Prifysgol Wrecsam
Wrexham University

Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory

Module Code	COM490
Module Title	CCNA - Enterprise Networking, Security and Automation
Level	4
Credit value	20
Faculty	FAST
HECoS Code	100365
Cost Code	GACP

Programmes in which module to be offered

Programme title	Is the module core or option for this programme
Stand-alone module aligned to BSc (Hons) Cyber Security for QA and assessment	Option

Pre-requisites

Breakdown of module hours

Learning and teaching hours	18 hrs
Placement tutor support	0 hrs
Supervised learning e.g. practical classes, workshops	18 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total active learning and teaching hours	**36** hrs
Placement / work based learning	0 hrs
Guided independent study	164 hrs
Module duration (total hours)	**200** hrs

For office use only	
Initial approval date	08/11/2023
With effect from date	Aug 2024
Date and details of revision	

For office use only	
Version number	1

Module aims

This module introduces the architecture, structure, functions, components and models of computer networks and the Internet. The Cisco Certified Network Associate (CCNA) - CCNA - CCNA - Enterprise Networking, Security and Automation material is the focus of study for this module. It uses the OSI and TCP layered models to examine the nature and roles of protocols and services at the application, network, data link and physical layers. The module delves into routing protocols, placing emphasis on the core concept of routing within networks and the internet. The goal is to provide a comprehensive understanding of routing principles and practices. Explore the principles and methodologies of designing scalable and reliable enterprise networks. Students will learn about network design considerations, including redundancy, fault tolerance, load balancing, and quality of service (QoS). Provide an overview of emerging trends and technologies in enterprise networking, security, and automation. This may include topics such as cloud networking, software-defined networking (SDN), network virtualization, containerization, and Internet of Things (IoT) security.

Module Learning Outcomes - at the end of this module, students will be able to:

1	Explain the principles and concepts of enterprise networking, including network design, architecture and scalability.
2	Demonstrate different network security threats and vulnerabilities in enterprise environments.
3	Explain the importance of network security controls and best practices for securing enterprise networks.
4	Apply the fundamentals of network automation and its role in managing and optimizing enterprise networks.
5	Demonstrate network automation tools and technologies, such as scripting languages, APIs, and network management platforms.

Assessment

Indicative Assessment Tasks:

This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

The module will involve continuous assessment using portfolio tasks that revolves around real-world scenarios centred on modern networking technologies. Key assessment tasks will focus on network design, implementation, and testing. The operation of switches, routers and wireless technologies will be the focus of the assessments. This includes creating local

area networks with suitable IP addressing schemes and configuring switches and routers to establish connectivity within a network topology.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	1, 2, 3, 4, 5	Portfolio	100%

Derogations

None

Learning and Teaching Strategies

In line with the Active Learning Framework, this module will be blended digitally with both a VLE and online community. Content will be available for students to access synchronously and asynchronously and may indicatively include first and third-party tutorials and videos, supporting files, online activities any additional content that supports their learning.

As this module progresses, the strategies will change to best support a diverse learning environment. Initially, the module will start with a heavier reliance on engaging tutor-led lectures, demonstrations, and workshops to ensure that the students get the relevant threshold concepts. As the module continues experiential and peer learning strategies will be encouraged as the students' progress with their portfolio work.

Assessment will occur throughout the module to build student confidence and self-efficacy in relation to applied mathematical and technical concepts

Indicative Syllabus Outline

Yearly content will be updated to represent the most appropriate content for current industry technologies, but a list of indicative topics could include:

- OSPF Concepts and Configuration
  - OSPF operations
  - Single area OSPF
- Network Security
  - Current state of cybersecurity
  - Threat actors
  - Threat actor tools
  - Malware
  - Common network attacks
  - TCP and UDP vulnerabilities
  - Access Control Lists (ACLs)
- WAN Concepts
  - NAT for IPv4
  - VPN and IPsec
- QoS concepts
- Optimize, Monitor and Troubleshoot Networks
- IOS Image Management
- Emerging Network Technologies
- Cloud computing

- Network Virtualisation
- Controllers

Indicative Bibliography:

Please note the essential reads and other indicative reading are subject to annual review and update.

Essential Reads

Cisco Certified Network Associate (CCNA) – Switching, Routing, and Wireless Essentials

Other indicative reading

O. Wendell, CCNA 200-301 Official Cert Guide Library: Advance Your It Career with Hands-On Learning, Cisco Press, 2020

L. Peterson, B. Davie, Computer Networks: A Systems Approach (The Morgan Kaufmann Series in Networking), Morgan Kaufmann, 2021