



Enterprise
Network

DEPI PROJECT

01/17



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**





OUTLINE

1

PROJECT
DESING

4

DHC
P

7

STATIC &
OSPF ROUTING

10

ACL

2

SSH

5

HSR
P

8

WIRELESS

11

AAA

3

VLAN

6

INTER-VLAN
ROUTING

9

PORT
SECURITY &
BPDU GUARD

12

GR
E

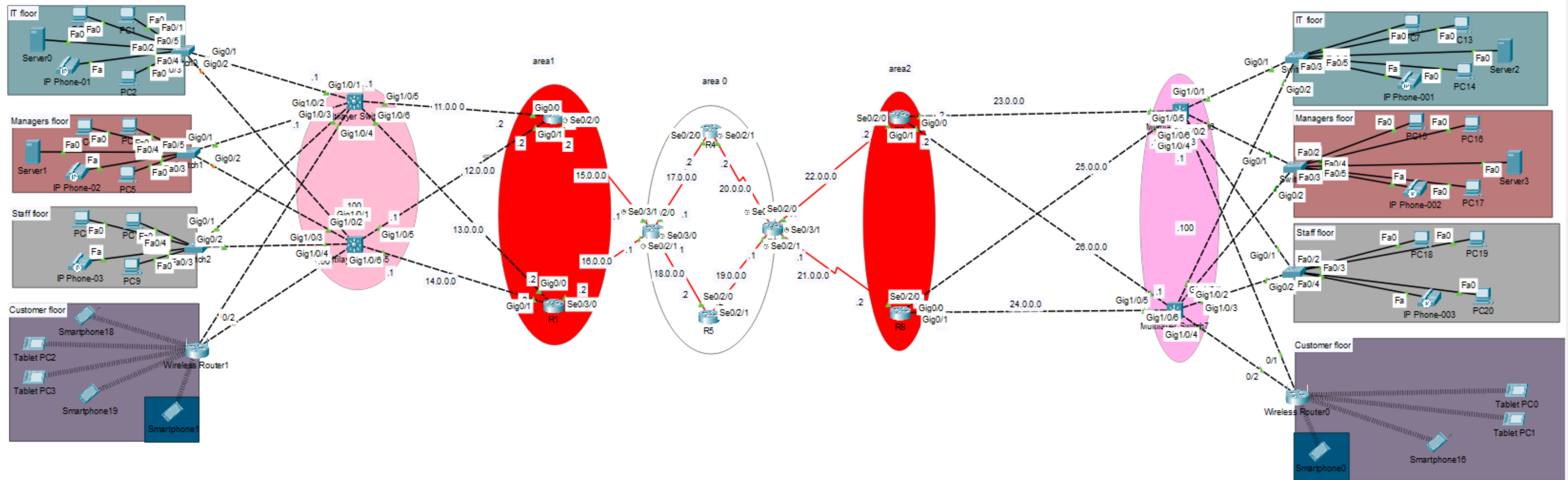




Enterprise
Network

PROJECT DESING

04/17





Enterprise
Network

SSH

05/17

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

The screenshot shows a PC1 window with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying an SSH Client window. The terminal output shows a password prompt, followed by the command 'MLswitsh1>ena', another password prompt, and then 'MLswitsh1#conf t'. A message 'Enter configuration commands, one per line. End with CNTL/Z.' is displayed, followed by the prompt 'MLswitsh1(config) #|'.

```
PC1
Physical Config Desktop Programming Attributes
SSH Client
Password:
MLswitsh1>ena
Password:
Password:
MLswitsh1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MLswitsh1(config) #|
```





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.

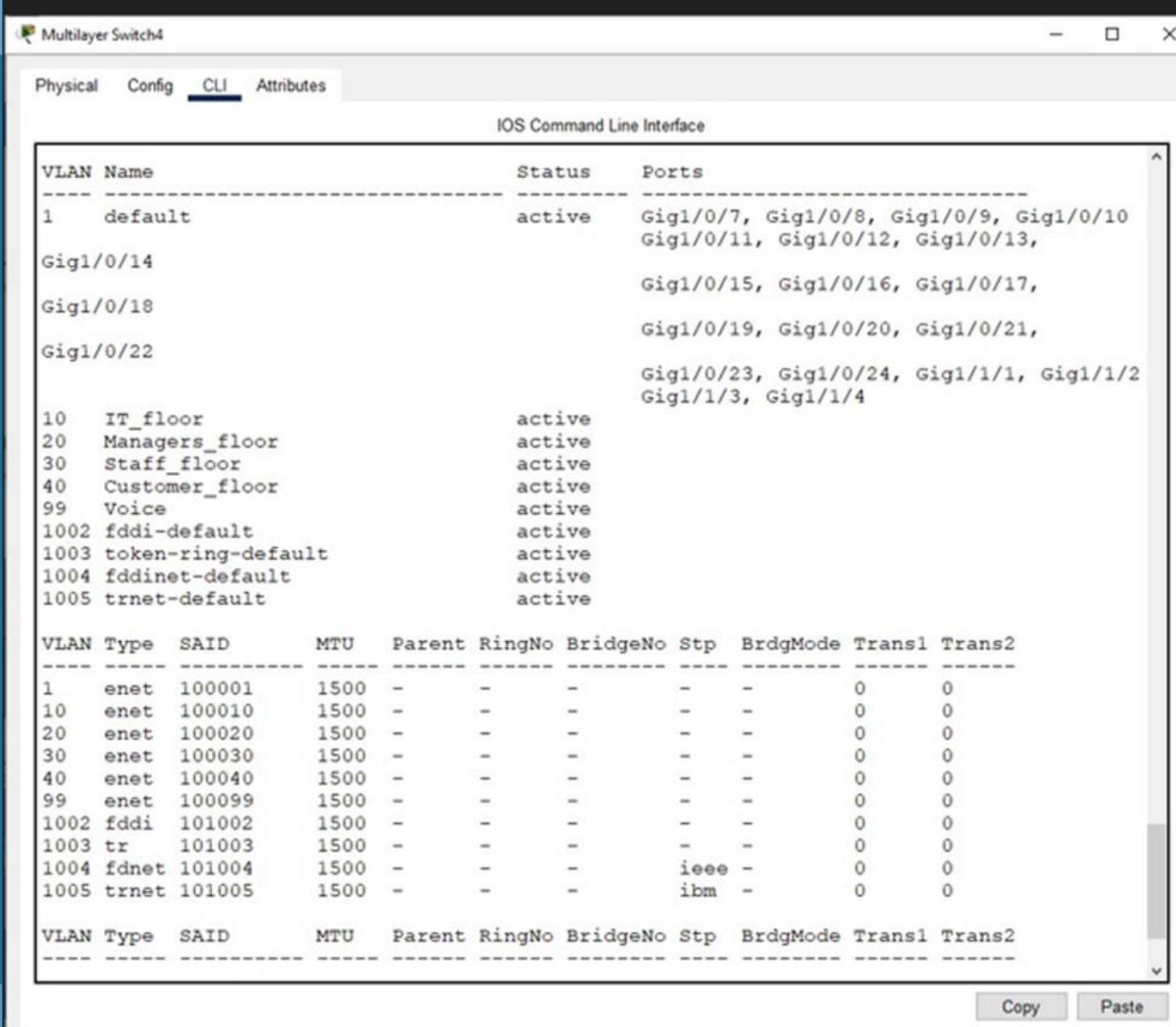
```
Multilayer Switch4
Physical  Config  CLI  Attributes
IOS Command Line Interface
ip dhcp pool vlan_20
  network 10.20.1.0 255.255.255.0
  default-router 10.20.1.100
  dns-server 8.8.8.8
ip dhcp pool vlan_30
  network 10.30.1.0 255.255.255.0
  default-router 10.30.1.100
  dns-server 8.8.8.8
ip dhcp pool vlan_40
  network 10.40.1.0 255.255.255.0
  default-router 10.40.1.100
  dns-server 8.8.8.8
ip dhcp pool vlan_10
  network 10.10.1.0 255.255.255.0
  default-router 10.10.1.100
  dns-server 8.8.8.8
!
```



VLAN

07/17

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.



Multilayer Switch4

Physical Config CLI Attributes

IOS Command Line Interface

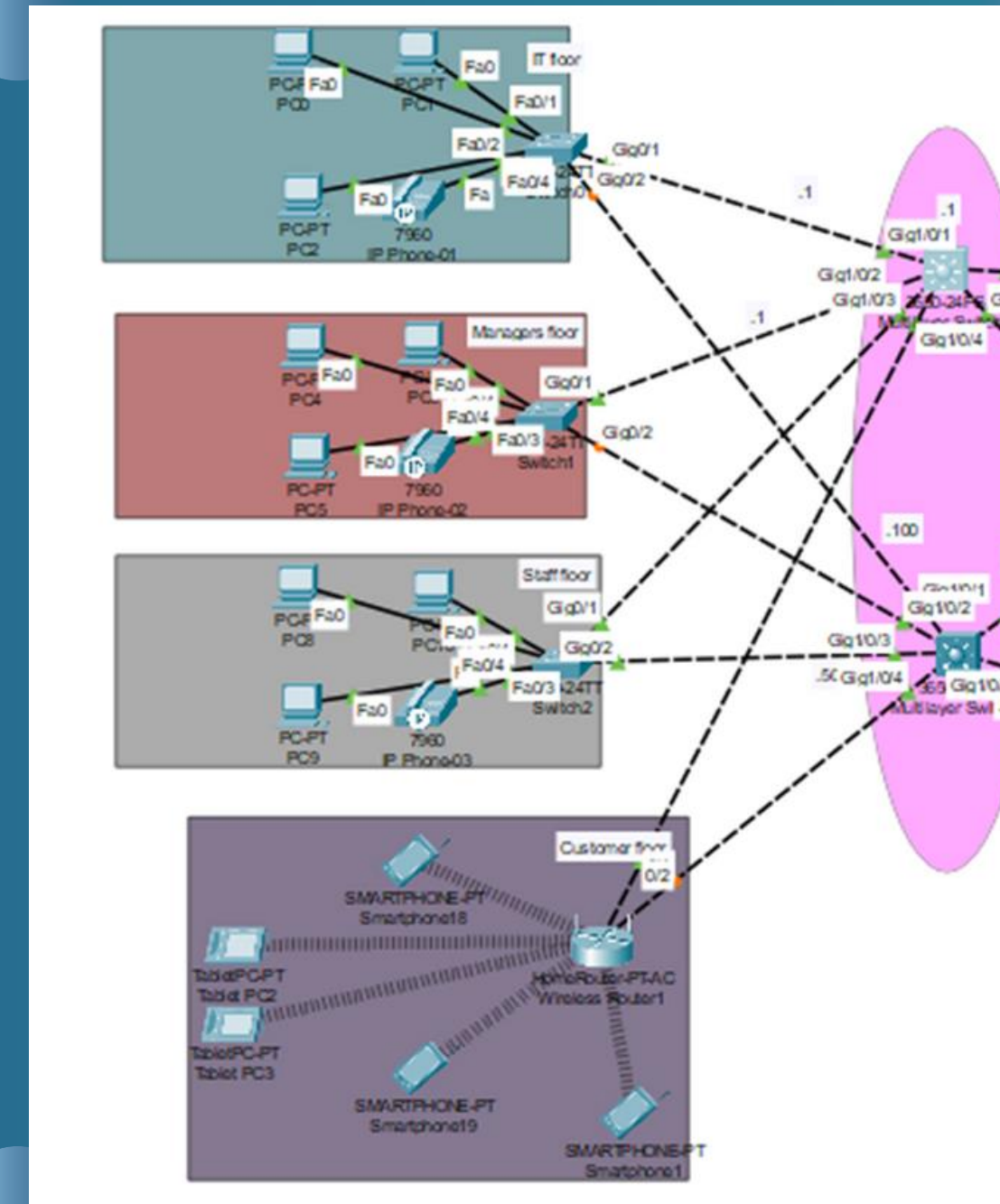
VLAN	Name	Status	Ports
1	default	active	Gig1/0/7, Gig1/0/8, Gig1/0/9, Gig1/0/10, Gig1/0/11, Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15, Gig1/0/16, Gig1/0/17, Gig1/0/18, Gig1/0/19, Gig1/0/20, Gig1/0/21, Gig1/0/22, Gig1/0/23, Gig1/0/24, Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4
10	IT_floor	active	
20	Managers_floor	active	
30	Staff_floor	active	
40	Customer_floor	active	
99	Voice	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
40	enet	100040	1500	-	-	-	-	-	0	0
99	enet	100099	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Copy Paste



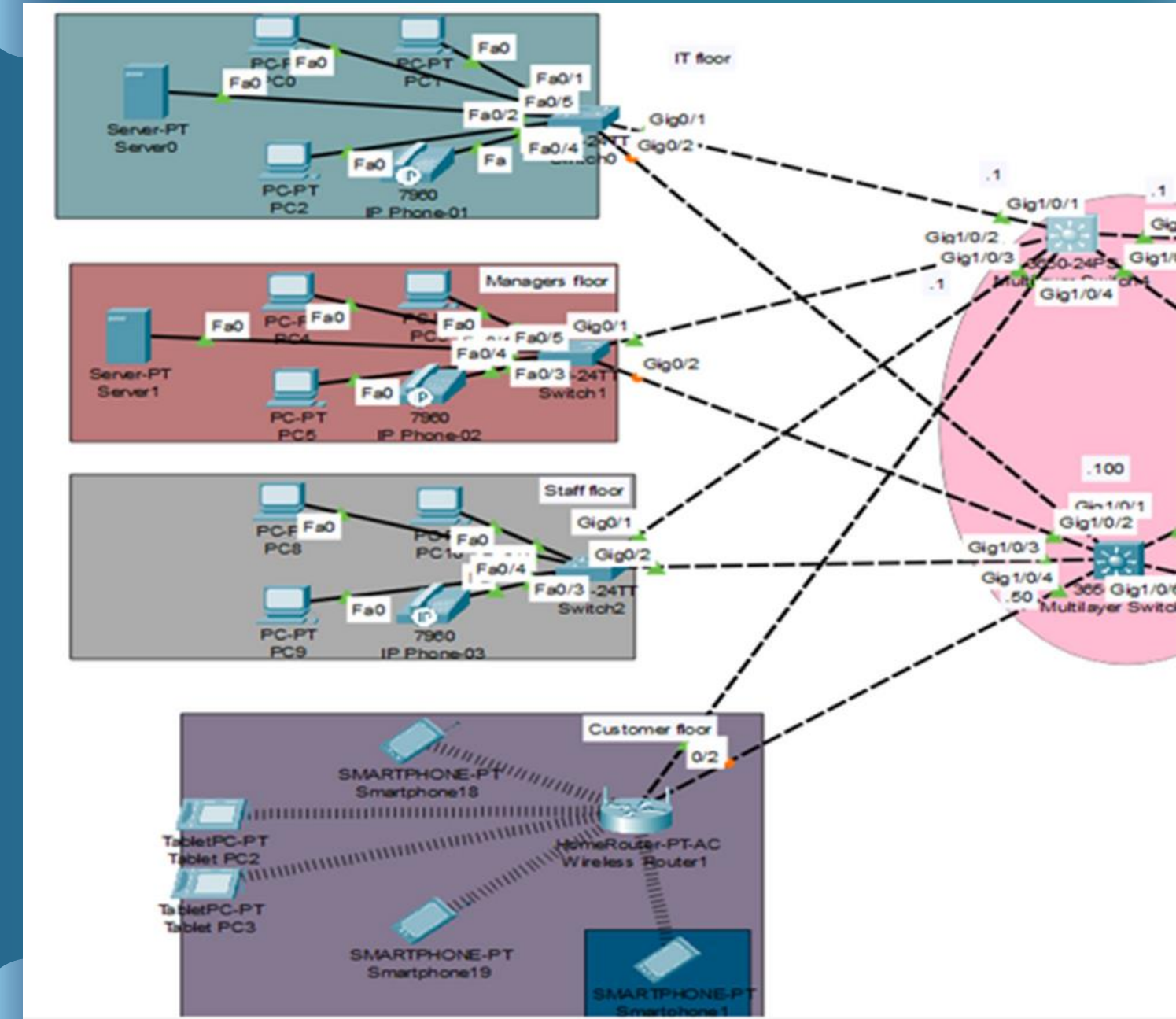
08/17



INTER-VLAN

09/17

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 SWITCHES WITH TRADITIONAL TENSIONS, MAKING IT EASIER TO MANAGE AND EXPAND THE 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
```





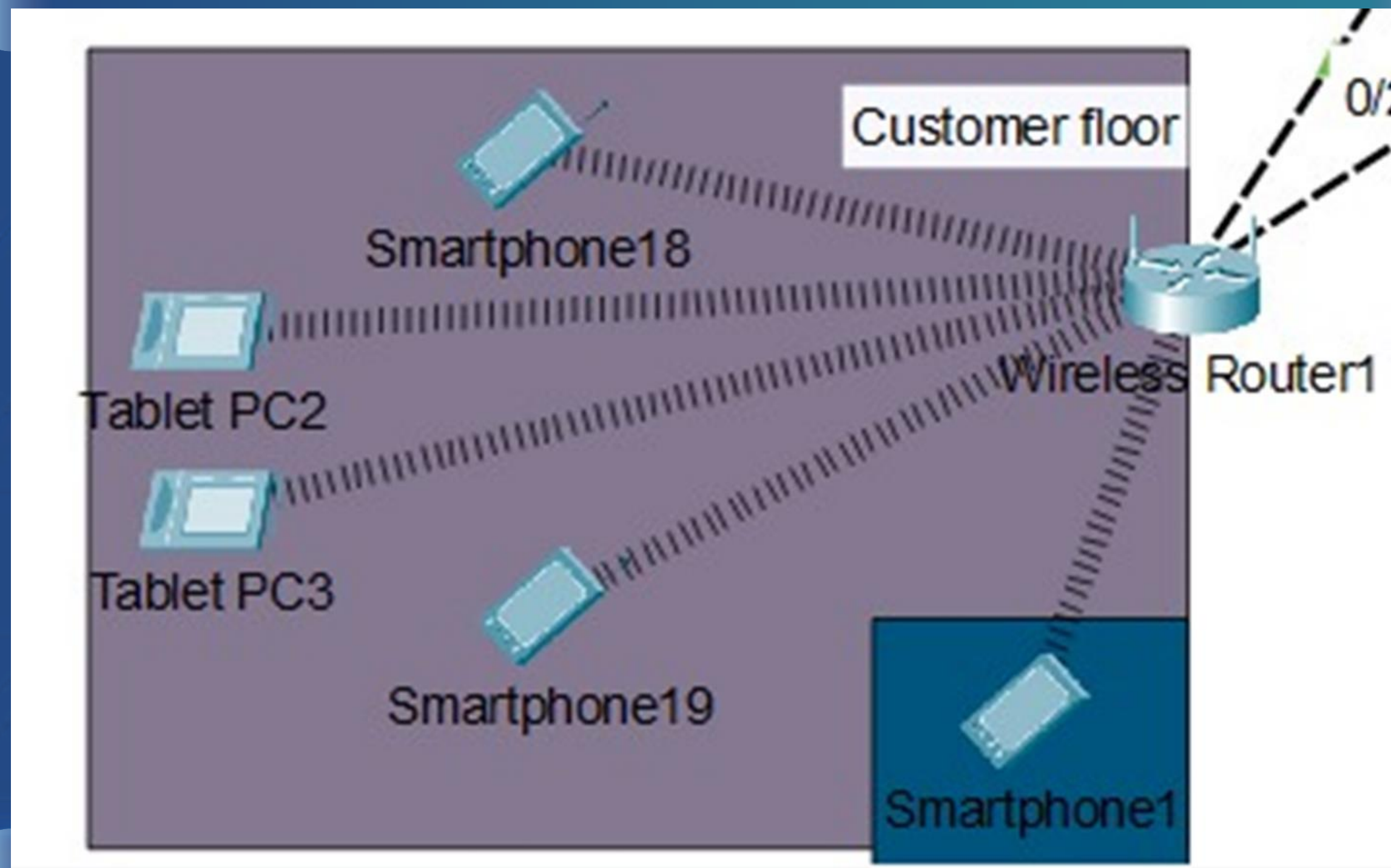
NAT

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)#|
```



WIRELESS





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
```





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

```
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.1.2

Pinging 10.10.1.2 with 32 bytes of data:

Reply from 15.0.0.5: bytes=32 time=43ms TTL=121
Reply from 15.0.0.5: bytes=32 time=4ms TTL=121
Reply from 15.0.0.5: bytes=32 time=40ms TTL=121
Reply from 15.0.0.5: bytes=32 time=13ms TTL=121

Ping statistics for 10.10.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 43ms, Average = 25ms

C:\>ping 10.20.1.2

Pinging 10.20.1.2 with 32 bytes of data:

Reply from 14.0.0.1: Destination host unreachable.
Reply from 11.0.0.1: Destination host unreachable.
Reply from 14.0.0.1: Destination host unreachable.
Reply from 11.0.0.1: Destination host unreachable.

Ping statistics for 10.20.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```





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

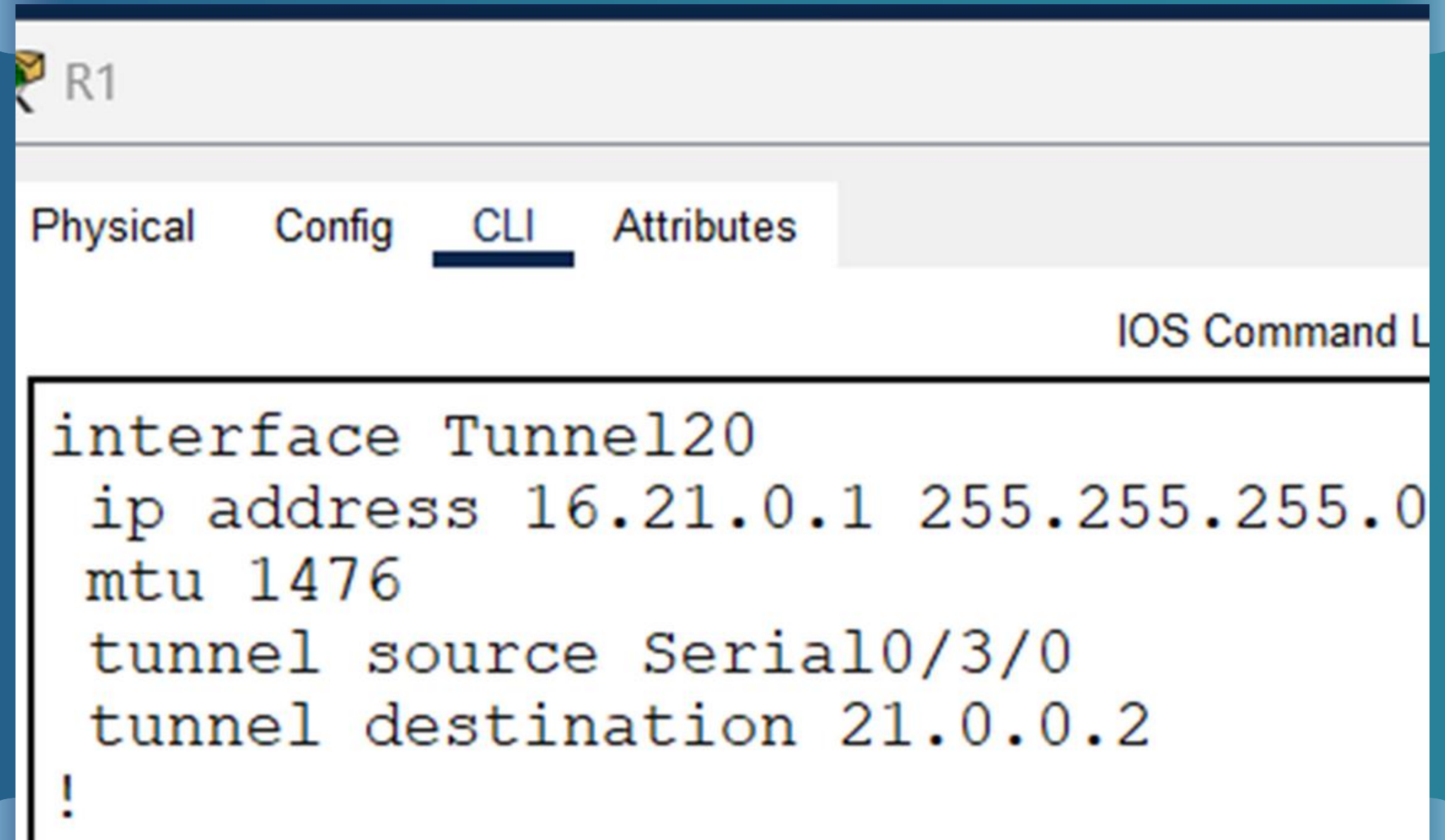
```
!  
!  
username Elkholy password 0 Elkholy  
username Eltaweel password 0 Eltaweel  
username Elwa password 0 Elwa  
username Mahmoud password 0 Mahmoud  
!
```





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



```
R1
Physical Config CLI Attributes
IOS Command Line
interface Tunnel20
 ip address 16.21.0.1 255.255.255.0
 mtu 1476
 tunnel source Serial0/3/0
 tunnel destination 21.0.0.2
!
```





Enterprise
Network

17/17

THANK
YOU!

