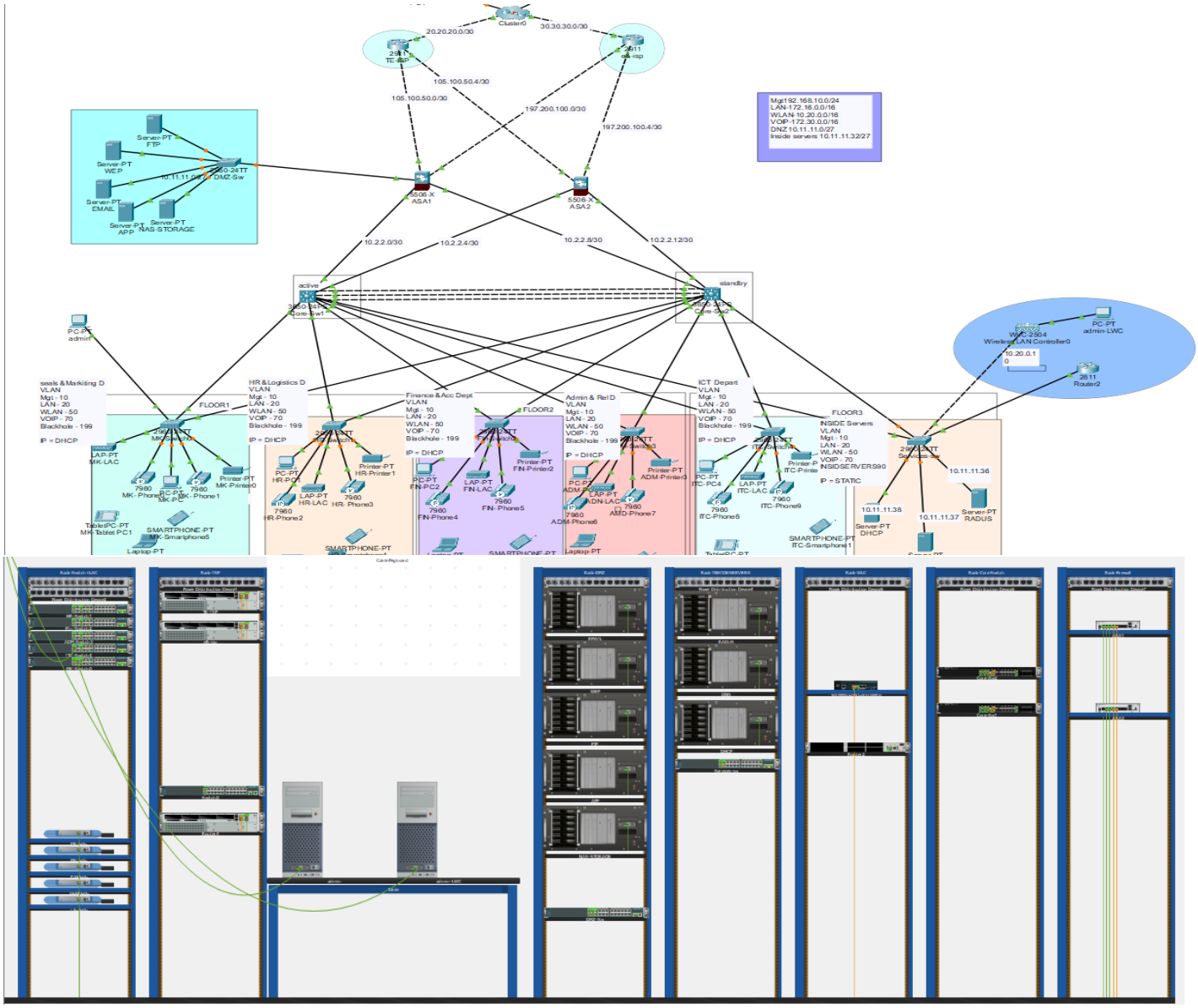
Digital Egypt Pioneers Initiative (DEPI)

Network Administration track

Final Project

Design and implementation of a security company to network system

Network Topology Diagram



The purpose of the project is to design and implement an integrated and secure network for Cytonn Innovation Ltd in its new building, which will house several departments such as Sales and Marketing, Human Resources, Finance, and IT. The main goal is to ensure smooth network operations while protecting it from both internal and external threats. The network will be divided into multiple security zones, including the inside, outside, and DMZ zones. Critical servers like DHCP, DNS, and Radius will be placed in the inside zone, while other servers like FTP, WEB, and Email will be located in the DMZ to control access and enhance security. This system will enable employees to work efficiently and securely access central resources, .ensuring data protection and operational security

Technologies Used

-VLANs for Network Segmentation .

-Configure EtherChannel using LACP.

-implement STP by Rapid STP.

-LAN Security Measures:

--Port fast .

--Port Security .

-- BPDU Guard (Spanning Tree Protocol Protection)

--Root Guard .

-High Availability with HSRP .

-Dynamic Routing with OSPF .

-DHCP (Dynamic Host Configuration Protocol) .

-VoIP .

-TFTP .

-Inter-VLAN Routing on the Multilayer Switch .

-Wireless LAN with (WLC) .

-Access Control Lists (ACLs) .

-Port Address Translation (PAT) .

-Configure the Cisco ASA Firewall .

-SSH (Secure Shell) for Remote Access .

Key Components:

1-VLANs for Network Segmentation:

VLANs (Virtual Local Area Networks) were configured to segment the network into distinct logical groups. Each VLAN isolates traffic and enhances network security.

Mgt 10 : native 192.168.10.0/24
LAN 20 -172.16.0.0/16
WLAN 50 -10.20.0.0/16
VOIP 70 -172.30.0.0/16
DNZ 10.11.11.0/27
Inside servers 10.11.11.32/27

A-SW1-6 , D-sw1-2
vlan 10
name Mgt
vlan 20
name LAN
vlan 50
name WLAN
vlan 70
name VOIP
vlan 199
name Blackhole
A-SW1-5
interface range f0/1-2
switchport mode access
switchport access vlan 20
no shutdown
interface range f0/5-6
switchport mode access
switchport voice vlan 70
no shutdown
interface f0/10
switchport mode access
switchport access vlan 50
no shutdown
interface range f0/3-4,f0/7-9,f0/11-24
switchport mode access
switchport access vlan 199
shutdown

2- Configure EtherChannel using LACP:

We create EtherChannel between D-sw1,2

cor-sw1

int r g1/0/8-10

channel-group 1 mode active

cor-sw2

int r g1/0/8-10

channel-group 1 mode passive

3- implement STP by Rapid STP:

(-)#spanning-tree mode rapid-pvst

"use the command on all switches"

D-SW1

spanning-tree vlan 10 priority 4096

spanning-tree vlan 20 priority 4096

spanning-tree vlan 1 priority 4096

spanning-tree vlan 50 priority 4096

spanning-tree vlan 70 priority 4096

spanning-tree vlan 199 priority 4096

D-SW2

spanning-tree vlan 10 priority 8192

spanning-tree vlan 20 priority 8192

spanning-tree vlan 1 priority 8192

spanning-tree vlan 50 priority 8192

spanning-tree vlan 70 priority 8192

spanning-tree vlan 199 priority 8192

4- LAN Security Measures

()# spanning-tree portfast

()#spanning-tree bpduguard enable

any interface connected to end devices

()#spanning-tree guard root

on all interface that connect to any switch in layer access

5-Port security:

was enabled to prevent unauthorized devices from connecting to the network. This feature limits the number of MAC addresses per port, protecting against MAC flooding attacks. Configure Violation Action (What happens when the rule is violated):

Shutdown – Shuts down the port when a violation occurs.

#int r f0/1-2,f0/5-6

#switchport port-security

#switchport port-security maximum 2

on any interface connected to end device

6-High Availability with HSRP

D-Sw1

interface vlan 10

standby 1 ip 192.168.10.254

standby 1 priority 110

standby 1 preempt

interface vlan 20

standby 2 ip 172.16.20.254

standby 2 priority 110

standby 2 preempt

interface vlan 50

standby 3 ip 10.20.50.254

standby 3 priority 110

standby 3 preempt

interface vlan 70

standby 4 ip 172.30.70.254

standby 4 priority 110

standby 4 preempt

interface vlan 90

standby 5 ip 10.11.11.35

standby 5 priority 110

standby 5 preempt

D-Sw2

interface vlan 10

standby 1 ip 192.168.10.254

standby 1 priority 90

interface vlan 20

standby 2 ip 172.16.20.254

standby 2 priority 90

interface vlan 50

standby 3 ip 10.20.50.254

standby 3 priority 90

interface vlan 70

standby 4 ip 172.30.70.254

standby 4 priority 90

interface vlan 90

standby 5 ip 10.11.11.35

standby 5 priority 90

7- Dynamic Routing with OSPF :

D-SW 1

router ospf 35

router-id 1.1.1.1

network 10.2.2.0 0.0.0.3 area 0

network 10.2.2.4 0.0.0.3 area 0

network 192.168.10.0 0.0.0.255 area 0

network 172.16.0.0 0.0.255.255 area 0

network 10.20.0.0 0.0.255.255 area 0

network 10.11.11.32 0.0.0.31 area 0

do wr

D-SW 2

router ospf 35

router-id 1.1.2.2

network 10.2.2.8 0.0.0.3 area 0

network 10.2.2.12 0.0.0.3 area 0

network 192.168.10.0 0.0.0.255 area 0

network 172.16.0.0 0.0.255.255 area 0

network 10.20.0.0 0.0.255.255 area 0

network 10.11.11.32 0.0.0.31 area 0

do wr

TE-ISP

router ospf 35

router-id 1.1.3.3

network 105.100.50.0 0.0.0.3 area 0

network 105.100.50.4 0.0.0.3 area 0

network 20.20.20.0 0.0.0.3 area 0

do wr

e&-isp

router ospf 35

router-id 1.1.4.4

network 197.200.100.0 0.0.0.3 area 0

network 197.200.100.4 0.0.0.3 area 0

network 30.30.30.0 0.0.0.3 area 0

do wr

8-DHCP (Dynamic Host Configuration Protocol)

Ip DHCP server 10.11.11.38

D-Sw1

interface vlan 10

no shutdown

ip helper-address 10.11.11.38

interface vlan 20

no shutdown

ip helper-address 10.11.11.38

interface vlan 50

no shutdown

ip helper-address 10.11.11.38

D-Sw2

interface vlan 10

no shutdown

ip helper-address 10.11.11.38

interface vlan 20

no shutdown

ip helper-address 10.11.11.38

interface vlan 50

no shutdown

ip helper-address 10.11.11.38

exit

default getway 172.16.0.254 for LAN network

172.16.0.0/16 for LAN

10.20.0.0/16 for Wireless

172.30.0.0./16 for VoIP

192.168.10.0/24 for Mgt

DNS = 10.11.11.37

9- VoIP

router

set ip address on sub interface f0/0.70

encapsulation dot1Q

ip add : 172.30.0.1 255.255.0.0

creat dhcp , name dhcp voic , network 172.30.0.0 255.255.0.0

option 150 1p 172.30.0.1

Router2(config)#telephony-service

Router2(config-telephony)#max-dn 10

Router2(config-telephony)#max-ephones 10

Router2(config-telephony)#ip source-address 172.30.0.1 port 2000

swServer

FLOOR3-Services(config-if)#int f0/24

FLOOR3-Services(config-if)#switchport mode trunk

sw

under switch that have ip phone

config-if-range)#no switchport access vlan 70)

config-if-range)#switchport voice vlan 70)

10-Inter-VLAN Routing on the Multilayer Switch .

Core-Sw1(config)#ip routing

Core-Sw1(config)#interface gigabitEthernet1/0/23

Core-Sw1(config-if)#no switchport

Core-Sw1(config-if)#ip address 10.2.2.1 255.255.255.252

Core-Sw1(config-if)#exit

Core-Sw1(config-if)#interface gigabitEthernet1/0/24

Core-Sw1(config-if)#no switchport

Core-Sw1(config-if)#ip address 10.2.2.5 255.255.255.252

Core-Sw1(config-if)#exit

Core-Sw1(config)#interface vlan 10

Core-Sw1(config-if)#ip address 192.168.10.1 255.255.255.0

Core-Sw1(config-if)#no shutdown

Core-Sw1(config-if)#exit

Core-Sw1(config)#interface vlan 50

Core-Sw1(config-if)#ip address 10.20.50.1 255.255.0.0

Core-Sw1(config-if)#no shutdown

Core-Sw1(config-if)#exit

Core-Sw1(config)#interface vlan 20

Core-Sw1(config-if)#ip address 172.16.20.1 255.255.0.0

Core-Sw1(config-if)#no shutdown

Core-Sw1(config-if)#exit

Core-Sw1(config)#interface vlan 70

Core-Sw1(config-if)#ip address 172.30.70.1 255.255.0.0

Core-Sw1(config-if)#no shutdown

D-Sw2

Core-Sw2(config)#ip routing

Core-Sw2(config-if)#interface gigabitEthernet 1/0/23

Core-Sw2(config-if)#no switchport

Core-Sw2(config-if)#ip address 10.2.2.9 255.255.255.252

Core-Sw2(config-if)#exit

Core-Sw2(config-if)#interface gigabitEthernet 1/0/24

Core-Sw2(config-if)#no switchport

Core-Sw2(config-if)#ip address 10.2.2.13 255.255.255.252

Core-Sw1(config-if)#exit

Core-Sw2(config)#interface vlan 10

Core-Sw2(config-if)#ip address 192.168.10.2 255.255.255.0

Core-Sw2(config-if)#no shutdown

Core-Sw2(config-if)#exit

Core-Sw2(config)#interface vlan 20

Core-Sw2(config-if)#ip address 172.16.20.2 255.255.0.0

Core-Sw2(config-if)#no shutdown

Core-Sw2(config-if)#exit

Core-Sw2(config-if)#interface vlan 50

Core-Sw2(config-if)#ip address 10.20.50.2 255.255.0.0

Core-Sw2(config-if)#no shutdown

Core-Sw2(config-if)#exit

Core-Sw2(config-if)#interface vlan 70

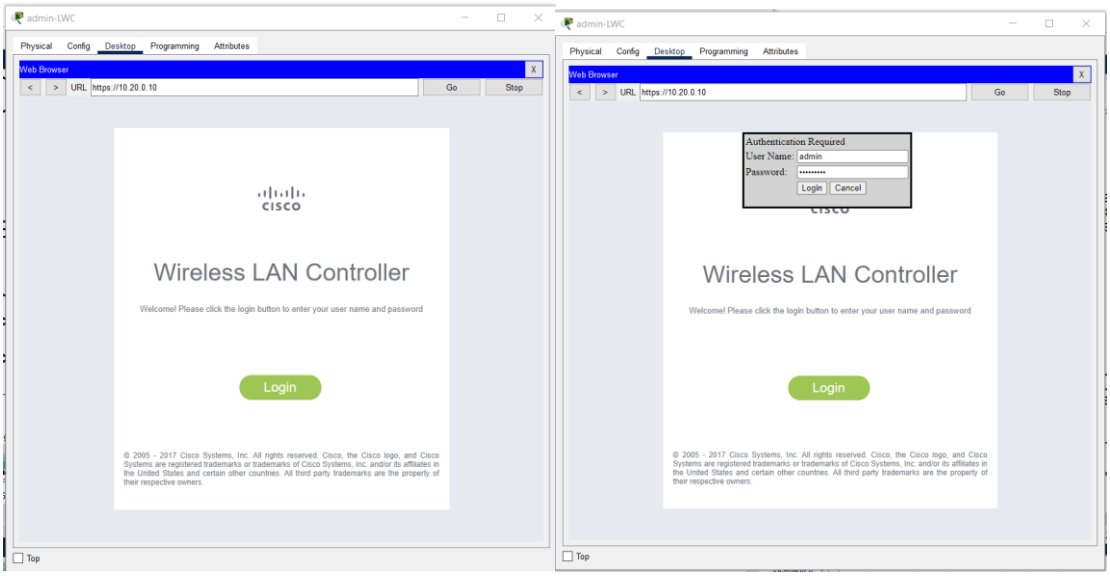
Core-Sw2(config-if)#ip address 172.30.70.2 255.255.0.0

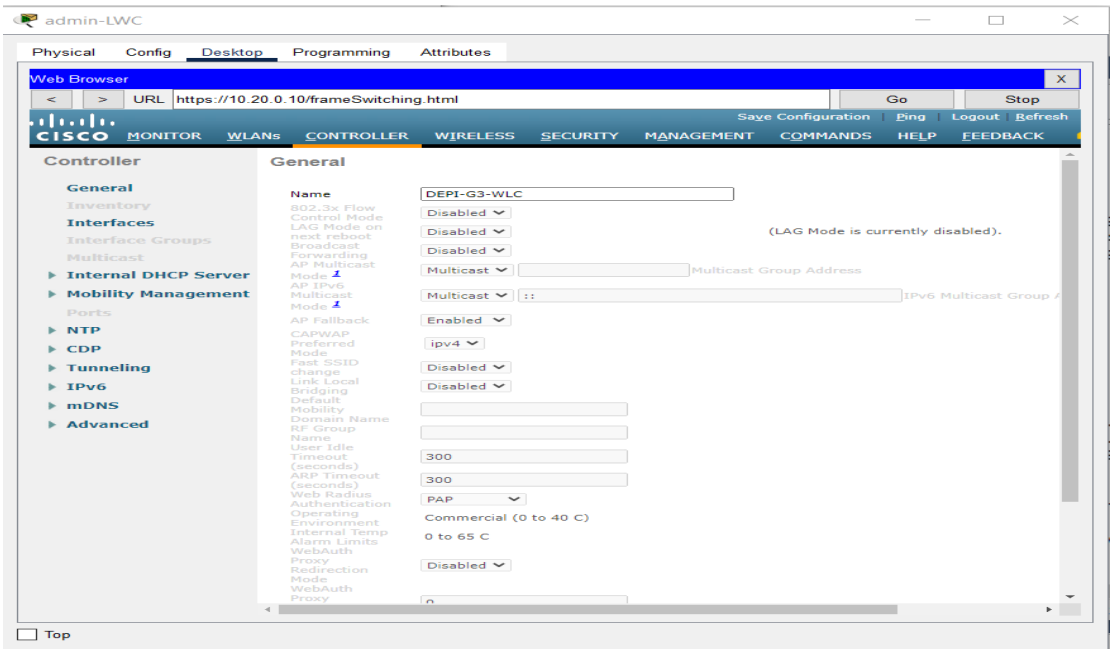
Core-Sw2(config-if)#no shutdown

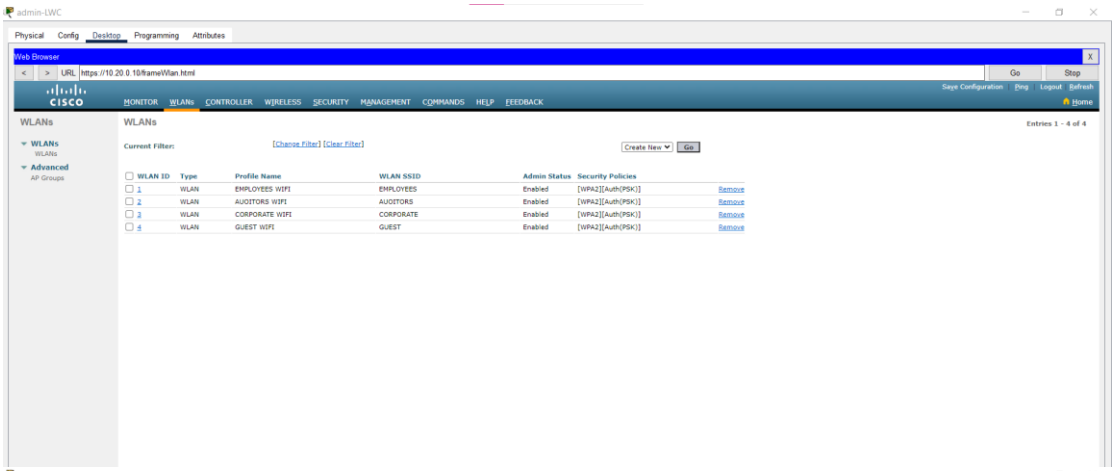
Core-Sw2(config-if)#exit

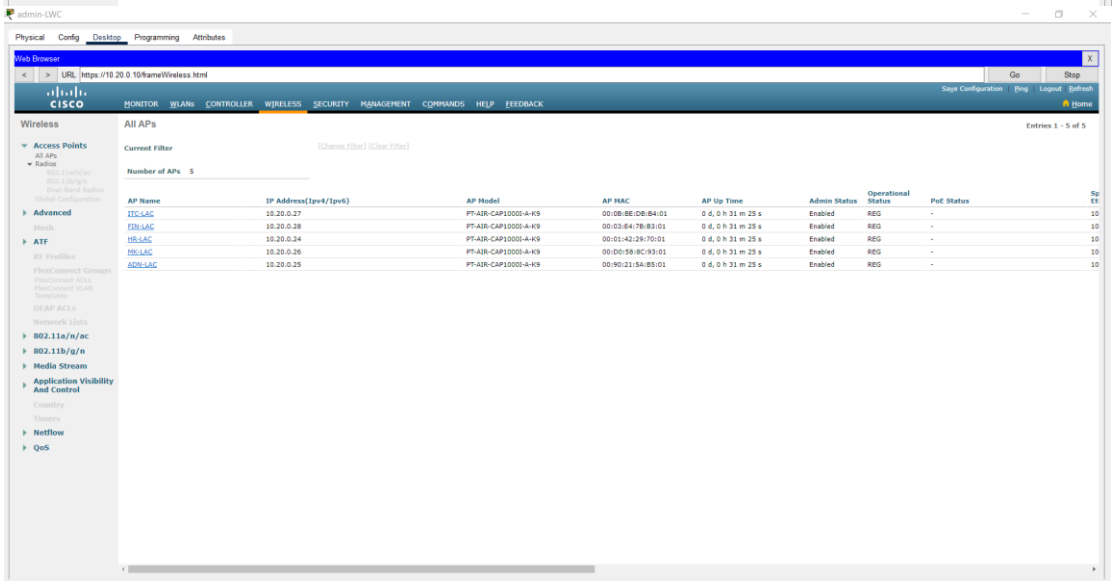
11-Wireless LAN with Security:

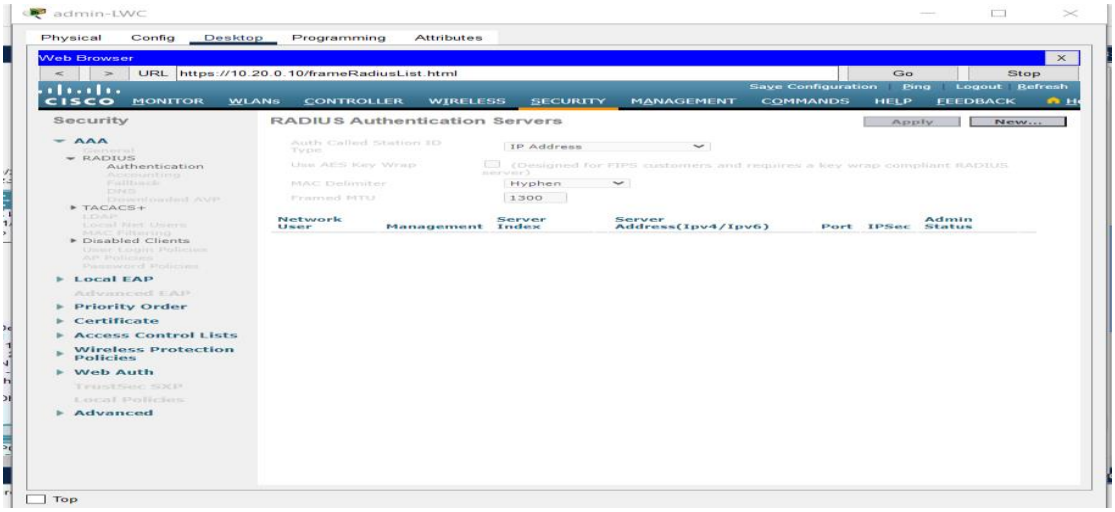
A secure Wireless LAN (WLAN) was set up using WPA2/WPA3 encryption for secure communication. A Wireless LAN Controller (WLC) manages the access points, ensuring central management and security. Clients can connect to the wireless network securely with encrypted sessions






admin-LWC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.20.0.10/frameWlan.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs
Entries 1 - 4 of 4
Current Filter:
[Change Filter] [Clear Filter]
Create New
Go
WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies
1 WLAN EMPLOYEES WIFI EMPLOYEES Enabled [WPA2][Auth(PSK)] Remove
2 WLAN AUDITORS WIFI AUDITORS Enabled [WPA2][Auth(PSK)] Remove
3 WLAN CORPORATE WIFI CORPORATE Enabled [WPA2][Auth(PSK)] Remove
4 WLAN GUEST WIFI GUEST Enabled [WPA2][Auth(PSK)] Remove


admin-LWC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.20.0.10/frameWireless.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
Wireless
All APs
Entries 1 - 5 of 5
Current Filter
[Change Filter] [Clear Filter]
Number of APs 5
AP Name IP Address(Ipv4/Ipv6) AP Model AP MAC AP Up Time Admin Status Operational Status PoE Status
ITC-LAC 10.20.0.27 PT-AIR-CAP1000I-A-K9 00:0B:BE:DB:B4:01 0 d, 0 h 31 m 25 s Enabled REG -
FIN-LAC 10.20.0.28 PT-AIR-CAP1000I-A-K9 00:03:E4:7B:83:01 0 d, 0 h 31 m 25 s Enabled REG -
HR-LAC 10.20.0.24 PT-AIR-CAP1000I-A-K9 00:01:42:29:70:01 0 d, 0 h 31 m 25 s Enabled REG -
MK-LAC 10.20.0.26 PT-AIR-CAP1000I-A-K9 00:D0:58:8C:93:01 0 d, 0 h 31 m 25 s Enabled REG -
ADN-LAC 10.20.0.25 PT-AIR-CAP1000I-A-K9 00:90:21:5A:B5:01 0 d, 0 h 31 m 25 s Enabled REG -


admin-LWC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.20.0.10/frameRadiusList.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security
RADIUS Authentication Servers
Apply
New...
Auth Called Station ID Type
IP Address
Use AES Key Wrap
(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
MAC Delimiter
Hyphen
Framed MTU
1300
Network User
Management
Server Index
Server Address(Ipv4/Ipv6)
Port
IPSec
Admin Status
AAA
RADIUS
Authentication
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Advanced EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection Policies
Web Auth
TrustSec SXP
Local Policies
Advanced
Top

12-SSH (Secure Shell) for Remote Access:

SSH was implemented to provide encrypted remote management of network devices, enhancing security and ensuring safe remote configuration.

<--switches

username admin password DEPI-G3-sw

ip domain-name DEPI.com

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

line vty 0 15

login local

transport input ssh

exit

access-list 1 permit 192.168.10.0 0.0.0.255

access-list 1 deny any

line vty 0 15

access-class 1 in

exit

do wr

<--MK-switch

FLOOR1-MK(config)#interface vlan 10

FLOOR1-MK(config-if)#ip address 192.168.10.2 255.255.255.0

FLOOR1-MK(config-if)#no shutdown

<--HR-switch

FLOOR1-HR(config)#interface vlan 10

FLOOR1-HR(config-if)#ip address 192.168.10.3 255.255.255.0

FLOOR1-HR(config-if)#no shutdown

<--FIN-switch

FLOOR2-FIN(config)#interface vlan 10

FLOOR2-FIN(config-if)#ip address 192.168.10.4 255.255.255.0

FLOOR2-FIN(config-if)#no shutdown

<--ADM-switch

FLOOR2-ADM(config)#interface vlan 10

FLOOR2-ADM(config-if)#ip address 192.168.10.5 255.255.255.0

FLOOR2-ADM(config-if)#no shutdown

<--ITC-switch

FLOOR3-ITC(config)#interface vlan 10

FLOOR3-ITC(config-if)#ip address 192.168.10.6 255.255.255.0

FLOOR3-ITC(config-if)#no shutdown

<--SERVICES-sw

FLOOR3-Services(config)#interface vlan 10

FLOOR3-Services(config-if)#ip address 192.168.10.7 255.255.255.0

FLOOR3-Services(config-if)#no shutdown

<--core switches

username admin password DEPI-G3-core

ip domain-name DEPI.com

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

line vty 0 15

login local

transport input ssh

exit

access-list 1 permit 192.168.10.0 0.0.0.255

access-list 1 deny any

line vty 0 15

access-class 1 in

exit

do wr

13-Configure the Cisco ASA Firewall :

enable password DEPI-G3

username admin password DEPI-G3

#

firewall interfaces security zones and levels*

ASA1-\#

in g1/2

no shut

ip add 10.2.2.2 255.255.255.252

nameif INSIDE1

security-level 100

exit

in g1/3

no shut

```
ip add 10.2.2.10 255.255.255.252
nameif INSIDE2
security-level 100
exit

in g1/1
no shut
ip add 10.11.11.1 255.255.255.224
nameif DMZ
security-level 70
exit

in g1/4
no shut
ip add 105.100.50.2 255.255.255.252
nameif OUTSIDE1
security-level 0
exit

in g1/5
no shut
ip add 197.200.100.2 255.255.255.252
nameif OUTSIDE2
security-level 0
exit
wr mem
```

#

ASA2-٢#

in g1/2

no shut

ip add 10.2.2.6 255.255.255.252

nameif INSIDE1

security-level 100

exit

in g1/3

no shut

ip add 10.2.2.14 255.255.255.252

nameif INSIDE2

security-level 100

exit

in g1/4

no shut

ip add 105.100.50.6 255.255.255.252

nameif OUTSIDE1

security-level 0

exit

in g1/5

no shut

ip add 197.200.100.6 255.255.255.252

nameif OUTSIDE2

security-level 0

exit

wr mem

#

firewall routing- ospf +static route*

ASA1-١

#

route OUTSIDE1 0.0.0.0 0.0.0.0 105.100.50.1

---route OUTSIDE2 0.0.0.0 0.0.0.0 197.200.100.1 70 ---backup

router ospf 35

router-id 1.1.0.0

network 105.100.50.0 255.255.255.252 area 0

network 197.200.100.0 255.255.255.252 area 0

network 10.2.2.0 255.255.255.252 area 0

network 10.2.2.8 255.255.255.252 area 0

exit

we mem

#

ASA2-٢#

route OUTSIDE1 0.0.0.0 0.0.0.0 105.100.50.5

route OUTSIDE2 0.0.0.0 0.0.0.0 197.200.100.5

router ospf 35

router-id 1.1.9.9

network 197.200.100.4 255.255.255.252 area 0

network 105.100.50.4 255.255.255.252 area 0

network 10.2.2.4 255.255.255.252 area 0

network 10.2.2.12 255.255.255.252 area 0

exit

wr mem

14- Port Address Translation (PAT):

firewall inspection policy configuration*

ASA1-\#

object network INSIDE1-OUTSIDE1

subnet 172.16.0.0 255.255.0.0

nat (INSIDE1,OUTSIDE1) dynamic interface

object network INSIDE2-OUTSIDE1

subnet 172.16.0.0 255.255.0.0

nat (INSIDE2,OUTSIDE1) dynamic interface

object network INSIDEw1-OUTSIDEw1

subnet 10.20.0.0 255.255.0.0

nat (INSIDE1,OUTSIDE1) dynamic interface

object network INSIDEw2-OUTSIDEw1

subnet 10.20.0.0 255.255.0.0

nat (INSIDE2,OUTSIDE1) dynamic interface

object network INSIDE1-OUTSIDE2

subnet 172.16.0.0 255.255.0.0

nat (INSIDE1,OUTSIDE2) dynamic interface

object network INSIDE2-OUTSIDE2

subnet 172.16.0.0 255.255.0.0

nat (INSIDE2,OUTSIDE2) dynamic interface

object network INSIDEw1-OUTSIDEw2

subnet 10.20.0.0 255.255.0.0

nat (INSIDE1,OUTSIDE2) dynamic interface

object network INSIDEw2-OUTSIDEw2

subnet 10.20.0.0 255.255.0.0

nat (INSIDE2,OUTSIDE2) dynamic interface

object network DMZ-OUTSIDE1

subnet 10.11.11.0 255.255.255.224

nat (DMZ,OUTSIDE1) dynamic interface

object network DMZ-OUTSIDE2

subnet 10.11.11.0 255.255.255.224

nat (DMZ,OUTSIDE2) dynamic interface

wr mem

#

ASA2-٢#

object network INSIDE1-OUTSIDE1

subnet 172.16.0.0 255.255.0.0

nat (INSIDE1,OUTSIDE1) dynamic interface

object network INSIDE2-OUTSIDE1

subnet 172.16.0.0 255.255.0.0

nat (INSIDE2,OUTSIDE1) dynamic interface

object network INSIDEw1-OUTSIDEw1

subnet 10.20.0.0 255.255.0.0

nat (INSIDE1,OUTSIDE1) dynamic interface

object network INSIDEw2-OUTSIDEw1

subnet 10.20.0.0 255.255.0.0

nat (INSIDE2,OUTSIDE1) dynamic interface

object network INSIDE1-OUTSIDE2

subnet 172.16.0.0 255.255.0.0

nat (INSIDE1,OUTSIDE2) dynamic interface

object network INSIDE2-OUTSIDE2

subnet 172.16.0.0 255.255.0.0

nat (INSIDE2,OUTSIDE2) dynamic interface

object network INSIDEw1-OUTSIDEw2

subnet 10.20.0.0 255.255.0.0

nat (INSIDE1,OUTSIDE2) dynamic interface

object network INSIDEw2-OUTSIDEw2

subnet 10.20.0.0 255.255.0.0

nat (INSIDE2,OUTSIDE2) dynamic interface

wr mem

15- Access Control Lists (ACLs):

ACLs control traffic flow and ensure that only authorized devices can access specific network parts. Standard and extended ACLs are applied to filter traffic based on IP addresses, protocols, and ports .

ASA1

access-list RES extended permit icmp any any

access-list RES extended permit tcp any any eq 80

access-list RES extended permit tcp any any eq 53

access-list RES extended permit udp any any eq 53

access-group RES in interface DMZ

access-group RES in interface OUTSIDE1

access-group RES in interface OUTSIDE2

do wr

ASA2

access-list RES extended permit icmp any any

access-list RES extended permit tcp any any eq 80

access-list RES extended permit tcp any any eq 53

access-list RES extended permit udp any any eq 53

access-group RES in interface OUTSIDE1

access-group RES in interface OUTSIDE2

do wr