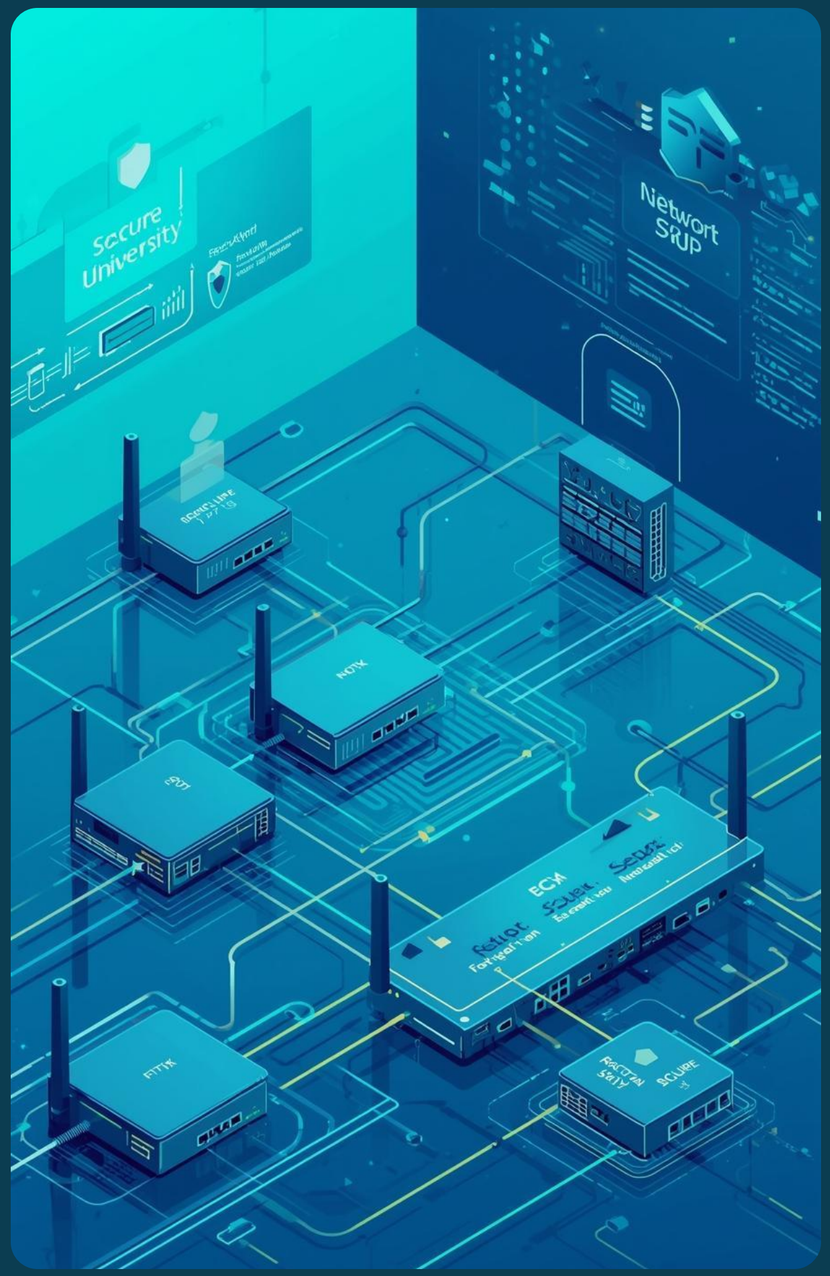
University Department Network with Guest Wi-Fi & Secure VLANs



The Challenge: Secure Campus Network

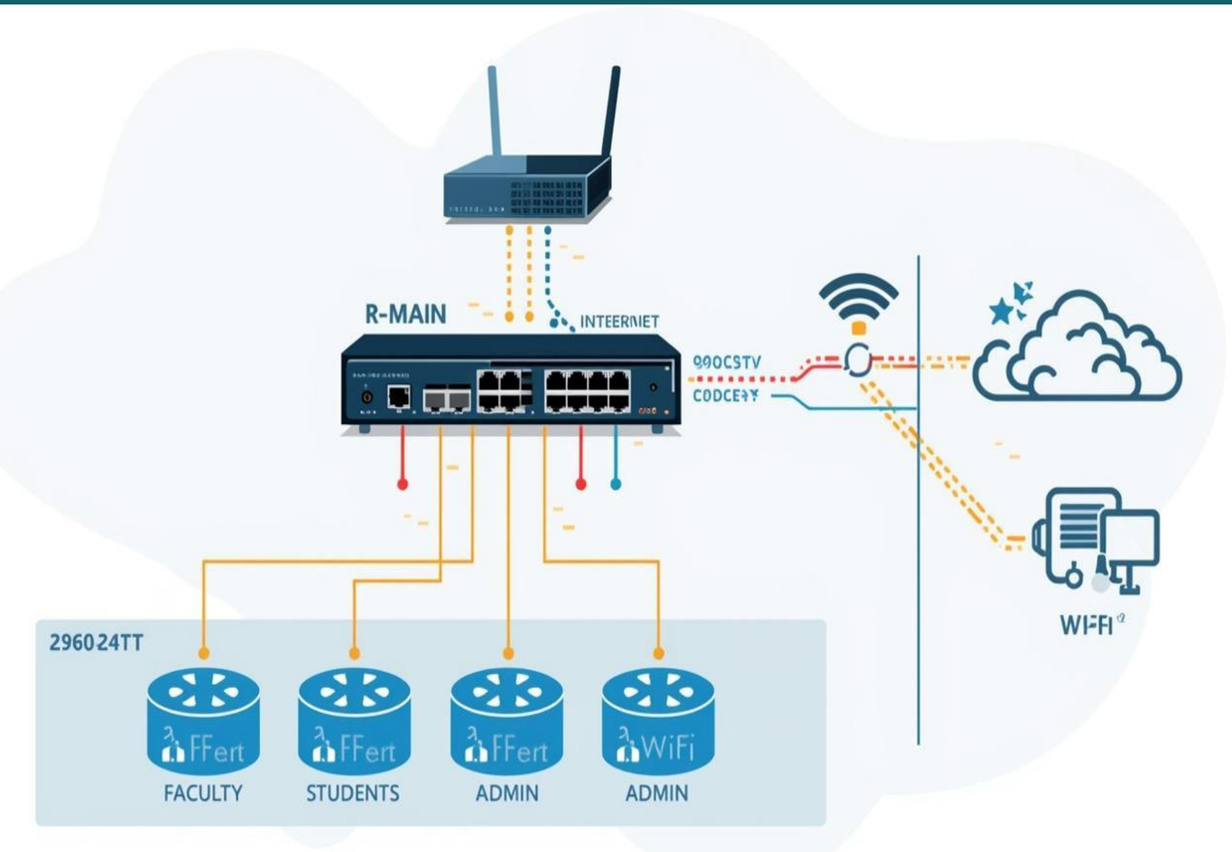
Scenario: Secure internal network for faculty, students, and admin + guest Wi-Fi with Internet access but NO internal system access

Main Objectives:

- **Implement VLAN segmentation for different user groups**
- **Configure inter-VLAN routing using router-on-a-stick**
- **Deploy DHCP for automatic IP assignment**
- **Apply ACLs for security policies**
- **Implement NAT for Internet connectivity**
- **Isolate guest network completely**
- **Monitor network usage via dashboard**

Network Topology Design

Network Diagram



Main Components:

✓ **Main Router (R-MAIN) - Router-on-a-Stick**

✓ **Main Switch (2960-24TT) - Central Distribution**

✓ **Faculty, Students, Admin Switches**

✓ **Wireless Access Point (Guest)**

✓ **Internet Connection**

Key Design: All VLANs traverse trunk links to router for inter-VLAN routing

Network Segmentation Strategy

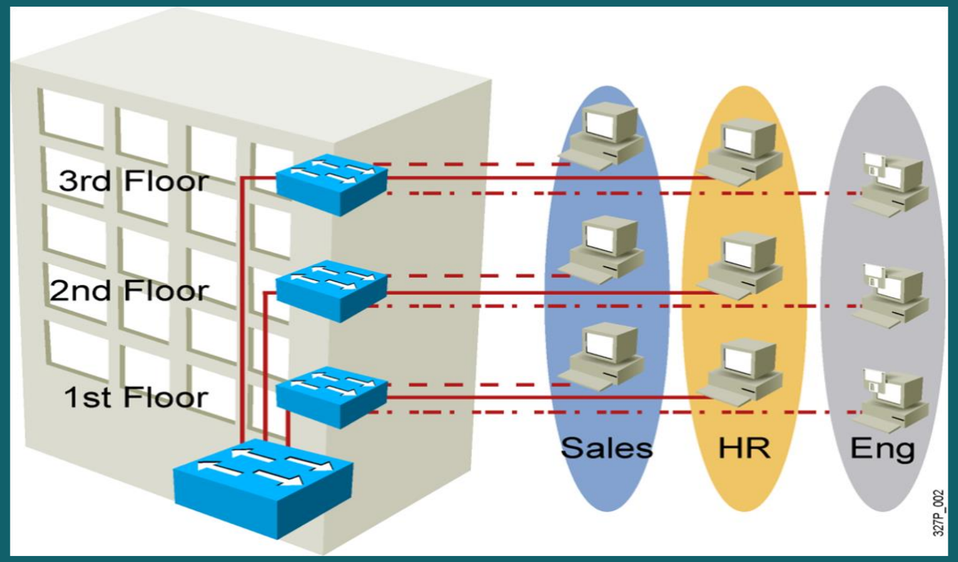
VLAN ID	VLAN Name	Network Subnet	Default Gateway	Purpose
١٠	Faculty	١٩٢,١٦٨,١٠,٠/٢٤	١٩٢,١٦٨,١٠,١	Faculty staff devices
٢٠	Students	١٩٢,١٦٨,٢٠,٠/٢٤	١٩٢,١٦٨,٢٠,١	Student devices
٣٠	Admin	١٩٢,١٦٨,٣٠,٠/٢٤	١٩٢,١٦٨,٣٠,١	Administrative systems
٩٩	Guest	١٩٢,١٦٨,٩٩,٠/٢٤	١٩٢,١٦٨,٩٩,١	Guest Wi-Fi (isolated)

✓ Network segmentation improves security
✓ Broadcast isolation reduces traffic
✓ Policy enforcement per group
✓ Easier network management and troubleshooting

Layer 2 Configuration: VLANs on Switches

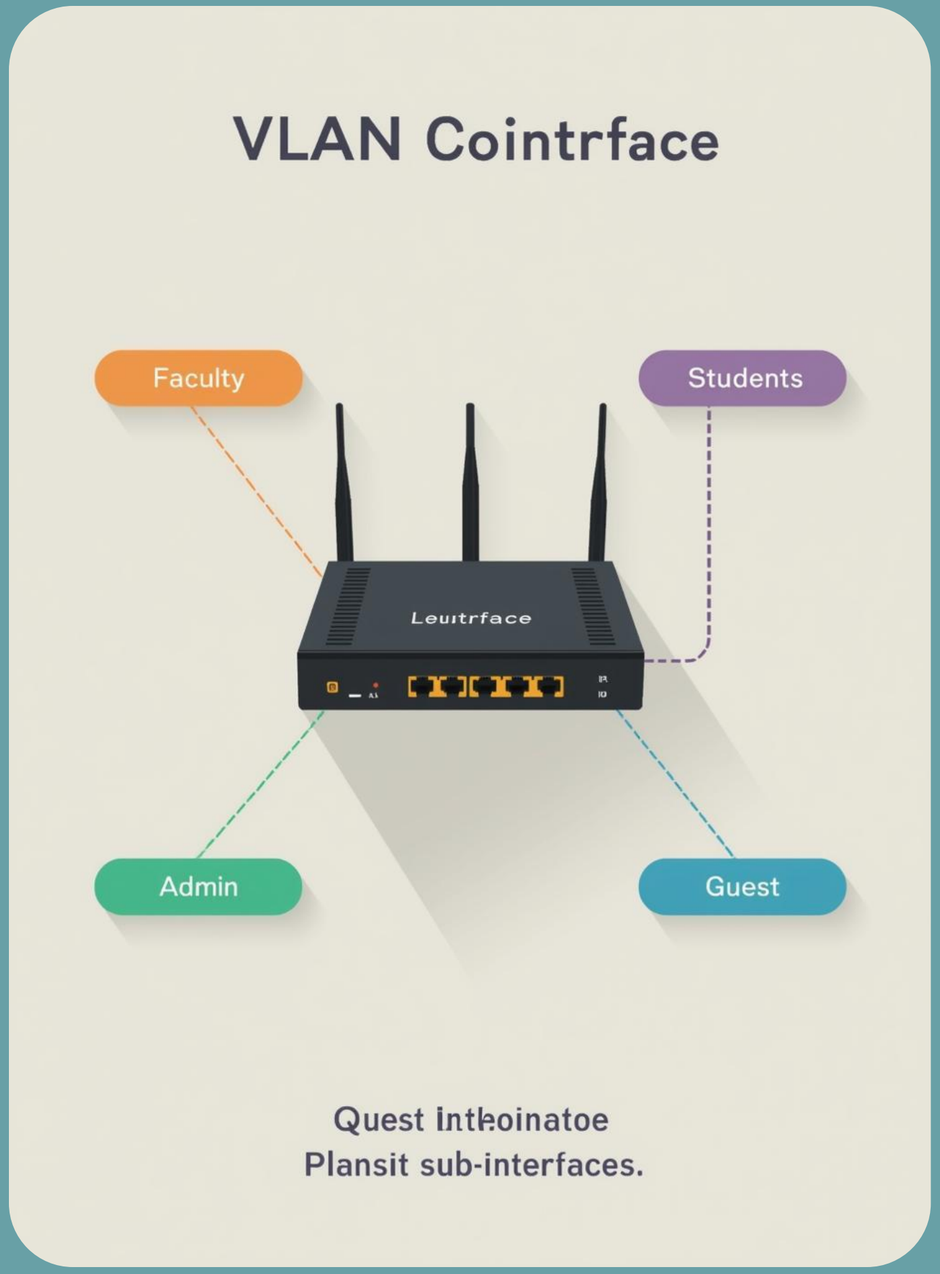
Main Switch Trunks:

vlan 10 - Faculty
vlan 20 - Students
vlan 30 - Admin
vlan 99 - Guest
Fa0/1-3: Trunk to Faculty Switch (VLAN 10,20,30,99)
Fa0/4-6: Trunk to Students Switch (VLAN 10,20,30,99)
Fa0/7-9: Trunk to Admin Switch (VLAN 10,20,30,99)
Fa0/10: Access port for Guest Wi-Fi AP (VLAN 99)
Gig0/1: Trunk to Main Router (all VLANs)



Access Switches:

- Faculty Switch: All ports in VLAN 10
- Students Switch: All ports in VLAN 20
- Admin Switch: All ports in VLAN 30



Inter-VLAN Routing Implementation

Router-on-a-Stick: Single router interface with multiple sub-interfaces (one per VLAN) using 802.1Q trunking

interface Gi0/0.10 → 192.168.10.1/24 (Faculty)
interface Gi0/0.20 → 192.168.20.1/24 (Students)
interface Gi0/0.30 → 192.168.30.1/24 (Admin)
interface Gi0/0.99 → 192.168.99.1/24 (Guest)

Encapsulation: dot1Q (VLAN tagging)
Each sub-interface serves as default gateway for its VLAN
All marked as "ip nat inside" for Internet access
Gi0/1 configured as "ip nat outside" for Internet connection

Automatic IP Address Assignment

Pool Name	Network	Gateway	DNS Server	Usable Range
FACULTY-POOL	١٩٢,١٦٨,١٠,٠/٢٤	١٩٢,١٦٨,١٠,١	٨,٨,٨,٨	٢٥٤. - ١١.
STUDENTS-POOL	١٩٢,١٦٨,٢٠,٠/٢٤	١٩٢,١٦٨,٢٠,١	٨,٨,٨,٨	٢٥٤. - ١١.
ADMIN-POOL	١٩٢,١٦٨,٣٠,٠/٢٤	١٩٢,١٦٨,٣٠,١	٨,٨,٨,٨	٢٥٤. - ١١.
GUEST-POOL	١٩٢,١٦٨,٩٩,٠/٢٤	١٩٢,١٦٨,٩٩,١	٨,٨,٨,٨	٢٥٤. - ١١.

🔄 Automatic configuration | ⚡ Plug-and-play connectivity | 📊 Centralized management

Guest Network Isolation with ACLs

Security Requirement: Guests access ONLY Internet, NOT internal VLANs

ACL 100 - Guest Isolation Policy:

deny ip 192.168.99.0 → 192.168.10.0 (Block Guest→Faculty)

deny ip 192.168.99.0 → 192.168.20.0 (Block Guest→Students)

deny ip 192.168.99.0 → 192.168.30.0 (Block Guest→Admin)

permit ip 192.168.99.0 → any (Allow Guest→Internet)

Applied OUTBOUND on interface Gi0/0.99

NAT Configuration (ACL 1)

- Permits all four VLANs to access Internet
- Uses PAT (Port Address Translation) overload
- Translates internal private IPs to public IP

✓ Complete isolation from sensitive data ✓ Internet-only access for guests

✓ Prevents lateral movement ✓ Protected faculty, student, and admin resources

Network Monitoring & Validation

Dashboard Monitoring:

- **Per-VLAN Bandwidth Utilization:** Track traffic usage for each network segment
- **Guest Access Alerts:** Detect unusual guest network activity
- **DHCP Lease Monitoring:** Track IP assignments
- **Security Event Logging:** Monitor ACL deny events

Sample Dashboard Graphs:

- Real-time bandwidth usage per VLAN (bar chart)
- Guest network connection timeline
- Failed access attempts from Guest VLAN

Network Monitoring & Validation

Testing Results:

Test Scenario	Expected Result	Status
Guest → Internet	✅ Success	PASS
Guest → Faculty VLAN	❌ Blocked	PASS
Guest → Students VLAN	❌ Blocked	PASS
Guest → Admin VLAN	❌ Blocked	PASS
Faculty → Internet	✅ Success	PASS
Student → Faculty	✅ Success	PASS
DHCP Assignment	✅ Auto-assigned	PASS

192.168.120.13/24
192.168.110.13/24
192.168.110.14/24
192.168.100.10/24
192.168.100.11/24
192.168.120.10/24
192.168.120.11/24
192.168.120.12/24
192.168.110.10/24
192.168.110.11/24
192.168.110.12/24
192.168.100.12/24
192.168.120.14/24

Thanks