Higher National Unit Specification

General information for centres

Unit title: Internetworking Concepts 2: Security and Business Concepts

Unit code: DF9V 34

Unit purpose: This Unit is designed to introduce candidates to the issues involved in using, configuring and describing the key components of internetworking technologies in a business context. It is intended for candidates undertaking an HNC or HND in Computing, Computer Networking or a related area who require a broad knowledge of internetworking technologies.

On completion of the Unit candidates should be able to:

1. Describe internetworking concepts.
2. Describe internetworking security.
3. Describe internetworking business concepts.

Credit value: 1 HN Credit at SCQF level 7 (8 SCQF credit points at SCQF level 7)

**SCQF credit points are used to allocate credit to qualifications in the Scottish Credit and Qualifications Framework (SCQF). Each qualification in the Framework is allocated a number of SCQF credit points at an SCQF level. There are 12 SCQF levels, ranging from Access 1 to Doctorates.*

Recommended prior knowledge and skills: Access to this Unit will be at the discretion of the Centre. There are no specific requirements but candidates would benefit from knowledge of computer hardware and software. This may be demonstrated by the possession of HN Units such as DG0K 33 Hardware Concepts, DF9L 33 Operating System Concepts, DF9P 34 Network Concepts and DF9T 34 Internetworking Concepts 1: Development and Delivery Concepts.

Core skills: There may be opportunities to gather evidence towards core skills in this Unit, although there is no automatic certification of core skills or core skills components.

Context for delivery: This Unit is included in the framework of a number of HNC and HND group awards. It is recommended that it should be taught and assessed within the context of the particular group award to which it contributes.

Assessment: Evidence for the knowledge and/or skills for the entire Unit must be produced using a set of 30 restricted-response questions to assess candidates' knowledge and understanding. This may be administered as a single end-of unit test, or as several subtests, each covering one or more outcomes.

Candidates must answer at least 70% of the questions correctly in order to obtain a pass. If subtests are used, they must also score at least 70% in each subtest.

General information for centres (cont)

Testing must take place in a closed-book environment where candidates have no access to books, handouts, notes or other learning material. Testing can be done in either a machine-based or paper-based format and must be invigilated by a tutor or mentor. There must be no communication between candidates and communication with the invigilator must be restricted to matters relating to the administration of the test.

If a candidate requires to be reassessed, a different selection of questions must be used. At least half the questions in the reassessment must be different from those used in the original test.

If an outcome has a practical component, this must be assessed by having the candidate use a logbook to record the practical tasks successfully completed. The logbook can be in paper or electronic form and must be authenticated by the tutor or mentor.

For some outcomes only a sample of the practical tasks needs to be completed and recorded for assessment purposes, e.g. three out of five. This is clearly indicated in the logbook instructions for the outcomes involved. Where this occurs, tutors must inform candidates of the tasks to be completed.

An Assessment Exemplar and Guidelines on the Delivery of the Unit have been produced to indicate the national standard of achievement required at SCQF level 7.

Higher National Unit specification: statement of standards

Unit title: Internetworking Concepts 2: Security and Business Concepts

Unit code: DF9V 34

The sections of the Unit stating the Outcomes, knowledge and/or skills, and evidence requirements are mandatory.

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. Candidates 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 Internetworking concepts

Knowledge and/Or Skills

- Internet infrastructure
- Connectivity problems
- Domain names and DNS
- Remote access protocols
- Application of protocols or services to their corresponding server
- Diagnostic tools
- Hardware and software connection devices
- Site monitoring procedures
- Networking topologies
- Application server providers

Evidence requirements

Restricted response test

The knowledge and skills component of Outcome 1 must be examined by twelve questions, derived from the 10 items listed below. One question must be derived from eight of the items and two questions from each of the two remaining items. Each question must be derived from a single item.

1. Internet infrastructure.

   Access points, backbone, hardware/software infrastructure, internetworking devices.

2. Connectivity problems

   From source to destination, relating to server roles, firewalls.

Higher National Unit specification: statement of standards (cont)

Unit title: Internetworking Concepts 2: Security and Business Concepts

3. Domain names and DNS

   Entry types, hierarchical structure, root domain servers, top level domains, Nslookup

4. Remote access protocols.

   SLIP, PPP, PPTP, L2TP, PPPOE, point-to-point, multi-point

5. Application of protocols and services to their corresponding server

   POP3, SMTP, HTTP, FTP, NNTP, LDAP and Telnet

6. Diagnostic tools

   Ping, winipcfg, ipconfig, ifconfig, ARP, tracert and Network Analyzer

7. Hardware and software connection devices

   Bridge, Brouter, Router, Switch, Repeater, Hub, Network Adapter, Cable Modem, *x*DSL Modem, Modem, CSU/DSU, Firewall, NAT server and Proxy Server

8. Describe the use of site monitoring procedures.

   Server log files, network traffic, server utilization, network bandwidth utilization

9. Networking topologies

   Star, Bus, Mesh and Ring

10. Application server providers.

    Web Hosting, e-mail services, fax services, web access to an application, shared access to expensive hardware.

The test may be administered on its own as a subtest or be combined with other outcome subtests in the Unit.

Alternatively, the 12 questions for this outcome may contribute towards a single end-of-unit test of 30 questions.

Higher National Unit specification: statement of standards (cont)

Unit title: Internetworking Concepts 2: Security and Business Concepts

Logbook

The logbook for Outcome 1 must record successful completion by the candidate of **both** the tasks listed below:

- Diagnostic tools

  Documentary evidence that the candidate can use at least five of the following diagnostic tools: ping, winipcfg, ipconfig, ifconfig, ARP, tracert and Network Analyzer

- Hardware and software connection devices

  The candidate must use tracert to determine the route to a remote host, then draw a logic diagram indicating a possible configuration of connection devices between the workstation and the host. The devices indicated must be selected from the following list: bridge, brouter, router, switch, repeater, hub, network adapter, cable modem, xDSL modem, modem, CSU/DSU, firewall, NAT server and proxy server

Assessment guidelines

It is suggested that all the above concepts be presented and explained within the context of current real-world practice and applications.

The suggested time allocation for a restricted response test is 2 minutes for each question plus 5 minutes starting-up time and 5 minutes finishing-off time, thus a total of 70 minutes should be allocated for a 30-question end-of-unit test.

Although individual outcome tests are permissible, it is suggested that if subtests are to be used, outcomes should be combined to produce tests of no fewer than 10 questions. A 10-question test would therefore have a time allocation of 30 minutes.

Outcome 2

Describe Internetworking security

Knowledge and/or skills

- Internet security concepts
- Suspicious activities
- Intrusion detection.
- Access control.
- Anti-virus software.
- Client security add-ons
- Firewalls.

- DMZ
- Authentication/encryption technologies

Evidence requirements

Restricted response test

The knowledge and skills component of Outcome 2 must be examined by twelve questions, derived from the nine items listed below. Two questions must be derived from any three of the items and one question derived from each of the remaining items. Each question must be derived from a single item.

1. Internet security concepts.

   Access control, authentication, encryption, SSL, security tools, auditing, SET

2. Suspicious network activities.

   Log-in failures, ping, mail and SYN floods, denial of service attacks, spoofing, repudiation

3. Intrusion detection.

   Auditing, review audit logs, network monitoring, unauthorised access notification.

4. Access control

   Mail server, web server.

5. Anti-virus software.

   Server, client, network

6. Client security add-ons.

   Encryption software, digital identification, personal firewall software

7. Firewalls

   Port filtering, packet filtering, application filtering and intrusion detection.

8. DMZ

   Bastion Host, three-homed firewall and back-to-back firewalls

9. Authentication/encryption technologies

   Username/password authentication, SmartCard, SSL, authentication versus encryption, PKI, asymmetric encryption, asymmetric encryption, one-way encryption.

The test may be administered on its own as a subtest or be combined with other outcome subtests in the Unit.

Alternatively, the 12 questions for this outcome may contribute towards a single end-of-unit test of 30 questions.

Logbook

The logbook for Outcome 2 must record successful completion by the candidate of **both** the tasks listed below:

- Anti-virus software.

  Documentary evidence that the candidate can install and configure anti-virus software on a client machine.

- Firewalls

  Documentary evidence that the candidate can install and configure a firewall on a client machine.

Assessment guidelines

It is suggested that all the above concepts be presented and explained within the context of current real-world practice and applications.

The suggested time allocation for a restricted response test is 2 minutes for each question plus 5 minutes starting-up time and 5 minutes finishing-off time, thus a total of 70 minutes should be allocated for a 30-question end-of-unit test.

Although individual outcome tests are permissible, it is suggested that if subtests are to be used, outcomes should be combined to produce tests of no fewer than 10 questions. A 10-question test would therefore have a time allocation of 30 minutes.

Higher National Unit specification: statement of standards (cont)

Unit title: Internetworking Concepts 2: Security and Business Concepts

Outcome 3

Describe internetworking business concepts.

Knowledge and/or skills

- E-commerce terms and concepts
- Features of intranets, extranets, local networks and the Internet
- E-business models
- Strategic marketing considerations
- Legal and regulatory considerations

Evidence requirements

Restricted response test

The knowledge and skills component of Outcome 3 must be examined by six questions, derived from the five items listed below. Two questions must be derived from one of the items and one question from each of the four remaining items. Each question must be derived from a single item.

1. E-commerce terms and concepts.

   Information Service Providers, Portals, SET (Secure Electronic Transactions), EFT (Electronic Funds Transfer), EBT (Electronic Benefits Transfer), EDI (Electronic Data Interchange), OBI (Open Buying on the Internet), OTP (Open Trading Protocol)

2. Features of intranets, extranets, local networks and the Internet

   Private Network, Intranet, Extranet, Internet

3. E-business models.

   Business-to-business, business-to-consumer, business-to-employee, business to government, consumer-to-business, consumer-to-consumer, storefront vs. e-business, customer expectations, aggregators.

4. Strategic marketing considerations

   Geographic/localization considerations, public relations; impact/risks of site failure

5. Legal and regulatory considerations

   Knowledge ownership / intellectual property rights, privacy, jurisdiction

The test may be administered on its own as a subtest or be combined with other outcome subtests in the Unit.

Alternatively, the 6 questions for this outcome may contribute towards a single end-of-unit test of 30 questions.

Logbook

There are no practical tasks associated with this Outcome.

Assessment guidelines

It is suggested that all the above concepts be presented and explained within the context of current real-world practice and applications.

The suggested time allocation for a restricted response test is 2 minutes for each question plus 5 minutes starting-up time and 5 minutes finishing-off time, thus a total of 70 minutes should be allocated for a 30-question end-of-unit test.

Although individual outcome tests are permissible, it is suggested that if subtests are to be used, outcomes should be combined to produce tests of no fewer than 10 questions. A 10-question test would therefore have a time allocation of 30 minutes.

Administrative Information

Unit code: DF9V 34

Unit title: Internetworking Concepts 2: Security and Business Concepts

Superclass category: CE

Date of publication: May 2004

Version 01

Source: SQA

Additional copies of this Unit specification can be purchased from the Scottish Qualifications Authority. The cost for each Unit specification is £2.50. (A handling charge of £1.95 will apply to all orders for priced items.)

Higher National Unit specification: support notes

Unit title: Internetworking Concepts

This part of the Unit specification is offered as guidance. The support notes 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.

The suggested time allocation for each outcome (including assessment) is as follows:

Outcome 1: 16 hours
Outcome 2: 16 hours
Outcome 3: 8 hours

Guidance on the content and context for this Unit

During the delivery of this unit it is important that every opportunity is taken to introduce real-world examples, opportunities for whole-class and group discussion and practical demonstrations wherever possible. Concepts and terminology should be presented in context throughout the Unit. Video presentations should be used where appropriate for providing an alternative explanation of a difficult topic, or as a focus for class discussion or group work.

Given the theoretical nature of this Unit, it is intended that a significant amount of time will be made available as a central part of the course for revision, tutorials and formative assessment exercises. Candidates should be strongly encouraged to undertake further reading, and opportunities for individual or group research should be provided.

The most important overall emphasis should be on the relevance and currency of content in such a rapidly-evolving field.

This Unit, in conjunction with Internetworking Concepts 1: Development and Delivery Concepts, may assist candidates in preparing for CompTIA examination IK0-001: I-Net+. Vendor certifications can change rapidly and candidates should be encouraged the check the current details at **www.comptia.org** to ensure that all objectives have been covered.

Outcome 1

This Outcome requires that candidates have the knowledge and skills to understand and be able to describe the core components of the Internet infrastructure; identify problems with Internet connectivity; understand how to use Internet domain names and DNS; understand the capabilities of popular remote access protocols; understand how various protocols or services apply to the function of their corresponding server; identify when to use various diagnostic tools for resolving Internet problems; create a logic diagram of Internet components; describe various hardware and software connection devices; understand when to use various site monitoring procedures; understand how common networking topologies are used; and understand the capabilities of application server providers.

Higher National Unit specification: support notes (cont)

Unit title: Internetworking Concepts

1 Internet infrastructure

Candidates should understand and be able to describe the core components of the Internet infrastructure, including network access points, backbone, hardware/software infrastructure and internetworking devices such as routers, switches and bridges.

2 Connectivity problems

Candidates should be able to identify problems with Internet connectivity from source to destination for various types of servers, including: e-mail server, web server, FTP server, news server, proxy server, caching server, media server, DNS server, certificate server, directory (LDAP) server and describe connecting through a firewall.

3 Domain names and DNS

Candidates should understand and be able to describe the use of Internet domain names and DNS, including DNS entry types, hierarchical structure, role of root domain servers, top level or original domains and Nslookup.

4 Remote access protocols

Candidates should also understand and be able to describe the capabilities of popular remote access protocols, including: SLIP, PPP, PPTP, L2TP, PPPOE, Point-to-point and multi-point.

5 Application of protocols or services to their corresponding server

Candidates should understand how various protocols or services apply to the function of their corresponding server, such as a mail server, a web server or a file transfer server. Content may include: POP3, SMTP, HTTP, FTP, NNTP, LDAP, Telnet,

6 Diagnostic tools

Candidates should be able to identify when to use various diagnostic tools for resolving Internet problems, such as ping, winipcfg, ipconfig, ifconfig, ARP, tracert and Network Analyzer.

7 Hardware and software connection devices

Candidates should be able to describe various hardware and software connection devices and when to use them and create a logic diagram of Internet components from the client to the server. Content may include the following: bridge, brouter, router, switch, hub, repeater, network adapter, cable modem, *x*DSL modem, modem, WAN link, CSU/DSU, firewall, Network Address Translation (NAT) server and proxy server

8 Site monitoring procedures

Candidates should know when to use various site monitoring procedures, including viewing server log files, monitoring network traffic, monitoring server utilization and monitoring server network bandwidth utilization

9 Networking topologies

Candidates should be able to describe how common networking topologies are used, including Star, Bus, Mesh and Ring.

10 Application server providers

They should also be able to describe how application server providers can provide Internet-based services on an as needed basis, such as: custom web hosting, e-mail services, fax services, access to an application over the web and shared access to expensive hardware, such as a mainframe computer.

Outcome 2

This outcome requires that the candidate have the knowledge and skills to understand various Internet security concepts; identify suspicious network activities; identify various methods for performing intrusion detection; identify appropriate access-control security features for an Internet server; describe the uses and proper instances to use anti-virus software; describe the uses and proper instances to use various client security add-ons; describe how firewalls are used to protect private networks; understand when to use various DMZ configurations; and describe various authentication/encryption technologies.

1 Internet security concepts

Candidates should be able to describe various Internet security concepts, including access control, authentication, encryption - PKI, Secure Socket Layers (SSL), access security tools, auditing and Secure Electronic Transactions (SET).

2 Suspicious activities

Candidates should also be able to identify suspicious network activities, including multiple log-in failures, Ping floods, denial of service (DOS) attacks, mail flooding, SYN floods, spoofing and repudiation.

3 Intrusion detection

Candidates should be able to identify various methods for performing intrusion detection, including configuring auditing on servers and firewalls, reviewing audit logs, configuring network monitoring software to alert administrator when suspicious types of traffic occur, configuring servers to notify administrator when unauthorized accesses are attempted.

4 Access control

Candidates should also be able to identify appropriate access-control security features for an Internet server such as: e-mail server, web server (Apache, NES, IIS).

5 Anti-virus software

Candidates should be able to describe the uses and proper instances to use anti-virus software for server anti-virus protection, client computer anti-virus protection and network anti-virus protection, such as on a firewall

6 Client security add-ons

Candidates should be able to describe the uses and proper instances to use various client security add-ons, such as encryption software, personal digital identification (such as a digital certificate) and personal firewall software.

7 Firewalls

Candidates should be able to describe how firewalls are used to protect private networks by means of port filtering, packet filtering application filtering and intrusion detection filtering

8 DMZ

Candidates should also be able to identify when to use various DMZ configurations such as: Bastion Host, three-homed firewall and back-to-back firewalls.

9 Authentication/encryption technologies

Candidates should be able to describe various authentication/encryption technologies, including username/password authentication, SmartCard authentication, SSL, authentication versus encryption, PKI, asymmetric encryption, including Blowfish, RC2, RC4, and RC5, symmetric encryption, including DES, triple DES, and Skipjack and One-Way encryption, including MD5 and SHA.

Outcome 3

This outcome requires candidates to be able to identify and or describe various e-business and e-commerce concepts and when they are used, including term definitions, e-business related network concepts, e-business models, strategic marketing considerations, and legal/regulatory considerations.

Higher National Unit specification: support notes (cont)

Unit title: Internetworking Concepts

1 E-commerce terms and concepts

Candidates should be able to describe e-commerce terms and concepts, including: Information Service Providers (ISPs), Portals, SET (Secure Electronic Transactions), EFT (Electronic Funds Transfer), EBT (Electronic Benefits Transfer), EDI (Electronic Data Interchange), OBI (Open Buying on the Internet) and OTP (Open Trading Protocol).

2 Features of intranets, extranets, local networks and the Internet

Candidates should be able to describe the differences between private networks, Intranets, Extranet and the Internet from a business standpoint.

3 E-business models

Candidates should be able to describe the types of e-business models being applied today, including business-to-business, business-to-consumer, business-to-employee, business to government, consumer-to-business and consumer-to-consumer. They should also be able to describe storefront (bricks & mortar) vs. e-business, new and changing customer expectations, e-business and the Internet and aggregators.

4 Strategic marketing considerations

Candidates should be able to identify key factors relating to strategic marketing considerations as they relate to launching an e-business initiative, including geographic/localization considerations (local customs/criteria, etc.), public relations; impact/risks of site failure.

5 Legal and regulatory considerations

Candidates should be able to identify key factors relating to legal and regulatory considerations when planning e-business solutions, for example: knowledge ownership / intellectual property rights, privacy, jurisdiction.

Higher National Unit specification: support notes (cont)

Unit title: Internetworking Concepts

Guidance on the delivery and assessment of this unit

This Unit is likely to form part of a group award which is primarily designed to provide candidates with technical or professional knowledge and skills related to a specific occupational area. It is highly technical in content and should not be adopted by group awards in other areas or delivered as a stand-alone Unit without careful consideration of its appropriateness. It is a Unit which candidates are likely to find accessible at an introductory level; it is suggested that it be delivered part of an HNC or first-year HND program in Computing or a related area, giving candidates experience of basic background topics involved in the hardware and software aspects of computer networks

To minimise assessment overhead, sets of multiple choice questions are used to provide evidence of candidates' knowledge for all Outcomes. It is suggested that multiple-choice questions can be used as the preferred assessment method – as well as reducing the time required for assessment and marking, these reduce the need for candidates to memorise details and encourage understanding. The numbers of questions which must be answered correctly in each assessment correspond to 70% of those set in each case.

Open learning

If this Unit is delivered by open or distance learning methods, additional planning and resources may be required for candidate support, assessment and quality assurance.

A combination of new and traditional authentication tools may have to be devised for assessment and re-assessment purposes.

For further information and advice, please see *Assessment and Quality Assurance for Open and Distance Learning* (SQA, February 2001 — publication code A1030).

Special needs

This Unit specification is intended to ensure that there are no artificial barriers to learning or assessment. Special needs of individual candidates should be taken into account when planning learning experiences, selecting assessment instruments or considering special alternative Outcomes for Units. For information on these, please refer to the SQA document *Guidance on Special Assessment Arrangements* (SQA, 2001).

General information for candidates

Unit title: Internetworking Concepts 2: Security and Business Concepts

This is a 1-credit Unit at Level 7 intended for candidates undertaking a Computing or IT-related qualification who require an understanding of Internetworking concepts. It is designed to develop an understanding of the issues involved using and constructing Internets and Intranets. On completion of the Unit you should be able to:

- Describe internetworking concepts
- Describe internetworking security
- Describe internetworking business concepts

The first section examines the technologies of the Internet, and covers topics such as backbones, routers and bridges, protocols and troubleshooting problems with Internet connectivity. You will also become familiar with the naming schemes in use on the Internet.

The second section is primarily aimed at the security issues that surround the web, including passwords, encryption, monitoring systems for suspicious activities and the different types of computer virus.

In final section you will study the activities that underlie business on the Internet. These include fund transfer, Intranets and the different types of businesses trading on the Internet. Another aspect of business on the Internet is the legal and regulatory considerations, featuring copyright, privacy and jurisdiction.

This Unit, in conjunction with Internetworking Concepts 1: Development and Delivery Concepts, may assist you in preparing for CompTIA examination IK0-001: I-Net+. Vendor certifications can change rapidly, so you should check the current details at **www.comptia.org** to ensure that all objectives have been covered.