

CCNA: INTRODUCTION TO NETWORKS

Cisco Networking Academy-Aligned Course Syllabus

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
Course Type	Career Technical Education / UC a-g "g" elective
Primary Curriculum	Cisco Networking Academy - CCNA: Introduction to Networks (ITN)

Course Mission

Students will learn how modern networks operate, configure foundational Cisco router and switch functions, design IPv4 and IPv6 addressing plans, troubleshoot connectivity, secure basic network access, and communicate technical work using professional documentation and industry practices.

1. Course Overview

CCNA: Introduction to Networks is a yearlong CTE networking course built around Cisco Networking Academy's Introduction to Networks curriculum. It is the first course in Cisco's three-course CCNA sequence and establishes the networking foundation required for more advanced switching, routing, wireless, cybersecurity, cloud, automation, and infrastructure coursework. Students learn through direct configuration, Packet Tracer simulation, physical equipment, troubleshooting exercises, documentation, and applied industry scenarios.

2. Course Framework and Alignment

The syllabus integrates four complementary structures:

- Cisco Networking Academy CCNA: Introduction to Networks competencies in network architecture, protocols, Ethernet, IP addressing, routing fundamentals, transport/application services, security fundamentals, and small-network design.
- Hands-on Cisco IOS configuration and troubleshooting using physical routers and switches and Cisco Packet Tracer.
- Career Technical Education practices emphasizing safety, documentation, teamwork, troubleshooting discipline, professional communication, and responsible technology use.
- Modern infrastructure context showing how networking supports AI-enabled systems, cloud services, IoT, industrial/OT environments, cybersecurity operations, and other connected technologies without turning ITN into an AI or OT specialization course.

3. Prerequisites and Student Readiness

- No formal networking prerequisite is required unless established by MVROP enrollment policy.
- Basic familiarity with computers and operating systems is helpful but not required.

- Students must be willing to read technical material, learn command-line syntax, document work, troubleshoot methodically, collaborate professionally, and persist through problems that may require multiple attempts.
- Success requires practical arithmetic and logical reasoning, especially binary/hexadecimal concepts, subnetting, addressing, and interpreting network behavior. Advanced mathematics is not required.

4. Student Learning Outcomes

- Explain how network components, topologies, protocols, and layered models support end-to-end communication.
- Use Cisco IOS command-line tools to perform basic router and switch configuration, verification, and management.
- Describe physical media, Ethernet framing, MAC addressing, switching behavior, and address resolution.
- Explain IPv4 and IPv6 packet delivery and the role of routers in forwarding traffic between networks.
- Design and document IPv4 subnetting plans using appropriate masks, prefixes, host ranges, network addresses, and broadcast addresses.
- Configure and verify IPv4 and IPv6 addressing on end devices and network devices.
- Use ICMP, ping, traceroute/tracert, ipconfig/ifconfig/ip, arp, show commands, and other approved tools to troubleshoot connectivity.
- Differentiate TCP and UDP and explain common application-layer services and protocols.
- Apply basic network security practices including secure device access, strong authentication, configuration protection, and awareness of common threats.
- Build, verify, document, and troubleshoot a functional small network using physical equipment and Packet Tracer.
- Explain how reliable, secure, scalable networking provides the infrastructure for AI, cloud, IoT, cybersecurity, and industrial systems.
- Communicate technical findings through diagrams, addressing tables, configuration records, troubleshooting notes, lab reports, and team briefings.

5. Course Content and Tentative Pacing

Pacing will be adjusted to the MVROP calendar, student needs, lab availability, equipment readiness, and the pace required for mastery. Cisco Networking Academy lists ITN as approximately 70 hours of curriculum; the yearlong MVROP course extends that foundation through additional physical-device labs, Packet Tracer practice, subnetting repetition, troubleshooting, projects, career applications, and cumulative review.

Instructional Block	Cisco ITN Modules	Primary Topics	Hands-on Emphasis	Modern Infrastructure Context	Tentative Timing
1. Network Foundations	1-3	Networks Today; basic switch/end-device configuration; protocols and models	Packet Tracer orientation; IOS CLI; hostnames; passwords; interfaces; connectivity verification	Networks as the foundation for cloud and AI services	Weeks 1-4
2. Media, Number Systems, and Ethernet	4-7	Physical layer; binary/hexadecimal; data link; Ethernet switching	Cabling; interface status; MAC tables; frame forwarding; binary/hex practice	High-speed wired infrastructure for data-intensive systems	Weeks 5-9
3. Network Layer and Routing Foundations	8-10	IPv4/IPv6 packet concepts; forwarding; ARP/ND concepts; basic router configuration	Router IOS; interfaces; default gateway; routing decisions; ARP observation	Routing between enterprise, cloud, IoT, and industrial segments	Weeks 10-14
4. IPv4, IPv6, and ICMP	11-13	IPv4 addressing/subnetting; IPv6 addressing; ICMP	Subnet design; VLSM awareness; IPv4/IPv6 configuration; ping/traceroute; troubleshooting	Address planning and reachability for scalable connected environments	Weeks 15-23

Instructional Block	Cisco ITN Modules	Primary Topics	Hands-on Emphasis	Modern Infrastructure Context	Tentative Timing
5. Transport and Application Services	14-15	TCP/UDP; ports; application-layer protocols and services	Protocol/port analysis; client-server traffic; Packet Tracer simulations	Application delivery, APIs, cloud services, telemetry, and AI workloads	Weeks 24-28
6. Security and Small-Network Integration	16-17	Network security fundamentals; small-network design, configuration, verification, troubleshooting	Secure access; backup configs; integrated Packet Tracer and physical-network build	Security-by-design for enterprise, IoT, OT, and AI-enabled environments	Weeks 29-34
Integration and Capstone	Cumulative	End-to-end network design, documentation, troubleshooting, career readiness	Small-network capstone; skills check; peer review; troubleshooting challenge	Connecting networking fundamentals to SRWE, cybersecurity, automation, and regional technology careers	Weeks 35-36

6. AI, IoT, and OT Infrastructure Context

- ITN remains a foundational networking course. AI, IoT, and Operational Technology (OT) are used as context to show why networking skills matter, not as separate technical specializations within this course.
- Students connect bandwidth, latency, addressing, routing, availability, and security concepts to AI-enabled applications and data movement.
- IoT examples demonstrate how sensors, endpoints, gateways, and services depend on correct addressing and reliable network connectivity.
- OT examples introduce the idea that industrial devices and control environments also depend on networking, while more specialized OT security concepts are addressed within the cybersecurity pathway.
- Students learn that AI can assist network professionals with analysis and troubleshooting, but human verification, configuration knowledge, and accountability remain essential.

7. Instructional Methods

- Instructor demonstrations and guided configuration practice.
- Cisco Networking Academy modules, quizzes, interactive activities, and skills practice.
- Cisco Packet Tracer simulation and troubleshooting activities.
- Physical Cisco router and switch configuration using console and Ethernet connections.
- Subnetting drills, addressing exercises, network diagrams, and configuration documentation.
- Individual and team troubleshooting scenarios requiring evidence-based diagnosis rather than guessing.
- Career and infrastructure scenarios linking networking to cybersecurity, cloud, AI, IoT, and industrial environments.
- Instructor-authorized AI-supported activities when they reinforce rather than replace student networking skills.

8. Primary Resources and Technology

- Cisco Networking Academy - CCNA: Introduction to Networks curriculum.
- Cisco Packet Tracer and instructor-provided Packet Tracer activities.
- School-managed Windows computers and approved networking software.
- Cisco routers, switches, console cables, Ethernet cabling, and related lab equipment.
- Command-line tools and approved diagnostic utilities such as ping, tracer/traceroute, ipconfig, arp, nslookup, and Wireshark when appropriate.
- Instructor-provided diagrams, addressing worksheets, troubleshooting cases, technical references, and current industry examples.

School-Managed Devices Only

Personal laptops and unapproved computing devices may not be connected to the classroom or lab network. Students will use school-managed systems and instructor-approved equipment and software.

9. Assessment and Grading

The proposed grading categories below may be adjusted to conform to final MVROP grading policy and instructor implementation. Students are evaluated on technical accuracy, demonstrated skill, troubleshooting process, documentation, and professional practice.

Category	Weight	Examples
Hands-on labs and configurations	35%	Router/switch configuration, Packet Tracer, cabling, addressing, verification, troubleshooting
Projects and applied network work	25%	Network builds, addressing plans, diagrams, troubleshooting scenarios, capstone
Unit assessments	25%	Quizzes, tests, subnetting assessments, practical skills checks
Cisco coursework and knowledge checks	10%	NetAcad modules, quizzes, interactive activities, review
Professional practice	5%	Preparedness, safety, documentation, teamwork, equipment care, ethical conduct

10. Assignment Submission and Late-Work Policy

- Assignments are due by the date and time posted by the instructor. Students are responsible for checking the learning-management system and maintaining current work throughout the term.
- Students should communicate early when illness, an approved absence, an accommodation, or an emergency affects completion of work. Extensions are not automatic and must be arranged in accordance with MVROP policy.
- Technical work may require revision after feedback. Revision opportunities, when offered, must be completed by the published deadline.

ABSOLUTELY NO BULK END-OF-TERM SUBMISSIONS

Multiple missing assignments submitted during the final week of a semester or the year-end grading period will not be accepted or graded. Students are expected to remain current throughout the term. This restriction does not eliminate legally required accommodations or individually approved exceptions established before the final week.

11. Artificial Intelligence Use for Coursework

- Artificial intelligence may be used for assignments only at the direction and under the guidance of the instructor. AI is a professional tool, not a substitute for student reasoning, technical skill, evidence, or accountability.
- Use AI only when the instructor explicitly authorizes it for the assignment or activity.
- Follow the stated purpose, tool, account, prompt, data, and collaboration restrictions.
- Do not enter student records, passwords, personally identifiable information, medical information, confidential school information, proprietary data, network credentials, or live network/security information into an AI system.
- Verify AI-generated commands, configurations, subnetting, calculations, citations, troubleshooting steps, and recommendations before use.
- Disclose and document AI assistance when required, including prompts, outputs, revisions, and sources.
- Do not use AI to complete an assessment, generate an entire submission, conceal a lack of understanding, fabricate lab results, or misrepresent authorship.

- Students remain responsible for the accuracy, safety, legality, ethics, and quality of all submitted work, regardless of AI assistance.
- The instructor may require students to reproduce, explain, defend, or complete work without AI support.

12. Network Ethics, Authorization, and Academic Integrity

- All configuration, discovery, packet analysis, troubleshooting, and network testing must remain within instructor-approved systems, accounts, devices, simulations, and lab boundaries.
- Students may not scan, probe, intercept, disrupt, bypass controls, obtain credentials for, or attempt unauthorized access to MVROP, school-district, public, private, or internet-connected systems.
- Network commands and diagnostic techniques taught for education may not be used against another person or organization without explicit authorization.
- Account sharing, password sharing, plagiarism, unauthorized collaboration, copied configurations, fabricated Packet Tracer results, and undisclosed AI-generated work are prohibited.
- Students must protect configuration files, addressing plans, credentials, device access, and other information designated by the instructor as privileged or restricted.
- Violations may result in loss of lab privileges, academic consequences, referral to administration, and other action under applicable policy or law.

13. Classroom and Laboratory Safety

- Follow all instructor directions before powering, cabling, opening, moving, or configuring equipment.
- Maintain clear walkways and manage Ethernet, console, power, and patch cables to prevent trip, electrical, and equipment hazards.
- Do not connect personal laptops, storage devices, adapters, cables, hotspots, switches, routers, access points, or other network equipment without permission.
- Report damaged equipment, exposed wiring, overheating, unusual odors, spills, safety concerns, and network/security incidents immediately.
- Do not remove equipment, media, cables, components, configuration files, or documents from the classroom or lab without authorization.
- Use electrostatic-discharge controls and other safety equipment when directed.

NO FOOD OR DRINK

Food and beverages are not permitted in the classroom or laboratory. This prohibition protects students and electrical, computer, and network equipment. Any medically required exception must be handled in accordance with applicable accommodation and safety procedures.

14. MVROP Cell Phone & Electronic Device Policy

MVROP Cell Phone & Electronic Device Policy Tentative pending Board approval Fall of 2026

To prepare you for professional industry standards and comply with California state law (AB 3216 / CA Education Code § 48901.7), our class follows a "Workplace-First" device policy.

1. Expectation: Off & Away

Unless explicit permission is given, all personal devices (phones, smartwatches, earbuds) must be turned off or silenced and stored out of sight in your backpack or assigned caddy.

2. Academic & CTE Exceptions

Your phone is a professional tool when used appropriately. Devices are only permitted when authorized by the instructor for relevant coursework, such as:

Accessing digital blueprints, safety manuals, or specialized software.

Scanning diagnostic QR codes or photographing lab/portfolio projects.

Participating in class check-ins or quick assessments.

Note: Academic permission is never an allowance for social media, texting, gaming, or unauthorized photos/videos.

3. Safety & Professionalism

Zero Tolerance in Active Labs: Phones and earbuds are strictly prohibited near machinery, power tools, lifts, welding equipment, or during clinical procedures. Distraction is a major safety hazard.

Privacy: Unauthorized audio or visual recording in labs or changing areas is strictly forbidden.

4. Legal & Medical Exemptions

Per state law, devices may be accessed for documented medical monitoring (for example, glucose tracking), IEP/504 accommodations, or genuine emergency situations.

Implementation Notice

This device-policy language is tentative pending final MVROP Board approval for Fall 2026 and must be conformed to the final Board-adopted policy, applicable sending-district requirements, student safety procedures, and California law.

15. Device-Policy Enforcement

- The instructor will use progressive classroom interventions consistent with the final MVROP policy and applicable student-discipline procedures.
- Unauthorized device use may result in the device being placed in the assigned storage location, loss of discretionary device privileges, parent/guardian contact, administrative referral, or other consequences authorized by policy.
- A student may not use a personal device to photograph, record, livestream, or distribute another person's image, voice, work, screen, credentials, or private information without authorization.
- Refusal to follow a safety-related direction may result in immediate removal from the active lab area.

16. Attendance, Participation, and Professional Standards

- Regular attendance is essential because many physical-device labs, Packet Tracer activities, demonstrations, team exercises, and troubleshooting scenarios cannot be fully replicated independently.
- Students are expected to arrive on time, prepared to work, and ready to follow the daily lab status and safety briefing.
- Professional conduct includes respectful communication, accurate documentation, methodical troubleshooting, care of equipment, accountability for assigned roles, and constructive participation.
- Students who miss class are responsible for obtaining instructions and completing eligible make-up work within the permitted timeline.

17. Student Support, Accessibility, and Accommodations

MVROP will provide support and legally required accommodations in accordance with applicable law, Board policy, IEPs, Section 504 plans, English-learner supports, and documented student needs. Students should communicate with the instructor, counselor, case manager, or administrator as early as possible when support is needed. Accommodations do not waive safety, ethics, authorization, or academic-integrity requirements, but may change how a student accesses instruction or demonstrates learning.

18. Cisco Certification and Pathway Preparation

- CCNA: Introduction to Networks is the first course in Cisco Networking Academy's three-course CCNA sequence.
- The course establishes foundational skills that support progression to CCNA: Switching, Routing, and Wireless Essentials and then Enterprise Networking, Security, and Automation.
- ITN supports preparation for entry-level networking competencies and contributes to broader CCNA preparation, but completion of ITN alone does not cover all objectives of the 200-301 CCNA certification exam.
- The broader current CCNA certification assesses network fundamentals, network access, IP connectivity, IP services, security fundamentals, and automation and programmability.

- Completion of the course does not guarantee certification, employment, college credit, or placement. Testing eligibility, fees, accommodations, and procedures are governed by Cisco, MVROP, and the testing center.

19. Student and Parent/Guardian Acknowledgment

By signing below, the student and parent/guardian acknowledge that they have reviewed this syllabus, understand the course expectations, and agree to support safe, ethical, professional, and timely participation. The signatures also acknowledge the following key requirements:

Network configuration and testing are permitted only within instructor-authorized systems and lab boundaries.

AI may be used only when and how the instructor authorizes it.

Personal devices must comply with the Workplace-First device policy and active-lab safety restrictions.

Food and drink are prohibited in the classroom and laboratory, except as formally authorized.

Multiple missing assignments submitted during the final week of a semester or year-end grading period will not be graded.

The device-policy section remains tentative pending final Board action and will be updated to match adopted policy.

Student Name (print)		
Student Signature		Date
Parent/Guardian Name (print)		
Parent/Guardian Signature		Date
Best Contact Email/Phone		

Questions or concerns: Please contact the instructor through the official MVROP communication channel.

20. Framework References

Cisco Networking Academy, CCNA: Introduction to Networks - current course catalog (70-hour instructor-led course; first in the CCNA three-course series).

Cisco, 200-301 CCNA v1.1 - current certification domains: network fundamentals, network access, IP connectivity, IP services, security fundamentals, and automation and programmability.

California Assembly Bill 3216 (Phone-Free Schools Act) and California Education Code § 48901.7.