

Higher National Unit Specification

General information for centres

Unit title: Network Infrastructure 2: Planning and Maintenance

Unit code: DG00 35

Unit purpose: This Unit is designed to introduce candidates to the issues involved in planning and maintaining a network infrastructure. It is intended for candidates undertaking an HNC or HND in Computing, Computer Networking or a related area who require a detailed knowledge of planning and maintaining a network infrastructure.

On completion of the Unit candidates should be able to:

1. Plan and implement server roles and server security.
2. Plan, implement and maintain a network infrastructure.
3. Plan, implement and maintain routing and remote access.
4. Plan, implement and maintain server availability.
5. Plan and maintain network security.

Credit value: 2 HN credits at SCQF level 8: (16 SCQF credit points at SCQF level 8)

**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 networks. This may be demonstrated by the possession of HN Units such as DF9P 34 Network Concepts, DF9N 34 Network Server Operating System and DF9R 35 Network Infrastructure 1: Implementation and Management.

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 50 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.

General information for centres (cont)

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.

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 administrator 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 8.

Higher National Unit specification: statement of standards

Unit title: Network Infrastructure 2: Planning and Maintenance

Unit code: DG00 35

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

Plan and implement server roles and server security.

Knowledge and/or skills

- ◆ Plan a secure baseline installation.
- ◆ Plan and configure security for servers that are assigned specific roles.
- ◆ Evaluate and select the operating system to install on computers in an enterprise.

Evidence requirements

Restricted response test

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

1. Plan a secure baseline installation.

Plan a strategy to enforce system default security settings on new systems, identify client operating system default security settings, identify all server operating system default security settings.

2. Plan security for servers that are assigned specific roles.

Domain controllers, web servers, database servers and mail servers; deploy the security configuration for servers; create custom security templates based on server roles.

3. Evaluate and select the operating system to install on computers in an enterprise.

Identify the minimum configuration to satisfy security requirements.

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

Higher National Unit specification: statement of standards (cont)

Unit title: Network Infrastructure 2: Planning and Maintenance

Alternatively, the 6 questions for this outcome may contribute towards a single end-of-unit test of 50 questions.

Logbook

The logbook for Outcome 1 must record successful completion by the candidate of **at least two** of the three tasks listed below. The tasks to be completed must be selected by the tutor.

1. Plan a secure baseline installation.

The candidate must produce a strategy to enforce system default security settings on new systems, identifying client operating system default security settings and server operating system default security settings.

2. Plan security for servers that are assigned specific roles.

Documentary evidence that the candidate has deployed the security configuration and created custom security templates based on server roles for at least two of the following roles: domain controller, web server, database server, mail server.

3. Evaluate and select the operating system to install on computers in an enterprise.

Documentary evidence that the candidate has selected a suitable operating system to install on computers in an enterprise and identified the minimum configuration to satisfy security requirements.

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 110 minutes should be allocated for a 50-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: Network Infrastructure 2: Planning and Maintenance

Outcome 2

Plan, implement and maintain a network infrastructure.

Knowledge and/or skills

- ◆ Plan a TCP/IP network infrastructure strategy.
- ◆ Plan and modify a network topology.
- ◆ Plan and troubleshoot Internet connectivity.
- ◆ Plan network traffic monitoring.
- ◆ Troubleshoot TCP/IP addressing.
- ◆ Plan and troubleshoot host name resolution.

Evidence requirements

Restricted response test

The knowledge and skills component of Outcome 2 must be examined by twelve questions, two derived from each of the six items listed below. Each question must be derived from a single item.

1. Plan a TCP/IP network infrastructure strategy.

Analyze IP addressing requirements; plan an IP routing solution; create an IP subnet scheme.

2. Plan and modify a network topology.

Plan physical placement of network resources; identify network protocols to be used.

3. Plan and troubleshoot Internet connectivity.

Network Address Translation (NAT), name resolution cache information, client configuration.

4. Plan network traffic monitoring.

Use system monitoring tools

5. Troubleshoot TCP/IP addressing.

Client computer configuration; DHCP server address assignment.

6. Plan and troubleshoot host name resolution

DNS namespace design, zone replication requirements and forwarding configuration; DNS security; interoperability of DNS with third-party DNS solutions; NetBIOS name resolution.

Higher National Unit specification: statement of standards (cont)

Unit title: Network Infrastructure 2: Planning and Maintenance

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 50 questions.

Logbook

The logbook for Outcome 2 must record successful completion by the candidate of **at least three** of the six tasks listed below. The tasks to be completed must be selected by the tutor.

1. Plan a TCP/IP network infrastructure strategy.

Documentary evidence that the candidate can analyse IP addressing requirements, plan an IP routing solution and create an IP subnet scheme.

2. Plan and modify a network topology.

A plan, produced by the candidate, showing the physical placement of network resources and identify the network protocols to be used.

3. Plan and troubleshoot Internet connectivity.

Documentary evidence that the candidate can plan Internet connectivity, making use of Network Address Translation (NAT) and defining the appropriate client configuration.

4. Plan network traffic monitoring.

Documentary evidence that the candidate can use system monitoring tools to plan and implement network traffic monitoring

5. Troubleshoot TCP/IP addressing.

Documentary evidence that the candidate can diagnose and resolve at least two TCP/IP addressing problems involving client computer configuration and/or DHCP server address assignment.

6. Plan and troubleshoot host name resolution

Documentary evidence that the candidate can diagnose and resolve at least two host name resolution problems arising from any of the following: DNS namespace design, zone replication requirements and forwarding configuration; DNS security; interoperability of DNS with third-party DNS solutions; NetBIOS name resolution.

Higher National Unit specification: statement of standards (cont)

Unit title: Network Infrastructure 2: Planning and Maintenance

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 110 minutes should be allocated for a 50-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 3

Plan, implement and maintain routing and remote access

Knowledge and/or skills

- ◆ Plan a routing strategy.
- ◆ Plan security for remote access users.
- ◆ Implement secure access between private networks.
- ◆ Troubleshoot TCP/IP routing.

Evidence requirements

Restricted response test

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

1. Plan a routing strategy.

Identify routing protocols to use in a specified environment; plan routing for IP multicast traffic.

2. Plan security for remote access users.

Plan remote access policies; analyze protocol security requirements; authentication methods for remote access clients.

3. Implement secure access between private networks.

Create and implement an IPSec policy.

Higher National Unit specification: statement of standards (cont)

Unit title: Network Infrastructure 2: Planning and Maintenance

4. Troubleshoot TCP/IP routing.

Use system tools.

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

Alternatively, the 8 questions for this outcome may contribute towards a single end-of-unit test of 50 questions.

Logbook

The logbook for Outcome 3 must record successful completion by the candidate of **at least two** of the four tasks listed below. The tasks to be completed must be selected by the tutor.

1. Plan a routing strategy.

Documentary evidence that the candidate can identify routing protocols to use in a specified environment and plan routing for IP multicast traffic.

2. Plan security for remote access users.

Documentary evidence that the candidate can plan remote access policies, analyze protocol security requirements and select authentication methods for remote access clients.

3. Implement secure access between private networks.

Documentary evidence that the candidate can create and implement an IPSec policy to provide secure access between private networks

4. Troubleshoot TCP/IP routing.

Documentary evidence that the candidate can use system tools to troubleshoot TCP/IP routing.

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 110 minutes should be allocated for a 50-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: Network Infrastructure 2: Planning and Maintenance

Outcome 4

Plan, implement and maintain server availability.

Knowledge and/or skills

- ◆ Plan services for high availability.
- ◆ Identify system bottlenecks.
- ◆ Implement a cluster server.
- ◆ Manage Network Load Balancing.
- ◆ Plan a backup and recovery strategy.

Evidence requirements

Restricted response test

The knowledge and skills component of Outcome 4 must be examined by ten questions, two derived from each of the five items listed below. Each question must be derived from a single item.

1. Plan services for high availability.

Clustering services, Network Load Balancing.

2. Identify system bottlenecks

Memory, processor, disk, and network related bottlenecks, using system tools

3. Implement and maintain a cluster server

Recover from cluster node failure.

4. Manage Network Load Balancing.

Use system tools.

5. Plan a backup and recovery strategy

Backup types (full, incremental, differential); volume shadow copy; system recovery.

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

Alternatively, the 10 questions for this outcome may contribute towards a single end-of-unit test of 50 questions.

Higher National Unit specification: statement of standards (cont)

Unit title: Network Infrastructure 2: Planning and Maintenance

Logbook

The logbook for Outcome 4 must record successful completion by the candidate of **at least three** of the five tasks listed below. The tasks to be completed must be chosen by the tutor.

1. Plan services for high availability.

The candidate must produce a plan to ensure high availability. The plan must include the use of clustering services and Network Load Balancing.

2. Identify system bottlenecks

Documentary evidence that the candidate can use system tools to identify bottlenecks related to memory, processor, disk and network.

3. Implement and maintain a cluster server

Documentary evidence that the candidate can recover from cluster node failure.

4. Manage Network Load Balancing.

Documentary evidence that the candidate can use system tools to manage Network Load Balancing.

5. Plan a backup and recovery strategy

The candidate must produce a backup and recovery strategy which makes use of multiple backup types, chosen from full, incremental and differential.

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 110 minutes should be allocated for a 50-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: Network Infrastructure 2: Planning and Maintenance

Outcome 5

Plan and maintain network security.

Knowledge and/or skills

- ◆ Plan and configure network protocol security.
- ◆ Plan and configure security for data transmission.
- ◆ Plan secure network administration methods.
- ◆ Plan security for wireless networks.
- ◆ Configure directory service for certificate publication.
- ◆ Plan a public key infrastructure (PKI) that uses Certificate Services.
- ◆ Plan a framework for planning and implementing security.

Evidence requirements

Restricted response test

The knowledge and skills component of Outcome 5 must be examined by fourteen questions, two derived from each of the seven items listed below. Each question must be derived from a single item.

1. Plan and configure network protocol security.

Specify required ports and protocols for services; Plan an IPSec policy for secure network communications; configure protocol security in a heterogeneous client computer environment; configure protocol security by using IPSec policies.

2. Plan and configure security for data transmission.

Secure data transmission between client computers to meet security requirements; secure data transmission by using IPSec; configure IPSec policy settings; troubleshoot security for data transmission. Use system tools.

3. Plan secure network administration methods.

Create a plan to offer Remote Assistance to client computers; Plan for remote administration.

4. Plan security for wireless networks.

WEP encryption, WEP authentication

5. Configure directory service for certificate publication.

Higher National Unit specification: statement of standards (cont)

Unit title: Network Infrastructure 2: Planning and Maintenance

6. Plan a public key infrastructure (PKI) that uses Certificate Services.

Identify the appropriate type of certificate authority to support certificate issuance requirements; plan the enrolment and distribution of certificates and the use of smart cards for authentication.

7. Plan a framework for planning and implementing security.

Plan for security monitoring; change and configuration management, security update infrastructure, use system tools

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

Alternatively, the 14 questions for this outcome may contribute towards a single end-of-unit test of 50 questions.

Logbook

The logbook for Outcome 5 must record successful completion by the candidate of **at least four** of the seven tasks listed below. The tasks to be completed must be chosen by the tutor.

1. Plan and configure network protocol security.

Documentary evidence that the candidate can specify the required ports and protocols for services and configure protocol security by using IPSec policies.

2. Plan and configure security for data transmission.

Documentary evidence that the candidate can configure IPSec and secure data transmission by using IPSec policy settings.

3. Plan secure network administration methods.

Documentary evidence that the candidate can offer remote assistance to client computers and carry out.

4. Plan security for wireless networks.

Documentary evidence that the candidate can plan security for wireless networks using WEP encryption and WEP authentication.

5. Configure directory service for certificate publication.

Documentary evidence that the candidate can configure directory service for certificate publication.

Higher National Unit specification: statement of standards (cont)

Unit title: Network Infrastructure 2: Planning and Maintenance

6. Plan a public key infrastructure (PKI) that uses Certificate Services.

Documentary evidence that the candidate can identify the appropriate type of certificate authority to support certificate issuance requirements and plan the enrolment and distribution of certificates.

7. Plan a framework for planning and implementing security.

Documentary evidence that the candidate can produce a security plan, taking account of security monitoring, change and configuration management and security update infrastructure.

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 110 minutes should be allocated for a 50-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:	DG00 35
Unit title:	Network Infrastructure 2: Planning and Maintenance
Superclass category:	CB
Date of publication:	May 2004
Version:	01
Source:	SQA

© Scottish Qualifications Authority 2004

This publication may be reproduced in whole or in part for educational purposes provided that no profit is derived from reproduction and that, if reproduced in part, the source is acknowledged.

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: Network Infrastructure 2: Planning and Maintenance

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 80 hours.

The recommended time allocations for each outcome (including assessment) are as follows:

Outcome 1:	10 hours
Outcome 2:	20 hours
Outcome 3:	13 hours
Outcome 4:	16 hours
Outcome 5:	21 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.

The following notes assume that the unit will be delivered using a Microsoft operating system, such as Windows 2000/2003 Server. However, no restriction is placed on the operating system to be used and centres are free to choose alternative operating systems such as Linux/Unix, although this may require changes in terminology.

This Unit may assist candidates in preparing for Microsoft examination 70-293: Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure. Vendor certifications can change rapidly and candidates should be encouraged to check the current details at www.microsoft.com/traincert to ensure that all objectives have been covered. This examination contributes towards the Microsoft Certified Systems Engineer (MCSE) award.

Higher National Unit specification: support notes (cont)

Unit title: Network Infrastructure 2: Planning and Maintenance

The content of this unit may be delivered using relevant vendor-supplied materials, such as Microsoft Official Curriculum (MOC). As these materials are under continuous development, centres should check carefully to ensure that such materials meet all the requirements for the unit. If MOC materials are used, some of the practical tasks involved may contribute towards the practical assessments required for the unit.

Outcome 1: Plan and Implement Server Roles and Server Security

1 Plan a secure baseline installation

Candidates should be able to plan a strategy to enforce system default security settings on new systems. They should also be able to identify client operating system default security settings and identify all server operating system default security settings.

2 Plan security for servers that are assigned specific roles

Candidates should be aware that roles include domain controllers, web servers, database servers, and mail servers. They should be able to deploy the security configuration for servers and create custom security templates based on server roles.

3 Evaluate and select the operating system to install on computers in an enterprise

Candidates should be able to identify the minimum configuration required to satisfy security requirements.

Outcome 2: Plan, Implement and Maintain a Network Infrastructure

1 Plan a TCP/IP network infrastructure strategy

Candidates should be able to describe the TCP/IP protocol suite and its role in a Windows 2000/2003 server network. They should be able to analyse IP addressing requirements, plan an IP routing solution, create an IP subnet scheme and choose an address configuration methodology (manual, dynamic or APIPA).

2 Plan and modify a network topology

Candidates should be able to plan the physical placement of network resources and identify network protocols to be used.

3 Plan and troubleshoot Internet connectivity

Candidates should be able to plan a strategy for internet connectivity and diagnose and resolve problems relating to Network Address Translation (NAT), name resolution cache information and client configuration.

Higher National Unit specification: support notes (cont)

Unit title: Network Infrastructure 2: Planning and Maintenance

4 Plan network traffic monitoring

Candidates should be able to use system tools such as Network Monitor and System Monitor.

5 Troubleshoot TCP/IP addressing

Candidates should be able to diagnose and resolve problems relating to client computer configuration and DHCP server address assignment.

6 Plan and troubleshoot host name resolution

Candidates should be able to plan a DNS namespace design, zone replication requirements and forwarding configuration, DNS security and interoperability of DNS with third-party DNS solutions. They should also be able to plan a WINS replication strategy and plan NetBIOS name resolution by using the Lmhosts file. They should be able to troubleshoot and resolve issues relating to DNS services and client computer configuration.

Outcome 3: Plan, Implement and Maintain Routing and Remote Access

1 Plan a routing strategy

Candidates should be able to identify the routing protocols to use in a specified environment and plan routing for IP multicast traffic.

2 Plan security for remote access users

Candidates should be able to plan remote access policies, analyse protocol security requirements and select authentication methods for remote access clients.

3 Implement secure access between private networks

Candidates should have knowledge of IPSec policies, rules and settings and be able to create and implement an IPSec policy.

4 Troubleshoot TCP/IP routing

Candidates should be able to use system tools such as the route, tracert, ping, pathping, and netsh commands and Network Monitor.

Outcome 4: Plan, Implement and Maintain Server Availability

1 Plan services for high availability.

Candidates should be able to plan a high availability solution that includes clustering services and uses Network Load Balancing.

Higher National Unit specification: support notes (cont)

Unit title: Network Infrastructure 2: Planning and Maintenance

2 Identify system bottlenecks

Candidates should be able to identify memory, processor, disk, and network related bottlenecks and use system tools such as System Monitor.

3 Implement and maintain a cluster server

Candidates should be able to implement a cluster server and recover from cluster node failure.

4 Manage Network Load Balancing

Candidates should be able to manage network load balancing by using system tools such as the Network Load Balancing Monitor MMC snap-in and the WLBS cluster control utility.

5 Plan a backup and recovery strategy

Candidates should be able to identify appropriate backup types (full, incremental, differential) and plan a backup strategy that uses volume shadow copy. They should also be able to plan system recovery using Automated System Recovery (ASR).

Outcome 5: Plan and Maintain Network Security

1 Plan and configure network protocol security.

Candidates must be able to specify required ports and protocols for services and plan an IPSec policy for secure network communications. They should also be able to configure protocol security in a heterogeneous client computer environment and configure protocol security by using IPSec policies.

2 Plan and configure security for data transmission.

Candidates should be able to secure data transmission between client computers to meet security requirements and secure data transmission by using IPSec. They should also be able to configure IPSec policy settings and troubleshoot security for data transmission. Tools should include the IP Security Monitor MMC snap-in and the Resultant Set of Policy (RSOP) MMC snap-in.

3 Plan secure network administration methods.

Candidates should be able to create a plan to offer remote assistance to client computers and plan for remote administration by using Terminal Services.

4 Plan security for wireless networks

Candidates should be able to use WEP encryption and WEP authentication.

Higher National Unit specification: support notes (cont)

Unit title: Network Infrastructure 2: Planning and Maintenance

5 Configure directory service for certificate publication.

Candidates should be able to configure the Active Directory service for certificate publication.

6 Plan a public key infrastructure (PKI) that uses Certificate Services.

Candidates should be able to identify the appropriate type of certificate authority to support certificate issuance requirements, plan the enrolment and distribution of certificates and plan for the use of smart cards for authentication.

7 Plan a framework for planning and implementing security.

Candidates should be able to plan for security monitoring and plan a change and configuration management framework for security. They should also be able to plan a security update infrastructure, using system tools such as Microsoft Baseline Security Analyser and Microsoft Software Update Services.

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 unlikely to find accessible at an introductory level; it is suggested that it be delivered only as part of an HNC/HND program in Computing, Computer Networking or a related area. It should be delivered in tandem with other Computing Units and opportunities for teaching and assessment integration explored.

To minimise assessment overhead, one or more sets of restricted-response questions, totalling 50 questions in all, should be used to provide evidence of candidates' knowledge for all Outcomes. It is suggested that multiple-choice questions should 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. 75% of the questions must be answered correctly to pass each assessment. Candidates must also complete a log book or checklist recording the practical work undertaken for each outcome.

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.

Higher National Unit specification: support notes (cont)

Unit title: Network Infrastructure 2: Planning and Maintenance

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: Network Infrastructure 2: Planning and Maintenance

This is a 2-credit Unit at Level 8 intended for candidates undertaking a Computing or IT-related qualification who require a detailed understanding of network infrastructure. It is designed to develop an understanding of the issues involved in planning and maintaining a network infrastructure. On completion of the Unit you should be able to:

- Plan and implement server roles and server security.
- Plan, implement and maintain a network infrastructure.
- Plan, implement and maintain routing and remote access.
- Plan, implement and maintain server availability.
- Plan and maintain network security.

In the first part of the course, you will study planning and implementing server roles and server security, including configuring security for servers that are assigned specific roles, planning a secure baseline installation, planning security for servers that are assigned specific roles and evaluating and selecting the operating system to install on computers in an enterprise.

The second section covers planning and maintaining a network infrastructure, including planning a TCP/IP network infrastructure strategy, planning and modifying a network topology, planning an internet connectivity strategy, planning network traffic monitoring, troubleshooting Internet connectivity and TCP/IP addressing and planning and troubleshooting host name resolution.

The third section covers planning, implementing and maintaining routing and remote access, including planning a routing strategy, planning security for remote access users, implementing secure access between private networks and troubleshooting TCP/IP routing.

The fourth section covers planning, implementing and maintaining server availability, including planning services for high availability, identifying system bottlenecks, implementing a cluster server, managing network load balancing and planning a backup and recovery strategy

The final section covers plan and maintain network security, including planning and configuring network protocol security, planning and configuring security for data transmission, planning secure network administration methods, planning security for wireless networks, configuring directory service for certificate publication, planning a public key infrastructure (PKI) that uses certificate services and planning a framework for planning and implementing security.

There will be a closed-book multiple-choice assessment covering all outcomes. You will be presented with 50 questions and expected to answer 75% of these correctly. You will also be expected to keep a checklist or log book recording the practical tasks you have carried out during the Unit. You must satisfy the requirements for these assessments in order to achieve the Unit.

This Unit may assist you in preparing for Microsoft examination 70-293: Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure. Vendor certifications can change rapidly, so you should check the current details at www.microsoft.com/traincert to ensure that all objectives have been covered. This examination contributes towards the Microsoft Certified Systems Engineer (MCSE) award.