Course Acronym:	CIS
Course Number:	143
Descriptive Title:	Securing and Automating Enterprise Networks Cisco 3
Division:	Business
Department:	Computer Information Systems
Course Disciplines:	Computer Information Systems
Catalog Description:	This course provides an understanding of how switches are interconnected and configured to provide network access to Local Area Network users. It also provides instruction on how to integrate wireless devices into Local Area Networks. This course is technically oriented and will prepare students for industry certification. This course also provides a fundamental understanding of WAN (Wide Area Network) networking concepts and a wide range of network technologies. Instruction will be given on several WAN technologies, including PPP (Point to Point), frame relay, and related topics, such as access control list, network address translation, and virtual private networks. *Note: This course is semester three in the Cisco Networking Academy program. (Preparation for the CCNA Certification)*
Prerequisite:	Computer Information Systems 142 with a minimum grade of C or equivalent experience
Co-requisite:	
Recommended Preparation:	
Enrollment Limitation:	
Hours Lecture (per week):	2
Hours Laboratory (per week):	3
Outside Study Hours:	4
Total Course Hours:	90
Course Units:	3
Grading Method:	Letter Grade and Pass/No Pass
Credit Status:	Credit, degree applicable
Transfer CSU:	Yes
Effective Date:	Fall 2007
Transfer UC:	No
Effective Date:	

General Education: ECC	
Term:	
Other:	
CSU GE:	
Term:	
Other:	
IGETC:	
Term:	
Other:	
Student Learning Outcomes:	**SLO #1 Internetworking Modules** Define and discuss internetworking models. Determine appropriate paths for internetworking. **SLO #2 Visual and Command Line User Interfaces** Install and use the graphical user interfaces and command line interfaces for network configuration **SLO #3 Automating Router Configurations** Configure hardware and software for routers using command line and automation tools to use both LAN and WAN protocols. **SLO #4 Configuring Networking Control Lists** Configure and manage traffic with network control lists. **SLO#5 Configure Access Control Lists** Configure and manage users and groups with access control lists **SLO#6 Configure a Virtual Private Network** Configure a virtual private network between a client and an enterprise network
Course Objectives:	1. Analyze the Hierarchical Network Model including the Access Layer, Distribution Layer, and the Core Layer. 2. Describe the principles of a Hierarchical Network Design. 3. Analyze a converged network. 4. Evaluate suitable switches for a Small and Medium Sized Business. 5. Evaluate design considerations for Ethernet/802.3 networks. 6. Compare switch forwarding methods. 7. Examine symmetric and asymmetric switching. 8. Evaluate mission-critical data types in a WAN (Wide Area Network). 9. Examine WAN physical layer concepts. 10. Select the appropriate WAN technology to meet different enterprise business requirements. 11. Examine the process of how the Cisco enterprise architecture provides integrated services over an enterprise network.

	12. Examine key WAN technology concepts. 13. Describe the fundamental concepts of point-to-point serial communication. 14. Describe key PPP (Point to Point) concepts. 15. Configure PPP encapsulation. 16. Explain and configure PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) authentication. 17. Identify security threats to enterprise networks. 18. Describe methods to mitigate security threats to enterprise networks. 19. Configure basic router security. 20. Disable unused router services and interfaces. 21. Manage files and software images with the Cisco IOS (Internetwork Operating System), and the IFS (Integrated File System). 22. Explain how ACLs (Access Control List) are used to secure a medium-size enterprise branch office network, including the concept of packet filtering, the purpose of ACLs, how ACLs are used to control access, and the types of Cisco ACLs. 23. Configure standard ACLs in a medium-size enterprise branch office network, including defining filtering criteria, configuring standard ACLs to filter traffic, and applying standard ACLs to router interfaces. 24. Configure extended ACLs in a medium-size enterprise branch office network, including configuring extended ACLs and named ACLs, configuring filters, verifying and monitoring ACLs, and troubleshooting extended ACL issues. 25. Describe complex ACLs in a medium-size enterprise branch office network, including configuring dynamic, reflexive, and timed ACLs, verifying and troubleshooting complex ACLs, and explaining relevant caveats. 26. Analyze the enterprise requirements for providing teleworker services, including the differences between private and public network infrastructures. 27. Examine the process of how VPN technology can be used to provide secure teleworker services to an enterprise network. 28. Configure NAT (Network Address Translation) on a Cisco router. This includes explaining key features and operation of NAT and NAT Overload, explaining advantages and disadvantages of NAT, configuring NAT and NAT Overload to conserve IP address space in a network, configuring port forwarding, and verifying and troubleshooting NAT configurations.

Major Topics:	.**Scaling Networks (1 hour, lecture)**
	    A. Network expansion design
	    B. Design for scalability
	    C. Redundancy Plan
	    D. Bandwidth increase
	  II. **Hierarchical Network Design Implementation (2 hours, lecture)**
	 . Network Scaling Requirements
	    A. Enterprise Business Devices
	    B. Hierarchical Network Design
	    C. Cisco Enterprise Architecture
	    D. Failure Domains
	  III. **Network Scaling Fundamentals (2 hours, lecture)**
	 . Switching hardware selection
	    A. Layered Network design
	    B. VLAN and LAN security
	    C. Switching Platforms
	  IV. **Network Expansion (2 hours, lecture)**

.   Design for Scalability
- A. Redundancy planning
- B. Bandwidth Increase issues
- C. Access Layer expansion
- D. Fine-tuning Routing Protocols

V. **LAN Redundancy (2 hours, lecture)**

.   Spanning-Tree concepts
- A. Spanning-Tree configuration
- B. First Hop Redundancy protocols
- C. Components of LAN

VI. **Link Aggregation (2 hours, lecture)**

.   Link Aggregation concepts
- A. EtherChannel operation
- B. EtherChannel interfaces configuration
- C. Configuration guidelines

VII. **Switch Hardware Issues (2 hours, lecture)**

.   Switch Platforms
- A. Port Density
- B. Forwarding Rates
- C. Power over Ethernet
- D. Multilayer Switching

VIII. **Devices Management (3 hours, lecture)**

.   IOS Files and Licensing Management
- A. In-Band versus Out-of-Band Management
- B. Basic Router CLI commands
- C. Basic Router show commands
- D. Basic Switch CLI commands
- E. Basic Switch Show commands

IX. **Wireless LANs (2 hours, lecture)**

.   Wireless concepts
- A. Wireless LAN (Local Area Network) standards
- B. Wireless Infrastructure components
- C. Threats to wireless security

X. **WAN Fundamentals (2 hours, lecture)**

.   Wide-Area Networks introduction
- A. The Evolving Enterprise
- B. WAN Technology Concepts
- C. WAN Connection Options
- D. Circuit-Switched Connection Options
- E. Packet-Switched Connection Options

XI. **PPP (2 hours, lecture)**

.   Serial Communication introduction
- A. HDLC Encapsulation
- B. PPP Concepts
- C. The Establishment of Link with LCP
- D. PPP Configuration Options
- E. PPP Authentication Protocols
- F. CHAP NCP Explained
- G. PPP Configuration with Authentication

XII. **Frame Relay (1 hour, lecture)**

.   Basic Frame Relay Concepts
- A. Frame Relay Address Mapping
- B. Frame Relay Configuration

        C. Advanced Frame Relay Concepts
        D. Frame Relay Flow Control
        E. Advanced Frame Relay Configuration
        F. Frame Relay Sub-interfaces Configuration

XIII. **Network Security (2 hours, lecture)**
. Introduction to Network Security
        A. Types of Network Attacks
        B. Cisco Routers Security
        C. Application of Cisco IOS Security Features to Routers
        D. Router Networking Services Security
        E. Routing Protocols Security
        F. Cisco SDM usage
        G. Router Configuration to Support SDM
        H. Secure Router Management
        I. Backup and Upgrading a Software Image
        J. Software Images Recovery

XIV. **ACLs (4 hours, lecture)**
. ACL utilization to Secure Networks
        A. Types of Cisco ACLs
        B. Standard and Extended ACL comparison
        C. Standard ACLs Configuration
        D. ACL Wildcard Mask
        E. Standard ACLs management
        F. Standard ACLs application to Interfaces
        G. Extended ACL Configuration
        H. Extended ACLs Application to Interfaces
        I. Complex ACLs Configuration
        J. Reflexive ACLs Management
        K. Dynamic ACLs Management
        L. Time-Based ACLs Management

XV. **Teleworker Services (1 hour, lecture)**
. Business Requirements for Teleworker Services
        A. Broadband Services
        B. Cable, DSL, Broadband Wireless
        C. VPN Technology
        D. Types of VPNs
        E. VPN Tunneling
        F. VPN Data Confidentiality and Integrity
        G. Characteristics of Secure VPNs

XVI. **IP Addressing Services (3 hours, lecture)**
. Introduction to DHCP
        A. Cisco Router Configuration as a DHCP Server
        B. DHCP Client Configuration
        C. DHCP Relay
        D. Networks Configuration with NAT
        E. Dynamic & Static NAT Configuration
        F. NAT Overload Configuration for a Pool of Public Addresses
        G. NAT Verification and NAT Overload
        H. IPv6 Addressing & Transition Strategies
        I. Cisco IOS Dual Stack
        J. IPv6 Tunneling
        K. IPv6 Addressing Configuration

XVII. **Network Troubleshooting (3 hours, lecture)**

   . Network Performance Baseline Establishment
   A. The Network Documentation Process
   B. Steps for Establishing a Network Baseline
   C. Troubleshoot Methodologies and Tools
   D. Layered Models utilization for Troubleshooting
   E. WAN Communications Review
   F. WAN Design Steps
   G. WAN Traffic and Topology Considerations
   H. WAN Technologies and Bandwidth
   I. OSI Model utilization for Network Troubleshooting
   J. Physical, Data Link, Network, Transport, and Application Layers

XVIII. **Introduction To WANs (3 hours, lab)**
 . Wide-Area Network
   A. Enterprise Evolution
   B. WAN Technology Concepts
   C. WAN Connection Options
   D. Circuit-Switched Connection Options
   E. Packet-Switched Connection Options

XIX. **PPP (4 hours, lab)**
 . Serial Communication
   A. HDLC Encapsulation
   B. PPP Concepts
   C. Link establishment with LCP
   D. PPP Configuration Options
   E. PPP Authentication Protocols
   F. CHAP NCP Explained
   G. PPP Configuration with Authentication

XX. **Frame Relay (3 hours, lab)**
 . Basic Frame Relay Concepts
   A. Frame Relay Address Mapping
   B. Frame Relay Configuration
   C. Advanced Frame Relay Concepts
   D. Frame Relay Flow Control
   E. Advanced Frame Relay Configuration
   F. Frame Relay Sub-interfaces Configuration

XXI. **Network Security (4 hours, lab)**
 . Network Security Fundamentals
   A. Types of Network Attacks
   B. Cisco Routers security
   C. Application of Cisco IOS Security Features to Routers
   D. Router Networking Services Security
   E. Routing Protocols Security
   F. Cisco SDM utilization
   G. Router Configuration to Support SDM
   H. Secure Router Management
   I. Backup and Upgrading a Software Image
   J. Software Images Recovery

XXII. **ACLs (4 hours, lab)**
 . ACL utilization to Secure Networks
   A. Types of Cisco ACLs
   B. Standard and Extended ACL comparison
   C. Standard ACLs Configuration
   D. ACL Wildcard Mask

E.　Standard ACLs application to Interfaces
　　　　F.　Extended ACL Configuration
　　　　G.　Extended ACLs application to Interfaces
　　　　H.　Complex ACLs Configuration
　　　　I.　Reflexive ACLs
　　　　J.　Dynamic ACLs
　　　　K.　Time-Based ACLs
　XXIII.　**Teleworker Services (4 hours, lab)**
　.　Business Requirements for Teleworker Services
　　　　A.　Broadband Services
　　　　B.　Cable, DSL, Broadband Wireless
　　　　C.　VPN Technology
　　　　D.　VPN Types
　　　　E.　VPN Tunneling
　　　　F.　VPN Data Confidentiality and Integrity
　　　　G.　Secure VPN characteristics
　XXIV.　**IP Addressing Services (4 hours, lab)**
　.　Introduction to DHCP
　　　　A.　Cisco Router Configuration as a DHCP Server
　　　　B.　DHCP Client Configuration
　　　　C.　DHCP Relay
　　　　D.　Network scaling with NAT
　　　　E.　Dynamic Configuration & Static NAT
　　　　F.　NAT Configuration Overload for a Pool of Public Addresses
　　　　G.　NAT and NAT Overload Verification
　　　　H.　IPv6 Addressing & Transition Strategies
　　　　I.　Cisco IOS Dual Stack
　　　　J.　IPv6 Tunneling
　　　　K.　IPv6 Addressing Configuration
　XXV.　**Network Troubleshooting (4 hours, lab)**
　.　Network Performance Baseline establishment
　　　　A.　Network Documentation Process
　　　　B.　Troubleshooting Methodologies and Tools
　　　　C.　Layered Models utilization for Troubleshooting
　　　　D.　WAN Communications Review
　　　　E.　WAN Design steps
　　　　F.　WAN Traffic and Topology Considerations
　　　　G.　WAN Technologies and Bandwidth
　　　　H.　OSI Model utilization for Network Troubleshooting
　　　　I.　Physical, Data Link, Network, Transport, and Application Layers
　XXVI.　**Wireless LANs Configuration (4 hours, lab)**
　.　Integrated wireless routers and Access points
　　　　A.　Wireless router and client configuration
　　　　B.　Connect a Linksys EA Series router to a wireless network
　　　　C.　WLAN Topologies
　XXVII.　**Advanced Single and Multi-Area OSPF (4 hours, lab)**
　.　Advanced Single-area OSPF Configuration
　　　　A.　Troubleshoot Single-area OSPF Implementations
　　　　B.　Multi-area OSPF Operation
　　　　C.　Configuration and verification of Multi-area OSPF
　XXVIII.　**Router Hardware (4 hours, lab)**
　.　Router Requirements
　　　　A.　Legacy Router Issues

	B. Cisco Routers and components
	C. Router Hardware issues
	XXIX. **Single and Multi-Area OSPF Troubleshooting and Configuration (4 hours, lab)**
	. Multi-area OSPFv2 configuration
	A. Multi-area OSPFv3 configuration
	B. Multi-area OSPFv2 and OSPFv3 troubleshooting
	C. Single-area OSPF verification
	XXX. **LAN Redundancy Configuration (4 hours, lab)**
	. Switched network building with redundant links
	A. Rapid PVST+, PortFast, and BPDU Guard configuration
	B. HSRP and GLBP configuration
	C. LAN Redundancy issues
	XXXI. **Link Aggregation Configuration and Verification (4 hours, lab)**
	. EtherChannel configuration
	A. Basic Switch settings configuration
	B. PAgP and LACP configuration
	C. Troubleshoot and verify EtherChannel
Total Lecture Hours:	36
Total Laboratory Hours:	54
Total Hours:	90
Primary Method of Evaluation:	Skills demonstration
Typical Assignment Using Primary Method of Evaluation:	Configure a Linksys WRT300N Access Point consistent with the LAN/WLAN topology. Configure port security on a Cisco switch, as well as static routes on multiple devices. Also configure frequency channels, MAC (Media Access Control) filters, password management, logging, and a firmware upgrade. Document the process, in writing, to be included in your Cisco Journal.
Critical Thinking Assignment 1:	Troubleshoot a switching scenario in a given IEEE 802.1D spanning tree protocol that is showing a convergence time of up to 50 seconds. The time delay is unacceptable in modern switched networks. Only three of the six trunks are forwarding frames. Implement the per-VLAN Cisco implementation of PVST+ (Per VLAN Spanning Tree Plus). The goal of PVST+ (Per VLAN Spanning Tree Plus) is to reduce the latency to 6 seconds or less. The lab will be complete when all wired trunks are carrying traffic and all three switches are participating in per-VLAN load balancing for the three user VLANs (Virtual Local Area Networks). Document the process, in writing, to be included in your Cisco Journal.
Critical Thinking Assignment 2:	Troubleshoot a switched network that has been designed and configured to support five VLANs (Virtual Local Area Networks) and a routed subnet just outside the LAN (Local Area Network). Inter-VLAN routing is being provided by an external router in a router-on-a-stick configuration, and the server network is routed across a separate Fast Ethernet interface. The network is not functioning properly, and you have received complaints from users. You will need to define the problem, and then analyze the existing configurations to determine and correct the problems and document it in your Cisco Journal.
Other Evaluation Methods:	Performance exams

	Other exams Quizzes Laboratory reports Class Performance Homework Problems Multiple Choice Completion Matching Items True/False Other (specify): 1. Students create a Technical Journal that is due at the end of each semester. Substantial writing and organization takes place when preparing this journal. 2. Students create and save a basic switch configuration, setup a TFTP (Trivial File Transfer Protocol) server, back up the switch Cisco IOS. Students are also required to pass the SBA (Skill Based Assessment) exam that includes hands-on activities in the Cisco Lab or on the NetLab.
Instructional Methods:	Demonstration, Discussion, Group Activities, Lab, Lecture, Multimedia presentations
If other:	
Work Outside of Class:	• Study • Answer questions • Skill practice • Required reading • Problem solving activities • Journal • Other (specify) o Students have the capability to login to the NetLab from any place where they have an Internet connection. NetLab is located on campus in the Cisco lab. In addition to the 2 weekly in-class lab hours, students have 1 hour lab assignments to complete each week. They can remotely access actual Routers and Switches in the lab.
If Other:	
Up-To-Date Representative Textbooks:	Cisco Networking Academy, Enterprise Networking, Security, and Automation Companion Guide (CCNAv7), 2020.
Alternative Textbooks:	
Required Supplementary Readings:	

Other Required Materials:	
Requisite:	Prerequisite
Category:	sequential
Requisite course(s): List both prerequisites and corequisites in this box.	Computer Information Systems 142 with a minimum grade of C or
Requisite and Matching skill(s):Bold the requisite skill. List the corresponding course objective under each skill(s).	**Understand basic Switch concepts and configuration, LAN (Local Area Network) Design, VLANs (Virtual Local Area Networks), VTP ((VLAN Trunking Protocol), and STP (Spanning Tree Protocol), Inter-VLAN Routing, and basic Wireless Concepts and Configurations.** CIS 142 - Identify a router as a computer with an operating system (OS) and hardware designed for the routing process. CIS 142 - Evaluate the process that a router uses to determine a path and how the router switches packets. CIS 142 - Describe the role of dynamic routing protocols and place these protocols in the context of modern network design. CIS 142 - Evaluate and explain the network discovery process of distance vector routing protocols using Routing Information Protocol (RIP). CIS 142 - Evaluate VLSM and explain the benefits of classless IP addressing. **Understand basic concepts of Routers and Packets.** CIS 142 - Evaluate the process that a router uses to determine a path and how the router switches packets.
Requisite Skill:	equivalent experience
Requisite Skill and Matching Skill(s): Bold the requisite skill(s). If applicable	Successful completion of this course requires a fundamental understanding of the integration of wireless devices into Local Area Networks (LAN), WAN (Wide Area Network) networking concepts, and a wide range of network technologies.
Requisite course:	
Requisite and Matching skill(s):Bold the requisite skill. List the corresponding course objective under each skill(s).	
Requisite Skill:	
Requisite Skill and Matching skill(s): Bold the requisite skill. List the corresponding course objective under	

each skill(s). If applicable	
Enrollment Limitations and Category:	
Enrollment Limitations Impact:	
Course Created by:	William Saichek
Date:	10/01/2000
Original Board Approval Date:	02/20/2001
Last Reviewed and/or Revised by:	Jesus Rubio
Date:	03/17/2023
Last Board Approval Date:	07/17/2023 effective FALL 2024