Universal Remedies new campus in Salt Lake City, UT

Network Topology Offer

Addressing Plan

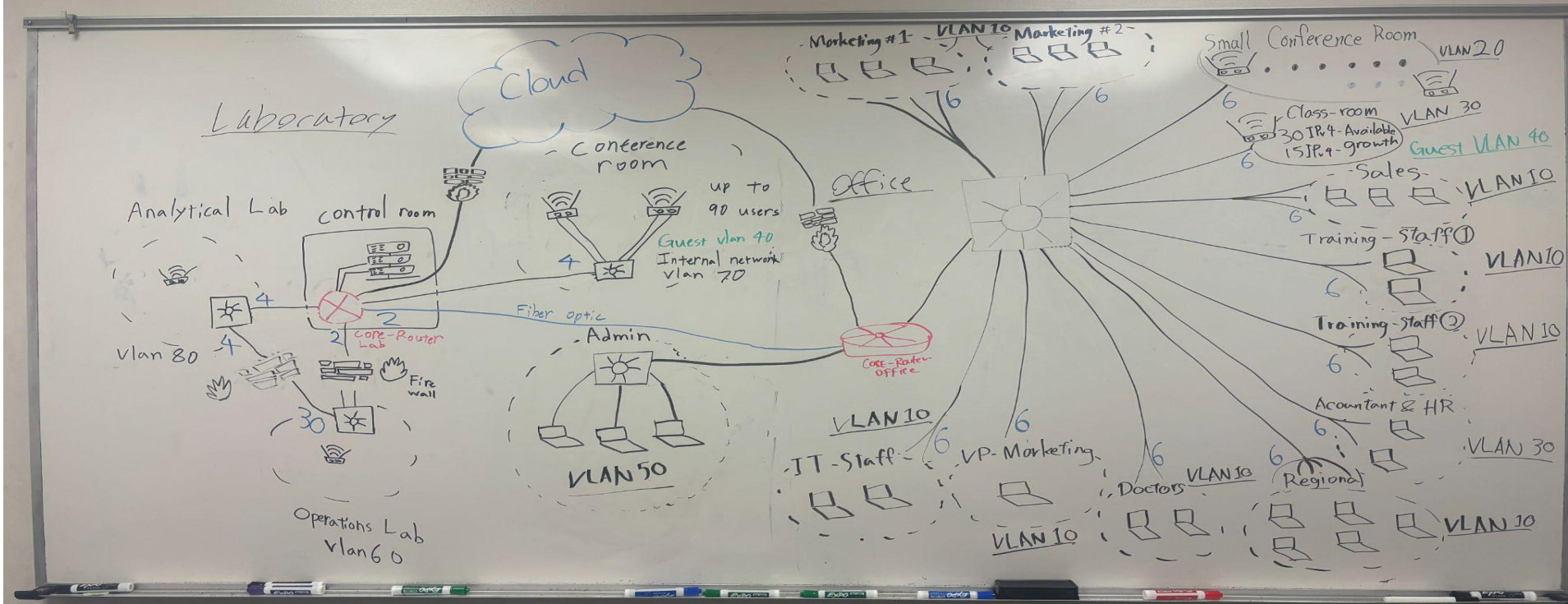
Cost-Effectiveness:

- Efficient Use of IP Addresses
- Scalability
- Centralized Management:
- Isolation of Networks

Security:

- Network Segmentation
- Isolated Networks for Sensitive Areas
- Guest Network
- Point-to-Point Links
- Controlled Access

https://docs.google.com/spreadsheets/d/1RlsJCZGKbrMcgcvOXPNFR0e8ChQSHSZ_BmfQwtddZnM/edit?gid=591449175#gid=591449175


Laboratory
Cloud
conference room
up to 90 users
Guest vlan 40
Internal network vlan 70
Analytical Lab
control room
Fiber optic
Admin
Core-Router Lab
Core-Router Office
Office
Vlan 80
Fire wall
Operations Lab
Vlan 60
VLAN 50
Marketing #1
VLAN 10
Marketing #2
Small Conference Room
VLAN 20
Class-room
30 IPv4-Available
15 IPv4-growth
VLAN 30
Guest VLAN 40
Sales
VLAN 10
Training-Staff①
Training-Staff②
Acountant & HR
IT-Staff
VP-Marketing
Doctors
Regional

Bill of Materials

Laboratory Capital Costs

Items:	Type:	Amount:	Prices per:
Router	Cisco ISR 4451-X	1	$6,000
Switches	Cisco Catalyst 9200 48-Port Gigabit	4	$2,500
Firewalls	Cisco Firepower 1000 Series	3	$3,500
Access Points	Uboquiti UniFi 6 Pro Wireless	5	$200
Ethernet Cables	Cat 6 Ethernet Cables	50	$50
Patch Panels	48-poer patch panel, Cat 6	2	$500
Media Converters	Fiber to RJ45	4	$150
Server	Dell PowerEdge R740	1	$10,000
UPS Systems	APC Smart UPS 1500VA	2	$500
	Total Capital Cost: $35,800		

Lab Labor Costs

Task/Installation:	Hours:	Cost:
Networking Equipment Install	20	$2,000
Server Installation/Configuration:	8	$1,200
Cabling & Patch Panel Install	15	$1,500
Wireless AP Install	8	$800
System Integration/Testing	10	$1,000

Total Install Cost:
$6,500

Office Capital Costs

Items:	Type:	Amount:	Price Per:
Router	Cisco ISR4451-X	1	$6,000
Switch	Cisco Catalyst 9200 48 Port	1	$2,500
Firewall	Cisco Firepower 1000 Series	1	$3,500
Wireless Access Points	Uboquiti UniFi 6 Pro Wireless	12	$200
UPS Systems	APC Smart-UPS 1500VA	5	$500
Ethernet Cables	Cat 6 Ethernet	120	$50
Fiber Cable	OS2 Riser Cable	2	$1,000

Total Capital Cost: $24,900

Capital Labor Costs

Task/Installation	Hours:	Price:	Total Cost:
Networking/Equipment Install	20	$2,000	$10,400
Cabling	30	$3,000	
Wireless AP Install	20	$2,400	
System Integration/Testing	10	$1,000	
Fiber Install(Between Buildings)	15	$2,000	

Operating Costs

Service:	Description	Monthly Cost:
Internet Service	Enterprise-grade ISP	$200/month
Maintenance Contracts	Networking/IT Support	$500/month
Energy Costs	UPS Power Backup	$600/month

Total Operating(Ongoing) Cost: $15,600

Total Cost

Laboratory Total: $42,300
Office Total: $35,300
Operating Total: $15,600

Grand Total: $93,200

Security Document

Network Security Goals

1. Ensure confidentiality, integrity, and availability of data.
2. Isolate critical networks (Operational Lab) from general access.
3. Protect internal and cloud-hosted resources from unauthorized access.
4. Secure communications between campus buildings, HQ, and the Internet.

Ports and Protocols

Service	Protocol	Port	Allowed Source	Allowed Destination	Purpose
HTTPS	TCP	443	All internal VLANs	Internet	Secure web browsing
DNS	UDP	53	All VLANs	DNS servers	Domain name resolution
IPsec VPN	UDP	500, 4500	HQ and Campus	HQ and Campus	Site-to-site VPN tunnel
Remote Desktop	TCP	3389	IT VLAN only	Internal Servers	Remote access for IT staff
SSH	TCP	22	IT VLAN only	Network Equipment	Secure device management
Lab Equipment (Custom)	TCP/UDP	Custom	Operational Lab VLAN	Operational Lab VLAN	Device-specific lab protocols

Physical Security Measures

1. **Access Control**:
    a. Use keycard access to secure network racks, server rooms, and critical areas (e.g., Control Room, Operational Lab).
    b. Limit access to IT staff and authorized personnel.
    c. Maintain a visitor log and ensure that visitors are always escorted when accessing sensitive areas.

2. **Surveillance**:
    a. Deploy CCTV cameras in server rooms and near access points.
    b. Retain footage for at least 30 days.
3. **Secure Cabling**:
    a. Use conduit to protect cables between buildings.
    b. Label cables to prevent misconfiguration or tampering.
4. **Equipment Protection**:
    a. Use secure cabinets and lockable racks for network equipment.
    b. Ensure that server rooms and network closets have adequate cooling and humidity control to protect equipment.
    c. Install fire suppression systems in data centers and server rooms to protect against fire damage.
5. **Physical Separation**:
    a. Ensure lab network devices are in a secure, restricted-access area.

. Network Security

Allowed and Disallowed Connections

Internal Network Access

Device/Resource	Allowed Connections	Disallowed Connections
Office Workstations	Internal resources, HQ, Internet	Operational Lab VLANs, Guest VLANs
Laboratory Workstations	Internal resources, HQ, Internet	Operational Lab VLANs, Guest VLANs
Operational Lab Devices	Other Operational Lab VLANs	Internet, Guest VLANs
Guest Devices	Internet only	Internal VLANs

Remote Access

- **Allowed**:
  - VPN access for HQ staff to internal resources.
  - IT staff can remotely manage equipment via VPN (e.g., SSH).
- **Disallowed**:
  - Direct Internet access to internal resources.

Firewall Rules

1. **Traffic Filtering**:
    a. Allow only necessary ports and protocols.
    b. Drop all traffic by default (deny all policy).
2. **Guest Network Isolation**:
    a. Use VLANs and ACLs to isolate guest traffic from internal networks.
    b. Provide Internet-only access.

Access Control

1. **Role-Based Access Control (RBAC)**:
    a. Restrict network access based on job roles (e.g., IT, Marketing, Lab Staff).
2. **User Authentication**:
    a. Use Active Directory for internal authentication.
    b. Implement Multi-Factor Authentication (MFA) for remote access.
3. **Captive Portal**:
    a. Use a captive portal for guest network access, requiring guests to agree to terms of service

Data Encryption

1. **Encrypt all sensitive data in transit:**
    a. Use IPsec VPN for site-to-site communication.
    b. Use HTTPS for web-based access.
2. **Encrypt data at rest for critical systems:**
    a. Employ AES-256 encryption for backup systems and servers.

Additional Security Considerations and Best Practices

Intrusion Detection and Prevention (IDPS)

- Deploy an IDPS at the network perimeter to detect and block malicious activities.
- A software called Suricata. (free)

Regular Updates and Patching

- Ensure all network equipment (routers, switches, firewalls) is updated regularly.
- Apply security patches to servers and endpoints within 30 days of release.
- Ensure all devices have up-to-date anti-malware software.

Backup and Disaster Recovery

- Use an on-premises NAS and cloud backup for critical data.
- Test backup recovery quarterly.

Logging and Monitoring

- Centralize logs using a Security Information and Event Management (SIEM) system (e.g., Splunk).
- Monitor traffic patterns to detect anomalies (e.g., excessive outbound traffic).

Multi-Factor Authentication (MFA)

- Implement MFA for accessing critical systems.

User Education:

- Train staff on security best practices and how to recognize threats.