T-LEVELS | Institute for Apprenticeships & Technical Education

T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Network Cabling

Assignment 1

Mark scheme

v1.1: Additional sample material
16 November 2023
603/6901/2

NCFE

T Level Technical Qualification in Digital Support Services
Occupational specialism assessment (OSA)

Network Cabling

Mark scheme

Assignment 1

Contents

Marking guidelines

General guidelines

You must apply the following marking guidelines to all marking undertaken throughout the marking period. This is to ensure fairness to all students, who must receive the same treatment. You must mark the first student in exactly the same way as you mark the last.

- the mark scheme must be referred to throughout the marking period and applied consistently, do not change your approach to marking once you have been standardised
- reward students positively giving credit for what they have shown, rather than what they might have omitted
- utilise the whole mark range and always award full marks when the response merits them
- be prepared to award 0 marks if the student's response has no creditworthy material
- do not credit irrelevant material that does not answer the question, no matter how impressive the response might be
- the marks awarded for each response should be clearly and legibly recorded
- if you are in any doubt about the application of the mark scheme, you must consult with your team leader or the chief examiner

Guidelines for using extended response marking grids

Extended response marking grids have been designed to award a student's response holistically for the relevant task or question and should follow a best-fit approach. The grids are broken down into bands, with each band having an associated descriptor indicating the performance at that band. You should determine the band before determining the mark.

Depending on the amount of evidence that the task produces, the grids will either be a single, holistic grid that covers the range of relevant performance outcomes (POs), and will require you to make a judgement across all the evidence, or they will consist of multiple grids, that will be targeted at specific POs, and will require you to make a judgement across all the evidence in relation to that particular grid in each case, therefore making multiple judgements for a single task to arrive at a final set of marks. Where there are multiple grids for a particular task, it is important that you consider all the evidence against each of the grids, as although the grids will focus on particular POs, awardable evidence for each grid may come from across the range of evidence the student has produced for the task.

When determining a band, you should look at the overall quality of the response and reward students positively, rather than focusing on small omissions. If the response covers aspects at different bands, you should use a best-fit approach at this stage and use the available marks within the band to credit the response appropriately.

When determining a mark, your decision should be based on the quality of the response in relation to the descriptors. Standardisation materials, marked by the chief examiner, will help you with determining a mark. You will be able to use exemplar student responses to compare to live responses, to decide if it is the same, better or worse.

To support your judgement, the indicative content is structured in such a way that mirrors the order of the different points within the band descriptors. This will allow you to use the 2 in conjunction with each other by providing examples of the types of things to look for in the response, for each descriptor. In other words, the indicative

content provides you with a starting point of possible examples and the bands express the range of options available to you in terms of the quality of the response. You should apply the standards that have been set at relevant standardisation events in a consistent manner.

You are reminded that the indicative content provided under the marking grid is there as a guide, and therefore you must credit any other suitable responses a student may produce. It is not a requirement either that students must cover all of the indicative content to be awarded full marks.

Performance outcomes (POs)

This assessment requires students to:

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data

PO2: Install and test cabling in line with technical and security requirements

PO3: Discover, evaluate and apply reliable sources of knowledge

Task 1: designing the new network

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data

Band	Mark	Descriptor
4	10–12	Highly detailed and effective information relating to types of data (for example, VoIP, email, web traffic) which will be transmitted across the network and where the data is stored. Comprehensive description of a fully relevant range of security measures that will be put in place to best ensure the integrity and 24-hour availability of the network.
3	7–9	Effective information relating to types of data (for example, VoIP, email, web traffic) which will be transmitted across the network and where the data is stored, which may miss one or two points. Detailed description of most relevant security measures that will be put in place to best ensure the integrity and 24-hour availability of the network.
2	4–6	Some information relating to types of data (for example, VoIP, email, web traffic) which will be transmitted across the network and where the data is stored, which shows understanding, but is missing key points. Reasonable description of some security measures that will be put in place to best ensure the integrity and 24-hour availability of the network but may miss key measures.
1	1–3	Limited information relating to types of data (for example, VoIP, email, web traffic) which will be transmitted across the network and where the data is stored. Minimal or limited description of a few security measures that will be put in place to best ensure the integrity and 24-hour availability of the network.
	0	No creditworthy material.

Indicative content

The diagram/documentation describes how on-site and remote workers will access the network. It will also look at the security considerations associated with remote access.

Access to the network could be shown using a VPN and associated protocols (for example, IPsec). A VPN can be provided through the router (for example, Cisco ASA) or through a server.

Security considerations will include relevant information, for example:

- firewalls

- wireless access points (WAPs)
- encryption
- malware protection
- CCTV
- secure rooms
- alarm systems
- any other appropriate security control or measure

Integrity and 24-hour availability of the network can be achieved through:

- off-site backups
- cloud storage
- intrusion detection systems
- intrusion protection systems
- disaster recovery plans

Typical data will be related to the services (protocols) offered on the network, which will include VoIP data, e-mail (SMTP and POP), secure file transfer data (SFTP) and web traffic (HTTP and HTTPS). This can be extended to include lower-level communication protocols such as DNS, ARP and SNMP and packets, segments and frames.

Network data storage is shown through on-site servers such as SAN systems, file servers or off-site cloud-based storage, or a combination of both.

There should be the mention of user/group security permissions across the network, restricting file and printer access to certain users.

Relevant physical security measures are included, for example, lockable cabinet/secure room built, UPS should be available, redundant internet connections and redundant equipment available should anything fail.

In this scenario the student could consider:

- where the server cabinet should be located
- whilst phones have not been added to the diagram, phones are required on each desk
- if the small single storey building an issue?

Note: the above is not an exhaustive list; credit should be given to other suggestions as appropriate to the scenario in the brief.

PO2: Install and test cabling in line with technical and security requirements

Band	Mark	Descriptor
4	13–16	Comprehensive evidence of the networking resources required for the installation is included in the diagram and the documentation, which at the top of the band will include all the components needed to meet the requirements with highly detailed reference to specifications. Comprehensive detail relating to principles of transmission is included in the supporting text. There is highly detailed information regarding cable lengths and signal types in the network diagram, which takes into account the implications of the information.
3	9–12	Effective evidence of the networking resources required for the installation, which includes most components needed to meet the requirements with some reference to specifications. Students may have missed non-essential elements of the network, but the network will still be capable of functioning. Effective detail relating to principles of transmission that would be considered sufficient for a functioning network. There is detailed information regarding cable lengths and signal types in the network diagram, but this may not always take into account the implications of that information for the network.
2	5–8	There is some evidence of the networking resources required for the installation, which includes some components needed to meet the requirements, but in the lower half of the band this may not be clear enough to be sufficient for a functioning network. Some detail relating to principles of transmission is included. There is some information regarding cable lengths and signal types. In both cases, the detail and information may not be considered satisfactory for a functioning network.
1	1–4	Clearly insufficient evidence of the networking resources required for the installation, which may include a few components needed to meet the requirements, but not all. Limited detail relating to principles of transmission. Insufficient or very limited information regarding cable lengths and signal types.
	0	No creditworthy material.

Indicative content

The network design proposal will include relevant information such as:

- the factors of structured network cabling design
- architectural structure of network design and network topology

- the purpose and components of a network design specification
- a technical overview of the components
- components of customer statement of requirement (SOR)

Networking resources required for the installation will include tools and equipment used for network cabling.

Physical components of the network:

- networking devices:
  - firewalls
  - routers
  - switches
  - hubs
  - bridges
  - modems
  - WAPs (wireless access points)
  - media converter
  - wireless range extender
  - VoIP (voice over IP) endpoints
  - CCTV
  - Servers
  - network interfaces
  - cabling (and associated components)
- servers
- end-user devices (EUDs):
  - printers
  - PCs/workstations
- fixtures and fittings for telecommunications equipment
- any other appropriate physical elements

Types and features of connectors that can be applied within network cabling will be covered, including use of correct standards and their deployment.

Students will have identified media supporting other data services and the necessary precautions to prevent interference or damage to systems:

- identifying supporting media:
  - telecommunications
  - security systems, for example CCTV

- alarm systems
- AV (audio-visual) systems
- WAPs (wireless access points)

- precautions to mitigate interference or damage to systems:
  - clearly label service cables
  - utilise effective change management
  - plan and monitor integration of new supporting media:
    - check records
    - IP scanners
    - check cable codes
    - segregate wireless networks

Factors relating to communications principles will be covered and how they apply to network cabling:

- signal type:
  - electrical based
  - light-based
- security:
  - tampering
  - signal loss
- need for segregation from electrical cables:
  - susceptibility to interference:
    - types of interference, for example, electromagnetic impact on signal, static, crosstalk
    - mitigation techniques, for example, shielding, run cables in parallel

In this scenario the student could also consider:

- did they run the cables along the walls or through a suspended ceiling?
- are cables kept to a minimum in the office and have they mentioned the physical security of the cables in the office?
- did they consider wireless access and/or how to secure this?

Note: the above is not an exhaustive list; credit should be given to other suggestions as appropriate to the scenario in the brief.

PO3: Discover, evaluate and apply reliable sources of knowledge

Band	Marks	Descriptor
4	10–12	Shows exceptional, and, at the top of the band, very comprehensive, critical thinking regarding the choices and decisions made in relation to network design for the given scenario.
3	7–9	Shows a good amount of effective critical thinking regarding the choices and decisions made in relation to network design for the given scenario, covering most of the key elements.
2	4–6	Shows some critical thinking regarding the choices and decisions made in relation to network design for the given scenario but may miss some key elements.
1	1–3	Shows limited or very limited critical thinking regarding the choices and decisions made in relation to network design for the given scenario.
	0	No creditworthy material.

Indicative content

A demonstration of critical thinking will arise in the decisions made during the task in relation to the given scenario.

Areas include:

- applying the process of critical thinking
- identifying key information that will be taken into account (for example, most efficient use of digital technologies)
- applying evaluation techniques, for example, triangulation
- interpreting and analysing the validity of the outcome of critical thinking

In this scenario the student could consider:

- where the server cabinet is in the open office and how to secure it
- there is no previous wired network installed
- there is no previous security system in place

Note: the above is not an exhaustive list; credit should be given to other suggestions as appropriate to the scenario in the brief.

Task 2: creating the network diagram

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data

Band	Mark	Descriptor
4	10–12	Highly effective application of security measures to be put in place, which provides highly accurate and complete details of how network security will be achieved and why.
3	7–9	Effective application of security measures to be put in place, which provides details of how network security will be achieved and is accurate but may not be complete.
2	4–6	Some application of security measures to be put in place, which may miss key points and provides some details of how network security will be achieved but may not always be accurate.
1	1–3	Insufficient application of security measures to be put in place, with little insight into how network security will be achieved.
	0	No creditworthy material.

Indicative content

Details of the logical security measures with consideration for remote working are included, such as:

- remote workers using a VPN and associated protocols (for example, IPsec).
- security considerations are taken into account, for example:
  - password and user management through server (for example, Active Directory)
  - use secure protocols (for example, SFTP, IPsec)
  - restrict access to limited IP address ranges through DHCP server
  - put access to resources behind VPN connections in a DMZ
  - air gapping

Details of the physical security measures put in place to best ensure its integrity and 24-hour availability, for example:

- router firewall
- VPN server
- DMZ
- fire suppression (for example, sprinklers, extinguishers)

- security guards
- alarm systems
- visible surveillance systems
- biometrics
- air gapping
- PKI
- patching of server and client-side software
- UPS

In addition, they could also consider adding the following

- VoIP phones
- IP cameras
- TV in reception – PC or smart TV
- biometric/security equipment

Note: the above is not an exhaustive list; credit should be given to other suggestions as appropriate to the scenario in the brief.

PO2: Install and test cabling in line with technical and security requirements

Band	Marks	Descriptor
4	7–8	Packet Tracer network design covers all required elements comprehensively, including correct addressing, labelling and incorporating required servers and additional services. Thorough evidence of the networking resources required for the installation, fully aligned with the requirements and providing highly detailed security considerations. Highly detailed and comprehensive consideration of factors relating to principles of transmission with correct connector types, cables and data flow.
3	5–6	Packet Tracer network design covers most required elements with correct addressing and labelling. Detailed evidence of the networking resources required for the installation, mostly aligned with the requirements and providing accurate details of the security. Broad consideration of factors relating to principles of transmission with correct connector types and cables but may be missing some elements.

Band	Marks	Descriptor
2	3–4	Packet Tracer network design with reasonable detail but missing some key design elements. Some reasonable evidence of the networking resources required for the installation, which is partially aligned with the requirements, but missing some components. Reasonable consideration of factors relating to principles of transmission, showing understanding, but with some errors related to connector types and cables.
1	1–2	A minimal or incomplete Packet Tracer network design with limited detail. Limited evidence of the networking resources required for the installation, which may not be aligned with the requirements, using incorrect components or missing most components. Minimal or limited consideration of factors relating to principles of transmission with incorrect or missing connector types and cables.
	0	No creditworthy material.

Indicative content

Packet Tracer network design to include all devices, connectors, media and security measures that make up the network, together with all tools used for the network cabling.

Network topology will take into account all components, fixtures and fittings that make up the network, for example:

- core network components
- hybrid network components
- servers
- end-user devices (EUDs)
- fixtures and fittings for telecommunications equipment (such as cabinets and trunking/containment)
- any other physical elements

Factors relating to communications principles will have been taken into account, such as connector types, including copper and fibre.

Note: the above is not an exhaustive list; credit should be given to other suggestions as appropriate to the scenario in the brief.

Performance outcome (PO) grid

Task	PO1	PO2	PO3	Total
1	12	16	12	40
2	12	8		20
Total marks	**24**	**24**	**12**	**60**
% weighting	40%	40%	20%	100%

Document information

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Additional sample material		01 September 2023
v1.1	Sample added as watermark	November 2023	16 November 2023