CCNA Exploration 4.0

1. Network Fundamentals

The goal of this course is to introduce you to fundamental networking concepts and technologies. These online course materials will assist you in developing the skills necessary to plan and implement small networks across a range of applications. The specific skills covered in each chapter are described at the start of each chapter.
More than just information
This computer-based learning environment is an important part of the overall course experience for students and instructors in the Networking Academy. These online course materials are designed to be used along with several other instructional tools and activities. These include:

- Class presentation, discussion, and practice with your instructor
- Hands-on labs that use networking equipment within the Networking Academy classroom
- Online scored assessments and a matching grade book
- Packet Tracer 4.1 simulation tool
- Additional software for classroom activities

Course Overview

As the course title states, the focus of this course is on learning the fundamentals of networking. In this course, you will learn both the practical and conceptual skills that build the foundation for understanding basic networking. First, you will examine human versus network communication and see the parallels between them. Next, you will be introduced to the two major models used to plan and implement networks: OSI and TCP/IP. You will gain an understanding of the "layered" approach to networks and examine the OSI and TCP/IP layers in detail to understand their functions and services. You will become familiar with the various network devices, network addressing schemes and, finally, the types of media used to carry data across the network.

In this course, you will gain experience using networking utilities and tools, such as Packet Tracer and Wireshark®, to explore networking protocols and concepts. These tools will help you to develop an understanding of how data flows in a network. A special "model Internet" is also used to provide a test environment where a range of network services and data can be observed and analyzed.

Chapter 1 - Chapter 1 presents the basics of communication and how networks have changed our lives. You will be introduced to the concepts of networks, data, local area networks (LANs), wide area networks (WANs), quality of service (QoS), security issues, network collaboration services, and Packet Tracer activities. In the labs, you will learn how to set up a wiki and establish an instant messaging session.

Chapter 2 - Chapter 2 focuses on how networks are modeled and used. You will be introduced to the OSI and TCP/IP models and to the process of data encapsulation. You will learn about the network tool Wireshark®, which is used for analyzing network traffic, and will explore the differences between a real network and a simulated network. In the lab, you will build your first network - a small peer-to-peer network.

Chapter 3 - Using a top-down approach to teaching networking, Chapter 3 introduces you to the top network model layer, the Application layer. In this context, you will explore the interaction of protocols, services, and applications, with a focus on HTTP, DNS, DHCP, SMTP/POP, Telnet and FTP. In the labs, you will practice installing a web server/client and use Wireshark® to analyze network traffic. The Packet Tracer activities let you explore how protocols operate at the Application layer.

Chapter 4 - Chapter 4 introduces the Transport layer and focuses on how the TCP and UDP protocols apply to the common applications. In the labs and activities, you will incorporate the use of Wireshark®, the Windows utilities command netstat, and Packet Tracer to investigate these two protocols.

Chapter 5 - Chapter 5 introduces the OSI Network layer. You will examine concepts of addressing and routing and learn about path determination, data packets, and the IP protocol. By the end of this chapter, you will configure hosts to access the local network and explore routing tables.
Chapter 6 - In Chapter 6, you will focus on network addressing in detail and learn how to use the address mask, or prefix length, to determine the number of subnetworks and hosts in a network. You will also be introduced to ICMP (Internet Control Message Protocol) tools, such as ping and trace.

Chapter 7 - Chapter 7 discusses the services provided by Data Link layer. An emphasis is placed on the encapsulation processes that occur as data travels across the LAN and the WAN.

Chapter 8 - Chapter 8 introduces the Physical layer. You will discover how data sends signals and is encoded for travel across the network. You'll learn about bandwidth and also about the types of media and their associated connectors.

Chapter 9 - In Chapter 9, you will examine the technologies and operation of Ethernet. You will use Wireshark®, Packet Tracer activities, and lab exercises to explore Ethernet.

Chapter 10 - Chapter 10 focuses on designing and cabling a network. You will apply the knowledge and skills developed in the previous chapters to determine the appropriate cables to use, how to connect devices, and develop an addressing and testing scheme.

Chapter 11 - In Chapter 11, you will connect and configure a small network using basic Cisco IOS commands for routers and switches. Upon completion of this final chapter, you will be prepared you to go on to either CCNA Exploration Routing or CCNA Exploration Switching courses.

2. Routing Protocols and Concepts

The goal is to develop an understanding of how a router learns about remote networks and determines the best path to those networks. This course includes both static routing and dynamic routing protocols. The specific skills covered in each chapter are described at the start of each chapter.

More than just information
This computer-based learning environment is an important part of the overall course experience for students and instructors in the Networking Academy. These online course materials are designed to be used along with several other instructional tools and activities. These include:

- Class presentation, discussion, and practice with your instructor
- Hands-on labs that use networking equipment within the Networking Academy classroom
- Online scored assessments and a matching grade book
- Packet Tracer 4.1 simulation tool
- Additional software for classroom activities

Course Overview

The primary focus of this course is on routing and routing protocols. The goal is to develop an understanding of how a router learns about remote networks and determines the best path to those networks. This course includes both static routing and dynamic routing protocols. By examining multiple routing protocols, you will gain a better understanding of each of the individual routing protocols and a better perspective of routing in general. Learning the configuration of routing protocols is fairly simple. Developing an understanding of the routing concepts themselves is more difficult, yet is critical for implementing, verifying, and troubleshooting routing operations.

Each static routing and dynamic routing protocol chapter uses a single topology throughout that chapter. You will be using that topology to configure, verify, and troubleshoot the routing operations discussed in the chapter.

The labs and Packet Tracer activities used in this course are designed to help you develop an understanding of how to configure routing operations while reinforcing the concepts learned in each chapter.

Chapter 1 Introduction to Routing and Packet Forwarding - In Chapter 1, you will be introduced to the router, its role in the networks, its main hardware and software components, and the packet forwarding process. You will also be given an overview of directly connected networks, static routing, and dynamic routing protocols, along with a brief introduction to the routing table. Each of these topics is discussed in more detail in later chapters. Chapter1 also includes a review of basic Cisco IOS commands.

Chapter 2 Static Routing - Chapter 2 focuses on the role and configuration of static routes. The routing table process is introduced, and you will be shown how to verify route entries as they are added and deleted from the routing table. This chapter also discusses Cisco Discovery Protocol, which is a tool that you can use to help verify network operations.

Chapter 3 Introduction to Dynamic Routing Protocols – Chapter 3 provides an overview of routing protocol concepts and the various dynamic routing protocols available for routing in IP networks. In this chapter, you will examine the role of routing protocols. There is an overview of the classification of dynamic routing protocols. This overview is useful for comparing and contrasting the different protocols. Most of the information in this chapter is examined in more detail in later chapters.

Chapter 4 Distance Vector Routing Protocols – Chapter 4 presents two different types of routing protocols: distance vector and link-state. You will examine distance vector concepts and operations, including network discovery, routing table maintenance, and the issue of routing loops. In this chapter, you will also be introduced to the concepts used in RIPv1, RIPv2, and EIGRP routing protocols. These routing protocols are discussed in more detail in later chapters.

Chapter 5 RIP version 1 – Chapter 5 is the first chapter that focuses on a specific dynamic routing protocol. In this chapter, you will learn about RIP (Routing Information Protocol) version 1. RIPv1, a classful, distance vector routing protocol, was one of the first IP routing protocols. You will examine the characteristics, operations, and limitations of RIPv1. You will also learn about RIPv1 configuration, verification, and troubleshooting techniques.

Chapter 6 VLSM and CIDR - Chapter 6 reviews the VLSM (Variable Length Subnet Mask) and CIDR (Classless Inter-Domain Routing) concepts that were presented in the Network Fundamentals course. You will explore the benefits of VLSM along with the role and benefits of CIDR in today's networks. Next, you will be introduced to the role of classless routing protocols. Classless routing protocols RIPv2, EIGRP, and OSPF are examined in later chapters.

Chapter 7 RIPv2 - Chapter 7 examines the next routing protocol presented in this course, RIPv2. RIPv2 is a classless, distance vector routing protocol. You will see how RIPv2 demonstrates the advantages and operations of a classless routing protocol. The chapter begins with a discussion of the limitations of the classful routing protocol, RIPv1. Then RIPv2 is introduced, to show how a classless routing protocol can be used to overcome these limitations. In this chapter, you will also learn the commands necessary to configure and verify RIPv2.

Chapter 8 The Routing Table: A Closer Look – Chapter 8 examines Cisco's IPv4 routing table in detail. The chapter begins with a discussion of the structure of the routing table. While examining the routing table, you will learn about the lookup process, how the routing table process determines the best match with a packet's destination IP address, and how to enter a route in the routing table. The chapter concludes with a discussion about the differences between classful and classless routing behaviors.

Chapter 9 EIGRP – Chapter 9 focuses on Cisco EIGRP (Enhanced Interior Gateway Routing Protocol). EIGRP is a classless, enhanced distance vector routing protocol. You will examine the advantages and operations of EIGRP's DUAL (Diffusing Update Algorithm). Then you will learn about the configuration of EIGRP, including verification and troubleshooting commands.

Chapter 10 Link-State Routing Protocols – Chapter 10 examines link-state routing protocol concepts. You will be introduced to link-state terminology and the link-state routing process. The chapter discusses the benefits and advantages of a link-state routing protocol compared to a distance vector routing protocol. You will then examine the Shortest Path First (SPF) algorithm and how it is used to build a topology map of the network. The link-state routing protocol OSPF is discussed in the following chapter.

Chapter 11 OSPF – The final chapter in this course is an examination of the classless, link-state routing protocol OSPF (Open Shortest Path First). In this chapter, you will examine OSPF operations and configuration, including verification and troubleshooting commands. By the end of this course, you should feel confident in your knowledge of routing and routing protocols. With continued study and practice, you will be able to put your new skills to work.

3. LAN Switching and Wireless

The goal is to develop an understanding of how switches are interconnected and configured to provide network access to LAN users. This course also teaches how to integrate wireless devices into a LAN. The specific skills covered in each chapter are described at the start of each chapter.
More than just information
This computer-based learning environment is an important part of the overall course experience for students and instructors in the Networking Academy. These online course materials are designed to be used along with several other instructional tools and activities. These include:

- Class presentation, discussion, and practice with your instructor
- Hands-on labs that use networking equipment within the Networking Academy classroom
- Online scored assessments and a matching grade book
- Packet Tracer simulation tool
- Additional software for classroom activities

Course Overview

The primary focus of this course is on LAN switching and wireless LANs. The goal is to develop an understanding of how a switch communicates with other switches and routers in a small- or medium-sized business network to implement VLAN segmentation.

This course focuses on Layer 2 switching protocols and concepts used to improve redundancy, propagate VLAN information, and secure the portion of the network where most users access network services.

Switching technologies are relatively straightforward to implement; however, as with routing, the underlying protocols and algorithms are often quite complicated. This course will go to great lengths to explain the underlying processes of the common Layer 2 switching technologies. The better the underlying concepts are understood, the easier it is to implement, verify, and troubleshoot the switching technologies.

Each switching concept will be introduced within the context of a single topology for each chapter. The individual chapter topologies will be used to explain protocol operations as well as providing a setting for the implementation of the various switching technologies.

The labs and Packet Tracer activities used in this course are designed to help you develop an understanding of how to configure switching operations while reinforcing the concepts learned in each chapter.

Chapter 1 LAN Design – In Chapter 1, you learn the fundamental aspects of designing local area networks. In particular, hierarchical network design utilizing the core-distribution-access layer model is introduced and referenced throughout the remainder of the course.

Chapter 2 Basic Switch Concepts and Configuration – Chapter 2 introduces switch forwarding methods, symmetric and asymmetric switching, memory buffering, and Layer 2 and Layer 3 switching. You are introduced to navigating the Cisco IOS CLI on a Catalyst 2960 and performing an initial switch configuration. An integral role of a switch administrator is to maintain a secure network; to this end, you learn to configure various passwords on the switch as well as SSH to mitigate common security attacks.

Chapter 3 VLANs – Chapter 3 presents the types of VLANs used in modern switched networks. It is important to understand the role of the default VLAN, user/data VLANs, native VLANs, the

management VLAN, and voice VLANs. VLAN trunks with IEEE 802.1Q tagging facilitate inter-switch communication with multiple VLANs. You learn to configure, verify, and troubleshoot VLANs and trunks using the Cisco IOS CLI.

Chapter 4 VTP – VTP is used to exchange VLAN information across trunk links, reducing VLAN administration and configuration errors. VTP allows you to create a VLAN once within a VTP domain and have that VLAN propagated to all other switches in the VTP domain. VTP pruning limits the unnecessary propagation of VLAN traffic across a LAN by determining which trunk ports forward which VLAN traffic. You learn to configure, verify, and troubleshoot VTP implementations.

Chapter 5 STP – STP makes it possible to implement redundant physical links in a switched LAN by creating a logical loop-free Layer 2 topology. By default Cisco switches implement STP in a per-VLAN fashion. The configuration of STP is fairly straightforward, but the underlying processes are quite complicated. IEEE 802.1D defined the original implementation of spanning-tree protocol. IEEE 802.1w defined an improved implementation of spanning tree called rapid spanning tree protocol. RSTP convergence time is approximately five times faster than convergence with 802.1D. RSTP introduces several new concepts, such as link types, edge ports, alternate ports, backup ports, and the discarding state. You will learn to configure both the original IEEE 802.1D implementation of STP as well as the newer IEEE 802.1w implementation of spanning tree.

Chapter 6 Inter-VLAN Routing – Inter-VLAN routing is the process of routing traffic between different VLANs. You learn the various methods of inter-VLAN routing. You learn to implement inter-VLAN routing in the router-on-a-stick topology, where a trunk link connects a Layer 2 switch to a router configured with logical subinterfaces paired in a one-to-one fashion with VLANs.

Chapter 7 Basic Wireless Concepts and Configuration – Wireless LAN standards are evolving for voice and video traffic, with newer standards being supported with quality of service. An access point connects to the wired LAN provides a basic service set to client stations that associate to it. SSIDs and MAC filtering are inherently insecure methods of securing a WLAN. Enterprise solutions such as WPA2 and 802.1x authentication enable very secure wireless LAN access. End users have to configure a wireless NIC on their client stations which communicates with and associates to a wireless access point. When configuring a wireless LAN, you should ensure that the devices have the latest firmware so that they can support the most stringent security options.

4. Accessing the WAN

The goal of this course is to introduce you to fundamental networking concepts and technologies. These online course materials will assist you in developing the skills necessary to plan and implement small networks across a range of applications. The specific skills covered in each chapter are described at the start of each chapter.

More than just information
This computer-based learning environment is an important part of the overall course experience for students and instructors in the Networking Academy. These online course materials are designed to be used along with several other instructional tools and activities. These include:

- Class presentation, discussion, and practice with your instructor
- Hands-on labs that use networking equipment within the Networking Academy classroom
- Online scored assessments and a matching grade book
- Packet Tracer 4.1 simulation tool
- Additional software for classroom activities

Course Overview

The primary focus of this course is on accessing wide area networks (WAN). The goal is to develop an understanding of various WAN technologies to connect small- to medium-sized business networks.

The course introduces WAN converged applications and quality of service (QoS). It focuses on WAN technologies including PPP, Frame Relay, and broadband links. WAN security concepts are discussed in detail, including types of threats, how to analyze network vulnerabilities, general methods for mitigating common security threats and types of security appliances and applications. The course then explains the principles of traffic control and access control lists (ACLs) and describes how to implement IP addressing services for an Enterprise network, including how to configure NAT and DHCP. IPv6 addressing concepts are also discussed. During the course, you will learn how to use Cisco Router and Security Device Manager (SDM) to secure a router and implement IP addressing services. Finally, students learn how to detect, troubleshoot and correct common Enterprise network implementation issues.

The labs and Packet Tracer activities used in this course are designed to help you develop an understanding of how to configure routing operations while reinforcing the concepts learned in each chapter.

Chapter 1 Introduction to WANs - In Chapter 1, you will learn the fundamentals enterprise WANs, the technologies available to implement them, and the terminology used to discuss them. You will learn how the Cisco enterprise architecture provides integrated services over an enterprise network and how to select the appropriate WAN technology to meet different enterprise business requirements.

Chapter 2 PPP - Chapter 2 focuses on serial point-to-point communications and the Point-to-Point Protocol (PPP). Understanding how point-to-point communication links function to provide access to a WAN is important to an overall understanding of how WANs function. Various aspects of PPP are discussed including securing PPP using either Password Authentication Protocol (PAP) or the more effective Challenge Handshake Authentication Protocol (CHAP).

Chapter 3 Frame Relay - Chapter 3 focuses on the high-performance Frame Relay WAN protocol. You will learn how to implement Frame Relay for use between LANs over a WAN.

Chapter 4 Network Security - Chapter 4 introduces network security which has moved to the forefront of network management and implementation. The overall security challenge is to find a balance between two important requirements: the need to open networks to support evolving business opportunities, and the need to protect private, personal, and strategic business information. You will learn to identify security threats to enterprise networks and mitigation techniques. You will also learn how to configure basic router security, disable unused resources and interfaces. Finally you will learn to manage configurations and IOS files.

Chapter 5 ACLs - Chapter 5 builds on the concepts introduced in Chapter 4 and focuses on the application of ACLs. One of the most important skills a network administrator needs is mastery of access control lists (ACLs). You will learn how to create firewalls using standard and extended ACLs. Finally, you learn about advanced ACL features including dynamic, reflexive and timed ACLs.

Chapter 6 Teleworker Services - Chapter 6 discusses broadband technologies from a telecommuter's perspective. Specifically, you will learn about cable, DSL, and wireless broadband options. You will also explore how VPNs are utilized to secure broadband connections.

Chapter 7 IP Addressing Services - Chapter 7 discusses how a branch site can provide IP addressing services to users. You will identify teleworker requirements and recommend architectures for providing teleworking services. Specifically, you will learn how to configure a router to be a Dynamic Host Configuration Protocol (DHCP) server and how to integrate private addresses and Network Address Translation (NAT). You will finish with an overview of IPv6 and how to configure routers to exchange IPv6 routes using RIPng.

Chapter 8 Network Troubleshooting - Chapter 8 is the capstone chapter for this course. You will learn how to establish a network baseline and develop network documentation to help in network troubleshooting. You will also develop your network troubleshooting skills by reviewing troubleshooting methodology. You will learn to identify and troubleshoot common enterprise network implementation issues using a layered model approach.