

# ccna

### Course outline

### **Module 1: Network Fundamentals**

Module 1: Network Fundamentals is the first module of the CCNA course. It covers the basics of networking, including the OSI model, TCP/IP, IP addressing, subnetting, routing protocols, and network security. It also introduces the Cisco IOS and how to configure and troubleshoot Cisco routers and switches.

#### Lessons

- Introduction to Networking
- Network Topologies
- Network Protocols
- Network Addressing
- Network Devices
- Network Security
- Network Troubleshooting
- Network Performance Monitoring
- Network Design
- . Network Automation

### After completing this module, students will be able to:

- Understand the fundamentals of networking, including the OSI model, IP addressing, and subnetting.
- Configure, verify, and troubleshoot basic IPv4 and IPv6 networks.
- Describe the purpose and basic operation of the protocols in the OSI and TCP/IP models.
- Identify security threats and mitigation techniques for networks.

# **Module 2: Network Access**

Module 2 of the CCNA course covers the fundamentals of network access, including topics such as network topologies, media types, network devices, and network protocols. It also covers the basics of configuring and troubleshooting network access, including topics such as IP addressing, subnetting, and routing.

### Lessons

• Introduction to Network Access

- Network Topologies
- Network Cabling
- Network Devices
- Network Protocols
- Network Addressing
- Network Security
- Network Troubleshooting
- Network Monitoring
- . Network Performance Optimization

- Understand the fundamentals of networking, including the OSI model, TCP/IP model, and network topologies.
- Configure, verify, and troubleshoot basic IPv4 and IPv6 networks.
- Configure, verify, and troubleshoot basic switching and routing technologies.
- Implement basic network security measures, such as access control lists and port security.

### **Module 3: IP Connectivity**

Module 3 of the CCNA course focuses on IP Connectivity. It covers topics such as IP addressing, subnetting, routing protocols, and network troubleshooting. Students will learn how to configure and troubleshoot IP networks, as well as how to use various tools to monitor and analyze network performance.

### Lessons

- Introduction to IP Connectivity
- Configuring IP Addresses and Subnet Masks
- Understanding Network Address Translation (NAT)
- Configuring Static and Default Routes
- Configuring Dynamic Routing Protocols
- Troubleshooting IP Connectivity
- Configuring DHCP
- Configuring Access Control Lists (ACLs)
- Configuring Network Address Port Translation (NAPT)
- . Configuring Quality of Service (QoS)

### After completing this module, students will be able to:

- Understand the fundamentals of IP addressing and subnetting.
- Configure and troubleshoot basic IPv4 and IPv6 networks.
- Implement and troubleshoot static and dynamic routing protocols.
- Implement and troubleshoot basic network security features.

### Module 4: IP Services

Module 4 of the CCNA course covers IP services, which includes topics such as DHCP, DNS, NAT, and IP addressing. This module provides an in-depth look at how these services are used to configure and manage networks. It also covers troubleshooting techniques for resolving common IP service issues.

#### Lessons

- Introduction to IP Services
- Configuring DHCP
- Configuring DNS
- Configuring NAT
- Configuring Access Control Lists
- Configuring Quality of Service
- Troubleshooting IP Services
- IPv6 Services
- Network Address Translation (NAT)
- . Network Address Port Translation (NAPT)
- . Network Time Protocol (NTP)
- . Dynamic Host Configuration Protocol (DHCP)
- . Domain Name System (DNS)
- . Network Address Translation (NAT)
- . Network Address Port Translation (NAPT)
- . Network Time Protocol (NTP)
- . Dynamic Host Configuration Protocol (DHCP)
- . Domain Name System (DNS)
- . Network Address Translation (NAT)
- . Network Address Port Translation (NAPT)
- . Network Time Protocol (NTP)
- . Dynamic Host Configuration Protocol (DHCP)
- . Domain Name System (DNS)
- . Network Address Translation (NAT)
- . Network Address Port Translation (NAPT)
- . Network Time Protocol (NTP)
- . Dynamic Host Configuration Protocol (DHCP)
- . Domain Name System (DNS)
- . Network Address Translation (NAT)
- . Network Address Port Translation (NAPT)
- . Network Time Protocol (NTP)
- . Dynamic Host Configuration Protocol (DHCP)
- . Domain Name System (DNS)
- . Network Address Translation (NAT)
- . Network Address Port Translation (NAPT)
- . Network Time Protocol (NTP)
- . Dynamic Host Configuration Protocol (DHCP)
- . Domain Name System (DNS)
- . Network Address Translation (NAT)
- . Network Address Port Translation (NAPT)
- . Network Time Protocol (NTP)
- . Dynamic Host Configuration Protocol (DHCP)
- . Domain Name System (DNS)

- . Network Address Translation (NAT)
- . Network Address Port Translation (NAPT)
- . Network Time Protocol (NTP)
- . Configuring Network Address Translation (NAT)
- . Configuring Network Address Port Translation (NAPT)
- . Configuring Network Time Protocol (NTP)
- . Configuring Dynamic Host Configuration Protocol (DHCP)

- Understand the purpose and function of IP services such as DHCP, DNS, NAT, and IPv6.
- Configure and troubleshoot DHCP, DNS, NAT, and IPv6 services.
- Utilize IP services to improve network performance and security.
- Implement IP services in a real-world network environment.

### **Module 5: Security Fundamentals**

Module 5: Security Fundamentals is a module in the CCNA course that covers the fundamentals of network security. It covers topics such as security threats, authentication, encryption, firewalls, and intrusion detection systems. It also covers the implementation of security policies and best practices.

### Lessons

- Introduction to Network Security
- Network Security Protocols
- Firewalls and Access Control Lists
- Network Security Best Practices
- Cryptography Basics
- Authentication and Authorization
- Network Security Threats and Vulnerabilities
- Network Security Monitoring and Auditing
- Network Security Incident Response
- . Network Security Disaster Recovery

### After completing this module, students will be able to:

- Understand the fundamentals of network security, including authentication, authorization, and encryption.
- Identify and mitigate common network security threats, such as malware, phishing, and DDoS attacks.
- Implement security measures such as firewalls, intrusion detection systems, and virtual private networks.
- Configure and manage Cisco security solutions, such as Cisco IOS Firewall, Cisco IOS IPS, and Cisco ASA.

# **Module 6: Routing Fundamentals**

Module 6: Routing Fundamentals is a module in the CCNA course that covers the basics of routing, including the different types of routing protocols, how to configure and troubleshoot routers, and how to use routing protocols to create a secure network. This module also covers topics such as route summarization, route redistribution, and route filtering.

### Lessons

- Introduction to Routing Protocols
- Configuring Static Routes
- Configuring Dynamic Routing Protocols
- Troubleshooting Routing Protocols
- Routing Protocol Authentication
- Routing Protocols in a Multi-Area Network
- Routing Protocols in a Multi-Vendor Network
- Routing Protocols in a Multi-Layer Network
- Routing Protocols in a Multi-Service Network
- . Routing Protocols in a Multi-Domain Network
- . Routing Protocols in a Multi-Path Network
- . Routing Protocols in a Multi-Hop Network
- . Routing Protocols in a Multi-Protocol Network
- . Routing Protocols in a Multi-Platform Network
- . Routing Protocols in a Multi-Media Network
- . Routing Protocols in a Multi-Link Network
- . Routing Protocols in a Multi-Cast Network
- . Routing Protocols in a Multi-Point Network
- . Routing Protocols in a Multi-Access Network
- . Routing Protocols in a Multi-Level Network

### After completing this module, students will be able to:

- Understand the purpose and function of routing protocols
- Configure and troubleshoot static and dynamic routing protocols
- · Utilize routing protocols to optimize network performance
- Implement routing protocols to ensure secure and reliable data transmission

# Module 7: WAN Technologies

Module 7 of the CCNA course covers Wide Area Network (WAN) technologies. It covers topics such as WAN topologies, WAN protocols, WAN services, and WAN security. It also covers the configuration of WAN technologies such as Frame Relay, Point-to-Point Protocol, and Metro Ethernet.

#### Lessons

- Introduction to WAN Technologies
- Types of WAN Connections
- Configuring WAN Connections
- Troubleshooting WAN Connections

- WAN Security
- WAN Optimization
- WAN Protocols
- WAN Network Design
- WAN Network Management
- . WAN Network Monitoring

- Understand the fundamentals of Wide Area Network (WAN) technologies and their applications.
- Configure and troubleshoot Point-to-Point Protocol (PPP) and Frame Relay connections.
- Implement and troubleshoot Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP).
- Utilize WAN technologies such as Metro Ethernet, Virtual Private Networks (VPNs), and Multiprotocol Label Switching (MPLS).

# **Module 8: Infrastructure Services**

Module 8 of the CCNA course covers Infrastructure Services, which includes topics such as network security, virtual private networks, and wireless networking. This module provides an overview of the different types of network security, how to configure and manage virtual private networks, and how to configure and manage wireless networks. Additionally, this module covers topics such as network troubleshooting, network monitoring, and network management.

#### Lessons

- Introduction to Network Infrastructure Services
- Configuring DHCP Services
- Configuring DNS Services
- Configuring NAT Services
- Configuring NTP Services
- Configuring SNMP Services
- Configuring Syslog Services
- Troubleshooting Network Infrastructure Services
- Securing Network Infrastructure Services
- . Implementing Network Access Control

### After completing this module, students will be able to:

- Understand the purpose and function of network infrastructure services such as DNS, DHCP, NAT, and NTP.
- Configure and troubleshoot DHCP services on Cisco routers and switches.
- Configure and troubleshoot NAT services on Cisco routers.
- Configure and troubleshoot NTP services on Cisco routers.

### **Module 9: Infrastructure Maintenance**

Module 9 of the CCNA course covers the fundamentals of infrastructure maintenance. It covers topics such as network monitoring, troubleshooting, and maintenance. It also covers the use of tools such as ping, traceroute, and telnet to diagnose and resolve network issues. Additionally, it covers the basics of network security and how to protect your network from threats.

### Lessons

- Introduction to Infrastructure Maintenance
- Network Troubleshooting
- Network Security
- Network Monitoring
- Network Performance Optimization
- Network Documentation
- Network Backup and Recovery
- Network Configuration Management
- Network Automation
- . Network Capacity Planning
- . Network Disaster Recovery
- . Network Maintenance Best Practices

### After completing this module, students will be able to:

- Understand the basics of network infrastructure maintenance and troubleshooting.
- Identify and resolve common network infrastructure issues.
- Utilize network monitoring and diagnostic tools to identify and resolve network infrastructure issues.
- Implement preventive maintenance procedures to ensure optimal network performance.

# Module 10: Troubleshooting

Module 10 of the CCNA course focuses on troubleshooting. It covers topics such as identifying and resolving network problems, using troubleshooting tools, and understanding the troubleshooting process. It also covers topics such as network performance, security, and troubleshooting protocols.

### Lessons

- Identifying and Resolving Common Network Issues
- Troubleshooting Network Connectivity Problems
- Analyzing Network Performance Issues
- Troubleshooting IP Routing Protocols
- Troubleshooting VLANs and Trunks
- Troubleshooting Spanning Tree Protocol
- Troubleshooting Access Control Lists
- Troubleshooting Network Security
- Troubleshooting Network Services
- . Troubleshooting Network Management Protocols

- Identify and resolve common network issues such as IP address conflicts, routing problems, and slow performance.
- Utilize network troubleshooting tools such as ping, traceroute, and telnet to diagnose network problems.
- Analyze network traffic using packet sniffers and protocol analyzers.
- Configure and troubleshoot network devices such as routers, switches, and firewalls.