|  |  |
| --- | --- |
| Qualification Code: | ICA60511 |
| Qualification Title: | ADVANCED DIPLOMA OF COMPUTER SYSTEMS TECHNOLOGY |
| Unit Code/s: | ICANWK506A |
| Unit Title/s: | Configure, verify and troubleshoot WAN links and IP services in a medium enterprise network |
| Assessment Due Date: |  |
| Assessment Name: | Assessment Task 1 |
| Student’s name: | Benjamen Calleja |
| Student’s number: | Cal14385330 |
| Student’s Signature |  |
| Teacher’s name: | Murad Quazi |
| Teacher’s email: | mquazi@kangan.edu.au |

|  |
| --- |
| 1. Task Instructions |

**The student will:**

Demonstrate achievement of the following elements

* Network components and services
* Dynamic host configuration protocol (DHCP)
* Network Address Translation (NAT)
* ACL
* IP addressing and network configuration
* VPN
* Frame relay, HDLC, PPP
* Network security
* Install and configure WAN links, ADSL
* Network management tools
* s

**Short Answer Questions**

1. **Describe complex ICT network that involves integrating multiple network services  
   A Large company that covers all over the globe which will require LANS and VLANS.**
2. **Define the following network protocols and provide an example**

* DNS  
  **DNS is an internet service that translates domain names into an IP address. Because domain names are in alphabetic order they are easier to remember. Every time you use a domain name, a DNS service must translate the name into the corresponding IP address.**
* Dynamic host configuration protocol (DHCP)  
  **Dynamic Host Configuration Protocol is a protocol for assigning dynamic IP address to devices on a network. With dynamic addressing a devices can have a different IP address every time it connect to the network  
    
  For example the a built in DHCP server automatically assigns IP address to the computers and other devise on each local area network or lan for short.**
* Network Address Translation (NAT)  
  **Network Address Translation is the process where a network device usually a firewall assigns a public address to a computer or a group of computers inside a private network. The main use of Nat is to limit the number of public IP addresses for economy and security purpose.**
* ACL  
  **Access Control List is a list of user permissions for a file, folder or other object. It defines what user and groups can access the object and what operations they can perform. These operations typically include read, write, and execute. For example, if an ACL specifies read-only access for a specific user of a file, that user will be able to open the file but cannot write to it or run the file.**
* IP addressing and network configuration  
  **An Internet Protocol address IP address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing.**

**Network configuration is the process of setting a network's controls, flow and operation to support the network communication of an organization and/or network owner. This broad term incorporates multiple configuration and setup processes on network hardware, software and other supporting devices and components.**

**Network configuration allows a system administrator to set up a network to meet communication objectives. The process involves the following tasks::**

**Router configuration: Specifies the correct IP addresses and route settings, etc.**

**Host configuration: Sets up a network connection on a host computer/laptop by logging the default network settings, such as IP addressing, proxy, network name and ID/password, to enable network connection and communication.**

* firewall configuration  
  **Firewall’s are a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented as both hardware and software, or a combination of both. Here is a list of some of the many different types of fire walls.  
  Packet filtering firewalls  
  stateful inspection firewalls  
  circuit level gateways.**
* Frame relay, HDLC, PPP  
  **Frame relay is a packet switching telecommunication service designed for cost efficient data transmission for intermittent traffic between LANS and between endpoints in WANS.  
    
  HDLC is a group of protocols or rules for transmitting data between network points. HDLC data is organized into a unit called a frame and sent across the network to a destination that verifies its successful arrival.  
    
  POINT TO POINT protocol is an encapsulation protocol for transporting ip Traffic across point to point links. PPP is made up of three primary components:**
* **Link Control Protocol (LCP)—Establishes working connections between two points.**
* **Authentication protocol—Enables secure connections between two points.**
* **Network control protocol (NCP)—Initializes the PPP protocol stack to handle multiple Network Layer protocols, such as IPv4, IPv6, and Connectionless Network Protocol (CLNP).**

* RIP  
  **Routing Information Protocol is a dynamic protocol used to find the best route or path from end to end over a network by using a routing a hop count algorithim. This algorithm is used to determine the shortest path from the source to destination, which allows the data to be delivered at high speed in a short time.**
* IGRP  
  **Interior Gateway Routing is a distance routing protocol used to communicate routing information within a host network. IGRP manages the flow of routing information withun connected routers in the host network or auto system. The protocol ensures that every router has routing tables updated with the best available path. IGRP also avoids routing loops by updating itself with the change**
* EIGRP  
  **Enhanced Interior Gateway Routing Protocol s an advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration. The protocol was designed by Cisco Systems as a proprietary protocol, available only on Cisco routers.**
* OSPF   
  **Open Shortest Path First is a router protocol used to find the best path for packets as they pass through a set of connected networks. It means dividing routers inside a single autonomous system running OSPF, into areas where each area consists of a group of connected routers. Having many routers exchange the link state database could flood the network and reduce its efficiency – this was the need that led to the creation of concept Areas.**
* BGP   
  **Border Gateway Protocol) is protocol that manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers.  
  BGP offers network stability that guarantees routers can quickly adapt to send packets through another reconnection if one internet path goes down. BGP makes routing decisions based on paths, rules or network policies configured by a network administrator.**
* Network security  
  **Network Security is any active designed to protect the usability and integrity of your network and data. It includes both hardware and software tech. Network security combines multiple layers of defences at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors is blocked from carrying out exploits and threats.**
* Install and configure WAN links, ADSL   
  **Wan link is a communication circuit that joins two or more local area networks into a wide area network. Many types of Wan links are possible between networks, depending on the networking protocols and telecommunications carrier services used  
    
  Asymmetric Digital Subscriber Line is a technology for transmitting**[**digital**](https://whatis.techtarget.com/definition/digital)**information at a high bandwidth on existing phone lines to homes and businesses. Unlike regular dialup phone service, ADSL provides continuously available “always on" connection.**

1. **Define and describe VPN connection  
   A VPN connection is the process of establishing a private and secure link or path between one or more local and remote network devices. A VPN connection is established through a VPN that utilizes networking protocols such as point to point tunnelling protocol and layer 2 tunnelling protocol.**
2. **How many bits are in an IPv6 address?  
   The number of bits we can have in a IPV6 address is 128 bits.**
3. **Which layer is responsible for transporting traffic between devices that are not locally attached?  
   The network layer which is OSI layer 3 is responsible for routing through an internetwork and for networking addressing. This means that the Network Layer is responsible for transporting traffic between devices.**
4. **What is the decimal equivalent to the binary number 11000001  
   193**
5. **List the layers of the OSI model from the top down, along with their counterparts in the TCP/IP model.  
   APPLICATION HTTP FTTP TELNET NTP DHCP PING  
   PRESENTATION HTTP FTTP TELNET NTP DHCP PING  
   SESSION HTTP FTTP TELNET NTP DHCP PING  
   TRANSPORT TCP UDP  
   NETWORK IP ARP ICMP IGMP  
   DATALINK ETHERNET  
   PHYSICAL ETHERNET**
6. **Define and describe VLSM  
   Variable Length Subnet Mask is a numerical masking sequence, or IP address subset, based on overall network requirements. A VLSM allows a network administrator to use long masks for networks with few hosts and short masks for networks with multiple hosts.**
7. **In IPv4 with a Class C address of 197.15.22.31 and a subnet mask of 255.255.255.224, how many bits have been borrowed to create a subnet?  
   3 bits have been borrowed.**
8. **How to implement router security  
   Some ways to implement router security are   
   Preform Auditing and mapping  
   Keep the network up to data  
   Physically secure the network   
   Consider Mac address filtering**

**Create an Addressing Scheme.**

**Step 1: Use the 192.168.156.0/22 address to create an addressing scheme to accommodate all hosts on the network. Begin the address assignments with the 192.168.157.0 address.**

Document all subnet addresses in Table 1.

**Table 1**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **Number of Hosts** | **Subnet** | **Subnet Mask** |
| HQ | **Fa0/0** | **90** | **192.168.158.0** | **255,255,255,128** |
| **Fa0/1** | **60** | **192.168.158.128** | **255.255.255.192** |
| **S0/0/1** | **2** | **192.168.159.96** | **255.255.255.252** |
| **S0/0/0** | **2** | **192.168.158.100** | **255.255.255.252** |
| Remote1 | **Fa0/0** | **30** | **192.168.159.64** | **255.255.255.224** |
| **Fa0/1** | **60** | **192.168.159.0** | **255.255.255.192** |
| **S0/0/1** | **2** | **192.168.159.104** | **255.255.255.252** |
| Remote2 | **Fa0/0** | **128** | **192.168.157.0** | **255.255.255.0** |
| **Fa0/1** | **60** | **192.168.158.192** | **255.255.255.192** |
| **S0/0/0** | **2** | **192.168.159.108** | **255.255.255.252** |

**Marking Criteria**

GRADED

20% of Total Mark.

|  |  |
| --- | --- |
| **Grade** |  |
| NN | * Assessment aims have not been met |
| P 50–59%  Cr 60- 69%  DI 70 – 79%  HD 80– 100% | * Understanding of WAN links * Understanding of network services * Understanding of network security, Firewall * Understanding of network protocols * Understanding of VPN, DHCP,NAT, ACLs |

|  |
| --- |
| 1. Submission instructions |

Answer all the questions and submit to your facilitator on the due date given.

|  |  |  |  |
| --- | --- | --- | --- |
| Student Signature: | Benjamen Calleja | Submission Date: | 12th February 2019 |

Comments:

|  |  |  |  |
| --- | --- | --- | --- |
| Teachers Signature: |  | Date: |  |