T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Network Cabling

Assignment 3 – Pass

Guide standard exemplification materials

v2.0: Specimen assessment materials
19 June 2023
603/6901/2

Internal reference: DSS-GSEM-14

T Level Technical Qualification in Digital Support Services
Occupational specialism assessment

Guide standard exemplification materials

Network Cabling

Assignment 3

Contents

Introduction

The material within this document relates to the Network Cabling occupational specialism sample assessment. These exemplification materials are designed to give providers and students an indication of what would be expected for the lowest level of attainment required to achieve a pass or distinction grade.

The examiner commentary is provided to detail the judgements examiners will undertake when examining the student work. This is not intended to replace the information within the qualification specification and providers must refer to this for the content.

In assignment 3, the student must troubleshoot a set of faulty cables, troubleshoot a proposed cabling installation and carry out a risk assessment of the client's network.

After each live assessment series, authentic student evidence will be published with examiner commentary across the range of achievement.

Assignment 3

Scenario

You have just been hired as a junior network cabler to work at a large company. The roles and responsibilities of your new role include undertaking a range of implementation, monitoring and testing tasks, as well as ensuring that all work is documented appropriately to meet organisation quality standards and best working practice. Below are 3 tasks you have been given to complete.

Task 1: troubleshooting faulty cables

Time limit

1 hour 30 minutes

You can use the time how you want but all parts of the task must be completed within the time limit.

(25 marks)

As your first task you have been asked to fix several cables that one of the apprentices has incorrectly constructed, so they can be reused. The cables have various problems that need troubleshooting before they can be used in a cabling installation. Issues you may encounter include latency, jitter, cross talk and poor connections in the cables.

You are required to:

- test the cables to find and fix the faults in accordance with TIA/EIA 568B standards
- document the faults in the test plan template provided and record suitable solutions
- fix the fault on each cable and document the test results in the test plan template
- take photographs of the corrected cables which clearly show the connections of the internal wiring to the RJ45 and the coloured outer cable

You will have access to the following equipment:

- a hand-held cable/network tester
- a network impairment simulator/network delay simulator
- a digital camera
- a supply of RJ45 connectors

Evidence required for submission to NCFE

Completed test plan template in .pdf format.

For each cable you need to provide in .pdf format:

- a clear photograph showing a close up of the RJ45 connector and the corrected wires within it, with the coloured cable clearly visible
- a photograph of the read-out from the cable tester showing the full results of testing, with the coloured cable clearly visible

Student evidence

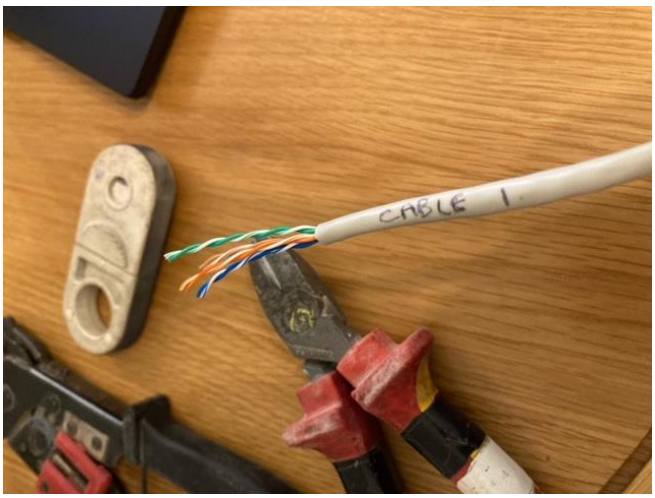
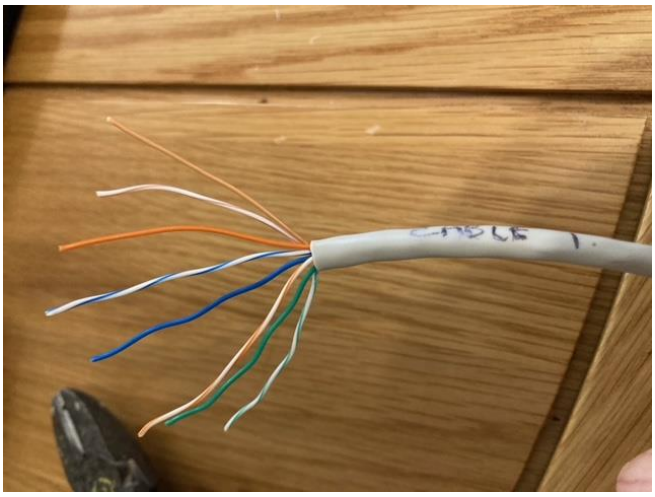
The table below shows the physical tests on the 5 cables.

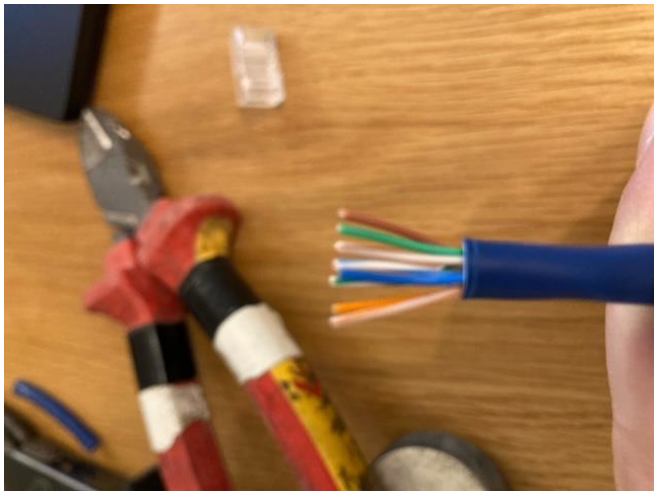
What is being tested?	How is it to be tested?	Expected outcome	Actual outcome	Solution	Remarks
Is the cable damaged	Look at it from end to end	Not damaged	Cable was ok	N/A	N/A
Are the RJ45 ends ok	Pull on the ends to make sure they stay on	Ends to stay on	They stayed on		
T568B standard	Visual check and network connectivity check with cable tester	Cables to be in the correct order	Wrong order	Redo the termination on the incorrect end and retest	Blue and green were mixed up. Once fixed the cable worked fine on the network tester

Does the cable work	Yes	The cable to work according to the network cable tester	It was successful	N/A	Had I performed this test earlier it would have failed but as I corrected the cable order in a previous test it worked

[Relevant photos supplied and annotated for which test they are for]

Equipment	

Cable 1: one RJ45 configured as cross-over cable. Produced on grey cable and labelled '**Cable 1**'.	  

Cable 2: short across wires inside one RJ45. Produced on blue cable and labelled '**Cable 2**'.	  

Cable 3: outer sheath of cable not gripped by crimp within one RJ45. Produced on green cable and labelled '**Cable 3**'.	 
Cable 4: one RJ45 has been wired 'upside down' but has not been crimped. Produced on yellow cable and labelled '**Cable 4**'.	

	
Cable 5: wires within one end of the cable do not reach the copper pins within the RJ45. Produced on purple cable and labelled '**Cable 5**'.	 

Task 2: troubleshooting the proposed cabling installation

Time limit

2 hours

You can use the time how you want but all parts of the task must be completed within the time limit.

(20 marks)

Your predecessor was in the process of designing 2 separate, interconnected networks for a law firm that is a client of your organisation. Unfortunately, because they have left the company, they were unable to finish the project. You have been asked by your manager to complete this project by troubleshooting and resolving any issues within the design of the interconnected networks.

You are to perform thorough troubleshooting of all cabling on the interconnected network design to identify and fix any faults identified prior to the customer conducting their own testing (UAT). You will describe how you will approach the troubleshooting, including why you will approach it that way, and record the results in a test plan.

You will be using the Cisco Packet Tracer file to carry out troubleshooting to ensure that data can be transmitted across all devices on the interconnected networks.

You must:

- write a brief description of how you will analyse, interpret and solve any issues which arise from the troubleshooting process - 4 marks are available for this element of the task
- document your troubleshooting in a logical order, demonstrating that no aspect of troubleshooting and analysis has been omitted
- use the test plan template provided to record the results of the troubleshooting
- you will have access to the following equipment:
    - word processing software
    - Cisco Packet Tracer

Evidence required for submission to NCFE

- screenshots of all issues identified and resolved within the Cisco Packet Tracer file, in .pdf format (this must be a before and after screenshot)
- completed test plan template in .pdf format
- written description of analysis and interpretation of issues, as well as solution of issues

Student evidence

I will first be completing connectivity tests to each device to diagnose problem areas. I will then attempt to correct any issues found, first checking the basics such as the cabling then moving onto the configuration if the simpler solutions do not resolve the issue.

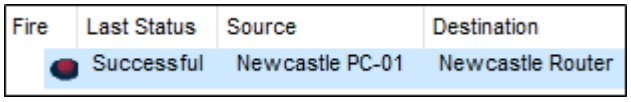
What is being tested?	How is it to be tested?	Expected outcome	Actual outcome	Solution	Remarks
Connectivity between routers	Ping	Successful ping	Success	N/A	As this was successful any issues that occur when testing site to site communication will not be the link between the sites
Connectivity from Newcastle server to Newcastle PCs	Ping	Successful ping	PC 01 – Success PC 02 – Success PC 03 – Success	N/A	N/A
Connectivity from Newcastle PCs to Newcastle server	Ping	Successful ping	PC 01 – Success PC 02 – Failed PC 03 – Success	The network port on PC02 was set to down, changed to up and repeated the test with success	With this issue I would have expected the server to not have been able to communicate but it could
Connectivity between London server and London PCs	Ping	Successful ping	PC 01 – Failed PC 02 – Failed PC 03 – Failed	The Fa0/1 port on the switch was misconfigured. After being set to up from down connectivity was achieved, however PC 01 could still not communicate but 02 and 03 could. 01 had	First checking the server, I saw no obvious reason these tests failed so this moved the investigation to the switch where the problem was discovered. Another issue was discovered with 01 and

				statically assigned IP addressing which were not correct for this network configuration after setting the IP addressing to DHCP the problem was resolved	resolved
Connectivity between London PCs and London server	Ping	Successful ping	PC 01 – Success PC 02 – Success PC 03 – Success	N/A	Some of these tests would likely have failed if not for the corrective work from the previous test
Connectivity between London and Newcastle servers	Ping	Successful ping	Failed Ping London server to London router – Success Ping Newcastle Server to Newcastle router – Failed	Removed Gig01 configuration on Newcastle router and moved it to Gig02 as this is the port being used and then enabled the port	N/A
Connectivity between London and Newcastle PCs	Ping	Successful ping	All successful	N/A	Previous resolutions ensured this test was successful

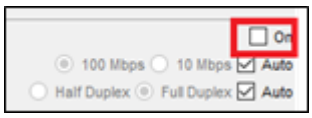
Check IP addressing is correct and DHCP is working Newcastle devices	Checking each device is configured correctly	All IP addressing to be configured correctly	All devices are configured correctly	N/A	Previous resolutions ensured addressing was correct on all PCs
Check IP addressing is correct and DHCP is working London devices	Checking each device is configured correctly	All IP addressing to be configured correctly	All devices are configured correctly	N/A	Previous resolutions ensured addressing was correct on all PCs

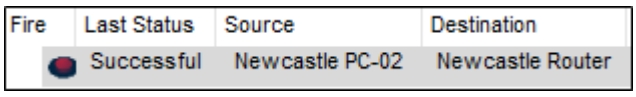
Fixing London server

Newcastle router fixed

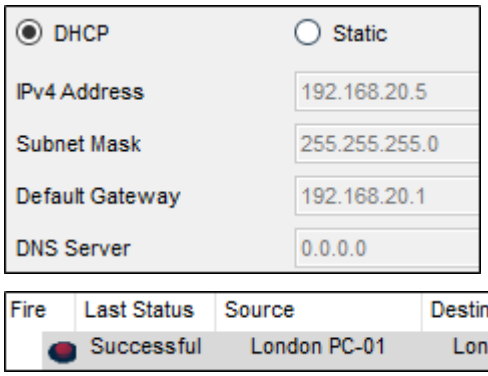


Newcastle PC-02 fixed

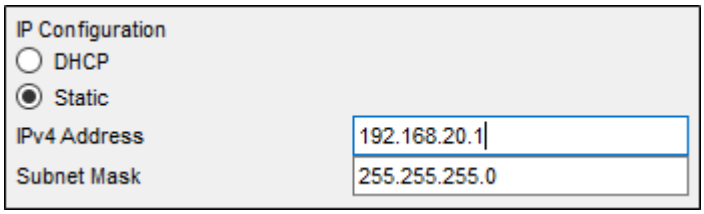




Fixing London PC-01



Fixing IP addressing on London server

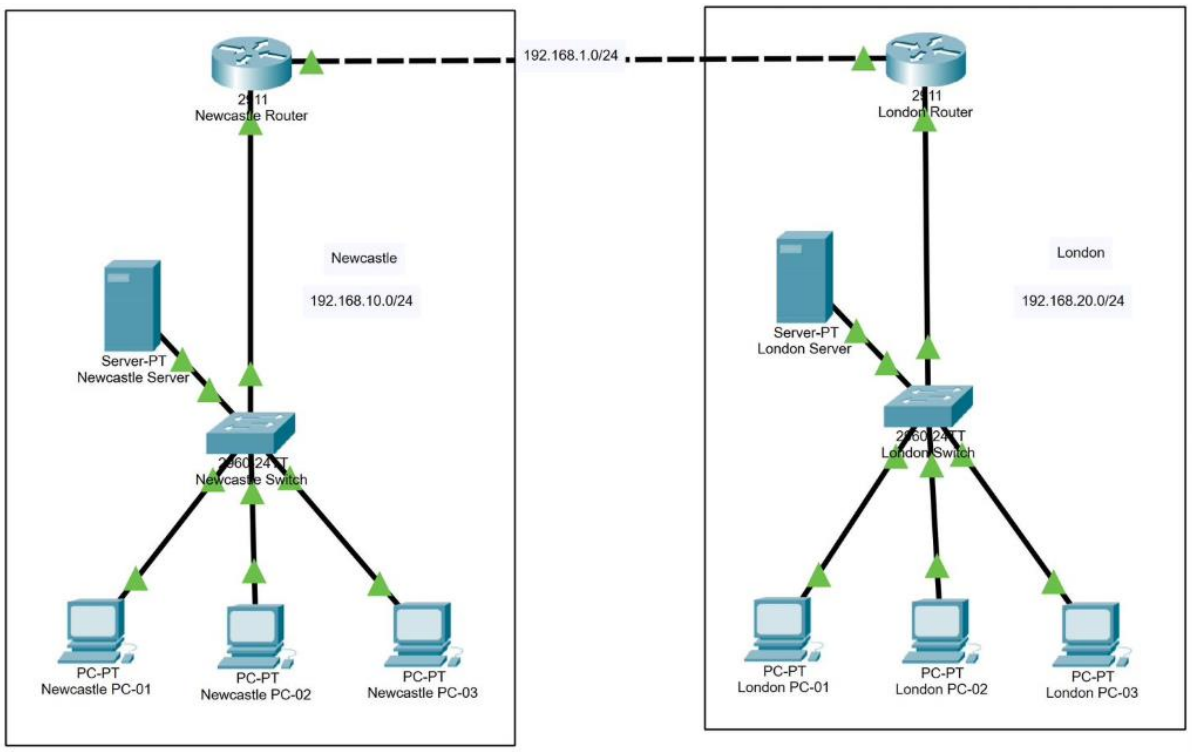


Task 3: carry out a risk assessment of the client's network

Time limit

2 hours

(16 marks)



The law firm in task 2 has now implemented your interconnected network design. You have been asked to perform a risk assessment on both the Newcastle and London sites. Your manager has given you the following details from an information gathering session that they attended.

Both sites are in industrial areas and have no record of flooding. They are in areas with a high level of reported crime. The 2 sites are linked through a site-to-site VPN configured on the routers and communication is vital between the 2 sites due to shared services. Both sites have high speed internet connections, so latency is rarely an issue. The London site also has a back-up mobile data (4G) connection.

Both sites have a single server. The London server is the law firm's domain controller and runs their DNS and DHCP. The Newcastle server is their file server and print server, however printing is rare and considered non-essential. Both servers have 4 network cards, however due to time constraints during the network setup only one was utilised.

Both sites have inert gas fire suppression systems for the server rooms to help prevent a fire from destroying the servers and switches. There are no other fire suppression systems installed in the rest of the building and fire safety relies on building evacuation. To prevent and detect intruders, the buildings are locked at night by the last member of staff to leave the building. All staff have a master key which can be used on any door in the building. There is currently no CCTV or burglar alarm system.

All infrastructure cabling is accessible due to easily opened trunking and floating ceilings. When your manager inspected this, they noted that Cat5e U/UTP cable is used for all machines and all infrastructure cabling. They also

noted that a large batch of the cabling was running parallel and near to the power cables. When inspecting the cabling, your manager noticed evidence of rodents possibly being above the floating ceiling.

The law firm has a large budget to pay for any changes that you recommend as a result of your risk assessment.

Your risk assessment should include:

- identification of possible threat to the interconnected networks
- vulnerability related to threat identified
- asset at risk
- impact if threat is exploited
- likelihood that threat is exploited
- overall risk to business
- recommended action
- type of control implemented as mitigation

You should consider:

- the information provided by your manager above
- both internal and external cabling
- security of the interconnected network on both sites
- all hardware network components
- documentation to support mitigation

You will have access to the following equipment:

- word processing software

Evidence required for submission to NCFE

Completed risk assessment document.

Student evidence

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Action	Control type
Rodents and wildlife damaging cables	Unprotected and exposed external cabling	Physical cables and data being transmitted	Medium Loss of service to customer Potential reputational damage for organisation Additional cost for replacement of cables	Medium Although the majority of cable is protected, some sections are exposed	Medium Cables are damaged by wildlife, leading to loss of service for client and damage to reputation for providing organisation	Ensure physical trunking protects cables in their entirety. Implement methods to deter wildlife where needed	Preventative
Loss of servers	Lack of redundancy with the networking to the servers Single point of failure for most services on the network	Services	Medium As each of these services are important to the network and a loss of either server will lose several of these services	Medium As the servers have no network redundancy, a single point of failure will result in a loss of services	High Users cannot log in Users cannot access file resources Users cannot navigate to webpages Users cannot print Devices cannot communicate on the network	Where possible implement power and network redundancy The servers have 4 network cards, utilising the 3 unused cards will give a large amount of network redundancy	Preventative
Loss of site to site link	Connection between sites	Connectivity Routers	Medium As servers to	Medium As there is	Medium Loss of	Consider installing secondary	Preventative

	Each router	Cabling	each site offer specific services and neither server offers a backup service	only one site to site link this can act as a single point of failure	services offered from each site to the other. This will result in the same risks as the “loss of servers” threat	fibre connections for a permanent secondary VPN connection	
Loss of internet at London	Main internet link Router	Connectivity and hardware	Low Potentially reduced productivity due to possibly slower 4G connection Loss of some services due to lost connectivity between sites	Low As there is a failover 4G connection the impact is minimum and may just result in slower connection speeds while the 4G connection is being used	Low Main impact is the loss of services supplied from the Newcastle site	A future consideration would be to upgrade this to a 5G connection once available or have it replaced with a secondary fibre or broadband connection	Acceptance Preventative
Loss of internet at Newcastle	Main internet link Router	Connectivity and hardware	Medium Loss of services from London site Productivity losses	Medium As there is no back up line here services are not only lost from the London site but there is a total loss of internet for the site	Medium Inability to complete work or use devices correctly on the network	Install a secondary 4G line Install a secondary fibre line at both sites to have a backup VPN connection	Preventative
Loss of a	The only	Connectivity	Medium	Medium	Medium	Install a	Preventative

network switch at either site	switches at each site	and hardware	Loss of services to both sites Financial loss dependant on down time Productivity loss	The lack of redundancy could lead to a serious network outage	Switch failure at either site	redundant switch at each site	
Theft/ malicious damage	Lack of security Same key for all doors in use by all staff	Physical assets	Medium Financial loss dependant on down time Financial loss dependant on damage/theft Productivity loss	High The area has a known high crime rate	Low Theft of equipment or damage of equipment with malicious intent	Install an alarm system and CCTV system Add signage about the security measures around the building	Deterrent Preventative

Risk levels:	**Business control types:**	**Mitigating control types:**
low | medium | high | critical	physical | administrative | technical	preventative | detective | corrective | deterrent | directive | compensating | acceptance

Assignment 3:

Examiner commentary

The student has performed enough tests on each cable to find the issue. Although it appears not many tests are being performed on this cable, a single test actually looks at multiple possible issues. Tests are named but the names might not be clear. The descriptions in each column although correct, lack detail. Any issues found are resolved and documented.

All testing that is required to complete the network and have it working have been completed but tests are not detailed in the table as in depth as they could be. Screenshots provided show only the problems and their resolutions but not the testing process or evidencing the tests, which worked without issue, which are some of the ways this submission could be improved.

All threats are applicable although there may not be a great range of threats, a major improvement for this submission would be to include a wider range with more detail in some of the weaker areas. The corrective actions are sensible for the threat and the impact and likelihood are appropriate. More detail in the recommendations and how they would improve the situations would push this higher up the marking band.

Overall grade descriptors

The performance outcomes form the basis of the overall grading descriptors for pass and distinction grades.

These grading descriptors have been developed to reflect the appropriate level of demand for students of other level 3 qualifications, the threshold competence requirements of the role and have been validated with employers within the sector to describe achievement appropriate to the role.

Occupational specialism overall grade descriptors:

Grade	Demonstration of attainment
Pass	The network diagrams are logical and display sufficient knowledge in response to the demands of the brief
	The student makes some use of relevant knowledge and understanding of network cabling theories and practices but demonstrates adequate understanding of perspectives or approaches associated with industry best practice.
	The student makes adequate use of facts/theories/approaches/concepts and attempts to demonstrate breadth and depth of knowledge and understanding in their designs and implementation, as well as in their testing and documentation.
	The student is able to identify some information from appropriate sources and makes use of appropriate information/appraise relevancy of information and can combine information to support decision making.
	The student makes sufficient judgements/takes some appropriate action/seeks clarification with guidance and is able to make adequate progress towards solving faults with network cables or

	resolving faults found in testing.
	The student attempts to demonstrate skills and knowledge of the relevant concepts and techniques reflected in network cabling, design and implementation and generally applies this across different contexts.
	The student shows adequate understanding of unstructured problems that have not been seen before, using sufficient knowledge to find solutions to problems and make some justification for strategies for solving problems.
Distinction	The network designed and developed is precise, logical and provides a detailed and informative resolution to the demands of the brief.
	The student makes extensive use of relevant knowledge and has extensive understanding of the network cabling practices and demonstrates an understanding of the different perspectives/approaches associated with designing, installing and testing networks.
	The student makes decisive use of facts/theories/approaches/concepts in their designs, demonstrating extensive breadth and depth of knowledge and understands and selects highly appropriate skills/techniques/methods to build and test their networks.
	The student is able to comprehensively identify information from a range of suitable sources and makes exceptional use of appropriate information/appraises relevancy of information and can combine information to make coherent decisions.
	The student makes well-founded judgements/takes appropriate action/seeks clarification and guidance and is able to use that to reflect on real life situations in resolving network cabling faults and network configuration.
	The student demonstrates extensive knowledge of relevant concepts and techniques reflected in network cabling, design and implementation and precisely applies this across a variety of contexts and tackles unstructured problems that have not been seen before, using their knowledge to analyse and find suitable solutions to the problems.
	The student can thoroughly examine network requirements in context and apply appropriate analysis in confirming or refuting conclusions and carrying out further work to justify strategies for solving problems, giving concise explanations for their reasoning.

* “Threshold competence” refers to a level of competence that:

- signifies that a student is well placed to develop full occupational competence, with further support and development, once in employment
- is as close to full occupational competence as can be reasonably expected of a student studying the TQ in a classroom-based setting (for example, in the classroom, workshops, simulated working and (where appropriate) supervised working environments)
- signifies that a student has achieved the level for a pass in relation to the relevant occupational specialism component

U grades

- if a student is not successful in reaching the minimum threshold for the core and/or occupational specialism component, they will be issued with a U grade

Document information

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Published final version.		May 2021
v1.1	NCFE rebrand		September 2021
v2.0	Annual review 2023: Amends to grade descriptors to ensure clarity	June 2023	19 June 2023