ACADEMY CAMPUS NETWORK

-

SECURE PROJECT

ANDRE JESUS
(Cybersecurity)

2024

Through this project, I aimed to implement advanced security measures while learning how to effectively safeguard our digital infrastructure. Along the way, I encountered numerous challenges that required extensive troubleshooting and prompted significant research using tools like Cisco Packet Tracer. By documenting my journey and the steps taken, I am not only creating a secure network that meets current challenges and prepares for future threats but also sharing valuable insights gained from hands-on experience.

INDEX

NETWORK DESIGN

Devices	Network IP addresses
3 Routers: ISP -> HQ-Router-> Branch-Router 2 Firewall: (One behind HQ-Router, other behind Branch-Router) - Cisco ASA Firewalls 5500-X series 4 Multilayer Switch (24 Ports) : 2 for each Building (HQ +Branch) - Core Switches - Cisco Catalyst 3650 9 Network Switch (1 for each department, including DMZ) - Access switches - Cisco Catalyst 2960 9 or 10 Access Points (1 each department + maybe 1 or 2 on the soccer field) 1 Wireless Lan Controller Each department will Have 1 PC + 1 Printer For testing Connectivity DMZ Server farm 6 SERVERS: 2 DHCP, 1 DNS, 1 Web-Server, 1 Email Server SMTP, 1 FTP Cloud Server + 3 Virtual Machines.	**HQ:** Management Network: range 192.168.10.0/24 Wlan: range 10.10.0.0/16 Lan: range 172.16.0.0/16 DMZ: range 10.20.20.0/27 **BRANCH:** Wlan: range 10.11.0.0/16 Lan: range 172.17.0.0/16 **CLOUD:** Network: 8.0.0.0/8

For security Purposes all LAN and wlan will be on a separate network segment within the same Building (HQ vs Branch) The Firewall will be used to secure these zones and filter traffic based on configure Inspection Policies. The Top of the line as of today, regarding Cisco Multilayer switches, would be something under the The catalyst 9300 series. But for project purposes, For the Core switches I went with the Cisco Catalyst 3650, operates at Layer 3 and has Gigabit Ethernet ports that operate at faster speeds.More than capable to handle the required workload of the project. Routing will be done by Firewall and Multilayer Switches.

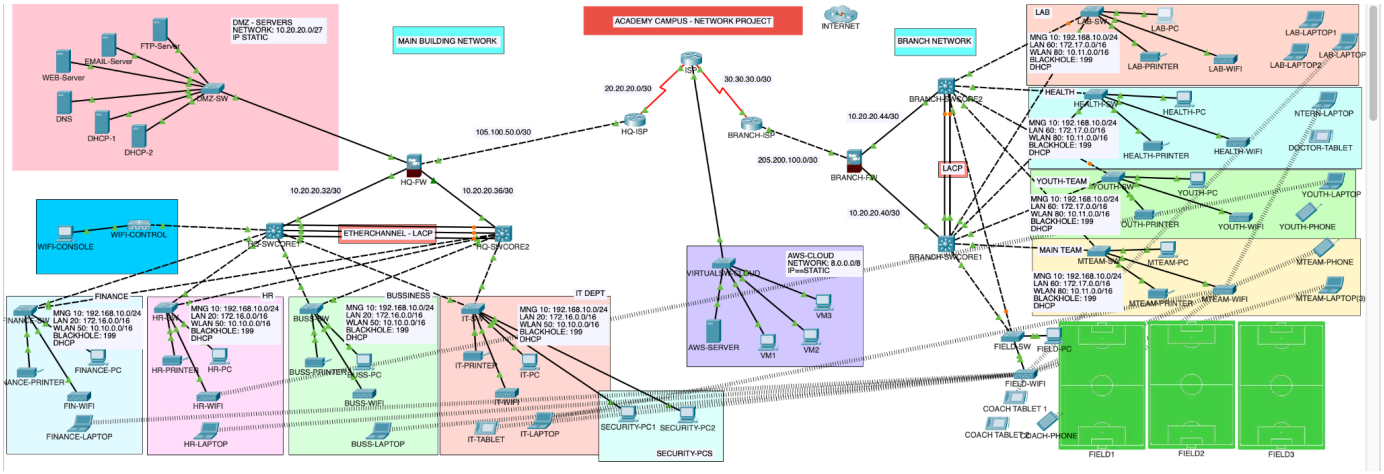
Public Addresses: 105.100.50./30 (HQ) / 205.200.100.0/30 (Branch)

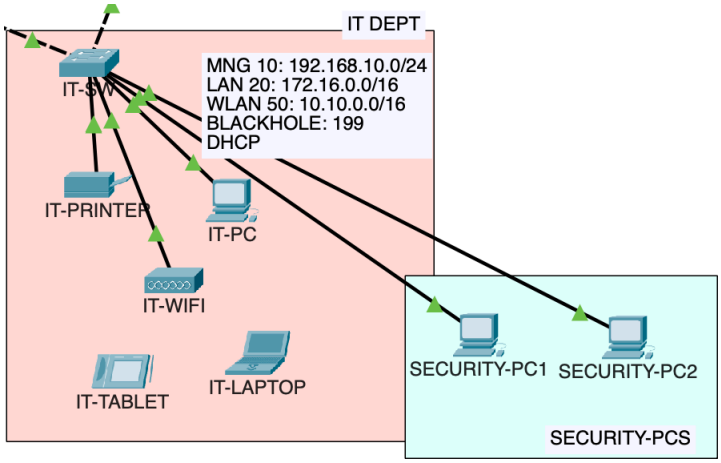
Interfaces (ISP, Firewall, Router, Core Switches)	VLAN ID'S	General Port Setup:
HQ-ISP -> Internet : 20.20.20.0/30 Branch-ISP -> Internet: 30.30.30.0/30 HQ-firewall -> HQ-ISP: 105.100.50.0/30 Branch-firewall -> Branch-ISP: 205.200.100.0/30 HQ-firewall ->HQ Core Switch A: 10.20.20.32/30 HQ-firewall -> HQ Core Switch B: 10.20.20.36/30 Branch-firewall -> Branch core Switch A:10.20.20.40/30 Branch-firewall -> Branch Core Switch B: 10.20.20.44/30	**HQ** Management -10 LAN - 20 WLAN - 50 BLACKHOLE - 150 **BRANCH** LAN 60 WLAN 80 BLACKHOLE 199	Port 1-2:Trunk (Connected to Firewall) Port 3-15:Lan Port 16-20: Management (For Security Computer) And also we want to be able to manage every department switch remotely. Port 21-24: Wlan (For Access Points) Port gig 1-2: Blackhole (IT Dept, these ports will be used for Security PC's)

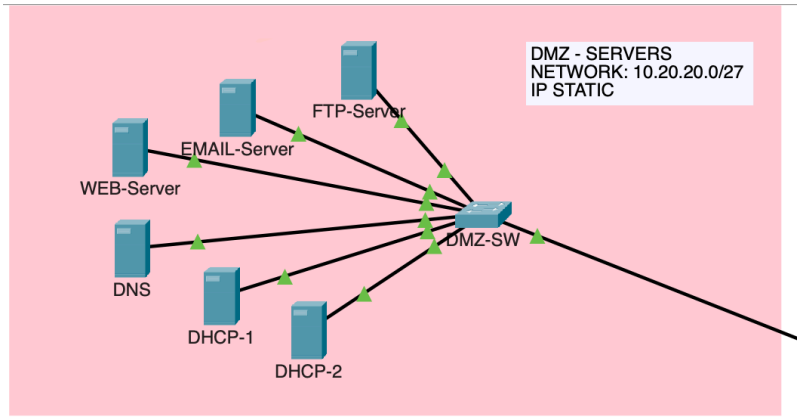
Objectives

Blackhole Vlan will be used to shut down unused ports and drive bad traffic away. The main objective for this project is to enable secure communication between all devices and branches. Establish an ACL for SSH on a VTY line to allow only the management network to access remotely and permit remote administrative tasks.Implement OSPF as routing protocol to advertise routes on the firewall, router and multilayer switches. Etherchannel: Implement LACP - Link Aggregation Control Protocol to enhance link aggregation efficiency - This will be the connection between Multilayers Switches. For each branch Between routers I used Serial DCE cable. (Must install DCE Module HWIC-2T first) And configure Clock rate later for a more efficient synchronization. A communication using Serial Cables can operate more efficiently at higher frequencies, it's more robust and still relevant today. Trunk Ports are necessary to allow traffic for Multiple Vlans, in order to link switches. Because Access Ports only accept traffic for a single Vlan. NAT should be configured. Implement HSRP protocol, STP Portfast, DHCP Pools to assign IP addresses Dynamically. And Subnetting LAN + WLAN considering both Branches could hold up to 60 thousand uses each.

Topology


DMZ - SERVERS
NETWORK: 10.20.20.0/27
IP STATIC
FTP-Server
EMAIL-Server
WEB-Server
DMZ-SW
DNS
DHCP-1
DHCP-2
MAIN BUILDING NETWORK
ACADEMY CAMPUS - NETWORK PROJECT
INTERNET
BRANCH NETWORK
ISP
HQ-ISP
BRANCH-ISP
105.100.50.0/30
20.20.20.0/30
30.30.30.0/30
205.200.100.0/30
10.20.20.44/30
10.20.20.40/30
HQ-FW
BRANCH-FW
10.20.20.32/30
10.20.20.36/30
WIFI-CONSOLE
WIFI-CONTROL
HQ-SWCORE1
ETHERCHANNEL - LACP
HQ-SWCORE2
BRANCH-SWCORE2
BRANCH-SWCORE1
LACP
LAB
LAB-SW
LAB-PC
LAB-LAPTOP1
LAB-LAPTOP2
LAB-PRINTER
LAB-WIFI
HEALTH
HEALTH-SW
HEALTH-PC
INTERN-LAPTOP
DOCTOR-TABLET
HEALTH-PRINTER
HEALTH-WIFI
YOUTH-TEAM
YOUTH-SW
YOUTH-PC
YOUTH-LAPTOP
YOUTH-PRINTER
YOUTH-WIFI
YOUTH-PHONE
MAIN TEAM
MTEAM-SW
MTEAM-PC
MTEAM-PHONE
MTEAM-PRINTER
MTEAM-WIFI
MTEAM-LAPTOP(3)
FINANCE
FINANCE-PC
FIN-WIFI
FINANCE-LAPTOP
HR
HR-SW
HR-PRINTER
HR-PC
HR-WIFI
HR-LAPTOP
BUSSINESS
BUSS-SW
BUSS-PRINTER
BUSS-PC
BUSS-WIFI
BUSS-LAPTOP
IT DEPT
IT-SW
IT-PRINTER
IT-PC
IT-WIFI
IT-TABLET
IT-LAPTOP
SECURITY-PC1
SECURITY-PC2
SECURITY-PCS
AWS-CLOUD
NETWORK: 8.0.0.0/8
IP=STATIC
VIRTUALAWS-CLOUD
AWS-SERVER
VM1
VM2
VM3
FIELD-SW
FIELD-PC
FIELD-WIFI
COACH TABLET 1
COACH TABLET2
COACH-PHONE
FIELD1
FIELD2
FIELD3


IT DEPT
IT-SW
MNG 10: 192.168.10.0/24
LAN 20: 172.16.0.0/16
WLAN 50: 10.10.0.0/16
BLACKHOLE: 199
DHCP
IT-PRINTER
IT-PC
IT-WIFI
IT-TABLET
IT-LAPTOP
SECURITY-PC1
SECURITY-PC2
SECURITY-PCS


DMZ - SERVERS
NETWORK: 10.20.20.0/27
IP STATIC
FTP-Server
EMAIL-Server
WEB-Server
DMZ-SW
DNS
DHCP-1
DHCP-2

SSH CONFIGURATION + ACL + LINE VTY

We want to be able to have remote access to this network devices, but we only want this to happen from The Management Network.
This configuration is done on each department **Access Switch + Multilayer Core Switch**

CLI Basic Config - ALL switches	**SSH configuration**

en
config t
hostname Finance (change Switch name for each department) enable password recovery (Set password to activate "en" command. Adds Extra Security)
banner motd #ADMIN USER ONLY!!# (warning or guidance message for user prior to login)
no ip domain-lookup (this prevents router from trying to resolve incorrect paste commands in the CLI sending a DNS Query)
service password-encryption (Hide password display)
Line console 0 (Protect line console to allow just 1 user)
Password cisco (Set Switch password. In real life, always use a more complex and robust password)
Login
Exec-timeout 2 0
`ADMIN USERS ONLY!!`
`User Access Verification`
`Password:`
`Finance-Switch>en`
`Password:`
`Finance-Switch#`
	username admin **password** cisco (set user + password)
	ip domain-name academy.com (set domain)
	crypto key generate rsa general-keys modulus 1024 (generate exchange keys for safe communication + length of the key)
	
	ACL for SSH
	(only allow management Network to configure, manage, and monitor the device remotely login through SSH)
	access-list 1 permit 192.168.10.0 0.0.0.255 (ONLY this network can SSH)
	Access-list 1 deny any (deny anything else)
	line vty 0 15 (configure CLI to give user access to the device control plane)*
	login local (use only local credentials previously set up in this case: admin:cisco)
	transport input ssh (Only allow SSH to be able to access a machine remotely. Telnet is NOT secure)
	access-class 1 in (bind access list to line vty)
	exit
	do wr

```
Switch>
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Finance-Switch
Finance-Switch(config)#line console 0
Finance-Switch(config-line)#password summer32
Finance-Switch(config-line)#login
Finance-Switch(config-line)#exec-timeout 2 0
Finance-Switch(config-line)#exit
Finance-Switch(config)#enable password recovery
Finance-Switch(config)#banner motd #ADMIN USERS ONLY!!#
Finance-Switch(config)#no ip domain-lookup
Finance-Switch(config)#service password-encryption
Finance-Switch(config)#username admin password complexpass789
Finance-Switch(config)#ip domain-name academy.com
Finance-Switch(config)#crypto key generate general-keys modulus 1024
                                                ^
% Invalid input detected at '^' marker.

Finance-Switch(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: Finance-Switch.academy.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 4:51:1.333: %SSH-5-ENABLED: SSH 1.99 has been enabled
Finance-Switch(config)#access-list 1 permit 192.168.10.0 255.255.255.0
Finance-Switch(config)#access-list 1 deny any
Finance-Switch(config)#line vty 0 15
Finance-Switch(config-line)#login local
Finance-Switch(config-line)#transport input ssh
Finance-Switch(config-line)#access-class 1 in
Finance-Switch(config-line)#exit
Finance-Switch(config)#do wr
Building configuration...
[OK]
Finance-Switch(config)#
Finance-Switch(config)#
```

Switch Basic Configuration + SSH

VLAN ID + PORT ASSIGNMENTS (Trunk + Access Ports)

Starting at Core Multilayer switches. Any port connecting from Core Switch to any Access Switch should be trunked and vice versa. The Connection to the Wireless Controller should be Access Port. The Vlan 199 (Blackhole) will not be created on the Multilayer switches, only on the Access Switches). The trunk ports should be the same for both Locations, as I was very consistent with the cable connections.

HQ-SWcore (Multilayer Switch)	**HQ-Access Switches**
en config t vlan 10 name MNGT vlan 20 name LAN vlan 50 name WLAN exit int range gig1/0/2-5 switchport mode trunk ex int gig1/0/6 switchport mode access Switchport access vlan 50 Ex do wr *Same configuration for MainB-CoreSwich, except doesn't have Access Ports	(this applies to all of the switches on the **Main campus**, except the IT department) en config t vlan 10 name MNGT vlan 20 name LAN vlan 50 name WLAN vlan 199 name BLACKHOLE exit int range fa0/1-2 switchport mode trunk ex int range fa0/3-20 switchport mode access switchport access vlan 20 ex int range fa0/21-24 switchport mode access switchport access vlan 50 ex int range gig0/1-2 switchport mode access switchport access vlan 199 shut ex do wr

```
Press RETURN to get started!

ADMIN USERS ONLY!!

User Access Verification

Password:

Finance-Switch>en
Password:
Finance-Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Finance-Switch(config)#vlan 10
Finance-Switch(config-vlan)#name
% Incomplete command.
Finance-Switch(config-vlan)#vlan 20
Finance-Switch(config-vlan)#name LAN
Finance-Switch(config-vlan)#vlan 50
Finance-Switch(config-vlan)#name WLAN
Finance-Switch(config-vlan)#vlan 199
Finance-Switch(config-vlan)#name BLACKHOLE
Finance-Switch(config-vlan)#exit
Finance-Switch(config)#int range fa0/1-2
Finance-Switch(config-if-range)#switchport mode trunk
Finance-Switch(config-if-range)#int range fa0/3-20
Finance-Switch(config-if-range)#switchport mode access
Finance-Switch(config-if-range)#switchport access  vlan 20
Finance-Switch(config-if-range)#
Finance-Switch(config-if-range)#int range fa0/21-24
Finance-Switch(config-if-range)#switchport mode access
Finance-Switch(config-if-range)#switchport access vlan 50
Finance-Switch(config-if-range)#int range gig0/1-2
Finance-Switch(config-if-range)#switchport mode access
Finance-Switch(config-if-range)#switchport access vlan 199
Finance-Switch(config-if-range)#shut

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
Finance-Switch(config-if-range)#ex
Finance-Switch(config)#do wr
Building configuration...
[OK]
Finance-Switch(config)#
```

Access Switch - VLAN + Port configuration

Access Switch IT department
(Slightly different configuration in order to Assign Vlan 10 - Management. And use the free Gig Ports 1 and 2 to connect Security Management computers, All Ports are assigned, so no need for Blackhole 199.)

int range gig0/1-2
switchport mode access
switchport access vlan 10 **(Management- Here you assigned vlan 10, the other departments we didn't)**
ex
do wr

Branch configuration
(Both Core and Access Switches will have similar configuration regarding port type. Except Vlan definition, as HQ and Branch will be on a different Network Segmentation.

Branch SWCore (1+2)	**BRANCH ACCESS SWITCHES**
(Create vlans + configure trunk ports) en config t vlan 60 name BRANCH-LAN vlan 80 Name BRANCH-WLAN vlan 199 name BRANCH-BLACKHOLE exit int range gig1/0/2-6 switchport mode trunk ex do wr	en config t vlan 60 name BRANCH-LAN vlan 80 Name BRANCH-WLAN vlan 199 name BRANCH-BLACKHOLE exit int range fa0/1-2 switchport mode trunk int range fa0/3-20 switchport mode access switchport access vlan 60 int range fa0/21-24 switchport mode access switchport access vlan 80 int range gig0/1-2 switchport mode access switchport access vlan 199 shut ex do wr

SPANNING TREE STP PORTFAST + BPDUGUARD - ACCESS PORTS CONFIGURE (ONLY)

DMZ-SWITCH	**HQ-SWCORE1**	**Access switches (main location)**
int range fa0/2-24 spanning-tree portfast Spanning-tree bpduguard enable exit do wr *SAME CONFIG FOR ACCESS SWITCHES EXCEPT is fa0/3-24	int gig1/0/6 spanning-tree portfast spanning-tree bpduguard enable exit do wr	int range fa0/3-24 spanning-tree portfast spanning-tree bpduguard enable exit do wr

EtherChannel - LACP (Between Core Multilayer Switches)

This protocol allows me to combine multiple physical links between Switches into one logic link , providing increased bandwidth, load balancing and redundancy. For cable management purposes and organization consistency, I configure this Connection on last ports 21-23 on all Core Switches. To implement LACP there are 2 modes: passive and active. Keep in mind that Passive-Passive doesn't form LACP, it has to be either Active-Passive or Active-Active between Switches.

HQ CoreSw 1 int range gig1/0/21-23 No shut Channel-group 1 mode active Ex Interface Port-channel 1 Switchport mode trunk ex Do wr	HQ CoreSw 2 int range gig1/0/21-23 No shut Channel-group 1 mode active Ex Interface Port-channel 1 Switchport mode trunk ex Do wr
Branch Core SW1 int range gig1/0/21-23 No shut Channel-group 2 mode active Ex Interface Port-channel 2 Switchport mode trunk ex Do wr	Branch CoreSW2 int range gig1/0/21-23 No shut Channel-group 2 mode passive Ex Interface Port-channel 2 Switchport mode trunk ex Do wr

** Check Configuration: Show etherchannel port-channel

```
Group: 1
----------
               Port-channels in the group:
               ---------------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 00d:00h:04m:58s
Logical slot/port   = 2/1       Number of ports = 3
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =  LACP
Port Security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gig1/0/21Active             0
  0     00     Gig1/0/22Active             0
  0     00     Gig1/0/23Active             0
Time since last port bundled:    00d:00h:04m:58s    Gig1/0/23
MainA-Switch#
MainA-Switch#
```

Protocol LACP Enable between Core Switches

IP ADDRESS CONFIGURATION/SUBNETTING

Core Multilayer Switch 1 + 2 - Enable Routing
(By default, These Multilayer Switches don't have routing capabilities enabled. We need to make it work as a Switch and a Router with the command: ip routing) Also set clock rate between DCE Serial connections to the same matching values: clock rate 64000.

Interfaces IP:

HQ-CoreSW1 to HQ-Firewall ip routing int gig1/0/1 no switchport ip add 10.20.20.33 255.255.255.252 ex do wr	**HQ-CoreSW2 to HQ-Firewall** ip routing int gig1/0/1 no switchport ip add 10.20.20.37 255.255.255.252 ex do wr
Branch-SWCore1 A to BRANCH-Firewall ip routing int gig1/0/1 no switchport ip add 10.20.20.41 255.255.255.252 ex do wr	**Branch-SWCORE2 to BRANCH Firewall** ip routing int gig1/0/1 no switchport ip add 10.20.20.45 255.255.255.252 ex do wr
HQ- ISP to INTERNET int se0/0/0 no shutdown ip add 20.20.20.2 255.255.255.252 do wr	**Branch-ISP to INTERNET** int se0/0/0 no shutdown ip add 30.30.30.2 255.255.255.252 do wr
INTERNET to HQ- ISP int se0/0/0 no shutdown ip add 20.20.20.1 255.255.255.252 do wr	**INTERNET to Branch-ISP** int se0/0/1 no shutdown ip add 30.30.30.1 255.255.255.252 do wr
HQ-ISP to Firewall HQ int gig0/1 No shutdown ip address 105.100.50.1 255.255.255.252 Do wr	**Branch-ISP to Firewall Branch** int gig0/1 No shutdown ip address 205.200.100.1 255.255.255.252 Do wr

Firewall IP configuration
(Name interfaces based on the Desired Zones: Inside, Outside and DMZ)

HQ-FIREWALL	BRANCH-FIREWALL
HQ Firewall to HQ-SWCORE1 int gig1/1 No shut Nameif INSIDE1 Security-level 100 ip add 10.20.20.34 255.255.255.252 ex	**Branch Firewall to BranchSWCORE1** int gig1/2 No shut Nameif INSIDE1 Security-level 100 ip add 10.20.20.42 255.255.255.252 ex

HQ Firewall to HQ-SWCORE2 int gig1/2 No shut Nameif INSIDE2 Security-level 100 ip add 10.20.20.38 255.255.255.252 Ex	**Branch Firewall to BranchSWCORE2 Switch** int gig1/1 No shut Nameif INSIDE2 Security-level 100 ip add 10.20.20.46 255.255.255.252 ex
HQ Firewall to DMZ int gig1/4 No shut Nameif DMZ Security-level 70 ip add 10.20.20.1 255.255.255.224 Ex	**Branch Firewall to Branch-ISP** int gig1/3 No shut Nameif OUTSIDE Security-level 0 ip add 205.200.100.2 255.255.255.252 ex Wr mem
HQ Firewall to HQ-ISP int gig1/3 No shut Nameif OUTSIDE Security-level 0 ip add 105.100.50.2 255.255.255.252 exit Wr mem	

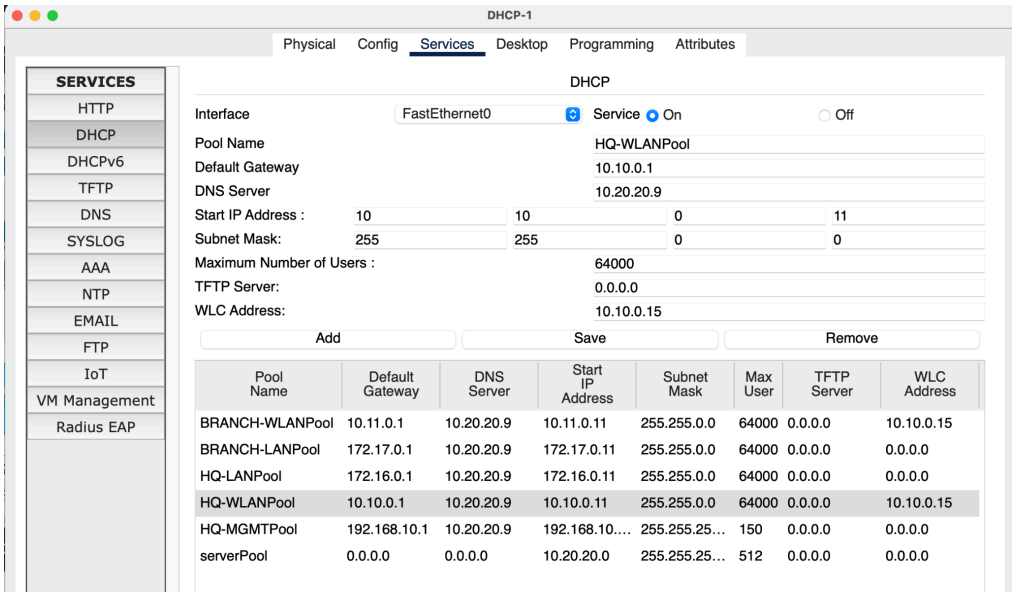
DMZ SERVERS IP ADDRESS (STATIC)

FTP - SERVER 10.20.20.6 255.255.255.224 Gateway: 10.20.20.1 (Same Interface to Firewall) DNS Server: 10.20.20.9	**DNS - SERVER** 10.20.20.9 255.255.255.224 Gateway: 10.20.20.1 DNS Server: 10.20.20.9
EMAIL SMTP - SERVER 10.20.20.7 255.255.255.224 Gateway: 10.20.20.1 DNS Server: 10.20.20.9	**DHCP 1 - SERVER** 10.20.20.10 255.255.255.224 Gateway: 10.20.20.1 DNS Server: 10.20.20.9
WEB - SERVER 10.20.20.8 255.255.255.224 Gateway: 10.20.20.1 DNS Server: 10.20.20.9	**DHCP 2 - SERVER** 10.20.20.11 255.255.255.224 Gateway: 10.20.20.1 DNS Server: 10.20.20.9

DHCP CONFIGURATION

We want both DHCPs servers to carry the same configuration. In order to attribute ip addresses to both HQ + Branch. There are 3 networks: Lan Wlan and MGMT,so we need to create 3 pools for Main HQ and 2 for Branch (as MGMT was only attributed in HQ IT-Dept). Before configuration make sure you are able to ping from any DHCP server to the default Gateway. The WLAN pool has extra configuration for the Wireless Controller.

HQ-POOLS	BRANCH POOLS
HQ-MGMT-POOL Default Gateway: 192.168.10.1 (1st IP as default gateway) DNS server: 10.20.20.9 Start IP Address: 192.168.10.11 Subnet Mask: 255.255.255.0 Maximum Number os users: 150	**BRANCH-LAN-POOL** Default Gateway: 172.17.0.1 (1st IP as default gateway) DNS server: 10.20.20.9 Start IP Address: 172.17.0.11 Subnet Mask: 255.255.0.0 Maximum Number os users: 60.000
HQ-LAN-POOL Default Gateway: 172.16.0.1 DNS server: 10.20.20.9 Start IP Address: 172.16.0.11 Subnet Mask: 255.255.0.0 Maximum Number os users: 40.000	**BRANCH-WLAN-POOL** Default Gateway: 10.11.0.1 (1st IP as default gateway) DNS server: 10.20.20.9 Start IP Address: 10.11.0.11 Subnet Mask: 255.255.0.0 Maximum Number os users: 150 WLC Address: 10.10.0.15
HQ-WLAN-POOL Default Gateway: 10.10.0.1 DNS server: 10.20.20.9 Start IP Address: 10.10.0.11 Subnet Mask: 255.255.0.0 Maximum Number os users: 64.000 WLC Address: 10.10.0.15	**** Branch MGMT is only attribute in HQ IT-DEPT**



DHCP POOL CONFIGURATIONS - CISCO PACKET TRACER

HSRP PROTOCOL + INTER-LAN ROUTING

This is done on All Core Switches, where we essentially create SVI's (Switch Virtual Interfaces). The HSRP(Hot Standby Router Protocol) works by allowing multiple routers to work together in a group, with one elected as the active router and others as standby. The active router handles traffic while the standby routers are ready to take over if the active router fails.The Standby Router(Always acts as the default router).

HQ- SWCORE1	**HQ- SWCORE2**
int vlan 10 ip add 192.168.10.3 255.255.255.0 ip helper-address 10.20.20.10 ip helper-address 10.20.20.11 standby 10 ip 192.168.10.1 exit int vlan 20 ip add 172.16.0.3 255.255.0.0 ip helper-address 10.20.20.10 ip helper-address 10.20.20.11 standby 20 ip 172.16.0.1 exit int vlan 50 ip add 10.10.0.3 255.255.0.0 ip helper-address 10.20.20.10 ip helper-address 10.20.20.11 standby 50 ip 10.10.0.1 Exit Do wr	int vlan 10 ip add 192.168.10.2 255.255.255.0 ip helper-address 10.20.20.10 ip helper-address 10.20.20.11 standby 10 ip 192.168.10.1 exit int vlan 20 ip add 172.16.0.2 255.255.0.0 ip helper-address 10.20.20.10 ip helper-address 10.20.20.11 standby 20 ip 172.16.0.1 exit int vlan 50 ip add 10.10.0.2 255.255.0.0 ip helper-address 10.20.20.10 ip helper-address 10.20.20.11 no standby 50 ip 10.10.0.1 Exit Do wr
Branch Core Switch A	**Branch Core Switch B**
int vlan 60 ip add 172.17.0.3 255.255.0.0 ip helper-address 10.20.20.10 ip helper-address 10.20.20.11 standby 60 ip 172.17.0.1 exit int vlan 80 ip add 10.11.0.3 255.255.0.0 ip helper-address 10.20.20.10 ip helper-address 10.20.20.11 standby 80 ip 10.11.0.1 Exit Do wr	int vlan 60 ip add 172.17.0.2 255.255.0.0 ip helper-address 10.20.20.10 ip helper-address 10.20.20.11 standby 60 ip 172.17.0.1 exit int vlan 80 ip add 10.11.0.2 255.255.0.0 ip helper-address 10.20.20.10 ip helper-address 10.20.20.11 standby 80 ip 10.11.0.1 Exit Do wr

```
MainA-Switch#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   100   Active   local           192.168.10.2    192.168.10.1
Vl20        20   100   Active   local           172.16.0.2      172.16.0.1
Vl50        10   100   Active   local           10.10.0.2       10.10.0.1
MainA-Switch#
```

HQ-CORE Switch1 - Active

```
Mainb-Switch#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   100   Standby  192.168.10.3    local           192.168.10.1
Vl20        20   100   Standby  172.16.0.3      local           172.16.0.1
Vl50        10   100   Standby  10.10.0.3       local           10.10.0.1
Mainb-Switch#
```

HQ-CORESwitch2 - Standby

OSPF (FIREWALL, ROUTERS + SWITCHES)

OSPF protocol is a dynamic routing protocol used to find the shortest paths for routing IP packets. offering fast convergence and scalable hierarchical design.Hello packets are sent periodically to establish and maintain neighbor relationships, building this way the entire network topology. A wild card mask is configured on Routers and Switches, and a subnet mask is configured on Firewall.

HQ-SWCORE1 *	**Branch SWCORE1**	**HQ-ISP Router**
Router ospf 15 Router-id 2.1.2.1 Network 10.20.20.32 0.0.0.3 area 0 Network 192.168.10.0 0.0.0.255 area 0 Network 172.16.0.0 0.0.0.255 area 0 Network 10.10.0.0 0.0.255.255 area 0 exit Do wr	router ospf 15 router-id 4.1.4.1 network 10.20.20.40 0.0.0.3 area 0 Network 172.17.0.0 0.0.0.255 area 0 Network 10.11.0.0 0.0.255.255 area 0 Exit Do wr	Router ospf 15 Router-id 6.1.6.1 network 20.20.20.0 0.0.0.3 area 0 network 105.100.50.0 0.0.0.3 area 0 Exit Do wr
HQ-SWCORE2 Switch	**Branch SWCORE2**	**Branch - ISP Router**
Router ospf 15 Router-id 3.1.3.1 Network 10.20.20.36 0.0.0.3 area 0 Network 192.168.10.0 0.0.0.255 area 0 Network 172.16.0.0 0.0.0.255 area 0 Network 10.10.0.0 0.0.255.255 area 0 exit Do wr	router ospf 15 router-id 5.1.5.1 network 10.20.20.44 0.0.0.3 area 0 Network 172.17.0.0 0.0.0.255 area 0 Network 10.11.0.0 0.0.255.255 area 0 Exit Do wr	Router ospf 15 Router-id 8.1.8.1 network 30.30.30.0 0.0.0.3 area 0 network 205.200.100.0 0.0.0.3 area 0 Exit Do wr
HQ-Firewall	**BRANCH-Firewall**	**ISP ROUTER**
Router ospf 15 Router-id 9.1.9.1 Network 105.100.50.0 255.255.255.252 area 0 Network 10.20.20.0 255.255.255.224 area 0 Network 10.20.20.32 255.255.255.252 area 0 Network 10.20.20.36 255.255.255.252 area 0 exit Wr mem	Router ospf 15 Router-id 10.1.10.1 Network 205.200.100.0 255.255.255.252 area 0 Network 10.20.20.40 255.255.255.252 area 0 Network 10.20.20.44 255.255.255.252 area 0 exit Wr mem	Router ospf 15 Router-id 7.1.7.1 network 20.20.20.0 0.0.0.3 area 0 network 30.30.30.0 0.0.0.3 area 0 Exit Do wr

* This devices needs to advertise 4 networks: 3 SVI previously created (MGMT, LAN AND WLAN), AND FIREWALL.

NAT + FIREWALL INSPECTION POLICIES

Before creating an Inspection Policy we will be Creating Object networks and associate them with NAT (Network Address Translation). NAT converts internal IP addresses to external ones for internet access and does the opposite for incoming traffic, allowing multiple devices to share a single public IP while keeping internal addresses private. In addition, configuring a firewall with a default static route is also a fundamental step in securing and managing networks. Any traffic that doesn't match specific allowed routes or policies is handled efficiently. Done in such a way that all the routes are forward to ISP.

HQ-firewall - Creating Objects + NAT

route OUTSIDE 0.0.0.0 0.0.0.0 105.100.50.1 (any IP address with any Subnet mask should be routed to ISP) - HERE WE SETTING DEFAULT STATIC ROUTE ON THE FIREWALLS.

MGMT	**LAN**	**WLAN**
object network INSIDE1-OUTSIDE Subnet 192.168.10.0 255.255.255.0 Nat (INSIDE1,OUTSIDE) dynamic interface object network INSIDE1a-OUTSIDE Subnet 192.168.10.0 255.255.255.0 nat (INSIDE2,OUTSIDE) dynamic interface ex	Config t object network INSIDE2-OUTSIDE Subnet 172.16.0.0 255.255.0.0 nat (INSIDE1,OUTSIDE) dynamic interface Ex Config t object network INSIDE2a-OUTSIDE Subnet 172.16.0.0 255.255.0.0 nat (INSIDE2,OUTSIDE) dynamic interface ex	Config t object network INSIDE3-OUTSIDE Subnet 10.10.0.0 255.255.0.0 nat (INSIDE1,OUTSIDE) dynamic interface Ex Config t object network INSIDE3a-OUTSIDE Subnet 10.10.0.0 255.255.0.0 nat (INSIDE2,OUTSIDE) dynamic interface Ex Wr mem

BRANCH-Firewall - Creating Objects + NAT

route OUTSIDE 0.0.0.0 0.0.0.0 205.200.100.1

	LAN	**WLAN**
No mgnt	object network INSIDE2-OUTSIDE Subnet 172.17.0.0 255.255.0.0 Nat (INSIDE1,OUTSIDE) dynamic interface object network INSIDE2A-OUTSIDE Subnet 172.17.0.0 255.255.0.0 Nat (INSIDE2,OUTSIDE) dynamic interface	object network INSIDE3-OUTSIDE Subnet 10.11.0.0 255.255.0.0 Nat (INSIDE1,OUTSIDE) dynamic interface object network INSIDE3A-OUTSIDE Subnet 10.11.0.0 255.255.0.0 Nat (INSIDE2,OUTSIDE) dynamic interface Wr mem

```
!
object network INSIDE1-OUTSIDE
 subnet 192.168.10.0 255.255.255.0
 nat (INSIDE1,OUTSIDE) dynamic interface
object network INSIDE1a-OUTSIDE
 subnet 192.168.10.0 255.255.255.0
 nat (INSIDE2,OUTSIDE) dynamic interface
object network INSIDE2-OUTSIDE
 subnet 172.16.0.0 255.255.0.0
 nat (INSIDE1,OUTSIDE) dynamic interface
object network INSIDE2a-OUTSIDE
 subnet 172.16.0.0 255.255.0.0
 nat (INSIDE2,OUTSIDE) dynamic interface
object network INSIDE3-OUTSIDE
 subnet 10.10.0.0 255.255.0.0
 nat (INSIDE1,OUTSIDE) dynamic interface
object network INSIDE3a-OUTSIDE
 subnet 10.10.0.0 255.255.0.0
 nat (INSIDE2,OUTSIDE) dynamic interface
!
route OUTSIDE 0.0.0.0 0.0.0.0 105.100.50.1 1
!
!
```

HQ-Firewall Objects + Static Routing

Creating Inspection Policies + ACLS
This will be a basic setup, for project purposes, I am not putting a lot of restrictions in place.

HQ-Firewall

access-list RESOURCE-RULES EXtended permit icmp any any
access-list RESOURCE-RULES extended permit udp any any eq 67 (Allow DHCP, witch uses udp on Port 67-68)
access-list RESOURCE-RULES extended permit udp any any eq 68
access-list RESOURCE-RULES extended permit udp any any eq 53 (Allow DNS, wich uses upd and tcp on port 53)
access-list RESOURCE-RULES extended permit tcp any any eq 53
access-list RESOURCE-RULES extended permit tcp any any eq 25 (Allow SMTP, port 25)
access-list RESOURCE-RULES extended permit tcp any any eq 20 (Allow FTP, port 20-21)
access-list RESOURCE-RULES extended permit tcp any any eq 21

Once you create your inspection policies you have to bind them into the interfaces:

access-group RESOURCE-RULES in interface DMZ
access-group RESOURCE-RULES in interface OUTSIDE
Wr mem
(Copy same configuration the the Branch Firewall, except NO DMZ zone)

WIFI AP'S + WIRELESS LAN CONTROLLER (SYNC)

At this stage we need to ensure that CAPWAP UDP ports 5246 and 5247 are enabled on the Firewall + LWAPP UDP ports 12222 and 12223.

HQ-Firewall (CAPWAP UDP ports)
access-list RESOURCE-RULES extended permit udp any any eq 5246
access-list RESOURCE-RULES extended permit udp any any eq 5247
access-list RESOURCE-RULES extended permit udp any any eq 12222
access-list RESOURCE-RULES extended permit udp any any eq 12223
Wr mem

```
Device Name: HR-WIFI
Device Model: LAP-PT

Port                Link   IP Address          MAC Address
GigabitEthernet0    Up     10.10.0.15/16       0060.4702.416E
Dot11Radio0         Up     <not set>           0000.0C78.5057

CAPWAP Status: Connected to 10.10.0.16
Providing WLANs:
    EMPLOYEE-WIFI (EMPLOYEE-WIFI)
    CORPORATE-WIFI (CORPORATE-WIFI)
    VISITOR-WIFI (VISITOR-WIFI)
```

WIFI CONTROLLER - HQ WIFI WLANS

```
Device Name: HEALTH-WIFI
Device Model: LAP-PT

Port                Link   IP Address          MAC Address
GigabitEthernet0    Up     10.11.0.13/16       0002.4ABD.7ECE
Dot11Radio0         Up     <not set>           0003.E435.C02D

CAPWAP Status: Connected to 10.10.0.16
Providing WLANs:
    EMPLOYEE-WIFI (EMPLOYEE-WIFI)
    CORPORATE-WIFI (CORPORATE-WIFI)
    VISITOR-WIFI (VISITOR-WIFI)
```

WIFI CONTROLLER- BRANCH WIFI WLANS (in sync) Success

SITE-TO-SITE IPsec VPN CHANNEL

This last configuration step (On the Firewalls) is to encrypt communication between both networks over the Internet(HQ + Branch). Asides from Facilitating secure connections between geographically dispersed locations, it keeps it more robust and secure.

HQ-FW

```
crypto ikev1 policy 10
Hash sha
Authentication pre-share
Group 2
Lifetime 86400
Encryption 3des
Exit
tunnel-group 205.200.100.2 type IPsec-l2l
tunnel-group 205.200.100.2 IPsec-attributes
ikev1 pre-shared-key ciscolandia
crypto ipsec ikev1 transform-set TSET esp-3des esp-sha-hmac
access-list VPN-ACL permit ip 192.168.10.0 255.255.255.0 172.17.0.0 255.255.0.0
access-list VPN-ACL permit ip 192.168.10.0 255.255.255.0 10.11.0.0 255.255.0.0
access-list VPN-ACL permit ip 172.16.0.0 255.255.255.0 172.17.0.0 255.255.0.0
access-list VPN-ACL permit ip 172.16.0.0 255.255.255.0 10.11.0.0 255.255.0.0
access-list VPN-ACL permit ip 10.10.0.0 255.255.255.0 172.17.0.0 255.255.0.0
access-list VPN-ACL permit ip 10.10.0.0 255.255.255.0 10.11.0.0 255.255.0.0
access-list VPN-ACL permit ip 10.20.20.0 255.255.255.224 172.17.0.0 255.255.0.0
access-list VPN-ACL permit ip 10.20.20.0 255.255.255.224  10.11.0.0 255.255.0.0
crypto map CMAP 10 set peer 205.200.100.2
crypto map CMAP 10 set ikev1 transform-set TSET
crypto map CMAP 10 match address VPN-ACL
Crypto map CMAP interface OUTSIDE
crypto ikev1 enable OUTSIDE
wr mem
```

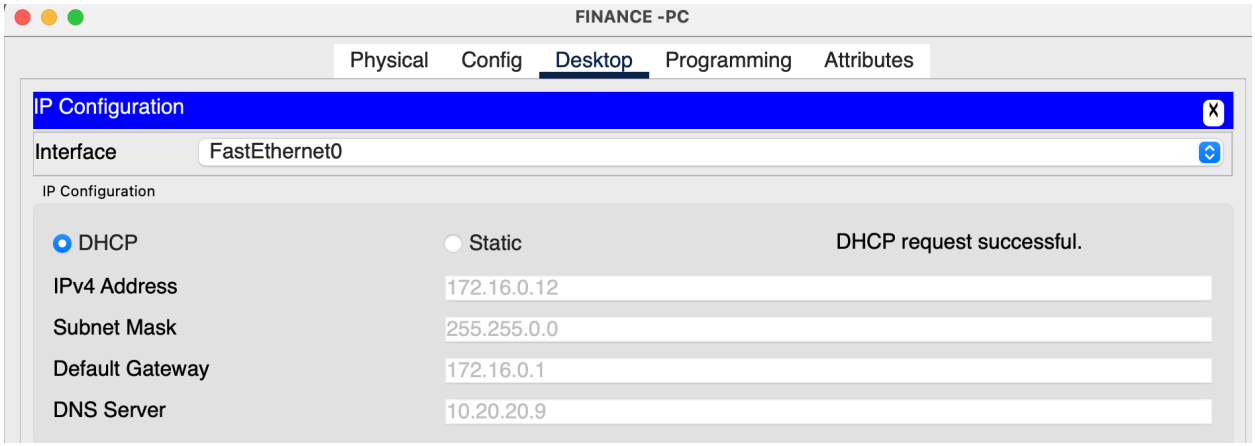
(to check settings: **show crypto isakmp sa** | to check packets encrypted: **show crypto ipsec sa**)

BRANCH-FW

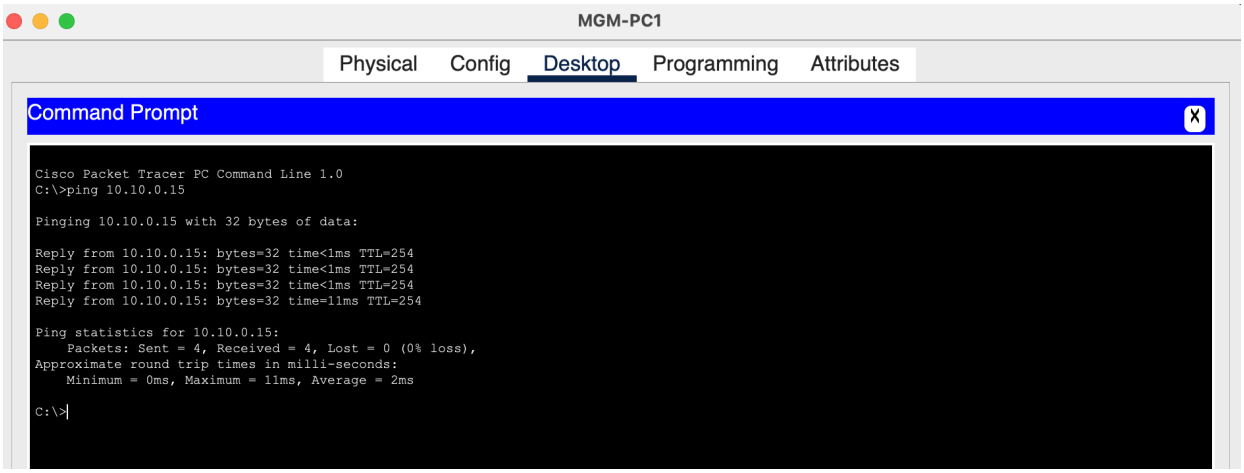
```
Crypto ikev1 policy 10
Hash sha
Authentication pre-share
Group 2
Lifetime 86400
Encryption 3des
Exit
tunnel-group 105.100.50.2 type IPsec-l2l
tunnel-group 105.100.50.2 IPsec-attributes
Ikev1 pre-shared-key ciscolandia
Crypto ipsec ikev1 transform-set TSET esp-3des esp-sha-hmac
access-list VPN-ACL permit ip 172.17.0.0 255.255.0.0 192.168.10.0 255.255.255.0
access-list VPN-ACL permit ip 10.11.0.0 255.255.0.0 192.168.10.0 255.255.255.0
access-list VPN-ACL permit ip 172.17.0.0 255.255.0.0 172.16.0.0 255.255.255.0
access-list VPN-ACL permit ip 10.11.0.0 255.255.0.0 172.16.0.0 255.255.255.0
access-list VPN-ACL permit ip 172.17.0.0 255.255.0.0 10.10.0.0 255.255.255.0
access-list VPN-ACL permit ip 10.11.0.0 255.255.0.0 10.10.0.0 255.255.255.0
access-list VPN-ACL permit ip 10.20.20.0 255.255.255.224 172.17.0.0 255.255.0.0
access-list VPN-ACL permit ip 10.11.0.0 255.255.0.0 10.20.20.0 255.255.255.224
crypto map CMAP 10 set peer 205.200.100.2
crypto map CMAP 10 set ikev1 transform-set TSET
crypto map CMAP 10 match address VPN-ACL
Crypto map CMAP interface OUTSIDE
crypto ikev1 enable OUTSIDE
wr mem
```

TESTING + TROUBLESHOOTING

DHCP IP Assigning (Lan + Wlan)

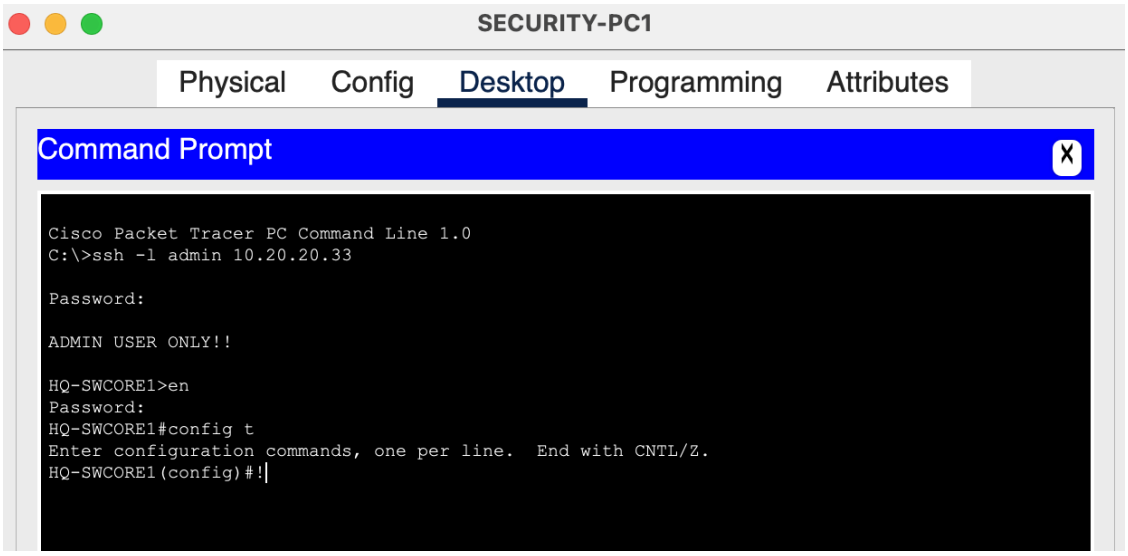


DHCP IP CONFIGURATION - Successful Request - Finance-PC HQ



Ping wireless controller from Security PC - 0% packets loss

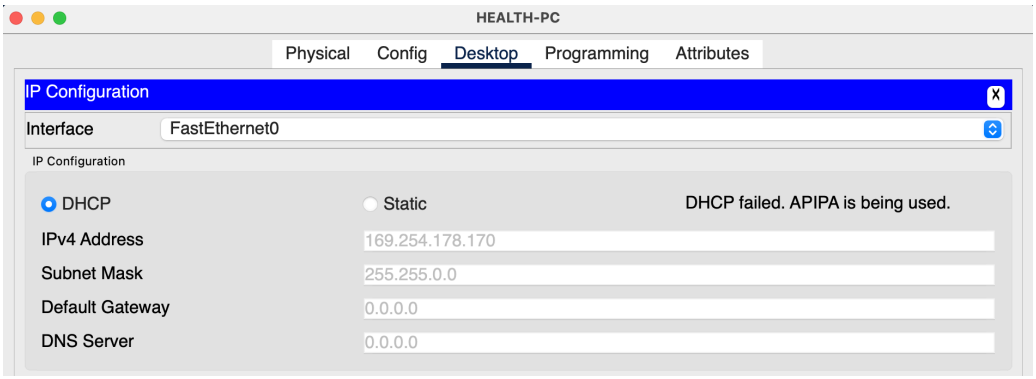
SSH From Security PC's Network



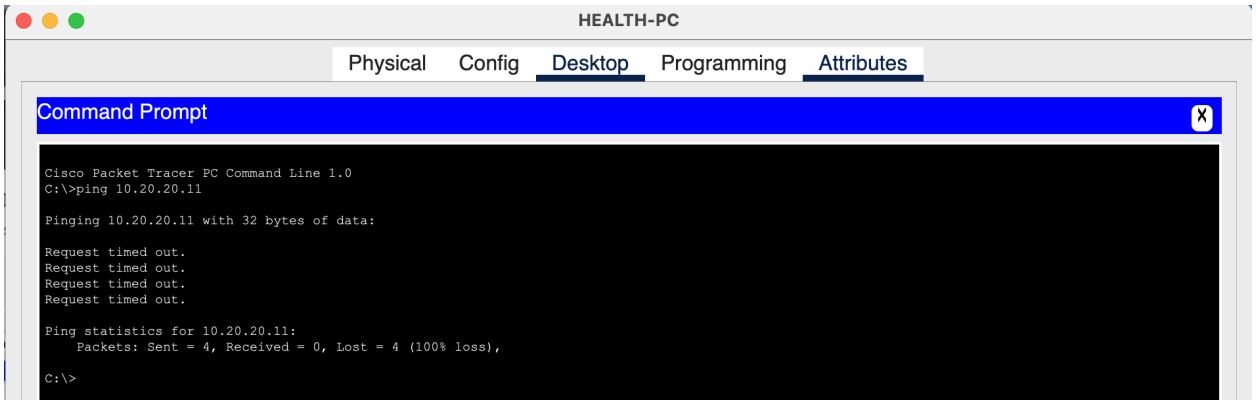
ssh to HQ-CoreSwitch from Security PC1 - successful.

Troubleshooting

Even though the DHCP Server Managed to provide IP addresses for All End-Point devices in the HQ Network, it failed to do so on the Branch Side, prompting a warning Sign *"DHCP Failed.APIPA is being used"* At this stage both Servers in the DMZ zone were behind 3 Routers and a Firewall before even reaching the Branch Multilayer Switches. At first I tried to ping both servers from all Branch Computers without success. The firewall was allowing ICMP traffic. Here is a list of relevant troubleshooting commands on Cisco devices: **Traceroute- Tarcert -d - Sh ip route - Sh ip interface - Sh ip interface brief - Sh interfaces serial0/0/1**



Branch Computer DHCP IP attribution Failed: APIPA is being used



PING ATTEMPT ON DHCP SERVER 10.20.20.11 - FAILED. 100% LOSS

```
ciscoasa#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300
access-list RESOURCE-RULES; 12 elements; name hash: 0xca76162d
access-list RESOURCE-RULES line 1 extended permit icmp any any(hitcnt=0) 0x336d10e4
access-list RESOURCE-RULES line 2 extended permit udp any any eq bootps(hitcnt=0) 0xbec08ce8
access-list RESOURCE-RULES line 3 extended permit udp any any eq bootpc(hitcnt=0) 0x7893b63d
access-list RESOURCE-RULES line 4 extended permit udp any any eq domain(hitcnt=0) 0xc381ce84
access-list RESOURCE-RULES line 5 extended permit tcp any any eq domain(hitcnt=0) 0x36ea18ce
access-list RESOURCE-RULES line 6 extended permit tcp any any eq smtp(hitcnt=0) 0x80cb82e4
access-list RESOURCE-RULES line 7 extended permit tcp any any eq 20(hitcnt=0) 0x6993c6cc
access-list RESOURCE-RULES line 8 extended permit tcp any any eq ftp(hitcnt=0) 0xd869a255
access-list RESOURCE-RULES line 9 extended permit udp any any eq 5246(hitcnt=0) 0x9e847390
access-list RESOURCE-RULES line 10 extended permit udp any any eq 5247(hitcnt=0) 0x4859ebac
access-list RESOURCE-RULES line 11 extended permit udp any any eq 12222(hitcnt=0) 0x86d4243c
access-list RESOURCE-RULES line 12 extended permit udp any any eq 12223(hitcnt=0) 0xb0bbc9ad
ciscoasa#
```

FIREWALL(BRANCH) CONFIGURATION ALLOWING ICMP TRAFFIC

Step by step I analyzed configurations from both locations, to make sure all Vlans and ports were assigned properly. On the Access Switches the interface fa-0/-1-2 were correctly set up to trunk Mode. However when I checked on the Multilayer Switch there seems to be a conflict on the HSRP protocol configuration. More specifically it was telling me that the Virtual IP was different on both Switches on the same Vlan 60. I Quickly fix this issue on Branch Multilayer Switch B, by resetting Vlan Configuration and adding the command: standby 60 ip 172.17.0.1 .

```
sh int status
Port      Name               Status       Vlan       Duplex  Speed Type
Po2                          connected    trunk      auto    auto
Gig1/0/1                     connected    routed     auto    auto  10/100BaseTX
Gig1/0/2                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/3                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/4                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/5                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/6                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/7                     notconnect   1          auto    auto  10/100BaseTX
Gig1/0/8                     notconnect   1          auto    auto  10/100BaseTX
Gig1/0/9                     notconnect   1          auto    auto  10/100BaseTX
Gig1/0/10                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/11                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/12                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/13                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/14                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/15                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/16                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/17                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/18                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/19                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/20                    notconnect   1          auto    auto  10/100BaseTX
 --More-- %HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
%HSRP-4-DIFFVIP1: Vlan60 Grp 60 active routers virtual IP address 172.17.0.2 is different to the locally configured address 172.17.0.1
```

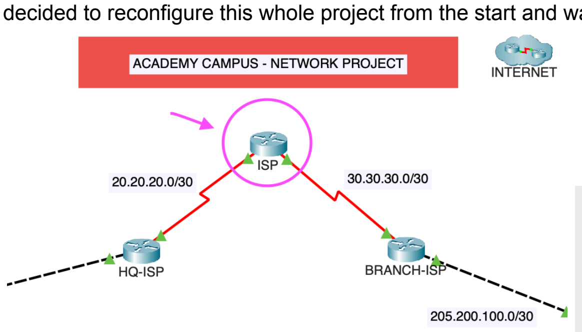
Branch Core Multilayer Switch - HSRP conflit

```
sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   100   Standby 192.168.10.5    local           192.168.10.1
Vl60        60   100   Active  local           172.17.0.2      172.17.0.1
Vl80        80   100   Active  local           10.11.0.2       10.11.0.1
BranchA-Switch#
```

```
                      |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   100   Active  local           192.168.10.4    192.168.10.1
Vl60        60   100   Standby 172.17.0.3      local           172.17.0.2
Vl80        80   100   Standby 10.11.0.3       local           10.11.0.1
```

BRANCH A VS BRANCH (CORE SWITCHES) ON Vlan 60, the Virtual IP was different between the Multilayer Switches.

I try a few extra steps in order to try and narrow down the extensive list of network issues:
Tried to reach DHCP server from a Computer on the Branch side that had configured a Static IP Address for testing - failed to reach.
Ping DHCP from Router HQ-ISP successfully, but the Router ISP failed to reach the DHCP server. This helped me identify that the problem was there. I had forgotten to configure the OSPF protocol on the ISP router, and failed to advertise both interfaces leading to and out between Serial DCE connections HQ and Branch. In addition to that, the Vlan interfaces were not properly set up. So I decided to reconfigure this whole project from the start and was able to fix the issues.




```
%SYS-5-CONFIG_I: Configured from console by console
ping 10.20.20.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.11, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Router#
```

ISP ROUTER UNABLE TO REACH DHCP SERVER - ping command

NETWORK SECURITY - MITIGATIONS

- Set up complex passwords on all Network and End Point Devices (Firewall, Core Switches + Access Layer Switches Dept PC's)
- All passwords must be different.
- Network Segmentation (VLans, DMZ, subnets)
- Allow SSH only to a specified secure Vlan (ex. IT Computers)
- Shut Down unused Ports on all Network Devices (Blackhole VLan) + Firewall Port Hardening
- Apply 0 trust to Outside Zone (Firewall configuration)
- Set up ACL's (Access control lists).
- Create Inspection Policies on the firewall to filter traffic.
- Employ VPN between both Branches to encrypt data transmission.
- Load Balance + Redundancy between imperial servers to ensure availability(In this project, i had 2 DHCP servers)
- Ensure WIFI security, respecting the latest up to date encryption protocols like WPA3 and disabling WPS1.0

RESOURCES

I am deeply grateful to GuruTechNetworks, particularly Mr. Benard Otom, for their invaluable educational videos and relentless support. Their platform, gurutechnetworks.otombenard.com, has been a beacon of knowledge, offering keen insights and patient guidance that have profoundly influenced my understanding of network architecture.This case study was developed under the influence of GuruTechNetworks and exemplifies this enriched understanding. It incorporates advanced principles of network architecture, seamlessly integrating theory with practical applications.

Research Links:

https://zindagitech.com/7-easy-steps-to-configure-site-to-site-ipsec-vpn-using-ikev1-on-cisco-asa/
https://gurutechnetworks.otombenard.com/about
https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/port_sec.html#wp1070356
https://httpdump.app/
https://www.cisco.com/c/en/us/support/index.htm
https://skillsforall.com/
https://learningnetwork.cisco.com/s/question/0D56e0000C4N9csCQC/ikev1-versus-ikev2
https://www.geeksforgeeks.org/portfast-configured-on-a-cisco-switch-port/