**Network Security – Practical Assignment (20 marks)**

This is an individual assignment. You are required to carry out the following two tasks as part of this assignment that carries 20% towards your final score.

**Note:** Plagiarism is a serious offence that may lead to failure of this module. Please be assured your independent work is much recognized, appreciated and awarded.

**Submission Details:**

The task-1 requires you to save the packet tracer file (.pkt) as “Admin No\_Name.pkt” and the task-2 as a word document in “Admin No\_Name.doc”. Zip them together and upload into BB under the submission tab as shown below. You will have about 3-4 weeks to submit. Due date is 6th February 2022 2359 Hrs. For late submissions up to a week after the due date will have up to 50% penalty (10% every day) and zero will be graded subsequently.

**Task 1 (16 marks)**

To design and implement a secured network infrastructure on packet tracer as per the scenario and requirement listed below.

**Scenario**

You are the Security Consultant of ‘Best Capital’ that offers online financial services to its clients. They have their HQ at Raffles Place, a branch office at Changi Business Park that hosts the IT development team and a satellite office at Jurong West.

**General Requirement**

· Company has Two network administrators namely Admin1 and Admin2. They have accounts created locally on the routers with secret password as ‘admin\_no\_AdminX’ à X is 1 and 2 respectively for Admin1 and Admin2. E.g. ‘123456D\_Admin1’ &’123456D\_Admin2’

O All the devices to have hostnames as ‘admin\_no\_location’ E.g. 123456D\_Branch

o All the devices to have enable passwords as ‘admin\_no\_enable’ E.g. 123456D\_enable’

· All the routers to accept only two(2) virtual lines through SSH and are authenticated (AAA) through Radius server located at branch@changi. In case radius server is not available, local accounts to be used for AAA. Radius Server has a user account ‘Admin3’ with password as’admin\_no\_Admin3’. Telnet, Console and Auxiliary connections not to be allowed.

· Passwords used on all the routers must be encrypted when displayed (Eg.sh run config)

· All the routers are time-synchronized with the NTP server set-up at Branch@Changi.

**NTP Parameters Table**

| NTP Server | Key | MD5 Password |
| --- | --- | --- |
| xx.xx.xx.xx | 1 | NetSec |

· The entire network must have OSPF as the routing protocol with Type 2 authentication with the key as “Admin\_no\_5%6Yhj”.

· Hello and Dead intervals between HQ and Branch routers to be set as 10 and 15 respectively. For Branch and Satellite routers, Hello and Dead intervals to be 10 and 20 respectively. Note there is no direct connectivity between Satellite office and HQ.

· Each network to have at least one PC connected to test connectivity.

**HQ @ Raffles**

· HQ hosts a single LAN consists of three departments across three floors namely HR(8 staff), Finance(6 staff) and Management(4 staff) and all the staff provided with only desktops. i.e You need to plan for a single subnet that consists of HR, Finance and Management departments.

· HQ hosts web server and online portal server that have public access over port 443.

· HQ has the budget to implement firewall (ASA5505) and secure the network infrastructure by implementing security policies for inside and DMZ network as per your learning in this module.

· Port Security is to be enabled as per the requirement above and unused ports must be administratively disabled. Any breaches must require administrator’s action.

**Branch Office @ Changi**

· Branch hosts only IT department that has 5 staff members with laptops.

· Branch hosts Radius Server that provides authentication to all the routers across Best Capital.

· Branch hosts NTP Server and all the routers across Best capital obtain clock information from this NTP Server.

· Branch does not have budget for a firewall and hence appropriate ACLs to be used to secure/restrict access.

o Access to the Radius Server to be limited (to only HQ/Satellite offices

o Access to other servers hosted at the branch to be limited to only the HQ/Satellite offices with the specific port numbers as applicable.

· Port Security is to be enabled with the maximum of 2 MAC addresses and rest of the unused ports to be administratively disabled. Any breaches do NOT require administrator’s action.

· Branch office has connectivity to the ISP and the required routing (Hint: Default route) is to be configured for all the devices to access Internet through this link. ISP uses router model 1841 and uses 64K serial link (DCE) to connect to the Branch office.

**Satellite Office @ Jurong**

· Purpose of satellite office is to allow mobile agents (about five) to use IT services. To assist them, two network ports have been set-up for the agents to connect their laptop to access resources at HQ.

· Port Security is to be enabled and configured as appropriate.

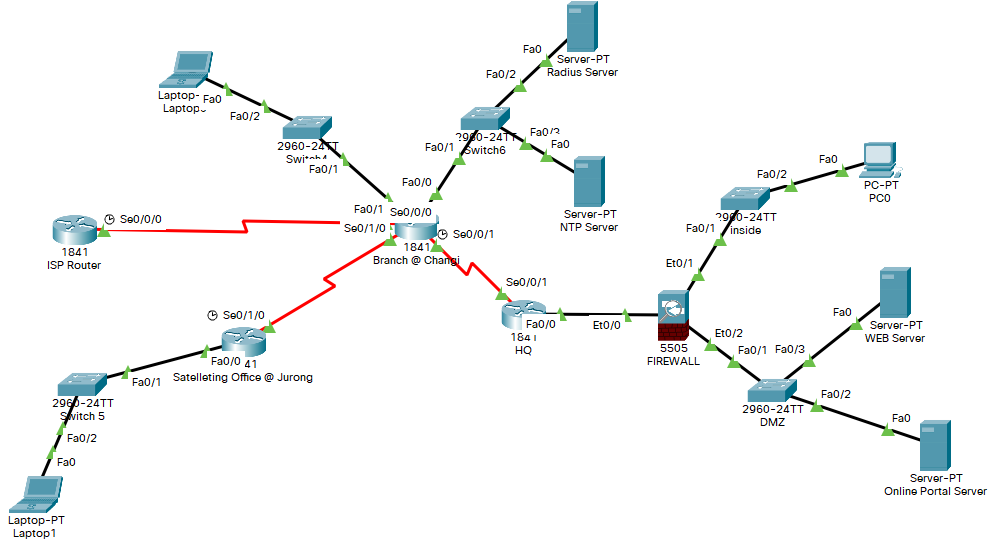
· No direct connectivity exists between this office and HQ but access through Branch office @ Changi

**Task 2 (4 marks)**

Write a detailed report that covers the following points:

· Your considerations for the network IP address and VLSM design.

· Tabulate (as per the table below) all the IP addresses used per location basis including the mask chosen. Do note that your choice of mask should be closer to the number of host machines required in the subnet as per the requirement in order not to waste any IP addresses.



**Number of hosts needed in each area**

**HQ @ Raffles**

* Firewall
  + VLAN 1 (Inside)
    - HR = 8
    - Finance = 6
    - Management = 4
    - VLAN Interface = 1
    - Total = **19**
  + VLAN 2 (DMZ)
    - Web Server = 1
    - Online Portal Server = 1
    - VLAN Interface = 1
    - Total = **3**
  + VLAN 3 (Outside)
    - HQ Router interface = 1
    - Firewall VLAN Interface = 1
    - IP addresses for DMZ servers to map to = 2
    - Total = **4**

**Branch Office @ Changi**

* IT = 5
* Radius Server = 1
* NTP Server = 1
* Router interface (Fa0/1 + Fa0/0) = 2
* Total = 5 + 1 + 1 + 2 = **10**

**Satellite Office @ Jurong**

* Mobile agents = 5, but only 2 ports is used
* Router interface = 1
* Total = 2 + 1 = **3**

| **Area** | **IP Address** | **Subnet Mask** | **First Usable** | **Last Usable** | **No . of usable IPs** |
| --- | --- | --- | --- | --- | --- |
| HQ @ Raffles | 192.168.1.0 | /24 = 255.255.255.0 | 192.168.1.1 | 192.168.1.255 | 254 |
| Branch @ Changi | 172.16.0.0 | /29 = 255.255.255.248 | 172.16.0.1 | 172.16.0.14 | 6 |
| Office @ Jurong | 10.0.0.0 | /29 = 255.255.255.248 | 10.0.0.1 | 10.0.0.6 | 6 |

| **HQ FIREWALL VLANs** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **VLAN** | **IP Address** | **Subnet Mask** | **First Usable** | **Last Usable** | **No. of usable IPs** |
| 1 (Inside) | 192.168.1.0 | /27 = 255.255.255.224 | 192.168.1.1 | 192.168.1.30 | 30 |
| 2 (DMZ) | 192.168.1.32 | /29 = 255.255.255.248 | 192.168.1.33 | 192.168.1.38 | 6 |
| 3 (Outside) | 192.168.1.40 | /29 = 255.255.255.248 | 192.168.1.41 | 192.168.1.48 | 6 |

| **HQ DMZ Servers** | | |
| --- | --- | --- |
| **VLAN** | **IP Address Mapping for Outside VLAN** | **Subnet Mask** |
| Web Server | 192.168.1.43 | /29 = 255.255.255.248 |
| Online Portal Server | 192.168.1.44 | /29 = 255.255.255.248 |

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** | **Switch Port** |
| --- | --- | --- | --- | --- | --- |
| Firewall | VLAN 1 (Inside) | 192.168.1.1 | 255.255.255.224 | NIL | Inside Fa0/1 and  DMZ Fa0/1 |
| Firewall | VLAN 2 (DMZ) | 192.168.1.33 | 255.255.255.224 | NIL | Inside Fa0/1 and  DMZ Fa0/1 |
| Firewall | VLAN 3 (Outside) | 192.168.1.42 | 255.255.255.248 | NIL | Inside Fa0/1 and  DMZ Fa0/1 |
| HQ @ Raffles | Fa0/0 (To Firewall) | 192.168.1.41 | 255.255.255.248 | NIL | NIL |
| HQ @ Raffles | Se0/0/1 (To Branch) | 10.1.255.1 | 255.255.255.252 | NIL | NIL |
| Branch @ Changi | Se0/0/1 (To HQ) | 10.1.255.2 | 255.255.255.252 | NIL | NIL |
| Branch @ Changi | Se0/0/0 (To ISP) | 209.165.200.2 | 255.255.255.252 | NIL | NIL |
| Branch @ Changi | Fa0/0 (To Switch6) | 172.16.0.1 | 255.255.255.248 | NIL | Switch 6 Fa0/1 |
| Branch @ Changi | Fa0/1 (To Switch4) | 172.16.0.9 | 255.255.255.248 | NIL | Switch 4 Fa0/1 |
| Branch @ Changi | Se0/1/0 (To Office) | 10.1.255.9 | 255.255.255.252 | NIL | NIL |
| ISP Router | Se0/0/0 (To Branch) | 209.165.200.1 | 255.255.255.252 | NIL | NIL |
| Satellite @ Jurong | Se0/1/0 (To Branch) | 10.1.255.10 | 255.255.255.252 | NIL | NIL |
| Satellite @ Jurong | Fa0/0 (To Switch5) | 10.0.0.1 | 255.255.255.248 | NIL | Switch 5 Fa0/1 |
| Laptop 1 | Fa0 (To Switch5) | 10.0.0.2 | 255.255.255.248 | 10.0.0.1 | Fa0/2 |
| Laptop 0 | Fa0 (To Switch4) | 172.16.0.14 | 255.255.255.248 | 172.16.0.9 | Fa0/2 |
| Radius Server | Fa0 (To Switch6) | 172.16.0.3 | 255.255.255.248 | 172.16.0.1 | Fa0/2 |
| NTP Server | Fa0 (To Switch6) | 172.16.0.4 | 255.255.255.248 | 172.16.0.1 | Fa0/3 |
| PC 0 | Fa0 (To Inside) | 192.168.1.30 | 255.255.255.224 | 192.168.1.1 | Fa0/2 |
| Web Server | Fa0 (To DMZ) | 192.168.1.34 | 255.255.255.224 | 192.168.1.33 | Fa0/3 |
| Online Portal Server | Fa0 (To DMZ) | 192.168.1.35 | 255.255.255.224 | 192.168.1.33 | Fa0/2 |

· Your considerations, justification and explanation of the security measures implemented at every location.

· Document the verification/test results by attaching screenshots where applicable.

· Any assumptions made must be stated clearly under a separate section “Assumptions”.

· Attach the current configuration of every device that you have implemented as annex.

**Assignment Rubrics**

| Individual | Excellent  (A) | Very Good  (B) | Good  (C) | Satisfactory  (D) | Unsatisfactory  (F) |
| --- | --- | --- | --- | --- | --- |
| Task – 1  Design and implementation of secured network infrastructure based on stated requirement | All requirements working seamlessly and well-implemented. | Most requirements working and well-implemented. | Some requirements working and generally well-implemented. | Some requirements are incomplete or erroneous. | Requirements are mostly incomplete or erroneous. |
| Task – 2  Detailed report on the network IP design, considerations, justifications for different security requirement and justifications. | Report is well organized and written. All information clearly explained and conveyed.  Good use of language, with no grammar and spelling mistakes. | Report is organized and written. Most information clearly explained and conveyed.  Good use of language, with few grammar and spelling mistakes. | Report is somewhat organized and written. Some information clearly explained and conveyed.  Good use of language, with some grammar and spelling mistakes. | Report is badly organised and written and lacking clear explanation of information.  Poor use of language, with many grammar and spelling mistakes. | Report is unclear, confusing, and badly organized/written.  Poor use of language, with too many grammar and spelling mistakes that leads to content being incomprehensible. |

**Assumptions/Suggestions**

1. Each area is assigned their own IP address range for futureproofing. It will be easier to increase the amount of usable IP addresses as they would only need to do so for one area compared to changing the addressing for all of the areas. It also helps reduce the chances of human error due to confusing the IP addresses as they are distinctly different compared to using IP ranges such as 192.168.1.0 and 192.168.0.0.
2. Only PC0 will be connected to the port Fa0/2 of Inside switch at HQ, and all the other 17 staff members’ desktops will be connected using one of the ports only
3. Inside switch ports Fa0/2 to Fa0/19 will be used for the HQ staff’s desktops and thus will not be administratively disabled while the other ports will be
4. There will only be one ACL on the Branch @ Changi for easier administration rather than creating ACLs on every port on the Branch router to only allow traffic originating from HQ and Satelliting Office going towards the Branch’s servers. Thus, the ACL will be placed on Branch’s Fa0/0 rather than as close to the source as possible.
5. Port-security is only configured on ports that are connected to end devices
6. For Branch’s Switch4, only ports F0/2 - F0/6 will be used for connecting to end devices
7. For Branch and Satellites’ switches, the administrators would also want the logs of when the switch’s port security settings are violated to allow for logging for future references.
8. Administrators will not be assigning the MAC-addresses themselves when setting the switches’ port-security. Thus, mac-address sticky is used instead
9. Satellite Office’s Switch 5’s port F0/2 and F0/3 will be used to allow the 5 agents to connect and will be used interchangeably. *Purpose of satellite office is to allow mobile agents (about five) to use IT services. To assist them, two network ports have been set-up for the agents to connect their laptop to access resources at HQ*
10. Best Capital’s ISP only provided them only one public IP address
11. HQ should be directly connected to the ISP router. This is because currently, in order for the public to access the DMZ servers, it has to go through the Branch router, then towards the HQ, then towards the DMZ. This is dangerous as the public will be able to access the other offices such as the Satelliting Office @ Jurong, and the Branch @ Changi since there are no security devices implemented such as Firewalls as it is only installed only on the HQ’s side.
12. Enable passive-interface by default so that OSPF update packets cannot be received from those ports, preventing rogue routers from modifying the OSPF database
13. HQ’s Inside VLAN should not be able to be pinged
14. ISP Router do not have to configure anything other than S0/0/0 port interface for testing purposes as we do not have access to the ISP router realistically.
15. DMZ switch

**Configurations**

**HQ**

***Hostname***

Router(config)#**hostname 204461H\_HQ**

***Enable password***

204461H\_HQ(config)#**enable secret 204461H\_enable**

***Local accounts***

204461H\_HQ(config)#**username Admin1 secret 204461H\_Admin1**

204461H\_HQ(config)#**username Admin2 secret 204461H\_Admin2**

***SSH only***

204461H\_HQ(config)#**line vty 0 1**

204461H\_HQ(config-line)#**transport input ssh**

204461H\_HQ(config-line)#**login authentication default**

204461H\_HQ(config)#**ip domain-name Best-Capital.com**

204461H\_HQ(config)#**crypto key zeroize rsa**

204461H\_HQ(config)#**crypto key generate rsa**

How many bits in the modulus [512]: **1024**

204461H\_HQ(config)#**line aux 0**

204461H\_HQ(config)#**transport output none**

204461H\_HQ(config)#**line con 0**

204461H\_HQ(config)#**transport output none**

***Radius authentication***

204461H\_HQ(config)#**radius host 172.16.0.3**

204461H\_HQ(config)#**aaa new-model**

204461H\_HQ(config)#**aaa authentication login default group radius local**

***Encrypt passwords***

204461H\_HQ(config)#**service password-encryption**

***NTP server***

204461H\_HQ(config)#**ntp server 172.16.0.4**

204461H\_HQ(config)#**ntp authenticate**

204461H\_HQ(config)#**ntp trusted-key 1**

204461H\_HQ(config)#**ntp authentication-key 1 md5 NetSec**

204461H\_HQ(config)#**ntp update-calendar**

***Interface configuration***

204461H\_HQ(config)#**int fa0/0**

204461H\_HQ(config-if)#**ip add 192.168.1.41 255.255.255.252**

204461H\_HQ(config-if)#**no shut**

204461H\_HQ(config-if)#**int s0/0/1**

204461H\_HQ(config-if)#**ip add 10.1.255.1 255.255.255.252**

204461H\_HQ(config-if)#**no shut**

***OSPF***

204461H\_HQ(config)#**router ospf 1**

204461H\_HQ(config-router)#**network 192.168.1.41 255.255.255.252 area 0**

204461H\_HQ(config-router)#**network 10.1.255.1 255.255.255.252 area 0**

204461H\_HQ(config-router)#**passive-interface default**

204461H\_HQ(config-router)#**no passive-interface s0/0/1**

***OSPF authentication***

204461H\_HQ(config-router)#**area 0 authentication message-digest**

204461H\_HQ(config)**int s0/0/1**

204461H\_HQ(config-router)#**ip ospf message-digest-key 1 md5 204461H\_5%6Yhj**

204461H\_HQ(config-if)#**ip ospf hello-interval 10**

204461H\_HQ(config-if)#**ip ospf dead-interval 15**

**Branch**

***Hostname***

Router(config)#**hostname 204461H\_Branch**

***Enable password***

204461H\_Branch(config)#**enable secret 204461H\_enable**

***Local accounts***

204461H\_Branch(config)#**username Admin1 secret 204461H\_Admin1**

204461H\_Branch(config)#**username Admin2 secret 204461H\_Admin2**

204461H\_Branch(config-line)#**login authentication default**

204461H\_Branch(config)#**crypto key zeroize rsa**

204461H\_Branch(config)#**crypto key generate rsa**

How many bits in the modulus [512]: **1024**

***SSH only***

204461H\_Branch(config)#**line vty 0 1**

204461H\_Branch(config-line)#**transport input ssh**

204461H\_Branch(config-line)#**login authentication default**

204461H\_Branch(config)#**ip domain-name Best-Capital.com**

204461H\_Branch(config)#**crypto key zeroize rsa**

204461H\_Branch(config)#**crypto key generate rsa**

How many bits in the modulus [512]: **1024**

204461H\_Brannch(config)#**line aux 0**

204461H\_Branch(config)#**transport output none**

204461H\_Branch(config)#**line con 0**

204461H\_Branch(config)#**transport output none**

***Radius authentication***

204461H\_Branch(config-line)#**radius host 172.16.0.3**

204461H\_Branch(config)#**aaa new-model**

204461H\_Branch(config)#**aaa authentication login default group radius local**

***Encrypt passwords***

204461H\_Branch(config)#**service password-encryption**

***NTP server***

204461H\_Branch(config)#**ntp server 172.16.0.4**

204461H\_Branch(config)#**ntp authenticate**

204461H\_Branch(config)#**ntp trusted-key 1**

204461H\_Branch(config)#**ntp authentication-key 1 md5 NetSec**

204461H\_Branch(config)#**ntp update-calendar**

***Interface configuration***

204461H\_Branch(config)#**int s0/0/1**

204461H\_Branch(config-if)#**ip add 10.1.255.2 255.255.255.252**

204461H\_Branch(config-if)#**no shut**

204461H\_Branch(config-if)#**int s0/0/0**

204461H\_Branch(config-if)#**ip add 10.1.255.5 255.255.255.252**

204461H\_Branch(config-if)#**no shut**

204461H\_Branch(config-if)#**int fa0/0**

204461H\_Branch(config-if)#**ip add 172.16.0.1 255.255.255.248**

204461H\_Branch(config-if)#**no shut**

204461H\_Branch(config-if)#**int fa0/1**

204461H\_Branch(config-if)#**ip add 172.16.0.9 255.255.255.248**

204461H\_Branch(config-if)#**no shut**

204461H\_Branch(config-if)#**int s0/1/0**

204461H\_Branch(config-if)#**ip add 10.1.255.9 255.255.255.252**

204461H\_Branch(config-if)#**no shut**

***OSPF***

204461H\_Branch(config-if)#**router ospf 1**

204461H\_Branch(config-router)#**network 10.1.255.2 255.255.255.252 area 0**

204461H\_Branch(config-router)#**network 172.16.0.1 255.255.255.248 area 0**

204461H\_Branch(config-router)#**network 172.16.0.9 255.255.255.248 area 0**

204461H\_Branch(config-router)#**network 10.1.255.9 255.255.255.252 area 0**

204461H\_Branch(config-router)#**passive-interface default**

204461H\_Branch(config-router)#**no passive-interface s0/1/0**

204461H\_Branch(config-router)#**no passive-interface s0/0/1**

***OSPF authentication***

204461H\_Branch(config-router)#**area 0 authentication message-digest**

204461H\_Branch(config-router)#**int s0/0/1**

204461H\_Branch(config-if)#**ip ospf message-digest-key 1 md5 204461H\_5%6Yhj**

204461H\_Branch(config-if)#**ip ospf hello-interval 10**

204461H\_Branch(config-if)#**ip ospf dead-interval 15**

204461H\_Branch(config)#**int s0/1/0**

204461H\_Branch(config-if)#**ip ospf message-digest-key 1 md5 204461H\_5%6Yhj**

204461H\_Branch(config-if)#**ip ospf hello-interval 10**

204461H\_Branch(config-if)#**ip ospf dead-interval 20**

***Access List***

204461H\_Branch(config)#**ip access-list extended Access-To-Servers**

204461H\_Branch(config)#**permit ip 10.1.255.0 0.0.0.3 host 172.16.0.3**

204461H\_Branch(config)#**permit ip 10.1.255.8 0.0.0.3 host 172.16.0.3**

204461H\_Branch(config)#**permit udp 10.1.255.0 0.0.0.3 host 172.16.0.4 eq 123**

204461H\_Branch(config)#**permit udp 10.1.255.0 0.0.0.3 host 172.16.0.4 eq 123**

204461H\_Branch(config)#**int f0/0**

204461H\_Branch(config)#**ip access-group Access-To-Servers out**

***ISP connection***

204461H\_Branch(config)#**ip route 0.0.0.0 0.0.0.0 209.165.200.1**

204461H\_Branch(config)#**router ospf 1**

204461H\_Branch(config-router)#**default-information originate**

204461H\_Branch(config)#**ip access-list extended Internet-Access**

204461H\_Branch(config-ext-nacl)#**permit ip any any**

204461H\_Branch(config)#**int range f0/0 - 1**

204461H\_Branch(config-if-range)#**ip nat inside**

204461H\_Branch(config)#**int s0/0/0**

204461H\_Branch(config-if)#**ip nat outside**

204461H\_Branch(config)#**int s0/1/0**

204461H\_Branch(config)#**ip nat inside**

204461H\_Branch(config)#**ip nat inside source list Internet-Access interface s0/0/0 overload**

***Refer to Assumptions/Suggestions point 10***

**Satellite**

***Hostname***

Router(config)#**hostname 204461H\_Satellite**

***Enable password***

204461H\_Satellite(config)#**enable secret 204461H\_enable**

***Local accounts***

204461H\_Satellite(config)#**username Admin1 secret 204461H\_Admin1**

204461H\_Satellite(config)#**username Admin2 secret 204461H\_Admin2**

***SSH only***

204461H\_Satellite(config)#**line vty 0 1**

204461H\_Satellite(config-line)#**transport input ssh**

204461H\_Satellite(config-line)#**login authentication default**

204461H\_Satellite(config)#**ip domain-name Best-Capital.com**

204461H\_Satellite(config)#**crypto key zeroize rsa**

204461H\_Satellite(config)#**crypto key generate rsa**

How many bits in the modulus [512]: **1024**

204461H\_Satellite(config)#**line aux 0**

204461H\_Satellite(config)#**transport output none**

204461H\_Satellite(config)#**line con 0**

204461H\_Satellite(config)#**transport output none**

***Radius authentication***

204461H\_Satellite(config)#**radius host 172.16.0.3**

204461H\_Satellite(config)#**aaa new-model**

204461H\_Satellite(config)#**aaa authentication login default group radius local**

***Encrypt passwords***

204461H\_Satellite(config)#**service password-encryption**

***NTP server***

204461H\_Satellite(config)#**ntp server 172.16.0.4**

204461H\_Satellite(config)#**ntp authenticate**

204461H\_Satellite(config)#**ntp trusted-key 1**

204461H\_Satellite(config)#**ntp authentication-key 1 md5 NetSec**

204461H\_Satellite(config)#**ntp update-calendar**

***Interface configuration***

204461H\_Satellite(config)#**int s0/1/0**

204461H\_Satellite(config-if)#**ip add 10.1.255.10 255.255.255.252**

204461H\_Satellite(config-if)#**no shut**

204461H\_Satellite(config-if)#**int fa0/0**

204461H\_Satellite(config-if)#**ip add 10.0.0.1 255.255.255.248**

204461H\_Satellite(config-if)#**no shut**

***OSPF***

204461H\_Satellite(config)#**router ospf 1**

204461H\_Satellite(config-router)#**network 10.1.255.10 255.255.255.252 area 0**

204461H\_Satellite(config-router)#**network 10.0.0.1 255.255.255.248 area 0**

204461H\_Satellite(config-router)#**passive-interface default**

204461H\_Satellite(config-router)#**no passive-interface s0/1/0**

***OSPF authentication***

204461H\_Satellite(config-router)**area 0 authentication message-digest**

204461H\_Satellite(config)#**int s0/1/0**

204461H\_Satellite(config-if)#**ip ospf message-digest-key 1 md5 204461H\_5%6Yhj**

204461H\_Satellite(config-if)#**ip ospf hello-interval 10**

204461H\_Satellite(config-if)#**ip ospf dead-interval 20**

**Firewall**

***Hostname***

ciscoasa(config)#**hostname 204461H-HQ-Firewall**

***A hostname for ASA device must start and end with a letter or digit, and have as interior characters only letters, digits, or a hyphen.***

***Interface configuration***

204461H-HQ-Firewall(config)#**int vlan 1**

204461H-HQ-Firewall(config-if)#**nameif inside**

204461H-HQ-Firewall(config-if)#**ip add 192.168.1.1 255.255.255.224**

204461H-HQ-Firewall(config-if)#**security-level 100**

204461H-HQ-Firewall(config)#**int vlan 2**

204461H-HQ-Firewall(config)#**no forward interface Vlan 1**

***Needed if want to name more than two interfaces***

204461H-HQ-Firewall(config-if)#**nameif dmz**

204461H-HQ-Firewall(config-if)#**security-level 70**

204461H-HQ-Firewall(config-if)#**ip add 192.168.1.33 255.255.255.248**

204461H-HQ-Firewall(config-if)#**int vlan 3**

204461H-HQ-Firewall(config-if)#**nameif outside**

204461H-HQ-Firewall(config-if)#**ip add 192.168.1.42 255.255.255.248**

204461H-HQ-Firewall(config-if)#**security-level 0**

204461H-HQ-Firewall(config-if)#**int Et0/0**

204461H-HQ-Firewall(config-if)#**switchport access vlan 3**

204461H-HQ-Firewall(config-if)#**int Et0/2**

204461H-HQ-Firewall(config-if)#**switchport access vlan 2**

***Check if VLAN is assigned properly in show run before continuing. If it is not assigned, run copy run start and reload the ASA***

***Route to outside network***

204461H-HQ-Firewall(config-if)#**route outside 0.0.0.0 0.0.0.0 192.168.1.41**

***Create network object for PAT for Inside network to Outside network***

204461H-HQ-Firewall(config)#**object network inside-net**

204461H-HQ-Firewall(config-network-object)#**subnet 192.168.1.0 255.255.255.224**

204461H-HQ-Firewall(config-network-object)#**nat (inside, outside) dynamic interface**

***Inspection policy***

204461H-HQ-Firewall(config)#**class-map inspection\_default**

204461H-HQ-Firewall(config-cmap)#**match default-inspection-traffic**

204461H-HQ-Firewall(config-cmap)#**policy-map global\_policy**

204461H-HQ-Firewall(config-pmap)#**class inspection\_default**

204461H-HQ-Firewall(config-pmap-c)#**inspect icmp**

204461H-HQ-Firewall(config-pmap-c)#**exit**

204461H-HQ-Firewall(config)#**service-policy global\_policy global**

***Tells Firewall to inspect and allow ICMP traffic***

***Ensure inside network is able to ping outside network before continuing***

***Create network object for NAT for DMZ network to Outside network***

204461H-HQ-Firewall(config)#**object network web-server**

204461H-HQ-Firewall(config-network-object)**#host 192.168.1.34**

204461H-HQ-Firewall(config-network-object)#**nat (dmz,outside) static 192.168.1.43**

***Map web server IP address to 192.168.1.43 which allows the users in the outside network to connect to***

204461H-HQ-Firewall(config)#**object network online-portal**

204461H-HQ-Firewall(config-network-object)**#host 192.168.1.35**

204461H-HQ-Firewall(config-network-object)#**nat (dmz,outside) static 192.168.1.44**

***Map online-portal server IP address to 192.168.1.44 which allows the users in the outside network to connect to***

***Create ACL to allow HTTPS traffic into DMZ***

204461H-HQ-Firewall(config)#**access-list OUTSIDE-DMZ permit tcp any 192.168.1.32 255.255.255.248 eq 443**

204461H-HQ-Firewall(config)#**access-group OUTSIDE-DMZ in interface outside**

**Inside Switch**

***Hostname***

Switch(config)#**hostname 204461H\_Inside\_Switch**

***Enable password***

204461H\_Inside\_Switch(config)#**enable secret 204461H\_enable**

***Switch port security***

204461H\_Inside\_Switch(config)#**int range f0/2 - 19**

***Refer to Assumption/Suggestions point 3***

204461H\_Inside\_Switch(config-if-range)#**switchport mode access**

***Needed or else an error occurs: Command rejected: FastEthernet0/2 is a dynamic port.***

204461H\_Inside\_Switch(config-if-range)#**switchport port-security**

204461H\_Inside\_Switch(config-if-range)#**switchport port-security maximum 1**

***Set to 1 device allowed only, refer to Assumption/Suggestions point 2.***

204461H\_Inside\_Switch(config-if-range)#**switchport port-security mac-address sticky**

204461H\_Inside\_Switch(config-if-range)#**switchport port-security violation shutdown**

204461H\_Inside\_Switch(config)#**int range f0/20 - 24**

204461H\_Inside\_Switch(config-if-range)#**shut**

204461H\_Inside\_Switch(config)#**int range g0/1 - 2**

204461H\_Inside\_Switch(config-if-range)#**shut**

**Switch 4**

***Hostname***

Switch(config)#**hostname 204461H\_Branch\_Switch4**

***Enable password***

204461H\_Branch\_Switch4(config)#**enable secret 204461H\_enable**

***Switch port security***

204461H\_Branch\_Switch4(config-if-range)#**int range f0/2 - 6**

***Refer to Assumption/Suggestions point 6***

204461H\_Branch\_Switch4(config-if-range)#**switchport mode access**

204461H\_Branch\_Switch4(config-if-range)#**switchport port-security**

204461H\_Branch\_Switch4(config-if-range)#**switchport port-security maximum 2**

204461H\_Branch\_Switch4(config-if-range)#**switchport port-security mac-address sticky**

204461H\_Branch\_Switch4(config-if-range)#**switchport port-security violation restrict**

***Refer to Assumption/Suggestions point 7***

204461H\_Branch\_Switch4(config)#**int range f0/7 - 24**

204461H\_Branch\_Switch4(config-if-range)#**shut**

204461H\_Branch\_Switch4(config)#**int range g0/1 - 2**

204461H\_Branch\_Switch4(config-if-range)#**shut**

**Switch 5**

***Hostname***

Switch(config)#**hostname 204461H\_Satellite\_Switch5**

204461H\_Satellite\_Switch5(config)#**int range f0/2-3**

***Refer to Assumption/Suggestions point 9***

204461H\_Satellite\_Switch5(config-if-range)#**switchport mode access**

204461H\_Satellite\_Switch5(config-if-range)#**switchport port-security**

204461H\_Satellite\_Switch5(config-if-range)#**switchport port-security maximum 5**

204461H\_Satellite\_Switch5(config-if-range)#**switchport port-security mac-address sticky**

204461H\_Satellite\_Switch5(config-if-range)#**switchport port-security violation restrict**

204461H\_Satellite\_Switch5(config)#**int range f0/4 - 24**

204461H\_Satellite\_Switch5(config-if-range)#**shut**

204461H\_Satellite\_Switch5(config)#**int range g0/1 - 2**

204461H\_Satellite\_Switch5(config-if-range)#**shut**

**DMZ Switch**

***Hostname***

Switch(config)#**hostname 204461H\_Branch\_Switch4**

***Interfaces***

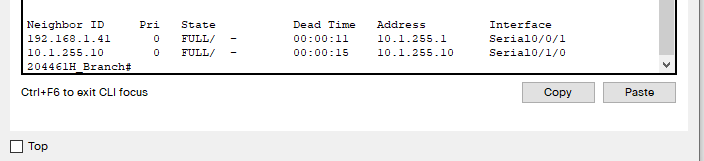
204461H\_Branch\_Switch4(config)#**int range f0/4-24**

204461H\_Branch\_Switch4(config-if-range)#**shut**

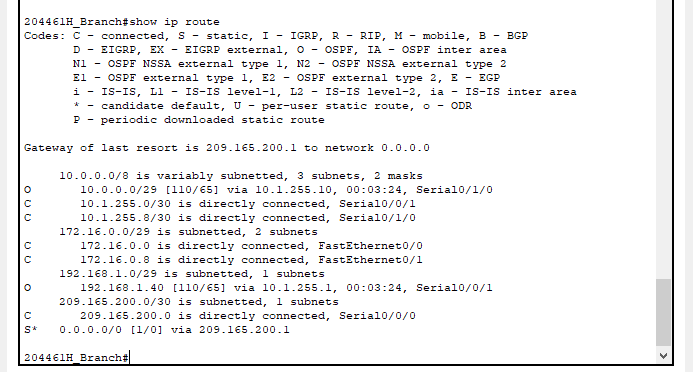
204461H\_Branch\_Switch4(config-if-range)#**int range g0/1-2**

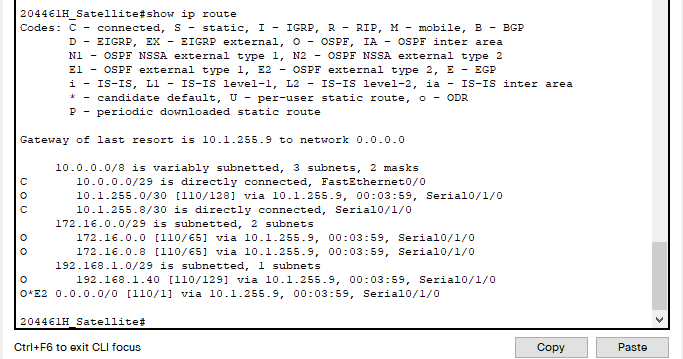
204461H\_Branch\_Switch4(config-if-range)#**shut**

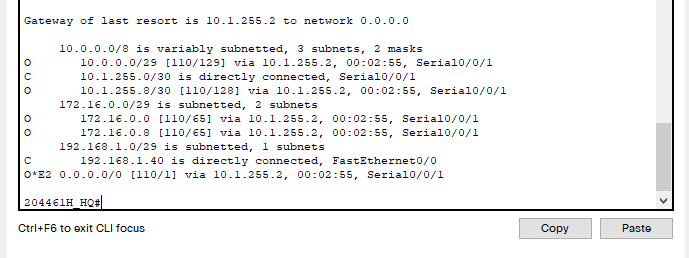
**Screenshots**

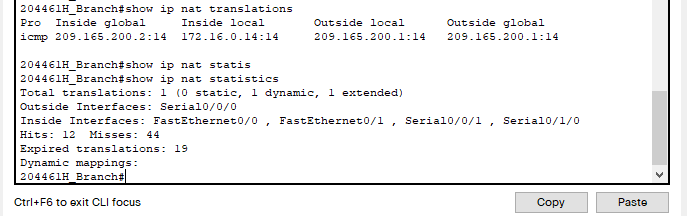
**OSPF**

**ISP connection**

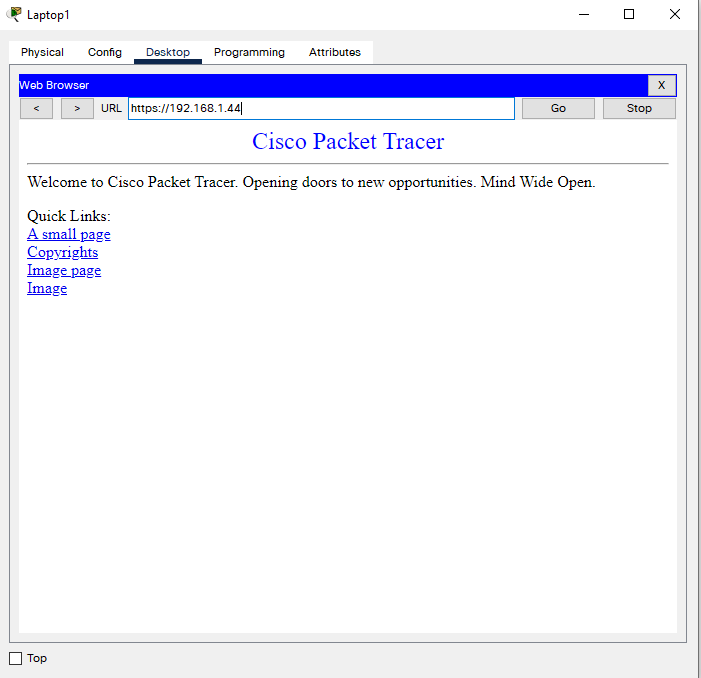
****

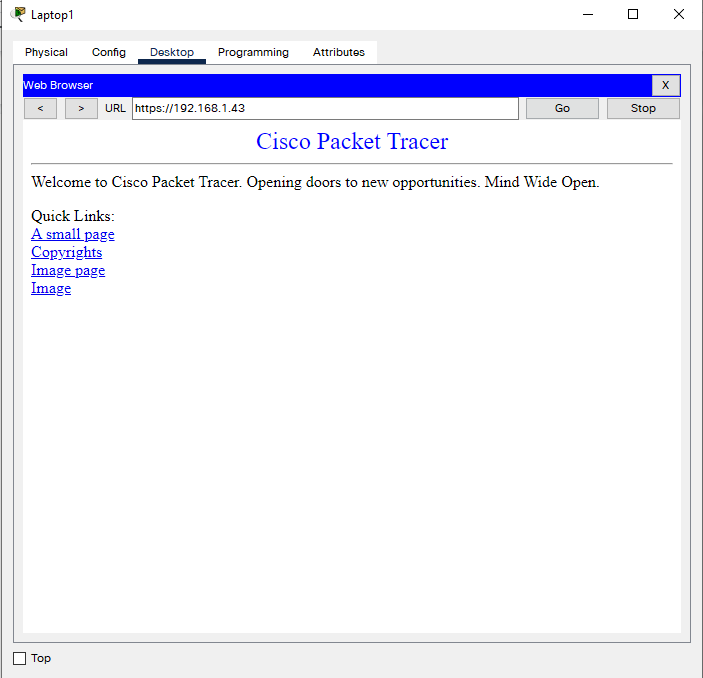
****

****

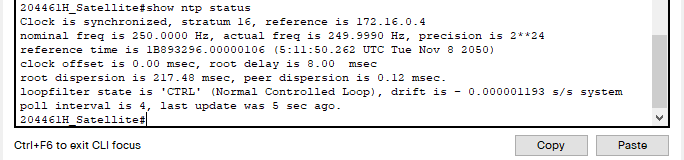
******

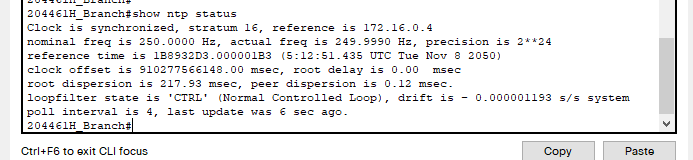
**Access to WEB Server and Online Portal Server through HTTPS only**

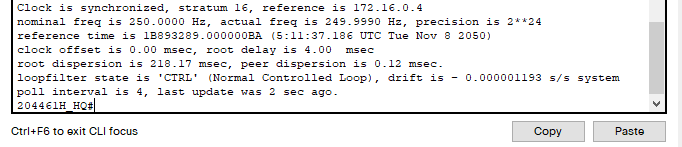
****

****

**NTP Status**

****

****

****