Higher National Unit Specification

General information for centres

Unit title: Server Concepts

Unit code: DF9W 34

Unit purpose: This Unit is designed to introduce candidates to the issues involved in installing, configuring and maintaining a network server. It is intended for candidates undertaking an HNC/D in Computing, Computer Networking or a related area who require a broad knowledge of network server hardware, and the main theories, concepts and principles in this area.

On completion of the Unit candidates should be able to:

1. Install and configure a network server.
2. Upgrade a network server.
3. Maintain a network server and its environment
4. Troubleshoot and resolve network server problems.
5. Plan for network server disaster recovery.

f

Credit value: 2 HN credits at SCQF level 7: (16 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 networks. This may be demonstrated by the possession of HN Units such as DF9P 34 Network Concepts and DF9N 34 Network Server Operating System.

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.

Higher National Unit specification: statement of standards

Unit title: Server Concepts

Unit code: DF9W 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

Install and configure a network server.

Knowledge and/or skills

- Plan the installation of a network server.
- Install a network server.
- Configure a network server.
- Test and document the network server configuration.

Evidence requirements

Restricted response test

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

1. Plan the installation of a network server

   Construct and verify installation plan, check hardware / NOS compatibility, check power, space and network availability, check component and cable availability.

2. Install a network server

   Install hardware, cabling, power, hard disks, external devices. Verify power-on sequence

3. Configure a network server

   Check/upgrade BIOS/firmware levels, configure hard disks, install and update NOS, configure network and verify connectivity, install drivers, configure external peripherals, install service tools

4. Test and document the network server configuration

   Perform baseline, document configuration.

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 1 must record successful completion by the candidate of **each** of the four tasks listed below.

1. Plan the installation of a network server

   Documentary evidence that the candidate can plan the installation of a network server, including constructing and verifying the installation plan, checking hardware / NOS compatibility, checking power, space and network availability and checking component and cable availability.

2. Install a network server.

   Documentary evidence that the candidate can install a network server, including hardware, cabling, power, hard disks and external devices and verify the power-on sequence.

3. Configure a network server.

   Documentary evidence that the candidate can configure a network server including checking/upgrading BIOS/firmware levels, configuring hard disks, installing and updating NOS, configuring the network and verifying connectivity, installing drivers, configuring external peripherals and installing service tools.

4. Test and document the network server configuration

   Documentary evidence that the candidate can test and document the network server configuration.

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 2

Upgrade a network server.

Knowledge and/or skills

- Perform backups.
- Add hardware.
- Upgrade BIOS/firmware.
- Upgrade adapters and peripherals.
- Upgrade service tools.

Evidence requirements

Restricted response test

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

1. Perform backups

   Full backup, verify backup, ERD disks etc.

2. Add Hardware

   Install processor, compatibility check, OS upgrade for multi processors, check manufacturer's recommendations, upgrade hard drives - check compatibility, install hard drive, check cabling, termination and settings, check disk administration, increase memory - check compatibility, install memory, confirm install.

3. Upgrade BIOS/firmware

   Perform BIOS and firmware upgrades.

4. Upgrade adapters and peripherals

   NICs, SCSI cards, RAID controllers; peripherals - check system resources, upgrade drivers.

5. Upgrade service tools

   Diagnostic, anti-virus, monitoring tools.

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.

Logbook

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

1. Perform backups

   Documentary evidence that the candidate can perform and verify a full backup.

2. Add Hardware

   Documentary evidence that the candidate can add hardware to a network server. At least two of the following must be added and tested: processor, hard drive, hard drive, memory.

3. Upgrade BIOS/firmware

   Documentary evidence that the candidate can perform a BIOS and/or firmware upgrade.

4. Upgrade adapters and peripherals

   Documentary evidence that the candidate can upgrade adapters and peripherals including checking system resources and upgrading drivers.

5. Upgrade service tools

   Documentary evidence that the candidate can upgrade diagnostic, anti-virus and monitoring tools.

Higher National Unit specification: statement of standards (cont)

Unit title: Server Concepts

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

Maintain a network server and its environment

Knowledge and/or skills

- Evaluate server performance.
- Perform housekeeping tasks.
- Carry out remote maintenance.
- Identify physical security issues.
- Identify server room environmental issues.

Evidence requirements

Restricted response test

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

1. Evaluate server performance

   Create baseline and compare performance, set SNMP thresholds

2. Perform housekeeping tasks

   Carry out regular backups, perform hardware verification.

3. Carry out remote maintenance

   Establish remote notification.

Higher National Unit specification: statement of standards (cont)

Unit title: Server Concepts

4. Identify physical security issues

   Limit access to server room and backup tapes, physical locks, anti-theft devices.

5. Identify server room environmental issues

   Temperature, humidity, ESD, power surges, back-up generator, fire suppression, flood considerations.

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.

Logbook

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

1. Evaluate server performance

   Documentary evidence that the candidate can evaluate server performance by creating a baseline and compare actual performance against it.

2. Perform housekeeping tasks

   Documentary evidence that the candidate can perform housekeeping tasks including carrying out regular backups and performing hardware verification.

3. Carry out remote maintenance.

   Documentary evidence that the candidate can carry out remote maintenance.

4. Identify physical security issues

   Documentary evidence that the candidate can identify physical security issues including limiting access to the server room and backup tapes, physical locks and anti-theft devices.

5. Identify server room environmental issues

   Documentary evidence that the candidate can identify server room environmental issues, including temperature, humidity, ESD, power surges, back-up generator, fire suppression and flood considerations.

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 4

Troubleshoot and resolve network server problems.

Knowledge and/or skills

- Identify network server problems.
- Carry out server diagnostics.
- Determine server bottlenecks.

Evidence requirements

Restricted response test

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

1. Identify network server problems.

   Use questioning techniques to determine circumstances (what, how, when, how); identify contact(s) responsible for problem resolution; use senses to observe problem.

2. Carry out server diagnostics.

   Identify, select and use diagnostic tools for a range of operating systems, identify and replace defective components, interpret system logs correctly, use documentation, locate and use hot fixes, perform remote troubleshooting.

3. Determine server bottlenecks.

   Diagnose and determine bottlenecks: processor, memory, disk space, bus transfer, NICs, network connectivity.

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

Alternatively, the 9 questions for this outcome may contribute towards a single end-of-unit test of 50 questions.

Logbook

The logbook for Outcome 4 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. Identify network server problems.

   Documentary evidence that the candidate can identify network server problems by using questioning techniques to determine what, how, when, identifying contact(s) responsible for problem resolution and using senses to observe problem.

2. Carry out server diagnostics.

   Documentary evidence that the candidate can identify, select and use diagnostic tools, identify and replace defective components, interpret system logs correctly, use documentation, locate and use hot fixes and perform remote troubleshooting.

3. Determine server bottlenecks.

   Documentary evidence that the candidate can diagnose and determine bottlenecks, including processor, memory, disk space, bus transfer, NICs and network connectivity.

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 5

Plan for network server disaster recovery.

Knowledge and/or skills

- Produce a disaster recovery plan.
- Plan hardware redundancy.
- Describe fault tolerance techniques.

Evidence requirements

Restricted response test

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

1. Produce a disaster recovery plan.

   Identify backup media, backup plan, Identify various backup methods, recovery plan.

2. Plan hardware redundancy.

   Plan for redundancy of hard drives, power supplies, fans, NICs, processors etc.

3. Describe fault tolerance techniques.

   RAID, hot, warm, spare swaps, clustering, replication, mirroring, backup/restore tests, hot and cold sites, hardware replacements.

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

Alternatively, the 9 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: Server Concepts

Logbook

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

1. Produce a disaster recovery plan.

   Documentary evidence that the candidate can produce a disaster recovery plan which identifies backup media and backup methods and includes a backup plan and a recovery plan.

2. Plan hardware redundancy.

   Documentary evidence that the candidate can plan for redundancy of hard drives, power supplies, fans, NICs and processors.

3. Describe fault tolerance techniques.

   Documentary evidence that the candidate can describe fault tolerance techniques, including RAID, hot, warm, spare swaps, clustering, replication, mirroring, backup/restore tests, hot and cold sites and hardware replacements.

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: DF9W 34

Unit title: Server Concepts

Superclass category: CB

Date of publication: May 2004

Version: 01

Source: SQA

Higher National Unit specification: support notes

Unit title: Server 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 80 hours.

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

Outcome 1: 28 hours
Outcome 2: 12 hours
Outcome 3: 16 hours
Outcome 4: 16 hours
Outcome 5: 8 hours

Guidance on the content and context for this Unit

As it is likely that the bulk of the material in this Unit will be delivered through lecturer exposition, 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 groupwork.

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 may assist candidates in preparing for the CompTIA Server+ examination. 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. The Network+ examination can also contribute to the Microsoft Certified System Administrator (MCSA) award. Full details can be found at **www.microsoft.com/traincert**

The aim of this unit is to provide the candidate with an in-depth working knowledge of servers, including hardware, software and troubleshooting techniques. The skills gained will allow them to plan, maintain, test and support server hardware. In the delivery candidates should be introduced to the major features of the current versions of at least the following operating systems:

- Microsoft Windows
- Unix / Linux
- Novell Netware

Log Sheets

Candidates should become familiar early on with the method of recording tasks, faults and identifying appropriate responsibility in line with Who, What, Where, When, How. Logbooks for this section should contain at least the following:

- Reported by: Name, Date, Time, Location, Network ID
- Reported to: Name, Location
- Task and/or fault
- Location of latest drivers, OS updates, software etc.
- Review of FAQs, instructions, facts and issues.
- Testing/pilot results.
- Estimated scheduled downtime.
- ESD and health and safety practices used.
- Confirm successful upgrade, baseline results.
- Document evidence.

Outcome 1: Install and configure a network server.

Candidates should be made aware of the use of installation and configuration requirements of various hardware components before planning, installation and configuration begins, for example RAID, SCSI, UPS, and how to prepare cabling. The topics covered in this outcome should include the following:

1 Plan the installation of a network server.

Planning the installation of a network server and verifying the installation is correct. Candidates should identify the main function of the server within the network, which will affect its role and configuration.

Hardware and software compatibility checklists should be used, in conjunction with power consumption requirements for the server and any peripheral equipment required for example UPS, tape drives etc.

Conformation should also be given on available space and the operational environment recommendations. Checklists should be used to ensure that all components such as cabling, software licenses, UPSs, and other equipment are delivered before installation.

It would also be advantageous to produce a checklist on the various server configurations required before installation for example what services have to be installed what protocols, IP addresses and gateways have to be used.

2 Install a network server.

Candidates should be aware of the health and safety risks and ESD requirements before installation begins, for example risk assessments, cable checks, use of anti-static precautions.

During the installation candidates must carry out the installation of hard disks (RAID if available), external devices, cabling, power and network operating system software etc.

3 Configure a network server.

Configuration of the installation will involve power on sequence, BIOS/firmware upgrades, hard disk configurations, correct drivers installed, network connections, NOS updates such as service packs and patches, service tools.

4 Test and document the network server configuration.

During and after the installation and configuration candidates should perform tests and document the results. They should be aware of the tools and commands required to perform baselines such as network monitoring, and built in protocol tools such as ping, ipconfig, tracert etc.

Outcome 2: Upgrade a network server.

The topics covered in this outcome should include the following:

1 Perform backups.

Full backup and verification of backup before upgrading begins in the event of a system failure after the upgrade. This should include the creation of emergency repair disks (ERD). Candidates should be made aware of the various methods of backups available such tape drive, RAID, server mirroring, and ghosting etc. as well as common good practices to adopt such as correct labelling, storage, tape rotation grandfather, father, son (GFS)), and disaster prevention such as hot swap offices, on site/off site storage etc.

2 Add hardware.

Before upgrading any components of a server, candidates must check the manufacturers recommendations and compatibility checklists. Benchmarking the server's performance should be encouraged after each upgrade. This can be achieved by running performance monitors and system stress tools.

Processors should be configured correctly using BIOS, jumper and or DIP-switch settings. It is important to check the manufacturer's recommendation for socket type, speed, multiplexer settings and recommended running temperature. For multi- processors it is important to check whether the OS, motherboard and BIOS supports them.

The upgrade of hard disks can be one of a number of different interface formats such as SCSI, RAID, EIDE and Serial ATA. For the method used during the upgrade candidates should be made aware of the different ways of configuring and upgrading all methods. For example: RAID 0, 1, 2, 3, 5, 10, SCSI IDS and termination, EIDE master and slave. Candidates should also be made aware of disk partitioning using FDISK, partition magic, volumes, disk quotes and various file system such as FAT, FAT32, NTFS, UNIX etc.

The upgrade of memory can also be a number of different types and sizes SIMMS, DIMMs, SDRAM, DDR, QDR, RIMMs etc. Candidates should aware of the various upgrade requirements regarding, banks of memory, parity, and ECC etc.

3 Upgrade BIOS/firmware.

The upgrade of the BIOS and/or firmware requires that candidates flash their BIOS or firmware for their motherboard to upgrade it with the most up to date version from the manufactures. It would be wise to test bed the upgrade on another less important machine to insure there are no problems.

4 Upgrade adapters and peripherals.

Upgrading adapter cards should include the upgrade of drivers and/or firmware for devices such as NICs, SCSI cards, RAID controllers etc. The upgrading of peripherals should involve the upgrade of device drivers and or software versions.

5 Upgrade service tools.

The upgrade of service tools can include the installation of monitoring tools, service packs, resource tools, and anti-virus updates of signature files.

Outcome 3: Maintain a network server and its environment

1 Evaluate server performance.

Candidates must perform a baseline of the server's performance either before the upgrade or after the upgrade. This will act as a benchmark to measure against any problems or improvements implemented in the future. Tools should be made available for candidates to analyse the network servers' performance. Suggested utilities such as, performance monitor, Simple Network Management Protocol (SNMP), and TCP/IP command results can be used. It is also suggested that stress tools are used to test the server under heavy loads. These tools can be available from resource kits for almost every network OS.

2 Perform housekeeping tasks.

It is important that good housekeeping techniques are encouraged for pro-active prevention of disasters. This should include regular backups over a period of time, hardware checks to verify integrity. Other good housekeeping techniques may include updates on anti virus and schedule tasks such as the creation of restore points, cable checks, CPU temperature checks etc.

3 Carry out remote maintenance.

Candidates should establish remote notification of events occurring on the server. This can be in the form of a network broadcast messages or an E-mail message. Most shutdown software (UPS software) now offers the ability to send a pager message or E-mail on predetermined power conditions. Traps can be set which are triggered to notify the administrator that there is a problem. This can be carried out using event logs, performance monitors and network monitoring tools such as SNMP. Most firewall software can also provide a means of notifying the server administrator of a security breach.

3 Identify physical security issues.

Consideration should be given to the physical security of the server. Limit access to server rooms, backup tapes, physical locks and anti-theft devices.

4 Identify server room environmental issues.

The environment in which the server operates is very important to its health. Intermittent faults can be generated simply by the environment in which the server is located. Careful consideration should be given to the temperature and humidity of the room. The manufactures temperature recommendations of the server should be evaluated for this range.

Problems can include over heating, cracking of components in extreme cold, corrosion, ESD, creeping of components caused by varying temperatures at different times of the day, electronic short outs due to expansion and contraction. Power spikes, glitches, blackouts and brown outs are also a real problem on networks and are caused mainly by weather conditions and fluctuation on power lines. They can be prevented by implementing surge protectors, UPSs and back-up generators.

More extreme environment conditions should also be considered such as fire suppression and flood considerations. In most cases they can't be prevented but precaution can be in place to reduce damage such as CO2 fire extinguishers, fire proof backup safes, servers raised off the floor in flood warning areas, and servers, tapes placed on different levels of the building.

Outcome 4: Troubleshoot and resolve network server problems.

1 Identify network server problems.

Candidates should use questioning techniques in their solution to a problem candidates should be made aware of methods used in narrowing down faults. Methods used should include the use of senses such as listening to fans, beep codes, looking at LEDS on screen error messages etc. Contacting the correct person responsible for a problem is also very important, for example, a user logon denied should be dealt with by the administrator were as a hard drive fault would be a technician. Again candidates should identify problems using detail analysis such as what, where, when, how, who.

2 Carry out server diagnostics.

Faults should be set-up on the server to test candidates ability to identify, select and use diagnostic tools for a range of operating systems, identify and replace defective components, interpret system logs correctly, use documentation, locate and use hot fixes, perform remote troubleshooting. An example fault could be the stopping of a service on the server which should be remotely administered and restarted. Other examples would be to remove a IDE cable from a hard drive, power failure warning from UPS, IP address conflicts.

3 Determine server bottlenecks.

Candidates should diagnose and determine bottlenecks by using performance-monitoring results and logs to determine potential bottlenecks from processor, memory, disk space, bus transfer, NICs, network connectivity.

Outcome 5: Plan for network server disaster recovery.

1 Produce a disaster recovery plan.

The aim of disaster recovery is to reduce on downtime. Pro-active planning in the event of a disaster can drastically reduce the time a server is not operational, and is an important part in the administration of a server.

Higher National Unit specification: support notes (cont)

Unit title: Server Concepts

As with outcome 2 candidates should identify backup media, produce a backup plan, identify various backup methods, and a recovery plan. A range of backup media and methods should be explored such as tape, disk mirroring, ghosting, GFS rotation etc. The plan can be assessed in the form of several detailed logs.

2 Plan hardware redundancy.

Candidates should produce evidence in the form of a log to show they are actively planning for redundancy of hard drives, power supplies, fans, NICs, processors etc.

3 Describe fault tolerance techniques.

Evidence of a plan to incorporate fault tolerance should be logged incorporating one or more of the following: RAID Hot, warm, spare swaps. clustering, replication, mirroring, backup restore tests, hot and cold sites, hardware replacements.

Useful Links

www.webopedia.com
www.howstuffworks.com
www.pcguide.com

Server+ Vendors

www.comptia.org
www.vue.com/comptia/

Server+ Notes and Books

www.examnotes.net/
www.computer-books-4jp.co.uk/certification/server+.htm
www.certexams.com/comptia/server+/exam-details.htm

Network Operating Systems

www.microsoft.com
www.unix.com
www.novell.com
www.redhat.com

Server+ Multiple choice practice questions

www.cramsession.com

www.certcities.com
www.simulationexams.com

Internet Network Glossary Websites

www.clock.org/~jss/glossary/
www.techweb.com/encyclopedia/
www.zocalo.net/tng/glossary/glossary.html
www.svisions.com/ml/net-glossary.html

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 not a Unit which candidates are likely to find accessible at an introductory level; it is suggested that it be delivered only as part of an HNC/D program in Computing, Computer Networking or a related area, after candidates have experience of basic background topics involved in the hardware and software aspects of computer networks.

To minimise assessment overhead, sets of restricted-response 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).

Higher National Unit specification: support notes (cont)

Unit title: Server Concepts

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: Server Concepts

This is a 2-credit Unit at Level 7 intended for candidates undertaking a Computing or IT-related qualification who require an understanding of Network Server Hardware. It is designed to develop an understanding of the issues involved in installing and maintaining network servers. On completion of the Unit you should be able to:

- Plan the installation of a network server.
- Install and configure a network server.
- Upgrade and maintain a network server.
- Troubleshoot and resolve network server problems.
- Plan for network server disaster recovery.

In the first part of the course, you will study installing and configuring a network server, including planning the installation, installing a network server, configuring a network server and testing and documenting a network server configuration.

The second section covers upgrading a network server, including performing backups, adding hardware, upgrading BIOS/firmware, upgrading adapters, peripherals and service tools

The third section covers maintaining a network server, including evaluating server performance, performing housekeeping tasks, carrying out remote maintenance, identifying physical security issues and identifying server room environmental issues.

The fourth section covers troubleshooting network server problems, including identifying network server problems, carrying out server diagnostics and determining server bottlenecks

The final section covers planning for network server disaster recovery, including producing a disaster recovery plan, planning hardware redundancy and describing fault tolerance techniques.

There will be one or more closed-book multiple-choice assessment covering all outcomes. You will be presented with a total of 50 questions and expected to answer 70% 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 the CompTIA Server+ examination. Vendor certifications can change rapidly and you should check the current details at **www.comptia.org** to ensure that all objectives have been covered. The Network+ examination can also contribute to the Microsoft Certified System Administrator (MCSA) award. Full details can be found at **www.microsoft.com/traincert**