**Assessment Task – Knowledge, Observation, Portfolio   
(Learner Version)**

**Assessment Task 1: Knowledge Questions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Learner information** | | | |
| **Learner name:** | Wilfred B Brown | **Learner ID:** | 100646761 |

| **Section A – Program/Course details** | | | |
| --- | --- | --- | --- |
| **Qualification code:** | 22610VIC | **Qualification title:** | Advanced Diploma of Cyber Security |
| **Unit code:** | ICTNWK541 | **Unit title:** | Configure, verify, and troubleshoot WAN links and IP services |

| **Section B – Assessment task details** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Assessment number:** | 1 of 2 | | **Semester/Year:** | | 2 / 2023 |
| **Due date:** | 11/11/2023 | **Duration of assessment:** | | 15 Sessions | |
| **Assessment task results:** | This assessment task will be marked as: | | | | |
| Ungraded result: Satisfactory or Not Satisfactory  Other (eg points): Click here to enter text. | | | | |

| **Section C – Instructions to learners** |
| --- |
| **Task instructions:** |
| * This is a knowledge question assessment where students will be given 15 questions to answer, you can answer on this paper itself digitally. * In this assessment, you need to answer all the questions correctly to get satisfactory result in this unit. Failing in the first attempt you will be given another chance to resubmit the assessment. * If not successful within the enrolment period as per Holmesglen assessment procedure, you will be requested to resubmit within seven days of receiving feedback. You are permitted two resubmissions per assessment task. |

| **Section D – Conditions for assessment** | |
| --- | --- |
| **Conditions:**  Learner to complete and attach Assessment Cover Sheet to the completed Assessment Task. | |
| * This is an individual assessment. * Discuss with your assessor if you feel you require special consideration or adjustment for this task. * Learners must meet all criteria listed in the marking guide to be deemed satisfactory in this task. * Learners may appeal an assessment decision according to the Holmesglen procedure. * Students are permitted two resubmissions if needed to complete this assessment task. | |
| **Equipment/resources learners must supply:** | **Equipment/resources to be provided by the RTO:** |
| Computer, Webcam, Internet access, External Hard disk  MS Word | Computer Access to Internet  Packet Tracer Application  Physical Cisco Routers and Switches  Cisco Netacad Access |

|  |  |  |  |
| --- | --- | --- | --- |
| **Section E – Marking Guide** | | | |
| **Assessment number:** | 1 | **Assessment title:** | Knowledge Questions |
| **Learner ID:** | 100646761 | **Learner name:** | Wilfred B Brown |
| **Unit code:** | ICTNWK541 | **Unit title:** | Configure, verify, and troubleshoot WAN links and IP services |
| **Date:** | Click here to enter a date. | | |

**Knowledge Task**

|  |  |  |  |
| --- | --- | --- | --- |
| **Questions: Provide your responses in the boxes below each question.** | | | |
| **Question 1:** | **What commands would you use to verify the IPv6 address configuration on router interfaces?** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:**  To verify the IPv6 address configuration on router interfaces, you can use the following commands:  1. show ipv6 interface: This command displays the configuration and status of all IPv6 interfaces on the router. It provides information such as the interface name, link-local address, global unicast addresses, prefixes, and interface status.  2. show ipv6 interface brief: This command provides a summary of the IPv6-enabled interfaces on the router. It shows the interface name, status, and IPv6 addresses assigned to each interface.  3. show ipv6 interface [interface-name] : By replacing [interface-name] with the actual interface name (e.g., GigabitEthernet0/0/0), this command displays detailed information about a specific IPv6-enabled interface. It includes the interface status, link-local address, global unicast addresses, prefixes, and other relevant parameters.  4. show ipv6 route: This command displays the IPv6 routing table on the router. It shows the routes learned or configured for IPv6 networks. You can verify if the connected networks, static routes, or routing protocol learned routes are correctly reflecting the expected IPv6 address configuration.  These commands provide valuable information about the IPv6 address configuration and routing on router interfaces, helping to ensure the correct setup and functioning of the IPv6 network. Cisco IOS IPV6 commands, [Cisco IOS IPv6 Command Reference - Cisco](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/command/ipv6-cr-book.html) | | **Comment:**  Click here to enter text. | |
| **Question 2:** | 1. **Explain the purpose of an ACL and explain the difference between a Standard and Extended ACL.** 2. **Show a sample ACL configuration if you need to block ONLY web traffic but allow all other type of traffic from a PC with IP address of 200.0.0.10 to a web server with IP address of 30.1.1.10.**   **Note. Please provide below a screenshot of the configuration with your name and student id visible in a notepad document.**  **(To complete this question, you will need to use Packet Tracer or network hardware appliances.)** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:**   1. Access Control Lists (ACLs) are a fundamental feature of network security that provide control over traffic flow in a network. ACLs define rules that determine whether to permit or deny network traffic based on various criteria, such as source/destination IP addresses, port numbers, protocols, or other packet attributes.   Standard ACLs and Extended ACLs are two types of ACLs commonly used in networking. Here's an explanation of each type and their differences:  1. Standard ACL:  - Purpose: Standard ACLs are used primarily for basic packet filtering based on the source IP address.  - Functionality: Standard ACLs examine only the source IP address of the incoming packets.  - Placement: Standard ACLs are typically applied closer to the destination, such as on an inbound interface of a router.  - Number Range: Standard ACLs are numbered from 1 to 99 and from 1300 to 1999.  - Example: An example of a standard ACL rule could be to deny traffic from a specific source IP address range.  2. Extended ACL:  - Purpose: Extended ACLs offer more granular control over network traffic by considering various packet attributes, including source/destination IP addresses, protocols, port numbers, and more.  - Functionality: Extended ACLs examine multiple packet attributes, allowing for more sophisticated filtering and traffic control.  - Placement: Extended ACLs are typically applied closer to the source, such as on an outbound interface of a router or on a firewall.  - Number Range: Extended ACLs are numbered from 100 to 199 and from 2000 to 2699.  - Example: An example of an extended ACL rule could be to permit only HTTP traffic (TCP port 80) from a specific source IP address to a specific destination IP address.  References:  1. Cisco Networking Academy. (n.d.). ACL Operation. Retrieved from <https://www.netacad.com/courses/packet-tracer/acl-operation/>.  2. Odom, W. (2019). CCENT/CCNA ICND1 100-105 Official Cert Guide. Cisco Press.  3. NetworkLessons.com. (2016). Standard and Extended Access-Lists Explained. Retrieved from <https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/standard-and-extended-access-lists-explained>  b)    Figure\_1: allowing the ICMP traffic, and all other traffics.    Figure\_2: Blocking the WEB traffic | | **Comment:**  Click here to enter text. | |
| **Question 3:** | **Once network is installed, configured and troubleshooting was completed, to whom you need to report and seek feedback? Explain, why is it important to report, seek feedback and act upon feedback?** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:**  After the installation, configuration, and troubleshooting of a network, it is important to report and seek feedback from relevant stakeholders, such as network administrators, clients, or end-users. Here's an explanation of why reporting, seeking feedback, and acting upon feedback are crucial:  1. Reporting: Reporting involves documenting and communicating the network installation, configuration, and troubleshooting processes, as well as any significant findings or outcomes. It helps provide a comprehensive overview of the network's status, changes made, and any remaining issues or concerns. Reporting ensures that stakeholders have a clear understanding of the network's current state and can make informed decisions based on that information.  2. Seeking Feedback: Seeking feedback involves actively soliciting input from stakeholders about their experience with the network. This can be done through surveys, interviews, or regular meetings. Feedback allows stakeholders to share their observations, suggestions, or concerns related to the network's performance, usability, or any ongoing issues they may have encountered. By seeking feedback, network administrators gain valuable insights into the user experience and can identify areas for improvement.  3. Acting upon Feedback: Acting upon feedback is essential for continuously improving the network's performance and addressing any identified shortcomings. By analysing the feedback received, network administrators can identify patterns, prioritize issues, and develop action plans to address them. Taking prompt action based on feedback demonstrates a commitment to addressing user needs, enhancing the network's functionality, and ensuring optimal performance.  Why is it important? Reporting, seeking feedback, and acting upon feedback are important for several reasons:  - Continuous Improvement: Feedback provides valuable insights and perspectives that can help identify areas for improvement and refine the network's design, configuration, or performance.  - User Satisfaction: By actively seeking feedback and acting upon it, network administrators can address user concerns, enhance user experience, and increase overall satisfaction with the network.  - Problem Resolution: Reporting issues and seeking feedback helps in identifying and resolving any ongoing or potential problems in the network, ensuring its smooth operation and minimizing downtime.  - Adaptability: Networks need to evolve with changing requirements and technology advancements. Reporting and feedback enable network administrators to adapt and make necessary adjustments to meet evolving needs.  References:  1. Zanero, S., & Mellia, M. (2015). Network Monitoring and Analysis: A Protocol Approach to Troubleshooting. Morgan Kaufmann.  2. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for Smart Cities. IEEE Internet of Things Journal, 1(1), 22-32. doi: 10.1109/JIOT.2014.2306328  3. Schultz, E. E., & Schultz, A. (2019). Computer Networking Basics: Concepts, Security and Applications. Syngress. | | **Comment:**  Click here to enter text. | |
| **Question 4:** | **Explain the purpose of a DHCP Server.** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:**  The purpose of a DHCP (Dynamic Host Configuration Protocol) server is to automate and simplify the process of assigning IP addresses and other network configuration parameters to devices on a network. Here's an explanation of the purpose of a DHCP server:  1. IP Address Assignment: The DHCP server's primary purpose is to dynamically assign IP addresses to devices within a network. It eliminates the need for manual IP address configuration, making the network management process more efficient and scalable. By automatically assigning unique IP addresses to devices, the DHCP server ensures proper communication and connectivity across the network.  2. Configuration Parameter Distribution: In addition to IP addresses, DHCP servers can distribute other configuration parameters to network devices, such as subnet masks, default gateways, DNS (Domain Name System) server addresses, and other network-specific information. This allows devices to obtain all the necessary configuration settings automatically, simplifying network setup and reducing configuration errors.  3. IP Address Lease Management: DHCP servers implement a lease management mechanism, which enables them to allocate IP addresses for a specific duration. Devices that request an IP address from the DHCP server are granted a lease, allowing them to use the assigned IP address for a defined period. This lease duration ensures efficient utilization of IP addresses within the network and allows for flexibility in IP address reassignment or reallocation.  4. Centralized Network Administration: By providing centralized control over IP address assignment and configuration parameters, DHCP servers simplify network administration tasks. Network administrators can manage and monitor IP address allocation, track device connectivity, and enforce network policies more effectively through the DHCP server.  References:  1. Droms, R. (1997). Dynamic Host Configuration Protocol. RFC 2131. Retrieved from https://datatracker.ietf.org/doc/html/rfc2131.  2. Comer, D. E. (2015). Internetworking with TCP/IP: Principles, Protocols, and Architecture. Pearson.  3. Cisco Networking Academy. (n.d.). DHCP Operation. Retrieved from <https://www.netacad.com/courses/packet-tracer/dhcp-operation/>.  4. Chappell, L. (2016). Understanding TCP/IP: A Clear and Comprehensive Guide. Wiley. | | **Comment:**  Click here to enter text. | |
| **Question 5:** | **Identify three (3) common issues that may prevent a PPP link to connect. Show sample commands to resolve the connectivity issue.** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:** Three common issues that may prevent a PPP (Point-to-Point Protocol) link from connecting are:  1. Authentication Failure: Incorrect authentication settings or mismatched credentials between the two endpoints can lead to authentication failures. This can occur when using PAP (Password Authentication Protocol) or CHAP (Challenge-Handshake Authentication Protocol).  To resolve this issue, you can verify and update the authentication settings as follows:  - Check the configured authentication methods on both ends:  Use the command: show running-config  - Verify the configured usernames and passwords:  show running config | include username    - Ensure that the authentication methods and credentials match on both ends of the link.  - If necessary, update the authentication settings with the correct credentials.  Reference: Cisco. (n.d.). PPP Authentication with PAP and CHAP. Retrieved from <https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html>.  2. IP Address Assignment Failure**:** If the PPP link does not receive or assign IP addresses properly, it can prevent connectivity.  To resolve this issue, you can check and configure IP address assignment as follows:  - Verify the configured IP addressing settings on both ends of the link:    show Ip interface brief.    - Ensure that the IP address ranges, subnet masks, and default gateway configurations are correct.  - If necessary, update the IP addressing settings to match the network requirements.  Reference: Cisco. (n.d.). Configuring PPP. Retrieved from <https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html>.  3. Link Encapsulation Mismatch: If the link encapsulation settings do not match between the two endpoints, the PPP link may not establish connectivity.  To resolve this issue, you can verify and update the link encapsulation settings as follows:  - Check the configured encapsulation type on both ends:  `  show running-config.    - Ensure that the encapsulation settings (e.g., PPP, HDLC) match on both ends of the link.  - If necessary, update the encapsulation settings to match on both ends.  Reference: Cisco. (n.d.). Configuring PPP Encapsulation. <https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html>.  Please note that the provided commands and steps are general examples. Actual commands and steps may vary depending on the specific network device and operating system being used. | | **Comment:**  Click here to enter text. | |
| **Question 6:** | **Refer to ADSL installation and configuration activity done in the class. (Screenshot shown as a reference below.)**    **Note. Please provide below a screenshot of your step-by-step configurations and connectivity testing with your name and student id visible in a notepad document.** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:**    Figure\_1: setting up the serial adapter and gigabyte interface for ISP according to the topology.    Figure\_2:    Figure\_3: | | **Comment:**  Click here to enter text. | |
| **Question 7:** | **Configure a router for PAT (NAT with overload) and verify its operation.**  **Note. Please provide below a screenshot of the configurations and verification with your name and student id visible in a notepad document.**  **(To complete this question, you will need to use Packet Tracer or network hardware appliances.)** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:**  Click here to enter text. | | **Comment:**  Click here to enter text. | |
| **Question 8:** | **What is the purpose of a VPN?** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:**  The purpose of a VPN (Virtual Private Network) is to establish a secure and encrypted connection over an untrusted network, such as the internet. Here's an explanation of the purpose of a VPN:  1. Secure Remote Access: One of the primary purposes of a VPN is to provide secure remote access to a private network. It allows remote users to connect to the internal resources of an organization securely, as if they were directly connected to the local network. This enables employees, remote offices, or business partners to access sensitive data, applications, or services while maintaining the confidentiality and integrity of the communication.  2. Data Privacy and Encryption: VPNs use encryption protocols to secure the data transmitted over the network. By encrypting the data, VPNs protect it from unauthorized access or interception by malicious actors. Encryption ensures that sensitive information, such as passwords, financial data, or confidential documents, remains private and secure while in transit.  3. Bypassing Geographical Restrictions: VPNs can also be used to bypass geographical restrictions and access content or services that may be restricted based on the user's physical location. By connecting to a VPN server located in a different region, users can appear as if they are accessing the internet from that region. This allows them to overcome censorship, access geo-restricted content, or maintain online privacy in regions with strict internet regulations.  4. Secure Data Transfer between Sites: VPNs are commonly used to establish secure connections between multiple sites or branches of an organization. By creating a VPN tunnel between different locations, organizations can securely transfer data and establish private communication channels over public networks, such as the internet. This ensures the confidentiality and integrity of data transmitted between sites.  References:  1. Cisco. (n.d.). Virtual Private Networks (VPNs). Retrieved from <https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/index.html>.  2. Microsoft. (n.d.). What is a VPN? Retrieved from <https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/what-is-vpn>.  3. Kurose, J. F., & Ross, K. W. (2017). Computer Networking: A Top-Down Approach. Pearson.  4. Singh, M. (2018). Mastering Network Security. Packet Publishing. | | **Comment:**  Click here to enter text. | |
| **Question 9:** | **Differentiate PAP and CHAP authentication process.** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:**  PAP (Password Authentication Protocol) and CHAP (Challenge-Handshake Authentication Protocol) are two authentication protocols used in Point-to-Point Protocol (PPP) connections. Here's a differentiation between PAP and CHAP authentication processes:  PAP (Password Authentication Protocol):  1. Authentication Process: PAP uses a two-step authentication process. The client sends its username and password to the server in plain text.  2. Credential Exchange: The client initiates the authentication process by sending its username and password to the server. The server compares the received credentials with its user database to authenticate the client.  3. Vulnerabilities: PAP is considered less secure because it transmits the password in clear text, making it vulnerable to eavesdropping and password interception attacks.  4. One-Time Authentication: PAP performs authentication only once during the PPP link establishment.  Reference: Cisco. (n.d.). PPP Authentication with PAP and CHAP. Retrieved from <https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html>.  CHAP (Challenge-Handshake Authentication Protocol):  1. Authentication Process: CHAP uses a three-step authentication process. The server challenges the client with a random value, and the client responds with a hashed value calculated using a shared secret.  2. Credential Exchange: After the initial link establishment, the server challenges the client by sending a random value. The client calculates a hash value using the shared secret and the challenge and sends it back to the server for verification.  3. Enhanced Security: CHAP provides enhanced security compared to PAP. The password is never transmitted across the network during the authentication process. Instead, only a hash value derived from the password and the challenge is exchanged.  4. Periodic Reauthentication: CHAP supports periodic reauthentication, where the client and server periodically perform the authentication process to ensure continued secure communication. This helps prevent unauthorized access if the session is compromised.  Reference: Cisco. (n.d.). PPP Authentication with PAP and CHAP. Retrieved from <https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html>.  In summary, PAP transmits passwords in clear text, while CHAP uses challenge-response mechanism with hashed values for secure authentication. CHAP provides better security and periodic reauthentication compared to PAP. | | **Comment:**  Click here to enter text. | |
| **Question 10:** | **Under what conditions a GRE tunnel is used?** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:**  A GRE (Generic Routing Encapsulation) tunnel is used in various networking scenarios to encapsulate and transport different types of network traffic across an IP network. Here are some common conditions and use cases where GRE tunnels are employed:  1. Connecting Disparate Networks: GRE tunnels are utilized to connect geographically dispersed networks or sites that use different routing protocols or have incompatible network infrastructures. By encapsulating the packets from one network within GRE packets, the traffic can be transmitted across an intermediate IP network, such as the internet, and then decapsulated at the receiving end.  2. VPN (Virtual Private Network): GRE tunnels are employed as a part of VPN solutions to establish secure connections between remote sites or networks. By encapsulating the VPN traffic within GRE packets, sensitive data can be securely transmitted over public networks, ensuring privacy and integrity.  3. Overlay Networks: GRE tunnels are commonly used to create overlay networks, where virtual networks are built on top of an existing network infrastructure. This allows for logical separation, scalability, and flexibility. GRE tunnels enable the transport of traffic between different virtual networks or virtual machines across physical networks.  4. Multicast Routing: GRE tunnels are sometimes employed to facilitate multicast routing over networks that do not natively support multicast. By encapsulating multicast traffic within GRE packets, the multicast packets can be forwarded across unicast-only networks, enabling multicast communication between disparate network segments.  References:  1. Cisco. (n.d.). Introduction to GRE Tunnels. <https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/118361-technote-gre-00.html>.  2. Odom, W. (2019). CCENT/CCNA ICND1 100-105 Official Cert Guide. Cisco Press.  3. NetworkLessons.com. (2013). GRE Tunnelling Explained. <https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/gre-tunneling-explained> | | **Comment:**  Click here to enter text. | |
| **Question 11:** | **You suspect an issue with the WAN link, what five steps you will take to gather information of symptoms to the resolve the issue?** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:**  When suspecting an issue with a WAN link, here are five steps you can take to gather information about the symptoms and resolve the problem:  1. Identify the Symptoms:  - Gather information about the observed symptoms, such as slow performance, intermittent connectivity, or complete link failure.  - Document any error messages, error codes, or abnormal behavior related to the WAN link.  2. Check Physical Connections:  - Ensure that all physical connections between the devices involved in the WAN link are secure and properly connected.  - Inspect cables, connectors, and interface status indicators for any signs of damage or connectivity issues.  - Verify that the correct cables and connectors are being used according to the WAN link requirements.  3. Verify Configuration Settings:  - Review the configuration settings for the devices involved in the WAN link, such as routers or switches.  - Check the interface configurations, IP addresses, subnet masks, default gateways, and any relevant routing protocols.  - Ensure that the configurations are accurate and match the requirements of the WAN link.  4. Test Connectivity and Performance:  - Use appropriate network diagnostic tools, such as ping, traceroute, or network monitoring tools, to test the connectivity and measure the performance of the WAN link.  - Verify if the WAN link is reachable, assess latency, packet loss, or other performance metrics.  - Conduct tests from both ends of the WAN link to identify potential issues.  5. Troubleshoot and Resolve the Issue:  - Analyse the gathered information, error messages, and test results to identify the root cause of the issue.  - Troubleshoot specific areas, such as misconfigurations, routing problems, QoS (Quality of Service) issues, or hardware failures.  - Apply appropriate troubleshooting steps or solutions based on the identified problem.  References:  1. Cisco. (n.d.). Troubleshooting WAN Connectivity. <https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html>.  2. Odom, W. (2019). CCENT/CCNA ICND1 100-105 Official Cert Guide. Cisco Press.  3. Russ White, D. D., & Ghanwani, A. (2021). Troubleshooting BGP: A Practical Guide to Understanding and Troubleshooting BGP. Addison-Wesley Professional. | | **Comment:**  Click here to enter text. | |
| **Question 12:** | **Why is it important to document a solution of a network issue (e.g., WAN link down)?** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:**  Click here to enter text. | | **Comment:**  Click here to enter text. | |
| **Question 13:** | **Write down the commands to setup (configure) a router as a DHCP Server.**  **Note. Please provide below a screenshot of the configurations and verification with your name and student id visible in a notepad document.**  **(To complete this question, you will need to use Packet Tracer or network hardware appliances.)????????????????????** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:**  To configure a router as a DHCP (Dynamic Host Configuration Protocol) server, you can use the following commands:  1. Enter global configuration mode:  configure terminal  2. Define the DHCP pool and specify the network range for IP address assignment:  Ip dhcp pool [pool-name]  network [network-address] [subnet-mask]  Replace `[pool-name]` with the desired name for the DHCP pool, `[network-address]` with the network address, and `[subnet-mask]` with the subnet mask of the network range.  3. Set the default gateway for DHCP clients (optional):  default-router [gateway-address]  Replace `[gateway-address] ` with the IP address of the default gateway for the network.  4. Specify DNS server(s) for DHCP clients (optional):  dns-server [dns-server-address]  Replace `[dns-server-address] ` with the IP address of the DNS server(s) to be provided to DHCP clients. You can repeat this command for multiple DNS servers if necessary.  5. Define lease duration (optional):  lease [lease-duration]  Replace `[lease-duration] ` with the desired lease duration for DHCP-assigned IP addresses.  6. Exit configuration mode:  exit  7. Save the configuration changes:  copy running-config startup-config.  These commands provide a basic configuration to set up the router as a DHCP server. Make sure to adjust the values within brackets ` [ ]` according to your network requirements.  Please note that the specific command syntax and options may vary depending on the router's operating system and software version.    Figure\_1: DHCP Pool and verification | | **Comment:**  Click here to enter text. | |
| **Question 14:** | **On a PC (use a Packet Tracer PC), show an example of IPv6 addressing configuration and verify it’s implemented.**  **Note. Please provide below a screenshot of the configurations and verification with your name and student id visible in a notepad document.** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:**    Figure\_1: IPV6 addressing configuration and verifying the implementation. | | **Comment:**  Click here to enter text. | |
| **Question 15:** | **If you suspect a WAN link’s PPP is not working, which show, and debug commands would you use to check? Write any 5 commands.** | **Satisfactory response** | |
| **Yes** | **No** |
| **Answer:**  When suspecting a WAN link's PPP (Point-to-Point Protocol) is not working, you can use the following show and debug commands to check and troubleshoot the issue:  1. \*\*show interfaces\*\*: This command provides an overview of the status and configuration of all interfaces on the router, including the WAN interface. It can help verify if the PPP interface is up, check for any errors or drops, and view the current interface settings.  2. \*\*show ppp all\*\*: This command displays information about the active PPP sessions on the router. It provides details such as the session ID, protocol in use (PAP, CHAP), authentication status, and other relevant information for troubleshooting PPP connections.  3. \*\*show ppp interface\*\*: This command provides detailed information about the PPP interface, including the configured parameters, negotiated options, authentication method, and the current state of the interface. It helps in verifying the PPP settings and identifying any misconfigurations or issues.  4. \*\*show ppp errors\*\*: This command displays statistics related to PPP errors, such as framing errors, CRC errors, or input/output errors. It can help identify potential issues with the PPP link or physical connectivity problems.  5. \*\*debug ppp negotiation\*\*: This debug command enables real-time debugging of the PPP negotiation process. It displays detailed information about the PPP negotiation steps, authentication exchanges, and error messages. This debug command can provide valuable insights into the PPP negotiation process and help identify any authentication failures or misconfigurations.  References:  1. Cisco. (n.d.). Troubleshooting PPP. <https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html>  2. Cisco. (n.d.). Basic PPP Configuration and Troubleshooting. <https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html> | | **Comment:**  Click here to enter text. | |

| **Section F – Feedback to Learners** | | |
| --- | --- | --- |
| **Has the learner successfully completed this assessment task?** | **Yes** | **No** |
|  |  |
| **Additional Assessor comments (as appropriate):** | | |

|  |
| --- |
| * Click here to enter text. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Resubmission allowed:** | **Yes** | **No** | **Resubmission due date:** | Click here to enter a date. |
| **Assessor name:** | Assessor name. | | | |
| **Assessor signature:** |  | | | |
| **Date:** | Click here to enter a date. | | | |