Qualification specification

NCFE Level 4 Diploma: Network Engineer

QN: 603/7749/5

Qualification summary

Qualification title	NCFE Level 4 Diploma: Network Engineer		
Ofqual qualification number (QN)	603/7749/5	**Aim reference**	60377495
Guided learning hours (GLH)	512	**Total qualification time (TQT)**	1200
Minimum age	18+		
Qualification purpose	This qualification is designed to give learners the knowledge and associated skills and behaviours required to work in a variety of roles in network engineering. It will also prepare learners to progress to further study and apprenticeships in this area. This qualification is designed for learners who want to upskill or retrain within the digital sector. It is also suitable for learners who want to further their studies in the digital sector. This higher technical qualification (HTQ) will give learners the skills, knowledge and behaviours to meet specific employer needs and industry requirements.		
Grading	Pass/merit/distinction		
Assessment method	Occupationally Relevant Simulated Project Assessments (ORSPAs): Externally set, internally assessed and externally quality assured. Learners must complete one ORSPA as part of this qualification. Assignments: externally set, internally assessed and externally quality assured. Learners must complete 2 assignments as part of this qualification. Multiple-choice question paper: externally set and marked. Learners must complete one multiple-choice question paper as part of this qualification.		
Apprenticeship standards	This HTQ content has been aligned with the Network Engineer (Level 4) apprenticeship standard. This HTQ is designed to be delivered as a standalone qualification which is an alternative to an apprenticeship. It does not form part of an apprenticeship.		

Contents

Section 1: introduction

Please note this is a draft version of the qualification specification and is likely to be subject to change before the final version is produced for the launch of the qualification.

If you are using this qualification specification for planning purposes, please make sure that you are using the most recent version.

A higher technical qualification (HTQ) is a prestigious, kite-marked qualification aimed at meeting employers' needs and increasing learner engagement in level 4 or 5 technical education. For more information about HTQs, please visit www.instituteforapprenticeships.org/higher-technical-qualifications.

This HTQ content has been aligned with the Network Engineer apprenticeship standard.

This qualification aims to:

- provide the knowledge, skills and behaviours that are needed to enter occupations across the country
- be understood and recognised as high-quality by employers and so have national labour market currency
- give learners confidence that those qualifications are recognised by employers and are perceived to be a credible, prestigious, and distinct pathway

Aims and objectives

This qualification aims to:

- focus on the study of network engineering within the digital sector
- offer breadth and depth of study, incorporating a key core of knowledge
- provide opportunities to acquire a number of practical and technical skills

The objectives of this qualification are to provide learners with knowledge, skills and behaviours related to the following themes:

- architecture
- legislation, policies and procedures
- security
- stakeholder engagement
- hardware and software implementation
- troubleshooting and testing
- monitoring and maintenance

Support handbook

This qualification specification must be used alongside the mandatory support handbook on the qualifications page on the NCFE website, which contains additional supporting information to help with the planning, delivery and assessment.

This qualification specification contains all of the qualification-specific information you will need that is not covered in the support handbook.

Entry guidance

This qualification is designed for learners who want to begin or advance their career within network engineering. It is also suitable for learners who wish to progress to further study in this specialised area.

Entry is at the discretion of the centre.

There are no specific prior skills/knowledge a learner must have for this qualification. However, learners may find it helpful if they have already achieved a level 3 qualification.

Centres are responsible for ensuring that all learners are able to meet the requirements of the mandatory knowledge, skills and behaviours covered within this qualification.

Centres are responsible for ensuring that all learners are able to meet health and safety requirements.

Learners registered on this qualification should not undertake another qualification at the same level, or with the same/a similar title, as duplication of learning may affect funding eligibility.

Achieving this qualification

Diploma

To be awarded this qualification, learners are required to successfully complete all mandatory themes.

To achieve this qualification, learners must successfully demonstrate their achievement of all content as detailed in this qualification specification.

Total qualification time (TQT) and independent learning hours for this qualification

The expectation for independent study (non-guided learning hours) is much greater at level 4 and 5 than for lower-level qualifications. This is reflected in the total qualification time (TQT) which has been set for this qualification. Independent study hours are essential for personal development and reflection, allowing learners to develop transferable skills such as time management, goal setting and self-motivation.

Some examples of activities which can be included in independent learning hours include:

- preparation for assessments
- practising skills
- reading articles/texts from a recommended reading list
- research and inquiry
- watching videos/listening to podcasts
- reviewing recordings/notes from study sessions
- peer activities, including peer feedback, meetings and discussions
- reflection

Progression including job roles

Learners who achieve this qualification could progress to the following:

- employment:
  - network technician
  - network engineer
  - systems engineer
  - network administrator
  - network architect
  - desk based engineer
  - field based engineer
  - infrastructure engineer
  - dynamic network engineer
- further education:
  - related apprenticeships
- higher education

Staffing requirements

Centres delivering any of NCFE's qualifications must:

- have a sufficient number of appropriately qualified/experienced assessors to assess the volume of learners they intend to register
- have a sufficient number of appropriately qualified/experienced internal quality assurers to internally quality assure the anticipated number of assessors and learners
- ensure that all staff involved in assessment and internal quality assurance are provided with appropriate training and undertake meaningful and relevant continuing professional development
- implement effective internal quality assurance systems and processes to ensure all assessment decisions are reliable, valid, authentic, sufficient and current. This should include standardisation to ensure consistency of assessment
- provide all staff involved in the assessment process with sufficient time and resources to carry out their roles effectively

Resource requirements

Providers must ensure that the learner has access to the necessary materials, resources and workspaces for delivery and assessment.

- computer
- internet access
- audio/visual recording equipment
- software:
  - word processing (for example, MS Word, Google Docs)
  - presentation (for example, MS PowerPoint, Google Slides)
  - spreadsheet (for example, MS Excel, Google Sheets)
  - project management (for example, MS Excel, MS Project)
  - programming software (for example, TextEdit)
  - web browsers (for example, Chrome, Firefox, Edge)
- data sources (for example, online, social media, analytical)
- research resources (for example, online, books, journals)

- a web server
- routers
- switches
- servers
- desktops
- a telnet client (for example, PuTTY or Windows 10 Telnet)
- a hypervisor (for example, Windows Hyper-V or VirtualBox running an emulation virtual machine)

Real work environment (RWE) recommendation

Where the assessment requirements for a qualification allow, it is essential that centres wishing to operate a RWE do so in an environment that reflects a real work setting and replicates the key characteristics of the workplace in which the skill to be assessed is normally employed. This is often used to support simulation. Use of a RWE is not mandatory for this qualification.

How the qualification is assessed

Assessment is the process of measuring a learner's skill, knowledge and understanding against the standards set in a qualification.

The assessment consists of 4 components:

- ORSPA:
  - multi-site networking assessment
- controlled assessments:
  - physical hardware assignment
  - virtual network assignment
- multiple-choice question paper

Resubmission

For the occupationally relevant simulated project assessments, one resubmission will be allowed for learners who fail a component at the first attempt. In these circumstances, learners can only achieve a pass grade for the relevant component(s).

Resit

Learners may resit a component that is graded as not yet achieved. There is no limit on the number of resit attempts, however the assessments are only offered once per year.

Learners must have completed all assessment components to gain the NCFE Level 4 Diploma: Network Engineer (603/7749/5).

All the evidence generated by the learner will be assessed against the standards expected of a level 4 learner.

For the delivery of assessments please refer to the centre guidance and sample assessment materials found on our website.

External assessment

Each learner is required to undertake 4 external assessments.

External assessments are set by NCFE and marked by the centre. The assessment assesses learners' knowledge, skills and behaviours from across the qualification content.

Assessment	Themes	Knowledge and skills statements
1: Controlled assessment: physical hardware set up assignment	1, 3, 4, 6, 7	K1.1, K1.5, K1.6, K1.7, K1.8, K1.9, K1.10, K1.12, K5.3, K6.1, K6.2, K6.3 S1.1, S3.1, S4.1, S4.2, S4.4, S4.5, S6.1, S6.2, S6.3, S7.2, S7.3, S7.4, S7.5
2: Multiple-choice exam	1, 2, 3, 4, 7	K1.2, K1.4, K1.12, K1.13, K1.14, K2.1, K2.3, K3.1, K4.1, K4.2, K7.1, K7.2, K7.3, K7.4 S3.1, S4.1
3: Controlled assessment: virtual network assignment	1, 3, 4, 6, 7	K1.2, K1.3, K1.5, K1.6, K1.7, K1.8, K1.9, K1.10, K1.12, K6.1, K6.2, K6.3 S1.1, S3.1, S4.2, S6.1, S6.2, S6.3, S7.1, S7.2, S7.3, S7.4, S7.5
4: ORSPA: multi-site networking assignment	1, 2, 4, 5, 6	K1.1, K1.3, K1.4, K1.5, K1.6, K1.8, K1.9, K1.10, K1.11, K1.12, K2.2, K5.1, K6.1, K6.2, K6.3 S1.1, S2.1, S4.1, S4.3, S4.4, S5.1, S5.2, S6.1, S7.1, S7.2, S7.5

The external assessment consists solely of or of a combination of:

- set date and time (invigilated) – NCFE specifies the exact date and time that the external assessment must be administered in the centre
- assessment window (supervised) – the centre arranges supervised periods of external assessment within a set window
- independent self-study (ORSPAs) – these are completed independently by learners

The assessment is administered under specified assessment conditions.

Assessment	Hours/timings
1: Controlled assessment: physical hardware set up assignment	4 hours
2: Multiple-choice question exam	1.5 hours
3: Controlled assessment: virtual network assignment	8 hours

4: ORSPA: multi-site networking assignment	36 hours

For further information, centres should refer to the regulations for the conduct of external assessments and qualification specific instructions for delivery documents, available on the policies & documents page on the NCFE website.

Where qualifications have external assessment, centres must have entered learners using the Portal to access the assessment.

Centres must enter learners at least 10 working days in advance of the assessment window to avoid late entry fees.

If applicable, pre-release material will be made available by NCFE in advance of the assessment. All centres with entries will be notified.

The external assessment material will be sent out in time for the start of the assessment. Assessment materials must be kept secure at all times.

Enquiries about results

All enquiries relating to learners' results must be submitted in line with our enquiries and appeals about results and assessment decisions policy, which is available on the policies & documents page on the NCFE website.

Assessment windows

For assessments sat in windows, the centre must enter learners to the specified window. This will be either a set date and time assessment or a window in which the assessment will be completed.

For qualifications with 'entry on registration', the centre will choose the assessment window at the point of registering the learner.

The Level 4 Diploma: Network Engineer consists of 4 assessments with the following windows:

Assessment	Window	Themes covered
1: Controlled assessment: physical hardware set up assignment	2 week window, starting in December	1, 3, 4, 6, 7
2: Multiple-choice exam	Fixed date and time examination in February	1, 2, 3, 4, 7
3: Controlled assessment: virtual network assignment	2 week window, starting in April	1, 3, 4, 6, 7
4: ORSPA: multi-site networking assignment	4 week window, starting in June	1, 2, 4, 5, 6

Assessment windows have been set to ensure centres have time to deliver relevant content before the assessment is sat. In each case, centres should review the coverage, including detailed coverage listed in the external assessment table above, to plan their delivery.

Types of external assessment

Each learner is required to undertake an externally set multiple-choice question paper/short-answer question paper/assignment/project.

Multiple-choice question (MCQ) paper

The multiple-choice question (MCQ) paper will be assessed on a set date and time specified by NCFE. The MCQ assessment for the qualification is available through our online assessment service.

Online assessment

For more information about how to get started with online assessment, please go to the delivery and learner support page on the NCFE website.

For instructions on conducting online external assessments, please refer to our regulations for the conduct of external assessments and qualification specific instructions for delivery documents, available on the policies & documents page on the NCFE website.

External assessment conditions

For more information on external assessment conditions, please see the regulations for the conduct of external assessments and qualification specific instructions for delivery on the policies & documents page on the NCFE website.

To access the external assessment, centres need to ensure that learners are entered for the external assessment through the online assessment platform as appropriate.

Please refer to the external assessment timetable on the NCFE website for specific dates for assessment windows.

There is no limit to the number of attempts a learner can have on the multiple-choice question paper.

For instructions on conducting external assessments, please refer to our regulations for the conduct of external assessments and qualification specific instructions for delivery documents, available on the policies & documents page on the NCFE website.

Grading information

To achieve the qualification, learners must achieve at least a pass in all of the assessments (or, where relevant, a near pass in the multiple-choice question paper).

The learner's final qualification grade is made up of an aggregation of their achievement in each of the assessments, based on the assessments' proportional importance to the final grade – this is represented as a percentage weighting.

Assessments are assigned an incremental weighting based on their percentage weighting. Each grade is assigned a points value: pass = 1, merit = 3 and distinction = 5. The value of each grade in each assessment is determined by multiplying the incremental value by the grade value.

Assessment	% weighting	Incremental weighting	Distinction		Merit		Pass	
			Grade value	Points	Grade value	Points	Grade value	Points
1: Controlled assessment – physical hardware set up assignment	17.5%	7	5	35	3	21	1	7
2: Multiple-choice exam	15%	6	5	30	3	18	1	6
3: Controlled assessment – virtual network assignment	17.5%	7	5	35	3	21	1	7

4: ORSPA – multi-site networking assignment	50%	20	5	100	3	60	1	20

The points achieved in each assessment are summed and the total is used to determine the overall qualification grade based on the following values:

Points score	Grade
160–200	Distinction
80–159	Merit
40–79	Pass
0–39	NYA

Assessment grading

Assessment tasks for the controlled assessments and ORSPAs are set by NCFE and assessed by the centre. MCQs are externally marked by NCFE.

With the exception of some practical tasks, where a mark-based approach is taken, NCFE's controlled assessments and ORSPAs are judged by the centre using level of response grade descriptors, ranging from zero evidence (and therefore no achievement) through near pass, pass, merit and distinction standards. In each case, these descriptors are written to reflect the mid-point, rather than the borderline, of that standard.

This approach, including the use of a near pass grade, allows for a degree of compensation across the tasks and assessments, to ensure that the final grade fairly reflects the learner's achievement against the standard.

Overall grade boundaries are set at a mid-point between bands. For example, the overall pass boundary lies at the mid-point between bands 1 and 2, which are aligned to the grading standard associated with the near pass and pass grades respectively. The near pass grade allows learner evidence that may be below the pass standard, but still represents some achievement, to be recognised in the final assessment grade.

The grade boundaries are aligned to the qualification level grade descriptors at pass and distinction. These descriptors have been written as a description of the typical or mid-point pass and distinction standard required in the context of the purpose of the qualification.

This means that a learner will have to demonstrate the grade standard in at least half of the tasks, with the remaining half being demonstrated at the band below, in order to achieve the minimum requirement for the grade. The grading model also allows a compensatory approach to be taken for all possible combinations of assessment decisions. For example, while a learner will achieve an overall distinction if they achieve 50% of tasks at distinction standard and 50% at merit, they can also achieve an overall distinction if they achieve a pass standard in some tasks but compensate for this by achieving more than 50% of tasks at distinction.

A grading calculator has been provided to produce assessment grades based on task-based assessment decisions. Centres should use this calculator to calculate their overall assessment grades

before submission to NCFE of grades (other than for the multiple-choice test, where relevant). Values have been provided in the tables below for information.

Assessment 1: controlled assessment – physical hardware set up assignment

Task	Weighting	Band			
		N	P	M	D
Total	100%	20	40	60	80
1	80%	16	32	48	64
2	20%	4	8	12	16

Assessment 2: external assessment – multiple-choice exam

The multiple-choice question paper consists of 40 marks, with the following default grade boundaries:

Grade	Boundary
NYA	0
N	20
P	25
M	30
D	35

Assessment 3: controlled assessment – virtual network assignment

Task	Weighting	Band			
		N	P	M	D
Total	100%	20	40	60	80
1	60%	12	24	36	48
2	40%	8	16	24	32

Assessment 4: ORSPA – multi-site networking assignment

Task	Weighting	Band			
		N	P	M	D
Total	100%	20	40	60	80
1	27.5%	5.5	11	16.5	22
2	27.5%	5.5	11	16.5	22
3	17.5%	3.5	7	10.5	14
4	27.5%	5.5	11	16.5	22

Qualification grade descriptors

The following descriptors represent the standard expected of a learner at the relevant grade. They describe the mid-point or typical standard for that grade (they do not attempt to describe the borderline pass or borderline distinction standard – rather the mid-point or typical standard for that grade):

Grade	Demonstration of attainment
Pass	Evidence is logical and displays relevant knowledge in response to the demands of the relevant brief.
	The learner makes good use of relevant knowledge and understanding, including how it informs practices of the sector, and demonstrates an understanding of perspectives or approaches associated with data networking.
	The learner makes good use of facts/theories/approaches/concepts and is able to demonstrate a reasonable breadth and depth of knowledge and understanding covering multiple aspects of data networking.
	The learner is able to identify and extract technical and non-technical information from appropriate sources and makes use of appropriate information, including appraising the relevance of information, and can combine information to make decisions that are relevant to the context of the brief.
	The learner makes judgements and takes appropriate action, or seeks clarification with guidance, and is able to solve hardware and software / configuration problems (which are routine in the context of the brief) in physical and virtual networking scenarios.
	The learner is able to demonstrate skills and knowledge of the relevant concepts and techniques aligned with the network engineer role including the practical application of skills related to hardware and software as well as the assimilation of the provided client brief and its conversion to a working design applied across different contexts.
	The learner shows good understanding of potential areas of issues, such as physical, software, configuration, and people based, that have not been seen before, using their knowledge and understanding to find solutions to problems and make justifications for the chosen strategies for solving problems, with a good ability to explain their reasoning.
	The learner shows good understanding of how to take a client brief, interpret the requirements and present a proposed solution back to the client.
	The learner is able to analyse physical, software, and configuration problems to identify a root cause and then have the ability to apply the fix required to remediate.
	The learner is able to understand the importance of change management and the potential impact of uncontrolled change.
	The learner is able to demonstrate a good understanding of how security is linked to the work of a network engineer and identify areas where potential issues could have a security impact.
Merit	The learner can identify and extract technical and non-technical information from appropriate sources and make good use of appropriate information, including an informed appraisal of the relevance of information, and can combine multiple strands of information to make decisions that are relevant to the context of the given brief.
	The learner makes well-founded judgements, including seeking clarification of the appropriate action, and is able to solve hardware and software/configuration problems in a way that shows good knowledge of the subject matter in both a routine and non-routine context of the brief, in physical and simulated scenarios finding appropriate solutions to the context of the given brief.

	The learner is able to demonstrate a good skillset and knowledge of the relevant concepts and techniques aligned with the network engineer role, including good practical application of skills related to hardware and software, as well as the informed assimilation of the provided client brief and its conversion to a working design applied across different contexts.
	The learner shows good understanding of potential areas of issues, such as physical, software, configuration, and people based, that have not been seen before, using their extensive knowledge and understanding to find appropriate solutions to problems and making good justifications for the chosen strategies for solving problems, with a demonstrable ability to explain their reasoning.
	The learner shows good understanding of how to take a client brief, interpret the requirements and present a reasoned proposed solution back to the client with clarity and confidence.
	The learner shows a good understanding of the analysis of physical, software and configuration problems to successfully identify a root cause and then has the ability to apply the fix required to remediate the problem explaining the results.
	The learner shows good understanding of the importance of change management and an informed knowledge of the potential impact of uncontrolled change.
	The learner can demonstrate a good understanding of how security is linked to the work of a network engineer and an extensive ability to identify areas where potential issues could have a security impact recommending any changes required to remediate.
	The learner can identify and extract technical and non-technical information from appropriate sources and making good use of appropriate information, including an informed appraisal of the relevance of information, and can combine multiple strands of information to make decisions that are relevant to the context of the given brief.
	The learner makes well-founded judgements, including seeking clarification of the appropriate action, and is able to solve hardware and software/configuration problems in a way that shows good knowledge of the subject matter in both a routine and non-routine context of the brief and in physical and simulated scenarios finding appropriate solutions to the context of the given brief.
	The learner is able to demonstrate a good skillset and knowledge of the relevant concepts and techniques aligned with the network engineer role, including good practical application of skills related to hardware and software, as well as the informed assimilation of the provided client brief and its conversion to a working design applied across different contexts.
Distinction	Evidence is highly logical and detailed, providing an informative and relevant response to the demands of the relevant brief.
	The learner makes very effective use of relevant knowledge and a detailed understanding of the practices of the sector, and demonstrates a very well developed and effective understanding of the different perspectives and approaches associated with data networking.
	The learner makes good use of facts/theories/approaches/concepts, demonstrating breadth and depth of knowledge and a detailed understanding of data networking selecting the appropriate skills/techniques/methods to carry out any assigned work in an informed manner.
	The learner is able to identify and extract complex technical and non-technical information from appropriate sources and making extensive use of appropriate information, including a detailed appraisal of the relevance of information, and can combine multiple strands of information to make decisions that are relevant to the context of the given brief.

	The learner makes very well founded judgements including seeking clarification of the appropriate action, and is able to solve hardware and software / configuration problems in a way that shows detailed knowledge of the subject matter in both a routine and non-routine context of the brief, in physical and simulated scenarios finding suitable, lasting solutions to the context of the given brief.
	The learner is able to demonstrate extensive skills and knowledge of the relevant concepts and techniques aligned with the network engineer role including and extensive practical application of skills related to hardware and software as well as the comprehensive assimilation of the provided client brief and its conversion to a working design applied across different contexts.
	The learner shows excellent understanding of potential areas of issues, such as physical, software, configuration, and people based, that have not been seen before, using their comprehensive knowledge and understanding to find appropriate solutions to problems and making well-reasoned justifications for the chosen strategies for solving problems, with an excellent ability to explain their reasoning.
	The learner shows excellent understanding of how to take a client brief, interpret the requirements and present a well-reasoned proposed solution back to the client with clarity and confidence.
	The learner shows excellent understanding of the analysis of physical, software and configuration problems to successfully identify a root cause and then has the ability to quickly apply the fix required to remediate the problem explaining the results.
	The learner shows excellent understanding of the importance of change management and a comprehensive knowledge of the potential impact of uncontrolled change.
	The learner can demonstrate an excellent understanding of how security is linked to the work of a network engineer and a comprehensive ability to identify areas where potential issues could have a security impact recommending any changes required to remediate.

NCFE does not anticipate any changes to our aggregation methods or any overall grade thresholds; however, there may be exceptional circumstances in which it is necessary to do so to secure the maintenance of standards over time. Therefore, overall grade thresholds published within this qualification specification may be subject to change.

Section 2: qualification content

This section provides details of the structure and content of this qualification.

The explanation of terms explains how the terms used in the content are applied to this qualification. This document can be found in section 3.

Behavioural framework

Embedded within higher technical qualifications is the opportunity for learners to develop behaviours relevant to their chosen discipline, in line with the qualification's knowledge and skills.

The following table identifies opportunities to demonstrate the behaviours – embedded within the skills – that will be assessed as part of this higher technical qualification. Learners may also naturally demonstrate these behaviours elsewhere, beyond the listing below. All listed behaviours are subject to assessment.

B1: Work independently and demonstrate initiative, being resourceful when faced with a problem and taking responsibility for solving problems within their own remit
B2: Work securely
B3: Take a wider view of the strategic objectives of the tasks/projects they are working on, including the implications for accessibility by users and diversity
B4: Work to meet or exceed stakeholders' requirements and expectations
B5: Identify issues quickly, investigate and solve complex problems and apply appropriate solutions, ensuring the true root cause of any problem is found and a solution is identified which prevents recurrence
B6: Work effectively under pressure, showing resilience
B7: Committed to continued professional development in order to ensure growth in professional skill and knowledge

	Behaviours						
Themes	B1	B2	B3	B4	B5	B6	B7
1: Architecture							
2: Legislation, policies and procedures		S2.1					K2.1
3: Security	S3.1	S3.1			S3.1		
4: Stakeholder engagement			K4.2 S4.1 S4.2 S4.4 S4.5	K4.2 S4.1 S4.2 S4.4 S4.5		S4.3	
5: Hardware and software implementation	S5.1 S5.2	S5.1 S5.2			S5.2	S5.2 S5.2	K5.2 K5.3
6: Troubleshooting and testing	S6.1 S6.2 S6.3	S6.1 S6.2 S6.3			K6.1 K6.2 S6.2		

					S6.3		
7: Monitoring and maintenance	S7.4 S7.5	S7.4 S7.5		S7.2			

Theme 1: Architecture

Knowledge – What you need to teach	

K1.1	**The learner must understand the implementation factors of network architecture**
	
	• availability and continuity of service:
	  ○ redundant network connectivity
	  ○ resilient environment
	  ○ virtualisation vs physical
	  ○ cloud vs on-premises
	• secure by design:
	  ○ edge controls
	  ○ systems hardening
	  ○ industry good practice guidelines
	• optimisation of network performance:
	  ○ hardware:
	  ▪ server
	  ▪ devices
	  ○ software:
	  ▪ operating system (OS)
	  ▪ applications
	  ○ networking:
	  ▪ Voice over Internet Protocol (VoIP)
	  ▪ latency
	  ▪ load balancing
	• monitoring:
	  ○ performance
	  ○ security
	  ○ compliance
	  ○ environmental impact and carbon footprint:
	  ▪ power utilisation
	  ▪ cooling utilisation
	• back-up:
	  ○ schedule
	  ○ testing
	  ○ back-up type
	  ○ location

K1.2	**The learner must understand the types of virtualisation and virtualisation management systems applied within network architecture**
	
	• types of virtualisation:
	  ○ virtualised networking
	  ○ virtualised storage
	  ○ server virtualisation:
	  ▪ multihoming and mirroring services
	  ○ Virtual Desktop Infrastructure (VDI)

	• virtualisation management systems:
	  ○ hypervisor types:
	  ▪ type 1 – bare metal
	  ▪ type 2 – OS-based
	  ○ hardware virtualisation
	  ○ software-defined
	  ○ cloud-based virtualisation management systems

K1.3	**The learner must understand the architectural considerations and tools used within operating system and application management to meet specific requirements**
	
	• considerations:
	  ○ version management
	  ○ update methodology:
	  ▪ patch levels and security fixes
	  ▪ manufacture imposed improvements
	  ▪ end of life support
	  ○ security:
	  ▪ hardening
	  ▪ removal of defaults
	  ○ licence management
	  ○ remote performance monitoring
	  ○ network orchestration
	• tools:
	  ○ PowerShell
	  ○ Command Line Interface (CLI)
	  ○ scripting
	  ○ metadata – Windows Management Instrumentation (WMI)
	  ○ packet analyser/sniffer management console

K1.4	**The learner must understand the types, technologies and protocols of Voice over Internet Protocol (VoIP) architecture within network infrastructure**
	
	• types:
	  ○ on-premises
	  ○ cloud
	  ○ hybrid
	• technologies:
	  ○ hard phone:
	  ▪ network configuration
	  ○ soft phone:
	  ▪ mobile app
	  ▪ desktop app
	  ○ integration with unified coms
	• protocols:
	  ○ User Datagram Protocol (UDP)
	  ○ Session Integration Protocol (SIP)
	  ○ Real-time Transport Protocol (RTP)
	• Quality of Service (QoS):
	  ○ VoIP prioritisation on the network

K1.5 **The learner must understand the utilisation of protocols at the appropriate layer of the TCP/IP and OSI models**

TCP/IP	OSI	Applications and protocols	Devices
Application layer	Application layer	DHCP, DNS, FTP, HTTP, HTTPS, IMAP, NFS, SMTP, SNMP, Telnet, POP3, NTP	
	Presentation layer	TLS, SSL, SSH	
	Session layer	NFS, SMB, SIP, NetBIOS	
Transport layer	Transport layer	TCP, UDP	Firewall
Network layer	Network layer	IPv4, IPv6, NAT, ICMP, RIP	Router
Network access layer	Data link layer	VLAN, VRF, MAC, LLC	Switch, bridge, wireless access point
	Physical layer	Physical connectivity	Cable, hub

K1.6 **The learner must understand the network services provided by protocols at each layer of the TCP/IP model**

Application layer:

- Dynamic Host Configuration Protocol (DHCP) and addressing:
  - manages Internet Protocol (IP) addressing
  - provides network configuration for information
- Domain Name System (DNS):
  - translates domain names into IP addresses
- Simple Mail Transfer Protocol (SMTP):
  - enables electronic mail transmission
- Server Message Block (SMB):
  - enables users to communicate with remote computers and servers
  - allows shared use of resources
- Network Basic Input/Output System (NetBIOS):

- allows applications on different computers to communicate within a Local Area Network (LAN)

Transport layer:

- Transmission Control Protocol (TCP):
  - provides communication between applications on IP network hosts
  - reliable, ordered and error checked
- User Datagram Protocol (UDP):
  - establishes low-latency and loss-tolerating connections between applications
  - integrity verification of header and payload

Network access:

- Virtual Local Area Network (VLAN):
  - partitions and isolates broadcast domain
  - separates network traffic
  - groups hosts
- Virtual Routing and Forwarding (VRF):
  - enables multiple routing tables on the same router
  - allows packets to be forwarded between interfaces
  - segments network paths to separate traffic
- Medium Access Control (MAC):
  - hardware addressing for network devices
  - controls the hardware responsible for interaction with the wired, optical or wireless transmission medium
  - provides flow control and multiplexing for transmission
- Logical Link Control (LLC):
  - interface between MAC and network layer
  - allows multiple network protocols:
    - to coexist within a multipoint network
    - to be transported over the same network medium
  - provides flow control and multiplexing for the logical link

Network layer:

- IP – IPv4 and IPv6:
  - delivers packets from source host to destination
- Network Address Translation (NAT):
  - modifies IP addresses in transit
  - maps multiple hosts to one public IP address
  - conserves global addressing in IPv4
- Internet Control Message Protocol (ICMP):
  - sends error messages and operational information
- Routing Information Protocol (RIP):
  - creates and updates a routing table of optimal routes between network devices
  - prevents routing loops by limiting the number of hops (maximum 15)

K1.7 The learner must understand the application of related ports and protocols

Port	Protocol	Application
20	FTP – File Transfer Protocol	Transfer of files between IP systems
22	SSH – Secure Shell	Encrypted data transfer
23	Telnet	Remote access to communication systems
25	SMTP – Simple Mail Transfer Protocol	Communication between mail servers
53	DNS – Domain Name System	Translation of domain names into IP addresses
67/68	DHCP – Dynamic Host Configuration Protocol	Dynamically assigning IP addresses and network configuration
80	HTTP – Hypertext Transfer Protocol	Sending and receiving web client information
110	POP3 – Post Office Protocol	Email clients to retrieve and download email from a mail server
123	NTP – Network Time Protocol	Clock synchronisation between computer systems
137	NetBIOS – Network Basic Input/Output System	Allowing applications on separate computers to communicate over a local area network
143	IMAP – Internet Message Access Protocol	Management of email storage on a mail server
161	SNMP – Simple Network Management Protocol	Collecting and organising information about managed devices on IP networks

443	HTTPS – Hypertext Transfer Protocol Secure	HTTP traffic encrypted with Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
445	SMB – Server Message Block	Providing access to shared network resources, files and printers
465	SMTP with SSL/TLS	SMTP traffic encrypted with SSL/TLS
993	IMAP with SSL/TLS	IMAP traffic encrypted with SSL/TLS
995	SMTP with SSL/TLS	SMTP traffic encrypted with SSL/TLS
2049	NFS – Network File System	Allowing client computers access to files across a network
5060	SIP – Session Initiation Protocol	Initiating, maintaining and terminating real-time sessions for voice, video and messaging
5061	SIP with SSL/TLS	SIP traffic encrypted with SSL/TLS

K1.8 The learner must understand the components of physical and logical addressing

Physical addressing:

- Medium Access Control (MAC) addressing:
  - layer 2 network addressing:
    - set by manufacturer
  - 12 digit hexadecimal number (6 octets):
    - first 6 digits (3 octets):
      - Organisationally Unique Identifier (OUI)
    - second 6 digits (3 octets)
      - Network Interface Controller (NIC) specific address
  - format:
    - colon-hexadecimal notation (for example, 00:00:00:00:00:00)
    - hyphen-hexadecimal notation (for example, 00-00-00-00-00-00)
  - MAC address types:
    - unicast MAC address – network frame intended to reach one receiving NIC
    - multicast MAC address – network frame intended to be received by a group of NICs
    - broadcast MAC address – network frame sent to all NICs

Logical addressing:

- IP addressing:
  - layer 3 networking address
  - static or dynamic
  - assigned locally or by DHCP
- IP version 4 (IPv4):
  - dotted decimal notation with 4 octets
  - 32-bit/4-byte address
  - range 0.0.0.0 to 255.255.255.255
- IP version 6 (IPv6):
  - colon-hexadecimal notation with 8 quartets of four-digit hexadectets/hextets
  - 128-bit/16-byte address
  - successor to IPv4 addresses
- subnet:
  - logical partitioning of an IP network
  - increases efficiency of local traffic
  - represented as an IP address
  - IPv4 – dotted decimal
  - IPv6 – colon-hexadecimal

K1.9 The learner must understand the concepts and characteristics of switching and routing in networking

- switching:
  - switches data packets between devices on the same network
  - operates at OSI data link layer
  - directs traffic based on MAC address
  - records ports in MAC address table
- Multilayer Switching (MLS):
  - operates on multiple layers (data link and network layers)
  - hardware-based routing
  - lower latency routing due to multiple layers
- routing:
  - routes data packets between devices on different networks
  - operates at OSI network layer

- direct traffic based on IP address
- routing table to determine destination
- routing protocols:
  - interior gateway protocols:
    - RIP – calculates shortest route based on number of hops
    - Open Shortest Path First (OSPF) – calculates fastest route based on algorithm
  - exterior gateway protocol:
    - Border Gateway Protocol (BGP) – routes based on paths or manual configuration

- static routing:
  - non-adaptive
  - routing table manually configured
- dynamic routing:
  - adaptive
  - routing table updated dynamically

K1.10	**The learner must understand the characteristics of hierarchical network architecture and tiered network topologies**
	
	Characteristics of hierarchical network architecture:
	• scalable as additional devices can be easily added
	• resilient as they minimise single points of failure
	• structured layers of hierarchical network architecture:
	  ○ core layer:
	  ▪ provides the network backbone
	  ▪ connects and aggregates traffic from distribution layer devices
	  ▪ performed by low latency, highly reliable data link layer switches
	  ○ distribution layer:
	  ▪ provides services and control boundary between access and core layers
	  ▪ applies distribution policies (for example, traffic filtering, IPS and inter-VLAN routing)
	  ▪ performed by multi-layer switches
	  ○ access layer:
	  ▪ physically connects end devices to the network
	  ▪ applies network access policies
	  ▪ performed by data link layer switches
	
	Tiered network topologies:
	• 3 tier topologies:
	  ○ consist of core, distribution and access layers
	• 2 tier topologies:
	  ○ core and distribution layers are merged (collapsed) into a single layer

K1.11	**The learner must understand the functions of network technologies**
	
	• Network Access Control (NAC):
	  ○ defines access policies
	  ○ sets security standards for joining devices:
	  ▪ antivirus
	  ▪ updates/patching
	  ▪ system configuration
	  ○ facilitates network segregation
	• VLANs:
	  ○ virtual partitioning of network traffic
	  ○ virtual segregation of the network
	  ○ applies tags to network frames to identify VLAN traffic
	• Spanning Tree Protocol (STP):
	  ○ path cost-based algorithm to optimise network topology
	  ○ operates on a single active path
	  ○ dynamically resolves path failure
	• traffic filtering:
	  ○ rulesets used to filter traffic:
	  ▪ pass by criteria
	  ▪ deny by criteria
	• QoS:
	  ○ traffic prioritisation to guarantee a specified level of performance
	• Intrusion Detection and Prevention Systems (IDPS):
	  ○ used to monitor network activity
	  ○ identifies, logs and blocks any suspected malicious activity
	  ○ automatically updates to maintain library relevance

K1.12	**The learner must understand the types and roles of network border services in network design**
	
	• default gateways:
	  ○ facilitates connections between networks and network protocols
	  ○ used as a router of last resort
	• web gateway:
	  ○ separates user devices and the internet
	  ○ monitors web requests for compliance against configured policies
	  ○ blocks traffic from a malicious source
	• firewall:
	  ○ network perimeter security device
	  ○ monitors and controls all incoming and outgoing traffic
	  ○ blocks traffic based on rules
	• Next-Generation Firewall (NGFW):
	  ○ deep packet inspection
	  ○ identity management
	  ○ intrusion prevention
	• Demilitarized Zone (DMZ):
	  ○ subnetwork containing external-facing services
	  ○ firewalled from the rest of the network to maintain security

K1.13	**The learner must understand the types and configuration factors of wireless technologies within network architecture**
	
	• wireless technologies:
	  ○ 802.11x
	  ○ WiMAX
	  ○ Bluetooth
	  ○ cellular:
	  ▪ 3G
	  ▪ 4G
	  ▪ 5G
	  ○ satellite
	• configuration factors:
	  ○ capacity management:
	  ▪ speed/bandwidth
	  ▪ latency
	  ▪ contention
	  ○ distance
	  ○ antennae design:
	  ▪ omnidirectional
	  ▪ directional
	  ○ interference
	  ○ environmental factors
	  ○ security:
	  ▪ device security
	  ▪ network security
	  ▪ security/encryption of data in transit
	  ○ frequency
	  ○ licensing

K1.14	**The learner must understand the implementation and optimisation of cloud concepts**
	
	• cloud concepts:
	  ○ types of cloud deployment:
	  ▪ private
	  ▪ public
	  ▪ community
	  ▪ hybrid
	  ○ types of service:
	  ▪ infrastructure as a service (IaaS)
	  ▪ containers as a service (CaaS)
	  ▪ platform as a service (PaaS)
	  ▪ function as a service (FaaS)
	  ▪ software as a service (SaaS)
	  ▪ security as a service (SecaaS)
	• cloud implementation:
	  ○ assessment of current infrastructure
	  ○ selection of appropriate services
	  ○ infrastructure preparations
	• cloud optimisation:
	  ○ workload and associated costs
	  ○ performance and scalability requirements of the organisation
	  ○ resilience and continuity of service and systems
	  ○ power requirements and consumption

Skills – What you need to teach	

S1.1	**The learner must be able to apply appropriate network addressing and numerical systems to meet specification requirements**
	
	• review the requirements of the task
	• apply the appropriate numerical system to meet requirements:
	  ○ binary notation
	  ○ MAC address
	  ○ IPv4
	  ○ IPv6
	  ○ subnet

Theme 2: Legislation, policies and procedures

Knowledge – What you need to teach	

K2.1	**The learner must understand the appropriate legislation and policies which impact organisational procedures**
	
	• Data Protection Act 2018:
	  ○ related organisational policies:
	  ▪ personal access policy
	  ▪ data location policy
	  ▪ acceptable use policy
	  ○ impact:
	  ▪ data collection
	  ▪ data processing
	  ▪ data storage
	  ▪ compliance with appropriate standard operating procedures
	  ▪ continued professional development to ensure compliance with current legislation and associated policies
	• Computer Misuse Act 1990:
	  ○ related organisational policies:
	  ▪ IT security policy:
	  • email policy
	  • bring your own device (BYOD)
	  • internet use policy
	  • social media use policy
	  • clear screen policy
	  ▪ information security policy
	  ▪ access policy
	  ○ impact:
	  ▪ use of company assets
	  ▪ sharing of information
	  ▪ compliance with appropriate standard operating procedures
	  ▪ continued professional development to ensure compliance with current legislation and associated policies
	• Health and Safety at Work etc Act 1974:
	  ○ related organisational policies:
	  ▪ health and safety policy:
	  • fire prevention and control
	  • asbestos
	  • working at height
	  • manual handling
	  • electrical safety
	  • Portable Appliance Testing (PAT)
	  ○ impact:
	  ▪ use of appropriate personal protective equipment (PPE)
	  ▪ adaptations to working environment
	  ▪ compliance with appropriate standard operating procedures (SOPs)
	  ▪ continued professional development to ensure compliance with current legislation and associated policies
	• Waste Electrical and Electronic Equipment (WEEE) Regulations 2013:
	  ○ related organisational policies:
	  ▪ equipment disposal policy

	○ impact: ▪ recycling of devices and equipment ▪ disposal of devices and equipment ▪ compliance with appropriate SOPs ▪ continued professional development to ensure compliance with current legislation and associated policies
K2.2	**The learner must understand the role of a network engineer in business continuity (BC) and disaster recovery (DR) planning** • critical asset assessment and prioritisation (hardware, software and services): ○ risk of assets being unavailable ○ impact of assets being unavailable ○ number of users affected by assets being unavailable ○ effect of assets on other services • network design to achieve agreed Recovery Time Objectives (RTOs) for assets: ○ design considerations: ▪ network reliability ▪ network availability ▪ redundancy ▪ geographically diverse ○ planning considerations: ▪ minimise downtime ▪ failover (manually and automatic) ▪ power (redundancy) ▪ mirroring and load balancing: • RAID including levels • service mirroring • clustering • back-up schedule design to meet Recovery Point Objectives (RPOs): ○ data/system back-up ○ off-site storage ○ cloud storage • establishing agreed communication requirements with stakeholders • critical response team responsibilities • monitoring and testing: ○ environmental monitoring ○ alert configuration ○ regular testing and BC and DR plans
K2.3	**The learner must understand the factors involved when processing information in compliance with appropriate legislation, policies and procedures** • factors: ○ data accuracy: ▪ error correction ▪ updating data ▪ authenticity of change requests ○ data storage: ▪ location (for example, data centre) ▪ encryption ○ data sharing: ▪ data access permissions ▪ data anonymisation

	▪ data masking ○ data deletion: ▪ data retention ▪ data removal ○ data archiving: ▪ long-term storage of data ▪ data retrieval ○ data rights: ▪ legal rights of individuals under data protection legislation ▪ rights associated with minors ▪ rights associated with vulnerable adults ▪ legal proxy co-operation

Skills – What you need to teach	
S2.1	**The learner must be able to operate securely in compliance with appropriate legislation, policies and processes when completing network tasks** • assess the requirements of the task • review the associated legislation and policy parameters • identify appropriate SOPs • complete task in compliance with policy and SOPs

Theme 3: Security

Knowledge – What you need to teach	

K3.1	**The learner must understand the types of security threats and mitigation on IT infrastructure**
	
	• security threat types:
	  ○ active threat – threat to the integrity and availably of the system with deliberate action to modify transmitted or stored data:
	  ▪ Trojan
	  ▪ virus and worms
	  ▪ Distributed Denial-of-Service (DDoS)
	  ▪ formjacking
	  ▪ Cross-Site Scripting (XSS)
	  ▪ Man-in-the-Middle (MITM) attacks
	  ▪ social engineering
	  ▪ ransomware attack
	  ▪ Remote-Access Trojans (RATs)
	  ▪ Structured Query Language (SQL) injection
	  ▪ malware
	  ▪ botnets
	  ▪ cryptojacking
	  ▪ DNS poisoning attacks
	  ○ passive threat – threat to the confidentiality of data; data is observed and copied without modification or damage to system:
	  ▪ phishing attacks
	  ▪ spyware
	  ▪ backdoors
	  ▪ port scanning
	  ▪ botnet
	  ▪ drive-by downloads
	  ▪ rootkits and bootkits
	  ▪ exploits and exploit kits
	• mitigation controls:
	  ○ security vulnerability scanning
	  ○ anti-virus and anti-malware
	  ○ endpoint security
	  ○ firewalls
	  ○ access controls
	  ○ intrusion prevention and detection
	  ○ data loss prevention
	  ○ packet sniffers
	  ○ multi-factor authentication
	  ○ Virtual Private Network (VPN)
	  ○ device hardening and physical access

Skills – What you need to teach	

S3.1	**The learner must be able to maintain the security and performance of a network from security threats**
	
	• assess current performance against network and security baseline:
	  ○ review of system logs
	  ○ record changes against network and security baselines
	  ○ vulnerability scanning and reviewing against security baseline
	  ○ review current threat vectors against network and security baselines
	  ○ continually update baselines based on analysis of review and risk assessment
	• check physical security systems
	• apply the appropriate mitigation controls to threats
	• complete appropriate maintenance tasks:
	  ○ apply or remove access controls
	  ○ manage user rights and privileges:
	  ▪ Principle of Least Privilege (POLP)
	• review and maintain firewall rules
	• set logging and traps
	• apply network automated network monitoring tools
	• apply required updates:
	  ○ operating system
	  ○ device software
	• remove or disable unused services
	• update malware threat databases

Theme 4: Stakeholder engagement

Knowledge – What you need to teach	

K4.1	**The learner must understand the features of Service Level Agreements (SLAs)**
	
	• features of SLAs:
	  ○ scope of work or service
	  ○ roles and responsibilities of service provider and customer:
	  ▪ key contacts
	  ▪ agreed communication methods
	  ○ KPIs:
	  ▪ time of service
	  ▪ data rate
	  ▪ performance level
	  ▪ error rate
	  ▪ network availably
	  ○ service reviews
	  ○ support availability:
	  ▪ response
	  ▪ resolution
	  ○ back-up provision
	  ○ schedule maintenance
	  ○ DR and BCP provision
	  ○ termination process

K4.2	**The learner must understand the implementation factors of SLAs to meet stakeholder and organisational requirements**
	
	• communication with stakeholders:
	  ○ requirements of all stakeholders:
	  ▪ technical constraints
	  ▪ desired outcomes
	  ▪ timescales
	  ○ responsibilities of stakeholders:
	  ▪ job role
	  ▪ remit
	  ○ scope of communication:
	  ▪ format
	  ▪ frequency
	  ▪ technical/non-technical terminology
	  ▪ formal/non-formal language
	  ○ content and context:
	  ▪ cultural
	  ▪ accessibility
	  ▪ diversity
	• interpretation of stakeholder requirements against SLA features:
	  ○ identify stakeholder types:
	  ▪ manager
	  ▪ customer
	  ▪ colleague
	  ▪ technical specialist
	  ○ assessing requirements:
	  ▪ clarifying details and expectations with stakeholder

	○ creation of an action plan: ▪ assess possible options ▪ determine approach ○ implementing action plan: ▪ executing plan ▪ recording of progress and outcomes ○ reviewing outcomes against requirements • organisation and prioritisation of tasks: ○ reviewing SLAs and stakeholder requirements ○ planning to meet requirements: ▪ considering response and resolution times: • scheduling of tasks based on SLA prioritisation ▪ compliance with organisational processes: • reporting on non-compliance or delays ▪ organising and prioritising tasks based on requirements ▪ allocating levels of responsibilities

Skills – What you need to teach	
S4.1	**The learner must be able to appropriately communicate with a range of stakeholders** • review and record the requirements of stakeholders • identify and clarify the responsibilities of stakeholders • apply agreed communication scope • agree and apply content and context to meet requirements
S4.2	**The learner must be able to interpret and accurately implement requirements from different types of stakeholders** • identify stakeholder types • assess requirements of stakeholders • create appropriate action plan • implement action plan • review outcome against requirements
S4.3	**The learner must be able to plan and prioritise work tasks to meet organisational and stakeholder requirements** • review SLA and stakeholder requirements • plan to meet requirements: ○ organise and prioritise tasks based on SLAs and requirements: ▪ determine response and resolution times ○ allocate levels of responsibility ○ operate in compliance with organisational processes • schedule updates with stakeholders on progress and outcomes
S4.4	**The learner must be able to accurately record progress of tasks across a range of communication types in line with organisational requirements** • determine appropriate method of recording based on communication type: ○ types: ▪ face-to-face

	▪ remote ▪ written o methods: ▪ minutes ▪ digital recording: • visual • sound ▪ report • accurately record task details in compliance with organisational and stakeholder requirements: o level of detail o visualisation requirements: ▪ format ▪ use of technical and non-technical terms
S4.5	**The learner must be able to communicate and record outcome information to stakeholders in line with specific requirements** • clarify stakeholder requirements for presentation of outcome: o visualisation presentation • create the communication: o comply with organisational and stakeholder requirements o determine level of detail required o visualisation requirements: ▪ format o use of technical and non-technical terms • communicate appropriately with the required stakeholders: o comply with customer service and SLA requirements: ▪ timely communication ▪ accurate communication based on level and knowledge of stakeholder • accurately record outcome details in compliance with organisational procedures

Theme 5: Hardware and software implementation

Knowledge – What you need to teach	

K5.1	**The learner must understand the integration factors for implementing a server into a network**
	
	• define server specification:
	  ○ role of server:
	  ▪ email servers
	  ▪ web and proxy
	  ▪ file servers
	  ▪ print servers
	  ▪ database servers
	  ○ hardware requirements, restraints and limitations:
	  ▪ virtualised vs physical
	  ▪ cloud vs on-premises
	  ○ software requirements:
	  ▪ OS
	  ○ components of an implementation plan:
	  ▪ installation plan
	  ▪ design specification
	  ▪ risk register
	• assessment of current infrastructure:
	  ○ users
	  ○ traffic
	  ○ hardware needs
	  ○ software needs
	  ○ configurations:
	  ▪ policy management
	  ▪ internal domain management
	  ▪ organisation and groups
	  ▪ user management
	  ▪ proxy management and filtering
	  ▪ clustering and load balancing
	  ○ configuring DNS:
	  ▪ domain and directory services
	  ▪ internal authoritative servers
	  ▪ external authoritative servers
	  ▪ anti DNS spoofing techniques
	  ▪ A records
	  ▪ MX records
	  ▪ DNS caching
	  ○ configuring NTP:
	  ▪ connecting to authoritative stratum
	  ▪ synchronising network devices via NTP
	  ▪ use of NTP in system logging
	  ▪ client device dependency on NTP
	  ○ contractual agreements:
	  ▪ resilience and availability
	  ▪ use of standby routing
	  ▪ alternative failover gateways
	  ○ synchronising of data and services

K5.2	**The learner must understand the importance of continued professional development associated with hardware and software developments**
	
	• hardware upgrades:
	  ○ additional functionality
	  ○ End of Life (EOL) and End of Service Life (ESOL)
	  ○ removal or changes to existing functionality and tools
	• software upgrades:
	  ○ additional features
	  ○ compatibility
	  ○ licencing agreements

K5.3	**The learner must understand the process and application of techniques used to identify professional development needs** • strengths, weaknesses, opportunities, threats (SWOT) analysis • skills audit • skills matrix • direct feedback • critical analysis • target setting

Skills – What you need to teach	

S5.1	**The learner must be able to install and configure components of a secure network to meet requirements**
	
	• review specification requirements
	• create installation plan:
	  ○ installation plan
	  ○ design specification
	  ○ risk register
	• install the new components in line with plan
	• configure new components
	• test network against agreed requirements

S5.2	**The learner must be able to upgrade, apply and test system components and maximise efficiency when meeting stakeholder requirements**
	
	• review of system to identify what needs upgrading
	• review implications of potential upgrades
	• develop and agree upgrade plan with stakeholders:
	  ○ agree back-up strategy
	  ○ agree downtime
	  ○ agree roll-back strategy
	• upgrade hardware/software resources based on upgrade plan
	• test upgrade based on agreed upgrade plan

Theme 6: Troubleshooting and testing

Knowledge – What you need to teach	

K6.1	**The learner must understand causes and impact of failures within network and IT infrastructure**
	
	• causes:
	  ○ malicious:
	  ▪ internal
	  ▪ external
	  ○ poor or incorrect configuration/implementation
	  ○ hardware failure
	  ○ environmental factors (for example, power outage, flooding)
	  ○ connectivity failure
	• impact:
	  ○ financial:
	  ▪ loss of income:
	  • personal
	  • organisational
	  ○ reputational damage
	  ○ legal liability
	  ○ confidentiality of data held with IT systems:
	  ▪ covert monitoring of services
	  ▪ theft of data
	  ○ integrity of IT system:
	  ▪ ransomed services
	  ▪ malware infection
	  ▪ proxy abuse of services
	  ○ availability of the IT system:
	  ▪ loss of communication
	  ▪ overloaded devices
	  ▪ compromised services
	  ▪ denial of service

K6.2	**The learner must understand troubleshooting techniques and testing methods applied within a network**
	
	Troubleshooting techniques:
	• comparison against known working device/configuration
	• replacement of the defective component and monitoring if the problem reoccurs
	• testing based on route taken by packets from source to destination
	• OSI and TCP/IP layer-based troubleshooting techniques:
	  ○ bottom up – testing each layer of the model in turn starting with physical layer and progressing up to application layer
	  ○ top down – testing each layer of the model in turn starting with application layer and progressing down to physical layer
	  ○ testing starting with a hypothesized layer and moving up or down the model depending on test result of each layer
	
	Testing methods:
	• concept testing – reviewing the system to ensure it meets organisational requirements

	• penetration testing – of potential vulnerabilities in a network • configuration testing – testing hardware and software configurations for integration • peak load testing – testing a server's ability to handle large amounts of traffic • volume testing – testing a system's ability to handle large amounts of data • usability testing – testing the accessibility and useability of the system

K6.3	**The learner must understand the types of diagnostic techniques and tools used to gather system performance data**
	
	• analysis of traffic:
	  ○ trace back:
	  ▪ origin of the traffic
	  ▪ route the traffic has taken
	  ○ packet analysis and sniffers:
	  ▪ source of traffic
	  ▪ destination of traffic
	• analysis of network performance:
	  ○ ping:
	  ▪ response time
	  ▪ packet loss
	  ○ trace route:
	  ▪ traffic route
	  ▪ number of hops
	• analysis of system/application performance:
	  ○ Performance Monitor (PerfMon):
	  ▪ resource utilisation
	  ▪ CPU usage
	  ▪ memory usage
	• analysis of system logs:
	  ○ log file:
	  ▪ errors
	  ▪ warnings
	  ▪ timeline of the system tasks

Skills – What you need to teach	
S6.1	**The learner must be able to apply testing methods to a network** • assess and record the current network performance • identify components to be tested • select and apply appropriate testing method • review test results against recorded network performance

S6.2	**The learner must be able to apply the appropriate techniques and tools to identify systems performance issues**
	
	• review system performance
	• apply the appropriate diagnostic techniques and tools:
	  ○ analysis of traffic
	  ○ analysis of network performance
	  ○ analysis of system/application performance

	○ analysis of system logs • identify and record potential system performance issues
S6.3	**The learner must be able to troubleshoot performance issues and take appropriate action to support solution** • analyse available performance issue data • isolate issue to determine root cause • document issue • take appropriate action to support solution: ○ repair ○ escalate • record outcomes

Theme 7: Monitoring and maintenance

Knowledge – What you need to teach	

K7.1	**The learner must understand the purpose of different types of network maintenance**
	
	• proactive:
	  ○ monitoring, tuning and optimising to improve network performance
	  ○ planning for network upgrades and growth
	  ○ ensure and maintain compliance
	  ○ scheduled implementation of new hardware and software
	  ○ system lifecycle management
	• reactive:
	  ○ corrective action based on fault or failure
	  ○ change in circumstances and requirements

K7.2	**The learner must understand the requirements and implementation of change management on the network engineering role**
	
	• identification:
	  ○ reason for change:
	  ▪ update to systems or services
	  ▪ identified vulnerabilities to network or services
	  ▪ capacity increase
	  ▪ identified fault or failure with software, hardware or system
	  ▪ upgrade
	  ▪ configuration changes
	  ○ determine scope
	  ○ categorisation of change:
	  ▪ standard
	  ▪ normal
	  ▪ major
	  ▪ emergency
	• planning:
	  ○ resource requirements:
	  ▪ staffing/skills
	  ▪ financial
	  ▪ hardware/software
	  ▪ permissions
	  ○ communication:
	  ▪ identification of stakeholders
	  ▪ Responsible, Accountable, Consulted, Informed (RACI) model
	  ○ roll-back plan:
	  ▪ back out plan
	  ▪ regression testing
	  ▪ back-up
	  ▪ disaster recovery
	  ○ impact of change:
	  ▪ downtime
	  ▪ system access
	  ▪ direct and indirect services
	  ○ timescales
	  ○ prioritisation/urgency
	  ○ risk and issues management

	• assessment/approval:
	  ○ request for change:
	  ▪ standard format in compliance with organisational processes
	  ▪ detail all areas of change (for example, identification and planning)
	  ○ approver:
	  ▪ Change Advisory Board (CAB)
	  ▪ emergency CAB
	• implementation:
	  ○ implementing changes in compliance with agreed plan
	  ○ document change
	  ○ compliance with organisation policies and processes
	• review:
	  ○ functional testing
	  ○ user acceptance testing
	  ○ quality assurance
	• closure:
	  ○ record change in Configuration Management Database (CMDB)
	  ○ lessons learned
	  ○ close down report

K7.3	**The learner must understand the appropriate techniques that can be applied to optimise and monitor network performance**
	
	Optimisation techniques:
	• traffic shaping – managing bandwidth through a defined ruleset or policy:
	  ○ throttling
	  ○ rate limiting
	• QoS – prioritisation of specific traffic across a network:
	  ○ traffic classification:
	  ▪ prioritising classes of traffic for a specific requirement (for example, VoIP)
	• load balancing – distribution of a computing process:
	  ○ static
	  ○ dynamic
	• caching – storing frequently used data to serve faster in the future:
	  ○ web caching
	  ○ CPU caching
	  ○ disk caching
	  ○ localised distribution and delivery
	
	Monitoring tools:
	• packet analyser/sniffer software
	• network orchestration software
	• management console and dashboards
	• vendor specific hardware management tools

K7.4	**The learner must understand the considerations for the potential for automation of common network tasks**
	
	• considerations:
	  ○ requirements of task
	  ○ functionality of system
	  ○ tools available for automation
	• common network tasks:
	  ○ software and image deployment

	○ update/patch management and deployment ○ vulnerability and compliance scanning ○ back-up ○ virus scanning

Skills – What you need to teach	
S7.1	**The learner must be able to comply with the change management process when undertaking network engineering tasks** • identify the scope of the task • plan requirements to complete the task: ○ resource requirements ○ communication ○ roll-back plan ○ impact of change • submit plan for approval • implement the plan to meet requirement outcome: ○ document change ○ comply with organisation policies and processes • review and test outcome • record outcome and close task
S7.2	**The learner must be able to implement techniques to optimise performance to meet specification requirements** • review the specification requirements • assess requirements against current performance: ○ company requirements ○ technical requirements • implement appropriate optimising techniques: ○ traffic shaping ○ QoS ○ load balancing ○ caching • test new system performance and review against specification requirements
S7.3	**The learner must be able to utilise network monitoring tools** • assess the defined specification requirements • apply appropriate network performance monitoring tools • record and interpret performance outcomes • compare specification requirements with performance outcome data
S7.4	**The learner must be able to select and apply the appropriate tools when upgrading physical and virtual networks** • assess the requirements of the task • identify and apply the appropriate tools: ○ physical: ▪ SSH ▪ command line

	▪ vendor specific Graphical User Interface (GUI) ○ virtual: ▪ SSH ▪ command line ▪ vendor specific GUI ▪ software defined orchestration tools ▪ hypervisor management tools • comply with organisation polices and processes
S7.5	**The learner must be able to identify, plan and implement proactive maintenance procedures to monitor the performance of a network** • monitor and review performance: ○ resource utilisation ○ speed/latency ○ availability and uptime • plan and schedule regular maintenance tasks: ○ applying patches and updates ○ back-up • configure appropriate alerts and error reporting: ○ logging ○ SMTP alerts • implement regular security and compliance scanning: ○ vulnerability scanning ○ anti-virus/anti-malware • plan system lifecycle management: ○ hardware/software end of life ○ manufacture support ○ replacement

Section 3: explanation of terms

This table explains how the terms used at level 4 in the content are applied to this qualification (not all verbs are used in this qualification).

Analyse	Break the subject or complex situations into separate parts and examine each part in detail. Identify the main issues and show how the main ideas are related to practice and why they are important. Reference to current research or theory may support the analysis.
Critically analyse	This is a development of 'analyse' which explores limitations as well as positive aspects of the main ideas in order to form a reasoned opinion.
Clarify	Explain the information in a clear, concise way showing depth of understanding.
Classify	Organise accurately according to specific criteria.
Collate	Collect and present information arranged in sequence or logical order which is suitable for purpose.
Compare	Examine the subjects in detail, consider and contrast similarities and differences.
Critically compare	This is a development of 'compare' where the learner considers and contrasts the positive aspects and limitations of the subject.
Consider	Think carefully and write about a problem, action or decision showing how views and opinions have been developed.
Demonstrate	Show an in-depth understanding by describing, explaining, or illustrating using examples.
Describe	Provide a broad range of detailed information about the subject or item in a logical way.
Discuss	Write a detailed account which includes contrasting perspectives.
Draw conclusions (which…)	Make a final decision or judgement based on reasons.
Evaluate	Examine strengths and weaknesses, arguments for and against and/or similarities and differences. Judge the evidence from the different perspectives and make a valid conclusion or reasoned judgement. Apply current research or theories to support the evaluation.
Critically evaluate	This is a development of 'evaluate' where the learner debates the validity of claims from the opposing views and produces a convincing argument to support the conclusion or judgement.
Explain	Apply reasoning to account for how something is or to show understanding of underpinning concepts. Responses could include examples to support these reasons.

Identify	Apply an in-depth knowledge to give the main points accurately (a description may also be necessary to gain higher marks when using compensatory marking).
Justify	Give a detailed explanation of the reasons for actions or decisions.
Reflect	Learners should consider their actions, experiences or learning and the implications of these in order to suggest significant developments for practice and professional development.
Review and revise	Look back over the subject and make corrections or changes based on additional knowledge or experience.
Summarise	Give the main ideas or facts in a concise way to develop key issues.

Section 4: support

Support materials

The following support materials are available to assist with the delivery of this qualification and are available on the NCFE website:

- evidence and grading tracker
- learning resources
- qualification fact sheet

Useful websites

Centres may find the following websites helpful for information, materials and resources to assist with the delivery of this qualification:

- www.instituteforapprenticeships.org/
- www.legislation.gov.uk/

These links are provided as sources of potentially useful information for delivery/learning of this subject area. NCFE does not explicitly endorse any learning resources available on these websites. For official NCFE endorsed learning resources please see the additional and teaching materials sections on the qualification page on the NCFE website.

Reproduction of this document

Reproduction by approved centres is permissible for internal use under the following conditions:

- you may copy and paste any material from this document; however, we do not accept any liability for any incomplete or inaccurate copying and subsequent use of this information
- the use of PDF versions of our support materials on QualHub will ensure that correct and up-to-date information is provided to learners
- any photographs in this publication are either our exclusive property or used under licence from a third-party. They are protected under copyright law and cannot be reproduced, copied or manipulated in any form. This includes the use of any image or part of an image in individual or group projects and assessment materials. All images have a signed model release

Contact us

NCFE
Q6
Quorum Park
Benton Lane
Newcastle upon Tyne
NE12 8BT

Tel: 0191 239 8000*
Fax: 0191 239 8001
Email: customersupport@ncfe.org.uk
Websites: www.qualhub.co.uk
(www.ncfe.org.uk)

DRAFT/Version 1.0 June 2022
Information in this qualification specification is correct at the time of publishing but may be subject to change.

To continue to improve our levels of customer service, telephone calls may be recorded for training and quality purposes.