CCNA 200-301 Quick Reference

This is a categorized study reference for the CCNA 200-301 exam, including acronyms, protocols, port numbers, default timers, and critical facts you must memorize.

---

1. Layered Models & Protocol Basics

OSI ↔ TCP/IP Model Mapping:

OSI Layer	TCP/IP Layer
Application	Application
Presentation	Application
Session	Application
Transport	Transport
Network	Internet
Data Link	Network Access
Physical	Network Access

Key Protocols & Concepts:

- **OSI Model:** Conceptual seven-layer framework enabling modular network design and interoperability.
- **TCP/IP Model:** Four-layer model comprising Application, Transport, Internet, and Network Access layers.
- **MTU (Maximum Transmission Unit):** Largest frame size (bytes) that can be transmitted; Ethernet default = 1500 bytes.
- **TTL (Time To Live):** IP header field decremented at each hop to prevent routing loops.
- **TCP (Transmission Control Protocol):** Connection-oriented transport ensuring reliable, ordered delivery via sequencing and acknowledgments.
- **UDP (User Datagram Protocol):** Connectionless transport providing low-latency, best-effort delivery without flow control.
- **IP (Internet Protocol):** Network layer responsible for addressing, routing, and fragmentation of packets.
- **ICMP (Internet Control Message Protocol):** Provides error reporting and diagnostics (e.g., echo request/reply).
- **ARP (Address Resolution Protocol):** Resolves IPv4 addresses to MAC addresses via broadcast queries.
- **CSMA/CD (Carrier Sense Multiple Access with Collision Detection):** Ethernet access method with collision detection and binary exponential backoff.
- **VRF (Virtual Routing & Forwarding):** Enables multiple independent routing tables on a single device for traffic segmentation.
- **OUI (Organizationally Unique Identifier):** First 24 bits of a MAC address identifying the vendor/manufacturer.

2. Physical Layer: Cabling & Media

- **Cat5e** (Category 5e): Twisted-pair copper; supports 1000BASE-T (1 Gbps) up to 100 m; IEEE 802.3ab
- **Cat6** (Category 6): Twisted-pair copper; supports 1000BASE-T up to 100 m; IEEE 802.3an
- **Multimode Fiber (MMF)**: OM1–OM4; supports 10G–100G speeds; typical max distances: OM1 = 275 m at 1 Gbps, OM3/OM4 = 300–400 m at 10 Gbps
- **Singlemode Fiber (SMF)**: OS1/OS2; supports 10 km+ for 10G–100G links
- **Ethernet Cable Types:**
- **Straight-through**: host ↔ switch
- **Crossover**: switch ↔ switch, host ↔ host
- **Auto-MDIX**: automatically corrects cable type
- **Connectors:** RJ45 for copper; LC for fiber
- **Media Characteristics:**
- **Bandwidth**: copper vs. fiber differences
- **Distance limits**: copper (100 m), MMF (up to 400 m), SMF (10 km+)

3. Switching & VLANs

- **MAC** – Media Access Control: layer 2 hardware address
- **VLAN** – Virtual LAN: logical broadcast domain
- **VTP** – VLAN Trunking Protocol (Cisco): propagates VLAN config
- **STP** – Spanning Tree Protocol: prevents switching loops
- **RSTP** – Rapid STP (802.1w): faster STP convergence
- **PVST+** – Per-VLAN STP Plus: Cisco STP per VLAN
- **MST** – Multiple Spanning Tree: groups VLANs to a STP instance
- **PAgP** – Port Aggregation Protocol (Cisco): bundles links into EtherChannel
- **LACP** – Link Aggregation Control Protocol (IEEE): open standard EtherChannel
- **BPDU** – Bridge Protocol Data Unit: STP messages

Key Show Commands:

- `show vlan brief`, `show spanning-tree`, `show interfaces trunk`, `show mac address-table`

4. Routing

Routing Protocols

- **IGP** – Interior Gateway Protocol: routing within AS
- **RIP** – Routing Information Protocol: distance-vector, max hop = 15
- **OSPF** – Open Shortest Path First: link-state, uses areas
- **EIGRP** – Enhanced Interior Gateway Routing Protocol: Cisco hybrid
- **BGP** – Border Gateway Protocol: inter-AS routing (EGP)
- **AS** – Autonomous System: collection of IP networks
- **CIDR** – Classless Inter-Domain Routing: allows VLSM
- **VLSM** – Variable Length Subnet Masking: subnets of subnets
- **DUAL** – Diffusing Update Algorithm: used by EIGRP

Default Timers

- **OSPF Hello/Dead** – 10/40 sec (broadcast), 30/120 sec (NBMA)
- **RIP update interval** – 30 sec
- **EIGRP Hello/Hold** – 5/15 sec
- **BGP Keepalive/Hold** – 60/180 sec

---

5. IP Addressing & Subnetting

- **IPv4** – 32-bit address
- **IPv6** – 128-bit address
- **IPv6 Address Types & Notation:**
- Global Unicast (2000::/3)
- Link-Local (FE80::/10)
- Unique Local (FC00::/7)
- **Compression rules:** omit leading zeros in each 16-bit block; use "::" once to replace consecutive zero blocks
- **CIDR Notation** – Slash format (e.g., /24 for IPv4, /64 for IPv6)
- **Private IPv4 Ranges:**
- Class A: 10.0.0.0/8
- Class B: 172.16.0.0 – 172.31.255.255
- Class C: 192.168.0.0 – 192.168.255.255

6. Security Fundamentals

- **ACL** – Access Control List: traffic filtering
- **AAA** – Authentication, Authorization, Accounting
- **SSH** – Secure Shell: encrypted remote access (Port 22)
- **Telnet** – Unsecure remote CLI (Port 23)
- **SNMP** – Simple Network Management Protocol (Ports 161/162)
- **TACACS+** – Cisco AAA protocol (TCP Port 49)
- **RADIUS** – AAA protocol (UDP Ports 1812/1813)
- **Port Security** – Limits MACs per port
- **MFA** – Multi-Factor Authentication
- **IPS/IDS** – Intrusion Prevention/Detection System
- **IPsec** – Internet Protocol Security: a suite for authenticating and encrypting IP packets, including Authentication Header (AH) and Encapsulating Security Payload (ESP)---
- **GRE (Generic Routing Encapsulation)** – Tunneling protocol that encapsulates diverse network layer protocols within IP packets, enabling the creation of virtual point-to-point or multipoint links across IP networks.
- **SSL/TLS (Secure Sockets Layer / Transport Layer Security)** – Cryptographic protocols that authenticate communicating parties and provide confidentiality and data integrity, commonly used for securing HTTP (HTTPS) and other application traffic.
- **DAI (Dynamic ARP Inspection)** – A security feature that intercepts and validates ARP packets against DHCP snooping bindings to prevent ARP spoofing and poisoning

7. Wireless

- **SSID** – Service Set Identifier: Wi-Fi network name

- **AP** – Access Point
- **WLC** – Wireless LAN Controller
- **WEP** – Wired Equivalent Privacy (insecure)
- **WPA/WPA2** – Wi-Fi Protected Access (stronger encryption)
- **WPA3** – **SAE** (Simultaneous Authentication of Equals) replaces PSK to resist offline dictionary attacks
- **PSK** – Pre-Shared Key: WPA2-Personal
- **EAP** – Extensible Authentication Protocol
- **802.1X** – Port-based network access control (used with EAP)

Standard	Frequency Band
802.11	2.4 GHz
802.11b	2.4 GHz
802.11a	5 GHz
802.11g	2.4 GHz
802.11n	2.4 & 5 GHz
802.11ac	5 GHz

8. WAN Technologies

- **PPP** – Point-to-Point Protocol: Layer 2 WAN protocol
- **HDLC** – High-Level Data Link Control: Cisco default WAN encapsulation
- **CAPWAP (Control And Provisioning of Wireless Access Points):** Lightweight AP to WLC protocol transporting both control (UDP 5246) and data (UDP 5247) tunnels, enabling centralized management, configuration synchronization, and firmware updates.
- **MPLS** – Multiprotocol Label Switching: high-performance routing
- **VPN** – Virtual Private Network: secure remote access
- **IPsec** – Suite for securing IP traffic in VPNs
- **GRE** – Generic Routing Encapsulation: tunneling protocol
- **DSL (Digital Subscriber Line)** – Broadband over existing copper telephone lines; includes ADSL (asymmetric) and VDSL (very high speed) variants.
- **Cable Internet** – Broadband delivered via coaxial cable networks using DOCSIS standards; offers high downstream speeds over shared medium.
- **Leased Line** – Dedicated point-to-point circuit (e.g., T1, E1) providing symmetrical bandwidth with guaranteed SLA for enterprise WAN connectivity.

---

9. IP Services

- **DHCP** – Dynamic Host Configuration Protocol: automatically assigns IPv4 addresses and network options to hosts (UDP 67/68)
- **DNS** – Domain Name System: resolves domain names to IP addresses; queries over UDP and zone transfers over TCP (53)
- **NTP** – Network Time Protocol: synchronizes device clocks using hierarchical strata (UDP 123)
- **Syslog** – Centralized logging service for network events and alerts (UDP 514)
- **CDP** – Cisco Discovery Protocol: proprietary Layer 2 neighbor discovery for topology mapping

- **LLDP** – Link Layer Discovery Protocol: IEEE 802.1AB vendor-neutral neighbor discovery
- **NetFlow** – Cisco flow-based traffic monitoring and analysis
- **SNMP** – Simple Network Management Protocol: monitoring and configuration (GET/SET/TRAP) with community/v3 security (UDP 161/162)
- **NMS** – Network Management System: aggregates SNMP, NetFlow, and syslog data for dashboards, alerts, and topology visualization
- **NAT** – Network Address Translation: static (1:1), dynamic (pool), and PAT (many-to-one) for private↔public IP mapping
- **HSRP (v1/v2)** – Hot Standby Router Protocol: FHRP with Active/Standby roles, load sharing via groups (224.0.0.2 / 224.0.0.102)
- **VRRP** – Virtual Router Redundancy Protocol: IETF-standard FHRP with Master/Backup roles, preemption, VRID 1–255 (224.0.0.18)
- **GLBP** – Gateway Load Balancing Protocol: FHRP combining redundancy and per-host load balancing via AVG/AVFs
- **DSCP** – Differentiated Services Code Point: 6-bit field in IP header for QoS traffic classification and prioritization.

10. Ports to Memorize

Service	Port	Protocol
UDP Services		
DHCP Server	67	UDP
DHCP Client	68	UDP
DNS	53	UDP/TCP
SNMP (Query)	161	UDP
SNMP (Trap)	162	UDP
TFTP	69	UDP
RADIUS	1812/1813	UDP
TCP Services		
FTP (Data)	20	TCP
FTP (Control)	21	TCP
SSH	22	TCP
Telnet	23	TCP
TACACS+	49	TCP
HTTP	80	TCP
HTTPS	443	TCP

11. Cloud, Virtualization & Automation

Cloud Service Models

- **IaaS (Infrastructure as a Service):** Maximum control over OS, middleware, and applications; provider manages virtualization and hardware.
- **PaaS (Platform as a Service):** Provider maintains OS, runtime, and middleware; customer focuses on application deployment and data.
- **SaaS (Software as a Service):** Fully managed applications; customer configures only settings and data.

Virtualization Benefits & Technologies

- **Benefits:** Enhanced resource utilization, tenant isolation, rapid provisioning, workload consolidation.
- **Hypervisors:**
- **Type 1:** Bare-metal (e.g., VMware ESXi) for performance.
- **Type 2:** Hosted (e.g., VirtualBox) for flexibility.
- **VRF (Virtual Routing & Forwarding):** Multiple routing tables per device for traffic segmentation.

---

12. Automation & Programming

APIs & Data Models

- **API** – Application Programming Interface: standardized interfaces for programmatic network control.
- **REST** – Representational State Transfer: stateless, client-server architecture for web APIs.
- **Key Constraints:**
    1. Uniform interface
    2. Client-server separation
    3. Stateless interactions
    4. Cacheable responses
    5. Layered system
    6. Code on demand (optional)
- **JSON** – JavaScript Object Notation: lightweight, human-readable data interchange format.
- **YANG** – Data modeling language: defines configuration and state data for network devices.
- **NETCONF** – Network Configuration Protocol: uses YANG models to manage device configuration over secure transport.

Northbound & Southbound APIs

- **Northbound APIs:** Interfaces between network controllers and higher-level applications or orchestration platforms.
- **Southbound APIs:** Protocols the controller uses to communicate directly with network devices (e.g., NETCONF, RESTCONF).

Configuration Management Tools

- **Ansible:** Agentless, YAML-based playbooks; uses SSH for network device automation; idempotent modules. Python.

- **Terraform:** Declarative language (HCL) for provisioning infrastructure and network services; maintains state file.
- **Puppet:** Agent-based, model-driven; uses manifests and modules to enforce desired device state.
- **Chef:** Agent-based, imperative recipes written in Ruby DSL; managed via Chef Server.
- **SaltStack:** Master-minion architecture; event-driven automation using Python/YAML; communicates via ZeroMQ.

AI & Analytics Tools

- **Machine Reasoning Engine (MRE):** AI module for automated root-cause analysis and corrective action in Cisco Catalyst Center.
- **AI Endpoint Analytics:** Uses AI to assess endpoint performance and behavior for optimization and security insights.
- **AI-Enhanced RRM:** Applies AI-driven radio resource management to optimize wireless coverage, capacity, and interference mitigation.

13. Administrative Distance & Routing Protocols

Routing Source	AD
Directly Connected Interface	0
Static Route	1
EIGRP Summary Route	5
External BGP (eBGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
External EIGRP	170
Internal BGP (iBGP)	200
Unknown/Unusable	255

14. HTTP Response Codes

Code	Description
200	OK
301	Moved Permanently

Code	Description
302	Found (Temporary Redirect)
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error
503	Service Unavailable

15. AP Operational Modes

- **Local Mode:** The default mode where the AP hosts one or more BSSs for client association; all client data and management traffic are tunneled to the WLC for forwarding and control.
- **FlexConnect Mode:** Supports local switching of client data at the AP when WLC connectivity is intact or broken; maintains centralized management while offloading data traffic to the local network if needed.
- **Sniffer Mode:** AP acts as a traffic sensor, capturing raw 802.11 frames and forwarding them to an external packet analyzer (e.g., Wireshark) for troubleshooting.
- **Monitor Mode:** AP listens passively on all channels to detect rogue APs and clients; reports unauthorized devices to the WLC and can optionally deauthenticate them.
- **Rogue Detector Mode:** AP listens on the wired network for ARP and other packets, uses WLC-supplied rogue device lists to identify intruders, and reports them for remediation.
- **Spectrum Analyzer Mode (SE-Connect):** AP performs RF spectrum scans across channels to identify interference sources; streams spectrum data to analysis tools (e.g., Cisco Spectrum Expert).
- **Bridge/Mesh Mode:** AP functions as a point-to-point or point-to-multipoint wireless bridge, connecting disparate LAN segments without client association.
- **FlexPlusBridge Mode:** Combines FlexConnect local switching with Bridge/Mesh functionality, enabling resilient, locally-switched bridging even during WLC connectivity loss.