

DHCP on IOS

```
Router(config)# ip dhcp pool LAN
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# dns-server 8.8.8.8
Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

- **DHCP relay** (`ip helper -ad dress`): forwards client broadcasts to a remote DHCP server — configured on the router interface facing clients.

- **Troubleshoot**: client gets APIPA → check pool, exclusions, relay, and that the server is reachable. `show ip dhcp binding` lists active leases.

More from ByteBar

CCNA 200-301 — Go Deeper

Like this cheat sheet? The full ByteBar CCNA (200-301) Study Guide covers all six exam domains in exam-weight order, with must-memorize tables, EXAM TIP boxes, and 30 practice questions with full explanations — in the ByteBar shop on Etsy (ByteBarExamPrep). Studying for one of the 19 simulator exams instead? Practice like it's test day — the ByteBar Practice Exam Simulator is \$9.99 one-time at bytebarhq.com. *Independent study resource. Not affiliated with Cisco Systems, Inc. Cisco and CCNA are trademarks of Cisco Systems, Inc.*

Updated practice question count from 30 to 100.

Exam-Day Rapid Fire

- **Simlets first**. CLI simulations pay the most and eat the most time — do them while fresh.
- **Subnet in the margins**. Write the CIDR ladder on scratch paper before starting — free reference for the whole exam.
- **Read like a troubleshooter**: match symptoms to causes (APIPA = DHCP, native mismatch = trunk, EXSTART stuck = MTU).
- **AD ladder**: 0-1-20-90-110-120-200. Longest prefix match beats everything.
- **Eliminate aggressively**. Two answers are usually nonsense — kill them, then decide between the survivors.
- **Never leave blanks**. No penalty for guessing.
- **Version check**: v2.0 blueprint exam goes live February 3, 2027 — booked before that date, you sit v1.1.
- About the exam: ~100 questions (multiple choice, drag-and-drop, simlets), 120 minutes, passing score not published, valid 3 years.

Essential CLI Commands

Command	Does what
<code>show ip route</code>	Routing table — [AD/metric], next-hop, exit interface
<code>show interfaces status</code>	Port status at a glance
<code>show interfaces trunk</code>	Verify trunking + allowed VLANs
<code>show vlan brief</code>	VLAN-to-port mapping
<code>show spanning-tree vlan 10</code>	Root bridge, port roles/states per VLAN
<code>show etherchannel summary</code>	Channel-group status: (P) bundled vs. (I) standalone
<code>show cdp neighbors</code> / <code>show lldp neighbors</code>	Directly connected neighbor identity and capabilities
<code>show ip ospf neighbor</code>	OSPF adjacencies and states (FULL, 2WAY...)
<code>show ip ospf interface brief</code>	OSPF-enabled interfaces
<code>show ip dhcp binding</code>	Active DHCP leases



Essential CLI Commands (cont)

`show standby brief`	HSRP/VRP active/standby roles
`ping / extended ping`	Basic reachability; extended sets source interface
`traceroute`	Hop-by-hop path (find where inter-VLAN routing breaks)

Protocols Quick Reference

Protocol	What the guide says
Telnet (23)	Block it in ACLs (`deny tcp... any eq 23`); disable in favor of SSH
SSH	Encrypted device management
DNS	Name resolution (A, AAAA, CNAME, MX, NS, PTR)
DHCP	Address assignment; relay with `ip helper -ad dress`; APIPA = DHCP failed
SNMP	Monitoring — v2c community strings (plaintext), v3 auth + privacy
Syslog	Centralized logging, severity 0–7
NTP	Time synchronization
TFTP	Insecure — never across untrusted networks
SFTP / SCP	Secure transfer of IOS images and configs
RADIUS / TACACS+	AAA — RADIUS open (encrypts password only), TACACS+ Cisco (encrypts whole payload)
IPsec / IKE	VPN tunnels; IKE negotiates the security association
HSRP / VRRP	First-hop redundancy — virtual IP + virtual MAC gateway
OSPF	Single-area (area 0) interior routing
CDP / LLDP	Neighbor discovery — CDP Cisco-proprietary, LLDP open (multi-vendor)
CAPWAP / LWAPP	Lightweight APs tunnel traffic to the WLC
ICMP	ping (extended ping sets source interface), traceroute (hop-by-hop path)

Management, Monitoring & Automation

Approaches

Approach	Know this
Device-based (traditional)	CLI/SSH per device — fine for small networks, doesn't scale
Controller-based (SDN)	Central controller (e.g., Catalyst Center) pushes policy; devices follow
Cloud-based	Management plane in the cloud (e.g., Meraki dashboard)
Automation / IaC	Configs as versioned code (Ansible playbooks, Terraform) — consistent, repeatable, reviewable

Planes: management (SSH/SNMP — how you administer), control (routing protocols — how devices learn paths), data (forwarding — the actual packets).

SNMP, Syslog, NTP

Tool	Know this
SNMPv2c	Community strings (plaintext) — `snmp-s erver community`; agents, managers, MIBs, traps
SNMPv3	Adds auth + privacy (encryption) — the secure choice
Syslog severity	0 Emergency → 7 Debug (mnemonic: Every Awesome Cisco Engineer Can Now Play Daily). Lower number = worse



By **bytebar**

cheatography.com/bytebar/

Published 24th September, 2026.

Last updated 22nd October, 2026.

Page 2 of 9.

Sponsored by **Readable.com**

Measure your website readability!

<https://readable.com>

Management, Monitoring & Automation (cont)

| NTP | Time sync for logs and certs — `ntp server 10.1.1.50` |

`

Router(config)# logging host 10.1.1.100

Router(config)# logging trap warnings

Router(config)# snmp-server community NETOPS RO

`

logging trap warnings sends severity 0–4 (that level and everything more severe).

Automation & AI

- **Ansible:** agentless automation over SSH; playbooks (YAML) declare desired state.

- **REST APIs / JSON:** how controllers and scripts talk to network devices programmatically.

- **Agentic AI in NetOps:** can analyze telemetry, suggest config changes, draft troubleshooting steps — but a human validates before anything touches production.

Wireless Principles

| Concept | Know this |

| --- | --- |

| Bands | 2.4 GHz (range), 5 GHz (speed/capacity), 6 GHz (Wi-Fi 6E/7, fastest) |

| Channels (2.4 GHz) | Only 1, 6, 11 are non-overlapping |

| Security | WPA3 current; WPA2-AES minimum; WEP is broken |

| Enterprise auth | 802.1X + RADIUS — per-user credentials, not a shared passphrase |

| Interference | Microwaves, Bluetooth, neighboring APs on 2.4 GHz; rogues and overlap generally |

| LWAPP/CAPWAP | Lightweight APs tunnel traffic to a wireless LAN controller (WLC) |

Management Security & VPNs

| Concept | Know this |

| --- | --- |

| SSH | Encrypted management: `crypto key generate rsa, ip ssh version 2`, **disable telnet** (line vty: `transport input ssh`) |

| Passwords | `service password-encryption` obscures type-7 passwords; `enable secret` uses strong MD5 for the privileged password |

| AAA | Authentication, Authorization, Accounting — TACACS+ (Cisco, encrypts whole payload) vs. RADIUS (open, encrypts password only) |

| SFTP/SCP | Secure file transfer for IOS images and configs — never TFTP across untrusted networks |

| IPsec VPN | Site-to-site (routers/firewalls) and remote-access (clients); tunnel vs. transport mode; IKE negotiates the SA |

Layer 2 Security

| Feature | Stops |

| --- | --- |

| Port security | MAC flooding / rogue devices — limit MACs per port; violation: protect, restrict, shutdown (default) |

| DHCP snooping | Rogue DHCP servers — trust only uplink ports; builds a binding table |

| Dynamic ARP Inspection (DAI) | ARP spoofing — validates ARP against the DHCP snooping table |

| Storm control | Broadcast/multicast storms — throttles when traffic exceeds a threshold |

| RA guard | Rogue IPv6 router advertisements |

`



Layer 2 Security (cont)

```
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
`
```

Violation modes: protect = drop only; restrict = drop + log/trap, port stays up; shutdown (default) = err-disables the port. DHCP snooping drops server messages (OFFER/ACK) arriving on untrusted ports.

ACLs — The Packet Filter

```
| Type | Range | Filters on | Place it |
| --- | --- | --- | --- |
| Standard | 1-99 | Source IP only | Close to the destination |
| Extended | 100-199 | Source + dest IP, protocol, ports | Close to the source |
`
```

```
Router(config)# access-list 101 deny tcp 192.168.10.0 0.0.0.255 any eq 23
Router(config)# access-list 101 permit ip any any
Router(config-if)# ip access-group 101 in
`
```

- Rules process top-down, first match wins, ending in an **implicit deny all** — finish with `permit ip any any` (or your traffic dies).
- **Wildcard masks** invert subnet masks: `/24 → 0.0.0.255`. `host 10.1.1.1 = 0.0.0.0 wildcard`. (`/26 → 0.0.0.63`.)
- Named ACLs allow editing/removal of individual lines; numbered are append-only (`ip access -list extended NAME`).

NAT / PAT

```
| Type | What it does |
| --- | --- |
| Static NAT | One private IP ↔ one public IP (1:1). For servers needing a fixed public address |
| Dynamic NAT | Pool of public IPs assigned on demand — 1:1 while in use |
| PAT (overload) | Many private IPs ↔ one public IP using port numbers — the SOHO/branch standard |
`
```

```
Router(config)# ip nat inside source list 1 interface Gi0/0 overload
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config-if)# ip nat inside
Router(config-if)# ip nat outside
`
```

Inside source translates private→public (outbound). Mark interfaces: `ip nat inside` on the LAN side, `ip nat outside` toward the ISP. Reversed = nothing translates.



Intro

CCNA 200-301 Cheat Sheet

The commands, tables, and exam traps from the CCNA 200-301 blueprint — subnetting, VLANs, STP, OSPF, ACLs, NAT, wireless, and automation on one page.

DNS Records

Record	Maps
A	Hostname → IPv4
AAAA	Hostname → IPv6
CNAME	Alias → canonical name
MX	Domain → mail server
NS	Domain → authoritative name servers
PTR	IP → hostname (reverse lookup)

Single-Area OSPFv2 / OSPFv3

Concept	Know this
Area	CCNA covers single-area only — backbone area 0
Router ID	Highest loopback IP, else highest active physical IP; or set manually (best practice)
DR/BDR election	Highest OSPF priority (default 1), tie-break: highest router ID. Priority 0 = never DR
Neighbor requirements	Same area, same hello/dead timers, same subnet, matching authentication, unique router IDs
Cost	Reference bandwidth (100 Mbps default) / interface bandwidth — lower cost = preferred path
OSPFv3	Same concepts for IPv6; uses link-local addresses for neighbor formation

```
Router(config)# router ospf 1
Router(config-router)# router-id 1.1.1.1
Router(config-router)# network 10.0.0.0 0.0.0.255 area 0
Router# show ip ospf neighbor
Router# show ip ospf interface brief
```

Troubleshooting: neighbors stuck in EXSTART/EXCHANGE → suspect MTU mismatch. Stuck in INIT → hellos aren't getting through (ACL, timer mismatch, or multicast blocked).

First Hop Redundancy (HSRP / VRRP)

- Give hosts a virtual IP + virtual MAC as their gateway; one router is active, another standby — failover is transparent to hosts.
- HSRP (Cisco-proprietary) vs. VRRP (open standard) — same idea, know both names.
- Verify with `show standby brief`; preemption lets the higher-priority router retake the active role.



Static Routing

```
Router(config)# ip route 192.168.20.0 255.255.255.0 10.0.0.2
Router(config)# ipv6 route 2001:db8::/32 2001:db8:1::2
Router(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.2
Router(config)# ip route 192.168.30.0 255.255.255.0 10.0.0.6 10 (floating static)
```

- **Default route (0.0.0.0/0):** the "route of last resort" — points toward the ISP/internet.
- **Floating static:** same destination with a higher AD (e.g., 10) — sleeps until the primary route fails.
- **Host route (/32):** a route to one specific address — most specific, always wins the match.

Reading a Routing Table

```
R1# show ip route
O 192.168.20.0/24 [110/2] via 10.0.0.2, 00:14:33, Gig0/1
```

Field	Meaning
---	---
O	Source protocol: O=OSPF, C=connected, S=static, D=EIGRP, B=BGP
110/2	Administrative distance / metric — lower AD wins between protocols
via 10.0.0.2	Next-hop address
Gig0/1	Exit interface

Route selection order: 1) longest prefix match (most specific wins), 2) lowest administrative distance, 3) lowest metric.

Administrative Distance Ladder (memorize: 0-1-20-90-110-120-200)

Source	AD
---	---
Connected	0
Static	1
eBGP	20
EIGRP	90
OSPF	110
RIP	120
iBGP	200

Equal prefix length → lowest AD wins, regardless of metric.

Switch Port Recipes

- **Desktop/printer:** access port in the right VLAN + PortFast.
- **IP phone:** access (data) VLAN + voice VLAN; trust QoS markings from the phone.
- **Wireless AP:** trunk carrying AP-management + SSID VLANs (or access port for single-SSID).
- **PoE:** powers phones/APs/cameras over the data cable — check the switch's power budget before adding devices.



Spanning Tree — Rapid PVST+

Concept	Know this
Purpose	Prevents Layer 2 loops by blocking redundant paths; one instance per VLAN (PVST+)
Root bridge election	Lowest bridge ID wins (priority + MAC). Default priority 32768; set 4096/8192 to force it
Port roles	Root port (toward root), designated (forwarding per segment), alternate (blocked backup)
PortFast	Edge ports skip listening/learning — hosts come up instantly. Never on trunk/uplink ports
BPDU guard	Shuts down (err-disables) a PortFast port if a BPDU arrives — rogue switch protection
Root guard	Blocks a port from becoming root (keeps the hierarchy stable)
Loop guard	Prevents alternate/blocked ports from wrongly transitioning to forwarding
 `

```
Switch(config)# spanning-tree vlan 10 root primary
Switch(config-if)# spanning-tree portfast
Switch(config-if)# spanning-tree bpduguard enable
`
```

Election order is everything: lowest bridge ID → root bridge. For root ports: lowest path cost to the root, then lowest neighbor bridge ID, then lowest port priority/number.

EtherChannel / LACP

Concept	Know this
Purpose	Bundle 2–8 physical links into one logical link — more bandwidth + redundancy
LACP modes	active (initiates) / passive (responds) — at least one side must be active
Static ('on' mode)	No negotiation protocol — both sides must be 'on'
Rules	Same speed/duplex, same VLAN config on all member ports; max 8 active + 8 standby
 `

```
Switch(config)# interface range Gi0/1-2
Switch(config-if-range)# channel-group 1 mode active
Switch(config)# interface port-channel 1
Switch(config-if)# switchport mode trunk
`
```

`show etherchannel summary` — (P) bundled vs. (I) standalone/misconfigured.

VLANs & Trunking

Concept	Know this
VLAN	Broadcast-domain segmentation at Layer 2; hosts in different VLANs need a router (SVI) to talk
Access port	Carries one VLAN — connects end hosts
Trunk port	Carries multiple VLANs using 802.1Q tagging — switch-to-switch
Native VLAN	Untagged traffic on a trunk (default VLAN 1 — change it for security)
Voice VLAN	Separates VoIP traffic; phone + PC can share one port (data + voice VLANs)
 `



VLANs & Trunking (cont)

```
\
Switch(config)# vlan 10
Switch(config-vlan)# name SALES
Switch(config)# interface Gi0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config)# interface Gi0/24
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20
\
```

Trunk troubleshooting: native VLAN mismatch on the two ends breaks untagged traffic, and a VLAN missing from `allowed vlan` silently drops that VLAN's frames. Check both first.

Inter-VLAN Routing

- **SVI (switched virtual interface):** the Layer 3 path between VLANs on a multilayer switch.
- **Router-on-a-stick:** a router subinterface per VLAN over one trunk link.
- Same-VLAN works + gateways respond but VLANs can't reach each other → inter-VLAN routing (SVI/router) is misconfigured or missing.

Cables & Interfaces — Diagnose Fast

```
| Issue | Symptom / check |
| --- | --- |
| Speed/duplex mismatch | Late collisions, terrible throughput — hard-code both sides or leave both auto |
| Wrong cable type | No link — straight-through vs. crossover (auto-MDIX fixes most modern gear) |
| Distance exceeded | 100 m copper limit; errors climb past it — move to fiber |
| Fiber: wrong type | Single-mode vs. multimode mismatch = no link; check TX/RX polarity |
| Dirty connectors | Intermittent errors on fiber — clean with proper tools, never touch the endface |
| Collisions | Half-duplex relic; full-duplex links shouldn't show collisions at all |
show interfaces status · show interfaces Gi0/1 counters errors
```

Layers — Quick Map (as used in the guide)

```
| Layer | Lives here | Examples from the blueprint |
| --- | --- | --- |
| Layer 2 | Switching | VLANs, trunks (802.1Q), STP, EtherChannel, MAC/frames |
| Layer 3 | Routing | IP addressing, static routes, OSPF, ACLs, NAT, packets |
```

IP Addressing Essentials

```
### IPv4
| Concept | Know this |
| --- | --- |
| Private (RFC 1918) | 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 |
| APIPA | 169.254.x.x — DHCP failed |
| Loopback | 127.0.0.0/8 (reserved, not Class A usable) |
```



IP Addressing Essentials (cont)

| Default route | 0.0.0.0/0 — "everything" |
| Limited broadcast | 255.255.255.255 — "everyone here" |
IPv6
Concept	Know this
Global unicast	2000::/3 — publicly routable
Link-local	fe80::/10 — auto-configured on every interface; used for neighbor discovery
EUI-64	Builds the host portion from the MAC: flip the 7th bit, insert ff:fe in the middle
SLAAC	Stateless auto-configuration — hosts self-assign using router advertisements
Shorthand	Compress the longest run of zeros once with :: (e.g., 2001:db8::1)

Subnetting — The 30-Second Method

1. **Magic number** = 256 – interesting octet. Subnets increment by the magic number.
2. **Broadcast** = next subnet – 1. **Usable range** = everything between.
3. Example: 192.168.1.0/26 → magic 64 → subnets .0, .64, .128, .192; first subnet usable .1–.62, broadcast .63.
4. Usable hosts = $2^{\text{(host bits)}} - 2$. Subnet and broadcast addresses are never assignable.
CIDR Ladder (memorize cold)
CIDR	Mask	Hosts	Use it for
/24	255.255.255.0	254	Standard LAN subnet
/25	255.255.255.128	126	Splitting a /24 in half
/26	255.255.255.192	62	Small departments
/27	255.255.255.224	30	Point-of-sale, small VLANs
/28	255.255.255.240	14	Tiny segments
/29	255.255.255.248	6	DMZ server clusters
/30	255.255.255.252	2	Point-to-point WAN links
Exam favorite: /30 = 2 usable hosts is the standard point-to-point mask.



By **bytebar**

cheatography.com/bytebar/

Published 24th September, 2026.

Last updated 22nd October, 2026.

Page 9 of 9.

Sponsored by **Readable.com**

Measure your website readability!

<https://readable.com>