Next Generation Higher National Unit Specification

Infrastructure Maintenance and Support (SCQF level 8)

Unit code:	J7E6 48
SCQF level:	8 (24 SCQF credit points)
Valid from:	session 2023–24

Prototype unit specification for use in pilot delivery only (version 1.1) February 2024

This unit specification provides detailed information about the unit to ensure consistent and transparent assessment year on year.

This unit specification is for teachers and lecturers and contains all the mandatory information required to deliver and assess the unit.

This edition: February 2024 (version 1.1)

Unit purpose

This unit focuses on the concepts and techniques of building, securing and maintaining a network infrastructure in an enterprise.

This is a specialist unit, aimed at learners with an interest in the design, security, monitoring and maintenance of an enterprise network. It is of interest to learners with a STEM background or a vocational interest in computer networking, who wish to progress to more advanced levels and/or seek vendor qualifications. It is particularly suitable for learners who are studying HND Networking & Cloud Infrastructure or seeking a vendor qualification in networking.

Learners should have a basic understanding of computer networks and the fundamentals of how computers work. They can evidence this by units in computing at SCQF level 7 or higher, such as Network Infrastructure SCQF level 7 or Computer Science SCQF level 7.

When learners finish the unit, they will have a sound understanding of the concepts and techniques of securing and maintaining networks and the devices that enable them. They will have practical skills in monitoring network performance and implementing maintenance and security strategies.

Learners may progress to other units in computing technology and network operations, such as Cloud Computing or Cyber Security.

Unit outcomes

Learners who complete this unit can:

1 explain the benefits of network infrastructure maintenance
2 produce network documentation
3 secure an existing enterprise network
4 create an information archive procedure
5 analyse an enterprise network
6 perform a disaster recovery procedure

Evidence requirements

Learners must provide product and knowledge evidence.

Learners' product evidence must show that they can correctly secure, analyse and support a network from a given scenario or brief. The network must be of sufficient size and complexity to enable learners to produce evidence of the required standard. The evidence may be presented as a report, or a presentation. Assessor checklists may also be used to evidence successful completion of tasks.

The product evidence can be produced over an extended period in lightly-controlled conditions. In this case, authentication of the learner's work is required.

The knowledge evidence is the underpinning theory required for all outcomes. Learners must produce the evidence individually and without assistance. It must demonstrate the range of learners' understanding of the knowledge statements and their application.

You can sample the knowledge evidence when testing is used, but you must include at least one item from each of the following topics:

- Benefits of network maintenance
- Required documentation for network maintenance
- Network security — devices and mitigation strategies
- Backup and failover
- Network analytics and performance
- Disaster recovery

Learners must produce evidence under controlled conditions in terms of supervision, location, timing and access to reference materials.

Knowledge and skills

The following table shows the knowledge and skills covered by the unit outcomes:

Knowledge	Skills
Learners should understand: ♦ the benefits of network maintenance, including: — routine daily and weekly checks — environmental controls and checks — device checks — service checks ♦ network documentation, including: — network maps — network device inventory — software inventory, including update management — device updating (N-1 approach) — software updating (N-1 approach) ♦ how to secure a network, including: — endpoint security — security devices — types of devices — types of security appliance — basic device security — failover configuration — security threats and mitigation — security configuration — security threat mitigations — configuration compliance checking — staff training	Learners can: ♦ identify routine daily and weekly checks ♦ design appropriate daily and weekly check logs ♦ create documentation, including: — logical topology — physical topologies — network device hardware and software documentation — recording of device names, settings, firmware and software update details — document software updates and patch management ♦ identify network security issues with: — endpoint security — security devices — types of network attacks ♦ implement security features, including: — basic security — advanced security configuration — failover configuration — security threat mitigations — compliance checking — test and document ♦ create a checklist for staff training, including identifying areas of training

Knowledge	**Skills**
Learners should understand: ♦ network device and information archives, including: — IOS — configuration ♦ data, including: — types of backup — methods of backup — 3-2-1 backup rule — backup policy — failover and fail-back — configuration backup and/or change control — preparation for change (rollback testing) ♦ the analysis of an enterprise network, including: — the baseline — network tools — network infrastructure analyser — network traffic analyser — network performance monitors — IP address monitors — ping-based monitors — Wi-Fi analysers ♦ automated network monitoring and analysis software ♦ disaster recovery procedure advantages ♦ disaster recovery process	Learners can: ♦ create a data archive procedure for an enterprise network ♦ implement an archive procedure using: — IOS — configuration tool ♦ monitor a network using various tools ♦ perform an infrastructure disaster recovery process using: — the documentation created — IOS backups — configuration backups

Meta-skills

Throughout this unit, learners develop meta-skills to enhance their employability in the computing sector.

Self-management

This meta-skill includes:

- focusing: critically reviewing a network design and monitoring information to maintain and support the security and efficiency of the enterprise network
- initiative: displaying independent thinking with a readiness to get started

Social intelligence

This meta-skill includes:

- communicating: many peer-to-peer group opportunities to discuss various network maintenance, support and security aspects of an enterprise network
- collaborating: group discussions that generate new ideas and clarify understanding, helping the learner's ability to produce independent evidence

Innovation

This meta-skill includes:

- creativity: implementing any new technologies into their network; exploring alternative and current aspects of network support, security and maintenance
- critical thinking: researching current security issues and newly developed tools to maintain and support the efficiency of the enterprise network

Literacies

Throughout this unit, learners have opportunities to develop their literacy skills.

Numeracy

Learners develop numeracy skills by utilising numbers in network configurations and sizing, for example, IP addresses, port numbers, and network throughput.

Communication

Learners develop communication skills by participating in peer-to peer learning and collaborative working on network solutions.

Digital

Learners develop digital skills and computer literacy by using software tools to configure and monitor computer networks.

Delivery of unit

This unit provides learners with an understanding of how to secure, maintain and support an enterprise network. Although learners should have a basic understanding of networking and network devices, we expect you to include underlying networking concepts in your lessons to provide learners with important background information.

We suggest the following distribution of time:

Outcome 1 — Demonstrate an understanding of the benefits of infrastructure maintenance (5 hours)

Outcome 2 — Produce network documentation (30 hours)

Outcome 3 — Secure an existing enterprise network (30 hours)

Outcome 4 — Create an information archive procedure (20 hours)

Outcome 5 — Analyse an enterprise network (15 hours)

Outcome 6 — Perform a disaster recovery procedure (20 hours)

Professional recognition

This unit is not approved by any professional body; however, some aspects are relevant to the Cisco Certified Network Associate (CCNA) award. If learners continue in the networking field with the intention of gaining the CCNA award, most of the technologies covered in the unit are beneficial.

Additional guidance

The guidance in this section is not mandatory.

Content and context for this unit

Demonstrate an understanding of the benefits of network infrastructure maintenance (outcome 1)

Teach learners about the benefits of network maintenance, such as:

- a well-maintained network encounters few issues
- it makes it easier to troubleshoot
- it provides early identification of issues and faults
- it enables an engineer to pre-empt network repairs to avoid unscheduled downtime

Routine daily and weekly checks

Learners create a checklist that includes:

- environmental controls checks
- temperature checks
- humidity checks
- checking for leaks: either visually or checking that leak detection equipment is functioning
- fire suppression equipment checks: is the system functioning, checking for warning lights
- devices checks, including:
  - visual checking of devices: are they powered up, are there any warning lights
  - visual checks for damage
- checking that the current backup was successful
- service checks, including checks on:
  - file server, print server, web server, mail server
  - storage: the amount available and that there is an acceptable amount of free storage capacity
  - all applications and services to check that they are functioning correctly

Produce network documentation (outcome 2)

Learners produce network documentation including:

- topologies: created on paper or through a software tool, for example Packet Tracer or Visio
- device documentation: created on paper or through a software tool, for example Excel
- the make, model, IOS version, settings, device name, passwords, and IP configuration:
  - recorded software, firmware and software update details, created on paper or through a software tool, for example Excel
  - document patch management: created on paper or through a software tool, for example Excel

Secure an existing enterprise network (outcome 3)

Provide learners with a basic enterprise network topology that has been created in Packet Tracer so that they can configure selected features. They also need a computer device or a virtual machine to configure end devices and firewall options.

Learners can include information on the following:

- endpoint security
- Windows firewall
  - anti-virus
- security devices
  - types of firewall
  - IPS (intrusion protection system)
  - email security appliances
  - webserver appliances
- basic device security
  - passwords
  - secure shell (SSH)
- security threats, for example:
  - virtual local area network (VLAN) attacks
  - dynamic host configuration protocol (DHCP) attacks
  - address resolution protocol (ARP) attacks
  - spanning tree protocol (STP) attacks
  - other current attack types

- security threat mitigations, for example:
  - closing unused ports and services
  - securing ports
  - DHCP snooping
  - Dynamic trunking protocol (DTP)
  - Enabling DAI (dynamic ARP inspection)
  - using PortFast and bridge protocol data units (BPDU) guard
  - other current mitigations
- security configuration
  - VLANs
  - virtual private networks (VPNs)
  - first hop redundancy protocol (FHRP) and hot standby router protocol (HSRP)
- configuration compliance checking
- staff training on:
  - phishing
  - social engineering

Create an information archive procedure (outcome 4)

Learners create an informative archive procedure that includes:

- backing up IOS on network devices: using Packet Tracer and applying trivial file transfer protocol (TFTP)
- backing up configuration on network devices: using Packet Tracer and applying TFTP
- data: learners can use end devices or a virtual machine. Their archive procedure should include:
  - types of backup
  - methods of backup
  - 3-2-1 backup rule
  - backup policy
  - failover and fail-back
  - configuration backup and change control
  - preparation for change (rollback testing)

Analyse an enterprise network (outcome 5)

Teach learners about:

- the importance of a baseline
- network tools, including:
  - network infrastructure analyser
  - network traffic analyser
  - network performance monitors
  - IP address monitors
  - ping-based monitors
  - Wi-Fi analysers
  - other available tools
- automated network monitoring: you should discuss advantages and disadvantages

Some of the following offer a free download (or timed trials):

- SolarWinds NetFlow Traffic Analyser
- NetFlow Traffic Analyser
- Paessler PRTG network monitor
- NetSpot
- ipMonitor
- other available tools

Perform a disaster recovery procedure (outcome 6)

In this outcome, learners:

- recreate a topology using their logical and physical topologies from previous outcomes
- restore IOS and configuration from previous created archives

Approaches to assessment

Learners’ product evidence must show that they can correctly secure, analyse and support a network from a given scenario or brief. You should provide a brief relating to a network that is of sufficient size and complexity to enable learners to produce evidence to the required standard.

Your brief should require learners to analyse the network, secure the network and perform a disaster recovery procedure. It should also require them to document the network and create an information archive procedure.

Learners can provide evidence in the form of a report, or a presentation (recorded or live). You should use assessor checklists to evidence successful completion of tasks.

Equality and inclusion

This unit is designed to be as fair and as accessible as possible with no unnecessary barriers to learning or assessment.

You should take into account the needs of individual learners when planning learning experiences, selecting assessment methods or considering alternative evidence.

Guidance on assessment arrangements for disabled learners and/or those with additional support needs is available on the assessment arrangements web page.

Information for learners

Infrastructure Maintenance and Support (SCQF level 8)

This information explains:

- what the unit is about
- what you should know or be able to do before you start
- what you need to do during the unit
- opportunities for further learning and employment

This is a specialist unit that introduces you to the design, security, monitoring and maintenance of an enterprise network. It focuses on the concepts and techniques of building and maintaining a network infrastructure in an enterprise.

The unit is particularly relevant to anyone with a vocational interest in the networking field or who wants to progress to higher education and/or to seek vendor qualifications.

You gain a sound understanding of the concepts and techniques you need to maintain an enterprise network. You demonstrate an understanding of the principles of securing and maintaining an enterprise network, including:

- the benefits of infrastructure maintenance
- network documentation
- securing an existing enterprise network
- an information archive procedure
- analysing an enterprise network
- disaster recovery procedure

You also gain practical skills in monitoring the performance and implementing maintenance and security strategies.

You are assessed on both your theoretical and practical knowledge of supporting, securing and monitoring an enterprise network through a combination of written and practical tasks.

When you finish the unit, you can configure security techniques, document a network, create a maintenance procedure and monitor a network’s usage and performance.

You can:

- support an enterprise network
- document an enterprise network
- backup all aspects of a network infrastructure
- monitor an enterprise network
- perform a disaster recovery process

Throughout the unit, you develop meta-skills covering self-management, social intelligence and innovation.

You can progress to other units in computing technology and network operations, such as Cloud Computing or Cyber Security.

Administrative information

Published: February 2024 (version 1.1)

Superclass: CB

History of changes

Version	Description of change	Date
1.1	Minor amendments made in 'Additional Guidance' for Outcome 3, for clarification.	February 2024

Note: please check SQA's website to ensure you are using the most up-to-date version of this document.