### **This Cisco Packet Tracer project simulates a hospital network where departments are separated using VLANs, and security policies are enforced using ACLs. It demonstrates how to isolate sensitive systems from public/guest access — a real-world example of network segmentation and access control.**

### 

### **Objective:**

* **Create separate VLANs for each department:**
  + **Admin (VLAN 10)**
  + **Medical (VLAN 20)**
  + **Security (VLAN 30)**
  + **Guest (VLAN 40)**
* **Allow inter-VLAN communication (routing)**
* **Block Guest VLAN from accessing secure departments**

### **What’s Configured:**

* **All PCs assigned to the correct VLANs with static IPs**
* **A router configured with router-on-a-stick setup (sub-interfaces for each VLAN)**
* **VLANs created and switchports assigned**
* **An Access Control List (ACL) applied to block Guest VLAN from reaching Admin, Medical, or Security networks**

### **Steps to Test the Project:**

1. **Open the .pkt file in Cisco Packet Tracer**
2. **Click PC6 or PC7 (Guest VLAN)**

* **Go to:  
    
   nginx  
  CopyEdit  
  Desktop → Command Prompt**
* **Ping the other VLANs:**  
    
   bash  
  CopyEdit  
  ping 192.168.10.10 ← Admin1
* ping 192.168.20.10 ← Medical1
* ping 192.168.30.10 ← Security1
* **Expected Result:** All pings should return:  
    
   csharp  
  CopyEdit  
  Request timed out.

1. This confirms the **Guest VLAN is blocked** from accessing private departments.

### **Security Showcase:**

* Guest devices can access the internet (if enabled) but **cannot interact** with internal systems
* This mirrors **real-world hospital security** setups (HIPAA compliance, Zero Trust policies, etc.)