PAKISTAN EMERGENCY SMART INFRASTRUCTURE (PESI)

Course Instructor: PROF Muhammad Azam
Student Name: Abdul Wahid
Student ID: 243699
Submission Date: December 27, 2025

Contents

1. INTRODUCTION

The **Pakistan Emergency Smart Infrastructure (PESI)** represents a comprehensive enterprise network solution designed to provide mission-critical communication services across multiple geographical sites. This infrastructure integrates corporate headquarters, emergency response centers, and remote branch offices into a unified, highly available network platform supporting 2,500+ concurrent users.

Objectives

The PESI network addresses five core organizational requirements:

1.Multi-Site-Connectivity

Seamless communication between 5 major locations: Headquarters, Emergency Response Center, three Branch Offices, and a Central Distribution Hub with dual-ISP redundancy.

2.Emergency-Services-Integration

Dedicated infrastructure supporting Police, Medical, Rescue, and Ambulance services with 10 emergency hotlines (115, 1122, 15, etc.) and 24/7 operational availability.

3.High-Availability-Architecture

Zero single-point-of-failure design featuring dual core switches (HSRP), dual edge routers (OSPF), dual firewalls (ASA), and dual ISP connectivity ensuring >99.9% uptime.

4.Unified-CommunicationsPlatform

VoIP telephony system with 19 IP phones enabling inter-branch calling and emergency hotline services using Cisco Call Manager Express.

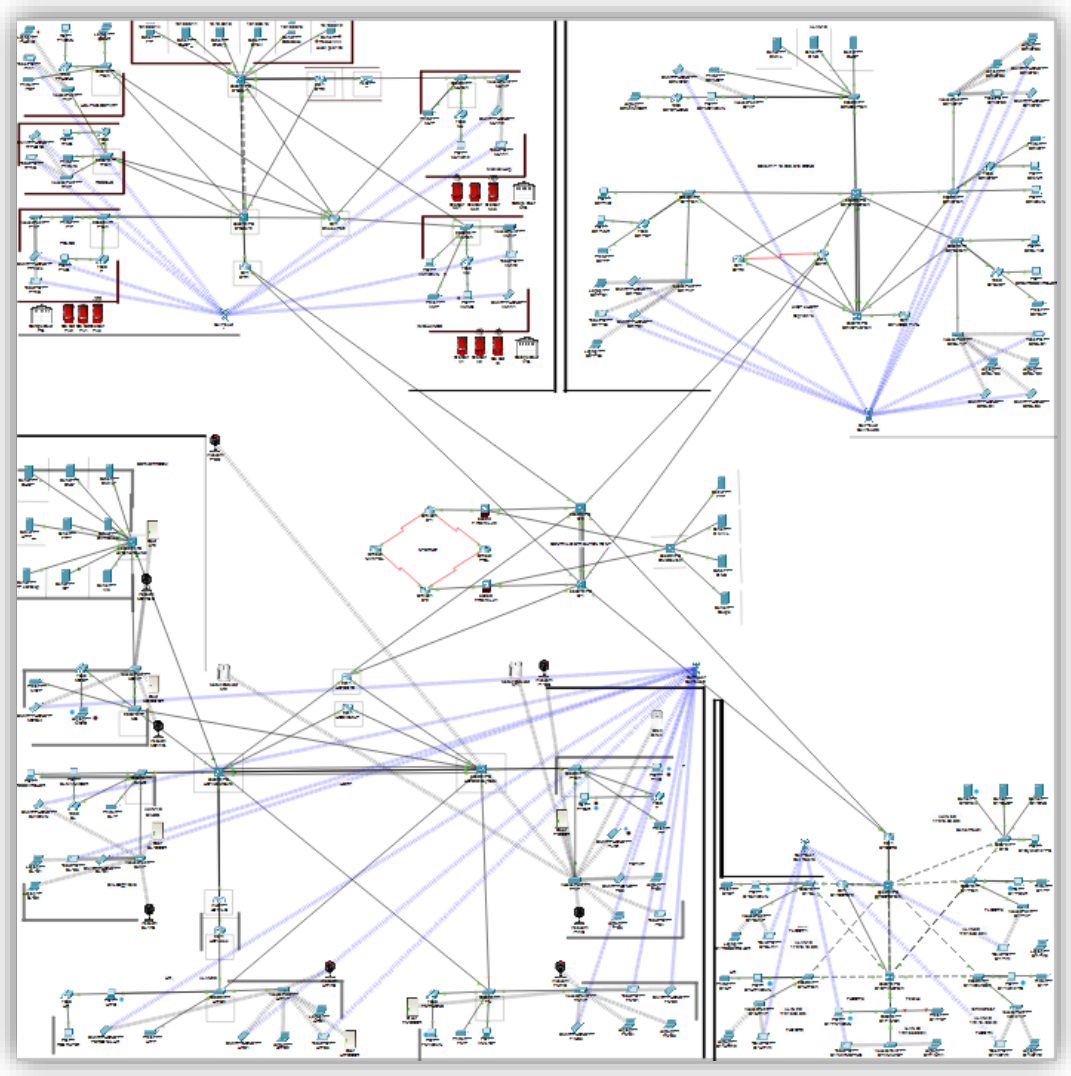
5.Enterprise-Security

Multi-layered protection including Cisco ASA firewalls with DMZ isolation, AAA/RADIUS authentication, SSH-only device access, and comprehensive ACL policies.

---

2. NETWORK DESIGN & ARCHITECTURE

2.1 Topology Overview

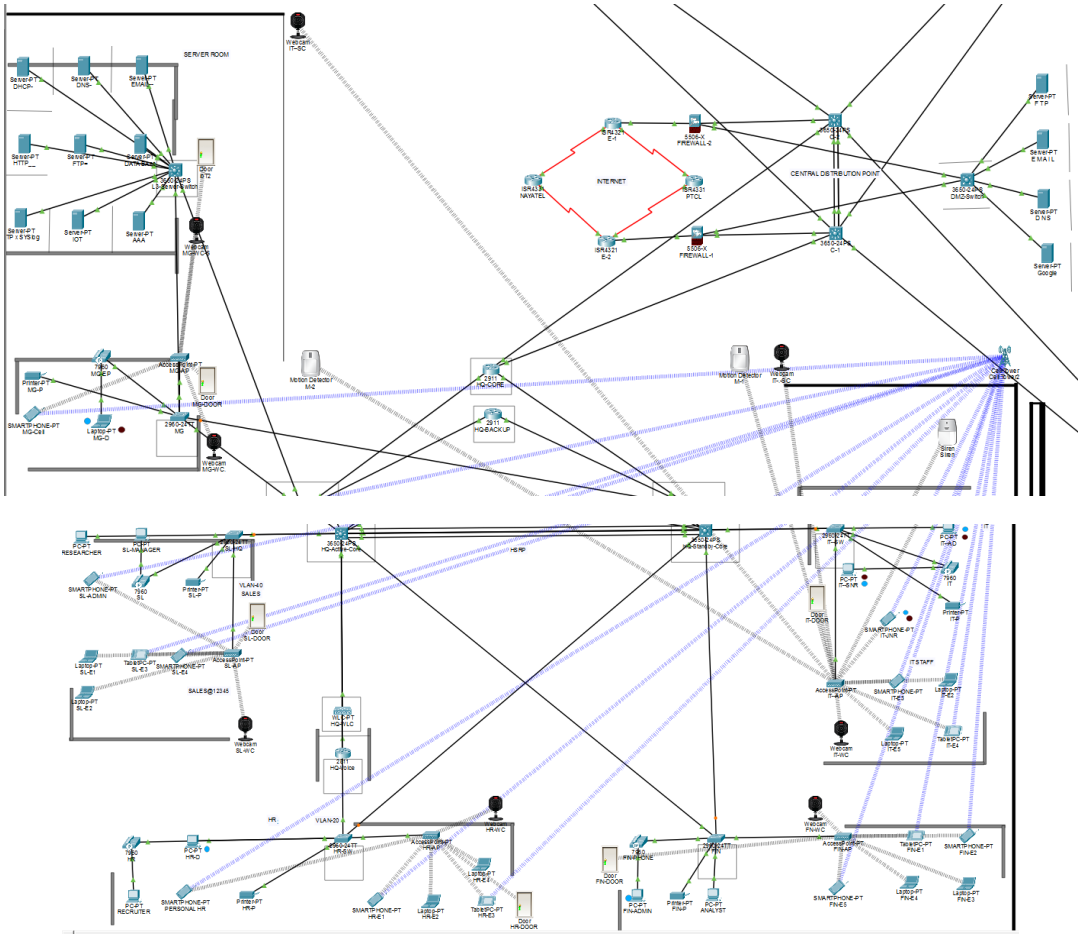


The PESI network implements a **hierarchical three-tier architecture**:

- **Core Layer:** L3 switches providing inter-VLAN routing with HSRP redundancy
- **Distribution Layer:** Edge routers connecting remote sites via OSPF multi-area routing
- **Access Layer:** L2 switches with trunk connections for end-user connectivity
- **Security Layer:** Dual Cisco ASA firewalls with DMZ for public services
- **WAN Layer:** Redundant ISP connections (PTCL & Nayatel) with IPSec VPN

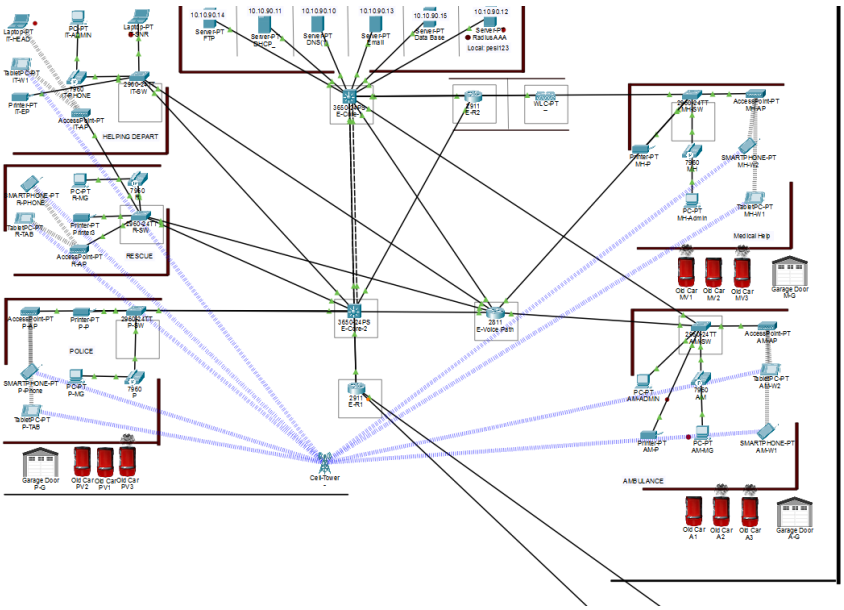
2.2 Site Infrastructure

Site 1: Headquarters



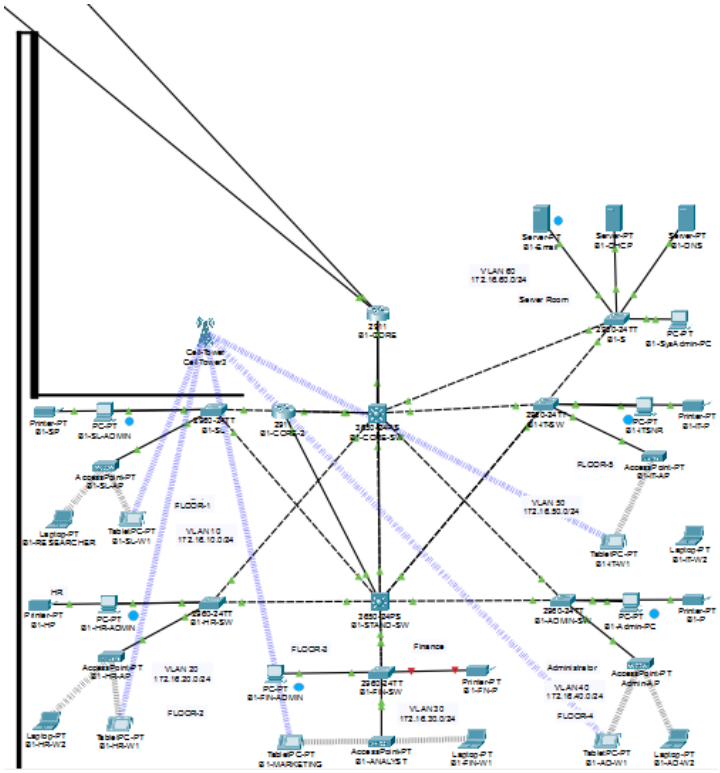
Parameter	Details
IP Range	50.50.0.0/16
OSPF Area	Area 0 (Backbone)
VLANs	9 (Servers, HR, Finance, Sales, IT, Management, Voice, IoT, WiFi)
Capacity	2,000+ users
Key Features	• 5 IP Phones (6001-6005) • Complete server farm (DHCP, DNS, Email, FTP, RADIUS, NTP) • IoT security system with motion detection

Site 2: Emergency Response Center



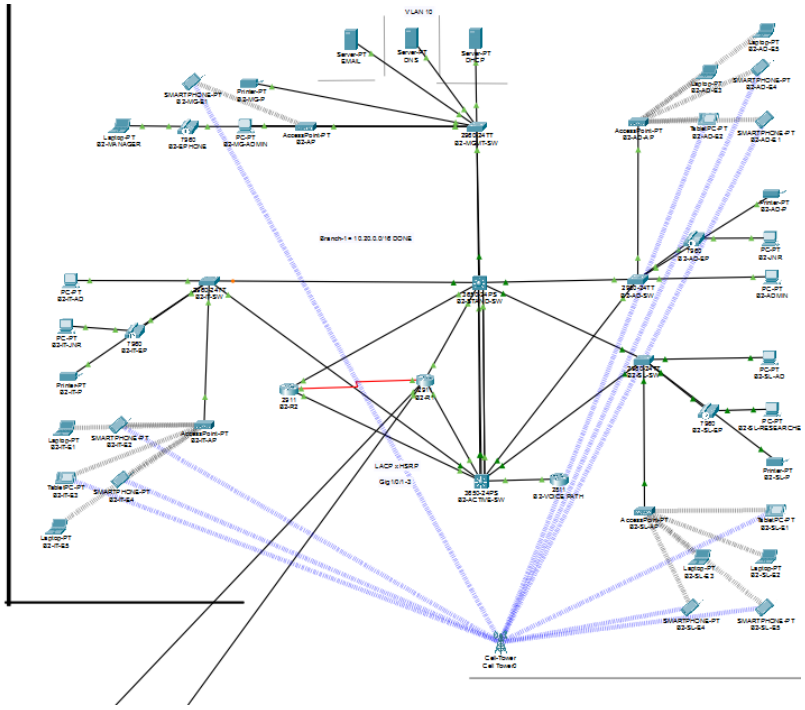
Parameter	Details
IP Range	10.10.0.0/16
OSPF Area	Area 2
VLANs	10 (Ambulance, Medical, Police, Rescue, Voice, IT, WiFi, IoT, Servers, Management)
Capacity	570+ devices
Key Features	• 10 emergency hotlines (115, 1122, 15, 1151, 2101, 3001, 4001, 5001, 10001) • AAA/RADIUS authentication • Dedicated database server • Load-balanced HSRP

Site 3: Branch Office 1



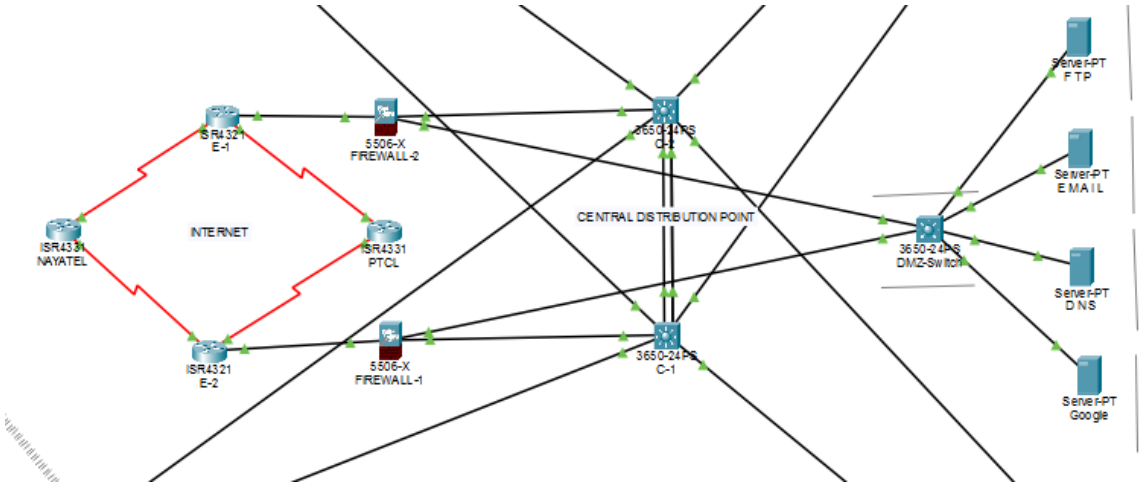
Parameter	Details
IP Range	172.16.0.0/16
OSPF Area	Area 1
VLANs	6 (Sales, HR, Finance, Admin, IT, Servers)
Capacity	1,200 users
Domain	b1pesi.com

Site 4: Branch Office 2



Parameter	Details
IP Range	10.20.0.0/16
OSPF Area	Area 3
VLANs	6 (Management, IT, Sales, CEO-Admin, Voice, Servers)
Capacity	1,200+ users
Key Features	• 4 IP Phones (2001-2004) • HSRPv2 gateway redundancy • 128 kbps serial backup link • Domain: b2pesi.com

Site 5: Central Distribution Point



Parameter	Details
Role	Network backbone hub
Key Components	• Dual ISPs (PTCL, Naya-Tel) • Dual Cisco ASA Firewalls • DMZ with 4 public servers • IPSec VPN tunnels
Public Services	Web Server, Mail Server, DNS Server, FTP Server
Security	NAT/PAT for all internal networks, ACL-based DMZ isolation

2.3 Design Justification

Why Hierarchical Architecture?

Benefit	Explanation
Scalability	New branches can be added to distribution layer without core redesign
Performance	Access layer traffic localization reduces core bandwidth consumption
Manageability	Clear functional separation simplifies troubleshooting and maintenance
Fault Isolation	Issues at access layer don't propagate to core infrastructure

Why OSPF Multi-Area Design?

Benefits:

- **Reduced routing overhead** through area segmentation (LSA flooding limited)
- **Faster convergence** with smaller routing tables per area
- **Route summarization** at Area Border Routers (ABRs) reduces routing table size
- **Scalability** supporting networks with 1000+ routers

Why Complete Redundancy?

Critical infrastructure demands zero single points of failure:

- **Dual Core Switches** with HSRP (Active-Standby) — <1 second failover
- **Dual Edge Routers** with OSPF load balancing — automatic path selection
- **Dual Firewalls** with stateful failover — seamless security continuity
- **Dual ISPs** with dynamic routing — automatic ISP failover

---

3. CONFIGURATION DETAILS

3.1 IP Addressing & VLAN Design

Addressing Scheme

Site	Network	Mask	OSPF Area	Gateway Protocol	Usable Hosts
Headquarters	50.50.0.0/16	255.255.0.0	Area 0	HSRP	65,534
Emergency Site	10.10.0.0/16	255.255.0.0	Area 2	HSRP (Load Balanced)	65,534
Branch 1	172.16.0.0/16	255.255.0.0	Area 3	Static	65,534
Branch 2	10.20.0.0/16	255.255.0.0	Area 1	HSRPv2	65,534
DMZ	172.16.0.0/24	255.255.255.0	—	Static	254

Headquarters VLANs:

VLAN	Department	Network	HSRP Gateway	Purpose
10	Servers	50.50.10.0/24	50.50.10.1	Server farm infrastructure
20	HR	50.50.20.0/24	50.50.20.1	Human resources workstations
30	Finance	50.50.30.0/24	50.50.30.1	Financial systems
50	IT	50.50.50.0/24	50.50.50.1	Network management
70	Voice	50.50.70.0/24	50.50.70.1	VoIP phones
80	IoT	50.50.80.0/24	50.50.80.1	Smart devices

Emergency Site VLANs (Load-Balanced HSRP):

VLAN	Service	Network	Active Switch	Priority
10	Ambulance 🚑	10.10.10.0/24	E-Core-1	110
20	Medical 🏥	10.10.20.0/24	E-Core-1	110
30	Police 👮	10.10.30.0/24	E-Core-1	110
40	Rescue 🚒	10.10.40.0/24	E-Core-2	110
60	IT	10.10.60.0/24	E-Core-2	110

Note: Traffic distribution across both core switches maximizes resource utilization.

3.2 Routing Protocol Configuration

OSPF Multi-Area Implementation

Key Configuration Elements:

```
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 passive-interface default
 no passive-interface GigabitEthernet0/0
 network 50.50.200.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.3 area 0
```

OSPF Features Implemented:

- **Loopback Router IDs** for stability during interface failures
- **Passive interfaces** on access ports (prevents unauthorized OSPF neighbors)
- **Point-to-point network type** on WAN links for faster convergence
- **Route summarization** at ABRs to minimize routing table size
- **Area Border Router (Central-2)** connecting Areas 0, 1, 2, and 3

3.3 High Availability Implementation

HSRP Configuration

Active-Standby Gateway Redundancy:

! Core-Active (Priority 110 - Active)

```
interface Vlan10
 ip address 50.50.10.2 255.255.255.0
 standby version 1
 standby 10 ip 50.50.10.1
 standby 10 priority 110
 standby 10 preempt
```

! Core-Standby (Priority 90 - Standby)

```
interface Vlan10
 ip address 50.50.10.3 255.255.255.0
 standby version 1
 standby 10 ip 50.50.10.1
 standby 10 priority 90
 standby 10 preempt
```

HSRP Benefits:

- **Sub-second failover** (<1 second during active switch failure)
- **Transparent operation** (clients continue using same gateway IP)
- **Load balancing capability** (different VLANs active on different switches)

LACP Link Aggregation

```
interface Port-channel1
 switchport mode trunk
interface range GigabitEthernet1/0/23-24, GigabitEthernet1/1/1
 switchport mode trunk
 channel-group 1 mode active
```

Advantages:

- 3 Gbps aggregate bandwidth (3 × 1 Gbps links)
- Automatic load distribution across links
- Link-level redundancy (surviving links continue if one fails)

Spanning Tree Protocol

```
spanning-tree mode rapid-pvst
spanning-tree vlan 1-99 priority 24576
```

Why Rapid-PVST:

- Convergence time: 2-3 seconds (vs. 30-50 seconds in traditional STP)
- Per-VLAN optimization allows load balancing
- Backward compatible with IEEE 802.1D

3.4 VoIP Telephony System

Site	Extension Range	Phone Count	CME IP	Codec
Headquarters	6001-6005	5	50.50.100.2	G.711
Branch 2	2001-2004	4	10.20.255.5	G.711
Emergency	115, 1122, 15, 1151, etc.	10	10.10.90.20	G.711

Total Phones: 19 across 3 sites

Cisco CME Configuration

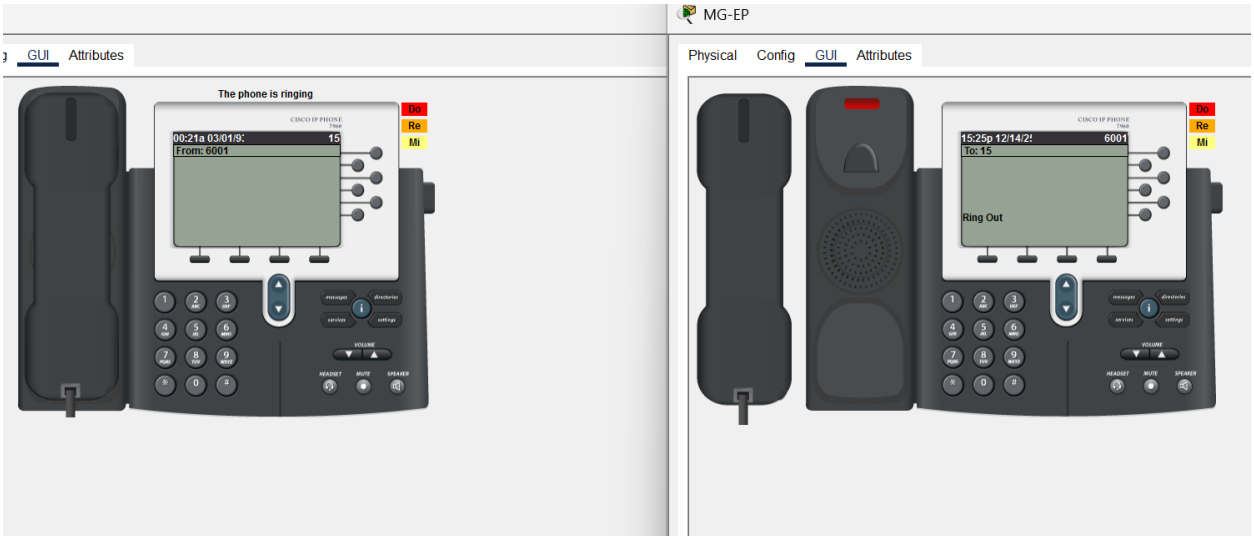
```
telephony-service
 max-ephones 42
 max-dn 100
 ip source-address 50.50.100.2 port 2000
 auto assign 1 to 5
ephone-dn 1
 number 6001
ephone 1
 mac-address 0001.96ED.A844
 button 1:1
```

Inter-Site Calling (Dial-Peer)

```
! HQ to Branch 2
dial-peer voice 2 voip
 destination-pattern 200[1-4]
 session target ipv4:10.20.255.5
 codec g711ulaw
```

Calling Capabilities:

- HQ ↔ Branch 2 ↔ Emergency Site (full mesh connectivity)
- Emergency hotlines accessible from all sites
- DTMF relay for interactive menus



3.5 Server Infrastructure

Headquarters Server Farm (50.50.10.0/24)

Server	IP	Services	Function
DHCP	50.50.10.10	DHCP	Automatic IP assignment (9 pools for 9 VLANs)
DNS	50.50.10.11	DNS	Internal resolution (domain: pesi.com)
Email	50.50.10.12	SMTP, POP3	Corporate email system
FTP	50.50.10.14	FTP	File sharing, IOS image repository
NTP/Syslog	50.50.10.16	NTP, Syslog	Time sync + centralized logging
AAA/RADIUS	50.50.10.18	RADIUS	Network device authentication (Port 1645)
IoT	50.50.10.17	IoT	Smart security system controller

DHCP Configuration Sample:

ip dhcp pool VOICE-POOL

network 50.50.70.0 255.255.255.0

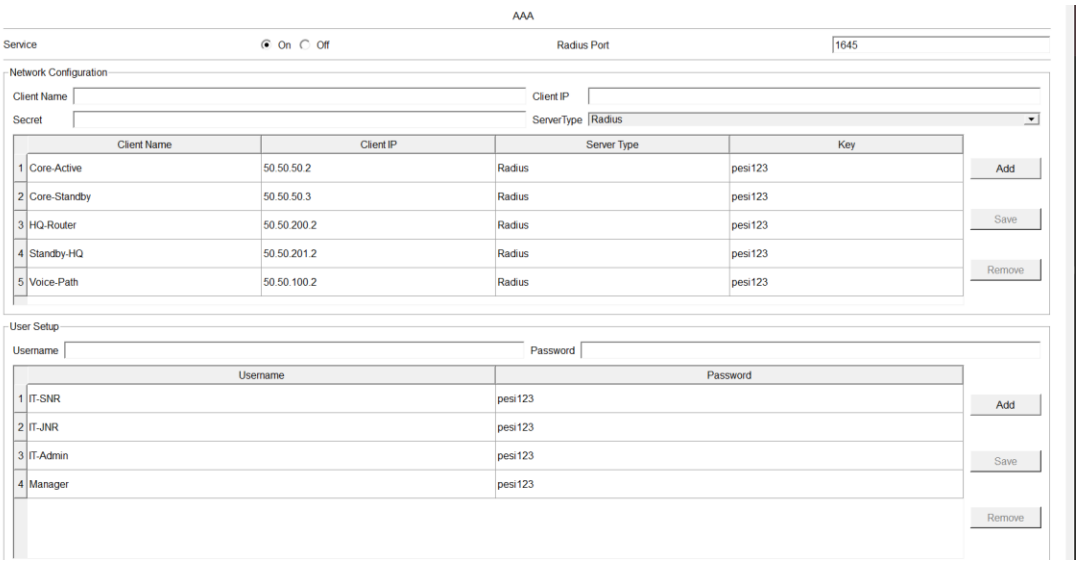
default-router 50.50.70.1

dns-server 50.50.10.11

option 150 ip 50.50.100.2

Emergency Site Servers (10.10.90.0/24)

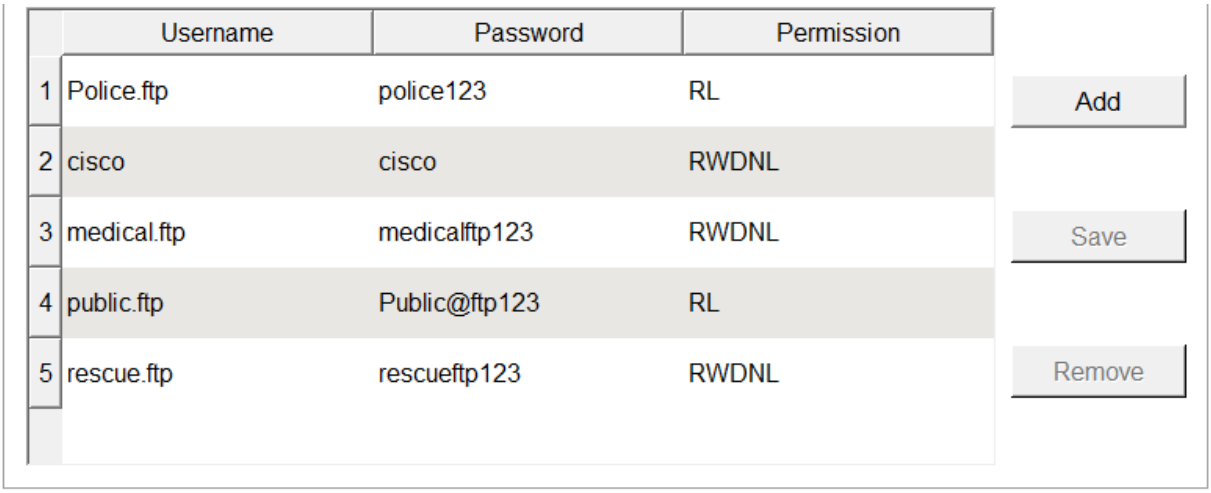
AAA/RADIUS Configuration:




```
[Connection to 50.50.100.2 closed by foreign host]
C:\>ssh -l admin 50.50.100.2

Password:
Voice-Path>enable
Password:
Voice-Path#
```

FTP Server (Emergency Access):



	Username	Password	Permission
1	Police.ftp	police123	RL
2	cisco	cisco	RWDNL
3	medical.ftp	medicalftp123	RWDNL
4	public.ftp	Public@ftp123	RL
5	rescue.ftp	rescueftp123	RWDNL

DMZ Public Servers (Central Distribution)

Server	Internal IP	Public IP (PTCL)	Public IP (Nayatel)	Service
Web	172.16.0.10	203.0.113.100	203.0.114.100	HTTP/HTTPS
Mail	172.16.0.11	203.0.113.101	203.0.114.101	SMTP (587)
DNS	172.16.0.12	203.0.113.102	203.0.114.102	DNS (53)
FTP	172.16.0.13	203.0.113.103	203.0.114.103	FTP (21)

Dual public IPs provide ISP redundancy and load balancing.

3.6 Security Architecture

FIREWALL-1 (Primary Cisco ASA):

Interface	Security Level	IP Address	Purpose
Outside1	0 (Untrusted)	203.0.113.6/30	PTCL ISP
Outside2	0 (Untrusted)	203.0.114.6/30	Nayatel ISP
DMZ	50 (Medium)	172.16.1.1/30	Public servers
Inside	100 (Trusted)	10.255.1.2/30	Corporate network

Security Policy:

- Inside → Outside: **Allowed** (NAT applied)
- Outside → DMZ: **Specific services only** (HTTP, SMTP, DNS, FTP)
- DMZ → Inside: **BLOCKED** (prevents compromised servers attacking internal network)

NAT Configuration

Dynamic PAT (Outbound Internet):

```
object network HQ-NET
 subnet 50.50.0.0 255.255.0.0
 nat (inside,outside1) dynamic interface

object network EMERGENCY-NET
 subnet 10.10.0.0 255.255.0.0
 nat (inside,outside1) dynamic interface
```

Static NAT (Inbound Public Services):

```
object network WEB-SERVER
 host 172.16.0.10
 nat (dmz,outside1) static 203.0.113.100    ! PTCL IP
 nat (dmz,outside2) static 203.0.114.100    ! Nayatel IP
```

Access Control Lists

Firewall Inbound ACL:

```
access-list OUTSIDE1-IN extended permit tcp any host 203.0.113.100 eq 80
access-list OUTSIDE1-IN extended permit tcp any host 203.0.113.100 eq 443
access-list OUTSIDE1-IN extended permit tcp any host 203.0.113.101 eq smtp
access-list OUTSIDE1-IN extended permit udp any host 203.0.113.102 eq domain
access-list OUTSIDE1-IN extended permit icmp any any
```

DMZ Isolation ACL:

```
! Block DMZ from accessing internal networks
access-list DMZ-TO-INSIDE deny ip 172.16.0.0 255.255.255.0 50.50.0.0 255.255.0.0
access-list DMZ-TO-INSIDE deny ip 172.16.0.0 255.255.255.0 10.10.0.0 255.255.0.0
access-list DMZ-TO-INSIDE deny ip 172.16.0.0 255.255.255.0 10.20.0.0 255.255.0.0
access-list DMZ-TO-INSIDE permit ip any any
```

AAA Authentication

```
aaa new-model
aaa authentication login default group radius local
aaa authorization exec default group radius local
aaa accounting exec default start-stop group radius

radius server PESI-AAA
 address ipv4 10.10.90.12 auth-port 1645
 key pesi123
```

Benefits:

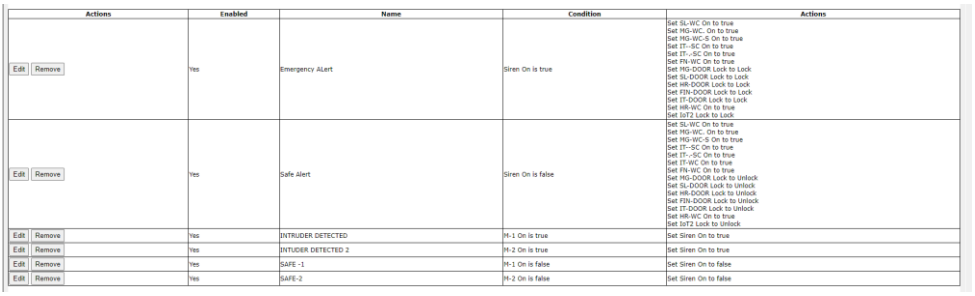
- Centralized user management across all network devices
- Detailed audit logs for compliance
- Role-based access control (privilege levels)
- Local fallback if RADIUS server unreachable

SSH Hardening

```
hostname HQ-Router
ip domain-name pesi.com
crypto key generate rsa modulus 2048
username admin privilege 15 secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
line vty 0 4
 transport input ssh
 login local
 exec-timeout 10 0
ip ssh version 2
```

IoT Security System (HQ)

Device	Status	Trigger	Action
Camera	Always ON	–	24/7 surveillance
Motion Detector	Armed	Motion detected	Activate siren + lock doors
Siren	Standby	Motion detector	Sound alarm
Smart Locks	Armed	Motion detector	Lock all entry points



Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Emergency ALert	Siren On is true	Set SL-WC On to true Set MG-WC_On to true Set MG-WC-S On to true Set IT--SC On to true Set IT--SC On to true Set FN-WC On to true Set MG-DOOR Lock to Lock Set SL-DOOR Lock to Lock Set HR-DOOR Lock to Lock Set FIN-DOOR Lock to Lock Set IT-DOOR Lock to Lock Set HR-WC On to true Set IoT2 Lock to Lock
Edit Remove	Yes	Safe Alert	Siren On is false	Set SL-WC On to true Set MG-WC_On to true Set MG-WC-S On to true Set IT--SC On to true Set IT--SC On to true Set IT-WC On to true Set FN-WC On to true Set MG-DOOR Lock to Unlock Set SL-DOOR Lock to Unlock Set HR-DOOR Lock to Unlock Set FIN-DOOR Lock to Unlock Set IT-DOOR Lock to Unlock Set HR-WC On to true Set IoT2 Lock to Unlock
Edit Remove	Yes	INTRUDER DETECTED	M-1 On is true	Set Siren On to true
Edit Remove	Yes	INTUDER DETECTED 2	M-2 On is true	Set Siren On to true
Edit Remove	Yes	SAFE -1	M-1 On is false	Set Siren On to false
Edit Remove	Yes	SAFE-2	M-2 On is false	Set Siren On to false

4. TESTING & VALIDATION

- ## LOGS

Syslog

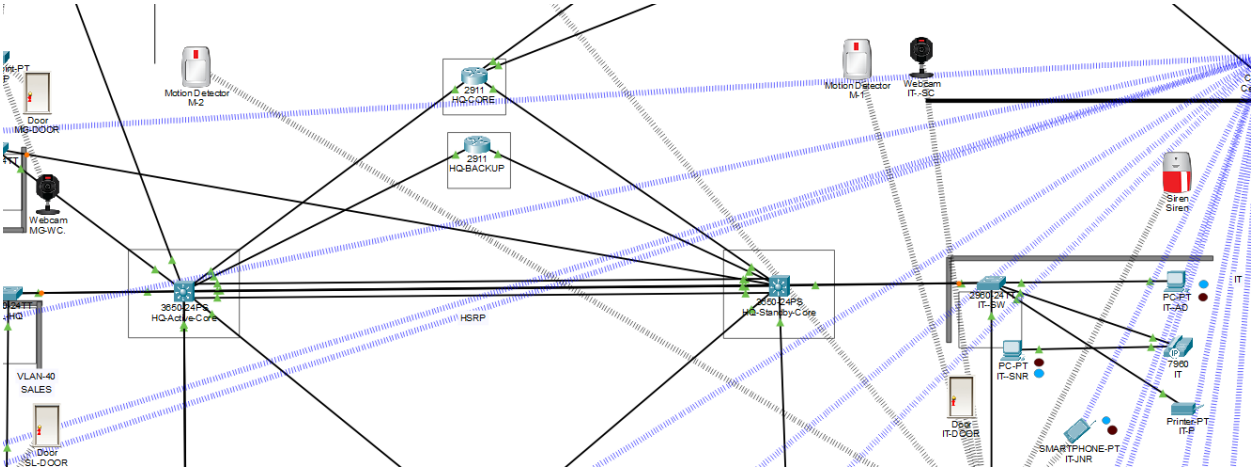
Syslog

Service

On Off

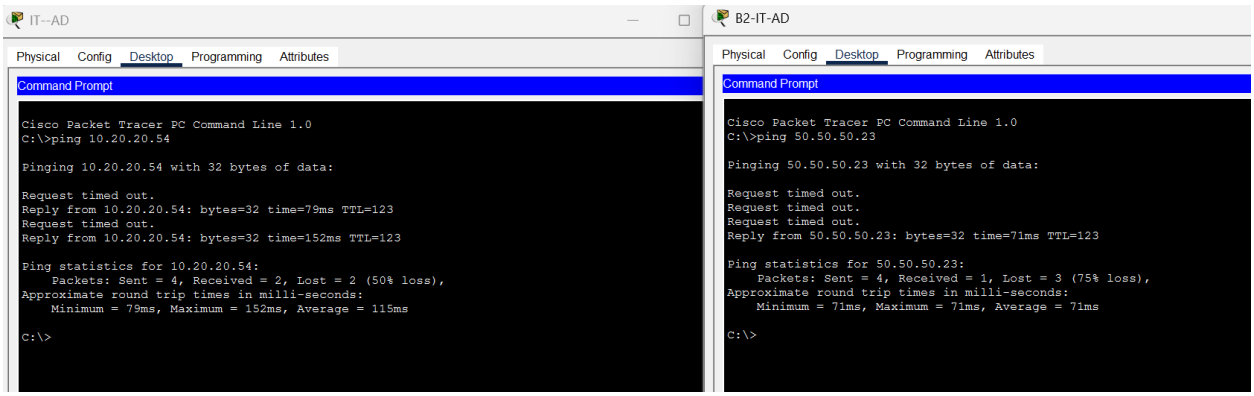
	Time	HostName	Message
1	12.14.2025 09:58:43.087 AM	50.50.10.3	%LINEPROTO-5-UPDOWN: Line protocol on Interface ...
2	12.14.2025 09:58:43.087 AM	50.50.10.3	%LINK-5-CHANGED: Interface GigabitEthernet1/0/5, changed state to up
3	12.14.2025 09:58:43.094 AM	50.50.10.2	%LINEPROTO-5-UPDOWN: Line protocol on Interface ...
4	12.14.2025 09:58:43.094 AM	50.50.10.2	%LINK-5-CHANGED: Interface GigabitEthernet1/0/7, changed state to up
5	12.14.2025 09:58:24.376 AM	50.50.10.3	09:58:24: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on ...
6	12.14.2025 09:58:24.376 AM	50.50.10.3	%LINEPROTO-5-UPDOWN: Line protocol on Interface ...
7	12.14.2025 09:58:24.376 AM	50.50.10.3	%LINK-3-UPDOWN: Interface GigabitEthernet1/0/5, changed state to down
8	12.14.2025 09:58:24.488 AM	50.50.10.2	09:58:24: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on ...
9	12.14.2025 09:58:24.488 AM	50.50.10.2	%LINEPROTO-5-UPDOWN: Line protocol on Interface ...
10	12.14.2025 09:58:24.488 AM	50.50.10.2	%LINK-3-UPDOWN: Interface GigabitEthernet1/0/7, changed state to down
11	12.14.2025 09:57:50.172 AM	50.50.100.2	%SYS-5-CONFIG_I: Configured from console by console

- ## Emergency Alert Checkup

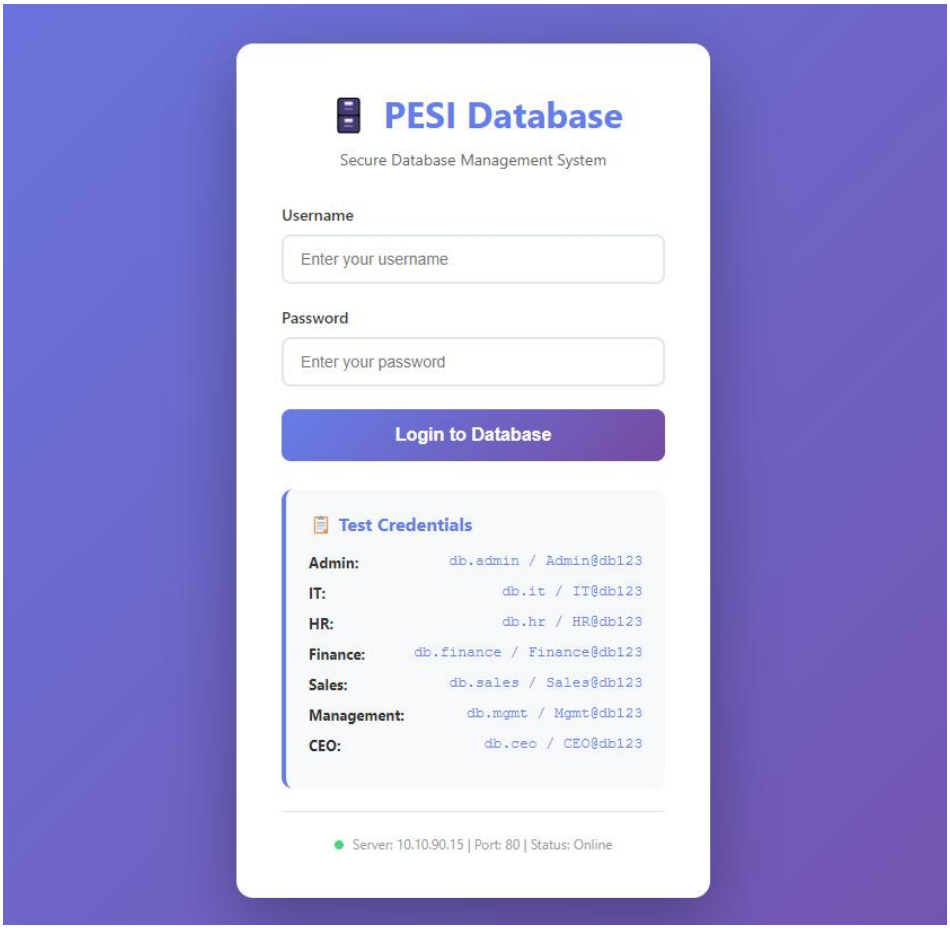


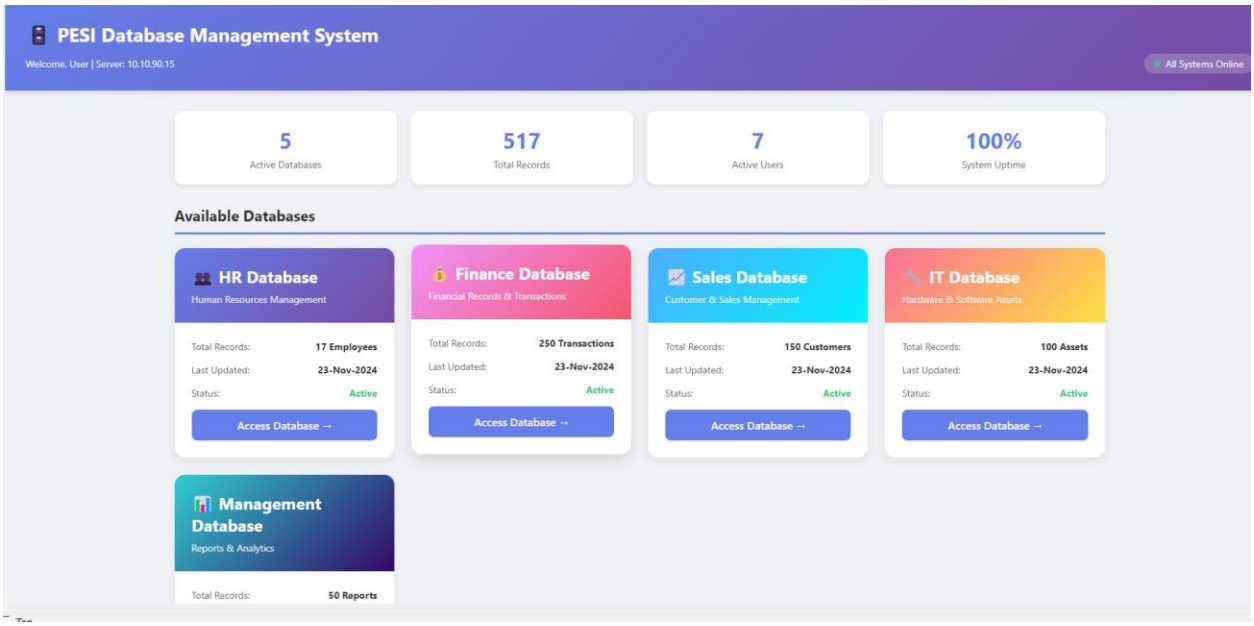
- Emergency Call 15 from HQ

- Ping Check from HQ to B1 & from B1 to HQ



- **Data-Base**


PESI Database
Secure Database Management System
Username
Enter your username
Password
Enter your password
Login to Database
Test Credentials
Admin: db.admin / Admin@db123
IT: db.it / IT@db123
HR: db.hr / HR@db123
Finance: db.finance / Finance@db123
Sales: db.sales / Sales@db123
Management: db.mgmt / Mgmt@db123
CEO: db.ceo / CEO@db123
Server: 10.10.90.15 | Port: 80 | Status: Online


PESI Database Management System
Welcome, User | Server: 10.10.90.15
All Systems Online
5
Active Databases
517
Total Records
7
Active Users
100%
System Uptime
Available Databases
HR Database
Human Resources Management
Total Records: 17 Employees
Last Updated: 23-Nov-2024
Status: Active
Access Database →
Finance Database
Financial Records & Transactions
Total Records: 250 Transactions
Last Updated: 23-Nov-2024
Status: Active
Access Database →
Sales Database
Customer & Sales Management
Total Records: 150 Customers
Last Updated: 23-Nov-2024
Status: Active
Access Database →
IT Database
Hardware & Software Assets
Total Records: 100 Assets
Last Updated: 23-Nov-2024
Status: Active
Access Database →
Management Database
Reports & Analytics
Total Records: 50 Reports

APPENDIX

Device Type	Model	Quantity	Deployment
L3 Core Switch	Cisco Catalyst 3650	8	All Sites
Edge Router	Cisco ISR 4431	6	HQ, Branches, Emergency
Firewall	Cisco ASA 5506-X	2	Central Distribution
L2 Access Switch	Cisco Catalyst 2960	15+	All Sites
IP Phone	Cisco 7960	19	HQ, Branch 2, Emergency
VPN Router	Cisco ISR 4331	2	Central Distribution

5. CONCLUSION

5.1 Achievement Summary

The Pakistan Emergency Smart Infrastructure (PESI) network successfully delivers a **mission-critical, enterprise-grade communication platform** serving **2,500+ users** across *5* **geographical locations**. All project objectives have been achieved:

Multi-Site Connectivity

All sites interconnected via OSPF multi-area routing with optimized traffic flow

High Availability

Zero single points of failure achieved through dual core switches (HSRP), dual routers, dual firewalls, and dual ISPs

Emergency Services Integration

Dedicated infrastructure for Police, Medical, Rescue, and Ambulance with 10 emergency hotlines operational 24/7

Unified Communications

19 IP phones deployed across 3 sites with full inter-branch calling capability using G.711 codec

Enterprise Security

Multi-layered protection including Cisco ASA firewalls with DMZ isolation, AAA/RADIUS authentication, NAT/PAT, and comprehensive ACL policies

Scalability

Each site uses /16 addressing supporting 65,000+ hosts with VLAN segmentation allowing easy department expansion

Centralized Management

Consolidated DHCP, DNS, Email, FTP, RADIUS services with NTP synchronization and centralized Syslog monitoring

---