Network Design Report – Wireless VLAN Simulation & Large Conference Scenario

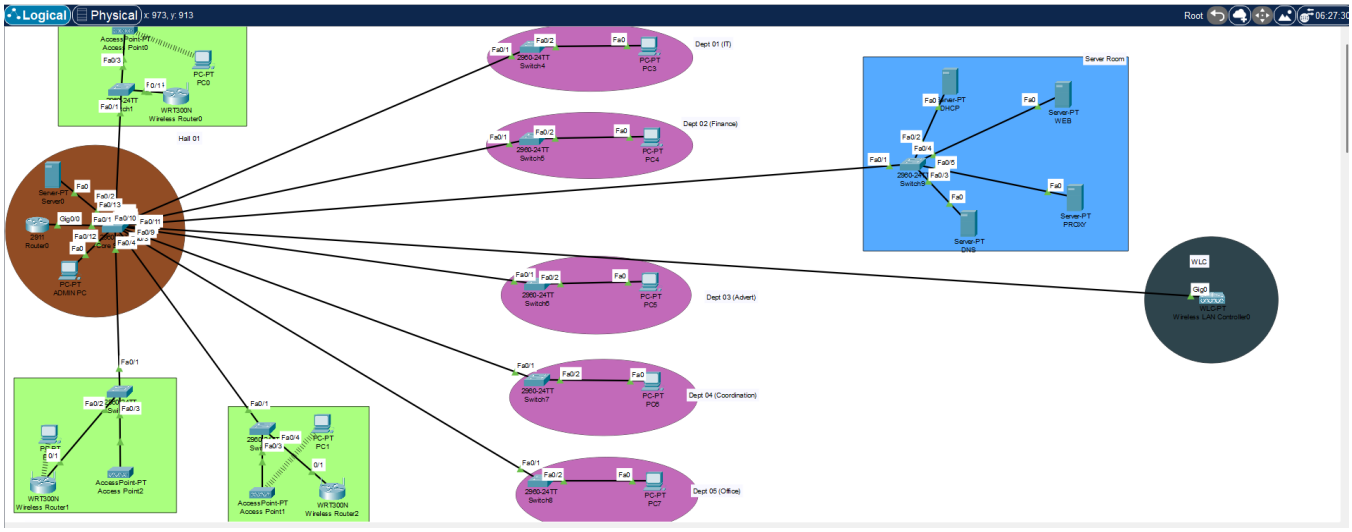
By- Anoshan Yoganathan

1. Project Overview

This report covers the design and simulation of a wireless and wired network for two environments:

1. **University VLAN-based Wireless Simulation**
2. **Large Conference Management Company Scenario**

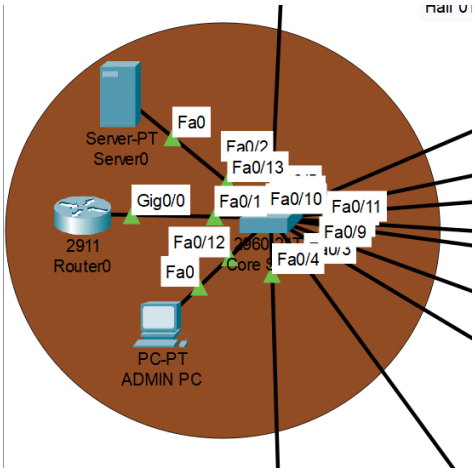
Both networks are modeled using **Cisco Packet Tracer**, applying VLANs, wireless connectivity, router-on-a-stick, and network security principles.



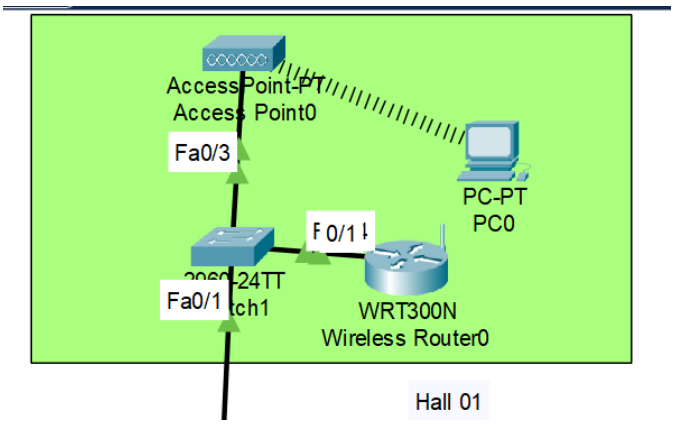
2. Scenario 1: University Wireless VLAN Simulation

Devices Used

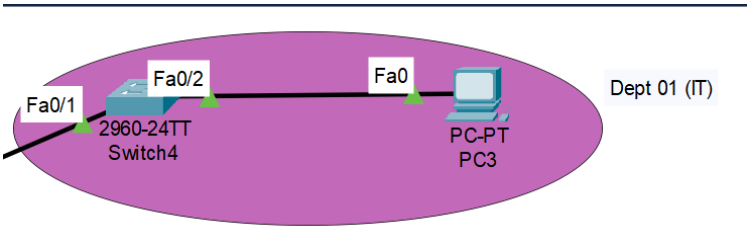
- Router (1)
- Switch (Core) (1)
- Wireless Routers (3)
- PCs (5)
- Server (1)



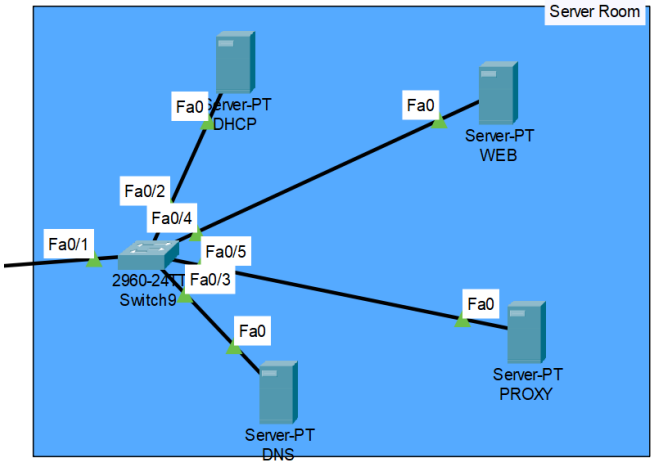
01. Admin



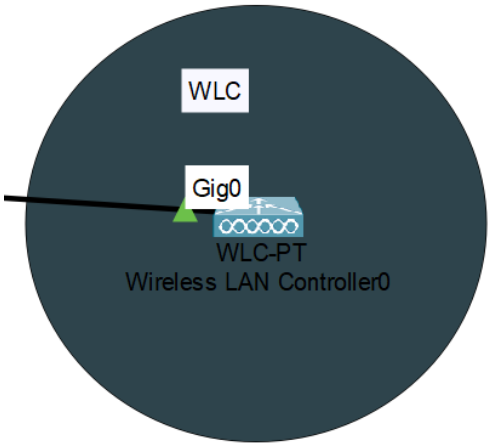
02 .Halls



03. Departments



04. Server Room



05. Wireless LAN Controller

VLAN Assignments

VLANs:
- VLAN 10: Hall 1 - 192.168.10.0/24
- VLAN 20: Hall 2 - 192.168.20.0/24
- VLAN 30: Hall 3 - 192.168.30.0/24
- VLAN 40: Department - 192.168.40.0/24
- VLAN 50: Admin - 192.168.50.0/24

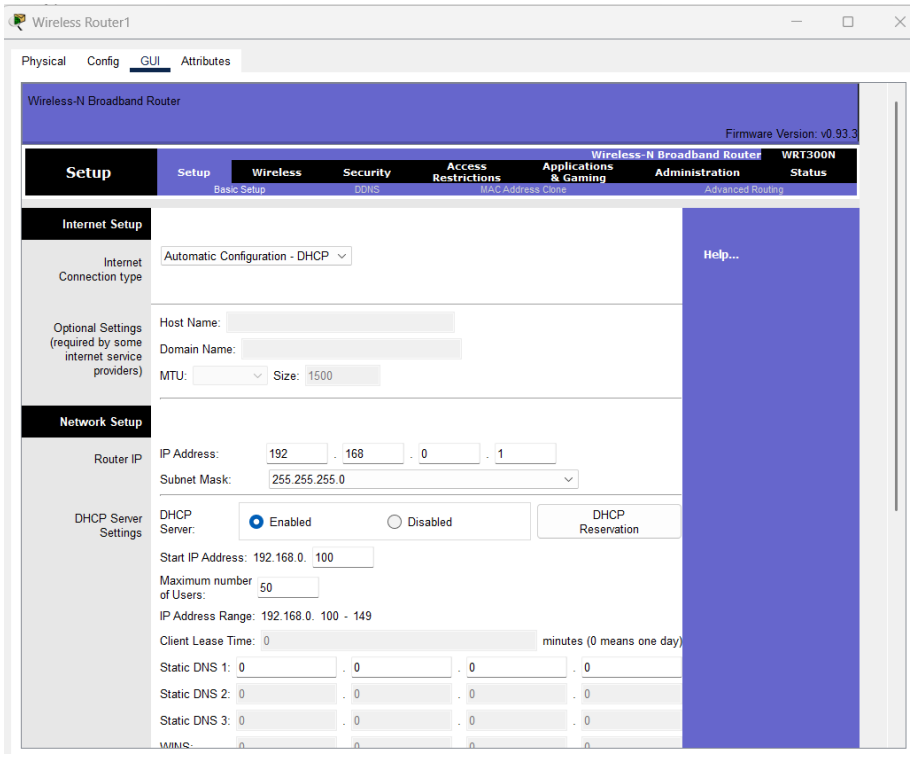
Router Subinterfaces

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0

interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0

interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0

interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 192.168.40.1 255.255.255.0

interface GigabitEthernet0/0.50
 encapsulation dot1Q 50
 ip address 192.168.50.1 255.255.255.0
```

Wireless PC Example Setup

SSID: Hall1-WiFi

Password: hall1pass
IP Address: 192.168.10.10
Gateway: 192.168.10.1



3. Scenario 2: Large Conference Management Company

Network Requirements

- Bandwidth: 300 Mbps (Fiber from ISP: 192.168.10.1/28)
- VLANs for each department and hall
- Services (DHCP, DNS, etc.) on separate subnet
- Bandwidth limits: 2 Mbps/user in halls, 50 Mbps per hall, 5 Mbps/user for departments (except IT)
- Office VLAN should not access other departments

Router Subinterfaces Example

```
interface GigabitEthernet0/0.11
 encapsulation dot1Q 11
 ip address 192.168.11.1 255.255.255.0
```

```
interface GigabitEthernet0/0.12
 encapsulation dot1Q 12
 ip address 192.168.12.1 255.255.255.0

interface GigabitEthernet0/0.13
 encapsulation dot1Q 13
 ip address 192.168.13.1 255.255.255.0

interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0

interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
```

Access Control Lists (ACLs)

```
access-list 100 deny ip 192.168.50.0 0.0.0.255 any
access-list 100 permit ip any any

interface GigabitEthernet0/0.50
 ip access-group 100 in
```

QoS Bandwidth Limiting Example (Per Hall)

```
class-map match-any HALL_TRAFFIC
 match access-group 101

policy-map HALL_POLICY
 class HALL_TRAFFIC
  police 2000000 8000 exceed-action drop

access-list 101 permit ip 192.168.11.0 0.0.0.255 any

interface GigabitEthernet0/0.11
 service-policy input HALL_POLICY
```

Network Design Functionality

This project simulates a **Large Conference Management Company** network using Cisco Packet Tracer. Each hall and department is connected through wired or wireless connections. A central core switch links all areas, and VLANs are used to isolate each department/hall in its own subnet. This improves security and performance.

Admin PC and Server

The **Admin PC** manages network configurations and monitoring. The **Server** provides DHCP, DNS, Proxy, Web Server, and Firewall services. It is manually configured with a static IP and is connected to all departments.

Wireless Access Points

Each hall is equipped with a **wireless router**. The wireless network in each hall has its own SSID and WPA2 password. Hall PCs connect wirelessly to these routers. Each router is assigned a specific IP and is configured with the correct gateway for its VLAN.

Departments and VLANs

Each department (IT, Finance, Advertising, Office, Coordinating) is assigned to a different **VLAN**. This helps to separate traffic and ensures security. Only allowed departments can communicate with each other based on access rules.

Access Control

Access is restricted between departments. For example, the Finance department can be accessed by all except the Office department. This is controlled using **Access Control Lists (ACLs)** configured on the router.

Bandwidth Management

Bandwidth for each hall is limited using QoS (Quality of Service). The halls are capped at **50 Mbps** overall and **2 Mbps per user**, while department users are limited to **5 Mbps per user**. This helps prevent any single user from consuming too much bandwidth.

Wireless Controller

A wireless controller is used to manage all wireless access points from a single interface. It ensures that security settings and SSIDs are consistently deployed across all halls.

Testing and Connectivity

Connectivity is tested using the **ping command** from each PC to the server and other PCs. Successful pings confirm correct VLAN, IP configuration, routing, and wireless connection.