INFOSEC Skills

LIVE BOOT CAMPS

## Get live, expert instruction from anywhere.

# CCNA Dual Certification Boot Camp

Infosec's authorized CCNA Dual Certification Boot Camp helps you build your knowledge of networking and provides hands-on experience installing, configuring and operating network devices — all while preparing you to earn two Cisco certifications.

### Course description

This innovative seven-day boot camp is designed specifically for network engineers and administrators requiring full knowledge of Cisco router and switch configuration. You'll gain hands-on experience by completing a series of labs in our Networking Cyber Range. The labs provide practical experience in a networking and switching environment and prepare you for the simulation-based questions you'll find on the CCNA exam.

In addition to gaining the in-depth knowledge about network access, IP connectivity, IP services, and automation and programmability for Cisco networks, you will learn about the hottest area of networking: network security. Our expert instructors first prepare you to pass the CCNA exam. After passing that exam, you will then train directly on the Cisco Certified CyberOps Associate curricula — all in one sitting.

### Who should attend

- » Network engineers
- » Network administrators
- » Systems administrators
- » System engineers
- » IT managers/directors
- » Anyone looking to improve their network skills

## Boot camp at a glance

### Certifications

- ✓ CCNA
- ✓ Cisco Certified CyberOps Associate

### Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

### Training duration

- ✓ Pre-study course
- ✓ 7-day boot camp
- ✓ 90-day extended access to all boot camp materials

### The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

**Start training immediately**

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

**Learn by doing in the cyber range**

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

**Get unlimited custom practice exams**

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

**700+ IT and security courses**

Earn CPEs and build new skills with 100s of additional training courses.

# What's included

- Seven days of live, expert instruction
- Exam Pass Guarantee
- Exam voucher
- Unlimited practice exam attempts
- 100% Satisfaction Guarantee
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- 90-day extended access to all boot camp video replays and materials
- Onsite proctoring of exam
- Pre-study learning path
- Knowledge Transfer Guarantee

### Prerequisites

Prior to attending the CCNA Dual Certification Boot Camp, you should be familiar with networking topics such as TCP/IP, IP configuration, peer-to-peer networking, subnetting, building a routing table and other network protocols, standards and architecture.

## CCNA certification objectives

Upon the completion of this boot camp, you will know how to:

- Make appropriate decisions concerning implementation of hardware and configuration, based on ISR routers and switches running the Cisco iOS
- Proficiently administer Cisco routers
- Install, configure and maintain dependable, functional networks
- Properly identify protocols involving
- Cisco networking devices
- Troubleshoot general network and security issues
- Successfully operate routers and switched LAN networks
- Follow enterprise network design principles
- Understand routing protocols design considerations (OSPF and EIGRP)

## Go beyond the CCNA

After successfully passing the CCNA exam, you will continue your study to prepare for the Cisco Certified CyberOps Associate by learning:

- Security concepts
- Security monitoring
- Host-based analysis
- Network intrusion analysis
- Security policies and procedures

## Dual certification details

After completing this boot camp, you will be certified with the following Cisco certifications:

- **CCNA certification:** The CCNA certification serves as the foundation for all the other certifications in the new Cisco certification program.
- **Cisco Certified CyberOps Associate certification:** Cisco Certified CyberOps Associates are prepared to work as a part of a Security Operations Center (SOC) team to detect and respond to network security threats.

## Skill up and get certified, guaranteed

### Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.

### 100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

### Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

# What our students are saying

We had exactly what was needed to prepare us for our exams. The instructor was great. You could tell he loves teaching and was able to keep your attention and get the class to understand the material. I would recommend him as a teacher for CCNA to anyone.

**Daniel Knight**
Hillphoenix

An excellent instructor that obviously knows the material by heart. He was always clear and concise in his explanations and would break it down if anyone in the class didn't quite get how something worked. He is by far one of my favorite instructors ever, even though I only spent seven days with him.

**Chris Soule**
Rocky Gap Resort

My instructor was excellent. He made sure that I not only knew the information in order to pass my exams. He took it upon himself to teach us real-world knowledge that is necessary to do my job today.

**Jeffrey McGill**
TIC Gums, Inc.

My CCNA instructor has thus far been the best I've had throughout my career (being in the military, that is a LOT of training). He was extremely knowledgeable on the material and was extremely skilled at teaching it.

**Shawn Tierney**
United States Air Force

# CCNA Dual Certification details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

| | Day 1 | Day 2 | Day 3 | Day 4 | Day 5 | Day 6 | Day 7 |
|---|---|---|---|---|---|---|---|
| Morning session | Network fundamentals | Network access | IP connectivity | IP services | Automation and programmability | Security concepts<br>Security monitoring | Network intrusion analysis (cont)<br>Security policies and procedures |
| Afternoon session | Network fundamentals | Network access | IP connectivity | Security fundamentals | Exam prep<br>Take CCNA 200-301 exam | Host-based analysis<br>Network intrusion analysis | Exam prep<br>Take 200-201 exam |
| Evening session | Optional group & individual study | Optional group & individual study | Optional group & individual study | Optional group & individual study | Optional group & individual study | Optional group & individual study | |

*Schedule may vary from class to class*

## Course Outline

### Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills, including an in-depth CCNA prep course, the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

## CCNA (200-301)

### Network fundamentals

- Role and function of network components
  - Routers
  - L2 and L3 switches
  - Next-generation firewalls and IPS
  - Access points
  - Controllers (Cisco DNA Center and WLC)
  - Endpoints
  - Servers
- Characteristics of network topology architectures
  - 2 tier
  - 3 tier
  - Spine-leaf
  - WAN
  - Small office/home office (SOHO)
  - On-premises and cloud
- Compare and contrast network topologies
- Physical interface and cabling types
  - Single-mode fiber, multimode fiber, copper
  - Connections (Ethernet shared media and point-to-point)
  - Concepts of PoE
- Interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
- TCP and UDP
- Configuring and verifying IPv4 addressing and subnetting
- The need for private IPv4 addressing
- Configuring and verifying IPv6 addressing and prefix
- IPv6 address types

    - Global unicast
    - Unique local
    - Link local
    - Anycast
    - Multicast
    - Modified EUI 64
- Verifying IP parameters for client OS (Windows, Mac OS, Linux)
- Wireless principles
    - Nonoverlapping Wi-Fi channels
    - SSID
    - RF
    - Encryption
- Virtualization fundamentals (virtual machines)
- Switching concepts
    - MAC learning and aging
    - Frame switching
    - Frame flooding
    - MAC address table

## Network access

- Configuring and verifying VLANs (normal range) spanning multiple switches
    - Access ports (data and voice)
    - Default VLAN
    - Connectivity
- Configuring and verifying interswitch connectivity
    - Trunk ports
    - 802.1Q
    - Native VLAN
- Configuring and verifying Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
- Configuring and verifying (Layer 2/ Layer 3) EtherChannel (LACP)
- The need for and basic operations of
- Rapid PVST+ Spanning Tree Protocol
    - Root port, root bridge (primary/ secondary), and other port names
    - Port states (forwarding/blocking)
    - PortFast benefits
- Cisco Wireless Architectures and AP modes
- Physical infrastructure connections of WLAN
- components (AP, WLC, access/ trunk ports, and LAG)
- AP and WLC management access connections (Telnet,
- SSH, HTTP, HTTPS, console and TACACS+/RADIUS)
- Configuring the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles and advanced WLAN settings

## IP connectivity

- Components of routing table
    - Routing protocol code
    - Prefix
    - Network mask
    - Next hop
    - Administrative distance
    - Metric
    - Gateway of last resort
- Determining how a router makes a forwarding decision by default
    - Longest match
    - Administrative distance
    - Routing protocol metric
- Configuring and verifying IPv4 and IPv6 static routing
    - Default route
    - Network route
    - Host route
    - Floating static
- Configuring and verifying single area OSPFv2
    - Neighbor adjacencies
    - Point-to-point
    - Broadcast (DR/BDR selection)
    - Router ID
- The purpose of first hop redundancy protocol

## IP services

- Configuring and verifying inside source NAT using static and pools

- Configuring and verifying NTP operating in a client and server mode
- Role of DHCP and DNS within the network
- Function of SNMP in network operations
- Use of syslog features including facilities and levels
- Configuring and verifying DHCP client and relay
- Understanding the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping
- Configuring network devices for remote access using SSH
- Capabilities and function of TFTP/FTP in the network

### Security fundamentals

- Key security concepts (threats, vulnerabilities, exploits and mitigation techniques)
- Security program elements (user awareness, training and physical access control)
- Configuring device access control using local passwords
- Security password policies elements: management, complexity and password alternatives (multifactor authentication, certificates and biometrics)
- Remote access and site-to-site VPNs
- Configuring and verifying access control lists
- Configuring Layer 2 security features (DHCP snooping, dynamic ARP inspection and port security)
- Authentication, authorization and accounting
- Wireless security protocols (WPA, WPA2 and WPA3)
- Configuring WLAN using WPA2 PSK using the GUI

### Automation and programmability

- How automation impacts network management
- Traditional networks vs. controller-based networking
- Controller-based and software defined architectures (overlay, underlay and fabric)
    - Separation of control plane and data plane
    - North-bound and south-bound APIs
- Traditional campus device management vs. Cisco DNA Center enabled device management
- Characteristics of REST-based APIs (CRUD, HTTP verbs and data encoding)
- Capabilities of configuration management mechanisms Puppet, Chef and Ansible
- Interpreting JSON encoded data

## Cisco Certified CyberOps Associate (200-201)

### Security concepts

- Describe the CIA triad
- Compare security deployments
    - Network, endpoint and application security systems
    - Agentless and agent-based protections
    - Legacy antivirus and antimalware
    - SIEM, SOAR and log management
- Describe security terms
    - Threat intelligence (TI)
    - Threat hunting
    - Malware analysis
    - Threat actor
    - Run book automation (RBA)
    - Reverse engineering
    - Sliding window anomaly detection
    - Principle of least privilege
    - Zero trust
    - Threat intelligence platform (TIP)
- Compare security concepts
    - Risk (risk scoring/risk weighting, risk reduction, risk assessment)
    - Threat
    - Vulnerability
    - Exploit
- Describe the principles of the

defense-in-depth strategy

- Compare access control models
  - Discretionary access control
  - Mandatory access control
  - Nondiscretionary access control
  - Authentication, authorization, accounting
  - Rule-based access control
  - Time-based access control
  - Role-based access control
- Describe terms as defined in CVSS
  - Attack vector
  - Attack complexity
  - Privileges required
  - User interaction
  - Scope
- Identify the challenges of data visibility (network, host, and cloud) in detection
- Identify potential data loss from provided traffic profiles
- Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs
- Compare rule-based detection vs. behavioral and statistical detection

## Security monitoring

- Compare attack surface and vulnerability
- Identify the types of data provided by these technologies
  - TCP dump
  - NetFlow
  - Next-gen firewall
  - Traditional stateful firewall
  - Application visibility and control
  - Web content filtering
  - Email content filtering
- Describe the impact of these technologies on data visibility
  - Access control list
  - NAT/PAT
  - Tunneling
  - TOR
  - Encryption
  - P2P
  - Encapsulation
  - Load balancing
- Describe the uses of these data types in security monitoring
  - Full packet capture
  - Session data
  - Transaction data
  - Statistical data
  - Metadata
  - Alert data
- Describe network attacks, such as protocolbased, denial of service, distributed denial of service and man-in-the-middle
- Describe web application attacks, such as SQL injection, command injections and crosssite scripting
- Describe social engineering attacks
- Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware and ransomware
- Describe evasion and obfuscation techniques, such as tunneling, encryption and proxies
- Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)
- Identify the certificate components in a given scenario
- Cipher-suite
  - X.509 certificates
  - Key exchange
  - Protocol version
  - PKCS

## Host-based analysis

- Describe the functionality of these endpoint technologies in regard to security monitoring
  - Host-based intrusion detection
  - Antimalware and antivirus
  - Host-based firewall

    - Application-level whitelisting/blacklisting
    - Systems-based sandboxing (such as Chrome, Java, Adobe Reader)
- Identify components of an operating system (such as Windows and Linux) in a given scenario
- Describe the role of attribution in an investigation
    - Assets
    - Threat actor
    - Indicators of compromise
    - Indicators of attack
    - Chain of custody
- Identify type of evidence used based on provided logs
    - Best evidence
    - Corroborative evidence
    - Indirect evidence
- Compare tampered and untampered disk image
- Interpret operating system, application, or command line logs to identify an event
- Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)
    - Hashes
    - URLs
    - Systems, events and networking

## Network intrusion analysis

- UMap the provided events to source technologies
    - IDS/IPS
    - Firewall
    - Network application control
    - Proxy logs
    - Antivirus
    - Transaction data (NetFlow)
- Compare impact and no impact for these items
    - False positive
    - False negative
    - True positive
    - True negative
    - Benign
- Compare deep packet inspection with packet filtering and stateful firewall operation
- Compare inline traffic interrogation and taps or traffic monitoring
- Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic
- Extract files from a TCP stream when given a PCAP file and Wireshark
- Identify key elements in an intrusion from a given PCAP file
    - Source address
    - Destination address
    - Source port
    - Destination port
    - Protocols
    - Payloads
- Interpret the fields in protocol headers as related to intrusion analysis
    - Ethernet frame
    - IPv4
    - IPv6
    - TCP
    - UDP
    - ICMP
    - DNS
    - SMTP/POP3/IMAP
    - HTTP/HTTPS/HTTP2
    - ARP
- Interpret common artifact elements from an event to identify an alert
    - IP address (source / destination)
    - Client and server port identity
    - Process (file or registry)
    - System (API calls)
    - Hashes
    - URI / URL
- Interpret basic regular expressions

## Security policies and procedures

- Describe management concepts
    - Asset management

  - Configuration management
  - Mobile device management
  - Patch management
  - Vulnerability management
- Describe the elements in an incident response plan as stated in NIST.SP800-61
- Apply the incident handling process (such as NIST.SP800-61) to an event
  Map elements to these steps of analysis based on the NIST.SP800-61
  - Preparation
  - Detection and analysis
  - Containment, eradication, and recovery
  - Post-incident analysis (lessons learned)
- Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP800-61)
  - Preparation
  - Detection and analysis
  - Containment, eradication, and recovery
  - Post-incident analysis (lessons learned)
- Describe concepts as documented in NIST.SP800-86
  - Evidence collection order
  - Data integrity
  - Data preservation
  - Volatile data collection
- Identify these elements used for network profiling
  - Total throughput
  - Session duration
  - Ports used
  - Critical asset address space
- Identify these elements used for server profiling
  - Listening ports
  - Logged in users/service accounts
  - Running processes
  - Running tasks
  - Applications
- Identify protected data in a network
  - PII
  - PSI
  - PHI
  - Intellectual property
- Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain
- Model and Diamond Model of Intrusion
- Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

## After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

## About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.