



# T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

## Network Cabling

Assignment 3 – Distinction

Guide standard exemplification materials

## T Level Technical Qualification in Digital Support Services Occupational specialism assessment

# Guide standard exemplification materials

## Network Cabling

Assignment 3

## Contents

<b>Introduction</b> .....	<b>3</b>
<b>Assignment 3</b> .....	<b>4</b>
<b>Scenario</b> .....	<b>4</b>
<b>Task 1:</b> .....	<b>4</b>
<b>Task 2:</b> .....	<b>13</b>
<b>Task 3:</b> .....	<b>27</b>
Examiner commentary .....	35
Overall grade descriptors .....	35
<b>Document information</b> .....	<b>37</b>
Change History Record .....	37

## 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 indicated the physical tests I have completed on each cable, the images below identify the 5 different cables, the issue and how I resolved them.

What is being tested?	How is it to be tested?	Expected outcome	Actual outcome	Solution	Remarks
Physical check - for cable damage	Checking the cable end to end thoroughly to ensure there is no obvious damage	Cable to be smooth with no feel of being buckled inside and no damage to the outer sleeve	Cable appeared to be damage free	N/A	Although the outer sleeve had some black marks on it this should not affect its performance
Physical check - RJ45 damage	Check both RJ45 ends to ensure they have no physical damage	Ends show no damage	Both ends show no sign of damage and both tabs are still intact	N/A	The tag on one end is a little looser but it is not loose enough to justify a new end
Physical check - crimped correctly	Check the RJ45 heads are firmly in place and the sleeve is clamped in the head	The RJ45 head not to come off the cable with an appropriate amount of force and the inner pairs of cable to be not visible outside of the boot	Cable ends did not come off and the cable appears to be clamped into the head firmly	N/A	N/A

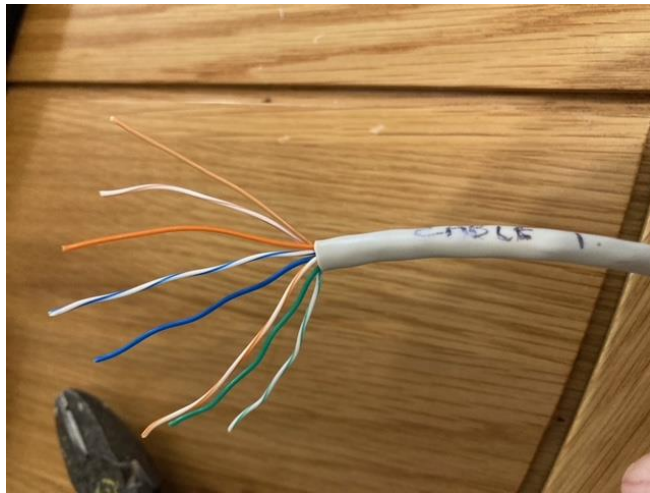
<p>Check against T568B standard</p>	<p>Use the cable tester to ensure connectivity on all pairs at both ends then check the cable order within the RJ45 head</p>	<p>Connectivity successful and the cable order to be (in either direction)</p> <p>Stripe orange                  Orange                  Stripe green                  Blue                  Stripe blue                  Green                  Stripe brown                  Brown</p>	<p>No connectivity, one of wires appears to be too short within the RJ45 head however they were in the correct order on both ends.</p>	<p>Cut the end of the cable off and terminate in a new RJ45 head.</p>	<p>The one short wire resulted in a failure. The solution was easy to implement as there was plenty of spare cable, had the cable already been the perfect length for its required task a new cable would have been required.</p>
-------------------------------------	--	--	--	---	---

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

**Equipment**

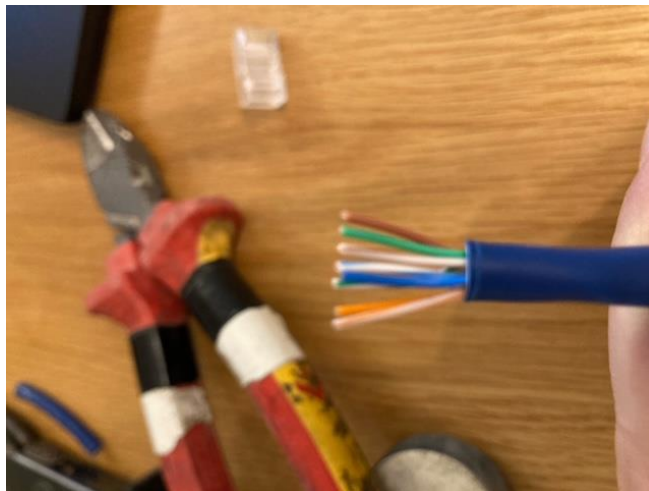


**Cable 1: one RJ45  
configured as cross-  
over cable – removed  
end and replaced.  
Labelled ‘Cable 1’**

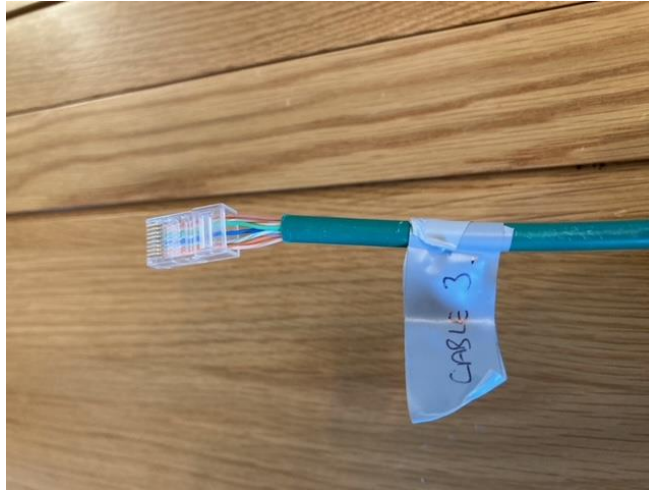




**Cable 2: short across wires inside one RJ45, replaced end and labelled 'Cable 2'**



**Cable 3: outer sheath of cable not gripped by crimp within one RJ45. Removed the end on the green cable and replaced – then labelled ‘Cable 3’**



**Cable 4: one RJ45 has been wired 'upside down' but has not been crimped, pulled off, replaced RJ45 and crimped. Then labelled 'Cable 4'**



**Cable 5: the wires within one end of the cable do not reach the copper pins within the RJ45, this was removed and replaced correctly. Then this was 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

To ensure the most efficient corrections are put in place to resolve the issues with the network I will be performing all testing first and not implementing any resolutions until all tests have been completed and the results of those tests recorded.

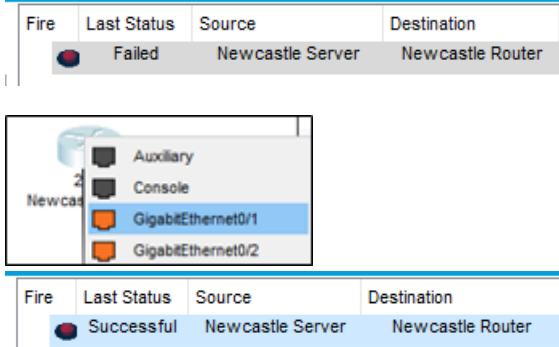
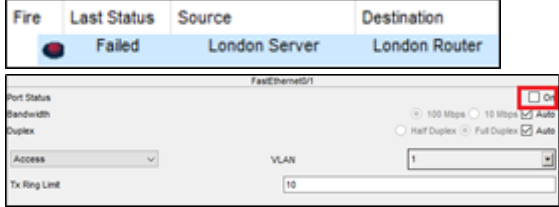
The testing will mostly consist of using the ping tool to confirm communication between devices and manually checking configuration of devices to ensure the details are correct.

Firstly, testing the connection between the 2 routers will be done as this is a simple test but any issues at this level will show up as failures in many other tests. Once done tests will be done on each site fully to see where connectivity issues lay within each network separately.




If there is an issue with the link between sites this will be resolved, then a test from communication between each device to the other site will be performed.

What is being tested?	How is it to be tested?	Expected outcome	Actual outcome	Solution	Remarks	Test
1.Connectivity of the site to site connection from each router	Ping from one router to the other	Successful communication	Success	N/a	N/a	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 4ms, Average = 2ms
2.Connectivity between Newcastle router and Newcastle switch	Ping between each device	Successful communication	Failed with the message "no functional ports"	This is due to the switch not having an IP address, but one is not required for communication	A none issue	
3.Connectivity between London router and London switch	Ping between each device	Successful communication	Failed with the message "no functional ports"	This is due to the switch not having an IP address, but one is not required for communication	A none issue	
4.Connectivity between Newcastle server and Newcastle switch	Ping between each device	Successful communication	Failed with the message "no functional ports"	This is due to the switch not having an IP address, but one is not required for	A none issue	

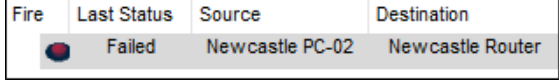
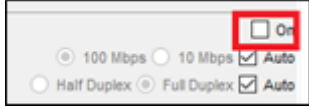
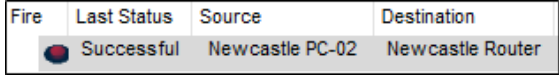


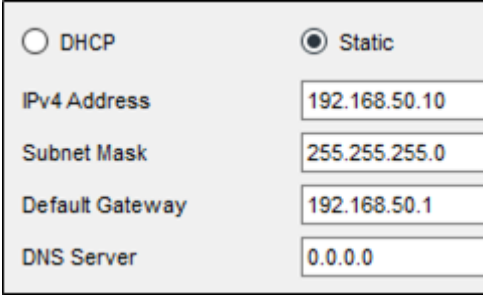
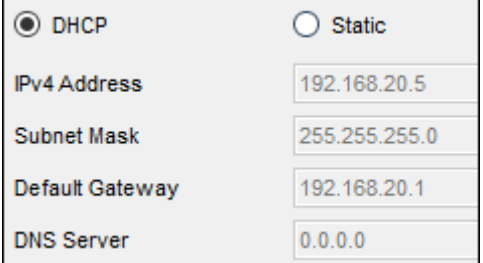
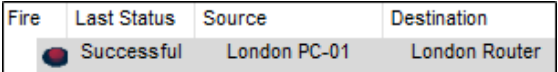
				communication		
5.Connectivity between Newcastle server and Newcastle router	Ping between each device	Successful communication	Ping failed	The cable was in the incorrect port. Moved from G0/2 to G0/1 which was properly configured.	N/a	
6.Connectivity between London server and London switch	Ping between each device	Successful communication	Failed with the message “no functional ports”	This is due to the switch not having an IP address, but one is not required for communication	A none issue	
7.Connectivity between London server and router	Ping between each device	Successful communication	Ping failed	Port F0/1 was disabled on the switch.	N/a	



						<table border="1"> <thead> <tr> <th>Fire</th> <th>Last Status</th> <th>Source</th> <th>Destination</th> </tr> </thead> <tbody> <tr> <td></td> <td>Successful</td> <td>London Server</td> <td>London Router</td> </tr> </tbody> </table>	Fire	Last Status	Source	Destination		Successful	London Server	London Router
Fire	Last Status	Source	Destination											
	Successful	London Server	London Router											
8.Connectivity between Newcastle PC-01 and Newcastle switch	Ping between each device	Successful communication	Failed with the message “no functional ports”	This is due to the switch not having an IP address, but one is not required for communication	A none issue									
9.Connectivity between Newcastle PC-02 and Newcastle switch	Ping between each device	Successful communication	Failed with the message “no functional ports”	This is due to the switch not having an IP address, but one is not required for communication	A none issue									
10.Connectivity between Newcastle PC-03 and Newcastle switch	Ping between each device	Successful communication	Failed with the message “no functional ports”	This is due to the switch not having an IP address, but one is not required for communication	A none issue									

11.Connectivity between London PC-01 and London switch	Ping between each device	Successful communication	Failed with the message “no functional ports”	This is due to the switch not having an IP address, but one is not required for communication	A none issue	
12.Connectivity between London PC-02 and London switch	Ping between each device	Successful communication	Failed with the message “no functional ports”	This is due to the switch not having an IP address, but one is not required for communication	A none issue	
13.Connectivity London PC-03 and London switch	Ping between each device	Successful communication	Failed with the message “no functional ports”	This is due to the switch not having an IP address, but one is not required for communication	A none issue	
14.Connectivity between Newcastle PC-01 and Newcastle router	Ping between each device	Successful communication	Communication failed	Cable was plugged into Gig0/2 on the router, after checking configuration of the other ports I discovered that Gig0/1 was	Another solution would have been to configure the Gig0/2 port to have the same IP addressing as Gig0/1 but the simpler solution was to move the	

				actually configured correctly, moving the cable from Gig0/2 to Gig0/1 resolved the issue.	cable.																	
15.Connectivity between Newcastle PC-02 and Newcastle router	Ping between each device	Successful communication	Communication failed	Fa0/1 on the PC was set to Down. Altering this to Up resolved the connectivity issue.	I expected the fix from the previous test to resolve this issue and when it did not further investigation was required on the device itself.	 <table border="1"> <thead> <tr> <th>Fire</th> <th>Last Status</th> <th>Source</th> <th>Destination</th> </tr> </thead> <tbody> <tr> <td></td> <td>Failed</td> <td>Newcastle PC-02</td> <td>Newcastle Router</td> </tr> </tbody> </table>   <table border="1"> <thead> <tr> <th>Fire</th> <th>Last Status</th> <th>Source</th> <th>Destination</th> </tr> </thead> <tbody> <tr> <td></td> <td>Successful</td> <td>Newcastle PC-02</td> <td>Newcastle Router</td> </tr> </tbody> </table>	Fire	Last Status	Source	Destination		Failed	Newcastle PC-02	Newcastle Router	Fire	Last Status	Source	Destination		Successful	Newcastle PC-02	Newcastle Router
Fire	Last Status	Source	Destination																			
	Failed	Newcastle PC-02	Newcastle Router																			
Fire	Last Status	Source	Destination																			
	Successful	Newcastle PC-02	Newcastle Router																			
16.Connectivity between Newcastle PC-03 and Newcastle router	Ping between each device	Successful communication	Communication failed	This connection now works with no further work. The misconfigured cable in a previous test has also resolved this issue	I also checked the IP addressing to ensure DHCP was working and it appears to be fine.																	

<p>17.Connectivity between London PC-01 and London router</p>	<p>Ping between each device</p>	<p>Successful communication</p>	<p>Communication failed</p>	<p>Address was set to static not DHCP.</p>	<p>The PC's IP addressing was set to static and had the wrong network address in. Resolving this did not resolve the issue so an investigation into the server revealed it was also configured correctly, this moved me onto the switch to discover the port the server was using was Down, marked it as Up and connectivity was achieved.</p>	  
<p>18.Connectivity between London PC-02 and London router</p>	<p>Ping between each device</p>	<p>Successful communication</p>	<p>Communication failed</p>	<p>Fixing the servers connectivity in the previous test appears to have resolved this machines connectivity issue after refreshing its DHCP</p>	<p>Previous connectivity issues caused by not being able to get an IP address as the server was not contactable.</p>	

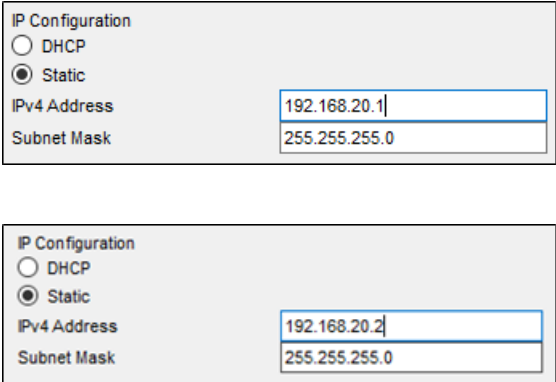
				information.		
19.Connectivity London PC-03 and London router	Ping between each device	Successful communication	Successful communication	Fixing the servers connectivity in the previous test appears to have resolved this machine's connectivity issue after refreshing its DHCP information.	Previous connectivity issues caused by not being able to get an IP address as the server was not contactable.	
20.Ping from server to server	Ping between each device	Successful communication	Successful communication	N/a	N/A	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 4ms, Average = 2ms

21.Connectivity between London PC-01 and Newcastle router	Ping between each device	Successful communication	Successful communication	N/a	N/a	<p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),                  Approximate round trip times in milli-seconds:                  Minimum = 2ms, Maximum = 4ms, Average = 2ms</p>
22.Connectivity between London PC-02 and Newcastle router	Ping between each device	Successful communication	Successful communication	N/a	N/a	<p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),                  Approximate round trip times in milli-seconds:                  Minimum = 2ms, Maximum = 4ms, Average = 2ms</p>
23.Connectivity London PC-03 and Newcastle router	Ping between each device	Successful communication	Successful communication	N/a	N/a	<p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),                  Approximate round trip times in milli-seconds:                  Minimum = 2ms, Maximum = 4ms, Average = 2ms</p>
24.Connectivity between Newcastle PC-01 and London router	Ping between each device	Successful communication	Successful communication	N/a	N/a	<p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),                  Approximate round trip times in milli-seconds:                  Minimum = 2ms, Maximum = 4ms, Average = 2ms</p>

25.Connectivity between Newcastle PC-02 and London router	Ping between each device	Successful communication	Successful communication	N/a	N/a	<p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),                  Approximate round trip times in milli-seconds:                  Minimum = 2ms, Maximum = 4ms, Average = 2ms</p>
26.Connectivity between Newcastle PC-03 and London router	Ping between each device	Successful communication	Successful communication	N/a	N/a	<p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),                  Approximate round trip times in milli-seconds:                  Minimum = 2ms, Maximum = 4ms, Average = 2ms</p>
27.Connectivity between London PC-01 and Newcastle server	Ping between each device	Successful communication	Successful communication	N/a	N/a	<p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),                  Approximate round trip times in milli-seconds:                  Minimum = 2ms, Maximum = 4ms, Average = 2ms</p>
28.Connectivity between London PC-02 and Newcastle server	Ping between each device	Successful communication	Successful communication	N/a	N/a	<p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),                  Approximate round trip times in milli-seconds:                  Minimum = 2ms, Maximum = 4ms, Average = 2ms</p>

29.Connectivity London PC-03 and Newcastle server	Ping between each device	Successful communication	Successful communication	N/a	N/a	<p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),                  Approximate round trip times in milli-seconds:                  Minimum = 2ms, Maximum = 4ms, Average = 2ms</p>
30.Connectivity between Newcastle PC- 01 and London server	Ping between each device	Successful communication	Successful communication	N/a	N/a	<p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),                  Approximate round trip times in milli-seconds:                  Minimum = 2ms, Maximum = 4ms, Average = 2ms</p>
31.Connectivity between Newcastle PC- 02 and London server	Ping between each device	Successful communication	Successful communication	N/a	N/a	<p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),                  Approximate round trip times in milli-seconds:                  Minimum = 2ms, Maximum = 4ms, Average = 2ms</p>
32.Connectivity between Newcastle PC- 03 and London server	Ping between each device	Successful communication	Successful communication	N/a	N/a	<p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),                  Approximate round trip times in milli-seconds:                  Minimum = 2ms, Maximum = 4ms, Average = 2ms</p>



<p>33.Ensure London Server has correct IP address details</p>	<p>Check the details manually</p>	<p>Details to be within the 192.168.20.0/24 scope</p>	<p>Correct IP address but the default gateway was pointing at the Newcastle router which would work but is not good practice.</p>	<p>Changed address to 192.168.20.1 for the server's default gateway</p>	<p>N/a</p>	
<p>34.Ensure Newcastle server has correct IP address details</p>	<p>Check the details manually</p>	<p>Details to be within the 192.168.10.0/24 scope</p>	<p>All correct</p>	<p>N/a</p>	<p>N/a</p>	
<p>35.Ensure DHCP is correctly configured on server at Newcastle</p>	<p>Manually check the server's configuration for the DHCP pool</p>	<p>192.168.10.0 pool with 255.255.255.0 subnet mask  And default gateway of 192.168.10.1</p>	<p>Configuration is correct</p>	<p>N/a</p>	<p>N/a</p>	
<p>36.Ensure DHCP is correctly</p>	<p>Manually check the server's configuration for</p>	<p>192.168.20.0 pool with 255.255.255.0</p>	<p>Configuration is correct</p>	<p>N/a</p>	<p>N/a</p>	

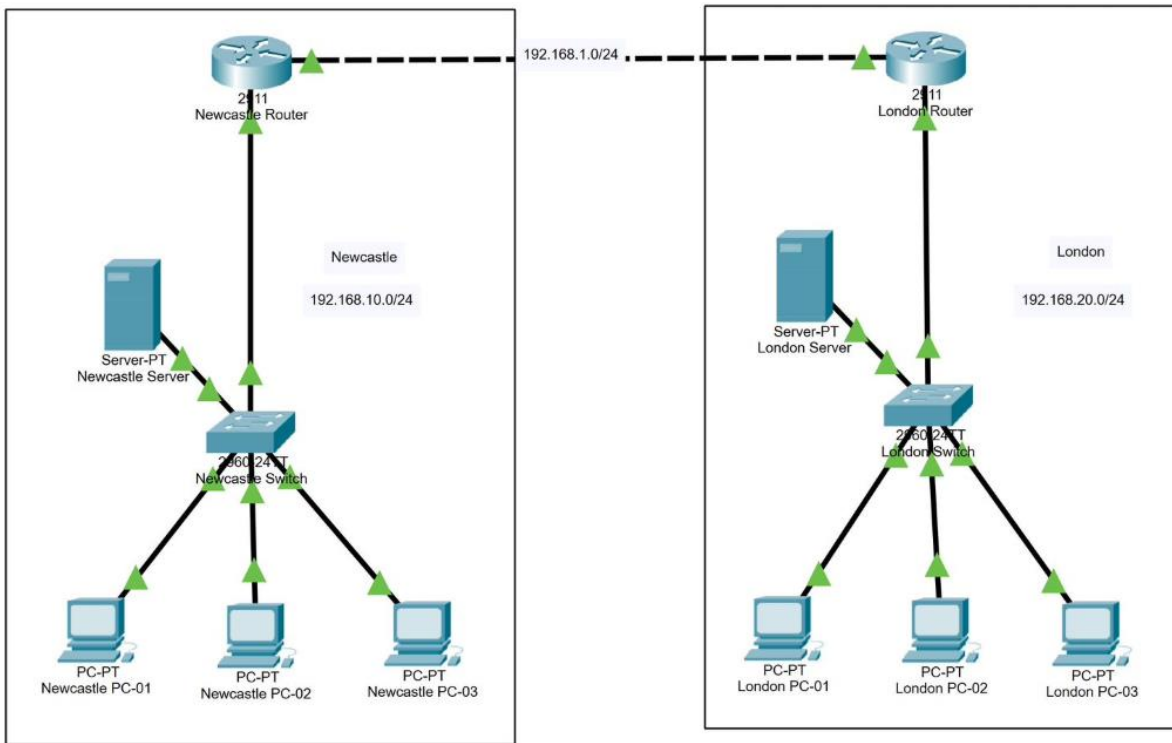
configured on server at London	the DHCP pool	subnet mask  And default gateway of 192.168.20.1				
--------------------------------------	---------------	--	--	--	--	--

## 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
<b>Rodents and wildlife damaging cables</b>	Unprotected and exposed external cabling	Physical cables and data being transmitted	High 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	High Cables are damaged by wildlife, leading to loss of service for client and damage to reputation for providing organisation	Ensure buried physical trunking protects cables in their entirety. Ensure cables for outdoor use are shielded in order to protect cables should the trunking be breached. Implement methods to deter wildlife where needed.	Preventative
<b>Single key pattern</b>	All doors use the same master key which all staff have a copy of.	All physical assets and digital assets residing on physical assets	High Potential GDPR issues depending on both physical and/or digital assets taken/damage Loss of service based on damage or theft Financial impact based on damage or theft	Medium Due to the number of users with this key pattern as well as the area being noticed as having a high level of crime	High Key is lost, stolen, not collected in when staff leave, or copies made without authorisation	Replace locks with unique lock barrels and only issue keys based on required access. Ensure key control is kept strict and logged  Alternative solution would be to replace locks with Keycard access, this would allow for not only strict monitoring of who is allowed access, but also would provide a full audit history of the access to these secure areas.	Preventative

<b>Flooding</b>	Ground floor equipment	Physical assets with potential impact on digital assets	High Damage to physical assets resulting in loss of digital data. This may result in downtime and have a financial impact	Low The area is noted to not have any flooding and no mention of water mains within the building being near important areas	Medium Equipment being water damaged leading to loss of service	Raise servers to a high points in the rack and ensure rack is off the floor where possible, this should ensure that should there be any water issues that the servers should be a lower risk.	Acceptance
<b>Fire – in server room</b>	All assets in the server room potentially spreading to the rest of the building	Physical assets within server room resulting in loss of digital assets and potential of spreading to other assets	High Loss of services with varying impact depending on site  Financial loss due to equipment or digital asset loss	Low Modern equipment coupled with a fire suppression system being implemented hugely reduces the risk of this potential threat	Medium Damage to equipment in the server room leading to loss of service	As there is already an electrical/hardware safe fire suppression system in place there are no further actions needed.  We must also ensure that the off-site backups are taking place to ensure that should there be a fire and the equipment be damaged then we have alternatives.	Acceptance
<b>Fire – in offices</b>	All assets in the offices potentially spreading	Physical assets in the office with potential to spread to other key areas	Medium Financial loss from replacement of equipment and down time	Medium As there is no fire suppression within the main offices any fire in this area would likely not be stopped leading to equipment loss	Medium Damage to office equipment leading to loss of service	As most fire suppression systems would be harmful to the equipment, other than installing the required fire extinguishers by law there is not much that can be done to prevent this other than good staff training and building maintenance to ensure the likelihood of a fire is kept as low as possible.  Ensuring that data is not	Acceptance

						stored locally on machines would mean that the loss would be limited to hardware and not data.	
<b>Break in/theft</b>	Loss of assets and/or data	Physical assets with potential loss of digital assets depending on the items taken/damaged	Medium Potential GDPR issues Loss of data Loss of equipment Damage of assets Financial loss	High Due to the lack of CCTV, alarm system and being in a high crime area as well as the doors sharing the same key	Medium Equipment could be damaged or stolen leading to a loss of productivity, financial loss as well as data loss which could lead to a GDPR issue	Install CCTV and alarm systems as this would deter would be thieves from attempting to access equipment. However also adding elements such as ASSET tagging and Smart Water systems would mean that should something be taken then they could be identified and returned.	Deterrent
<b>Loss of site to site communication</b>		Routers, cabling, configuration	Medium Loss of services made available from the other site.	Medium	Medium As only London has a 4G backup line a secondary site to site link cannot be created	Add a 4G failover backup line at to both routers which would allow for site to site communication should the main internet connection fail at either office.	Preventative
<b>Loss of service – Active Directory</b>	Server/service	Digital services	Medium Logging into devise will be impacted where not using cached accounts	Medium As only one server offers this service for both networks this is a single point of failure	Medium Loss of business-critical service resulting in a loss of productivity and potential financial impact	Ensuring that we have a secondary Active Directory server would ensure that should the main server fail there was a secondary option.	Preventative

<b>Loss of service – DNS</b>	Server/service	Digital services	Medium Loss of ability to translate domain names to IP addresses, this will affect name translation on the network and ability to visit websites	Medium As only one server offers this service for both networks this is a single point of failure	Medium Loss of business-critical service resulting in a loss of productivity and potential financial impact	Configure the alternative server to act as a secondary DNS server to avoid a single point of failure.  Also configuring the routers to use an alternative DNS should the internal DNS server fail would allow for extra redundancy.	Preventative
<b>Loss of service – file storage</b>	Server/service	Digital services	Medium Loss of file services which will reduce productivity and have a potential financial impact	Medium As only one server offers this service for both networks this is a single point of failure	Medium Loss of business-critical service resulting in a loss of productivity and potential financial impact	Utilise the alternative server as a file storage backup which can be used in the event the main file storage is lost.  Instigate off site file storage backup to ensure that should the site where the server is stored then there is access from the other site.	Preventative
<b>Loss of service – DHCP</b>	Server/service	Digital services	Medium Loss of devices being able to communicate on the network which will reduce productivity and have a potential financial impact	Medium As only one server offers this service for both networks this is a single point of failure	Medium Loss of business-critical service resulting in a loss of productivity and potential financial impact	Configure the alternative server to act as a secondary DHCP server to avoid a single point of failure	Preventative
<b>Loss of service</b>	Server/service	Digital services	Low	Medium	Medium	As this is specified as rarely used and not vital it could be	Acceptance



<b>– printing</b>			Loss of user's ability to print	As only one server offers this service for both networks this is a single point of failure	Loss of no business-critical service resulting in a loss of some productivity	left on one server as it is not business critical.  Would be advised that during next replacement the printers are replaced with self-managing network printers to reduce the risk of this happening.	
<b>Issues with network communication</b>	Server/services/network communication	Data communication between devices	Medium  Intermittent service loss and general network unreliability	High  Due to cables being ran next to power that are not suitable	Medium  Data loss and reduction of productivity	Replacing all infrastructure cabling with at least Cat5e S/FTP to reduce interference from power lines and other EMF sources.  Rearrange cables to not go near power or add shielding wherever possible.	Preventative
<b>Security breach between sites</b>	The site to site connection	Data communication between sites	Medium  Confidential data loss potentially resulting in GDPR	Low  Due to the site to site connection utilising a VPN connection to secure traffic between the 2 sites	Medium  The site to site link is breached by a third party without authorisation	To ensure the connection is not breached regular monitoring of logs and scheduled changes to the pre-shared key used to secure the VPN.  Access controls will be monitored regularly.	Preventative  Detective
<b>Loss of network connectivity to servers</b>	One or more services are lost	Data communication between network and server	Medium  Potential loss of several services depending on the server	High  As the servers only use 1 out of their 4 network cards that is a single point of failure	Medium  Depending on the server lost, different services will be affected ranging from:  • logging in	Utilising 2 or more network cards would allow for load balancing or redundancy.  Ensuring load balancing and Spanning Tree Protocol were enabled on the switches would minimise this risk.	Preventative

					<ul style="list-style-type: none"> <li>• access files</li> <li>• accessing webpages</li> <li>• accessing network resources</li> <li>• printing</li> </ul>		
--	--	--	--	--	---	--	--

<b>Risk levels:</b> low   medium   high   critical	<b>Business control types:</b> physical   administrative   technical	<b>Mitigating control types:</b> preventative   detective   corrective   deterrent   directive   compensating   acceptance
---	---	---

## Assignment 3

### Examiner commentary

The student has performed a variety of tests on each cable. The tests are all relevant, given clear names and the way they are tested is appropriate. Any issues found are resolved and documented.

Detailed testing table with screenshots evidence the failings of the network, the corrective work, and the result after the corrective work. Although screen shots are present the submission could be improved with more detailed screenshots with more annotation. The tests are all relevant and show methodical testing structure.

The threats are well considered with their impact, likelihood and actions being relevant to the issue and the solutions. The solutions are reasonable and would address the threat where applicable in a reasonable way.

### 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/seek 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/seek 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

Copyright in this document belongs to, and is used under licence from, the Institute for Apprenticeships and Technical Education, © 2020-2023.

'T-LEVELS' is a registered trade mark of the Department for Education.

'T Level' is a registered trade mark of the Institute for Apprenticeships and Technical Education.

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education. NCFE is currently authorised by the Institute to develop and deliver the T Level Technical Qualification in Digital Support Services.

'Institute for Apprenticeships & Technical Education' and logo are registered trade marks of the Institute for Apprenticeships and Technical Education.

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