POINTFUL EDUCATION

Networking

Syllabus

» Course Overview

The Networking course is intended to identify the key components of Networking in today's fast-moving world. From network fundamentals to automation and programming, students will learn the details of network access, IP connectivity and services, and security fundamentals. Through exciting and engaging interactivities, simulations, and projects students will explore firsthand these networking concepts to further their future with preparation for the Cisco Certified Network Associate (CCNA) exam.

» Course Outline by Module

Module 1	Introduction to Networking and Careers	**Module 5**	IP Connectivity
Module 2	Network Components Part I	**Module 6**	IP Services
Module 3	Network Components Part II	**Module 7**	Security Fundamentals
Module 4	Network Access	**Module 8**	Automation and Programmability

» Module Overview and Learning Objectives

Module 1. Construction Documents, Contracts, and Specifications

In this module, students will learn about the basics of networking and its components. They will gain an understanding of the different career paths they can choose in the networking industry, and how a CCNA certification can help them get on the right career track. They will also learn key networking terms that must be familiar with before embarking on this course.

***Learning Objectives*:** In this module, students will:

- Define networking and its components.
- Compare and contrast careers in networking.
- Examine the benefits of having a certification as a Cisco Certified Network Associate (CCNA).
- Examine the format of the Cisco Certified Network Associate (CCNA) exam.
- Explore necessary vocabulary and technical skills for success in this Networking course.

Module 2. Network Components Part I

This module will give you a detailed explanation of the different types of networking components that make up a network. You will learn about the architecture and different topologies of networks. You will also learn more about ethernet and the different types of network interfaces and cables, and the issues associated with them.

***Learning Objectives*:** In this module, students will:

- Explain the role and function of network components including routers, L2 and L3 switches, next-generation firewalls and IPS, access points, controllers, endpoints, and servers.
- Describe characteristics of network topology architectures including 2 tier, 3tier, spine-leaf, WAN, SOHO, on-premises, and cloud.
- Compare physical interface and cabling types including single-mode fiber, multimode fiber, copper, ethernet shared media, point-to-point, and PoE concepts.
- Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed).
- Compare TCP to UDP.

Module 3. Network Components Part II

In this module, students will learn how to configure and verify IPv4 and IPv6 IP addresses. They will learn the difference between the two types of addresses. They will also learn about IP parameters and how they can be verified for different operating systems. Students will learn about key wireless principles and how virtual machines work. Finally, students will learn about various switching concepts and MAC learning.

***Learning Objectives*:** In this module, students will:

- Configure and verify IPv4 addressing and subnetting and describe the need for private IPv4 addressing
- Configure and verify IPv6 addressing and prefix and compare IPv6 address types including global unicast, unique local, link-local, anycast, multicast, and modified EUI 64.
- Verify IP parameters for Client OS (Windows, Mac OS, Linux)
- Describe wireless principles including nonoverlapping WIFI channels, SSID, RF, and encryption and explain virtualization fundamentals (virtual machines)
- Describe switching concepts including MAC learning and aging, frame switching, frame flooding, and MAC address table

Module 4. Network Access

In this module, students will start by learning all about VLANs and Interswitch connectivity. They will learn about layer 2 discovery protocols, EtherChannel and Rapid PVST+. Students will learn about different Cisco wireless architectures. They will also learn all about WLANs, their components, and AP and WLC management. Finally, they will learn about WLAN configuration.

***Learning Objectives*:** In this module, students will:

- Configure and verify VLANs (normal range) spanning multiple switches including access ports (data and voice), default VLAN, and connectivity.
- Configure and verify Interswitch connectivity including trunk ports, 802.1Q, and native VLAN.
- Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
- Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
- Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations including root port, primary and secondary root bridge, other port names, forwarding/blocking port states, and PortFast benefits.
- Compare Cisco Wireless Architectures and AP modes
- Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
- Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)
- Configure 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.

Module 5. IP Connectivity

In this module, students will learn about the various components of a routing table. They will learn how routers take decisions to transmit data using various standards and protocols. Students will also learn how to configure and verify static routing and use OSPFv2 protocols in their configuration. Finally, they will learn about first hop redundancy protocol and its purpose.

Learning Objectives**:** In this module, students will:

- Interpret the components of a routing table including routing protocol code, prefix, network mask, next hop, administrative distance, metric, and gateway of last resort.
- Determine how a router makes a forwarding decision by default including longest match, administrative distance, and routing protocol metric.
- Configure and verify IPv4 and IPv6 static routing including a default route, network route, host route, and floating static.
- Configure and verify single area OSPFv2 including neighbor adjacencies, point-to-point, broadcast (DR/BDR selection), and Router ID.
- Describe the purpose of first hop redundancy protocol.

Module 6. IP Services

In this module, students will learn about NAT and NTP protocols and how they can configure them. They will learn about DHCP and DNS and their importance in modern network operations. Students will learn about the purpose of syslog features. They will also learn about the importance of the quality of service or QoS in a network and how they can configure network devices using SSH so they can be accessed remotely. Finally, students will learn about the importance of TFTP and FTP, the differences between them, and how they both work.

Learning Objectives**:** In this module, students will:

- Configure and verify inside source NAT using static and pools as well as NTP operating in a client and server mode.
- Explain the role of DHCP and DNS within the network and the function of SNMP in network operations.
- Describe the use of Syslog features including facilities and levels as well as configure and verify DHCP client and relay.
- Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping.
- Configure network devices for remote access using SSH and describe the capabilities and function of TFTP/FTP in the network.

Module 7. Security Fundamentals

In this module, students will learn about key security concepts and elements of a security program. Students will also learn how to use passwords to c device access control using password policies. They will also learn about remote access and VPNs and how to configure different layer 2 security features. Finally, students will learn about different wireless security protocols.

***Learning Objectives*:** In this module, students will:

- Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques) and describe security program elements (user awareness, training, and physical access control).
- Configure device access control using local passwords and describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics).
- Describe remote access and site-to-site VPNs and configure and verify access control lists.
- Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security) and differentiate authentication, authorization, and accounting concepts.
- Describe wireless security protocols (WPA, WPA2, and WPA3) and configure WLAN using WPA2 PSK using the GUI.

Module 8. Automation and Programmability

In this module, students will get an introduction to network automation and how controller-based networking is used to manage and automate networks. They will learn about different SDN architectures and understand the different planes and APIs in an SDN system. Students will also learn about the characteristics of REST APIs and different configuration management tools like Ansible, Puppet and Chef. Finally, they will learn about JSON data and how to prepare for the CCNA exam.

Networking

Syllabus

***Learning Objectives*:** In this module, students will:

- Explain how automation impacts network management and compare traditional networks with controller-based networking.
- Describe controller-based and software defined architectures (overlay, underlay, and fabric) including separation of control plane and data plane, north-bound, and southbound APIs and compare traditional campus device management with Cisco DNA Center enabled device management.
- Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding) and recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible.
- Interpret JSON encoded data.
- Prepare for the Cisco Certified Network Associate (CCNA) exam.