Higher National Unit Specification

General information

Unit title: Computer Networking: Concepts, Practice and Introduction to Security (SCQF level 7)

Unit code: J0HJ 34

Superclass: CA

Publication date: August 2018

Source: Scottish Qualifications Authority

Version: 02

Unit purpose

The purpose of this unit is to introduce learners to the basic components of contemporary Local Area Networks (LAN). Learners will gain the underpinning knowledge of how data is transmitted from one location to another. Learners will also gain practical experience of implementing a client server LAN using industry-standard equipment and protocols.

This is a **specialist unit**, intended for learners who have an interest in cyber security. The unit is appropriate for learners undertaking an HNC in Cyber Security or a related HN level course in the Computing framework. The knowledge and skills covered will allow learners to understand contemporary networks, including the detail of how these networks pass information and how to identify the technology used in this communication.

At the completion of this unit, the learner will know how to capture traffic/packets sent between network devices and will have developed an understanding of implementing basic security within a LAN environment.

Outcomes

On successful completion of the unit, the learner will be able to:

1 Describe OSI and TCP/IP models and encapsulation/decapsulation process.
2 Create a client server switched local area network, with secure endpoints.
3 Create a secure wireless network.
4 Capture the transmitted/received data using network sniffer technology.

Higher National Unit Specification

General information

Unit title: Computer Networking: Concepts, Practice and Introduction to Security (SCQF level 7)

Credit points and level

1 Higher National unit credit at SCQF level 7: (8 SCQF credit points at SCQF level 7)

Recommended entry to the unit

No previous knowledge or experience is required. However, it would be beneficial, albeit not essential, if learners possessed knowledge of local area networks and some of the commonly used technology and terminology, used in local area networks.

Core Skills

Achievement of this Unit gives automatic certification of the following Core Skills component:

Complete Core Skill	None
Core Skill component	Critical Thinking at SCQF level 5

There are also opportunities to develop aspects of Core Skills which are highlighted in the Support Notes of this Unit specification.

Context for delivery

If this unit is delivered as part of a group award, it is recommended that it should be taught and assessed within the subject area of the group award to which it contributes.

It is suggested that this unit is delivered as part of the HNC Cyber Security. It is also advisable that the unit is taught along with other relevant units. For example, learners could use skills that are learned in this unit within J0HE 34 *Securing Network Devices*, and enhance the practical knowledge gained in this unit with the practical knowledge they will gain with J0HE 34 *Securing Network Devices*.

The Assessment Support Pack (ASP) for this unit provides assessment and marking guidelines that exemplify the national standard for achievement. It is a valid, reliable and practicable assessment. Centres wishing to develop their own assessments should refer to the ASP to ensure a comparable standard. A list of existing ASPs is available to download from SQA's website **(http://www.sqa.org.uk/sqa/46233.2769.html)**.

Equality and inclusion

This unit specification has been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners should be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence.

Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**.

Higher National Unit Specification: Statement of standards

Unit title: Computer Networking: Concepts, Practice and Introduction to Security (SCQF level 7)

Acceptable performance in this unit will be the satisfactory achievement of the standards set out in this part of the unit specification. All sections of the statement of standards are mandatory and cannot be altered without reference to SQA.

Where evidence for outcomes is assessed on a sample basis, the whole of the content listed in the knowledge and/or skills section must be taught and available for assessment. Learners should not know in advance the items on which they will be assessed and different items should be sampled on each assessment occasion.

Outcome 1

Describe OSI and TCP/IP models and encapsulation/decapsulation process.

Knowledge and/or skills

- Seven layered OSI model and the PDU encapsulation/decapsulation process
- Four layered TCP/IP protocol suite
- Encryption techniques used to ensure confidentiality of data transfer
- Checksum techniques used to ensure integrity of data transfer
- Internetworking devices and their operating characteristics
- MAC addressing
- IPv4 and IPv6 logical addressing
- Contemporary secure protocols

Outcome 2

Create a client server switched local area network, with secure endpoints.

Knowledge and/or skills

- Basic IP addressing, naming of hosts
- Switched networks
- Basic endpoint hardening
- Basic network functions (directory services, name resolution, DHCP)
- Authentication of clients/users to server

Outcome 3

Create a secure wireless network.

Knowledge and/or skills

- Wireless media/devices
- Wireless authentication methods
- Wireless encryption methods
- Wireless MAC address filtering

Higher National Unit Specification: Statement of standards (cont)

Unit title: Computer Networking: Concepts, Practice and Introduction to Security (SCQF level 7)

Outcome 4

Capture the transmitted/received data using network sniffer technology.

Knowledge and/or skills

- Data exchange between two hosts
- Secured and non-secured packet traffic
- Wireless traffic, both secured and non-secured

Evidence requirements for this unit

Learners will need to provide evidence to demonstrate the knowledge and/or skills across all outcomes. The evidence requirements for this unit will take two forms.

1 Knowledge evidence (Outcome 1)
2 Product evidence (Outcomes 2, 3 and 4)

The **knowledge evidence** will relate to Outcome 1. Knowledge evidence will be required for all knowledge and/or skills statements in Outcome 1. The following knowledge must be demonstrated:

- How data communications occur with specific reference to the theoretical seven layered OSI model and the PDU encapsulation and decapsulation process
- The relationship between the OSI model and the practically implemented four layered TCP/IP protocol suite
- Encryption techniques used to ensure confidentiality of data transfer
- Checksum techniques used to ensure integrity of data transfer
- Internetworking devices and their operating characteristics
- Structure and importance of MAC addressing
- Structure of IPv4 and IPv6 logical addressing
- Common secure protocols

Sampling may be permissible when a traditional test is used. When testing is used, it must be under supervised conditions and it must be controlled in terms of location and timing. Access to reference material is not permitted.

The knowledge evidence may be written or oral or a combination of these. Evidence may be captured, stored and presented in a range of media (including audio and video) and formats (analogue and digital).

The **product evidence** will relate to Outcomes 2, 3 and 4. It will demonstrate that the learner has a vocational ability to carry out the following practical elements of this unit, and produce documentation/evidence to show their vocational skills.

Higher National Unit Specification: Statement of standards (cont)

Unit title: Computer Networking: Concepts, Practice and Introduction to Security (SCQF level 7)

The **product evidence** is required to demonstrate that the learner can:

- Set up and configure (naming and IP address) a small switched LAN network that includes **at least** one client and one server
- Install/configure endpoint hardening technology, such as firewalls, anti-virus, and latest updates
- Configure basic directory services, name resolution, and DHCP
- Create network user accounts
- Authenticate network users
- Identify suitable wireless device for integration into practical tasks in Outcome 2
- Implement a wireless network to include securing the network using suitable authentication, encryption methods — user and device authentication should be implemented
- Use suitable network analysis tools, capture and show DHCP traffic (or other suitable communication between two hosts)
- Use suitable network analysis tools, capture and show the difference between secure and non-secure FTP traffic (or other protocols that can be sent secured and non-secured)
- Use suitable network analysis tools, capture and show the difference between wireless traffic, both non-secure and secure

This evidence may be produced over the life of the unit, under controlled conditions (including access to reference materials). Authentication will be necessary (see below).

The SCQF level of this unit (level 7) provides additional context on the nature of the required evidence and the associated standards. The following level descriptors are particularly relevant to the evidence.

- Demonstrate and/or work with:
  - overall appreciation of the body of knowledge that constitutes a subject/discipline/sector
  - knowledge that is embedded in the main theories, concepts and principles of the subject/discipline/sector
  - an awareness of the dynamic nature of knowledge and understanding
- Apply knowledge, skills and understanding:
  - in practical contexts
  - in using some of the basic and routine professional skills, techniques, practices and/or materials associated with the subject/discipline/sector
  - to practise these in both routine and non-routine contexts

These level descriptors should be used (explicitly or implicitly) when making judgements about the evidence.

When evidence is produced in uncontrolled or loosely controlled conditions, it must be authenticated. The Guide to Assessment provides further advice on methods of authentication.

The support notes section of this specification provides specific examples of instruments of assessment that will generate the required evidence.

Higher National Unit Support Notes (cont)

Unit title: Computer Networking: Concepts, Practice and Introduction to Security (SCQF level 7)

Unit support notes are offered as guidance and are not mandatory.

While the exact time allocated to this unit is at the discretion of the centre, the notional design length is 40 hours.

Guidance on the content and context for this unit

This unit will introduce learners to the basic components of contemporary Local Area Networks (LAN). Learners will gain the underpinning knowledge of how data is transmitted from one location to another. Learners will also gain practical experience of implementing a client server LAN, with wireless, using industry-standard equipment and protocols. Learners will learn how to capture the traffic/packets sent between network devices. Learners will also gain an understanding of implementing basic security within a LAN environment.

This is a **specialist** unit, intended for learners who have an interest in cyber security. It is particularly suitable for learners who have to understand contemporary networks including the detail of how these networks pass information and how to identify the technology used in this communication.

Please note that the following guidance, relating to specific outcomes, does not seek to explain each knowledge/skills statement, which is left to the professionalism of the teacher. It seeks to clarify the statement of standards where it is potentially ambiguous. It also focuses on non-apparent teaching and learning issues that may be over-looked, or not emphasised, during unit delivery. As such, it is not representative of the relative importance of each knowledge/skill.

Outcome 1

This outcome relates to the underpinning knowledge of what a network is, what devices exist within contemporary networks. The outcome also covers a knowledge of how data is transmitted from one location to another. The teaching and learning within this outcome should highlight that the securing of network devices and data transmission does exist, and that the proper implementation of these features can aid in protecting the network against basic attacks that will inevitably happen. Coverage of protocols which have built in security should be discussed.

It may be possible to present some of the knowledge and skills of Outcome 1 alongside the practical elements of Outcomes 2, 3 and 4. If this is the case, then it is suggested that the summative assessment for Outcome 1 is carried out towards the end of the unit.

It is important that learners develop basic knowledge of the encapsulation/decapsulation process and how IP addressing and MAC addressing is used within these processes. Learners should be made aware of data integrity and encryption techniques that are designed into the TCP/IP protocol stack.

Popular network security protocols include Secure Shell (SSH), Secure File Transfer Protocol (SFTP), Secure Hypertext Transfer Protocol (HTTPS), Secure Socket Layer (SSL), and Internet Protocol Security (IPSEC) should also be covered.

Higher National Unit Support Notes (cont)

Unit title: Computer Networking: Concepts, Practice and Introduction to Security (SCQF level 7)

Outcome 2, 3 and 4

These three outcomes are practical in nature. However, this does not preclude learners gaining underpinning knowledge relating to the specific tasks being carried out. The unit design allows for a holistic approach to these three outcomes. This can be carried out within a virtual environment or within real hardware (depending on the centre's resource availability). In the event that a virtual environment is used, then the wireless element will typically have to reside external to the virtual environment. The bridging of the virtual environment to the wireless environment is possible using basic wireless dongles on a standard workstation that has virtualisation software installed. At the time of writing there are many examples of virtualisation software than can be used for this purpose (Vmware Workstation, VMware player, Oracle Virtualbox, Microsoft hyper-V to name but a few). The wireless element can be implemented using standard Wireless Access Points, or equivalents such as a Raspberry Pi configured as an AP.

The local area network setup can be virtual, providing that the learner is aware that the virtualisation software uses virtual switches instead of real physical switches.

With regard to the use of packet sniffers or traffic analysers, the most widely used tool for carrying out network packet sniffing, at the time of writing, is Wireshark; if using **https://www.wireshark.org/download.html** as a resource, educators should be aware that the learners will, most likely, have never used them before. Therefore, their use within this unit should be understood as an introduction. This will involve their installation (ie, where to install) and using the tools' filtering mechanisms to identify protocols that are being studied within the unit (in this unit, it has been suggested that it will be DHCP, FTP and wireless traffic, typically the capturing of wireless data, such as SSID and Passwords — depending on the encryption being used). However, other protocols may be used if they allow the collection of the traffic examples required.

There are some National Occupational standards (NOS) to which this unit can relate to. This unit itself will not cover complete NOS standards. However, the content could contribute towards the larger NOS requirements, if taught with reference to organisational security requirements:

- TECIS60541: Carry out operational information security management activities
- TECIS60341: Carry out information security architecture activities
- TECIS60331: Contribute to information security architecture activities
- ESKITU051: Configure digital systems
- TECIS60533: Contribute to information security identity and access management activities

Guidance on approaches to delivery of this unit

The recommended sequence of delivery would be Outcome 1, followed by a holistic approach to the rest of the learning outcomes.

Outcome 1 will typically be delivered using traditional teaching and learning methods, such as lecture, classroom paper-based research, online investigations, and online videos.

Higher National Unit Support Notes (cont)

Unit title: Computer Networking: Concepts, Practice and Introduction to Security (SCQF level 7)

Outcomes 2, 3 and 4 are practical in nature. These may be deployed as practical lab exercises, or as part of a larger case study that requires the implementation of a secured client server network with inclusion of wireless technology. Visits into most colleges'/schools' IT infrastructure would benefit the learners in seeing how the wired and wireless LAN technologies co-exist.

Demonstration and/or step-by-step guides could be used to allow learners to complete the practical elements of this unit. If resources are at a premium, group work could be used for the practical. However, it is essential that the authenticity of assessment evidence is maintained, this could be helped by the use of differing subnet assignments and computer/domain names being specific to each learner/group.

Except for the wireless elements, all of the other practical elements can be carried out within a virtual environment (providing that the learners are aware of what and how physical switches and routers operate). The virtual environment can be 'bridged' out of the virtual environment and into the physical network to allow integration of the wireless along with the virtual hosts. Innovative ways of integrating wireless technology exist, which allow the wireless element to co-exist with the virtual element within a classroom environment. This would provide an enriched learning experience for the learners.

A suggested distribution of time, across the outcomes, is:

Outcome 1: 10 hours
Outcome 2: 10 hours
Outcome 3: 10 hours
Outcome 4: 10 hours

Summative assessment may be carried out at any time. However, when testing is used (see evidence requirements) it is recommended that this is carried out towards the end of the unit (but with sufficient time for remediation and re-assessment). When continuous assessment is used (such as the use of a web log), this could commence early in the life of the unit and be carried out throughout the duration of the unit.

There are opportunities to carry out formative assessment at various stages in the unit. For example, formative assessment could be carried out on the completion of each outcome to ensure that learners have grasped the knowledge contained within it. This would provide assessors with an opportunity to diagnose misconceptions, and intervene to remedy them before progressing to the next outcome.

Guidance on approaches to assessment of this unit

Evidence can be generated using different types of assessment. The following are suggestions only. There may be other methods that would be more suitable to learners.

Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met. Where learners experience a range of assessment methods, this helps them to develop different skills that should be transferable to work or further and higher education.

Higher National Unit Support Notes (cont)

Unit title: Computer Networking: Concepts, Practice and Introduction to Security (SCQF level 7)

Evidence for Outcome 1 could be in the form of a 20 multiple-choice question assessment. This assessment should be closed-book and time-limited to 60 minutes. This assessment could be carried out electronically or it could be paper-based, providing that the closed-book requirement is maintained. Successful completion will be deemed as gaining 60% of the answers correct (12 correct out of 20).

Evidence for Outcomes 2, 3 and 4 will be product evidence. Learners will be required to show that they are able to configure the listed items within the knowledge and skills section of each outcome. This could be done using electronic submissions (vlog, blog, video, screenshots within a pro-forma document) or written evidence.

Authentication of learner evidence should be ensured eg, providing each learner/group with a different subnet address or different names for the computers to ensure authenticity of learners' work.

Other methods of ensuring authenticity exist, such as Turnitin (a commonly used plagiarism tool used alongside Moodle VLE's to check learners' work against locally submitted work as well as internet materials).

Formative assessment could be used to assess learners' knowledge at various stages throughout the life of the unit. An ideal time to gauge their knowledge would be at the end of each outcome. This assessment could be delivered through an item bank of selected response questions, providing diagnostic feedback to learners (when appropriate).

If a blog is used for summative assessment, it would also facilitate formative assessment since learning (including misconceptions) would be apparent from the blog, and intervention could take place to correct misunderstandings on an on-going basis.

Opportunities for e-assessment

E-assessment may be appropriate for some assessments in this unit. By e-assessment we mean assessment which is supported by Information and Communication Technology (ICT), such as e-testing or the use of e-portfolios or social software. Centres which wish to use e-assessment must ensure that the national standard is applied to all learner evidence and that conditions of assessment as specified in the evidence requirements are met, regardless of the mode of gathering evidence.

The most up-to-date guidance on the use of e-assessment to support SQA's qualifications is available at **www.sqa.org.uk/e-assessment**.

Opportunities for developing Core and other essential skills

This Unit has the Critical Thinking component of Problem Solving embedded in it. This means that when learners achieve the Unit, their Core Skills profile will also be updated to show they have achieved Critical Thinking at SCQF level 5.

History of changes to unit

Version	Description of change	Date
02	Core Skills Component Critical Thinking at SCQF level 5 embedded.	31/08/18

General information for learners

Unit title: Computer Networking: Concepts, Practice and Introduction to Security (SCQF level 7)

This section will help you decide whether this is the unit for you by explaining what the unit is about, what you should know or be able to do before you start, what you will need to do during the unit and opportunities for further learning and employment.

This unit is designed to introduce you to the basic components of contemporary Local Area Networks (LAN). You will gain practical experience of implementing a client server local area network, including wireless technology, using industry-standard equipment and protocols. You will also learn how to collect the traffic/packets that are sent between clients and servers when using specific technology.

This is a **specialist unit**, intended for learners who have an interest in cyber security. It is particularly suitable for learners who have to understand contemporary networks including the detail of how these networks pass information and how to identify the technology used in this communication.

The unit consists of four outcomes. The first outcome is theoretical in nature, aimed at providing the underpinning knowledge of how networks operate and transmit data from one location to another. Within this outcome, you will learn about the various devices used in networks to allow this data transmission to take place. You will also learn about the contemporary addressing methods being used in networks. You will also learn about common protocols that have security designed into them.

Outcome 2 is practical in nature and will allow you to build a small wired network, set up basic security on the endpoints (servers/clients) of the network. This will be expanded upon in Outcome 3 with the addition of wireless technology set-up and configuration.

In Outcome 4 you will have the opportunity to utilise network sniffer software to look at and understand how some of the basic protocols are sent across the network as well as how they look when specific types of security have been added to the protocols.

The assessment will be carried out in two parts. Part one will be to cover Outcome 1 and this will be a closed-book assessment. Part two may require you to produce a record/log of the steps you have taken to build and configure the wired and wireless networks, as well as a section explaining how you have captured the data packets on the network.

This unit will provide you with the basic underpinning knowledge and skills for understanding how network devices communicate, and how you can obtain the detail of the packet transmission. The unit is suitable as a basis for multiple units within the HNC in Cyber Security, in particular J0HE 34 *Securing Network Devices*.

On completion of this unit, you may be able to progress the HND Cyber Security or another related HN level course.

This Unit has the Critical Thinking component of Problem Solving embedded in it. This means that when you achieve the Unit, your Core Skills profile will also be updated to show you have achieved Critical Thinking at SCQF level 5.