COURSE OUTLINE: CYB204 - CISCO TECHNOLOGIES

Prepared: IT Studies
Approved: Corey Meunier, Dean, Technology, Trades, and Apprenticeship

Course Code: Title	CYB204: CISCO TECHNOLOGIES (CCNA)
Program Number: Name	2198: CYBERSECURITY 5911: CYBERSECURITY
Department:	PPP triOS
Academic Year:	2023-2024
Course Description:	In this course, students learn key LAN, WAN, and WLAN concepts, as well as their configuration using Cisco routers and switches. Moreover, students learn how to manage IP configuration, mitigate security threats, and automate the configuration of networks. Through this course, students will be introduced to topics included on the Cisco Certified Network Associate (CCNA) certification exam.
Total Credits:	6
Hours/Week:	6
Total Hours:	84
Prerequisites:	There are no pre-requisites for this course.
Corequisites:	There are no co-requisites for this course.
Vocational Learning Outcomes (VLO's) addressed in this course: **Please refer to program web page for a complete listing of program outcomes where applicable.**	**2198 - CYBERSECURITY** VLO 1 Develop and implement cyber security solutions to protect network systems and data VLO 2 Plan and implement security assessment methodologies, vulnerability management strategies and incident response procedures to generate and communicate security analysis reports and recommendations to the proper level of the organization VLO 3 Recommend processes and procedures for maintenance and deployment of cyber security VLO 4 Select and deploy optimal security appliances and technologies to safeguard an organization’s network **5911 - CYBERSECURITY** VLO 1 Develop and implement cyber security solutions to protect network systems and data. VLO 2 Plan and implement security assessment methodologies, vulnerability management strategies and2.incident response procedures to generate and communicate security analysis reports and recommendations to the proper level of the organization. VLO 3 Recommend processes and procedures for maintenance and deployment of cyber security solutions. VLO 4 Select and deploy optimal security appliances and technologies to safeguard an organization’s network.

Essential Employability Skills (EES) addressed in this course:	EES 4 Apply a systematic approach to solve problems. EES 5 Use a variety of thinking skills to anticipate and solve problems. EES 6 Locate, select, organize, and document information using appropriate technology and information systems. EES 7 Analyze, evaluate, and apply relevant information from a variety of sources. EES 10 Manage the use of time and other resources to complete projects.
Course Evaluation:	Passing Grade: 50%, D A minimum program GPA of 2.0 or higher where program specific standards exist is required for graduation.
Other Course Evaluation & Assessment Requirements:	To successfully pass this course, the student must receive passing grades for both the Test portion of the class AND the Laboratory portion. Grade Definition Grade Point Equivalent A+ 90 - 100% 4.00 A 80 - 89% B 70 - 79% 3.00 C 60 - 69% 2.00 D 50 - 59% 1.00 F (Fail) 49% and below 0.00 CR (Credit) Credit for diploma requirements has been awarded. S Satisfactory achievement in field /clinical placement or non-graded subject area. U Unsatisfactory achievement in field/clinical placement or non-graded subject area. X A temporary grade limited to situations with extenuating circumstances giving a student additional time to complete the requirements for a course. NR Grade not reported to Registrar`s office. W Student has withdrawn from the course without academic penalty. OTHER EVALUATION CONSIDERATIONS 1. In order to pass this course, the student must obtain an overall test/quiz average of 50% or better, as well as an overall assignment average of 50% or better. A student who is not present to write a particular test/quiz and does not notify the professor beforehand of their intended absence, may be subject to a zero grade on that test/quiz. 2. There will be no supplemental or make-up quizzes/tests in this course unless there are extenuating circumstances. 3. Assignments must be submitted by the due date according to the specifications of the professor. Late assignments will normally be given a mark of zero. Late assignments will only be marked at the discretion of the professor in cases where there were extenuating circumstances. 4. Any assignment/projects submissions, deemed to be copied, will result in a zero grade being assigned to all students involved in that particular incident. 5. It is the responsibility of the student to ask the professor to clarify any assignment requirements. 6. The professor reserves the right to modify the assessment process to meet any changing needs of the class. Attendance: Sault College is committed to student success. There is a direct correlation between academic

performance and class attendance, therefore, for the benefit of all its constituents, all students are encouraged to attend all of their scheduled learning and evaluation sessions. This implies arriving on time and remaining for the duration of the scheduled session. It is the departmental policy that once the classroom door has been closed, the learning process has begun. Late arrivers may not be granted admission to the room.

Books and Required Resources:

Cisco CCNA Certification: Exam 200-301, 2 Volume Set by Todd Lammie
Publisher: Sybex (Wiley)
ISBN: 978-1-119-67761-1

Course Outcomes and Learning Objectives:

Course Outcome 1	**Learning Objectives for Course Outcome 1**
Review fundamental network concepts and configure network components.	NETWORK FUNDAMENTALS 1.1 Explain the role and function of network components. 1.2 Describe the characteristics of network topology architectures. 1.3 Compare physical interface and cabling types. 1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed). 1.5 Compare TCP to UDP. 1.6 Configure and verify IPv4 addressing and subnetting. 1.7 Describe the need for private IPv4 addressing. 1.8 Configure and verify IPv6 addressing and prefix. 1.9 Compare IPv6 address types. 1.10 Verify IP parameters for Client OS (Windows, macOS, Linux). 1.11 Describe wireless principles. 1.12 Explain virtualization fundamentals (virtual machines). 1.13 Describe switching concepts.
Course Outcome 2	**Learning Objectives for Course Outcome 2**
Configure and verify network access protocol standards and best practices.	NETWORK ACCESS 2.1 Configure and verify VLANs (normal range) spanning multiple switches. 2.2 Configure and verify inter-switch connectivity. 2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP). 2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP). 2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations. 2.6 Compare Cisco Wireless Architectures and AP modes. 2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG). 2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS). 2.9 Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings.
Course Outcome 3	**Learning Objectives for Course Outcome 3**

Interpret the components of a routing table and configure and verify IP connectivity.	IP CONNECTIVITY 3.1 Interpret the components of routing table. 3.2 Determine how a router makes a forwarding decision by default. 3.3 Configure and verify IPv4 and IPv6 static routing. 3.4 Configure and verify single area OSPFv2. 3.5 Examine the purpose of first hop redundancy protocol.
Course Outcome 4	**Learning Objectives for Course Outcome 4**
Configure and verify various IP services.	IP SERVICES 4.1 Configure and verify inside source NAT using static and pools. 4.2 Configure and verify NTP operating in a client and server mode. 4.3 Explain the role of DHCP and DNS within the network. 4.4 Explain the function of SNMP in network operations. 4.5 Describe the use of syslog features including facilities and levels. 4.6 Configure and verify DHCP client and relay. 4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping. 4.8 Configure network devices for remote access using SSH. 4.9 Describe the capabilities and function of TFTP/FTP in the network.
Course Outcome 5	**Learning Objectives for Course Outcome 5**
Assess security concepts and program elements and configure multiple security features.	SECURITY FUNDAMENTALS 5.1 Elaborate key security concepts (threats, vulnerabilities, exploits, and mitigation techniques). 5.2 Describe security program elements (user awareness, training, and physical access control). 5.3 Configure device access control using local passwords. 5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics). 5.5 Describe remote access and site-to-site VPNs. 5.6 Configure and verify access control lists. 5.7 Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security). 5.8 Differentiate authentication, authorization, and accounting concepts. 5.9 Describe wireless security protocols (WPA, WPA2, and WPA3). 5.10 Configure WLAN using WPA2 PSK using the GUI.
Course Outcome 6	**Learning Objectives for Course Outcome 6**
Evaluate the impact of automation and programmability on network	AUTOMATION AND PROGRAMMABILITY 6.1 Explain how automation impacts network management. 6.2 Compare traditional networks with controller-based

	management.	networking. 6.3 Describe controller-based and software defined architectures (overlay, underlay, and fabric). 6.4 Compare traditional campus device management with Cisco DNA Center enabled device management. 6.5 Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding). 6.6 Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible. 6.7 Interpret JSON encoded data.

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Final Exam	30%
Lab Work and Assignments	60%
Professional Performance	10%

Date: July 5, 2023

Addendum: Please refer to the course outline addendum on the Learning Management System for further information.