CCNA Cheatsheet

Your quick reference guide to core CCNA concepts: networking models, IP addressing, subnetting, routing, and switching fundamentals.

Networking Fundamentals & Models

OSI Model

Layer 7	Application: HTTP, FTP, DNS. Provides network services to applications.
Layer 6	Presentation: SSL/TLS, JPEG, MPEG. Data formatting, encryption, compression.
Layer 5	Session: NetBIOS, RPC. Manages sessions between applications.
Layer 4	Transport: TCP, UDP. End-to-end connection management, reliability, flow control.
Layer 3	Network: IP, ICMP, OSPF. Logical addressing, routing.
Layer 2	Data Link: Ethernet, PPP, Frame Relay. Framing, physical addressing (MAC), error detection.
Layer 1	Physical: Cables, connectors, hubs. Physical transmission of bits.
Tip	Mnemonics like “Please Do Not Throw Sausage Pizza Away” (bottom-up) or “All People Seem To Need Data Processing” (top-down) can help memorize the layers.

TCP/IP Model

Application	Combines OSI 5, 6, 7. Protocols: HTTP, FTP, SMTP, DNS.
Transport	Corresponds to OSI 4. Protocols: TCP, UDP.
Internet	Corresponds to OSI 3. Protocols: IP, ICMP, ARP.
Network Access	Combines OSI 1, 2. Protocols: Ethernet, PPP, device drivers. Often called ‘Link’ or ‘Network Interface’ layer.
TCP (Transmission Control Protocol)	Connection-oriented, reliable, ordered delivery, flow control, error checking. Used for web browsing, file transfers.
UDP (User Datagram Protocol)	Connectionless, unreliable, faster delivery, no flow control or error checking. Used for streaming, online gaming, DNS, VoIP.
Practice	Identify which layer common protocols operate at (e.g., DHCP, SNMP, BGP).
Key Diff	OSI is a conceptual model, TCP/IP is more implementation-oriented. TCP/IP layers map roughly to OSI but combine several layers.

Network Devices & Functions

Hub	Layer 1 device. Simply repeats signals to all connected devices. Creates one collision domain and one broadcast domain.
Switch	Layer 2 device. Uses MAC addresses to forward frames to the correct port. Creates multiple collision domains (one per port) but one broadcast domain (by default).
Router	Layer 3 device. Uses IP addresses to forward packets between networks. Creates multiple broadcast domains (one per interface) and multiple collision domains (one per interface).
Access Point (AP)	Connects wireless devices to a wired network.
Firewall	Security device that filters traffic based on predefined rules (ACLs).
Bridge	Layer 2 device. Connects network segments and forwards frames based on MAC addresses. Splits collision domains, but not broadcast domains.
Repeater	Layer 1 device. Extends network distance by regenerating signals. Does not segment collision or broadcast domains.
Best Practice	Use switches to reduce collisions and improve performance within a LAN segment. Use routers to connect different networks and control broadcast traffic.

IP Addressing & Subnetting

IPv4 Basics

Format	32-bit address, divided into 4 octets (8 bits each), separated by dots. E.g., 192.168.1.1
Classes	• Class A: 1-126.x.x.x (First octet defines network) • Class B: 128-191.x.x.x (First two octets define network) • Class C: 192-223.x.x.x (First three octets define network) • Class D: 224-239.x.x.x (Multicast) • Class E: 240-255.x.x.x (Experimental)
Private IP Ranges	• Class A: 10.0.0.0 - 10.255.255.255 • Class B: 172.16.0.0 - 172.31.255.255 • Class C: 192.168.0.0 - 192.168.255.255
Loopback	127.0.0.1 (Tests the TCP/IP stack on the local machine).
APIPA	169.254.0.0/16 (Automatic Private IP Addressing - assigned when DHCP fails).
Subnet Mask	Identifies the network portion of an IP address. Written in dotted decimal or CIDR notation (e.g., 255.255.255.0 or /24).
Network Address	First address in a subnet. All host bits are 0. Cannot be assigned to a host.
Broadcast Address	Last address in a subnet. All host bits are 1. Used to send traffic to all hosts on the subnet.
Usable Hosts	Total addresses - 2 (network and broadcast). Calculated as 2^h - 2, where h is the number of host bits.

Subnetting IPv4

Purpose	Divide a large network into smaller, more manageable subnets. Improves efficiency, security, and reduces broadcast traffic.
Borrowing Bits	Borrowing bits from the host portion of the address to create subnets. The number of borrowed bits determines the number of subnets and hosts per subnet.
# of Subnets	2^s, where s is the number of subnet bits (borrowed bits). (Note: Historically, some methods disallowed using the first/last subnet, but modern CIDR allows 2^s subnets).
# of Hosts/Subnet	2^h - 2, where h is the number of host bits remaining after borrowing for subnets.
Slash Notation (CIDR)	Compact way to represent the subnet mask. E.g., /24 means 24 network bits (255.255.255.0).
Subnet Zero	The first subnet where all subnet bits are 0. Usable with modern equipment.
Broadcast Subnet	The last subnet where all subnet bits are 1. Usable with modern equipment.
Practice Tip	Master binary conversions! Know the values of each bit position (128, 64, 32, 16, 8, 4, 2, 1).
Example	Given 192.168.1.0/24, subnet to get 8 subnets. 2^s >= 8 implies s=3 (borrow 3 bits from host portion). Original mask: 255.255.255.0 (/24). New mask: 255.255.255.224 (/27). h = 32 - 27 = 5. Hosts/subnet: 2^5 - 2 = 30. Subnet block size: 256 - 224 = 32. Subnets start at 192.168.1.0, 192.168.1.32, 192.168.1.64, etc.

IPv6 Basics

Format	128-bit address, written as 8 groups of 4 hexadecimal digits, separated by colons. E.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334
Simplification 1	Leading zeros in any group can be omitted. E.g., `0db8` becomes `db8`, `0000` becomes `0`.
Simplification 2	One or more consecutive groups of `0000` can be replaced by a double colon (::). Can only be used once per address.
Prefix Length	Similar to subnet mask in IPv4, uses CIDR notation. E.g., /64 means the first 64 bits are the network portion.
Address Types	• Unicast: One-to-one communication. • Multicast: One-to-many communication (replaces IPv4 broadcast). • Anycast: One-to-nearest (out of a group) communication.
Link-Local	Addresses starting with `fe80::/10`. Automatically assigned to interfaces, used for communication on the local link only. Not routable.
Unique Local	Addresses starting with `fc00::/7`. Similar to IPv4 private addresses, used within a site. Routable only within the site.
Global Unicast	Routable addresses used on the internet. Most start with `2000::/3`.
EUI-64	Method to generate the interface ID (host portion) of an IPv6 address from the MAC address. Inserts `fffe` in the middle and inverts the 7th bit of the MAC.

Routing Fundamentals

Routing Concepts

Routing Table	A database used by a router to store routes to various destinations. Contains network addresses, next-hop IP/interface, and metric.
Directly Connected	Networks configured on the router's active interfaces. Automatically added to the routing table.
Static Route	Manually configured route by an administrator. Useful for simple networks or default routes. High administrative distance (1).
Dynamic Route	Routes learned from other routers using routing protocols (RIP, OSPF, EIGRP, BGP).
Administrative Distance (AD)	Value used by a router to rank the trustworthiness of routing information sources. Lower AD is preferred.
Metric	Value used by a routing protocol to determine the best path to a destination network. Metric calculation varies by protocol (hop count for RIP, cost for OSPF, bandwidth/delay for EIGRP).
Next-Hop	The IP address of the next router along the path to the destination network, or the exit interface on the local router.
Longest Match	Routers choose the route with the longest prefix match in the routing table when forwarding a packet.
Tip	AD is protocol-specific; metric is path-specific within a protocol. AD compares different protocols, metric compares paths within the same protocol.

Routing Protocols Basics

RIP (Routing Information Protocol)	Distance-Vector. Uses hop count as metric (max 15 hops). Updates sent every 30s. Classful by default (RIPv1), RIPv2 is classless. AD 120.
OSPF (Open Shortest Path First)	Link-State. Uses cost (based on bandwidth) as metric. Hierarchical design with areas. Uses Dijkstra's algorithm. AD 110.
EIGRP (Enhanced Interior Gateway Routing Protocol)	Advanced Distance-Vector (Hybrid). Cisco proprietary. Uses bandwidth and delay (by default) for metric. Uses DUAL algorithm for fast convergence. AD 90 (internal), 170 (external).
BGP (Border Gateway Protocol)	Path-Vector. Used between Autonomous Systems (AS) on the internet (Exterior Gateway Protocol). Uses path attributes for routing decisions. AD 20 (eBGP), 200 (iBGP).
Distance Vector	Routers send their entire routing table to neighbors. 'Routing by rumor'.
Link State	Routers send information about their directly connected links to *all* other routers in the area. Routers build a complete topology map.
Interior Gateway Protocol (IGP)	Operates within a single Autonomous System (AS). E.g., RIP, OSPF, EIGRP.
Exterior Gateway Protocol (EGP)	Operates between different Autonomous Systems (AS). E.g., BGP.

Cisco Router Commands

`show ip route` Displays the IPv4 routing table.
`show ip protocols` Displays parameters and state of active routing protocols.
`traceroute <destination_ip>` Traces the path packets take to a destination.
`ping <destination_ip>` Tests connectivity to a host.
`ip route <network> <mask> {<next-hop-ip> | <exit-interface>}` Configures a static IPv4 route.

`router ospf <process-id>`
`network <network> <wildcard-mask> area <area-id>`
 	
Configures OSPF.

`router eigrp <AS-number>`
`network <network-address>`
 	
Configures EIGRP.

`copy running-config startup-config` Saves the current configuration to NVRAM.
Tip: Use `do` before privileged EXEC commands when in configuration mode (e.g., `do show ip route`).

Switching Concepts & Configuration

Ethernet & Switching

MAC Address	48-bit (6-octet) physical address burned into network interface cards (NICs). Globally unique. Used by switches at Layer 2.
CAM Table (MAC Address Table)	Table on a switch that maps MAC addresses to switch ports. Used to forward frames efficiently.
Switch Functions	1. Learning (MAC addresses) 2. Flooding (unknown unicast, broadcast, multicast) 3. Forwarding/Filtering (based on CAM table) 4. Aging (removing old entries from CAM table)
Collision Domain	A network segment where collisions can occur. Switches segment collision domains (one per port).
Broadcast Domain	A network segment where broadcast frames are forwarded. Switches typically form a single broadcast domain by default.
Duplex	• Half-Duplex: Devices cannot send and receive simultaneously (collision possible). • Full-Duplex: Devices can send and receive simultaneously (no collisions).

Auto-Negotiation	Process where two connected devices agree on the optimal speed and duplex settings.
Best Practice	Configure speed and duplex manually on both ends if auto-negotiation fails or for critical links to avoid mismatch issues.

VLANs (Virtual LANs)

Purpose	Logically segment a physical network into smaller broadcast domains. Improves security and network management.
Access Port	Belongs to a single VLAN. Frames sent/received on this port are untagged. Used for connecting end devices (PCs, printers).
Trunk Port	Carries traffic for multiple VLANs between switches or between a switch and router/server. Uses tagging (802.1Q) to identify VLAN membership of frames.
802.1Q Tagging	Adds a 4-byte header to the Ethernet frame containing a VLAN ID (VID).
Native VLAN	VLAN on a trunk port that sends/receives *untagged* frames. Should be consistent on both ends of a trunk and preferably unused for user data for security.
Default VLAN	VLAN 1. All switch ports belong to VLAN 1 by default. Used for control plane traffic (STP, VTP, CDP).
Inter-VLAN Routing	Routing traffic between different VLANs. Requires a Layer 3 device (router or Layer 3 switch).
Router-on-a-Stick	A single router interface configured with subinterfaces, each handling traffic for a different VLAN on a trunk link to a switch.
Tip	VLANs create multiple broadcast domains. To communicate between VLANs, you *must* route.

Spanning Tree Protocol (STP)

Purpose	Prevent Layer 2 loops in a switched network by blocking redundant links. Loops cause broadcast storms, MAC table instability, and multiple frame copies.
BPDU	Bridge Protocol Data Unit. Messages exchanged by switches to communicate STP information (Root ID, Bridge ID, Path Cost).
Bridge ID (BID)	Identifies a switch in the STP domain. Consists of Priority (32768 by default, can be changed) + System ID Extension (VLAN ID) + MAC address. Lower BID is preferred.
Root Bridge	The switch with the lowest BID in the STP domain. All path calculations are from the perspective of the Root Bridge.
Root Port (RP)	The port on a non-root bridge that has the lowest cost path to the Root Bridge. There is only one RP per non-root bridge.
Designated Port (DP)	The port on a network segment that has the lowest cost path to the Root Bridge for that segment. There is one DP per segment. Root Bridge ports are always DPs.
Blocked Port (BP)	A port that is blocked to prevent loops. It receives BPDUs but does not forward data frames.
STP Port States	1. Blocking: Receives BPDUs. 2. Listening: Sends/Receives BPDUs, listens for topology changes. 3. Learning: Builds MAC table, listens for topology changes. 4. Forwarding: Sends/Receives data, sends/receives BPDUs. 5. Disabled: Administratively shut down.
Convergence	The process of all switches agreeing on the STP topology. Can take up to 50 seconds with classic STP (20s Listening + 15s Learning + 15s Forwarding Delay).