Hospital Network Segmentation Project Documentation

Executive Summary

This document provides a professional, structured record of the design, configuration, and testing of a segmented hospital lab network using Cisco switches. Patient monitors are isolated in their own VLAN to protect sensitive data, while administrative and medical-staff devices are separated into dedicated segments. Access Control Lists (ACLs) and port security enforce strict traffic policies.

1. Project Objectives

- Isolate patient monitoring devices from general and administrative traffic.
- Enforce least-privilege access using VLANs, ACLs, and port security.
- Enable secure inter-VLAN routing for essential services.
- Document configurations and test results for operational handover.

2. Network Overview

Component	Model	Role
Core Switch	Cisco 2960	Layer-3 inter-VLAN routing
Access Switch	Cisco 2960	Layer-2 access for end devices
Patient Monitor PCs	Generic PCs	VLAN 10 endpoints
Administrative PCs	Generic PCs	VLAN 20 endpoints
Medical-Staff PCs	Generic PCs	VLAN 30 endpoints
Management Network	VLAN 99	Switch management and services

3. IP Addressing & VLAN Plan

VLAN ID	Name	Subnet	Gateway	Connected Devices
10	Patient-Monitors	192.168.10.0/24	192.168.10.1	PC0 (10), PC1 (11), PC2 (12)
20	Administrative	192.168.20.0/24	192.168.20.1	PC3 (10), PC4 (11)

30	Medical-Staff	192.168.30.0/24	192.168.30.1	PC5 (10), PC6 (11)
99	Management	192.168.99.0/24	192.168.99.1	Switch SVIs, SNMP, logging

4. Physical & Logical Topology

A Core Switch connects via a trunk port to an Access Switch. End devices attach to the Access Switch on access ports assigned to VLAN 10, 20, or 30. All VLANs traverse the trunk, with VLAN 99 as the native management VLAN.

5. Configuration Summary

5.1 Core Switch (Core-SW-Hospital)

```
enable
configure terminal
hostname Core-SW-Hospital

! VLANs
vlan 10 name Patient-Monitors
vlan 20 name Administrative
vlan 30 name Medical-Staff
vlan 99 name Management

! SVIs for inter-VLAN routing
interface vlan 10
  ip address 192.168.10.1 255.255.255.0
interface vlan 20
  ip address 192.168.20.1 255.255.255.0
interface vlan 30
  ip address 192.168.30.1 255.255.255.0
interface vlan 99
  ip address 192.168.99.1 255.255.255.0
ip routing

! Trunk to Access Switch
interface gigabitethernet0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
```

```
  switchport trunk native vlan 99
  switchport trunk allowed vlan 10,20,30,99
  no shutdown

! ACLs for security
ip access-list extended ACL_PM
  permit tcp 192.168.10.0 0.0.0.255 any eq 22
  permit icmp 192.168.10.0 0.0.0.255 any
  permit ip 192.168.10.0 0.0.0.255 host 192.168.10.1
  deny ip any any log
interface vlan 10
  ip access-group ACL_PM in
```

5.2 Access Switch (Access-SW-Hospital)

```
enable
configure terminal
hostname Access-SW-Hospital

! VLANs
vlan 10 name Patient-Monitors
vlan 20 name Administrative
vlan 30 name Medical-Staff
vlan 99 name Management

! Trunk to Core Switch
interface fastethernet0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 99
  switchport trunk allowed vlan 10,20,30,99
  no shutdown

! Access ports
interface range fastethernet0/2-4
  switchport mode access
  switchport access vlan 10
  switchport port-security
  switchport port-security maximum 1
```

```
  switchport port-security mac-address sticky
  switchport port-security violation shutdown

interface range fastethernet0/5-6
  switchport mode access
  switchport access vlan 20
  switchport port-security
  switchport port-security maximum 1
  switchport port-security mac-address sticky
  switchport port-security violation restrict

interface range fastethernet0/7-8
  switchport mode access
  switchport access vlan 30
  switchport port-security
  switchport port-security maximum 1
  switchport port-security mac-address sticky
  switchport port-security violation protect

! Global port-security settings
errdisable recovery cause psecure-violation
errdisable recovery interval 300
```

6. Testing & Validation

Test Scenario	Command/Action	Expected Result
VLAN membership	`show vlan brief`	Ports in correct VLANs
Inter-VLAN routing	`ping 192.168.20.10 source 192.168.10.10`	Successful ICMP from VLAN 10→20
ACL enforcement (deny HTTP/HTTPS)	Attempt HTTP from PC0 (Patient VLAN)	Traffic dropped (no response)
Port security violation	Connect unauthorized device on FA0/2	Port shutdown and violation counter inc.

7. Backup, Monitoring & Maintenance

- Save running configs to startup:

```
copy running-config startup-config
```

- Off-site backup via TFTP:

```
copy startup-config tftp://192.168.99.10/core-backup.cfg
```

- Logging & SNMP:

```
logging host 192.168.99.10
logging trap informational
snmp-server community HospitalRO RO
snmp-server host 192.168.99.10 HospitalRO
```

8. Appendix

- **PC IP Assignments**
    - PC0–PC2: 192.168.10.10–12/24, GW 192.168.10.1
    - PC3–PC4: 192.168.20.10–11/24, GW 192.168.20.1
    - PC5–PC6: 192.168.30.10–11/24, GW 192.168.30.1
- **Definitions**
    - **ACL**: Access Control List
    - **SVI**: Switch Virtual Interface