

WM143-24 Networks, Communications and Cyber Defence

24/25

Department

WMG

Level

Undergraduate Level 1

Module leader

Hany Atlam

Credit value

24

Module duration

30 weeks

Assessment

100% coursework

Study location

University of Warwick main campus, Coventry

Description

Introductory description

The Internet and computer networks are now ubiquitous and a growing number of computing activities strongly depend on the correct operation of the underlying network. Networks, both fixed and mobile, are a key part of the computing environment of today and tomorrow. Many computing applications that are used today would not be possible without networks. This dependency on the underlying network is likely to increase in the future. This module develops a theoretical understanding of core networks and communications concepts, instantiation of these concepts in the dominant suite of protocols comprising Ethernet, Internet Protocol (IP), Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), the practical realisation of devices to operate these protocols (switches, routers and firewalls in particular) and the cyber consequences of the organisation and configuration of these devices.

Module aims

This module aims to equip students with the essential knowledge and skills required to understand and work with computer networks effectively by providing a solid grounding of core networks, communication concepts, and network cyber defence establishing a strong foundation for students in this field.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

The content of this module will be taught from a cyber security perspective.

- Introduction
- Networked applications
- Reliable data delivery
- Routing and forwarding
- Subnetting and VLSM
- Local area networks
- Resource allocation
- Mobility
- Network Security principles

Learning outcomes

By the end of the module, students should be able to:

- Articulate the key principles behind the organisation and operation of typical communication networks and layered protocols using domain terminology.
- Understand network designs for small to medium-sized businesses.
- Configure network devices to achieve the required operating characteristics.
- Outline network diagrams and implement appropriate addressing schemes at a sub-network level.
- Explain network behaviour from captured network traffic.
- Apply network security principles and best practices to enhance the security posture of networks.

Indicative reading list

Stallings, William. Computer Organization and Architecture, Global Edition, Pearson Education LTD (2022)

A, Jesin. Packet Tracer Network Simulator, Packt Publishing, Limited (2014).

Kurose, J., & Ross, K., " Computer Networking: A Top-Down Approach (7th Edition)". Pearson Education Limited (2016)

Howser, G. "Computer Networks and the Internet: A hands-on approach. Cham, Switzerland: Springer (2020)

Stallings, W., Brown, L., "Computer Security: Principles and Practice, Global Edition", Pearson Education Limited (2018)

[View reading list on Talis Aspire](#)

Subject specific skills

Students should be able to know:

- The process of planning, designing and managing computer networks with an overall focus on the services and capabilities that network infrastructure solutions enable in an organisational context.
- The fundamental building blocks (e.g. routers, switches, hubs) and typical architectures (e.g. server/client) of computers, networks and the Internet.
- The main features of routing and Internet network protocols in use, their purpose and relationship to each other, including the physical and data link layer (e.g. HTTP, SMTP, SNMP, TCP, IP, etc.).
- The main factors that affect network performance (e.g. the relationship between bandwidth, number of users, nature of traffic, contention).
- The ability to plan, design and manage computer networks with an overall focus on the services and capabilities that network infrastructure solutions enable in an organisational context.
- The issues that may arise in the day-to-day operation of networks and how to resolve them.
- The security configurations and best practices for maintaining a secure network.

Transferable skills

Students should be able to demonstrate:

- Problem-solving
 - Critical thinking
 - Communication Skills
 - Teamwork and Collaboration
 - Ethical Awareness
 - Leadership
-

Study

Study time

Type	Required
Supervised practical classes	48 sessions of 1 hour (20%)
Online learning (scheduled sessions)	30 sessions of 1 hour (12%)
Private study	66 hours (28%)
Assessment	96 hours (40%)
Total	240 hours

Private study description

Independent activity between workshops.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A2

	Weighting	Study time
Coursework 1	50%	48 hours
Students will prepare a written report to assess their knowledge and skills to apply the key principles of computer networks and how tools and techniques can be used to configure network devices.		
Coursework 2	50%	48 hours
Students will prepare a written report to assess their understanding of configuring network devices for a specific case study and explain network behaviour from captured network traffic.		

Feedback on assessment

Written feedback for each assignment
Verbal feedback during tutorial sessions
Solutions provided to tutorial questions
Summative feedback on assignments and exam

Availability

Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
 - Year 1 of H651 Cyber Security
 - Year 1 of H651 Cyber Security
 - Year 1 of H651 Cyber Security