Next Generation Higher National Unit Specification

Advanced Network Technology (SCQF level 8)

Unit code: J7E2 48

SCQF level: 8 (24 SCQF credit points)

Valid from: session 2023–24

Prototype unit specification for use in pilot delivery only (version 1.0) June 2023

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: June 2023 (version 1.0)

Unit purpose

This unit provides learners with an understanding of wide area network (WAN) technologies and secure network services required by converged applications in enterprise networks. During the unit they learn how to select the appropriate devices and technologies to meet network requirements.

This is a specialist unit, intended for learners with an interest in the design, implementation and maintenance of secure enterprise networks. The unit is suited to learners with a basic knowledge of network systems, devices and operations, who wish to understand the challenges of implementing and operating modern and future network technologies.

The unit covers the concepts and principles of network routing technologies, network security and WAN technologies.

On completion of the unit, learners can:

- implement and configure common routing protocols
- apply WAN security concepts
- understand the principles of traffic priority
- implement access control
- understand addressing services
- detect, troubleshoot, and correct common enterprise network implementation issues
- progress to other units that deal with more advanced aspects of networking

Unit outcomes

Learners who complete this unit can:

1 demonstrate an understanding of network routing technologies
2 explain the principles of network security
3 explain the concepts and applications of WAN technologies
4 plan, build and test a network to meet the requirements of a given brief

Evidence requirements

The unit requires both knowledge and product evidence.

Knowledge evidence

Learners' knowledge evidence should demonstrate that they have sufficient knowledge and understanding for each of the unit outcomes. Where this evidence is in a portfolio of work, such as reports, diagrams and screenshots, it must cover all of the knowledge in the 'Knowledge and skills' section.

You can sample the knowledge evidence when testing is used, but you must include at least the following:

- two items from routing algorithms
- two items from network segmentation
- one item from static routing
- two items from dynamic routing
- two items from bandwidth management
- two items from access control
- three items from intrusion detection and prevention
- two items from network address translation
- two items from network tunnelling
- two items from software-defined networking
- three items from WAN technologies

Learners' knowledge evidence must be produced under test conditions in terms of location, timing and access to reference materials.

Product evidence

Learners' product evidence should demonstrate that they can correctly plan, build and test a network from a brief that includes routing, network security and WAN technologies.

Learners' product evidence can include plans, diagrams, screenshots and printouts, and the observation checklists that you complete. The product evidence must cover the requirements set out in the brief.

Learners can produce product evidence over an extended period in lightly-controlled conditions. Learners should have access to learning materials. Evidence produced in lightly-controlled conditions must be authenticated. The Guide to Assessment provides further advice on methods of authentication.

Knowledge and skills

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

Knowledge	Skills
Learners should understand: **Routing technologies** ♦ contemporary routing algorithms and protocols ♦ network segmentation ♦ static routing: — default route — administrative distance — exterior versus interior — time to live ♦ dynamic routing: — protocols (routing internet protocol (RIP), open shortest path first (OSPF), enhanced interior gateway routing protocol (EIGRP), border gateway protocol (BGP)) — link state versus distance vector versus hybrid ♦ bandwidth management: — purpose — traffic shaping — quality of service (QoS) **Network security** ♦ access control: — access control lists (ACLs): purpose and types — data loss prevention — behavioural analytics	Learners can plan, build and test a network from a brief, to include: ♦ static routing ♦ dynamic routing ♦ at least two local area networks (LANs), connected via an exterior routing protocol ♦ at least one Internet Protocol version 4 (IPv4) access control list (ACL) and at least one Internet Protocol version 6 (IPv6) ACL ♦ basic traffic shaping ♦ load balancing and failover ♦ network address translation with port address translation ♦ implemented firewall technologies to allow implementation of a demilitarised zone (DMZ) ♦ configured user and server ports, using a minimum of 10 ports ♦ creation of a private tunnel between two parts of a network ♦ a script for a network configuration ♦ network testing at appropriate stages ♦ assessing network capacity and planning for increase ♦ noting the risks and vulnerabilities in decisions and actions ♦ a diagrammatic representation of networks

Knowledge	Skills
Learners should understand: **Network security (continued)** ♦ intrusion detection and prevention: — firewall technologies — threats, vulnerabilities and exploits — authentication methods — risk management — web security — port security ♦ network address translation: — benefits, types and methods of implementation — benefits: Internet Protocol (IP) address conservation, security — static — dynamic — overloading port address translation (PAT) — overlapping — secure network address translation (NAT) ♦ network tunnelling: — virtual private networking (VPN) — packet encapsulation — common tunnelling methods ♦ network automation: — monitoring and troubleshooting — remote network management ♦ software-defined networking (SDN): — SDN benefits: network control, dynamic load balancing, security, configuration management — types of SDN and their implementation **WAN technologies** ♦ operations (open systems interconnection (OSI) model) ♦ topologies	

Knowledge	Skills
Learners should understand: **WAN technologies (continued)** ♦ carrier connection technologies ♦ small office, campus, branch, and distributed ♦ circuit switching and packet switching techniques ♦ leased line ♦ ethernet over multiprotocol label switching (MPLS) **Health and safety** ♦ working safely and securely with network products	

Meta-skills

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

Self-management

This meta-skill includes:

- adapting: critically reviewing network designs and implementations; allowing for expansion and growth
- initiative: displaying independent thinking

Social intelligence

This meta-skill includes:

- communicating: sharing information
- collaborating: working in groups to discuss, analyse and formulate a solution to a given problem
- leading: independently finding solutions to compare and contrast with those of others

Innovation

This meta-skill includes:

- curiosity: exploring alternative and additional features and functions of networking design and implementation
- creativity: appreciating the alternatives available when designing and programming networks
- sense-making: understanding the innovative approaches that could be taken

Delivery of unit

You can deliver most of the knowledge and understanding in this unit through class and group instruction. You should take every opportunity to introduce real-world examples, opportunities for whole-class and group discussion, and practical demonstrations.

You should present concepts and terminology in context throughout the unit. Where appropriate, you should use video presentations to provide an alternative explanation of a difficult topic, or as a focus for class discussion or group work. Given the theoretical elements in the unit, a significant amount of time should be made available for revision, tutorials and formative assessment exercises.

You should strongly encourage learners to carry out further reading and provide opportunities for individual or group research. You must emphasise the relevance and currency of content in this rapidly evolving field.

Based on 120 hours of delivery and assessment time, we suggest the following distribution:

Outcome 1 — Demonstrate an understanding of network routing technologies (30 hours)

Outcome 2 — Explain the principles of network security (30 hours)

Outcome 3 — Explain the concepts and applications of WAN technologies (20 hours)

Outcome 4 — Plan, build and test a network to meet the requirements of a given brief (40 hours)

Professional recognition

There is no automatic professional recognition in this unit. However, if you deliver the unit using Cisco Networking Academy resources and learners take appropriate assessments and/or exams, there is an opportunity for vendor certification.

Additional guidance

The guidance in this section is not mandatory.

Content and context for this unit

Routing technologies

You should teach learners the theory of routing so they can understand the difference between link state, distance vector and hybrid routing protocols.

You should cover contemporary routing algorithms and protocols, such as:

- routing internet protocol (RIP)
- open shortest path first (OSPF)
- enhanced interior gateway routing protocol (EIGRP)
- border gateway protocol (BGP)
- any other contemporary routing protocols

You should cover bandwidth management, such as identifying different types of data (for example voice or video on demand), and traffic shaping policies and priorities for different types of traffic. Learners should also look at quality of service (QoS) guarantees for data throughput.

Network security

You should cover areas of network security, starting with looking at threats, vulnerabilities and exploits, with a view to putting mitigations in place. Mitigations could be the implementation of:

- access control lists (ACLs) of differing types
- intrusion detection and prevention using firewall technologies
- authentication methods
- web security
- port security

Network address translation

You should teach the benefits, types and methods of implementation of network address translation (NAT), taking into account IP address conservation and security benefits. You should cover both static and dynamic network address translation, as well as overloading, by use of port address translation (PAT) and secure NAT.

Network tunnelling

You should discuss the use of tunnelling to create VPNs. You should include a definition of what a VPN is, along with packet encapsulation techniques and the common tunnelling methods currently used, such as generic routing encapsulation (GRE), and GRE with internet protocol security (IPsec).

Network automation

You should cover the monitoring and troubleshooting of a network from a remote location, simple network management protocol (SNMP), and network automation in the event of failure, such as hot standby router protocol.

Software-defined networking (SDN)

You should show learners the benefits of SDN, including uses such as the control of a network, configuration management, dynamic load balancing and security.

You should cover types of SDN and their implementation and include open, application programming interfaces (API), overlay, and hybrid.

WAN concepts

You should cover the purpose of a WAN and WAN operations in relation to the OSI model. You should cover differing WAN topologies and carrier connection technologies to include situations such as small office, campus, branch or distributed networks. Learners should understand the difference between circuit switching and packet switching techniques, and current technologies such as leased line WANs and ethernet over MPLS.

Approaches to assessment

Learners' knowledge evidence can be produced from a question paper that satisfies the constraints in the 'Evidence requirements' section. Alternatively, they can produce a portfolio of evidence in the form of reports, designs, diagrams, screenshots or other forms that cover all the knowledge in the 'Knowledge and skills' section.

Learners can produce product evidence through assignments for each of the unit outcomes. However, we recommend that you use a single assessment that is sufficiently complex to enable learners to demonstrate all the skills listed in the 'Knowledge and skills' section. Learners should produce evidence for the unit individually and without assistance.

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: www.sqa.org.uk/assessmentarrangements.

Information for learners

Advanced Network Technology (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

Unit information

This is a specialist unit, intended for learners with an interest in the design, implementation and maintenance of secure enterprise networks.

The unit is of relevance to you if you have a basic knowledge of network systems, devices and operations and wish to understand the challenges of implementing and operating modern and future network technologies.

The unit covers a range of competencies including routing technologies, network security and wide area network (WAN) technologies.

The purpose of the unit is to provide you with an understanding of the WAN technologies and secure network services required by converged applications in enterprise networks. You learn how to select the appropriate devices and technologies to meet network requirements.

On completion of the unit, you can implement and configure common data link protocols. You can apply WAN security concepts, principles of traffic, access control, and addressing services. You can detect, troubleshoot, and correct the common enterprise network implementation issues that are covered by the following outcomes:

1 Demonstrate an understanding of network routing technologies
2 Explain the principles of network security
3 Explain the concepts and applications of WAN technologies
4 Plan, build and test a network to meet the requirements of a given brief

You must produce evidence to verify that you have knowledge and understanding of the concepts and principles of network routing, security, and WAN technologies. This could be produced by extended-response questions in test conditions or by maintaining a portfolio of work over the duration of the course.

You can produce portfolio evidence over an extended period in lightly-controlled, open-book conditions. Authentication is required to validate the integrity of your submission.

We may use a single assessment to demonstrate that you can evidence the skills required for the unit. You should produce this evidence on your own and without assistance.

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

On completion of the unit, you can progress to more advanced topics in networking and infrastructure.

Administrative information

Published: June 2023 (version 1.0)

Superclass: CB

History of changes

Version	Description of change	Date

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