Network Security (CCF2C01)

Case Study Report Submission

Practical Class : P02

Submitted by: <1900353B > <Zachary Phoon Jun Ze>

Date: 20/11/2020

"By submitting this work, I am are declaring that I am the originator(s) of this work and that all other original sources used in this work has been appropriately acknowledged.

I understand that plagiarism is the act of taking and using the whole or any part of another person's work and presenting it as my/ our own without proper acknowledgement.

I also understand that plagiarism is an academic offence, and that disciplinary action will be taken for plagiarism."

NAME AND SIGNATURE OF STUDENT: ……………………………………

Temasek POLYTECHNIC

School of Informatics & IT
AY 2020/2021 Oct Semester (Level 2)
Diploma In Cybersecurity & Digital Forensics
Network Security (NWS)
[Subject Code – CCF2C01]

ASSIGNMENT REPORT

FOR

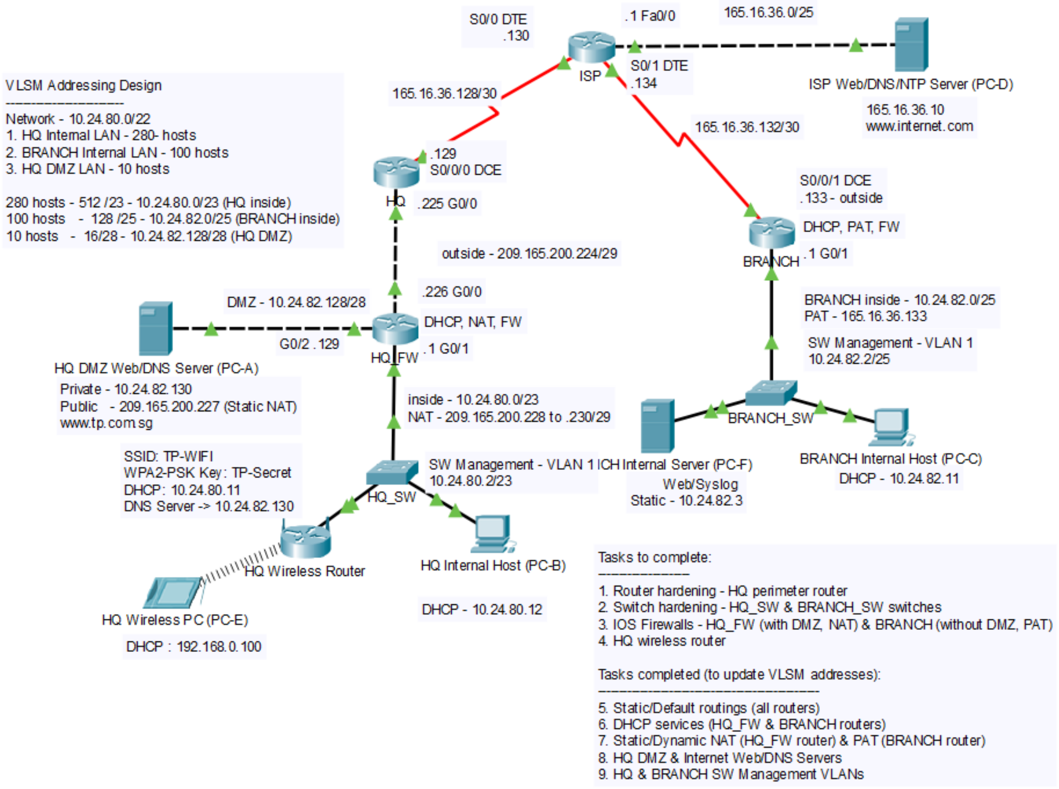
NETWORK SECURITY

(INDIVIDUAL)

Suggested Assignment Report Format / Contents:

Overall Note: Remember to include the **Answers** to the questions in the sections below corresponding to the respective sections as listed in the original NWS Assignment Requirements document!

1. Introduction



VLSM Addressing Design

Network - 10.24.80.0/22
1. HQ Internal LAN - 280- hosts
2. BRANCH Internal LAN - 100 hosts
3. HQ DMZ LAN - 10 hosts

280 hosts - 512 /23 - 10.24.80.0/23 (HQ inside)
100 hosts - 128 /25 - 10.24.82.0/25 (BRANCH inside)
10 hosts - 16/28 - 10.24.82.128/28 (HQ DMZ)

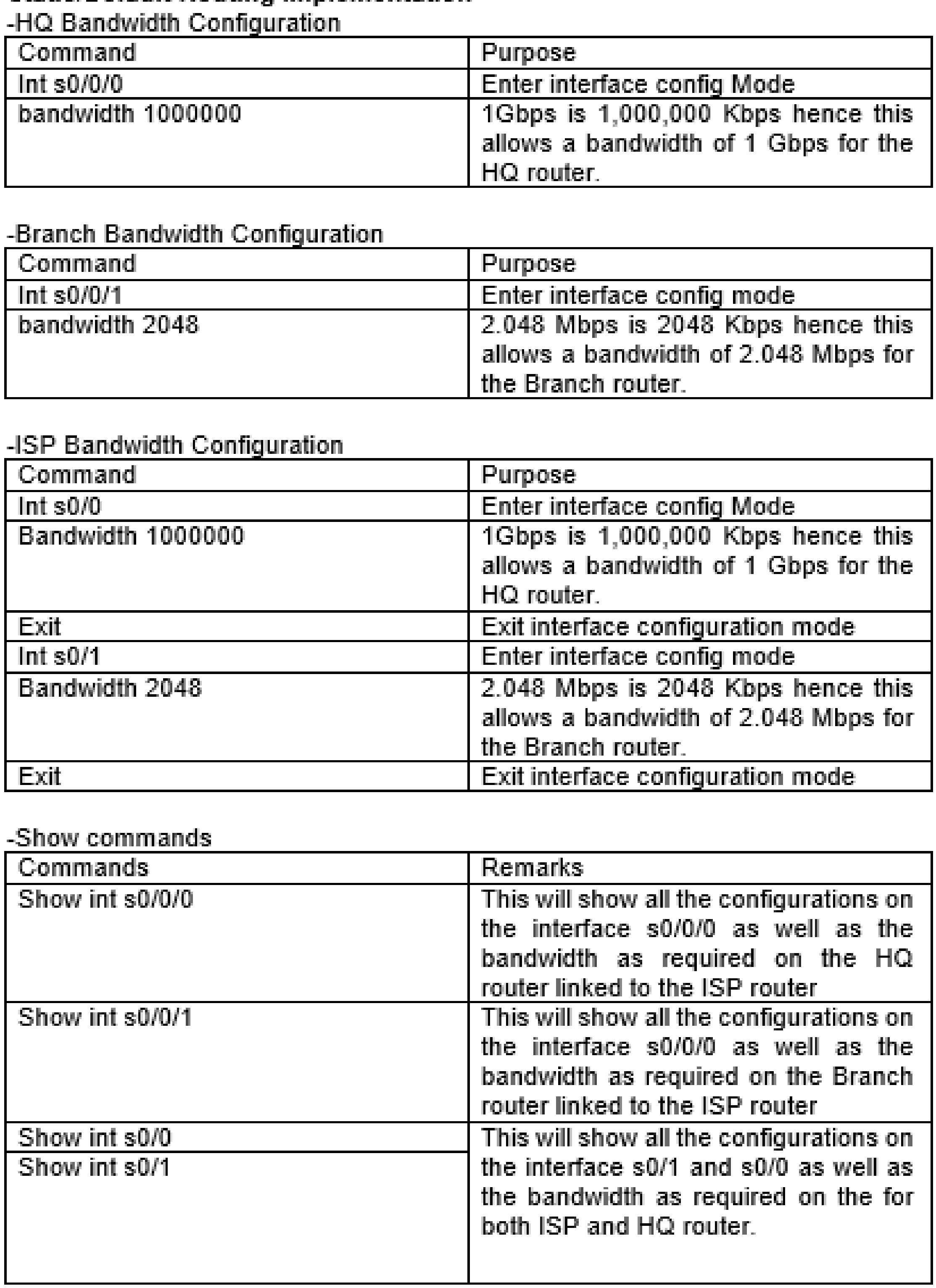
Tasks to complete:
----
1. Router hardening - HQ perimeter router
2. Switch hardening - HQ_SW & BRANCH_SW switches
3. IOS Firewalls - HQ_FW (with DMZ, NAT) & BRANCH (without DMZ, PAT)
4. HQ wireless router

Tasks completed (to update VLSM addresses):
----
5. Static/Default routings (all routers)
6. DHCP services (HQ_FW & BRANCH routers)
7. Static/Dynamic NAT (HQ_FW router) & PAT (BRANCH router)
8. HQ DMZ & Internet Web/DNS Servers
9. HQ & BRANCH SW Management VLANs

Brief description of assignment case study scenario

ALL Configuration COMMANDS START IN configuration Mode unless specified
All Show Commands are in Privileged EXEC mode.

2. Static/Default Routing Implementation



-HQ Bandwidth Configuration

Command	Purpose
Int s0/0/0	Enter interface config Mode
bandwidth 1000000	1Gbps is 1,000,000 Kbps hence this allows a bandwidth of 1 Gbps for the HQ router.

-Branch Bandwidth Configuration

Command	Purpose
Int s0/0/1	Enter interface config mode
bandwidth 2048	2.048 Mbps is 2048 Kbps hence this allows a bandwidth of 2.048 Mbps for the Branch router.

-ISP Bandwidth Configuration

Command	Purpose
Int s0/0	Enter interface config Mode
Bandwidth 1000000	1Gbps is 1,000,000 Kbps hence this allows a bandwidth of 1 Gbps for the HQ router.
Exit	Exit interface configuration mode
Int s0/1	Enter interface config mode
Bandwidth 2048	2.048 Mbps is 2048 Kbps hence this allows a bandwidth of 2.048 Mbps for the Branch router.
Exit	Exit interface configuration mode

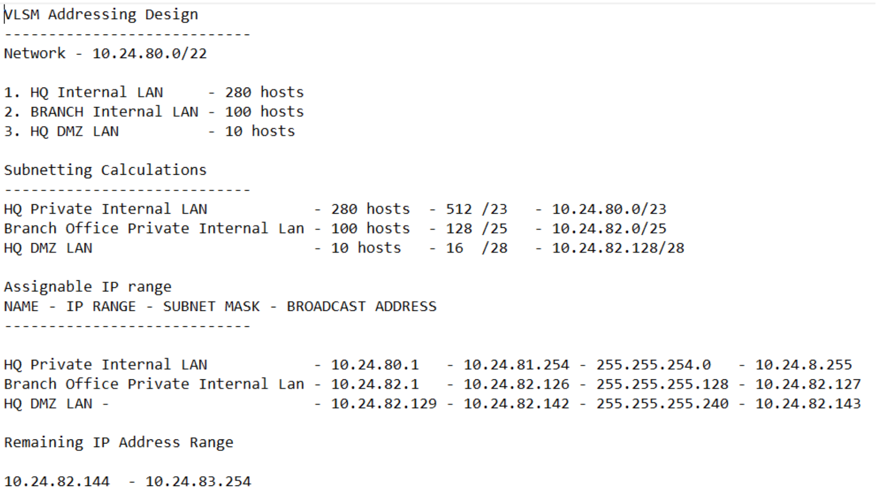
-Show commands

Commands	Remarks
Show int s0/0/0	This will show all the configurations on the interface s0/0/0 as well as the bandwidth as required on the HQ router linked to the ISP router
Show int s0/0/1	This will show all the configurations on the interface s0/0/0 as well as the bandwidth as required on the Branch router linked to the ISP router
Show int s0/0	This will show all the configurations on the interface s0/1 and s0/0 as well as the bandwidth as required on the for both ISP and HQ router.
Show int s0/1	

3. VLSM IP Addressing Design

LAN / WAN	Router / Firewall	Interface	Network Address	IP address
HQ external public LAN (outside)	HQ perimeter router	G 0/0	209.165.200.224/29	209.165.200.225/29
	HQ firewall router	G 0/0		209.165.200.226/29
HQ DMZ LAN (Sacrificial LAN) (DMZ)	HQ firewall router	G 0/2	10.24.82.128/28	10.24.82.129/28
	HQ DMZ Web/DNS server	Fa0 (NIC)		10.24.82.130/28
HQ internal private LAN (inside)	HQ firewall router	G 0/1	10.24.80.0/23	10.24.80.1/23
	HQ switch	Mgmt VLAN Interface VLAN1		10.24.80.2/23
HQ wireless LAN	HQ wireless router	HQ wireless LAN connections	192.168.0.0/24	Obtain via DHCP service from HQ wireless router (start from 192.168.1.100)
Branch internal private LAN (inside)	Branch perimter router	G 0/1	10.24.82.0/25	10.24.82.1/25
	Branch switch	Mgmt VLAN Interface VLAN1		10.24.82.2/25
	Branch internal Web.Syslog server	Fa0 (NIC)		10.24.82.3/25
Public WAN between HQ and ISP	HQ perimeter router	S 0/0/0 (DCE)	165.16.36.128/30	165.16.36.129/30
	ISP router	S 0/0/0 (DTE)		165.16.36.130/30
Public WAN between Branch and ISP	Branch perimeter router	S 0/0/1 (DCE)	165.16.36.132/30	165.16.36.133/30
	ISP router	S 0/0/1 (DTE)		165.16.36.134/30
ISP Router LAN	ISP router	Fa 0/0	165.16.36.0/25	165.16.36.1/25

Table 1: Interfaces used and IP addresses



```
VLSM Addressing Design
----------------------------
Network - 10.24.80.0/22

1. HQ Internal LAN     - 280 hosts
2. BRANCH Internal LAN - 100 hosts
3. HQ DMZ LAN          - 10 hosts

Subnetting Calculations
----------------------------
HQ Private Internal LAN            - 280 hosts  - 512 /23   - 10.24.80.0/23
Branch Office Private Internal Lan - 100 hosts  - 128 /25   - 10.24.82.0/25
HQ DMZ LAN                         - 10 hosts   - 16  /28   - 10.24.82.128/28

Assignable IP range
NAME - IP RANGE - SUBNET MASK - BROADCAST ADDRESS
----------------------------

HQ Private Internal LAN            - 10.24.80.1   - 10.24.81.254 - 255.255.254.0   - 10.24.8.255
Branch Office Private Internal Lan - 10.24.82.1   - 10.24.82.126 - 255.255.255.128 - 10.24.82.127
HQ DMZ LAN -                       - 10.24.82.129 - 10.24.82.142 - 255.255.255.240 - 10.24.82.143

Remaining IP Address Range

10.24.82.144  - 10.24.83.254
```

(Q: What is the disadvantage of this implementation, and how would you suggest to overcome it?)
Ans: External Attacker can guess the ip addresss used for the switches can attack those switches to and attempt to elevate access by hopping vlans.

(Q: Why do servers need static IP addresses?)
Ans: This ensures that all the revelvant data is transported back to the correct address. If the server does not have a static IP , the users data deos not have a definite location hence may cuase information to be leaked which is a bridge of confidentialty in the CIA triad.

4. DHCP, NAT/PAT and Wireless LAN Implementation

ALL Configuration COMMANDS START IN configuration Mode unless specified

All Show Commands are in Privileged EXEC mode.

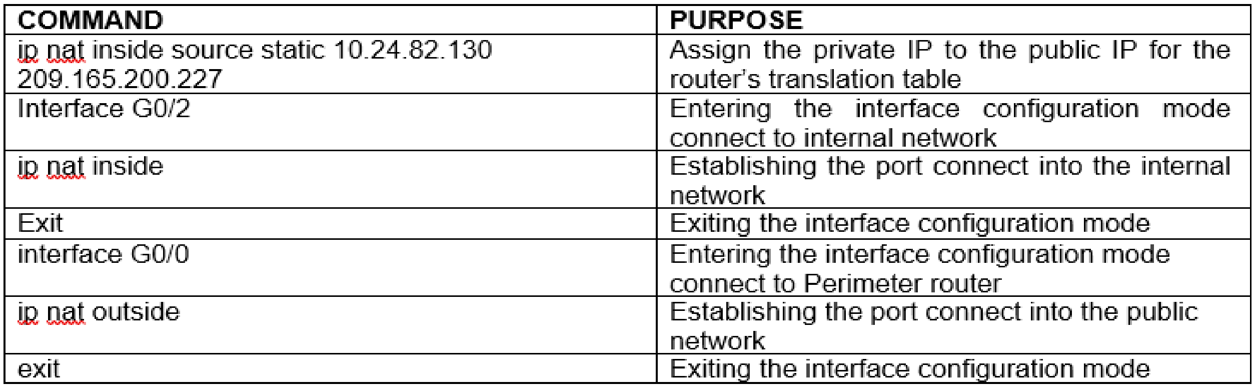
- **HQ FW router DHCP commands**:

COMMAND	PURPOSE
ip dhcp pool HQ_LAN	Establishing the DHCP and the name
network 10.24.80.0 255.255.254.0	Address range to give out
default-router 10.24.80.1	Setting the router which gives out the Ips
dns-server 10.24.82.130	Specifying the DNS for machines which receives the DHCP IP
exit	Exit the DHCP configuration mode
ip dhcp excluded-address 10.24.80.1 10.24.80.10	Excluding the first 10 IP

- **BRANCH router DHCP commands**:

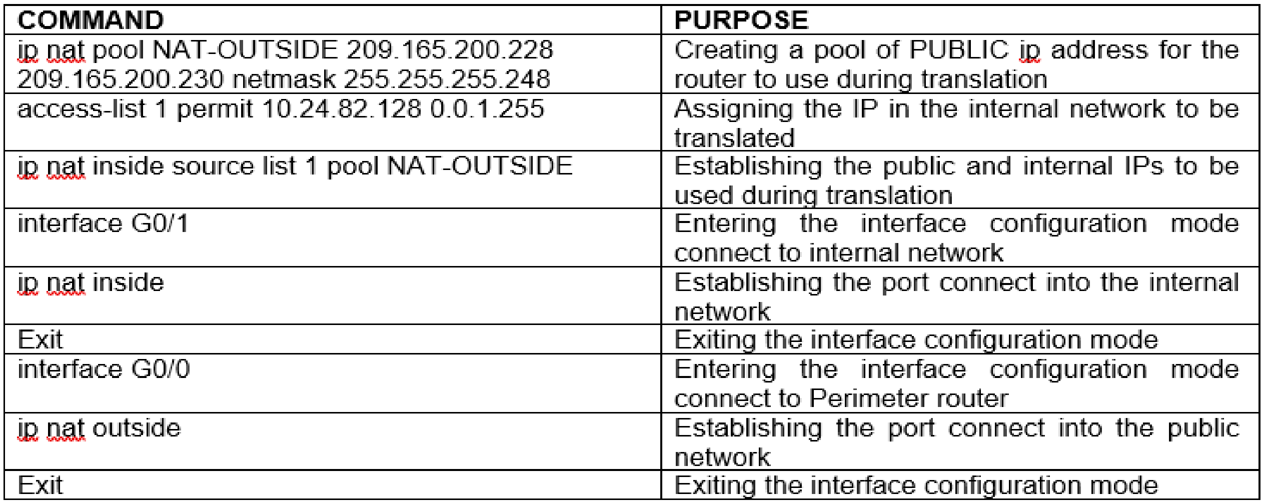
COMMAND	PURPOSE
ip dhcp pool BRANCH_DHCP	Establishing the DHCP and the name
network 10.24.82.0 255.255.255.128	Address range to give out
default-router 10.24.82.1	Setting the router which gives out the Ips
dns-server 165.16.36.10	Specifying the DNS for machines which receives the DHCP IP
exit	Exit the DHCP configuration mode
ip dhcp excluded-address 10.24.82.1 10.24.82.10	Excluding the first 10 IP

- **STATIC NAT commands AT HQ FW router:**



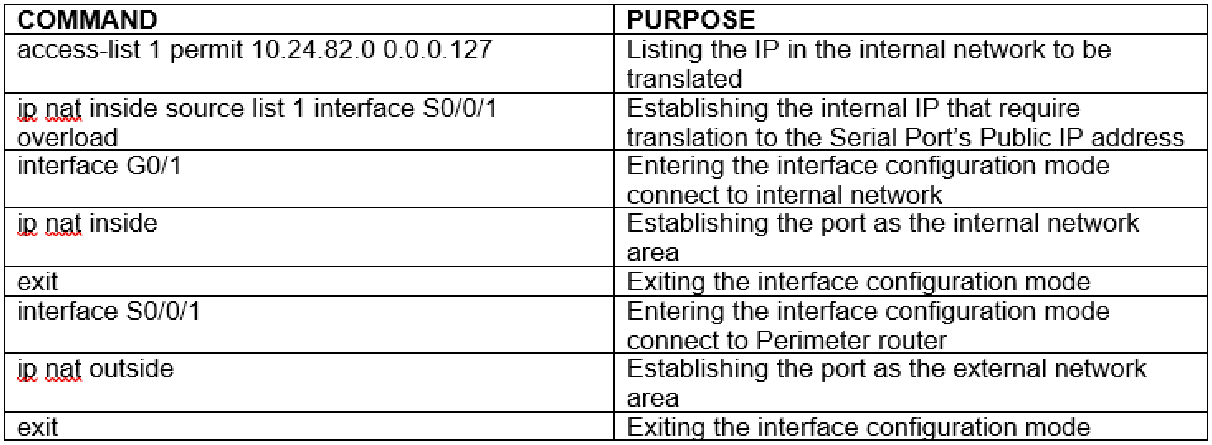
COMMAND	PURPOSE
ip nat inside source static 10.24.82.130 209.165.200.227	Assign the private IP to the public IP for the router's translation table
Interface G0/2	Entering the interface configuration mode connect to internal network
ip nat inside	Establishing the port connect into the internal network
Exit	Exiting the interface configuration mode
interface G0/0	Entering the interface configuration mode connect to Perimeter router
ip nat outside	Establishing the port connect into the public network
exit	Exiting the interface configuration mode

- **DYNAMIC NAT commands AT HW FW router:**



COMMAND	PURPOSE
ip nat pool NAT-OUTSIDE 209.165.200.228 209.165.200.230 netmask 255.255.255.248	Creating a pool of PUBLIC ip address for the router to use during translation
access-list 1 permit 10.24.82.128 0.0.1.255	Assigning the IP in the internal network to be translated
ip nat inside source list 1 pool NAT-OUTSIDE	Establishing the public and internal IPs to be used during translation
interface G0/1	Entering the interface configuration mode connect to internal network
ip nat inside	Establishing the port connect into the internal network
Exit	Exiting the interface configuration mode
interface G0/0	Entering the interface configuration mode connect to Perimeter router
ip nat outside	Establishing the port connect into the public network
Exit	Exiting the interface configuration mode

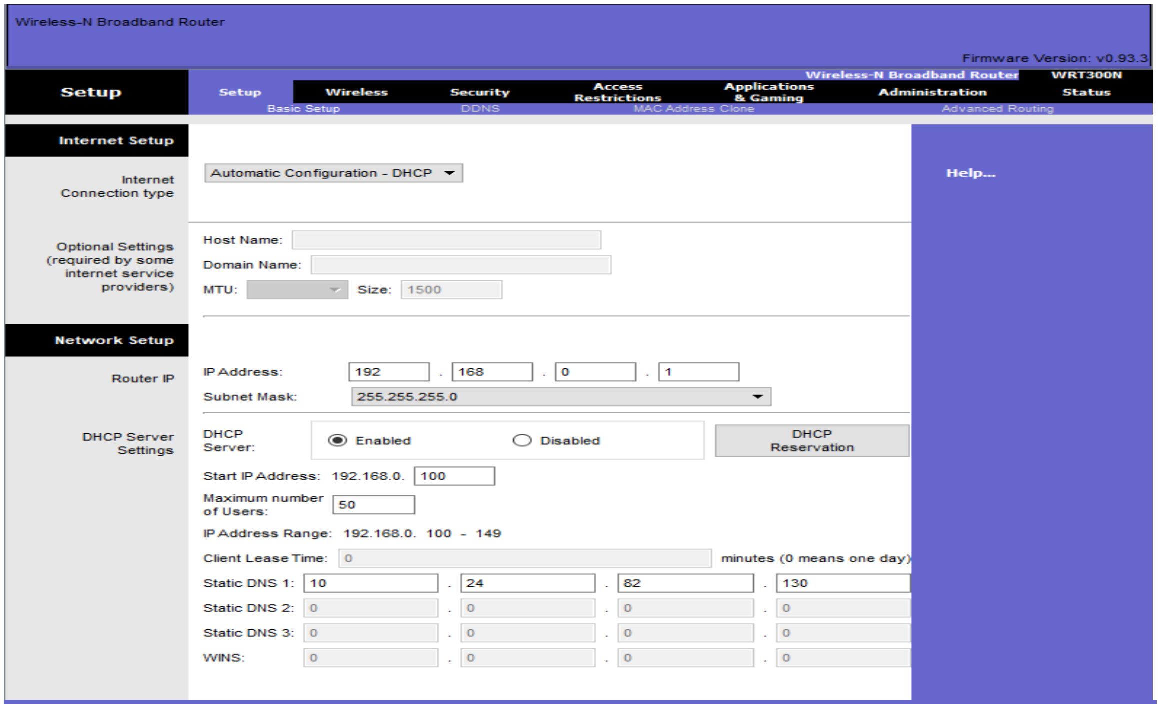
- **DYANAMIC PAT commands AT BRANCH router:**



COMMAND	PURPOSE
access-list 1 permit 10.24.82.0 0.0.0.127	Listing the IP in the internal network to be translated
ip nat inside source list 1 interface S0/0/1 overload	Establishing the internal IP that require translation to the Serial Port's Public IP address
interface G0/1	Entering the interface configuration mode connect to internal network
ip nat inside	Establishing the port as the internal network area
exit	Exiting the interface configuration mode
interface S0/0/1	Entering the interface configuration mode connect to Perimeter router
ip nat outside	Establishing the port as the external network area
exit	Exiting the interface configuration mode

- **Image of configuration of Wireless LAN on HQ Wireless router:**

1.



Wireless-N Broadband Router

Firmware Version: v0.93.3

Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers)

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255.255.255.0

DHCP Server Settings

DHCP Server: ● Enabled ○ Disabled

Start IP Address: 192.168.0. 100

Maximum number of Users: 50

IP Address Range: 192.168.0. 100 - 149

Client Lease Time: 0 minutes (0 means one day)

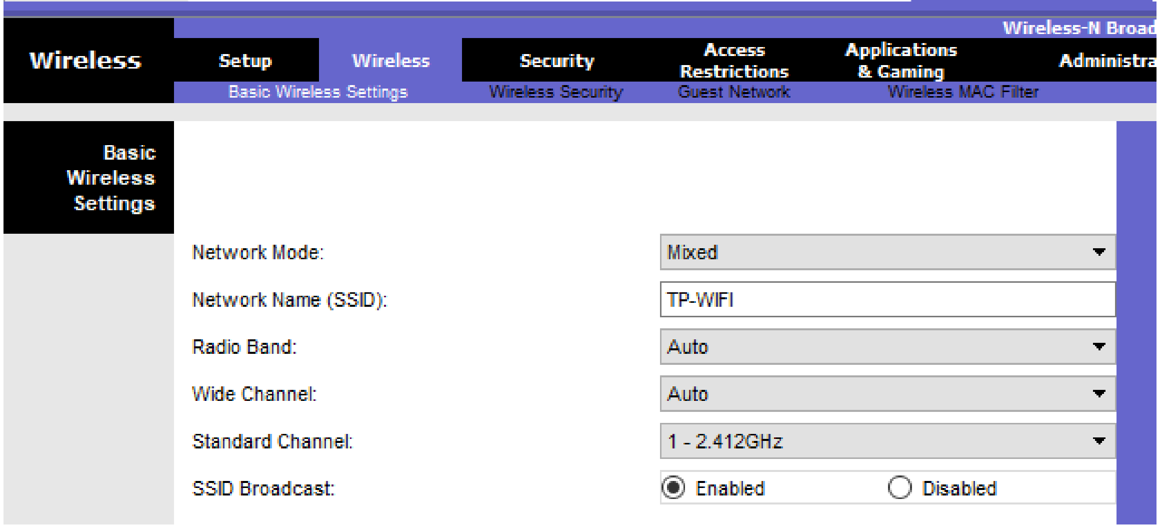
Static DNS 1: 10 . 24 . 82 . 130

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

2.



Basic Wireless Settings

Network Mode: Mixed

Network Name (SSID): TP-WIFI

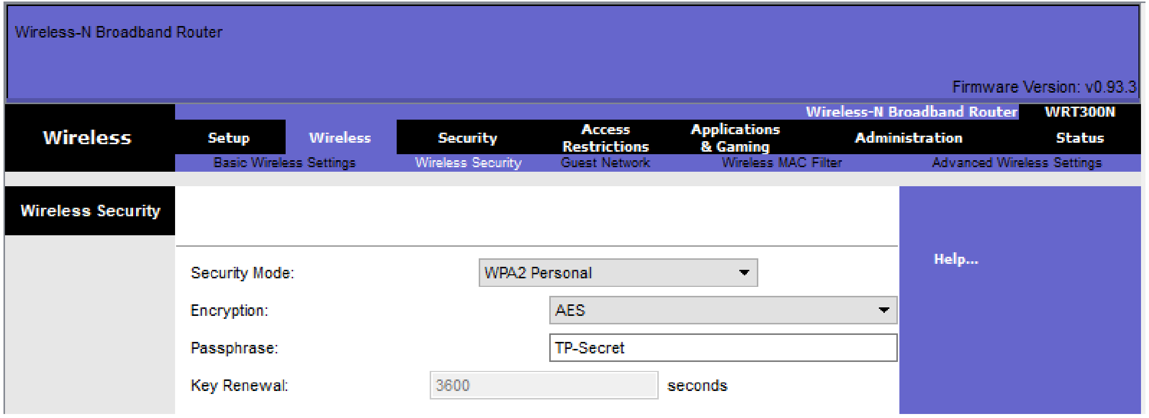
Radio Band: Auto

Wide Channel: Auto

Standard Channel: 1 - 2.412GHz

SSID Broadcast: ● Enabled ○ Disabled

3.



Wireless-N Broadband Router

Firmware Version: v0.93.3

Wireless Security

Security Mode: WPA2 Personal

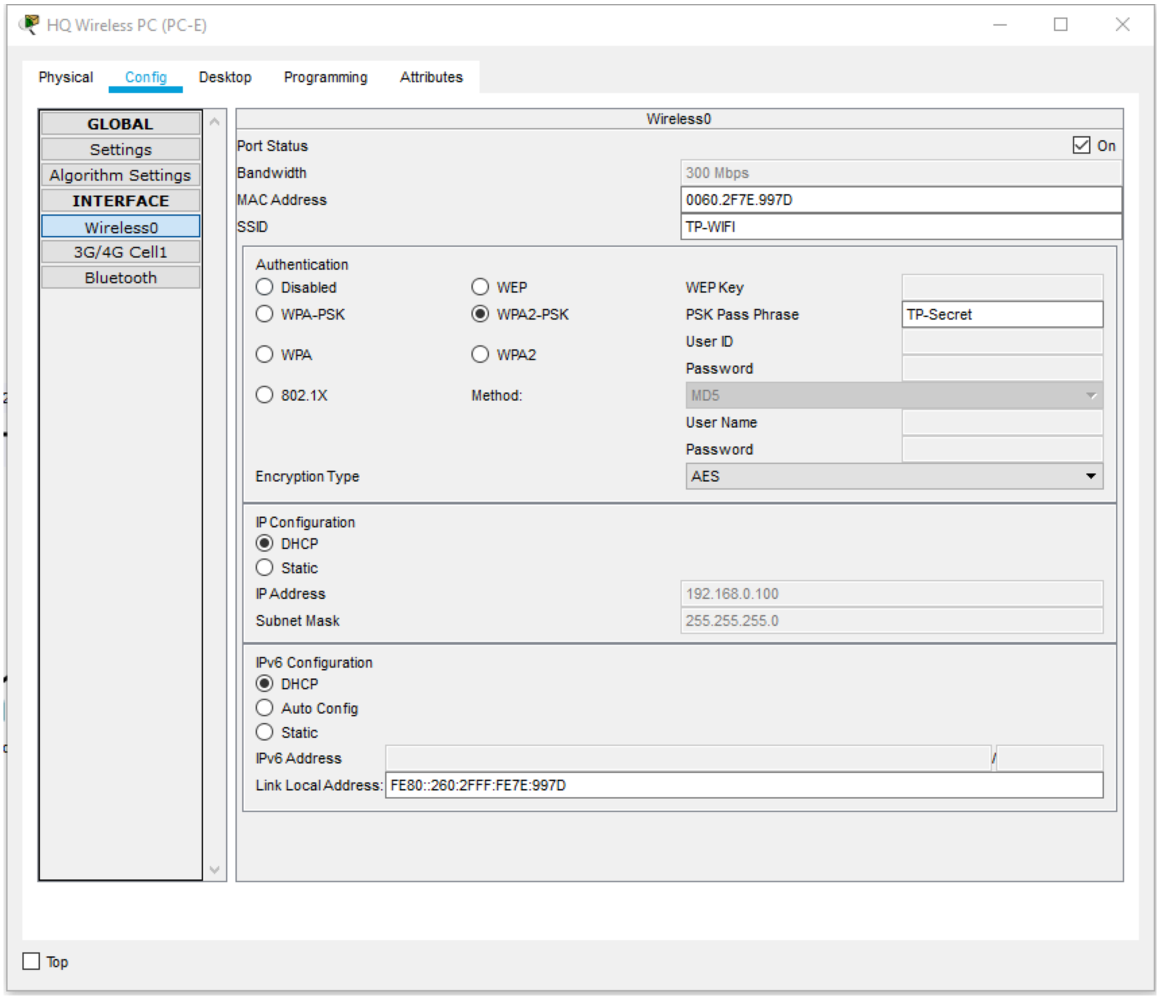
Encryption: AES

Passphrase: TP-Secret

Key Renewal: 3600 seconds

1. Image 1 shows the configurations of the router's Wireless IP and DHCP settings

2. Images 2 and 3 shows the configuration of the wireless network which will be required by users to connect to the wireless router



Wireless0

Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 0060.2F7E.997D

SSID TP-WIFI

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

○ WPA ○ WPA2

○ 802.1X

WEP Key

PSK Pass Phrase TP-Secret

User ID

Password

Method: MD5

User Name

Password

Encryption Type AES

IP Configuration

● DHCP

○ Static

IP Address 192.168.0.100

Subnet Mask 255.255.255.0

IPv6 Configuration

● DHCP

○ Auto Config

○ Static

IPv6 Address /

Link Local Address: FE80::260:2FFF:FE7E:997D

1\.

Image 4 is the wireless configurations on the HQ wireless PC (PC-E)

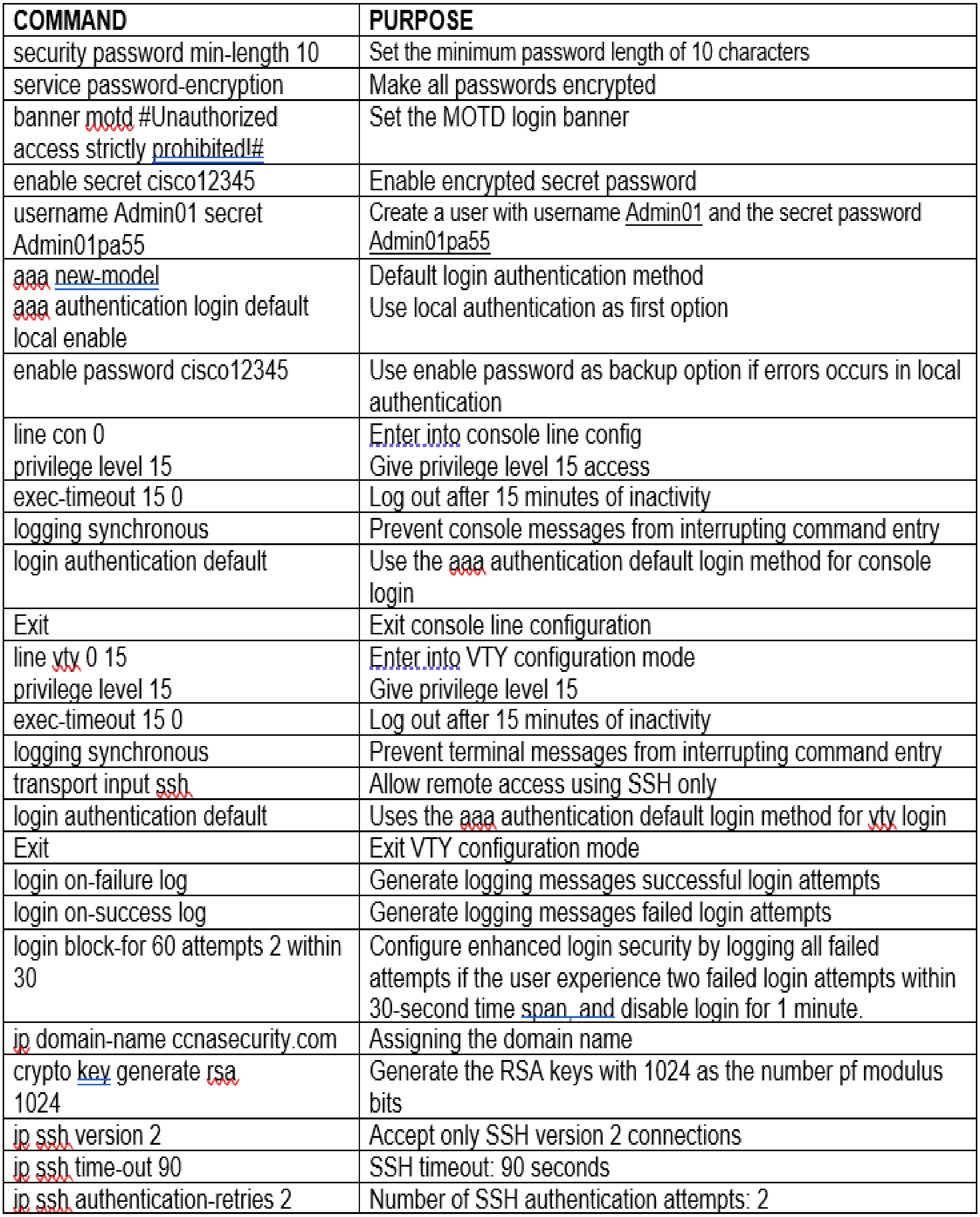
- **Show Commands:**

DHCP:	show ip dhcp pool HQ_LAN
NAT:	show ip nat statistics show ip nat translations
PAT:	show ip nat statistics

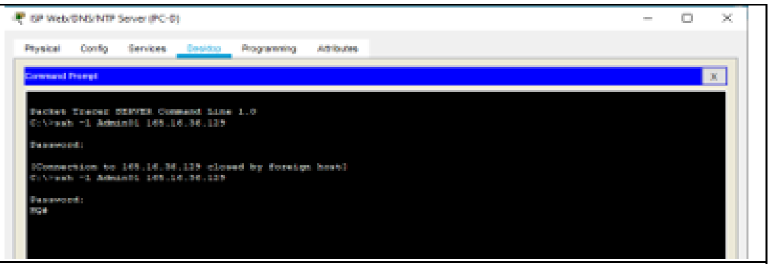
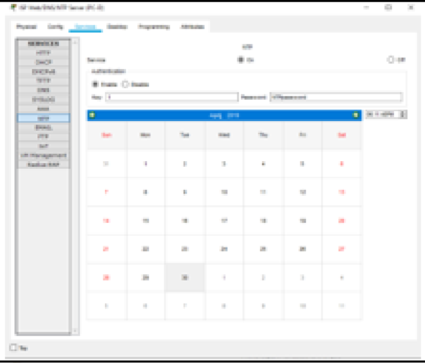
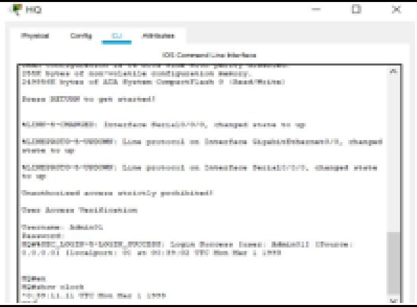
5. Security Implementation

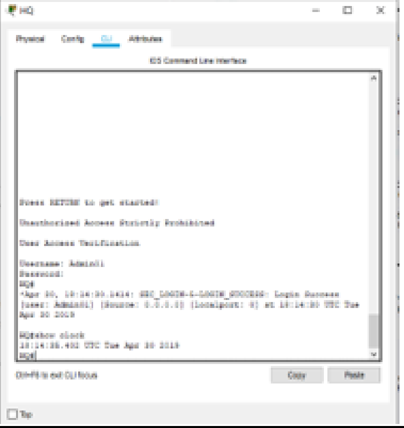
5.1 Router Hardening (including Wireless Router Hardening)

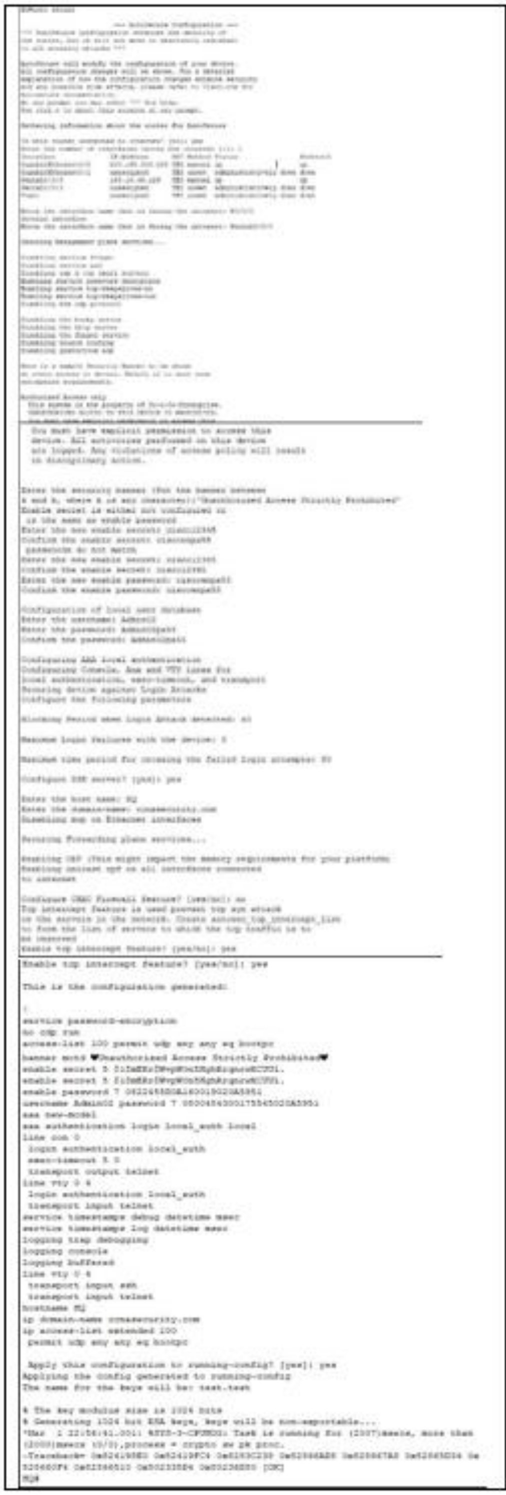
- HQ Perimeter router Hardening commands:



COMMAND	PURPOSE
security password min-length 10	Set the minimum password length of 10 characters
service password-encryption	Make all passwords encrypted
banner motd #Unauthorized access strictly prohibited!#	Set the MOTD login banner
enable secret cisco12345	Enable encrypted secret password
username Admin01 secret Admin01pa55	Create a user with username Admin01 and the secret password Admin01pa55
aaa new-model aaa authentication login default local enable	Default login authentication method Use local authentication as first option
enable password cisco12345	Use enable password as backup option if errors occurs in local authentication
line con 0 privilege level 15	Enter into console line config Give privilege level 15 access
exec-timeout 15 0	Log out after 15 minutes of inactivity
logging synchronous	Prevent console messages from interrupting command entry
login authentication default	Use the aaa authentication default login method for console login
Exit	Exit console line configuration
line vty 0 15 privilege level 15	Enter into VTY configuration mode Give privilege level 15
exec-timeout 15 0	Log out after 15 minutes of inactivity
logging synchronous	Prevent terminal messages from interrupting command entry
transport input ssh	Allow remote access using SSH only
login authentication default	Uses the aaa authentication default login method for vty login
Exit	Exit VTY configuration mode
login on-failure log	Generate logging messages successful login attempts
login on-success log	Generate logging messages failed login attempts
login block-for 60 attempts 2 within 30	Configure enhanced login security by logging all failed attempts if the user experience two failed login attempts within 30-second time span, and disable login for 1 minute.
ip domain-name ccnasecurity.com	Assigning the domain name
crypto key generate rsa 1024	Generate the RSA keys with 1024 as the number pf modulus bits
ip ssh version 2	Accept only SSH version 2 connections
ip ssh time-out 90	SSH timeout: 90 seconds
ip ssh authentication-retries 2	Number of SSH authentication attempts: 2

ssh –l Admin01 165.16.36.129	ISP Web/DNS/NTP Server (PC-0) Command Prompt Packet Tracer SERVER Command Line 1.0 C:\>ssh -l Admin01 165.16.36.129 Password: [Connection to 165.16.36.129 closed by foreign host] C:\>ssh -l Admin01 165.16.36.129 Password: HQ#
ISP Web/DNS/NTP Server (PC-0) NTP Service ● On ○ Off Authentication ● Enable ○ Disable Key: 1 Password: NTPpassword April 2019	NTP MASTER CONFIG Please refer appendix part 7 for clearer image.
HQ IOS Command Line Interface 32768 bytes of non-volatile configuration memory. 249856K bytes of ATA System CompactFlash 0 (Read/Write) Press RETURN to get started! %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up Unauthorized access strictly prohibited! User Access Verification Username: Admin01 Password: HQ#%SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Admin01] [Source: 0.0.0.0] [localport: 0] at 00:39:02 UTC Mon Mar 1 1993 HQ#en HQ#show clock *0:39:11.11 UTC Mon Mar 1 1993	Current date and time before NTP Please refer to appendix part 7 for clearer image.
ntp authentication-key 1 md5 NTPpassword	NTP authentication key number 1 with MD5 hashing and password NTPpassword
ntp trusted-key 1	Use the NTP trusted key above for authentication.
ntp authenticate	Enable NTP authentication feature.
ntp server 10.24.82.130 key 1	Configure the router (as NTP client) to access its NTP master (ISP Web/DNS/NTP server IP address) with authentication key number 1
ntp update-calendar	Enable NTP client to periodically update the calendar with the NTP time source

HQ IOS Command Line Interface Press RETURN to get started! Unauthorized Access Strictly Prohibited User Access Verification Username: Admin01 Password: HQ# *Apr 30, 18:14:30.1414: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Admin01] [Source: 0.0.0.0] [localport: 0] at 18:14:30 UTC Tue Apr 30 2019 HQ#show clock 18:14:35.432 UTC Tue Apr 30 2019 HQ#	NEW NTP TIME Please Refer to appendix part 7 for clearer image.
Auto secure	This begins the auto secure service.

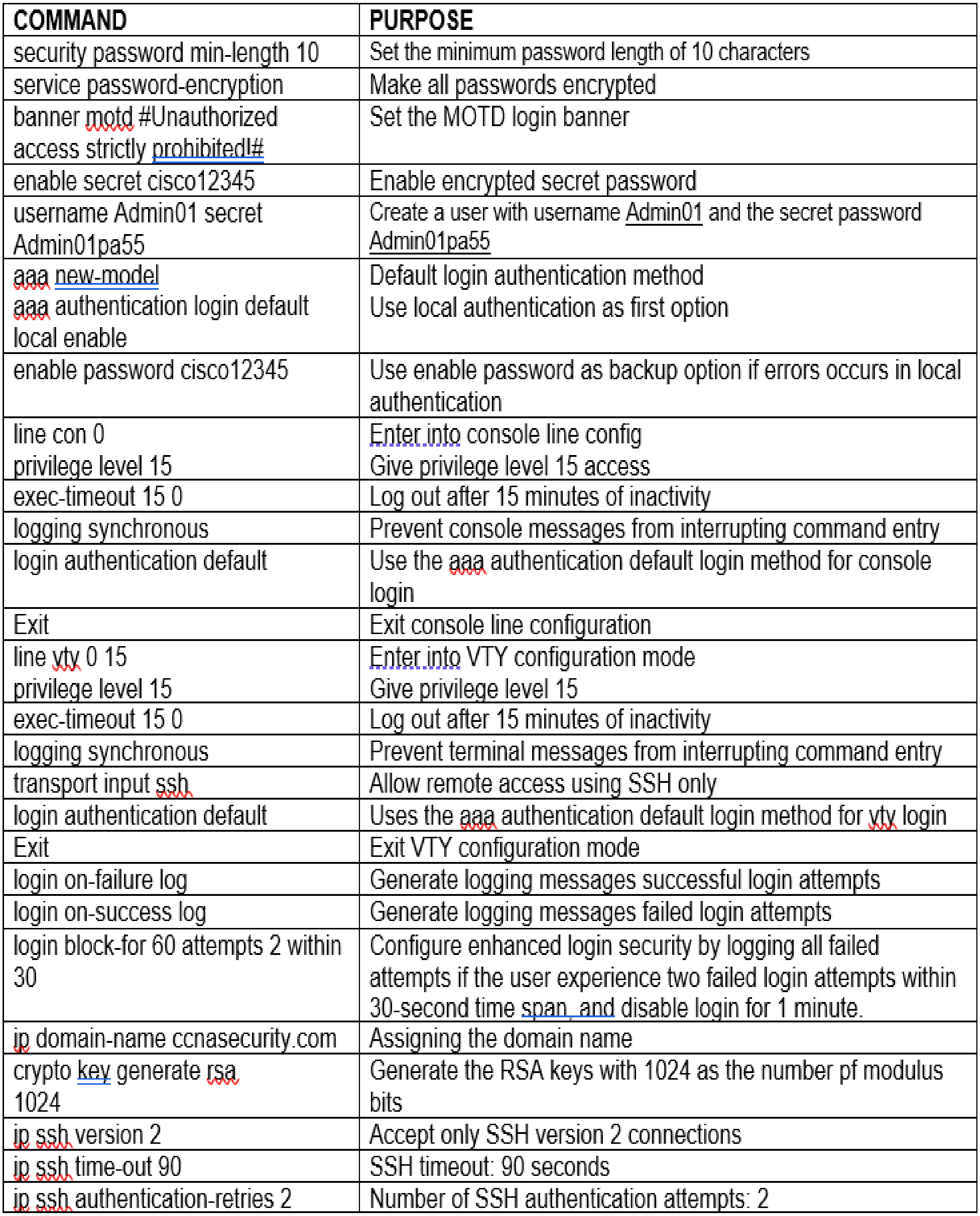


```
[illegible]

                    --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: 1
Interface            IP-Address      OK? Method Status                Protocol
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]

Enter the interface name that is facing the internet: [illegible]
[illegible]
Enter the interface name that is facing the internet: [illegible]

Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
  This system is the property of [illegible] Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.


Enter the security banner {Put the banner between
k and k, where k is any character}:"Unauthorized Access Strictly Prohibited"
Enable secret is either not configured or
 is the same as enable password
Enter the new enable secret: cisco12345
Confirm the enable secret: ciscoenpa55
 passwords do not match
Enter the new enable secret: cisco12345
Confirm the enable secret: cisco12345
Enter the new enable password: ciscoenpa55
Confirm the enable password: ciscoenpa55

Configuration of local user database
Enter the username: Admin01
Enter the password: Admin01pa55
Confirm the password: Admin01pa55

Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 60

Maximum Login failures with the device: 3

Maximum time period for crossing the failed login attempts: 30

Configure SSH server? [yes]: yes

Enter the host name: MJ
Enter the domain-name: ccnasecurity.com
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected
to internet

Configure CBAC Firewall feature? [yes/no]: no
Tcp intercept feature is used prevent tcp syn attack
on the servers in the network. Create autosec_tcp_intercept_list
to form the list of servers to which the tcp traffic is to
be observed
Enable tcp intercept feature? [yes/no]: yes
Enable tcp intercept feature? [yes/no]: yes

This is the configuration generated:

!
service password-encryption
no cdp run
access-list 100 permit udp any any eq bootpc
banner motd ♥Unauthorized Access Strictly Prohibited♥
enable secret 5 [illegible]
enable secret 5 [illegible]
enable password 7 [illegible]
username Admin01 password 7 [illegible]
aaa new-model
aaa authentication login local_auth local
line con 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
service timestamps debug datetime msec
service timestamps log datetime msec
logging trap debugging
logging console
logging buffered
line vty 0 4
 transport input ssh
 transport input telnet
hostname MJ
ip domain-name ccnasecurity.com
ip access-list extended 100
 permit udp any any eq bootpc

 Apply this configuration to running-config? [yes]: yes
Applying the config generated to running-config
The name for the keys will be: test.test

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
*Mar  1 22:56:41.001: %SYS-3-CPUHOG: Task is running for (2007)msecs, more than
(2000)msecs (0/0),process = crypto sw pk proc.
-Traceback= [illegible]
[illegible] [OK]
MJ#
```

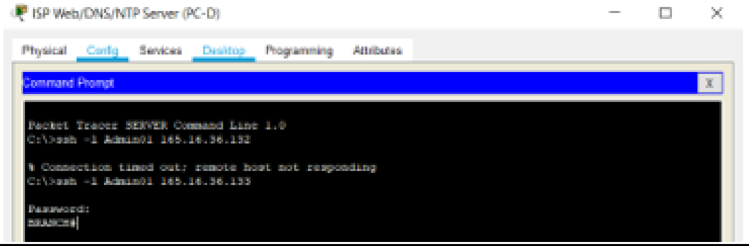
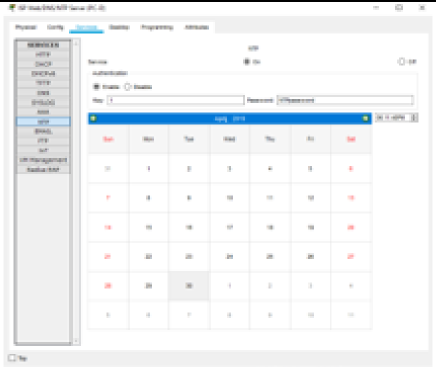
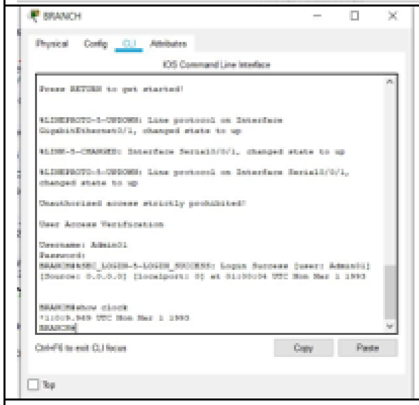
AUTO SECURE SCREEN SHOTS

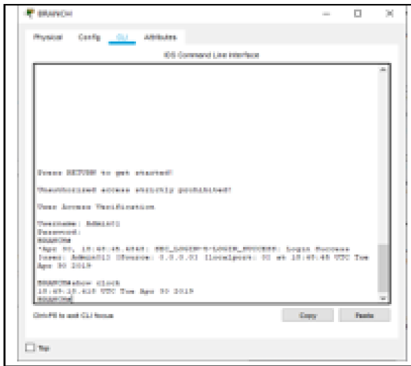
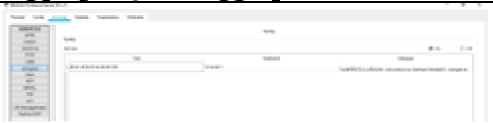
Please refer to appendix number 7 for clearer screenshots.

- Branch Perimeter router Hardening commands:



COMMAND	PURPOSE
security password min-length 10	Set the minimum password length of 10 characters
service password-encryption	Make all passwords encrypted
banner motd #Unauthorized access strictly prohibited!#	Set the MOTD login banner
enable secret cisco12345	Enable encrypted secret password
username Admin01 secret Admin01pa55	Create a user with username Admin01 and the secret password Admin01pa55
aaa new-model aaa authentication login default local enable	Default login authentication method Use local authentication as first option
enable password cisco12345	Use enable password as backup option if errors occurs in local authentication
line con 0 privilege level 15	Enter into console line config Give privilege level 15 access
exec-timeout 15 0	Log out after 15 minutes of inactivity
logging synchronous	Prevent console messages from interrupting command entry
login authentication default	Use the aaa authentication default login method for console login
Exit	Exit console line configuration
line vty 0 15 privilege level 15	Enter into VTY configuration mode Give privilege level 15
exec-timeout 15 0	Log out after 15 minutes of inactivity
logging synchronous	Prevent terminal messages from interrupting command entry
transport input ssh	Allow remote access using SSH only
login authentication default	Uses the aaa authentication default login method for vty login
Exit	Exit VTY configuration mode
login on-failure log	Generate logging messages successful login attempts
login on-success log	Generate logging messages failed login attempts
login block-for 60 attempts 2 within 30	Configure enhanced login security by logging all failed attempts if the user experience two failed login attempts within 30-second time span, and disable login for 1 minute.
ip domain-name ccnasecurity.com	Assigning the domain name
crypto key generate rsa 1024	Generate the RSA keys with 1024 as the number pf modulus bits
ip ssh version 2	Accept only SSH version 2 connections
ip ssh time-out 90	SSH timeout: 90 seconds
ip ssh authentication-retries 2	Number of SSH authentication attempts: 2

ssh –l Admin01 165.16.36.133	Please Refer to Appendix 8 for clearer image  ISP Web/DNS/NTP Server (PC-D) Packet Tracer SERVER Command Line 1.0 C:\>ssh -l Admin01 165.16.36.132 % Connection timed out; remote host not responding C:\>ssh -l Admin01 165.16.36.133 Password: BRANCH#
 NTP Service ● On ○ Off Authentication ● Enable ○ Disable Key: 1 Password: NTPpassword	NTP MASTER CONFIG Please Refer to Appendix 8 for clearer image
 BRANCH IOS Command Line Interface Press RETURN to get started! %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up Unauthorized access strictly prohibited! User Access Verification Username: Admin01 Password: BRANCH#%SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Admin01] [Source: 0.0.0.0] [localport: 0] at 01:00:04 UTC Mon Mar 1 1993 BRANCH#show clock *1:01:9.949 UTC Mon Mar 1 1993 BRANCH#	Current date and time before NTP Please Refer to Appendix 8 for clearer image
ntp authentication-key 1 md5 NTPpassword	NTP authentication key number 1 with MD5 hashing and password NTPpassword
ntp trusted-key 1	Use the NTP trusted key above for authentication
ntp authenticate	Enable NTP authentication feature
ntp server 10.24.82.130 key 1	Configure the router (as NTP client) to access its NTP master (ISP Web/DNS/NTP server IP address) with authentication key number 1
ntp update-calendar	Enable NTP client to periodically update the calendar with the NTP time source

 Press RETURN to get started! Unauthorized access strictly prohibited! User Access Verification Username: Admin01 Password: BRANCH# *Apr 30, 15:45:45.454: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Admin01] [Source: 0.0.0.0] [localport: 0] at 15:45:45 UTC Tue Apr 30 2019 BRANCH#show clock 15:49:10.410 UTC Tue Apr 30 2019 BRANCH#	NEW NTP TIME Please Refer to Appendix 8 for clearer image
service timestamps log datetime msec	
logging 10.24.82.3	
logging trap debugging	
	SYSLOG SCREENSHOTS Please Refer to Appendix 8 for clearer image

- HQ FW router Hardening commands:

COMMAND	PURPOSE
security password min-length 10	Set the minimum password length of 10 characters
service password-encryption	Make all passwords encrypted
banner motd #Unauthorized access strictly prohibited!#	Set the MOTD login banner
enable secret cisco12345	Enable encrypted secret password
username Admin01 secret Admin01pa55 privilege 15	Create a user with username Admin01 and the secret password Admin01pa55
aaa new-model aaa authentication login default local enable	Default login authentication method Use local authentication as first option
enable password cisco12345	Use enable password as backup option if errors occurs in local authentication
line con 0 privilege level 15	Enter into console line config Give privilege level 15 access
exec-timeout 15 0	Log out after 15 minutes of inactivity
logging synchronous	Prevent console messages from interrupting command entry
login authentication default	Use the aaa authentication default login method for console login
Exit	Exit console line configuration
line vty 0 15 privilege level 15	Enter into VTY configuration mode Give privilege level 15
exec-timeout 15 0	Log out after 15 minutes of inactivity
logging synchronous	Prevent terminal messages from interrupting command entry
transport input ssh	Allow remote access using SSH only

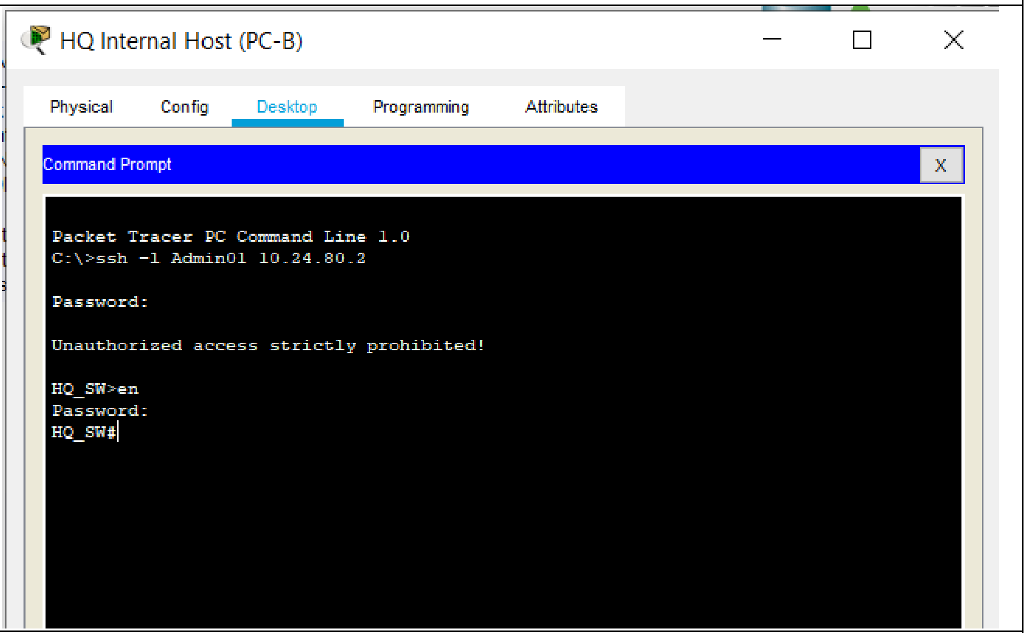
login authentication default	Uses the aaa authentication default login method for vty login
Exit	Exit VTY configuration mode
login on-failure log	Generate logging messages successful login attempts
login on-success log	Generate logging messages failed login attempts
login block-for 60 attempts 2 within 30	Configure enhanced login security by logging all failed attempts if the user experience two failed login attempts within 30-second time span, and disable login for 1 minute.
ip domain-name ccnasecurity.com	Assigning the domain name
crypto key generate rsa 1024	Generate the RSA keys with 1024 as the number pf modulus bits
ip ssh version 2	Accept only SSH version 2 connections
ip ssh time-out 90	SSH timeout: 90 seconds
ip ssh authentication-retries 2	Number of SSH authentication attempts: 2
ssh –l Admin01 165.16.36.129	

- **Wireless Router Hardening**

5.2 Switch Hardening

- HQ SWITCH

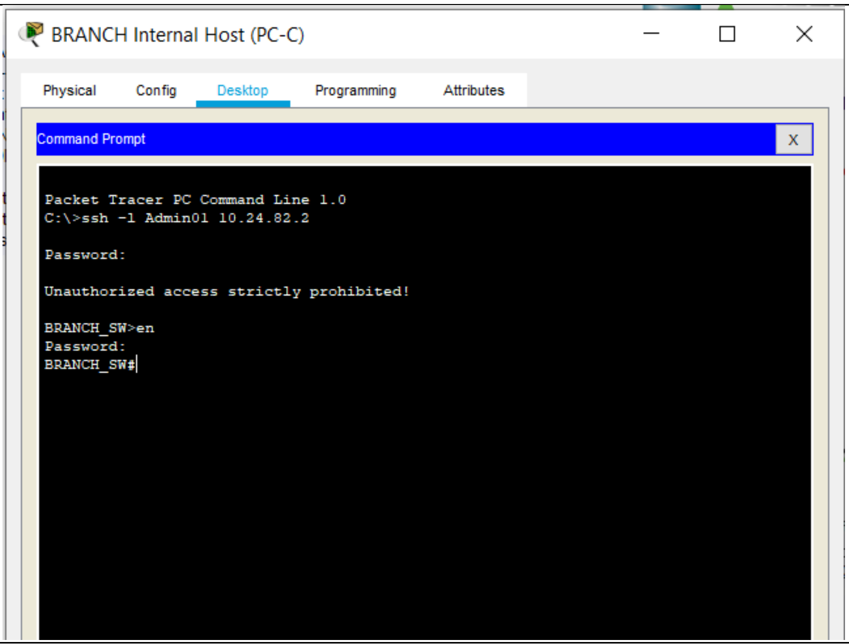
Command	**Purpose**
no ip http server no ip http secure-server	Prevent HTTP access by disabling both the HTTP server and HTTP secure server
service password-encryption	Ensure all password stored is encrypted
banner motd #Unauthorized access strictly prohibited!#	Provides a warning to unauthorized user when access this router
enable secret cisco12345	Sets the password to enter privilege mode
username Admin01 secret Admin01pa55	Creating the new user with password
line con 0 privilege level 15	Entering console line Give privilege 15 access only
exec-timeout 15 0	Log out user who is are not doing anything after 15 mins
logging synchronous	Prevent console message form interrupting when commands being entered
login local	Login with local user database
exit	Exit config mode
line vty 0 15 privilege level 15	Enter into VTY configuration mode Give privilege level 15
exec-timeout 15 0	Log out after 15 minutes of inactivity
logging synchronous	Log out after 15 minutes of inactivity
login local	Login with local user database
transport input ssh	Allow remote access using SSH only
exit	Exit config mode

ip domain-name ccnasecurity.com	Assigning the domain name
crypto key generate rsa 1024	Generate the RSA keys with 1024 as the number pf modulus bits
ip ssh version 2	Accept only SSH version 2 connections
ip ssh time-out 90	SSH timeout: 90 seconds
ip ssh authentication-retries 2	Number of SSH authentication attempts: 2
ssh –l Admin01 10.24.80.2	 HQ Internal Host (PC-B) Physical Config Desktop Programming Attributes Command Prompt X Packet Tracer PC Command Line 1.0 C:\>ssh -l Admin01 10.24.80.2 Password: Unauthorized access strictly prohibited! HQ_SW>en Password: HQ_SW#
Int range fa0/1-24 Switchport mode access	Disable trunking on all switch ports except G0/0 and G0/1
spanning-tree portfast default	Enable STP (Spanning Tree Protocol) PortFast mode on all switch ports
Int range fa0/1-24 spanning-tree bpduguard enable	Enable BPDU (Bridge Protocol Data Unit) guard on all switch access ports
Int range fa0/1-24 switchport port-security	First enable switch port security
switchport port-security maximum 2 switchport port-security violation shutdown	Set maximum MAC addresses to 2 and violation action to shutdown
switchport port-security mac-address sticky	Sticky option to allow secure MAC address that is dynamically learned on a port to be saved to the switch running configuration
exit	Exit config mode
Int range fa0/1-17	Disable all unused ports
Shutdown	
exit	
Int range fa0/20-23	
Shutdown	

exit	

- **BRANCH SWITCH**

Commands	**Purpose**
no ip http server no ip http secure-server	Prevent HTTP access by disabling both the HTTP server and HTTP secure server
service password-encryption	Ensure all password stored is encrypted
banner motd #Unauthorized access strictly prohibited!#	Provides a warning to unauthorized user when access this router
enable secret cisco12345	Sets the password to enter privilege mode
username Admin01 secret Admin01pa55	Creating the new user with password
line con 0 privilege level 15	Entering console line Give privilege 15 access only
exec-timeout 15 0	Log out user who is are not doing anything after 15 mins
logging synchronous	Prevent console message form interrupting when commands being entered
login local	Login with local user database
exit	
line vty 0 15 privilege level 15	Enter into VTY configuration mode Give privilege level 15
exec-timeout 15 0	Log out after 15 minutes of inactivity
logging synchronous	Log out after 15 minutes of inactivity
login local	Login with local user database
transport input ssh	Allow remote access using SSH only
exit	Exit config mode
ip domain-name ccnasecurity.com	Assigning the domain name
crypto key generate rsa 1024	Generate the RSA keys with 1024 as the number pf modulus bits
ip ssh version 2	Accept only SSH version 2 connections
ip ssh time-out 90	SSH timeout: 90 seconds
ip ssh authentication-retries 2	Number of SSH authentication attempts: 2

ssh -l Admin01 10.24.82.2	 BRANCH Internal Host (PC-C)
	Physical
	Config
	Desktop
	Programming
	Attributes
	Command Prompt
	X
	`Packet Tracer PC Command Line 1.0`
	`C:\>ssh -l Admin01 10.24.82.2`
	
	`Password:`
	
	`Unauthorized access strictly prohibited!`
	
	`BRANCH_SW>en`
	`Password:`
	`BRANCH_SW#`

Int range fa0/1-24 Switchport mode access	Disable trunking on all switch ports except G0/0 and G0/1
spanning-tree portfast default	Enable STP (Spanning Tree Protocol) PortFast mode on all switch ports
Int range fa0/1-24 spanning-tree bpduguard enable	Enable BPDU (Bridge Protocol Data Unit) guard on all switch access ports
Int range fa0/1-24 switchport port-security	First enable switch port security
switchport port-security maximum 2	Set maximum MAC addresses to 2 and violation action to shutdown
switchport port-security mac-address sticky	Sticky option to allow secure MAC address that is dynamically learned on a port to be saved to the switch running configuration
exit	Exit config mode
Int range fa0/1-4	Disable all unused ports
Shutdown	
exit	
Int range fa0/6-17	
Shutdown	
Exit	
Int range fa0/20-24	
shutdown	
exit	

5.3 IOS Firewall Implementation

5.3.1 IOS ZPF without DMZ implementation at BRANCH router

COMMAND	PURPOSE
zone security INSIDE	Creates INSIDE and OUTSIDE security zones
Exit	

zone security OUTSIDE	
Exit	
class-map type inspect match-any ALLOWED-PROTOCOLS	Creates an inspect class-map named ALLOWED-PROTOCOLS to match the traffic to be allowed from the INSIDE zone to the OUTSIDE zone. Because we trust the INSIDE zone, we allow ANY of the following main protocols (tcp, udp and icmp)
match protocol tcp	
match protocol udp	
match protocol icmp	
Exit	Exit config mode
Exit	Exit config mode
policy-map type inspect INSIDE-TO-OUTSIDE	Creates an inspect policy-map named INSIDE-TO-OUTSIDE. Bind the ALLOWED-PROTOCOLS class-map created above to this policy-map. All packets matched by this class-map will be inspected
class type inspect ALLOWED-PROTOCOLS	
inspect	
Exit	Exit config mode
Exit	Exit config mode
zone-pair security INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE	Creates a zone-pair called INSIDE-TO-OUTSIDE that allows traffic initiated from the BRANCH internal LAN to the external (public) network. Apply the policy-map INSIDE-TO-OUTSIDE created above to this zone-pair.
service-policy type inspect INSIDE-TO-OUTSIDE	
Exit	Exit config mode
Access-list 100 permit ip anu 10.24.82.0 0.0.0.127	Creates an extended access-list that allow the return traffic from external public network to the original BRANCH internal LAN.
Class-map type inspect match-all ALLOWED-TRAFFIC	Creates another inspect class-map named ALLOWED-TRAFFIC to match both the traffic as well as the protocols from the OUTSIDE zone to the INSIDE zone
Match access-group 100	
Match class-map ALLOWED-PROTOCOLS	
Exit	Exit config mode
Exit	Exit config mode
Policy-map type inspect OUTSIDE-TO-INSIDE	Creates another inspect policy-map named OUTSIDE-TO-INSIDE. Bind the ALLOWED-TRAFFIC class-map created above to this policy-map. All packets matched by this class-map will be inspected
Class type inspect ALLOWED-TRAFFIC	
Inspect	
Exit	Exit config mode
Exit	Exit config mode
Zone-pair security OUTSIDE-TO-INSIDE source OUTSIDE destination INISDE	Creates another zone-pair called OUTSIDE-TO-INSIDE that allows the retrun traffic originally initiated from the BRANCH internal LAN to the external (public) network. Apply the policy-map OUTSIDE-TO-INSIDE created above to this zone-pair
Service-policy type inspect OUTSIDE-TO-INSIDE	
Exit	Exit config mode

Int g0/1	Assigning zone interfaces for the router to know which network is suppose to be which area.
Zone-member security INSIDE	
Exit	
Int s0/0/0	
Zone-member security OUTSIDE	
exit	

5.3.2 IOS ZPF with DMZ implementation at HQ FW router

COMMAND	PURPOSE
Zone security INSDIE	Creates INSIDE, OUTSIDE and DMZ security zones
Exit	
Zone security OUTSIDE	
Exit	
Zone security DMZ	
Exit	
Access-list 100 permit ip any 10.24.80.0 0.0.1.255	Creates an extended access-list that allow the return traffic from external public network to the original HQ internal LAN
Class-map type inspect match-any ALLOWED-PROTOCOLS	Creates an inspect class-map named ALLOWED-PROTOCOLS to match the traffic to be allowed from the INSIDE zone to the OUTSIDE zone (and vice versa for return traffic). Because we trust the INSIDE zone, we allow ANY of the following main protocols (tcp, udp and icmp)
Match protocol tcp	
Match protocol udp	
Match protocol icmp	
exit	Exit config mode
Class-map type inspect match-all ALLOWED-INSIDE-TRAFFIC	Creates another inspect class-map named ALLOWED-INSIDE-TRAFFIC to match both the return traffic as well as the protocols from the OUTSIDE zone to the INSIDE zone
Match class-map ALLOWED-PROTOCOLS	
Match access-group 100	
Exit	Exit config mode
Policy-map type inspect INSIDE-TO-OUTSIDE	Creates an inspect policy-map named INSIDE-TO-OUTSIDE. Bind the ALLOWED-PROTOCOLS class-map created above to this policy-map. All packets matched by this class-map will be inspected.
Class type inspect ALLOWED-PROTOCOLS	
Inspect	
Exit	Exit config mode
Exit	Exit config mode
Policy-map type inspect OUTSIDE-TO-INSIDE	Creates another inspect policy-map named OUTSIDE-TO-INSIDE. Bind the ALLOWED-INSIDE-TRAFFIC class-map created above to this policy-map. All packets matched by this class-map will be inspected.
Class type inspect ALLOWED-INSIDE-TRAFFIC	
Inspect	
Exit	Exit config mode
Exit	Exit config mode
Zone-pair security INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE	Creates a zone-pair named INSIDE-TO-OUTSIDE that allows traffic initiated from the

Service-policy type inspect INSIDE-TO-OUTSIDE	BRANCH internal LAN to the external (public) network. Apply the policy-map INSIDE-TO-OUTSIDE created above to this zone-pair.
Exit	Exit config mode
Zone-pair security OUTSIDE-TO-INSIDE source OUTSIDE destination INSIDE	Creates another zone-pair named OUTSIDE-TO-INSIDE that allows the return traffic originally initiated from the HQ internal LAN to the external (public) network. Apply the policy-map OUTSIDE-TO-INSIDE created above to this zone-pair.
Service-policy type inspect OUTSIDE-TO-INSIDE	
Exit	Exit config mode
Policy-map type inspect INSIDE-TO-DMZ	Creates an inspect policy-map named INSIDE-TO-DMZ that bind to ALLOWED-PROTOCOLS.
Class type inspect ALLOWED-PROTOCOLS	
Inspect	
Exit	Exit config mode
Exit	Exit config mode
Policy-map type inspect DMZ-TO-INSIDE	Create another inspect policy-map named DMZ-TO-INSIDE that bind to ALLOWED-INSIDE-TRAFFIC.
Class type inspect ALLOWED-INSIDE-TRAFFIC	
inspect	
Exit	Exit config mode
Exit	Exit config mode
Zone-pair security INSDIE-TO-DMZ source INSIDE destination DMZ	Creates a zone-pair named INSIDE-TO-DMZ and bind to the inspect-policy map INSIDE-TO-DMZ.
Service-policy type inspect INSIDE-TO-DMZ	
Exit	Exit config mode
Zone-pair security DMZ-TO-INSIDE source DMZ destination INSIDE	Creates another zone-pair named DMZ-TO-INSIDE and bind to the inspect-policy map DMZ-TO-INSIDE.
Service-policy type inspect DMZ-TO-INSIDE	
Exit	Exit config mode
Access-list 101 permit ip any 10.24.82.128 0.0.0.15	Create a new extended access-list to allow public traffic to HQ DMZ LAN
Class-map type inspect match-all ALLOWED-DMZ-TRAFFIC	Create a new inspect class-map named ALLOWED-DMZ-TRAFFIC to match both the public traffic to HQ DMZ LAN as well as the protocols from the OUTSIDE zone to the DMZ.
Match access-group 101	
Match class-map ALLOWED-RPOTOCOLS	
Exit	Exit config mode
Policy-map type inspect OUTSIDE-TO-DMZ	Create an inspect policy-map named OUTSIDE-TO-DMZ that bind to ALLOWED-DMZ-TRAFFIC
Class type inspect ALLOWED-DMZ-TRAFFIC	
Inspect	
Exit	Exit config mode
exit	Exit config mode
Policy-map type inspect DMZ-TO-OUTSIDE	Create another inspect policy-map named DMZ-TO-OUTSIDE that bind to ALLOWED-PROTOCOLS
Class-type inspect ALLOWED-PROTOCOLS	
Inspect	
Exit	Exit config mode

Exit	Exit config mode
Zone-pair security DMZ-TO-OUTSIDE source DMZ destination OUTSIDE	Create another zone-pair named DMZ-TO-OUTSIDE and bind to the inspect-policy map DMZ-TO-OUTSIDE accordingly
Service-policy type inspect DMZ-TO-OUTSDIE	
Exit	Exit config mode
Zone-pair security OUTISDE-TO-DMZ source OUTSIDE destination DMZ	Create a zone-pair named OUTSIDE-TO-DMZ and bind to the inspect-policy map OUTSIDE-TO-DMZ accordingly
Service-policy type inspect OUTSIDE-TO-DMZ	
exit	Exit config mode
Int g0/1	Assigned HQ FW router's interface G0/0 to the OUTSIDE security zone, interface G0/1 to the INSIDE security zone, and interface G0/2 to the DMZ security zone
Zone-member security INSIDE	
exit	
Int g0/0	
Zone-member security OUTSIDE	
exit	
Int g0/2	
Zone-member security DMZ	
exit	

6. Cryptographic System Research Topic

RSA public key exchange is an asymmetric encryption algorithm. RSA can be used for service such as digital signatures, key exchanges and for encryption purposes.

An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem is an open question. There are no published methods to defeat the system if a large enough key is used.

RSA is a relatively slow algorithm. Because of this, it is not commonly used to directly encrypt user data. More often, RSA is used to transmit shared keys for symmetric key cryptography, which are then used for bulk encryption-decryption.

RSA involves a *public key* and a *private key*. The public key can be known by everyone, and it is used for encrypting messages. The intention is that messages encrypted with the public key can only be decrypted in a reasonable amount of time by using the private key. The public key is represented by the integers *n* and *e*; and, the private key, by the integer *d* (although *n* is also used during the decryption process, so it might be considered to be a part of the private key, too). *m* represents the message (previously prepared with a certain technique explained below).

Example Sam wants to send information to Zac. If they decide to use RSA, Sam must know Zac's public key to encrypt the message and Zac must use his private key to decrypt the message.

To enable Sam to send his encrypted messages, Zac transmits his public key (*n*, *e*) to Sam via a reliable, but not necessarily secret, route. Zac's private key (*d*) is never distributed. After Sam obtains Zac's public key, he can send a message *M* to Zac.

To do it, he first turns *M* (strictly speaking, the un-padded plaintext) into an integer *m* (strictly speaking, the padded plaintext), such that 0 ≤ *m* < *n* by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext *c*, using Zac's public key *e*, corresponding to

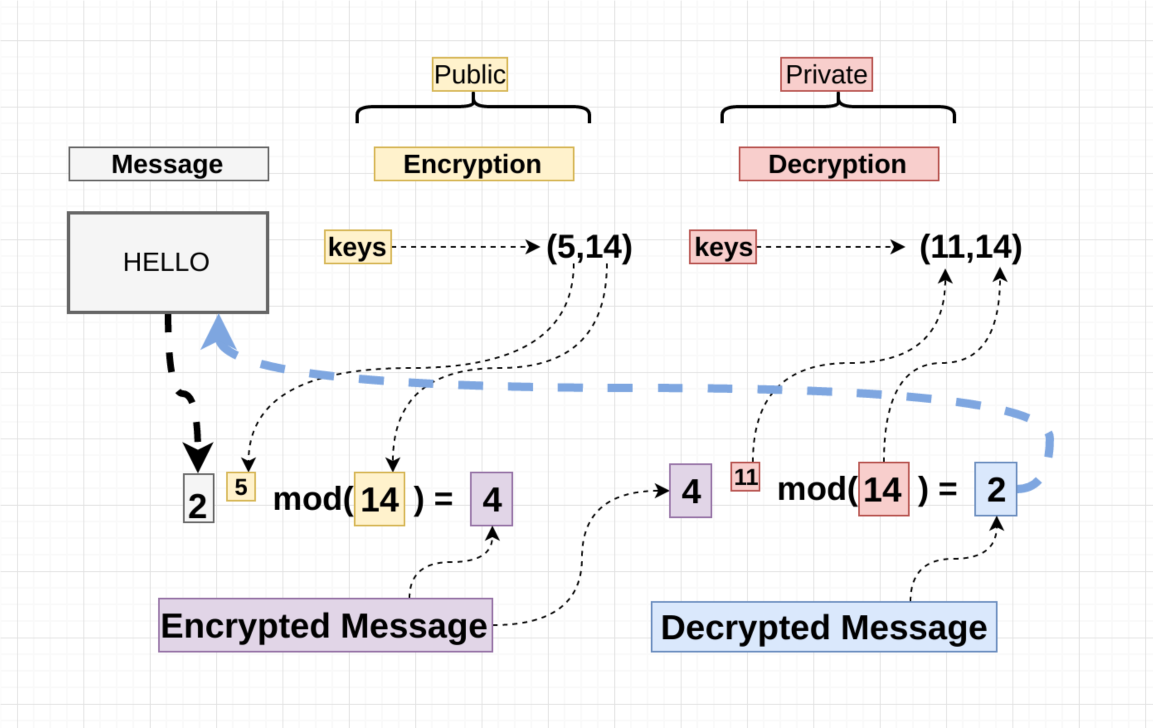
$$m^e \equiv c \pmod{n}$$

This can be done reasonably quickly, even for very large numbers, using modular exponentiation. Sam then transmits *c* to Zac.

Zac can recover *m* from *c* by using his private key exponent *d* by computing

$$c^d \equiv (m^e)^d \equiv m \pmod{n}$$

Given *m*, he can recover the original message *M* by reversing the padding scheme.



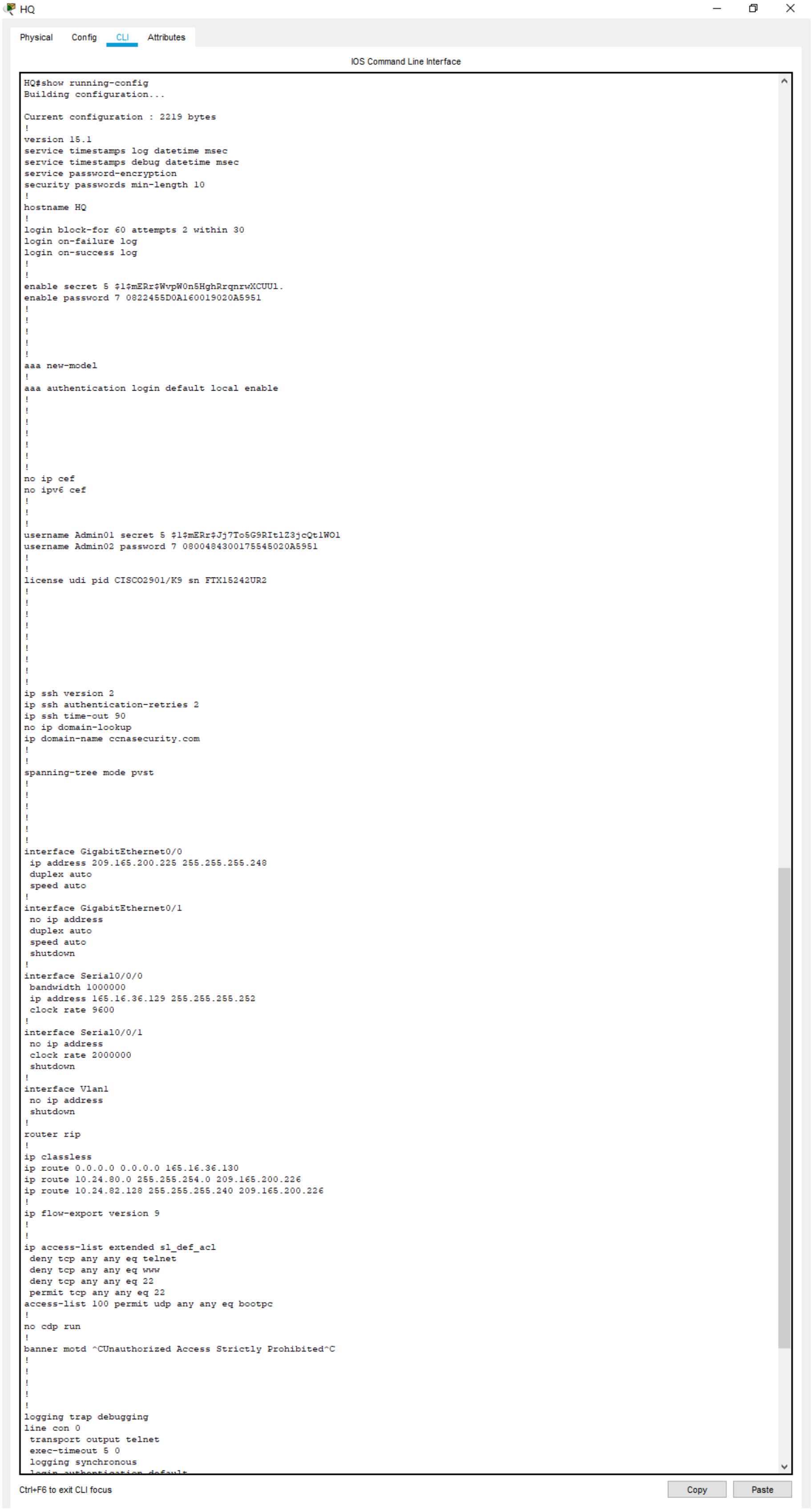
7. Conclusions

I have learned how to configure Static and Dynamic NAT , Dynamic PAT, DHCP as well as DHCP Wireless router in a Network. Router and switch hardening were things I feel I will remember the most as they are very relevant with our current daily lives. IOS zone based firewall is important as well as it helps me understand how to limit access and assign roles and policies to ensure outside network is not able to access internal network.

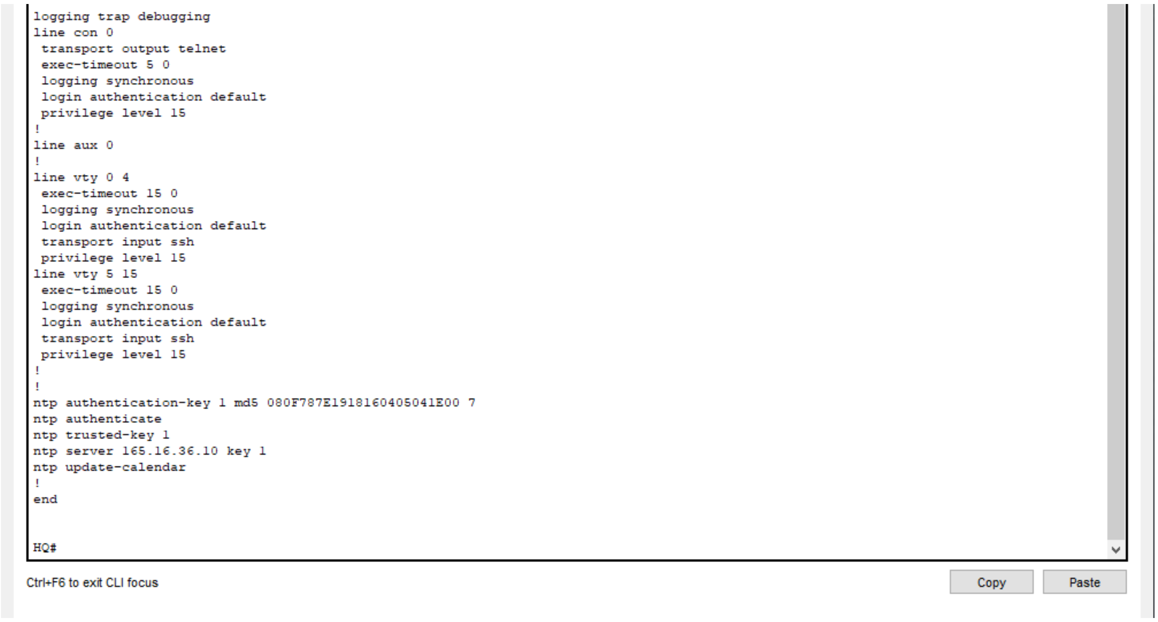
Appendices

Including all the relevant running configurations for the HQ, HQ_FW, BRANCH, ISP routers and HQ, BRANCH switches.

1. HQ ROUTER

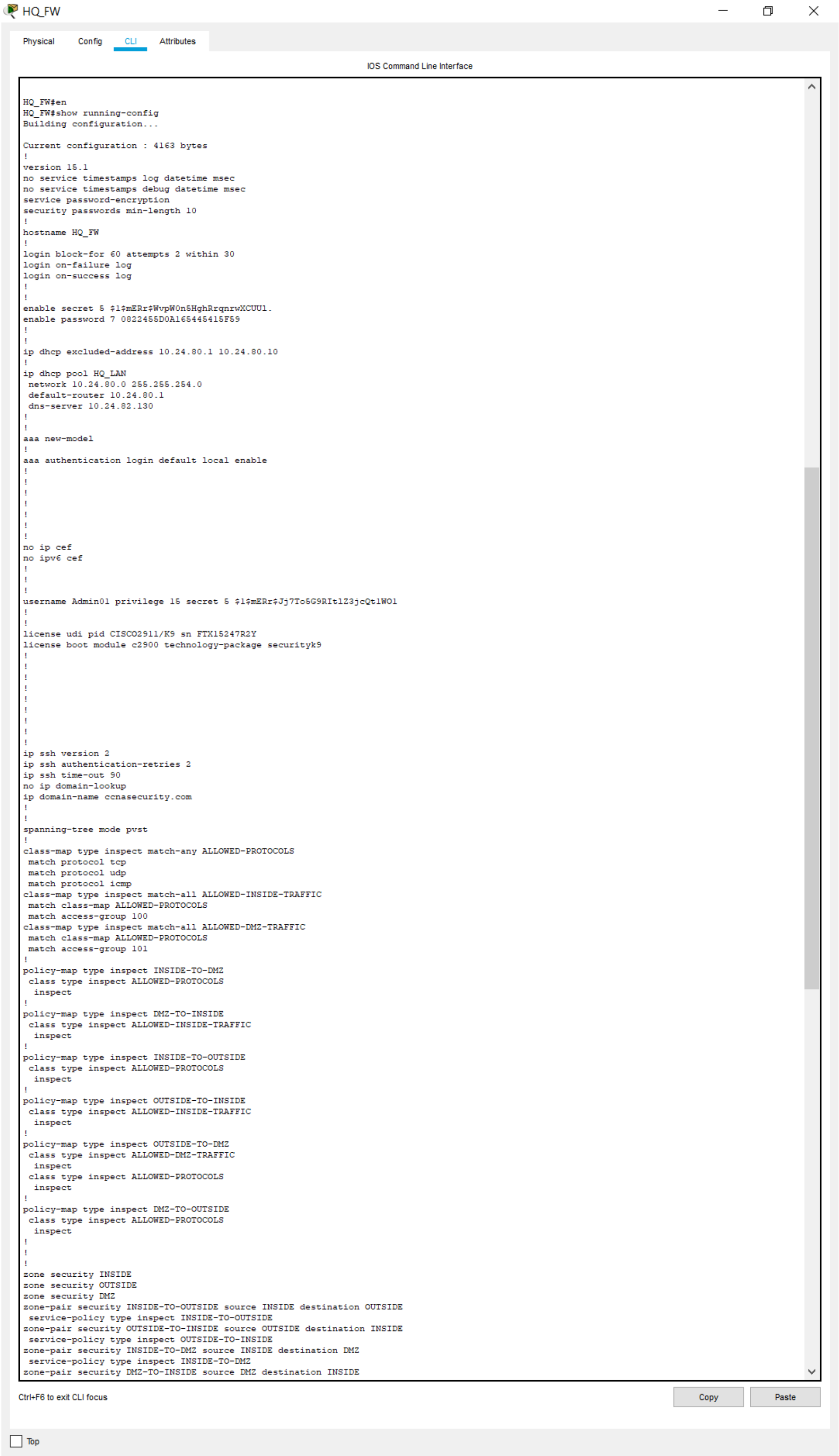


```
HQ#show running-config
Building configuration...

Current configuration : 2219 bytes
!
version 15.1
service timestamps log datetime msec
service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname HQ
!
login block-for 60 attempts 2 within 30
login on-failure log
login on-success log
!
!
enable secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUU1.
enable password 7 0822455D0A16001902OA5951
!
!
!
!
!
aaa new-model
!
aaa authentication login default local enable
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username Admin01 secret 5 $1$mERr$Jj7To5G9RItlZ3jcQt1WO1
username Admin02 password 7 08004843001755450 20A5951
!
!
license udi pid CISCO2901/K9 sn FTX15242UR2
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 90
no ip domain-lookup
ip domain-name ccnasecurity.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 209.165.200.225 255.255.255.248
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 bandwidth 1000000
 ip address 165.16.36.129 255.255.255.252
 clock rate 9600
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router rip
!
ip classless
ip route 0.0.0.0 0.0.0.0 165.16.36.130
ip route 10.24.80.0 255.255.254.0 209.165.200.226
ip route 10.24.82.128 255.255.255.240 209.165.200.226
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www
 deny tcp any any eq 22
 permit tcp any any eq 22
access-list 100 permit udp any any eq bootpc
!
no cdp run
!
banner motd ^CUnauthorized Access Strictly Prohibited^C
!
!
!
!
!
logging trap debugging
line con 0
 transport output telnet
 exec-timeout 5 0
 logging synchronous
 login authentication default
```

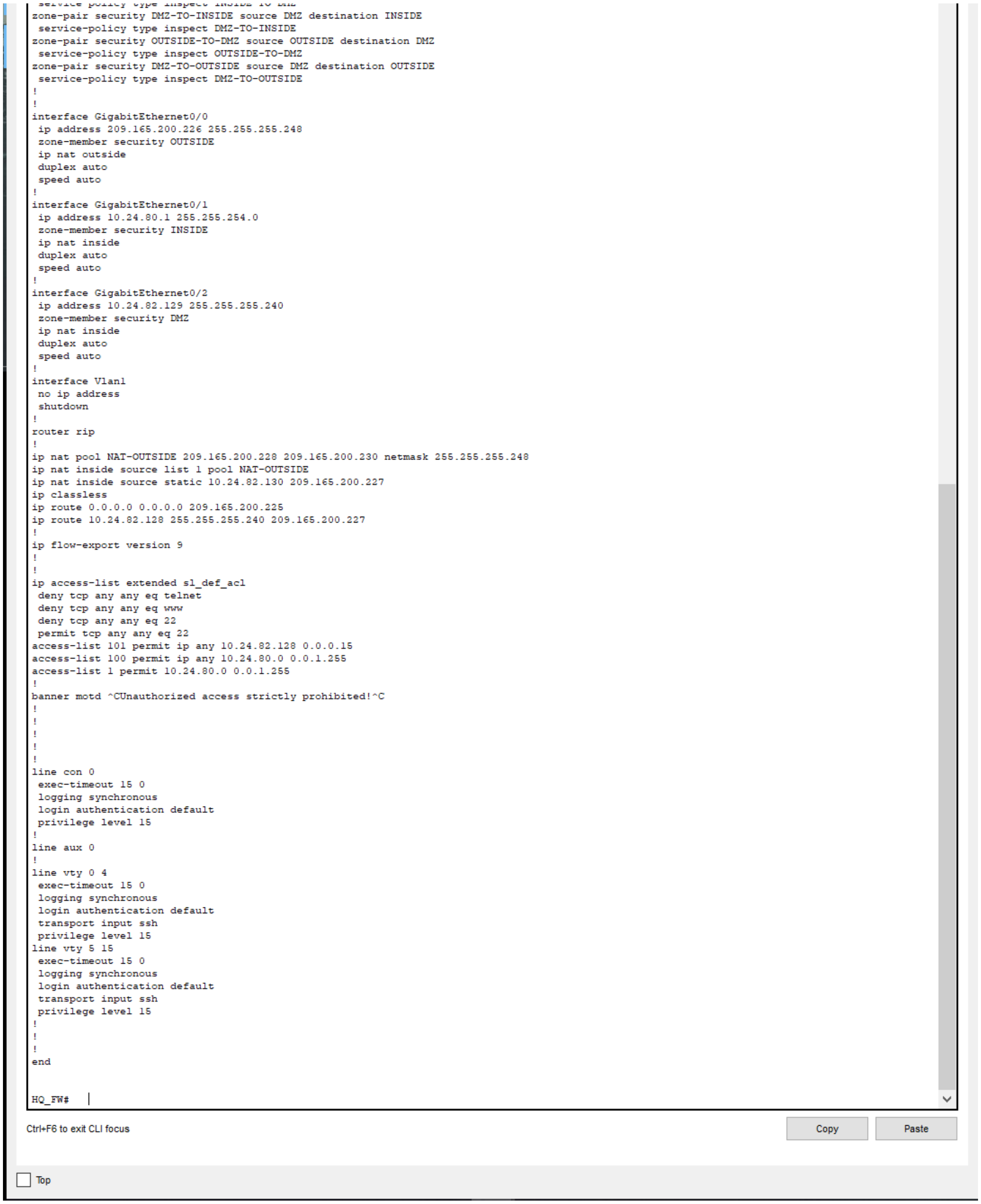


```
logging trap debugging
line con 0
 transport output telnet
 exec-timeout 5 0
 logging synchronous
 login authentication default
 privilege level 15
!
line aux 0
!
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login authentication default
 transport input ssh
 privilege level 15
line vty 5 15
 exec-timeout 15 0
 logging synchronous
 login authentication default
 transport input ssh
 privilege level 15
!
!
ntp authentication-key 1 md5 080F787E1918160405041E00 7
ntp authenticate
ntp trusted-key 1
ntp server 165.16.36.10 key 1
ntp update-calendar
!
end


HQ#
```

2. HQ_FW ROUTER

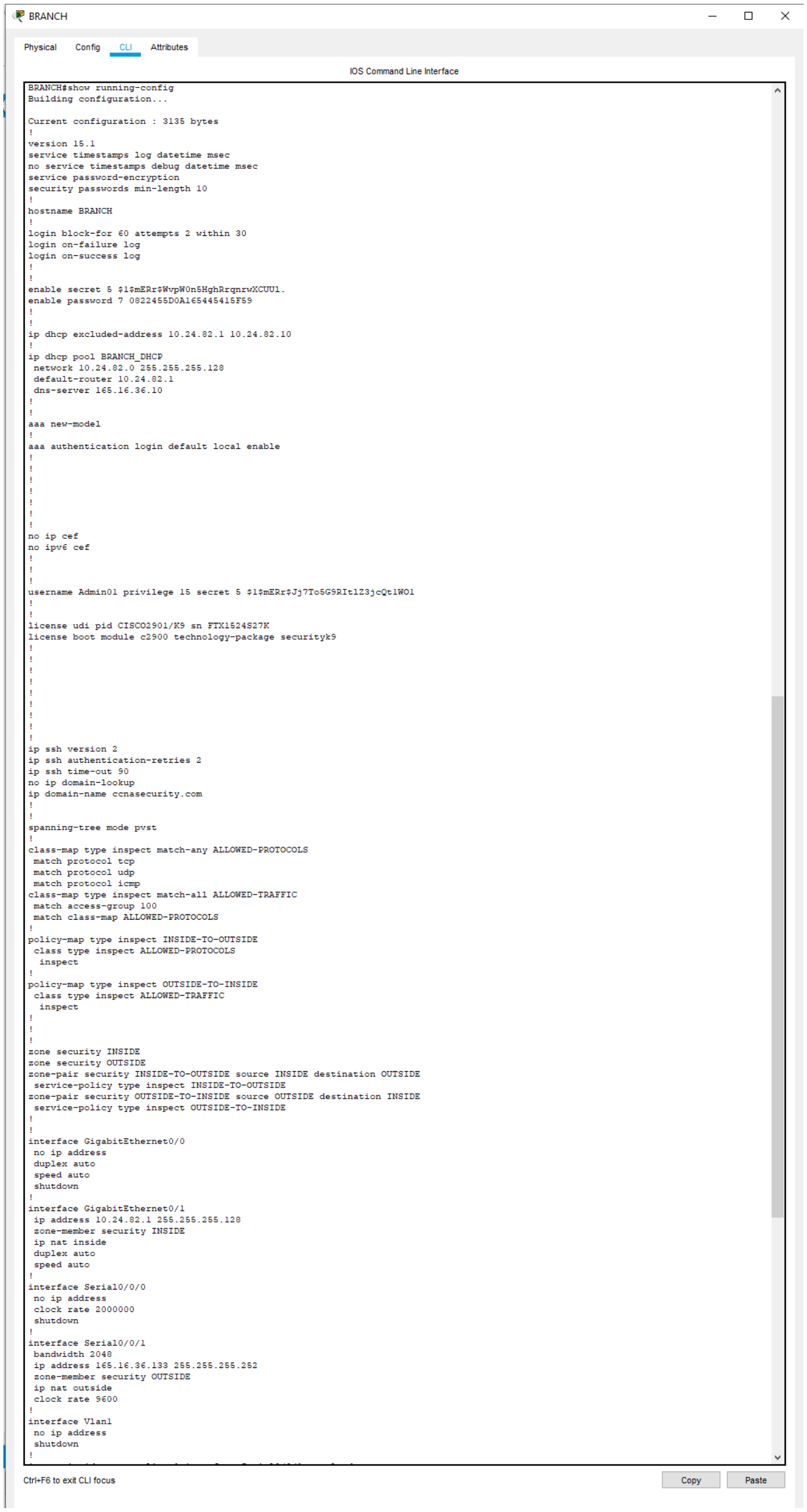


```
HQ_FW#en
HQ_FW#show running-config
Building configuration...

Current configuration : 4163 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname HQ_FW
!
login block-for 60 attempts 2 within 30
login on-failure log
login on-success log
!
!
enable secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUU1.
enable password 7 0822455D0A165445415F59
!
!
ip dhcp excluded-address 10.24.80.1 10.24.80.10
!
ip dhcp pool HQ_LAN
 network 10.24.80.0 255.255.254.0
 default-router 10.24.80.1
 dns-server 10.24.82.130
!
!
aaa new-model
!
aaa authentication login default local enable
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username Admin01 privilege 15 secret 5 $1$mERr$Jj7To5G9RItlZ3jcQtlWO1
!
!
license udi pid CISCO2911/K9 sn FTX15247R2Y
license boot module c2900 technology-package securityk9
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 90
no ip domain-lookup
ip domain-name ccnasecurity.com
!
!
spanning-tree mode pvst
!
class-map type inspect match-any ALLOWED-PROTOCOLS
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-all ALLOWED-INSIDE-TRAFFIC
 match class-map ALLOWED-PROTOCOLS
 match access-group 100
class-map type inspect match-all ALLOWED-DMZ-TRAFFIC
 match class-map ALLOWED-PROTOCOLS
 match access-group 101
!
policy-map type inspect INSIDE-TO-DMZ
 class type inspect ALLOWED-PROTOCOLS
  inspect
!
policy-map type inspect DMZ-TO-INSIDE
 class type inspect ALLOWED-INSIDE-TRAFFIC
  inspect
!
policy-map type inspect INSIDE-TO-OUTSIDE
 class type inspect ALLOWED-PROTOCOLS
  inspect
!
policy-map type inspect OUTSIDE-TO-INSIDE
 class type inspect ALLOWED-INSIDE-TRAFFIC
  inspect
!
policy-map type inspect OUTSIDE-TO-DMZ
 class type inspect ALLOWED-DMZ-TRAFFIC
  inspect
 class type inspect ALLOWED-PROTOCOLS
  inspect
!
policy-map type inspect DMZ-TO-OUTSIDE
 class type inspect ALLOWED-PROTOCOLS
  inspect
!
!
!
zone security INSIDE
zone security OUTSIDE
zone security DMZ
zone-pair security INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE-TO-OUTSIDE
zone-pair security OUTSIDE-TO-INSIDE source OUTSIDE destination INSIDE
 service-policy type inspect OUTSIDE-TO-INSIDE
zone-pair security INSIDE-TO-DMZ source INSIDE destination DMZ
 service-policy type inspect INSIDE-TO-DMZ
zone-pair security DMZ-TO-INSIDE source DMZ destination INSIDE
```

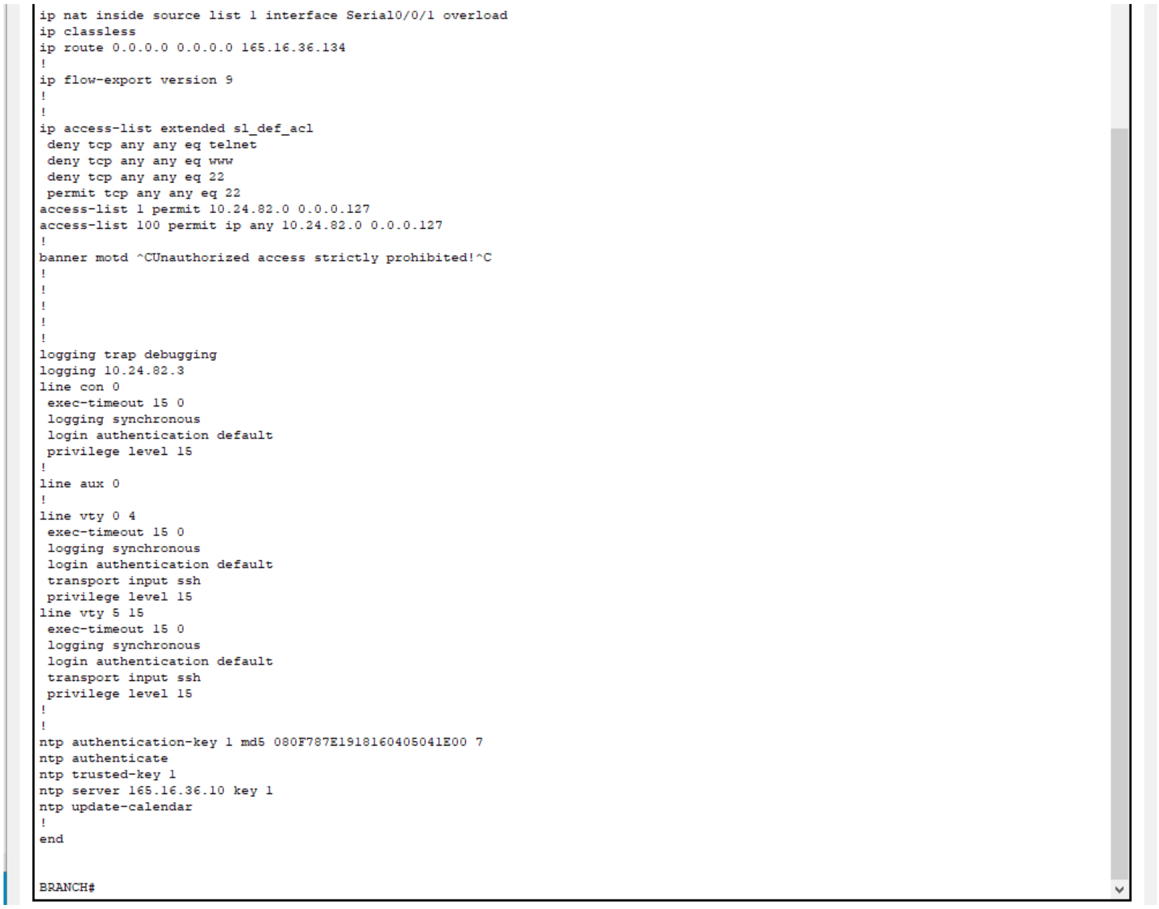


```
 service-policy type inspect INSIDE-TO-DMZ
zone-pair security DMZ-TO-INSIDE source DMZ destination INSIDE
 service-policy type inspect DMZ-TO-INSIDE
zone-pair security OUTSIDE-TO-DMZ source OUTSIDE destination DMZ
 service-policy type inspect OUTSIDE-TO-DMZ
zone-pair security DMZ-TO-OUTSIDE source DMZ destination OUTSIDE
 service-policy type inspect DMZ-TO-OUTSIDE
!
!
interface GigabitEthernet0/0
 ip address 209.165.200.226 255.255.255.248
 zone-member security OUTSIDE
 ip nat outside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.24.80.1 255.255.254.0
 zone-member security INSIDE
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 10.24.82.129 255.255.255.240
 zone-member security DMZ
 ip nat inside
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router rip
!
ip nat pool NAT-OUTSIDE 209.165.200.228 209.165.200.230 netmask 255.255.255.248
ip nat inside source list 1 pool NAT-OUTSIDE
ip nat inside source static 10.24.82.130 209.165.200.227
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.225
ip route 10.24.82.128 255.255.255.240 209.165.200.227
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www
 deny tcp any any eq 22
 permit tcp any any eq 22
access-list 101 permit ip any 10.24.82.128 0.0.0.15
access-list 100 permit ip any 10.24.80.0 0.0.1.255
access-list 1 permit 10.24.80.0 0.0.1.255
!
banner motd ^CUnauthorized access strictly prohibited!^C
!
!
!
!
!
line con 0
 exec-timeout 15 0
 logging synchronous
 login authentication default
 privilege level 15
!
line aux 0
!
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login authentication default
 transport input ssh
 privilege level 15
line vty 5 15
 exec-timeout 15 0
 logging synchronous
 login authentication default
 transport input ssh
 privilege level 15
!
!
!
end


HQ_FW#
```

3. BRANCH ROUTER

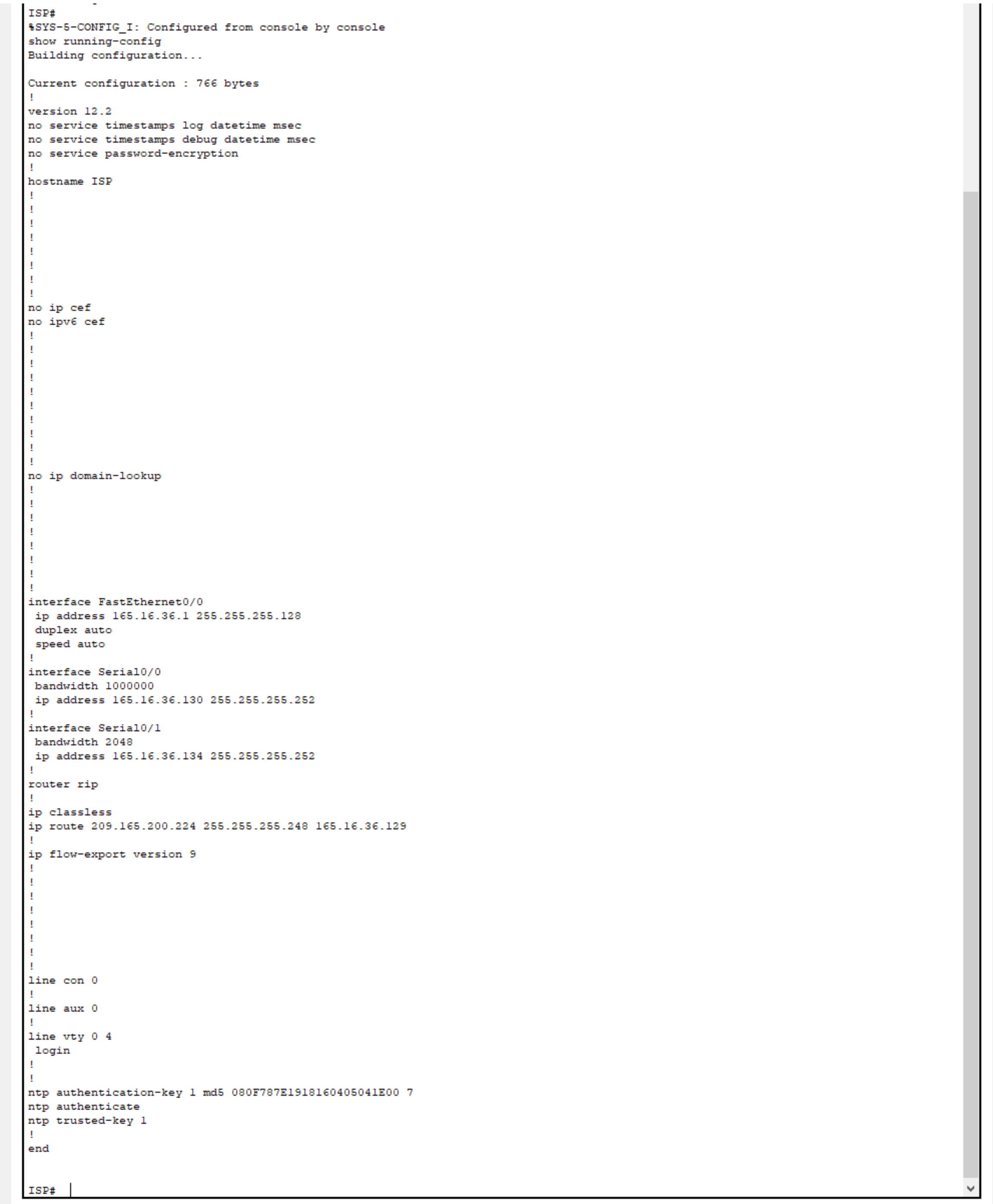


```
BRANCH#show running-config
Building configuration...

Current configuration : 3135 bytes
!
version 15.1
service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname BRANCH
!
login block-for 60 attempts 2 within 30
login on-failure log
login on-success log
!
!
enable secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUUl.
enable password 7 0822455D0A165445415F59
!
!
ip dhcp excluded-address 10.24.82.1 10.24.82.10
!
ip dhcp pool BRANCH_DHCP
 network 10.24.82.0 255.255.255.128
 default-router 10.24.82.1
 dns-server 165.16.36.10
!
!
aaa new-model
!
aaa authentication login default local enable
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username Admin01 privilege 15 secret 5 $1$mERr$Jj7To5G9RItlZ3jcQtlWO1
!
!
license udi pid CISCO2901/K9 sn FTX1524S27K
license boot module c2900 technology-package securityk9
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 90
no ip domain-lookup
ip domain-name ccnasecurity.com
!
!
spanning-tree mode pvst
!
class-map type inspect match-any ALLOWED-PROTOCOLS
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-all ALLOWED-TRAFFIC
 match access-group 100
 match class-map ALLOWED-PROTOCOLS
!
policy-map type inspect INSIDE-TO-OUTSIDE
 class type inspect ALLOWED-PROTOCOLS
  inspect
!
policy-map type inspect OUTSIDE-TO-INSIDE
 class type inspect ALLOWED-TRAFFIC
  inspect
!
!
!
zone security INSIDE
zone security OUTSIDE
zone-pair security INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE-TO-OUTSIDE
zone-pair security OUTSIDE-TO-INSIDE source OUTSIDE destination INSIDE
 service-policy type inspect OUTSIDE-TO-INSIDE
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 ip address 10.24.82.1 255.255.255.128
 zone-member security INSIDE
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 bandwidth 2048
 ip address 165.16.36.133 255.255.255.252
 zone-member security OUTSIDE
 ip nat outside
 clock rate 9600
!
interface Vlan1
 no ip address
 shutdown
!
```



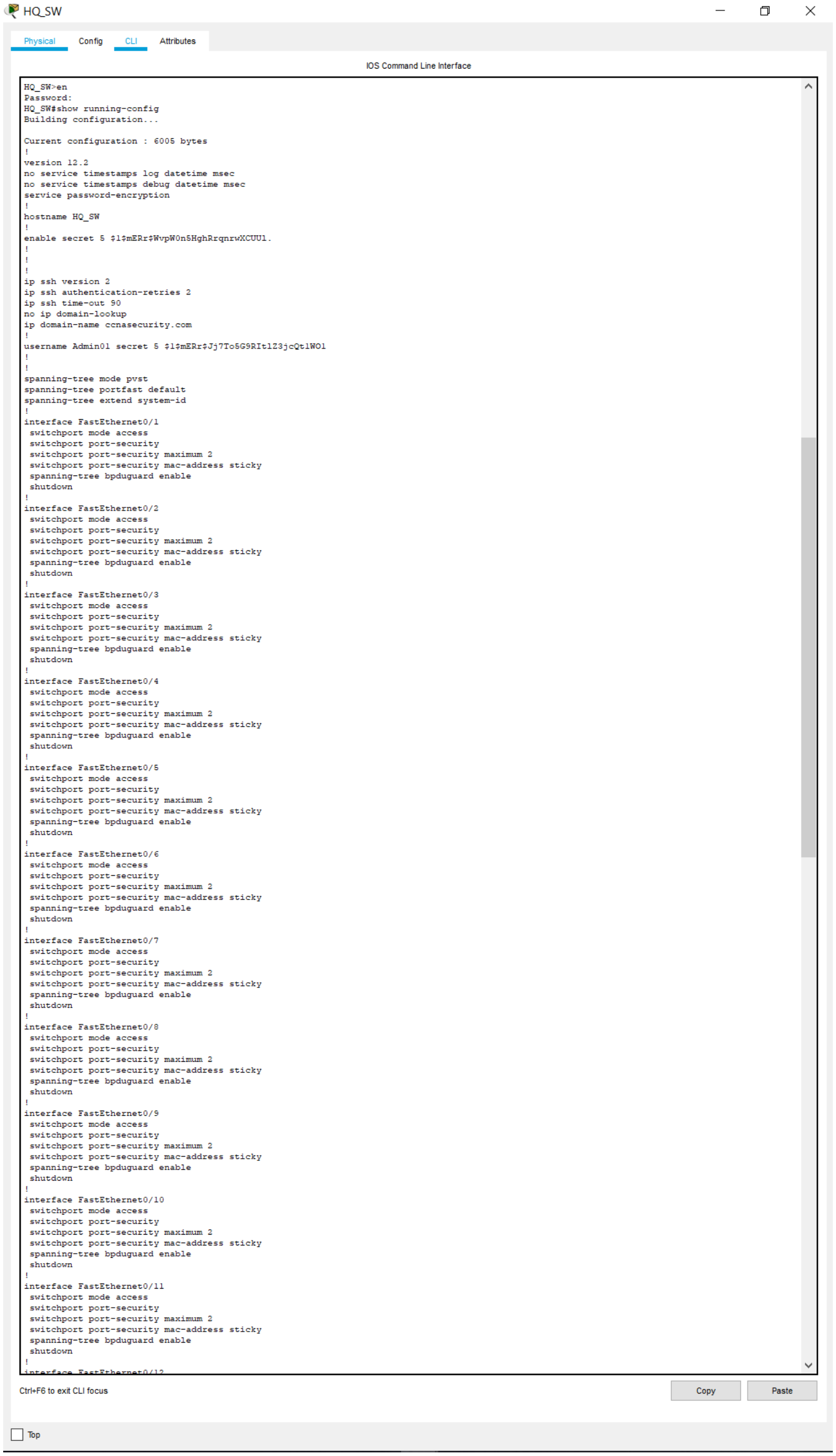
```
ip nat inside source list 1 interface Serial0/0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 165.16.36.134
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www
 deny tcp any any eq 22
 permit tcp any any eq 22
access-list 1 permit 10.24.82.0 0.0.0.127
access-list 100 permit ip any 10.24.82.0 0.0.0.127
!
banner motd ^CUnauthorized access strictly prohibited!^C
!
!
!
!
!
logging trap debugging
logging 10.24.82.3
line con 0
 exec-timeout 15 0
 logging synchronous
 login authentication default
 privilege level 15
!
line aux 0
!
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login authentication default
 transport input ssh
 privilege level 15
line vty 5 15
 exec-timeout 15 0
 logging synchronous
 login authentication default
 transport input ssh
 privilege level 15
!
!
ntp authentication-key 1 md5 080F787E1918160405041E00 7
ntp authenticate
ntp trusted-key 1
ntp server 165.16.36.10 key 1
ntp update-calendar
!
end


BRANCH#
```

4. ISP ROUTER

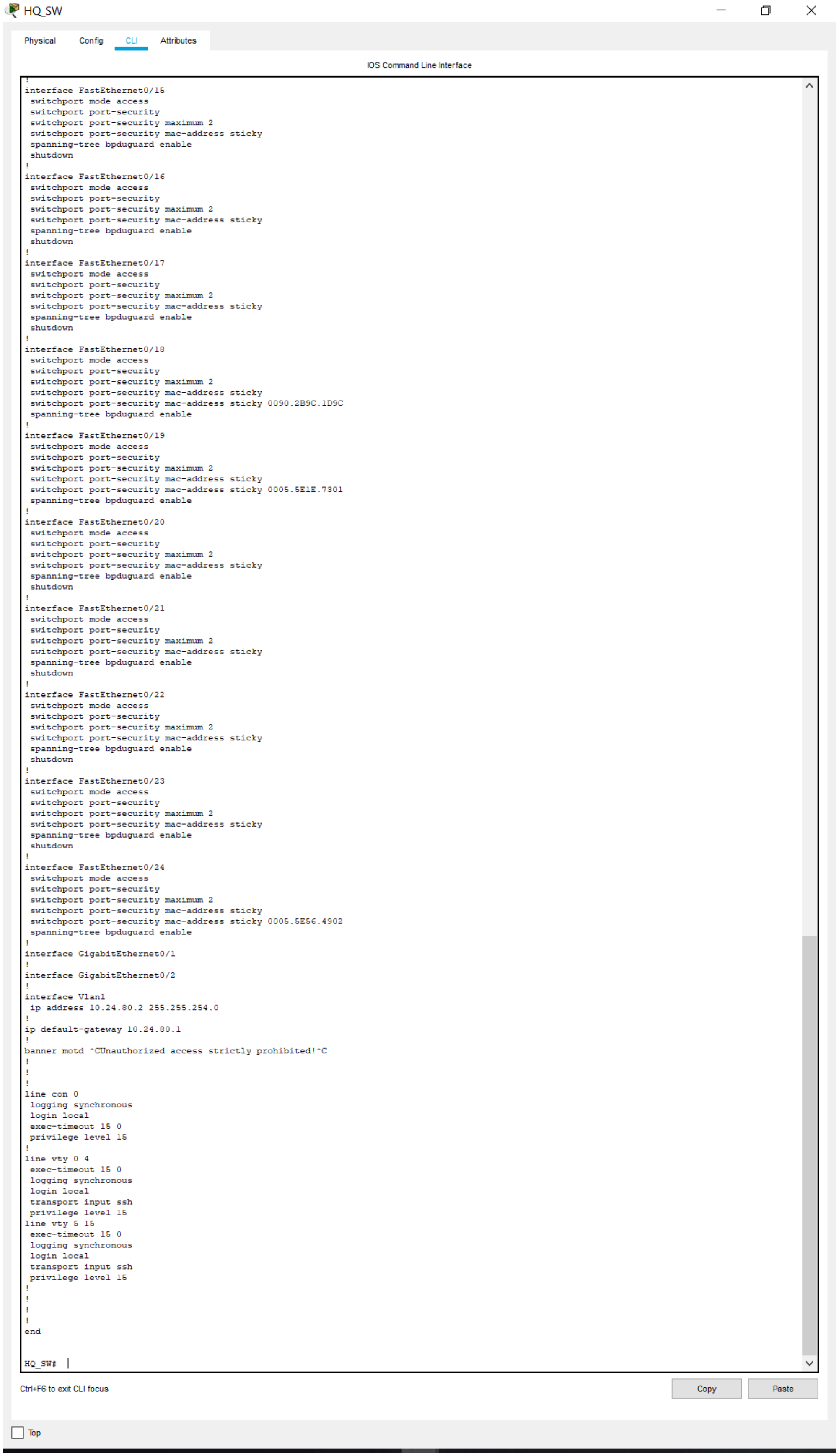


```
ISP#
%SYS-5-CONFIG_I: Configured from console by console
show running-config
Building configuration...

Current configuration : 766 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ISP
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 165.16.36.1 255.255.255.128
 duplex auto
 speed auto
!
interface Serial0/0
 bandwidth 1000000
 ip address 165.16.36.130 255.255.255.252
!
interface Serial0/1
 bandwidth 2048
 ip address 165.16.36.134 255.255.255.252
!
router rip
!
ip classless
ip route 209.165.200.224 255.255.255.248 165.16.36.129
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
ntp authentication-key 1 md5 080F787E1918160405041E00 7
ntp authenticate
ntp trusted-key 1
!
end


ISP#
```

5. HQ SWITCH

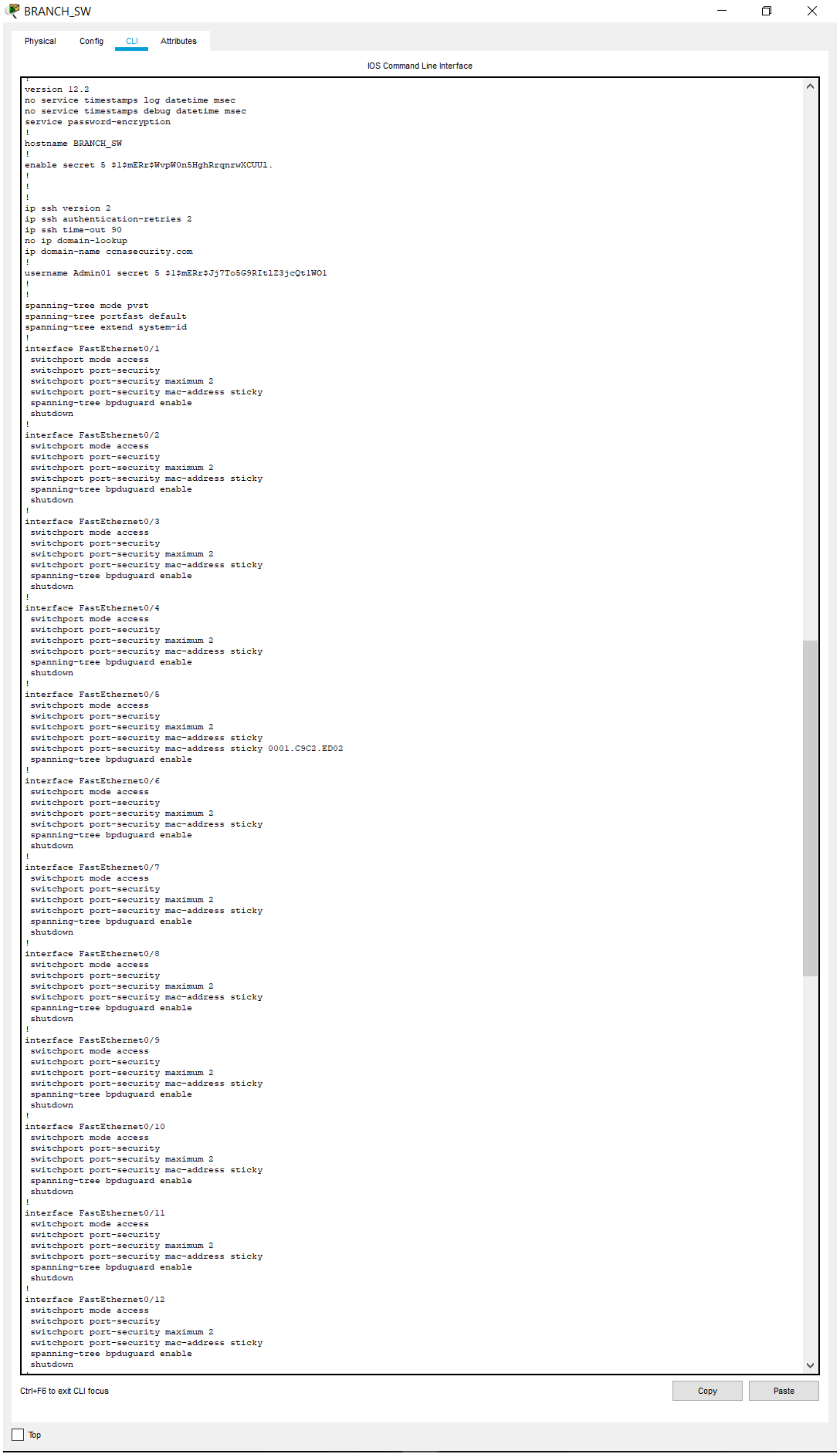


```
HQ_SW>en
Password:
HQ_SW#show running-config
Building configuration...

Current configuration : 6005 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname HQ_SW
!
enable secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUU1.
!
!
!
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 90
no ip domain-lookup
ip domain-name ccnasecurity.com
!
username Admin01 secret 5 $1$mERr$Jj7To5G9RItlZ3jcQtlWO1
!
!
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/3
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/4
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/6
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/7
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/8
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/9
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/10
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/11
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/12
```

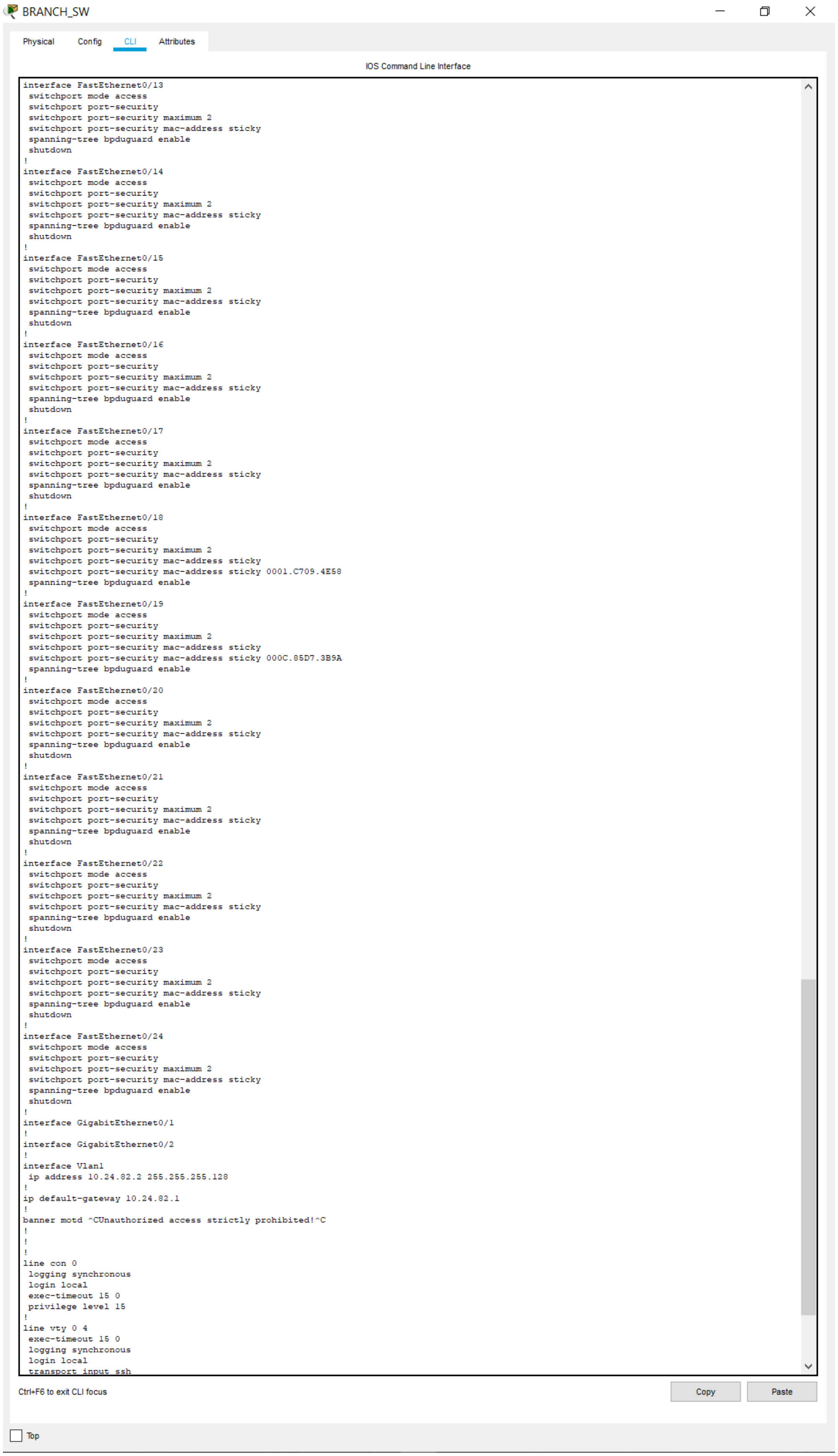


```
!
interface FastEthernet0/15
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/16
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/17
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/18
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0090.2B9C.1D9C
 spanning-tree bpduguard enable
!
interface FastEthernet0/19
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0005.5E1E.7301
 spanning-tree bpduguard enable
!
interface FastEthernet0/20
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/21
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/22
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/23
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/24
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0005.5E56.4902
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 10.24.80.2 255.255.254.0
!
ip default-gateway 10.24.80.1
!
banner motd ^CUnauthorized access strictly prohibited!^C
!
!
!
line con 0
 logging synchronous
 login local
 exec-timeout 15 0
 privilege level 15
!
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login local
 transport input ssh
 privilege level 15
line vty 5 15
 exec-timeout 15 0
 logging synchronous
 login local
 transport input ssh
 privilege level 15
!
!
!
!
end


HQ_SW#
```

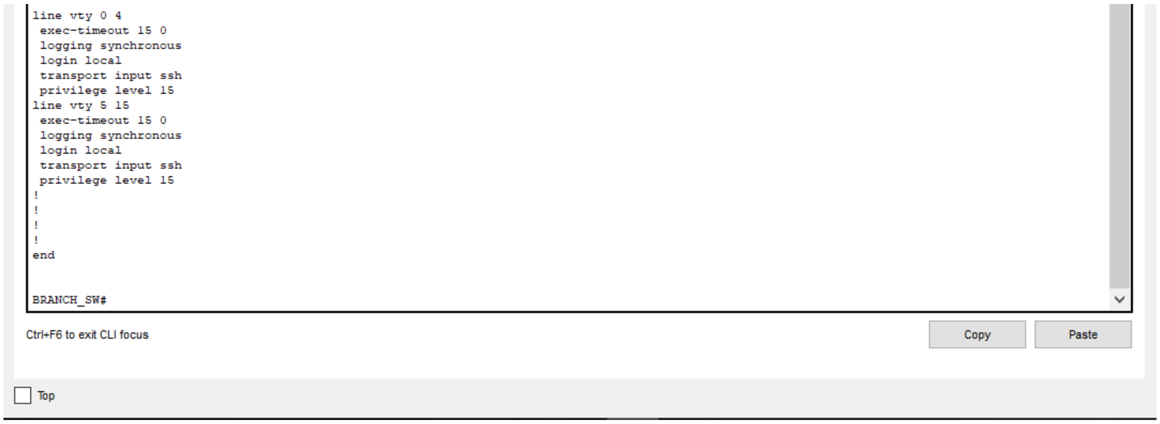
6. BRANCH SWITCH



```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname BRANCH_SW
!
enable secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUU1.
!
!
!
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 90
no ip domain-lookup
ip domain-name ccnasecurity.com
!
username Admin01 secret 5 $1$mERr$Jj7To5G9RItlZ3jcQtlWO1
!
!
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/3
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/4
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.C9C2.ED02
 spanning-tree bpduguard enable
!
interface FastEthernet0/6
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/7
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/8
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/9
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/10
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/11
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/12
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
```

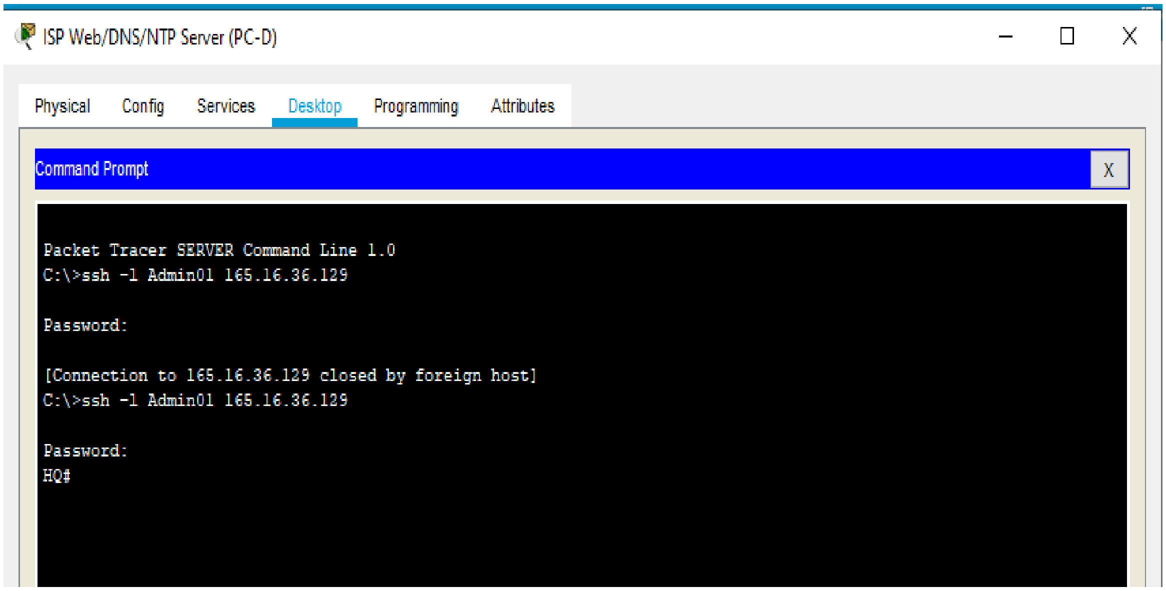


```
interface FastEthernet0/13
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/14
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/15
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/16
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/17
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/18
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.C709.4E58
 spanning-tree bpduguard enable
!
interface FastEthernet0/19
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000C.85D7.3B9A
 spanning-tree bpduguard enable
!
interface FastEthernet0/20
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/21
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/22
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/23
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/24
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
 shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 10.24.82.2 255.255.255.128
!
ip default-gateway 10.24.82.1
!
banner motd ^CUnauthorized access strictly prohibited!^C
!
!
!
line con 0
 logging synchronous
 login local
 exec-timeout 15 0
 privilege level 15
!
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login local
 transport input ssh
```



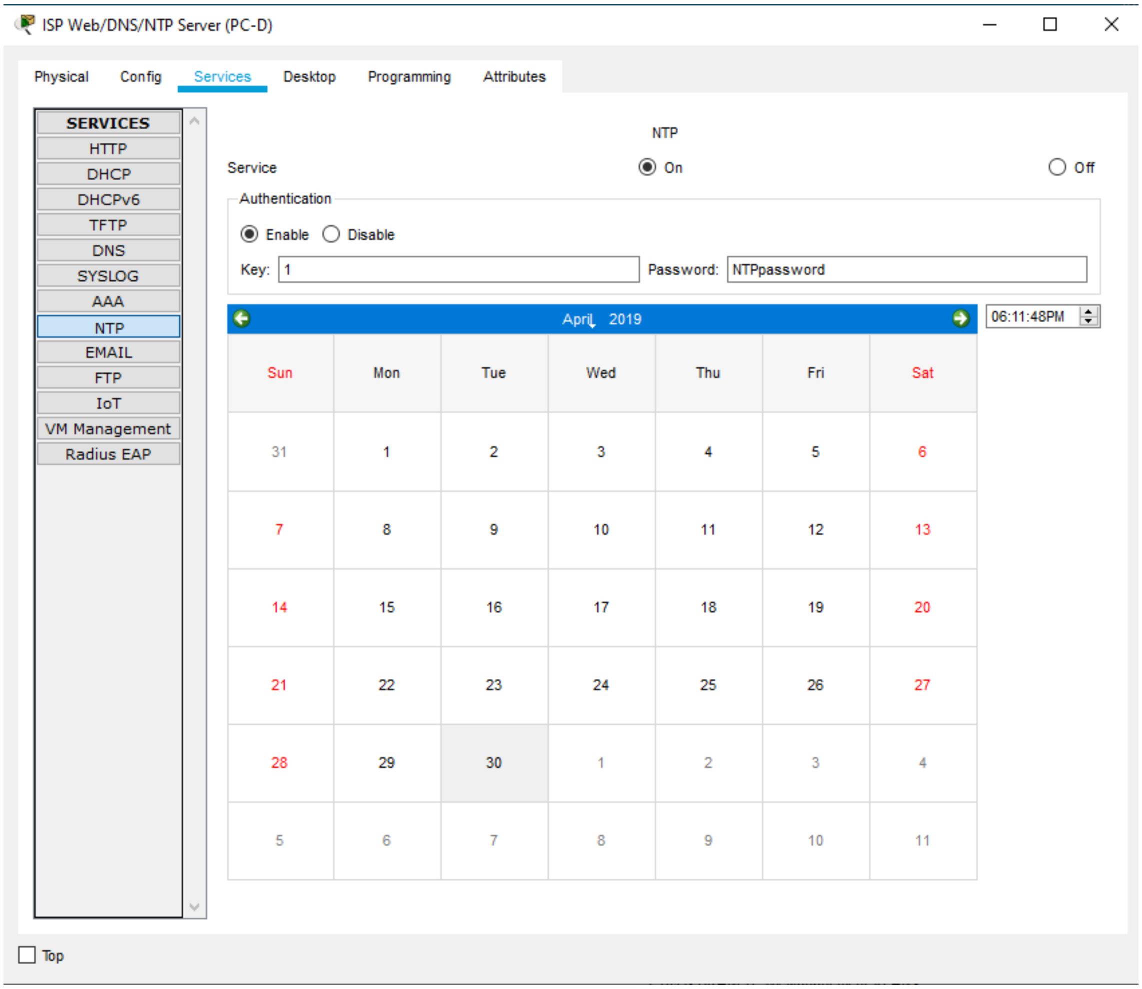
```
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login local
 transport input ssh
 privilege level 15
line vty 5 15
 exec-timeout 15 0
 logging synchronous
 login local
 transport input ssh
 privilege level 15
!
!
!
!
end

BRANCH_SW#
```

7. HQ ROUTER SCREENSHOTS TO BE DISPLAY SHH CONNECTION:



```
Packet Tracer SERVER Command Line 1.0
C:\>ssh -l Admin01 165.16.36.129

Password:

[Connection to 165.16.36.129 closed by foreign host]
C:\>ssh -l Admin01 165.16.36.129

Password:
HQ#
```

NTP MASTER CONFIG:



NTP

Service ● On ○ Off

Authentication

● Enable ○ Disable

Key: 1

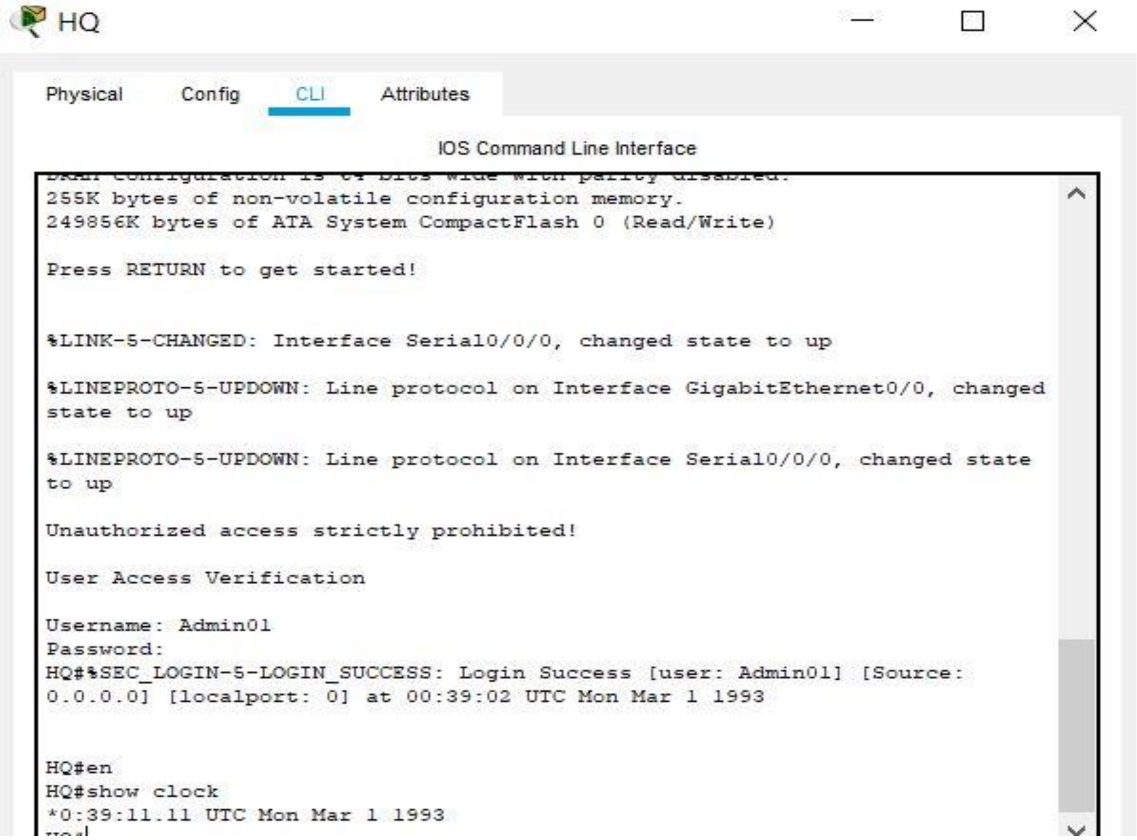
Password: NTPpassword

April 2019

06:11:48PM

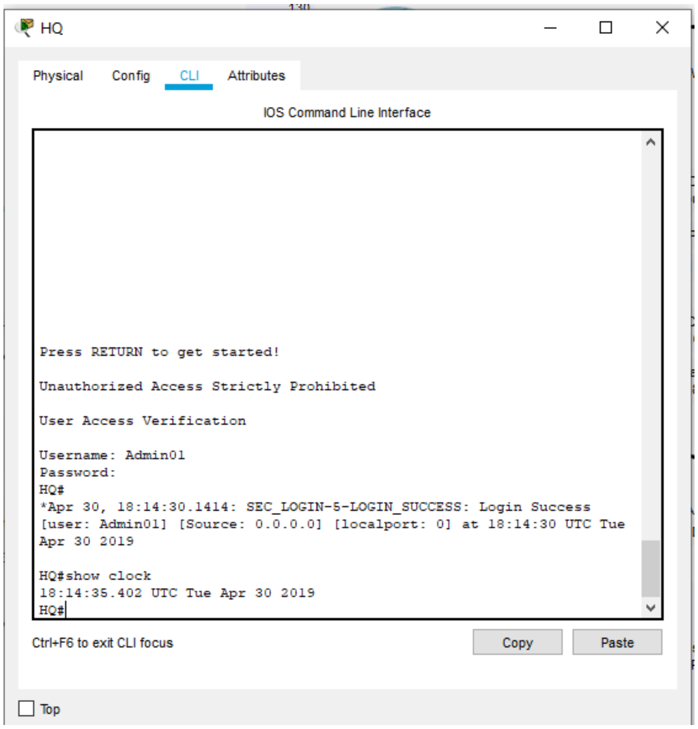
Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

DATE AND TIME BEFORE NTP:



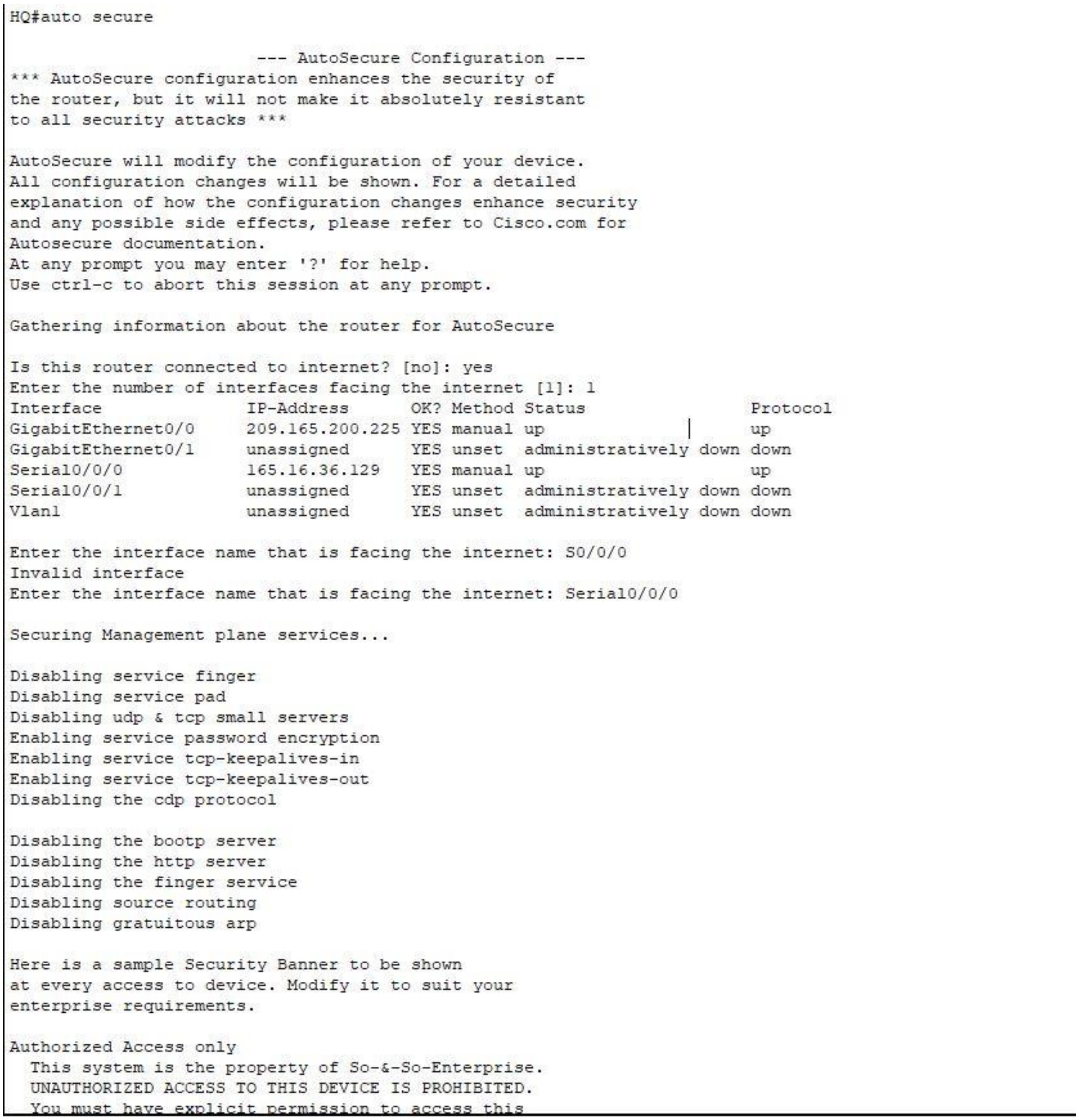
```
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up

Unauthorized access strictly prohibited!

User Access Verification

Username: Admin01
Password:
HQ#%SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Admin01] [Source:
0.0.0.0] [localport: 0] at 00:39:02 UTC Mon Mar 1 1993


HQ#en
HQ#show clock
*0:39:11.11 UTC Mon Mar 1 1993
HQ#
```

NEW NTP TIMING:

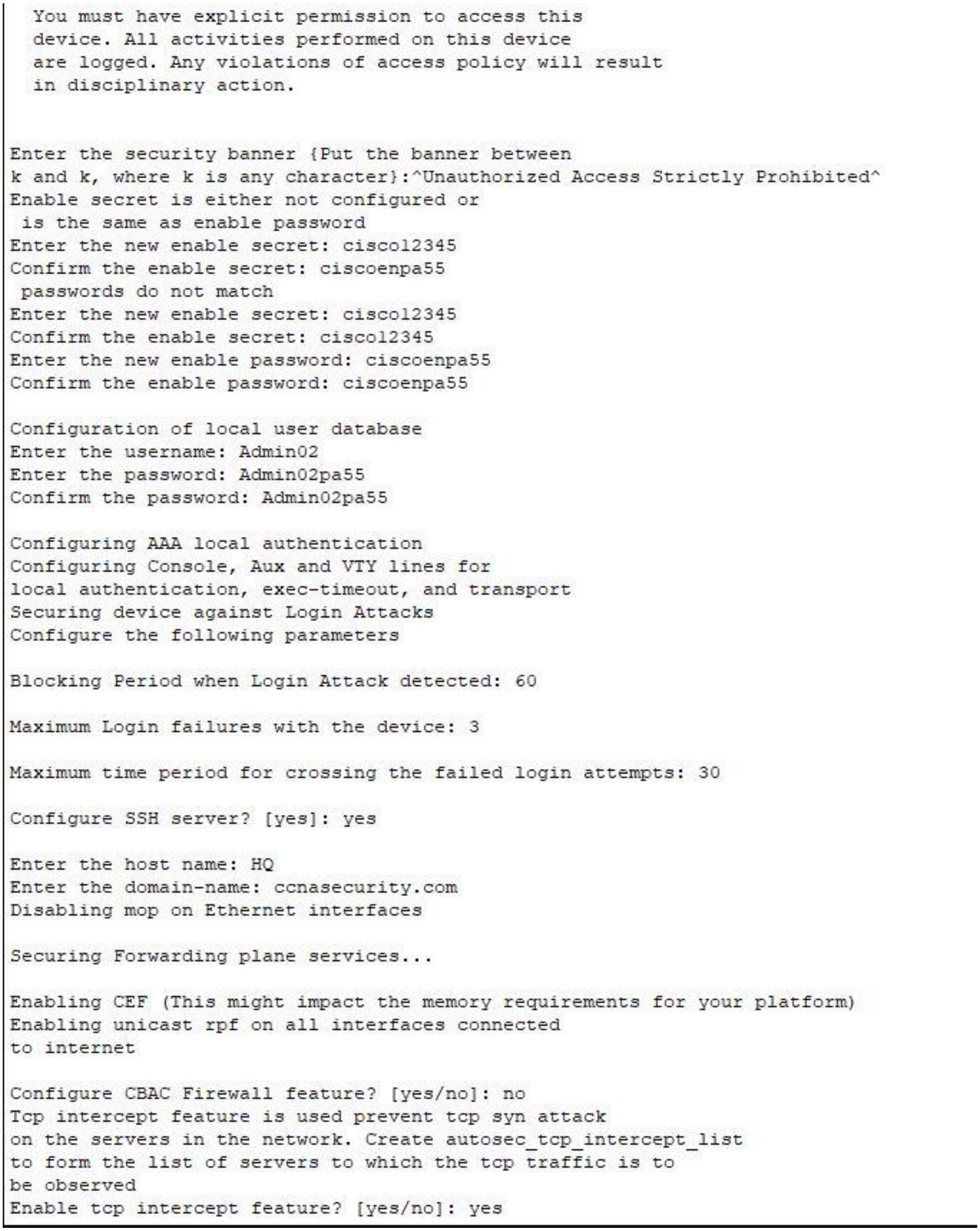


```
Press RETURN to get started!

Unauthorized Access Strictly Prohibited

User Access Verification

Username: Admin01
Password:
HQ#
*Apr 30, 18:14:30.1414: SEC_LOGIN-5-LOGIN_SUCCESS: Login Success
[user: Admin01] [Source: 0.0.0.0] [localport: 0] at 18:14:30 UTC Tue
Apr 30 2019

HQ#show clock
18:14:35.402 UTC Tue Apr 30 2019
HQ#
```

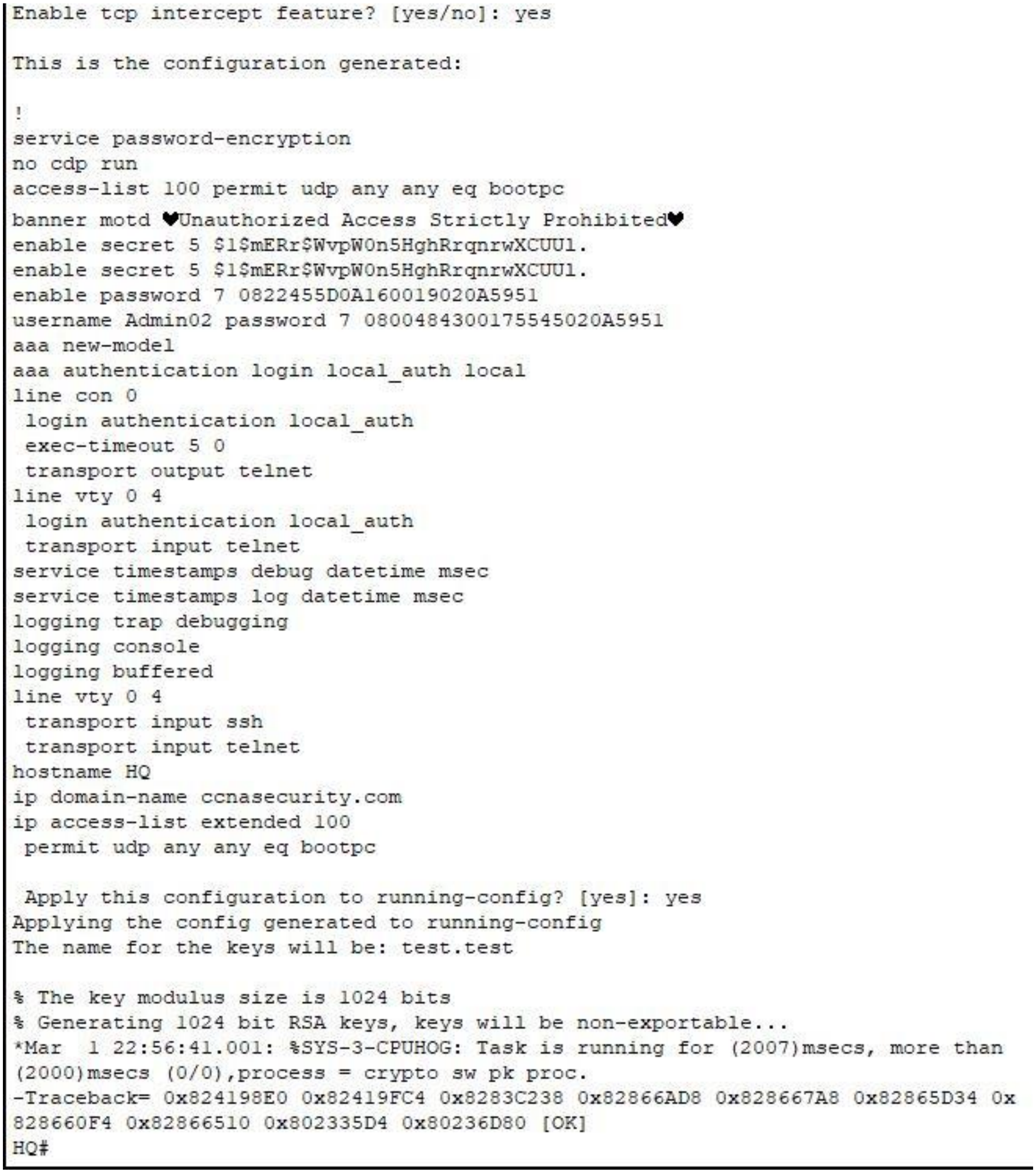
AUTO SECURE CONFIGURATION:



```
HQ#auto secure

                        --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: 1
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     209.165.200.225 YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            165.16.36.129   YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down

Enter the interface name that is facing the internet: S0/0/0
Invalid interface
Enter the interface name that is facing the internet: Serial0/0/0

Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
  This system is the property of So-&-So-Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
```

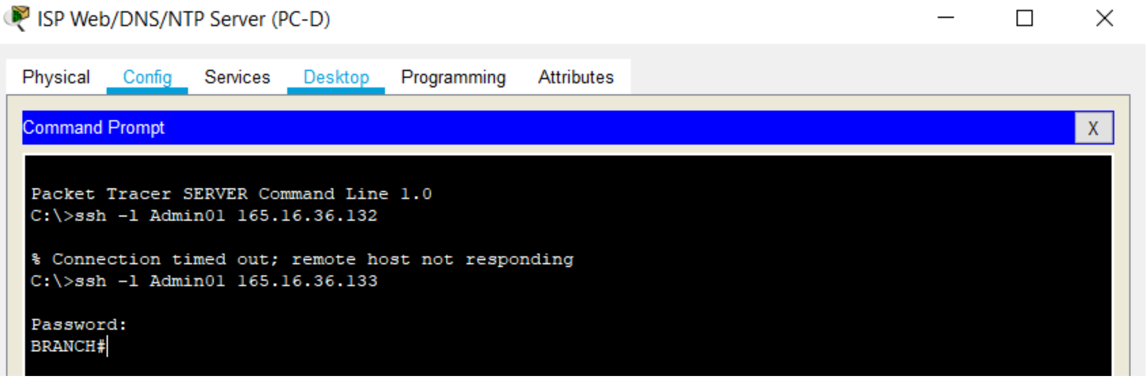


```
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.


Enter the security banner {Put the banner between
k and k, where k is any character}:^Unauthorized Access Strictly Prohibited^
Enable secret is either not configured or
 is the same as enable password
Enter the new enable secret: cisco12345
Confirm the enable secret: ciscoenpa55
 passwords do not match
Enter the new enable secret: cisco12345
Confirm the enable secret: cisco12345
Enter the new enable password: ciscoenpa55
Confirm the enable password: ciscoenpa55

Configuration of local user database
Enter the username: Admin02
Enter the password: Admin02pa55
Confirm the password: Admin02pa55

Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 60

Maximum Login failures with the device: 3

Maximum time period for crossing the failed login attempts: 30

Configure SSH server? [yes]: yes

Enter the host name: HQ
Enter the domain-name: ccnasecurity.com
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected
to internet

Configure CBAC Firewall feature? [yes/no]: no
Tcp intercept feature is used prevent tcp syn attack
on the servers in the network. Create autosec_tcp_intercept_list
to form the list of servers to which the tcp traffic is to
be observed
Enable tcp intercept feature? [yes/no]: yes
```



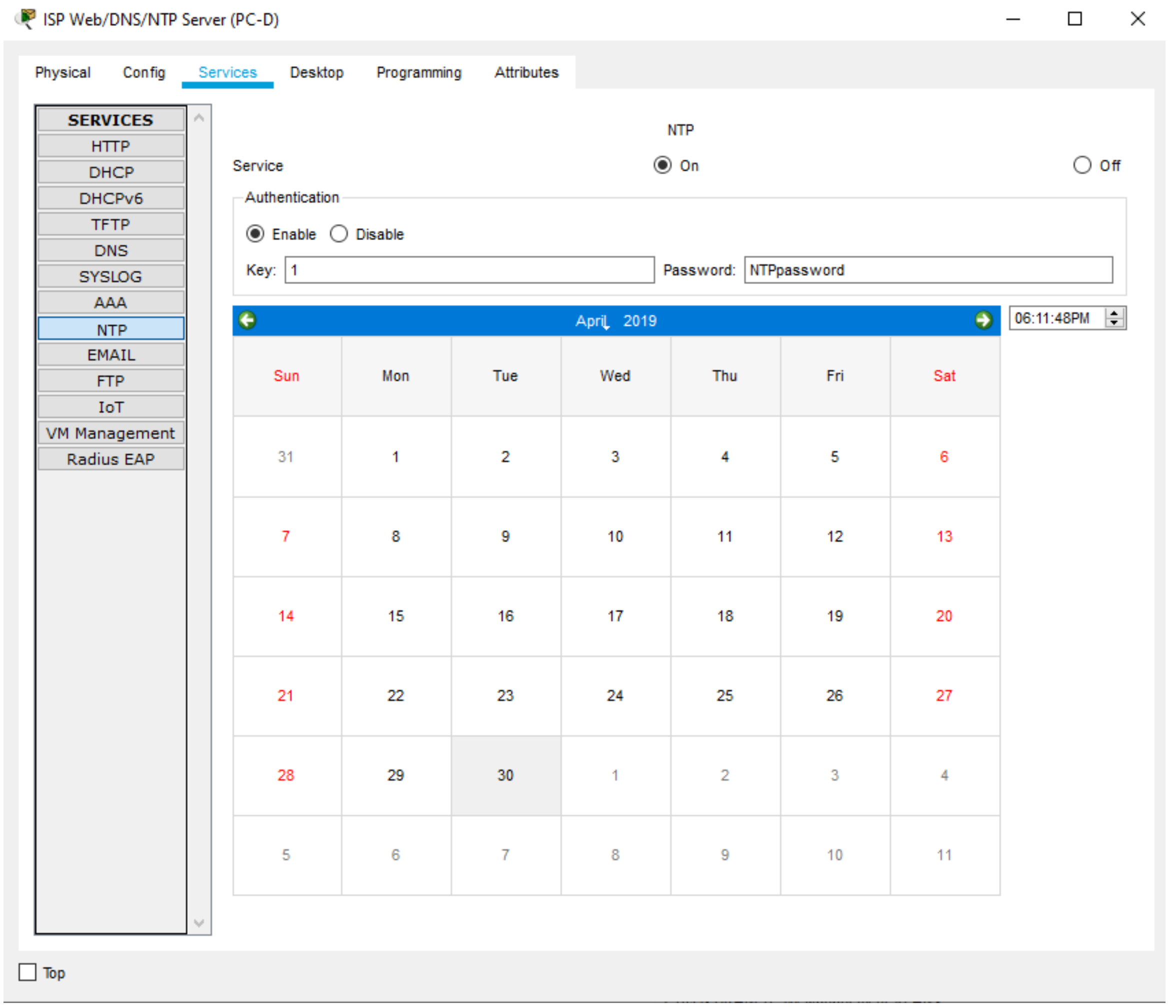
```
Enable tcp intercept feature? [yes/no]: yes

This is the configuration generated:

!
service password-encryption
no cdp run
access-list 100 permit udp any any eq bootpc
banner motd ♥Unauthorized Access Strictly Prohibited♥
enable secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUU1.
enable secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUU1.
enable password 7 0822455D0A160019020A5951
username Admin02 password 7 0800484300175545020A5951
aaa new-model
aaa authentication login local_auth local
line con 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
service timestamps debug datetime msec
service timestamps log datetime msec
logging trap debugging
logging console
logging buffered
line vty 0 4
 transport input ssh
 transport input telnet
hostname HQ
ip domain-name ccnasecurity.com
ip access-list extended 100
 permit udp any any eq bootpc

 Apply this configuration to running-config? [yes]: yes
Applying the config generated to running-config
The name for the keys will be: test.test

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
*Mar  1 22:56:41.001: %SYS-3-CPUHOG: Task is running for (2007)msecs, more than
(2000)msecs (0/0),process = crypto sw pk proc.
-Traceback= 0x824198E0 0x82419FC4 0x8283C238 0x82866AD8 0x828667A8 0x82865D34 0x
828660F4 0x82866510 0x802335D4 0x80236D80 [OK]
HQ#
```

8. SSH connection



```
Packet Tracer SERVER Command Line 1.0
C:\>ssh -l Admin01 165.16.36.132

% Connection timed out; remote host not responding
C:\>ssh -l Admin01 165.16.36.133

Password:
BRANCH#
```

NTP MASTER CONFIG



NTP

Service ● On ○ Off

Authentication

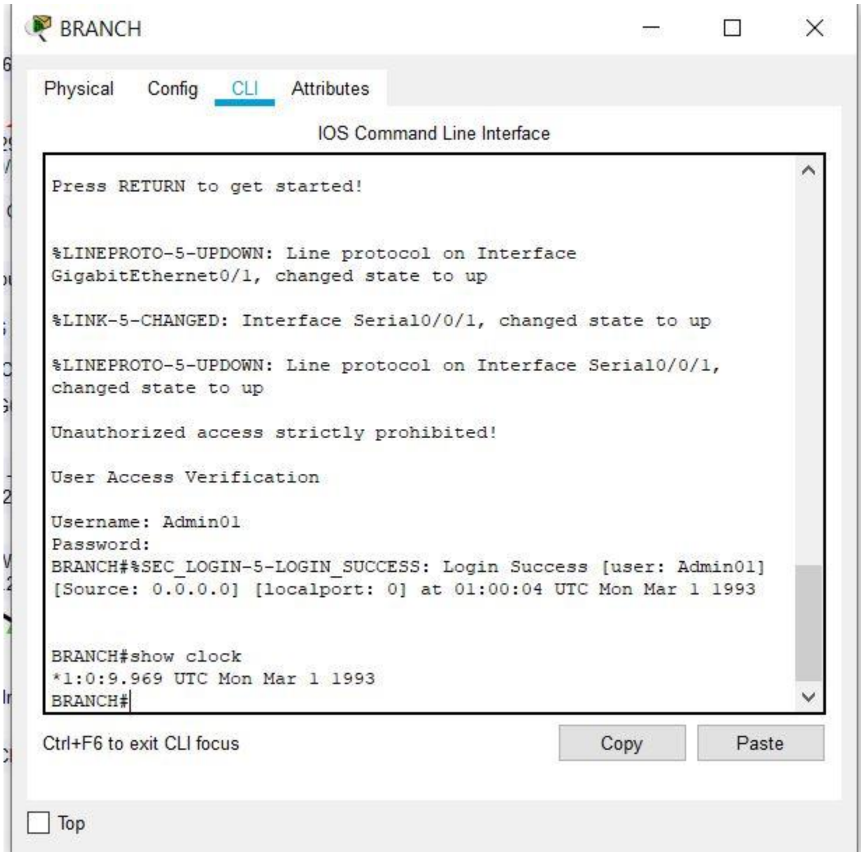
● Enable ○ Disable

Key: 1 Password: NTPpassword

April 2019 06:11:48PM

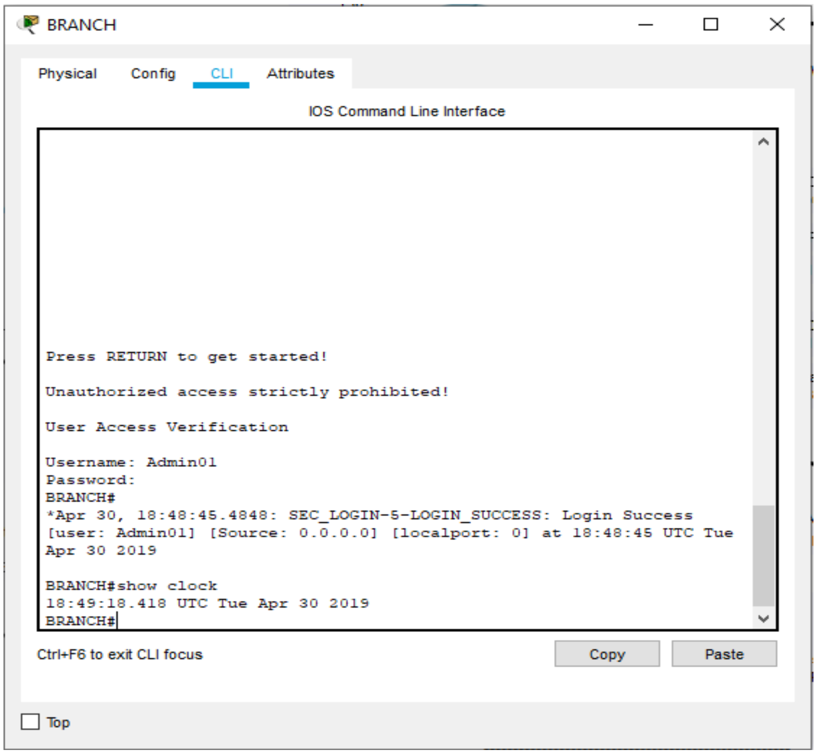
Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

ORGINAL TIMING BEFORE NTP



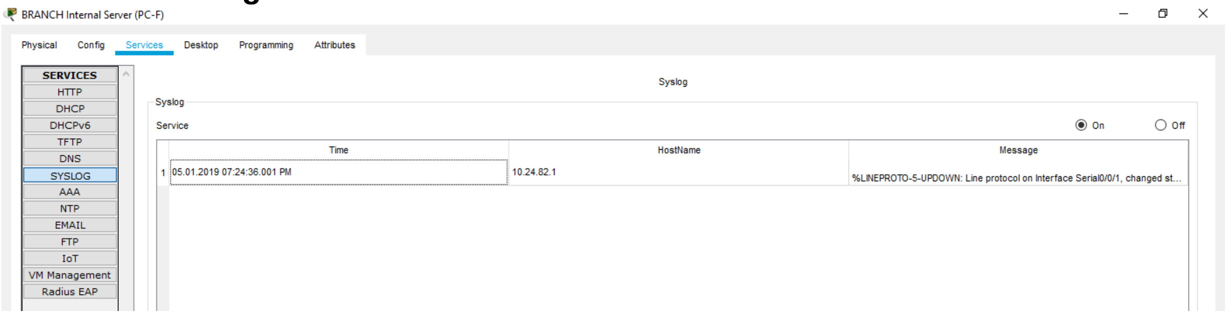
```
Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up

Unauthorized access strictly prohibited!

User Access Verification

Username: Admin01
Password:
BRANCH#%SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Admin01]
[Source: 0.0.0.0] [localport: 0] at 01:00:04 UTC Mon Mar 1 1993


BRANCH#show clock
*1:0:9.969 UTC Mon Mar 1 1993
BRANCH#
```

NEW TIMING WITH NTP



```
Press RETURN to get started!

Unauthorized access strictly prohibited!

User Access Verification

Username: Admin01
Password:
BRANCH#
*Apr 30, 18:48:45.4848: SEC_LOGIN-5-LOGIN_SUCCESS: Login Success
[user: Admin01] [Source: 0.0.0.0] [localport: 0] at 18:48:45 UTC Tue
Apr 30 2019

BRANCH#show clock
18:49:18.418 UTC Tue Apr 30 2019
BRANCH#
```

SYSLOG Message on Server



Syslog

Service ● On ○ Off

	Time	HostName	Message
1	05.01.2019 07:24:36.001 PM	10.24.82.1	%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed st...