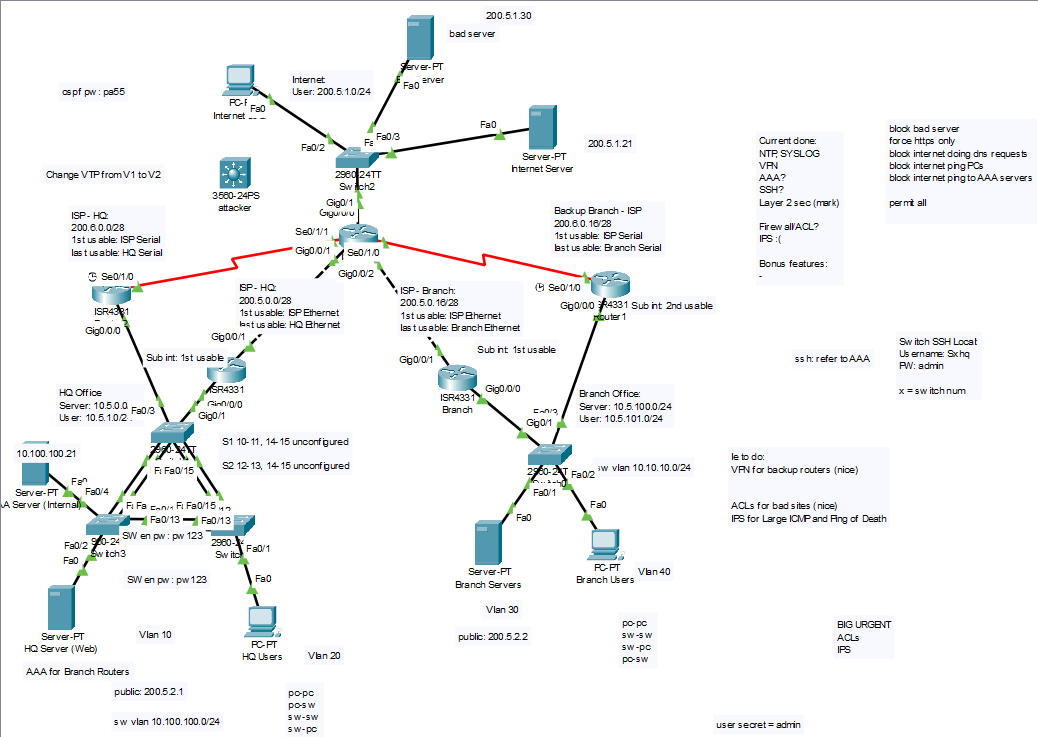
**Systems and Network Security Assignment (Report)**

**Members: Olfsen, Mark, Jiun Jie**

**Final Topology**

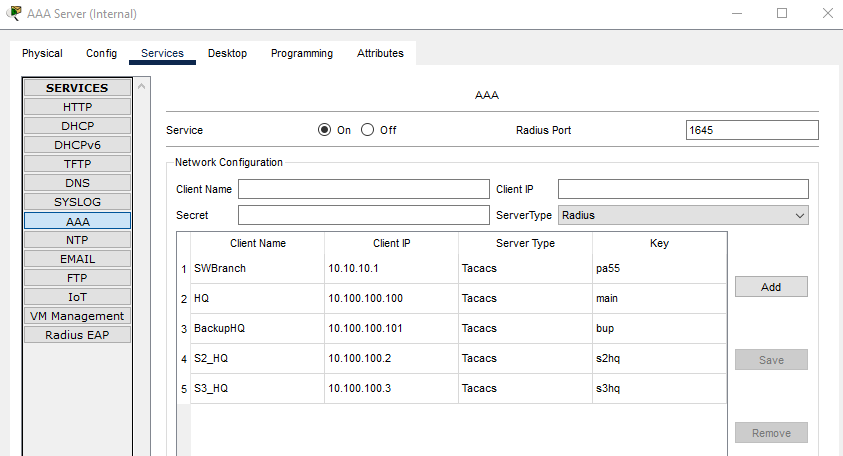


**IP Address Table**

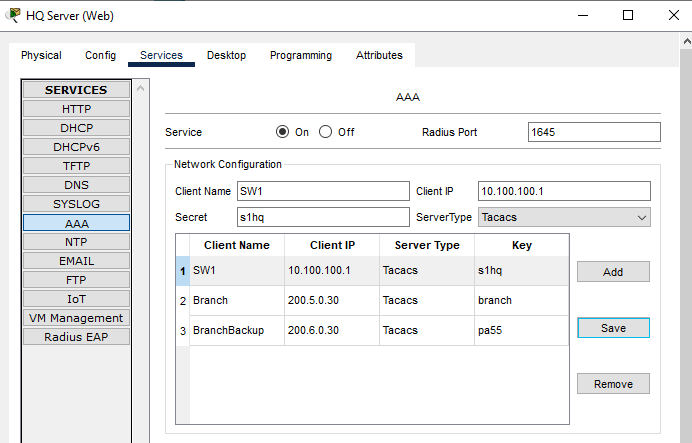
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device Name | Interface | IP Address | Subnet Mask | Default Gateway | VLAN |
| HQ Office (Main Router) | G0/0/0.1 | 10.5.0.1 | /24 | N/A | 10 |
| G0/0/0.2 | 10.5.1.1 | /24 | N/A | 20 |
| G0/0/0.100 | 10.100.100.100 | /24 | N/A | 100 |
| G0/0/1 | 200.5.0.14 | /28 | N/A | N/A |
| HQ Office (Backup Router) | G0/0/0.1 | 10.5.0.3 | /24 | N/A | 10 |
| G0/0/0.2 | 10.5.1.3 | /24 | N/A | 20 |
| G0/0/0.100 | 10.100.100.101 | /24 | N/A | 100 |
| S0/1/0 | 200.6.0.14 | /28 | N/A | N/A |
| Branch Office (Main Router) | G0/0/0.3 | 10.5.100.1 | /24 | N/A | 30 |
| G0/0/0.4 | 10.5.101.1 | /24 | N/A | 40 |
| G0/0/0.100 | 10.10.10.10 | /24 | N/A | 100 |
| G0/0/1 | 200.5.0.30 | /28 | N/A | N/A |
| Branch Office (Backup Router) | G0/0/0.3 | 10.5.100.2 | /24 | N/A | 30 |
| G0/0/0.4 | 10.5.101.2 | /24 | N/A | 40 |
| G0/0/0.100 | 10.10.10.11 | /24 | N/A | 100 |
| S0/1/0 | 200.6.0.30 | /28 | N/A | N/A |
| ISP Router | G0/0/0 | 200.5.1.1 | /24 | N/A | N/A |
| G0/0/1 | 200.5.0.1 | /28 | N/A | N/A |
| G0/0/2 | 200.5.0.17 | /28 | N/A | N/A |
| S0/1/0 | 200.6.0.17 | /28 | N/A | N/A |
| S0/1/1 | 200.6.0.1 | /28 | N/A | N/A |
| HQ AAA Server  (Internal) | Fa0 | 10.100.100.21 | /24 | 10.100.100.254 | 100 |
| HQ Web Server  (AAA for Branch Routers) | Fa0 | 10.5.0.2  (200.5.2.1) | /24 | 10.5.0.254 | 10 |
| Branch Server | Fa0 | 10.5.100.2  (200.5.2.2) | /24 | 10.5.100.254 | 30 |
| Internet Server (Good) | Fa0 | 200.5.1.21 | /24 | 200.5.1.1 | N/A |
| Internet Server (Bad) | Fa0 | 200.5.1.30 | /24 | 200.5.1.1 | N/A |
| S1 (HQ) | SVI | 10.100.100.1 | /24 | 10.100.100.254 | 100 |
| S2 (HQ) | SVI | 10.100.100.2 | /24 | 10.100.100.254 | 100 |
| S3 (HQ) | SVI | 10.100.100.3 | /24 | 10.100.100.254 | 100 |
| SW Branch | SVI | 10.10.10.1 | /24 | 10.10.10.254 | 100 |
| HQ PC | Fa0 | DHCP | /24 | 10.5.1.254 | 20 |
| Branch PC | Fa0 | DHCP | /24 | 10.5.100.254 | 40 |
| Internet PC | Fa0 | 200.5.1.4 | /24 | 200.5.1.1 | N/A |

**Credentials**

*AAA Server (Internal):*



*AAA Server (Branch Routers and SW1 (HQ)):*

**

*IP Address Table w/ Zones*

|  |  |  |
| --- | --- | --- |
| **Zone** | **Network** | **VLAN** |
| HQ Office (Server) | 10.5.0.0/24 | 10 |
| HQ Office (User) | 10.5.1.0/24 | 20 |
| Branch Office (Server) | 10.5.100.0/24 | 30 |
| Branch Office (User) | 10.5.101.0/24 | 40 |
| Internet | 200.5.1.0/24 | N/A |
| ISP - HQ (Main) | 200.5.0.0/28 | N/A |
| ISP - HQ (Backup) | 200.6.0.0/28 | N/A |
| ISP - Branch (Main) | 200.5.0.16/28 | N/A |
| ISP - Branch (Backup) | 200.6.0.16/28 | N/A |
| Switches (HQ) | 10.100.100.0/24 | 100 |
| Switch (Branch) | 10.10.10.0/24 | 100 |

*Local Credentials:*

*S1, S2, S3:*

Username Sxhq (x = switch number)

Password: admin

*Branch Switch:*

Username: SBack

Password: admin

Switch Enable Password: pw123

*HQ Router*

Username: hqrouter

Password: admin

*HQ Backup Router*

Username: Backup

Password: admin

*Branch Router*

Username: Branch

Password: admin

*Branch Backup Router*

Username: BBack

Password: admin

**Milestone 1**

The features were done by the following members:

* Olfsen
  + PAT, DHCP
* Mark
  + VTP, Trunking (Milestone 1)
* Jiun Jie
  + OSPF, Inter-VLAN routing (Milestone 1)

PAT Configurations (HQ Router):



G0/0/1: ip nat outside

Subinterfaces of G0/0/0: ip nat inside

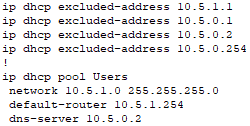
PAT Configurations (Branch Router):



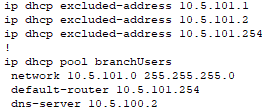
G0/0/1: ip nat outside

Subinterfaces of G0/0/0: ip nat inside

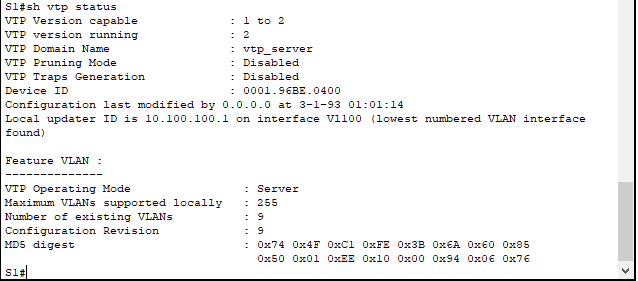
DHCP Configurations (HQ Router):

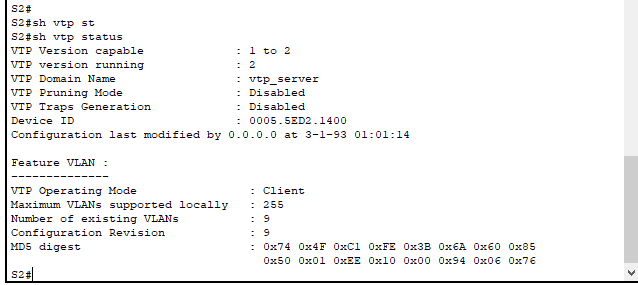


DHCP Configurations (Branch Router):

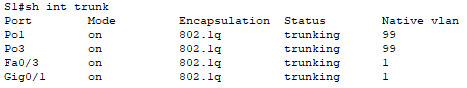


VTP Configurations (HQ):





Trunking Configuration (S1)



Trunking Configuration (S2, S3)

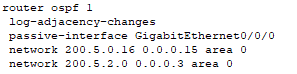


Command: switchport mode trunk

OSPF Configuration (HQ Router)



OSPF Configuration (Branch Router)



**Milestone 2**

For Milestone 2, the features were done by the following members:

* Olfsen
  + IPS, VPN, Firewall/ACL
  + HSRP w/ Tracking (Extra Feature)
* Mark
  + Layer 2 Security, AAA
  + FTP, EtherChannel (Extra Feature)
* Jiun Jie
  + NTP, SSH
  + OSPF Type 2 Authentication (Extra Feature)

***IPS (Intrusion Prevention System)***

IPS has been introduced to company perimeter routers to complement basic ACL functions of permitting or denying traffic. What makes IPS useful is its ability to detect signatures, or structures of traffic that could be deemed as harmful.

In this assignment, IPS has been implemented to detect ICMP traffic bound for the HQ Web Server specifically. This is done to prevent the possible scenario of information gathering by a malicious actor. Unfortunately, the full list of signatures couldn’t be obtained freely, and as a result, ICMP was selected for the demonstration of the feature.

***IPS Configuration (Commands)***

*# mkdir [ips directory name]*

*(config)# ip ips config location flash:[ips directory name]*

*(config)# ip ips name [ips name] list [ACL number]* (defining traffic to be subjected to IPS)

*(config)# ip ips notify log* (sends information to a syslog server)

*(config)# ip ips signature-category*

*(config-ips-category)# category all*

*(config-ips-category-action)# retired true*

*(config-ips-category-action)# exit*

*(config-ips-category)# category ios\_ips basic*

*(config-ips-category-action)# retired false*

*(config-ips-category-action)# exit*

*(config-ips-category)# exit*

*(config)# interface g0/1*

*(config-if)# ip ips [ips name] in* (checks inbound traffic for the internal network)

*(config)# ip ips signature-definition*

*(config-sigdef)# signature 2004 0*

*(config-sigdef-sig)# status*

*(config-sigdef-sig-status)# retired false*

*(config-sigdef-sig-status)# enabled true*

*(config-sigdef-sig-status)# exit*

*(config-sigdef-sig)# engine*

*(config-sigdef-sig-engine)# event-action produce-alert*

*(config-sigdef-sig-engine)# event-action deny-packet-inline*

*(config-sigdef-sig-engine)# exit*

*(config-sigdef-sig)# exit*

*(config-sigdef)# exit*

*IPS Parameters*

* IPS Name
  + iosips
* IPS Directory
  + ipsdir
* ACL Used
  + 101

***VPN (Virtual Private Network)***

A VPN was made to promote security between two sites. This being HQ and Branch networks, through the ISP who doesn’t know about the traffic that’s going through it.

***VPN Configuration (Commands)***

* Phase 1
  + (config)# *crypto isakmp policy 10*
    - *encryption aes 256*
    - *authentication pre-share*
    - *group 5*
  + (config)# crypto isakmp key [key password] address [peer address]
* Phase 2
  + (config)# crypto ipsec transform-set [set name] esp-aes esp-sha-hmac
  + (config)# crypto map vpnmap 10 ipsec-isakmp
    - set peer [peer address]
    - set transform-set [set name]
    - match address [ACL number] (Interesting traffic to be subjected to VPN encapsulation)
* Implementation
  + Main Routers’ G0/0/1, Backup Routers’ S0/1/0
    - crypto map vpnmap

***VPN Parameters:***

*Key Password: sitevpn*

*HQ Router’s (Main) Peer Address: 200.5.0.30*

*HQ Router’s (Backup) Peer Address: 200.6.0.30*

*Branch Router’s (Main) Peer Address: 200.5.0.14*

*Branch Router’s (Backup) Peer Address: 200.6.0.14*

*VPN Set: vpn-set*

*VPN Map: vpnmap*

**Firewall/ACL (Access Control List)**

ACLs are implemented as a means of filter addresses, whether to permit or deny based on conditions. In this assignment, there is a known malicious server in the Internet network. As a result, it will be denied from having any interaction with devices behind the company’s routers. Also, to promote good security practice, HTTPS (port 443) has been allowed, while its unencrypted version, HTTP (port 80), is denied.

It is also used for VPN to identify interesting traffic that should be encapsulated and sent over from one site to another. Just like VPN, PAT also uses ACLs to identify traffic and specific protocols that should be translated before exiting the network.

Lastly, it is also applied for IPS to inspect the specified traffic for possible malicious structures based on known signatures.

***Firewall/ACL Configuration (Commands)***

HQ Router (incl. Backup):

Extended IP access list 100 (PAT)

10 permit icmp 10.5.1.0 0.0.0.255 200.5.1.0 0.0.0.255

20 permit ip 10.5.1.0 0.0.0.255 200.5.1.0 0.0.0.255

30 permit ip 10.5.1.0 0.0.0.255 host 200.5.2.2

40 permit tcp 10.5.1.0 0.0.0.255 host 200.6.0.30 eq 22

Extended IP access list 110 (VPN)

10 permit ip 10.5.0.0 0.0.255.255 10.5.0.0 0.0.255.255

20 permit ip 10.100.100.0 0.0.0.255 10.10.10.0 0.0.0.255

30 permit ip 10.100.100.0 0.0.0.255 10.5.101.0 0.0.0.255

40 permit ip 10.5.1.0 0.0.0.255 10.10.10.0 0.0.0.255

Extended IP access list 120 (Internet)

10 deny ip host 200.5.1.30 any

20 permit tcp host 200.5.2.2 any eq 443 established

30 permit tcp host 200.5.1.21 any eq 443 established

32 deny tcp host 200.5.2.2 any eq www established

33 deny tcp host 200.5.1.21 any eq www established

40 deny tcp host 200.5.1.21 eq www any

50 permit ip any any

Extended IP access list 101 (IPS)

10 permit ip host 200.5.1.30 host 200.5.2.1 (permit IPS inspection)

Branch Router (incl. Backup)

Extended IP access list 100 (PAT)

10 permit ip 10.5.101.0 0.0.0.255 200.5.1.0 0.0.0.255

20 permit ip 10.5.101.0 0.0.0.255 host 200.5.2.1

30 permit tcp 10.5.101.0 0.0.0.255 host 200.6.0.14 eq 22

Extended IP access list 110 (VPN)

10 permit ip 10.5.0.0 0.0.255.255 10.5.0.0 0.0.255.255

20 permit ip 10.10.10.0 0.0.0.255 10.100.100.0 0.0.0.255

30 permit ip 10.5.0.0 0.0.255.255 10.100.100.0 0.0.0.255

40 permit ip 10.10.10.0 0.0.0.255 10.5.0.0 0.0.255.255

Extended IP access list 120 (Internet)

10 deny ip host 200.5.1.30 any

20 permit tcp host 200.5.2.2 any eq 443 established

30 permit tcp host 200.5.1.21 any eq 443 established

32 deny tcp host 200.5.2.2 any eq www established

33 deny tcp host 200.5.1.21 any eq www established

40 deny tcp host 200.5.1.21 eq www any

50 deny udp 200.5.1.0 0.0.0.255 host 200.5.2.2 eq domain

60 permit ip any any

Extended IP access list 101 (IPS)

10 permit ip host 200.5.1.30 host 200.5.2.2

***HSRP (Hot Standby Routing Protocol) w/ Tracking (Extra Feature)***

HSRP has been implemented as part of redundancy in the network in the event connection to the main router on either side of the network fails. On top of that, tracking is also implemented on connections going to the router. HSRP alone does not maintain redundancy and availability for that scenario, but with tracking, it can be maintained.

***HSRP /w Tracking Configurations (Commands)***

HQ Router (incl. Backup\*\*\*)

G0/0/0.2

standby version 2

standby 20 ip 10.5.1.254 (VLAN 20, Users)

standby 20 priority 105

standby 20 preempt

standby 20 track GigabitEthernet0/0/1

G0/0/0.100

standby version 2

standby 100 ip 10.100.100.254 (VLAN 100, Switch SVIs)

standby 100 priority 105

standby 100 preempt

standby 100 track GigabitEthernet0/0/1

Branch Router (incl. Backup\*\*\*)

G0/0/0.4

standby version 2

standby 40 ip 10.5.101.254

standby 40 priority 105

standby 40 preempt

standby 40 track GigabitEthernet0/0/1

G0/0/0.100

standby version 2

standby 100 ip 10.10.10.254

standby 100 priority 105

standby 100 preempt

standby 100 track GigabitEthernet0/0/1

\*\*\*Backup Routers did not have priority or preempt configured\*\*\*

***HSRP Parameters***

|  |  |  |  |
| --- | --- | --- | --- |
| **Router** | **Standby ID** | **VLAN** | **Virtual Default Gateway** |
| HQ Main | 20 | 20 | 10.5.1.254 |
| HQ Backup | 100 | 100 | 10.100.100.254 |
| Branch Main | 40 | 40 | 10.5.101.254 |
| Branch Backup | 100 | 100 | 10.10.10.254 |

***Layer 2 security***

*Port Security:*

Port security sets a limit on MAC addresses learned to prevent a malicious attacker from plugging in or even posing as their target system. It can also set actions onto what is done in such a situation.

*Port Security (S1, S2, S3, SWBranch) (Commands):*

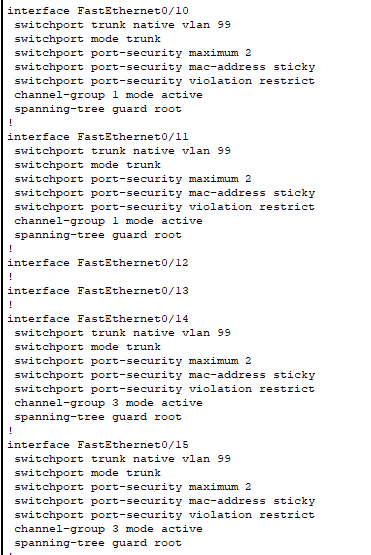
switchport port-security maximum 2

switchport port-security mac-address sticky

switchport port-security violation restrict

*STP Security (Root Guard)*

To prevent manipulation of STP, root guard is implemented to clearly define who is the root bridge. This is done in S1 on the HQ network by the ‘spanning-tree guard root’ on its respective interfaces



*Portfast & BPDU Guard*

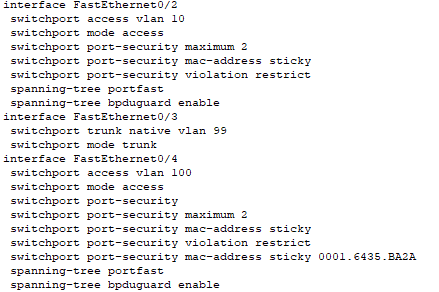
Portfast is done on access ports, therefore not utilizing STP. This typically is applied to end devices like PCs or servers. This helps to speed up connecting these devices to the network, skipping or shortening the default timers set.

BPDU Guard

This is implemented on ports that should not receive BPDUs, typically access ports.

*Portfast & BPDU Guard (Commands)*

*HQ (S3):*

**

*S2, and SWBranch are similarly configured*

*spanning-tree portfast*

*spanning-tree bpduguard enable*

***EtherChannel (Extra Feature)***

EtherChannels are great for not only providing redundancy by having a second connection between the two devices, but also effectively doubling the effective bandwidth with that second connection.

***EtherChannel Configuration (Commands)***

*HQ Switches (S1, S2, S3):*

*interface Port-channel1*

*switchport trunk native vlan 99*

*switchport mode trunk*

*interface Port-channel2*

*switchport trunk native vlan 99*

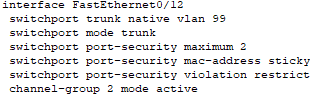
*switchport mode trunk*

*interface Port-channel3*

*switchport trunk native vlan 99*

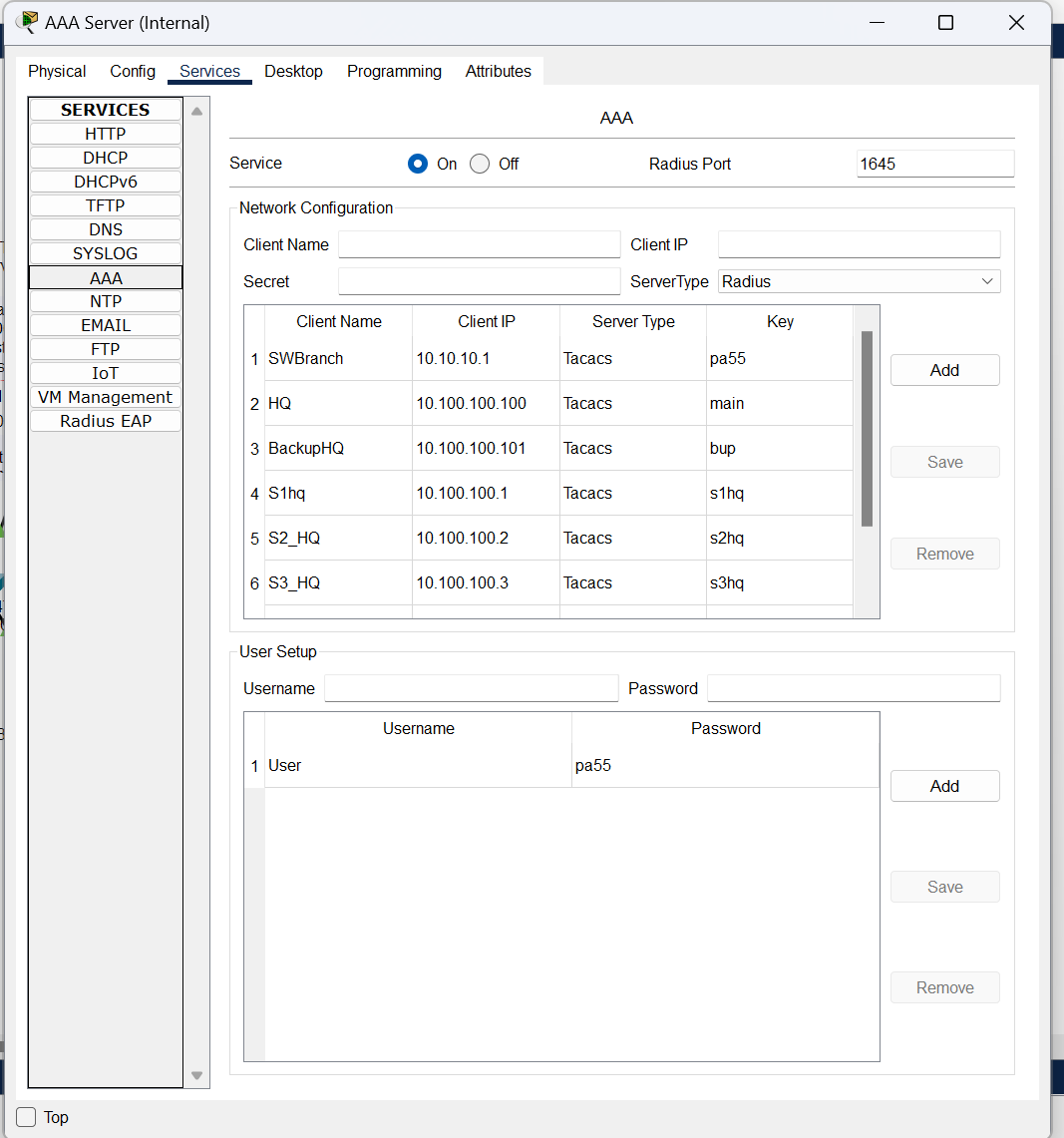
*switchport mode trunk*

These configurations are then applied to the respective interfaces using the ‘channel-group [number] mode active’ command

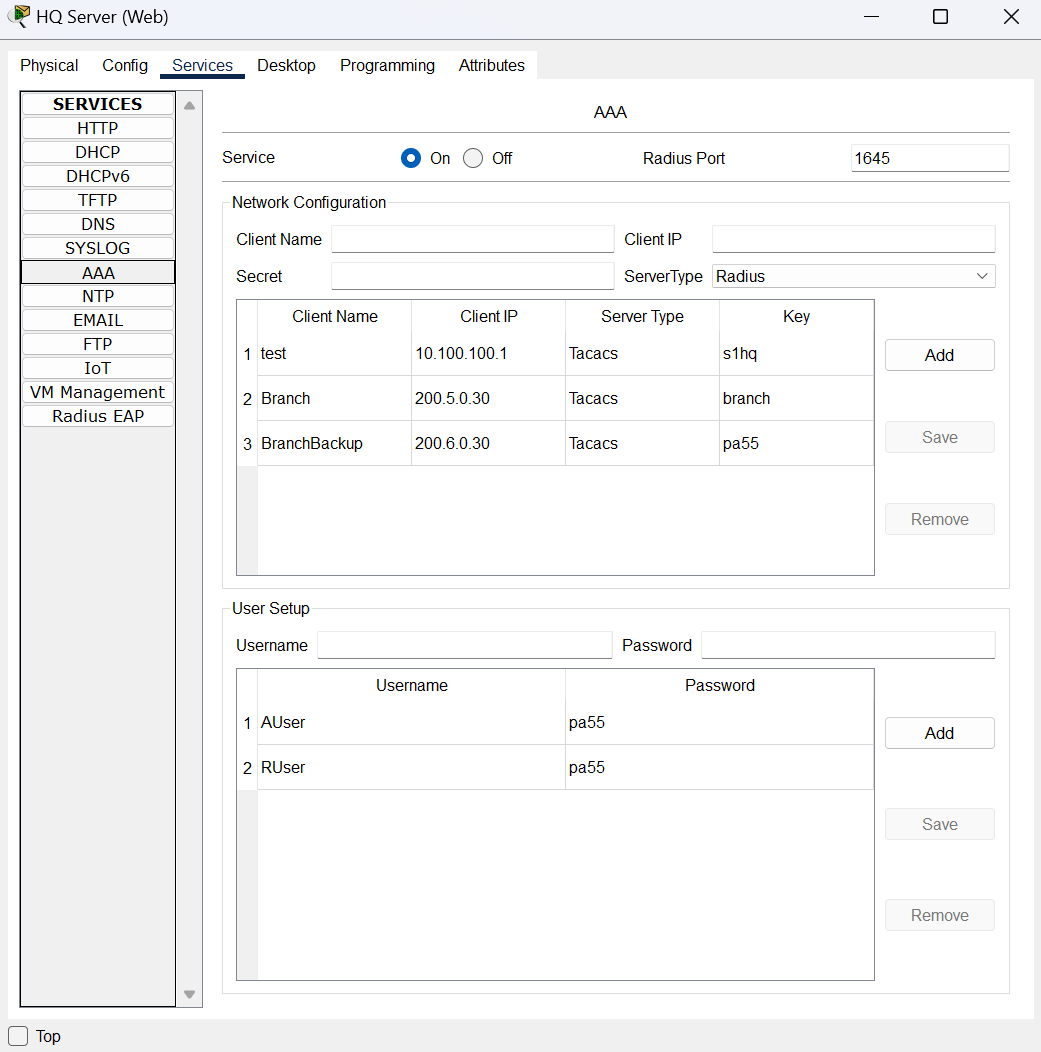
**

***AAA***

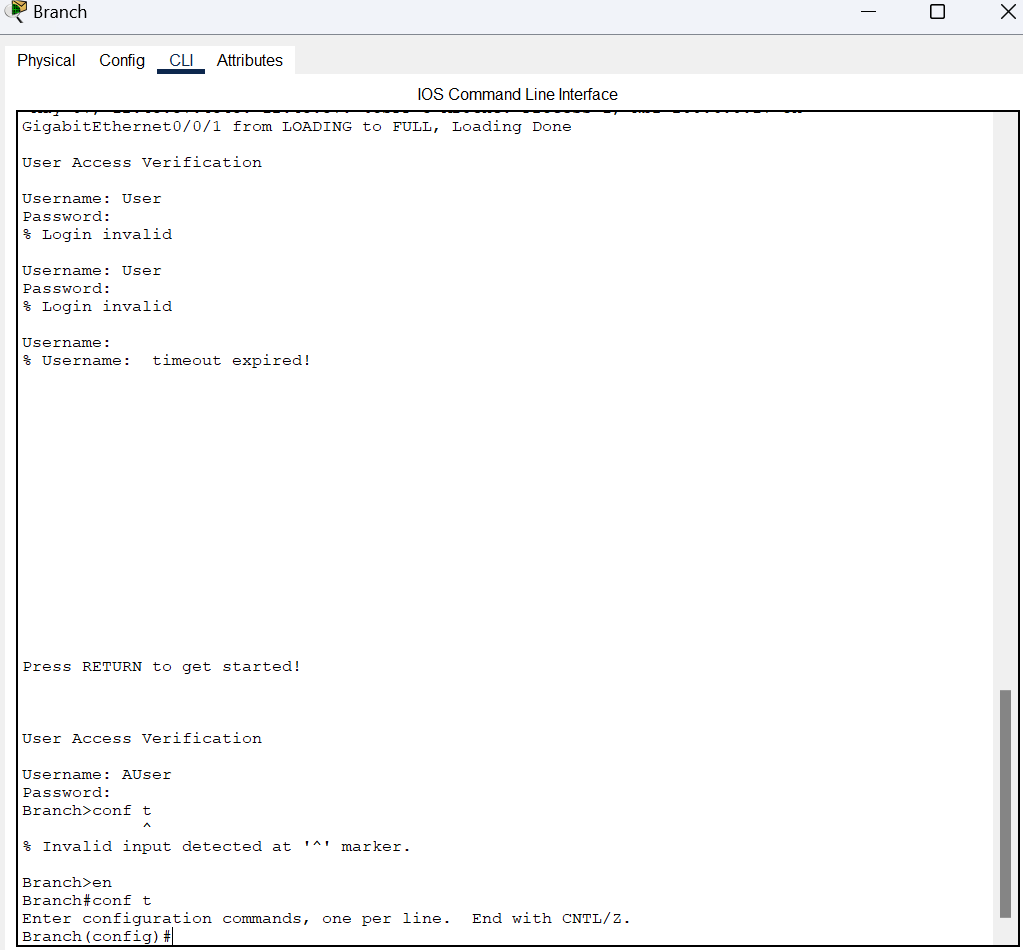
*For the screenshot below, a client from internal AAA Server will be logged in via username as “User” and password as “pa55”.*

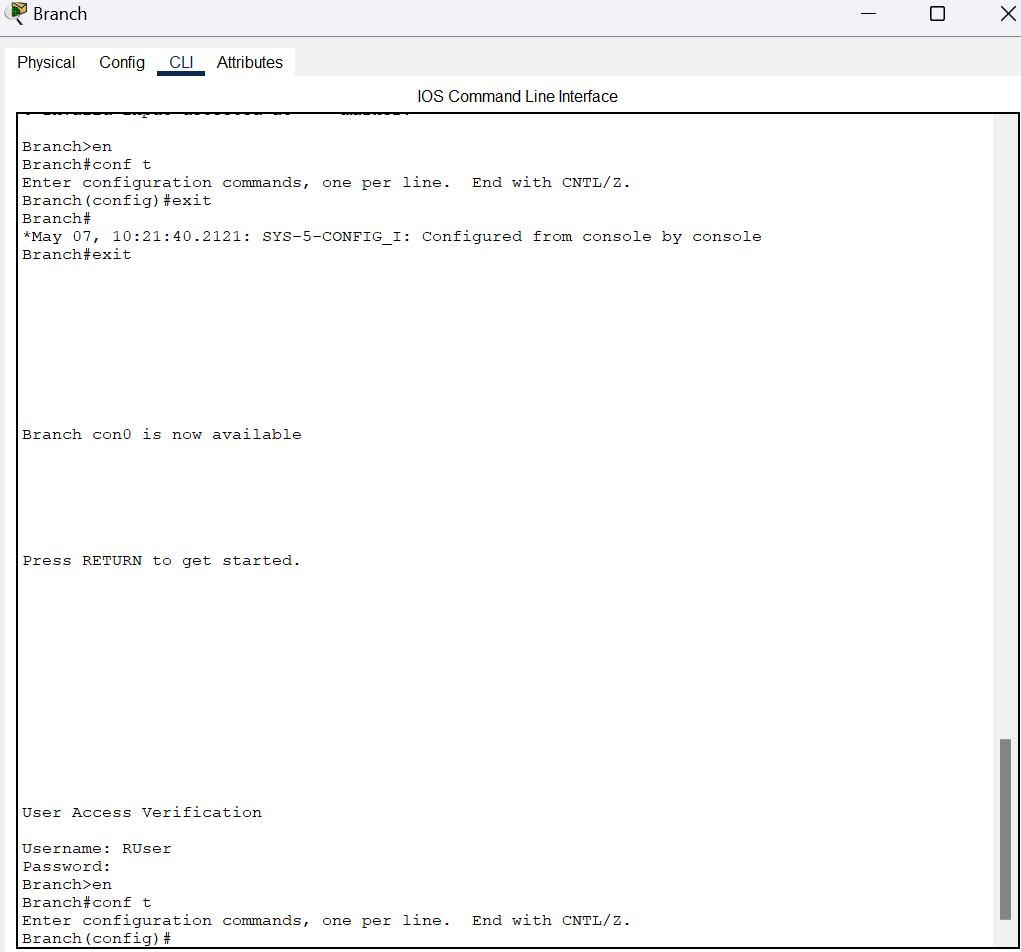
**

*For test, Branch and BranchBackup will be use “AUser” or “Ruser”, password will be “pa55”.*

**

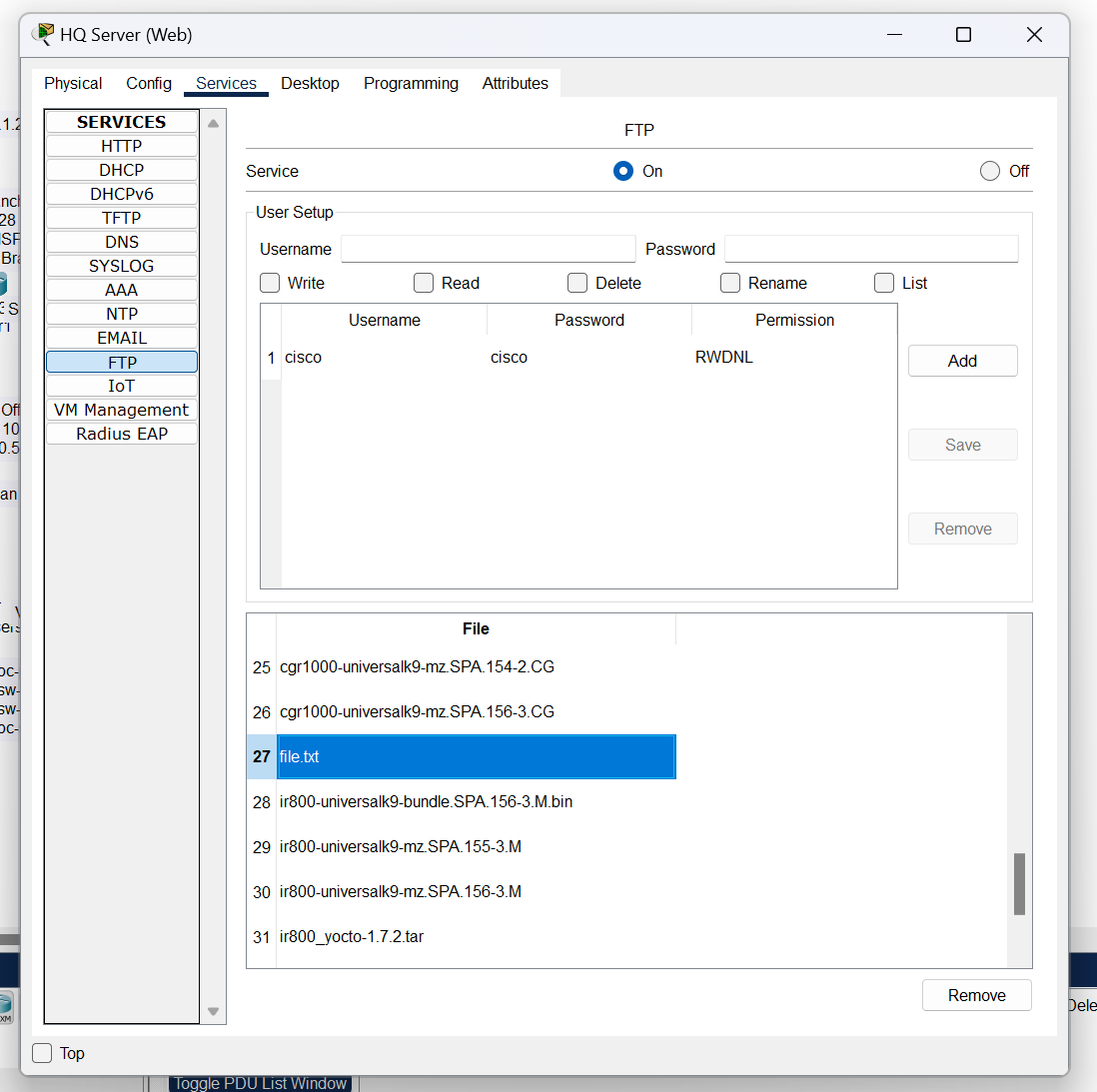
*This is the part that shows you can login to branch by using AUser and RUser.*

**

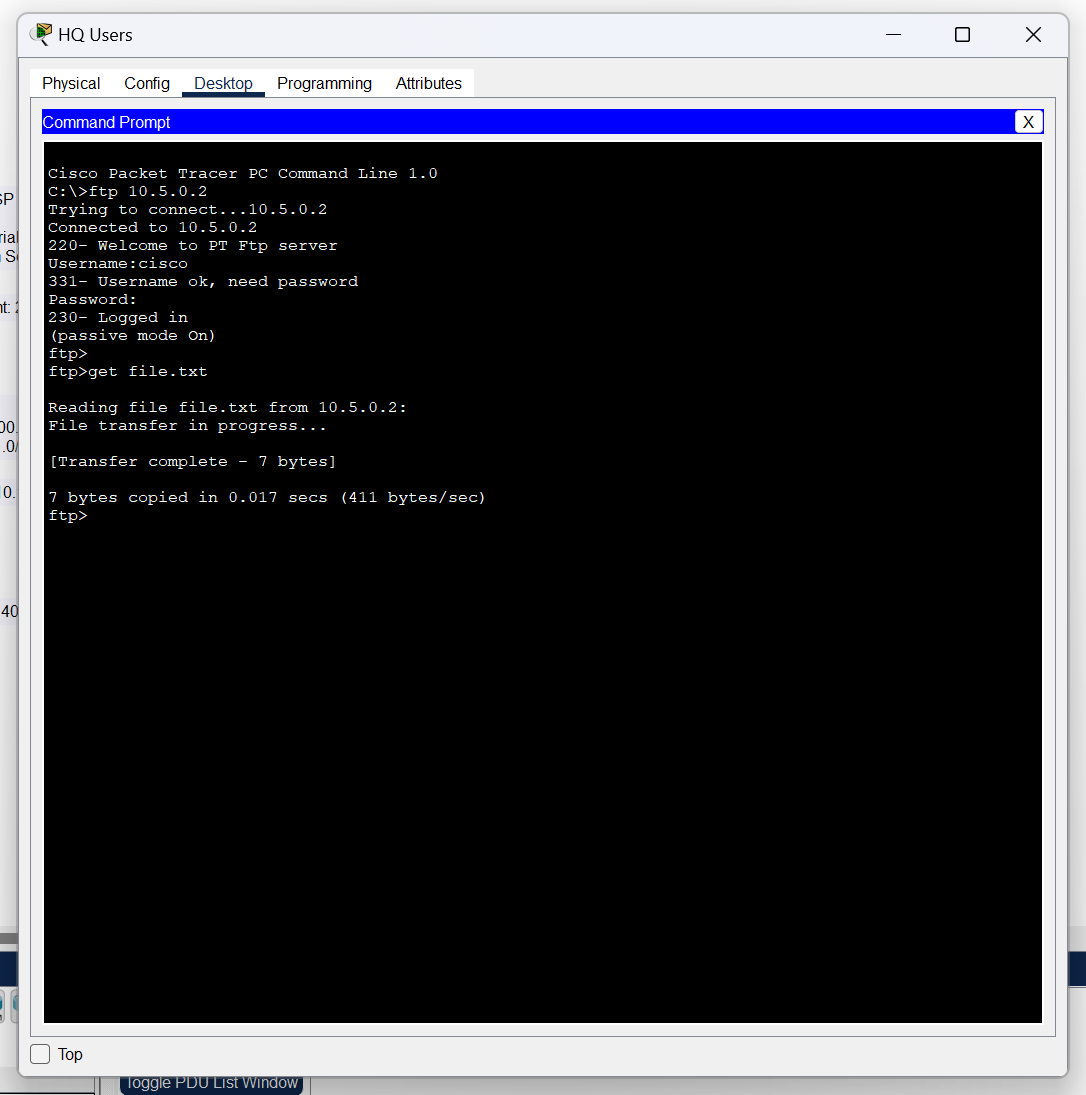
**

***FTP Configuration (Extra Feature)***

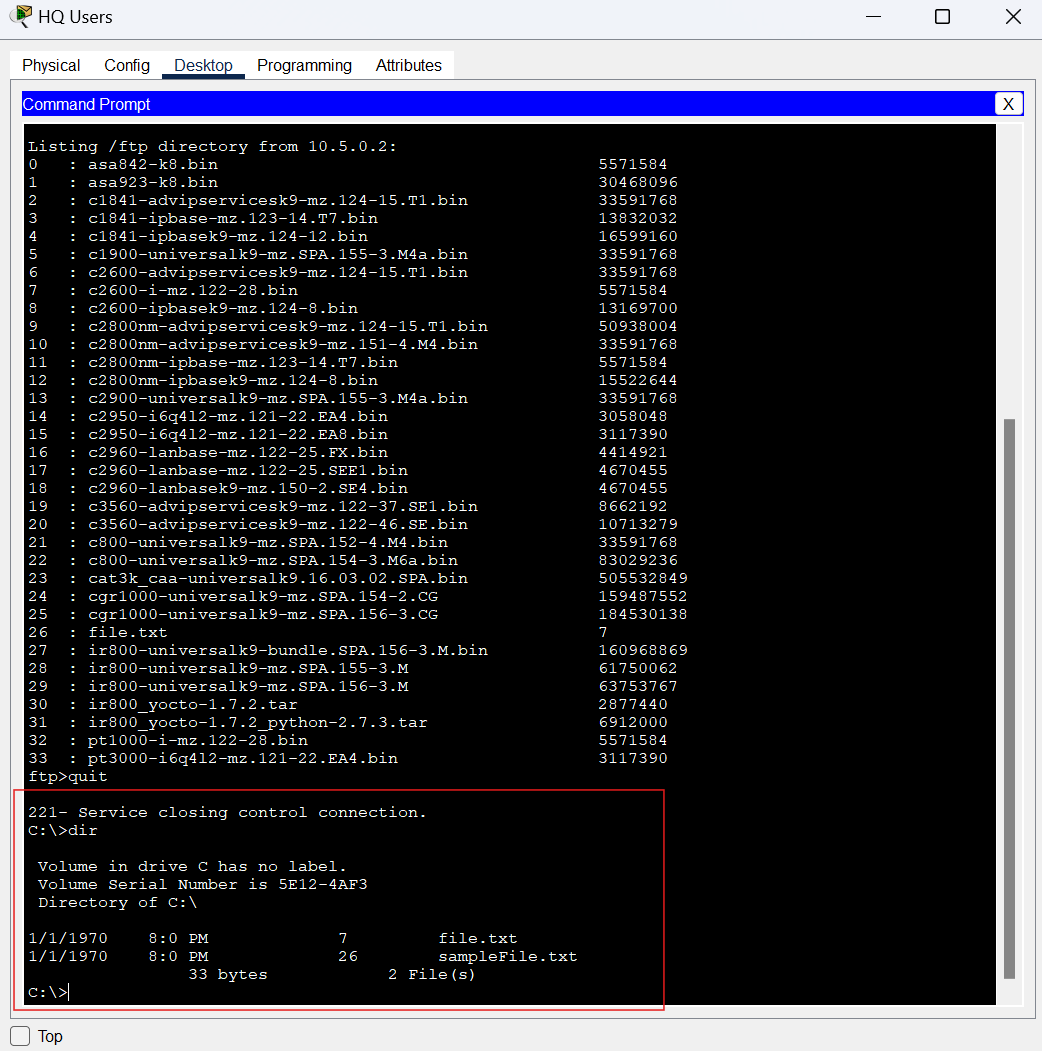
*I created a file called file.txt*

**

*From HQ Users PC login via FTP 10.5.0.2 to get the file.txt from FTP*

**

*As you can see, the HQ users PC got the file.txt*

**

***NTP Configuration (Command)***

*ntp authentication-key 1 md5 <key>*

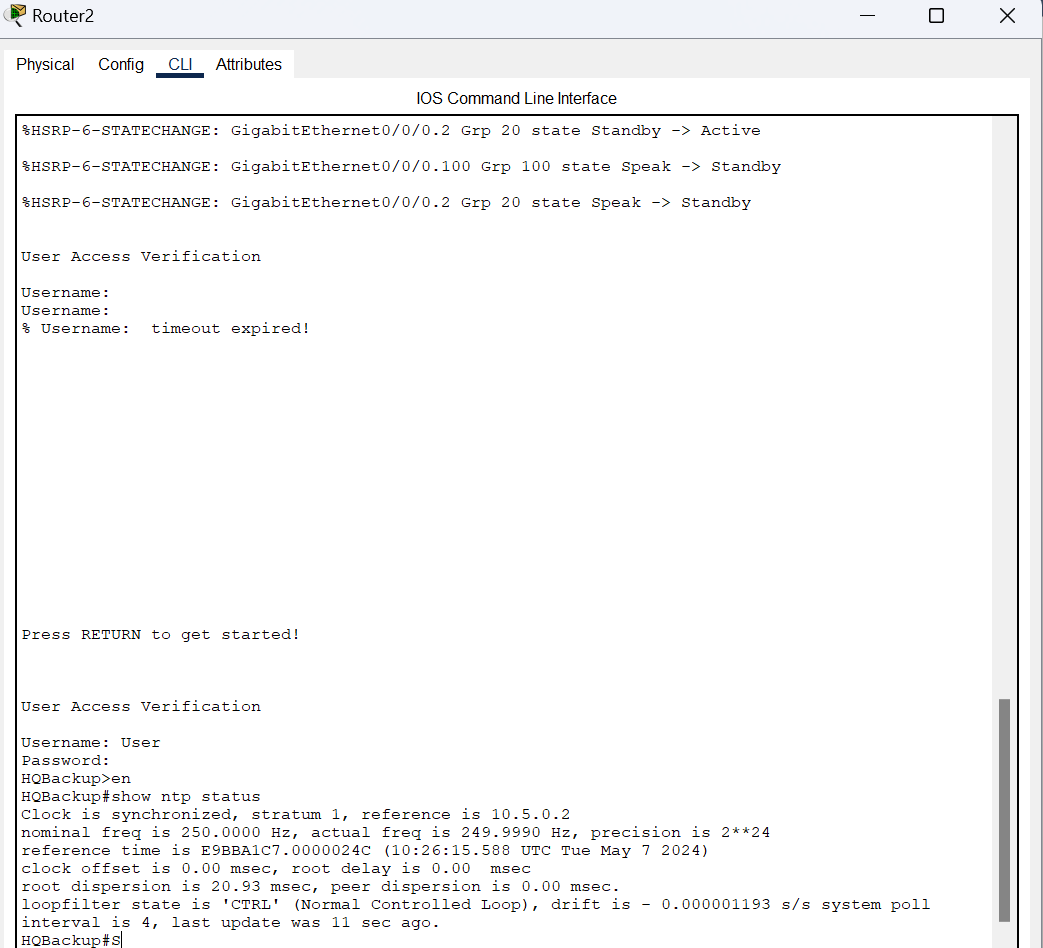
*ntp authenticate*

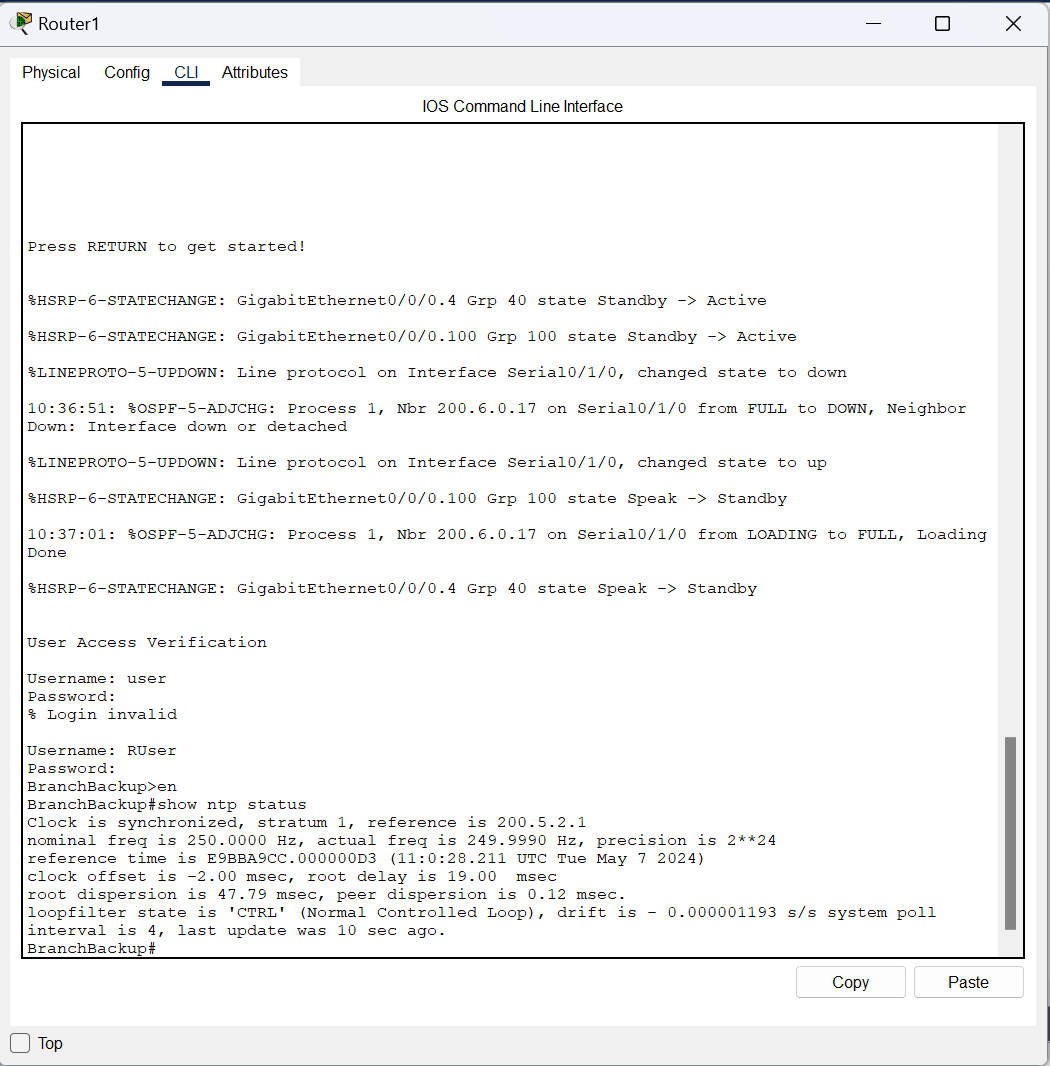
*ntp trusted-key 1*

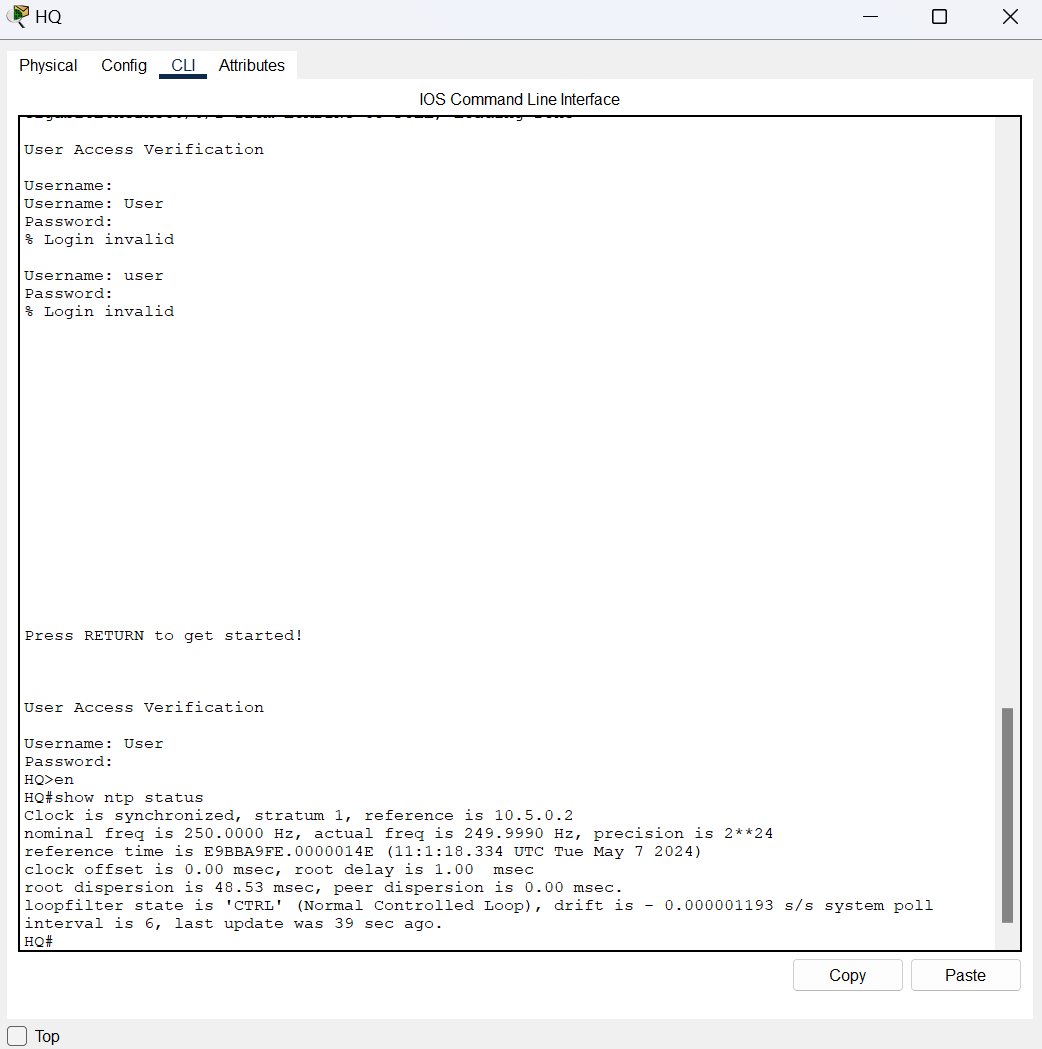
*ntp server 10.5.0.2*

*ntp update-calendar*

*As you can see, the clock is synchronized.*

******

******

******

***SSH Configuration (Command)***

***HQBackup Router***

*ip ssh version 2*

*ip domain-name HQBackup.com*

*username Backup secret admin*

*crypto key generate rsa*

*line vty 0 4*

*login authentication default*

*transport input ssh*

*line vty 5 15*

*login authentication default*

*transport input ssh*

***HQ Router***

*ip ssh version 2*

*ip domain-name HQrouter.com*

*username hqrouter secret admin*

*crypto key generate rsa*

*line vty 0 4*

*login authentication default*

*transport input ssh*

*line vty 5 15*

*login authentication default*

*transport input ssh*

***Branch Backup Router***

*ip ssh version 2*

*ip domain-name BBack.com*

*username BBack secret admin*

*crypto key generate rsa*

*line vty 0 4*

*login authentication default*

*transport input ssh*

*line vty 5 15*

*login authentication default*

*transport input ssh*

***Branch Router***

*ip ssh version 2*

*ip domain-name Branch .com*

*username Branch secret admin*

*crypto key generate rsa*

*line vty 0 4*

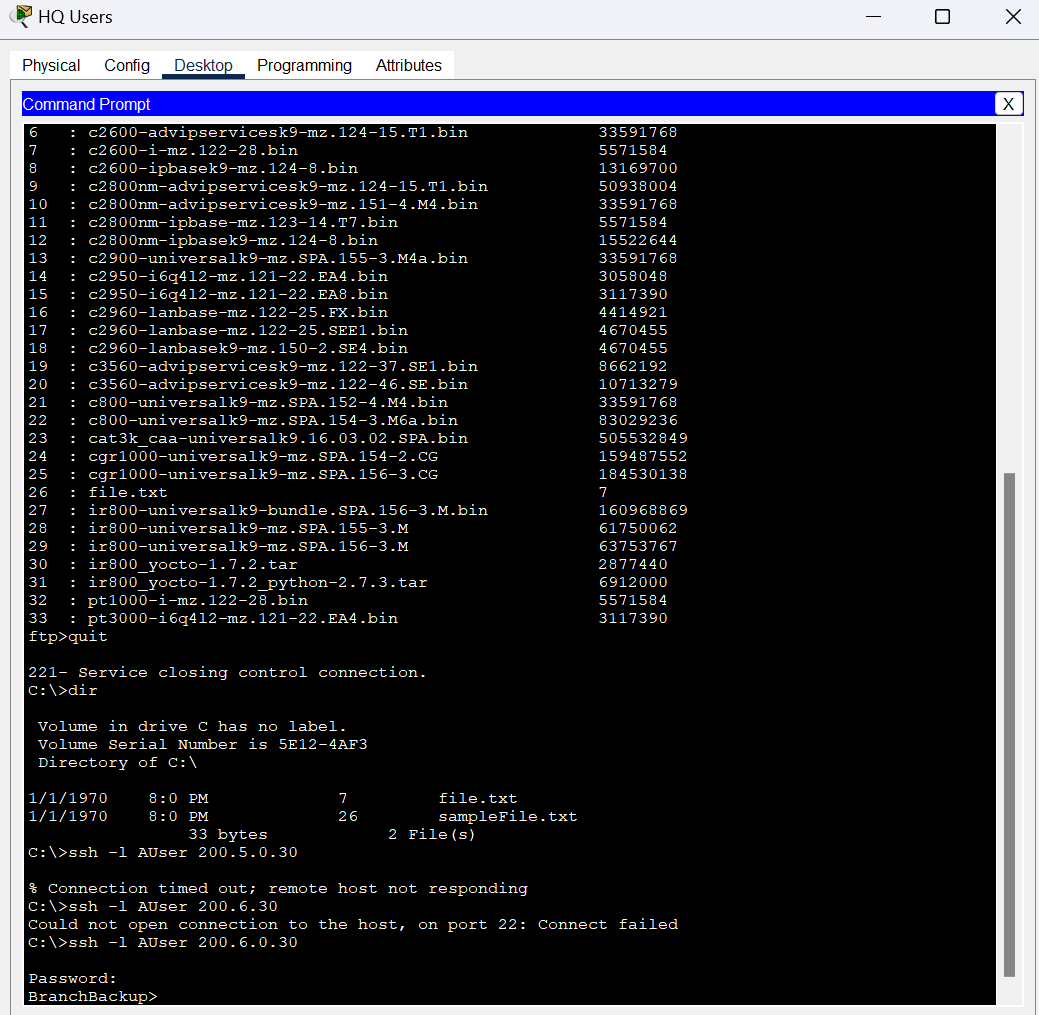
*login authentication default*

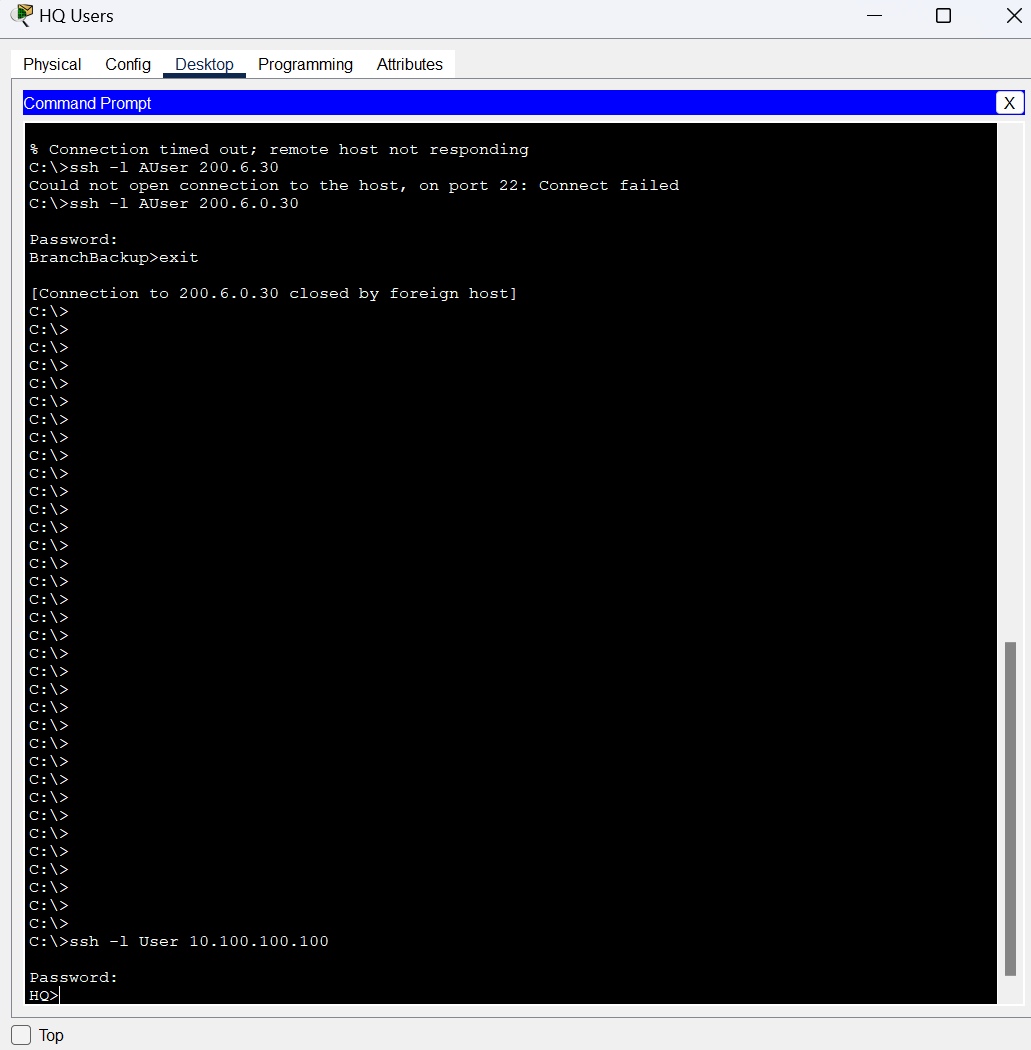
*transport input ssh*

*line vty 5 15*

*login authentication default*

*transport input ssh*

**

**

***OSPF Type 2 authentication Configuration (command)***

***Backup Router***

*interface s0/1/0*

*ip ospf authentication message-digest*

*ip ospf message-disgest-key 1 md5 pa55*

***Backup Router***

*interface G0/0/1*

*ip ospf authentication message-digest*

*ip ospf message-digest-key 1 md5 pa55*

***Branch Router***

*interface G0/0/1*

*ip ospf authentication message-digest*

*ip ospf message-digest-key 1 md5 pa55*

***Backup Branch Router***

*interface S0/1/0*

*ip ospf authentication message-digest*

*ip ospf message-digest-key 1 md5 pa55*