

CCNA: INTRODUCTION TO NETWORKS

Course Outline - Cisco Networking Academy

School Year 2026-2027

"The only roadblock to your success rests between your ears."

Program	Mission Valley Regional Occupational Program (MVROP)
Instructor	Hector Albizo
Grade Level	Grades 11-12
Course Length	Full academic year; block schedule
Credits	10 high school credits, subject to MVROP policy
Primary Curriculum	Cisco Networking Academy - CCNA: Introduction to Networks (ITN)
Cisco Position	First course in the three-course CCNA sequence

Course Purpose

Provide students with the networking foundation required to configure and troubleshoot small networks, continue into CCNA Switching, Routing, and Wireless Essentials, and understand the infrastructure supporting cybersecurity, cloud, AI, IoT, and industrial technologies.

1. 1. Course Competencies

- Explain network architectures, devices, protocols, layered communication, and data flow.
- Configure basic Cisco switch and router settings using IOS CLI.
- Explain physical media, Ethernet, MAC addressing, switching, ARP, and network-layer forwarding.
- Design and apply IPv4 subnetting and configure IPv4/IPv6 addressing.
- Use ICMP and diagnostic commands to verify and troubleshoot connectivity.
- Explain TCP/UDP, ports, and common application-layer services.
- Apply foundational security and secure-management practices.
- Build, document, verify, and troubleshoot a small network using Packet Tracer and physical Cisco equipment.
- Connect networking fundamentals to cybersecurity, automation, AI infrastructure, IoT, and OT environments.

2. 2. Module-by-Module Course Outline

The sequence below follows the CCNA: Introduction to Networks instructional progression. Timing is tentative and intentionally provides additional practice for configuration, subnetting, troubleshooting, and physical labs.

Module	Core Content	Demonstrated Skills / Labs	Applied Context	Tentative Pacing
1. Networking Today	Network impact; components; representations; topologies; LAN/WAN/Internet; reliable networks; trends	Identify devices/roles; interpret topology diagrams; explore Packet Tracer	Enterprise, cloud, AI, IoT and industrial systems all depend on networks	Week 1
2. Basic Switch and End Device Configuration	IOS access; command structure; hostnames; passwords; interfaces; IP settings	Console/CLI access; basic switch setup; end-device addressing; save/verify configs	Professional device-management fundamentals	Weeks 2-3
3. Protocols and Models	Rules; protocols; suites; standards; OSI and TCP/IP; encapsulation; data access	Trace encapsulation; identify PDU at each layer; compare OSI/TCP-IP models	Framework for troubleshooting and cybersecurity analysis	Week 4

Module	Core Content	Demonstrated Skills / Labs	Applied Context	Tentative Pacing
4. Physical Layer	Signals; bandwidth; copper; fiber; wireless; connectors; media selection	Cable/media identification; physical-layer troubleshooting; interface status	Bandwidth and media choices for AI/data, Wi-Fi, IoT and industrial environments	Weeks 5-6
5. Number Systems	Binary; decimal; hexadecimal conversions; IPv4 bit structure; Ethernet hexadecimal notation	Binary/decimal/hex conversion; prefix/mask preparation	Foundation for addressing, subnetting, MAC and IPv6 interpretation	Week 7
6. Data Link Layer	Frames; MAC sublayer; media access; topologies; LAN/WAN data-link concepts	Analyze frame roles; identify Layer 2 addressing and access methods	Understanding switching, wireless, and local delivery	Week 8
7. Ethernet Switching	Ethernet frames; MAC addresses; MAC tables; switch forwarding/filtering; switching methods	Observe MAC learning; inspect MAC table; troubleshoot Layer 2 connectivity	High-speed LAN switching for users, servers and connected devices	Week 9
8. Network Layer	IPv4/IPv6 packet; host forwarding; default gateway; routing tables; router forwarding	Determine local/remote delivery; inspect routing information; trace packet path	Foundation for routed enterprise, cloud and segmented networks	Weeks 10-11
9. Address Resolution	MAC/IP relationships; ARP; IPv6 Neighbor Discovery; default-gateway resolution	Inspect ARP cache; observe address resolution; diagnose local-delivery issues	Endpoint-to-network communication and troubleshooting	Week 12
10. Basic Router Configuration	Initial router settings; interfaces; gateway configuration; verification	Configure router hostname/security/interfaces; save and verify configuration	Core router administration and change discipline	Weeks 13-14
11. IPv4 Addressing	Address structure; public/private; subnet masks; prefixes; subnetting; variable host needs	Calculate subnets; create addressing plans; configure/verify IPv4 networks	Scalable network design; major mastery emphasis	Weeks 15-20
12. IPv6 Addressing	IPv6 need/format; unicast types; static/dynamic addressing; link-local; multicast; subnetting	Configure IPv6; identify address types; verify IPv6 reachability	Modern dual-stack infrastructure and large address spaces	Weeks 21-22
13. ICMP	ICMPv4/v6; reachability; ping; traceroute/tracert; message purpose	Use ping and traceroute; interpret success/failure; isolate faults	Evidence-based troubleshooting rather than guessing	Week 23
14. Transport Layer	Segmentation; TCP vs UDP; ports; sockets; reliability; connection establishment	Identify TCP/UDP use; interpret port numbers and session behavior	Application performance, services, telemetry and security awareness	Weeks 24-25
15. Application Layer	Client-server; peer-to-peer; web/email/DNS/DHCP/file services; application protocols	Map applications to protocols/ports; observe service dependencies	Cloud, web, API and enterprise-service delivery	Weeks 26-28
16. Network Security Fundamentals	Threats; vulnerabilities; attacks; device hardening; authentication; secure access	Apply basic security settings; secure credentials; discuss common attack surfaces	Bridge from networking into cybersecurity coursework	Weeks 29-31
17. Build a Small Network	Design; addressing; device selection; protocols; verification; troubleshooting	Plan/build/configure/document/troubleshoot an integrated small network	Cumulative network engineering and workplace practice	Weeks 32-34
Capstone and Review	Cumulative skills; troubleshooting; documentation; career alignment	Physical/Packet Tracer capstone; practical skills check; peer review	Preparation for SRWE and continued networking/cybersecurity pathway	Weeks 35-36

3. 3. Hands-on Laboratory Progression

- Packet Tracer orientation and topology construction.
- Cisco IOS command-line navigation and configuration management.
- Switch setup, end-device addressing, connectivity testing, and MAC-table observation.
- Router interface configuration and default-gateway implementation.
- IPv4 subnet design and implementation using repeated practical exercises.
- IPv6 configuration and dual-stack connectivity verification.
- Protocol and traffic observation using approved diagnostic tools and Wireshark where appropriate.
- Integrated small-network build using physical Cisco routers/switches and/or Packet Tracer.
- Structured troubleshooting challenge requiring symptoms, evidence, hypothesis, corrective action, and verification.

4. 4. Assessment Evidence

Evidence Type	Purpose	Typical Evidence
Hands-on configuration	Demonstrate technical skill	IOS configurations, screenshots/output, instructor observation, physical-device checks

Evidence Type	Purpose	Typical Evidence
Packet Tracer	Apply concepts in simulation	Completed topologies, addressing, device configuration, verification
Subnetting and addressing	Demonstrate numerical/logic mastery	Subnet worksheets, addressing plans, IPv4/IPv6 practical assessments
Troubleshooting	Demonstrate diagnostic reasoning	Fault isolation notes, show-command evidence, corrective action, validation
Knowledge assessments	Measure conceptual understanding	Cisco module checks, quizzes, unit tests
Capstone	Integrate course competencies	Small-network design/build, documentation, verification, presentation

5. 5. AI, IoT, OT, and Cybersecurity Connections

- AI: Students learn the addressing, switching, routing, bandwidth, latency, and reliability concepts that AI-enabled systems depend on. AI may assist analysis only when instructor-directed.
- IoT: Sensors and connected endpoints are used as examples of devices requiring appropriate media, addressing, gateway access, and application connectivity.
- OT: Industrial/operational systems are introduced as another networked environment; specialized OT cybersecurity remains an embedded strand of the cybersecurity coursework rather than a separate ITN course.
- Cybersecurity: Secure access, device hardening, traffic awareness, segmentation concepts, and troubleshooting provide prerequisites for later cybersecurity operations work.

6. 6. Professional and CTE Expectations

- Follow lab safety and equipment-handling procedures.
- Use only instructor-authorized devices, networks, software, accounts, and diagnostic techniques.
- Document addressing, cabling, configurations, tests, and results accurately.
- Protect credentials and configuration information and never share accounts.
- Communicate and collaborate professionally during labs and troubleshooting.
- Maintain current coursework; bulk submission of missing work during the final week of a semester or year-end grading period will not be graded.
- No food or drink is permitted in the classroom or lab except as formally authorized.
- AI and personal-device use are governed by the full syllabus and instructor direction.

7. 7. Pathway Progression

ITN establishes the foundation for continued networking and cybersecurity study. The intended progression is ITN -> CCNA Switching, Routing, and Wireless Essentials (SRWE) -> advanced networking/cybersecurity applications. The full CCNA certification extends beyond ITN into network access, IP services, security, and automation/programming.

8. 8. Reference Basis

Cisco Networking Academy, CCNA: Introduction to Networks - current course catalog.

Cisco, 200-301 CCNA v1.1 certification overview and exam domains.

MVROP classroom, laboratory, academic-integrity, AI-use, and device-policy expectations as stated in the companion syllabus.

Document status: Sequence and pacing may be adjusted for the MVROP calendar, equipment, student mastery, Cisco curriculum updates, and administrative direction.