Miami Dade College

Course Description

CTS2653 | CCNA 4: Connecting Networks |4.00 credits

This is the fourth and final course of the four-course Cisco curriculum that will prepare the student for certification as a Cisco Certified Network Associate (CCNA). Students will learn how to implement a hierarchical network design, configure wide area networks (WANs), including point-to-point and frame relay connections, implement IP addressing services such as Network Address Translation, VPN and broadband solutions, monitoring and troubleshooting enterprise networks. Prerequisite: CTS2652.

Course Competencies:

Competency 1: The student will demonstrate an understanding of designing and connecting networks by:

1. Describing the hierarchical network design model, including the Cisco Enterprise Architecture and other evolving network architectures
2. Describing the features and operation of borderless networks, data centers and virtualization, and collaboration technology
3. Researching and recommending architecture for a given enterprise network requirement

Competency 2: The student will demonstrate an understanding of wide area networks (WAN) by:

1. Identifying various wide area network (WAN) technologies and architectures currently in use and identifying their features, advantages and disadvantages
2. Explaining how WAN services are provided and what infrastructure is required for connections to an Internet Service Provider (ISP) and mobile users
3. Electing a WAN technology solution to fulfill a given requirement

Competency 3: The student will demonstrate an understanding of Point-to-Point connections by:

1. Describing the features and operation of circuit-switched and leased line serial communications
2. Explaining the features and operation of Point-to-Point Protocol (PPP), including establishment of data link and network sessions
3. Identifying the different types of PPP technologies, encapsulation types and frame formats
4. Configuring a router for PPP operations, including options such as authentication, link quality, compression and multilink
5. Verifying, monitoring and troubleshooting PPP connectivity

Competency 4: The student will demonstrate an understanding of Frame-Relay Connections by:

1. Describing the features and operation of packet-switched serial communications
2. Explaining the features and operation of Frame-Relay, including network topologies, data link connection identifier (DLCI), switched and permanent virtual circuits, address mapping, flow control and bursting, and Local Management Interface (LMI)
3. Configuring a router for Frame-Relay operations, including static mapping, addressing, sub interfaces, LMI messaging and Frame-Relay type
4. Verifying, monitoring and troubleshooting Frame-Relay operations

Competency 5: The student will demonstrate an understanding of Network Addressing Translation by:

1. Describing the purpose, features and operation of Network Address Translation (NAT) and Port Address Translation (PAT) for private networks
2. Explaining how Cisco devices perform NAT functions, including port forwarding, and how NAT issues can be avoided
3. Calculating and mapping IP Addresses and subnet masks for NAT operation
4. Configuring, verifying, and troubleshooting NAT on a router, including static translation, use of IP Address pools, and sharing a public IP address on a router interface
5. Designing, implementing and troubleshooting NAT for a given private network

Competency 6: The student will demonstrate an understanding of broadband solutions by:

1. Describing the benefits and categories of Teleworking
2. Comparing various broadband solutions, including Digital Subscription Lines (DSL), Cable Modem, satellite communications, WiMAX, LTE and cellular data
3. Describing the features and operation of the various DSL technologies
4. Configuring a PPP over Ethernet client for DSL connectivity

Competency 7: The student will demonstrate an understanding of remote access by:

1. Identifying and describing Internet protocols that permit the remote access of enterprise networks
2. Describing the features and operation of virtual private networks (VPNs), IPSec, and tunneling within the public Internet
3. Configuring, implementing and troubleshooting IPSec and GRE tunnels on routers
4. Stablishing, securing and testing site-to- site connectivity

Competency 8: The student will demonstrate an understanding of network maintenance, support and troubleshooting by:

1. Describing the requirements of maintaining a robust and fault tolerant Network
2. Describing the current hardware and software solutions and protocols used for maintaining and monitoring enterprise networks, including Syslog, Simple Network Management Protocol (SNMP), and NetFlow
3. Describing the features and operation of Syslog, including its protocols, message format, client and server functions, severity levels, security auditing, log analysis, and debugging
4. Configuring, securing and troubleshooting Syslog clients and servers
5. Describing the features and operation of SNMP in network management systems to monitor devices for conditions that require administrative attention
6. Configuring network devices to send SNMP traps and alerts to network management systems
7. Describing the features and operation of NetFlow for collecting IP traffic statistics in a network
8. Configuring and troubleshooting NetFlow on Cisco routers to collect IP traffic statistics and export NetFlow records to a NetFlow server
9. Monitoring network operations and reviewing event logs from Syslog, SNMP, and NetFlow
10. Optimizing traffic flow conditions on network connections based on analysis of traffic types, characteristics and end user needs

Competency 9: The student will demonstrate an understanding of troubleshooting network issues by:

1. Describing network troubleshooting methodologies using a systematic approach
2. identifying the symptoms and causes of network problems
3. identifying network troubleshooting tools and their use
4. performing testing and monitoring of operational network devices
5. reviewing and interpreting error messages
6. documenting a network topology and performing backups of IOS and configuration files
7. troubleshooting a given network topology exhibiting common network issues

Competency 10: The student will demonstrate an understanding of network security by:

1. Identifying network security threats and explaining how to mitigate common threats to network devices and hosts
2. Escribing the functions of common security technologies and applications
3. Implementing recommended security practices to secure network devices
4. Testing a network topology for security and access control

Learning Outcomes:

- Use quantitative analytical skills to evaluate and process numerical data
- Solve problems using critical and creative thinking and scientific reasoning
- Use computer and emerging technologies effectively