CSIS-592: CCNA 3 ENTERPRISE NETWORKING, SECURITY, AND AUTOMATION

Effective Term
Fall 2026

BOT Approval Date
05/15/2025

Discipline
CSIS - Computer Sci/Info Systems
Course Number
592

Course Title
CCNA 3 Enterprise Networking, Security, and Automation

Short Title
Enterprise Networking

Credit Status (CB 04)
D - Credit - Degree applicable

Units

Lecture Units
3.00

Total Units
3.00

Hours

Lecture Contact Hours
48-54
Out of Class Hours Lecture
96-108

Total Contact Hours
48 - 54

Total Out of Class Hours
96 - 108

Total Student Learning Hours
144 - 162

Distance Education
Yes

Distance Education

Distance Education Type
Both Fully Online and Hybrid Online

Fully Online Delivery Requirements:
a. Students must be notified via the college schedule of classes and the syllabus for the class if proctored tests are required for this course

b. Any planned face-to-face meetings, such as an orientation or study session, must be optional
c. The MSJC curriculum committee requires the use of accessible, asynchronous discussion as a component of every fully online course

Are you using publisher content?

No

Regular Substantive Interaction

Instructor-to-student, student-to-student, and student-to-content contact shall be distributed in a manner that will ensure regular substantive interaction (RSI) is maintained not only weekly but also for the duration of the course. Instructor interactions should be equivalent in time, quality and consistency to the engagement students would receive in a face-to-face course—for example, through announcements, discussion participation, personalized feedback, video messages, or other instructional communications. Instructors are expected to be responsive to student inquiries within a 24-72 hour time frame excluding holidays. RSI will be maintained through a variety of methods: • Orientation - Students must be oriented to the online and face-to-face portions at the start of the course. • Announcements - Announcements using the course management system must be posted at least weekly to keep students current on course events, due dates, materials, etc. • Discussion Forums - Content-related discussion forums within the designated CMS will include appropriate instructor participation and will be initiated and maintained, with timely feedback provided. Instructors are required to monitor the discussions and related activities to provide guidance and direction. Open-ended discussion boards may be used to further learning and interaction. • MSJC Communication – Instructor will use MSJC-administered communication tools (such as email or the designated CMS communication tools) to regularly communicate with and provide ease of access to students. • Timely Feedback - Timely feedback on student work will be provided by the instructor, which may include comments and/or rubrics, within the Grades area of the designated CMS. • Scheduled Meetings – Hybrid and synchronous courses will meet at regularly scheduled times. ADA Compliance - All course interactions and content must be designed with accessibility in mind and meet ADA requirements.

Catalog Description

This course provides a comprehensive, theoretical, and practical approach to learning the technologies and protocols needed to design and implement a converged switched network. Students learn about the hierarchical network design model and how to select devices for each layer. The course explains how to configure a switch for basic functionality and how to implement Virtual LANs, VTP, and Inter-VLAN routing in a converged network.

Requisites

Prerequisite(s)

Prerequisite(s) (must be taken before)
CSIS-791 (with a grade of C or better).

Codes

TOP Code (CB 03)

0708.10* - *Computer Networking

CIP Code

11.0901 - Computer Systems Networking and Telecommunications.

Repeatability Code

No

Grading Option

Letter grade OR P/NP

Minimum Qualifications

Minimum Qualifications	And/Or
Computer Information Systems	End

Learning Objectives

Learning Objectives

Learning Objective
1. Evaluate basic concepts and terminologies related to Wide Area Networks (WANs)
2. Evaluate and troubleshoot enterprise networks.
3. Analyze how social engineering exploits systemic inequalities and racial bias, and propose inclusive cybersecurity strategies to protect marginalized communities from targeted cyber threats.
4. Design and implement secure and scalable VPN configurations for enterprise networks.
5. Analyze and optimize network performance using monitoring and diagnostic tools to improve efficiency in large-scale deployments.
6.Compose and troubleshoot PPP, Frame Relay, and router security configurations to ensure secure and reliable enterprise network connectivity.
7.Prepare and troubleshoot ACL, DHCP, and NAT configurations to enhance network security, accessibility, and traffic management.

Learning Outcome Information

Course Learning Outcomes

Learning Outcome
1.The student will be able to establish single-area OSPFv2 in both point-to-point and multiaccess networks.
2.The student will be able demonstrate how to mitigate threats and enhance network security using access control lists and security best practices.
3.The student will be able to apply standard IPv4 ACLs to filter traffic and secure administrative access.
4.The student will be able to deploy NAT services on the edge router to provide IPv4 address scalability.
5.The student will be able to analyze how to optimize, monitor, and troubleshoot scalable network architectures.

Content

Course Lecture Content

1. Introduction to WAN
   a. Providing Integrated Services to the Enterprise
   b. WAN Technology Concepts
   c. WAN Connection Options
   d. Scalability Considerations in Enterprise WAN
   e. Ensuring Inclusive and Equitable WAN Access
2. PPP
   a. Serial Point-to-Point Links
   b. PPP Concepts
   c. Configuring PPP
   d. Configuring PPP with Authentication
   e. Optimizing PPP for Large-Scale Networks
   f. Chapter Labs
3. Frame Relay
   a. Basic Frame Relay Concepts
   b. Configuring Frame Relay
   c. Advanced Frame Relay Concepts
   d. Configuring Advanced Frame Relay
   e. Performance Tuning and Troubleshooting
   f. Chapter Labs
4. Network Security
   a. Introduction to Network Security
   b. Securing Cisco Routers
   c. Secure Router Network Services

   d. Using Cisco SDM
   e. Secure Router Management
   f. Implementing Scalable VPNs for Secure Communications
   g. Ensuring Inclusive and Accessible Security Policies
   h. Chapter Labs
5. ACLs
   a. Using ACLs to Secure Networks
   b. Configuring Standard ACLs
   c. Configuring Extended ACLs
   d. Configuring Complex ACLs
   e. Access Control Strategies for Enterprise Networks
   f. Chapter Labs
6. Teleworker Services
   a. Business Requirements for Teleworker Services
   b. Broadband Services
   c. VPN Technology
   d. Designing Secure and Scalable Remote Work Solutions
   e. Ensuring Equitable Network Access for Remote Users
7. IP Addressing Services
   a. DHCP
   b. Scaling Networks with NAT
   c. IPv6
   d. Addressing Strategies for Enterprise Scalability
   e. Chapter Labs
8. Network Troubleshooting
   a. Establishing the Network Performance Baseline
   b. Troubleshooting Methodologies and Tools
   c. Common WAN Implementation Issues
   d. Network Troubleshooting
   e. Optimizing Network Performance in Large-Scale Deployments
   f. Using Monitoring and Diagnostic Tools
   g. Chapter Labs
9. VPN and Secure Remote Access
   a. Introduction to VPN Technologies
   b. Designing and Implementing Site-to-Site VPNs
   c. Configuring Remote Access VPNs
   d. Optimizing VPN Performance for Enterprise Networks
   e. Ensuring Secure and Inclusive Access Policies
   f. Chapter Labs
10. Network Performance and Scalability
   a. Assessing Network Scalability for Large User Populations
   b. Traffic Analysis and Load Balancing
   c. Implementing Quality of Service (QoS) Strategies
   d. Scaling Enterprise Networks Efficiently
   e. Ensuring Fair and Equitable Network Resource Allocation
11. Cloud-Based Networking
   a. Introduction to Cloud Networking
   b. Cloud-Based Security Solutions
   c. Hybrid Cloud Network Architectures
   d. Ensuring Scalability and Redundancy in Cloud Networks
12. Automation and Network Orchestration
   a. Introduction to Network Automation
   b. Using Python and Ansible for Network Configuration
   c. Automating Network Security Policies
   d. Enhancing Efficiency in Enterprise Network Operations

13. Social Engineering and Systemic Racism
    a. Understanding Social Engineering Tactics
    b. Systemic Racism and Its Role in Targeting Vulnerable Groups
    c. Mitigating the Impact Through Inclusive Security Practices

Methods of Instruction

Method

Discussion

Integration

Each week, students will participate in a collaborative discussion to compare and contrast composing and troubleshooting key network configurations, including PPP, Frame Relay, router security, ACL, and NAT configurations. Discussions will also focus on the evaluation and troubleshooting of WAN and Enterprise Networks and the role of VLANs and Spanning Tree Protocols in multi-switch environments.
Team-Based Problem Solving:
Students will be assigned to small groups to analyze a given troubleshooting scenario related to one of the covered topics (e.g., misconfigured ACL, PPP authentication failure, spanning-tree issues).
Groups will collaborate to diagnose the issue, propose solutions, and explain their troubleshooting approach.

DE Adaptations for MOI

Discussions will take place using the discussion tool in the course management system (CMS), which is designed with accessibility in mind. Features such as screen reader support, adjustable text size, and keyboard navigation ensure that all students can fully participate. Feedback on discussion posts will be provided through the CMS within one week, ensuring timely and accessible responses for each student.

Method

Homework

Integration

Weekly homework will be given to guide students through the practical application of such concepts as the evaluation of basic concepts and terminologies related to Wide Area Networks (WANs), the evaluation of enterprise networks, and the configuration of DHCP and NAT.

DE Adaptations for MOI

Homework will be evaluated based on accuracy, completeness, and adherence to the provided instructions, with assignments submitted through the course management system (CMS) assignment editor. Students will receive detailed feedback via the CMS grading tool within one week of the submission deadline, including comments highlighting strengths and areas for improvement. Depending on assignment requirements, students may also submit work through discussion boards, blogs, or wiki tools within the CMS. Accessibility requirements will be met to ensure that all students, including those with disabilities or specific learning needs, can fully complete and submit assignments without barriers. This includes providing alternative formats for assignments when necessary, such as screen reader-friendly documents or captions for multimedia, allowing flexible submission methods to accommodate assistive technology use, and ensuring that all CMS tools used for submissions and feedback comply with accessibility standards such as WCAG 2.1 or ADA guidelines. Additionally, adaptations or extended deadlines will be offered where necessary based on documented accessibility needs, and technical support and accommodations will be provided for students requiring assistance in navigating or using digital tools required for assignments.

Method

Lecture

Integration

Lecture, with supporting visual materials (presentations or multimedia), will introduce conceptual and practical skills such as composing and troubleshooting PPP configurations, router security configurations, and DHCP and NAT configurations. In addition to technical proficiency, lectures will also integrate Diversity, Equity, and Inclusion (DEI) learning objectives by examining how systemic inequalities impact cybersecurity vulnerabilities. Students will explore how social engineering tactics disproportionately target marginalized communities and analyze real-world case studies that highlight the role of bias in network security. Through discussions on inclusive security practices and equitable network design, students will develop a broader understanding of how networking technologies can be adapted to protect diverse user populations. Visual materials and examples will emphasize the contributions

of diverse professionals to networking advancements and reinforce the importance of bias-free cybersecurity policies to ensure equitable access and protection for all users.

DE Adaptations for MOI

The CMS will serve as a central hub for online students, providing access to recorded lectures, online presentations, and supplementary materials. To foster inclusivity, live webinars and recorded lectures will include closed captions (CC), allowing for real-time interaction and discussions. Additionally, accessibility requirements will be met by ensuring that all recorded content is available in alternative formats, such as transcripts for audio materials and screen reader-compatible documents. Interactive elements, including discussions and Q&A sessions, will be facilitated using accessible communication tools to accommodate diverse learning needs.

Method

Observation and Demonstration

Integration

Observation and demonstration will illustrate lecture principles and reading assignments with a focus on fundamental networking concepts and applying them to problem solving and potential solutions to homework assignments. Guided practice will include the troubleshooting of frame relay, router security, PPP, DHCP and NAT configurations.

DE Adaptations for MOI

Observation and demonstrations will be available through the CMS, featuring closed-captioned videos, web-based tutorials, and hands-on activities. Interactive software simulations hosted on the CMS will offer students opportunities for real-time engagement and practical experience, ensuring accessibility and promoting active learning for all participants.

Methods of Evaluation

Method

Final Performance

Integration

A Comprehensive final exam that measures each student's ability to synthesize and apply course concepts such as composing and troubleshooting PPP, Frame Relay, router security, ACL, and NAT configurations; Evaluation and troubleshooting WAN and Enterprise Networks; VLANs and Spanning Tree protocols over multiple switches. The comprehensive final exam will be evaluated on completeness and correctness along with proper configuration.

DE Adaptations for MOE

The comprehensive final exam will be administered through the course management system (CMS), consisting of multiple-choice, true/false, and short-answer questions. Students will submit their completed exams directly through the CMS. Immediate feedback will be provided for objective questions, such as multiple-choice and true/false, while feedback on short-answer responses will be given in appropriate timing. This approach ensures timely reinforcement of key concepts and provides clarity on areas that may require further improvement. Accessibility requirements will be met to ensure that all students, including those using assistive technologies, can fully engage with the exam. This includes providing alternative formats for exam content when needed, such as screen reader-compatible text or transcripts for audio elements. The CMS exam platform will also be tested for compliance with WCAG 2.1 and ADA guidelines to ensure full accessibility.

Method

Exams/Tests

Integration

Weekly exams consisting of short-answer and multiple-choice questions will be given to assess students' mastery of key networking concepts, including the composition and troubleshooting of PPP, Frame Relay, router security, DHCP, and NAT configurations, as well as WAN and Enterprise Network performance and VLANs and Spanning Tree Protocols over multiple switches. In addition to evaluating technical proficiency, these exams will also assess students' ability to apply Diversity, Equity, and Inclusion (DEI) principles to network security and cybersecurity practices. Specifically, students will demonstrate their understanding of how systemic racism and social inequalities impact cybersecurity risks, particularly in relation to social engineering attacks targeting marginalized communities. Exam questions will require students to analyze case studies on social engineering and bias in cybersecurity, propose

inclusive security policies, and apply equitable network design principles to reduce cybersecurity vulnerabilities for diverse user populations. Grading will be based on technical correctness, completeness, and the ability to integrate DEI considerations into networking solutions. By embedding both technical and ethical assessments, the exams ensure that students develop not only strong networking skills but also a broader understanding of how cybersecurity practices must be designed to be inclusive, equitable, and accessible to all users.

DE Adaptations for MOE

Weekly exams will be administered through the course management system (CMS) and will consist of multiple-choice, true/false, and short-answer questions. Students will submit their completed exams directly through the CMS. Immediate feedback will be provided for objective questions, while feedback on short-answer responses will be given in appropriate time, ensuring timely reinforcement of learning and offering guidance on areas for improvement. Accessibility requirements will be met to ensure that all students, including those using assistive technologies, can fully participate in exams. This includes providing alternative formats for exam content when needed, such as screen reader-compatible text or transcripts for audio elements, as well as offering extended time or other accommodations for students with documented accessibility needs. The CMS exam platform will also be tested for compliance with WCAG 2.1 and ADA guidelines to ensure full accessibility.

Method

Homework

Integration

Weekly homework assignments will be given that apply important concepts and skills to the student's experience outside the classroom. The focus might be on the evaluation and troubleshooting of enterprise networks, router security, and Frame Relay configurations. Homework will be evaluated based on following directions, correctness, completeness, and proper documentation.

DE Adaptations for MOE

Homework will be evaluated based on accuracy, completeness, and adherence to the provided instructions. Assignments will be submitted through the assignment editor in the course management system (CMS). Students will receive detailed feedback through the CMS grading tool, with comments highlighting strengths and areas for improvement. Feedback will be provided within one week of the submission deadline. Depending on the task, students may also submit assignments using discussion boards, blogs, or wiki tools within the CMS. Accessibility requirements will be met to ensure all students can complete and submit assignments without barriers. This includes providing alternative formats when necessary, such as screen reader-compatible documents or transcripts for multimedia content, allowing flexible submission methods to accommodate assistive technology use, and ensuring the CMS is compliant with WCAG 2.1 and ADA guidelines. Additionally, extended deadlines or other accommodations will be offered for students with documented accessibility needs.

Assignments

Assignment Type

Writing

In-class and/or outside of class

In-class
Outside of class

Formative or Summative

Formative

Assignment

Background:
This assignment is designed to help you recognize and prevent social engineering, a common threat in information security. Through research and analysis, you will gain a deeper understanding of how social engineering attacks occur and how to protect against them. This assignment will help you apply theoretical knowledge to real-world scenarios.

Assignment Overview:
You have been tasked with investigating a recent social engineering incident at an organization where an attacker posed as a trusted individual to gain access to confidential information. Your goal is to research real-world social engineering cases to understand how these attacks happen, present your findings, and suggest strategies for identifying and preventing such attacks in the future.

Tasks:
Presentation on Social Engineering:
Create a presentation (5-7 slides) summarizing three real-world examples of social engineering incidents you found in your research.
For each example, include:
A brief description of the incident
The method used by the social engineer
The impact of the attack
Explain how each incident could have been prevented or mitigated.
One-Page Report on Recognizing and Preventing Social Engineering:
Write a one-page report discussing three common signs of social engineering attacks and how to recognize them.
Research methods that organizations use to prevent social engineering, and include three specific strategies or procedures in your report.

Grading and Feedback: Evaluate the accuracy and thoroughness of the social engineering examples researched, ensuring that they are relevant and well-explained. Examine the quality of the one-page report, focusing on its comprehensiveness, organization, and clarity in discussing recognition and prevention strategies. For the presentation, assess the clarity of content, the structure of the slides, and the effectiveness of the prevention recommendations provided. Feedback should be objective and take into account different levels of familiarity with social engineering concepts, recognizing diverse perspectives. Grading and feedback will be provided through the course management system within one week of submission.

How assignment will be adapted in online format

This course will integrate research activities, presentations, and discussions within the online learning environment. You will access course materials and submit your presentation and one-page report electronically through the course management system (CMS). The PowerPoint presentation will be submitted as a file upload, and the report will be submitted as a text entry or PDF upload in the same CMS. Discussion forums and interactive simulations will be available for activities related to social engineering cases, and virtual communication tools will facilitate discussions and feedback. Instructors will provide feedback through the CMS within one week of submission, offering comments on your presentation content, report structure, and relevance. Virtual office hours will be available for students who need additional guidance or clarification, ensuring timely and supportive feedback throughout the course.

Accessibility requirements will be met to ensure that all students, including those using assistive technologies, can fully engage with course content and activities. Course materials will be provided in alternative formats, such as screen reader-compatible documents and transcripts for multimedia content. Discussion forums and simulations will be designed to be accessible for students using assistive technologies, and the CMS submission system will be tested for compliance with WCAG 2.1 and ADA guidelines. Virtual communication tools will include closed captioning and transcription options for recorded sessions and live discussions. Additionally, accommodations such as extended deadlines or alternative participation methods will be available for students with documented accessibility needs.

Assignment Type

Writing

In-class and/or outside of class

In-class
Outside of class

Formative or Summative

Summative

Assignment

Complete a final project that demonstrates your understanding of Cisco router configuration and password recovery procedures. This project simulates a real-world scenario where network administrators must regain access to a Cisco router by recovering or resetting a lost password using ROMMON and configuration register settings.

Example Final Project:
Design and implement a password recovery procedure for a Cisco router model of your choice. The project will include:
Researching and explaining the purpose and common settings of the configuration register, including how different values affect router behavior.
Detailing the step-by-step process for recovering or resetting the password, including accessing ROMMON mode and using relevant commands.
Configuring the router to restore normal operation after completing the password recovery.
Documenting the procedure, tools used, commands entered, and the rationale behind each step.

Grading and Feedback:
Evaluate the technical accuracy and completeness of the password recovery process. Assess the quality of documentation, ensuring that the project report is well-structured, explains each step in detail, and provides clear instructions for executing the procedure. If a presentation is required, evaluate clarity, confidence, and the ability to answer questions about the process. Feedback will be provided through the course management system within one week of the project submission.

How assignment will be adapted in online format

The final project will be submitted through the course management system (CMS), along with any supporting documentation and files. Instructors will provide feedback and guidance throughout the project development process. Students will receive a comprehensive evaluation of their final submission, including feedback on both technical accuracy and documentation quality. Final feedback will be delivered through the CMS within one week of the project submission, ensuring students receive timely and detailed insights into their performance.Accessibility requirements will be met to ensure that all students, including those using assistive technologies, can fully participate in assignments. Assignments and supporting materials will be provided in alternative formats, such as screen reader-compatible documents and transcripts for multimedia. Flexible submission options will be available to accommodate assistive technology needs, and the CMS will be tested for compliance with WCAG 2.1 and ADA guidelines to ensure full accessibility. Additionally, accommodations, such as extended deadlines or modified submission formats, will be provided for students with documented accessibility needs.

Assignment Type

Reading

In-class and/or outside of class

Outside of class

Formative or Summative

Formative

Assignment

Reading:
"Systemic Racism Is a Cybersecurity Threat" by the Council on Foreign Relations

Background:
After reading the assigned article, you will explore how social engineering attacks exploit human vulnerabilities, particularly within marginalized communities. Racial bias and systemic inequalities can increase the likelihood of these groups being targeted by cybercriminals through disinformation campaigns, phishing schemes, and scams that take advantage of social and economic disparities. In this assignment, you will analyze these issues, examine real-world cases, and propose solutions to mitigate the risks for vulnerable populations.

What You Will Do:Work in small groups (3-4 students) to select and analyze a real-world case where social engineering targeted a marginalized group.
1. Analyze Social Engineering Techniques
Identify and explain different social engineering tactics (e.g., phishing, pretexting, baiting) and how they manipulate human behavior.
Discuss the psychological principles behind these attacks and the goals of cybercriminals.
Investigate how certain tactics are specifically adapted to target marginalized communities and why they are effective.
2. Examine Racial Bias in Cyber Targeting
Explore how systemic racism, economic disparities, and social inequalities make some groups more vulnerable to social engineering attacks.
Identify real-world examples of cyber scams or disinformation campaigns that have disproportionately affected marginalized communities.
Discuss how bias in cybersecurity practices can contribute to the increased risks faced by these populations.
3. Conduct a Case Study Analysis
Select a case where social engineering tactics were used to target a minority group (e.g., phishing campaigns targeting immigrant communities, disinformation aimed at racial minorities).
Analyze:
Why this group was targeted
How the attack was carried out
What impact it had on the community
Explain lessons learned and how cybersecurity awareness can help prevent similar attacks in the future.
4. Propose Solutions to Reduce Risk
Develop at least two strategies to reduce the risk of social engineering attacks on vulnerable communities. These may include:

Awareness programs
Inclusive security practices
Policy changes
Explain how these solutions can help bridge the cybersecurity gap and protect different demographic groups.
Provide guidelines for implementing these strategies in the cybersecurity field.

Grading and Feedback:
Evaluation will focus on the depth of understanding of social engineering techniques and the accuracy of the analysis regarding racial bias in targeting. The quality of the case study report will be assessed for being comprehensive, well-structured, and clearly documented. For presentations, clarity, confidence, and the ability to respond to questions will be evaluated. Feedback will be objective and unbiased, recognizing diverse perspectives and backgrounds. The final project will be graded by finals week.

How assignment will be adapted in online format

The assignment will take place through an online discussion board, where students will submit their analyses and proposed solutions as initial posts, followed by responses to at least two classmates' submissions to foster peer discussion. Group discussions will be facilitated through video conferencing for collaborative case study analysis. Feedback will be provided through the course management system (CMS) within one week of submission, ensuring it is timely, constructive, and reflective of diverse perspectives. Accessibility requirements will be met to ensure all students, including those using assistive technologies, can fully engage in discussion-based assignments. Online discussion boards will be screen reader-compatible and allow alternative text input for students with disabilities. Video conferencing sessions will include live captions and transcription options to ensure accessibility for all participants. Flexible participation options, such as text-based alternatives, will be available for students unable to engage in video discussions. The CMS and discussion platforms will be tested for compliance with WCAG 2.1 and ADA guidelines to ensure full accessibility. Additionally, accommodations such as extended deadlines or alternative participation methods will be offered for students with documented accessibility needs.

Course Materials

Textbooks

CCNA 200-301 Official Cert Guide and Network Simulator Library, Second Edition(Aug 29, 2024)
Copyright 2025
Edition: 1st
Book
ISBN-10: 0-13-537138-4
ISBN-13: 978-0-13-537138-1

Other Resources

Cisco Network Academy. Cisco Exploration: LAN Switching and Wireless, ed. Cisco Systems Inc., 2011

Class Size Information

Class Size

35

Class Size Category

B - Facilitated learning 35

Diversity and Inclusion

Course Design and Materials: Course will incorporate diverse perspectives, authors, and examples that reflect a variety of cultures, identities, and lived experiences. Instructional materials will be reviewed regularly to ensure representation, inclusivity, and alignment with equity-minded practices across disciplines.

Inclusive Learning Environment: Instructors will establish classroom norms and policies that promote respect, civil discourse, and belonging in both online and face-to-face classes. Clear expectations for communication and engagement will support a learning space where all students feel valued and heard.

Accessible Instruction: Course content will be delivered using accessible design. Materials will follow accessibility guidelines within the CMS, including captioned media, readable document formats, and multiple means of engagement to support diverse learning.

Equitable Teaching Practices: Instructors will use transparent and grading criteria, varied assessment methods, and timely feedback to promote fairness and student success. Opportunities for revision, reflection, and multiple demonstrations of learning may be incorporated when appropriate to the discipline.

Culturally Responsive Pedagogies: Instructional strategies will encourage critical thinking about diverse perspectives and systems of power relevant to the course content. Faculty will foster opportunities for students to connect course material to real-world contexts.

Ongoing Reflection and Improvement: Faculty will engage in continuous professional development related to IDEAA principles and reflect on course practices using metacognition to identify opportunities for increased equity, inclusion, and accessibility.

Explain how diversity and inclusion(e.g., gender, culture/race, sexuality, etc.) is infused into the course.

Diversity and inclusion are central to our Scaling Networks course, ensuring that every student engages with multiple perspectives and understands the impact of biases, systemic inequalities, and cultural differences in networking and cybersecurity. The course integrates inclusive teaching methods, real-world case studies, and critical discussions that highlight how network technologies can be leveraged or misused to target specific populations.For example, students explore the intersection of systemic racism and cybersecurity by analyzing how social engineering attacks disproportionately target marginalized communities. Through case studies, such as phishing campaigns aimed at immigrant populations or disinformation campaigns targeting racial minorities, students critically assess the vulnerabilities of different groups and propose inclusive security solutions that ensure equitable protection. Additionally, they examine how bias in cybersecurity practices can lead to disproportionate risks for certain demographic groups, reinforcing the need for ethical and inclusive approaches to network design and security.Beyond security concerns, representation in networking innovations is emphasized. For example, Dr. Arogyaswami Paulraj, an Indian engineer, made significant contributions to wireless networking through Multiple-Input Multiple-Output (MIMO) technology, which has greatly improved the scalability and performance of modern networks. By studying such contributions, students recognize the global and multicultural nature of networking advancements.
By embedding diversity and inclusion throughout the curriculum, this course ensures that students not only develop strong technical skills but also understand the broader social implications of networking technologies. This prepares them to become network professionals who design and manage systems that are inclusive, equitable, and secure for all users.

Describe how assignments, instruction, evaluation, course content, and interactions are contextualized for diverse learners promoting an equitable course.

Enterprise Networking, Security, and Automation course is designed to ensure that assignments, instruction, evaluation, course content, and interactions accommodate diverse learning styles, providing an equitable learning experience for all students. Assignments will focus on real-world enterprise networking scenarios, requiring students to apply their knowledge to scalable network design, security implementation, and automation strategies. Students will engage in hands-on configuration tasks, troubleshooting exercises, and case studies that reflect industry challenges in networking. Practical assignments will emphasize network security best practices, VPN configuration, and the integration of automation tools, ensuring students develop both technical proficiency and problem-solving skills necessary for managing enterprise networks. Through structured assessments, scenario-based problem-solving, and configuration labs, students will learn to analyze and implement solutions that reflect current industry standards in network management and security.Instruction will incorporate interactive demonstrations, guided practice, and live troubleshooting exercises, allowing students to observe and apply advanced networking concepts in real time. The use of simulation tools such as Cisco Packet Tracer will enable students to practice network configurations in a virtual environment before applying their skills to physical network hardware. Video tutorials, step-by-step configuration guides, and instructor-led walkthroughs will provide students with multiple modes of instruction to reinforce key concepts. Additionally, the course will incorporate real-world case studies on enterprise networking challenges, allowing students to analyze how scalability, security, and automation impact large-scale network infrastructures.Evaluation methods will ensure that students are assessed on both their technical competency and problem-solving abilities. Assessments will include practical exams, where students configure and troubleshoot enterprise network environments, as well as written evaluations that require students to analyze network security risks and propose mitigation strategies. Regular peer and instructor feedback will be provided on network design projects, ensuring that students receive constructive insights to refine their technical approach. Students will also complete scenario-based assessments, where they must diagnose and resolve issues related to routing, switching, VPNs, and automation, simulating real-world network troubleshooting tasks.Course content will be structured to progressively build students' expertise in enterprise networking, covering key areas such as WAN architecture, network security, scalable VPN configurations, and performance optimization. Students will gain experience with Layer 3 routing protocols, network automation tools, and security hardening techniques, ensuring they develop a comprehensive understanding of enterprise network management. Learning modules will integrate case studies on network infrastructure failures and successes, enabling students to critically evaluate design decisions and their impact on network performance and security. The course will also cover Cisco best practices for automation and network scalability, preparing students for real-world enterprise networking roles and CCNA certification success.tudent interactions will foster collaboration and knowledge sharing through group-based troubleshooting labs, peer review sessions, and structured discussions on network security and automation. Team projects will require students to design, implement, and document scalable and secure network solutions, mimicking industry practices in enterprise IT teams. Discussion boards will provide a space for students to exchange ideas, troubleshoot common networking challenges, and compare different automation approaches. Instructor feedback and mentorship will be actively provided through live Q&A sessions, discussion forums, and structured office hours, ensuring students receive guidance on technical concepts and network problem-solving strategies.

Interactions

Explain how the course will incorporate student-to-student interaction.

Collaborative Projects: Throughout the course, students will participate in group assignments designed to encourage teamwork and problem-solving, fostering peer-to-peer interaction and a sense of camaraderie. For example, as part of the assignment on Social Engineering Analysis, groups will collaboratively research and present on recent social engineering incidents, analyzing attack methods, impacts, and prevention strategies. This aligns with the Methods of Instruction (MOI) for Observation and Demonstration, where students can observe each other's findings and learn through collaborative analysis. Evaluation will follow the Methods of Evaluation (MOE) for Homework, assessing the thoroughness of their research and the quality of the presentation.
Interactive Classroom Sessions: During live lectures or webinars, small-group discussions will allow students to engage in active collaboration. For instance, students might work together to analyze a case study on social engineering targeting marginalized communities, discussing the psychological principles behind the attacks. These activities promote engagement with the course content and align with the MOI for Lectures, encouraging students to connect theoretical knowledge with real-world scenarios. Participation and collaboration during these sessions will be considered in the evaluation criteria for Homework, with feedback provided through the CMS.
Online Discussion Platforms: The CMS will feature a "Student Lounge" discussion board where students can discuss course-related topics, such as recognizing signs of social engineering or sharing strategies for preventing cyber threats. Random groups may be formed to facilitate structured peer interactions, and tools such as Wikis, Blogs, and Journals will be used to create collaborative content, like case study analyses or prevention guidelines. This setup supports the MOI for Discussion by fostering continuous peer-to-peer engagement and aligns with the MOE for Homework, with students receiving feedback on the quality and depth of their contributions.

Explain how the course will incorporate instructor-to-student interaction.

Course Introduction Package: At the course's outset, students will receive a personalized welcome letter and orientation video from the instructor. The video will cover key course components, such as the structure of the Final Project on Cisco Router Configuration and Password Recovery, assignment expectations, and navigating the CMS. This approach ensures that students have a clear understanding of the course requirements and aligns with the MOI for Lecture, helping to set the stage for a supportive learning environment.
Weekly Updates: The instructor will post weekly announcements in the CMS to highlight important concepts covered in lectures, such as the role of configuration registers in router behavior, and remind students about upcoming tasks like submitting the One-Page Report on Social Engineering Prevention. These updates are part of the MOE for Homework, ensuring students stay informed and engaged with the course's progression.
Interactive Discussion Platforms: Dedicated discussion boards for each unit will enable students to pose questions and seek clarification on topics, such as recognizing different types of social engineering techniques. The instructor will participate in these discussions to provide guidance, reinforcing the MOI for Discussion. Feedback will be given through the CMS within one week, in line with the MOE for Exams/Tests, ensuring timely reinforcement of learning.
Accessible Support Channels: The instructor will hold regular virtual office hours and be available via email for personalized support, especially regarding complex assignments like the Final Project on Cisco Router Password Recovery. This aligns with the MOE for Comprehensive Final Exam, allowing students to receive one-on-one feedback to help them refine their understanding and project deliverables.

Explain how the course will incorporate student-to-content interaction.

Interactive Lecture Sessions: Online lectures will incorporate interactive segments, such as "test your knowledge" quizzes on social engineering prevention methods or password recovery techniques for Cisco routers. These quizzes will offer immediate feedback, helping students assess their understanding before moving forward. This approach aligns with the MOI for Lecture by encouraging active learning and adhering to universal design principles for accessibility. Evaluation will focus on participation and comprehension, similar to the MOE for Exams/Tests.
Educational Video Clips: Supplementary video content will be provided to reinforce critical concepts, such as recognizing signs of social engineering or understanding router configuration settings. Each clip will include closed captions and transcripts to ensure accessibility, supporting the MOI for Observation and Demonstration. These clips will complement the Writing Assignment on Social Engineering, where students will analyze various cases based on what they learned from the videos.
Application Exercises and Practice Materials: Students will have access to problem sets, practice exams, and real-world scenarios, such as designing a password recovery procedure for a Cisco router. These resources will help them apply course concepts and prepare for the Comprehensive Final Exam. The exercises will follow the MOE for Homework, allowing students to receive feedback on their practice work to improve their performance on graded assessments.

Explain how the course will incorporate student-to-self interaction (metacognitive).

Reflective Self-Evaluation: After completing significant tasks, such as the Case Study Analysis on Social Engineering Targeting Vulnerable Communities, students will submit self-assessments reflecting on their learning progress, strengths, and areas for improvement. This practice aligns with formative evaluation methods by encouraging students to take ownership of their learning journey and develop metacognitive skills.

Diverse Problem-Solving Approaches: Assignments will prompt students to explore different strategies for solving cybersecurity challenges. For instance, when working on the Final Project on Cisco Router Configuration, students will be encouraged to document various approaches they considered for password recovery and reflect on why certain techniques were more effective. This aligns with the MOI for Observation and Demonstration by promoting flexible thinking and metacognitive development, with evaluation following the criteria for Homework and considering the depth of self-reflection and problem-solving insights.

Key: 1092