

**COMET CISCO CERTIFIED NETWORK ASSOCIATE
(CCNA)
COURSE BROCHURE**

Overview

The **Implementing and Administering Cisco Solutions** (CCNA) v1.0 course gives you a broad range of fundamental knowledge for all IT careers. Through a combination of lecture, hands-on labs, and self-study, you will learn how to install, operate, configure, and verify basic IPv4 and IPv6 networks. The course covers configuring network components such as switches, routers, and wireless LAN controllers; managing network devices; and identifying basic security threats. The course also gives you a foundation in network programmability, automation, and software-defined networking.

This course helps you prepare to take the **200-301 Cisco® Certified Network Associate (CCNA®)** exam. By passing this one exam, you earn CCNA certification. The **200-301 CCNA** exam goes live on February 24, 2020.

Course Objectives

After taking this course, you should be able to:

- Identify the components of a computer network and describe their basic characteristics.
- Understand the model of host-to-host communication.
- Describe the features and functions of the Cisco Internetwork Operating System (IOS®) software.
- Describe LANs and the role of switches within LANs.
- Describe Ethernet as the network access layer of TCP/IP and describe the operation of switches.
- Install a switch and perform the initial configuration.
- Describe the TCP/IP Internet layer, IPv4, its addressing scheme, and subnetting.
- Describe the TCP/IP Transport layer and Application layer.
- Explore functions of routing.
- Implement basic configuration on a Cisco router.
- Explain host-to-host communications across switches and routers.
- Identify and resolve common switched network issues and common problems associated with IPv4 addressing.
- Describe IPv6 main features and addresses, and configure and verify basic IPv6 connectivity.
- Describe the operation, benefits, and limitations of static routing.
- Describe, implement, and verify Virtual Local Area Networks (VLANs) and trunks.
- Describe the application and configuration of inter-VLAN routing.
- Explain the basics of dynamic routing protocols and describe components and terms of Open Shortest Path First (OSPF).
- Explain how Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) work.
- Configure link aggregation using Ether Channel.
- Describe the purpose of Layer 3 redundancy protocols.

- Describe basic WAN and VPN concepts.
- Describe the operation of Access Control Lists (ACLs) and their applications in the network.
- Configure Internet access using Dynamic Host Configuration Protocol (DHCP) clients and explain and configure Network Address Translation (NAT) on Cisco routers.
- Describe basic Quality of Service (QoS) concepts.
- Describe the concepts of wireless networks, which types of wireless networks can be built, and how to use Wireless LAN Controllers (WLCs).
- Describe network and device architectures and introduce virtualization.
- Introduce the concept of network programmability and Software-Defined Networking (SDN) and describe smart network management solutions such as Cisco DNA Center™, Software-Defined Access (SD-Access), and Software-Defined Wide Area Network (SD-WAN).
- Configure basic IOS system monitoring tools.
- Describe the management of Cisco devices.
- Describe the current security threat landscape.
- Describe threat defence technologies.
- Implement a basic security configuration of the device management plane.
- Implement basic steps to harden network devices.

Audience Profile

- This course is designed for anyone seeking CCNA certification. The course also provides foundational knowledge for all support technicians involved in the basic installation, operation, and verification of Cisco networks.

Prerequisites

- Before taking this course, you should have:
- Basic computer literacy.
- Basic PC operating system navigation skills.
- Basic Internet usage skills.
- Basic IP address knowledge.

Network Basics:

- Understand the operation of data networks.
- Know the purpose and functions of network devices such as routers, switches, bridges and hubs.
- Understand how certain applications can impact network performance.
- Know the protocols, purpose and operation of both the OSI and TCP/IP models.
- Be able to choose the most appropriate cables, media, ports and connectors to connect network devices and hosts to a LAN.
- Describe the need for public and private addresses for IPv4.
- Understand IPv6 addresses.
- Describe the appropriate IPv4 addressing scheme for a LAN/WAN environment, including VLSM and summarization.
- Describe the technologies required to run IPv6 and IPv4 concurrently such as dual stack.

LAN SWITCHING

- Understand the media access control method for Ethernet.
- Describe the basic switching concepts and the operation of switches.
- Configure and verify switch configuration including remote access management.
- Verify a network and switch operation using basic utilities such as ping, telnet and SSH.
- Describe VLANs and the need for routing between VLANs.
- Be able to configure and verify VLANs.
- Configure and verify trunking on Cisco switches.
- Understand advanced switching technologies:
- Be able to configure and verify STP, PVSTP and RSTP operation.
- Describe the process of root bridge election.

IP ROUTING

- Understand the basic routing concepts.
- Understand the boot process of a Cisco router.
- Configure and verify a basic router configuration using the command line interface.
- Be able to verify the network connectivity and configuration of a router.
- Configure a static or default route given specific requirements, then verify.
- Manage Cisco IOS files and image(s).
- Understand and distinguish different methods of routing and routing protocols.
- Configure and verify EIGRP in a single autonomous system.
- Configure and verify OSPF (v2 and v3) in a single area.
- Configure and verify BGP
- Configure and verify interVLAN routing using router-on-a-stick.
- Be able to configure SVI interfaces.
- Configure and verify DHCP on a Cisco router.
- Recognize high availability FHRP.

NETWORK DEVICE SECURITY

- Understand the features and applications of each type of ACL.
- Be able to configure and verify ACLs.
- Understand the basic operation of NAT.
- Configure and verify NAT based on a set of network requirements.
- Be able to configure and verify NTP as a client.
- Understand, configure and verify Syslog and utilize Syslog output.
- Be able to configure and verify device security features.
- Understand, configure and verify switch port security features.
- Configure and verify ACLs for filtering network traffic.
- Limit telnet and SSH access to a router by configuring ACLs.

TROUBLESHOOTING/ PRACTICAL SESSION

- Troubleshoot and correct common issues concerning IP addressing and host configurations.
- Be able to utilize netflow and monitor data.
- Troubleshoot and fix spanning tree operation.
- Troubleshoot and resolve routing issues, including OSPF, and EIGRP.
- Troubleshoot and correct VLAN problems.
- Identify and resolve interVLAN problems.
- Troubleshoot and resolve switch trunking issues.
- Troubleshoot and fix ACL problems.
- Troubleshoot and correct layer 1 problems.
- Troubleshoot and correct WAN issues.
- Troubleshoot EtherChannel issues.



Our Students Testimonials

CONTACT US

Mobile : +91 9940068251 / 58251

Mail : ramesh@cometcompuserve.com / ilanchezhian@cometcompuserve.com