**BMIT3094 Advanced Computer Networks**

**Skill Based Assessment (SBA)**

**Semester: 202201**

**Instructions**

Update the User Profile by remove *Guest* and key in your name. Enter your email address into the User Profile Dialog Box.

**Background / Scenario**

Zylen Corporation is a company that has Head Quarter (HQ) in KL and a Branch Office in Kampar. The company had subscribed to two Internet Service Providers (ISPs) namely ISP\_1 and ISP\_2. ISP\_1 is the preferred service provider in order to allow its devices and users to connect over the Internet. Public\_Server is to host company websites and to act as DNS server. HQ is using 38.38.38.0/29 whereas Branch Office is using 88.88.88.0/30 for Internet access. Addressing table to support the network topology as shown in the following table.

**Addressing Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IP address/Subnet Mask** | **Default Gateway** |
| ISP\_1 | S0/0/0 (DCE) | 20.20.20.5/30 | - |
| S0/1/0 (DCE) | 8.8.8.1/30 | - |
| S0/1/1 (DCE) | 8.8.8.6/30 | - |
| G0/0 | 18.18.18.1/27 | - |
| ISP\_2 | S0/0/0 (DCE) | 20.20.20.1/30 | - |
| S0/1/0 | 20.20.20.6/30 | - |
| Main | S0/2/0 | 8.8.8.2/30 | - |
| S0/2/1 | 20.20.20.2/30 | - |
| S0/1/0 (DCE) | 172.16.20.1/30 | - |
| S0/1/1 (DCE) | 172.16.30.1/30 | - |
| G0/0/0 | 172.16.10.1/30 | - |
| Tunnel 1 | 192.168.99.1/30 | - |
| Block\_A | G1/0/1 | 172.16.10.2/30 | - |
| G1/0/2 | 192.168.1.1/29 | - |
| G1/0/3 | 172.16.50.1/30 | - |
| Block\_B | S0/1/0 | 172.16.20.2/30 | - |
| S0/1/1 | 172.16.40.2/30 | - |
| G0/0/1 | 172.16.50.2/30 | - |
| G0/0/0.10 | 192.168.2.1/24 | - |
| G0/0/0.20 | 192.168.3.1/24 | - |
| Block\_C | S0/0/0 | 172.16.30.2/30 | - |
| S0/1/0 (DCE) | 172.16.40.1/30 | - |
| G0/0 | 192.168.4.1/29 | - |
| Edge | S0/1/0 | 8.8.8.5/30 | - |
| G0/0 | 10.10.10.1/27 | - |
| G0/1 | 10.10.20.1/29 | - |
| Tunnel 1 | 192.168.99.2/30 | - |
| Public\_PC | NIC | 18.18.18.3/27 | 18.18.18.1 |
| Developer\_Laptop | NIC | 10.10.10.5/27 | 10.10.10.1 |
| IT\_Admin\_PC | NIC | 192.168.4.2/29 | 192.168.4.1 |
| Public\_Server | NIC | 192.168.1.4/29 | 192.168.1.1 |
| Local\_Server | NIC | 10.10.20.6/29 | 10.10.20.1 |
| Designer\_PC | NIC | DHCP Client | |
| HR\_PC | NIC | DHCP Client | |

**Objectives**

This SBA will cover hand-on skills that are related to Static Routing, GRE, OSPF, DHCP, NAT and ACL.

**Pre-configurations**

Public\_PC, Public\_Server, Local\_Server, IT\_Admin\_PC and Developer\_Laptop were configured with IP addresses. Block\_B Router is configured to support Inter-VLAN routings between Design Department and HR Department. **Main Router** had been set with passwords. The password to access to line console is ***Pass1***. Enable secret is ***Pass2***. SSH account has been configured for Main Router. Username is ***Admin*** and password is ***RemotePass***. You are not required to access to CLI of ISP\_2 Router and S1.

**Tasks**

**Part 1: Configure static routes at ISP\_1 Router.**

**Step 1:** Configure a static route (38.38.38.0/29) based on **next hop IP address** in order to support HQ network.

ISP\_1(config)#ip route 38.38.38.0 255.255.255.248 8.8.8.2

**Step 2:** Configure a floating static route (38.38.38.0/29) based on next hop IP address in order to support HQ network via ISP\_2 with an AD of 5.

ISP\_1(config)#ip route 38.38.38.0 255.255.255.248 20.20.20.6 5

**Step 3:** Configure a static route (88.88.88.0/30) based on exit interface in order to support Branch Office network.

ISP\_1(config)#ip route 38.38.38.0 255.255.255.252 s0/1/1

**Part 2: Configure default static routes at Main Router and Edge Router.**

**Step 1:** Configure a default static route based on exit interface that Main Router is connecting to ISP\_1 Router.

Main(config)#ip route 0.0.0.0 0.0.0.0 s0/2/0

**Step 2:** In case connection to ISP\_1 is interrupted and therefore perform configuration of a floating default static route based on next hop IP address that Main Router is connecting to ISP\_2 Router with an AD of 5.

Main(config)#ip route 0.0.0.0 0.0.0.0 20.20.20.1 5

**Step 3:** Configure a default static route based on next hop IP address that Edge Router is connecting to ISP\_1 Router.

Edge(config)#ip route 0.0.0.0 0.0.0.0 8.8.8.6

**Part 3: Configure a GRE Tunnel.**

**Step 1:** Configure a GRE Tunnel at Main Router and Edge Router.

Main(config)#int tunnel 1

Main(config-if)#ip add 192.168.99.1 255.255.255.252

Main(config-if)#tunnel source s0/2/0

Main(config-if)#tunnel destination 8.8.8.5

Edge(config)#int tunnel 1

Edge(config-if)#ip add 192.168.99.2 255.255.255.252

Edge(config-if)#tunnel source s0/1/0

Edge(config-if)#tunnel destination 8.8.8.2

**Part 4: Configure OSPF with Process ID 33.**

**Step 1:**Activate routing for the Multi Layer Switch.

Block\_A(config)#ip routing

**Step 2:**Router ID for Main Router is 4.4.4.4. Router-ID for Block\_A Router is 3.3.3.3. Block\_B Router will use 2.2.2.2 as the Router ID whereas 1.1.1.1 is the Router ID for Block\_C Router.

Main(config)#router ospf 33

Main(config-router)#router-id 4.4.4.4

Block\_A(config)#router ospf 33

Block\_A(config-router)#router-id 3.3.3.3

Block\_B(config)#router ospf 33

Block\_B(config-router)#router-id 2.2.2.2

Block\_C(config)#router ospf 33

Block\_C(config-router)#router-id 1.1.1.1

**Step 3:**Advertise all the possible routes (refer to the topology diagram and addressing table for details).

Block\_B(config)#router ospf 33

Block\_B(config-router)#network 172.16.20.0 0.0.0.3 area 0

Block\_B(config-router)#network 172.16.40.0 0.0.0.3 area 0

Block\_B(config-router)#network 172.16.50.0 0.0.0.3 area 0

Block\_B(config-router)#network 192.168.2.0 0.0.0.255 area 0

Block\_B(config-router)#network 192.168.3.0 0.0.0.255 area 0

Block\_A(config)#router ospf 33

Block\_A(config-router)#network 172.16.10.0 0.0.0.3 area 0

Block\_A(config-router)#network 172.16.50.0 0.0.0.3 area 0

Block\_A(config-router)#network 192.168.1.0 0.0.0.7 area 0

Main(config-router)#network 8.8.8.0 0.0.0.3 area 0

Main(config-router)#network 20.20.20.0 0.0.0.3 area 0

Main(config-router)#network 172.16.10.0 0.0.0.3 area 0

Main(config-router)#network 172.16.20.0 0.0.0.3 area 0

Main(config-router)#network 172.16.30.0 0.0.0.3 area 0

Block\_C(config-router)#network 172.16.30.0 0.0.0.3 area 0

Block\_C(config-router)#network 172.16.40.0 0.0.0.3 area 0

Block\_C(config-router)#network 192.168.4.0 0.0.0.7 area 0

**Step 4:**Configure passive interfaces for all the OSPF routers in order to allowed OSPF packets to be sent to OSPF neighbor routers only.

Block\_B(config-router)#passive-interface g0/0/0

Block\_B(config-router)#passive-interface g0/0/0.10

Block\_B(config-router)#passive-interface g0/0/0.20

Block\_C(config-router)#passive-interface g0/0

Main(config-router)#passive-interface s0/2/0

Main(config-router)#passive-interface s0/2/1

Block\_A(config-router)#passive-interface g1/0/2

**Step 5:** Inject the default route into the OSPF routing domain and propagate the route to all OSPF routers in the HQ network.

Main(config-router)#default-information originate

**Part 5: Configure DHCP at Block\_C Router.**

**Step 1:**That router will provide IP addressing to DHCP clients for two networks (192.168.2.0/24 and 192.168.3.0/24)

**Step 2:** The first 10 addresses of 192.168.2.0/24 are not supposed to be used by DHCP clients. DHCP clients from 192.168.3.0/24 will use a start address of 192.168.3.16 until 192.168.3.254.

**Step 3:**DHCP Pool is *VLAN10User* for 192.168.2.0/24 network whereas 192.168.3.0/24 network is based on a DHCP Pool called as *VLAN20User*.

**Step 4:** The DNS Server is referred to the Public\_Server with IPv4 address of 192.168.1.4

**Step 5:** Configure Designer\_PC and HR\_PC to be the DHCP clients.

Block\_C(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10

Block\_C(config)#ip dhcp pool VLAN10User

Block\_C(dhcp-config)#network 192.168.2.0 255.255.255.0

Block\_C(dhcp-config)#default-router 192.168.2.1

Block\_C(dhcp-config)#dns-server 192.168.1.4

Block\_C(config)#ip dhcp excluded-address 192.168.3.1 192.168.3.15

Block\_C(config)#ip dhcp pool VLAN20User

Block\_C(dhcp-config)#network 192.168.3.0 255.255.255.0

Block\_C(dhcp-config)#default-router 192.168.3.1

Block\_C(dhcp-config)#dns-server 192.168.1.4

Block\_B(config-if)#int g0/0/0.10

Block\_B(config-subif)#ip helper-address 172.16.40.1

Block\_B(config-subif)#int g0/0/0.20

Block\_B(config-subif)#ip helper-address 172.16.40.1

**Part 6: Configure NAT at HQ network and Branch Office network.**

**Step 1:** Configure Public\_Server to use a public IPv4 address of 38.38.38.1/29.

Main(config)#ip nat inside source static 192.168.1.4 38.38.38.1

**Step 2:** Configure ip nat outside and inside for all the necessary router interfaces at HQ network.

Main(config)#int g0/0/0

Main(config-if)#ip nat inside

Main(config-if)#int s0/1/0

Main(config-if)#ip nat inside

Main(config-if)#int s0/1/1

Main(config-if)#ip nat inside

Main(config-if)#int s0/2/1

Main(config-if)#ip nat outside

Main(config-if)#int s0/2/0

Main(config-if)#ip nat outside

**Step 3:** Configure a Dynamic NAT by using a name called *IT\_Department* that will use the public IPv4 addresses from 38.38.38.2 to 38.38.38.4. Use an ACL number *1* that allowed Block\_C Router LAN to use the addresses from 38.38.38.2 to 38.38.38.4.

Main(config)#ip nat pool IT\_Department 38.38.38.2 38.38.38.4 netmask 255.255.255.248

Main(config)#access-list 1 permit 192.168.4.0 0.0.0.7

Main(config)#ip nat inside source list 1 pool IT\_Department

**Step 4:** Configure PAT for 192.168.2.0/24 network by using a pool name called as *Design\_Department* and use **a shared public IPv4 address of 38.38.38.5**. Use ACL number *2*that is allowed users from 192.168.2.0/24 network to access to Internet.

Main(config)#ip nat pool Design\_Department 38.38.38.5 38.38.38.5 netmask 255.255.255.248

Main(config)#access-list 2 permit 192.168.2.0 0.0.0.255

Main(config)#ip nat inside source list 2 pool Design\_Department overload

**Step 5:** Configure NAT Overload for 192.168.3.0/24 network by using a pool name called as *HR\_Department* and use a shared public IPv4 address of 38.38.38.6. Use ACL number *3*that is allowed users from 192.168.3.0/24 network to access to Internet.

Main(config)#ip nat pool HR\_Department 38.38.38.6 38.38.38.6 netmask 255.255.255.248

Main(config)#access-list 3 permit 192.168.3.0 0.0.0.255

Main(config)#ip nat inside source list 3 pool HR\_Department overload

**Step 6:** Configure a Dynamic NAT by using a name called *IT\_Department\_Branch* that will use two public IPv4 addresses from 88.88.88.0/30. Use an ACL number *1* that allowed Edge Router G0/0 LAN to online.

Edge(config)#ip nat pool IT\_Department\_Branch 88.88.88.1 88.88.88.2 netmask 255.255.255.252

Edge(config)#access-list 1 permit 10.10.10.0 0.0.0.31

Edge(config)#ip nat inside source list 1 pool IT\_Department\_Branch

**Step 7:** Configure ip nat outside and inside for all the necessary router interfaces at Branch Office network.

Edge(config)#int g0/0

Edge(config-if)#ip nat inside

Edge(config-if)#int s0/1/0

Edge(config-if)#ip nat outside

**Part 7: Configure ACL**

**Step 1:**Prepare an extended ACL called as *OpenToPublic*. Internet PCs from outside of Zylen Corporation are not allowed to ping and send echo messages tpero the Public\_Server, permit WWW traffics, permit HTTPS traffics that is based on the port number of 443, permit DNS traffics that is based on the port number of 53, and permit general IPv4 packets. Implement the ACL to **Main Router** that is related to interfaces for S0/2/0 and S0/2/1.

Main(config)#ip access-list extended OpenToPublic

Main(config)#deny icmp any host 38.38.38.1 echo

Main(config)#permit tcp any any eq www

Main(config)#permit tcp any any eq 443

Main(config)#permit tcp any any eq 53

Main(config)#permit ip any any

Main(config)#int s0/2/0

Main(config- line)#ip access-group OpenToPublic in

Main(config)#int s0/2/1

Main(config- line)#ip access-group OpenToPublic in

**Step 2:** Use a standard ACL with number *10* that allowing IT\_Admin\_PC to use **Main Router** **via SSH only.**

Main(config)#access-list 10 permit host 192.168.4.2

Main(config)#line vty 0 4

Main(config-line)#access-class 10 in

Main(config-line)#transport input ssh

**Step 3:** According to the company policy, lower half of 192.168.2.0/24 whereby those clients were not allowed to communicate with HR personnel and the HR network address is 192.168.3.0/24. Other PCs are allowed to communicate with network 192.168.3.0/24. Prepare a standard ACL with a name called as *Restrict\_Access*. Implement the ACL at interface G0/0/0.20 of **Block\_B Router**.

Block\_B(config)#ip access-list standard Restrict\_Access

Block\_B(config-std-nacl)#deny 192.168.2.0 0.0.0.127

Block\_B(config-std-nacl)#permit any

Block\_B(config-std-nacl)#int g0/0/0.20

Block\_B(config-subif)#ip access-group Restrict\_Access out

**Step 4:**Configure an ACL with number *128*for Block\_C Router.

The first statement is to permit 192.168.2.0/24 to use DHCP service in order for **DHCP clients** to detect and communicate with the DHCP server (Block\_C Router).

The second statement is to permit 192.168.3.0/24 to use DHCP service.

The third statement is to allow DNS traffics to go through by using *domain*keyword.

The fourth is to permit http traffics by using a port number of 80. Following of the next statement that is allow https traffics to go through by using a port number of 443.

Last ACE statement of that ACL list is to allowed and permit OSPF packets. Implement the list at interface S0/1/0 of **Block\_C Router** with the appropriate traffic direction.

Block\_C(config)#access-list 128 permit udp 192.168.2.0 0.0.0.255 eq bootpc any eq bootps

Block\_C(config)#access-list 128 permit udp 192.168.3.0 0.0.0.255 eq bootpc any eq bootps

Block\_C(config)#access-list 128 permit udp any any eq domain

Block\_C(config)#access-list 128 permit tcp any any eq 80

Block\_C(config)#access-list 128 permit tcp any any eq 443

Block\_C(config-if)#access-list 128 permit ospf any any

Block\_C(config)#int s0/1/0

Block\_C(config-if)#ip access-group 128 in

**Part 8: Connectivity tests and verifications by using ping, trace route and web browser of PCs.**

**Step 1:** Public\_PC is able to view Zylen website by using URL namely www.zylen.com. Public\_PC is not allowed to ping to the Public\_Server.

**Step 2:**All internal client hosts that are used by users (Designer\_PC, HR\_PC, IT\_Admin\_PC and Developer\_Laptop) can online by ping to Public\_PC and can access to Intranet (www.zylendic.com)

**Step 3:**All internal client hosts that are used by users (Designer\_PC, HR\_PC, IT\_Admin\_PC and Developer\_Laptop) can use the Local\_Server. Trace route to Local\_Server from IT\_Admin\_PC. The packets will be sent over to the tunnel.

**Step 4:**According to the policy of the company, Designer\_PC is not allowed to ping to HR\_PC. IT\_Admin\_PC is the only host that can use SSH to the Main Router.

~~~~~~~~~~ THE END ~~~~~~~~~~