Assessment Task
Portfolio of Evidence

ICTNWK529_546_AT1_PE_TQM_v2

Student Name		**Student Number**	
Unit Code/s & Name/s	ICTNWK529 Install and manage complex ICT networks ICTNWK546 Manage network security		
Cluster Name *If applicable*	Complex Cluster		
Assessment Name	Network Setup, Testing, Troubleshooting, and Verification	**Assessment Task No.**	1 of 3
Assessment Due Date		**Date Submitted**	/ /
Assessor Name			

Student Declaration: I declare that this assessment is my own work. Any ideas and comments made by other people have been acknowledged as references. I understand that if this statement is found to be false, it will be regarded as misconduct and will be subject to disciplinary action as outlined in the TAFE Queensland Student Rules. I understand that by emailing or submitting this assessment electronically, I agree to this Declaration in lieu of a written signature.

Student Signature		**Date**	/ /

PRIVACY STATEMENT: TAFE Queensland is collecting your personal information on this form for the purpose of assessment. In accordance with the Information Privacy Act 2009 (Qld), your personal information will only be accessed by staff employed by TAFE Queensland for the purposes of conducting assessment. Your information will not be provided to any other person or agency unless you have provided TAFE Queensland with permission, if authorised under our Privacy Policy (available at https://tafeqld.edu.au/global/privacy-policy.html) or disclosure is otherwise permitted or required by law. Your information will be stored securely. If you wish to access or correct any of your information, discuss how it has been managed or have a concern or complaint about the way the information has been collected, used, stored, or disclosed, please contact the TAFE Queensland Privacy Officer at privacy@tafeqld.edu.au

Instructions to Student	This task is designed to assess your knowledge and skills for analysing business requirements, network design, network security plan, technical specifications, and practical configurations. This assessment is divided into three parts based on the case study: • AT1 requires students to perform physical hands-on labs to build and configure the network equipment (including routers, switches, servers, or other devices) to meet client requirements. • AT2 requires students to develop new physical and logical topologies, calculate IP addressing and required bandwidth and

equipment costs. **Students should use the template provided by this assessment to finish the report.**

- AT3 requires students to formulate a new network security plan (including the internal and external security of buildings and the security of hardware and software) after analysing current network environment according to the case study. **Students should use the template provided by this assessment to finish the report**.

Materials to be supplied:

- ICTNWK529_546_AT1_PE_TQM_v2.docx
  - Helpyou First Floor Plan.vsd
  - Helpyou Network Topology.pkt
- ICTNWK529_546_AT2_Template_SH_TQM_v2.docx
- ICTNWK529_546_AT3_Template_SH_TQM_v2.docx

Facilities to be supplied:

Network devices including routers, switches, firewalls, IP phones, and PCs will be provided in the classroom.

Work, Health and Safety:

Please ensure you setup your workstation comfortably keeping in line with the WHS rules and suggested practices for a safe workspace. If you have any questions, please see your teacher.

Assessment Criteria:

To achieve a satisfactory result, your assessor will be looking for your ability to demonstrate the following key skills/tasks/knowledge to industry standard:

- Define a process for designing security.
- Identify threats to network security.
- Analyse security risks.
- Create a security design.
- Design and implement responses to security incidents.
- Plan and design a complex network to meet business requirements.
- Design and implement a security strategy.
- Install and configure a complex network to meet business requirements.
- Provide integrated network services across a complex network.

	● Plan, design and implement voice and video business communications system. ● Manage and support a complex network. ● Test network functionality and obtain sign-off. ● Prepare to install medium enterprise WAN links. ● Configure WAN links. ● Configure and verify IP services on a router. ● Secure a network using router services. ● Troubleshoot medium enterprise WAN links. **Details of location:** TAFE will provide a simulated work environment in the classroom. AT1 needs to be conducted in the classroom and sign-off from the teacher is required. Research activities, including AT2 and AT3 may be conducted in the classroom or at home. If you are unable to attend a scheduled assessment activity, you must notify your teacher before the assessment is due and supply a doctor's certificate and approval from the team manager for an extension. **Time restrictions:** You will be working through this portfolio of evidence in class every week. **Interactions:** Teamwork skills are essential in the IT industry therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment parts individually (unless indicated). **Level of assistance permitted:** Staff cannot directly show students answers or solutions but support and guide them to complete parts individually. Teachers and tutors should be available in class, and accessible by email for students working from home. **Reasonable Adjustments:** Reasonable adjustment is available to students for a variety of reasons, including: disability, language, literacy and numeracy (LLN) problems or extenuating circumstances. Talk to your teacher, counsellor, or disability officer if you require extra support or an extension based on the conditions identified.

	Number of Attempts: You will receive up to two (2) attempts at this assessment task. Should your 1st attempt be unsatisfactory (U), your teacher will provide feedback and discuss the relevant sections / questions with you and will arrange a due date for the submission of your 2nd attempt. If your 2nd submission is unsatisfactory (U), or you fail to submit a 2nd attempt, you will receive an overall unsatisfactory result for this assessment task. Only one re-assessment attempt may be granted for each assessment task. **For more information, refer to the Student Rules.**
Submission details (if relevant)	**Insert your details on page 1 and sign the Student Declaration**. Include this template with your submission. Completed template must be submitted. Assessment to be submitted via: ● TAFE Queensland Learning Management System (Connect): *https://connect.tafeqld.edu.au/d2l/login* ● **Username:** 9 digit student number ● **For Password:** Reset password go to: *https://passwordreset.tafeqld.edu.au/default.aspx*
Instructions to Assessor	The evidence gathered in this assessment needs to demonstrate consistent performance between parts in workplace conditions that are safe. If performed in a simulated environment, this must closely replicate the workplace, where noise levels, production flow, interruptions and time variances need to be typical of those experienced in a workplace in the IT networking industry. The workplace or simulated environment must include access to: ● network design and business requirements documents ● a complex network or hardware and software required to build a network involving multiple servers, multiple physical locations (or simulation of) and a combination of network services ● a site where ICT needs and strategic directions of the organisation are coordinated ● detailed information relating to a strategic organisation plan, objectives, and direction ● organisational policies and procedures relating to the implementation of ICT changes ● individual superior in the organisation ● information on current ICT systems and practices in the organisation including operating systems, hardware, and security ● client functional requirements

	● business specifications ● database software ● simulation software ● organisational guidelines ● a network or computer layout ● site design software and hardware ● information on a range of ICT business solutions. **Marking:** Refer to following documents for this unit. Marking Criteria. Benchmark Answers. **Materials to be supplied:** Copy of Assessment Task (this document). Computer with access to Internet and word processing software. Network devices, such as routers, switches, servers, PCs, etc. Access to Connect Learning Management System.
Note to Student	*An overview of all Assessment Tasks relevant to this unit is located in the Unit Study Guide.*

Case study

General information

Helpyou mortgage company has a head office in Brisbane Australia, with a branch office in Cairns Queensland.

At head office there are 40 people:

- 5 top-level managers and executive officers.
- 5 middle managers in charge of loan business.
- 5 customer service staff who deal with significant events, usually ones that require legal procedures.
- 10 administrative staff who deal with the paperwork, procedures etc.
- 10 marketing staff that develop and execute marketing strategies.
- 3 HR staff who deal with employee data.
- 2 IT staff who maintain the existing IT infrastructure.

These 40 people occupy the first floor of a high-rise building, and the space is extremely tight. Recently, the upper floor was vacant, and Helpyou Mortgage Company chose to purchase this space to expand the head office. At the same time, 30 employees were added to the head office. The total number of employees in the head office reached 70 people. The plan is to have 35 people upstairs and downstairs.

At Cairns branch office there are 8 people:

- 1 Branch Office Manager and 7 other staff

Existing IT infrastructure

Helpyou head office has the following equipment already installed:

- Each person has a PC with a static IP address and an analogue (non-VOIP) phone.
- There are two 24-port Cisco Catalyst switches (Catalyst 2940) which are cross-linked.
  - 24 100M access ports, with one 1G uplink port on each switch used to cross-link them.
- There is an ADSL router which provides basic internet connectivity.
- 100BaseT network cards on all computers and the servers.
- Cat 5e cables connecting the computers and server via the two switches.
- Two Linux machines apart from the windows servers and windows PC.
- There are four servers which provide the following services:
  - Web, the internal web server used by all staff.
  - HR-DB, the database and application server used by HR.
  - Market-FS, the file server used by Marketing for brochures, etc.

- CS-FS, the file server which is used by Customer Service to hold details of existing customer issues and legal documents.

Current shortcomings (or Issues) of the IT infrastructure

- The Web server constantly generates messages that there isn't enough disk space or memory to perform the tasks.
- Many staff members experience slow connection to the HR-DB, Market-FS, and CS-FS.
- No remote access functionality is in place.
- No backup or redundancy is in place.
- ISP provider is not reliable and internet connection drops every so often.
- Wireless access to network resources is available to IT staff only.
- Staff storage of files on local computers making them unavailable to others and vulnerable to all kinds of theft, loss, damage, and misuse.
- Desktop computers run on different operating systems: Windows Server 2012, Windows 10.
- Many staff members complain that the network is too slow.

The floor plans, existing physical wiring and server room rack layout is shown in the embedded files attached below.


Helpyou First Floor Plan.vsd


Helpyou Network Topology.pkt

All PCs are cabled back to patch panels in the server room using Category 5e UTP cable. There are 96 UTP runs on this floor back to the patch panels in the server room.

On the new floor above the existing floor, there is an empty server room with two racks. One rack has patch panels, and the other rack used to have equipment from the previous tenant but is now empty. This floor has 120 Category 6 UTP runs from room ports back to the patch panels in the server room.

Business concerns and strategic plan

At present, the IT requirements of Helpyou are unclear. With the expansion of the business, the CIO realises that both their existing network infrastructure and security systems need to be upgraded and improved. After a short interview with CIO, their basic requirements will be:

- Network infrastructure needs to be more secure and reliable with more redundancy, backups, security elements, network monitoring, and maintenance schedules.
- Keep a log of all staff system access and usage, plus access to data should be on need-to-know basis according to bushiness role.
- Data should be accessible to staff as and when they need it from their location.
- Traditional PSTN phone communication services are inadequate and phone bills are too high, particularly on international calls.
- Videoconferencing would help the organisation as it gives them the flexibility to have conference with multiple staff remotely.
- An email server within the company server is required.
- DHCP and DNS servers should be used to manage IP addresses and web connections.
- A network monitoring server to manage network traffic.
- Manage file sharing between different platforms.
- No remote access which is difficult for branch office staff to share data with the head office.
- Staff currently are not familiar with the new software for managing accounts and are not efficiently completing their tasks.
- Visitors have problems connecting to the internet in the office, but it does need to be controlled.
- Implementation needs to be completed in the next 4 months, so Helpyou can regain and increase its market share and increase revenue for the financial year.
- Evaluate and verify your design against industry best practices.
- Update office facilities to cater for implementation of new technologies with a budget of $500,000.

Organisational Policies and procedures

- Data privacy of staff and clients is to be maintained at all times.
- Copyright and Intellectual Property rights are to be respected at all times, for our own property and others.
- Transactions made in/by our business will have the clients' best interest at heart.
- Negligence will not be tolerated, particularly around loss of information and breach of legislation. Staff must be aware and follow process.
- Honesty and respect are expected in all business dealings.

Assessment Task 1: Network Setup, Testing, Troubleshooting, and Verification

You are required to perform a series of parts using physical equipment. These parts are designed to set up a complex network based on a given case study. Your skills and knowledge required for technical specifications, and practical configurations in ICTNWK529 will be assessed.

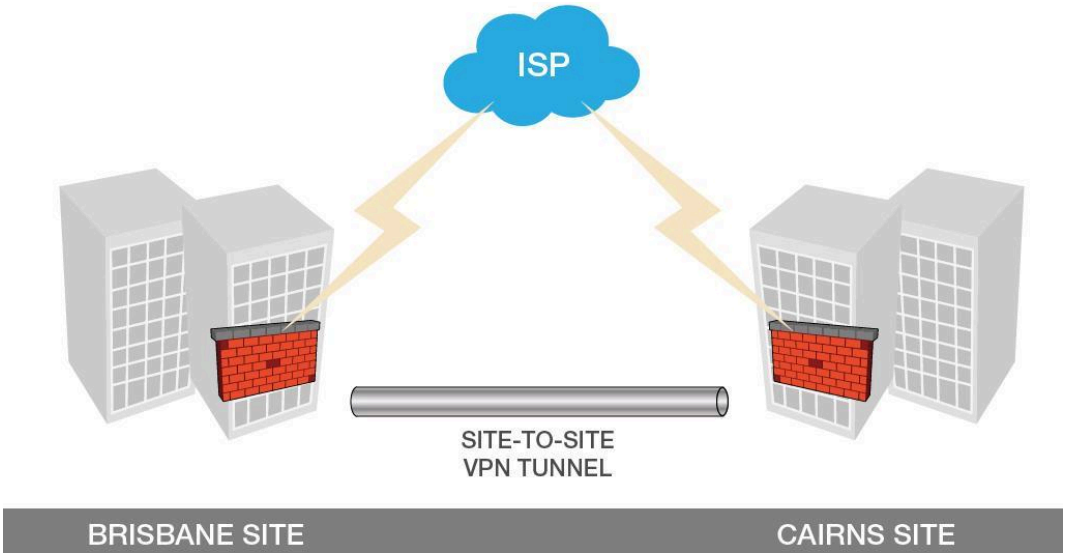
Every part is supposed to be done weekly, but the schedule may be altered depending on your skill set and instructor's teaching plan. Additionally, these parts are designed to be completed in order, meaning that parts are not to be selected randomly as prior parts prepare you for the next one. This implies that you need to **save the physical devices' configurations when one part is finished,** which will prepare you for the next part scheduled in the following week. Respectively, when the next lesson begins in the following week, it is expected of you to start where you left off and complete that week's part; you can quickly setup the lab environment as described for that specific week.

Furthermore, it is required of you to take screenshots* of your successful lab results (according to your teacher's instructions) and attach them to your portfolio so it can be marked on LMS. These screenshots are evidence that the part has been successfully completed.

*The screenshots that are to be taken will be decided by your instructor.

Part 1: Remote access via a secure Site-to-Site VPN tunnel

Two work sites located in Brisbane and Cairns. You need to obtain instructions from your instructor to set up a secure Site-to-Site VPN tunnel to connect these two work sites together. The diagram below demonstrates the topology:



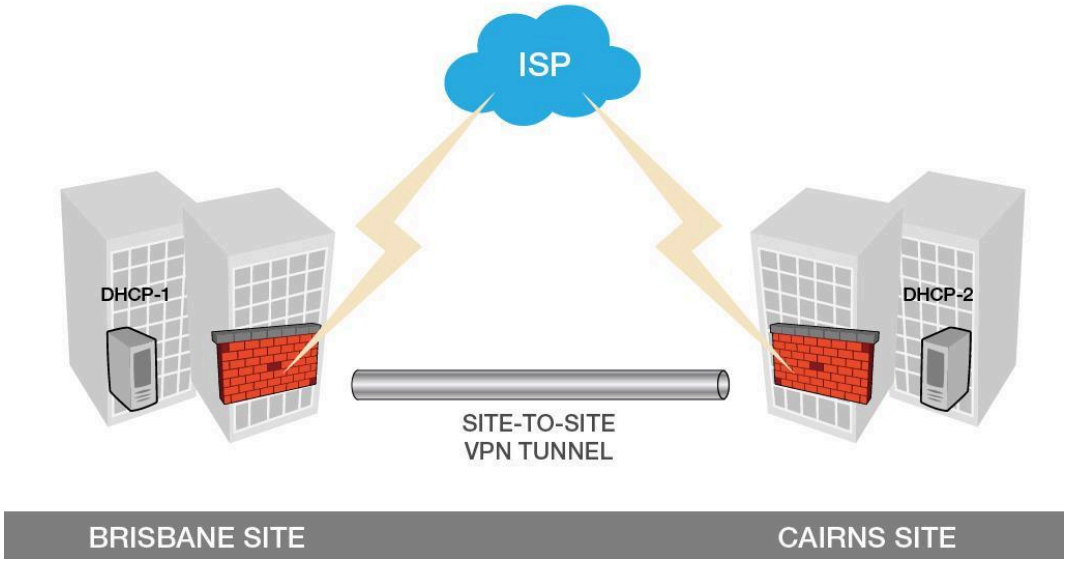
277956620 / TechnoVectors / Shutterstock, modified by TAFE Queensland

In this part you will do basic configuration on these devices. For this part:

1. Prepare the work site as per legislative and WHS requirements.
2. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the case study according to the instructions provided by your instructor.
3. Install and configure servers, routers, switches or other devices to provide the Site-to-Site VPN service.
4. Implement NAT functionality in your LAN's connection to the ISP.
5. Implement a Firewall between your LAN and the ISP on both Brisbane LAN and Cairns LAN.
6. Configure security policies on the firewall to protect the LAN from the ISP side.
7. Configure and troubleshoot all of the devices in the diagram above with the IP addresses, netmasks and default gateways from your table. Confirm that this is correct by pinging each device from every other device.
8. Demonstrate to the teacher that you can configure a proxy server and take screenshots of the proxy server configuration and screenshots of proxy client configuration. Briefly describe what is proxy in writing format.
9. Briefly describe in writing what are the steps to configure this firewall. Briefly describe what firewall applications are.
10. Briefly describe what VPN is in writing format.
11. You need to demonstrate that the part is successfully completed to your instructor. Obtain a written sign-off.
12. You need to take screenshots of the successful lab results according to the instructions provided and paste them to your portfolio file for future submission on LMS for marking.

Make sure that you have backup your lab configuration for the next part!

Part 2: Implement DHCP services on the LANs of Brisbane and Cairns



277956620 / TechnoVectors / Shutterstock, modified by TAFE Queensland

Add the DHCP servers to your network, DHCP-1 in Brisbane LAN and DHCP-2 in Cairns LAN.

Using the information provided to you by your teacher, configure DHCP servers in the Brisbane LAN and Cairns Lan to automatically distribute IP addresses to the end devices dynamically.

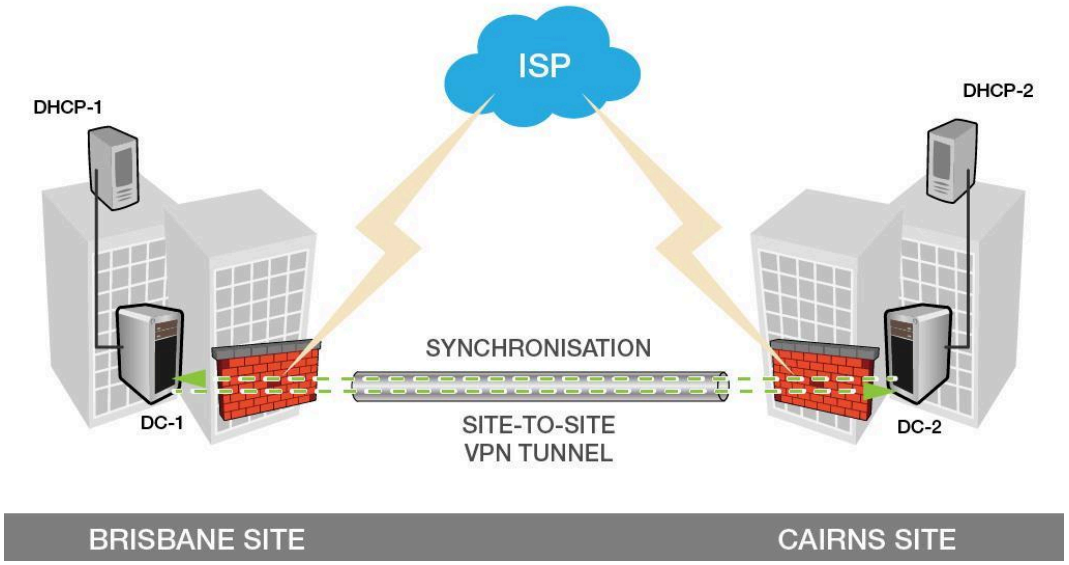
In this part you will implement DHCP services. For this part:

1. Prepare the work site as per legislative and WHS requirements covered in the e-mail in the previous part.
2. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the DHCP servers according to the instructions provided by your instructor.
3. Install and configure DHCP servers to provide the DHCP services for Brisbane and Cairns LANs.
4. Configure and troubleshoot all of the devices in the diagram above with the IP addresses, netmasks and default gateways from your table. Confirm that the end devices in each LAN successfully obtain IP addresses from the corresponding DHCP server automatically.
5. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.
6. You need to take screenshots of the successful lab results according to the instructions provided and paste them to your portfolio file for future submission on LMS for marking.

Make sure that you have backup your lab configuration for the next part!

Part 3: Implement integrated ADDS services and DNS services on the LANs of Brisbane and Cairns

For this part, you need to install and configure ADDS (Active Directory Domain Service) services in your network. You need to install and configure two Domain Controllers in your network, DC-1 in Brisbane LAN and DC-2 in Cairns LAN as demonstrated in the diagram below. These two DCs are managing the same Active Domain.



277956620 / TechnoVectors / Shutterstock, modified by TAFE Queensland

Using the information provided to you by your teacher, configure Domain Controller servers in the Brisbane LAN and Cairns LAN. Synchronize the active directory between DC-1 and DC-2 to make sure the directory information are consistent in two sites.

In this part you will implement ADDS services. For this part:

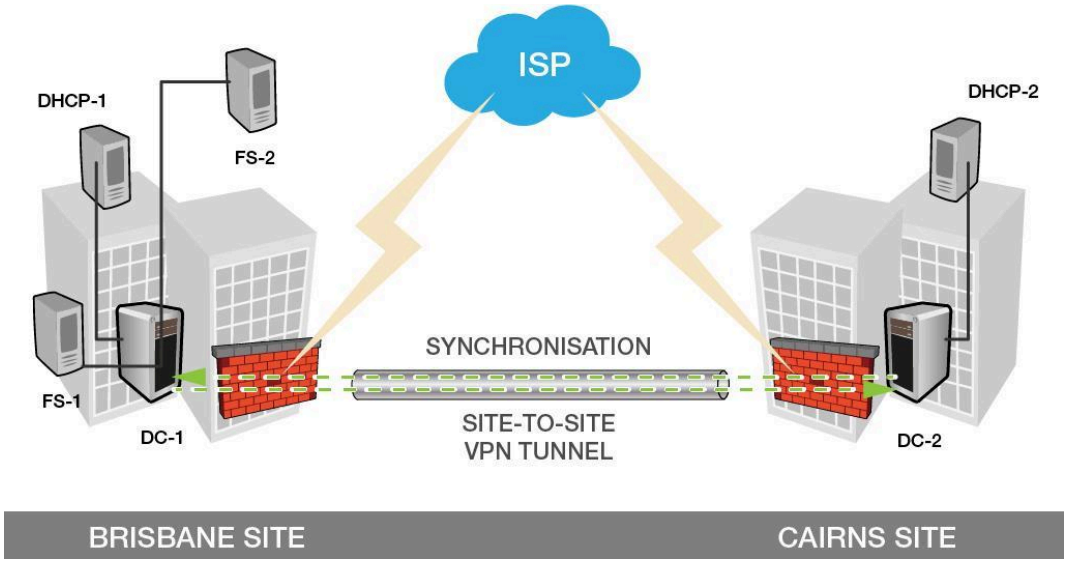
1. Prepare the work site as per legislative and WHS requirements covered in the e-mail in the previous part.
2. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the DC servers according to the instructions provided by your instructor.
3. Install and configure Domain Controller servers to provide the ADDS services for Brisbane and Cairns LANs. Compare and keep the time zone settings on the two DCs to be consistent with each other to make sure NTP is used for time synchronisation. Please describe what is NTP.
4. Install and configure DNS (Domain Name Service) service on the Domain Controller servers in Brisbane and Cairns LANs. Compare and keep the time zone settings on the two DCs to be consistent with each other to make sure NTP is used for time synchronization.
5. Configure and troubleshoot all of the devices in the diagram above with the IP addresses, netmasks and default gateways from your table. Confirm that the end devices in each LAN successfully join the Domain servers correspondently.

6. Create Site Brisbane and Site Cairns in the Active Directory as these two sites connected with a WAN link are two networks located separately in Brisbane and Cairns. Sites would automatically direct users requests to the closest resources. For example, for users located in Brisbane, their ADDS requests will be directed to the domain controller DC-1 configured in site Brisbane instead of DC-2. Please use your own language to describe in writing that how ADDS Sites implement load balancing across DCs to share with the client AD requests.
7. Create subnets for the two sites according to the IP address tables you designed for this project.
8. Move the domain controllers to the corresponding sites. DC-1 under Brisbane Site and DC-2 under Cairns Site.
9. Configure the IP site link schedules to replicate the Active Directory data between DC-1 and DC-2 during the off peak hours.
10. Modify the firewall policies on the LAN border in both sites to allow the communication between DC-1 and DC-2.
11. Create OUs on one DC and force replication between two DCs to verify the synchronisation between the two sites.
12. Briefly describe what user authentication is in writing format. Briefly describe what Active Directory is in writing format.
13. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.
14. You need to take screenshots of the successful lab results according to the instructions provided and paste them to your portfolio file for future submission on LMS for marking.

Make sure that you have backup your lab configuration for the next part!

Part 4: Implement DFS, FSRM, Desktop Management, Anti-Virus Software Deployment on the LANs of Brisbane and Cairns

For this part, you need to add two File servers in Brisbane LAN, FS-1 and FS-2 as demonstrated in the diagram below.



277956620 / TechnoVectors / Shutterstock, modified by TAFE Queensland

Using the information provided to you by your teacher, configure two file servers in the Brisbane LAN.

In this part you will install and configure DFS (Distributed File System), FSRM (File Server Resource Manager), Desktop Management, and Anti-virus software deployment. For this part:

1. Prepare the work site as per legislative and WHS requirements covered in the e-mail in the previous part.
2. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the File servers according to the instructions provided by your instructor.
3. Add two file servers to the Brisbane LAN using the IP addresses in step 2.
4. Install and configure Distributed File System (DFS) on FS-1 and FS-2 to (based on detailed instructions from your instructor)
    a) Allow distributed shares on multiple servers.
    b) Configure DFS Namespace to allow easier management of the distributed shares created in 4.a.
    c) Configure DFS replication between shares created in 4.a.
5. Install and configure File Server Resource Manager on FS-1 and FS-2 to (based on detailed instructions from your instructor)
    a) Configure storage quotas based on users' needs.
    b) Configure file screening to prevent movies from being stored to a folder based on the filename extension.
    c) Generate storage reports that show the state of file server volumes and anyone who exceeds

the quota or users files that aren't allowed.

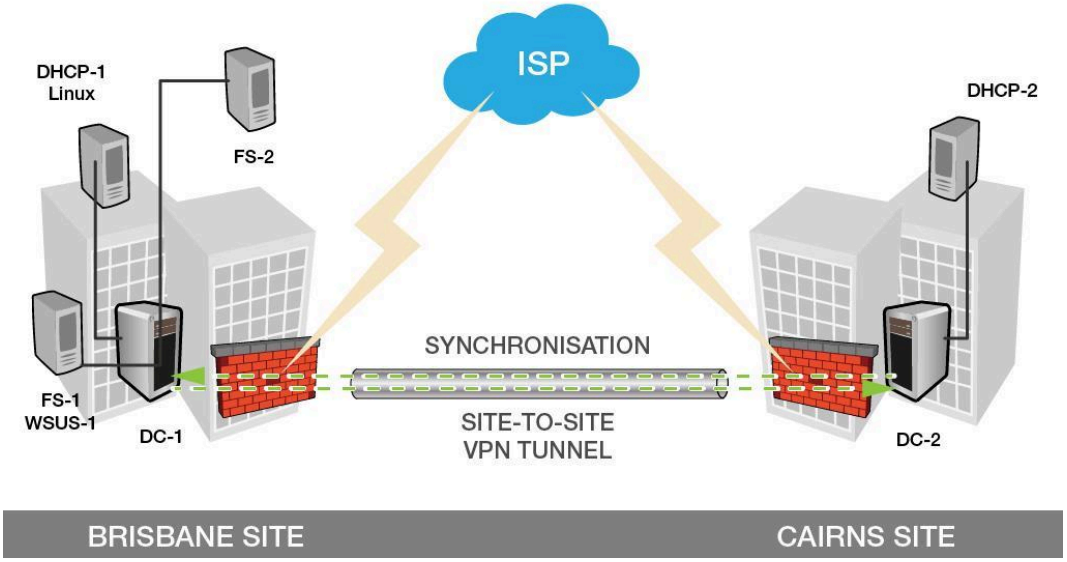
6. Deploy desktop management via Group Policy Object (GPO) on DC-1 (based on detailed instructions from your instructor).
   a) Share a desktop background wallpaper jpeg image to everyone in the domain.
   b) Deploy a GPO on DC-1 to force all the end devices in the domain to use the jpeg image as its background wallpaper.
   c) Disallow changes to the items on the desktop.
   d) Force active directory replication to synchronize this policy to DC-2.
7. Configure anti-virus software deployment via Group Policy Object (GPO) on DC-1(based on detailed instructions from your instructor).
   a) Share an anti-virus software MSI package to all the computers in the domain.
   b) Deploy a GPO on DC-1 to force all the end devices in the domain to install the anti-virus software automatically.
   c) Test it on the end devices to verify the GPO effects.
8. Install a simple FTP server and demonstrate the FTP services running. Briefly describe in writing what is FTP protocol.
9. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.
10. You need to take screenshots of the successful lab results according to the instructions provided and paste them to your portfolio file for future submission on LMS for marking.

Make sure that you have backup your lab configuration for the next part!

Part 5: Install a WSUS server and Implement interoperability between Linux and Windows

For this part, you need to

- install and configure a WSUS server service role on FS-1 server in Brisbane LAN as demonstrated in the diagram below
- join a Linux server to the existing ADDS domain and share files between the Linux server and the windows workstations.



277956620 / TechnoVectors / Shutterstock, modified by TAFE Queensland

For this part:

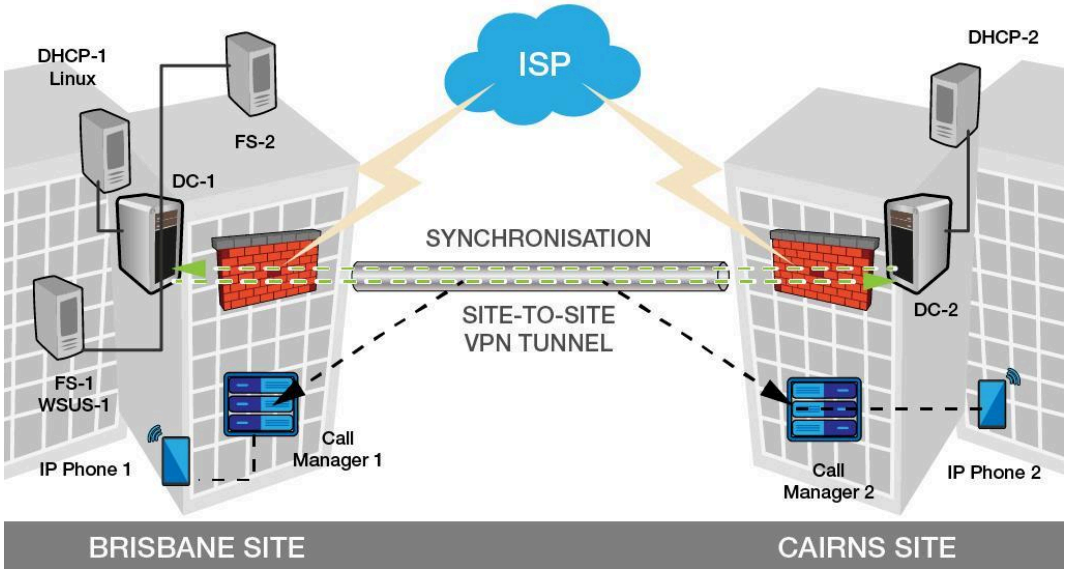
1. Prepare the work site as per legislative and WHS requirements covered in the e-mail in the previous part.
2. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the WSUS server and the Linux server according to the instructions provided by your instructor.
3. Install and configure a WSUS server service role on FS-1 server as described below:
   a) Install and configure Windows Server Update Services role on the FS-1 server according to the instructions given by your instructor. FS-1 will become WSUS-1 server as well.
   b) Download and approve the windows updates as instructed by your instructor.
   c) Create and configure a computer-based domain Group policy named “Auto Windows Update” to allow the domain computers to detect and pull the windows updates from the WSUS-1 server.
   d) Reboot FS-2 to verify that the Auto Windows Update policy is effective.
4. Describe briefly what is web services and take screenshots of the IIS Web server has been installed on the WSUS server to confirm that the WSUS server is acting as a web server as well.

5. Join a Linux server to the existing ADDS domain and enable file sharing between the Linux Server and FS-2. (Note: if the DHCP server implemented previously is a Linux server, adding a new Linux server is not necessary.)
6. Install a simple eMail server on either the Brisbane site.
7. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.
8. You need to take screenshots of the successful lab results according to the instructions provided and paste them to your portfolio file for future submission on LMS for marking.

Make sure that you have backup your lab configuration for the next part!

Part 6: Install and Configure VoIP services on the LANs of Brisbane and Cairns

For this part, you need to implement VoIP services in Brisbane LAN and Cairns LAN and enable cross-site communication between Brisbane and Cairns. The topology is demonstrated in the diagram below.



277956620 / TechnoVectors / Shutterstock, modified by TAFE Queensland

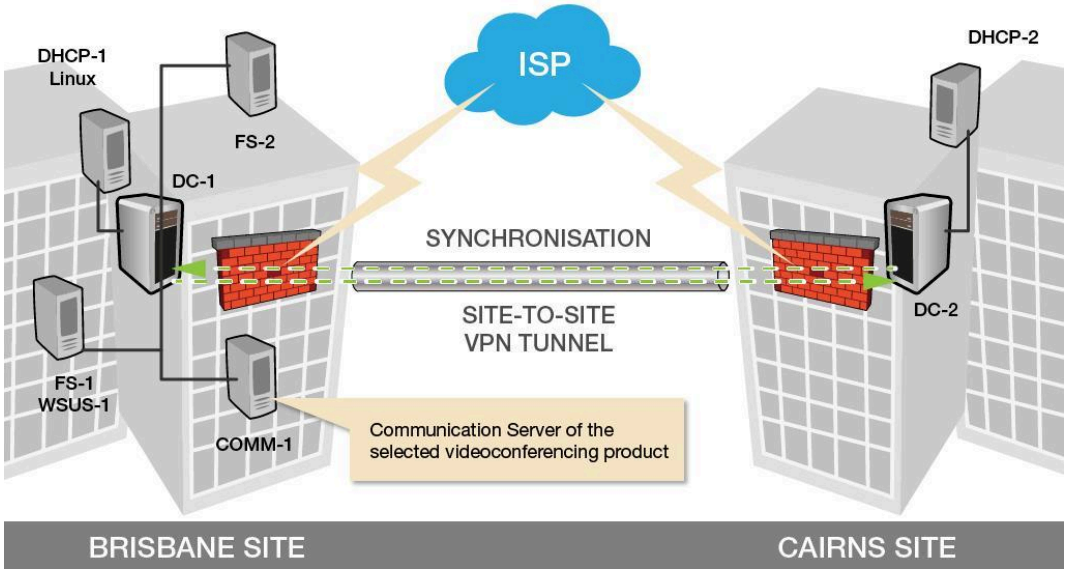
For this part:

1. Prepare the work site as per legislative and WHS requirements covered in the e-mail in the previous part.
2. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the Call Manager-1, Call-Manager-2, and the VLAN VoIP according to the instructions provided by your instructor.
3. Install and configure two Call-Manager servers with selected voice codec according to your instructor's instructions.
4. Install and configure IP Phone-1 and IP Phone-2 and make sure these two IP phones can communicate with each other across the Site-To-Site VPN Tunnel.
5. Describe what VoIP is in writing format.
6. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.
7. You need to take screenshots of the successful lab results according to the instructions provided and paste them to your portfolio file for future submission on LMS for marking.

Make sure that you have backup your lab configuration for the next part!

Part 7: Implement Videoconferencing services on the LANs of Brisbane and Cairns

For this part, you need to implement Videoconferencing services in Brisbane LAN and Cairns LAN and enable cross-site video communication between Brisbane and Cairns. The topology is demonstrated in the diagram below.



277956620 / TechnoVectors / Shutterstock, modified by TAFE Queensland

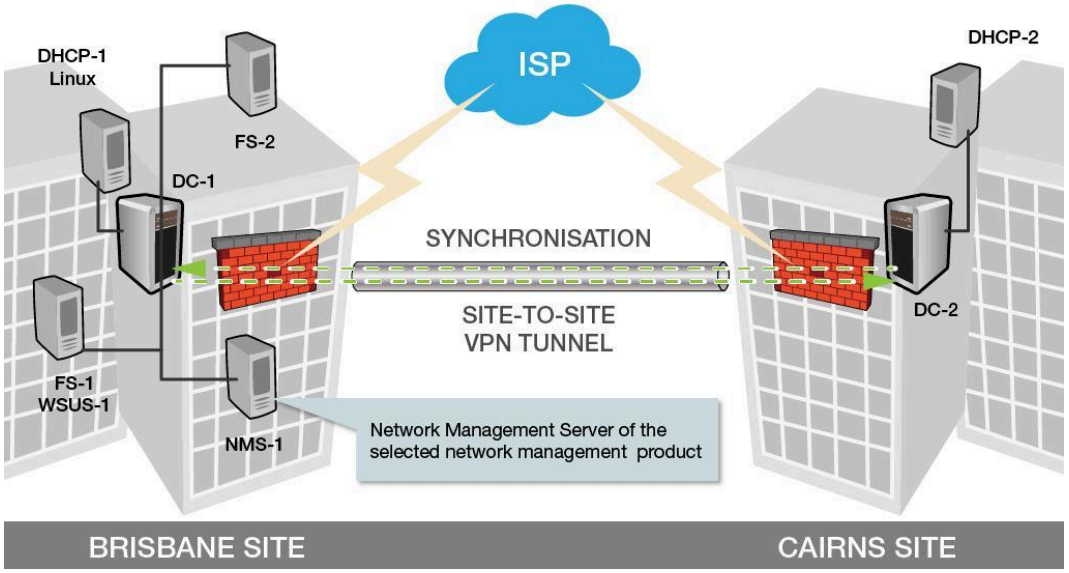
For this part:

1. Prepare the work site as per legislative and WHS requirements covered in the e-mail in the previous part.
2. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the Comm-1 server, which is the communication server for a selected videoconferencing product of your instructor's choice. For example, the Comm-1 server could be a Skype for Business Front End Server if chosen. Request more detailed instructions from your instructor.
3. Install and configure videoconferencing services on Comm-1.
4. Verify that a video meeting can be started on a client workstation from Brisbane site and communicated through to the other site with another client on Cairns via audio and video. It should work in both directions.
5. Research for what codecs you can choose from for the videoconferencing software of your selection. Record what you have found in your portfolio.
6. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.
7. You need to take screenshots of the successful lab results according to your instructor's instructions provided and paste them to your portfolio file for future submission on LMS for marking.

Make sure that you have backup your lab configuration for the next part!

Part 8: Install and configure a network management software on the LANs of Brisbane and Cairns

For this part, you need to implement network management tools in Brisbane LAN and Cairns LAN to assist in the monitoring and administration of network performance. The topology is demonstrated in the diagram below.



277956620 / TechnoVectors / Shutterstock, modified by TAFE Queensland

For this part:

1. Prepare the work site as per legislative and WHS requirements covered in the e-mail in the previous part.
2. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the NMS-1 server, which is the network management server for a selected network management product of your instructor's choice. For example, the NMS-1 server could be a PRTG Server if chosen. Request more detailed instructions from your instructor.
3. Install and configure the NMS-1 to collect Syslog and SNMP messages from servers and/or network devices.
4. Set and monitor alerts and logs on the monitored devices and reflect it on the NMS-1 to supervise the network performance in real time.
5. Generate traffic or create alerts on the monitored devices purposely. Verify the generated traffic or created alerts can be captured on the NMS-1 in real time. Briefly analyze the captured performance data on your portfolio with sample pictures and compose a short paragraph of analysis.
6. Obtain instructions from your instructor orally and enable SNMP on monitored devices.
7. Modify security policies on the company's firewalls and the firewall policies on the monitored devices to specifically allow NMS-1 to remotely manage the monitored devices via SNMP.
8. Briefly describe what SNMP is in writing format.

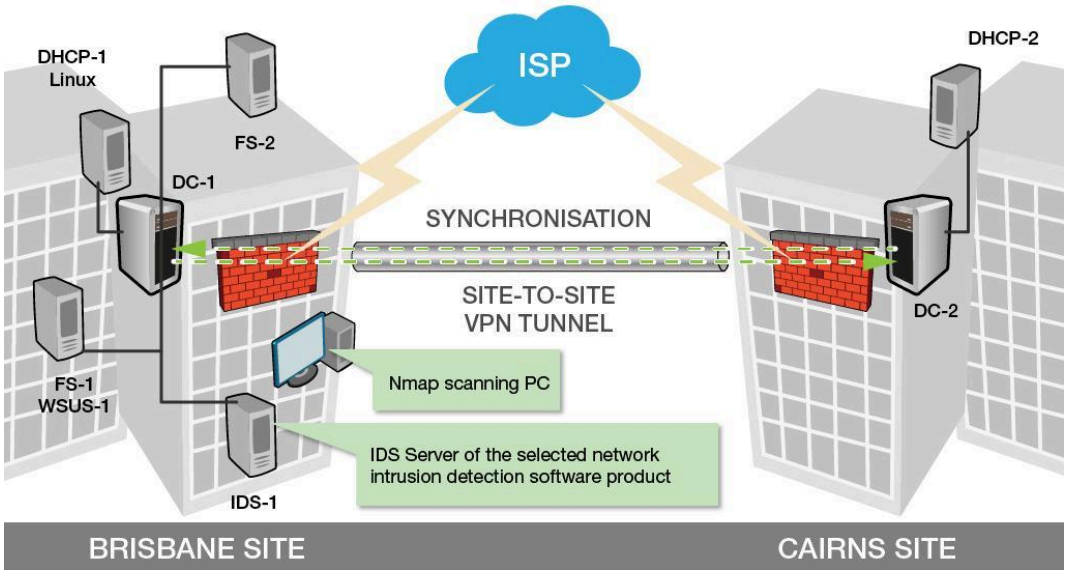
9. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.
10. You need to take screenshots of the successful lab results according to your instructor's instructions provided and paste them to your portfolio file for future submission on LMS for marking.

Make sure that you have backup your lab configuration for the next part!

Part 9: Implement Ongoing Monitoring of Network security

For this part, you need to

- install and configure an IDS server in Brisbane LAN;
- deploy a Nmap penetration test workstation at the network edge of Brisbane LAN. See the diagram below:



277956620 / TechnoVectors / Shutterstock, modified by TAFE Queensland

For this part:

1. Prepare the work site as per legislative and WHS requirements covered in the e-mail in the previous part.
2. Write out a table of IP addresses, netmasks and default gateways (where applicable) for the Nmap scanning PC, and the IDS-1 server, which is the Intrusion Detection Server for a selected IDS software product of your instructor's choice. For example, the NMS-1 server could be a Secure Onion Server if chosen. Request more detailed instructions from your instructor.
3. Install and configure the IDS-1 to analyze network traffic, respectively, and provide log and alert data for detected anomalous events and activity.
4. Install a Nmap scanning PC at the edge of the Brisbane LAN.
5. Launch a Nmap scanning from the Nmap scanning PC against the Brisbane LAN and verify that IDS-1 can pick up this suspicious event and generate alert on it.
6. You need to demonstrate that the part is successfully completed to your instructor. Describe orally what this part is and how you implement it. Obtain a written sign-off.
7. You need to take screenshots of the successful lab results according to your instructor's instructions provided and paste them to your portfolio file for future submission on LMS for marking.

You need to upload your Part 1 portfolio file into the appropriate submission area on the LMS for marking.

Make sure that you have copied your router configurations to start-up!

Part 10: Troubleshooting report

For this part:

1. Write a troubleshooting report about the following aspects:
    a) Describe network symptoms came across to you.
    b) Describe what troubleshooting tools and techniques, including any network diagnostic utilities you use to find out what is the cause to the network issues.
    c) Describe how you resolve the issues.

End of Assessment

