MODULE SPECIFICATION

Part 1: Information			
Module Title	Networking		
Module Code	UFCFDU-30-1	Level	Level 4
For implementation from	2020-21		
UWE Credit Rating	30	ECTS Credit Rating	15
Faculty	Faculty of Environment & Technology	Field	
Department	FET Dept of Computer Sci & Creative Tech		
Module type:	Standard		
Pre-requisites	None		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description

Overview: The aim of this unit is to provide students with knowledge of computer networking essentials, how they operate, protocols, standards, security considerations and a range of networking technologies.

It gives the students the knowledge and skills that they need for the planning, designing, implementation and management of computer networks and understanding of the network infrastructure capabilities and limitations.

Educational Aims: Contributes the networking element of foundation technical knowledge.

Outline Syllabus: You will cover:

network foundations, connections, internetworking, protocols, standards, performance, security and server virtualisation

fundamental building blocks (e.g. routers, switches, hubs, storage, transmission) and typical architectures (e.g. server/client, hub/spoke) of computer networks and the Internet

data and protocols and how they relate to each other

data formats and simple protocols in current use

failure modes in protocols

error control

network protocols in widespread use on the Internet and their purpose and relationship to each other, including the physical and data link layer – e.g., HTTP, SMTP, SNMP, TCP/IP, BGP, DNS, etc

network performance

virtualisation techniques

network monitoring and mapping

static and dynamic routing protocols

wireless network security

common types of security hardware and software which are used to protect systems e.g., firewalls, encryption for data at rest, encryption for communication, intrusion detection systems (IDS), intrusion protection systems (IPS), identity and access management (IDAM) tools, anti-virus, web proxy, application firewalls, cross domain components, hardware security module (HSM), trusted platform module (TPM), unified threat module (UTM)

how these may be used to deliver risk mitigation or implement a security case

benefits/limitations

considering the implicit assurance (including supplier assurance and considering the benefits and risks of open source options) of the component

residual risks

Teaching and Learning Methods: Lecture sessions cover the technical knowledge required. Designated practical work is included to ensure that apprentices have absorbed and understood the key principles involved.

Part 3: Assessment
This module is assessed by a combination of techniques: a presentation (30 minutes) and a report (3,000 words) . The report gives the students the opportunity to describe the functional and technical aspects of the project that they have undertaken. In the presentation, the focus is more discursive and is supported by a Q&A session in which students are encouraged to reflect on the their design and implementation choices and non-functional aspects of their project. Component A Presentation (30 minutes including Q&A) Students will be given a design requirement (including security) for a network along with an implementation. In the presentation they will: Explain how the given implementation and components function Explain how the given implementation meets, or does meet, the design requirement Propose changes to the given implementation to take account of scalability

Component B Practical Report (3,000 words)

Students will build a network to a given specification. They will be assessed through a written report detailing the selection of components, system configuration, optimisation, testing and troubleshooting. A conclusion will be required stating how well the implementation met the requirements.

At referral, students will address deficiencies in their main sit work, using assessment feedback to guide them.

First Sit Components	**Final Assessment**	**Element weighting**	**Description**
Presentation - Component A		60 %	30 minute presentation and Q&A session.
Report - Component B	✓	40 %	A report on the the practical networking project undertaken.
Resit Components	**Final Assessment**	**Element weighting**	**Description**
Presentation - Component A		60 %	Presentation followed by Q&A session, 30 minute in total.
Report - Component B	✓	40 %	A re-worked version of the original report.

Part 4: Teaching and Learning Methods

Learning Outcomes

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

Module Learning Outcomes	**Reference**
Design, build, configure, optimise, test and troubleshoot simple and complex networks.	MO1
Explain networking devices and operations.	MO2
Compare common networking principles and how protocols enable the effectiveness of networked systems.	MO3
Explain the impact of network topology, communication and bandwidth requirements.	MO4

Contact Hours

Independent Study Hours:	
Independent study/self-guided study	135
Total Independent Study Hours:	135
Placement Study Hours:	
Placement	75

	Total Placement Study Hours:	75
	Scheduled Learning and Teaching Hours:	
	Face-to-face learning	90
	Total Scheduled Learning and Teaching Hours:	90
	Hours to be allocated	300
	Allocated Hours	300
Reading List	*The reading list for this module can be accessed via the following link:* https://rl.talis.com/3/uwe/lists/B5A7E8F9-1D80-E959-6FA6-3B41E4B856C1.html	

Part 5: Contributes Towards
This module contributes towards the following programmes of study: BSc (Hons) Cyber Security Technical Professional (integrated degree) BSc (Hons) 2020-21