

## Course Outline for CNT 8004

### CISCO CCNA4 R&S CONNECTING NETWORKS

Effective: Fall 2018

#### I. CATALOG DESCRIPTION:

CNT 8004 — CISCO CCNA4 R&S CONNECTING NETWORKS — 3.00 units

CCNA4 is the final course that may be used to prepare for the Cisco Certified Network Associate (CCNA). CCNA4 discusses the WAN technologies and network services required by converged applications in a complex network. The course enables students to understand the selection criteria of network devices and WAN technologies to meet network requirements. Students learn how to configure and troubleshoot network devices and resolve common issues with data link protocols. By the end of this course, students will be able to configure and troubleshoot routers and switches, and resolve common issues with BGP, ACLs, WAN technologies, SPAN & RSPAN, Netflow, SNMPv1-3, Syslog, and IPSec & virtual private network (VPN) operations in a complex network. In addition, the course will assist the student in developing the skills necessary to plan and implement switching and routing policies. CCNA4 introduces students to intermediate level networking concepts and technologies using a hands-on approach. All work can be done on real current equipment and on virtual simulated equipment. LPC courses emphasize critical thinking, problem solving, collaboration, and the practical application of skills. Prerequisite: CCNA3 Scaling Networks, or permission of the instructor.

2.50 Units Lecture 0.50 Units Lab

#### Prerequisite

CNT 8003 - Cisco CCNA3 Scaling Networks  
with a minimum grade of C  
(May be taken concurrently)

#### Grading Methods:

Letter or P/NP

#### Discipline:

- Computer Service Technology

	<b>MIN</b>
<b>Lecture Hours:</b>	45.00
<b>Lab Hours:</b>	27.00
<b>Total Hours:</b>	72.00

#### II. NUMBER OF TIMES COURSE MAY BE TAKEN FOR CREDIT: 1

#### III. PREREQUISITE AND/OR ADVISORY SKILLS:

**Before entering the course a student should be able to:**

##### A. CNT8003

1. Configure and troubleshoot enhanced switching technologies such as VLANs, Rapid Spanning Tree Protocol (RSTP), Per VLAN Spanning Tree Plus Protocol (PVST+), and EtherChannel
2. Configure and troubleshoot first hop redundancy protocols (HSRP) in a switched network
3. Configure and troubleshoot wireless routers and wireless clients
4. Configure and troubleshoot routers in a complex routed IPv4 or IPv6 network using single-area OSPF, multiarea OSPF, and Enhanced Interior Gateway Routing Protocol (EIGRP)
5. Manage Cisco IOS® Software licensing and configuration files

#### IV. MEASURABLE OBJECTIVES:

**Upon completion of this course, the student should be able to:**

- A. Describe the operations and benefits of virtual private networks (VPNs), multipoint virtual private network (DMVPN), and tunneling;
- B. Learn the practical use of switched port analyzer (SPAN)
- C. Explore many aspects of QoS
- D. Investigate and repair issues with IPv6 ACLs
- E. Implement Point-To-Point Protocol over Ethernet (PPPoE)
- F. Learn and describe Border Gateway Protocol (BGP)
- G. Configure and troubleshoot serial connections, broadband connections, tunneling operations, Network Address Translation (NAT) operations
- H. Monitor and troubleshoot network operations using syslog, SNMPv1 – v3, and NetFlow
- I. Describe network architectures: Borderless networks, Data centers and virtualization, Collaboration technology and solutions, and

## V. CONTENT:

- A. Hierarchical Network Design
  - 1. Explain the structured engineering principles for network design: Hierarchy
  - 2. Modularity, Resiliency, Flexibility
  - 3. Describe the three layers of a hierarchical network and how they are used in network design
  - 4. Describe the Cisco Enterprise Architecture Model.Connecting to the WAN
- B. Connecting to the WAN
  - 1. Describe the purpose of a Wide Area Network (WAN) and how it relates to the OSI model
  - 2. Describe WAN operations and the services available
  - 3. Compare various private/public WAN technologies
  - 4. Select the appropriate WAN protocol and service for a specific network requirement
- C. Point-to-Point Connections
  - 1. Explain the fundamentals of point-to-point serial communication across a WAN
  - 2. Explore Time Division Multiplexing (TDM)
  - 3. Configure High-Level Data Link Control (HDLC) encapsulation on a point-to-point serial link
  - 4. Describe the benefits of using Point-to-Point Protocol (PPP) compared to HDLC in a WAN
  - 5. Define the working layers of PP with respect to: Link Control Protocol (LCP) and Network Control Protocol (NCP)
  - 6. Explain how a PPP session is established
  - 7. Use CLI to configure PPP encapsulation, use authentication on a point-to-point serial link and troubleshoot PPP
- D. Frame Relay
  - 1. Describe the fundamental concepts of Frame Relay technology, including operation, implementation requirements, maps, and Local Management Interface (LMI) operation
  - 2. se CLI to configure a basic Frame Relay permanent virtual circuit (PVC), including configuring and troubleshooting Frame Relay on a router serial interface and configuring a static Frame Relay map
- E. Network Address Translation for IPv4
  - 1. Describe NAT characteristics and the benefits and drawbacks of NAT
  - 2. Define NAT terminology
  - 3. Use CLI to configure, verify and troubleshoot: static NAT, dynamic NAT and NAT-PT
  - 4. Configure port forwarding using the CLI
  - 5. Explore NAT for IPv6 or "NAT-64"
- F. Broadband Solutions
  - 1. Explore teleworking and how it affects networks and business operations
  - 2. Determine how to select broadband solutions to support remote connectivity in a small-to-medium-sized business network
  - 3. Describe a cable system and cable broadband access
  - 4. Describe a DSL system and DSL broadband access
  - 5. Describe broadband wireless options
  - 6. Explore PPP-over-Ethernet "PPPoE"
  - 7. Use CLI to configure and verify PPPoE
- G. Securing Site-to-Site Connectivity
  - 1. Describe benefits of Virtual Private Networks (VPN) technology and describe the types of VPNs available
  - 2. Explore the purpose and benefits of Generic Routing Encapsulation (GRE) tunnels
  - 3. Configure a site-to-site GRE tunnel
  - 4. Describe the characteristics of authentication and encryption using IPsec
  - 5. Compare IPsec and SSL remote access VPNs
- H. Monitoring the Network
  - 1. Explain Syslog operation in a small-to-medium-sized business network
  - 2. Configure Syslog to compile messages on a small-to-medium-sized business network management device
  - 3. Configure Simple Network Management Protocol (SNMP) to compile messages on a small-to-medium-sized business network
  - 4. Describe Cisco's monitoring tool "NetFlow" and how it's used in a small-to-medium-sized business network
  - 5. Configure NetFlow data export on a router
  - 6. Examine sample NetFlow data to determine traffic pattern
- I. Troubleshooting the Network
  - 1. Explain how network documentation is developed and used to troubleshoot network issues
  - 2. Describe the general troubleshooting process
  - 3. Compare troubleshooting methods that use a systematic, layered approach
  - 4. Describe troubleshooting tools used to gather and analyze symptoms of network problems
  - 5. Determine the symptoms and causes of network problems using a layered model
  - 6. Troubleshoot a network using the layered model
- J. CCNv6 Bridging Material
  - 1. Explore Dynamic Multipoint VPN "DMVPN", which builds on a student's knowledge of IPsec and GRE
  - 2. Explore Boarder Gateway Protocol (BGP) and how it differs from other dynamic routing protocols
  - 3. Learn how to configure and test IPv6 ACLs
  - 4. Describe detailed security best practices for LANs
  - 5. Learn how SNMPv3 operates and how to configure it
  - 6. Explore port and traffic flow monitoring by use of Switched Port Analyzer (SPAN)
  - 7. Learn how cloud services are deployed
  - 8. Explore various quality of service (QoS) methods

## VI. METHODS OF INSTRUCTION:

- A. **Demonstration** -
- B. **Lab** -
- C. **Discussion** -
- D. **Lecture** -

## VII. TYPICAL ASSIGNMENTS:

- A. Using the network simulator, configure each router with a Banner MOTD, Console Password & VTY Passwords (cisco), Enable

- Secret Password (class), and IP Domain (DNS) Server. Configure other interfaces with IP addresses as necessary. PPP- Configure a 128-Kbps PPP link from Phoenix to Bango with CHAP authentication; password = Cisco123ork.
- B. Configure the Phoenix router to be the DHCP server for the BANGOR-LAN-1 and BANGOR-WIRELESS using the address ranges specified in the diagram. For pool BANGOR-LAN-1 dynamically assign addresses from 128 to 255. For pool BANGOR-WIRELESS exclude addresses 0 thru 3. Have helper addresses point to the Phoenix Loopback-7 interface.

#### VIII. EVALUATION:

##### A. **Methods**

1. Exams/Tests
2. Quizzes
3. Home Work
4. Lab Activities

##### B. **Frequency**

1. One mid-term and one final examination will be administered.
2. Weekly quizzes
3. Weekly home work
4. Weekly labs

#### IX. TYPICAL TEXTS:

1. Cisco Networking Academy . *Connecting Networks Companion Guide Lab Manual*. 1st ed., Cisco Press, 2017.
2. Cisco Networking Academy. *Connecting Networks Companion Guide v6*. 1st ed., Cisco Press, 2017.
3. Cisco Networking Academy . *Connecting Networks Companion Guide v6 Labs & Study Guide*. 1st ed., Cisco Press, 2017.
4. Cisco Networking Academy on-line curriculum.

#### X. OTHER MATERIALS REQUIRED OF STUDENTS: