

# CCNA 2: Router and Routing Basics

---

**Cisco Networking Academy Program**  
**Version 3.0**

## Table of Contents

<b>CCNA 2: ROUTER AND ROUTING BASICS .....</b>	<b>1</b>
TARGET AUDIENCE.....	3
PREREQUISITES.....	3
COURSE DESCRIPTION.....	3
COURSE OBJECTIVES.....	3
COURSE OVERVIEW.....	4
COURSE OUTLINE.....	5
<i>Module 1.    WANs and Routers.....</i>	<i>5</i>
<i>Module 2.    Introduction to Router.....</i>	<i>5</i>
<i>Module 3.    Configuring a Router.....</i>	<i>6</i>
<i>Module 4.    Learning about Other Devices.....</i>	<i>7</i>
<i>Module 5.    Managing Cisco IOS.....</i>	<i>7</i>
<i>Module 6.    Routing and Routing Protocols.....</i>	<i>8</i>
<i>Module 7.    Distance Vector Routing Protocols.....</i>	<i>8</i>
<i>Module 8.    TCP/IP Suite Error and Control Messages.....</i>	<i>9</i>
<i>Module 9.    Basic Router Troubleshooting.....</i>	<i>10</i>
<i>Module 10.   Intermediate TCP/IP.....</i>	<i>11</i>
<i>Module 11.   Access Control Lists (ACLs).....</i>	<i>11</i>

## Target Audience

Anyone desires a practical, technical introduction to the field of networking. High-school, community college, and lifelong-learning students interested in careers as network technicians, network engineers, network administrators, and network help-desk staff.

## Prerequisites

- Students should have Reading Age Level (RAL) of 13.
- Successful completion of CCNA 1.
- Prior experience with computer hardware and command line computer interfaces desired but not required.
- Background in computer programming beneficial.

## Course Description

CCNA 2: Routers and Routing Basics is the second of four CCNA courses leading to the Cisco Certified Network Associate (CCNA) designation. CCNA 2 focuses on initial router configuration, Cisco IOS Software management, routing protocol configuration, TCP/IP, and access control lists (ACLs). Students will develop skills on how to configure a router, managing Cisco IOS Software, configuring routing protocol on routers, and set the access lists to control the access to routers.

## Course Objectives

The CCNA certification indicates knowledge of networking for the small-office, home-office (SOHO) market and the ability to work in small businesses or organizations whose networks have fewer than 100 nodes. A CCNA certified individual can:

- Install and configure Cisco switches and routers in multiprotocol internetworks using LAN and WAN interfaces
- Provide Level 1 troubleshooting service
- Improve network performance and security
- Perform entry-level tasks in the planning, design, installation, operation and troubleshooting of Ethernet, TCP/IP Networks.

CCNA 2 is an integral step towards achieving CCNA Certification.

Upon completion of this course, students will be able to perform tasks related to:

- Routers and their role in WANs

- Cisco IOS
- Router Configuration
- Router File Management
- RIP and IGRP Routing Protocols
- TCP/IP Error and Control Messages
- Router Troubleshooting
- Intermediate TCP
- Access Control Lists

## Course Overview

The course has been designed for 70 contact hours. Approximately 35 hours will be designated to lab activities and 35 hours on curriculum content. A case study on structured cabling is required, but format and timing are determined by the Local Academy.

### What has changed from CCNA versions 2.x?

- More emphasis on router configuration early in semester
- More efficient presentation and practice of IOS
- IGRP moved from CCNA 3 to CCNA 2
- Access Lists moved from CCNA 3 to CCNA 2
- Revisions to TCP/IP coverage
- Focus on understanding routing tables
- Case study required; format and timing determined by Local Academy
- More interactive flash activities
- Sequence of > 40 eLabs
- Lab focus on 2-router labs

# Course Outline

## Module 1. WANs and Routers

### Overview

#### 1.1 WANs

- 1.1.1 Introduction to wide-area networks (WANs)
- 1.1.2 WAN devices
- 1.1.3 WAN standards
- 1.1.4 Introduction to routers in a WAN
- 1.1.5 Router functions
- 1.1.6 Academy approach to hands-on labs

#### 1.2 WAN Technologies

- 1.2.1 WAN services
- 1.2.2 Circuit switching
- 1.2.3 Packet switched services
- 1.2.4 Cell switched services
- 1.2.5 Other WAN services

#### 1.3 Routers

- 1.3.1 Router internal components
- 1.3.2 Router physical characteristics
- 1.3.3 Router external connections
- 1.3.4 Management port connections
- 1.3.5 Connecting console interfaces
- 1.3.6 Connecting LAN interfaces
- 1.3.7 Connecting WAN interfaces

### Summary

## Module 2. Introduction to Router

### Overview

#### 2.1 Operating Cisco IOS

- 2.1.1 The purpose of Cisco IOS
- 2.1.2 Router user interface
- 2.1.3 Router user interface modes
- 2.1.4 Cisco IOS features
- 2.1.5 Operation of the Cisco IOS

## 2.2 Starting a Router

- 2.2.1 Initial startup of Cisco routers
- 2.2.2 Router LED indicators
- 2.2.3 Examining the initial bootup output of the router
- 2.2.4 Establishing a HyperTerminal session
- 2.2.5 Logging into the router
- 2.2.6 Keyboard help in the router CLI
- 2.2.7 Enhanced editing commands
- 2.2.8 Router command history
- 2.2.9 Troubleshooting command line errors
- 2.2.10 The show version command

Summary

## **Module 3. Configuring a Router**

Overview

### 3.1 Configuring a Router

- 3.1.1 Command-line interface command modes
- 3.1.2 Configuring name of a router
- 3.1.3 Configuring router passwords
- 3.1.4 Examining the show commands
- 3.1.5 Configuring a serial interface
- 3.1.6 Executing adds, moves, and changes
- 3.1.7 Configuring an Ethernet interface

### 3.2 Finishing the Configuration

- 3.2.1 Importance of configuration standards
- 3.2.2 Interface descriptions
- 3.2.3 Configuring interface descriptions
- 3.2.4 Login banners
- 3.2.5 Configuring message of the day (MOTD)
- 3.2.6 Host name resolutions
- 3.2.7 Configuring host tables
- 3.2.8 Configuration backup and documentation
- 3.2.9 Copying, editing, and pasting configurations

Summary

## **Module 4. Learning about Other Devices**

### Overview

#### 4.1 Discovering and Connecting to Neighbors

- 4.1.1 Introduction to CDP
- 4.1.2 Information obtained with CDP
- 4.1.3 Implementation, monitoring, and maintenance of CDP
- 4.1.4 Creating a network map of the environment
- 4.1.5 Disabling CDP
- 4.1.6 Troubleshooting CDP

#### 4.2 Getting Information about Remote Devices

- 4.2.1 Telnet
- 4.2.2 Establishing and verifying a Telnet connection
- 4.2.3 Disconnecting Telnet operation
- 4.2.4 Advanced Telnet operation
- 4.2.5 Alternate connectivity tests
- 4.2.6 Troubleshooting IP address issues

### Summary

## **Module 5. Managing Cisco IOS**

### Overview

#### 5.1 Router Boot Sequence and Verification

- 5.1.1 Stages of the router power-on boot sequence
- 5.1.2 How a Cisco device locates and loads IOS
- 5.1.3 Using the boot system command
- 5.1.4 Configuration register
- 5.1.5 Troubleshooting IOS boot failure

#### 5.2 Managing the Cisco Router File System

- 5.2.1 IOS file system overview
- 5.2.2 IOS naming conventions
- 5.2.3 Configuration file management using TFTP
- 5.2.4 Configuration file management by using cut and paste
- 5.2.5 Managing IOS images with TFTP
- 5.2.6 Managing IOS images with Xmodem
- 5.2.7 File system verification

## Summary

### **Module 6. Routing and Routing Protocols**

#### Overview

##### 6.1 Overview of Static Routing

- 6.1.1 Introducing routing
- 6.1.2 Static route operation
- 6.1.3 Configuring static routes
- 6.1.4 Configuring default route forwarding
- 6.1.5 Verifying static route configuration
- 6.1.6 Troubleshooting static route configuration

##### 6.2 Dynamic Routing Overview

- 6.2.1 Introduction to routing protocols
- 6.2.2 Autonomous systems
- 6.2.3 Purpose of a routing protocol and autonomous systems
- 6.2.4 Identifying the classes of routing protocols
- 6.2.5 Distance vector routing protocol features and examples
- 6.2.6 Link state routing protocol features and examples
- 6.2.7 Hybrid routing protocol features and examples

##### 6.3 Routing Protocols Overview

- 6.3.1 Route determination
- 6.3.2 Routing configuration
- 6.3.3 Routing protocols (RIP, IGRP, OSPF, EIGRP, BGP)
- 6.3.4 Autonomous systems and IGP versus EGP
- 6.3.5 Distance vector routing
- 6.3.6 Link state routing

#### Summary

### **Module 7. Distance Vector Routing Protocols**

#### Overview

##### 7.1 Distance Vector Routing

- 7.1.1 Distance vector protocol updates
- 7.1.2 Distance vector routing loop issues
- 7.1.3 Defining a maximum count to prevent count to infinity
- 7.1.4 Eliminating routing loops through split horizon



- 7.1.5 Route Poisoning
- 7.1.6 Avoiding routing loops with triggered updates
- 7.1.7 Preventing routing loops with hold-down timers
- 7.2 RIP
  - 7.2.1 RIP process
  - 7.2.2 Configuring RIP
  - 7.2.3 Using the ip classless command
  - 7.2.4 Common RIP configuration issues
  - 7.2.5 Verifying RIP configuration
  - 7.2.6 Troubleshooting RIP update issues
  - 7.2.7 Preventing routing updates through an interface
  - 7.2.8 Load balancing with RIP
  - 7.2.9 Load balancing across multiple paths
  - 7.2.10 Integrating static routes with RIP
- 7.3 IGRP
  - 7.3.1 IGRP features
  - 7.3.2 IGRP metrics
  - 7.3.3 IGRP routes
  - 7.3.4 IGRP stability features
  - 7.3.5 Configuring IGRP
  - 7.3.6 Migrating RIP to IGRP
  - 7.3.7 Verifying IGRP configuration
  - 7.3.8 Troubleshooting IGRP
- Summary

## **Module 8. TCP/IP Suite Error and Control Messages**

### Overview

- 8.1 Overview of TCP/IP Error Message
  - 8.1.1 Internet Control Message Protocol (ICMP)
  - 8.1.2 Error reporting and error correction
  - 8.1.3 ICMP message delivery
  - 8.1.4 Unreachable network
  - 8.1.5 Using PING to test destination reachability
  - 8.1.6 Detecting excessively long routes
  - 8.1.7 Echo message

- 8.1.8 Destination unreachable message
- 8.1.9 Miscellaneous error reporting
- 8.2 Overview of TCP/IP Control Messages
  - 8.2.1 Introduction to control messages
  - 8.2.2 ICMP redirect/change requests
  - 8.2.3 Clock synchronization and transit time estimation
  - 8.2.4 Information requests and reply message formats
  - 8.2.5 Address mask requests
  - 8.2.6 Router discovery message
  - 8.2.7 Router solicitation message
  - 8.2.8 Congestion and flow control messages
- Summary

## **Module 9. Basic Router Troubleshooting**

### Overview

#### 9.1 Examining the Routing Table

- 9.1.1 The show ip route command
- 9.1.2 Determining the gateway of last resort
- 9.1.3 Determining the route source and destination address
- 9.1.4 Determining L2 and L3 addresses from the route source to the route destination
- 9.1.5 Determining the route administrative distance
- 9.1.6 Determining the route metric
- 9.1.7 Determining the route next hop
- 9.1.8 Determining last route update
- 9.1.9 Observe multiple paths to destination

#### 9.2 Network Testing

- 9.2.1 Introduction to network testing
- 9.2.2 Using a structured approach to troubleshooting
- 9.2.3 Testing by OSI layers
- 9.2.4 Layer 1 troubleshooting using indicators
- 9.2.5 Layer 3 troubleshooting using ping
- 9.2.6 Layer 7 troubleshooting using Telnet

#### 9.3 Troubleshooting Router Issues Overview

- 9.3.1 Troubleshooting Layer 1 using show interface
- 9.3.2 Troubleshooting Layer 2 using show interface

- 9.3.3 Troubleshooting using show cdp
- 9.3.4 Troubleshooting using traceroute
- 9.3.5 Troubleshooting routing issues using show ip route and show ip protocol
- 9.3.6 Troubleshooting using show controllers serial
- 9.3.7 Introduction to debug

Summary

## **Module 10. Intermediate TCP/IP**

Overview

### 10.1 TCP Operation

- 10.1.1 TCP operation description
- 10.1.2 Synchronization process (3 way handshake)
- 10.1.3 Denial-of-service attacks
- 10.1.4 Windowing and window size
- 10.1.5 Sequencing numbers
- 10.1.6 Positive ACK
- 10.1.7 UDP operation

### 10.2 Overview of Transport Layer Ports

- 10.2.1 Multiple conversations between hosts
- 10.2.2 Ports for services
- 10.2.3 Ports for clients
- 10.2.4 Port numbering and well known ports
- 10.2.5 Example of multiple sessions between hosts
- 10.2.6 Comparison of MAC addresses, IP addresses, and port numbers

Summary

## **Module 11. Access Control Lists (ACLs)**

Overview

### 11.1 Access Control List Fundamentals

- 11.1.1 What are ACLs
- 11.1.2 How ACLs work
- 11.1.3 Creating ACLs
- 11.1.4 The purpose and function of wildcard mask bits
- 11.1.5 Verifying ACLs

## 11.2 Access Control Lists

11.2.1 Standard ACLs

11.2.2 Extended ACLs

11.2.3 Named ACLs

11.2.4 Placing ACLs

11.2.5 Firewalls

11.2.6 Restricting virtual terminal access

Summary