EET-2313: CISCO III

Cuyahoga Community College

Viewing: EET-2313 : Cisco III

Board of Trustees:
November 2020

Academic Term:
Fall 2021

Subject Code
EET - Electrical/Electronic Engineer

Course Number:
2313

Title:
Cisco III

Catalog Description:
Covers the architecture, components, operations, and security to scale for large, complex networks, including wide area network (WAN) technologies. Emphasis on network security concepts and network virtualization and automation.

Credit Hour(s):
3

Lecture Hour(s):
2

Lab Hour(s):
2

Requisites

Prerequisite and Corequisite
EET-2303 Cisco II.

Outcomes

Course Outcome(s):
Configure, troubleshoot, and secure enterprise network devices and explain how application programming interfaces (API) and configuration management tools enable network automation.

Essential Learning Outcome Mapping:
Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):
1. Configure single-area Open Shortest Path First version 2 (OSPFv2) in both point-to-point and multi-access networks.
2. Explain how to mitigate threats and enhance network security using access control lists (ACLs) and security best practices.
3. Implement standard Internet Protocol version4 (IPv4) ACLs to filter traffic and secure administrative access.
4. Configure Network Address Translation (NAT) services on the edge router to provide IPv4 address scalability.
5. Explain techniques to provide address scalability and secure remote access for Wide Area Networks (WANs).
6. Explain how to optimize, monitor, and troubleshoot scalable network architectures.
7. Explain how networking devices implement Quality of Service (QoS).
8. Implement protocols to manage the network.
9. Explain how technologies such as virtualization, software-defined networking, and automation affect evolving networks.

Methods of Evaluation:

Evaluation can include any combination of the following:

1. Assignments
2. Quizzes
3. Exams
4. Lab Assignments
5. Projects
6. Reports
7. Oral Evaluations

Course Content Outline:

1. Single-Area OSPF Concepts
   - A. OSPF features and characteristics
   - B. OSPF packet types used in single-area OSPF
   - C. Single-area OSPF operation
2. Single-Area OSPFv2 Configuration
   - A. OSPFv2 router ID
   - B. OSPFv2 in a point-to-point network
   - C. OSPF interface priority
   - D. Modifications to the operation of single-area OSPFv2
   - E. Default route propagation
   - F. Single-area OSPFv2 implementation
3. Network Security Concepts
   - A. State of cybersecurity and vectors of data loss
   - B. Tools used by threat actors to exploit networks
   - C. Malware types
   - D. Common network attacks
   - E. Internet Protocol (IP) vulnerabilities
   - F. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) vulnerabilities
   - G. IP service exploits
   - H. Best practices for protecting a network
   - I. Cryptographic processes used to protect data in transit
4. ACL Concepts
   - A. Traffic Filtering
   - B. Wildcard masks
   - C. ACL creation
   - D. Standard and extended IPv4 ACLs
5. ACLs for IPv4 Configuration
   - A. Standard IPv4 ACLs
   - B. Sequence numbers to edit existing standard IPv4 ACLs
   - C. Configure a standard ACL to secure Virtual Teletype (VTY) access
   - D. Extended IPv4 ACLs to filter traffic according to networking requirements
6. NAT for IPv4
   - A. Purpose and function of NAT
   - B. Types of NAT
   - C. NAT Advantages and Disadvantages
   - D. Static NAT
   - E. Dynamic NAT
   - F. Port Address Translation (PAT)
   - G. NAT64
7. WAN Concepts
   - A. Purpose of WANs
   - B. WAN Operations

C. Traditional WAN Connectivity
D. Modern WAN Connectivity
E. Internet-Based Connectivity

8. Virtual Private Network (VPN) and Internet Protocol Security (IPsec) Concepts
   A. VPN Technology
   B. Types of VPNs
   C. IPsec
9. QoS Concepts
   A. Network Transmission Quality
   B. Traffic Characteristics
   C. Queuing Algorithms
   D. QoS Models
   E. QoS Implementation Techniques
10. Network Management
   A. Device Discovery with Cisco Discovery Protocol (CDP)
   B. Device Discovery with Link Layer Discovery Protocol (LLDP)
   C. Network Time Protocol (NTP)
   D. Simple Network Management Protocol (SNMP)
   E. System logging Protocol
   F. Router and Switch File Maintenance
   G. Internet Operating System (IOS) Image Management
11. Network Design
   A. Hierarchical Networks
   B. Scalable Networks
   C. Switch Hardware
   D. Router Hardware
12. Network Troubleshooting
   A. Network Documentation
   B. Troubleshooting Process
   C. Troubleshooting Tools
   D. Symptoms and Causes of Network Problems
   E. Troubleshooting IP Connectivity
13. Network Virtualization
   A. Cloud Computing
   B. Virtualization
   C. Virtual Network Infrastructure
   D. Software-Defined Networking
   E. Controllers
14. Network Automation
   A. Automation Overview
   B. Data Formats
   C. Application Programming Interfaces (APIs)
   D. Representational State Transfer (REST)
   E. Configuration Management
   F. Intent Based Networking (IBN) and Cisco Digital Network Architecture (DNA) Center

Resources

Cisco Press. (2020) *Enterprise networking, security, and automation v7.*, Indianapolis: Cisco Press.

Cisco Press. (2020) *Introduction to networks v7*, Indianapolis: Cisco Press.

Cisco Press. (2020) *Switching, routing, and wireless essentials v7*, Indianapolis: Cisco Press.

Top of page
Key: 4855