**UNIVERSITI TUNKU ABDUL RAHMAN**

A blue sign with white text

Description automatically generated

**FACULTY OF INFORMATION SYSTEM & COMMUNICATION TECHNOLOGY**

**Session: March 2024**

**UCCN2243 Internetworking Principles and Practices**

**Assignment Group Name: Desserts**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Group Member** | **Student ID** | **Practical Group** | **Programme** |
| **1** | Raymond Tan Zhi Yong | 2104090 | P11 | CS |
| **2** | Tan Xin Sheng | 2104653 | P11 | CS |
| **3** | Tan Yi Xin | 2101990 | P12 | CS |

**Q1.**

**(a) Show the running configuration of Router 0 and Router 1.**

Configuration on Router 0:

A screenshot of a computer program

Description automatically generatedA screenshot of a computer program

Description automatically generated



Router 0:

|  |  |
| --- | --- |
| Command | Explanation |
| hostname R0 | Set the name of the router to “R0”. |
| int fa0/0  ip addr 192.168.1.254 255.255.255.0  ip nat inside | In the interface fast FastEthernet0/0, set an 192.168.1.254 with a subnet mask 255.255.255.0 as it’s interface IP address. The 192.168.1.254 is the last usable IP address off the network 192.168.1.0/24.  Then, configure the interface as inside for the Network Address Translation. |
| int fa0/1  ip addr 201.1.1.1 255.255.255.0  ip nat outside | In the interface fast FastEthernet0/1, set an 201.1.1.1 with a subnet mask 255.255.255.0 as it’s interface IP address, which is the public IP address for the network 192.168.1.0/24. |
| access-list 1 permit 192.168.1.0 0.0.0.255 | Create an access-list with numbered 1 to permit all the traffic from the private network 192.168.1.0/24. |
| ip nat inside source list int fa0/1 overload | This command is used for Port Address Translation (PAT) to specify traffic leaving the private network access to public network. In the PAT, the router can overload a single public IP to allow multiple IP addresses for outgoing traffic through the interface FastEthernet0/1.  It is associated with ACL numbered 1 that specifies all the hosts in the network 192.168.1.0/24 are allowed to access the internet by using a public IP address (201.1.1.1). |
| ip route 0.0.0.0 0.0.0.0 201.1.1.2 | Configure a default route on Router 0. It specifies that any traffic with a destination IP address for which there is no specific route in the routing table should be forwarded to the next-hop IP address (201.1.1.2). |
| ip helper-address 192.168.2.1 | Configure to specify the router is a relay agent to the DHCP server 0, which has an ip address of 192.168.2.1. It forward UDP broadcast message to the DHCP server 0. |

Configuration on Router 1:



A screen shot of a computer

Description automatically generatedA screenshot of a computer program

Description automatically generated



Router 1:

|  |  |
| --- | --- |
| Command | Explanation |
| hostname R1 | Set the name of the router to “R1”. |
| int fa0/0  ip addr 192.168.2.254 255.255.255.0  ip nat inside | In the interface fast FastEthernet0/0, set an 192.168.2.254 with a subnet mask 255.255.255.0 as it’s interface IP address. The 192.168.2.254 is the last usable IP address off the network 192.168.2.0/24.  Then, configure the interface as inside for the Network Address Translation. |
| int fa0/1  ip addr 201.1.1.2 255.255.255.0  ip nat outside | In the interface fast FastEthernet0/1, set an 201.1.1.2 with a subnet mask 255.255.255.0 as it’s interface IP address, which is the public IP address for the network 192.168.2.0/24. |
| access-list 1 permit 192.168.2.0 0.0.0.255 | Create an access-list with numbered 2 to permit all the traffic from the private network 192.168.2.0/24. |
| ip nat inside source list int fa0/1 overload | This command is used for Port Address Translation (PAT) to specify traffic leaving the private network access to public network. In the PAT, the router can overload a single public IP to allow multiple IP addresses for outgoing traffic through the interface FastEthernet0/1.  It is associated with ACL numbered 1 that specifies all the hosts in the network 192.168.2.0/24 are allowed to access the internet by using a public IP address (201.1.1.2). |
| ip route 0.0.0.0 0.0.0.0 201.1.1.1 | Configure a static route to forward all the packets to the next-hop router which has an ip address of 201.1.1.1. |

**(b) Show that PC0, PC1, and PC2 has successfully obtained their IP addresses from the Remote DHCP Server 0. Include descriptions.**

The Dynamic Host Configuration Protocol (DHCP) is an application layer protocol that allows the DHCP server to dynamically assign IP addresses to the DHCP client. DHCP employs UDP services and is based on a client-server model and works on discovery, offer, request, and acknowledgment. The port number used for the DHCP server is 68, while the DHCP client’s port number is 67 [1].

In the process of DHCP client obtained an IP address from the DHCP server, which included mainly 4 DHCP messages to make a connection. This communication is also called the DHCP DORA process, which stands for Discover (D), Offer (O), Request (R), and Acknowledgement (A).

**1. Discover(D):** DHCP clients (PC0, PC1, and PC2) will send out a DHCP broadcast discovery request to 255.255.255.255 by using source IP of 0.0.0.0. The “0.0.0.0” IP address is an unspecified address that is used to indicate that the client does not have a configured IP address yet. The request will reach every device in the network including the DHCP server.

The header information of the discovery message**:**

* ***Source IP address****: 0.0.0.0*
* ***Destination IP address****: 255.255.255.255*
* ***Source MAC address****: MAC address of DHCP clients.* (For example: PC0 is 00E0.A3BA.04B)
* ***Destination MAC address****: FF:FF:FF:FF:FF: FF*

**2. Offer (O):** Upon receiving the Discover request, the DHCP Server (Server 0) will respond with a DHCP offer message, offering a range of available IP addresses to the clients via broadcast. Hence, the Offer message contains the source IP of the DHCP server and the destination IP address of 255.255.255.255.

Header info of offer message:

* ***Source IP address****: 192.168.2.1*
* ***Destination IP address****: 255.255.255.255*
* ***Source MAC address****:  0001.C795.D19C*
* ***Destination MAC address****: MAC address of DHCP clients.* (For example: PC0 is 00E0.A3BA.04B)

**3. Request (R):** The client will select the IP address from the offered range list and send a DHCP Request message to the DHCP server to request the selected IP address. Since the client still has not obtained the IP address formally, then the source IP address (DHCP client) is still in 0.0.0.0.

Header info of request message:

* ***Source IP address****: 0.0.0.0*
* ***Destination IP address****: 255.255.255.255*
* ***Source MAC address****: MAC address of DHCP clients.* (For example: PC0 is 00E0.A3BA.04B)
* ***Destination MAC address****:  0001.C795.D19C*

**4. Acknowledgment (A):** The DHCP server 0 receives the Request message, and it will then acknowledge the request by sending a DHCP Acknowledgment message back to the clients.

Header info of acknowledge message:

* ***Source IP address****: 192.168.2.1*
* ***Destination IP address****: 255.255.255.255*
* ***Source MAC address****:  0001.C795.D19C*
* ***Destination MAC address****: MAC address of DHCP clients.* (For example: PC0 is 00E0.A3BA.04B)

Upon the success of the DORA process, the DHCP client has now obtained their dynamic IP from the server.

For the network above, the DHCP server (192.168.2.1) is a centralized deployment, where the DHCP server is in a separate subnet or network from the DHCP client. The DHCP client is the PC0, PC1, and PC2 in the network 192.168.1.0/24. As per the IP subnet rules, different network addresses are unable to communicate with each other. Initially, the DHCP client is unable to obtain their dynamic IP address from the server because they are in different networks, as shown in the diagram below. “DHCP failed. APIPA is being used”, even the DHCP server and the Port Address Translation (PAT) have been configured properly. Hence, the routing between two networks is necessary to enable communication between the hosts across the network.

Routing is a process of forwarding data packets between different networks. It involves determining the optimal path for data to travel from a source to a destination across multiple interconnected networks [2]. By setting the default routing for both Router 0 and Router 1, the two networks which are 192.168.1.0/24 and 192.168.2.0/24 is now can communicate. The default route is used to allow DHCP client traffic to reach the DHCP server, which is located on a different network. Before getting an IP, the DHCP client does not have specific routing information for the DHCP server’s network. By using the default route, it will catch all to send the DHCP request to the next hop router (Router 1). Router 1 will then be responsible for forwarding traffic from the current public network into the local subnet.

In this stage, all the host in the 192.168.1.0/24 still cannot ping with the Server 0, since they have no IP address yet. To test the routing has been properly configured, manually type an IP address to the PC2 with IP address of 192.168.1.2 as shown in the diagram below.

A screenshot of a computer

Description automatically generated

Now, test the traffic by ping to the Server 0 which IP address is 192.168.2.1.

A computer screen shot of a computer program

Description automatically generated

The successful pinging shows that the routing for both networks has been configured correctly for both routers. But we need to obtained the dynamic IP to the PC0, PC1, and PC2 from DHCP server, still we need to configure on the Router 0 furthermore.

In the provided network, Router 0 functions as a DHCP Relay Agent. This is because the DHCP client and the DHCP server are located on different network segments. As using the DORA process, the DHCP clients use broadcast messages to discover DHCP servers on the local network segment. However, these broadcast messages will not be traversed beyond the local network due to the nature of broadcast traffic [3]. The relay agent works with broadcast forwarding then intercepts the broadcast DHCP message and converts it into a unicast message. Then, it will further forward this unicast message to the DHCP Server that is in the network 192.168.2.0/24 from 192.168.1.0/24. When Server 0 responds to the DHCP discovery message, Router 0 intercepts the response forwards it back to the DCHP Client and converts it again into broadcast message. After configuring the command “ip helper-address” on Router 0, Router 0 now becomes a DHCP Relay Agent which facilitates the communication between the DHCP clients and server across different networks. Finally, the DHCP Clients can obtain their dynamic IP address from its server.

A computer screen shot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**(c) Could PC0, PC1, and PC2 DIRECTLY ping the Remote DHCP Server 0? Explain WHY / WHY NOT.**

Before PC0, PC1, and PC2 get their IP address from the DHCP Server 0, they are not able to ping to the Remote DHCP Server 0. This is because the PCs do not have an assigned IP address until the DHCP DORA processes. Before the PCs get their IP address, the “0.0.0.0” IP address will be used, which is an unspecified address that is used to indicate that the client does not have a configured IP address yet. This address is not routable on a network. Configuring a server to listen on 0.0.0.0 means that it will accept connections on any IP address assigned to the machine. Thus, the DHCP server 0 will listen for incoming connections on all available network interfaces, including both IPv4 and IPv6 addresses. This helps the Server 0 to be accessible from multiple networks. [4]. Therefore, until the PCs (DHCP clients) successfully obtain an IP address and network configuration parameters from the DHCP Server 0, they are not able to establish direct communication with any other devices including the DHCP Server itself.

Once the PCs successfully obtain an IP address from the DHCP Server 0, it can establish communication with other devices including the remote DHCP Server 0 which is placed in a different network in case all the routing has been configured properly. Upon PCs receiving an IP address from DHCP Server 0, the PC0, PC1, and PC2 (DHCP Client) configure their network interface with assigned IP address, subnet mask, and default gateway. Now, PCs can communicate with other devices in their network. With the setup in the static routing for both Router 0 and Router 1, now all the PCs can directly ping to the Remote DHCP Server 0.

A computer screen shot of a computer program

Description automatically generatedA computer screen shot of a computer program

Description automatically generated

A computer screen shot of a computer program

Description automatically generated

**Q2(a) Show (include description) the relevant running configuration for the Edge router.**

**Edge Router IP address configuration**

|  |  |
| --- | --- |
| Command | Description |
| Int fa0/0  ip add 192.168.1.254 255.255.255.0  no shut | configure fa0/0 interface with the IP address 192.168.1.254 and a subnet mask of 255.255.255.0 |
| Int fa0/1  ip add 200.1.1.2 255.255.255.0  no shut | configure fa0/1 interface with the IP address 200.1.1.2 and a subnet mask of 255.255.255.0 |
| int fa1/0  ip add 10.1.1.1 255.255.255.0  no shut0 | configure fa1/0 interface with the IP address 10.1.1.1 and a subnet mask of 255.255.255.0 |

A screenshot of a computer

Description automatically generated

**Configure NAT at each Edge Router interface**

|  |  |
| --- | --- |
| Command | Description |
| int fa0/0  ip nat inside | This configuration designates interface fa0/0 as an inside interface for NAT |
| int fa0/1  ip nat outside | This configuration designates interface fa0/1 as an outside interface for NAT |

A black background with white text

Description automatically generated

**Create  Access List**

|  |  |
| --- | --- |
| Command | Description |
| access-list 1 permit 192.168.1.1 0.0.0.15  ip nat inside source list 1 int fa0/1 overload | This configuration allows devices with IP addresses ranging from 192.168.1.1 to 192.168.1.15 to access the internet through the router's int fa0/1.  Overload keyword enables PAT, allowing multiple internal private IP addresses to be translated to a single public IP address [5] |



**Configure port forwarding**

|  |  |
| --- | --- |
| Command | Description |
| ip nat inside source static tcp 10.1.1.2 23 200.1.1.2 23 | Creates a static NAT translation for TCP traffic, allowing devices from outside the network to access a Telnet server at the external IP address 200.1.1.2 on port 23, which is translated to the internal device with IP address 10.1.1.2 on port 23 |



Q2) b) i) **PC1 able to ping Internet Gateway and Telnet Server**

A screenshot of a computer

Description automatically generated

**192.168.1.1(PC1) ping 200.1.1.1 (Internet Gateway)**

The Wireshark result contains request from PC1 and reply from Internet Gateway, which shown PC1 is successfully ping to Internet Gateway

A screenshot of a computer

Description automatically generated

**192.168.1.1(PC1) ping 10.1.1.2(Telnet Server)**

The Wireshark result contains request from PC1 and reply from Telnet Server, which shown PC1 is successfully ping to Telnet Server

b) ii) **PC2 unable to ping Internet Gateway but able to ping Telnet Server**

A screenshot of a computer

Description automatically generated

**192.168.1.20(PC2) ping 200.1.1.1(Internet Gateway)**

The Wireshark result showed that PC2 requested Internet Gateway but got **no reply** from Internet Gateway, which means that **PC2 is unable to ping Internet Gateway**.

The reason is the configuration of NAT inside with the access-list 1{access-list 1 permit 192.168.1.1 0.0.0.15} on the edge router is only allowed IP range from 192.168.1.1 to 192.168.1.15 devices can access to Internet Gateway. PC2 is out of range for the NAT translation.

A screenshot of a computer

Description automatically generated

**192.168.1.20(PC2) ping 10.1.1.2(Telnet Server)**

The Wireshark result contains a request from PC2 and reply from Telnet Server, which shows PC2 is successfully ping to Telnet Server.

**b) iii) The relevant NAT occurring in the Wireshark results**

**PC1 ping Internet Gateway**

**A screenshot of a computer

Description automatically generated**

**Diagram above showing the capture of Edge Router at int fa0/0**

**A screenshot of a computer

Description automatically generated**

**Diagram above showing the capture of Edge Router at int fa0/1**

From the result above which has shown that NAT is occurring, when PC1 ping to Internet Gateway, the NAT of the Edge router translates PC1’s IP address into public address which is 200.1.1.2.

**PC1(192.168.1.1) > Edge Router (NAT translate 192.168.1.1 to 200.1.1.2) > Internet Gateway (200.1.1.1)**

**C) Internet Gateway is able to telnet to the Telnet Server but unable to ping to Telnet Server**

A screen shot of a computer

Description automatically generated

**References**

[1] “What is DHCP | Relay Agent | DORA Process - A complete Guide,” *PyNetLabs*, Aug. 10, 2022. https://www.pynetlabs.com/what-is-dhcp/#:~:text=DHCP%20DORA%20process.-

[2] R. Aresco, “An Introductory Guide to Routing & Switching,” *Erie Institute of Technology*, Oct. 02, 2023. https://erieit.edu/introductory-guide-routing-switching/#:~:text=Routing%20and%20switching%20are%20the

[3] “CompTIA Network+ Rapid Review: Network Concepts | Microsoft Press Store,” *www.microsoftpressstore.com*, Dec. 15, 2012. https://www.microsoftpressstore.com/articles/article.aspx?p=2201313&seqNum=2#:~:text=on%20the%20network.- (accessed Apr. 03, 2024).

[4] baeldung, “Is 0.0.0.0 a Valid IP Address? | Baeldung on Computer Science,” *www.baeldung.com*, Feb. 03, 2023. https://www.baeldung.com/cs/ip-all-zeroes#:~:text=on%20Computers%2FServers- (accessed Apr. 03, 2024).

[5] O. Ergun, “NAT Overloading,” orhanergun.net. https://orhanergun.net/nat-overloading

‌