Cisco Packet Analyzer Network: Project 1

Project Overview:

In this project, Cisco Packet Analyzer was used to build a comprehensive network setup, including configuration of IP addresses, subnets, VLANs, and essential services such as DHCP, DNS, and VOIP. The project also involved the implementation of basic security features like encrypted password account protection and port security.

Cisco Packet Analyzer Network File - network1.pkt

Key Skills Demonstrated:

- **Network Design & Configuration:**
  - Built a fully functional network, including configuration of IP address ranges, subnets, and VLANs.
  - Ensured efficient network segmentation and routing between different network segments.
  - Configured DHCP for automated IP address assignment.
- **Internet & Server Connectivity:**
  - Configured network elements for stable and secure internet access.
  - Set up and connected web servers and DNS to ensure proper network resolution and hosting.
- **Security Implementation:**
  - Set-up Encrypted Password Protection
  - Designated Account Privileges
  - Configured Port Security
  - Implemented VPN for remote access to the network, ensuring secure communication channels for remote workers.
- **Voice Over IP (VOIP):**
  - Configured VOIP for network communication, enabling effective voice communication across the network.

Technical Steps Taken:

- **Designed a base network and wired each device.**
- **Defined IP addresses and subnets and labeled each section of the network.**
- **Switch 1 Configuration for Trunk Link / VTP / VLAN**
    - **CLI**
        - enable
        - Terminal
        - Conf t
        - hostname SW1
        - interface range fastethernet 0/23 - 24
        - switchport mode trunk
        - [control + z]
        - Wr
        - Conf t
        - Vtp mode server
        - Vtp domain CISCO
        - Vtp password test
        - [control + z]
        - Wr
        - Conf t
        - Vlan 10
        - Name SALES
        - Exit
        - Vlan 20
        - Name RESEARCH
        - Exit
        - Vlan 30
        - Name MANAGEMENT
        - Exit
        - Vlan 40
        - Name SERVERS
        - [control + z]
        - Wr
        - Show vtp status
        - Show vlan brief
        - Conf t
        - interface range fastethernet 0/1 - 20
        - switchport mode access
        - Switchport access vlan 10
        - [control + z]
        - Wr

- **Switch 2 Configuration for Trunk Link**
    - **CLI**
        - enable
        - terminal
        - hostname SW1
        - interface range fastethernet 0/23 - 24
        - switchport mode trunk
        - [control + z]
        - Wr
        - Show vtp status
        - Conf t
        - Vtp password test
        - [control + z]
        - Wr
        - Conf t
        - interface range fastethernet 0/1 - 20
        - switchport mode access
        - Switchport access vlan 20
        - [control + z]
        - Wr

- **Switch 3 Configuration for Trunk Link**
    - **CLI**
        - enable
        - terminal
        - hostname SW3
        - interface range fastethernet 0/23 - 24
        - switchport mode trunk
        - [control + z]
        - Wr
        - Show vtp status
        - Conf t
        - Vtp password test
        - [control + z]
        - Wr
        - Conf t
        - interface range fastethernet 0/1 - 9
        - switchport mode access
        - Switchport access vlan 30
        - interface range fastethernet 0/10 - 20
        - switchport mode access
        - Switchport access vlan 40
        - [control + z]

        - Wr

- **Router Configuration for VLAN**
    - **CLI**
        - Enable
        - Conf t
        - Hostname R1
        - Interface fastethernet 0/0
        - No ip address
        - No shutdown
        - exit
        - Interface fastethernet 0/0.10
        - encapsulation dot1Q 10
        - ip address 172.16.10.254 255.255.255.0
        - exit
        - Interface fastethernet 0/0.20
        - encapsulation dot1Q 20
        - ip address 172.16.11.62 255.255.255.0
        - exit
        - Interface fastethernet 0/0.30
        - encapsulation dot1Q 30
        - ip address 172.16.11.94 255.255.255.0
        - exit
        - Interface fastethernet 0/0.40
        - encapsulation dot1Q 40
        - ip address 172.16.11.110 255.255.255.0
        - Exit
        - Wr
        - Show ip int brief

    - **Internal Server Configuration for Static IP**
        - Desktop > IP Configuration
        - Select Static
        - IPv4 Address: 172.16.11.97
        - Subnet Mask: 255.255.255.240
        - Default Gateway: 172.16.11.110
        - DNS Server: 10.10.10.1
        - Confirm by opening the Command Prompt
        - Ipconfig /all

- **DNS Server Configuration for Static IP**
  - Desktop > IP Configuration
  - Select Static
  - IPv4 Address: 10.10.10.1
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 10.10.10.254
  - DNS Server: 10.10.10.1
  - Confirm by opening the Command Prompt
  - Ipconfig /all

- **Configure ISP**
  - Open CLI
  - enable
  - conf t
  - hostname ISP
  - Interface fastethernet 0/0
  - ip add 10.10.10.254 255.255.255.0
  - No shutdown
  - Exit
  - Interface serial 0/0/1
  - Ip add 88.40.12.2 255.255.255.252
  - Clock rate 128000
  - Bandwidth 128
  - No shut
  - Ctrl + z
  - Wr
  - Sh ip int br

- **Configure Internal Router**
  - R1>enable
  - R1#conf t
  - Enter configuration commands, one per line. End with CNTL/Z.
  - R1(config)#int s0/0/0
  - R1(config-if)#ip add 88.40.12.1 255.255.255.252
  - R1(config-if)#bandw
  - R1(config-if)#bandwidth 128
  - R1(config-if)#no shut
  - Ctrl + z
  - Wr
  - Test connectivity using ping
  - Ping 88.40.12.2

- **Configuring DHCP for each Internal Subnet**
  - R1#conf t
  - Enter configuration commands, one per line. End with CNTL/Z.
  - R1(config)#ip dhcp pool VLAN10
  - R1(dhcp-config)#net
  - R1(dhcp-config)#network 172.16.10.0 255.255.255.0
  - R1(dhcp-config)#default-router 172.16.10.254
  - R1(dhcp-config)#dns
  - R1(dhcp-config)#dns-server 10.10.10.1
  - R1(dhcp-config)#exit
  - R1#conf t
  - Enter configuration commands, one per line. End with CNTL/Z.
  - R1(config)#ip dhcp pool VLAN20
  - R1(dhcp-config)#net
  - R1(dhcp-config)#network 172.16.11.0 255.255.255.192
  - R1(dhcp-config)#default-router 172.16.11.62
  - R1(dhcp-config)#dns
  - R1(dhcp-config)#dns-server 10.10.10.1
  - R1(dhcp-config)#exit
  - R1#conf t
  - Enter configuration commands, one per line. End with CNTL/Z.
  - R1(config)#ip dhcp pool VLAN30
  - R1(dhcp-config)#net
  - R1(dhcp-config)#network 172.16.11.64 255.255.255.224
  - R1(dhcp-config)#default-router 172.16.11.94
  - R1(dhcp-config)#dns
  - R1(dhcp-config)#dns-server 10.10.10.1
  - Ctrl + z
  - wr
  - Open PC0, PC1, and PC3
  - Go to Desktop > IP Configuration and select DHCP

- **Configure Wireless Access Point**
  - Click on AP
  - Go to Config Tab and change the SSID to SALES
  - Select WPA2-PSK
  - Set the PSK Pass Phase
  - Close and select the laptop to connect
  - Shutdown, Swap hardware to wireless, turn back on
  - Go to config tab and select WIRELESS
  - Change the SSID to SALES
  - Select WPA2-PSK and enter the pass phrase you chose earlier.

- **Ping testing**
  - Ping 172.16.10.1 (success)
  - Ping 172.16.11.65 (success)
  - Ping 10.10.10.1 (failure)

- **Configuring Default Static Route**
  - R1>enable
  - R1#conf t
  - Enter configuration commands, one per line. End with CNTL/Z.
  - R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
  - %Default route without gateway, if not a point-to-point interface, may impact performance
  - R1(config)#exit
  - R1#
  - %SYS-5-CONFIG_I: Configured from console by console
  - wr
  - Building configuration...
  - [OK]
  - R1#show ip route
  - Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
  - D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
  - N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
  - E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
  - i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
  - * - candidate default, U - per-user static route, o - ODR
  - P - periodic downloaded static route
  - Gateway of last resort is 0.0.0.0 to network 0.0.0.0
  - 88.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
  - C 88.40.12.0/30 is directly connected, Serial0/0/0
  - L 88.40.12.1/32 is directly connected, Serial0/0/0
  - 172.16.0.0/16 is variably subnetted, 8 subnets, 5 masks
  - C 172.16.10.0/24 is directly connected, FastEthernet0/0.10
  - L 172.16.10.254/32 is directly connected, FastEthernet0/0.10
  - C 172.16.11.0/26 is directly connected, FastEthernet0/0.20
  - L 172.16.11.62/32 is directly connected, FastEthernet0/0.20
  - C 172.16.11.64/27 is directly connected, FastEthernet0/0.30
  - L 172.16.11.94/32 is directly connected, FastEthernet0/0.30
  - C 172.16.11.96/28 is directly connected, FastEthernet0/0.40
  - L 172.16.11.110/32 is directly connected, FastEthernet0/0.40
  - S* 0.0.0.0/0 is directly connected, Serial0/0/0

- **Configuring Route Pointing Back**
  - Select the ISP Route and go to the CLI
  - ISP>enable
  - ISP#conf t
  - Enter configuration commands, one per line. End with CNTL/Z.
  - ISP(config)#ip route 172.16.10.0 255.255.254.0 88.40.12.1
  - ISP(config)#exit
  - ISP#
  - %SYS-5-CONFIG_I: Configured from console by console
  - wr
  - Building configuration...
  - [OK]

- **Testing Web Servers**
  - Retest ping from wireless laptop to 10.10.10.1 (success)
  - Test external web server in web browser 10.10.10.1 (success)
  - Test internal web server in web browser 172.16.11.97 (success)

- **Configuring DNS**
  - Select the external web server and go to Services
  - Select DNS > On
  - Create a Record
    - Name www.ext.co.usa
    - Type A Record
    - Address 10.10.10.1
    - Click Add
    - Name www.int.co.usa
    - Type A Record
    - Address 172.16.11.97
    - Click Add
  - Use the browser inside of the laptop to test each URL
  - Success

- **Implementing Basic Security**
  - **Username, passwords, privilege levels, and password encryption**
    - Select internal router and open CLI
    - R1>enable
    - R1#conf t
    - R1(config)#security passwords min-length 8
    - Line console 0

- Password atleast8
- Login local
- Exit
- R1(config)#username jay secret atleast8
    - Clear text password
- R1(config)#username secure secret atleast8#
    - Encrypted password
- R1(config)#username joe privilege 15 secret admin123
    - Set privileges
- R1(config)#username paul privilege 3 secret worker123
- R1(config)#enable secret enablesecret
- R1(config)#service password-encryption
- Ctrl + z

- **Idle Timeout**
    - R1#conf t
    - Enter configuration commands, one per line. End with CNTL/Z.
    - R1(config)#line console 0
    - R1(config-line)#exec-time
    - R1(config-line)#exec-timeout 1 30
        - 1 minute 30 seconds

- **Login Blocking**
    - R1(config)#login block-for 120 attempts 5 within 45

- **Banner Creation**
    - R1(config)#banner motd & DO NOT ATTEMPT TO LOGIN AND ACCESS THIS ROUTER &

- **SSH Access**
    - R1(config)#ip domain-name testdomain
    - R1(config)#crypto key generate rsa
    - The name for the keys will be: R1.testdomain
    - Choose the size of the key modulus in the range of 360 to 4096 for your
    - General Purpose Keys. Choosing a key modulus greater than 512 may take
    - a few minutes.
    - How many bits in the modulus [512]: 2048
    - % Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
    - R1(config)#line vty 0 4

- R1(config-line)#transport input ssh
- TEST using laptop Command line
    - C:\>ssh -l joe 172.16.10.254

- **Switchport Port Security**
    - SW1(config)#interface fastEthernet 0/3
    - SW1(config-if)#swit
    - SW1(config-if)#switchport port
    - SW1(config-if)#switchport port-security
    - SW1(config-if)#swit
    - SW1(config-if)#switchport port
    - SW1(config-if)#switchport port-security mac
    - SW1(config-if)#switchport port-security mac-address sti
    - SW1(config-if)#switchport port-security mac-address sticky
    - SW1(config-if)#switchport port-security viol
    - SW1(config-if)#switchport port-security violation shutdown
    - SW1(config-if)#switchport port-security vmax
    - SW1(config-if)#switchport port-security max
    - SW1(config-if)#switchport port-security maximum 1
    - Test by connecting a new pc to the switch
    - Enable DHCP on new PC
    - Disconnect and connect a new PC > Enable DHCP
        - If it fails, it's working
    - SW1#show port-security
    - Conf t
    - Interface fastethernet 0/3
    - No shutdown
    - Shutdown
    - No shutdown
        - This changes the state of the port back to up

- **Configuring Remote Acces VPN**

    - **Configure Remote User Physical Connection**
        - Add and connect User PC > Modem > Cloud
        - Connect the Cloud to the Internal Router.
        - In Cloud, Config > DSL > Add Modem and Ethernet connections (Modem4 / Ethernet6)
        - R1#config t
        - Enter configuration commands, one per line. End with CNTL/Z.
        - R1(config)#conf t
        - %Invalid hex value

- R1(config)#enable
- % Incomplete command.
- R1(config)#line console 0
- R1(config-line)#exec-timeout 10
- R1(config-line)#exit
- R1(config)#exit
- R1#
- %SYS-5-CONFIG_I: Configured from console by console
- wr
- Building configuration...
- [OK]
- R1#conf t
- Enter configuration commands, one per line. End with CNTL/Z.
- R1(config)#in
- R1(config)#interface fas
- R1(config)#interface fastEthernet 0/1
- R1(config-if)#ip address 72.44.20.14 255.255.255.240
- R1(config-if)#no shutdown
- R1(config-if)#
- %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
- %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
- R1(config-if)#exit
- R1(config)#ip dhcp pool REMOTE_POOL
- R1(dhcp-config)#net
- R1(dhcp-config)#network 72.44.20.14 255.255.255.240
- R1(dhcp-config)#default-router 72.44.20.14
- R1(dhcp-config)#dns-server 10.10.10.1
- R1(dhcp-config)#^Z
- R1#
- %SYS-5-CONFIG_I: Configured from console by console

- **Configuring AAA**
  - R1(config)#aaa new-model
  - R1(config)#aaa authentication login
  - R1(config)#aaa authentication login REMOTE
  - % Incomplete command.
  - R1(config)#aaa authentication login REMOTE local
  - R1(config)#aaa authorization network REMOTE local
  - R1(config)#username VPN secret supersecure

- **Configuring Remote Access VPN**

- R1(config)#
- R1(config)#crypto isakmp policy 10
- R1(config-isakmp)#encryption aes 256
- R1(config-isakmp)#
- R1(config-isakmp)#
- R1(config-isakmp)#hash ?
- md5 Message Digest 5
- sha Secure Hash Standard
- R1(config-isakmp)#hash
- % Incomplete command.
- R1(config-isakmp)#hash md5
- R1(config-isakmp)#au
- R1(config-isakmp)#authentication pre
- R1(config-isakmp)#authentication pre-share
- R1(config-isakmp)#group 2
- R1(config-isakmp)#lifetime 21600
- R1(config-isakmp)#exit
- R1(config)#crypto isakmp client confi
- R1(config)#crypto isakmp client configuration group REMOTE
- R1(config-isakmp-group)#key CISCO
- R1(config-isakmp-group)#pool MYPOOL
- R1(config-isakmp-group)#exit
- R1(config)#cr
- R1(config)#crypto ipsec transform-set MYSET esp-aes 256 esp-md5-hmac
- R1(config)#crypto dynamic-map DYNMAP 10
- R1(config-crypto-map)#set transform-set MYSET
- R1(config-crypto-map)#rever
- R1(config-crypto-map)#reverse-route
- R1(config-crypto-map)#exit
- R1(config)#crypto map CLIENT_MAP client auth
- R1(config)#crypto map CLIENT_MAP client authentication list REMOTE
- R1(config)#crypto map CLIENT_MAP isakmp auth
- R1(config)#crypto map CLIENT_MAP isakmp authorization list REMOTE
- R1(config)#crypto map CLIENT_MAP client configuration address respond
- R1(config)#crypto map CLIENT_MAP 10 ipsec-isakmp dynamic DYNMAP
- R1(config)#ip local pool MYPOOL 172.16.10.150 172.16.10.200
- R1(config)#int
- R1(config)#interface fas
- R1(config)#interface fastEthernet 0/1

- R1(config-if)#cry
- R1(config-if)#crypto map CLIENT_MAP
- *Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

- **Testing the VPN**
  - Go the the PC in the VPN Network.
  - Desktop > VPN
    - Group Name: REMOTE
    - Group Key: CISCO
    - Host IP: 172.44.20.14
    - Username: VPN
    - Password: supersecure
  - Connect (Success)
  - R1#show crypto ipsec sa
  - interface: FastEthernet0/1
  - Crypto map tag: CLIENT_MAP, local addr 72.44.20.14
  - protected vrf: (none)
  - local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  - remote ident (addr/mask/prot/port): (172.16.10.150/255.255.255.255/0/0)
  - current_peer 72.44.20.1 port 500
  - PERMIT, flags={origin_is_acl,}
  - #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  - #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  - #pkts compressed: 0, #pkts decompressed: 0
  - #pkts not compressed: 0, #pkts compr. failed: 0
  - #pkts not decompressed: 0, #pkts decompress failed: 0
  - #send errors 0, #recv errors 0
  - local crypto endpt.: 72.44.20.14, remote crypto endpt.:72.44.20.1
  - path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
  - current outbound spi: 0xCB95CCA8(3415592104)
  - inbound esp sas:
  - spi: 0xFA1368BF(4195575999)
  - R1#show crypto isakmp sa
  - IPv4 Crypto ISAKMP SA
  - dst src state conn-id slot status
  - 72.44.20.1 72.44.20.14 QM_IDLE 1025 0 ACTIVE
  - IPv6 Crypto ISAKMP SA

- **Configure VOIP (IP Telephony)**

- **Designing and Adapting the existing network for VOIP**
  - Add 1 IP Phone to each subnet (DO NOT CONNECT YET)

- **Configuring Separate Voice VLAN**
  - VLAN 100 DG - 192.168.54.254/23
  - On main switch , go to CLI
  - SW1(config)#vlan 100
  - SW1(config-vlan)#name VOICE
  - SW1(config-vlan)#exit
  - SW1(config)#do sh vlan brief
  - VLAN Name Status Ports
  - ---- -------------------------------- --------- -------------------------------
  - 1 default active Fa0/21, Fa0/22
  - 10 SALES active Fa0/1, Fa0/2, Fa0/3, Fa0/4
  - Fa0/5, Fa0/6, Fa0/7, Fa0/8
  - Fa0/9, Fa0/10, Fa0/11, Fa0/12
  - Fa0/13, Fa0/14, Fa0/15, Fa0/16
  - Fa0/17, Fa0/18, Fa0/19, Fa0/20
  - 20 RESEARCH active
  - 30 MANAGEMENT active
  - 40 SERVERS active
  - 100 VOICE active
  - 1002 fddi-default active
  - 1003 token-ring-default active
  - 1004 fddinet-default active
  - 1005 trnet-default active
  - SW1(config)#interface fastEthernet 0/1
  - SW1(config-if)#switchport voice vlan 100
  - SW1(config-if)#spanning-tree portfast
  - Ctrl + z
  - Wr
  - Repeat for other 2 switches
  - SW2>enable
  - SW2#conf t
  - Enter configuration commands, one per line. End with CNTL/Z.
  - SW2(config)#inter
  - SW2(config)#interface fast
  - SW2(config)#interface fastEthernet 0/1
  - SW2(config-if)#switchport voice vlan 100
  - SW2(config-if)#span
  - SW2(config-if)#spanning-tree port
  - SW2(config-if)#spanning-tree portfast

- %Warning: portfast should only be enabled on ports connected to a single
- host. Connecting hubs, concentrators, switches, bridges, etc... to this
- interface when portfast is enabled, can cause temporary bridging loops.
- Use with CAUTION
- %Portfast has been configured on FastEthernet0/1 but will only
- have effect when the interface is in a non-trunking mode.
- SW2(config-if)#^Z
- SW2#
- %SYS-5-CONFIG_I: Configured from console by console
- wr
- Building configuration...
- [OK]
- SW3>enable
- SW3#conf t
- Enter configuration commands, one per line. End with CNTL/Z.
- SW3(config)#interf
- SW3(config)#interface fast
- SW3(config)#interface fastEthernet 0/1
- SW3(config-if)#swi
- SW3(config-if)#switchport voice vlan 100
- SW3(config-if)#spann
- SW3(config-if)#spanning-tree port
- SW3(config-if)#spanning-tree portfast
- %Warning: portfast should only be enabled on ports connected to a single
- host. Connecting hubs, concentrators, switches, bridges, etc... to this
- interface when portfast is enabled, can cause temporary bridging loops.
- Use with CAUTION
- %Portfast has been configured on FastEthernet0/1 but will only
- have effect when the interface is in a non-trunking mode.
- SW3(config-if)#exit
- SW3(config)#exit
- SW3#
- %SYS-5-CONFIG_I: Configured from console by console
- wr
- Building configuration...
- [OK]

■ **Configuring Sub-Interface for the Voice Subnet**

- R1(config)#interface fastEthernet 0/0.100
- R1(config-subif)#
- %LINK-5-CHANGED: Interface FastEthernet0/0.100, changed state to up
- %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.100, changed state to up
- R1(config-subif)#
- R1(config-subif)#encapsulation dot1Q 100
- R1(config-subif)#ip address 192.168.55.254 255.255.254.0
- R1(config-subif)#exit

- **Configuring a DHCP Pool for the IP Phones**
  - R1(config)#ip dhcp pool VOICE_POOL
  - R1(dhcp-config)#network 192.168.54.0 255.255.254.0
  - R1(dhcp-config)#def
  - R1(dhcp-config)#default-router 192.168.55.254
  - R1(dhcp-config)#dn
  - R1(dhcp-config)#dns-server 10.10.10.1
  - R1(dhcp-config)#option 150 ip 192.168.55.254
  - R1(dhcp-config)#exit
  - R1(config)#exit
  - R1#
  - %SYS-5-CONFIG_I: Configured from console by console
  - wr
  - Building configuration...
  - [OK]

- **Configuring Telepohony Service**
  - R1(config)#telephony-service
  - R1(config-telephony)#ip source-address 192.168.55.254 port 2000
  - R1(config-telephony)#max-ephones 3
  - R1(config-telephony)#max-dn 3
  - R1(config-telephony)#exit
  - R1(config)#ephone 1
  - R1(config-ephone)#type 7960
  - Remove cable from switch 1 and connect to phone 1 PC port.
  - Connect switch to phone 1 switch port
  - R1(config)#ephone-dn 1
  - R1(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up
  - R1(config-ephone-dn)#number 2001
  - R1(config-ephone-dn)#exit
  - R1(config)#ephone 1

- R1(config-ephone)#button 1:1
- R1(config-ephone)#
- %IPPHONE-6-REGISTER: ephone-1 IP:192.168.54.1 Socket:2 DeviceType:Phone has registered.
- R1(config-ephone)#
- R1(config-ephone)#exit
- R1(config)#ephone 2
- R1(config-ephone)#type 7960
- Remove cable from switch 2 and connect to phone 2 PC port.
- Connect switch to phone 2 switch port
- R1(config)#ephone-dn 2
- R1(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up
- R1(config-ephone-dn)#number 2002
- R1(config-ephone-dn)#exit
- R1(config)#ephone 2
- R1(config-ephone)#button 1:2
- R1(config-ephone)#
- %IPPHONE-6-REGISTER: ephone-1 IP:192.168.54.1 Socket:2 DeviceType:Phone has registered.
- R1(config-ephone)#
- R1(config-ephone)#exit
- R1(config)#ephone 3
- R1(config-ephone)#type 7960
- Remove cable from switch 3 and connect to phone 3 PC port.
- Connect switch to phone 3 switch port
- R1(config)#ephone-dn 3
- R1(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up
- R1(config-ephone-dn)#number 2003
- R1(config-ephone-dn)#exit
- R1(config)#ephone 3
- R1(config-ephone)#button 1:3
- R1(config-ephone)#
- %IPPHONE-6-REGISTER: ephone-1 IP:192.168.54.1 Socket:2 DeviceType:Phone has registered.
- R1(config-ephone)#
- R1(config-ephone)#exit
- R1#clock set 16:52:00 26 March 2025
- R1#show clock
- 16:52:2.501 UTC Wed Mar 26 2025
- R1(config)#telephony-service
- R1(config-telephony)#create cnf-files
- Creating CNF files

- CNF-FILES: Clock is not set or synchronized, retaining old versionStamp
- Ctrl + z
- %SYS-5-CONFIG_I: Configured from console by console
- wr
- Building configuration...
- [OK]

Conclusion:

- **Gained hands-on experience in multiple aspects of Networking.**
  - **Network Design**
  - **Network Configuration**
  - **Subnetting and VLANs**
  - **DHCP**
  - **DNS**
  - **VOIP**
- **Gained hands-on experience utilizing basic Network Security features.**
  - **Account Configuration**
  - **Password Encryption**
  - **Port Security**
  - **VPN**
- **Gained hands-on experience using Cisco Packet Analyzer**