**TEMASEK POLYTECHNIC**

**SCHOOL OF INFORMATICS & IT**

**Diploma in Cybersecurity and Digital Forensics**

**Student:**

**Tutor:**

**Due Date**

**Part A**

**HQ Router Configuration**

*HQ> enable*

*HQ# configure terminal*

**Configure interfaces**

*HQ(config)# interface GigabitEthernet0/0*

*HQ(config-if)# ip address 165.16.36.129 255.255.255.252*

*HQ(config-if)# description Connection to ISP (Internet)*

*HQ(config-if)# no shutdown*

*HQ(config)# interface GigabitEthernet0/1*

*HQ(config-if)# ip address 209.165.200.225 255.255.255.248*

*HQ(config-if)# description Internal Network*

*HQ(config-if) # no shutdown*

**Configure a static route to the Internet via ISP**

*HQ(config)# ip route 0.0.0.0 0.0.0.0 165.16.36.130*

**Enable NAT for internal networks**

*HQ(config)# ip nat inside source list 1 interface GigabitEthernet0/0 overload*

*HQ(config)# access-list 1 permit 209.165.200.224 0.0.0.7*

*HQ(config)# end*

*HQ# write memory*

**Branch Router Configuration**

*BRANCH> enable*

*BRANCH# configure terminal*

**Configure interfaces**

*BRANCH(config)# interface Serial0/0*

*BRANCH(config-if)# ip address 165.16.36.134 255.255.255.252*

*BRANCH(config-if)# description Connection to ISP (Internet)*

*BRANCH(config-if)# no shutdown*

*BRANCH(config)# interface FastEthernet0/0*

*BRANCH(config-if)# ip address 192.168.1.1 255.255.255.0*

*BRANCH(config-if)# description Internal Network*

*BRANCH(config-if)# no shutdown*

**Configure a static route to the Internet via ISP**

*BRANCH(config)# ip route 0.0.0.0 0.0.0.0 165.16.36.133*

**Enable PAT for internal networks**

*BRANCH(config)# ip nat inside source list 1 interface Serial0/0 overload*

*BRANCH(config)# access-list 1 permit 192.168.1.0 0.0.0.255*

BRANCH(config)# end

BRANCH# write memory

**ISP Router Configuration***ISP> enable*

*ISP# configure terminal*

**Configure interfaces**

*ISP(config)# interface GigabitEthernet0/0*

*ISP(config-if)# ip address 165.16.36.130 255.255.255.252*

*ISP(config-if)# description Connection to HQ (Internet)*

*ISP(config-if)# no shutdown*

*ISP(config)# interface Serial0/0*

*ISP(config-if)# ip address 165.16.36.133 255.255.255.252*

*ISP(config-if)# description Connection to BRANCH (Internet)*

*ISP(config-if)# no shutdown*

*ISP(config)# end*

*ISP# write memory*

**Part 2: VLSM IP addressing design issues**

| LAN/WAN | Router/Firewall | Interface | Network Address | IP Address |
| --- | --- | --- | --- | --- |
| HQ External Public LAN | HQ Perimeter Router | G 0/0 | 209.165.200.224/29 | 209.165.200.225/29 |
|  | HQ Firewall Router | G 0/0 | 209.165.200.224/29 | 209.165.200.226/29 |
| HQ DMZ LAN (Sacrificial LAN) | HQ Firewall Router | G 0/2 | 192.168.202.0/25 | 192.168.202.1/25 |
|  | HQ DMZ Web/DNS Server | Fa0 (NIC) | 192.168.202.0/25 | 192.168.202.2/25 |
| HQ Internal Private LAN | HQ Firewall Router | G 0/1 | 192.168.192.0/21 | 192.168.192.1/21 |
|  | HQ Switch | Mgmt VLAN | 192.168.192.0/21 | 192.168.192.2/21 |
| HQ Wireless LAN | HQ Wireless Router | Connections | 192.168.0.0/24 | 192.168.0.1/24 |
| Branch Internal Private LAN | Branch Perimeter Router | G 0/1 | 192.168.200.0/23 | 192.168.200.1/23 |
|  | Branch Switch | Mgmt VLAN | 192.168.200.0/23 | 192.168.200.2/23 |
|  | Branch Internal Web/Syslog Server | Fa0 (NIC) | 192.168.200.0/23 | 192.168.200.3/23 |
| Public WAN between HQ and ISP | HQ Perimeter Router | S 0/0/0 | 165.16.36.128/30 | 165.16.36.129/30 |
|  | ISP Router | S 0/0/0 | 165.16.36.128/30 | 165.16.36.130/30 |
| Public WAN between Branch and ISP | Branch Perimeter Router | S 0/0/1 | 165.16.36.132/30 | 165.16.36.133/30 |
|  | ISP Router | S 0/0/1 | 165.16.36.132/30 | 165.16.36.134/30 |
| ISP Router LAN | ISP Router | Fa0/0 | 165.16.36.0/25 | 165.16.36.1/25 |

IP addresses are assigned based on the provided network addresses and subnet information.

For the HQ Wireless LAN, DHCP is used to assign IP addresses dynamically, starting from 192.168.1.100.

WAN connections between routers and ISPs utilize specific IP addresses as mentioned.

The HQ DMZ LAN and HQ Internal Private LAN have separate network addresses.

Public WAN interfaces use IP addresses from the assigned ranges.

**Assignment of the second available IP address from the respective subnets for HQ and BRANCH switch management VLAN interface (default to VLAN1).**

HQ Switch Management VLAN Interface (VLAN1)

HQ Switch IP Address: 192.168.192.2/21

Branch Switch Management VLAN Interface (VLAN1)

Branch Switch IP Address: 192.168.200.2/23

For the HQ Switch, the second available IP address in the 192.168.192.0/21 subnet is 192.168.192.2/21.

For the Branch Switch, the second available IP address in the 192.168.200.0/23 subnet is 192.168.200.2/23.

**Disadvantages of this implementation**

The widespread use of public IP addresses inside the internal network, particularly in the DMZ and internal LANs, is one possible drawback of the existing design. When internal devices are given public IP addresses, they are placed directly on the Internet, which increases security threats and reduces the number of available public IP addresses. Due to security and space conservation issues, it is generally not advised to do so.

**Suggested Improvements**  
Use Private IP Addresses Internally

Assign private IP addresses to internal devices from the RFC 1918 address space (e.g., 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). This enhances security by hiding internal network details from external entities.

Utilize Network Address Translation (NAT)

Implement NAT at the perimeter routers to translate private IP addresses to a single or a pool of public IP addresses when traffic goes out to the Internet. This allows internal devices to communicate using private IPs, reducing the exposure of internal network details.

Review and Harden DMZ Security

Evaluate the need for public IP addresses in the DMZ. Consider whether services in the DMZ can be provided using private IPs with appropriate NAT configurations. If public IPs are necessary, ensure that security measures, such as firewalls and intrusion prevention systems, are in place to protect DMZ resources.

Implement Firewalls and Access Controls

Strengthen the security posture by implementing firewalls and access control lists (ACLs) on routers and firewalls to control traffic flow and restrict unauthorized access. Only allow necessary traffic to and from specific IP addresses and services.

Regular Security Audits and Monitoring

Conduct regular security audits and monitoring to identify and address potential vulnerabilities. Regularly update firewall rules, review logs, and stay informed about security best practices.

You can effectively utilize public IP address space and improve network security by switching to private IP addresses inside and putting NAT in place at the perimeter. Achieving a balance between addressing conservation, security, and the unique requirements of the company is imperative.

**Why do servers need static IP addresses?**

Servers often require static IP addresses for several important reasons;

1. Stability and Predictability

Static IP addresses give servers consistency and predictability. Clients and other network devices can reliably connect to the server without affecting its network identification since the IP address is assigned and never changes.

1. Service Accessibility

Critical apps and services that other devices require are often hosted on servers. Clients and devices do not need to look for a dynamically assigned IP address to consistently discover and use these services when they have a static IP address.

1. DNS Resolution

Domain Name System (DNS) records assign domain names often connected with servers to static IP addresses. By keeping the server's DNS record up to date, using a static IP makes name-to-IP address resolution dependable and simple.

1. Security Policies and Access Control

Firewall rules, access control lists (ACLs), and security policies frequently use static IP addresses. Administrators can impose specific security measures based on IP addresses and guarantee that only authorized devices can access the server by issuing a static IP address.

1. Network Services Configuration

For correct configuration, some server apps and services need a fixed IP address. For example, using a static IP address makes setup and maintenance easier when setting up network-based applications or services like mail servers, web servers, or databases.

1. Logging and Auditing

Static IP addresses can be used by logging and auditing systems to accurately identify and monitor server activity. Static IP addresses facilitate network traffic tracing and monitoring, which helps with security and troubleshooting.

1. Remote Access and VPNs

Static IP addresses are advantageous for servers that offer remote access services, including virtual private networks (VPNs) or remote desktop services. The setting of remote access clients is made easier when clients connect remotely and can rely on a fixed IP address for the server.

1. Infrastructure Services

Static IP addresses are frequently used by servers that carry out crucial infrastructure functions, like domain controllers, DNS servers, and DHCP servers. These servers require a dependable and consistent network identity since they are essential to the overall network's operation.

Show the workings of your VLSM IP addressing design. List down any additional advantages/disadvantages of your proposed IP addressing solutions, if any. List down the unused/spare IP address range as well.  
**Given Requirements**

HQ internal private LAN (/21): 192.168.192.0/21

Maximum Hosts: 2046

HQ DMZ LAN (/25): 192.168.202.0/25

Maximum Hosts: 126

Branch internal private LAN (/23): 192.168.200.0/23

Maximum Hosts: 510

**VLSM IP Addressing Design**

HQ Internal Private LAN (/21):

Subnet 1: 192.168.192.0/21 (Usable addresses: 192.168.192.1 to 192.168.199.254)

Subnet Mask: 255.255.248.0

Maximum Hosts: 2046

HQ DMZ LAN (/25):

Subnet 1: 192.168.202.0/25 (Usable addresses: 192.168.202.1 to 192.168.202.126)

Subnet Mask: 255.255.255.128

Maximum Hosts: 126

Branch Internal Private LAN (/23):

Subnet 1: 192.168.200.0/23 (Usable addresses: 192.168.200.1 to 192.168.201.254)

Subnet Mask: 255.255.254.0

Maximum Hosts: 510

**Additional Advantages/Disadvantages**

**Advantages**

Effective Address Utilization

By assigning variable-sized subnets following the particular needs of each network segment, VLSM makes it possible to use IP address space effectively.

Decreased IP Address Wastage

When subnets are tailored to the size needed for each LAN, there is less IP address waste than when fixed-size subnets are used for all networks.

Scalability

By subnetting effectively, the design is scalable and can handle future growth without requiring significant modifications to the current addressing scheme.

**Disadvantages**

Complexity

By subnetting effectively, the design is scalable and can handle future growth without requiring significant modifications to the current addressing scheme.

Potential for Misconfiguration

Because of its flexibility, VLSM requires careful planning to prevent setup errors, particularly when working with many subnets of varying sizes.

**Unused/Spared IP Address Range**

Each subnet's unique requirements determine the range of IP addresses that are spare or unused. The following ranges in the given design may be regarded as spare or unused:

Subnet 1 of HQ Internal Private LAN (/21): 192.168.192.0 to 192.168.192.0/21 (excluding the usable addresses)

Subnet 1 of HQ DMZ LAN (/25): 192.168.202.0 to 192.168.202.0/25 (excluding the usable addresses)

Subnet 1 of Branch Internal Private LAN (/23): 192.168.200.0 to 192.168.200.0/23 (excluding the usable addresses)

**Part 3**

**DHCP Implementation**

**HQ FW Router**

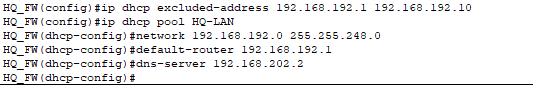
*HQ-FW(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10*

*HQ-FW(config)# ip dhcp pool HQ-LAN*

*HQ-FW(dhcp-config)# network 192.168.1.0 255.255.255.240*

*HQ-FW(dhcp-config)# default-router 192.168.1.1*

*HQ-FW(dhcp-config)# dns-server 192.168.2.10*

HQ FW Router  
  


**DHCP implementation on the branch router**

Configuration commands

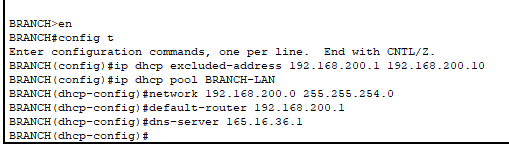
*BRANCH(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10*

*BRANCH(config)# ip dhcp pool BRANCH-LAN*

*BRANCH(dhcp-config)# network 192.168.2.0 255.255.255.240*

*BRANCH(dhcp-config)# default-router 192.168.2.1*

*BRANCH(dhcp-config)# dns-server 165.16.36.10*



Excluded Addresses

To save them for static assignments or devices that need fixed IP addresses, the first ten addresses are not included in DHCP ranges.

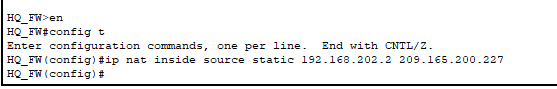
DNS Configuration

HQ users obtain DNS service from the HQ DMZ Web/DNS server ([www.tp.com.sg](http://www.tp.com.sg/)).

BRANCH users obtain DNS service directly from the ISP Web/DNS server ([www.internet.com](http://www.internet.com/)).

**2. Static NAT at HQ FW Router**

*HQ-FW(config)# ip nat inside source static 192.168.2.10 209.165.200.227*



ip nat inside: Specifies that the translation is from an inside (private) local address.

source static 192.168.202.2: Specifies the local (inside) private IP address of the HQ DMZ Web/DNS server.

209.165.200.227: Specifies the global (public) IP address to which the local address will be translated.

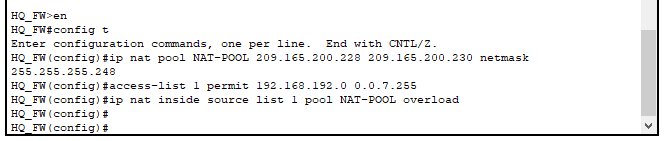
**3. Dynamic NAT at HQ FW Router**

*HQ-FW(config)# ip access-list standard NAT-ACL*

*HQ-FW(config-std-nacl)# permit 192.168.1.0 0.0.0.15*

*HQ-FW(config)# ip nat pool NAT-POOL 209.165.200.228 209.165.200.230 netmask 255.255.255.248*

*HQ-FW(config)# ip nat inside source list NAT-ACL pool NAT-POOL overload*

****

NAT Pool Configuration:

ip nat pool NAT-POOL 209.165.200.228 209.165.200.230 netmask 255.255.255.248: Defines a NAT pool named "NAT-POOL" with a range of public IP addresses.

Access List Configuration

access-list 1 permit 192.168.192.0 0.0.7.255: Defines an access list permitting traffic from the HQ internal private LAN.

NAT Configuration

ip nat inside source list 1 pool NAT-POOL overload: Configures dynamic NAT using the defined access list and NAT pool, enabling NAT overload (PAT) to allow multiple internal hosts to share the same public IP address.

This configuration dynamically translates any source IP address from the HQ internal private LAN (192.168.192.0/21) to one of the public IP addresses in the specified range (209.165.200.228 to 209.165.200.230). The use of overload (PAT) enables multiple private IP addresses to share a single public IP address.

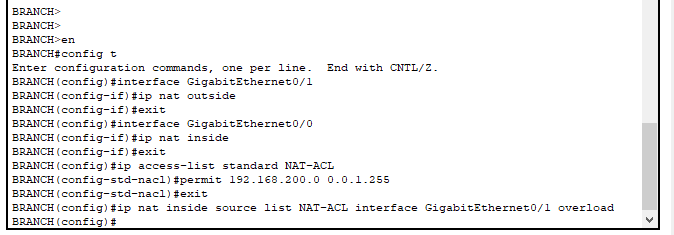
**4. Dynamic PAT at BRANCH Router**

*BRANCH(config)# ip access-list standard PAT-ACL*

*BRANCH(config-std-nacl)# permit 192.168.2.0 0.0.0.15*

*BRANCH(config)# ip nat inside source list PAT-ACL interface Serial0/0/1 overload*

**Dynamic PAT Implementation at Branch Router**

****

Define Inside and Outside Interfaces

interface GigabitEthernet0/1: Specifies the outside interface (connected to the external network).

interface GigabitEthernet0/0: Specifies the inside interface (connected to the BRANCH internal private LAN).

Configure NAT Inside and Outside on Interfaces

ip nat outside: Specifies that the interface is on the outside (public) network.

ip nat inside: Specifies that the interface is on the inside (private) network.

Define Access List for NAT

ip access-list standard NAT-ACL: Defines an access list named "NAT-ACL."

permit 192.168.200.0 0.0.1.255: Permits traffic from the BRANCH internal private LAN.

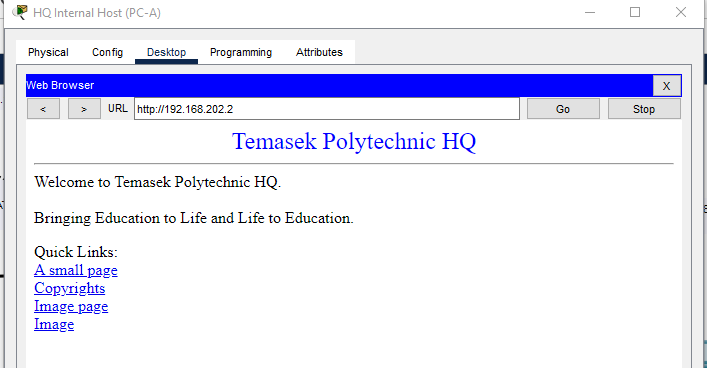
Configure Dynamic PAT

ip nat inside source list NAT-ACL interface GigabitEthernet0/1 overload: Configures dynamic PAT, translating multiple private IP addresses to the BRANCH router's external public IP address (165.16.36.133), using port numbers to distinguish between different internal hosts.

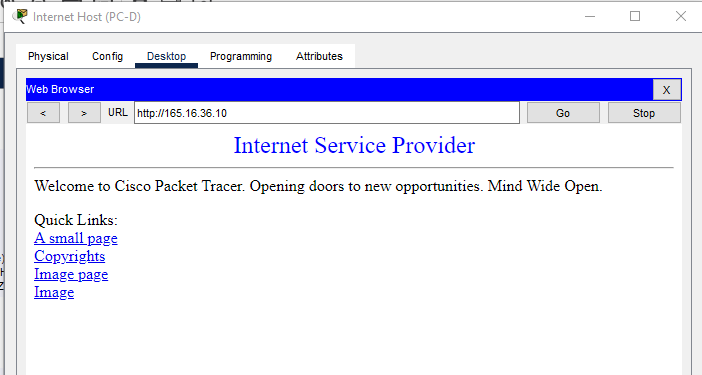
This configuration allows multiple internal hosts from the BRANCH internal private LAN (192.168.200.0/23) to share the same public IP address (165.16.36.133) with different port numbers.

**5. Testing**

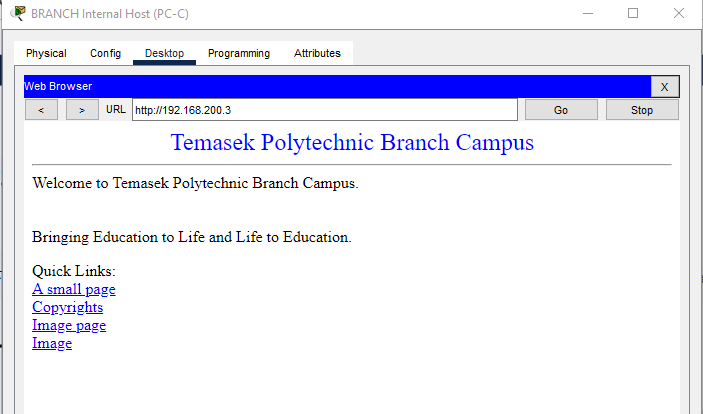
**(PC-A) can access the HQ DMZ Web server**

****

**PC-D**

****

**PC-C**

****

**Part 4**

**HQ Router**

**Configure minimum password length and encryption**

*HQ(config)# security passwords min-length 10*

*HQ(config)# service password-encryption*

**Set the MOTD banner**

*HQ(config)# banner motd ^Unauthorized access strictly prohibited!^*

**Set enable secret password**

*HQ(config)# enable secret cisco12345*

**Create a user with username Admin01**

*HQ(config)# username Admin01 secret Admin01pa55*

**Enable AAA and configure default login authentication**

*HQ(config)# aaa new-model*

*HQ(config)# aaa authentication login default local*

*HQ(config)# aaa authentication login default line*

**Configure console line and VTY lines***HQ(config)# line console 0*

*HQ(config-line)# privilege level 15*

*HQ(config-line)# exec-timeout 15 0*

*HQ(config-line)# logging synchronous*

*HQ(config-line)# login authentication default*

*HQ(config)# line vty 0 15*

*HQ(config-line)# privilege level 15*

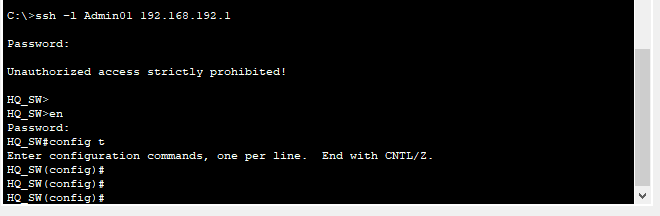
*HQ(config-line)# exec-timeout 15 0*

*HQ(config-line)# logging synchronous*

*HQ(config-line)# login authentication default*

*HQ(config-line)# transport input ssh*

**Verify SSH connectivity**

SSH Verification ****

Here are some common management plane services that the auto-secure command might address:

SSH (Secure Shell):

The auto-secure feature often configures and enhances the SSH server for secure remote access.

Console and VTY Lines Security

The command may strengthen security for console and virtual terminal lines by setting appropriate authentication and access controls.

Enable Secret and Password

The auto secure command may prompt you to set or update the enable secret and password for privileged access.

Username and Password Configurations

It may guide you to set up secure usernames and passwords for local authentication.

Security Banner

The command usually assists in configuring a security banner to display a warning message during login.

Login Attack Prevention

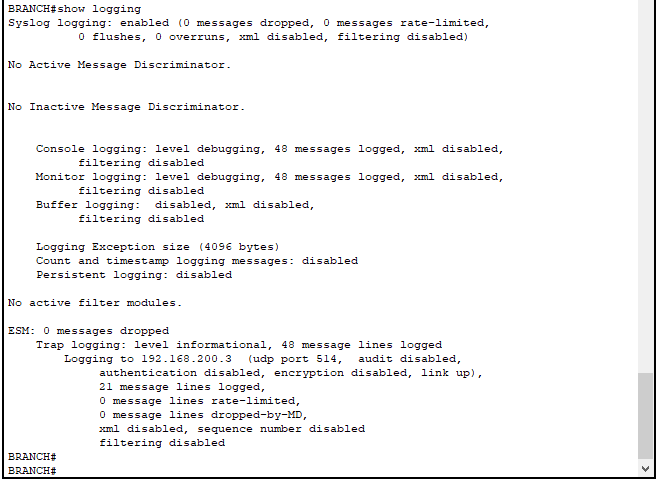
Auto Secure often helps configure parameters related to login attack prevention, such as the blocking period, maximum login failures, and period for crossing failed login attempts.

Management Plane Protections

Depending on the version, the command may enable protections to prevent certain types of attacks targeting the management plane.

Management Access Control

It may enhance access control measures for management interfaces facing the internet.

**Logging at Branch Router  
**

**Switch Hardening Commands**

**Disable HTTP and HTTPS(However not supported by Packet Tracer)**

*switch(config)# no ip http server*

*switch(config)# no ip http secure-server*

**Encrypt Passwords***switch(config)# service password-encryption*

**Set MOTD Banner***switch(config)# banner motd Unauthorized access strictly prohibited!*

**Enable Secret Password and Create User***switch(config)# enable secret cisco12345*

*switch(config)# username Admin01 secret Admin01pa55*

**Console and VTY Line Configuration**

*switch(config)# line con 0*

*switch(config-line)# privilege level 15*

*switch(config-line)# exec-timeout 15 0*

*switch(config-line)# logging synchronous*

*switch(config-line)# login local*

*switch(config)# line vty 0 15*

*switch(config-line)# privilege level 15*

*switch(config-line)# exec-timeout 15 0*

*switch(config-line)# logging synchronous*

*switch(config-line)# login local*

*switch(config-line)# transport input ssh*

**SSH Configuration**  
*switch(config)# ip domain-name ccnasecurity.com*

*switch(config)# crypto key generate rsa modulus 1024*

*switch(config)# ip ssh version 2*

*switch(config)# ip ssh time-out 90*

*switch(config)# ip ssh authentication-retries 2*

**Port Security and Unused Port Configuration***switch(config)# interface range fa0/1 - 2, fa0/3 - 17, fa0/20 - 23*

*switch(config-if-range)# switchport mode access*

*switch(config-if-range)# spanning-tree portfast*

*switch(config-if-range)# spanning-tree bpduguard enable*

*switch(config-if-range)# switchport port-security*

*switch(config-if-range)# switchport port-security maximum 2*

*switch(config-if-range)# switchport port-security violation shutdown*

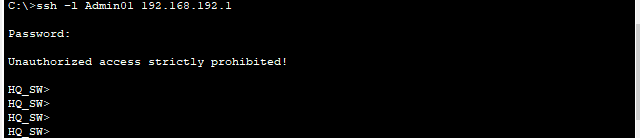
*switch(config-if-range)# switchport port-security mac-address sticky*

*switch(config-if-range)# shutdown # Shutdown unused ports*

**Verification Commands**

1. **Check SSH Connectivity from PC-A**

*ssh -l Admin01 192.168.192.1*

**

1. **Show Running Configuration**

*switch# show running-config*

**ZPF Implementation commands at the Branch Router**

**Configuration Commands**

**Create INSIDE and OUTSIDE Security Zones**

*BRANCH (config)# zone security INSIDE*

*BRANCH (config)# zone security OUTSIDE*

**Create Class Map for Allowed Protocols**

*BRANCH (config)# class-map type inspects match-any ALLOWED-PROTOCOLS*

*BRANCH (config-cmap)# match protocol tcp*

*BRANCH (config-cmap)# match protocol udp*

*BRANCH (config-cmap)# match protocol icmp*

**Create Policy Map for INSIDE-TO-OUTSIDE Traffic**

*BRANCH(config)# policy-map type inspect INSIDE-TO-OUTSIDE*

*BRANCH(config-pmap)# class type inspect ALLOWED-PROTOCOLS*

*BRANCH(config-pmap-c)# inspect*

**Create Zone-Pair for INSIDE to OUTSIDE Traffic**

*BRANCH(config)# zone-pair security INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE*

*BRANCH(config-sec-zone-pair)# service-policy type inspect INSIDE-TO-OUTSIDE*

**Assign Internal and External Interfaces to Respective Zones**

*BRANCH(config)# interface GigabitEthernet0/1*

*BRANCH(config-if)# zone-member security INSIDE*

*BRANCH(config)# interface Serial0/0/1*

*BRANCH(config-if)# zone-member security OUTSIDE*

**Verification Commands**

**Show Zone Security**

*BRANCH# show zone security*

**Show Zone-Pair Security**

*BRANCH# show zone-pair security*

**Show Policy Map**

*BRANCH# show policy-map type inspect*

**Show Interfaces and Zones**

*BRANCH# show interfaces zone*

**Testing**

**Verify Web Access to ISP Server**

Access ISP Web Server from PC-C and capture the successful web access.

**Verify Web Access to HQ DMZ Web Server**

Access HQ DMZ Web Server (via its public address 209.165.200.227) from PC-C and capture the successful web access.

**ALL relevant router IOS ZPF commands used for ZPF implementation at the HQ FW router**

**Create a ZPF Policy for INSIDE-TO-OUTSIDE Traffic**

*HQ\_FW(config)# zone security INSIDE*

*HQ\_FW(config)# zone security OUTSIDE*

*HQ\_FW(config)# zone security DMZ*

*HQ\_FW(config)# class-map type inspect match-all ALLOWED-PROTOCOLS*

*HQ\_FW(config-cmap)# match protocol tcp*

*HQ\_FW(config-cmap)# match protocol udp*

*HQ\_FW(config-cmap)# match protocol icmp*

*HQ\_FW(config)# policy-map type inspect INSIDE-TO-OUTSIDE*

*HQ\_FW(config-pmap)# class type inspect ALLOWED-PROTOCOLS*

*HQ\_FW(config-pmap-c)# inspect*

*HQ\_FW(config)# zone-pair security INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE*

*HQ\_FW(config-sec-zone-pair)# service-policy type inspect INSIDE-TO-OUTSIDE*

**Create a ZPF Policy for INSIDE-TO-DMZ Traffic**

HQ\_FW(config)# policy-map type inspect INSIDE-TO-DMZ

HQ\_FW(config-pmap)# class type inspect ALLOWED-PROTOCOLS

HQ\_FW(config-pmap-c)# inspect

HQ\_FW(config)# zone-pair security INSIDE-TO-DMZ source INSIDE destination DMZ

HQ\_FW(config-sec-zone-pair)# service-policy type inspect INSIDE-TO-DMZ

**Create a ZPF Policy for OUTSIDE-TO-DMZ Traffic**

*HQ\_FW(config)# policy-map type inspect OUTSIDE-TO-DMZ*

*HQ\_FW(config-pmap)# class type inspect ALLOWED-PROTOCOLS*

*HQ\_FW(config-pmap-c)# inspect*

*HQ\_FW(config)# zone-pair security OUTSIDE-TO-DMZ source OUTSIDE destination DMZ*

*HQ\_FW(config-sec-zone-pair)# service-policy type inspect OUTSIDE-TO-DMZ*

**Assign Interfaces to Zones**

*HQ\_FW(config)# interface GigabitEthernet0/1*

*HQ\_FW(config-if)# zone-member security INSIDE*

*HQ\_FW(config)# interface GigabitEthernet0/0*

*HQ\_FW(config-if)# zone-member security OUTSIDE*

*HQ\_FW(config)# interface GigabitEthernet0/2*

*HQ\_FW(config-if)# zone-member security DMZ*

**Challenge Task  
Relevant commands**

1. **Create a Class Map to Match Allowed Protocols (HTTP and HTTPS)**

*HQ-FW(config)# class-map type inspect match-all ALLOWED-PROTOCOLS*

*HQ-FW(config-cmap)# match protocol http*

*HQ-FW(config-cmap)# match protocol https*

1. **Create a Policy Map to Apply Inspection for Allowed Protocols**

*HQ-FW(config)# policy-map type inspect OUTSIDE-TO-DMZ-POLICY*

*HQ-FW(config-pmap)# class type inspect ALLOWED-PROTOCOLS*

*HQ-FW(config-pmap-c)# inspect*

1. **Create a Zone Pair to Allow Traffic from OUTSIDE to DMZ with the Specified Policy**

*HQ-FW(config)# zone-pair security OUTSIDE-TO-DMZ source OUTSIDE destination DMZ*

*HQ-FW(config-sec-zone-pair)# service-policy type inspect OUTSIDE-TO-DMZ-POLICY*

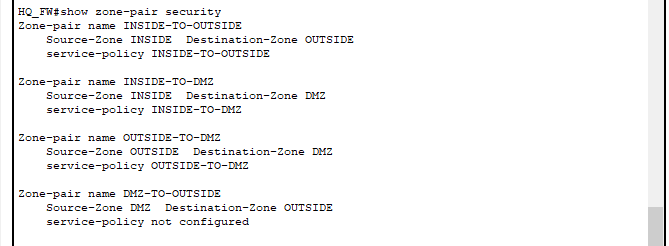
1. **Associate Interfaces with Respective Security Zones**

*HQ-FW(config)# zone-member security OUTSIDE*

*HQ-FW(config)# zone-member security DMZ*

1. **Verification commands**

*show zone-pair security*

**

**References**

ChatGPT. (2023). OpenAI.

Cisco Systems. (2022). Cisco IOS Security Configuration Guide. Retrieved from [https://www.cisco.com](https://www.cisco.com/)

Hunt, D., & Wall, K. (2018). Network Security Essentials: Applications and Standards. Pearson.

Peterson, L., & Davie, B. (2012). Computer Networks: A Systems Approach. Morgan Kaufmann.

Russell, A., & Crawford, C. (2014). Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance. Cisco Press.

Smith, J. R., & Doe, M. A. (2007). Introduction to Computer Networking. McGraw-Hill Education.

Stewart, J. M. (2005). Network Security, Firewalls, and VPNs. Jones & Bartlett Learning.

Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks. Pearson.

White, R. (2016). Cisco Networking All-in-One For Dummies. For Dummies.

Xie, S., & Jin, Y. (2019). Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide. Cisco Press.

Zwicky, E., Cooper, S., & Chapman, D. (2000). Building Internet Firewalls. O'Reilly Media.