COURSE NUMBER: CE3370

COURSE TITLE: Switching & L2 Security

COURSE DESCRIPTION:

This course continues the learner's education in IP-based communications. In this course the learner will explore concepts in LAN design, the operation and configuration of LAN switches, virtual Local Area Networks (VLANs), spanning tree protocol (STP), and LAN switch security.

PREREQUISITES: CE1210 – Basic Communications Networks I

CO-REQUISITES: None

CREDIT VALUE: Four (4)

COURSE HOURS PER WEEK: Three (3)

LAB HOURS PER WEEK: Two (2)

SUGGESTED TEXT:

Lewis, W. (2012). *LAN switching and wireless: CCNA exploration companion guide*. CA: Cisco Press. ISBN-13: 9781587132735; ISBN-10: 1587132737

LEARNING RESOURCES:

Cisco Networking Academy http://www.cisco.com/web/learning/netacad/index.html

MAJOR TOPICS:

1.0 Local Area Network (LAN) Design
2.0 LAN Switch Configuration
3.0 Virtual Local Area Networks (VLANs) and VLAN Trunking Protocol (VTP)
4.0 Redundant Links and Spanning Tree
5.0 Inter-VLAN Routing
6.0 Wireless LAN Configuration
7.0 LAN Switch Security

LEARNING OBJECTIVES:

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

1.0 Local Area Network (LAN) Design

1.1 Describe the hierarchical network model
1.2 Identify the principles of hierarchical network design
1.3 Explain the issues associated with network convergence including legacy equipment and advanced technologies
1.4 Design a switched LAN to meet specified requirements applying the principles of hierarchical network design

2.0 LAN Switch Configuration

2.1 Describe the key elements of Ethernet/802.3 networks including media access methods, duplex communications, and device addressing
2.2 Identify Ethernet/802.3 network factors that can affect design and performance including data transfer rates, collisions and broadcasts, latency and congestion, and segmentation
2.3 Describe the operation of a LAN switch with respect to traffic forwarding, port and switch speed, buffering, and Layer 3 switching
2.4 Configure a LAN switch to meet specified requirements utilizing the command line interface, including the help facility
2.5 Configure a LAN switch for remote access via:
- 2.5.1 Telnet
- 2.5.2 Secure Shell (SSH)
- 2.5.3 Hypertext Transfer Protocol (HTTP)

2.6 Utilize the command line interface of a LAN switch to:
- 2.6.1 Confirm the switch configuration
- 2.6.2 Back up the switch configuration
- 2.6.3 Restore a switch configuration

2.7 Configure LAN switch security to prevent unauthorized local and remote access including encrypting passwords and setting login banners
2.8 Configure the LAN switch port security feature to defend against common attacks such as:
- 2.8.1 Media Access Control (MAC) address flooding
- 2.8.2 Spoofing
- 2.8.3 Cisco Discovery Protocol (CDP)
- 2.8.4 Telnet

3.0 Virtual Local Area Networks (VLANs) and VLAN Trunking Protocol (VTP)

3.1 Explain the following related aspects of Virtual Local Area Networks (VLANs):
- 3.1.1 Concepts
- 3.1.2 Benefits

3.2 Describe the types of VLANs available

3.3 Differentiate between normal range and extended range VLANs
3.4 Explain the VLAN membership process
3.5 Explain assigning a host to a VLAN
3.6 Differentiate between access links and trunk links
3.7 Configure trunks on a LAN switch to meet a specified requirement
3.8 Configure VLANs on a LAN switch to meet a specified requirement
3.9 Identify common problems associated with VLANs and trunks
3.10 Demonstrate how these issues are resolved
3.11 Configure a LAN switch to defend against VLAN attacks such as VLAN hopping
3.12 Describe the operation of the VLAN Trunking Protocol (VTP) including VTP modes, VTP advertising, and VTP pruning
3.13 Configure VTP on a LAN switch
3.14 Identify potential security threats posed by VTP
3.15 Identify countermeasures to potential security threats posed by VTP

4.0 Redundant Links and Spanning Tree

4.1 Explain the need redundant links in a switched LAN
4.2 Describe the operation of the spanning tree protocol
4.3 Explain how Spanning-Tree Protocol (STP) manages redundant links
4.4 Describe the STP topology including port types and roles:
- 4.4.1 Root bridge
- 4.4.2 Root port
- 4.4.3 Designated port
- 4.4.4 Non-designated port

4.5 Differentiate between proprietary STP (PVST, PVST+, and Rapid PVST+) and standard STP (RTSP and MSTP)
4.6 Describe common STP attacks
4.7 Describe effective countermeasures to STP attacks

5.0 Inter-VLAN Routing

5.1 Explain how traffic is routed between VLANs in a switched LAN
5.2 Describe the common methods of inter-VLAN routing explaining the benefits
5.3 Describe the drawbacks of each method of inter-VLAN routing
5.4 Configure a LAN switch and router combination to provide inter-VLAN routing
5.5 Identify common problems associated with inter-VLAN routing
5.6 Describe methods of addressing common problems associated with inter-VLAN routing
5.7 Describe the use of next-hop addresses in path determination
5.8 Explain how routers forward packets
5.9 Differentiate between static and dynamic routing
5.10 Identify common routing protocols

6.0 Wireless LAN Configuration

6.1 Differentiate between wired and wireless LANs with respect to connectivity, media access, and data transfer
6.2 Compare wireless LAN standards with respect to operating frequency, operating channels, modulation methods, data transfer rates
6.3 Evaluate the pros and cons of each wireless LAN standard with respect to the comparison developed in 6.2
6.4 Explain the importance of standards and regulation in wireless LANs including the roles of standards and regulating bodies and the role of each
6.5 Describe wireless LAN components including the operation and role of each device
6.6 Explain how clients distinguish between different wireless LANs
6.7 Describe the common topologies used with wireless LANs including operating mode, connection type, and coverage
6.8 Describe the process of association and authentication of wireless LAN clients
6.9 Design a wireless LAN to meet specified requirements
6.10 Identify common security threats in wireless LANs
6.11 Describe how these common security threats in wireless LANs can be mitigated
6.12 Configure wireless LAN security
6.13 Determine suitable locations for wireless access point placement based on reachability, congestion, RF interference, and overlap with other access points

7.0 LAN Switch Security

7.1 Describe the security triad
7.2 Discuss risk management with respect to risk analysis and risk control
7.3 Demonstrate access control and identity management in a switched LAN environment
7.4 Identify the security vulnerabilities of Dynamic Host Configuration Protocol (DHCP) and Address Resolution Protocol (ARP)
7.5 Describe effective countermeasures to the types of attacks referenced in 7.4
7.6 Describe the security threats posed by:
  7.6.1 IPv6 Neighbor Discovery
  7.6.2 Router Advertisement

7.7 Explain how the types of attacks referenced in 7.6 might be prevented
7.8 Identify the security threats to Power over Ethernet (PoE)
7.9 Identify the measures to mitigate the threats referenced in 7.8
7.10 Identify the various types of Access Control Lists (ACLs) available on a LAN switch
7.11 Demonstrate how each ACL can be employed to secure a switched network
7.12 Configure identity based network services such as IEEE 802.1x to improve security in a switched LAN
7.13 Discuss emerging trends and technologies in LAN security such as IEEE 802.1AE

EVALUATION:

Laboratories:	10%
Quizzes:	10%
Practical Exam:	40%
Final Exam:	40%

DATE DEVELOPED: March 2012 **DATE REVIEWED:**

REVISION NUMBER: **DATE REVISED:**

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