Computer Communication & Networks

CEN 223

Project Report

Group Members:

- Chaudhary Muhammad Abubakar

Submitted To:

Ma'am Purva Bashir & Adil Ali Raja

Section:

4A

Design and Implementation of Bahria University Wah Campus Network Prototype (IoT Optimized)

---

1. Introduction

This project focuses on designing a comprehensive campus network for Bahria University's Wah Campus using Cisco Packet Tracer. The network connects 7 departmental buildings using a robust backbone and incorporates a centralized Smart Campus security system using IoT technology.

2. Updated Problem Statement

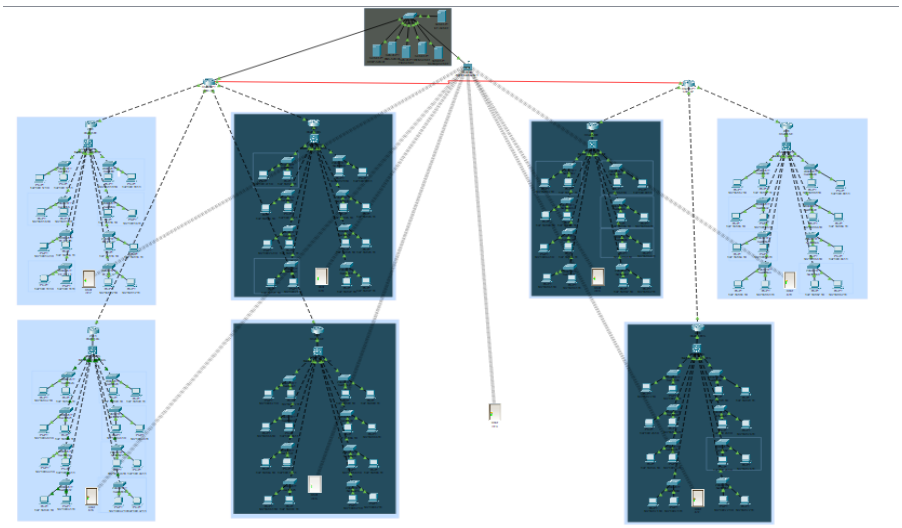
The network must support:

- 7 Buildings: EE, RIS, CS, CE, SE, ME, E&ES.
- Central Server Farm: Dedicated nodes for DHCP, DNS, Web, and a new IoT Registration Server.
- Integrated Physical Security: Centralized control of smart doors across all lab blocks.

3. Revised Network Design

3.1 Hierarchical Model

- Core Layer: Two main routers connecting the server farm to the departments.
- Distribution Layer: Multilayer switches managing departmental traffic and IoT bridging.
- Access Layer: Switches in each lab connecting 112 computers and various smart device



4. IP Addressing & Server Farm

Server/Device	IP Address	Role
DHCP Server	192.168.0.10	Automatic IP assignment for the campus
DNS Server	192.168.0.11	Domain Name resolution (e.g., www.bkr.com)
IoT Server	192.168.0.15	Dedicated Registration Server for Smart Devices
Web Server	192.168.0.20	Hosting the Campus Portal at www.bkr.com
Home Gateway	192.168.0.20 (Static)	Bridges IoT Wireless to the Server Switch

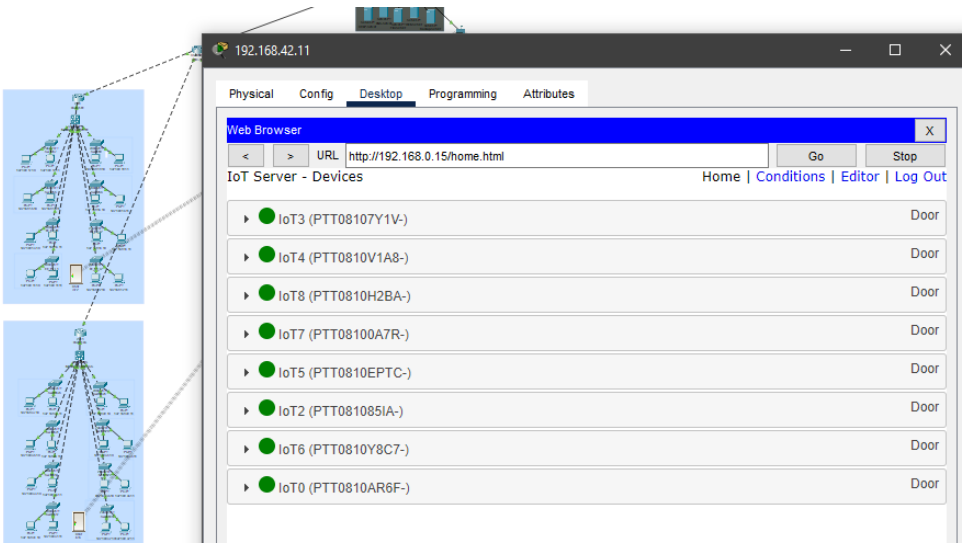
5. Advanced IoT Integration

We implemented a centralized Smart Door System to enhance campus security:

- Home Gateway: Connected directly to the Server Switch to reduce latency. It acts as a bridge for all wireless IoT traffic.
- Smart Doors: Swapped standard adapters for wireless modules (PT-IOT-NM-1W) to connect to the HomeGateway SSID.
- Registration: All doors are registered to the Remote IoT Server at 192.168.0.15.

6. Management and Monitoring

- Dashboard Access: Administrators can log into the IoT Monitor from any authorized PC using the server's IP.
- Real-time Control: Through the web interface, the "Digital Slots" of the smart doors can be toggled to lock (Red LED) or unlock (Green LED) buildings remotely.



7. Challenges Faced

- IoT Server Conflict: Initially, IoT and Web services were on one server, causing timeouts. We fixed this by deploying a dedicated IoT Server at 192.168.0.15.
- Wireless Range: Ensuring all 7 lab blocks could communicate with a single centralized Home Gateway required careful gateway placement in the topology.

8. Conclusion

The network successfully integrates standard enterprise routing (OSPF/RIP) with modern IoT automation. By separating the IoT Registration Server from the public web server, we achieved a secure, scalable "Smart Campus" prototype that provides both data connectivity and physical security management.

END OF THE REPORT