NOVA COLLEGE-WIDE COURSE CONTENT SUMMARY
ITN 156 – ENTERPRISE NETWORKING, SECURITY, AND AUTOMATION - CISCO (4 CR.)

Course Description

Provides instruction in the fundamentals of networking environments, the basics of router operations, and basic router and switch configuration. Lecture 3 hours. Laboratory 2 hours. Total 5 hours per week.

General Course Purpose

The third course in the CCNAv7 curriculum describes the architectures and considerations related to designing, securing, operating, and troubleshooting enterprise networks. This course covers wide area network (WAN) technologies and quality of service (QoS) mechanisms used for secure remote access. ENSA also introduces software-defined networking, virtualization, and automation concepts that support the digitalization of networks. Students gain skills to configure and troubleshoot enterprise networks, and learn to identify and protect against cybersecurity threats. They are introduced to network management tools and learn key concepts of software-defined networking, including controller-based architectures and how application programming interfaces (APIs) enable network automation.

Course Prerequisites/Corequisites

Prerequisites: ITN 155

Course Objectives

Upon completing the course, the student will be able to:

- Configure single-area OSPFv2 in both point-to-point and multiaccess networks.
- Explain how to mitigate threats and enhance network security using access control lists and security best practices.
- Implement standard IPv4 ACLs to filter traffic and secure administrative access.
- Configure NAT services on the edge router to provide IPv4 address scalability.
- Explain techniques to provide address scalability and secure remote access for WANs.
- Explain how to optimize, monitor, and troubleshoot scalable network architectures.
- Explain how networking devices implement QoS.
- Implement protocols to manage the network.
- Explain how technologies such as virtualization, software defined networking, and automation affect evolving networks.

Major Topics to be Included

- OSPF
- Network Security and ACL Concepts
- NAT for IPv4
- WAN Concepts
- VPN and IPSec Concepts
- QoS Concepts
- Network Design

- Network Management and Troubleshooting
- Network Virtualization and Automation

Student Learning Outcomes

OSPF v2 Concepts
- Describe basic OSPF features and characteristics.
- Describe the OSPF packet types used in single-area
- Explain how single-area OSPF operates

OSPF v2 Configuration
- Configure an OSPFv2 router ID
- Configure single-area OSPFv2 in a point-to-point network.
- Configure the OSPF interface priority to influence the DR/BDR election in a multiaccess network.
- Implement modifications to change the operation of singlearea OSPFv2.
- Configure OSPF to propagate a default route

Network Security
- Describe the current state of cybersecurity and vectors of data loss.
- Describe the threat actors who exploit networks
- Describe malware types and common network attacks
- Explain how IP , TCP and UDP vulnerabilities are exploited by threat actors
- Describe common cryptographic processes used to protect data in transit
- Describe best practices for protecting a network

Access Control List Concepts
- Explain how ACLs are used as part of a network security policy
- Configure standard IPv4 ACLs to filter traffic to meet networking requirements.
- Use sequence numbers to edit existing standard IPv4 ACLs.
- Configure a standard ACL to secure vty access.
- Configure extended IPv4 ACLs to filter traffic according to networking requirements

NAT for IPv4
- Configure NAT services on the edge router to provide IPv4 address scalability.
- Explain the operation of different types of NAT
- Configure static NAT using the CLI.
- Configure dynamic NAT using the CLI
- Configure PAT using the CLI.
- Describe NAT for IPv6

WAN
- Explain the purpose of a WAN.
- Explain how WANs operate.
- Compare traditional and modern WAN connectivity options.
- Compare internet-based WAN connectivity options.

VPN and IPsec Concepts
- Explain how VPNs and IPsec secure site-to-site and remote access connectivity
- Describe benefits of VPN technology.
- Describe different types of VPNs
- Explain how the IPsec framework is used to secure network traffic

QOS Concepts
- Explain how network transmission characteristics impact quality.
- Describe minimum network requirements for voice, video, and data traffic

- Describe the queuing algorithms used by networking devices.
- Describe the different QoS models

Network Design
- Explain the characteristics of scalable network architectures.
- Hierarchical Networks: Explain how data, voice, and video are converged in a switched network.
- Explain considerations for designing a scalable network.
- Explain how switch hardware features support network requirements.
- Describe the types of routers available for small to-mediumsized business networks.

Network Management
- Use CDP to map a network topology.
- Use LLDP to map a network topology.
- Implement NTP between an NTP client and NTP server.
- Explain SNMP operation.
- Explain syslog operation.
- Use commands to back up and restore an IOS configuration file.
- Perform an upgrade of an IOS system image.

Network Troubleshooting
- Explain how network documentation is developed and used to troubleshoot network
- Compare troubleshooting methods that use a systematic, layered approach
- Describe different networking troubleshooting tools
- Troubleshoot a network using the layered model.

Network Virtualization and Automation
- Cloud Computing : Explain the importance of cloud computing.
- Virtualization : Explain the importance of virtualization.
- Virtual Network Infrastructure: Describe the virtualization of network devices and services.
- Software-Defined Networking : Describe software-defined networking. Controllers Describe controllers used in network programming
- Automation Overview - Describe automation.
- Data Formats: Compare JSON, YAML, and XML data formats.
- APIs: Explain how APIs enable computer to computer communications.
- REST : Explain how REST enables computer to computer communications.
- Compare the configuration management tools Puppet, Chef, Ansible, and SaltStack
- Explain how Cisco DNA center enables intent-based networking

Required Time Allocation per Topic

In order to standardize the core topics of ITN 156, the following student contact hours per topic are required. Each syllabus should be created to adhere as closely as possible to these allocations. Of course, the topics cannot be followed sequentially. Many topics are taught best if it reflects the current android version. There are normally 60 student contact-hours per semester for a four credit course. (This includes 15 weeks of instruction and does not include the final exam week so 15* 4 = 60 hours. Sections of the course that are given in alternative formats from the standard 16 week section still meet for the same number of contact hours.) The final exam time is not included in the time table. The changes in Android Development are happening so fast that some of the content easily could be less significant soon. So it is really important to include the changes in syllabus. Also, additional topic/ Optional Content, leaves ample time for an instructor to tailor the course to special needs or resources.

Topic	Hours	Percentage
OSPF	6	10%
Network Security and ACLs	6	10%
NAT for IPv4	6	10%
WAN Concepts	10	16%
VPN and IPsec	8	14%
QOS	8	14%
Network Design, Management and T-shooting	10	16%
Network Virtualization and Automation	6	10%
Total	60	100%