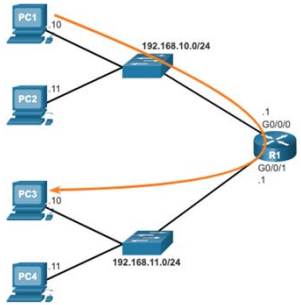

485

10.3 Configure the Default Gateway

486

Configure the Default Gateway
Default Gateway on a Host

- The default gateway is used when a host sends a packet to a device on another network.
- The default gateway address is generally the router interface address attached to the local network of the host.
- To reach PC3, PC1 addresses a packet with the IPv4 address of PC3, but forwards the packet to its default gateway, the G0/0/0 interface of R1.



Note: The IP address of the host and the router interface must be in the same network.

487

Configure the Default Gateway
Default Gateway on a Switch

- A switch must have a default gateway address configured to remotely manage the switch from another network.
- To configure an IPv4 default gateway on a switch, use the **ip default-gateway** *ip-address* global configuration command.

488

Configure Initial Router Settings

Packet Tracer – Connect a Router to a LAN

In this Packet Tracer, you will do the following:

- Display the router information.
- Configure router interfaces.
- Verify the configuration.

Configure Initial Router Settings

Packet Tracer – Troubleshoot Default Gateway Issues

In this Packet Tracer, you will do the following:

- Verify the network documentation and use tests to isolate problems.
- Determine an appropriate solution for a given problem.
- Implement the solution.
- Test to verify the problem is resolved.
- Document the solution.

10.4 Module Practice and Quiz

Module Practice and Quiz

Video – Network Device Differences: Part 1

This video will cover the different physical characteristics of the following:

- Cisco 4000 Series Router.
- Cisco 2900 Series Router.
- Cisco 1900 Series Router.

Module Practice and Quiz

Video – Network Device Differences: Part 2

This video will cover the different configurations of the following:

- Cisco 4000 Series Router.
- Cisco 2900 Series Router.
- Cisco 1900 Series Router.

 493

493

Configure Initial Router Settings

Packet Tracer – Basic Device Configuration

In this Packet Tracer, you will do the following:

- Complete the network documentation.
- Perform basic device configurations on a router and a switch.
- Verify connectivity and troubleshoot any issues.

 494

494

Configure Initial Router Settings

Packet Tracer – Build a Switch and Router Network – Physical Mode
Lab – Build a Switch and Router Network

In both the Packet Tracer Physical Mode activity and in the Lab, you will complete the following objectives:

- Set up the topology and initialize devices.
- Configure devices and verify connectivity.
- Display device information.

 495

495

Module Practice and Quiz

What did I learn in this module?

- The tasks that should be completed when configuring initial settings on a router.
  - Configure the device name.
  - Secure privileged EXEC mode.
  - Secure user EXEC mode.
  - Secure remote Telnet / SSH access.
  - Secure all passwords in the config file.
  - Provide legal notification.
  - Save the configuration.
- For routers to be reachable, the router interfaces must be configured.
  - Using the **no shutdown** command activates the interface. The interface must also be connected to another device, such as a switch or a router, for the physical layer to be active. There are several commands that can be used to verify interface configuration including the **show ip interface brief** and **show ipv6 interface brief**, the **show ip route** and **show ipv6 route**, as well as **show interfaces**, **show ip interface** and **show ipv6 interface.**

 496

496

Module Practice and Quiz

What did I learn in this module (Cont.)?

- For an end device to reach other networks, a default gateway must be configured.
  - The IP address of the host device and the router interface address must be in the same network.
- A switch must have a default gateway address configured to remotely manage the switch from another network.
  - To configure an IPv4 default gateway on a switch, use the **ip default-gateway** *ip-address* global configuration command.

497

Module 10: Basic Router Configuration

New Terms and Commands

- **show ip interface brief**
- **show ipv6 interface brief**
- **show ip route**
- **show ipv6 route**
- **show interfaces**
- **show ip interface**
- **show ipv6 interface**
- **ip default-gateway**

498

Module 11: IPv4 Addressing

Instructor Materials

Introduction to Networks v7.0
(ITN)

499

Module 11: IPv4 Addressing

Introduction to Networks v7.0
(ITN)

513

Module Objectives

Module Title: IPv4 Addressing

Module Objective: Calculate an IPv4 subnetting scheme to efficiently segment your network.

Topic Title	Topic Objective
IPv4 Address Structure	Describe the structure of an IPv4 address including the network portion, the host portion, and the subnet mask.
IPv4 Unicast, Broadcast, and Multicast	Compare the characteristics and uses of the unicast, broadcast and multicast IPv4 addresses.
Types of IPv4 Addresses	Explain public, private, and reserved IPv4 addresses.
Network Segmentation	Explain how subnetting segments a network to enable better communication.
Subnet an IPv4 Network	Calculate IPv4 subnets for a /24 prefix.

514

Module Objectives (Cont.)

Module Title: IPv4 Addressing

Module Objective: Calculate an IPv4 subnetting scheme to efficiently segment your network.

Topic Title	Topic Objective
Subnetting a /16 and a /8 Prefix	Calculate IPv4 subnets for a /16 and a /8 prefix.
Subnetting to Meet Requirements	Given a set of requirements for subnetting, implement an IPv4 addressing scheme.
Variable Length Subnet Masking (VLSM)	Explain how to create a flexible addressing scheme using variable length subnet masking (VLSM).
Structured Design	Implement a VLSM addressing scheme.

515

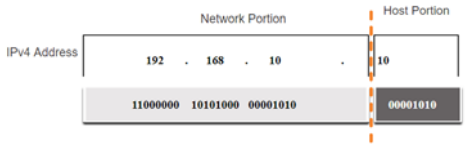
11.1 IPv4 Address Structure

516

IPv4 Address Structure

Network and Host Portions

- An IPv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion.
- When determining the network portion versus the host portion, you must look at the 32-bit stream.
- A subnet mask is used to determine the network and host portions.

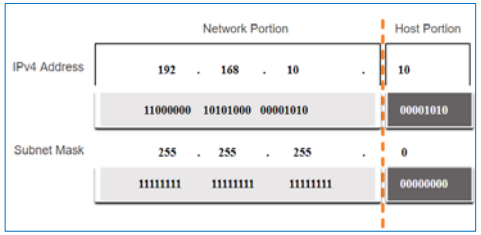


517

IPv4 Address Structure

The Subnet Mask

- To identify the network and host portions of an IPv4 address, the subnet mask is compared to the IPv4 address bit for bit, from left to right.
- The actual process used to identify the network and host portions is called ANDing.



518

IPv4 Address Structure

The Prefix Length

- A prefix length is a less cumbersome method used to identify a subnet mask address.
- The prefix length is the number of bits set to 1 in the subnet mask.
- It is written in “slash notation” therefore, count the number of bits in the subnet mask and prepend it with a slash.

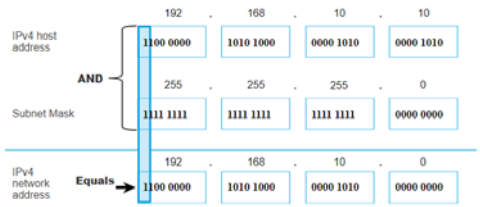
Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

519

IPv4 Address Structure

Determining the Network: Logical AND

- A logical AND Boolean operation is used in determining the network address.
  - Logical AND is the comparison of two bits where only a 1 AND 1 produces a 1 and any other combination results in a 0.
  - 1 AND 1 = 1, 0 AND 1 = 0, 1 AND 0 = 0, 0 AND 0 = 0
  - 1 = True and 0 = False
- To identify the network address, the host IPv4 address is logically ANDed, bit by bit, with the subnet mask to identify the network address.



520

IPv4 Address Structure

Video – Network, Host and Broadcast Addresses

This video will cover the following:

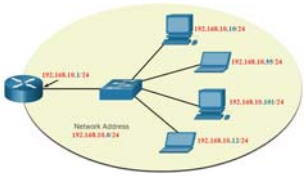
- Network address
- Broadcast Address
- First usable host
- Last usable host

521

IPv4 Address Structure

Network, Host, and Broadcast Addresses

- Within each network are three types of IP addresses:
  - Network address
  - Host addresses
  - Broadcast address



	Network Portion			Host Portion	Host Bits
Subnet mask **255.255.255.**0 or **/24**	255 11111111	255 11111111	255 11111111	0 00000000	
Network address **192.168.10.**0 or **/24**	192 11000000	168 10100000	10 00001010	0 00000000	All 0s
First address **192.168.10.**1 or **/24**	192 11000000	168 10100000	10 00001010	1 00000001	All 0s and a 1
Last address **192.168.10.**254 or **/24**	192 11000000	168 10100000	10 00001010	254 11111110	All 1s and a 0
Broadcast address **192.168.10.**255 or **/24**	192 11000000	168 10100000	10 00001010	255 11111111	All 1s

522

11.2 IPv4 Unicast, Broadcast, and Multicast

523

IPv4 Unicast, Broadcast, and Multicast

Unicast

- Unicast transmission is sending a packet to one destination IP address.
- For example, the PC at 172.16.4.1 sends a unicast packet to the printer at 172.16.4.253.

524

IPv4 Unicast, Broadcast, and Multicast

Broadcast

- Broadcast transmission is sending a packet to all other destination IP addresses.
- For example, the PC at 172.16.4.1 sends a broadcast packet to all IPv4 hosts.

525

IPv4 Unicast, Broadcast, and Multicast

Multicast

- Multicast transmission is sending a packet to a multicast address group.
- For example, the PC at 172.16.4.1 sends a multicast packet to the multicast group address 224.10.10.5.

 526

526

11.3 Types of IPv4 Addresses

 527

527

Types of IPv4 Addresses

Public and Private IPv4 Addresses

- As defined in in RFC 1918, public IPv4 addresses are globally routed between internet service provider (ISP) routers.
- Private addresses are common blocks of addresses used by most organizations to assign IPv4 addresses to internal hosts.
- Private IPv4 addresses are not unique and can be used internally within any network.
- However, private addresses are not globally routable.

Network Address and Prefix	RFC 1918 Private Address Range
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

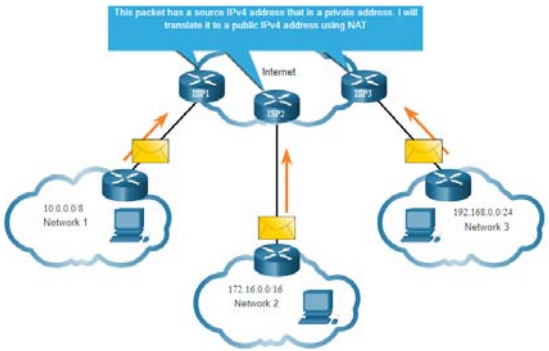
 528

528

Types of IPv4 Addresses

Routing to the Internet

- Network Address Translation (NAT) translates private IPv4 addresses to public IPv4 addresses.
- NAT is typically enabled on the edge router connecting to the internet.
- It translates the internal private address to a public global IP address.



529

Types of IPv4 Addresses

Special Use IPv4 Addresses

Loopback addresses

- 127.0.0.0 /8 (127.0.0.1 to 127.255.255.254)
- Commonly identified as only 127.0.0.1
- Used on a host to test if TCP/IP is operational.

```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

Link-Local addresses

- 169.254.0.0 /16 (169.254.0.1 to 169.254.255.254)
- Commonly known as the Automatic Private IP Addressing (APIPA) addresses or self-assigned addresses.
- Used by Windows DHCP clients to self-configure when no DHCP servers are available.

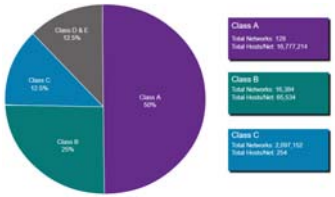
530

Types of IPv4 Addresses

Legacy Classful Addressing

RFC 790 (1981) allocated IPv4 addresses in classes

- Class A (0.0.0.0/8 to 127.0.0.0/8)
- Class B (128.0.0.0 /16 – 191.255.0.0 /16)
- Class C (192.0.0.0 /24 – 223.255.255.0 /24)
- Class D (224.0.0.0 to 239.0.0.0)
- Class E (240.0.0.0 – 255.0.0.0)



- Classful addressing wasted many IPv4 addresses.

Classful address allocation was replaced with classless addressing which ignores the rules of classes (A, B, C).

531

Types of IPv4 Addresses

Assignment of IP Addresses

- The Internet Assigned Numbers Authority (IANA) manages and allocates blocks of IPv4 and IPv6 addresses to five Regional Internet Registries (RIRs).
- RIRs are responsible for allocating IP addresses to ISPs who provide IPv4 address blocks to smaller ISPs and organizations.

532

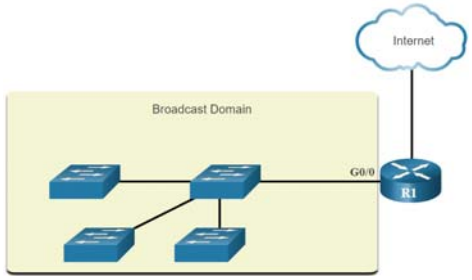
11.4 Network Segmentation

533

Network Segmentation

Broadcast Domains and Segmentation

- Many protocols use broadcasts or multicasts (e.g., ARP use broadcasts to locate other devices, hosts send DHCP discover broadcasts to locate a DHCP server.)
- Switches propagate broadcasts out all interfaces except the interface on which it was received.



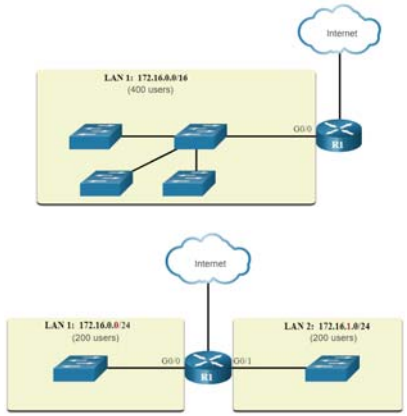
- The only device that stops broadcasts is a router.
- Routers do not propagate broadcasts.
- Each router interface connects to a broadcast domain and broadcasts are only propagated within that specific broadcast domain.

534

Network Segmentation

Problems with Large Broadcast Domains

- A problem with a large broadcast domain is that these hosts can generate excessive broadcasts and negatively affect the network.
- The solution is to reduce the size of the network to create smaller broadcast domains in a process called subnetting.
- Dividing the network address 172.16.0.0 /16 into two subnets of 200 users each: 172.16.0.0 /24 and 172.16.1.0 /24.
- Broadcasts are only propagated within the smaller broadcast domains.



535

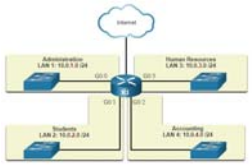
Network Segmentation

Reasons for Segmenting Networks

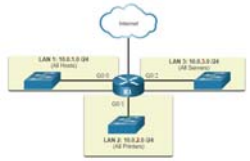
- Subnetting reduces overall network traffic and improves network performance.
- It can be used to implement security policies between subnets.
- Subnetting reduces the number of devices affected by abnormal broadcast traffic.
- Subnets are used for a variety of reasons including by:

Location

Group or Function



Device Type



536

11.5 Subnet an IPv4 Network

537

Subnet an IPv4 Network

Subnet on an Octet Boundary

- Networks are most easily subnetted at the octet boundary of /8, /16, and /24.
- Notice that using longer prefix lengths decreases the number of hosts per subnet.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	**255**.0.0.0	**nnnnnnnn**.hhhhhhhh.hhhhhhhh.hhhhhhhh **11111111**.00000000.00000000.00000000	16,777,214
/16	**255.255**.0.0	**nnnnnnnn.nnnnnnnn**.hhhhhhhh.hhhhhhhh **11111111.11111111**.00000000.00000000	65,534
/24	**255.255.255**.0	**nnnnnnnn.nnnnnnnn.nnnnnnnn**.hhhhhhhh **11111111.11111111.11111111**.00000000	254

538

Subnet an IPv4 Network

Subnet on an Octet Boundary (Cont.)

- In the first table 10.0.0.0/8 is subnetted using /16 and in the second table, a /24 mask.

Subnet Address (256 Possible Subnets)	Host Range (65,534 possible hosts per subnet)	Broadcast
10.0.0.0/**16**	**10.0**.0.1 - **10.0**.255.254	**10.0**.255.255
10.1.0.0/**16**	**10.1**.0.1 - **10.1**.255.254	**10.1**.255.255
10.2.0.0/**16**	**10.2**.0.1 - **10.2**.255.254	**10.2**.255.255
10.3.0.0/**16**	**10.3**.0.1 - **10.3**.255.254	**10.3**.255.255
10.4.0.0/**16**	**10.4**.0.1 - **10.4**.255.254	**10.4**.255.255
10.5.0.0/**16**	**10.5**.0.1 - **10.5**.255.254	**10.5**.255.255
10.6.0.0/**16**	**10.6**.0.1 - **10.6**.255.254	**10.6**.255.255
10.7.0.0/**16**	**10.7**.0.1 - **10.7**.255.254	**10.7**.255.255
...	...	...
10.255.0.0/**16**	**10.255**.0.1 - **10.255**.255.254	**10.255**.255.255

Subnet Address (65,536 Possible Subnets)	Host Range (254 possible hosts per subnet)	Broadcast
10.0.0.0/**24**	**10.0.0**.1 - **10.0.0**.254	**10.0.0**.255
10.0.1.0/**24**	**10.0.1**.1 - **10.0.1**.254	**10.0.1**.255
10.0.2.0/**24**	**10.0.2**.1 - **10.0.2**.254	**10.0.2**.255
…	…	…
10.0.255.0/**24**	**10.0.255**.1 - **10.0.255**.254	**10.0.255**.255
10.1.0.0/**24**	**10.1.0**.1 - **10.1.0**.254	**10.1.0**.255
10.1.1.0/**24**	**10.1.1**.1 - **10.1.1**.254	**10.1.1**.255
10.1.2.0/**24**	**10.1.2**.1 - **10.1.2**.254	**10.1.2**.255
…	…	…
10.100.0.0/**24**	**10.100.0**.1 - **10.100.0**.254	**10.100.0**.255
...	...	...
10.255.255.0/**24**	**10.255.255**.1 - **10.2255.255**.254	**10.255.255**.255

539

Subnet an IPv4 Network

Subnet within an Octet Boundary

- Refer to the table to see six ways to subnet a /24 network.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

540

Subnet an IPv4 Network

Video – The Subnet Mask

- This video will demonstrate the process of subnetting.

541

Subnet an IPv4 Network

Video – Subnet with the Magic Number

- This video will demonstrate subnetting with the magic number.

542

Subnet an IPv4 Network

Packet Tracer – Subnet an IPv4 Network

In this Packet Tracer, you will do the following:

- Design an IPv4 Network Subnetting Scheme
- Configure the Devices
- Test and Troubleshoot the Network

543

11.6 Subnet a Slash 16 and a Slash 8 Prefix

544

Subnet a Slash 16 and a Slash 8 Prefix

Create Subnets with a Slash 16 prefix

- The table highlights all the possible scenarios for subnetting a /16 prefix.

Prefix Length	Subnet Mask	Network Address (n = network, h = host)	# of subnets	# of hosts
/17	255.255.**128**.0	nnnnnnnn.nnnnnnnn.**n**hhhhhhh.hhhhhhhh 11111111.11111111.**1**0000000.00000000	**2**	32766
/18	255.255.**192**.0	nnnnnnnn.nnnnnnnn.**nn**hhhhhh.hhhhhhhh 11111111.11111111.**11**000000.00000000	**4**	16382
/19	255.255.**224**.0	nnnnnnnn.nnnnnnnn.**nnn**hhhhh.hhhhhhhh 11111111.11111111.**111**00000.00000000	**8**	8190
/20	255.255.**240**.0	nnnnnnnn.nnnnnnnn.**nnnn**hhhh.hhhhhhhh 11111111.11111111.**1111**0000.00000000	**16**	4094
/21	255.255.**248**.0	nnnnnnnn.nnnnnnnn.**nnnnn**hhh.hhhhhhhh 11111111.11111111.**11111**000.00000000	**32**	2046
/22	255.255.**252**.0	nnnnnnnn.nnnnnnnn.**nnnnnn**hh.hhhhhhhh 11111111.11111111.**111111**00.00000000	**64**	1022
/23	255.255.**254**.0	nnnnnnnn.nnnnnnnn.**nnnnnnn**h.hhhhhhhh 11111111.11111111.**1111111**0.00000000	**128**	510
/24	255.255.**255**.0	nnnnnnnn.nnnnnnnn.**nnnnnnnn**.hhhhhhhh 11111111.11111111.**11111111**.00000000	**256**	254
/25	255.255.**255**.**128**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.n**hhhhhhh 11111111.11111111.**11111111.1**0000000	**512**	126
/26	255.255.**255**.**192**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nn**hhhhhh 11111111.11111111.**11111111.11**000000	**1024**	62
/27	255.255.**255**.**224**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnn**hhhhh 11111111.11111111.**11111111.111**00000	**2048**	30
/28	255.255.**255**.**240**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnn**hhhh 11111111.11111111.**11111111.1111**0000	**4096**	14
/29	255.255.**255**.**248**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnnn**hhh 11111111.11111111.**11111111.11111**000	**8192**	6
/30	255.255.**255**.**252**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnnnn**hh 11111111.11111111.**11111111.111111**00	**16384**	2

545

Subnet a Slash 16 and a Slash 8 Prefix

Create 100 Subnets with a Slash 16 prefix

Consider a large enterprise that requires at least 100 subnets and has chosen the private address 172.16.0.0/16 as its internal network address.

- The figure displays the number of subnets that can be created when borrowing bits from the third octet and the fourth octet.
- Notice there are now up to 14 host bits that can be borrowed (i.e., last two bits cannot be borrowed).

To satisfy the requirement of 100 subnets for the enterprise, 7 bits (i.e., 2^7 = 128 subnets) would need to be borrowed (for a total of 128 subnets).

 546

546

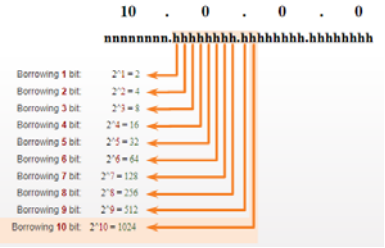
Subnet a Slash 16 and a Slash 8 Prefix

Create 1000 Subnets with a Slash 8 prefix

Consider a small ISP that requires 1000 subnets for its clients using network address 10.0.0.0/8 which means there are 8 bits in the network portion and 24 host bits available to borrow toward subnetting.

- The figure displays the number of subnets that can be created when borrowing bits from the second and third.
- Notice there are now up to 22 host bits that can be borrowed (i.e., last two bits cannot be borrowed).

To satisfy the requirement of 1000 subnets for the enterprise, 10 bits (i.e., 2^{10}=1024 subnets) would need to be borrowed (for a total of 128 subnets)



 547

547

Subnet a Slash 16 and a Slash 8 Prefix

Video – Subnet Across Multiple Octets

This video will demonstrate creating subnets across multiple octets.

 548

548

Subnet a Slash 16 and a Slash 8 Prefix

Lab – Calculate IPv4 Subnets

In this lab, you will complete the following objectives:

- Part 1: Determine IPv4 Address Subnetting
- Part 2: Calculate IPv4 Address Subnetting

 549

549

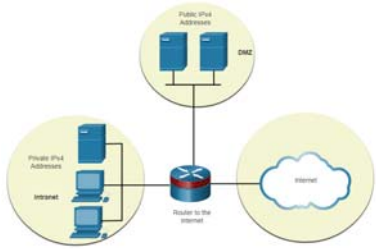
11.7 Subnet to Meet Requirements

550

Subnet to Meet Requirements
Subnet Private versus Public IPv4 Address Space

Enterprise networks will have an:

- Intranet - A company's internal network typically using private IPv4 addresses.
- DMZ – A companies internet facing servers. Devices in the DMZ use public IPv4 addresses.
- A company could use the 10.0.0.0/8 and subnet on the /16 or /24 network boundary.
- The DMZ devices would have to be configured with public IP addresses.



551

Subnet to Meet Requirements
Minimize Unused Host IPv4 Addresses and Maximize Subnets

There are two considerations when planning subnets:

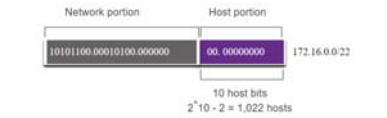
- The number of host addresses required for each network
- The number of individual subnets needed

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

552

Subnet to Meet Requirements
Example: Efficient IPv4 Subnetting

- In this example, corporate headquarters has been allocated a public network address of 172.16.0.0/22 (10 host bits) by its ISP providing 1,022 host addresses.
- There are five sites and therefore five internet connections which means the organization requires 10 subnets with the largest subnet requires 40 addresses.
- It allocated 10 subnets with a /26 (i.e., 255.255.255.192) subnet mask.



553

Subnet to Meet Requirements

Packet Tracer – Subnetting Scenario

In this Packet Tracer, you will do the following:

- Design an IP Addressing Scheme
- Assign IP Addresses to Network Devices and Verify Connectivity

554

11.8 VLSM

555

VLSM

Video – VLSM Basics

- This video will explain VLSM basics.

556

VLSM

Video – VLSM Example

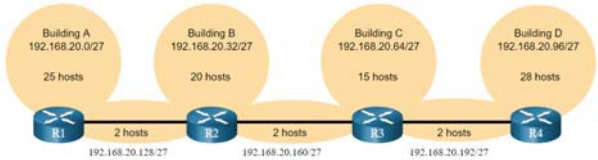
- This video will demonstrate creating subnets specific to the needs of the network.

557

VLSM
IPv4 Address Conservation

Given the topology, 7 subnets are required (i.e, four LANs and three WAN links) and the largest number of host is in Building D with 28 hosts.

- A /27 mask would provide 8 subnets of 30 host IP addresses and therefore support this topology.



558

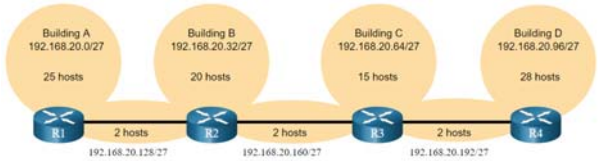
VLSM
IPv4 Address Conservation (Cont.)

However, the point-to-point WAN links only require two addresses and therefore waste 28 addresses each for a total of 84 unused addresses.

Host portion
2^5 – 2 = 30 host IP addresses per subnet

30 – 2 = 28
Each WAN subnet wastes 28 addresses

28 x 3 = 84
84 addresses are unused

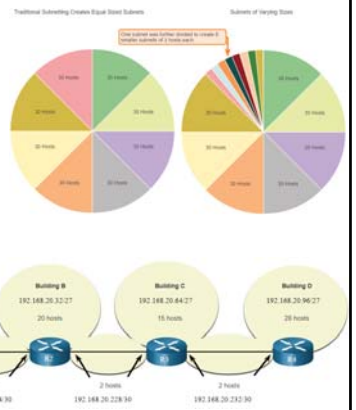


- Applying a traditional subnetting scheme to this scenario is not very efficient and is wasteful.
- VLSM was developed to avoid wasting addresses by enabling us to subnet a subnet.

559

VLSM
VLSM

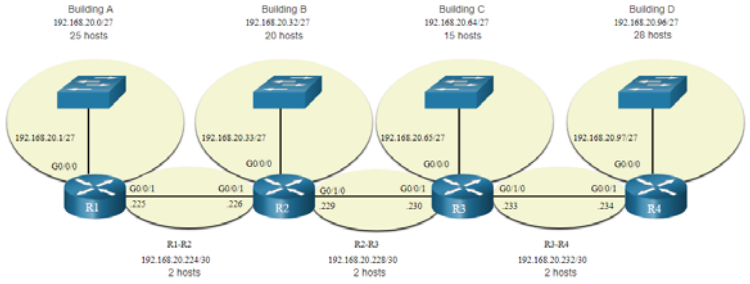
- The left side displays the traditional subnetting scheme (i.e., the same subnet mask) while the right side illustrates how VLSM can be used to subnet a subnet and divided the last subnet into eight /30 subnets.
- When using VLSM, always begin by satisfying the host requirements of the largest subnet and continue subnetting until the host requirements of the smallest subnet are satisfied.
- The resulting topology with VLSM applied.



560

VLSM
VLSM Topology Address Assignment

- Using VLSM subnets, the LAN and inter-router networks can be addressed without unnecessary waste as shown in the logical topology diagram.



561

11.9 Structured Design

562

Structured Design

IPv4 Network Address Planning

IP network planning is crucial to develop a scalable solution to an enterprise network.

- To develop an IPv4 network wide addressing scheme, you need to know how many subnets are needed, how many hosts a particular subnet requires, what devices are part of the subnet, which parts of your network use private addresses, and which use public, and many other determining factors.

Examine the needs of an organization's network usage and how the subnets will be structured.

- Perform a network requirement study by looking at the entire network to determining how each area will be segmented.
- Determine how many subnets are needed and how many hosts per subnet.
- Determine DHCP address pools and Layer 2 VLAN pools.

563

Structured Design

Device Address Assignment

Within a network, there are different types of devices that require addresses:

- **End user clients** – Most use DHCP to reduce errors and burden on network support staff. IPv6 clients can obtain address information using DHCPv6 or SLAAC.
- **Servers and peripherals** – These should have a predictable static IP address.
- **Servers that are accessible from the internet** – Servers must have a public IPv4 address, most often accessed using NAT.
- **Intermediary devices** – Devices are assigned addresses for network management, monitoring, and security.
- **Gateway** – Routers and firewall devices are gateway for the hosts in that network.

When developing an IP addressing scheme, it is generally recommended that you have a set pattern of how addresses are allocated to each type of device.

564

Structured Design

Packet Tracer – VLSM Design and Implementation Practice

In this Packet Tracer, you will do the following:

- Examine the Network Requirements
- Design the VLSM Addressing Scheme
- Assign IP Addresses to Devices and Verify Connectivity

565

11.10 Module Practice and Quiz

566

Structured Design

Packet Tracer – Design and Implement a VLSM Addressing Scheme

In this Packet Tracer, you will do the following:

- Design a VLSM IP addressing scheme given requirements
- Configure addressing on network devices and hosts
- Verify IP connectivity
- Troubleshoot connectivity issues as required.

567

Structured Design

Packet Tracer – Design and Implement a VLSM Addressing Scheme - Physical Mode
Lab – Design and Implement a VLSM Addressing Scheme

In both the Packet Tracer Physical Mode activity and in the Lab, you will complete the following objectives:

- Examine Network Requirements
- Design the VLSM Address Scheme
- Cable and Configure the IPv4 Network

568

Module Practice and Quiz

What did I learn in this module?

- The IP addressing structure consists of a 32-bit hierarchical network address that identifies a network and a host portion. Network devices use a process called ANDing using the IP address and associated subnet mask to identify the network and host portions.
- Destination IPv4 packets can be unicast, broadcast, and multicast.
- There are globally routable IP addresses as assigned by the IANA and there are three ranges of private IP network addresses that cannot be routed globally but can be used on all internal private networks.
- Reduce large broadcast domains using subnets to create smaller broadcast domains, reduce overall network traffic, and improve network performance.
- Create IPv4 subnets using one or more of the host bits as network bits. However, networks are most easily subnetted at the octet boundary of /8, /16, and /24.
- Larger networks can be subnetted at the /8 or /16 boundaries.
- Use VLSM to reduce the number of unused host addresses per subnet.

569

Module Practice and Quiz

What did I learn in this module? (Cont.)

- VLSM allows a network space to be divided into unequal parts. Always begin by satisfying the host requirements of the largest subnet. Continue subnetting until the host requirements of the smallest subnet are satisfied.
- When designing a network addressing scheme, consider internal, DMZ, and external requirements. Use a consistent internal IP addressing scheme with a set pattern of how addresses are allocated to each type of device.

Module 11: IPv4 Addressing

New Terms and Commands

• prefix length • logical AND • network address • broadcast address • first usable address • last usable address • unicast, broadcast, and multicast transmissions • private addresses • public addresses • Network Address Translation (NAT) • loopback addresses • Automatic Private IP Addressing (APIPA) addresses • classful addressing (Class A, B, C, D, and E)	Internet Assigned Numbers Authority (IANA) Regional Internet Registries (RIRs) AfriNIC, APNIC, ARIN, LACNIC, and RIPE NCC broadcast domains subnets octet boundary variable-length subnet mask (VLSM)

Module 12: IPv6 Addressing

Instructor Materials

Introduction to Networks v7.0 (ITN)

What to Expect in this Module

- To facilitate learning, the following features within the GUI may be included in this module:

Feature	Description
Animations	Expose learners to new skills and concepts.
Videos	Expose learners to new skills and concepts.
Check Your Understanding(CYU)	Per topic online quiz to help learners gauge content understanding.
Interactive Activities	A variety of formats to help learners gauge content understanding.
Syntax Checker	Small simulations that expose learners to Cisco command line to practice configuration skills.
PT Activity	Simulation and modeling activities designed to explore, acquire, reinforce, and expand skills.

What to Expect in this Module (Cont.)

- To facilitate learning, the following features may be included in this module:

Feature	Description
Packet Tracer Physical Mode Activity	These activities are completed using Packet Tracer in Physical Mode.
Hands-On Labs	Labs designed for working with physical equipment.
Class Activities	These are found on the Instructor Resources page. Class Activities are designed to facilitate learning, class discussion, and collaboration.
Module Quizzes	Self-assessments that integrate concepts and skills learned throughout the series of topics presented in the module.
Module Summary	Briefly recaps module content.

 575

575

584

Module Objectives

Module Title: IPv6 Addressing

Module Objective: Implement an IPv6 Addressing scheme.

Topic Title	Topic Objective
IPv4 Issues	Explain the need for IPv6 addressing.
IPv6 Address Representation	Explain how IPv6 addresses are represented.
IPv6 Address Types	Compare types of IPv6 network addresses.
GUA and LLA Static Configuration	Explain how to Configure static global unicast and link-local IPv6 network addresses.
Dynamic Addressing for IPv6 GUAs	Explain how to configure global unicast addresses dynamically.

 585

585

Module Objectives (Cont.)

Module Title: IPv6 Addressing

Module Objective: Implement an IPv6 Addressing scheme.

Topic Title	Topic Objective
Dynamic Addressing for IPv6 LLAs	Configure link-local addresses dynamically.
IPv6 Multicast Addresses	Identify IPv6 addresses.
Subnet an IPv6 Network	Implement a subnetted IPv6 addressing scheme.

 586

586

12.1 IPv4 Issues

587

IPv4 Issues

Need for IPv6

- IPv4 is running out of addresses. IPv6 is the successor to IPv4. IPv6 has a much larger 128-bit address space.
- The development of IPv6 also included fixes for IPv4 limitations and other enhancements.
- With an increasing internet population, a limited IPv4 address space, issues with NAT and the IoT, the time has come to begin the transition to IPv6.

588

IPv4 Issues

IPv4 and IPv6 Coexistence

Both IPv4 and IPv6 will coexist in the near future and the transition will take several years.

The IETF has created various protocols and tools to help network administrators migrate their networks to IPv6. These migration techniques can be divided into three categories:

- **Dual stack** -The devices run both IPv4 and IPv6 protocol stacks simultaneously.
- **Tunneling** – A method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet.
- **Translation** - Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4.

Note: Tunneling and translation are for transitioning to native IPv6 and should only be used where needed. The goal should be native IPv6 communications from source to destination.

589

12.2 IPv6 Address Representation

590

IPv6 Address Representation

IPv6 Addressing Formats

- IPv6 addresses are 128 bits in length and written in hexadecimal.
- IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.
- The preferred format for writing an IPv6 address is x:x:x:x:x:x:x:x, with each "x" consisting of four hexadecimal values.
- In IPv6, a hextet is the unofficial term used to refer to a segment of 16 bits, or four hexadecimal values.
- Examples of IPv6 addresses in the preferred format:

```
2001:0db8:0000:1111:0000:0000:0000:0200
2001:0db8:0000:00a3:abcd:0000:0000:1234
```


591

IPv6 Address Representation

Rule 1 – Omit Leading Zero

The first rule to help reduce the notation of IPv6 addresses is to omit any leading 0s (zeros).

Examples:

- 01ab can be represented as 1ab
- 09f0 can be represented as 9f0
- 0a00 can be represented as a00
- 00ab can be represented as ab

Note: This rule only applies to leading 0s, NOT to trailing 0s, otherwise the address would be ambiguous.

Type	Format
Preferred	2001 : **0**db8 : **000**0 : 1111 : **000**0 : **000**0 : **000**0 : **0**200
No leading zeros	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200

592

IPv6 Address Representation

Rule 2 – Double Colon

A double colon (::) can replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros.

Example:

- 2001:db8:cafe:1:0:0:0:1 (leading 0s omitted) could be represented as 2001:db8:cafe:1::1

Note: The double colon (::) can only be used once within an address, otherwise there would be more than one possible resulting address.

Type	Format
Preferred	2001 : **0**db8 : **000**0 : 1111 : **0000** : **0000** : **0000** : **0**200
Compressed	2001:db8:0:1111::200

593

12.3 IPv6 Address Types

594

IPv6 Address Types

Unicast, Multicast, Anycast

There are three broad categories of IPv6 addresses:

- **Unicast** – Unicast uniquely identifies an interface on an IPv6-enabled device.
- **Multicast** – Multicast is used to send a single IPv6 packet to multiple destinations.
- **Anycast** – This is any IPv6 unicast address that can be assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device having that address.

Note: Unlike IPv4, IPv6 does not have a broadcast address. However, there is an IPv6 all-nodes multicast address that essentially gives the same result.

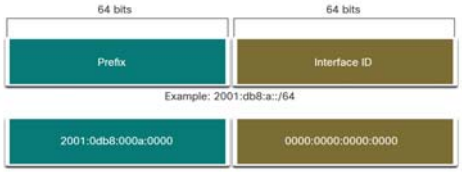
595

IPv6 Address Types

IPv6 Prefix Length

Prefix length is represented in slash notation and is used to indicate the network portion of an IPv6 address.

The IPv6 prefix length can range from 0 to 128. The recommended IPv6 prefix length for LANs and most other types of networks is /64.



Note: It is strongly recommended to use a 64-bit Interface ID for most networks. This is because stateless address autoconfiguration (SLAAC) uses 64 bits for the Interface ID. It also makes subnetting easier to create and manage.

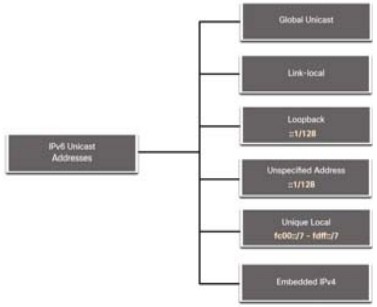
596

IPv6 Address Types

Types of IPv6 Unicast Addresses

Unlike IPv4 devices that have only a single address, IPv6 addresses typically have two unicast addresses:

- **Global Unicast Address (GUA)** – This is similar to a public IPv4 address. These are globally unique, internet-routable addresses.
- **Link-local Address (LLA)** - Required for every IPv6-enabled device and used to communicate with other devices on the same local link. LLAs are not routable and are confined to a single link.



597

IPv6 Address Types

A Note About the Unique Local Address

The IPv6 unique local addresses (range fc00::/7 to fdff::/7) have some similarity to RFC 1918 private addresses for IPv4, but there are significant differences:

- Unique local addresses are used for local addressing within a site or between a limited number of sites.
- Unique local addresses can be used for devices that will never need to access another network.
- Unique local addresses are not globally routed or translated to a global IPv6 address.

Note: Many sites use the private nature of RFC 1918 addresses to attempt to secure or hide their network from potential security risks. This was never the intended use of ULAs.

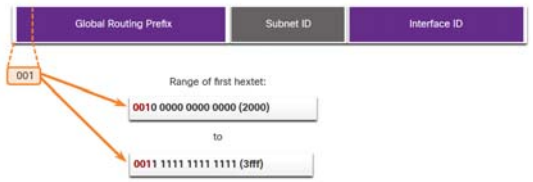
598

IPv6 Address Types

IPv6 GUA

IPv6 global unicast addresses (GUAs) are globally unique and routable on the IPv6 internet.

- Currently, only GUAs with the first three bits of 001 or 2000::/3 are being assigned.
- Currently available GUAs begins with a decimal 2 or a 3 (This is only 1/8th of the total available IPv6 address space).



599

IPv6 Address Types

IPv6 GUA Structure

Global Routing Prefix:

- The global routing prefix is the prefix, or network, portion of the address that is assigned by the provider, such as an ISP, to a customer or site. The global routing prefix will vary depending on ISP policies.

Subnet ID:

- The Subnet ID field is the area between the Global Routing Prefix and the Interface ID. The Subnet ID is used by an organization to identify subnets within its site.

Interface ID:

- The IPv6 interface ID is equivalent to the host portion of an IPv4 address. It is strongly recommended that in most cases /64 subnets should be used, which creates a 64-bit interface ID.

Note: IPv6 allows the all-0s and all-1s host addresses can be assigned to a device. The all-0s address is reserved as a Subnet-Router anycast address, and should be assigned only to routers.

600

IPv6 Address Types

IPv6 LLA

An IPv6 link-local address (LLA) enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet).

- Packets with a source or destination LLA cannot be routed.
- Every IPv6-enabled network interface must have an LLA.
- If an LLA is not configured manually on an interface, the device will automatically create one.
- IPv6 LLAs are in the fe80::/10 range.

1. Routers use the LLA of neighbor routers to send routing updates.
2. Hosts use the LLA of a local router as the default-gateway.

601

12.4 GUA and LLA Static Configuration

602

GUA and LLA Static Configuration

Static GUA Configuration on a Router

Most IPv6 configuration and verification commands in the Cisco IOS are similar to their IPv4 counterparts. In many cases, the only difference is the use of **ipv6** in place of **ip** within the commands.

- The command to configure an IPv6 GUA on an interface is: **ipv6 address** *ipv6-address/prefix-length.*
- The example shows commands to configure a GUA on the G0/0/0 interface on R1:

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
```

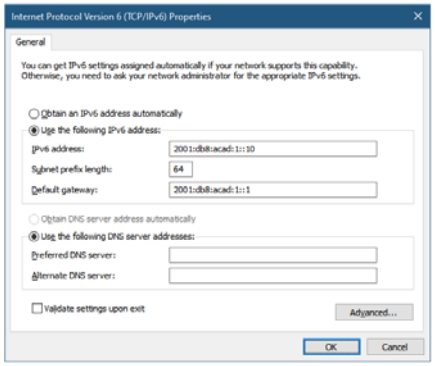

603

GUA and LLA Static Configuration

Static GUA Configuration on a Windows Host

- Manually configuring the IPv6 address on a host is similar to configuring an IPv4 address.
- The GUA or LLA of the router interface can be used as the default gateway. Best practice is to use the LLA.

Note: When DHCPv6 or SLAAC is used, the LLA of the router will automatically be specified as the default gateway address.



604

GUA and LLA Static Configuration

Static GUA Configuration of a Link-Local Unicast Address

Configuring the LLA manually lets you create an address that is recognizable and easier to remember.

- LLAs can be configured manually using the **ipv6 address** *ipv6-link-local-address* **link-local** command.
- The example shows commands to configure a LLA on the G0/0/0 interface on R1

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address fe80::1:1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
```

Note: The same LLA can be configured on each link as long as it is unique on that link. Common practice is to create a different LLA on each interface of the router to make it easy to identify the router and the specific interface.

605

12.5 Dynamic Addressing for IPv6 GUAs

606

Dynamic Addressing for IPv6 GUAs

RS and RA Messages

Devices obtain GUA addresses dynamically through Internet Control Message Protocol version 6 (ICMPv6) messages.

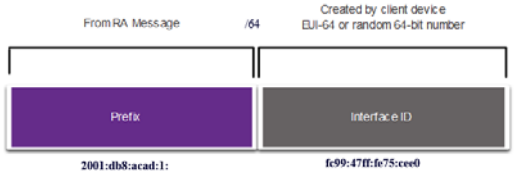
- Router Solicitation (RS) messages are sent by host devices to discover IPv6 routers
- Router Advertisement (RA) messages are sent by routers to inform hosts on how to obtain an IPv6 GUA and provide useful network information such as:
  - Network prefix and prefix length
  - Default gateway address
  - DNS addresses and domain name
- The RA can provide three methods for configuring an IPv6 GUA :
  - SLAAC
  - SLAAC with stateless DHCPv6 server
  - Stateful DHCPv6 (no SLAAC)

607

Dynamic Addressing for IPv6 GUAs

Method 1: SLAAC

- SLAAC allows a device to configure a GUA without the services of DHCPv6.
- Devices obtain the necessary information to configure a GUA from the ICMPv6 RA messages of the local router.
- The prefix is provided by the RA and the device uses either the EUI-64 or random generation method to create an interface ID.



608

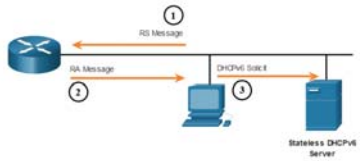
Dynamic Addressing for IPv6 GUAs

Method 2: SLAAC and Stateless DHCP

An RA can instruct a device to use both SLAAC and stateless DHCPv6.

The RA message suggests devices use the following:

- SLAAC to create its own IPv6 GUA
- The router LLA, which is the RA source IPv6 address, as the default gateway address
- A stateless DHCPv6 server to obtain other information such as a DNS server address and a domain name



609

Dynamic Addressing for IPv6 GUAs

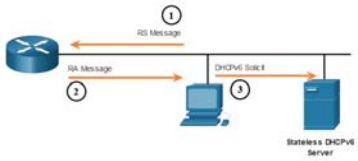
Method 3: Stateful DHCPv6

An RA can instruct a device to use stateful DHCPv6 only.

Stateful DHCPv6 is similar to DHCP for IPv4. A device can automatically receive a GUA, prefix length, and the addresses of DNS servers from a stateful DHCPv6 server.

The RA message suggests devices use the following:

- The router LLA, which is the RA source IPv6 address, for the default gateway address.
- A stateful DHCPv6 server to obtain a GUA, DNS server address, domain name and other necessary information.

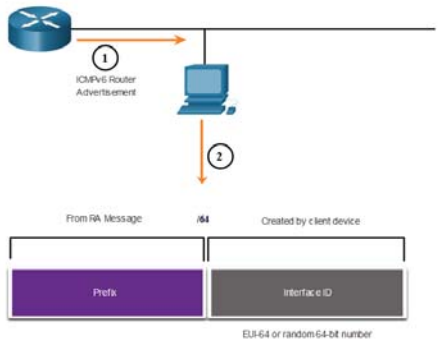


610

Dynamic Addressing for IPv6 GUAs

EUI-64 Process vs. Randomly Generated

- When the RA message is either SLAAC or SLAAC with stateless DHCPv6, the client must generate its own interface ID.
- The interface ID can be created using the EUI-64 process or a randomly generated 64-bit number.



611

Dynamic Addressing for IPv6 GUAs

EUI-64 Process

The IEEE defined the Extended Unique Identifier (EUI) or modified EUI-64 process which performs the following:

- A 16 bit value of fffe (in hexadecimal) is inserted into the middle of the 48-bit Ethernet MAC address of the client.
- The 7th bit of the client MAC address is reversed from binary 0 to 1.
- Example:

48-bit MAC	fc:99:47:75:ce:e0
EUI-64 Interface ID	fe:99:47:ff:fe:75:ce:e0

612

Dynamic Addressing for IPv6 GUAs

Randomly Generated Interface IDs

Depending upon the operating system, a device may use a randomly generated interface ID instead of using the MAC address and the EUI-64 process.

Beginning with Windows Vista, Windows uses a randomly generated interface ID instead of one created with EUI-64.

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
Default Gateway . . . . . . . . . : fe80::1
C:\>
```

Note: To ensure the uniqueness of any IPv6 unicast address, the client may use a process known as Duplicate Address Detection (DAD). This is similar to an ARP request for its own address. If there is no reply, then the address is unique.

613

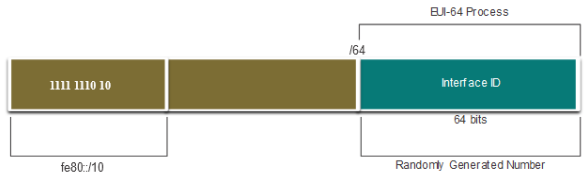
12.6 Dynamic Addressing for IPv6 LLAs

614

Dynamic Addressing for IPv6 LLAs

Dynamic LLAs

- All IPv6 interfaces must have an IPv6 LLA.
- Like IPv6 GUAs, LLAs can be configured dynamically.
- The figure shows the LLA is dynamically created using the fe80::/10 prefix and the interface ID using the EUI-64 process, or a randomly generated 64-bit number.



615

Dynamic Addressing for IPv6 LLAs

Dynamic LLAs on Windows

Operating systems, such as Windows, will typically use the same method for both a SLAAC-created GUA and a dynamically assigned LLA.

EUI-64 Generated Interface ID:

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
Link-local IPv6 Address . . . . . : fe80::fc99:47ff:fe75:cee0
Default Gateway . . . . . . . . . : fe80::1
C:\>
```

Random 64-bit Generated Interface ID:

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
   Default Gateway . . . . . . . . . : fe80::1
C:\>
```


616

Dynamic Addressing for IPv6 LLAs

Dynamic LLAs on Cisco Routers

Cisco routers automatically create an IPv6 LLA whenever a GUA is assigned to the interface. By default, Cisco IOS routers use EUI-64 to generate the interface ID for all LLAs on IPv6 interfaces.

Here is an example of a LLA dynamically configured on the G0/0/0 interface of R1:

```
R1# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Hardware is ISR4221-2x1GE, address is 7079.b392.3640 (bia 7079.b392.3640)
(Output omitted)
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
FE80::7279:B3FF:FE92:3640
2001:DB8:ACAD:1::1
```


617

Dynamic Addressing for IPv6 LLAs

Verify IPv6 Address Configuration

Cisco routers automatically create an IPv6 LLA whenever a GUA is assigned to the interface. By default, Cisco IOS routers use EUI-64 to generate the interface ID for all LLAs on IPv6 interfaces.

Here is an example of a LLA dynamically configured on the G0/0/0 interface of R1:

```
R1# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Hardware is ISR4221-2x1GE, address is 7079.b392.3640 (bia 7079.b392.3640)
(Output omitted)
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
FE80::7279:B3FF:FE92:3640
2001:DB8:ACAD:1::1
```


618

Module Practice and Quiz

Packet Tracer – Configure IPv6 Addressing

In this Packet Tracer, you will do the following:

- Configure IPv6 Addressing on the router
- Configure IPv6 Addressing on the servers
- Configure IPv6 Addressing on the clients
- Test and verify network connectivity

12.7 IPv6 Multicast Addresses

IPv6 Multicast Addresses

Assigned IPv6 Multicast Addresses

IPv6 multicast addresses have the prefix ff00::/8. There are two types of IPv6 multicast addresses:

- Well-Known multicast addresses
- Solicited node multicast addresses

Note: Multicast addresses can only be destination addresses and not source addresses.

IPv6 Multicast Addresses

Well-Known IPv6 Multicast Addresses

Well-known IPv6 multicast addresses are assigned and are reserved for predefined groups of devices.

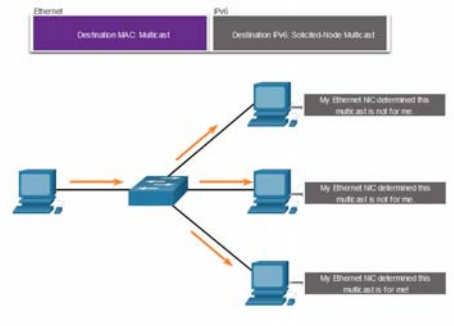
There are two common IPv6 Assigned multicast groups:

- **ff02::1 All-nodes multicast group** - This is a multicast group that all IPv6-enabled devices join. A packet sent to this group is received and processed by all IPv6 interfaces on the link or network.
- **ff02::2 All-routers multicast group** - This is a multicast group that all IPv6 routers join. A router becomes a member of this group when it is enabled as an IPv6 router with the **ipv6 unicast-routing** global configuration command.

IPv6 Multicast Addresses

Solicited-Node IPv6 Multicast

- A solicited-node multicast address is similar to the all-nodes multicast address.
- A solicited-node multicast address is mapped to a special Ethernet multicast address.
- The Ethernet NIC can filter the frame by examining the destination MAC address without sending it to the IPv6 process to see if the device is the intended target of the IPv6 packet.



623

Module Practice and Quiz

Lab – Identify IPv6 Addresses

In this lab, you complete the following objectives:

- Identify the Different Types of IPv6 Addresses
- Examine a Host IPv6 Network Interface and Address
- Practice IPv6 Address Abbreviation

624

12.8 Subnet an IPv6 Network

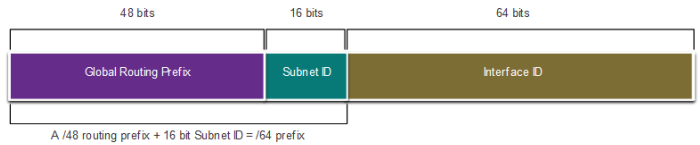
625

Subnet an IPv6 Network

Subnet Using the Subnet ID

IPv6 was designed with subnetting in mind.

- A separate subnet ID field in the IPv6 GUA is used to create subnets.
- The subnet ID field is the area between the Global Routing Prefix and the interface ID.



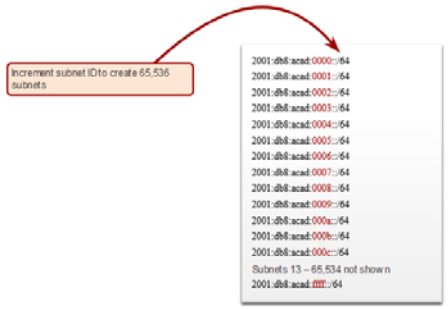
626

Subnet an IPv6 Network

IPv6 Subnetting Example

Given the 2001:db8:acad::/48 global routing prefix with a 16 bit subnet ID.

- Allows 65,536 /64 subnets
- The global routing prefix is the same for all subnets.
- Only the subnet ID hextet is incremented in hexadecimal for each subnet.



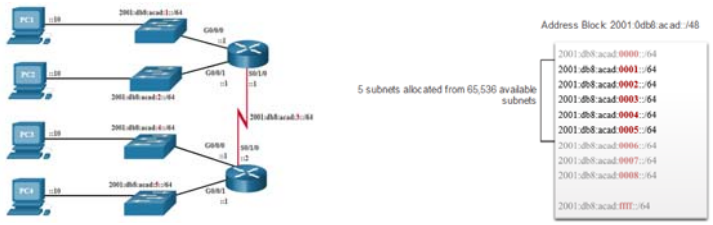
627

Subnet an IPv6 Network

IPv6 Subnet Allocation

The example topology requires five subnets, one for each LAN as well as for the serial link between R1 and R2.

The five IPv6 subnets were allocated, with the subnet ID field 0001 through 0005. Each /64 subnet will provide more addresses than will ever be needed.



628

Subnet an IPv6 Network

Router Configured with IPv6 Subnets

The example shows that each of the router interfaces on R1 has been configured to be on a different IPv6 subnet.

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
```


629

2.9 Module Practice and Quiz

630

Module Practice and Quiz

Packet Tracer – Implement a Subnetted IPv6 Addressing Scheme

In this Packet Tracer, you will do the following:

- Determine IPv6 subnets and addressing scheme
- Configure IPv6 addressing on routers and PCs
- Verify IPv6 connectivity

 631

631

Packet Tracer - Configure IPv6 Addresses on Network Devices - Physical Mode
Lab – Configure IPv6 Addresses on Network Devices

In this Packet Tracer activity, you will complete the following objectives:

- Set Up the Network Topology
- Configure PC Hosts
- Configure and Verify Basic Switch Settings

In this Lab, you complete the following objectives:

- Set up the topology and configure basic router and switch settings
- Configure IPv6 addresses manually
- Verify end-to-end connectivity

 632

632

Module Practice and Quiz

What did I learn in this module?

- IPv4 has a theoretical maximum of 4.3 billion addresses.
- The IETF has created various protocols and tools to help network administrators migrate their networks to IPv6. The migration techniques can be divided into three categories: dual stack, tunneling, and translation.
- IPv6 addresses are 128 bits in length and written as a string of hexadecimal values.
- The preferred format for writing an IPv6 address is x:x:x:x:x:x:x:x, with each “x” consisting of four hexadecimal values.
- There are three types of IPv6 addresses: unicast, multicast, and anycast.
- An IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device.
- IPv6 global unicast addresses (GUAs) are globally unique and routable on the IPv6 internet.
- An IPv6 link-local address (LLA) enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet).
- The command to configure an IPv6 GUA on an interface is **ipv6 address** *ipv6-address/prefix-length*.
- A device obtains a GUA dynamically through ICMPv6 messages. IPv6 routers periodically send out ICMPv6 RA messages, every 200 seconds, to all IPv6-enabled devices on the network.

 633

633

Module Practice and Quiz

What did I learn in this module? (Cont.)

- RA messages have three methods: SLAAC, SLAAC with a stateless DHCPv6 server, and stateful DHCPv6 (no SLAAC).
- The interface ID can be created using the EUI-64 process or a randomly generated 64-bit number.
- The EUIs process uses the 48-bit Ethernet MAC address of the client and inserts another 16 bits in the middle of MAC address to create a 64-bit interface ID.
- Depending upon the operating system, a device may use a randomly generated interface ID.
- All IPv6 devices must have an IPv6 LLA. An LLA can be configured manually or created dynamically.
- Cisco routers automatically create an IPv6 LLA whenever a GUA is assigned to the interface.
- There are two types of IPv6 multicast addresses: well-known multicast addresses and solicited node multicast addresses.
- Two commonIPv6 assigned multicast groups are: ff02::1 All-nodes multicast group and ff02::2 All-routers multicast group.
- A solicited-node multicast address is similar to the all-nodes multicast address. The advantage of a solicited-node multicast address is that it is mapped to a special Ethernet multicast address.
- IPv6 was designed with subnetting in mind. A separate subnet ID field in the IPv6 GUA is used to create subnets.

 634

634

Module 12: WLAN Concepts

New Terms and Commands

- Hextet
- Link-local address (LLA)
- ipv6 address
- show ipv6 interface brief
- SLAAC
- Router advertisement
- Router solicitation
- EUI-64
- Solicited node multicast

635

Module 13: ICMP

Instructor Materials

Introduction to Networks v7.0
(ITN)

636

Module 13: ICMP

Introduction of Networks v7.0
(ITN)

645

Module Objectives

Module Title: ICMP

Module Objective: Use various tools to test network connectivity.

Topic Title	Topic Objective
ICMP Messages	Explain how ICMP is used to test network connectivity.
Ping and Traceroute Testing	Use ping and traceroute utilities to test network connectivity.

646

13.1 ICMP Messages

647

ICMP Messages

ICMPv4 and ICMPv6 Messages

- Internet Control Message Protocol (ICMP) provides feedback about issues related to the processing of IP packets under certain conditions.
- ICMPv4 is the messaging protocol for IPv4. ICMPv6 is the messaging protocol for IPv6 and includes additional functionality.
- The ICMP messages common to both ICMPv4 and ICMPv6 include:
  - Host reachability
  - Destination or Service Unreachable
  - Time exceeded

Note: ICMPv4 messages are not required and are often not allowed within a network for security reasons.

648

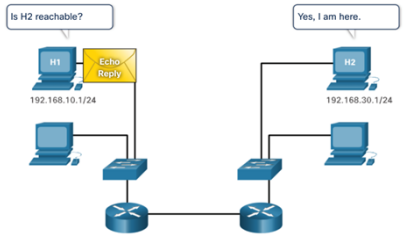
ICMP Messages

Host Reachability

ICMP Echo Message can be used to test the reachability of a host on an IP network.

In the example:

- The local host sends an ICMP Echo Request to a host.
- If the host is available, the destination host responds with an Echo Reply.



649

ICMP Messages

Destination or Service Unreachable

- An ICMP Destination Unreachable message can be used to notify the source that a destination or service is unreachable.
- The ICMP message will include a code indicating why the packet could not be delivered.

A few Destination Unreachable codes for ICMPv4 are as follows:

- 0 - Net unreachable
- 1 - Host unreachable
- 2 - Protocol unreachable
- 3 - Port unreachable

A few Destination Unreachable codes for ICMPv6 are as follows:

- 0 - No route to destination
- 1 - Communication with the destination is administratively prohibited (e.g., firewall)
- 2 – Beyond scope of the source address
- 3 - Address unreachable
- 4 - Port unreachable

Note: ICMPv6 has similar but slightly different codes for Destination Unreachable messages.

650

ICMP Messages

Time Exceeded

- When the Time to Live (TTL) field in a packet is decremented to 0, an ICMPv4 Time Exceeded message will be sent to the source host.
- ICMPv6 also sends a Time Exceeded message. Instead of the IPv4 TTL field, ICMPv6 uses the IPv6 Hop Limit field to determine if the packet has expired.

```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Note: Time Exceeded messages are used by the **traceroute** tool.

651

ICMP Messages

ICMPv6 Messages

ICMPv6 has new features and improved functionality not found in ICMPv4, including four new protocols as part of the Neighbor Discovery Protocol (ND or NDP).

Messaging between an IPv6 router and an IPv6 device, including dynamic address allocation are as follows:

- Router Solicitation (RS) message
- Router Advertisement (RA) message

Messaging between IPv6 devices, including duplicate address detection and address resolution are as follows:

- Neighbor Solicitation (NS) message
- Neighbor Advertisement (NA) message

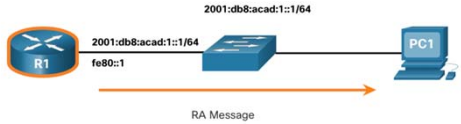
Note: ICMPv6 ND also includes the redirect message, which has a similar function to the redirect message used in ICMPv4.

652

ICMP Messages

ICMPv6 Messages (Cont.)

- RA messages are sent by IPv6-enabled routers every 200 seconds to provide addressing information to IPv6-enabled hosts.
- RA message can include addressing information for the host such as the prefix, prefix length, DNS address, and domain name.
- A host using Stateless Address Autoconfiguration (SLAAC) will set its default gateway to the link-local address of the router that sent the RA.

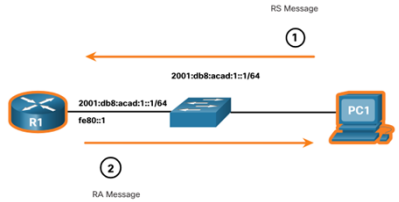


653

ICMP Messages

ICMPv6 Messages (Cont.)

- An IPv6-enabled router will also send out an RA message in response to an RS message.
- In the figure, PC1 sends a RS message to determine how to receive its IPv6 address information dynamically.
  - R1 replies to the RS with an RA message.
  - PC1 sends an RS message, "Hi, I just booted up. Is there an IPv6 router on the network? I need to know how to get my IPv6 address information dynamically."
  - R1 replies with an RA message. "Hi all IPv6-enabled devices. I'm R1 and you can use SLAAC to create an IPv6 global unicast address. The prefix is 2001:db8:acad:1::/64. By the way, use my link-local address fe80::1 as your default gateway."

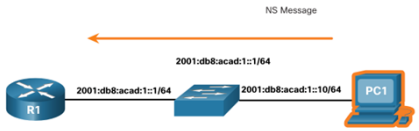


654

ICMP Messages

ICMPv6 Messages (Cont.)

- A device assigned a global IPv6 unicast or link-local unicast address, may perform duplicate address detection (DAD) to ensure that the IPv6 address is unique.
- To check the uniqueness of an address, the device will send an NS message with its own IPv6 address as the targeted IPv6 address.
- If another device on the network has this address, it will respond with an NA message notifying to the sending device that the address is in use.



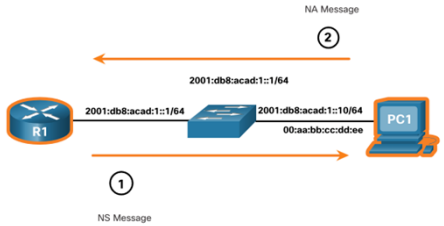
Note: DAD is not required, but RFC 4861 recommends that DAD is performed on unicast addresses.

655

ICMP Messages

ICMPv6 Messages (Cont.)

- To determine the MAC address for the destination, the device will send an NS message to the solicited node address.
- The message will include the known (targeted) IPv6 address. The device that has the targeted IPv6 address will respond with an NA message containing its Ethernet MAC address.
- In the figure, R1 sends a NS message to 2001:db8:acad:1::10 asking for its MAC address.



656

13.2 Ping and Traceroute Tests

657

Ping and Traceroute Tests

Ping – Test Connectivity

- The **ping** command is an IPv4 and IPv6 testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts and provides a summary that includes the success rate and average round-trip time to the destination.
- If a reply is not received within the timeout, ping provides a message indicating that a response was not received.
- It is common for the first ping to timeout if address resolution (ARP or ND) needs to be performed before sending the ICMP Echo Request.

```
S1#ping 192.168.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

```
R1#ping 2001:db8:acad:1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

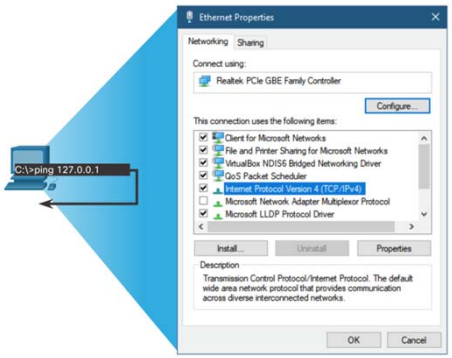

658

Ping and Traceroute Tests

Ping the Loopback

Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host. To do this, **ping** the local loopback address of 127.0.0.1 for IPv4 (::1 for IPv6).

- A response from 127.0.0.1 for IPv4, or ::1 for IPv6, indicates that IP is properly installed on the host.
- An error message indicates that TCP/IP is not operational on the host.



659

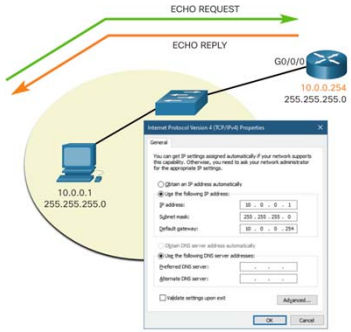
Ping and Traceroute Tests

Ping the Default Gateway

The **ping** command can be used to test the ability of a host to communicate on the local network.

The default gateway address is most often used because the router is normally always operational.

- A successful **ping** to the default gateway indicates that the host and the router interface serving as the default gateway are both operational on the local network.
- If the default gateway address does not respond, a **ping** can be sent to the IP address of another host on the local network that is known to be operational.



660

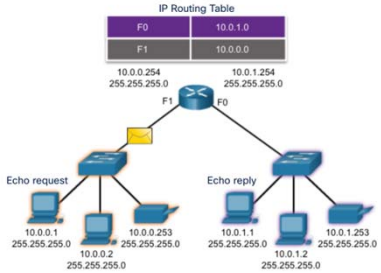
Ping and Traceroute Tests

Ping a Remote Host

Ping can also be used to test the ability of a local host to communicate across an internetwork.

A local host can ping a host on a remote network. A successful **ping** across the internetwork confirms communication on the local network.

Note: Many network administrators limit or prohibit the entry of ICMP messages therefore, the lack of a **ping** response could be due to security restrictions.



661

Ping and Traceroute Tests

Traceroute – Test the Path

- Traceroute (**tracert**) is a utility that is used to test the path between two hosts and provide a list of hops that were successfully reached along that path.
- Traceroute provides round-trip time for each hop along the path and indicates if a hop fails to respond. An asterisk (*) is used to indicate a lost or unreplied packet.
- This information can be used to locate a problematic router in the path or may indicate that the router is configured not to reply.

```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2

  1   192.168.10.2    1 msec    0 msec    0 msec
  2   192.168.20.2    2 msec    1 msec    0 msec
  3   192.168.30.2    1 msec    0 msec    0 msec
  4   192.168.40.2    0 msec    0 msec    0 msec
```

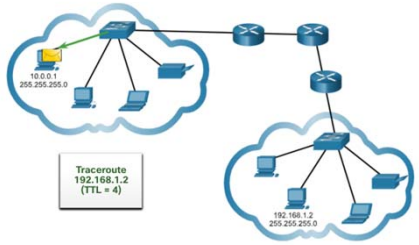
Note: Traceroute makes use of a function of the TTL field in IPv4 and the Hop Limit field in IPv6 in the Layer 3 headers, along with the ICMP Time Exceeded message.

662

Ping and Traceroute Tests

Traceroute – Test the Path (Cont.)

- The first message sent from traceroute will have a TTL field value of 1. This causes the TTL to time out at the first router. This router then responds with a ICMPv4 Time Exceeded message.
- Traceroute then progressively increments the TTL field (2, 3, 4...) for each sequence of messages. This provides the trace with the address of each hop as the packets time out further down the path.
- The TTL field continues to be increased until the destination is reached, or it is incremented to a predefined maximum.



Ping and Traceroute Tests

Packet Tracer – Verify IPv4 and IPv6 Addressing

In this Packet Tracer, you will do the following:

- Complete the Addressing Table Documentation
- Test Connectivity Using Ping
- Discover the Path by Tracing the Route

Ping and Traceroute Tests

Packet Tracer – Use Ping and Traceroute to Test Network Connectivity

In this Packet Tracer, you will do the following:

- Test and Restore IPv4 Connectivity
- Test and Restore IPv6 Connectivity

13.3 Module Practice and Quiz

Module Practice and Quiz

Packet Tracer – Use ICMP to Test and Correct Network Connectivity

In this Packet Tracer, you will do the following:

- Use ICMP to locate connectivity issues.
- Configure network devices to correct connectivity issues.

 667

667

Module Practice and Quiz

Packet Tracer - Use Ping and Traceroute to Test Network Connectivity - Physical Mode
Lab – Use Ping and Traceroute to Test Network Connectivity

In this Packet Tracer Physical Mode activity, you will complete the following objectives:

- Use Ping Command for Basic Network Testing
- Use Tracert and Traceroute Commands for Basic Network Testing
- Troubleshoot the Topology

In this Lab, you complete the following objectives:

- Build and Configure the Network
- Use Ping Command for Basic Network Testing
- Use Tracert and Traceroute Commands for Basic Network Testing
- Troubleshoot the Topology

 668

668

Module Practice and Quiz

What did I learn in this module?

- The purpose of ICMP messages is to provide feedback about issues related to the processing of IP packets under certain conditions.
- The ICMP messages common to both ICMPv4 and ICMPv6 are: Host reachability, Destination or Service Unreachable, and Time exceeded.
- The messages between an IPv6 router and an IPv6 device including dynamic address allocation include RS and RA. The messages between IPv6 devices include the redirect (similar to IPv4), NS and NA.
- Ping (used by IPv4 and IPv6) uses ICMP echo request and echo reply messages to test connectivity between hosts
- Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host.
- Traceroute (tracert) generates a list of hops that were successfully reached along the path.

 669

669

Module 13 : ICMP

New Terms and Commands

- ICMP
- ICMPv4
- ICMPv6
- ping
- traceroute
- tracert
- Network Discovery Protocol
- Router Solicitation (RS)
- Router Advertisement (RA)
- Neighbor Solicitation (NS)
- Neighbor Advertisement (NA)
- TTL

 670

670

671

What to Expect in this Module

- To facilitate learning, the following features within the GUI may be included in this module:

Feature	Description
Animations	Expose learners to new skills and concepts.
Videos	Expose learners to new skills and concepts.
Check Your Understanding(CYU)	Per topic online quiz to help learners gauge content understanding.
Interactive Activities	A variety of formats to help learners gauge content understanding.
Syntax Checker	Small simulations that expose learners to Cisco command line to practice configuration skills.
PT Activity	Simulation and modeling activities designed to explore, acquire, reinforce, and expand skills.

 673

673

What to Expect in this Module (Cont.)

- To facilitate learning, the following features may be included in this module:

Feature	Description
Hands-On Labs	Labs designed for working with physical equipment.
Class Activities	These are found on the Instructor Resources page. Class Activities are designed to facilitate learning, class discussion, and collaboration.
Module Quizzes	Self-assessments that integrate concepts and skills learned throughout the series of topics presented in the module.
Module Summary	Briefly recaps module content.

 674

674

680

Module Objectives

Module Title: Transport Layer

Module Objective: Compare the operations of transport layer protocols in supporting end-to-end communication.

Topic Title	Topic Objective
Transportation of Data	Explain the purpose of the transport layer in managing the transportation of data in end-to-end communication.
TCP Overview	Explain characteristics of TCP.
UDP Overview	Explain characteristics of UDP.
Port Numbers	Explain how TCP and UDP use port numbers.
TCP Communication Process	Explain how TCP session establishment and termination processes facilitate reliable communication.
Reliability and Flow Control	Explain how TCP protocol data units are transmitted and acknowledged to guarantee delivery.
UDP Communication	Compare the operations of transport layer protocols in supporting end-to-end communication.

681

14.1 Transportation of Data

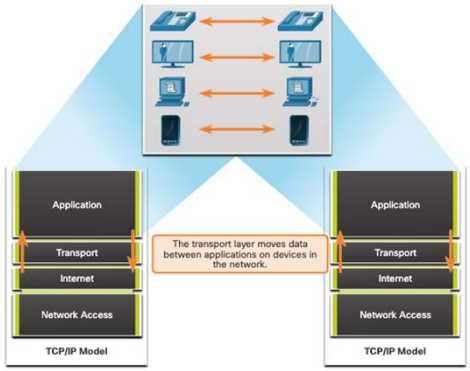
682

Transportation of Data

Role of the Transport Layer

The transport layer is:

- responsible for logical communications between applications running on different hosts.
- The link between the application layer and the lower layers that are responsible for network transmission.



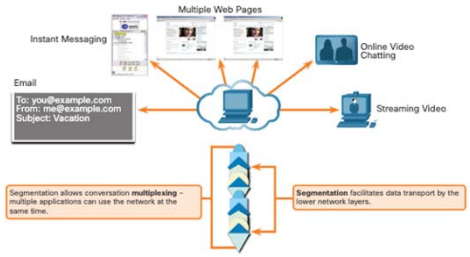
683

Transportation of Data

Transport Layer Responsibilities

The transport layer has the following responsibilities:

- Tracking individual conversations
- Segmenting data and reassembling segments
- Adds header information
- Identify, separate, and manage multiple conversations
- Uses segmentation and multiplexing to enable different communication conversations to be interleaved on the same network

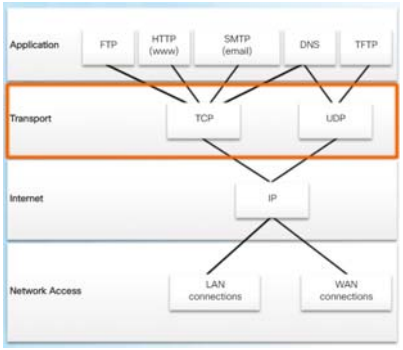


684

Transportation of Data

Transport Layer Protocols

- IP does not specify how the delivery or transportation of the packets takes place.
- Transport layer protocols specify how to transfer messages between hosts, and are responsible for managing reliability requirements of a conversation.
- The transport layer includes the TCP and UDP protocols.



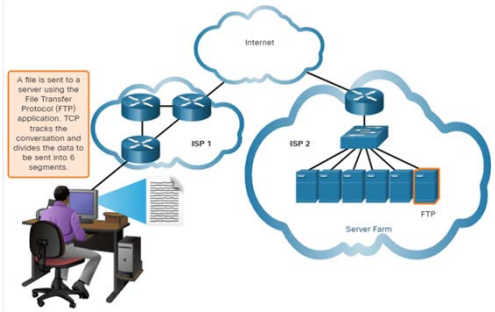
685

Transportation of Data

Transmission Control Protocol

TCP provides reliability and flow control. TCP basic operations:

- Number and track data segments transmitted to a specific host from a specific application
- Acknowledge received data
- Retransmit any unacknowledged data after a certain amount of time
- Sequence data that might arrive in wrong order
- Send data at an efficient rate that is acceptable by the receiver



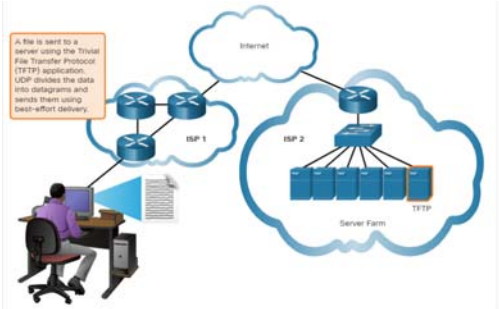
686

Transportation of Data

User Datagram Protocol (UDP)

UDP provides the basic functions for delivering datagrams between the appropriate applications, with very little overhead and data checking.

- UDP is a connectionless protocol.
- UDP is known as a best-effort delivery protocol because there is no acknowledgment that the data is received at the destination.



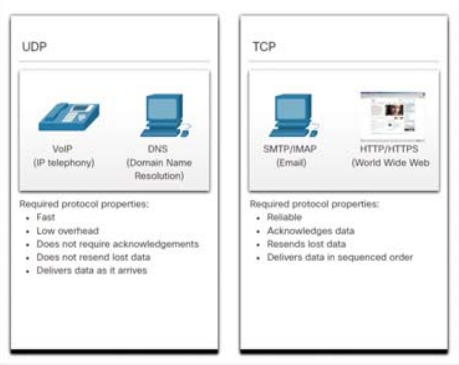
687

Transportation of Data

The Right Transport Layer Protocol for the Right Application

UDP is also used by request-and-reply applications where the data is minimal, and retransmission can be done quickly.

If it is important that all the data arrives and that it can be processed in its proper sequence, TCP is used as the transport protocol.



688

14.2 TCP Overview

689

TCP Overview

TCP Features

- **Establishes a Session** - TCP is a connection-oriented protocol that negotiates and establishes a permanent connection (or session) between source and destination devices prior to forwarding any traffic.
- **Ensures Reliable Delivery** - For many reasons, it is possible for a segment to become corrupted or lost completely, as it is transmitted over the network. TCP ensures that each segment that is sent by the source arrives at the destination.
- **Provides Same-Order Delivery** - Because networks may provide multiple routes that can have different transmission rates, data can arrive in the wrong order.
- **Supports Flow Control** - Network hosts have limited resources (i.e., memory and processing power). When TCP is aware that these resources are overtaxed, it can request that the sending application reduce the rate of data flow.

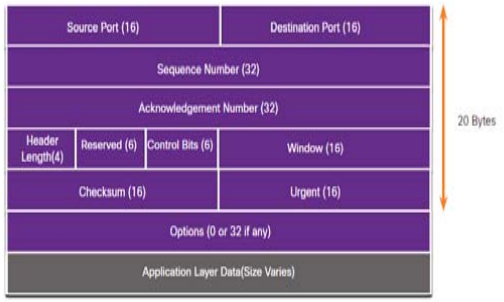
690

TCP Overview

TCP Header

TCP is a stateful protocol which means it keeps track of the state of the communication session.

TCP records which information it has sent, and which information has been acknowledged.



691

TCP Overview

TCP Header Fields

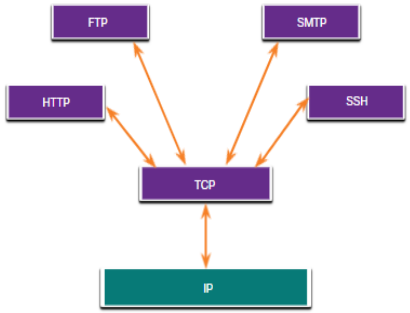
TCP Header Field	Description
Source Port	A 16-bit field used to identify the source application by port number.
Destination Port	A 16-bit field used to identify the destination application by port number.
Sequence Number	A 32-bit field used for data reassembly purposes.
Acknowledgment Number	A 32-bit field used to indicate that data has been received and the next byte expected from the source.
Header Length	A 4-bit field known as "data offset" that indicates the length of the TCP segment header.
Reserved	A 6-bit field that is reserved for future use.
Control bits	A 6-bit field used that includes bit codes, or flags, which indicate the purpose and function of the TCP segment.
Window size	A 16-bit field used to indicate the number of bytes that can be accepted at one time.
Checksum	A 16-bit field used for error checking of the segment header and data.
Urgent	A 16-bit field used to indicate if the contained data is urgent.

692

TCP Overview

Applications that use TCP

TCP handles all tasks associated with dividing the data stream into segments, providing reliability, controlling data flow, and reordering segments.



693

14.3 UDP Overview

694

UDP Overview

UDP Features

UDP features include the following:

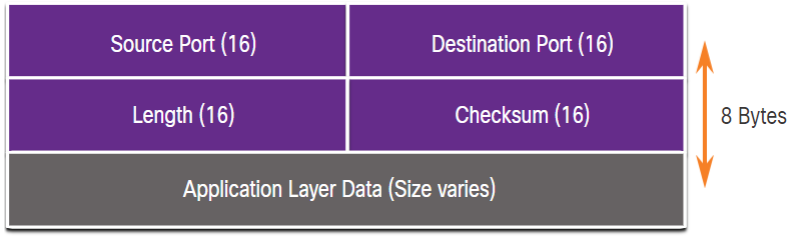
- Data is reconstructed in the order that it is received.
- Any segments that are lost are not resent.
- There is no session establishment.
- The sending is not informed about resource availability.

695

UDP Overview

UDP Header

The UDP header is far simpler than the TCP header because it only has four fields and requires 8 bytes (i.e. 64 bits).



696

UDP Overview

UDP Header Fields

The table identifies and describes the four fields in a UDP header.

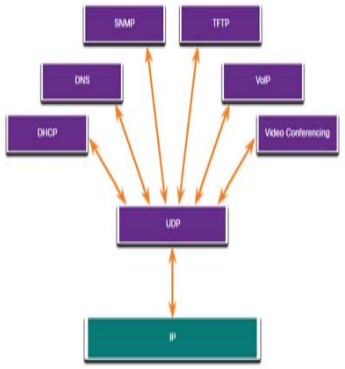
UDP Header Field	Description
Source Port	A 16-bit field used to identify the source application by port number.
Destination Port	A 16-bit field used to identify the destination application by port number.
Length	A 16-bit field that indicates the length of the UDP datagram header.
Checksum	A 16-bit field used for error checking of the datagram header and data.

697

UDP Overview

Applications that use UDP

- Live video and multimedia applications - These applications can tolerate some data loss but require little or no delay. Examples include VoIP and live streaming video.
- Simple request and reply applications - Applications with simple transactions where a host sends a request and may or may not receive a reply. Examples include DNS and DHCP.
- Applications that handle reliability themselves - Unidirectional communications where flow control, error detection, acknowledgments, and error recovery is not required, or can be handled by the application. Examples include SNMP and TFTP.



698

14.4 Port Numbers

699

Port Numbers

Multiple Separate Communications

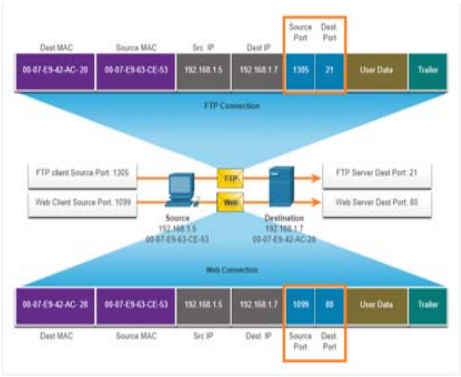
TCP and UDP transport layer protocols use port numbers to manage multiple, simultaneous conversations.

The source port number is associated with the originating application on the local host whereas the destination port number is associated with the destination application on the remote host.

700

Port numbers
Socket Pairs

- The source and destination ports are placed within the segment.
- The segments are then encapsulated within an IP packet.
- The combination of the source IP address and source port number, or the destination IP address and destination port number is known as a socket.
- Sockets enable multiple processes, running on a client, to distinguish themselves from each other, and multiple connections to a server process to be distinguished from each other.



701

Port Numbers
Port Number Groups

Port Group	Number Range	Description
Well-known Ports	**0 to 1,023**	•These port numbers are reserved for common or popular services and applications such as web browsers, email clients, and remote access clients. •Defined well-known ports for common server applications enables clients to easily identify the associated service required.
Registered Ports	**1,024 to 49,151**	•These port numbers are assigned by IANA to a requesting entity to use with specific processes or applications. •These processes are primarily individual applications that a user has chosen to install, rather than common applications that would receive a well-known port number. •For example, Cisco has registered port 1812 for its RADIUS server authentication process.
Private and/or **Dynamic Ports**	**49,152 to 65,535**	•These ports are also known as *ephemeral ports*. •The client's OS usually assign port numbers dynamically when a connection to a service is initiated. •The dynamic port is then used to identify the client application during communication.

702

Port Numbers
Port Number Groups (Cont.)

Well-Known Port Numbers

Port Number	Protocol	Application
20	TCP	File Transfer Protocol (FTP) - Data
21	TCP	File Transfer Protocol (FTP) - Control
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	UDP, TCP	Domain Name Service (DNS)
67	UDP	Dynamic Host Configuration Protocol (DHCP) - Server
68	UDP	Dynamic Host Configuration Protocol - Client
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol version 3 (POP3)
143	TCP	Internet Message Access Protocol (IMAP)
161	UDP	Simple Network Management Protocol (SNMP)
443	TCP	Hypertext Transfer Protocol Secure (HTTPS)

703

Port Numbers
The netstat Command

Unexplained TCP connections can pose a major security threat. Netstat is an important tool to verify connections.

```
C:\> netstat
Active Connections
Proto Local Address          Foreign Address                State
TCP   192.168.1.124:3126     192.168.0.2:netbios-ssn        ESTABLISHED
TCP   192.168.1.124:3158     207.138.126.152:http           ESTABLISHED
TCP   192.168.1.124:3159     207.138.126.169:http           ESTABLISHED
TCP   192.168.1.124:3160     207.138.126.169:http           ESTABLISHED
TCP   192.168.1.124:3161     sc.msn.com:http                ESTABLISHED
TCP   192.168.1.124:3166     www.cisco.com:http             ESTABLISHED
```


704

14.5 TCP Communication Process

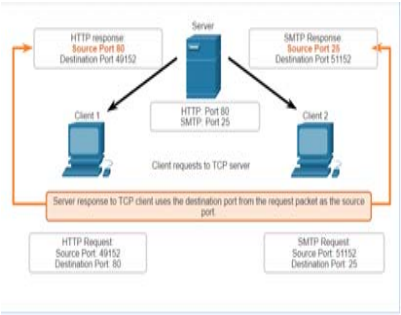
705

TCP Communication Process

TCP Server Processes

Each application process running on a server is configured to use a port number.

- An individual server cannot have two services assigned to the same port number within the same transport layer services.
- An active server application assigned to a specific port is considered open, which means that the transport layer accepts, and processes segments addressed to that port.
- Any incoming client request addressed to the correct socket is accepted, and the data is passed to the server application.



706

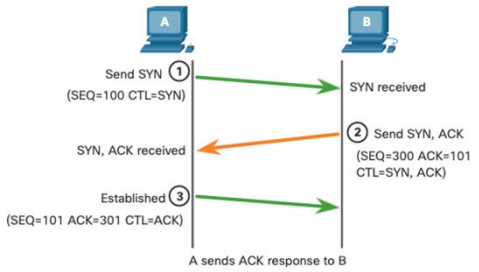
TCP Communication Process

TCP Connection Establishment

Step 1: The initiating client requests a client-to-server communication session with the server.

Step 2: The server acknowledges the client-to-server communication session and requests a server-to-client communication session.

Step 3: The initiating client acknowledges the server-to-client communication session.



707

TCP Communication Process

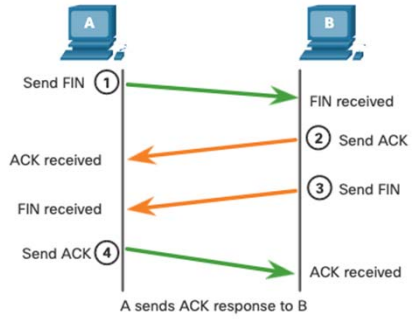
Session Termination

Step 1: When the client has no more data to send in the stream, it sends a segment with the FIN flag set.

Step 2: The server sends an ACK to acknowledge the receipt of the FIN to terminate the session from client to server.

Step 3: The server sends a FIN to the client to terminate the server-to-client session.

Step 4: The client responds with an ACK to acknowledge the FIN from the server.



708

TCP Communication Process

TCP Three-Way Handshake Analysis

Functions of the Three-Way Handshake:

- It establishes that the destination device is present on the network.
- It verifies that the destination device has an active service and is accepting requests on the destination port number that the initiating client intends to use.
- It informs the destination device that the source client intends to establish a communication session on that port number.

After the communication is completed the sessions are closed, and the connection is terminated. The connection and session mechanisms enable TCP reliability function.

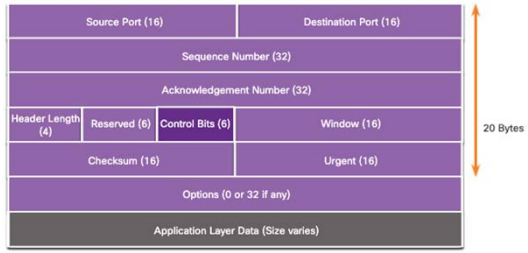
709

TCP Communication Process

TCP Three-Way Handshake Analysis (Cont.)

The six control bit flags are as follows:

- **URG** - Urgent pointer field significant
- **ACK** - Acknowledgment flag used in connection establishment and session termination
- **PSH** - Push function
- **RST** - Reset the connection when an error or timeout occurs
- **SYN** - Synchronize sequence numbers used in connection establishment
- **FIN** - No more data from sender and used in session termination



710

TCP Communication Process

Video TCP 3-Way Handshake

The video covers the following:

- TCP 3-Way Handshake
- Termination of a TCP conversation

711

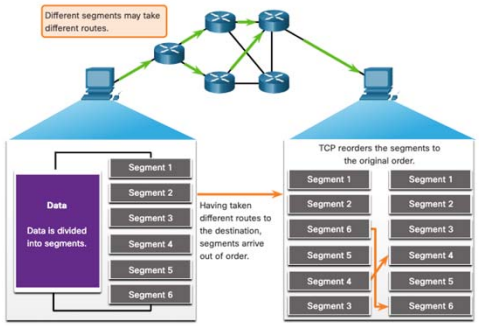
14.6 Reliability and Flow Control

712

Reliability and Flow Control

TCP Reliability- Guaranteed and Ordered Delivery

- TCP can also help maintain the flow of packets so that devices do not become overloaded.
- There may be times when TCP segments do not arrive at their destination or arrive out of order.
- All the data must be received and the data in these segments must be reassembled into the original order.
- Sequence numbers are assigned in the header of each packet to achieve this goal.



713

Reliability and Flow Control

Video -TCP Reliability- Sequence Numbers and Acknowledgments

This video depicts a simplified example of the TCP operations.

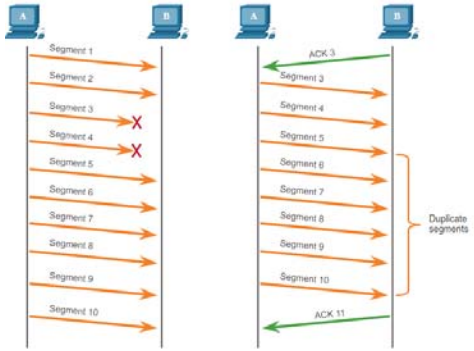
714

Reliability and Flow Control

TCP Reliability – Data Loss and Retransmission

No matter how well designed a network is, data loss occasionally occurs.

TCP provides methods of managing these segment losses. Among these is a mechanism to retransmit segments for unacknowledged data.



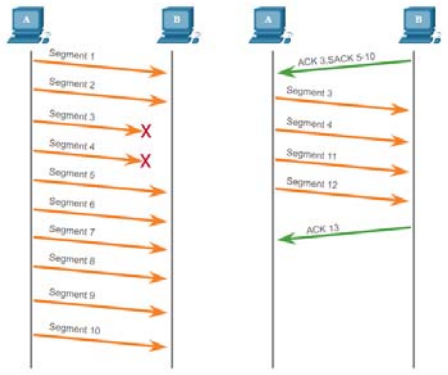
715

Reliability and Flow Control

TCP Reliability – Data Loss and Retransmission (Cont.)

Host operating systems today typically employ an optional TCP feature called selective acknowledgment (SACK), negotiated during the three-way handshake.

If both hosts support SACK, the receiver can explicitly acknowledge which segments (bytes) were received including any discontinuous segments.



716

Reliability and Flow Control

Video - TCP Reliability – Data Loss and Retransmission

This video shows the process of resending segments that are not initially received by the destination.

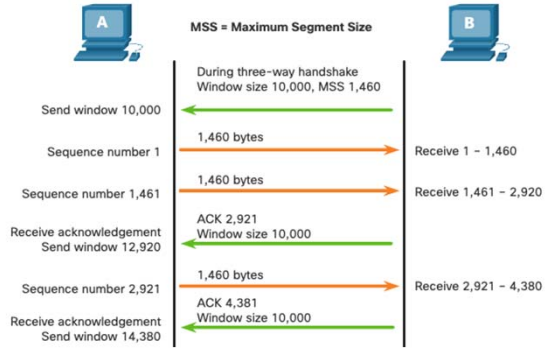
717

Reliability and Flow Control

TCP Flow Control – Window Size and Acknowledgments

TCP also provides mechanisms for flow control as follows:

- Flow control is the amount of data that the destination can receive and process reliably.
- Flow control helps maintain the reliability of TCP transmission by adjusting the rate of data flow between source and destination for a given session.



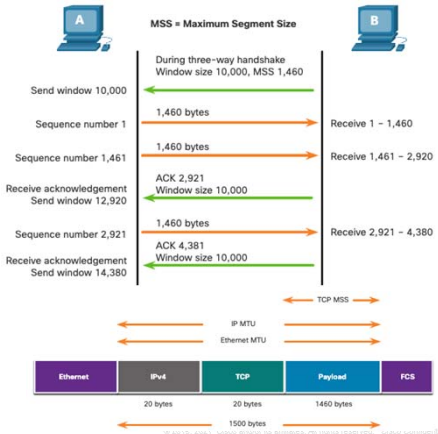
718

Reliability and Flow Control

TCP Flow Control – Maximum Segment Size

Maximum Segment Size (MSS) is the maximum amount of data that the destination device can receive.

- A common MSS is 1,460 bytes when using IPv4.
- A host determines the value of its MSS field by subtracting the IP and TCP headers from the Ethernet maximum transmission unit (MTU), which is 1500 bytes be default.
- 1500 minus 40 (20 bytes for the IPv4 header and 20 bytes for the TCP header) leaves 1460 bytes.



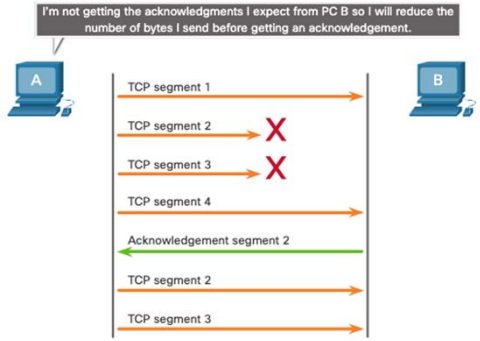
719

Reliability and Flow Control

TCP Flow Control – Congestion Avoidance

When congestion occurs on a network, it results in packets being discarded by the overloaded router.

To avoid and control congestion, TCP employs several congestion handling mechanisms, timers, and algorithms.



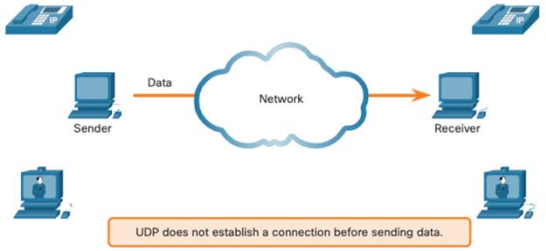
720

14.7 UDP Communication

721

UDP Communication
UDP Low Overhead versus Reliability

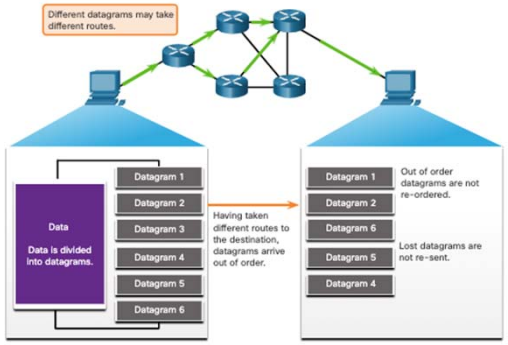
UDP does not establish a connection. UDP provides low overhead data transport because it has a small datagram header and no network management traffic.



722

UDP Communication
UDP Datagram Reassembly

- UDP does not track sequence numbers the way TCP does.
- UDP has no way to reorder the datagrams into their transmission order.
- UDP simply reassembles the data in the order that it was received and forwards it to the application.

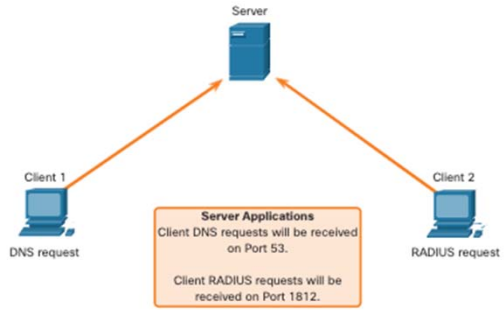


723

UDP Communication
UDP Server Processes and Requests

UDP-based server applications are assigned well-known or registered port numbers.

UDP receives a datagram destined for one of these ports, it forwards the application data to the appropriate application based on its port number.

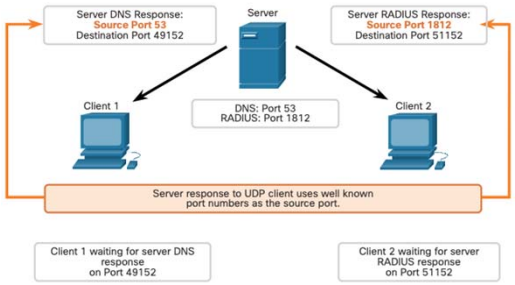


724

UDP Communication

UDP Client Processes

- The UDP client process dynamically selects a port number from the range of port numbers and uses this as the source port for the conversation.
- The destination port is usually the well-known or registered port number assigned to the server process.
- After a client has selected the source and destination ports, the same pair of ports are used in the header of all datagrams in the transaction.



725

14.8 Module Practice and Quiz

726

Module Practice and Quiz

Packet Tracer - TCP and UDP Communications

In this Packet Tracer, you will do the following:

- Generate Network Traffic in Simulation Mode.
- Examine the Functionality of the TCP and UDP Protocols.

727

Module Practice and Quiz

What did I learn in this module?

- The transport layer is the link between the application layer and the lower layers that are responsible for network transmission.
- The transport layer includes TCP and UDP.
- TCP establishes sessions, ensures reliability, provides same-order delivery, and supports flow control.
- UDP is a simple protocol that provides the basic transport layer functions.
- UDP reconstructs data in the order it is received, lost segments are not resent, no session establishment, and UPD does not inform the sender of resource availability.
- The TCP and UDP transport layer protocols use port numbers to manage multiple simultaneous conversations.
- Each application process running on a server is configured to use a port number.
- The port number is either automatically assigned or configured manually by a system administrator.
- For the original message to be understood by the recipient, all the data must be received and the data in these segments must be reassembled into the original order.

728

Module Practice and Quiz

What did I learn in this module (Cont.)?

- Sequence numbers are assigned in the header of each packet.
- Flow control helps maintain the reliability of TCP transmission by adjusting the rate of data flow between source and destination.
- A source might be transmitting 1,460 bytes of data within each TCP segment. This is the typical MSS that a destination device can receive.
- The process of the destination sending acknowledgments as it processes bytes received and the continual adjustment of the source's send window is known as sliding windows.
- To avoid and control congestion, TCP employs several congestion handling mechanisms.

729

Module 14: Transport Layer

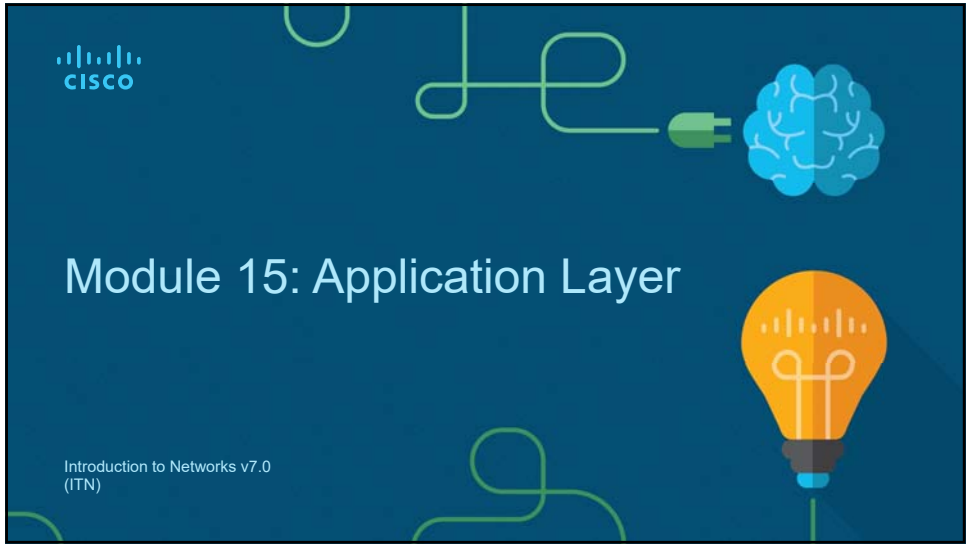
New Terms and Commands

- Conversation Multiplexing
- Segments
- Datagrams
- Connection-Oriented Protocol
- Connectionless Protocol
- Stateless Protocol
- Flow Control
- Same-Order Delivery
- Socket Pairs
- netstat

- Three-Way Handshake
- SYN
- ACK
- FIN
- URG
- PSH
- RST
- Initial Sequence Number (ISN)
- Selective Acknowledgement (SACK)
- Sliding Window
- Maximum Segment Size (MSS)
- Maximum Transmission Unit (MTU)
- Congestion Avoidance

730

731



740

Module Objectives

- **Module Title**: Application Layer
- **Module Objective**: Explain the operation of application layer protocols in providing support to end-user applications.

Topic Title	Topic Objective
Application, Presentation, and Session	Explain how the functions of the application layer, presentation layer, and session layer work together to provide network services to end user applications.
Peer-to-Peer	Explain how end user applications operate in a peer-to-peer network.
Web and Email Protocols	Explain how web and email protocols operate.
IP Addressing Services	Explain how DNS and DHCP operate.
File Sharing Services	Explain how file transfer protocols operate.

 741

741

15.1 Application, Presentation, and Session

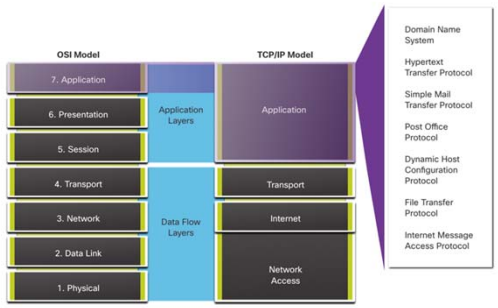
 742

742

Application, Presentation, and Session

Application Layer

- The upper three layers of the OSI model (application, presentation, and session) define functions of the TCP/IP application layer.
- The application layer provides the interface between the applications used to communicate, and the underlying network over which messages are transmitted.
- Some of the most widely known application layer protocols include HTTP, FTP, TFTP, IMAP and DNS.



 743

743

Application, Presentation, and Session

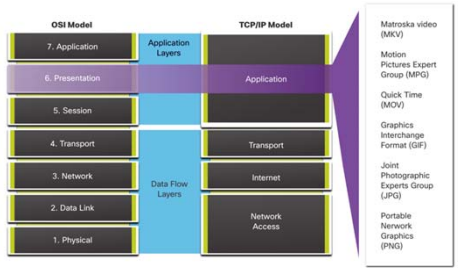
Presentation and Session Layer

The presentation layer has three primary functions:

- Formatting, or presenting, data at the source device into a compatible format for receipt by the destination device
- Compressing data in a way that can be decompressed by the destination device
- Encrypting data for transmission and decrypting data upon receipt

The session layer functions:

- It creates and maintains dialogs between source and destination applications.
- It handles the exchange of information to initiate dialogs, keep them active, and to restart sessions that are disrupted or idle for a long period of time.



 744

744

Application, Presentation, and Session

TCP/IP Application Layer Protocols

- The TCP/IP application protocols specify the format and control information necessary for many common internet communication functions.
- Application layer protocols are used by both the source and destination devices during a communication session.
- For the communications to be successful, the application layer protocols that are implemented on the source and destination host must be compatible.

Name System
DNS - Domain Name System (or Service)
- TCP, UDP client 53
- Translates domain names, such as cisco.com, into IP addresses.

Host Config
DHCP - Dynamic Host Configuration Protocol
- UDP client 68, server 67
- Dynamically assigns IP addresses to be re-used when no longer needed

Web
HTTP - Hypertext Transfer Protocol
- TCP 80, 8080
- A set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web

745

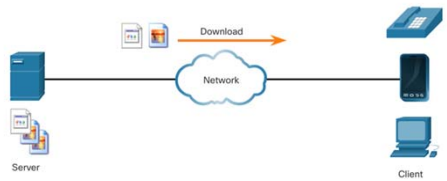
15.2 Peer-to-Peer

746

Peer-to-Peer

Client-Server Model

- Client and server processes are considered to be in the application layer.
- In the client/server model, the device requesting the information is called a client and the device responding to the request is called a server.
- Application layer protocols describe the format of the requests and responses between clients and servers.

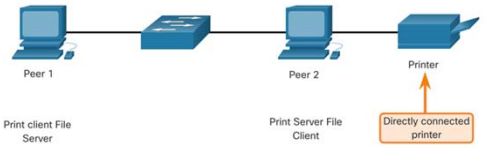


747

Peer-to-Peer

Peer-to-Peer Networks

- In a peer-to-peer (P2P) network, two or more computers are connected via a network and can share resources (such as printers and files) without having a dedicated server.
- Every connected end device (known as a peer) can function as both a server and a client.
- One computer might assume the role of server for one transaction while simultaneously serving as a client for another. The roles of client and server are set on a per request basis.

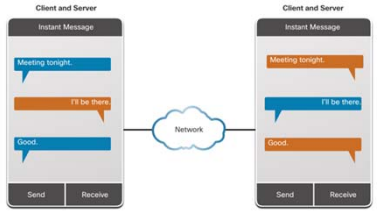


748

Peer-to-Peer

Peer-to-Peer Applications

- A P2P application allows a device to act as both a client and a server within the same communication.
- Some P2P applications use a hybrid system where each peer accesses an index server to get the location of a resource stored on another peer.



749

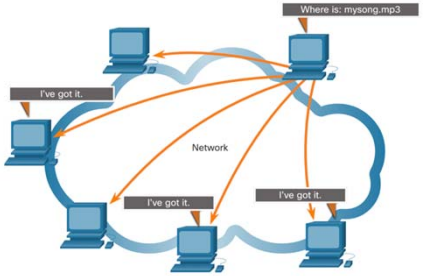
Peer-to-Peer

Common P2P Applications

With P2P applications, each computer in the network that is running the application can act as a client or a server for the other computers in the network that are also running the application.

Common P2P networks include the following:

- BitTorrent
- Direct Connect
- eDonkey
- Freenet



750

15.3 Web and Email Protocols

751

Web and Email Protocols

Hypertext Transfer Protocol and Hypertext Markup Language

When a web address or Uniform Resource Locator (URL) is typed into a web browser, the web browser establishes a connection to the web service. The web service is running on the server that is using the HTTP protocol.

To better understand how the web browser and web server interact, examine how a web page is opened in a browser.

Step 1
The browser interprets the three parts of the URL:
- http (the protocol or scheme)
- www.cisco.com (the server name)
- index.html (the specific filename requested)

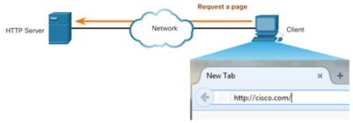
752

Web and Email Protocols

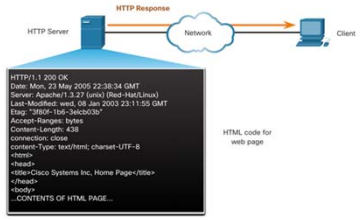
Hypertext Transfer Protocol and Hypertext Markup Language (Cont.)

Step 2
The browser then checks with a name server to convert www.cisco.com into a numeric IP address, which it uses to connect to the server.

The client initiates an HTTP request to a server by sending a GET request to the server and asks for the index.html file.



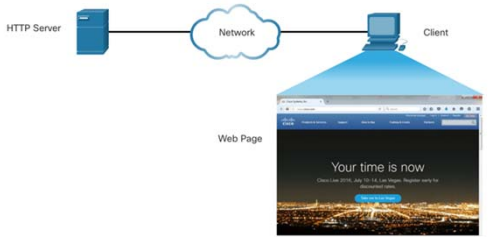
Step 3
In response to the request, the server sends the HTML code for this web page to the browser.



Web and Email Protocols

Hypertext Transfer Protocol and Hypertext Markup Language (Cont.)

Step 4
The browser deciphers the HTML code and formats the page for the browser window.



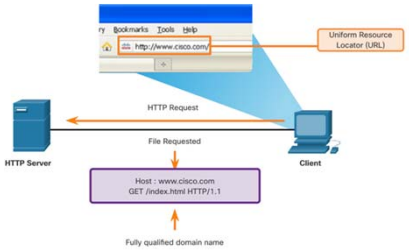
Web and Email Protocols

HTTP and HTTPS

HTTP is a request/response protocol that specifies the message types used for that communication.

The three common message types are GET, POST, and PUT:

- **GET** - This is a client request for data. A client (web browser) sends the GET message to the web server to request HTML pages.
- **POST** - This uploads data files to the web server, such as form data.
- **PUT** - This uploads resources or content to the web server, such as an image.



Note: HTTP is not a secure protocol. For secure communications sent across the internet, HTTPS should be used.

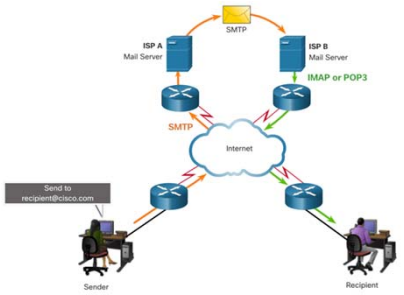
Web and Email Protocols

Email Protocols

Email is a store-and-forward method of sending, storing, and retrieving electronic messages across a network. Email messages are stored in databases on mail servers. Email clients communicate with mail servers to send and receive email.

The email protocols used for operation are:

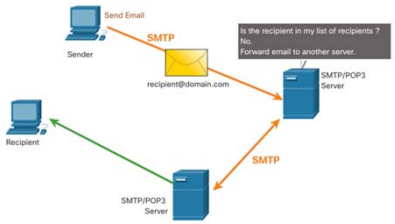
- Simple Mail Transfer Protocol (SMTP) – used to send mail.
- Post Office Protocol (POP) & IMAP – used for clients to receive mail.



Web and Email Protocols

SMTP, POP and IMAP

- When a client sends email, the client SMTP process connects with a server SMTP process on well-known port 25.
- After the connection is made, the client attempts to send the email to the server across the connection.
- When the server receives the message, it either places the message in a local account, if the recipient is local, or forwards the message to another mail server for delivery.
- The destination email server may not be online or may be busy. If so, SMTP spools messages to be sent at a later time.



Note: SMTP message formats require a message header (recipient email address & sender email address) and a message body.

 757

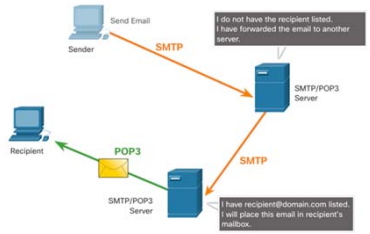
757

Web and Email Protocols

SMTP, POP and IMAP (Cont.)

POP is used by an application to retrieve mail from a mail server. When mail is downloaded from the server to the client using POP the messages are then deleted on the server.

- The server starts the POP service by passively listening on TCP port 110 for client connection requests.
- When a client wants to make use of the service, it sends a request to establish a TCP connection with the server.
- When the connection is established, the POP server sends a greeting.
- The client and POP server then exchange commands and responses until the connection is closed or aborted.



Note: Since POP does not store messages, it is not recommended for small businesses that need a centralized backup solution.

 758

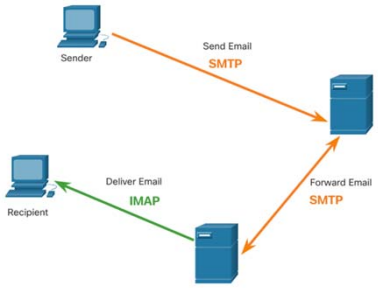
758

Web and Email Protocols

SMTP, POP and IMAP (Cont.)

IMAP is another protocol that describes a method to retrieve email messages.

- Unlike POP, when a user connects to an IMAP server, copies of the messages are downloaded to the client application. The original messages are kept on the server until manually deleted.
- When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.



 759

759

15.4 IP Addressing Services

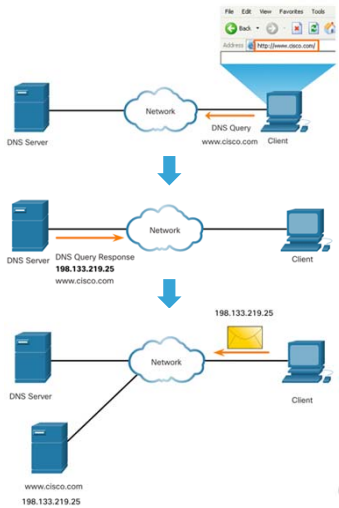
 760

760

IP Addressing Services

Domain Name Service

- Domain names were created to convert the numeric IP addresses into a simple, recognizable name.
- Fully-qualified domain names (FQDNs), such as http://www.cisco.com, are much easier for people to remember than 198.133.219.25.
- The DNS protocol defines an automated service that matches resource names with the required numeric network address. It includes the format for queries, responses, and data.



761

IP Addressing Services

DNS Message Format

The DNS server stores different types of resource records that are used to resolve names. These records contain the name, address, and type of record.

Some of these record types are as follows:

- **A** - An end device IPv4 address
- **NS** - An authoritative name server
- **AAAA** - An end device IPv6 address (pronounced quad-A)
- **MX** - A mail exchange record

When a client makes a query, the server DNS process first looks at its own records to resolve the name. If it is unable to resolve the name by using its stored records, it contacts other servers to resolve the name.

After a match is found and returned to the original requesting server, the server temporarily stores the numbered address in the event that the same name is requested again.

762

IP Addressing Services

DNS Message Format (Cont.)

DNS uses the same message format between servers, consisting of a question, answer, authority, and additional information for all types of client queries and server responses, error messages, and transfer of resource record information.

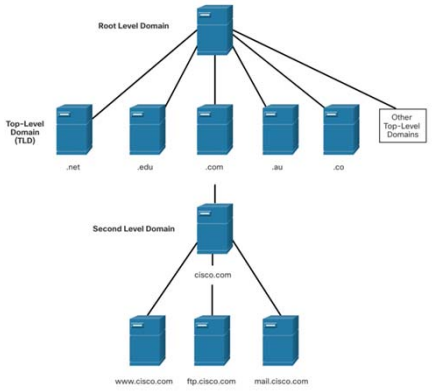
DNS message section	Description
Question	The question for the name server
Answer	Resource Records answering the question
Authority	Resource Records pointing toward an authority
Additional	Resource Records holding additional information

763

IP Addressing Services

DNS Hierarchy

- DNS uses a hierarchical system to create a database to provide name resolution.
- Each DNS server maintains a specific database file and is only responsible for managing name-to-IP mappings for that small portion of the entire DNS structure.
- When a DNS server receives a request for a name translation that is not within its DNS zone, the DNS server forwards the request to another DNS server within the proper zone for translation.
- Examples of top-level domains:
  - **.com** - a business or industry
  - **.org** - a non-profit organization
  - **.au** - Australia



764

IP Addressing Services

The nslookup Command

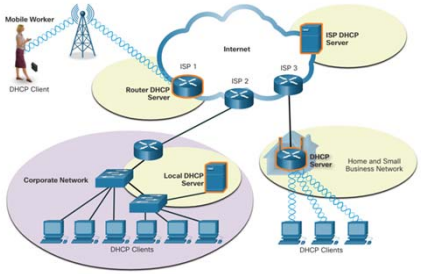
- Nslookup is a computer operating system utility that allows a user to manually query the DNS servers configured on the device to resolve a given host name.
- This utility can also be used to troubleshoot name resolution issues and to verify the current status of the name servers.
- When the **nslookup** command is issued, the default DNS server configured for your host is displayed.
- The name of a host or domain can be entered at the **nslookup** prompt.

```
C:\Users> nslookup
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183
> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    origin-www.cisco.com
Addresses:  2001:420:1101:1::a
          173.37.145.84
Aliases:  www.cisco.com
> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    cisco.netacad.net
Address:  72.163.6.223
>
```


IP Addressing Services

Dynamic Host Configuration Protocol

- The Dynamic Host Configuration Protocol (DHCP) for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters.
- DHCP is considered dynamic addressing compared to static addressing. Static addressing is manually entering IP address information.
- When a host connects to the network, the DHCP server is contacted, and an address is requested. The DHCP server chooses an address from a configured range of addresses called a pool and assigns (leases) it to the host.
- Many networks use both DHCP and static addressing. DHCP is used for general purpose hosts, such as end user devices. Static addressing is used for network devices, such as gateway routers, switches, servers, and printers.



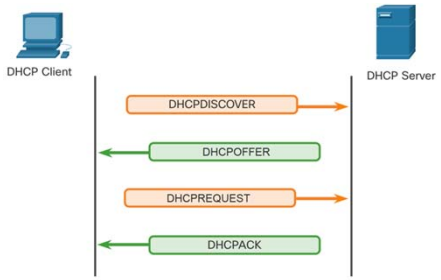
Note: DHCP for IPv6 (DHCPv6) provides similar services for IPv6 clients. However, DHCPv6 does not provide a default gateway address. This can only be obtained dynamically from the Router Advertisement message of the router.

IP Addressing Services

DHCP Operation

The DHCP Process:

- When an IPv4, DHCP-configured device boots up or connects to the network, the client broadcasts a DHCP discover (DHCPDISCOVER) message to identify any available DHCP servers on the network.
- A DHCP server replies with a DHCP offer (DHCPOFFER) message, which offers a lease to the client. (If a client receives more than one offer due to multiple DHCP servers on the network, it must choose one.)
- The client sends a DHCP request (DHCPREQUEST) message that identifies the explicit server and lease offer that the client is accepting.
- The server then returns a DHCP acknowledgment (DHCPACK) message that acknowledges to the client that the lease has been finalized.
- If the offer is no longer valid, then the selected server responds with a DHCP negative acknowledgment (DHCPNAK) message and the process must begin with a new DHCPDISCOVER message.



Note: DHCPv6 has a set of messages that is similar to those for DHCPv4. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.

IP Addressing Services

Lab – Observe DNS Resolution

In this lab, you complete the following objectives:

- Observe the DNS Conversion of a URL to an IP Address
- Observe DNS Lookup Using the **nslookup** Command on a Web Site
- Observe DNS Lookup Using the **nslookup** Command on Mail Servers

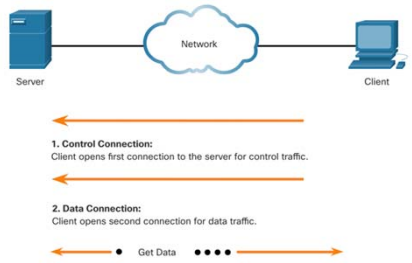
15.5 File Sharing Services

769

File Sharing Services

File Transfer Protocol

FTP was developed to allow for data transfers between a client and a server. An FTP client is an application which runs on a computer that is being used to push and pull data from an FTP server.



Step 1 - The client establishes the first connection to the server for control traffic using TCP port 21. The traffic consists of client commands and server replies.

Step 2 - The client establishes the second connection to the server for the actual data transfer using TCP port 20. This connection is created every time there is data to be transferred.

Step 3 - The data transfer can happen in either direction. The client can download (pull) data from the server, or the client can upload (push) data to the server.

770

File Sharing Services

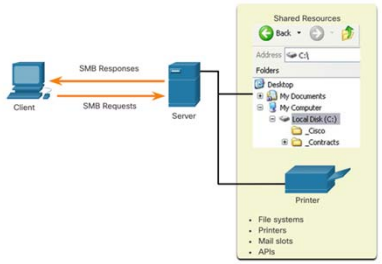
Server Message Block

The Server Message Block (SMB) is a client/server, request-response file sharing protocol. Servers can make their own resources available to clients on the network.

Three functions of SMB messages:

- Start, authenticate, and terminate sessions
- Control file and printer access
- Allow an application to send or receive messages to or from another device

Unlike the file sharing supported by FTP, clients establish a long-term connection to servers. After the connection is established, the user of the client can access the resources on the server as though the resource is local to the client host.



771

15.6 Module Practice and Quiz

772

Module Practice and Quiz

What did I learn in this module?

- Application layer protocols are used to exchange data between programs running on the source and destination hosts. The presentation layer has three primary functions: formatting, or presenting data, compressing data, and encrypting data for transmission and decrypting data upon receipt. The session layer creates and maintains dialogs between source and destination applications.
- In the client/server model, the device requesting the information is called a client and the device responding to the request is called a server.
- In a P2P network, two or more computers are connected via a network and can share resources without having a dedicated server.
- The three common HTTP message types are GET, POST, and PUT.
- Email supports three separate protocols for operation: SMTP, POP, and IMAP.
- DNS protocol matches resource names with the required numeric network address.
- DHCP for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.
- An FTP client is an application which runs on a computer that is being used to push and pull data from an FTP server.
- Three functions of SMB messages: start, authenticate, and terminate sessions, control file and printer access, and allow an application to send or receive messages to or from another device.

773

Module 15 : Application Layer

New Terms and Commands

• Application Layer	• IMAP
• Presentation Layer	• Domain Name Service (DNS)
• Session Layer	• Fully-Qualified Domain Names (FQDNs)
• Client-server model	• nslookup
• Peer-to-peer	• Dynamic Host Configuration Protocol (DHCP)
• Uniform Resource Locator (URL)	• DHCPDISCOVER
• Uniform Resource Identifiers (URI)	• DHCPOFFER
• HTTP/HTTPS	• DHCPREQUEST
• GET	• DHCPACK
• POST	• File Transfer Protocol (FTP)
• PUT	• Server Message Block (SMB)
• SMTP	
• POP	

774

Module 16: Network Security Fundamentals

Instructor Materials

Introduction to Networks v7.0 (ITN)

775

What to Expect in this Module

To facilitate learning, the following features within the GUI may be included in this module:

Feature	Description
Animations	Expose learners to new skills and concepts.
Videos	Expose learners to new skills and concepts.
Check Your Understanding(CYU)	Per topic online quiz to help learners gauge content understanding.
Interactive Activities	A variety of formats to help learners gauge content understanding.
Syntax Checker	Small simulations that expose learners to Cisco command line to practice configuration skills.
PT Activity	Simulation and modeling activities designed to explore, acquire, reinforce, and expand skills.

777

What to Expect in this Module (Cont.)

To facilitate learning, the following features may be included in this module:

Feature	Description
Hands-On Labs	Labs designed for working with physical equipment.
Class Activities	These are found on the Instructor Resources page. Class Activities are designed to facilitate learning, class discussion, and collaboration.
Module Quizzes	Self-assessments that integrate concepts and skills learned throughout the series of topics presented in the module.
Module Summary	Briefly recaps module content.

 778

778

784

Module Objectives

Module Title: Network Security Fundamentals

Module Objective: Configure switches and routers with device hardening features to enhance security.

Topic Title	Topic Objective
Security Threats and Vulnerabilities	Explain why basic security measure are necessary on network devices.
Network Attacks	Identify security vulnerabilities.
Network Attack Mitigation	Identify general mitigation techniques.
Device Security	Configure network devices with device hardening features to mitigate security threats.

 785

785

16.1 Security Threats and Vulnerabilities

 786

786

Security Threats and Vulnerabilities

Types of Threats

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 called threat actors.

After the threat actor gains access to the network, four types of threats may arise:

- Information Theft
- Data Loss and manipulation
- Identity Theft
- Disruption of Service

 787

787

Security Threats and Vulnerabilities

Types of Vulnerabilities

Vulnerability is the degree of weakness in a network or a device. Some degree of vulnerability is inherent in 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 Vulnerabilities might include TCP/IP Protocol weaknesses, Operating System Weaknesses, and Network Equipment weaknesses.
- Configuration Vulnerabilities might include unsecured user accounts, system accounts with easily guessed passwords, misconfigured internet services, unsecure default settings, and misconfigured network equipment.
- Security Policy Vulnerabilities might include lack of a written security policy, politics, lack of authentication continuity, logical access controls not applied, software and hardware installation and changes not following policy, and a nonexistent disaster recovery plan.

All three of these sources of vulnerabilities can leave a network or device open to various attacks, including malicious code attacks and network attacks.

 788

788

Security Threats and Vulnerabilities

Physical Security

If network resources can be physically compromised, a threat actor can deny the use of network resources. The four classes of physical threats are as follows:

- **Hardware threats -** This includes physical damage to servers, routers, switches, cabling plant, and workstations.
- **Environmental threats -** This includes temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry).
- **Electrical threats -** This includes voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss.
- **Maintenance threats -** This includes poor handling of key electrical components (electrostatic discharge), lack of critical spare parts, poor cabling, and poor labeling.

A good plan for physical security must be created and implemented to address these issues.

 789

789

16.2 Network Attacks

 790

790

Network Attacks
Types of Malware

Malware is short for malicious software. It is code or software specifically designed to damage, disrupt, steal, or inflict “bad” or illegitimate action on data, hosts, or networks. The following 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.
- **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.
- **Trojan Horses -** It is a harmful piece of software that looks legitimate. Unlike viruses and worms, Trojan horses do not reproduce by infecting other files. They self-replicate. Trojan horses must spread through user interaction such as opening an email attachment or downloading and running a file from the internet.

791

Network Attacks
Reconnaissance Attacks

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 three major categories:

- **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.

For reconnaissance attacks, external threat actors 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, a threat actor can then ping the publicly available IP addresses to identify the addresses that are active.

792

Network Attacks
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.

Access attacks can be classified into four types:

- **Password attacks -** Implemented using brute force, trojan horse, and packet sniffers
- **Trust exploitation -** A threat actor uses unauthorized privileges to gain access to a system, possibly compromising the target.
- **Port redirection**: - A threat actor uses a compromised system as a base for attacks against other targets. For example, a threat actor using SSH (port 22) to connect to a compromised host A. Host A is trusted by host B and, therefore, the threat actor can use Telnet (port 23) to access it.
- **Man-in-the middle -** The threat actor is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties.

793

Network Attacks
Denial of Service Attacks

Denial of service (DoS) attacks are the most publicized form of attack and among the most difficult to eliminate. However, 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. To help prevent DoS attacks it is important to stay up to date with the latest security updates for operating systems and applications.
- DoS attacks are a major risk because they interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled threat actor.
- A DDoS is similar to a DoS attack, but it originates from multiple, coordinated sources. For example, a threat actor builds a network of infected hosts, known as zombies. A network of zombies is called a botnet. The threat actor uses a command and control (CnC) program to instruct the botnet of zombies to carry out a DDoS attack.

794

Network Attacks
Lab – Research Network Security Threats

In this lab, you will complete the following objectives:

- Part 1: Explore the SANS Website
- Part 2: Identify Recent Network Security Threats
- Part 3: Detail a Specific Network Security Threat

795

16.3 Network Attack Mitigations

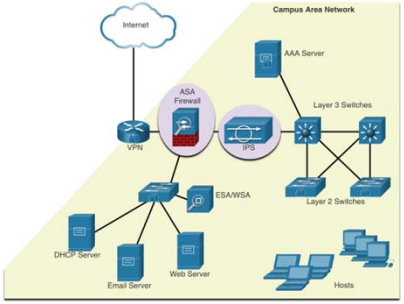
796

Network Attack Mitigations
The Defense-in-Depth Approach

To mitigate network attacks, you must first secure devices including routers, switches, servers, and hosts. Most organizations employ a defense-in-depth approach (also known as a layered approach) to security. This requires a combination of networking devices and services working in tandem.

Several security devices and services are implemented to protect an organization's users and assets against TCP/IP threats:

- VPN
- ASA Firewall
- IPS
- ESA/WSA
- AAA Server



797

Network Attack Mitigations
Keep Backups

Backing up device configurations and data is one of the most effective ways of protecting against data loss. Backups should be performed on a regular basis as identified in the security policy. Data backups are usually stored offsite to protect the backup media if anything happens to the main facility.

The table shows backup considerations and their descriptions.

Consideration	Description
Frequency	•Perform backups on a regular basis as identified in the security policy. •Full backups can be time-consuming, therefore perform monthly or weekly backups with frequent partial backups of changed files.
Storage	•Always validate backups to ensure the integrity of the data and validate the file restoration procedures.
Security	•Backups should be transported to an approved offsite storage location on a daily, weekly, or monthly rotation, as required by the security policy.
Validation	•Backups should be protected using strong passwords. The password is required to restore the data.

798

Network Attack Mitigations

Upgrade, Update, and Patch

As new malware is released, enterprises need to keep current with the latest versions of antivirus software.

- The most effective way to mitigate a worm attack is to download security updates from the operating system vendor and patch all vulnerable systems.
- One solution to the management of critical security patches is to make sure all end systems automatically download updates.

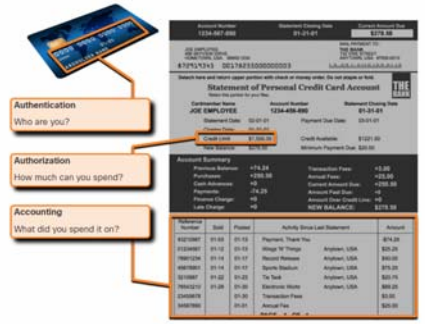
799

Network Attack Mitigations

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 network devices.

- AAA is a way to control who is permitted to access a network (authenticate), what actions they perform while accessing the network (authorize), and making a record of what was done while they are there (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.



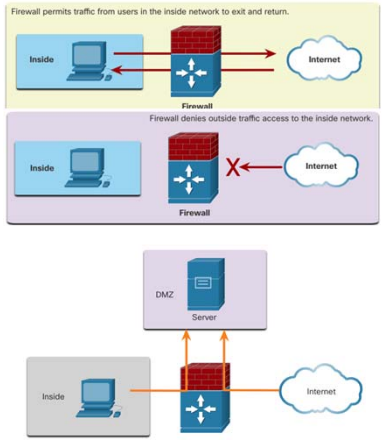
800

Network Attack Mitigations

Firewalls

Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access.

A firewall could allow outside users controlled access to specific services. For example, servers accessible to outside users are usually located on a special network referred to as the demilitarized zone (DMZ). The DMZ enables a network administrator to apply specific policies for hosts connected to that network.



801

Network Attack Mitigations

Types of Firewalls

Firewall products come packaged in various forms. These products use different techniques for determining what will be permitted or denied access to a network. They include the following:

- **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).

802

Network Attack Mitigations
Endpoint Security

An endpoint, or host, is an individual computer system or device that acts as a network client. Common endpoints 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.

 803

803

16.4 Device Security

 804

804

Device Security
Cisco AutoSecure

The security settings are set to the default values when a new operating system is installed on a device. In most cases, this level of security is inadequate. For Cisco routers, the Cisco AutoSecure feature can be used to assist securing the system.

In addition, there are some simple steps that should be taken that apply to most operating systems:

- 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.
- Often, devices shipped from the manufacturer have been sitting in a warehouse for a period of time and do not have the most up-to-date patches installed. It is important to update any software and install any security patches prior to implementation.

 805

805

Device Security
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 eight characters, preferably 10 or more characters.
- 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.
- Deliberately misspell a password. For example, Smith = Smyth = 5mYth or Security = 5ecur1ty.
- Change passwords often. If a password is unknowingly compromised, the window of opportunity for the threat actor to use the password is limited.
- Do not write passwords down and leave them in obvious places such as on the desk or monitor.

On Cisco routers, leading spaces are ignored for passwords, but spaces after the first character are not. Therefore, one method to create a strong password is to use the space bar and create a phrase made of many words. This is called a passphrase. A passphrase is often easier to remember than a simple password. It is also longer and harder to guess.

 806

806

Device Security
Additional Password Security

There are several steps that can be taken to help ensure that passwords remain secret on a Cisco router and switch including these:

- Encrypt all plaintext passwords with the **service password-encryption** command.
- Set a minimum acceptable password length with the **security passwords min-length** command.
- Deter brute-force password guessing attacks with the **login block-for # attempts # within #** command.
- Disable an inactive privileged EXEC mode access after a specified amount of time with the **exec-timeout** command.

```
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)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
Router#
```

 807

807

Device Security
Enable SSH

It is possible to configure a Cisco device to support SSH using the following steps:

1. **Configure a unique device hostname**. A device must have a unique hostname other than the default.
2. **Configure the IP domain name**. Configure the IP domain name of the network by using the global configuration mode command **ip-domain name**.
3. **Generate a key to encrypt SSH traffic**. SSH encrypts traffic between source and destination. However, to do so, a unique authentication key must be generated by using the global configuration command **crypto key generate rsa general-keys modulus** *bits*. The modulus *bits* determines the size of the key and can be configured from 360 bits to 2048 bits. The larger the bit value, the more secure the key. However, larger bit values also take longer to encrypt and decrypt information. The minimum recommended modulus length is 1024 bits.
4. **Verify or create a local database entry**. Create a local database username entry using the **username** global configuration command.
5. **Authenticate against the local database**. Use the **login local** line configuration command to authenticate the vty line against the local database.
6. **Enable vty inbound SSH sessions**. By default, no input session is allowed on vty lines. You can specify multiple input protocols including Telnet and SSH using the **transport input [ssh | telnet]** command.

 808

808

Device Security
Disable Unused Services

Cisco routers and switches start with a list of active services that may or may not be required in your network. Disable any unused services to preserve system resources, such as CPU cycles and RAM, and prevent threat actors from exploiting these services.

- The type of services that are on by default will vary depending on the IOS version. For example, IOS-XE typically will have only HTTPS and DHCP ports open. You can verify this with the **show ip ports all** command.
- IOS versions prior to IOS-XE use the **show control-plane host open-ports** command.

 809

809

Device Security
Packet Tracer – Configure Secure Passwords and SSH

In this Packet Tracer, you will configure passwords and SSH:

- The network administrator has asked you to prepare RTA and SW1 for deployment. Before they can be connected to the network, security measures must be enabled.

 810

810

Device Security

Lab – Configure Network Devices with SSH

In this lab, you will complete the following objectives:

- Part 1: Configure Basic Device Settings
- Part 2: Configure the Router for SSH Access
- Part 3: Configure the Switch for SSH Access
- Part 4: SSH from the CLI on the Switch

 811

811

16.5 Module Practice and Quiz

 812

812

Module Practice and Quiz

Packet Tracer – Secure Network Devices

In this activity you will configure a router and a switch based on a list of requirements.

 813

813

Module Practice and Quiz

Lab – Secure Network Devices

In this lab, you will complete the following objectives:

- Configure Basic Device Settings
- Configure Basic Security Measures on the Router
- Configure Basic Security Measures on the Switch

 814

814

Module Practice and Quiz

What Did I Learn In This Module?

- After the threat actor gains access to the network, four types of threats may arise: information theft, data loss and manipulation, identity theft, and disruption of service.
- There are three primary vulnerabilities or weaknesses: technological, configuration, and security policy.
- The four classes of physical threats are: hardware, environmental, electrical, and maintenance.
- Malware is short for malicious software. It is code or software 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.
- Network attacks can be classified into three major categories: reconnaissance, access, and denial of service.
- To mitigate network attacks, you must first secure devices including routers, switches, servers, and hosts. Most organizations employ a defense-in-depth approach to security. This requires a combination of networking devices and services working together.
- Several security devices and services are implemented to protect an organization’s users and assets against TCP/IP threats: VPN, ASA firewall, IPS, ESA/WSA, and AAA server.

 815

815

Module Practice and Quiz

What Did I Learn In This Module? (Cont.)

- Infrastructure devices should have backups of configuration files and IOS images on an FTP or similar file server. If the computer or a router hardware fails, the data or configuration can be restored using the backup copy.
- The most effective way to mitigate a worm attack is to download security updates from the operating system vendor and patch all vulnerable systems. To manage critical security patches, to make sure all end systems automatically download updates.
- 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).
- Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access.
- Securing endpoint devices is critical to network security. A company must have well-documented policies in place, which may include the use of antivirus software and host intrusion prevention. More comprehensive endpoint security solutions rely on network access control.

 816

816

Module Practice and Quiz

What Did I Learn In This Module? (Cont.)

- For Cisco routers, the Cisco AutoSecure feature can be used to assist securing the system. For most OSs 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, and any unnecessary services and applications should be turned off and uninstalled when possible.
- To protect network devices, it is important to use strong passwords. A passphrase is often easier to remember than a simple password. It is also longer and harder to guess.
- For routers and switches, encrypt all plaintext passwords, setting a minimum acceptable password length, deter brute-force password guessing attacks, and disable an inactive privileged EXEC mode access after a specified amount of time.
- Configure appropriate devices to support SSH, and disable unused services.

 817

817

Module 16: Network Security Fundamentals

New Terms and Commands

- threat actor
- malware
- reconnaissance attacks
- access attacks
- defense-in-depth
- authentication, authorization, and accounting (AAA)
- demilitarized zone (DMZ)
- Cisco AutoSecure
- passphrase

- **service password-encryption**
- **security passwords min-length**
- **login block-for**
- **exec-timeout**
- **crypto key generate rsa general-keys modulus**
- **username password | secret**
- **login local**
- **transport input ssh**
- **show ip ports all**
- **show control-plan host open-ports**

 818

818

Module 17: Build a Small Network

Instructor Materials

Introduction to Networks v7.0
(ITN)

819

Module 17: Build a Small Network

Introduction to Networks v7.0
(ITN)

830

Module Objectives

Module Title: Build a Small Network

Module Objective: Implement a network design for a small network to include a router, a switch, and end devices.

Topic Title	Topic Objective
Devices in a Small Network	Identify the devices used in a small network.
Small Network Applications and Protocols	Identify the protocols and applications used in a small network.
Scale to Larger Networks	Explain how a small network serves as the basis of larger networks.
Verify Connectivity	Use the output of the ping and tracert commands to verify connectivity and establish relative network performance.
Host and IOS Commands	Use host and IOS commands to acquire information about the devices in a network.
Troubleshooting Methodologies	Describe common network troubleshooting methodologies.
Troubleshooting Scenarios	Troubleshoot issues with devices in the network.

 831

831

17.1 Devices in a Small Network

 832

832

Devices in a Small Network

Small Network Topologies

- The majority of businesses are small most of the business networks are also small.
- A small network design is usually simple.
- Small networks typically have a single WAN connection provided by DSL, cable, or an Ethernet connection.
- Large networks require an IT department to maintain, secure, and troubleshoot network devices and to protect organizational data. Small networks are managed by a local IT technician or by a contracted professional.

 833

833

Devices in a Small Network

Device Selection for a Small Network

Like large networks, small networks require planning and design to meet user requirements. Planning ensures that all requirements, cost factors, and deployment options are given due consideration. One of the first design considerations is the type of intermediary devices to use to support the network.

Factors that must be considered when selecting network devices include:

- cost
- speed and types of ports/interfaces
- expandability
- operating system features and services

 834

834

Devices in a Small Network

IP Addressing for a Small Network

When implementing a network, create an IP addressing scheme and use it. All hosts and devices within an internetwork must have a unique address. Devices that will factor into the IP addressing scheme include the following:

- End user devices - The number and type of connections (i.e., wired, wireless, remote access)
- Servers and peripherals devices (e.g., printers and security cameras)
- Intermediary devices including switches and access points

It is recommended that you plan, document, and maintain an IP addressing scheme based on device type. The use of a planned IP addressing scheme makes it easier to identify a type of device and to troubleshoot problems.

 835

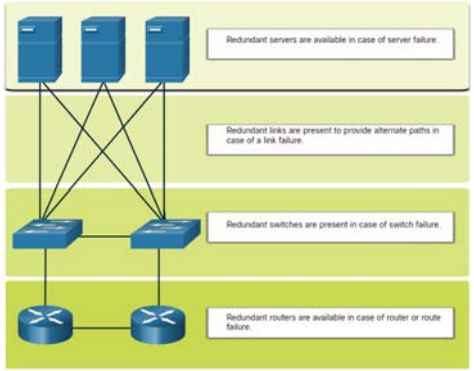
835

Devices in a Small Network

Redundancy in a Small Network

In order to maintain a high degree of reliability, *redundancy* is required in the network design. Redundancy helps to eliminate single points of failure.

Redundancy can be accomplished by installing duplicate equipment. It can also be accomplished by supplying duplicate network links for critical areas.

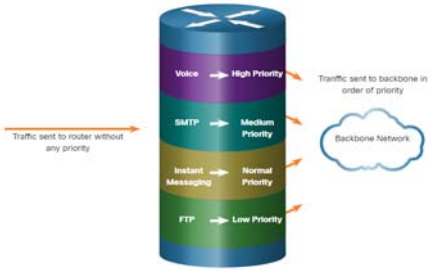


 836

836

Devices in a Small Network
Traffic Management

- The goal for a good network design is to enhance the productivity of the employees and minimize network downtime.
- The routers and switches in a small network should be configured to support real-time traffic, such as voice and video, in an appropriate manner relative to other data traffic. A good network design will implement quality of service (QoS).
- Priority queuing has four queues. The high-priority queue is always emptied first.



837

17.2 Small Network Applications and Protocols

838

Small Network Applications and Protocols
Common Applications

After you have set it up, your network still needs certain types of applications and protocols in order to work. The network is only as useful as the applications that are on it.

There are two forms of software programs or processes that provide access to the network:

- **Network Applications**: Applications that implement application layer protocols and are able to communicate directly with the lower layers of the protocol stack.
- **Application Layer Services**: For applications that are not network-aware, the programs that interface with the network and prepare the data for transfer.

839

Small Network Applications and Protocols
Common Protocols

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

- Network administrators commonly require access to network devices and servers. The two most common remote access solutions are Telnet and Secure Shell (SSH).
- Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTP) are used between web clients and web servers.
- Simple Mail Transfer Protocol (SMTP) is used to send email, Post Office Protocol (POP3) or Internet Mail Access Protocol (IMAP) are used by clients to retrieve email.
- File Transfer Protocol (FTP) and Security File Transfer Protocol (SFTP) are used to download and upload files between a client and an FTP server.
- Dynamic Host Configuration Protocol (DHCP) is used by clients to acquire an IP configuration from a DHCP Server.
- The Domain Name Service (DNS) resolves domain names to IP addresses.

Note: A server could provide multiple network services. For instance, a server could be an email, FTP and SSH server.

840

Small Network Applications and Protocols

Common Protocols (Cont.)

These network protocols comprise the fundamental toolset of a network professional, defining:

- 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.

Many companies have established a policy of using secure versions (e.g., SSH, SFTP, and HTTPS) of these protocols whenever possible.

 841

841

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, as well as enabling their employees to work remotely.
- The network administrator must ensure the proper equipment is installed in the network and that the network devices are configured to ensure priority delivery.
- The factors that a small network administrator must consider when supporting real-time applications:
  - **Infrastructure -** Does it have the capacity and capability to support real-time applications?
  - **VoIP -** VoIP is typically less expensive than IP Telephony, but at the cost of quality and features.
  - **IP Telephony -** This employs dedicated servers form call control and signaling.
  - **Real-Time Applications -** The network must support Quality of Service (QoS) mechanisms to minimize latency issues. Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP) and two protocols that support real-time applications.

 842

842

17.3 Scale to Larger Networks

 843

843

Scale to Larger Networks

Small Network Growth

Growth is a natural process for many small businesses, and their networks must grow accordingly. Ideally, the network administrator has enough lead-time to make intelligent decisions about growing the network in alignment with the growth of the company.

To scale a network, several elements 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 and their respective traffic requirements should be documented

These elements are used to inform the decision-making that accompanies the scaling of a small network.

 844

844

Scale to Larger Networks

Protocol Analysis

It is important to understand the type of traffic that is crossing the network as well as the current traffic flow. There are several network management tools that can be used for this purpose.

To determine traffic flow patterns, it is important to do the following:

- Capture traffic during peak utilization times to get a good representation of the different traffic types.
- Perform the capture on different network segments and devices as some traffic will be local to a particular segment.
- 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 to make decisions on how to manage the traffic more efficiently.

 845

845

Scale to Larger Networks

Employee Network Utilization

Many operating systems provide built-in tools to display such network utilization information. These tools can be used to capture a “snapshot” of information such as the following:

- OS and OS Version
- CPU utilization
- RAM utilization
- Drive utilization
- Non-Network applications
- Network applications

Documenting snapshots for employees in a small network over a period of time is very useful to identify evolving protocol requirements and associated traffic flows.

 846

846

17.4 Verify Connectivity

 847

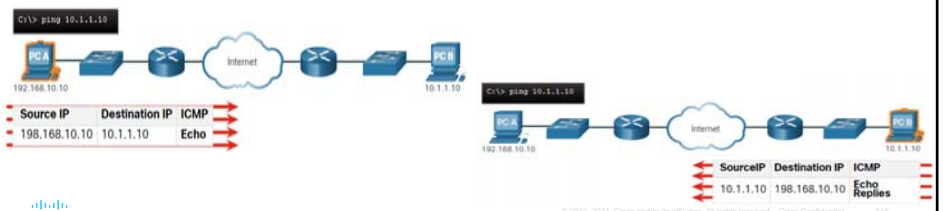
847

Verify Connectivity

Verify Connectivity with Ping

Whether your network is small and new, or you are scaling an existing network, you will always want to be able to verify that your components are properly connected to each other and to the internet.

- The ping command, available on most operating systems, is the most effective way to quickly test Layer 3 connectivity between a source and destination IP address.
- The ping command uses the Internet Control Message Protocol (ICMP) echo (ICMP Type 8) and echo reply (ICMP Type 0) messages.



 848

848

Verify Connectivity

Verify Connectivity with Ping (Cont.)

On a Windows 10 host, the ping command sends four consecutive ICMP echo messages and expects four consecutive ICMP echo replies from the destination. The IOS ping sends five ICMP echo messages and displays an indicator for each ICMP echo reply received.

IOS Ping Indicators are as follows:

Element	Description
!	•Exclamation mark indicates successful receipt of an echo reply message. •It validates a Layer 3 connection between source and destination.
.	•A period means that time expired waiting for an echo reply message. •This indicates a connectivity problem occurred somewhere along the path.
U	•Uppercase **U** indicates a router along the path responded with an ICMP Type 3 "destination unreachable" error message. •Possible reasons include the router does not know the direction to the destination network or it could not find the host on the destination network.

Note: Other possible ping replies include Q, M, ?, or &. However, the meaning of these are out of scope for this module.

Verify Connectivity

Extended Ping

The Cisco IOS offers an "extended" mode of the **ping** command.

Extended ping is entered in privileged EXEC mode by typing **ping** without a destination IP address. You will then be given several prompts to customize the extended **ping**.

Note: Pressing **Enter** accepts the indicated default values. The **ping ipv6** command is used for IPv6 extended pings.

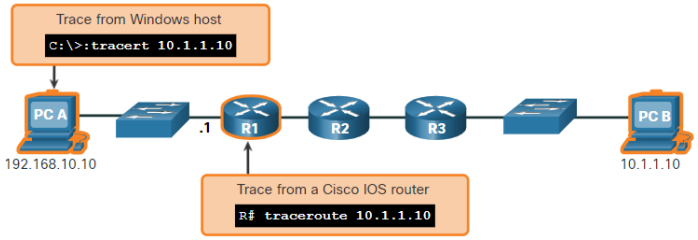
```
R1# ping
Protocol [ip]:
Target IP address: 10.1.1.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Ingress ping [n]:
Source address or interface: 192.168.10.1
DSCP Value [0]:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0x0000ABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```


Verify Connectivity

Verify Connectivity with Traceroute

The ping command is useful to quickly determine if there is a Layer 3 connectivity problem. However, it does not identify where the problem is located along the path.

- Traceroute can help locate Layer 3 problem areas in a network. A trace returns a list of hops as a packet is routed through a network.
- The syntax of the trace command varies between operating systems.



Verify Connectivity

Verify Connectivity with Traceroute (Cont.)

- The following is a sample output of **tracert** command on a Windows 10 host.

  Note: Use **Ctrl-C** to interrupt a **tracert** in Windows.
- The only successful response was from the gateway on R1. Trace requests to the next hop timed out as indicated by the asterisk (*), meaning that the next hop router did not respond or there is a failure in the network path. In this example there appears to be a problem between R1 and R2.

```
C:\Users\PC-A> tracert 10.1.1.10
Tracing route to 10.1.1.10 over a maximum of 30 hops:
  1     2 ms     2 ms     2 ms  192.168.10.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
^C
C:\Users\PC-A>
```


Verify Connectivity

Verify Connectivity with Traceroute (Cont.)

The following are sample outputs of traceroute command from R1:

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3 10.1.1.10 1 msec 0 msec
R1#
```

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3 *  *  *
  4 *  *  *
  5 *
```

- On the left, the trace validated that it could successfully reach PC B.
- On the right, the 10.1.1.10 host was not available, and the output shows asterisks where replies timed out. Timeouts indicate a potential network problem.
- Use **Ctrl-Shift-6** to interrupt a **traceroute** in Cisco IOS.

Note: Windows implementation of traceroute (tracert) sends ICMP Echo Requests. Cisco IOS and Linux use UDP with an invalid port number. The final destination will return an ICMP port unreachable message.

853

Verify Connectivity

Extended Traceroute

Like the extended **ping** command, there is also an extended **traceroute** command. It allows the administrator to adjust parameters related to the command operation.

The Windows **tracert** command allows the input of several parameters through options in the command line. However, it is not guided like the extended traceroute IOS command. The following output displays the available options for the Windows **tracert** command:

```
C:\Users\PC-A> tracert /?
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name
Options:
    -d                  Do not resolve addresses to hostnames.
    -h maximum_hops     Maximum number of hops to search for target.
    -j host-list        Loose source route along host-list (IPv4-only).
    -w timeout          Wait timeout milliseconds for each reply.
    -R                  Trace round-trip path (IPv6-only).
    -S srcaddr          Source address to use (IPv6-only).
    -4                  Force using IPv4.
    -6                  Force using IPv6.
C:\Users\PC-A>
```


854

Verify Connectivity

Extended Traceroute (Cont.)

- The Cisco IOS extended **traceroute** option enables the user to create a special type of trace by adjusting parameters related to the command operation.
- Extended traceroute is entered in privileged EXEC mode by typing **traceroute** without a destination IP address. IOS will guide you through the command options by presenting a number of prompts related to the setting of all the different parameters.
- **Note**: Pressing **Enter** accepts the indicated default values.

```
R1# traceroute
Protocol [ip]:
Target IP address: 10.1.1.10
Ingress traceroute [n]:
Source address: 192.168.10.1
DSCP Value [0]:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.10.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 1 msec 1 msec
  2 209.165.200.230 0 msec 1 msec 0 msec
  3 *
    10.1.1.10 2 msec 2 msec
R1#
```


855

Verify Connectivity

Network Baseline

- One of the most effective tools for monitoring and troubleshooting network performance is to establish a network baseline.
- One method for starting a baseline is to copy and paste the results from an executed ping, trace, or other relevant commands into a text file. These text files can be time stamped with the date and saved into an archive for later retrieval and comparison.
- Among items to consider are error messages and the response times from host to host.
- Corporate networks should have extensive baselines; more extensive than we can describe in this course. Professional-grade software tools are available for storing and maintaining baseline information.

856

Verify Connectivity

Lab – Test Network Latency with Ping and Traceroute

In this lab, you will complete the following objectives:

- Part 1: Use Ping to Document Network Latency
- Part 2: Use Traceroute to Document Network Latency

857

17.5 Host and IOS Commands

858

Host and IOS Commands

IP Configuration on a Windows Host

In Windows 10, you can access the IP address details from the **Network and Sharing Center** to quickly view the four important settings: address, mask, router, and DNS. Or you can issue the **ipconfig** command at the command line of a Windows computer.

- Use the **ipconfig /all** command to view the MAC address, as well as a number of details regarding the Layer 3 addressing of the device.
- If a host is configured as a DHCP client, the IP address configuration can be renewed using the **ipconfig /release** and **ipconfig /renew** commands.
- The DNS Client service on Windows PCs also optimizes the performance of DNS name resolution by storing previously resolved names in memory. The **ipconfig /displaydns** command displays all of the cached DNS entries on a Windows computer system.

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```


859

Host and IOS Commands

IP Configuration on a Linux Host

- Verifying IP settings using the GUI on a Linux machine will differ depending on the Linux distribution and desktop interface.
- On the command line, use the **ifconfig** command to display the status of the currently active interfaces and their IP configuration.
- The Linux **ip address** command is used to display addresses and their properties. It can also be used to add or delete IP addresses.

```
[analyst@secOps ~]$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:b5:d6:cb
          inet addr: 10.0.2.15  Bcast:10.0.2.255  Mask: 255.255.255.0
          inet6 addr: fe80::57c6:ed95:b3c9:2951/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1332239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105910 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1855455014 (1.8 GB)  TX bytes:13140139 (13.1 MB)
lo: flags=73  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Note: The output displayed may vary depending on the Linux distribution.

860

Host and IOS Commands

IP Configuration on a macOS Host

- In the GUI of a Mac host, open **Network Preferences > Advanced** to get the IP addressing information.
- The **ifconfig** command can also be used to verify the interface IP configuration at the command line.
- Other useful macOS commands to verify the host IP settings include **networksetup -listallnetworkservices** and the **networksetup -getinfo <***network service***>**.

```
MacBook-Air:~ Admin$ networksetup -listallnetworkservices
An asterisk (*) denotes that a network service is disabled.
iPhone USB
Wi-Fi
Bluetooth PAN
Thunderbolt Bridge
MacBook-Air:~ Admin$
MacBook-Air:~ Admin$ networksetup -getinfo Wi-Fi
DHCP Configuration
IP address: 10.10.10.113
Subnet mask: 255.255.255.0
Router: 10.10.10.1
Client ID:
IPv6: Automatic
IPv6 IP address: none
IPv6 Router: none
Wi-Fi ID: c4:b3:01:a0:64:98
MacBook-Air:~ Admin$
```


861

Host and IOS Commands

The arp Command

The **arp** command is executed from the Windows, Linux, or Mac command prompt. The command lists all devices currently in the ARP cache of the host.

- The **arp -a** command displays the known IP address and MAC address binding. The ARP cache only displays 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.
- The cache can be cleared by using the **netsh interface ip delete arpcache** command in the event the network administrator wants to repopulate the cache with updated information.

Note: You may need administrator access on the host to be able to use the **netsh interface ip delete arpcache** command.

862

Host and IOS Commands

Common show Commands Revisited

Command	Description
show running-config	Verifies the current configuration and settings
show interfaces	Verifies the interface status and displays any error messages
show ip interface	Verifies the Layer 3 information of an interface
show arp	Verifies the list of known hosts on the local Ethernet LANs
show ip route	Verifies the Layer 3 routing information
show protocols	Verifies which protocols are operational
show version	Verifies the memory, interfaces, and licenses of the device

863

Host and IOS Commands

The show cdp neighbors Command

CDP provides the following information about each CDP neighbor device:

- **Device identifiers** - The configured host name of a switch, router, or other device
- **Address list** - Up to one network layer address for each protocol supported
- **Port identifier** - The name of the local and remote port in the form of an ASCII character string, such as FastEthernet 0/0
- **Capabilities list** - Whether a specific device is a Layer 2 switch or a Layer 3 switch
- **Platform** - The hardware platform of the device.

The **show cdp neighbors detail** command reveals the IP address of a neighboring 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,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S3               Gig 0/0/1         122             S I   WS-C2960+ Fas 0/5
Total cdp entries displayed : 1
R3#
```


864

Host and IOS Commands

The show ip interface brief Command

One of the most frequently used commands is the **show ip interface brief** command. This command provides a more abbreviated output than the **show ip interface** command. It provides a summary of the key information for all the network interfaces on a router.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.254.250 YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  up                    up
```


865

Host and IOS Commands

Video – The show version Command

This video will demonstrate using the show version command to view information about the router.

866

Host and IOS Commands

Packet Tracer – Interpret show Command Output

This activity is designed to reinforce the use of router **show** commands. You are not required to configure, but rather analyze the output of several show commands.

867

17.6 Troubleshooting Methodologies

868

Troubleshooting Methodologies

Basic Troubleshooting Approaches

Step	Description
Step 1. Identify the Problem	•This is the first step in the troubleshooting process. •Although tools can be used in this step, a conversation with the user is often very helpful.
Step 2. Establish a Theory of Probable Causes	•After the problem is identified, try to establish a theory of probable causes. •This step often yields more than a few probable causes to the problem.
Step 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 may apply a quick fix to test and see if it solves the problem. •If a quick fix does not correct the problem, you might need to research the problem further to establish the exact cause.
Step 4. Establish a Plan of Action 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.
Step 5. Verify Solution and Implement Preventive Measures	•After you have corrected the problem, verify full functionality. •If applicable, implement preventive measures.
Step 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.

869

Troubleshooting Methodologies

Resolve or Escalate?

- In some situations, it may not be possible to resolve the problem immediately. A problem should be escalated when it requires a manager decision, some specific expertise, or network access level unavailable to the troubleshooting technician.
- A company policy should clearly state when and how a technician should escalate a problem.

870

Troubleshooting Methodologies

The debug Command

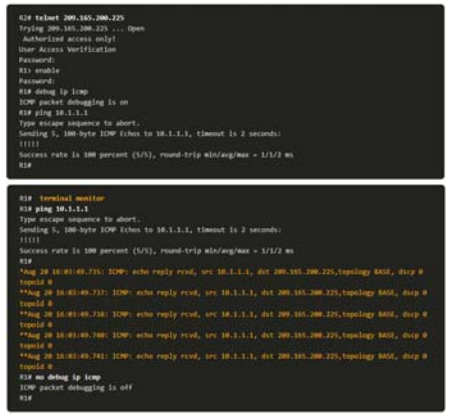
- The IOS **debug** command allows the administrator to display OS process, protocol, mechanism and event messages in real-time for analysis.
- All **debug** commands are entered in privileged EXEC mode. The Cisco IOS allows for narrowing the output of **debug** to include only the relevant feature or subfeature. Use **debug** commands only to troubleshoot specific problems.
  - To list a brief description of all the debugging command options, use the **debug ?** command in privileged EXEC mode at the command line.
  - To turn off a specific debugging feature, add the **no** keyword in front of the **debug** command
  - Alternatively, you can enter the **undebug** form of the command in privileged EXEC mode.
  - To turn off all active debug commands at once, use the **undebug all** command.
- Be cautious using some **debug** commands, as they may generate a substantial amount of output and use a large portion of system resources. The router could get so busy displaying **debug** messages that it would not have enough processing power to perform its network functions, or even listen to commands to turn off debugging.

871

Troubleshooting Methodologies

The terminal monitor Command

- **debug** and certain other IOS message output is not automatically displayed on remote connections. This is because log messages are prevented from being displayed on vty lines.
- To display log messages on a terminal (virtual console), use the **terminal monitor** privileged EXEC command. To stop logging messages on a terminal, use the **terminal no monitor** privileged EXEC command.



872

17.7 Troubleshooting Scenarios

873

Troubleshooting Scenarios
Duplex Operation and Mismatch Issues

- Interconnecting Ethernet interfaces must operate in the same duplex mode for best communication performance and to avoid inefficiency and latency on the link.
- The Ethernet autonegotiation feature facilitates configuration, minimizes problems and maximizes link performance between two interconnecting Ethernet links. The connected devices first announce their supported capabilities and then choose the highest performance mode supported by both ends.
- If one of the two connected devices is operating in full-duplex and the other is operating in half-duplex, a duplex mismatch occurs. While data communication will occur through a link with a duplex mismatch, link performance will be very poor.
- Duplex mismatches are typically caused by a misconfigured interface or in rare instances by a failed autonegotiation. Duplex mismatches may be difficult to troubleshoot as the communication between devices still occurs.

874

Troubleshooting Scenarios
IP Addressing Issues on IOS Devices

- Two common causes of incorrect IPv4 assignment are manual assignment mistakes or DHCP-related issues.
- Network administrators often have to manually assign IP addresses to devices such as servers and routers. If a mistake is made during the assignment, then communications issues with the device are very likely to occur.
- On an IOS device, use the **show ip interface** or **show ip interface brief** commands to verify what IPv4 addresses are assigned to the network interfaces. For example, issuing the **show ip interface brief** command as shown would validate the interface status on R1.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```


875

Troubleshooting Scenarios
IP Addressing Issues on End Devices

- On Windows-based machines, when the device cannot contact a DHCP server, Windows will automatically assign an address belonging to the 169.254.0.0/16 range. This feature is called Automatic Private IP Addressing (APIPA).
- A computer with an APIPA address will not be able to communicate with other devices in the network because those devices will most likely not belong to the 169.254.0.0/16 network.
  - **Note**: Other operating systems, such Linux and OS X, do not use APIPA.
- If the device is unable to communicate with the DHCP server, then the server cannot assign an IPv4 address for the specific network and the device will not be able to communicate.
- To verify the IP addresses assigned to a Windows-based computer, use the **ipconfig** command.

876

Troubleshooting Scenarios

Default Gateway Issues

- The default gateway for an end device is the closest networking device, belonging to the same network as the end device, that can forward traffic to other networks. If a device has an incorrect or nonexistent default gateway address, it will not be able to communicate with devices in remote networks.
- Similar to IPv4 addressing issues, default gateway problems can be related to misconfiguration (in the case of manual assignment) or DHCP problems (if automatic assignment is in use).
- To verify the default gateway on Windows-based computers, use the **ipconfig** command.
- On a router, use the **show ip route** command to list the routing table and verify that the default gateway, known as a default route, has been set. This route is used when the destination address of the packet does not match any other routes in its routing table.

 877

877

Troubleshooting Scenarios

Troubleshooting DNS Issues

- It is common for users to mistakenly relate the operation of an internet link to the availability of the DNS.
- DNS server addresses can be manually or automatically assigned via DHCP.
- Although it is common for companies and organizations to manage their own DNS servers, any reachable DNS server can be used to resolve names.
- Cisco offers OpenDNS which provides secure DNS service by filtering phishing and some malware sites. OpenDNS addresses are 208.67.222.222 and 208.67.220.220. Advanced features such as web content filtering and security are available to families and businesses.
- Use the **ipconfig /all** as shown to verify which DNS server is in use by the Windows computer.
- The **nslookup** command is another useful DNS troubleshooting tool for PCs. With **nslookup** a user can manually place DNS queries and analyze the DNS response.

 878

878

Troubleshooting Scenarios

Packet Tracer – Troubleshoot Connectivity Issues

The objective of this Packet Tracer activity is to troubleshoot and resolve connectivity issues, if possible. Otherwise, the issues should be clearly documented and so they can be escalated.

 879

879

Troubleshooting Scenarios

Packet Tracer – Troubleshoot Connectivity Issues – Physical Mode
Lab - Troubleshoot Connectivity Issues

In this Packet Tracer Physical Mode activity and in the Lab, you will complete the following objectives:

- Identify the Problem
- Implement Network Changes
- Verify Full Functionality
- Document Findings and Configuration Changes

 880

880

17.8 Module Practice and Quiz

881

Troubleshooting Scenarios

Packet Tracer – Design and Build a Small Business Network – Physical Mode
Lab – Design and Build a Small Business Network

In this Packet Tracer Physical Mode activity and in the Lab, you will complete the following objectives:

- Design and build a network
- Explain how a small network of directly connected segments is created, configured, and verified

882

Troubleshooting Scenarios

Packet Tracer – Skills Integration Challenge

In this Packet Tracer activity, you will use all the skills you have acquired over throughout this course.

Scenario:

The router Central, ISP cluster, and the Web server are completely configured. You must create a new IPv4 addressing scheme that will accommodate 4 subnets using the 192.168.0.0/24 network. The IT department requires 25 hosts. The Sales department needs 50 hosts. The subnet for the rest of the staff requires 100 hosts. A Guest subnet will be added in the future to accommodate 25 hosts. You must also finish the basic security settings and interface configurations on R1. Then, you will configure the SVI interface and basic security settings on switches S1, S2, and S3.

883

Troubleshooting Scenarios

Packet Tracer – Troubleshooting Challenge

In this Packet Tracer activity, you will troubleshoot and resolve a number of issues in an existing LAN.

884

Module Practice and Quiz

What Did I Learn In This Module?

- Factors to consider when selecting network devices for a small network are cost, speed and types of ports/interfaces, expandability, and OS features and services.
- When implementing a network, create an IP addressing scheme and use it on end devices, servers and peripherals, and intermediary devices.
- Redundancy can be accomplished by installing duplicate equipment, but it can also be accomplished by supplying duplicate network links for critical areas.
- The routers and switches in a small network should be configured to support real-time traffic, such as voice and video, in an appropriate manner relative to other data traffic.
- There are two forms of software programs or processes that provide access to the network: network applications and application layer services.
- To scale a network, several elements are required: network documentation, device inventory, budget, and traffic analysis.
- The ping command is the most effective way to quickly test Layer 3 connectivity between a source and destination IP address.
- The Cisco IOS offers an "extended" mode of the ping command which lets the user create special types of pings by adjusting parameters related to the command operation.

Module Practice and Quiz

What Did I Learn In This Module (Cont.)?

- A trace returns a list of hops as a packet is routed through a network.
- There is also an extended traceroute command. It allows the administrator to adjust parameters related to the command operation.
- Network administrators view the IP addressing information (address, mask, router, and DNS) on a Windows host by issuing the ipconfig command. Other necessary commands are **ipconfig /all**, **ipconfig /release** and **ipconfig /renew**, and **ipconfig /displaydns**.
- Verifying IP settings by using the GUI on a Linux machine will differ depending on the Linux distribution (distro) and desktop interface. Necessary commands are ifconfig, and ip address.
- In the GUI of a Mac host, open Network Preferences > Advanced to get the IP addressing information. Other IP addressing commands for Mac are ifconfig, and networksetup -listallnetworkservices and networksetup -getinfo <network service>.
- The **arp** command is executed from the Windows, Linux, or Mac command prompt. The 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 **arp -a** command displays the known IP address and MAC address binding.

Module Practice and Quiz

What Did I Learn In This Module (Cont.)?

- Common show commands are **show running-config**, **show interfaces**, **show ip address**, **show arp**, **show ip route**, **show protocols**, and **show version**. The **show cdp neighbor** command 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 help determine if one of the CDP neighbors has an IP configuration error.
- The **show ip interface brief** command output displays all interfaces on the router, the IP address assigned to each interface, if any, and the operational status of the interface.
- The six basic steps to troubleshooting Step 1. Identify the problem Step 2. Establish a theory of probably causes. Step 3. Test the theory to determine the cause. Step 4. Establish a plan of action and implement the solution. Step 5. Verify the solution and implement preventive measures. Step 6. Document findings, actions, and outcomes.
- A problem should be escalated when it requires a decision of a manager, some specific expertise, or network access level unavailable to the troubleshooting technician.
- OS processes, protocols, mechanisms and events generate messages to communicate their status. The IOS debug command allows the administrator to display these messages in real-time for analysis.
- To display log messages on a terminal (virtual console), use the terminal monitor privileged EXEC command.

Module 17: Build a Small Network

New Terms and Commands

- network applications
- application layer services
- extended ping
- extended traceroute
- network Baseline
- **ifconfig**
- **netsh interface ip delete arpcache**
- scientific method
- **debug**
- **terminal monitor**

889