CISCO Certified Network Associate

Course outline

Module 1: Network Fundamentals

Module 1: Network Fundamentals for Cisco Certified Network Associate (200-301 CCNA) course provides an introduction to the fundamentals of networking. It covers topics such as network topologies, network devices, IP addressing, routing protocols, and network security. It also provides an overview of the Cisco Certified Network Associate (CCNA) certification and the skills and knowledge required to pass the exam.

Lessons

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

After completing this module, students will be able to:

- 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 security measures, such as access control lists and network segmentation.

Module 2: Network Access

Module 2 of the Cisco Certified Network Associate (200-301 CCNA) course covers the fundamentals of network access, including topics such as network topologies, network devices, and network protocols. It also covers the configuration of network devices, such as routers and switches, and the implementation of network security measures. This module provides a comprehensive overview of the skills and knowledge needed to successfully configure and manage a network.

Lessons

- Introduction to Network Access
- Network Access Control Protocols
- Configuring Access Control Lists
- Troubleshooting Network Access Issues
- Implementing Network Access Security
- Network Access Authentication
- Network Access Authorization
- Network Access Control Lists (ACLs)
- Network Access Control Protocols (NAC)
- . Network Access Control Models
- . Network Access Control Technologies
- . Network Access Control Best Practices
- . Network Access Control Strategies
- . Network Access Control Solutions
- . Network Access Control Design Considerations

After completing this module, students will be able to:

- 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 and troubleshoot basic WAN technologies.

Module 3: IP Connectivity

Module 3 of the Cisco Certified Network Associate (200-301 CCNA) course covers IP Connectivity. This module 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 IPv4 Addressing and Subnetting
- Configuring IPv6 Addressing and Subnetting
- Configuring DHCP
- Troubleshooting IP Connectivity
- Configuring Static and Default Routes
- Configuring RIPv2
- Configuring EIGRP
- Configuring OSPF
- . Configuring NAT
- . Configuring VPNs
- . Troubleshooting IP Routing Protocols

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 DHCP and DNS services in a network.
- Configure and troubleshoot basic network security features such as ACLs and NAT.

Module 4: IP Services

Module 4 of the Cisco Certified Network Associate (200-301 CCNA) course covers IP Services, which includes topics such as IP addressing, subnetting, routing protocols, and network security. This module provides an in-depth look at the fundamentals of IP services and how they are used to configure and manage networks. It also covers advanced topics such as Quality of Service (QoS), Network Address Translation (NAT), and Virtual Private Networks (VPNs).

Lessons

- Introduction to IP Services
- Configuring DHCP
- Configuring DNS
- Configuring NAT
- Configuring Access Control Lists
- Configuring Quality of Service
- Configuring Network Address Translation
- Configuring IP Routing Protocols
- Configuring IP Multicast
- . Troubleshooting IP Services

After completing this module, students will be able to:

- Understand the fundamentals of IP addressing and subnetting.
- Configure and troubleshoot DHCP services.
- Configure and troubleshoot NAT services.
- Implement and troubleshoot IPv6 addressing and routing protocols.

Module 5: Security Fundamentals

Module 5: Security Fundamentals for Cisco Certified Network Associate (200-301 CCNA) course provides an introduction to the fundamentals of network security. It covers topics such as security threats, security policies, authentication, encryption, firewalls, and intrusion detection systems. It also covers the basics of network security, including access control, network segmentation, and secure remote access.

Lessons

- Introduction to Network Security
- Network Security Protocols
- Firewalls and Access Control Lists

- Network Address Translation
- Virtual Private Networks
- Wireless Security
- Network Security Monitoring
- Cryptography
- Security Policies and Best Practices
- . Security Auditing and Compliance

After completing this module, students will be able to:

- Understand the fundamentals of network security, including authentication, authorization, and encryption.
- Implement security protocols such as 802.1X, IPsec, and SSL/TLS.
- Configure and troubleshoot network security devices such as firewalls, intrusion prevention systems, and VPNs.
- Implement secure network access control using ACLs, VLANs, and other technologies.

Module 6: Automation and Programmability

Module 6 of the Cisco Certified Network Associate (200-301 CCNA) course covers Automation and Programmability. This module focuses on the use of automation and programmability to configure, manage, and monitor networks. Topics include the use of APIs, Python scripting, and network programmability. Students will learn how to use these tools to automate network tasks and create custom solutions.

Lessons

- Introduction to Automation and Programmability
- Automation and Programmability Protocols
- Automating Network Configuration with Python
- Automating Network Configuration with Ansible
- Automating Network Configuration with NETCONF/YANG
- Automating Network Configuration with REST APIs
- Automating Network Configuration with EEM
- Automating Network Configuration with NX-OS
- Automating Network Configuration with Cisco DNA Center
- . Automating Network Configuration with Cisco SD-WAN

After completing this module, students will be able to:

- Understand the fundamentals of automation and programmability in Cisco networks.
- Utilize Python scripting to automate network tasks.
- Implement Cisco APIs to automate network tasks.
- Configure and troubleshoot network automation solutions.

Module 7: WAN Technologies

Module 7 of the Cisco Certified Network Associate (200-301 CCNA) course covers Wide Area Network (WAN) technologies. It provides an overview of WAN technologies, including their components, features, and applications. It also covers topics such as WAN topologies, WAN protocols, and WAN security. This module is designed to help students understand the fundamentals of WAN technologies and how to configure and troubleshoot them.

Lessons

- Introduction to WAN Technologies
- WAN Topologies
- Point-to-Point Protocols
- Frame Relay
- Metro Ethernet
- Virtual Private Networks
- Multiprotocol Label Switching
- Quality of Service
- Network Security
- . Troubleshooting WAN Technologies

After completing this module, students will be able to:

- Understand the fundamentals of Wide Area Network (WAN) technologies, including their components, features, and benefits.
- Configure and troubleshoot Point-to-Point Protocol (PPP) and Point-to-Point Protocol over Ethernet (PPPoE) connections.
- Configure and troubleshoot Frame Relay and Multiprotocol Label Switching (MPLS) networks.
- Implement and troubleshoot Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP) services.

Module 8: Troubleshooting

Module 8 of the Cisco Certified Network Associate (200-301 CCNA) course covers troubleshooting techniques for networks. It provides an overview of the troubleshooting process, including identifying the problem, gathering information, isolating the cause, and implementing a solution. It also covers troubleshooting tools and techniques, such as ping, traceroute, and show commands. Finally, it covers troubleshooting of common network issues, such as IP addressing, routing, and switching.

Lessons

- Troubleshooting Network Connectivity Issues
- Troubleshooting VLANs and Trunks
- Troubleshooting Spanning Tree Protocol
- Troubleshooting OSPF and EIGRP
- Troubleshooting Access Control Lists
- Troubleshooting DHCP
- Troubleshooting NAT
- Troubleshooting IPv6
- Troubleshooting Network Security

- . Troubleshooting Network Performance Issues

After completing this module, students will be able to:

- Identify and resolve common network issues such as IP addressing, routing, switching, and wireless connectivity.
- Utilize troubleshooting tools such as ping, traceroute, and show commands to diagnose and resolve network issues.
- Configure and troubleshoot network devices such as routers, switches, and wireless access points.
- Implement best practices for network security and performance optimization.