

Module Title:	Networking III	
Language of Instruction:	English	
Credits:	5	
NFQ Level:	7	
Module Delivered In	4 programme(s)	
Teaching & Learning Strategies:	A mix of traditional lectures, laboratory work and take-home projects will enable the learner to fully understand and practice the various networking concepts presented.	
Module Aim:	To develop the learners understanding of the architecture, components, operations, and security for large, complex networks, including wide area network (WAN) technologies.	
Learning Outcomes		
On successful completion of this module the learner should be able to:		
LO1	Explain how to mitigate threats and enhance network security using access control lists and security best practices.	
LO2	Install, configure and evaluate appropriate technologies and protocols for LAN interconnection and VPNs.	
LO3	Implement techniques to provide address scalability and secure remote access for WANs.	
Pre-requisite learning		
Module Recommendations		
This is prior learning (or a practical skill) that is recommended before enrolment in this module.		
8915	NETW	Networking: Switching and VLAN Concepts
8916	NETW	Networking: Wireless and Routing Concepts
Incompatible Modules		
These are modules which have learning outcomes that are too similar to the learning outcomes of this module.		
No incompatible modules listed		
Co-requisite Modules		
No Co-requisite modules listed		
Requirements		
This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed.		
No requirements listed		

Module Content & Assessment

Indicative Content

Dynamic Routing (20%)

Describe dynamic routing protocol features and characteristics (OSPF, RIP). Explain how single-area OSPF operates. Explain concepts for OSPF routing such as; Router IDs, Point-to-Point networks, Multiaccess networks, Default Route Propagation. Configure and verify single-area OSPF.

IP Services and Security (40%):

Configure and verify IP addresses using address assignment technologies (e.g. DHCP, NAT), Analysis, specify and apply Access Control Lists (ACLs)(e.g. named ACLs, numbered ACLs, standard ACLs, extended ACLs), Design, configure and verify Network Address Translation (NAT) for a given network (e.g. Static NAT, Dynamic NAT, PAT)

WAN technologies and protocols (20%):

Examine access network and core network function and technologies (e.g. DSL, cable, PPPoE, HFC and MPLS)

Virtual Private Networks (20%):

VPNs, site-to-site GRE tunnels, IPsec, remote access VPNs.

Assessment Breakdown

%

Continuous Assessment

25.00%

Project

75.00%

Continuous Assessment

Assessment Type	Assessment Description	Outcome addressed	% of total	Assessment Date
Case Studies	n/a	1,2,3	25.00	n/a

Project

Assessment Type	Assessment Description	Outcome addressed	% of total	Assessment Date
Project	n/a	1	10.00	Week 3
Project	n/a	1,2,3	30.00	Week 12
Project	Project Defence	1,2,3	35.00	Week 12

No Practical

No End of Module Formal Examination

SETU Carlow Campus reserves the right to alter the nature and timings of assessment

Module Workload

Workload: Full Time		
<i>Workload Type</i>	<i>Frequency</i>	<i>Average Weekly Learner Workload</i>
Lecture	12 Weeks per Stage	2.00
Laboratory	12 Weeks per Stage	2.00
Estimated Learner Hours	15 Weeks per Stage	5.13
Total Hours		125.00

Module Delivered In

Programme Code	Programme	Semester	Delivery
CW_KCCYB_B	Bachelor of Science (Honours) in Cyber Crime and IT Security	5	Mandatory
CW_KCCIT_B	Bachelor of Science (Honours) in Information Technology Management	5	Mandatory
CW_KCCYB_D	Bachelor of Science in Cybercrime and IT Security	5	Mandatory
CW_KCCSY_D	Bachelor of Science in Information Technology Management	5	Mandatory