Enterprise Network

DEPI PROJECT

TEAM MEMBERS

Ali Abdulqawi Ali

Fresh graduate from the Faculty of Computers and Information, IT Department. I have certification in CCNA, MCSA and CCNA.

Mohamed Abdelaziz Eltawil

Fresh graduate from the Faculty of Computers and Information, IT Department. I have certification in CCNA, MCSA and CCNA.

Mahmoud Ibrahim Kamal

A hardworking computer science and AI student with CCNA and CCNP certifications, I enjoy presenting on the latest tech developments and seek to join an innovative team focused on creating cutting-edge solutions.

Abdelrahman Moustafa Elsayed

Fresh graduate from the Faculty of Computers and Information, IT Department. I have certification in CCNA, MCSA and CCNA.

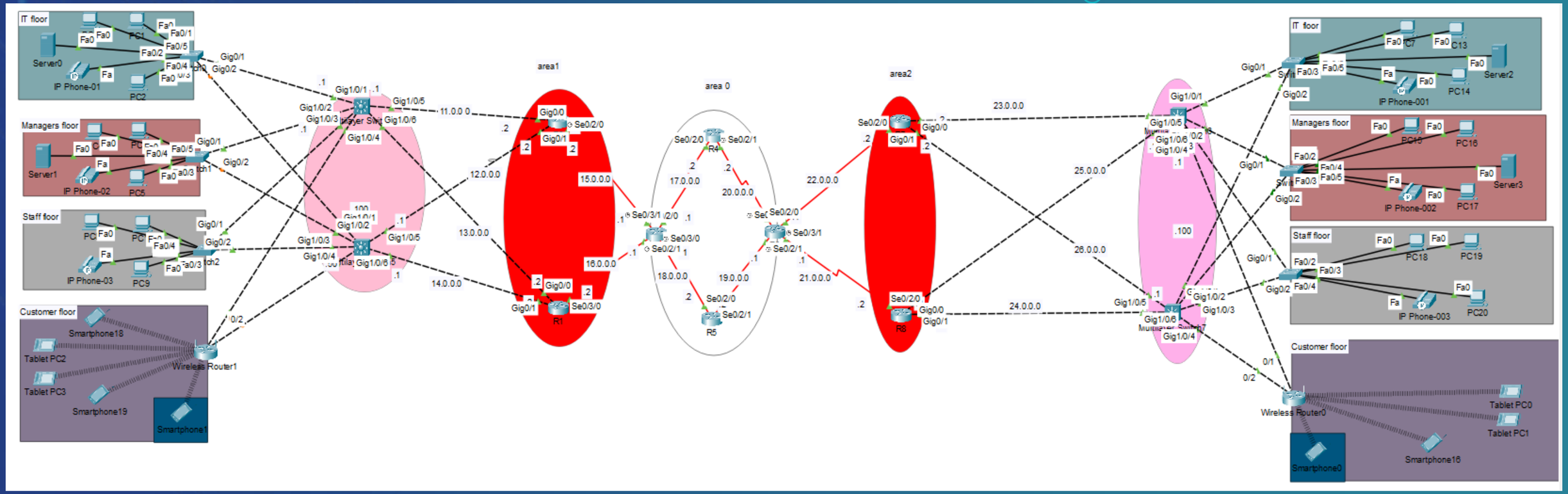
Supervisor Eng. Magdy Ibrahim

Enterprise Network

OUTLINE

Enterprise Network

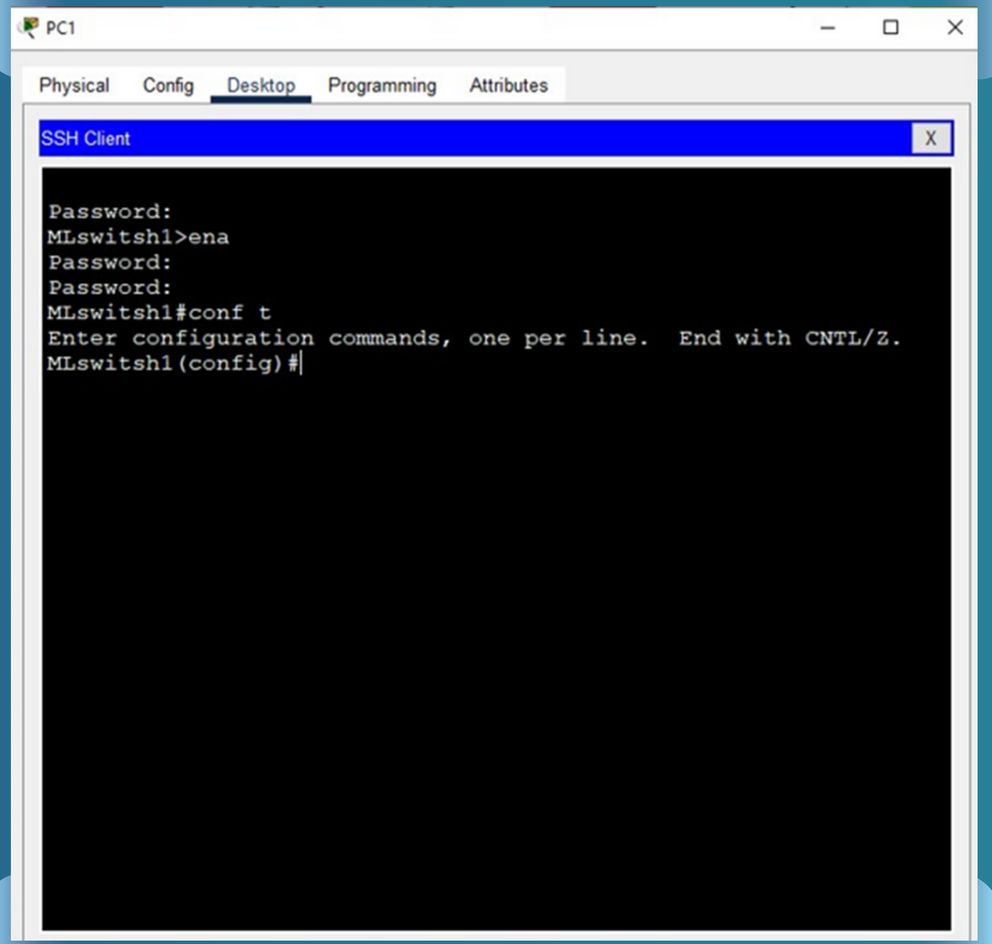
PROJECT DESING



Enterprise Network

SSH

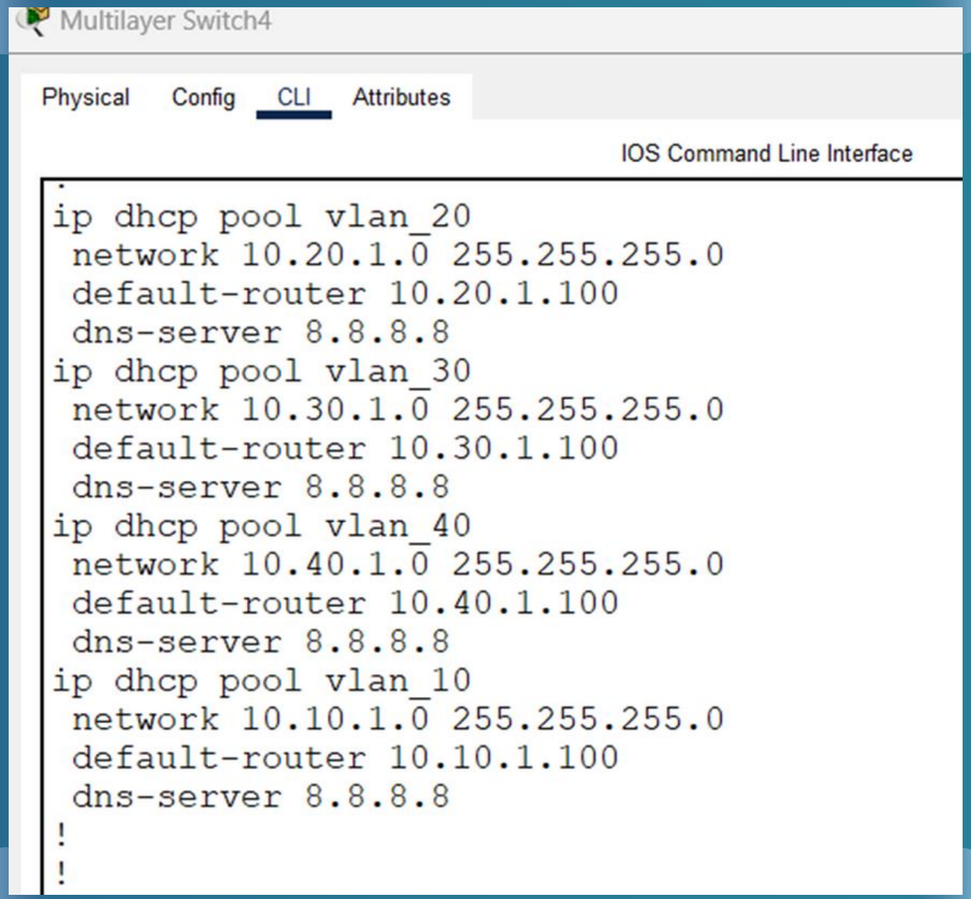
WE PRIORITIZED SECURITY BY IMPLEMENTING SSH ON OUR NETWORK ROUTERS AND SWITCHES. SSH ENCRYPTS DATA, MAKING IT A SAFER ALTERNATIVE TO TELNET. THIS PROTECTS CRUCIAL INFORMATION LIKE PASSWORDS AND CONFIGURATIONS FROM POTENTIAL CYBERATTACKS



Enterprise Network

DHCP

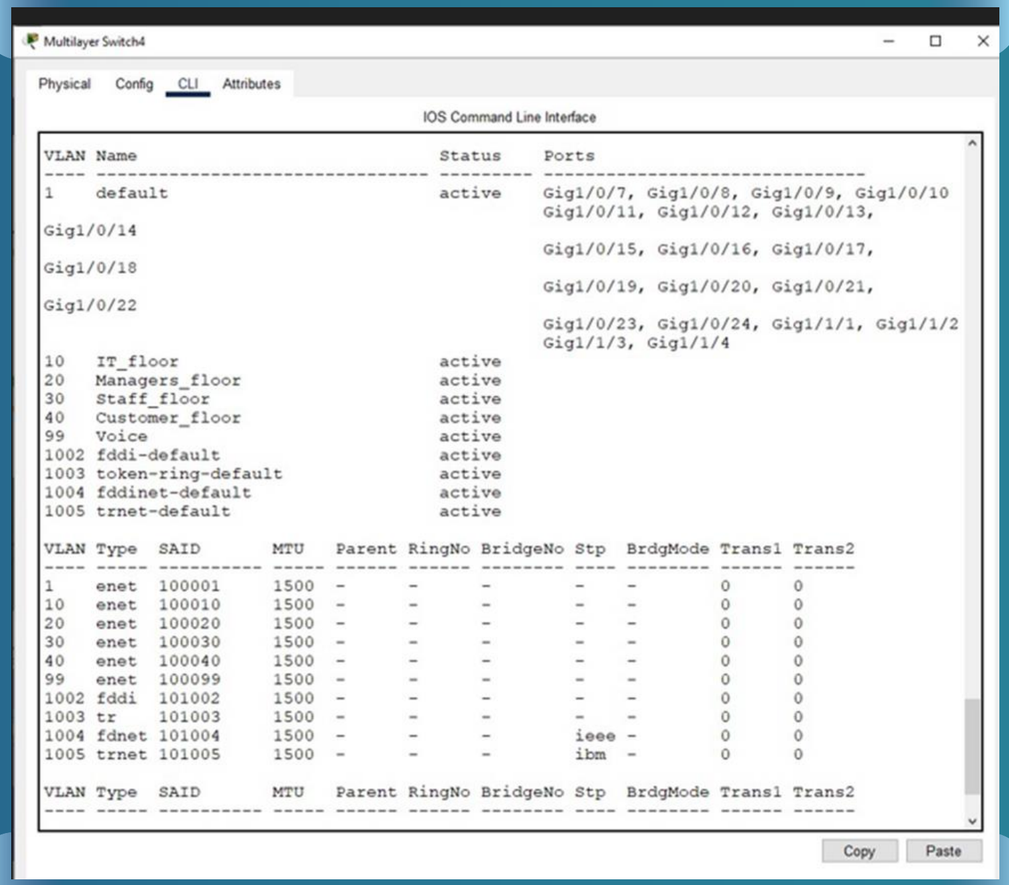
TO ENSURE EFFICIENT IP ADDRESS MANAGEMENT, WE IMPLEMENTED DHCP ON OUR NETWORK. THIS AUTOMATED SYSTEM DYNAMICALLY ASSIGNS IP ADDRESSES, SUBNET MASKS, GATEWAYS, AND DNS SETTINGS TO DEVICES AS THEY CONNECT TO THE NETWORK. THIS ELIMINATES THE NEED FOR MANUAL CONFIGURATION, SAVING TIME AND PREVENTING IP ADDRESS CONFLICTS.



Enterprise Network

VLAN

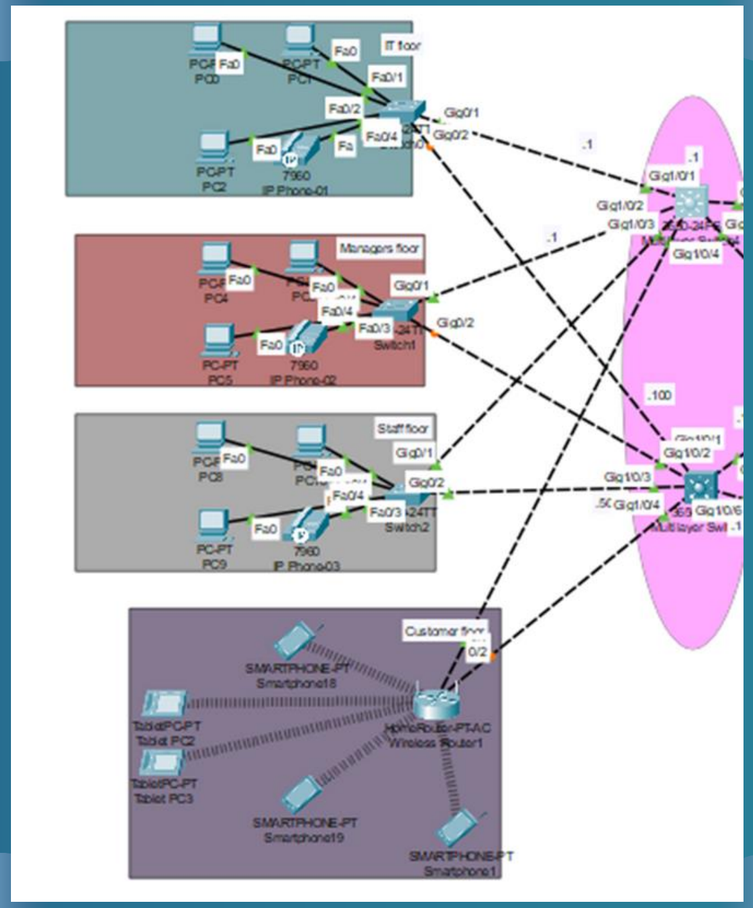
WE IMPLEMENTED VLANS TO ENHANCE NETWORK SECURITY AND EFFICIENCY. BY SEGREGATING NETWORK TRAFFIC INTO DIFFERENT DEPARTMENTS (IT, MANAGEMENT, STAFF, AND CUSTOMER), WE IMPROVED PERFORMANCE AND MINIMIZED SECURITY RISKS. EACH VLAN HAD ITS OWN IP ADDRESS RANGE, FURTHER BOLSTERING SECURITY.



Enterprise Network

HSRP

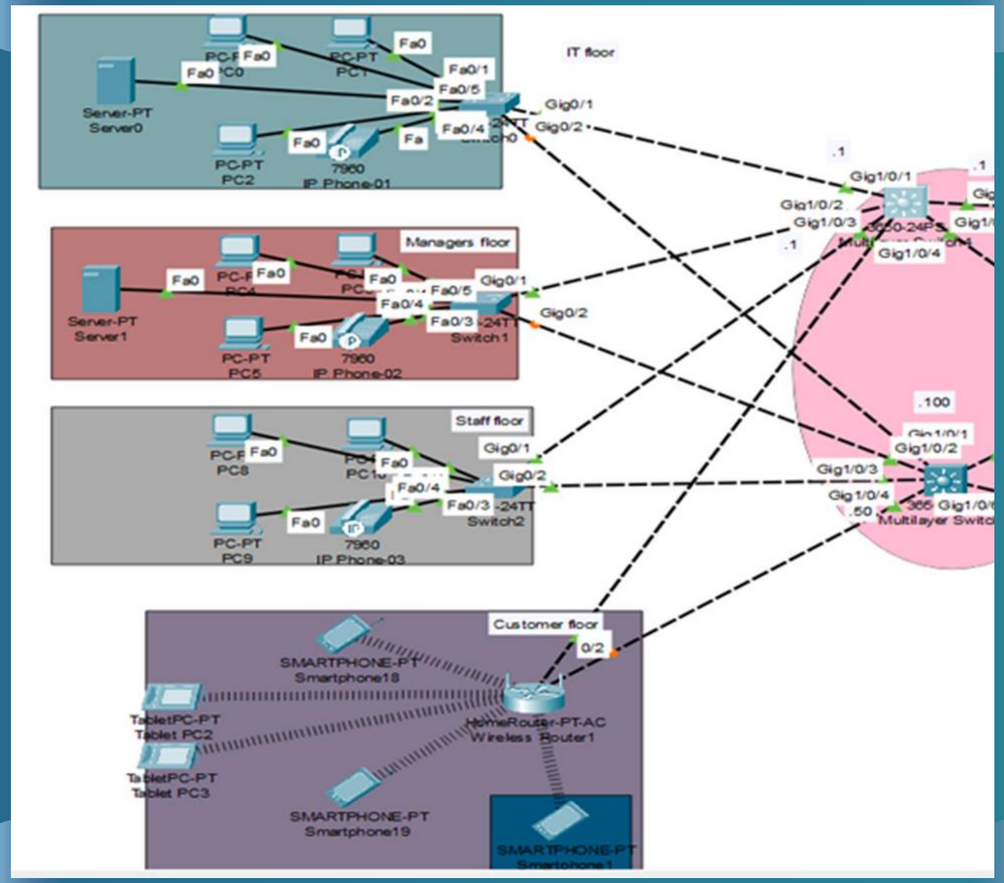
TO ENSURE UNINTERRUPTED NETWORK SERVICES, WE IMPLEMENTED HSRP ON OUR ROUTERS. THIS REDUNDANCY PROTOCOL ALLOWS MULTIPLE ROUTERS TO WORK TOGETHER, WITH ONE ACTING AS THE PRIMARY AND THE OTHERS AS BACKUPS. IF THE PRIMARY ROUTER FAILS, A BACKUP AUTOMATICALLY TAKES OVER, ENSURING MINIMAL DOWNTIME AND CONTINUOUS NETWORK ACCESS.



Enterprise Network

INTER-VLAN

TO ACHIEVE A MORE EFFICIENT AND FLEXIBLE NETWORK, WE CHOSE MLS AS THE BEST SOLUTION TO CONNECT VLANS IN OUR PROJECT. THIS TECHNOLOGY COMBINES THE ADVANTAGES OFFERED BY SWATCHES WITH TRADITIONAL TENSIONS, MAKING IT EASIER TO MANAGE AND EXPAND THE NETWORK.



Enterprise Network

STATIC & OSPF ROUTING

IN OUR PROJECT, WE USED A HYBRID SOLUTION THAT COMBINES A MULTI-AREA OSPF PROTOCOL WITH STATIC ROUTING TO ACHIEVE GREATER NETWORK MANAGEMENT FLEXIBILITY. WE REDISTRIBUTED STATIC NETWORKS WITHIN OSPF REGIONS TO ENSURE SEAMLESS ACCESS BETWEEN DIFFERENT PARTS OF THE NETWORK

```
     10.0.0.0/24 is subnetted, 5 subnets
O E2    10.10.1.0/24 [110/20] via 17.0.0.1, 00:01:15, Serial0/2/0
O E2    10.20.1.0/24 [110/20] via 17.0.0.1, 00:01:15, Serial0/2/0
O E2    10.30.1.0/24 [110/20] via 17.0.0.1, 00:01:15, Serial0/2/0
O E2    10.40.1.0/24 [110/20] via 17.0.0.1, 00:01:15, Serial0/2/0
O E2    10.99.1.0/24 [110/20] via 17.0.0.1, 00:01:15, Serial0/2/0
                     [110/20] via 20.0.0.1, 00:01:15, Serial0/2/1
     11.0.0.0/24 is subnetted, 1 subnets
O IA    11.0.0.0/24 [110/129] via 17.0.0.1, 00:01:15, Serial0/2/0
     12.0.0.0/24 is subnetted, 1 subnets
O IA    12.0.0.0/24 [110/129] via 17.0.0.1, 00:01:15, Serial0/2/0
     13.0.0.0/24 is subnetted, 1 subnets
O IA    13.0.0.0/24 [110/129] via 17.0.0.1, 00:01:15, Serial0/2/0
     14.0.0.0/24 is subnetted, 1 subnets
O IA    14.0.0.0/24 [110/129] via 17.0.0.1, 00:01:15, Serial0/2/0
     15.0.0.0/24 is subnetted, 1 subnets
O IA    15.0.0.0/24 [110/128] via 17.0.0.1, 00:01:15, Serial0/2/0
     16.0.0.0/24 is subnetted, 1 subnets
O IA    16.0.0.0/24 [110/128] via 17.0.0.1, 00:01:15, Serial0/2/0
     17.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       17.0.0.0/24 is directly connected, Serial0/2/0
L       17.0.0.2/32 is directly connected, Serial0/2/0
     18.0.0.0/24 is subnetted, 1 subnets
O       18.0.0.0/24 [110/128] via 17.0.0.1, 00:01:15, Serial0/2/0
     19.0.0.0/24 is subnetted, 1 subnets
O       19.0.0.0/24 [110/128] via 20.0.0.1, 00:01:15, Serial0/2/1
     20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       20.0.0.0/24 is directly connected, Serial0/2/1
L       20.0.0.2/32 is directly connected, Serial0/2/1
     21.0.0.0/24 is subnetted, 1 subnets
```

Enterprise Network

NAT

TO FACILITATE COMMUNICATION BETWEEN INTERNAL AND EXTERNAL NETWORKS, WE IMPLEMENTED NAT ON OUR CORE ROUTERS. THIS ENABLED MULTIPLE DEVICES TO SHARE A SINGLE PUBLIC IP ADDRESS FOR INTERNET ACCESS, CONSERVING IP ADDRESSES AND PROVIDING A LAYER OF SECURITY BY PREVENTING DIRECT EXTERNAL ACCESS TO INTERNAL DEVICES

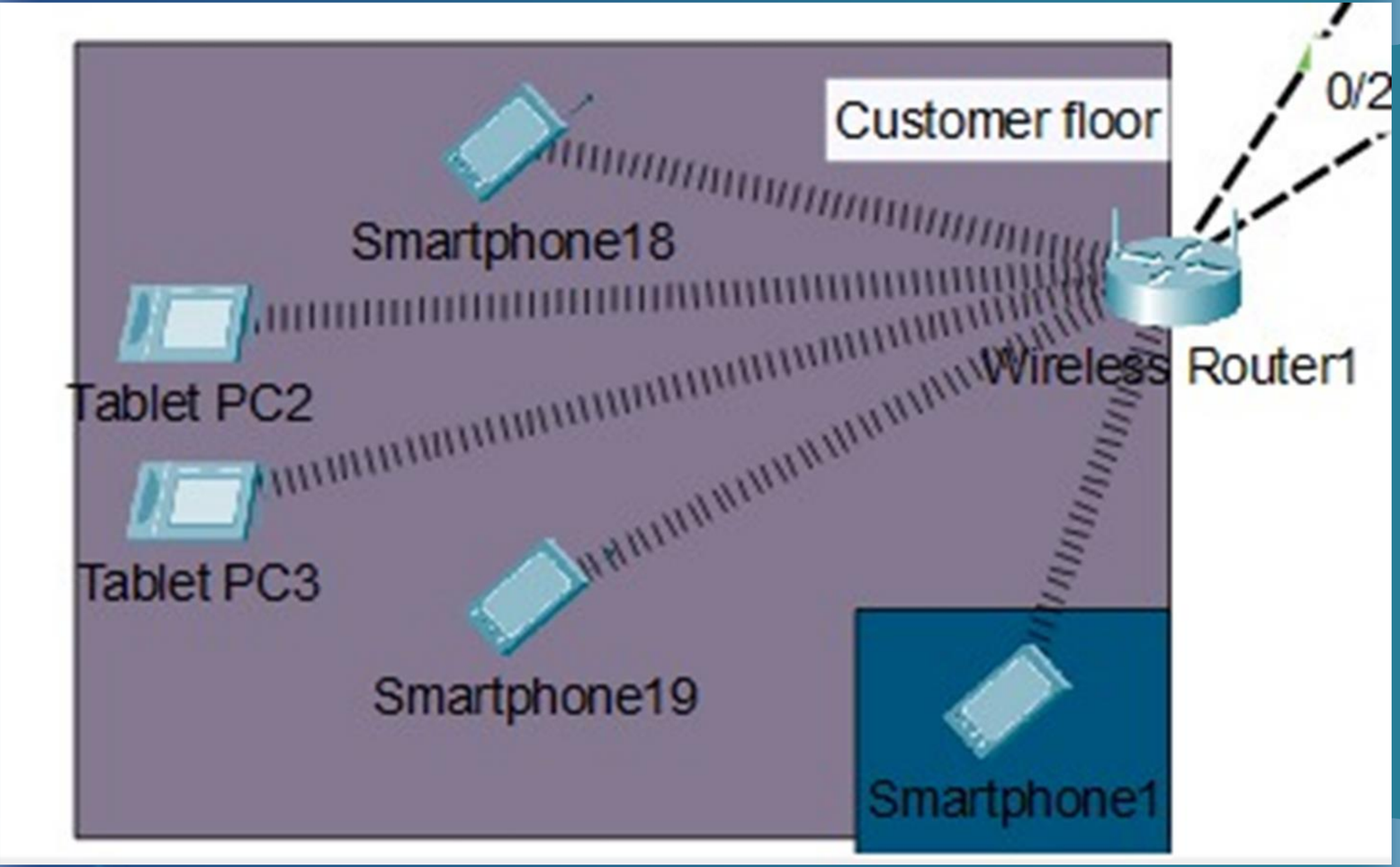
IOS Command Line Interface

```
Username: Elwa
Password:
r1>ena
Password:
r1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r1(config)#do show ip nat translation
r1(config)#do show ip nat st
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/2/0
Inside Interfaces: GigabitEthernet0/0 , GigabitEthernet0/1
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list NAT-ACL pool pat refCount 0
 pool pat: netmask 255.255.255.252
       start 15.0.0.5 end 15.0.0.6
       type generic, total addresses 2 , allocated 0 (0%), misses 0
r1(config)#do show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 15.0.0.5:1        10.10.1.5:1        192.168.10.3:1     192.168.10.3:1
icmp 15.0.0.5:2        10.10.1.5:2        192.168.10.3:2     192.168.10.3:2
icmp 15.0.0.5:3        10.10.1.5:3        192.168.10.3:3     192.168.10.3:3
icmp 15.0.0.5:4        10.10.1.5:4        192.168.10.3:4     192.168.10.3:4
icmp 15.0.0.5:5        10.10.1.5:5        192.168.10.3:5     192.168.10.3:5

r1(config)#
```

Enterprise Network

WIRELESS



Enterprise Network

PORT SECURITY & BPDU GUARD

TO PROTECT AGAINST MAC ADDRESS TABLE ATTACKS, WE IMPLEMENTED PORT SECURITY ON ALL SWITCHES IN THE NETWORK.

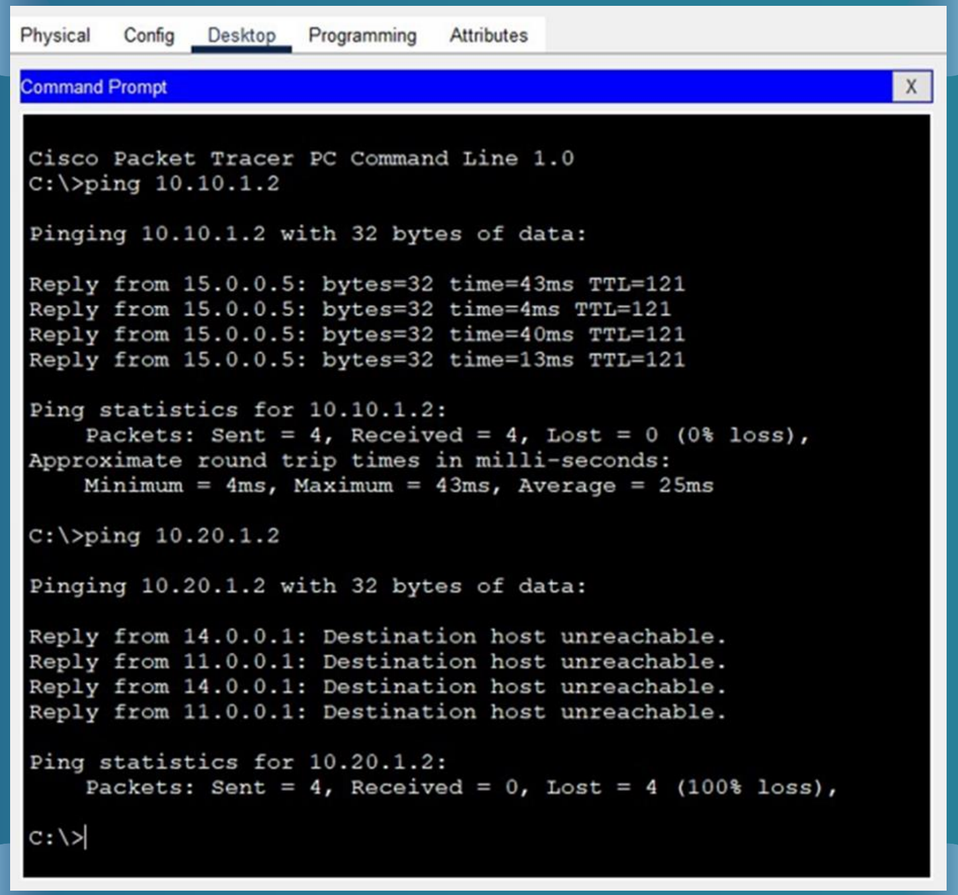
AND ALSO TO PREVENT STP ATTACKS, WE ENABLED PORT FAST AND BPDU GUARD ON ALL SWITCHES. PORT FAST SPEEDS UP NETWORK CONVERGENCE, WHILE BPDU GUARD BLOCKS UNAUTHORIZED BPDUS.

```
Switch#sho port-security interface f0/1
Port Security                   : Enabled
Port Status                     : Secure-up
Violation Mode                  : Restrict
Aging Time                      : 10 mins
Aging Type                      : Absolute
SecureStatic Address Aging      : Disabled
Maximum MAC Addresses           : 4
Total MAC Addresses             : 1
Configured MAC Addresses        : 0
Sticky MAC Addresses            : 1
Last Source Address:Vlan        : 0060.3E35.5A01:10
Security Violation Count        : 0
```

Enterprise Network

ACL

WE CONFIGURED ACLS TO REGULATE THE FLOW OF TRAFFIC,
allowing only authorized devices and users to access specific
parts of the network. ACLs provide a foundational layer of security, preventing malicious traffic from entering critical areas of the network, like the management or IT floors. With
precise ACL rules, we've minimized the risk of internal and external threats



Enterprise Network

AAA

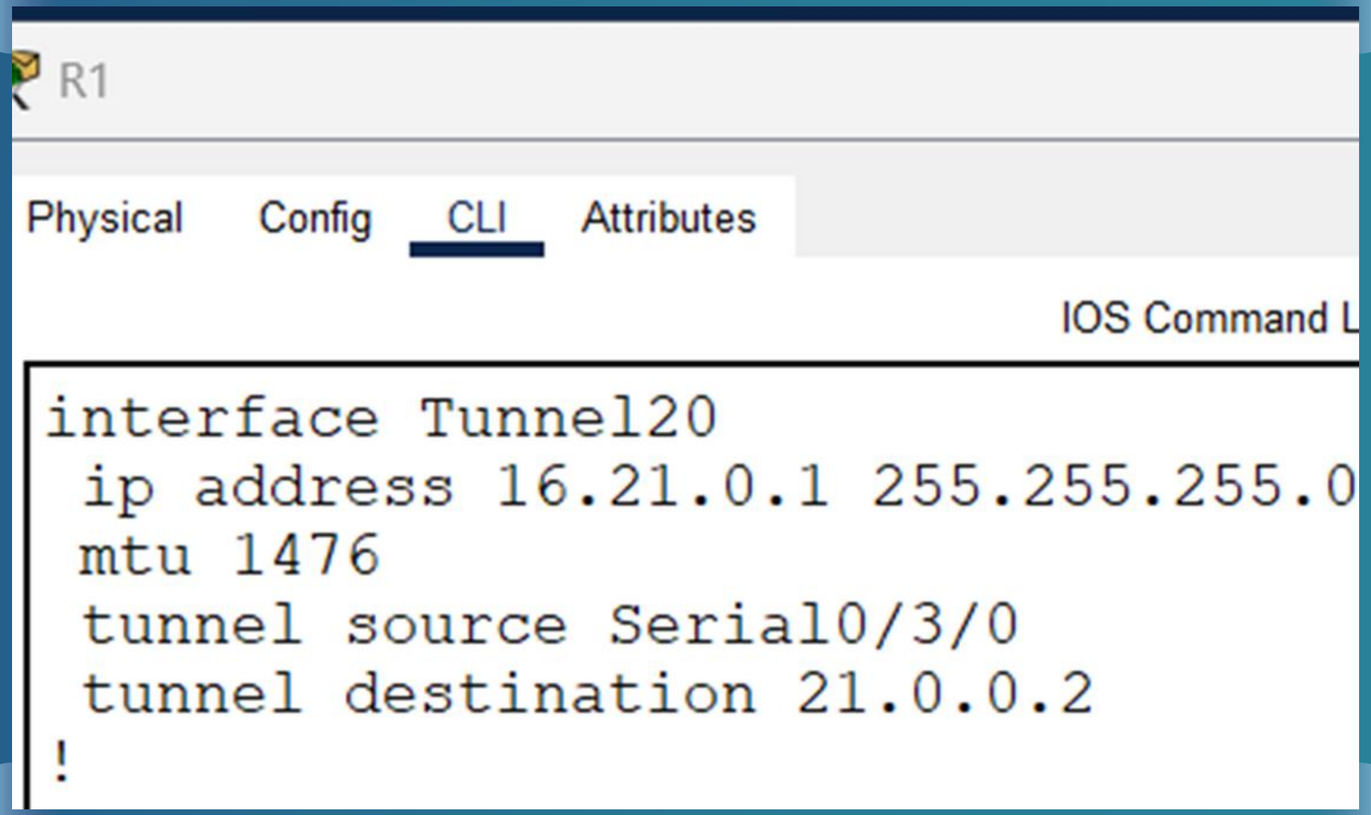
TO ENHANCE NETWORK SECURITY, WE IMPLEMENTED AN AAA FRAMEWORK. THIS FRAMEWORK MANAGES USER ACCESS BY VERIFYING THEIR IDENTITY, DEFINING THEIR PRIVILEGES, AND TRACKING THEIR NETWORK ACTIVITY. WE USE RADIUS TO SECURE NETWORK ACCESS, ENSURING ONLY AUTHORIZED USERS CAN ACCESS RESOURCES AND ALL ACTIVITIES ARE LOGGED FOR AUDITING

```
!
!
username Elkholy password 0 Elkholy
username Eltaweel password 0 Eltaweel
username Elwa password 0 Elwa
username Mahmoud password 0 Mahmoud
!
```

Enterprise Network

GRE

WE USED GRE AS A BASIC MECHANISM TO CREATE VIRTUAL PRIVATE NETWORK INFRASTRUCTURE, ALLOWING US TO CONNECT OUR REMOTE SITES RELIABLY AND AS A FUTURE STEP, WE PLAN TO DEVELOP A MORE COMPREHENSIVE VPN SOLUTION BY ENCRYPTING GRE TUN USING POWERFUL ENCRYPTION PROTOCOLS SUCH AS IPSEC



Enterprise Network

THANK YOU!