

CCNA v7 Study Guide - Complete Chapter Summaries

Introduction to Networks Companion Guide

Created for: Ivan's CCNA Certification Study

Source: CCNAv7 Introduction to Networks Companion Guide

Focus: Essential terminology, concepts, and IOS commands

Chapter 1: Networking Today

Key Terminology

Network Types:

- **LAN** (Local Area Network) - Small geographic area, single organization
- **WAN** (Wide Area Network) - Large geographic area, multiple locations
- **MAN** (Metropolitan Area Network) - City-wide network
- **WLAN** (Wireless LAN) - Wireless local network
- **SAN** (Storage Area Network) - Dedicated high-speed network for storage
- **Intranet** - Private network accessible only to organization members
- **Extranet** - Controlled access to portions of network for external users
- **Internet** - Global network of interconnected networks

Network Components:

- **End Devices** - Computers, printers, phones, cameras, servers
- **Intermediary Devices** - Routers, switches, wireless access points, firewalls
- **Network Media** - Copper cables, fiber-optic cables, wireless
- **NIC** (Network Interface Card) - Physical connection to network
- **Physical Port** - Connector where media connects
- **Interface** - Specialized port on networking device

Network Representations:

- **Topology Diagram** - Visual representation of network layout
- **Physical Topology** - Physical connections and locations
- **Logical Topology** - Shows logical paths and data flows

Network Characteristics:

- **Fault Tolerance** - Network continues operating despite failures
- **Scalability** - Network can expand to support new users/applications
- **QoS** (Quality of Service) - Prioritizes time-sensitive traffic
- **Security** - Protects network infrastructure and data

Network Trends:

- **BYOD** (Bring Your Own Device) - Personal devices on corporate network
- **Online Collaboration** - Web-based tools for remote collaboration
- **Video Communications** - Video calls, conferencing, live streaming
- **Cloud Computing** - Applications and storage on internet servers
- **IoT** (Internet of Things) - Connected devices and sensors
- **Smart Home Technology** - Automated home systems

Connection Types:

- **DSL** (Digital Subscriber Line) - High-speed over phone lines
- **Cable** - High-speed over cable TV infrastructure
- **Cellular** - Wireless using cell towers
- **Satellite** - Wireless using satellites
- **Dial-up** - Low-speed over phone lines (legacy)

Security Threats:

- **Virus** - Malicious code that replicates
- **Worm** - Self-replicating malware
- **Trojan Horse** - Malware disguised as legitimate
- **Spyware** - Gathers information without consent
- **DoS** (Denial of Service) - Overwhelms network resources
- **DDoS** (Distributed DoS) - Attack from multiple sources
- **Data Interception** - Capturing data in transit
- **Identity Theft** - Stealing personal information

Security Solutions:

- **Antivirus/Antimalware** - Detects and removes malicious software

- **Firewall** - Filters network traffic
- **ACL** (Access Control List) - Filters traffic based on criteria
- **IPS** (Intrusion Prevention System) - Actively blocks threats
- **VPN** (Virtual Private Network) - Encrypted connection over public network

Essential Concepts

1. Network Reliability Factors:

- Fault tolerance through redundancy
- Scalability for growth
- Quality of Service for prioritization
- Security at all levels

2. Common Network Architectures:

- Client-Server: Centralized services and data
- Peer-to-Peer: Decentralized, devices as both client and server

3. IT Professional Roles:

- Network Administrator
- Network Architect
- Network Security Specialist
- Network Operations Center (NOC) Technician

IOS Commands (None for this chapter - conceptual overview)

Chapter 2: Basic Switch and End Device Configuration

Key Terminology

IOS Modes:

- **User EXEC Mode** - Limited examination commands (prompt: `>`)
- **Privileged EXEC Mode** - Detailed examination, testing, file management (prompt: `#`)
- **Global Configuration Mode** - Device configuration (prompt: `(config)#`)
- **Line Configuration Mode** - Console, SSH, Telnet configuration
- **Interface Configuration Mode** - Specific interface settings

Configuration Types:

- **Running Configuration (running-config)** - Active config in RAM
- **Startup Configuration (startup-config)** - Saved config in NVRAM
- **NVRAM** (Non-Volatile RAM) - Retains config after power off
- **Flash Memory** - Stores IOS and other files
- **ROM** (Read-Only Memory) - POST and bootstrap program

Access Methods:

- **Console** - Physical connection via console cable
- **SSH** (Secure Shell) - Encrypted remote access
- **Telnet** - Unencrypted remote access (insecure)
- **AUX Port** - Legacy dial-up remote access

Addressing:

- **IPv4 Address** - 32-bit logical address (e.g., 192.168.1.1)
- **Subnet Mask** - Defines network/host portions
- **Default Gateway** - Router interface for reaching other networks
- **DHCP** (Dynamic Host Configuration Protocol) - Automatic IP assignment
- **Static IP** - Manually configured IP address

Essential IOS Commands

Navigation:

enable	# Enter privileged EXEC mode
disable	# Return to user EXEC mode
configure terminal	# Enter global config mode
exit	# Move back one level
end	# Return to privileged EXEC from any level

Basic Configuration:

```
hostname [name]          # Set device hostname
enable secret [password] # Set encrypted privileged EXEC password
enable password [password] # Set unencrypted password (legacy)
line console 0           # Enter console line config
line vty 0 15            # Enter virtual terminal lines (SSH/Telnet)
password [password]      # Set line password
login                   # Enable password checking on line
service password-encryption # Encrypt all plaintext passwords
banner motd # [message] # # Set message of the day
no ip domain-lookup      # Disable DNS lookups (prevents typo delays)
```

Interface Configuration:

```
interface [type] [number] # Enter interface config mode
# Examples:
interface gigabitethernet 0/1
interface vlan 1
interface fastethernet 0/0

ip address [ip] [subnet-mask] # Assign IP address to interface
ipv6 address [ipv6/prefix]    # Assign IPv6 address
description [text]           # Add interface description
no shutdown                   # Activate interface
shutdown                      # Disable interface
```

Saving and Managing Configurations:

```
show running-config      # Display active config in RAM
show startup-config      # Display saved config in NVRAM
copy running-config startup-config # Save running to startup (also: write or write memory)
erase startup-config     # Delete startup config
reload                   # Restart device
```

Verification Commands:

```
show ip interface brief      # Summary of all interfaces (IP, status)
show ipv6 interface brief    # IPv6 interface summary
show interfaces [type number] # Detailed interface information
show version                 # IOS version, hardware, uptime
show mac address-table       # MAC address table (switches only)
show ip route                 # IP routing table (routers)
ping [ip-address]            # Test connectivity
traceroute [ip-address]      # Trace packet path
```

Help and Editing:

```
?                # Context-sensitive help
Tab              # Command completion
Ctrl+A          # Move to beginning of line
Ctrl+E          # Move to end of line
Ctrl+C          # Exit configuration mode
Ctrl+Z          # Return to privileged EXEC
Ctrl+Shift+6    # Interrupt process (ping, traceroute)
```

Configuration Example

Basic Switch Configuration:

```
enable
configure terminal
hostname SW1
enable secret Cisco123
line console 0
  password console123
  login
  exit
line vty 0 15
  password vty123
  login
  exit
banner motd # Authorized Access Only #
no ip domain-lookup
service password-encryption
interface vlan 1
  ip address 192.168.1.10 255.255.255.0
  no shutdown
  exit
ip default-gateway 192.168.1.1
end
copy running-config startup-config
```

Basic Router Configuration:

```
enable
configure terminal
hostname R1
enable secret Cisco123
line console 0
  password console123
  login
  logging synchronous      # Prevents console messages from interrupting typing
  exit
line vty 0 4
  password vty123
  login
  exit
banner motd # Authorized Access Only #
no ip domain-lookup
service password-encryption
interface gigabitethernet 0/0
  description Link to LAN
  ip address 192.168.1.1 255.255.255.0
  no shutdown
  exit
interface gigabitethernet 0/1
  description Link to ISP
  ip address 209.165.200.225 255.255.255.224
  no shutdown
  exit
end
copy running-config startup-config
```

Essential Concepts

1. IOS Mode Hierarchy:

- User EXEC → Privileged EXEC → Global Config → Specific Config Modes

2. Configuration Best Practices:

- Always use `enable secret` (encrypted) instead of `enable password`
- Use `service password-encryption` for line passwords
- Save configuration with `copy run start`
- Document interfaces with descriptions
- Use secure protocols (SSH not Telnet)

3. Switch vs Router Interfaces:

- **Switch:** Layer 2 switchport interfaces (default on), SVI (VLAN 1) for management
 - **Router:** Layer 3 routed interfaces (default shutdown), each interface requires IP
-

Chapter 3: Protocols and Models

Key Terminology

Protocol Concepts:

- **Protocol** - Set of rules governing communication
- **Protocol Suite** - Group of related protocols working together
- **Encapsulation** - Wrapping data with protocol information
- **De-encapsulation** - Unwrapping data at destination
- **PDU** (Protocol Data Unit) - Data at specific layer
- **Multiplexing** - Multiple applications sharing network

Network Models:

- **OSI Model** (Open Systems Interconnection) - 7-layer reference model
- **TCP/IP Model** - 4-layer practical model
- **Reference Model** - Conceptual framework for understanding networks

Protocol Types:

- **Network Communication Protocols** - Format and transmit data
- **Network Security Protocols** - Authentication and encryption
- **Routing Protocols** - Exchange route information
- **Service Discovery Protocols** - Detect devices/services

Standards Organizations:

- **IEEE** (Institute of Electrical and Electronics Engineers) - LAN/WLAN standards
- **IETF** (Internet Engineering Task Force) - Internet protocols (RFC)
- **IANA** (Internet Assigned Numbers Authority) - IP addresses, domains
- **ISO** (International Organization for Standardization) - OSI model
- **ITU** (International Telecommunication Union) - Telecommunications

OSI Model (7 Layers)

7. Application Layer:

- User interface, network services
- Protocols: HTTP, HTTPS, FTP, TFTP, DNS, DHCP, SMTP, POP3, IMAP
- PDU: Data

6. Presentation Layer:

- Data format, encryption, compression
- Functions: Translation, encryption/decryption, compression
- PDU: Data

5. Session Layer:

- Manages connections between applications
- Functions: Session establishment, maintenance, termination
- PDU: Data

4. Transport Layer:

- End-to-end connections, reliability
- Protocols: TCP (connection-oriented), UDP (connectionless)
- Functions: Segmentation, flow control, error control
- PDU: Segment (TCP) or Datagram (UDP)

3. Network Layer:

- Logical addressing, routing between networks
- Protocols: IP (IPv4, IPv6), ICMP, routing protocols (OSPF, EIGRP, BGP)
- Functions: Logical addressing, path determination, packet forwarding
- PDU: Packet

2. Data Link Layer:

- Physical addressing, access to media
- Sub-layers: LLC (Logical Link Control), MAC (Media Access Control)
- Protocols: Ethernet, Wi-Fi (802.11), PPP, HDLC
- Functions: Framing, physical addressing (MAC), error detection

- PDU: Frame

1. Physical Layer:

- Transmission of raw bits over physical media
- Specifications: Cables, connectors, signaling, encoding
- Functions: Bit transmission, physical characteristics
- PDU: Bits

TCP/IP Model (4 Layers)

4. Application Layer:

- Combines OSI layers 5, 6, 7
- User applications and services
- Protocols: HTTP, FTP, DNS, DHCP, SMTP, etc.

3. Transport Layer:

- Same as OSI layer 4
- TCP and UDP protocols
- Port numbers for multiplexing

2. Internet Layer:

- Same as OSI layer 3
- IP addressing and routing
- Protocols: IPv4, IPv6, ICMP, routing protocols

1. Network Access Layer:

- Combines OSI layers 1 and 2
- Physical and data link functions
- Media-specific protocols

Data Encapsulation Process

Sending Process (Top to Bottom):

1. **Data** - Application layer data
2. **Segment** - Transport layer adds header (L4)

3. **Packet** - Network layer adds header (L3)
4. **Frame** - Data link layer adds header and trailer (L2)
5. **Bits** - Physical layer transmits as signals (L1)

Receiving Process (Bottom to Top):

1. **Bits** - Received and converted
2. **Frame** - De-encapsulated, checked
3. **Packet** - De-encapsulated, routed
4. **Segment** - De-encapsulated, reassembled
5. **Data** - Delivered to application

Common Protocol Suite Components

TCP/IP Protocol Suite:

- **Application Layer:** HTTP, HTTPS, FTP, TFTP, DNS, DHCP, SMTP, POP3, IMAP, Telnet, SSH
- **Transport Layer:** TCP, UDP
- **Internet Layer:** IPv4, IPv6, ICMP, ICMPv6, OSPF, EIGRP, BGP
- **Network Access:** Ethernet, WLAN, PPP, ARP

Essential Concepts

1. Protocol Characteristics:

- Message encoding (format)
- Message formatting and encapsulation
- Message size
- Message timing
- Message delivery options (unicast, multicast, broadcast)

2. Addressing Types:

- **Physical Address (MAC)** - Layer 2, local delivery
- **Logical Address (IP)** - Layer 3, end-to-end delivery

3. Communication Types:

- **Unicast** - One-to-one
- **Multicast** - One-to-many (specific group)
- **Broadcast** - One-to-all (local network)

IOS Commands (Related)

show protocols	# Display configured Layer 3 protocols
show ip protocols	# Display IP routing protocol information
debug ip packet	# Display IP packet processing (use carefully)
undebg all	# Turn off all debugging

Chapter 4: Physical Layer

Key Terminology

Physical Media Types:

- **Copper Media** - Electrical signals through copper conductors
- **Fiber-Optic Media** - Light pulses through glass/plastic fiber
- **Wireless Media** - Electromagnetic waves through air

Copper Cable Types:

- **UTP** (Unshielded Twisted Pair) - Most common, 8 wires in 4 pairs
- **STP** (Shielded Twisted Pair) - Additional shielding for EMI protection
- **Coaxial Cable** - Center conductor with shield (legacy for LANs)

UTP Categories:

- **Cat 3** - 10 Mbps, phone lines (obsolete for data)
- **Cat 5** - 100 Mbps (obsolete)
- **Cat 5e** - 1 Gbps, 100 MHz, 100 meters max
- **Cat 6** - 10 Gbps (55m), 250 MHz
- **Cat 6a** - 10 Gbps (100m), 500 MHz
- **Cat 7** - 10 Gbps+, shielded
- **Cat 8** - 40 Gbps, data centers, 30 meters max

UTP Cable Termination Standards:

- **TIA/EIA-568A** - Standard wiring scheme
- **TIA/EIA-568B** - Alternative wiring scheme (more common)

Cable Types by Function:

- **Straight-Through** - Connects unlike devices (PC to switch, switch to router)
- **Crossover** - Connects like devices (switch to switch, PC to PC, router to router)
- **Rollover/Console** - Connects PC to console port (blue cable)

Fiber Optic Types:

- **SMF** (Single-Mode Fiber) - Long distance (100s of km), laser, smaller core (9 microns)
- **MMF** (Multimode Fiber) - Shorter distance (<500m), LED, larger core (50/62.5 microns)

Fiber Connectors:

- **SC** (Subscriber Connector) - Square connector, push-pull
- **LC** (Lucent Connector) - Small form factor, common in Gigabit
- **ST** (Straight Tip) - Round, bayonet twist-lock (older)

Wireless Standards (802.11):

- **802.11a** - 5 GHz, 54 Mbps
- **802.11b** - 2.4 GHz, 11 Mbps
- **802.11g** - 2.4 GHz, 54 Mbps
- **802.11n** (Wi-Fi 4) - 2.4/5 GHz, 600 Mbps, MIMO
- **802.11ac** (Wi-Fi 5) - 5 GHz, 1+ Gbps, MU-MIMO
- **802.11ax** (Wi-Fi 6) - 2.4/5/6 GHz, 9.6 Gbps

Physical Layer Characteristics:

- **Bandwidth** - Data carrying capacity (bps, Mbps, Gbps)
- **Throughput** - Actual data transfer rate
- **Goodput** - Usable data transfer (excludes overhead)
- **Latency** - Time delay in transmission
- **EMI** (Electromagnetic Interference) - Signal disruption
- **Crosstalk** - Signal interference between adjacent wires
- **Attenuation** - Signal strength loss over distance

Encoding:

- **Manchester Encoding** - Combines clock and data signals
- **4B/5B Encoding** - Maps 4 data bits to 5 signal bits

- **8B/10B Encoding** - Maps 8 data bits to 10 signal bits

UTP Wiring Standards

T568A Standard:

1. White/Green
2. Green
3. White/Orange
4. Blue
5. White/Blue
6. Orange
7. White/Brown
8. Brown

T568B Standard (More Common):

1. White/Orange
2. Orange
3. White/Green
4. Blue
5. White/Blue
6. Green
7. White/Brown
8. Brown

Cable Selection Guide:

- **Straight-through:** Both ends T568B (or both T568A)
 - PC to Switch
 - Switch to Router
 - Router to Server
- **Crossover:** One end T568A, other end T568B
 - Switch to Switch
 - PC to PC
 - Router to Router
- **Auto-MDIX:** Modern devices automatically detect and adjust (makes cable type less critical)

Essential Concepts

1. Physical Layer Functions:

- Physical components (cables, connectors, NICs)
- Encoding techniques
- Signaling methods
- Bandwidth and throughput characteristics

2. Media Selection Criteria:

- Distance requirements
- Environment (EMI concerns)
- Bandwidth needs
- Cost
- Installation ease

3. Fiber vs Copper:

- **Fiber Advantages:** Higher bandwidth, longer distance, no EMI, secure
- **Copper Advantages:** Less expensive, easier installation, powered devices (PoE)

4. Wireless Coverage:

- 2.4 GHz: Better penetration, more interference, longer range
- 5 GHz: Less interference, higher speeds, shorter range
- 6 GHz: Cleanest spectrum, highest speeds, shortest range (Wi-Fi 6E)

IOS Commands

```
show interfaces [type number]    # Detailed interface information
show ip interface brief          # Interface summary
show controllers [type number]    # Physical layer information, cable type
show interfaces status           # Switch port status (switches)
show interfaces description      # Interface descriptions
speed {10 | 100 | 1000 | auto}   # Set interface speed
duplex {auto | full | half}      # Set duplex mode
mdix auto                       # Enable Auto-MDIX (crossover detection)
```

Interface Status Interpretation:

- **Line protocol is up, line status is up** - Interface working properly
- **Line protocol is down, line status is down** - Physical problem (cable, port)

- **Line protocol is down, line status is up** - Data link problem (encapsulation, clocking)
-

Chapter 5: Number Systems

Key Terminology

Number Systems:

- **Binary** - Base 2 (0, 1)
- **Decimal** - Base 10 (0-9)
- **Hexadecimal** - Base 16 (0-9, A-F)
- **Octet** - 8 bits
- **Nibble** - 4 bits (half an octet)
- **Bit** - Binary digit (0 or 1)
- **Byte** - 8 bits

Positional Values:

- **Least Significant Bit (LSB)** - Rightmost bit
- **Most Significant Bit (MSB)** - Leftmost bit

Binary System

8-Bit Positional Values:

Position:	7	6	5	4	3	2	1	0
Value:	128	64	32	16	8	4	2	1

Conversion Examples:

Binary to Decimal:

Binary: 11001010
 $128 + 64 + 0 + 0 + 8 + 0 + 2 + 0 = 202$

Binary: 10101010
 $128 + 0 + 32 + 0 + 8 + 0 + 2 + 0 = 170$

Decimal to Binary:

Decimal: 192

$192 = 128 + 64$

Binary: 11000000

Decimal: 255

$255 = 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1$

Binary: 11111111

Decimal: 172

$172 = 128 + 32 + 8 + 4$

Binary: 10101100

Common Binary Values:

- 0 = 00000000
- 1 = 00000001
- 128 = 10000000
- 192 = 11000000
- 224 = 11100000
- 240 = 11110000
- 248 = 11111000
- 252 = 11111100
- 254 = 11111110
- 255 = 11111111

Hexadecimal System

Hex Values:

Decimal: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Hex: 0 1 2 3 4 5 6 7 8 9 A B C D E F

Binary: 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

Conversion Examples:

Hex to Binary:

Hex: A5

A = 1010

5 = 0101

Binary: 10100101

Hex: FF

F = 1111

F = 1111

Binary: 11111111

Hex: C0

C = 1100

0 = 0000

Binary: 11000000

Binary to Hex:

Binary: 11001010

1100 = C

1010 = A

Hex: CA

Binary: 10101100

1010 = A

1100 = C

Hex: AC

Hex to Decimal:

Hex: A5

$$A \times 16 + 5 \times 1 = 160 + 5 = 165$$

Hex: FF

$$F \times 16 + F \times 1 = 240 + 15 = 255$$

Essential Concepts

1. Why Binary in Networking:

- Computers operate on binary (on/off, 1/0)
- IP addresses stored as 32 bits (IPv4) or 128 bits (IPv6)
- Subnet masks use binary for network calculations

2. Why Hexadecimal:

- Compact representation of binary
- MAC addresses use hex (e.g., 00:1A:2B:3C:4D:5E)
- IPv6 addresses use hex
- Easier for humans to read than binary

3. Networking Applications:

- **IP Address:** 192.168.1.1 = 11000000.10101000.00000001.00000001
- **Subnet Mask:** 255.255.255.0 = 11111111.11111111.11111111.00000000
- **MAC Address:** 00:1A:2B:3C:4D:5E (hex notation)
- **IPv6 Address:** 2001:0DB8:0000:0000:0000:0000:0001 (hex notation)

Quick Reference Tables

Powers of 2:

$2^0 = 1$
 $2^1 = 2$
 $2^2 = 4$
 $2^3 = 8$
 $2^4 = 16$
 $2^5 = 32$
 $2^6 = 64$
 $2^7 = 128$
 $2^8 = 256$
 $2^9 = 512$
 $2^{10} = 1024$

Common Subnet Masks (Binary):

$/24 = 255.255.255.0 = 11111111.11111111.11111111.00000000$
 $/25 = 255.255.255.128 = 11111111.11111111.11111111.10000000$
 $/26 = 255.255.255.192 = 11111111.11111111.11111111.11000000$
 $/27 = 255.255.255.224 = 11111111.11111111.11111111.11100000$
 $/28 = 255.255.255.240 = 11111111.11111111.11111111.11110000$
 $/29 = 255.255.255.248 = 11111111.11111111.11111111.11111000$
 $/30 = 255.255.255.252 = 11111111.11111111.11111111.11111100$

IOS Commands (None specific - used in addressing chapters)

Chapter 6: Data Link Layer

Key Terminology

Data Link Layer Functions:

- **Framing** - Encapsulates packets into frames
- **Addressing** - Physical addressing (MAC addresses)
- **Error Detection** - Identifies corrupted frames (FCS)
- **Media Access Control** - Controls access to shared media

Layer 2 Components:

- **LLC** (Logical Link Control) - Upper sublayer, interfaces with network layer
- **MAC** (Media Access Control) - Lower sublayer, controls media access
- **NIC** (Network Interface Card) - Physical adapter for network connection
- **MAC Address** - 48-bit physical address (also called hardware or physical address)

Frame Components:

- **Header** - Source/destination addresses, control information
- **Data** - Encapsulated packet from network layer
- **Trailer** - Error detection field (FCS)
- **FCS** (Frame Check Sequence) - Error detection using CRC

Topologies:

- **Physical Topology** - Actual cable layout and connections
- **Logical Topology** - Data flow paths

Physical Topologies:

- **Point-to-Point** - Direct connection between two devices
- **Bus** - All devices on single cable (legacy)
- **Ring** - Devices connected in circular fashion
- **Star** - All devices connect to central hub/switch (most common)
- **Extended Star** - Multiple stars interconnected
- **Mesh** - Multiple paths between devices
 - **Full Mesh** - Every device connects to every other device

- **Partial Mesh** - Some devices have multiple connections
- **Hybrid** - Combination of topologies

Logical Topologies:

- **Broadcast** - All devices receive frame (Ethernet)
- **Token Passing** - Token controls transmission (legacy - Token Ring, FDDI)

WAN Topologies:

- **Point-to-Point** - Dedicated connection between two sites
- **Hub and Spoke** - Central site with connections to remote sites
- **Full Mesh** - All sites connect to all other sites
- **Dual-Homed** - Device connects to two separate providers/devices

Access Methods:

- **Contention-Based** - CSMA/CD (Ethernet on half-duplex)
- **Controlled Access** - Token passing, polling
- **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) - Half-duplex Ethernet
- **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance) - Wireless

MAC Address Structure

Format:

- 48 bits (6 octets)
- Written as 12 hexadecimal digits
- Example: 00:1A:2B:3C:4D:5E or 00-1A-2B-3C-4D-5E

Components:

- **OUI** (Organizationally Unique Identifier) - First 24 bits (vendor assigned by IEEE)
- **Device Identifier** - Last 24 bits (manufacturer assigned)

Special MAC Addresses:

- **Unicast** - Single destination (bit 0 of first octet = 0)
- **Multicast** - Group destination (bit 0 of first octet = 1)
- **Broadcast** - All devices (FF:FF:FF:FF:FF:FF)

Frame Types

Ethernet II Frame (Most Common):

Preamble	Destination MAC	Source MAC	Type	Data	FCS
7 bytes	6 bytes	6 bytes	2 bytes	46-1500	4 bytes

802.3 Frame Fields:

- **Preamble** - 7 bytes, synchronization pattern
- **Start Frame Delimiter (SFD)** - 1 byte, indicates start of frame
- **Destination MAC** - 6 bytes
- **Source MAC** - 6 bytes
- **Type/Length** - 2 bytes (EtherType or length)
- **Data** - 46-1500 bytes
- **FCS** - 4 bytes, error checking

Minimum Frame Size: 64 bytes (excluding preamble and SFD) **Maximum Frame Size:** 1518 bytes (excluding preamble and SFD)

Essential Concepts

1. Data Link Layer Services:

- Provides service to network layer
- Frames packets for physical transmission
- Adds physical addresses
- Detects errors (but typically doesn't correct them)
- Controls access to media

2. Full-Duplex vs Half-Duplex:

- **Full-Duplex:** Simultaneous bidirectional transmission (modern switches)
- **Half-Duplex:** One direction at a time (hubs, legacy)
- **Simplex:** One direction only (not used in Ethernet)

3. Layer 2 Standards:

- IEEE 802.3 (Ethernet)
- IEEE 802.11 (Wireless LAN)
- PPP (Point-to-Point Protocol)
- HDLC (High-Level Data Link Control)

- Frame Relay (legacy)

4. Why Two Addresses (MAC and IP)?

- **MAC:** Local delivery (same network segment)
- **IP:** End-to-end delivery (across networks)
- MAC addresses change at each hop; IP addresses remain constant

IOS Commands

```
show mac address-table      # Display MAC address table (switches)
show mac address-table dynamic  # Show dynamically learned MAC addresses
show mac address-table static  # Show statically configured MAC entries
clear mac address-table dynamic  # Clear dynamic MAC entries
show interfaces [type number]  # Show MAC address of interface
show arp                     # Display ARP table (IP to MAC mappings)
show version                 # Shows base MAC address of device
```

MAC Address Table Aging:

```
mac address-table aging-time [seconds] # Set aging time (default: 300 seconds)
```

Chapter 7: Ethernet Switching

Key Terminology

Ethernet Standards:

- **Ethernet** - 10 Mbps (10BASE-T)
- **Fast Ethernet** - 100 Mbps (100BASE-TX)
- **Gigabit Ethernet** - 1000 Mbps (1000BASE-T, 1000BASE-SX/LX)
- **10 Gigabit Ethernet** - 10 Gbps (10GBASE-T, 10GBASE-SR/LR)
- **40/100 Gigabit Ethernet** - Data center speeds

Ethernet Naming Convention:

[Speed] BASE [Media Type]

↓ ↓ ↓

10 Baseband T (Twisted Pair)
 F (Fiber)
 X (Multiplexed)

Examples:

- 10BASE-T: 10 Mbps, baseband, twisted pair
- 100BASE-TX: 100 Mbps, baseband, twisted pair (Cat5e)
- 1000BASE-T: 1 Gbps, baseband, twisted pair (Cat5e+)
- 1000BASE-SX: 1 Gbps, baseband, short-range fiber (MMF)
- 1000BASE-LX: 1 Gbps, baseband, long-range fiber (SMF)

Switch Functions:

- **Learning** - Builds MAC address table from source addresses
- **Flooding** - Sends frame out all ports except source (unknown unicast)
- **Forwarding** - Sends frame to specific port (known unicast)
- **Filtering** - Does not forward to unnecessary ports
- **Aging** - Removes old MAC entries (default 300 seconds)

Frame Forwarding Methods:

- **Store-and-Forward** - Receives entire frame, checks FCS, then forwards (most common)
- **Cut-Through** - Forwards after reading destination MAC (low latency, no error checking)
 - **Fast-Forward** - Forwards immediately after destination MAC
 - **Fragment-Free** - Checks first 64 bytes (collision fragment size)

Switch Memory:

- **CAM** (Content Addressable Memory) - Stores MAC address table
- **TCAM** (Ternary CAM) - Stores ACLs, QoS rules (wildcards)

Port Types:

- **Access Port** - Connects end devices (single VLAN)
- **Trunk Port** - Carries multiple VLANs between switches
- **SPAN Port** (Switch Port Analyzer) - Mirror port for monitoring

Auto-Negotiation:

- Automatically negotiates speed and duplex
- Falls back to lower speeds if needed
- Can cause duplex mismatches if one side is manual

MAC Address Table

How It Works:

1. Frame arrives on port
2. Switch learns source MAC address and associates with port
3. Switch checks destination MAC address
4. If known, forwards to specific port
5. If unknown, floods to all ports except source
6. Broadcast/multicast frames always flooded

MAC Table Entry Components:

- **MAC Address**
- **Port Number**
- **VLAN ID**
- **Type** (Dynamic or Static)

Duplex and Speed Issues

Duplex Mismatch:

- One side full-duplex, other side half-duplex
- Causes: Collision errors, poor performance
- Detection: High late collisions, CRC errors

Common Misconfigurations:

Correct Configuration:

Both sides: Auto/Auto or Both sides: Manual matching settings

Problematic:

One side: Auto, Other side: Manual (can cause duplex mismatch)

Switch Performance

Switching Rate:

- Measured in frames per second (fps) or packets per second (pps)
- Wire speed: Ability to forward at maximum theoretical rate

Factors Affecting Performance:

- Forwarding method (store-and-forward slower than cut-through)
- Port speed
- Buffer memory
- Internal bandwidth
- CPU processing power

Essential Concepts

1. Collision Domains and Broadcast Domains:

- **Collision Domain:** Area where collisions can occur (each switch port is separate)
- **Broadcast Domain:** Area where broadcasts propagate (all ports in same VLAN)
- **Hub:** Single collision domain, single broadcast domain
- **Switch:** Multiple collision domains (one per port), single broadcast domain per VLAN
- **Router:** Separates broadcast domains

2. Switch Frame Processing:

- Ingress: Frame received on port
- Table lookup: Check destination MAC in CAM table
- Egress: Forward to destination port or flood

3. MAC Address Aging:

- Prevents table from filling with stale entries
- Default: 300 seconds (5 minutes)
- Entry refreshed when traffic from that MAC is seen

4. Frame Error Handling:

- **Store-and-Forward:** Drops frames with FCS errors
- **Cut-Through:** Cannot detect errors (forwards corrupt frames)
- **Fragment-Free:** Drops collision fragments

IOS Commands

MAC Address Table Commands

```
show mac address-table          # Display entire MAC table
show mac address-table address [mac]  # Show specific MAC entry
show mac address-table interface [type number] # Show MACs on specific port
show mac address-table vlan [vlan-id]  # Show MACs in specific VLAN
show mac address-table count          # Count of MAC addresses
clear mac address-table dynamic      # Clear all dynamic entries
clear mac address-table dynamic address [mac] # Clear specific MAC
clear mac address-table dynamic interface [type number] # Clear MACs on port
```

Interface Configuration

```
interface [type number]
  speed {10 | 100 | 1000 | auto}    # Set speed
  duplex {auto | full | half}        # Set duplex mode
  mdix auto                          # Enable Auto-MDIX
  description [text]                # Interface description
  switchport mode access             # Set as access port (default)
```

Port Statistics

```
show interfaces [type number]      # Detailed interface stats
show interfaces [type number] status  # Port status summary
show interfaces counters errors      # Error counters
```

Verification

```
show interfaces status              # All ports status summary
show interfaces description          # All interface descriptions
show running-config interface [type number] # Interface configuration
```

Interpreting Interface Errors:

```
show interfaces gigabitethernet 0/1
```

Key Error Counters:

- Runt: Frames < 64 bytes (collision fragments)
- Giants: Frames > 1518 bytes
- CRC Errors: Failed FCS check
- Collisions: Normal for half-duplex, problem for full-duplex
- Late Collisions: Duplex mismatch indicator
- Input Errors: Total input errors
- Output Errors: Total output errors

Configuration Example

```
# Basic Switch Port Configuration
enable
configure terminal
interface gigabitethernet 0/1
    description Desktop-PC1
    speed 1000
    duplex full
    mdix auto
    no shutdown
exit

# Configure multiple ports
interface range gigabitethernet 0/1-10
    description Access Ports
    speed auto
    duplex auto
    mdix auto
    switchport mode access
    no shutdown
exit

# View MAC table
show mac address-table
show mac address-table dynamic

# Clear MAC table
clear mac address-table dynamic
```

Chapter 8: Network Layer

Key Terminology

Network Layer Functions:

- **Addressing** - Logical addressing (IP addresses)
- **Encapsulation** - Creates packets from segments
- **Routing** - Path determination and packet forwarding
- **De-encapsulation** - Extracts data from packets

Routing Concepts:

- **Routing Table** - Database of known networks and paths
- **Default Route** - Path used when no specific route exists (0.0.0.0/0)
- **Static Route** - Manually configured route
- **Dynamic Route** - Routes learned via routing protocols
- **Routing Protocol** - Protocol that exchanges routing information (OSPF, EIGRP, BGP)

Packet Components:

- **IP Header** - Source/destination IP, TTL, protocol information
- **Data** - Encapsulated segment from transport layer

IP Characteristics:

- **Connectionless** - No dedicated path, each packet independent
- **Best Effort** - No guaranteed delivery
- **Media Independent** - Works over any physical media

Path Selection:

- **Metric** - Value used to determine best path
- **Administrative Distance (AD)** - Trustworthiness of routing source
- **Next-Hop** - Next router in path to destination
- **Longest Match** - Most specific route used when multiple matches exist

Routing Table Information:

- **Route Source** - How route was learned (C, L, S, D, O, etc.)
- **Destination Network**
- **Administrative Distance/Metric**
- **Next-hop IP or Exit Interface**
- **Route timestamp**

IPv4 Packet Header

Fields:

- **Version** - 4 bits (value: 4 for IPv4)
- **IHL** (Internet Header Length) - 4 bits (header length in 32-bit words)

- **DSCP** (Differentiated Services Code Point) - 6 bits (QoS marking)
- **ECN** (Explicit Congestion Notification) - 2 bits
- **Total Length** - 16 bits (packet size including header)
- **Identification** - 16 bits (fragment reassembly)
- **Flags** - 3 bits (fragmentation control)
- **Fragment Offset** - 13 bits (position in original packet)
- **TTL** (Time to Live) - 8 bits (hop count limit)
- **Protocol** - 8 bits (upper layer protocol: 1=ICMP, 6=TCP, 17=UDP)
- **Header Checksum** - 16 bits (error checking)
- **Source IP Address** - 32 bits
- **Destination IP Address** - 32 bits
- **Options** - Variable (rarely used)

IPv6 Packet Header (Simplified)

Fields:

- **Version** - 4 bits (value: 6 for IPv6)
- **Traffic Class** - 8 bits (QoS)
- **Flow Label** - 20 bits (QoS flow identification)
- **Payload Length** - 16 bits
- **Next Header** - 8 bits (upper layer protocol or extension header)
- **Hop Limit** - 8 bits (replaces TTL)
- **Source IPv6 Address** - 128 bits
- **Destination IPv6 Address** - 128 bits

Host Routing

Host Routing Decision:

1. Is destination on local network?
 - Yes → Send directly to destination
 - No → Send to default gateway
2. Check routing table for match
3. Send packet to:
 - Destination (if local)
 - Default gateway (if remote)

ARP Process for Local Delivery:

1. Check ARP cache for destination MAC
2. If not found, send ARP request (broadcast)
3. Destination replies with MAC address
4. Add to ARP cache
5. Send frame with destination MAC

Router Routing

Router Routing Process:

1. Receive frame on ingress interface
2. De-encapsulate to examine packet
3. Check destination IP
4. Look up destination in routing table
5. Find best match (longest prefix match)
6. Determine egress interface and next-hop
7. Re-encapsulate packet in new frame
8. Forward frame out egress interface
9. Decrement TTL

TTL (Time to Live):

- Prevents routing loops
- Decrement by 1 at each router
- Packet dropped when TTL reaches 0
- Router sends ICMP Time Exceeded message to source

Route Sources and Codes

Common Routing Table Codes:

- **L** - Local (interface IP address)
- **C** - Connected (directly attached network)
- **S** - Static (manually configured)
- **D** - EIGRP
- **O** - OSPF

- **R** - RIP
- **B** - BGP
- **i** - IS-IS
- **S*** - Default static route

Administrative Distance (AD):

Route Source	AD
Connected	0
Static	1
EIGRP Summary	5
eBGP	20
EIGRP Internal	90
OSPF	110
IS-IS	115
RIP	120
EIGRP External	170
iBGP	200
Unknown/Untrusted	255

Essential Concepts

1. Routing Table Lookup:

- Longest prefix match wins
- Example: 192.168.1.10/32 is more specific than 192.168.1.0/24

2. Default Route:

- Route of last resort (0.0.0.0/0 or ::/0)
- Used when no other route matches
- Common on edge routers

3. Connected vs Local Routes:

- **Connected (C):** Network range of interface
- **Local (L):** Specific IP address of interface (/32 or /128)

4. Packet vs Frame Addresses:

- **Packet (Layer 3):** Source/dest IP remains constant end-to-end
- **Frame (Layer 2):** Source/dest MAC changes at each hop

5. IPv4 vs IPv6 Differences:

- IPv6 header simplified (8 fields vs 12+ in IPv4)

- No header checksum in IPv6 (performance improvement)
- No fragmentation by routers in IPv6
- Built-in security (IPsec) in IPv6

IOS Commands

```
# Routing Table Display
show ip route           # Display IPv4 routing table
show ipv6 route         # Display IPv6 routing table
show ip route [network] # Show route to specific network
show ip route static    # Show only static routes
show ip route connected # Show only connected routes
show ip route summary   # Summary of routing table

# Route Details
show ip route [destination-ip] # Show route used to reach IP
show ip protocols              # Show routing protocol information
show running-config | section route # Show route config

# Static Route Configuration (covered in detail in Chapter 10)
ip route [dest-network] [mask] [next-hop | exit-int] # IPv4 static route
ipv6 route [dest-network/prefix] [next-hop | exit-int] # IPv6 static route
ip route 0.0.0.0 0.0.0.0 [next-hop]                  # Default route (IPv4)
ipv6 route ::/0 [next-hop]                            # Default route (IPv6)

# Verification
show ip interface brief    # Quick interface status and IP
show ipv6 interface brief  # IPv6 interface summary
ping [ip-address]          # Test connectivity
traceroute [ip-address]    # Trace packet path
```

Routing Table Example:

```
Router# show ip route
```

Codes: L - local, C - connected, S - static, D - EIGRP, O - OSPF

Gateway of last resort is 10.1.1.1 to network 0.0.0.0

```
S* 0.0.0.0/0 [1/0] via 10.1.1.1
```

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

```
C 10.1.1.0/30 is directly connected, GigabitEthernet0/0
```

```
L 10.1.1.2/32 is directly connected, GigabitEthernet0/0
```

```
C 10.1.2.0/24 is directly connected, GigabitEthernet0/1
```

```
L 10.1.2.1/32 is directly connected, GigabitEthernet0/1
```

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

```
C 192.168.1.0/24 is directly connected, GigabitEthernet0/2
```

```
L 192.168.1.1/32 is directly connected, GigabitEthernet0/2
```

Reading a Route Entry:

```
S 192.168.10.0/24 [1/0] via 10.1.1.1
```

```
↑      ↑      ↑↑      ↑
```

Code	Network	AD Metric	Next-hop
------	---------	-----------	----------

S = Static route

192.168.10.0/24 = Destination network

[1/0] = [Administrative Distance / Metric]

via 10.1.1.1 = Next-hop router IP

Chapter 9: Address Resolution

Key Terminology

ARP (Address Resolution Protocol):

- Maps IPv4 addresses to MAC addresses
- Required for local delivery
- Operates at boundary between Layer 2 and Layer 3
- Uses broadcast requests, unicast replies

ARP Components:

- **ARP Request** - Broadcast asking "Who has IP X?"

- **ARP Reply** - Unicast response with MAC address
- **ARP Cache** - Table storing IP-to-MAC mappings
- **ARP Table** - Same as ARP cache

IPv6 Neighbor Discovery (ND):

- Replaces ARP in IPv6
- Uses ICMPv6 messages instead of broadcasts
- More efficient and secure than ARP
- Multicast-based (not broadcast)

ND Messages:

- **NS** (Neighbor Solicitation) - Similar to ARP request
- **NA** (Neighbor Advertisement) - Similar to ARP reply
- **RS** (Router Solicitation) - Host requests router information
- **RA** (Router Advertisement) - Router sends configuration info
- **Redirect** - Better route notification

Additional Functions:

- **DAD** (Duplicate Address Detection) - Ensures address uniqueness
- **SLAAC** (Stateless Address Autoconfiguration) - Automatic IPv6 addressing

ARP Process (IPv4)

Scenario: PC1 (192.168.1.10) wants to reach PC2 (192.168.1.20)

1. PC1 checks ARP cache:

```
arp -a
```

- If 192.168.1.20 found → use MAC, send frame
- If not found → continue to step 2

2. PC1 sends ARP Request (broadcast):

Destination MAC: FF:FF:FF:FF:FF:FF (broadcast)

Source MAC: PC1's MAC

Payload: "Who has 192.168.1.20? Tell 192.168.1.10"

3. All devices receive broadcast:

- Only PC2 (192.168.1.20) responds
- Others discard the request

4. PC2 sends ARP Reply (unicast):

Destination MAC: PC1's MAC (learned from request)

Source MAC: PC2's MAC

Payload: "192.168.1.20 is at [PC2's MAC]"

5. PC1 updates ARP cache:

- Adds entry: 192.168.1.20 → PC2's MAC
- Cache entry has timeout (typically 2-20 minutes)

6. PC1 sends data:

- Now knows destination MAC
- Can send frames directly to PC2

ARP for Remote Networks

Scenario: PC1 (192.168.1.10) wants to reach Server (209.165.200.10) via Router (192.168.1.1)

1. PC1 determines destination is remote:

- Applies subnet mask
- Destination network \neq source network

2. PC1 uses default gateway:

- Needs MAC of 192.168.1.1 (router)
- Checks ARP cache for default gateway

3. ARP for default gateway:

- If not in cache, sends ARP request for 192.168.1.1
- Router replies with its MAC address

4. PC1 sends packet:

Layer 3 (Packet):

Source IP: 192.168.1.10

Dest IP: 209.165.200.10

Layer 2 (Frame):

Source MAC: PC1's MAC

Dest MAC: Router's MAC

5. Router processes frame:

- Receives frame (dest MAC matches)
- De-encapsulates to examine packet
- Looks up 209.165.200.10 in routing table
- Forwards to next hop
- Creates new frame with new MAC addresses (Layer 2 rewrite)

IPv6 Neighbor Discovery

Key Differences from ARP:

- Uses ICMPv6 (not separate protocol)
- Uses multicast (not broadcast)
- More secure (can use IPsec)
- Additional functionality (router discovery, autoconfiguration)

ICMPv6 Message Types:

Type 133: Router Solicitation (RS)

Type 134: Router Advertisement (RA)

Type 135: Neighbor Solicitation (NS)

Type 136: Neighbor Advertisement (NA)

Type 137: Redirect

NS/NA Process (Similar to ARP):

1. PC1 sends NS (Neighbor Solicitation):

Destination IPv6: Solicited-node multicast address

ICMPv6 Type 135: "Who has 2001:db8::20?"

2. PC2 sends NA (Neighbor Advertisement):

ICMPv6 Type 136: "2001:db8::20 is at [MAC]"

Multicast Addresses:

- **Solicited-Node Multicast:** FF02::1:FF00:0/104
 - Last 24 bits match last 24 bits of target IPv6
 - More efficient than broadcast (only interested nodes listen)

Router Discovery:

1. **Host sends RS** (when it boots)
2. **Router sends RA** (periodically or in response to RS)
 - Contains: Prefix, prefix length, default gateway, DNS
 - Used for SLAAC addressing

DAD (Duplicate Address Detection):

1. Before using IPv6 address, device sends NS for its own address
2. If no NA received → address is unique
3. If NA received → address conflict, cannot use

ARP Security Issues

ARP Spoofing/Poisoning:

- Attacker sends fake ARP replies
- Associates attacker's MAC with victim's IP
- Traffic redirected to attacker (man-in-the-middle)

Mitigation:

- **Dynamic ARP Inspection (DAI)** - Switch feature validating ARP packets
- **Static ARP entries** - Manual IP-to-MAC mappings
- **Port security** - Limit MAC addresses per port

Essential Concepts

1. **Why Two Addresses?**

- **IP:** Logical, hierarchical, for routing between networks
- **MAC:** Physical, flat, for local delivery on same network
- Need mapping between them for communication

2. **ARP Cache Aging:**

- Entries timeout to prevent stale data
- Refreshed when device communicates
- Can be cleared manually

3. **Gratuitous ARP:**

- Device sends ARP reply without request
- Announces its own IP/MAC mapping
- Updates other devices' ARP caches
- Detects IP conflicts

4. **Proxy ARP:**

- Router answers ARP requests on behalf of another device
- Used when devices don't have default gateway configured
- Can cause routing problems
- Generally disabled on modern networks

5. **IPv6 Improvements:**

- No broadcast (uses efficient multicast)
- Built-in security
- Automatic addressing (SLAAC)
- Duplicate detection built-in

IOS Commands

ARP Commands (IPv4)

```
show arp          # Display ARP table (routers)
show ip arp       # Display ARP table (alternate)
clear arp-cache   # Clear dynamic ARP entries
clear arp [ip-address] # Clear specific ARP entry
arp [ip-address] [mac-address] arpa # Static ARP entry
```

IPv6 Neighbor Discovery

```
show ipv6 neighbors # Display IPv6 neighbor table
clear ipv6 neighbors # Clear dynamic neighbor entries
```

```

ipv6 neighbor [ipv6] [mac] [interface] # Static neighbor entry

# Interface Configuration
no ip proxy-arp          # Disable proxy ARP (recommended)
ipv6 nd dad attempts [number] # Set DAD attempts (default: 1)
ipv6 nd ns-interval [milliseconds] # NS retransmit interval

# Debugging (use sparingly on production)
debug arp                # Debug ARP activity
debug ipv6 nd            # Debug IPv6 Neighbor Discovery
undebug all              # Turn off all debugging

```

ARP Table Example:

```

Router# show arp

```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.1	-	0019.e86a.6f80	ARPA	GigabitEthernet0/0
Internet	192.168.1.10	18	0050.56be.8c34	ARPA	GigabitEthernet0/0
Internet	192.168.1.20	5	0050.56be.1a2b	ARPA	GigabitEthernet0/0

IPv6 Neighbor Table Example:

```

Router# show ipv6 neighbors

```

IPv6 Address	Age	Link-layer Addr	State	Interface
2001:DB8::10	0	0050.56be.8c34	REACH	Gi0/0
2001:DB8::20	15	0050.56be.1a2b	STALE	Gi0/0
FE80::1	-	0019.e86a.6f80	REACH	Gi0/0

Neighbor States:

- **INCMP** (Incomplete) - Resolution in progress
- **REACH** (Reachable) - Confirmed reachable
- **STALE** - Not recently confirmed but presumed reachable
- **DELAY** - Waiting for confirmation
- **PROBE** - Sending NS to verify reachability

Host Commands (Windows/Linux)

Windows:

```
arp -a          # Display ARP cache
arp -d          # Delete all ARP entries
arp -d [ip-address]  # Delete specific entry
arp -s [ip] [mac]    # Add static entry
ipconfig /all      # Show IP configuration
netsh interface ipv6 show neighbors # IPv6 neighbors
```

Linux:

```
arp -a          # Display ARP cache
arp -n          # Display without DNS resolution
arp -d [ip-address]  # Delete specific entry
arp -s [ip] [mac]    # Add static entry
ip neighbor show   # Show neighbor cache (modern)
ip -6 neighbor show # Show IPv6 neighbors
```

Chapter 10: Basic Router Configuration

Key Terminology

Router Components:

- **CPU** - Executes IOS instructions
- **RAM** - Running configuration, routing tables, ARP cache
- **ROM** - Bootstrap, ROMMON, miniature IOS
- **NVRAM** - Startup configuration
- **Flash** - IOS image files
- **Interfaces** - Network connections (different from switches)

Router Functions:

- **Path Determination** - Choose best route to destination
- **Packet Forwarding** - Send packets toward destination
- **Routing Table Maintenance** - Keep routing information current

Boot Process:

1. **POST** (Power-On Self-Test) - Hardware check
2. **Bootstrap loader** - Loads IOS from ROM

3. **IOS location** - Find and load IOS from flash
4. **Configuration** - Load startup-config from NVRAM

Router Interfaces:

- **Routed Interface** - Layer 3 interface with IP address
- **Management Interface** - For device management (not data forwarding)
- **Serial Interface** - WAN connections (legacy)
- **Ethernet Interface** - LAN connections (FastEthernet, GigabitEthernet, etc.)

Basic Router Configuration

Initial Configuration Steps:

1. Name the device
2. Secure privileged EXEC mode
3. Secure user EXEC mode (console)
4. Secure remote access (VTY lines)
5. Secure passwords
6. Provide legal notification (banner)
7. Configure interfaces
8. Save configuration

Essential Commands

Basic Device Configuration:

```
enable
configure terminal
hostname R1
enable secret class
no ip domain-lookup

# Console line
line console 0
  password cisco
  login
  logging synchronous      # Prevents messages from interrupting
  exec-timeout 0 0         # Disables timeout (lab only!)
  exit

# VTY lines (remote access)
line vty 0 4
  password cisco
  login
  exec-timeout 5 0         # 5 minute timeout
  transport input ssh      # SSH only (secure)
  exit

# Banner
banner motd # Unauthorized Access Prohibited #

# Encrypt passwords
service password-encryption

# Save
end
copy running-config startup-config
```

Interface Configuration:

```
interface gigabitethernet 0/0
  description Link to LAN
  ip address 192.168.1.1 255.255.255.0
  ipv6 address 2001:db8:acad:1::1/64
  ipv6 address fe80::1 link-local
  no shutdown
  exit

interface gigabitethernet 0/1
  description Link to ISP
  ip address 209.165.200.225 255.255.255.224
  ipv6 address 2001:db8:acad:2::1/64
  ipv6 address fe80::1 link-local
  no shutdown
  exit

interface serial 0/0/0 (if present)
  description WAN Link
  ip address 10.1.1.1 255.255.255.252
  clock rate 128000      # DCE side only
  no shutdown
  exit
```

IPv6 Configuration:

```
# Enable IPv6 routing globally
ipv6 unicast-routing      # Required for router to forward IPv6

# Configure interface
interface gigabitethernet 0/0
  ipv6 address 2001:db8:acad:1::1/64    # Global unicast
  ipv6 address fe80::1 link-local      # Link-local (optional to specify)
  no shutdown
  exit
```

Default Gateway Configuration

Switch (Layer 2) Default Gateway:

```
# Switch needs default gateway for management access
ip default-gateway 192.168.1.1
```

Host Default Gateway:

- Configured on end device (PC, server)
- Points to router interface IP
- Required for reaching remote networks

Router Default Gateway:

- Routers use **default route** instead
- Configured as static route

```
ip route 0.0.0.0 0.0.0.0 [next-hop-ip]
# or
ip route 0.0.0.0 0.0.0.0 [exit-interface]
```

Interface Configuration Best Practices

Router Interface Shutdown by Default:

- All router interfaces are administratively down by default
- Must use `no shutdown` to activate
- Different from switches (switch ports up by default)

IPv6 Link-Local Addresses:

- Required on every IPv6-enabled interface
- Can be auto-generated or manually configured
- Used for next-hop addresses in routing table
- Format: FE80::/10
- Recommended: Manually configure for consistency

```
ipv6 address fe80::1 link-local
```

Description Best Practice:

- Always add descriptions to interfaces
- Helps with documentation and troubleshooting
- Include: Remote device, circuit ID, purpose

description Link to R2 G0/0 - Circuit ABC123

Verification Commands

Basic Verification:

```
show running-config      # Display active configuration
show startup-config      # Display saved configuration
show version             # IOS version, uptime, hardware
show interfaces           # All interfaces detailed info
show ip interface brief   # IPv4 interface summary
show ipv6 interface brief # IPv6 interface summary
show protocols           # Layer 3 protocol status
show ip route            # IPv4 routing table
show ipv6 route          # IPv6 routing table
```

Interface Specific:

```
show interfaces [type number] # Detailed single interface
show ip interface [type number] # IPv4 info for interface
show ipv6 interface [type number] # IPv6 info for interface
show controllers [type number] # Physical layer info (DCE/DTE)
```

Connectivity Testing:

```
ping [ip-address]        # IPv4 ping
ping ipv6 [ipv6-address]  # IPv6 ping
traceroute [ip-address]   # IPv4 traceroute
traceroute ipv6 [ipv6-address] # IPv6 traceroute
```

Configuration Management:

```
show history              # Show command history
terminal history size [number] # Set history buffer size
copy running-config startup-config # Save configuration
copy startup-config running-config # Load saved config
erase startup-config      # Delete startup config
reload                    # Restart device
```

Interface Status Codes

show ip interface brief output:

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.1.1	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/0/0	10.1.1.1	YES	manual	up	down

Status Meanings:

- **up/up** - Interface working properly
- **up/down** - Physical layer up, data link layer down (no keepalives, wrong encapsulation)
- **down/down** - Interface disabled or cable problem
- **administratively down/down** - Interface shut down with `shutdown` command

Configuration Example - Complete Router Setup

```

! Basic Router Configuration
enable
configure terminal
hostname R1
enable secret Cisco123
no ip domain-lookup

! Console Line
line console 0
  password console123
  login
  logging synchronous
  exec-timeout 0 0
  exit

! VTY Lines
line vty 0 4
  password vty123
  login
  transport input ssh
  exec-timeout 5 0
  exit

! Banner
banner motd # Authorized Access Only! #

! Encrypt Passwords

```

```
service password-encryption
```

```
! IPv6 Routing
```

```
ipv6 unicast-routing
```

```
! Interface G0/0 - LAN
```

```
interface gigabitethernet 0/0
```

```
description LAN Interface
```

```
ip address 192.168.1.1 255.255.255.0
```

```
ipv6 address 2001:db8:acad:1::1/64
```

```
ipv6 address fe80::1 link-local
```

```
no shutdown
```

```
exit
```

```
! Interface G0/1 - WAN
```

```
interface gigabitethernet 0/1
```

```
description WAN to ISP
```

```
ip address 209.165.200.225 255.255.255.224
```

```
ipv6 address 2001:db8:acad:2::1/64
```

```
ipv6 address fe80::1 link-local
```

```
no shutdown
```

```
exit
```

```
! Save Configuration
```

```
end
```

```
copy running-config startup-config
```

Essential Concepts

1. Router vs Switch Configuration Differences:

- **Router interfaces:** Shutdown by default, require `no shutdown`
- **Switch ports:** Up by default (unless admin down)
- **Router:** Requires IP address on each interface for routing
- **Switch:** Uses SVI (VLAN interface) for management only

2. Configuration File Locations:

- **Running-config:** RAM (volatile, lost on reboot)
- **Startup-config:** NVRAM (non-volatile, survives reboot)
- **IOS:** Flash memory
- Must save running to startup to preserve changes

3. Router Boot Sequence:

- POST → Bootstrap → IOS Load → Config Load
- Can interrupt with Break sequence for ROMMON

4. IPv6 Routing Requirement:

- Must enable `ipv6 unicast-routing` globally
- Without it, router won't forward IPv6 packets
- Not required on switches

5. Serial Interface Considerations:

- One end is DCE (provides clocking with `clock rate`)
 - Other end is DTE (receives clock)
 - Use `show controllers` to determine DCE/DTE
 - Most new routers use Ethernet WAN interfaces instead
-
-

Chapter 11: IPv4 Addressing

Key Terminology

IP Address Components:

- **Network Portion** - Identifies the network
- **Host Portion** - Identifies the host within network
- **Subnet Mask** - Defines network/host boundary
- **Prefix Length** - Number of network bits (CIDR notation)
- **CIDR** (Classless Inter-Domain Routing) - Modern IP addressing

Address Classes (Legacy):

- **Class A:** 1.0.0.0 to 126.255.255.255 (/8 default), first octet 1-126
- **Class B:** 128.0.0.0 to 191.255.255.255 (/16 default), first octet 128-191
- **Class C:** 192.0.0.0 to 223.255.255.255 (/24 default), first octet 192-223
- **Class D:** 224.0.0.0 to 239.255.255.255 (Multicast)
- **Class E:** 240.0.0.0 to 255.255.255.255 (Experimental)

Address Types:

- **Network Address** - All host bits are 0 (identifies network)

- **Broadcast Address** - All host bits are 1 (all hosts in network)
- **Host Address** - Usable addresses between network and broadcast
- **Unicast** - Single destination
- **Broadcast** - All hosts in network
- **Multicast** - Specific group of hosts

Special Addresses:

- **0.0.0.0** - This host, this network
- **127.0.0.0/8** - Loopback (127.0.0.1 most common)
- **169.254.0.0/16** - APIPA (Automatic Private IP Addressing)
- **255.255.255.255** - Limited broadcast (local network)

Private Address Ranges (RFC 1918):

- **10.0.0.0/8** - 10.0.0.0 to 10.255.255.255 (Class A)
- **172.16.0.0/12** - 172.16.0.0 to 172.31.255.255 (Class B)
- **192.168.0.0/16** - 192.168.0.0 to 192.168.255.255 (Class C)

Subnet Terminology:

- **Subnetting** - Dividing network into smaller networks
- **Subnet** - Subdivision of network
- **VLSM** (Variable Length Subnet Masking) - Different size subnets
- **CIDR** - Classless addressing, variable prefix lengths
- **Supernet** - Combining networks (aggregation)
- **Route Summarization** - Representing multiple routes as one

Subnet Masks

Common Subnet Masks:

CIDR	Subnet Mask	Binary	Hosts
/24	255.255.255.0	11111111.11111111.11111111.00000000	254
/25	255.255.255.128	11111111.11111111.11111111.10000000	126
/26	255.255.255.192	11111111.11111111.11111111.11000000	62
/27	255.255.255.224	11111111.11111111.11111111.11100000	30
/28	255.255.255.240	11111111.11111111.11111111.11110000	14
/29	255.255.255.248	11111111.11111111.11111111.11111000	6
/30	255.255.255.252	11111111.11111111.11111111.11111100	2
/31	255.255.255.254	11111111.11111111.11111111.11111110	2 (point-to-point)
/32	255.255.255.255	11111111.11111111.11111111.11111111	1 (host route)

Formula: Number of Hosts:

Usable Hosts = $2^{(\text{host bits})} - 2$

/24 = $2^8 - 2 = 256 - 2 = 254$ hosts

/25 = $2^7 - 2 = 128 - 2 = 126$ hosts

/26 = $2^6 - 2 = 64 - 2 = 62$ hosts

/27 = $2^5 - 2 = 32 - 2 = 30$ hosts

/28 = $2^4 - 2 = 16 - 2 = 14$ hosts

/29 = $2^3 - 2 = 8 - 2 = 6$ hosts

/30 = $2^2 - 2 = 4 - 2 = 2$ hosts

-2 accounts for network address and broadcast address

Formula: Number of Subnets:

Number of Subnets = $2^{(\text{borrowed bits})}$

Borrow 1 bit: $2^1 = 2$ subnets

Borrow 2 bits: $2^2 = 4$ subnets

Borrow 3 bits: $2^3 = 8$ subnets

Borrow 4 bits: $2^4 = 16$ subnets

Subnetting Process

Steps to Subnet:

1. Determine requirements (networks needed, hosts per network)
2. Calculate bits to borrow
3. Determine new subnet mask
4. Calculate subnet ranges

5. Identify network, first host, last host, broadcast for each subnet

Example: Subnet 192.168.1.0/24 into 4 subnets

Step 1: Need 4 subnets

- $2^2 = 4$, so borrow 2 bits

Step 2: New subnet mask

- Original: /24 (255.255.255.0)
- Borrow 2: /26 (255.255.255.192)

Step 3: Subnet size

- Host bits: $32 - 26 = 6$ bits
- Block size: $2^6 = 64$
- Usable hosts: $64 - 2 = 62$

Step 4: Subnet ranges (increment by 64)

Subnet 0: 192.168.1.0/26

Network: 192.168.1.0

First Host: 192.168.1.1

Last Host: 192.168.1.62

Broadcast: 192.168.1.63

Subnet 1: 192.168.1.64/26

Network: 192.168.1.64

First Host: 192.168.1.65

Last Host: 192.168.1.126

Broadcast: 192.168.1.127

Subnet 2: 192.168.1.128/26

Network: 192.168.1.128

First Host: 192.168.1.129

Last Host: 192.168.1.190

Broadcast: 192.168.1.191

Subnet 3: 192.168.1.192/26

Network: 192.168.1.192

First Host: 192.168.1.193

Last Host: 192.168.1.254

Broadcast: 192.168.1.255

VLSM (Variable Length Subnet Masking)

Purpose:

- Efficient use of address space
- Different sized subnets based on requirements
- Subnet the subnets

VLSM Example: Given 192.168.1.0/24, create:

- Branch A: 100 hosts
- Branch B: 50 hosts
- Branch C: 25 hosts
- 2 point-to-point links

Solution:

Branch A (100 hosts): Need /25 (126 hosts)

192.168.1.0/25

Network: 192.168.1.0

Range: 192.168.1.1 - 192.168.1.126

Broadcast: 192.168.1.127

Branch B (50 hosts): Need /26 (62 hosts)

192.168.1.128/26

Network: 192.168.1.128

Range: 192.168.1.129 - 192.168.1.190

Broadcast: 192.168.1.191

Branch C (25 hosts): Need /27 (30 hosts)

192.168.1.192/27

Network: 192.168.1.192

Range: 192.168.1.193 - 192.168.1.222

Broadcast: 192.168.1.223

Link 1 (2 hosts): Need /30 (2 hosts)

192.168.1.224/30

Network: 192.168.1.224

Range: 192.168.1.225 - 192.168.1.226

Broadcast: 192.168.1.227

Link 2 (2 hosts): Need /30 (2 hosts)

192.168.1.228/30

Network: 192.168.1.228

Range: 192.168.1.229 - 192.168.1.230

Broadcast: 192.168.1.231

Remaining: 192.168.1.232 - 192.168.1.255 (available for growth)

Route Summarization (Supernetting)

Purpose:

- Reduce routing table size
- Improve routing efficiency
- Aggregate multiple networks into one route

Requirements:

- Networks must be contiguous

- Must be able to find common prefix

Example: Summarize these networks:

192.168.16.0/24
192.168.17.0/24
192.168.18.0/24
192.168.19.0/24

Process:

1. Convert to binary and find common bits

192.168.16.0 = 11000000.10101000.00010000.00000000
192.168.17.0 = 11000000.10101000.00010001.00000000
192.168.18.0 = 11000000.10101000.00010010.00000000
192.168.19.0 = 11000000.10101000.00010011.00000000
↑ Common: 22 bits

2. Summary route: **192.168.16.0/22**

- Covers 192.168.16.0 through 192.168.19.255

Subnet Planning Best Practices

Design Methodology:

1. **Largest to Smallest** - Allocate largest subnets first
2. **Leave Room for Growth** - Don't use all address space
3. **Document Everything** - Maintain IP addressing scheme
4. **Use VLSM** - Efficient use of addresses
5. **Consider Route Summarization** - Plan for aggregation

Common Requirements:

Point-to-Point Links: /30 or /31
Small Office (< 30): /27
Medium Office (< 60): /26
Large Office (< 120): /25
Department (< 250): /24

Essential Concepts

1. Magic Number (Block Size):

- Quick way to find subnet boundaries
- Magic Number = 256 - Subnet Octet
- /26: 256 - 192 = 64 (increment by 64)
- /27: 256 - 224 = 32 (increment by 32)
- /28: 256 - 240 = 16 (increment by 16)

2. Determining Network Address:

- AND IP address with subnet mask
- All host bits become 0

3. Determining Broadcast Address:

- OR IP address with inverted subnet mask
- All host bits become 1

4. Subnet Zero and All-Ones Subnet:

- Modern networks use all subnets (including first and last)
- Legacy equipment excluded subnet zero
- `ip subnet-zero` (enabled by default on modern IOS)

5. /31 Point-to-Point Links:

- RFC 3021 allows /31 for point-to-point
- No network or broadcast address needed
- 2 usable addresses (both used)
- Saves address space

IOS Commands

```
# Display IP Configuration
show ip interface brief      # Interface IP summary
show running-config | include ip  # Show IP-related config
show ip route                # Routing table

# Interface IP Configuration
interface gigabitethernet 0/0
ip address [ip] [subnet-mask]  # Set IP and mask
no shutdown
exit
```

```
# Secondary IP (multiple IPs on one interface)
interface gigabitethernet 0/0
  ip address 192.168.1.1 255.255.255.0
  ip address 192.168.2.1 255.255.255.0 secondary
exit

# Helper Commands
show ip interface [type number]  # Detailed IP info
show protocols                    # Layer 3 protocol status

# Enable Subnet Zero (default on)
ip subnet-zero                    # Allow use of subnet zero
```

Quick Subnetting Reference

Memorize These Values:

/24 = 256 addresses, 254 hosts
/25 = 128 addresses, 126 hosts (block size 128)
/26 = 64 addresses, 62 hosts (block size 64)
/27 = 32 addresses, 30 hosts (block size 32)
/28 = 16 addresses, 14 hosts (block size 16)
/29 = 8 addresses, 6 hosts (block size 8)
/30 = 4 addresses, 2 hosts (block size 4)

Binary Values for Last Octet:

128 = 10000000 = /25
192 = 11000000 = /26
224 = 11100000 = /27
240 = 11110000 = /28
248 = 11111000 = /29
252 = 11111100 = /30
254 = 11111110 = /31
255 = 11111111 = /32

Chapter 12: IPv6 Addressing

Key Terminology

IPv6 Basics:

- **128-bit Address** - 4 times longer than IPv4 (32 bits)
- **Hexadecimal Notation** - Written in hex (not decimal)
- **Eight Hextets** - 8 groups of 16 bits each
- **Prefix Length** - Network portion (no subnet mask)
- **Interface ID** - Host portion (last 64 bits typically)

IPv6 Address Types:

- **GUA** (Global Unicast Address) - Routable internet address
- **LLA** (Link-Local Address) - Local link only (FE80::/10)
- **ULA** (Unique Local Address) - Private addressing (FC00::/7, FD00::/8 used)
- **Multicast** - One-to-many (FF00::/8)
- **Anycast** - Nearest instance of multiple identical addresses

Special Addresses:

- **::** - All zeros (unspecified address)
- **::1** - Loopback (equivalent to 127.0.0.1)
- **::/0** - Default route
- **FF02::1** - All nodes multicast
- **FF02::2** - All routers multicast
- **FF02::1:FFxx:xxxx** - Solicited-node multicast

IPv6 Prefixes:

- **2000::/3** - Global unicast range (2000:: to 3FFF::)
- **FE80::/10** - Link-local range
- **FC00::/7** - Unique local (private)
- **FF00::/8** - Multicast
- **/64** - Standard subnet size (recommended)
- **/48** - Typical site allocation
- **/32** - ISP allocation

IPv6 Address Format

Full Format:

```
2001:0DB8:0000:0001:0000:0000:0000:0001
```

Rule 1 - Omit Leading Zeros:

```
2001:DB8:0:1:0:0:0:1
```

Rule 2 - Double Colon (Consecutive Zeros):

```
2001:DB8:0:1::1
```

- Can only use :: once per address
- Represents one or more hextets of all zeros

Examples:

Full: 2001:0DB8:0000:0000:0000:0000:0000:0001

Compressed: 2001:DB8::1

Full: FE80:0000:0000:0000:0123:4567:89AB:CDEF

Compressed: FE80::123:4567:89AB:CDEF

Full: FF02:0000:0000:0000:0000:0000:0000:0001

Compressed: FF02::1

IPv6 Address Configuration Methods

1. Static Configuration:

- Manually configure GUA and/or LLA
- Full control over addresses

```
interface g0/0
  ipv6 address 2001:DB8:ACAD:1::1/64
  ipv6 address FE80::1 link-local
  no shutdown
```

2. SLAAC (Stateless Address Autoconfiguration):

- Host creates own GUA from RA (Router Advertisement)
- Uses prefix from RA + own Interface ID

- No server required (stateless)
- Process:
 1. Host sends RS (Router Solicitation)
 2. Router sends RA with prefix
 3. Host creates GUA: Prefix + Interface ID
 4. Host uses DAD to verify uniqueness

3. DHCPv6:

- **Stateful DHCPv6** - Server tracks addresses (like DHCPv4)
- **Stateless DHCPv6** - Server provides options only (DNS, domain)

RA Flags (Router Advertisement):

- **A Flag** (Autonomous) - Use SLAAC
- **O Flag** (Other) - Use Stateless DHCPv6 for options
- **M Flag** (Managed) - Use Stateful DHCPv6
- **Combinations:**
 - A=1, O=0, M=0 → SLAAC only
 - A=1, O=1, M=0 → SLAAC + Stateless DHCPv6
 - A=0, O=1, M=1 → Stateful DHCPv6

Link-Local Addresses (LLA)

Characteristics:

- Required on every IPv6-enabled interface
- Not routable beyond local link
- Used for local communication (neighbor discovery, routing)
- Range: FE80::/10
- Typically FE80::/64 in practice

LLA Creation Methods:

1. Automatically (EUI-64):

FE80::/64 + Interface ID (from MAC)
 Example: FE80::0123:45FF:FE67:89AB

2. Random:

- Many OSes use privacy extensions
- Random 64-bit Interface ID

3. Manual:

```
interface g0/0
  ipv6 address fe80::1 link-local
```

- Recommended for routers (easier to remember)
- Common choices: FE80::1, FE80::2, etc.

EUI-64 Process

Modified EUI-64 Algorithm:

1. Take MAC address (48 bits): 00:1A:2B:3C:4D:5E
2. Insert FF:FE in middle: 00:1A:2B:**FF:FE**:3C:4D:5E
3. Flip 7th bit (U/L bit): 02:1A:2B:FF:FE:3C:4D:5E
4. Result: 021A:2BFF:FE3C:4D5E

Example:

```
MAC: 00:1A:2B:3C:4D:5E
Prefix: 2001:DB8:ACAD:1::/64
GUA: 2001:DB8:ACAD:1:021A:2BFF:FE3C:4D5E
```

IOS Configuration (EUI-64):

```
interface g0/0
  ipv6 address 2001:DB8:ACAD:1::/64 eui-64
```

Global Unicast Address (GUA)

Structure:

| Global Routing Prefix | Subnet ID | Interface ID |
(48 bits) (16 bits) (64 bits)

Typical breakdown of 2001:DB8:ACAD:1::1/64:

2001:DB8:ACAD = Global Routing Prefix (assigned by ISP)

1 = Subnet ID (your subnetting)

::1 = Interface ID (host portion)

Characteristics:

- Globally routable
- Equivalent to IPv4 public address
- Starts with 2000::/3 range
- Standard subnet: /64

Unique Local Address (ULA)

Characteristics:

- Private addressing (like RFC 1918 in IPv4)
- Range: FC00::/7 (FD00::/8 commonly used)
- Not routable on internet
- Can be routed within organization

Format:

FD00::/8

Example: FD00:1234:5678:1::1/64

IPv6 Multicast Addresses

Important Multicast Addresses:

FF02::1 - All nodes (like IPv4 broadcast)
FF02::2 - All routers
FF02::5 - OSPF routers
FF02::6 - OSPF DR/BDR
FF02::9 - RIP routers
FF02::A - EIGRP routers
FF02::1:2 - DHCP agents
FF02::1:FFxx:xxxx - Solicited-node multicast

Solicited-Node Multicast:

- Format: FF02::1:FF + last 24 bits of IPv6 address
- Used for neighbor discovery (NS/NA)
- Example:
 - IPv6: 2001:DB8::1234:5678
 - Solicited-node: FF02::1:FF34:5678

IPv6 Subnetting

Standard Practice:

- Use /64 for all subnets
- Subnet in fourth hextet (16-bit subnet field)
- Provides 65,536 subnets
- Each subnet has 18 quintillion host addresses

Example - Subnet 2001:DB8:ACAD::/48:

Subnet 0: 2001:DB8:ACAD:0000::/64
Subnet 1: 2001:DB8:ACAD:0001::/64
Subnet 2: 2001:DB8:ACAD:0002::/64
...
Subnet 10: 2001:DB8:ACAD:000A::/64
...
Subnet 255: 2001:DB8:ACAD:00FF::/64
...
Subnet 65535: 2001:DB8:ACAD:FFFF::/64

Simplified Subnetting:

Given: 2001:DB8:ACAD::/48

Need: 4 subnets

Solution:

Subnet A: 2001:DB8:ACAD:1::/64

Subnet B: 2001:DB8:ACAD:2::/64

Subnet C: 2001:DB8:ACAD:3::/64

Subnet D: 2001:DB8:ACAD:4::/64

Essential Concepts

1. Why IPv6?

- IPv4 exhaustion (4.3 billion addresses)
- IPv6 provides 340 undecillion addresses
- Simplified header (faster processing)
- Built-in security (IPsec)
- No broadcasts (uses multicast)
- Autoconfiguration (SLAAC)

2. Dual Stack:

- Run IPv4 and IPv6 simultaneously
- Common transition method
- Devices maintain both protocol stacks

```
interface g0/0
```

```
ip address 192.168.1.1 255.255.255.0
```

```
ipv6 address 2001:DB8::1/64
```

3. IPv6 Advantages:

- Larger address space
- No NAT required
- Efficient routing
- Better mobility support
- Mandatory IPsec support

4. IPv6 vs IPv4 Key Differences:

- No broadcast (uses multicast)

- No ARP (uses Neighbor Discovery)
- No DHCP required (SLAAC)
- Simplified header
- Built-in QoS support

IOS Commands

```
# Enable IPv6 Routing
ipv6 unicast-routing      # Global config - required on routers

# Interface Configuration
interface gigabitethernet 0/0
  ipv6 address [ipv6-address/prefix]    # Static GUA
  ipv6 address [ipv6-address] link-local # Static LLA
  ipv6 address [prefix] eui-64          # EUI-64 GUA
  ipv6 enable                          # Enable IPv6, auto LLA
  no shutdown
  exit

# Verification
show ipv6 interface brief      # Interface summary
show ipv6 interface [type number] # Detailed interface info
show ipv6 route                # IPv6 routing table
show ipv6 neighbors            # Neighbor table (like ARP)

# Connectivity Testing
ping ipv6 [ipv6-address]      # IPv6 ping
traceroute ipv6 [ipv6-address] # IPv6 traceroute

# Static Routes
ipv6 route [destination/prefix] [next-hop | exit-interface]
ipv6 route ::/0 [next-hop]      # Default route

# DHCPv6 Configuration (Basic)
ipv6 dhcp pool POOL1
  address prefix 2001:DB8:ACAD:1::/64
  dns-server 2001:DB8:ACAD::100
  domain-name example.com
  exit
interface g0/0
  ipv6 dhcp server POOL1
  ipv6 nd other-config-flag      # Set O flag for stateless
```

```
# or
ipv6 nd managed-config-flag      # Set M flag for stateful
exit

# Debugging
debug ipv6 nd                    # Debug neighbor discovery
debug ipv6 packet                # Debug IPv6 packets
undebug all                      # Turn off all debugging
```

Configuration Example

```
# Complete IPv6 Router Configuration
enable
configure terminal
hostname R1
ipv6 unicast-routing            # Enable IPv6 routing

# Interface G0/0 - LAN 1
interface gigabitethernet 0/0
  description LAN 1
  ipv6 address 2001:DB8:ACAD:1::1/64
  ipv6 address FE80::1 link-local
  no shutdown
  exit

# Interface G0/1 - LAN 2
interface gigabitethernet 0/1
  description LAN 2
  ipv6 address 2001:DB8:ACAD:2::1/64
  ipv6 address FE80::1 link-local
  no shutdown
  exit

# Interface S0/0/0 - WAN Link
interface serial 0/0/0
  description WAN to R2
  ipv6 address 2001:DB8:ACAD:12::1/64
  ipv6 address FE80::1 link-local
  clock rate 128000
  no shutdown
  exit

# Default Route
```

```
ipv6 route ::/0 2001:DB8:ACAD:12::2
```

```
end
```

```
copy running-config startup-config
```

IPv6 Address Examples

Valid IPv6 Addresses:

2001:DB8::1

FE80::1

::1

::

2001:0DB8:0000:0001:0000:0000:0000:0001

FF02::1

Invalid IPv6 Addresses:

2001:DB8:G123::1 # G is not hex

2001:DB8:::1 # Too many colons

2001:DB8::1::2 # Double colon used twice

Chapter 13: ICMP

Key Terminology

ICMP (Internet Control Message Protocol):

- Network layer protocol
- Reports errors and provides diagnostics
- Used by ping and traceroute
- Encapsulated in IP packets
- No reliability mechanism

ICMPv4 Message Types:

- **Type 0** - Echo Reply (ping response)
- **Type 3** - Destination Unreachable
- **Type 5** - Redirect
- **Type 8** - Echo Request (ping)
- **Type 11** - Time Exceeded (TTL=0)

ICMPv6 Message Types:

- **Type 1** - Destination Unreachable
- **Type 128** - Echo Request
- **Type 129** - Echo Reply
- **Type 133** - Router Solicitation (RS)
- **Type 134** - Router Advertisement (RA)
- **Type 135** - Neighbor Solicitation (NS)
- **Type 136** - Neighbor Advertisement (NA)

ICMP Components:

- **Type** - Message category
- **Code** - Specific reason within type
- **Checksum** - Error detection
- **Data** - Original packet that caused error

ICMP Messages

Destination Unreachable (Type 3):

Code 0 - Network unreachable
Code 1 - Host unreachable
Code 2 - Protocol unreachable
Code 3 - Port unreachable
Code 4 - Fragmentation needed but DF set
Code 6 - Network unknown
Code 7 - Host unknown
Code 9 - Network administratively prohibited
Code 10 - Host administratively prohibited
Code 13 - Communication administratively prohibited

Time Exceeded (Type 11):

Code 0 - TTL expired in transit (used by traceroute)
Code 1 - Fragment reassembly time exceeded

Redirect (Type 5):

- Router informs host of better route

- Host updates routing table

Code 0 - Redirect for network

Code 1 - Redirect for host

Ping (Packet Internet Groper)

Purpose:

- Tests connectivity
- Verifies IP configuration
- Measures round-trip time (RTT)

How Ping Works:

1. Source sends ICMP Echo Request (Type 8)
2. Destination receives and processes
3. Destination sends ICMP Echo Reply (Type 0)
4. Source receives reply and calculates RTT

Ping Output (Cisco IOS):

```
Router# ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Ping Characters:

```
! - Echo reply received (success)
. - No response (timeout)
U - Destination unreachable
C - Congestion encountered
I - User interrupted
? - Unknown packet type
& - Packet lifetime exceeded
```

Extended Ping (Cisco):

```
Router# ping
Protocol [ip]:
Target IP address: 192.168.1.10
Repeat count [5]: 100
Datagram size [100]: 1500
Timeout in seconds [2]: 5
Extended commands [n]: y
  Source address or interface: 10.1.1.1
  Type of service [0]:
  Set DF bit in IP header? [no]:
  Validate reply data? [no]:
  Data pattern [0xABCD]:
  Loose, Strict, Record, Timestamp, Verbose[none]:
  Sweep range of sizes [n]:
```

Traceroute

Purpose:

- Traces path packets take to destination
- Identifies each hop along the way
- Diagnoses routing issues
- Shows where failures occur

How Traceroute Works:

1. Sends packets with incrementing TTL values
2. TTL=1 for first packet (reaches first router)
3. First router decrements TTL to 0, drops packet
4. First router sends ICMP Time Exceeded (Type 11)
5. Source identifies first hop from ICMP source
6. TTL=2 for second packet (reaches second router)
7. Process repeats until destination reached
8. Destination sends ICMP Echo Reply (Type 0) or Port Unreachable (Type 3, Code 3)

Traceroute Output (Cisco IOS):

```
Router# traceroute 8.8.8.8
```

Type escape sequence to abort.

Tracing the route to 8.8.8.8

```
 1 10.1.1.1 4 msec 4 msec 4 msec
 2 172.16.1.1 12 msec 12 msec 12 msec
 3 209.165.200.1 16 msec 16 msec 20 msec
 4 8.8.8.8 24 msec 28 msec 24 msec
```

Traceroute Characters (Cisco):

nn msec - Round-trip time for each probe

* - Timeout (no response)

U - Destination unreachable

N - Network unreachable

P - Protocol unreachable

H - Host unreachable

A - Administratively prohibited

Platform Differences:

Cisco IOS: Uses UDP packets (port 33434+)

Windows: Uses ICMP Echo Request

Linux: Uses UDP packets (port 33434+)

ICMPv6 Differences

ICMPv6 Enhancements:

- Incorporates ARP functionality (Neighbor Discovery)
- Router discovery (RS/RA)
- Duplicate Address Detection (DAD)
- More efficient than ICMPv4

Key ICMPv6 Messages:

Type 1 - Destination Unreachable
Type 2 - Packet Too Big
Type 3 - Time Exceeded
Type 4 - Parameter Problem
Type 128 - Echo Request
Type 129 - Echo Reply
Type 133 - Router Solicitation (RS)
Type 134 - Router Advertisement (RA)
Type 135 - Neighbor Solicitation (NS)
Type 136 - Neighbor Advertisement (NA)
Type 137 - Redirect Message

Essential Concepts

1. ICMP is Informational:

- Does not correct errors
- Reports conditions to source
- Source decides how to respond

2. ICMP and Security:

- Can be used for reconnaissance (network mapping)
- Often blocked by firewalls
- Ping of death attacks (historical)
- ICMP tunneling (covert channels)
- Best practice: Allow needed ICMP, block rest

3. Troubleshooting with ICMP:

- **Ping fails:** Connectivity issue or firewall
- **Traceroute times out:** Routing problem at timeout point
- **Destination unreachable:** No route or access blocked
- **Time exceeded:** Routing loop or TTL too small

4. ICMP Rate Limiting:

- Routers may rate-limit ICMP
- Prevents ICMP flooding
- May affect traceroute accuracy

5. MTU Discovery:

- Uses ICMP Fragmentation Needed (Type 3, Code 4)

- Determines maximum transmission unit
- Path MTU Discovery (PMTUD)

IOS Commands

Ping Commands

```
ping [ip-address]          # Basic IPv4 ping
ping ipv6 [ipv6-address]   # IPv6 ping
ping                      # Extended ping (interactive)
```

Common Ping Options

```
ping 192.168.1.10 repeat 100  # Send 100 packets
ping 192.168.1.10 size 1500   # Set packet size
ping 192.168.1.10 timeout 5   # Set timeout
ping 192.168.1.10 source g0/0 # Specify source interface
```

Traceroute Commands

```
traceroute [ip-address]      # IPv4 traceroute
traceroute ipv6 [ipv6-address] # IPv6 traceroute
```

Verification

```
show ip interface [type number] # Check if ICMP enabled
show ipv6 interface [type number] # IPv6 interface info
```

ICMP Control (Rarely Used)

```
interface g0/0
  no ip redirects      # Disable ICMP redirects
  no ip unreachable    # Disable unreachable
  no ipv6 redirects    # Disable IPv6 redirects
exit
```

Debugging

```
debug ip icmp          # Debug ICMPv4
debug ipv6 icmp        # Debug ICMPv6
undebug all            # Turn off debugging
```

Troubleshooting Scenarios

Scenario 1: Ping Fails Completely

```
Router# ping 192.168.1.10
```

```
.....
```

```
Success rate is 0 percent (0/5)
```

Possible Causes:

- No route to destination
- Destination device down
- Firewall blocking ICMP
- Wrong IP address
- Interface down

Scenario 2: Some Pings Fail

```
Router# ping 192.168.1.10
```

```
!!..!!
```

```
Success rate is 80 percent (4/5)
```

Possible Causes:

- Intermittent connectivity
- Congestion
- Interface errors
- Duplex mismatch

Scenario 3: Traceroute Shows Loop

```
Router# traceroute 10.1.1.10
```

```
 1 10.1.1.1 4 msec 4 msec 4 msec
```

```
 2 172.16.1.1 12 msec 12 msec 12 msec
```

```
 3 10.1.1.1 16 msec 16 msec 16 msec
```

```
 4 172.16.1.1 20 msec 20 msec 20 msec
```

```
...
```

Cause: Routing loop between 10.1.1.1 and 172.16.1.1

Scenario 4: Traceroute Times Out Mid-Path

```
Router# traceroute 8.8.8.8
```

```
 1 10.1.1.1 4 msec 4 msec 4 msec
 2 172.16.1.1 12 msec 12 msec 12 msec
 3 * * *
 4 * * *
```

Possible Causes:

- Router not sending ICMP Time Exceeded
- Firewall blocking ICMP
- Routing black hole

Host Commands

Windows:

```
ping [ip-address]           # Basic ping
ping -t [ip-address]        # Continuous ping
ping -n 100 [ip-address]    # Send 100 packets
ping -l 1500 [ip-address]   # Set packet size
tracert [ip-address]        # Traceroute
pathping [ip-address]       # Combined ping/traceroute
```

Linux:

```
ping [ip-address]           # Continuous ping (Ctrl+C to stop)
ping -c 100 [ip-address]    # Send 100 packets
ping -s 1500 [ip-address]   # Set packet size
ping -i 0.5 [ip-address]    # 0.5 second interval
traceroute [ip-address]     # Traceroute
mtr [ip-address]            # Advanced traceroute (real-time)
```

Chapter 14: Transport Layer

Key Terminology

Transport Layer Functions:

- **Segmentation** - Divide application data into segments
- **Multiplexing** - Multiple applications share network
- **Session Management** - Track conversations

- **Reliability** (TCP) - Ensure delivery
- **Flow Control** (TCP) - Prevent overwhelming receiver
- **Error Recovery** (TCP) - Retransmit lost segments

Protocols:

- **TCP** (Transmission Control Protocol) - Connection-oriented, reliable
- **UDP** (User Datagram Protocol) - Connectionless, best-effort

TCP Characteristics:

- Connection-oriented (three-way handshake)
- Reliable delivery (acknowledgments)
- Ordered delivery (sequencing)
- Flow control (windowing)
- Error detection and recovery

UDP Characteristics:

- Connectionless (no handshake)
- Best-effort delivery (no guarantees)
- No sequencing
- No flow control
- Minimal overhead (faster)

Port Numbers:

- **Well-Known Ports** - 0-1023 (server applications)
- **Registered Ports** - 1024-49151 (user applications)
- **Dynamic/Private Ports** - 49152-65535 (client source ports)

Socket:

- Combination of IP address and port number
- Uniquely identifies connection endpoint
- Format: IP:Port (e.g., 192.168.1.10:80)

TCP Segment Format

TCP Header Fields:

Source Port (16 bits)	- Sender's port
Destination Port (16 bits)	- Receiver's port
Sequence Number (32 bits)	- Byte number of first data byte
Acknowledgment Number (32)	- Next expected byte
Data Offset (4 bits)	- Header length
Reserved (6 bits)	- Future use
Flags (6 bits)	- Control flags
Window Size (16 bits)	- Flow control
Checksum (16 bits)	- Error detection
Urgent Pointer (16 bits)	- Urgent data location
Options (variable)	- Additional features
Data (variable)	- Application data

TCP Flags:

URG - Urgent pointer field significant
 ACK - Acknowledgment field significant
 PSH - Push function
 RST - Reset connection
 SYN - Synchronize sequence numbers
 FIN - No more data from sender

TCP Three-Way Handshake

Connection Establishment:

Client	Server
1. SYN (SEQ=100)	
----->	
2. SYN-ACK (SEQ=300, ACK=101)	
<-----	
3. ACK (SEQ=101, ACK=301)	
----->	
Connection Established	

Step 1 (SYN):

- Client sends SYN flag

- Initial sequence number (ISN)
- Requests connection

Step 2 (SYN-ACK):

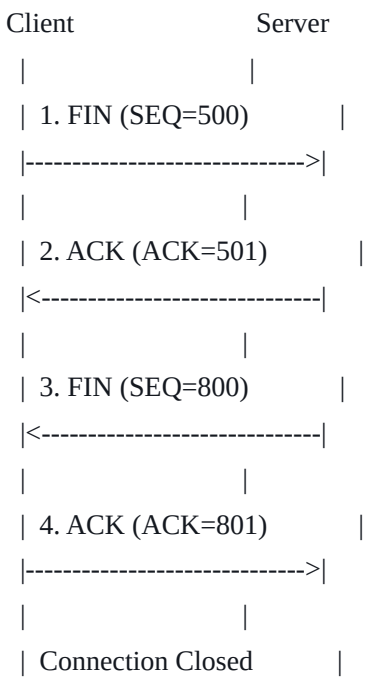
- Server responds with SYN and ACK flags
- Acknowledges client's SYN
- Sends own ISN

Step 3 (ACK):

- Client acknowledges server's SYN
- Connection established
- Data transfer can begin

TCP Connection Termination

Four-Way Termination:



RST (Reset):

- Abrupt connection termination
- Used for errors or rejected connections
- No graceful shutdown

TCP Flow Control

Window Size:

- Receiver advertises buffer space
- Sender limits data to window size
- Prevents buffer overflow

Sliding Window:

Window Size = 3 segments

Send: [1][2][3] | [4][5][6]

↑ Window

After ACK for 1,2,3:

Send: [4][5][6] | [7][8][9]

↑ Window slides

Window Scaling:

- Window size field is 16 bits (max 65,535)
- Window scaling option allows larger windows
- Important for high-bandwidth links

Zero Window:

- Receiver buffer full
- Tells sender to stop
- Sender probes with small packets
- Resumes when window opens

TCP Reliability

Acknowledgment Methods:

Positive Acknowledgment:

- Receiver sends ACK for received segments
- ACK number indicates next expected byte

Retransmission:

- Sender retransmits if no ACK received
- Uses retransmission timer
- Exponential backoff on multiple failures

Example:

Client	Server
SEQ=100 (Data: bytes 100-199)	
----->	
ACK=200 (Next byte expected)	
<-----	
SEQ=200 (Data: bytes 200-299)	
---X (lost)	
(Timeout, retransmit)	
SEQ=200 (Data: bytes 200-299)	
----->	
ACK=300	
<-----	

UDP Datagram Format

UDP Header (8 bytes):

Source Port (16 bits)	- Sender's port
Destination Port (16 bits)	- Receiver's port
Length (16 bits)	- Total length (header + data)
Checksum (16 bits)	- Error detection (optional in IPv4)
Data (variable)	- Application data

UDP Characteristics:

- Much smaller header (8 bytes vs 20+ for TCP)
- No connection setup delay
- No retransmission delay
- No sequencing overhead
- No flow control overhead

Well-Known Port Numbers

TCP Ports:

20 - FTP Data
21 - FTP Control
22 - SSH
23 - Telnet
25 - SMTP (email)
53 - DNS (also UDP)
80 - HTTP
110 - POP3 (email)
143 - IMAP (email)
443 - HTTPS
3389 - RDP (Remote Desktop)

UDP Ports:

53 - DNS (also TCP)
67 - DHCP Server
68 - DHCP Client
69 - TFTP
123 - NTP (Network Time Protocol)
161 - SNMP
162 - SNMP Trap
514 - Syslog

Both TCP and UDP:

53 - DNS

Transport Layer Multiplexing

Socket Pairs:

- Combination of source and destination sockets
- Example: 192.168.1.10:49152 → 8.8.8.8:53

Multiple Connections:

Client (192.168.1.10)	Servers
Port 49152 ----->	8.8.8.8:53 (DNS)
Port 49153 ----->	172.217.1.1:80 (HTTP)
Port 49154 ----->	192.168.1.100:443 (HTTPS)
Port 49155 ----->	8.8.8.8:53 (DNS)

Same Destination, Different Connections:

All to 8.8.8.8:80
192.168.1.10:49152 → 8.8.8.8:80 (Connection 1)
192.168.1.10:49153 → 8.8.8.8:80 (Connection 2)
192.168.1.10:49154 → 8.8.8.8:80 (Connection 3)

TCP vs UDP Selection

Use TCP when:

- Reliable delivery required
- Order matters
- Error recovery needed
- Examples: HTTP, FTP, SSH, email

Use UDP when:

- Speed is critical
- Some loss is acceptable
- Real-time data
- Low overhead needed
- Examples: VoIP, video streaming, DNS, DHCP, online gaming

Application Examples:

TCP Applications:

- Web browsing (HTTP/HTTPS)
- File transfer (FTP)
- Email (SMTP, POP3, IMAP)
- Remote access (SSH, Telnet)

UDP Applications:

- DNS queries
- DHCP
- VoIP (voice calls)
- Video streaming
- Online gaming
- SNMP
- TFTP

Essential Concepts

1. Connection-Oriented vs Connectionless:

- **TCP:** Handshake, tracking, acknowledgments, termination
- **UDP:** Send and forget, no setup, no tracking

2. Reliability Trade-offs:

- **TCP:** Reliable but slower, more overhead
- **UDP:** Fast but no guarantees

3. Port Number Ranges:

- Well-known: Servers listen (0-1023)
- Registered: Applications (1024-49151)
- Dynamic: Clients source ports (49152-65535)

4. Sequence and Acknowledgment:

- Sequence numbers track bytes sent
- ACK numbers indicate next expected byte
- Both increment by data bytes sent/received

5. Flow Control vs Congestion Control:

- **Flow Control:** Receiver-based (window size)
- **Congestion Control:** Network-based (slow start, congestion avoidance)

IOS Commands

View Active Connections (Limited on Cisco devices)

show tcp brief # Brief TCP connections

show tcp # Detailed TCP connections

show udp # UDP listeners

Access Lists (Filter by Port)

access-list 100 permit tcp any any eq 80 # HTTP

access-list 100 permit tcp any any eq 443 # HTTPS

access-list 100 permit udp any any eq 53 # DNS

access-list 100 permit tcp any any eq 22 # SSH

Port-Based Access (on interfaces)

ip access-group 100 in # Apply ACL

Debugging

debug ip tcp transactions # Debug TCP

debug ip udp # Debug UDP

undebug all # Turn off debugging

Host Commands

Windows:

netstat -an # All connections and listeners

netstat -ano # Include PID

netstat -r # Routing table

netstat -s # Protocol statistics

netstat -e # Ethernet statistics

TCPView (Sysinternals) # GUI tool for connections

Linux:

netstat -tuln # TCP/UDP listeners numeric

netstat -tupn # Include PID

ss -tuln # Modern alternative to netstat

lsof -i # List open files (including sockets)

lsof -i :80 # Specific port

nmap localhost # Scan open ports

Packet Analysis

TCP Segment Example:

Source Port: 49152
Destination Port: 80
Sequence Number: 1000
Acknowledgment: 5000
Flags: ACK
Window: 64240
Checksum: 0x3a4f

Analysis:

- Client port 49152 connecting to web server (80)
- Client has sent bytes up to 1000
- Client acknowledges server's byte 5000
- Client can receive 64240 more bytes

UDP Datagram Example:

Source Port: 53821
Destination Port: 53
Length: 45
Checksum: 0x1a2b

Analysis:

- Client querying DNS server
- No sequence, ACK, or flags (connectionless)
- Small packet (DNS query)

Chapter 15: Application Layer

Key Terminology

Application Layer:

- Top layer of OSI (Layer 7) and TCP/IP models
- Provides network services to applications
- Interface between applications and network

Client-Server Model:

- **Server** - Provides services, listens on well-known ports
- **Client** - Requests services, uses dynamic source ports
- **Daemon/Service** - Server application running in background

Peer-to-Peer (P2P):

- Each device acts as both client and server
- Decentralized architecture
- Examples: BitTorrent, blockchain networks

Application Layer Protocols:

- Operate above transport layer
- Use services of TCP or UDP
- Define message format and rules

Web and Email Protocols

HTTP (Hypertext Transfer Protocol):

- Port: TCP 80
- Web page retrieval
- Request/response protocol
- Stateless (no session tracking)

HTTPS (HTTP Secure):

- Port: TCP 443
- Encrypted HTTP using TLS/SSL
- Secure web communication
- Certificate-based authentication

HTTP Methods:

GET - Retrieve resource
POST - Submit data to server
PUT - Upload resource
DELETE - Delete resource
HEAD - Retrieve headers only

HTTP Status Codes:

1xx - Informational

2xx - Success

200 OK

201 Created

204 No Content

3xx - Redirection

301 Moved Permanently

302 Found (temporary)

304 Not Modified

4xx - Client Error

400 Bad Request

401 Unauthorized

403 Forbidden

404 Not Found

5xx - Server Error

500 Internal Server Error

502 Bad Gateway

503 Service Unavailable

Email Protocols:

SMTP (Simple Mail Transfer Protocol):

- Port: TCP 25 (unencrypted), 587 (TLS)
- Send email (client to server, server to server)
- Push protocol
- Text-based commands

POP3 (Post Office Protocol v3):

- Port: TCP 110 (unencrypted), 995 (SSL)
- Download email from server
- Typically deletes from server
- Simple, download-and-delete model

IMAP (Internet Message Access Protocol):

- Port: TCP 143 (unencrypted), 993 (SSL)
- Manages email on server
- Folder synchronization

- Multiple client access
- More complex than POP3

Email Flow:

Sender → SMTP → Mail Server 1 → SMTP → Mail Server 2 → POP3/IMAP → Recipient

IP Addressing Services

DNS (Domain Name System):

- Port: UDP/TCP 53 (UDP for queries, TCP for zone transfers)
- Resolves domain names to IP addresses
- Hierarchical, distributed database
- Caching for performance

DNS Record Types:

A - IPv4 address
AAAA - IPv6 address
CNAME - Canonical name (alias)
MX - Mail exchanger
NS - Name server
PTR - Reverse lookup (IP to name)
SOA - Start of authority
TXT - Text information

DNS Query Process:

1. Client queries local DNS resolver
2. If not cached, query root server
3. Root server directs to TLD server (.com, .org)
4. TLD server directs to authoritative server
5. Authoritative server provides IP address
6. Result cached at each level

DHCP (Dynamic Host Configuration Protocol):

- Ports: UDP 67 (server), UDP 68 (client)
- Automatic IP address assignment
- Provides: IP address, subnet mask, default gateway, DNS servers

- Lease-based (addresses reclaimed)

DHCP Process (DORA):

1. Discover - Client broadcasts: "I need an IP"
2. Offer - Server unicasts: "Here's an IP: 192.168.1.100"
3. Request - Client broadcasts: "I'll take that IP"
4. Acknowledge - Server unicasts: "It's yours"

DHCPv6:

- Similar to DHCP but for IPv6
- Stateful or stateless modes
- Can work with SLAAC

File Sharing Services

FTP (File Transfer Protocol):

- Ports: TCP 20 (data), TCP 21 (control)
- File upload/download
- Separate control and data connections
- Active vs Passive modes
- Unencrypted (credentials in clear text)

FTPS (FTP Secure):

- FTP over TLS/SSL
- Encrypted file transfer

SFTP (SSH File Transfer Protocol):

- Port: TCP 22
- FTP over SSH
- Encrypted and secure
- Single connection (unlike FTP's two)

TFTP (Trivial FTP):

- Port: UDP 69
- Simple, no authentication

- Used for network booting, IOS transfers
- Unreliable transport (application handles retransmission)

SMB (Server Message Block):

- Port: TCP 445
- File/printer sharing (Windows)
- CIFS (Common Internet File System) - legacy name
- Also used for authentication

Remote Access

Telnet:

- Port: TCP 23
- Remote terminal access
- Unencrypted (insecure)
- Text-based
- Should not be used (use SSH instead)

SSH (Secure Shell):

- Port: TCP 22
- Encrypted remote access
- Replaces Telnet
- Public key authentication
- Also used for SFTP, SCP

RDP (Remote Desktop Protocol):

- Port: TCP 3389
- Windows remote desktop
- Graphical interface
- Supports encryption

Network Management

SNMP (Simple Network Management Protocol):

- Ports: UDP 161 (agent), UDP 162 (trap)

- Network monitoring and management
- MIB (Management Information Base) - data structure
- Versions: SNMPv1, SNMPv2c, SNMPv3 (secure)

SNMP Components:

- **Manager** - Monitoring station
- **Agent** - Software on managed device
- **MIB** - Database of manageable objects
- **Trap** - Unsolicited alert from agent

Syslog:

- Port: UDP 514
- Centralized logging
- Severity levels (0-7)
- Network event logging

Syslog Severity Levels:

- 0 - Emergency - System unusable
- 1 - Alert - Immediate action needed
- 2 - Critical - Critical condition
- 3 - Error - Error condition
- 4 - Warning - Warning condition
- 5 - Notice - Normal but significant
- 6 - Informational - Informational message
- 7 - Debug - Debug message

NTP (Network Time Protocol):

- Port: UDP 123
- Time synchronization
- Stratum levels (accuracy)
- Critical for logging, authentication

Essential Concepts

1. Client-Server vs Peer-to-Peer:

- **Client-Server:** Centralized, scalable, easier to manage

- **P2P:** Decentralized, resilient, harder to control

2. Port Number Assignment:

- Servers use well-known ports (consistent)
- Clients use dynamic ports (changes per connection)
- Firewall rules typically based on destination port

3. Encrypted vs Unencrypted:

- Always prefer encrypted protocols (HTTPS, SSH, SFTP)
- Legacy protocols (HTTP, Telnet, FTP) send credentials in clear text
- Compliance often requires encryption (HIPAA, PCI-DSS)

4. DNS Importance:

- Critical for internet functionality
- Single point of failure if misconfigured
- Caching improves performance
- Security concerns (DNS poisoning, DDoS)

5. DHCP Benefits:

- Centralized management
- Reduces configuration errors
- Automatic reclamation of unused addresses
- Supports mobile devices

IOS Commands

DNS Configuration:

```
ip domain-lookup          # Enable DNS lookups (default)
ip name-server [dns-ip]   # Configure DNS server
ip domain-name [domain]   # Set domain name
no ip domain-lookup        # Disable DNS (speeds up typos)
```

DHCP Server Configuration (Router):

```
ip dhcp pool LAN1          # Create DHCP pool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1  # Default gateway
dns-server 8.8.8.8 8.8.4.4  # DNS servers
lease 7                    # Lease time (days)
domain-name example.com
exit
ip dhcp excluded-address 192.168.1.1 192.168.1.10 # Reserve addresses
```

DHCP Client Configuration:

```
interface gigabitethernet 0/0
ip address dhcp          # Obtain IP via DHCP
no shutdown
exit
```

Verification:

```
show ip dhcp binding      # Show assigned leases
show ip dhcp pool          # Pool statistics
show ip dhcp conflict      # Address conflicts
clear ip dhcp binding *    # Clear all bindings
```

NTP Configuration:

```
ntp server 129.6.15.28     # Configure NTP server
ntp server 132.163.4.102   # Multiple for redundancy
show ntp status            # NTP synchronization status
show ntp associations      # NTP server relationships
```

Syslog Configuration:

```
logging [syslog-server-ip] # Send logs to syslog server
logging trap [level]       # Set logging level
logging console [level]    # Console logging level
logging buffered [size] [level] # Buffer logging
service timestamps log datetime # Add timestamps
```

SSH Configuration:

```
hostname R1                # Set hostname (required)
ip domain-name example.com  # Set domain (required)
crypto key generate rsa     # Generate RSA keys
    modulus 2048            # Key size
username admin privilege 15 secret Cisco123
line vty 0 15
    login local              # Use local database
    transport input ssh      # SSH only
    exit
ip ssh version 2            # Use SSHv2
```

Telnet Configuration (Not Recommended):

```
line vty 0 15
    password cisco
    login
    transport input telnet   # Allow Telnet
    exit
```

SNMP Configuration:

```
snmp-server community public RO  # Read-only community
snmp-server community private RW # Read-write community
snmp-server location "Data Center"
snmp-server contact "admin@example.com"
snmp-server enable traps          # Enable SNMP traps
snmp-server host 192.168.1.100 public # SNMP manager
```

Configuration Examples

Complete DNS/DHCP Server Configuration:

! DNS Configuration

```
ip domain-lookup
ip name-server 8.8.8.8
ip name-server 8.8.4.4
ip domain-name example.com
```

! DHCP Pool 1

```
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp pool LAN1
  network 192.168.1.0 255.255.255.0
  default-router 192.168.1.1
  dns-server 8.8.8.8 8.8.4.4
  lease 7
  domain-name example.com
exit
```

! DHCP Pool 2

```
ip dhcp excluded-address 192.168.2.1 192.168.2.10
ip dhcp pool LAN2
  network 192.168.2.0 255.255.255.0
  default-router 192.168.2.1
  dns-server 8.8.8.8 8.8.4.4
  lease 7
  domain-name example.com
exit
```

Secure Remote Access Configuration:

! SSH Configuration

hostname R1

ip domain-name example.com

crypto key generate rsa modulus 2048

username admin privilege 15 secret Admin123

! VTY Lines

line vty 0 15

login local

transport input ssh

exec-timeout 10 0

logging synchronous

exit

! SSH Version

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 3

Host Commands

Windows:

```
nslookup [domain]           # DNS query
nslookup [domain] [dns-server] # Query specific server
ipconfig /all                # Show DNS, DHCP info
ipconfig /release            # Release DHCP lease
ipconfig /renew              # Renew DHCP lease
ipconfig /displaydns         # Show DNS cache
ipconfig /flushdns           # Clear DNS cache

telnet [ip] [port]          # Test port connectivity
ssh user@hostname           # SSH connection
ftp [ip]                    # FTP connection
```

Linux:

nslookup [domain]	# DNS query
dig [domain]	# Detailed DNS query
host [domain]	# Simple DNS lookup
dhclient -r	# Release DHCP lease
dhclient	# Renew DHCP lease
ssh user@hostname	# SSH connection
scp file user@host:/path	# Secure copy
sftp user@hostname	# Secure FTP
ftp [ip]	# FTP connection

Chapter 16: Network Security Fundamentals

Key Terminology

Security Threats:

- **Threat** - Potential danger to assets
- **Vulnerability** - Weakness that can be exploited
- **Exploit** - Method of attacking vulnerability
- **Attack** - Attempt to compromise security
- **Risk** - Likelihood and impact of threat

Threat Actors:

- **White Hat** - Ethical hackers
- **Black Hat** - Malicious hackers
- **Gray Hat** - Between white and black
- **Script Kiddies** - Unskilled attackers using tools
- **Hacktivist** - Politically/socially motivated
- **State-Sponsored** - Government-backed
- **Insider** - Internal threat

Common Attacks:

- **Malware** - Malicious software
- **Social Engineering** - Psychological manipulation
- **Phishing** - Fraudulent emails/messages

- **DoS/DDoS** - Denial of Service attacks
- **Man-in-the-Middle (MITM)** - Intercept communications
- **Password Attack** - Brute force, dictionary, etc.

Malware Types

Virus:

- Malicious code requiring host file
- Spreads through user action
- Attaches to executable files

Worm:

- Self-replicating
- Spreads automatically over network
- Does not need host file

Trojan Horse:

- Disguised as legitimate software
- Provides backdoor access
- User unknowingly installs

Ransomware:

- Encrypts user data
- Demands payment for decryption
- Example: WannaCry, CryptoLocker

Spyware:

- Gathers information without consent
- Tracks browsing, keystrokes
- Sends data to attacker

Adware:

- Displays unwanted advertisements
- Tracks browsing habits
- May slow system

Rootkit:

- Provides privileged access
- Hides presence from detection
- Modifies OS

Botnet:

- Network of compromised computers
- Controlled remotely
- Used for DDoS, spam, etc.

Network Attacks**DoS (Denial of Service):**

- Overwhelm system/network resources
- Makes service unavailable
- Single source

DDoS (Distributed DoS):

- Multiple sources (botnet)
- Much harder to mitigate
- Amplification attacks common

Common DoS/DDoS Types:

SYN Flood - Exploit TCP handshake
UDP Flood - Flood with UDP packets
ICMP Flood - Ping flood
HTTP Flood - Legitimate-looking HTTP requests
Amplification - Use third-party to amplify attack

Reconnaissance:

- Information gathering
- Port scanning
- Network mapping
- Vulnerability scanning

Access Attacks:

- **Password Attack:**
 - Brute force (try all combinations)
 - Dictionary (common passwords)
 - Rainbow table (precomputed hashes)
- **Spoofing:** Impersonate legitimate source
- **MITM:** Intercept and modify communications

Social Engineering:

- **Phishing:** Fraudulent emails
- **Spear Phishing:** Targeted phishing
- **Vishing:** Voice phishing (phone)
- **Smishing:** SMS phishing
- **Pretexting:** Create scenario to extract info
- **Baiting:** Offer something to trick victim
- **Tailgating:** Follow authorized person

Security Solutions

Defense in Depth:

- Multiple layers of security
- No single point of failure
- Comprehensive protection

Security Layers:

1. Physical Security
2. Perimeter Security (Firewall)
3. Network Security (IPS, ACLs)
4. Endpoint Security (Antivirus)
5. Application Security
6. Data Security (Encryption)
7. User Security (Authentication)

Firewall:

- Filters network traffic
- Allows or blocks based on rules
- Stateless or stateful
- Types:
 - **Packet Filtering:** Basic rules
 - **Stateful:** Track connections
 - **Application Layer:** Deep inspection
 - **Next-Generation:** Advanced features

IPS/IDS:

- **IDS** (Intrusion Detection System): Monitors and alerts
- **IPS** (Intrusion Prevention System): Monitors and blocks
- Signature-based or anomaly-based

VPN (Virtual Private Network):

- Encrypted tunnel over public network
- Secure remote access
- Site-to-site connectivity
- Types:
 - **Remote-Access VPN:** Individual users
 - **Site-to-Site VPN:** Connects networks

AAA (Authentication, Authorization, Accounting):

- **Authentication:** Verify identity (who are you?)
- **Authorization:** Grant permissions (what can you do?)
- **Accounting:** Track activities (what did you do?)

Access Control:

- **ACL** (Access Control List): Filter traffic by criteria
- **Port Security:** Limit MACs per switch port
- **802.1X:** Port-based authentication
- **VLAN Segmentation:** Isolate traffic

Device Security

Password Security:

- Strong password policy
- Minimum length (8-12 characters)
- Complexity requirements
- Regular changes (controversial)
- No default passwords

Password Best Practices:

1. Use enable secret (not enable password)
2. Encrypt all passwords (service password-encryption)
3. Use strong passwords
4. Limit login attempts
5. Use two-factor authentication where possible

Physical Security:

- Lock equipment rooms
- Cable locks for devices
- Console port security
- Disable unused ports

Software Security:

- Keep IOS updated
- Apply security patches
- Remove unnecessary services
- Disable unused interfaces

Configuration Security:

- Backup configurations
- Secure backup storage
- Version control
- Document changes

Encryption and Hashing

Encryption:

- **Symmetric:** Same key for encrypt/decrypt (AES, DES, 3DES)
- **Asymmetric:** Public/private key pair (RSA, ECC)

Common Algorithms:

Symmetric:

- AES (Advanced Encryption Standard) - Strong, fast
- 3DES (Triple DES) - Legacy but still used
- DES (Data Encryption Standard) - Obsolete

Asymmetric:

- RSA - Widely used, key exchange
- ECC (Elliptic Curve) - Smaller keys, efficient

Hashing:

- One-way function
- Creates fixed-size output (hash/digest)
- Verify integrity, store passwords
- Common algorithms:
 - **MD5:** 128-bit (obsolete, vulnerable)
 - **SHA-1:** 160-bit (deprecated)
 - **SHA-256:** 256-bit (current standard)
 - **SHA-512:** 512-bit (very strong)

Digital Signatures:

- Verify authenticity and integrity
- Uses asymmetric encryption
- Non-repudiation

Certificates:

- Digital identity verification
- Issued by Certificate Authority (CA)
- Contains public key
- Used in HTTPS, VPN, etc.

Essential Concepts

1. CIA Triad:

- **Confidentiality:** Only authorized access
- **Integrity:** Data not altered
- **Availability:** Access when needed

2. Security Through Obscurity:

- Not a real security measure
- Never rely solely on hiding information
- Use proper security controls

3. Principle of Least Privilege:

- Give minimum necessary permissions
- Limit damage from compromise
- Applies to users and services

4. Zero Trust:

- Never trust, always verify
- Verify every access request
- Assume breach mentality

5. Security Awareness:

- Humans are often weakest link
- Regular training essential
- Update on current threats

IOS Security Commands

Password Security:

```
# Strong Password Configuration
enable secret 9 $9$password_hash # Enable secret (type 9 - scrypt)
username admin privilege 15 secret 5 $1$hash # Local user

# Encrypt All Passwords
service password-encryption # Encrypt type 7 (weak)

# Password Policy
security passwords min-length 10 # Minimum password length
```

Login Security:

```
# Console Security
line console 0
  password cisco
  login
  exec-timeout 5 0      # Auto logout
  logging synchronous
  exit

# VTY Security
line vty 0 15
  login local           # Use local database
  transport input ssh   # SSH only
  exec-timeout 10 0
  exit

# Login Attempt Limits
login block-for 300 attempts 3 within 60
# Block for 300s after 3 failed attempts in 60s
```

SSH Configuration:

```
hostname R1
ip domain-name example.com
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2

username admin privilege 15 secret Admin123
line vty 0 15
  login local
  transport input ssh
  exit
```

Port Security:

```
# Switch Port Security
interface gigabitethernet 0/1
  switchport mode access
  switchport port-security      # Enable
  switchport port-security maximum 2 # Max 2 MACs
  switchport port-security mac-address sticky # Learn MACs
  switchport port-security violation shutdown # Action on violation
exit
```

```
# Verify
show port-security interface g0/1
show port-security address
```

```
# Violation Actions:
# shutdown - Disable port (default)
# restrict - Drop packets, log
# protect - Drop packets, no log
```

ACL (Access Control List) - Basic:

```

# Standard ACL (source IP only)
access-list 10 permit 192.168.1.0 0.0.0.255
access-list 10 deny any
interface g0/0
  ip access-group 10 in
exit

# Extended ACL (source, dest, port)
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 443
access-list 100 deny ip any any
interface g0/1
  ip access-group 100 out
exit

# Named ACL
ip access-list extended INTERNET_ACCESS
  permit tcp 192.168.1.0 0.0.0.255 any eq 80
  permit tcp 192.168.1.0 0.0.0.255 any eq 443
  permit udp 192.168.1.0 0.0.0.255 any eq 53
  deny ip any any
exit
interface g0/1
  ip access-group INTERNET_ACCESS out
exit

```

Disable Unused Services:

```

no ip http server          # Disable HTTP
no ip http secure-server   # Disable HTTPS
no cdp run                 # Disable CDP globally
no service tcp-small-servers # Disable echo, discard
no service udp-small-servers # Disable echo, discard
no ip bootp server         # Disable BOOTP

```

Secure Unused Interfaces:

```

interface range g0/2-24
  shutdown
  switchport mode access
  switchport access vlan 999 # Unused VLAN
exit

```

Banner:

```
banner login ^
*****
*   UNAUTHORIZED ACCESS PROHIBITED   *
* This system is for authorized use only *
*   All activity is logged and monitored *
*****
^
```

Logging:

```
logging [syslog-server]      # Send to syslog
logging trap informational   # Log level
service timestamps log datetime # Timestamp logs
```

SNMP Security:

```
# SNMPv3 (Secure)
snmp-server group ADMIN v3 priv
snmp-server user admin1 ADMIN v3 auth sha AuthPass priv aes 128 PrivPass
snmp-server host 192.168.1.100 version 3 priv admin1

# Disable SNMPv1/v2c
no snmp-server community public
no snmp-server community private
```

Verification Commands

```
show running-config          # Check security config
show users                   # Show logged-in users
show line                    # Line status
show ip ssh                  # SSH status
show port-security           # Port security summary
show port-security interface g0/1 # Specific port
show access-lists            # Display ACLs
show ip access-lists         # IPv4 ACLs
show login                   # Login attempt statistics
```

Best Practices Summary

1. **Always use SSH, never Telnet**
 2. **Use strong, unique passwords**
 3. **Enable service password-encryption**
 4. **Disable unused services and ports**
 5. **Implement port security on switches**
 6. **Use ACLs to filter traffic**
 7. **Keep IOS updated**
 8. **Regular backups of configurations**
 9. **Monitor logs for suspicious activity**
 10. **Physical security of devices**
 11. **Principle of least privilege**
 12. **Regular security audits**
-

Chapter 17: Build a Small Network

Key Terminology

Small Network Characteristics:

- **Scalable** - Can grow as needed
- **Reliable** - Minimal downtime
- **Secure** - Protected from threats
- **Manageable** - Easy to administer
- **Cost-Effective** - Within budget

Network Design:

- **Topology** - Physical and logical layout
- **Redundancy** - Backup paths/devices
- **Hierarchy** - Layered design (access, distribution, core)
- **Modularity** - Independent functional areas

Common Small Network Devices:

- **Router** - Connects networks, WAN access

- **Switch** - Connects devices within network
- **Wireless AP** - Wireless connectivity
- **Firewall** - Security
- **Modem** - Internet connection

Network Applications:

- **File Sharing** - Share documents/resources
- **Email** - Communication
- **Web Services** - Websites, portals
- **VoIP** - Voice over IP
- **Video Conferencing** - Remote meetings

Small Network Design

Typical Small Network:

```

Internet
|
[Modem/Router]
|
[Firewall/Router]
|
[Core Switch]
|
+--[Access Switch]--[PCs, Printers]
|
+--[Wireless AP]--[Laptops, Mobile]
  
```

Design Principles:

1. Hierarchical Design:

```

Access Layer:  End devices connect here
               Switches, Wireless APs

Distribution:  Aggregates access layer (larger networks)
               Routing, policies

Core Layer:    High-speed backbone (enterprise)
               Fast switching, no policies
  
```

Small networks typically only have access layer

2. Redundancy:

- Multiple internet connections
- Dual power supplies
- Backup equipment
- RAID storage

3. Scalability:

- Room for growth
- Modular design
- Extra ports/capacity
- VLAN support

Common Protocols and Applications

DHCP:

- Automatic IP addressing
- Reduces admin overhead
- Centralized management

DNS:

- Name resolution
- Critical service
- Internal and external

NAT/PAT:

- Conserve public IPs
- Hide internal addressing
- Security through obscurity

Wireless:

- Flexible connectivity
- Mobile device support
- Security concerns (WPA2/WPA3)

File Services:

- SMB/CIFS (Windows)
- NFS (Linux)
- FTP/SFTP

Print Services:

- Network printers
- Print servers
- Queue management

Scaling to Larger Networks

Growth Considerations:

- Bandwidth requirements
- Number of users
- Security needs
- Redundancy requirements
- Budget constraints

Scaling Challenges:

- IP address management
- Broadcast traffic
- Security
- Performance
- Management complexity

Solutions:

- **VLANs** - Segment broadcast domains
- **Routing** - Interconnect networks
- **Hierarchical design** - Structured growth
- **Redundancy** - High availability
- **Documentation** - Track changes

Troubleshooting Methodologies

Structured Troubleshooting:

1. OSI Layer Approach:

Layer 1 (Physical): Cable, power, lights
Layer 2 (Data Link): MAC, switching, VLAN
Layer 3 (Network): IP addressing, routing
Layer 4 (Transport): TCP/UDP, ports
Layer 5-7 (Upper): Applications, services

2. Divide and Conquer:

- Test middle layer
- Narrow problem scope
- Isolate quickly

3. Top-Down:

- Start at application layer
- Work down to physical
- User-perspective approach

4. Bottom-Up:

- Start at physical layer
- Work up to application
- Systematic verification

5. Follow the Path:

- Trace packet route
- Test each hop
- Identify failure point

6. Substitution:

- Replace suspected component
- Verify if problem resolved
- Useful for hardware issues

Troubleshooting Steps:

1. Identify the problem
 - Gather information
 - Question users
 - Identify symptoms
 - Determine recent changes
2. Establish theory of probable cause
 - Question the obvious
 - Consider multiple approaches
 - Top-down, bottom-up, divide and conquer
3. Test theory to determine cause
 - Confirm theory
 - If confirmed, determine next steps
 - If not confirmed, establish new theory
4. Establish plan of action
 - Identify potential effects
 - Plan implementation
5. Implement solution or escalate
 - Implement and test
 - Escalate if beyond scope
6. Verify full system functionality
 - Confirm resolution
 - Verify no new issues created
7. Document findings
 - Actions taken
 - Outcome
 - Lessons learned

Verification Tools and Commands

Physical Layer:

```
show interfaces [type number]    # Interface status
show controllers [type number]    # Cable type, errors
show version                     # Hardware, uptime
show environment                  # Power, temperature (if supported)
```

Data Link Layer:

show mac address-table	# MAC table
show interfaces status	# Port status
show interfaces switchport	# Switchport info
show vlan	# VLAN information
show spanning-tree	# STP status
show cdp neighbors	# Connected devices
show interfaces trunk	# Trunk ports

Network Layer:

show ip interface brief	# Interface IPs
show ip route	# Routing table
show arp	# ARP table
show ipv6 interface brief	# IPv6 interfaces
show ipv6 route	# IPv6 routing table
show ipv6 neighbors	# IPv6 neighbor table
ping [ip]	# Test connectivity
traceroute [ip]	# Trace path

Troubleshooting Commands:

show running-config	# Active configuration
show startup-config	# Saved configuration
show logging	# System logs
show processes	# CPU processes
show memory	# Memory usage
show interfaces counters errors	# Interface errors
debug [protocol]	# Real-time debugging (use carefully!)
terminal monitor	# See debug/log output in SSH session

Connectivity Testing:

Test Local Configuration

show ip interface brief

show interfaces g0/0

Test Default Gateway

ping [default-gateway]

show arp

Test Remote

ping [remote-ip]

tracert [remote-ip]

Test DNS

ping [domain-name]

nslookup [domain]

Common Issues and Solutions

1. Can't Connect to Network:

Symptoms:

- No network connectivity
- Can't reach anything

Troubleshooting:

1. Check physical (cable, lights)

show interfaces g0/0

2. Check IP configuration

show ip interface brief

3. Check default gateway

show ip route

ping [gateway]

4. Check switch port

show interfaces status

2. Can Reach Some but Not All Resources:

Symptoms:

- Local network works
- Can't reach internet

Troubleshooting:

1. Verify default route
show ip route
2. Check NAT configuration
show ip nat translations
3. Verify DNS
nslookup google.com
4. Test routing
traceroute [destination]

3. Intermittent Connectivity:

Symptoms:

- Connection drops randomly
- Slow performance

Troubleshooting:

1. Check for duplex mismatch
show interfaces g0/0
Look for: collisions, late collisions, CRC
2. Check interface errors
show interfaces counters errors
3. Verify bandwidth utilization
4. Check for broadcast storms
show interfaces g0/0 | include broadcast

4. VLAN Issues:

Symptoms:

- Devices can't communicate across VLANs
- Trunk not passing traffic

Troubleshooting:

1. Verify VLAN configuration
show vlan brief
2. Check switchport mode
show interfaces switchport
3. Verify trunk configuration
show interfaces trunk
4. Check allowed VLANs
show interfaces g0/1 switchport

5. DHCP Not Working:

Symptoms:

- Clients get 169.254.x.x (APIPA)
- No IP assignment

Troubleshooting:

1. Verify DHCP pool
show ip dhcp pool
2. Check bindings
show ip dhcp binding
3. Verify interface DHCP relay (if needed)
show ip interface g0/0
4. Check conflicts
show ip dhcp conflict
5. Verify DHCP not excluded
show running-config | include dhcp

6. Routing Issues:

Symptoms:

- Can't reach specific networks
- Routing loop

Troubleshooting:

1. Verify routing table
show ip route
2. Check for route
show ip route [network]
3. Verify next hop reachable
ping [next-hop]
4. Check administrative distance
show ip route [network] | include metric
5. Look for loops
tracert [destination]

Host Commands for Troubleshooting

Windows:

ipconfig	# IP configuration
ipconfig /all	# Detailed info
ipconfig /release	# Release DHCP
ipconfig /renew	# Renew DHCP
ipconfig /flushdns	# Clear DNS cache
ping [ip/hostname]	# Test connectivity
tracert [ip/hostname]	# Trace route
pathping [ip/hostname]	# Ping + traceroute
nslookup [domain]	# DNS lookup
netstat -an	# Active connections
netstat -r	# Routing table
route print	# Display routes
arp -a	# ARP cache
net view	# View shared resources
net use	# Map network drives

Linux:

ifconfig	# IP configuration (legacy)
ip addr show	# IP configuration (modern)
ip route show	# Routing table
ping [ip/hostname]	# Test connectivity
ping6 [ipv6]	# IPv6 ping
traceroute [ip/hostname]	# Trace route
mtr [ip/hostname]	# Advanced traceroute
nslookup [domain]	# DNS lookup
dig [domain]	# Detailed DNS info
host [domain]	# Simple DNS lookup
netstat -tuln	# Listening ports
ss -tuln	# Modern netstat
ip neighbor show	# ARP cache (modern)
arp -a	# ARP cache (legacy)

Network Documentation

Essential Documentation:

1. Network Diagram:

- Physical topology
- Logical topology
- IP addressing scheme
- VLAN assignments
- Naming conventions

2. Configuration Files:

- Router configurations
- Switch configurations
- Backup dates
- Version control

3. IP Address Management:

Network: 192.168.1.0/24

Gateway: 192.168.1.1 (Router)

DHCP Pool: 192.168.1.100-200

Static Assignments:

192.168.1.10 - Server1

192.168.1.11 - Server2

192.168.1.20 - Printer1

Reserved: 192.168.1.1-99

4. Change Log:

- Date of change
- Person who made change
- Reason for change
- What was changed
- Verification results

5. Troubleshooting History:

- Problem description
- Symptoms
- Root cause
- Solution
- Prevention measures

Network Baseline

Why Baseline:

- Establish normal performance
- Detect anomalies
- Capacity planning
- Troubleshooting reference

What to Baseline:

Interface Statistics:

- Bandwidth utilization
- Packet counts
- Error rates
- Discards

CPU and Memory:

- Average utilization
- Peak usage times
- Trends over time

Application Performance:

- Response times
- Throughput
- Latency

Tools:

- SNMP monitoring
- NetFlow
- Built-in show commands
- Third-party tools (PRTG, SolarWinds, etc.)

Configuration Example - Small Network

Router Configuration:

```
hostname Branch-Router
enable secret Cisco123
no ip domain-lookup

! Interfaces
interface gigabitethernet 0/0
  description LAN Interface
  ip address 192.168.1.1 255.255.255.0
  ip nat inside
  no shutdown

interface gigabitethernet 0/1
  description WAN to ISP
  ip address dhcp
  ip nat outside
  no shutdown

! NAT
ip nat inside source list 1 interface g0/1 overload
access-list 1 permit 192.168.1.0 0.0.0.255

! DHCP
ip dhcp excluded-address 192.168.1.1 192.168.1.50
ip dhcp pool LAN
  network 192.168.1.0 255.255.255.0
  default-router 192.168.1.1
  dns-server 8.8.8.8 8.8.4.4

! Default Route
ip route 0.0.0.0 0.0.0.0 g0/1

! Security
line console 0
  password cisco
  login
  logging synchronous
line vty 0 4
  login local
  transport input ssh
username admin privilege 15 secret Admin123

banner motd ^Authorized Access Only^
```

end

copy run start

Switch Configuration:

```
hostname Branch-Switch
enable secret Cisco123

! VLANs
vlan 10
    name DATA
vlan 20
    name VOICE
vlan 99
    name MANAGEMENT

! Management Interface
interface vlan 99
    ip address 192.168.1.2 255.255.255.0
    no shutdown
ip default-gateway 192.168.1.1

! Access Ports
interface range g0/1-10
    switchport mode access
    switchport access vlan 10
    switchport voice vlan 20
    spanning-tree portfast
    no shutdown

! Unused Ports
interface range g0/11-24
    shutdown
    switchport access vlan 999

! Trunk to Router
interface g0/0
    switchport mode trunk
    switchport trunk native vlan 99
    no shutdown

! Security
line console 0
    password cisco
    login
line vty 0 15
    login local
    transport input ssh
```

```
username admin privilege 15 secret Admin123
```

```
banner motd ^Authorized Access Only^
```

```
end
```

```
copy run start
```

Appendices

Quick Reference Tables

Subnet Mask Quick Reference:

CIDR	Subnet Mask	Hosts	Networks (from /24)
/24	255.255.255.0	254	1
/25	255.255.255.128	126	2
/26	255.255.255.192	62	4
/27	255.255.255.224	30	8
/28	255.255.255.240	14	16
/29	255.255.255.248	6	32
/30	255.255.255.252	2	64

Common Port Numbers:

20/21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
67/68	DHCP
69	TFTP
80	HTTP
110	POP3
143	IMAP
161/162	SNMP
443	HTTPS
3389	RDP

IOS Command Modes:

User EXEC	Router>
Privileged EXEC	Router#
Global Config	Router(config)#
Interface Config	Router(config-if)#
Line Config	Router(config-line)#
Router Config	Router(config-router)#

Key Keyboard Shortcuts:

Ctrl+C	Exit config mode
Ctrl+Z	Return to privileged EXEC
Tab	Complete command
?	Context help
Ctrl+A	Beginning of line
Ctrl+E	End of line
Ctrl+Shift+6	Break sequence

Study Tips for CCNA

1. Hands-On Practice:

- Use Packet Tracer, GNS3, or EVE-NG
- Build networks, configure, troubleshoot
- Practice every command

2. Subnetting Practice:

- Master binary conversion
- Practice until automatic
- Critical exam skill

3. Command Memorization:

- Create flashcards
- Practice show commands
- Know verification steps

4. Troubleshooting:

- Follow methodologies
- Practice scenarios
- Document solutions

5. Time Management:

- Exam is timed
- Don't get stuck on hard questions
- Review flagged questions

Common Exam Topics

Must-Know Areas:

- IP addressing and subnetting
- VLANs and trunking
- Static and default routing
- OSI and TCP/IP models
- Switch operations
- Basic security
- Wireless fundamentals
- Network troubleshooting

Configuration Tasks:

- Router/switch basic config
- Interface configuration
- VLAN creation and assignment
- Trunk configuration
- Static routes
- DHCP configuration
- ACL configuration
- Port security

End of CCNA v7 Study Guide

This comprehensive guide covers all 17 chapters of the Introduction to Networks Companion Guide (CCNAv7). Use it as a reference for terminology, concepts, and IOS commands as you prepare for your CCNA certification.

Good luck with your studies, Ivan!