CCNA

Short notes for beginners · Cisco 200-301 · networking students · NOC

Uncodemy Handwritten Notes · free for students

1. Networking Fundamentals

- **Network** = devices connected to share data and resources. Types: **PAN** (personal), **LAN** (building), **MAN** (city), **WAN** (country or world, e.g. internet). Topologies: star (most common), bus, ring, mesh, hybrid.

Device	OSI layer	Job
Hub	1	Repeats bits to all ports (one collision domain)
Switch	2	Forwards frames by MAC address, each port = own collision domain
Router	3	Forwards packets by IP, connects networks, each port = own broadcast domain
Firewall	3 to 7	Filters traffic by rules
Access point	2	Connects Wi-Fi clients to the wired LAN

- **Cisco 3 tier model**: Access (users connect) → Distribution (policy, routing between VLANs) → Core (fast backbone). Small networks use a 2 tier **collapsed core**.
- Cables: UTP Cat5e / Cat6 up to 100 m. Straight-through for different devices (PC to switch), crossover for similar devices. Fibre: single mode (long distance), multimode (short).
- **Collision domain** = devices that can collide on shared media. **Broadcast domain** = devices that receive a broadcast. Switches split collision domains, routers (and VLANs) split broadcast domains.

2. OSI, TCP/IP and Protocols

Layer	OSI	Protocols / PDU
7	Application	HTTP, DNS, DHCP, SMTP, FTP, SSH, Telnet
6	Presentation	Encryption, JPEG, ASCII

Layer	OSI	Protocols / PDU
5	Session	Sessions, NetBIOS
4	Transport	TCP, UDP / Segment
3	Network	IP, ICMP / Packet
2	Data Link	Ethernet, ARP, PPP / Frame
1	Physical	Cables, signals / Bits

- **Encapsulation**: data → segment → packet → frame → bits on the sender; reverse on the receiver. TCP/IP model: Application, Transport, Internet, Network Access.
- **TCP**: reliable, connection based, 3 way handshake (SYN, SYN-ACK, ACK), sequence numbers, windowing. **UDP**: fast, no guarantee, used for voice, video, DNS, DHCP.

Port	Service	Port	Service
20 / 21	FTP data / control	67 / 68	DHCP server / client
22	SSH	80	HTTP
23	Telnet	110	POP3
25	SMTP	143	IMAP
53	DNS (UDP/TCP)	443	HTTPS
69	TFTP	161 / 162	SNMP

3. IPv4 Addressing

- IPv4 address = 32 bits written as 4 octets (e.g. 192.168.1.10). Each octet 0 to 255. Subnet mask separates the network part and host part. CIDR writes it as a prefix: /24 = 24 network bits.

Class	First octet	Default mask	Note
A	1 to 126	255.0.0.0 (/8)	Very large networks
B	128 to 191	255.255.0.0 (/16)	Medium networks
C	192 to 223	255.255.255.0 (/24)	Small networks
D	224 to 239	-	Multicast
E	240 to 255	-	Experimental

- **Private ranges** (RFC 1918): 10.0.0.0/8, 172.16.0.0/12 (172.16 to 172.31), 192.168.0.0/16. **Loopback**: 127.0.0.1. **APIPA**: 169.254.0.0/16 (when DHCP fails).

EXAMPLE 192.168.1.10 → binary 11000000.10101000.00000001.00001010. Convert 10: 8 + 2 = 00001010.

- **Unicast** one to one, **Broadcast** one to all (255.255.255.255), **Multicast** one to a group (224.0.0.0/4). First address of a subnet = network ID, last = broadcast. Both cannot be given to hosts.

4. Subnetting and IPv6

FORMULA Usable hosts = 2^h - 2 (h = host bits). Subnets = 2^n (n = borrowed bits). Block size = 256 - mask octet value.

CIDR	Mask	Block	Usable hosts
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2

EXAMPLE Network 192.168.10.0/26: block 64. Subnets: .0, .64, .128, .192. Take the third: network 192.168.10.128, usable .129 to .190, broadcast .191. Hosts = 2^6 - 2 = 62.

EXAMPLE Host 192.168.1.100/27: block 32. 100 lies in 96 to 127 → network 192.168.1.96, usable .97 to .126, broadcast .127.

- **VLSM** uses different masks in one network to avoid waste: give the largest subnet first. **Summarisation** combines routes, e.g. 192.168.0.0/24 to 192.168.3.0/24 = 192.168.0.0/22.
- **IPv6**: 128 bits, 8 groups of hex, no broadcast. Shorten by removing leading zeros and one :: for a run of zeros. Types: global unicast 2000::/3, link-local FE80::/10, unique local FC00::/7, multicast FF00::/8, loopback ::1.

5. Cisco IOS Basics

Prompt	Mode	How to enter
Router>	User EXEC	Default login, limited commands
Router#	Privileged EXEC	enable
Router(config)#	Global config	configure terminal
Router(config-if)#	Interface config	interface g0/0
Router(config-line)#	Line config	line console 0 / line vty 0 4

- Useful commands: hostname R1, enable secret pass, interface g0/0, ip address 192.168.1.1 255.255.255.0, no shutdown, description, banner motd #text#, service password-encryption.
- Show commands: show running-config, show startup-config, show ip interface brief, show interfaces, show ip route, show version, show vlan brief, show mac address-table, show cdp neighbors.
- Save with copy running-config startup-config (or write memory). Running config is in RAM and lost on reload; startup config is in NVRAM. Use ? for help and Tab to complete a command. Remote access: SSH preferred over Telnet.

REMEMBER Interfaces on a router are shut down by default. Always apply no shutdown. Check with show ip interface brief (up / up is good).

6. Switching, VLANs and STP

- Switch logic: **learn** source MAC → **flood** unknown destination → **forward** known destination to the port → **filter** so it does not go elsewhere. MAC table is also called the CAM table.
- **VLAN** splits one switch into separate logical LANs (separate broadcast domains). Access port carries one VLAN. **Trunk** port carries many VLANs using **802.1Q** tagging; native VLAN is untagged. Default VLAN is 1. Normal range 1 to 1005, extended 1006 to 4094.

EXAMPLE vlan 10 / name SALES then interface f0/1 / switchport mode access / switchport access vlan 10. Trunk: switchport mode trunk.

- **Inter-VLAN routing**: router on a stick (sub interfaces with dot1q encapsulation) or a Layer 3 switch with SVIs (interface vlan 10).
- **STP** (802.1D) stops loops. Switch with the lowest Bridge ID (priority 32768 + VLAN + MAC) becomes the **root bridge**. Port roles: root, designated, alternate (blocked). States: blocking, listening, learning, forwarding. **RSTP** (802.1w) converges faster. PortFast + BPDU Guard on access ports.
- **EtherChannel** bundles links (LACP 802.3ad open, PAgP Cisco). **Port security** limits MAC addresses per port. **CDP** (Cisco) / **LLDP** (standard) discover neighbours.

7. Routing

- A router picks the route with the longest prefix match. If several routes are equal length, lower **Administrative Distance (AD)** wins; inside one protocol, lower **metric** wins.

Source	AD	Source	AD
Connected	0	OSPF	110
Static	1	RIP	120
eBGP	20	External EIGRP	170
EIGRP (internal)	90	iBGP	200

- **Static route**: ip route 192.168.2.0 255.255.255.0 10.0.0.2 (network, mask, next hop). **Default route**: ip route 0.0.0.0 0.0.0.0 next-hop (gateway of last resort).

Protocol	Type	Key facts
RIP v2	Distance vector	Hop count metric, max 15 hops, slow
EIGRP	Advanced distance vector	Cisco origin, bandwidth + delay metric, fast
OSPF	Link state	Open standard, cost metric, areas, Dijkstra SPF
BGP	Path vector	Between autonomous systems (internet)

- **OSPF**: router ospf 1 → network 192.168.1.0 0.0.0.255 area 0. Area 0 is the backbone. Cost = reference bandwidth (100 Mbps) / interface bandwidth. Hello 10 s, dead 40 s on Ethernet. DR and BDR are elected on multi-access links. Highest priority / router ID wins.

EXAMPLE OSPF cost = 100 / bandwidth in Mbps: 10 Mbps Ethernet = 100/10 = 10. FastEthernet 100 Mbps = 1. Serial T1 1.544 Mbps ≈ 64.

8. IP Services: DHCP, NAT, ACL

- **DHCP** gives IP, mask, gateway and DNS automatically. Four steps DORA: Discover, Offer, Request, Acknowledge. A router can forward requests with ip helper-address. **DNS** resolves names to IPs.
- **NAT** translates private to public addresses. Static (one to one), dynamic (pool), **PAT / overload** (many to one using ports, most common). Terms: inside local, inside global, outside local, outside global.
- **ACL** (Access Control List) filters packets, read top to bottom, first match wins, with an implicit deny at the end. **Standard** ACL (1 to 99) checks source only, place near the destination. **Extended** (100 to 199) checks source, destination, protocol, port, place near the source.

EXAMPLE access-list 10 permit 192.168.1.0 0.0.0.255 then interface g0/1 / ip access-group 10 out. Wildcard mask = inverse of subnet mask: 255.255.255.0 → 0.0.0.255.

9. Wireless, Security and Automation

Standard	Band	Max speed (theory)
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
802.11ac (Wi-Fi 5)	5 GHz	Several Gbps
802.11ax (Wi-Fi 6)	2.4 / 5 GHz (6 GHz in 6E)	About 9.6 Gbps

- 2.4 GHz non-overlapping channels: 1, 6 and 11. Wi-Fi security: WPA2 (AES-CCMP) and WPA3. Avoid WEP and open networks.
- Security basics: strong passwords, AAA (RADIUS, TACACS+), port security, DHCP snooping, Dynamic ARP Inspection, VPNs (site to site, remote access), user awareness.
- Automation: **SDN** (control plane separated from data plane), controllers like Cisco DNA Center, REST APIs with JSON, tools Ansible, Puppet, Chef, Python. CCNA 200-301 weights: Network fundamentals 20%, Network access 20%, IP connectivity 25%, IP services 10%, Security 15%, Automation 10%.

10. Most Asked Questions (practice)

1. Explain the OSI model with protocols and devices at each layer.
2. TCP vs UDP. Explain the three way handshake.
3. Subnet 192.168.1.0/26: subnets, hosts, ranges and broadcast.
4. What is VLSM? What is route summarisation?
5. What is a VLAN? Access port vs trunk port. Configure a VLAN.
6. Explain STP, root bridge election and port states.
7. Static vs dynamic routing. Compare RIP, EIGRP, OSPF.
8. What is administrative distance? Explain longest prefix match.
9. Explain DHCP DORA, NAT types and standard vs extended ACL.
10. Router configuration: hostname, IP, no shutdown, route, save config.

TIP Practise daily in Cisco Packet Tracer or GNS3. Subnetting and the show commands decide most CCNA marks, so be fast. Check the Cisco site for the latest exam details.