Module Specification

Introduction to Networking

Version: 2026-27, v1.0, Approved

Contents

Module Specification 1

Part 1: Information 2

Part 2: Description 2

Part 3: Teaching and learning methods 4

Part 4: Assessment 5

Part 5: Contributes towards 6

Part 1: Information

Module title: Introduction to Networking

Module code: UFCEYD-10-1

Level: Level 4

For implementation from: 2026-27

UWE credit rating: 10

ECTS credit rating: 5

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

Partner institutions: UWE Bristol International College

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: This module introduces the fundamentals of computer networking, focusing on basic concepts and practical skills. Students will learn about network types, topologies, and essential devices such as routers and switches. Core topics include wired and wireless media, the OSI and TCP/IP models, common protocols, and IP addressing with subnetting basics. The module also covers introductory network security principles, including firewalls and encryption. Through hands-on

activities, students will gain experience in configuring simple networks and using tools like Wireshark for protocol analysis and troubleshooting.

Features: UWEBIC Module Code: TBC

Educational aims: The aim of this module is to provide students with a solid foundation in computer networking principles and practices. It seeks to develop both theoretical understanding and practical skills in network design, configuration, and troubleshooting. By introducing key concepts such as communication protocols, addressing schemes, and network security, the module develops foundational skills in configuring and troubleshooting simple networks, preparing learners for further study in networking and cybersecurity studies.

Outline syllabus: This module introduces the fundamentals of computer networking and security. Core topics include:

Networking Basics: What is a network? Types: LAN, WAN, MAN, PAN

Network Topologies: Star, Bus, Ring, Mesh, Hybrid

Network Devices: Router, Switch, Hub, Access Point

Transmission Media: Wired (Twisted Pair, Coaxial, Fiber Optic) vs Wireless (Wi-Fi, Bluetooth)

Protocols and Models: OSI Model (7 layers), TCP/IP Model

Common Protocols: HTTP, FTP, SMTP, DNS, DHCP

IP Addressing: IPv4 vs IPv6, Subnetting basics

Network Security Basics: Firewalls, encryption, authentication

Linux for Networking & Cybersecurity: Introduction to Linux OS, basic commands for network configuration and security

Practical Skills: Wireshark for protocol analysis and troubleshooting

Part 3: Teaching and learning methods

Teaching and learning methods: Teaching on this module will combine tutor-led delivery of technical knowledge with interactive activities that reinforce understanding through practice. Inputs will introduce core networking concepts, models, and processes, providing students with the theoretical foundation needed to design and configure networks. These sessions will be complemented by guided discussions to encourage critical thinking about real-world networking scenarios.

Practical activities will form a significant part of the learning experience, enabling students to apply concepts through hands-on exercises. Problem-solving tasks and troubleshooting exercises will help students develop confidence in applying networking principles.

Formative feedback will be embedded throughout the module, particularly during practical sessions. Tutors will provide constructive, real-time feedback, helping students refine both their technical skills and their acquisition of conceptual knowledge. This iterative process ensures that learners build towards success in the summative assessment, demonstrating attainment of all learning outcomes.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Describe fundamental networking principles and how common communication protocols support secure network operations.

MO2 Describe key networking devices, models (e.g. OSI/TCP/IP), and technologies used in network infrastructures.

MO3 Design and implement IP addressing schemes and configure small networks with basic security measures.

MO4 Apply practical skills to build, troubleshoot, and analyse networks using tools such as Wireshark and Linux commands.

Hours to be allocated: 100

Contact hours:

Independent study/self-guided study = 70 hours

Face-to-face learning = 30 hours

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://uwe.rl.talis.com/index.html

Part 4: Assessment

Assessment strategy: Students are required to complete a series of formative tasks designed to support progress toward the final scenario-based written assignment. Formative activities will include structured checkpoints for network design and configuration, providing timely feedback linked to the module learning outcomes.

The summative assessment consists of an individual written submission requiring clear demonstration of network design, configuration steps, and analysis using appropriate tools such as Wireshark. By engaging with key concepts such as communication protocols, addressing schemes, and network security, students will demonstrate their ability to apply networking fundamentals to real-world scenarios and develop essential technical competencies for further study in networking and cybersecurity.

The reassessment task will be equivalent to the first-sit assessment task.

Assessment tasks:

Written Assignment (First Sit)

Description: Written assignment (individual) – scenario-based assessment design, implement, and analyse a simple network with some security features (nominally 1000 words).
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO4

Written Assignment (Resit)
Description: Written assignment (individual) – scenario-based assessment design, implement, and analyse a simple network with some security features (nominally 1000 words).
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO4

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Digital Forensics {with International Year One}[UWEBIC] BSc (Hons) 2026-27

Cyber Security and Digital Forensics {with International Year One}[UWEBIC] BSc (Hons) 2026-27