Module Code:	**CMS 3408**
Module Title:	**NETWORK SECURITY AND MANAGEMENT**
Schools involved in delivery:	School of Computing and Engineering
Name of Course(s):	MSc Network Technology and Management MSc Internet Security
Module Leader:	Dr. David Wilson
Location for delivery:	Queensgate, Department of Informatics
Module Type:	Compulsory
Credit Rating:	15
Level:	M - Masters
Learning Methods:	Supervised Learning 36 hrs Directed Unsupervised Activity 114 hrs
Pre-requisites:	None
Recommended Prior Study:	None
Co-requisites:	None
Professional Body Requirements:	N/A
Barred Combinations:	None
Graded or Non Graded:	Graded

Module Synopsis
Whilst networks are now an integral part of organisations large and small, they still need to be managed and maintained. Technology in the IT industry changes fast and network managers need to keep up with or be ahead of those changes. This module offers an insight into the provision of contemporary network systems and the management decisions required to implement and maintain a successful network system. With the benefits to the organisation of local and wide area distribution of information over integrated networks comes the responsibility to protect the organisation and its stakeholders from outside interference. This module also serves to inform and investigate techniques for the security of network based systems. An additional benefit of this module is the optional Cisco accreditation scheme. The syllabus for the Network Security and Management module covers many aspects of the prior learning required for the Cisco examinations – an important certification scheme for potential network technicians and managers.

Outline Syllabus
Review and debate the key issues surrounding:

Prior learning for CISCO Accreditation
Wireless Networking Technologies
Design, construction, evaluation and management of large networks (enterprise level) – evaluation backbones, media types, interconnection devices, systems requirements, key criteria (e.g. performance/ cost/ security/ reliability/ traceability)
Planning/ management: capacity/ service level agreements and service level management/ risk assessment/ disaster planning and recovery.
Network Performance (QoS and DiffServ).
Network Management (SNMP).
UDP: Datagram Transport Service.
Network monitoring.
Intrusion detection
Honeynets
Log analysis
Network Security.
Queuing theory.
Egress filtering.
Border Gateway Protocol/Autonomous System Number
Analysing network packet data (packet crafting)
DNSSEC: Security Extensions for DNS

Learning Outcomes

1. Knowledge and Understanding Outcomes

Upon completion of this module the learner will have a critical awareness of:
1.1 The principles of resource allocation and management in networked computer systems.
1.2 The available strategies for the deployment and maintenance of networking solutions.
1.3 The varied technologies, standards, tools and components of a networked system.
1.4 Applied techniques for network security.

2. Ability Outcomes

Upon completion of this module the learner will be able to:
2.1 Identify and apply appropriate methods to support the development of an effective networking strategy;
2.2 Provide reasoned and well-argued recommendations on network provision to an organisation.
2.3 Implement effective security measures for the protection of network systems.

Assessment Strategy

Formative assessment

Feedback will be provided by means of observation of performance in tutorial and practical sessions with appropriate feedback from tutors. Formative feedback will also take place through students completing the class exercises during the tutorial and practical sessions. Informal feedback will be provided by both tutors and other students involved in discussions.

Summative Assessment

Assessment tasks (including assessment weightings)

Assignment One: An in-class Practical Demonstration (30% of the overall assessment for the module)

This assignment will involve the implementation of a security measure for specific elements of the network technology as indicated in the Outline Syllabus at the end of the module period through practical demonstration. This assignment will assess ability outcome 2.3.

Assignment Two: A Management Report (70% of the overall assessment for the module)
Assignment two is the final assessment for this module.

This report will be based on a series of activities involving the application of the technologies studied to given organisational scenarios. For example, students may be presented with the current network layout for an organisation and predicted requirements. They will then be asked to design and submit a specification for a new/upgraded networked system based on this information. This assignment will assess Learning Outcomes 1.1 to 2.2.

Assessment Criteria

Assignment One – Practical Demonstration: Quality of construction/design criteria/presentation of solution

At Pass level, the student will be able to demonstrate a good understanding of a security strategy relevant to the maintenance of a network infrastructure.

At Modal level, the student will be able to demonstrate the aforementioned but the solution will be complete and fully effective, all design criteria are met and justified plus a very clear, concise and well-argued presentation.

Assignment Two – Report: Quality of discussion, technical correctness, critical evaluation and quality of written work.

At Pass level, the student will be able to demonstrate a good understanding of the pertinent technology relating to the deployment of a network infrastructure.

At Modal level, the student will show an ability to think critically and make informed decisions based on knowledge of the technology and current research indicating the strengths and weaknesses of different approaches to implementing the technology.

Note:
Both assignments will be eligible for tutor reassessment.

Both assignments will be submitted for marking with an approved cover sheet containing the student's name, identity number and date of submission.

Learning Strategy
Teaching and learning methods will include pre-class reading as an important element of this module. Students are expected to direct their own learning, making professional use of resources and others as necessary. Use will be made of guest speakers and practitioners where appropriate. During the block period, there will be a series of lectures, seminars, tutorials and practicals. Lectures will present the academic concepts and major networking technologies. In tutorials and practicals students will be able to apply this knowledge to particular scenarios, and engage in group discussion and debate during seminars.

Appendix: Indicative References

Books (including e-books):

Bradford (2007) *The Art of Computer Networking*, Prentice-Hall

Burke (2003) Network Management: Concepts and Practice, a Hands-On Approach Prentice Hall.

Conti (2007) *Security Data Visualisation*, No Starch Press.

Day (2008) Patterns in Network Architecture: A Return to Fundamentals, Prentice-Hall

Farrel (2008) Network Management: Know It All, Kaufmann.

Fetig (2005) Twisted: Network Programming Essentials, O'Riley.

Forouzan (2006) Data Communications Networking, McGraw-Hill.

Kozierok (2005) The TCP/IP Guide: A Comprehensive Illustrated Internet Protocols Reference, No Starch Press.

Marty (2008) Applied Security Visualisation, Adison Wesley.

Peterson (2007) Computer Networks: A Systems Approach, Kaufmann.

Provos (2008) *Virtual Honeypots*, Adison Wesley,

Sanders (2007) Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems, No Starch Press.

Stevens (1994) TCP/IP Illustrated: Protocols v. 1: The Protocols (APC), Addison Wesley.