

---

# *Network Project*


---

**“UniNet Smart Campus”**

**Name : Zeyad Ashraf Mahmoud Elbanna**

**Section : 2**

# **Empowering Education through a Smart University Network:**

 In the ever-evolving landscape of higher education, the role of technology in shaping the learning environment has become more pivotal than ever. A robust university network serves as the backbone, connecting students, faculty, and resources seamlessly. As we delve into the intricacies of this network project, it is essential to understand not only the significance of a well-established university network but also the transformative power of integrating Internet of Things (IoT) technologies within this academic ecosystem.

## **What is IOT?**

- The Internet of Things (IoT) is a revolutionary paradigm that has transformed the way we interact with the digital and physical worlds. At its core, IoT refers to the network of interconnected devices, sensors, and systems that communicate easily over the internet. These devices, ranging from everyday objects to sophisticated machinery, are embedded with sensors, actuators, and software, allowing them to collect, exchange, and act upon data.
- In the IoT ecosystem, devices gather information from their surroundings, and share this data through the internet. This interconnected web enables a lot of applications and services, enhancing efficiency, convenience, and automation across various industries and daily life. From smart homes and wearable devices to industrial automation and smart cities, the applications of IoT are diverse and continually expanding.

## MQTT Protocol

- **MQTT** (Message Queuing Telemetry Transport) is a lightweight, open, and efficient messaging protocol designed for low-bandwidth, high-latency networks. It is commonly used in scenarios where a small code footprint is required, such as in Internet of Things (IoT) devices. MQTT follows a publish-subscribe model and is designed to be simple and easy to implement.
- **Publish-Subscribe Model:**
  - **Publishers:** Devices that generate data and publish messages.  
Such as Sensors and Detectors.
  - **Subscribers:** Devices that express interest in certain types of messages and receive notifications when those messages are published. Such as PC or Laptop (Client)
- **Broker:**
  - In MQTT, communication is facilitated through a central entity called the broker.
  - The broker is responsible for receiving messages from publishers and delivering them to subscribers.
- **Topics:**
  - Messages are categorized into topics, which act as channels for communication.
  - Subscribers can express interest in specific topics, and publishers send messages to specific topics.

## **Switching and Port Security: The Foundation of Network Efficiency**

- Switching is the cornerstone of modern network infrastructure, allowing devices within a Local Area Network (LAN) to communicate efficiently. Unlike traditional hubs, switches intelligently forward data only to the device that needs it, reducing network congestion and enhancing performance. Port security, a vital component of switching, adds an extra layer of protection by controlling which devices can access the network through specific switch ports. This ensures that only authorized devices are allowed, mitigating security risks, and preventing unauthorized access.

## **Dividing LAN into Virtual VLANs: Tailoring Network Segmentation**

- Virtual LANs (VLANs) enable the logical segmentation of a LAN, creating multiple broadcast domains within a single physical network. This not only enhances network security by isolating traffic but also provides flexibility in network management. VLANs allow for the grouping of devices based on function, department, or project, simplifying administration, and optimizing bandwidth utilization. By dividing the LAN into virtual segments, we create a more agile and secure network environment that aligns with the dynamic needs of our institution.

# Routing: Navigating the Pathways of Network Communication

- Routing plays a pivotal role in connecting different networks, enabling data to traverse through various pathways to reach its destination. As our network expands, the need for efficient routing becomes paramount. Routers determine the best path for data packets, considering factors like speed, reliability, and cost. Whether it's connecting different departments within the university or providing access to external resources, routing ensures that data reaches its intended destination swiftly and securely. It forms the backbone of interconnectivity, allowing our network to seamlessly integrate with the broader digital landscape.

## Routing Strategies: Static vs. Dynamic

- ✚ Routing is crucial for guiding data through our network, and the choice between static and dynamic routing impacts our network's security.
- **Dynamic Routing:** Adaptive, but Vulnerable Dynamic routing adapts to network changes dynamically, optimizing data paths. However, the constant sharing of routing information makes it more vulnerable to unauthorized access and potential manipulation.
- **Static Routing:** Predictable Security Shield In contrast, static routing involves manually configured routes, reducing the exchange of information. While less adaptive, this predictability enhances security by minimizing the attack surface and making it harder for malicious actors to exploit vulnerabilities.

# **RIP Routing Protocol: Swift and Reliable Navigation**

## **“Why I choose RIP Routing Protocol.”**

RIP, or Routing Information Protocol, is our choice for network routing, bringing several advantages to the forefront:

### **1. Simplicity:**

- RIP's straightforward implementation simplifies network management, making it an ideal choice for ease of use.

### **2. Fast Convergence:**

- Rapid convergence ensures quick adaptation to changes in the network, minimizing disruptions.

### **3. Low Resource Utilization:**


- RIP operates with minimal resource requirements, optimizing performance without straining network hardware.

### **4. Ideal for Small to Medium Networks:**

- Suited for our university network's scale, RIP's design prioritizes efficiency in smaller to medium-sized environments.


### **5. Proven Reliability:**

- With a track record of reliability, RIP contributes to a stable and consistent network experience, aligning with our network goals.

 **In embracing RIP, we secure a swift and reliable navigation framework that aligns seamlessly with the dynamics of our academic network.**

# **Conclusion: Fortifying Tomorrow's Academic Landscape**

**“Why we choose these protocols and techniques.”**

 As we draw the curtains on our exploration of network enhancements within our university, it becomes evident that the integration of port security, VLANs, static routing, and IoT is not just a technological upgrade but a strategic imperative. Together, these elements form the bedrock of a resilient, secure, and forward-looking network infrastructure.

## **1. Port Security: Locking the Gateway**

- Port security acts as the guardian of our network, ensuring that only authorized devices gain entry. By meticulously controlling access through individual switch ports, we create a robust defense against unauthorized intrusion. This not only safeguards sensitive data but also fosters a climate of trust in our digital environment.

## **2. VLANs: Tailoring Connectivity**

- The deployment of Virtual LANs (VLANs) brings a level of sophistication to our network architecture. By logically segmenting our LAN, we optimize bandwidth, enhance security, and streamline network management. This tailored connectivity aligns with the diverse and dynamic needs of our academic community, providing a scalable and adaptable infrastructure.

### **3. Static Routing: Predictable Security**

- In the realm of routing, the choice of static routing proves to be a deliberate strategy for security. The predictability of manually configured routes reduces the attack surface, offering a stable and secure pathway for data transmission. In an era where cybersecurity is paramount, static routing emerges as a stalwart protector of our network integrity.

### **4. IoT Integration: Bridging the Physical and Digital**

- The infusion of IoT into our network transcends conventional boundaries, linking the physical and digital realms of our academic environment. From smart classrooms to connected laboratories, IoT not only enhances efficiency but also opens avenues for innovative teaching methods and resource optimization. This integration positions our institution at the forefront of the digital revolution in education.

### **Looking Forward: Navigating the Digital Horizon**

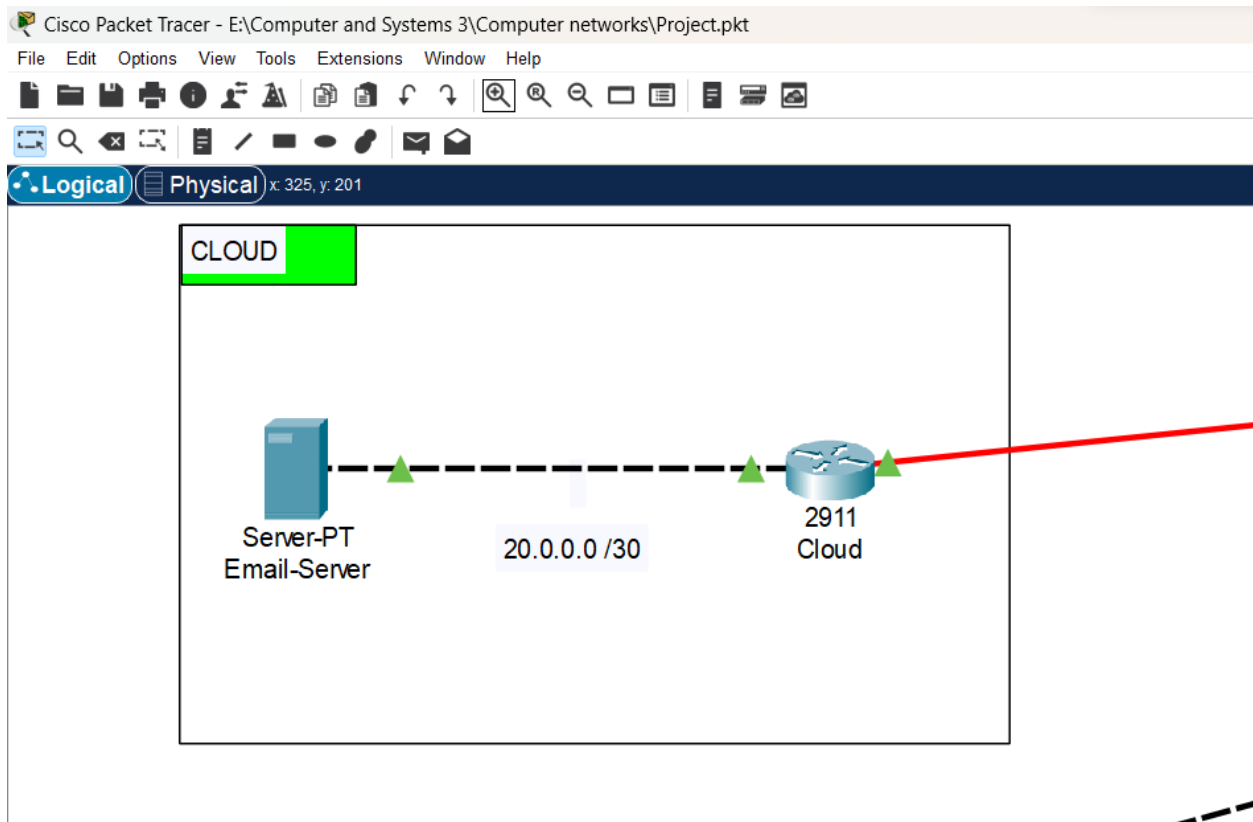
- ✚ As we embrace these enhancements, we set the stage for a technologically advanced, secure, and interconnected academic landscape. The fusion of port security, VLANs, static routing, and IoT is not merely a convergence of technologies but a strategic investment in shaping the future of education. It empowers us to navigate the digital horizon with confidence, ensuring that our network is not just a conduit for data but a catalyst for transformative learning experiences.



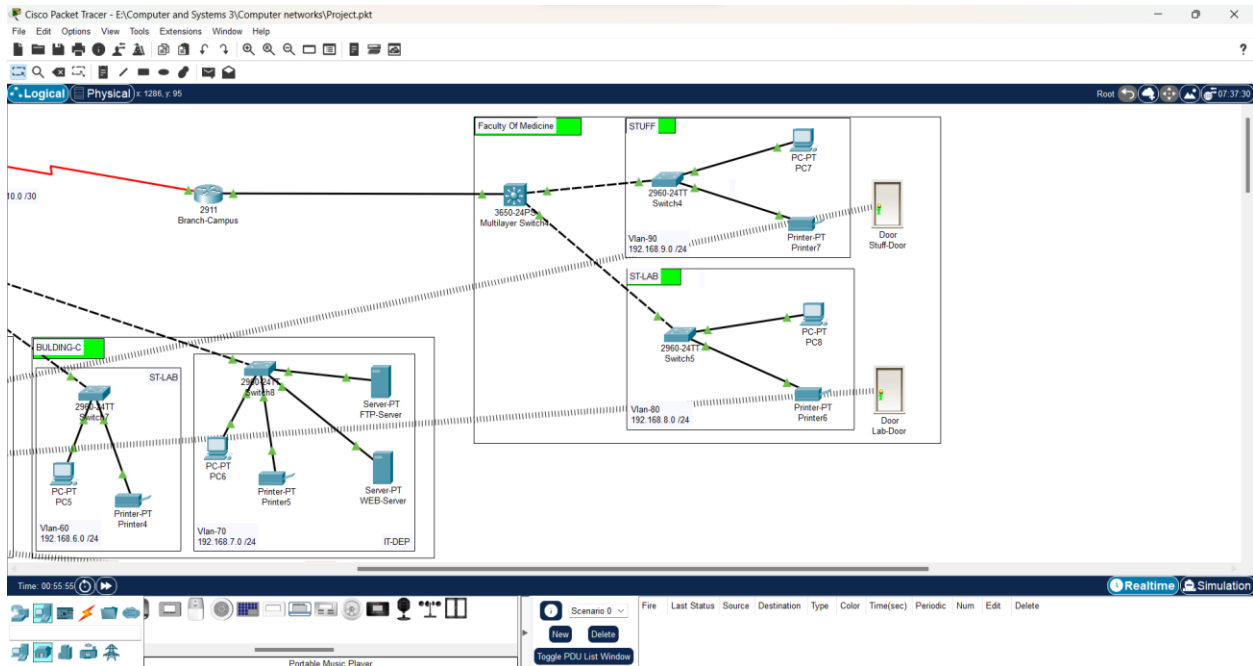
✚ In conclusion, the journey to fortify our network infrastructure reflects our commitment to providing a secure and innovative platform for the academic pursuits of tomorrow. The amalgamation of these technologies is a testament to our dedication to excellence, resilience, and adaptability in an ever-evolving digital era.

## Design and Simulation of System

Firstly, we have an external Email-server on an external network :



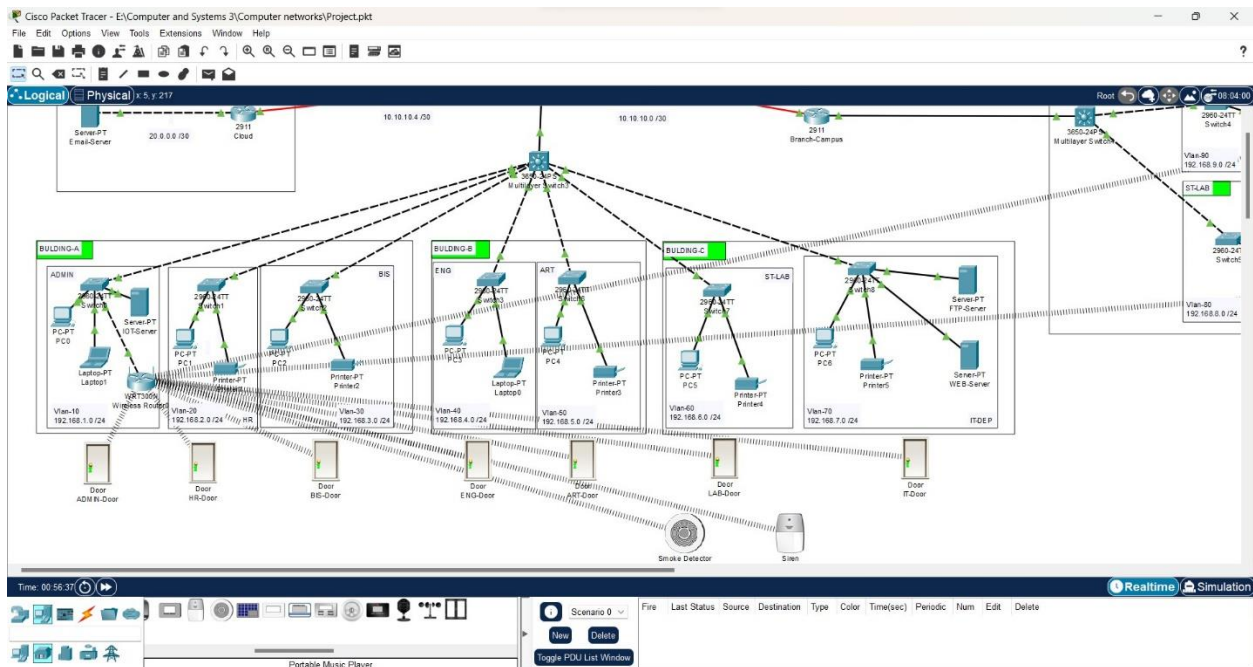
**Secondly** , we have the branch campus which have its own network and contain faculty of medicine which consists of two floors :



**Then** we have the main campus which consists of three buildings :

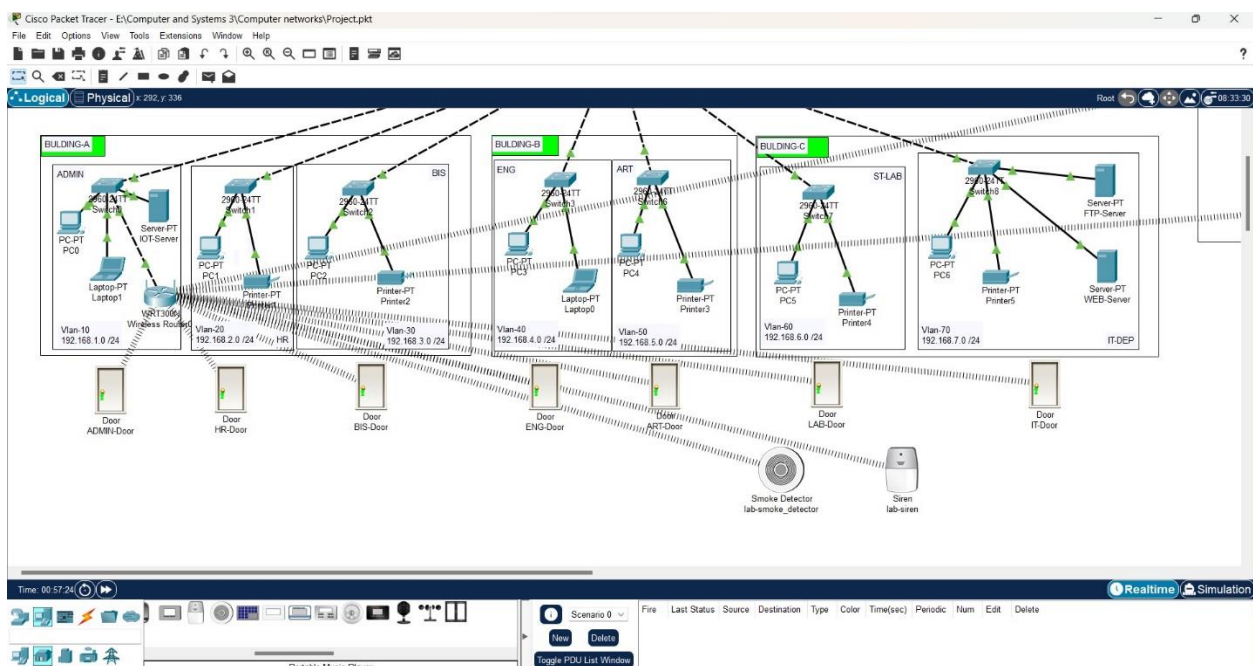
- Building-A :
  - Admin building
  - HR building
  - BIS building
- Building-B :
  - ENG building
  - ART building
- Building-B :
  - Students' labs
  - IT building

✚ Each building has its own network which is divided into several Vlans to get more security .

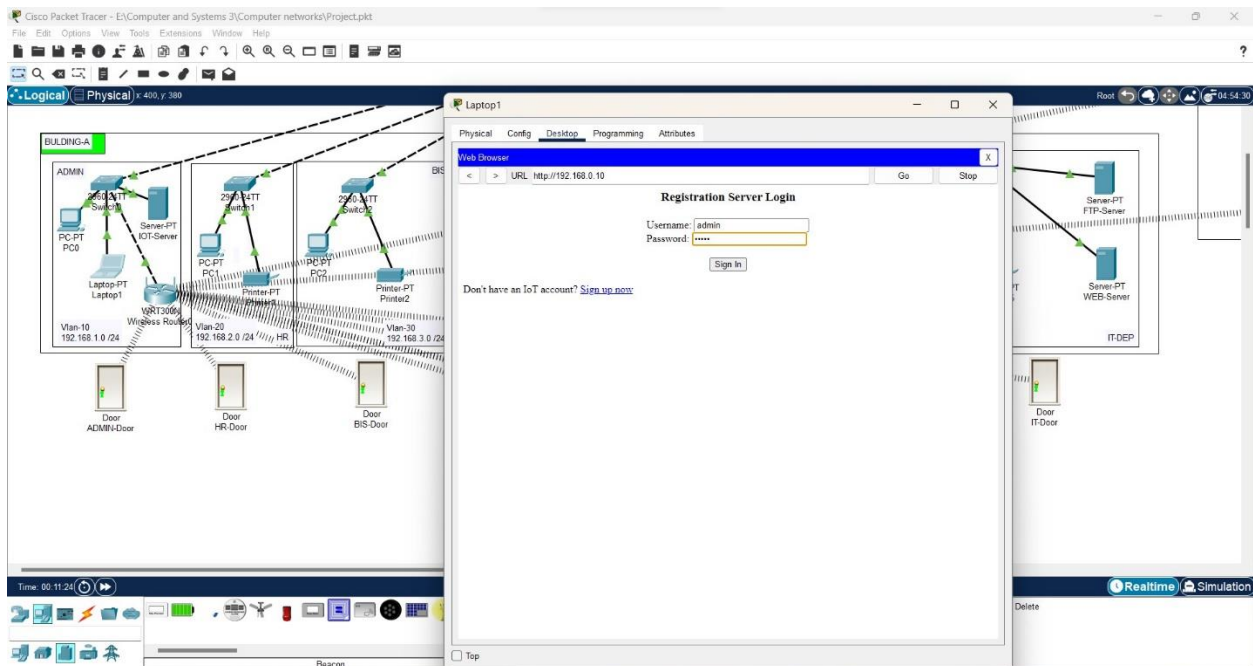


Then we have iot components :

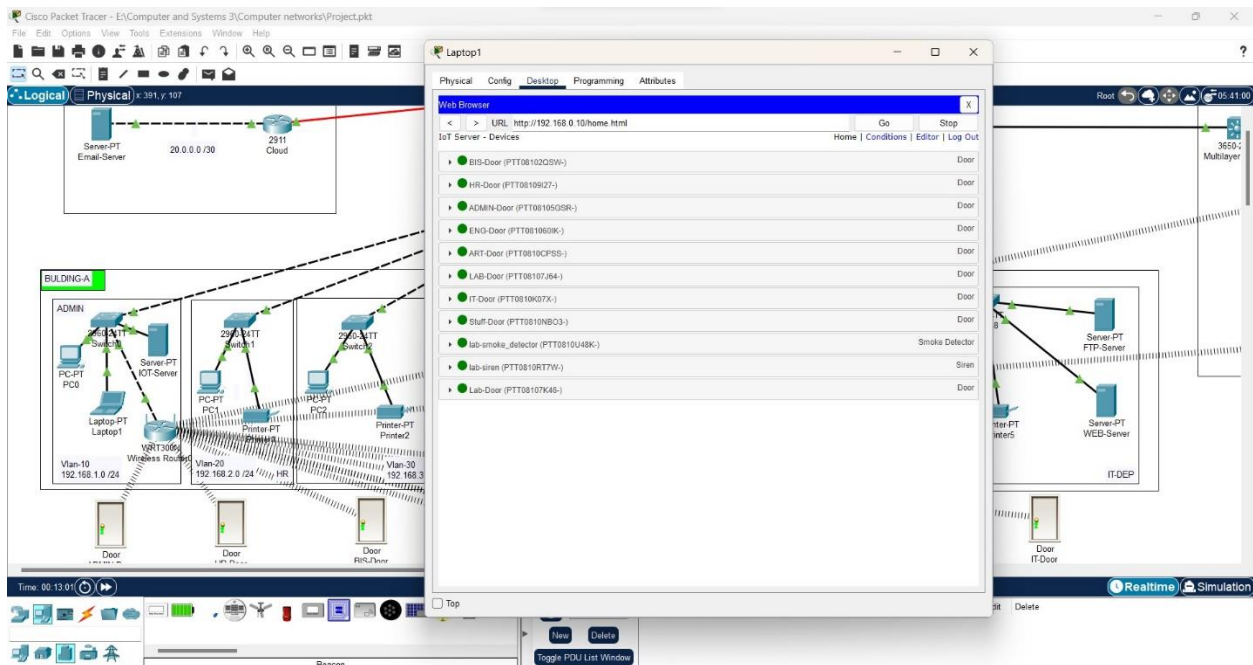
- **Smart door** : to control the closing and opening of them from admin building.
- **Smart smoke detector** : to detect any fire accident that occurs in student labs.
- **Siren** : to be aware of all people in the university if any accident occurred .



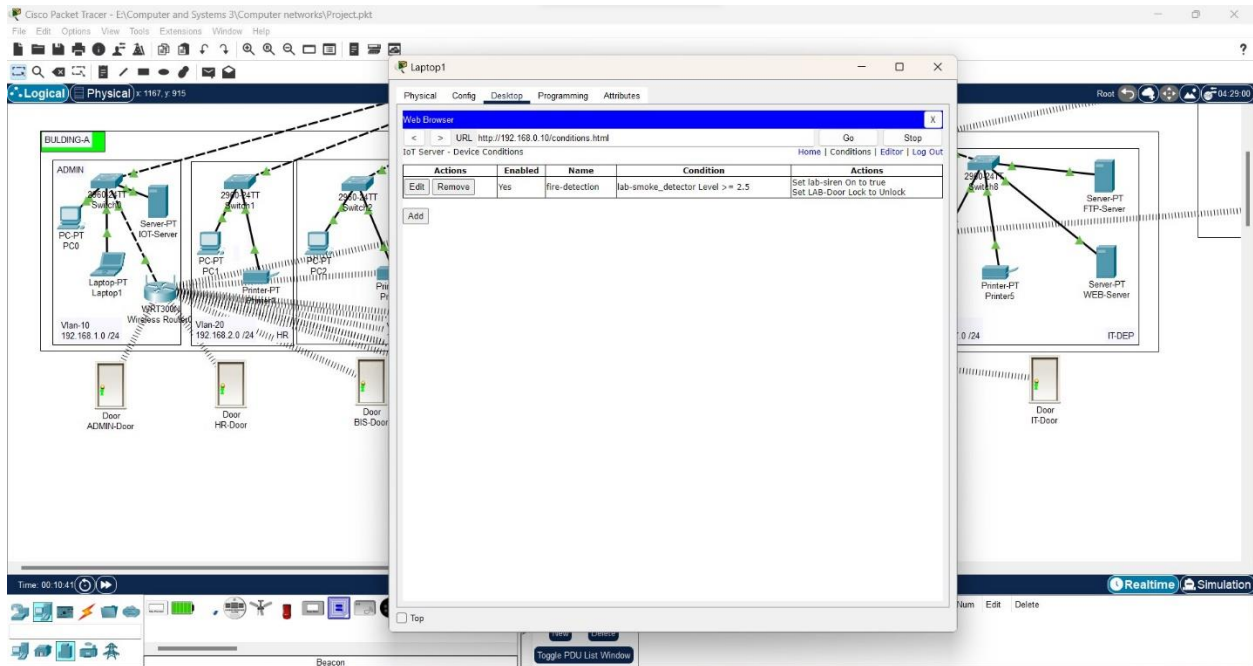
## Login to iot server :



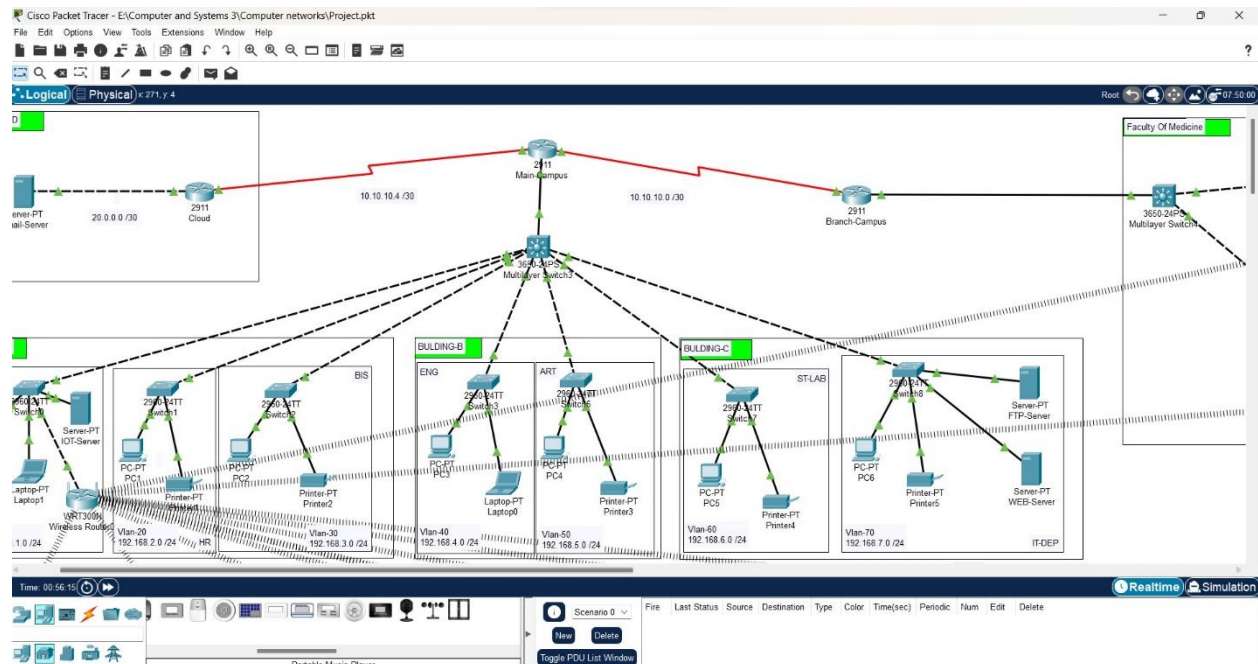
## lot components :



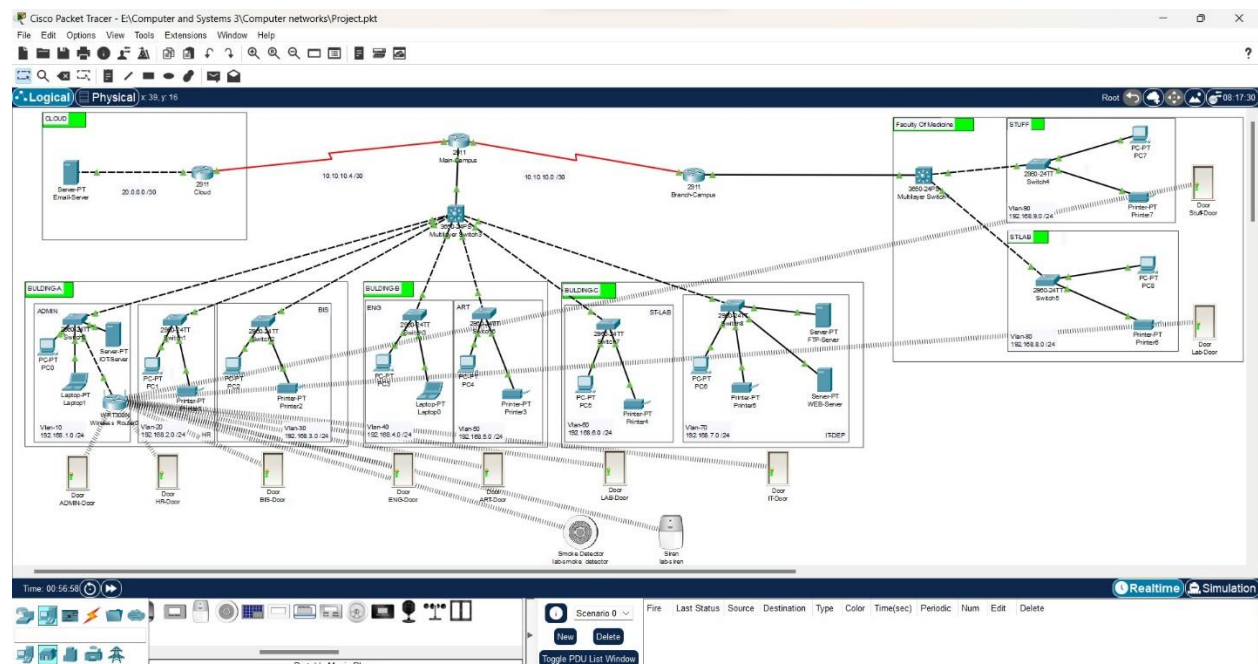
## Connection between smoke detector and serin alarm and lab door :



**Finally**, we have the main networks which connect all the buildings of the university with each other's and with the external servers on the external clouds using static routing techniques and RIP protocol :



**An overview over the whole system :**





## References :

- [What Is the Internet of Things \(IoT\)? | Oracle Egypt](#)
- [Internet of things - Wikipedia](#)
- [Constrained Application Protocol - Wikipedia](#)
- Stallings, W. (2013). **Network Security Essentials: Applications and Standards**. Pearson.
- Cisco VLAN Guide
- Cisco Port Security Guide
- Halabi, S. (2000). **Internet Routing Architectures**
- Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., & Bassi, A. (2014). **Internet of Things Strategic Research Roadmap**