

COURSE NUMBER: CE3270

COURSE TITLE: WANs & SP Operations

COURSE DESCRIPTION:

This course provides the learner with an understanding of Wide Area Networks (WANs) and Service Provider (SP) Operations. In this course learners will complete their studies of Internet Protocol (IP) networking and examine the relationship between IP traffic and the carrier networks that transport data. Learners will gain practical experience with SP Operations such as network management and provisioning WAN services.

PREREQUISITES: CE3381 – Advanced Routing & Switching
CE3371 – Switching & Routing

CO-REQUISITES: None

CREDIT VALUE: Four (4)

COURSE HOURS PER WEEK: Three (3)

LAB HOURS PER WEEK: Two (2)

SCHEDULED TEXT: To be determined by instructor

LEARNING RESOURCES: To be determined by instructor

MAJOR TOPICS:

- 1.0 Wide Area Networks (WANs)
- 2.0 Point to Point Protocol (PPP)
- 3.0 Multiprotocol Label Switching (MPLS)
- 4.0 Network Security and Access Control Lists (ACLs)
- 5.0 Virtual Private Networks (VPN)
- 6.0 Addressing Services and Mobile Internet Protocol
- 7.0 Network Management and Performance Issues

LEARNING OBJECTIVES:

The expected learning outcomes are that the learner will be able to:

1.0 Wide Area Networks (WANs)

- 1.1 Explain the concept of a *Wide Area Network* (WAN)

- 1.2 Explain the need for WANs
- 1.3 Describe the hierarchical network architecture
- 1.4 Describe the enterprise architecture
- 1.5 Describe the WAN *Physical Layer* concepts
- 1.6 Describe the WAN *Data Link Layer* concepts
- 1.7 Describe WAN switching options
- 1.8 Describe WAN connection options
- 1.9 Specify a WAN connection option for a given situation

2.0 Point to Point Protocol (PPP)

- 2.1 Describe the fundamental concepts of point-to-point serial communications
- 2.2 Describe the components of PPP
- 2.3 Describe the architecture of PPP
- 2.4 Describe the PPP frame structure
- 2.5 Explain the operation of PPP
- 2.6 Explain the *Network Control Protocol* (NCP) process
- 2.7 Configure PPP on network devices for a given situation
- 2.8 Configure PPP authentication on network devices
- 2.9 Troubleshoot PPP configuration issues

3.0 Multiprotocol Label Switching (MPLS)

- 3.1 Introduction to *Multiprotocol Label Switching* (MPLS)
 - 3.1.1 Explain basic core MPLS technology and concepts
 - 3.1.2 Explain the function of *MPLS Labels* and *Label Stack*
 - 3.1.3 Describe the characteristics and behaviors of *Label Distribution in Frame-mode MPLS*
 - 3.1.4 Explain *Convergence in Frame-mode MPLS*
 - 3.1.5 Describe the characteristics and behaviors of *Label Distribution over LC-ATM Interfaces* and *VC Merge*
 - 3.1.6 Describe the features of *MPLS Label Allocation, Distribution, and Retention Modes*
 - 3.1.7 Explain the process of *LDP Neighbor Discovery*
- 3.2 Implementing MPLS
 - 3.2.1 Configure *Frame-mode MPLS* on a router
 - 3.2.2 Configure *Label-Controlled ATM MPLS* on a router
 - 3.2.3 Monitor MPLS operation on a router
 - 3.2.4 Troubleshoot MPLS configuration issues
- 3.3 MPLS *Virtual Private Networks* (VPN)
 - 3.3.1 Explain Major VPN Categorization
 - 3.3.2 Describe MPLS VPN Architecture
 - 3.3.3 Describe the MPLS VPN *Routing Model*
 - 3.3.4 Explain the process of MPLS VPN *Packet Forwarding*

- 3.3.5 Configure MPLS VPN on a router using specified routing protocols
- 3.3.6 Troubleshoot basic MPLS VPN configuration issues

4.0 Network Security and Access Control Lists (ACLs)

- 4.1 Network Security
 - 4.1.1 Describe common security threats to enterprise networks
 - 4.1.2 Describe methods to mitigate security threats to enterprise networks
 - 4.1.3 Develop a security policy for an enterprise network
 - 4.1.4 Configure network devices to implement a security policy
 - 4.1.5 Conduct a network security audit
- 4.2 *Access Control Lists (ACLs)*
 - 4.2.1 Explain the purpose of ACLs
 - 4.2.2 Differentiate between types of ACLs
 - 4.2.3 Explain the operation of ACLs
 - 4.2.4 Design ACLs for given situations
 - 4.2.5 Explain the functions of ACLs
 - 4.2.6 Explain the guidelines for using ACLs
 - 4.2.7 Configure network devices to implement ACLs
 - 4.2.8 Troubleshoot and resolve issues with ACLs

5.0 Virtual Private Networks (VPN)

- 5.1 State the benefits of VPN
- 5.2 Describe the components of VPN
- 5.3 Describe the characteristics of a secure VPN
- 5.4 Explain VPN tunneling
- 5.5 Differentiate amongst *VPN Tunneling Protocols*
- 5.6 Discuss the methods used to ensure data confidentiality and integrity in VPNs
- 5.7 Describe the IPsec security protocols
- 5.8 Design a VPN solution for a given situation
- 5.9 Implement a VPN solution for a given situation
- 5.10 Troubleshoot and resolve issues associated with VPNs

6.0 Addressing Services and Mobile Internet Protocol

- 6.1 Dynamic Host Configuration Protocol (DHCP)
 - 6.1.1 Differentiate between DHCP and Bootstrap Protocol (BOOTP)
 - 6.1.2 Implement DHCP to support an enterprise network
 - 6.1.3 Configure a router to provide DHCP services
 - 6.1.4 Implement DHCP Relay to support clients on different subnets
 - 6.1.5 Troubleshoot and resolve issues with DHCP
- 6.2 Network Address Translation (NAT)
 - 6.2.1 Define NAT

- 6.2.2 Describe the components of NAT
- 6.2.3 Explain the operation of NAT
- 6.2.4 Differentiate between Static NAT and Dynamic NAT
- 6.2.5 Configure NAT overloading
- 6.2.6 Describe the benefits and drawbacks of using NAT
- 6.2.7 Implement NAT for a given situation
- 6.2.8 Troubleshoot and resolve issues with NAT
- 6.3 Mobile Internet
 - 6.3.1 Explain the concept of mobile Internet
 - 6.3.2 Describe the challenges associated with providing mobile Internet services
 - 6.3.3 Explain the concept of *Federated Identity* as it applies to mobile Internet
 - 6.3.4 Describe the impact of mobile Internet on the *Data Link Layer*
 - 6.3.5 Describe the impact of mobile Internet on the *Network Layer*
 - 6.3.6 Describe the impact of mobile Internet on the *Transport Layer*
 - 6.3.7 Describe the impact of mobile Internet on the *Application Layer*
 - 6.3.8 Design a mobile Internet solution for a given situation
 - 6.3.9 Implement a mobile Internet solution for a given situation

7.0 Network Management and Performance Issues

- 7.1 Network Management
 - 7.1.1 Describe how a trouble ticket processes through the *Network Operations Center* (NOC)
 - 7.1.2 Apply an *Incident Management Process*
 - 7.1.3 Perform incident management using basic tools and documentation
 - 7.1.4 Develop a *Network Management Plan* using appropriate network management tools to monitor network status
 - 7.1.5 Diagnose network problems using network management tools
 - 7.1.6 Implement a network management plan to perform maintenance tasks such as
 - 7.1.6.1 Backup device configurations
 - 7.1.6.2 Maintain a network inventory
- 7.2 Performance Issues
 - 7.2.1 Implement a network documentation plan that includes
 - 7.2.1.1 Change management
 - 7.2.1.2 Network upgrades
 - 7.2.2 Implement *Service Level Agreement* (SLA) monitoring on network devices
 - 7.2.3 Resolve network performance issues using troubleshooting methodologies and tools
 - 7.2.4 Implement a problem resolution scheme using a layered model approach
- 7.3 Network Monitoring

- 7.3.1 Explain syslog operation
- 7.3.2 Configure syslog to log messages to a syslog server
- 7.3.3 Explain Simple Network Management Protocol (SNMP) operation
- 7.3.4 Configure SNMP for a given network
- 7.3.5 Explain NetFlow operation
- 7.3.6 Configure NetFlow for a given network

EVALUATION:

Laboratories	20 %
Projects	20 %
Tests	20 %
Final Exam	40 %

DATE DEVELOPED: March 2012

DATE REVIEWED:

REVISION NUMBER: 1

DATE REVISED: June 2014

Note to instructor: Check PIRS to ensure this outline is the most current version.