Virginia Western Community College
ITN 156
Basic Switching and Routing - Cisco

Prerequisites
ITN 155

Course Description
Centers instruction in LAN segmentation using bridges, routers, and switches. Includes fast Ethernet, access lists, routing protocols, spanning tree protocol, virtual LANS and network management.

Semester Credits: 4 Lecture Hours: 4 Lab/Clinical/Internship Hours: 0

Required Materials

Textbook:
All reading material is located on netacad.com

Other Required Materials:
Packet Tracer Software (available from the class website)

Course Outcomes

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

- Explain how single-area OSPF operates in both point-to-point and broadcast multiaccess networks.
- Implement single-area OSPFv2 in both point-to-point and broadcast multiaccess networks.
- Explain how vulnerabilities, threats, and exploits can be mitigated to enhance network security.
- Explain how ACLs are used as part of a network security policy.
- Implement IPv4 ACLs to filter traffic and secure administrative access.
- Configure NAT services on the edge router to provide IPv4 address scalability.
- Explain how WAN access technologies can be used to satisfy business requirements.
- Explain how VPNs and IPsec secure site-to-site and remote access connectivity.
- Explain how networking devices implement QoS.
- Implement protocols to manage the network.
- Explain the characteristics of scalable network architectures.
- Troubleshoot enterprise networks.
- Explain the purpose and characteristics of network virtualization.

- Explain how network automation is enabled through RESTful APIs and configuration management tools.

Topical Description

CCNAv7: ENSA		
Module	**Topic**	**Objective**
Single-Area OSPFv2 Concepts		Explain how single-area OSPF operates in both point-to-point and broadcast multiaccess networks.
	OSPF Features and Characteristics	Describe basic OSPF features and characteristics.
	OSPF Packets	Describe the OSPF packet types used in single-area OSPF.
	OSPF Operation	Explain how single-area OSPF operates.
Module	**Topic**	**Objective**
Single-Area OSPFv2 Configuration		Implement single-area OSPFv2 in both point-to-point and broadcast multiaccess networks.
	OSPF Router ID	Configure an OSPFv2 router ID.
	Point-to-Point OSPF Networks	Configure single-area OSPFv2 in a point-to-point network.
	Multiaccess OSPF Networks	Configure the OSPF interface priority to influence the DR/BDR election in a multiaccess network.
	Modify Single-Area OSPFv2	Implement modifications to change the operation of single area OSPFv2.
	Default Route Propagation	Configure OSPF to propagate a default route.
	Verify Single-Area OSPFv2	Verify a single-area OSPFv2 implementation.
Module	**Topic**	**Objective**
Network Security Concepts		Explain how vulnerabilities, threats, and exploits can be mitigated to enhance network security.
	Current State of Cybersecurity	Describe the current state of cybersecurity and vectors of data loss.
	Threat Actors	Describe the threat actors who exploit networks.

	Threat Actor Tools	Describe tools used by threat actors to exploit networks.
	Malware	Describe malware types.
	Common Network Attacks	Describe common network attacks.
	IP Vulnerabilities and Threats	Explain how IP vulnerabilities are exploited by threat actors.
	TCP and UDP Vulnerabilities	Explain how TCP and UDP vulnerabilities are exploited by threat actors.
	IP Services	Explain how IP services are exploited by threat actors.
	Network Security Best Practices	Describe best practices for protecting a network.
	Cryptography	Describe common cryptographic processes used to protect data in transit.
Module	**Topic**	**Objective**
ACL Concepts		Explain how ACLs are used as part of a network security policy.
	Purpose of ACLs	Explain how ACLs filter traffic.
	Wildcard Masks in ACLs	Explain how ACLs use wildcard masks.
	Guidelines for ACL Creation	Explain how to create ACLs.
	Types of IPv4 ACLs	Compare standard and extended IPv4 ACLs.
Module	**Topic**	**Objective**
ACLs for IPv4 Configuration		Implement IPv4 ACLs to filter traffic and secure administrative access.
	Configure Standard IPv4 ACLs	Configure standard IPv4 ACLs to filter traffic to meet networking requirements.

	Modify IPv4 ACLs	Use sequence numbers to edit existing standard IPv4 ACLs.
	Secure VTY Ports with a Standard IPv4 ACL	Configure a standard ACL to secure vty access.
	Configure Extended IPv4 ACLs	Configure extended IPv4 ACLs to filter traffic according to networking requirements.
Module	**Topic**	**Objective**
NAT for IPv4		Configure NAT services on the edge router to provide IPv4 address scalability.
	NAT Characteristics	Explain the purpose and function of NAT.
	Types of NAT	Explain the operation of different types of NAT.
	NAT Advantages	Describe the advantages and disadvantages of NAT.
	Configure Static NAT	Configure static NAT using the CLI.
	Configure Dynamic NAT	Configure dynamic NAT using the CLI.
	Configure PAT	Configure PAT using the CLI.
	NAT64	Describe NAT for IPv6.
Module	**Topic**	**Objective**
WAN Concepts		Explain how WAN access technologies can be used to satisfy business requirements.
	Purpose of WANs	Explain the purpose of a WAN.
	WAN Operations	Explain how WANs operate.
	Traditional WAN Connectivity	Compare traditional WAN connectivity options.

	Modern WAN Connectivity	Compare modern WAN connectivity options.
	Internet-Based Connectivity	Compare internet-based WAN connectivity options.
Module	**Topic**	**Objective**
VPN and IPsec Concepts		Explain how VPNs and IPsec secure site-to-site and remote access connectivity.
	VPN Technology	Describe benefits of VPN technology.
	Types of VPNs	Describe different types of VPNs
	IPsec	Explain how the IPsec framework is used to secure network traffic.
Module	**Topic**	**Objective**
QoS Concepts		Explain how networking devices implement QoS.
	Network Transmission Quality	Explain how network transmission characteristics impact quality.
	Traffic Characteristics	Describe minimum network requirements for voice, video, and data traffic.
	Queuing Algorithms	Describe the queuing algorithms used by networking devices.
	QoS Models	Describe the different QoS models.
	QoS Implementation Techniques	Explain how QoS uses mechanisms to ensure transmission quality.
Module	**Topic**	**Objective**
Network Management		Implement protocols to manage the network.
	Device Discovery with CDP	Use CDP to map a network topology.

	Device Discovery with LLDP	Use LLDP to map a network topology.
	NTP	Implement NTP between an NTP client and NTP server.
	SNMP	Explain SNMP operation.
	Syslog	Explain syslog operation.
	Router and Switch File Maintenance	Use commands to back up and restore an IOS configuration file.
	IOS Image Management	Perform an upgrade of an IOS system image.
Module	**Topic**	**Objective**
Network Design		Explain the characteristics of scalable network architectures.
	Hierarchical Networks	Explain how data, voice, and video are converged in a switched network.
	Scalable Networks	Explain considerations for designing a scalable network.
	Switch Hardware	Explain how switch hardware features support network requirements.
	Router Hardware	Describe the types of routers available for small to-mediumsized business networks.
Module	**Topic**	**Objective**
Network Troubleshooting		Troubleshoot enterprise networks.
	Network Documentation	Explain how network documentation is developed and used to troubleshoot network issues.
	Troubleshooting Process	Compare troubleshooting methods that use a systematic, layered approach.
	Troubleshooting Tools	Describe different networking troubleshooting tools.

	Symptoms and Causes of Network Problems	Determine the symptoms and causes of network problems using a layered model.
	Troubleshooting IP Connectivity	Troubleshoot a network using the layered model.
Module	**Topic**	**Objective**
Network Virtualization		Explain the purpose and characteristics of network virtualization.
	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.
Module	**Topic**	**Objective**
Network Automation		Explain how network automation is enabled through RESTful APIs and configuration management tools.
	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.
	Configuration Management	Compare the configuration management tools Puppet, Chef, Ansible, and SaltStack
	IBN and Cisco DNA Center	Explain how Cisco DNA center enables intent-based networking.

Notes to Instructors

- All instructors are to use a combination of Packet Tracer and hands on labs (via classroom equipment or the Netlab+ online lab server)
- Assignments consist of labs, quizzes, chapter tests, skills based exam, and a final exam