Information Security Final Project  
IoT System Simulation, Security Attacks and Analyzation.

Project Report



Group Members:

Suresh Maheshwari (BAI-23S-006)

Sameer Javed (BAI-23S-007)

Bhawana Dhera (BAI-23S-049)

**Information Security Project Report**

**IoT Simulation, Analyzation and Performing a Security Attack**

**Introduction:**

The Internet of Things, or IoT, refers to the network of interconnected devices embedded with sensors, software, and other technologies, enabling them to collect and exchange data over the internet. These devices can range from simple everyday objects to sophisticated industrial tools, all equipped with the ability to communicate and interact with each other, as well as with other internet-enabled devices and systems.

**Software and technology used:**

* We have used Cisco Packet Tracer for Simulation.
* Used Packet Tracer for perform security attack.
* Discussed analyzation structurally.

**Smart Office:**

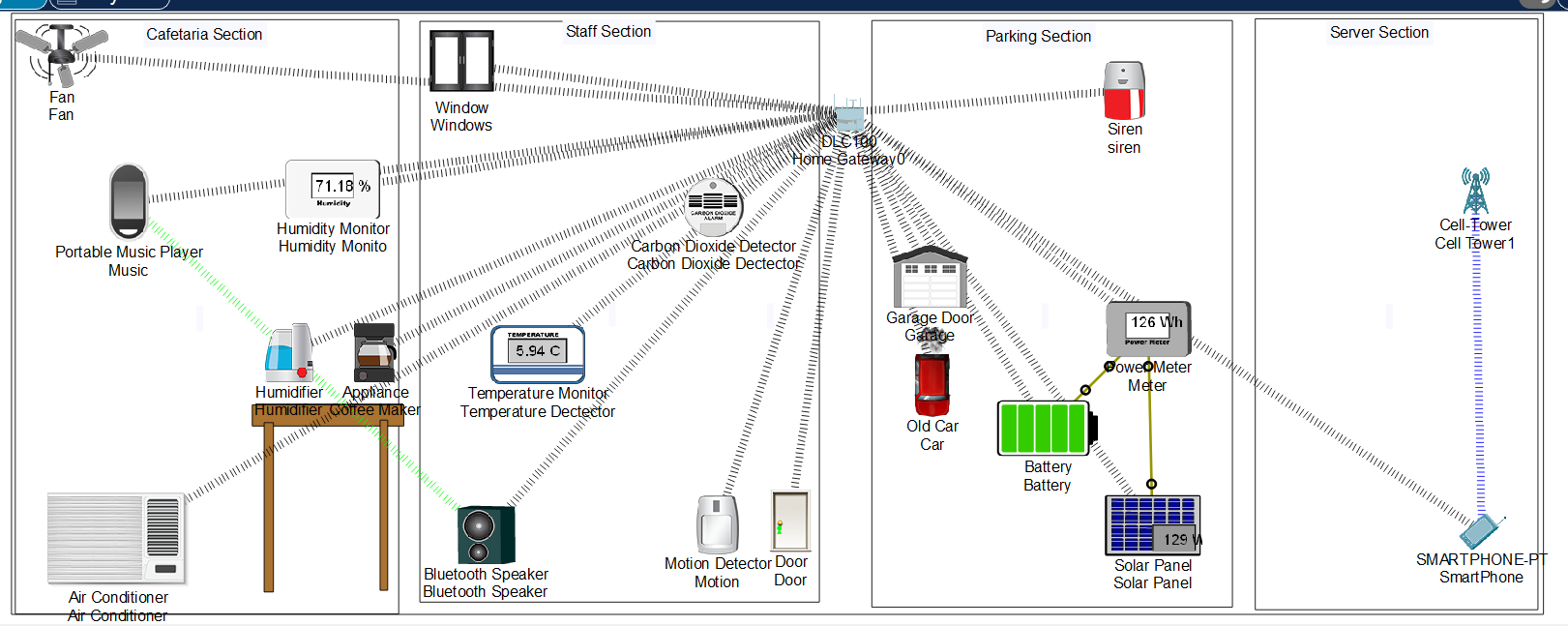
There are many things that should show how IoT is implemented on them and advance the functionality of IoT, but we have chosen Smart Office system for our project. In this simulation we are going to divide office in to 3 different section **Cafeteria** which is available in every office, **Staff Section** which is specifically for staff to do their office work we just have kept the useful device which we are going to simulate through cisco, Parking **Section** which is basically an outdoor section containing those things which are used in outdoor like solar panel, garage etc. And the last section **Server Section** which is basically the actual operational section for the Smart Office in which our all the operational is going to performed related to IoT device and which is containing all our IoT devices, and which is the backbone of our office.

**Simulation of Smart Office:**

* **Cafeteria Section:** Starting with the cafeteria section, we have added the following devices in cafeteria section in cisco packet tracer for simulation.
* **Fan:** For cooling in the cafeteria.
* **Portable Music Player:** For any announcements or any kind of motivational music etc.
* **Humidity Monitor:** For monitoring humidity around the office.
* **Humidifier:** For adding moisture to the air.
* **Coffee Maker:** Coffee maker for lunch break or tea break for employees.
* **Air Conditioner:** For extra cooling in the entire office.
* **Staff Section:** In the staff section we have added necessary items in this section and remove those items which are already being added in the cafeteria section.
* **Digital Window:** Digital Window for maintaining temperature and regulating air around the office.
* **Carbon Dioxide Detector:** Carbon dioxide for detecting the carbon dioxide level around the office.
* **Bluetooth Speaker:** Connecting portable music player with Bluetooth speaker for playing music player.
* **Motion Detector:** For detection of motion around the gate.
* **Digital Door:** Digital door attached with motion detector to look and unlock door easily.
* **Parking Section:** In the parking section we have added all the possible useful items which are used in parking section.
* **Solar Panel:** For supplying power to some components in the office.
* **Digital Garage Door:** Digital garage door for easily to be opened and close for parking cars.
* **Siren:** For alerting the staff.
* **Power Meter and Battery:** Used for solar panel.
* **Old Car:** For demonstration for digital garage door.
* **Central Device:** We have used a central device for sending data over internet and act as a backbone for IoT.
* **Home Gateway:** In Packet Tracer, a Home Gateway is the boss of your home network, handling internet access, device traffic, and security.
* **Detailed Discussion about the simulation:**

As we have discussed which components are used now, we are going to describe the complete functionality of the entire simulation. For cafeteria section, we have used the devices and tried to automate them with IoT starting with the fan we have set the to be off if the temperature drops below 10 degrees and if the solar panel which is in the parking section if it gets charged more than 50 WH. Portable music players connected with the Bluetooth speaker. The humidifier is here to manage the humidity around the office and the logic we have set for this if the humidity monitor shows the percentage below 50% then humidifier starts humidification around the office. The coffee machine is not doing any automation, it is going to operate according to usage. The air conditioner is going to operate according to temperature if temperature rises to over 12 degrees, then air conditioner will start and if the temperature drops to 5 degrees, then air conditioner will stop, and it is connected to temperature monitor. Moving forward to the staff section we have connected digital window which is basically going to operate according to temperature if temperature dropped to 8 degrees, then window is going to opened. The motion detector is going to detect motion if any motion is detected by the motion, then the door is going to looked and unlocked accordingly. Moving to the parking section we have siren which is going to function accordingly to the solar panel if the solar panel generates power to over 50 WH then siren is going to ring. Garage door is going to perform according to the car if it senses the motion of the car then door is going to opened or closed. Furthermore, we have added battery, power meter and for solar panel. Lastly, in the Server section we have added cell tower for generating cellular network for the smartphone and we have added mobile phone to be perform all the IoT functions if required. All the operations are performing through our important backbone of the system which is basically responsible for all the task is Home Gateway.

**Simulation Interface:**



**Devices and IoT implementation:**

**A screenshot of a computer

Description automatically generated**

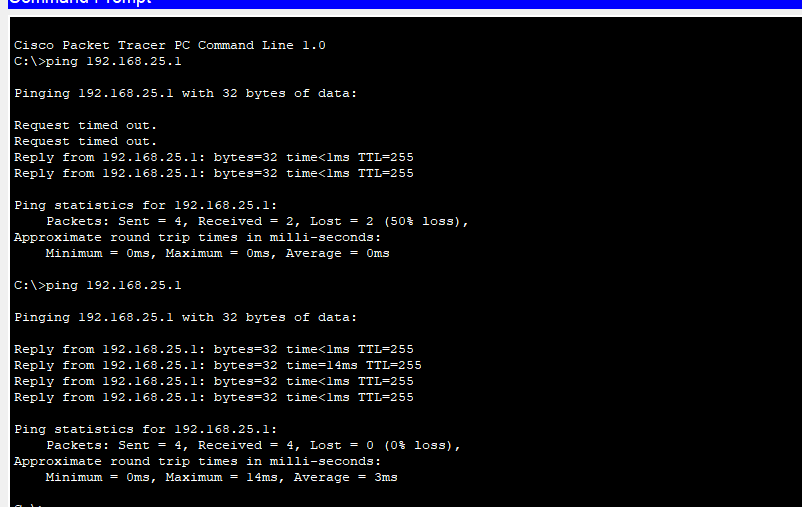
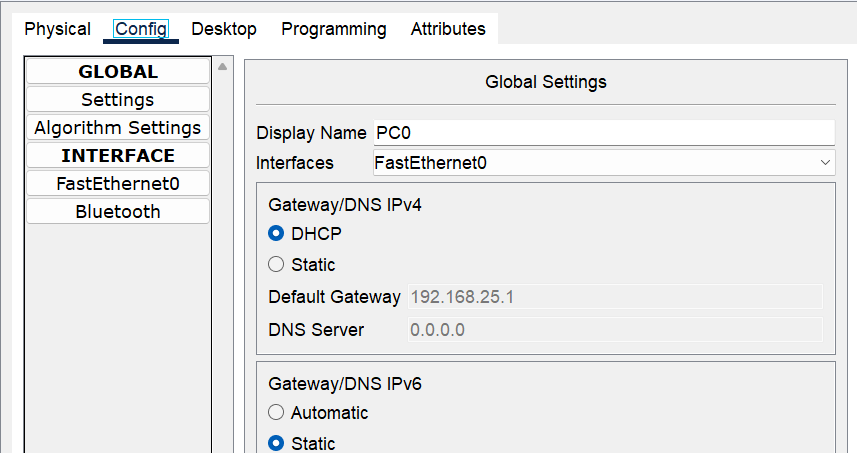
**A screenshot of a computer

Description automatically generated**

**Performing Security Attack:**

**Man-In-The-Middle (MITM):**

* **Introduction :** In [cryptography](https://en.wikipedia.org/wiki/Cryptography) and [computer security](https://en.wikipedia.org/wiki/Computer_security), a man-in-the-middle (MITM) attack, or on-path attack, is a [cyberattack](https://en.wikipedia.org/wiki/Cyberattack) where the attacker secretly relays and possibly alters the [communications](https://en.wikipedia.org/wiki/Data_communication) between two parties who believe that they are directly communicating with each other, as the attacker has inserted themselves between the two user parties.
* **Spoofing with ARP in Packet tracer:**

1. First, we added another PC to act as an attacker and connected the attacker to our network by using the IP address of our home gateway device from the DHCP of connected PC. ****
2. Then we gathered the information related to the IP address and MAC address of gateway device using ARP -a command on CMD of our PC.

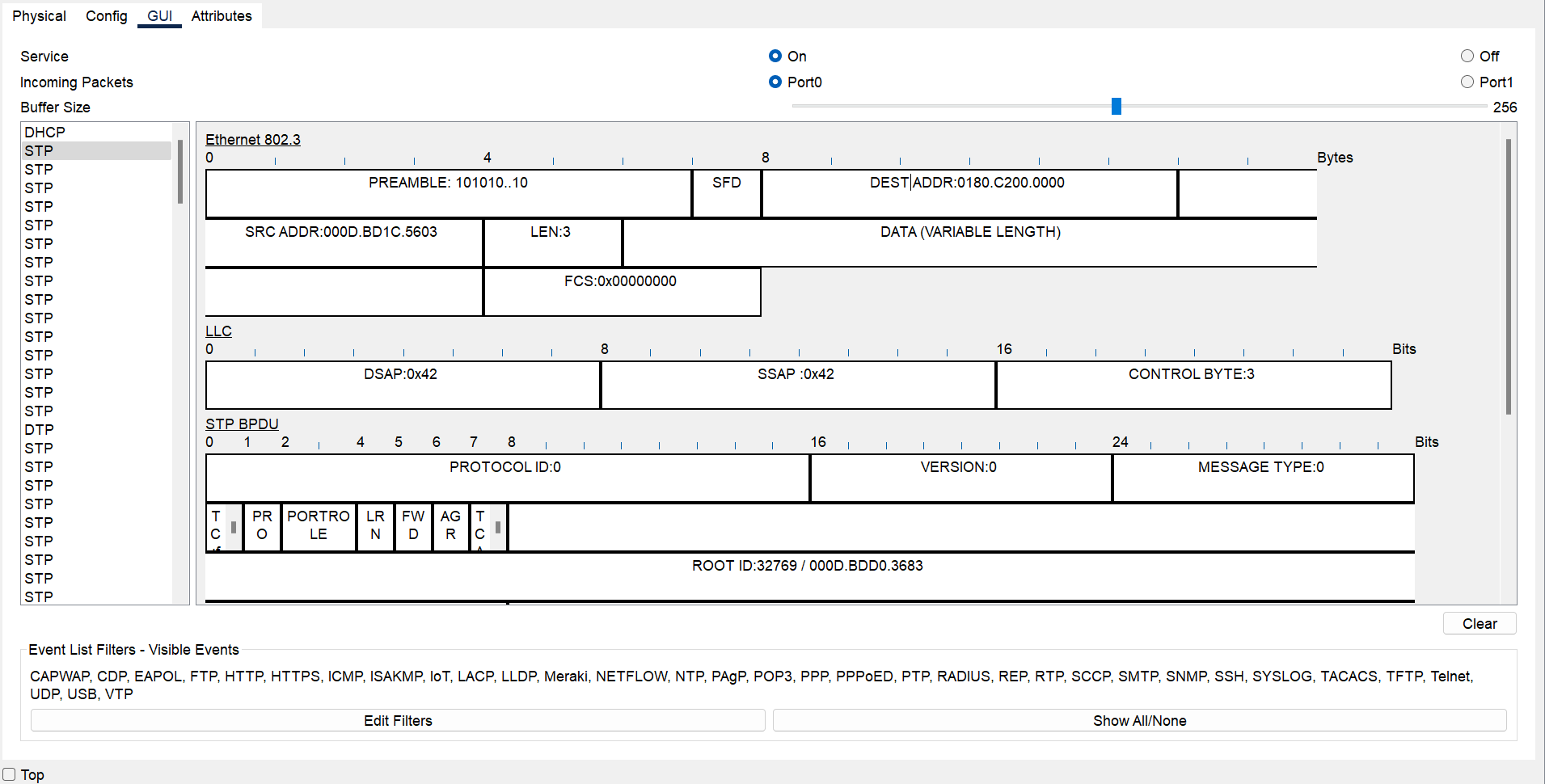
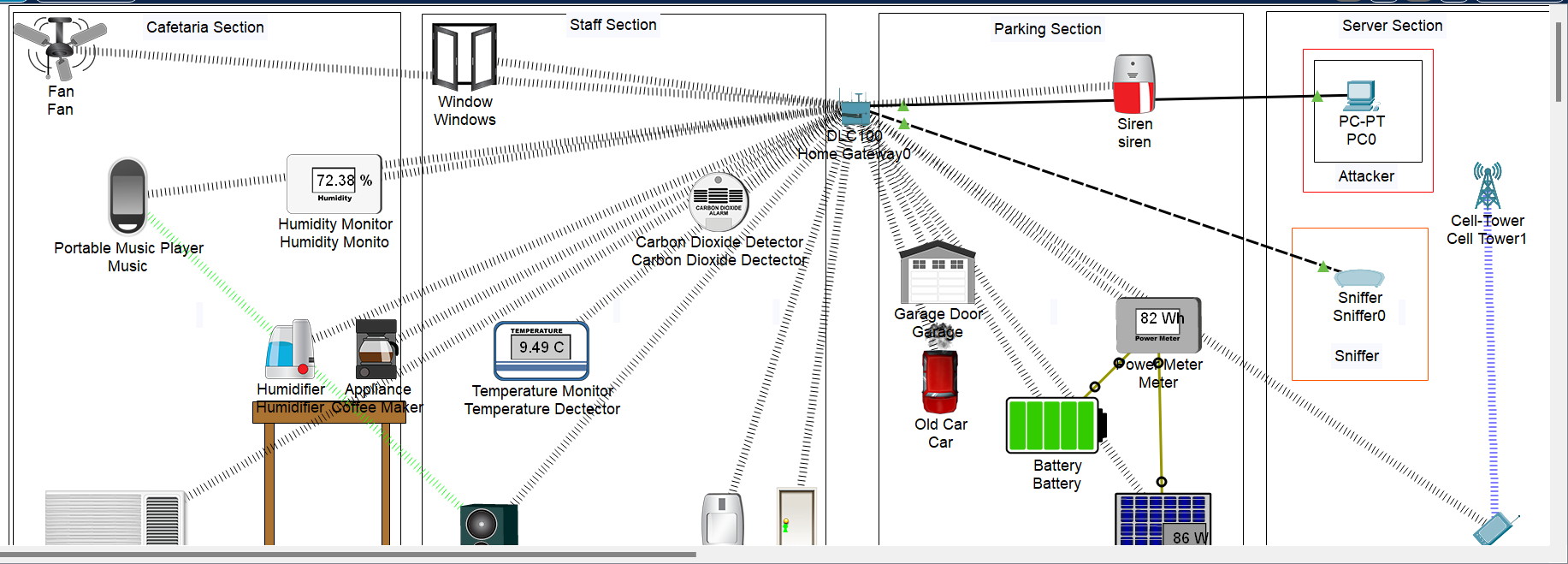
**A computer screen with white text

Description automatically generated**

1. As we have got the IP and MAC address of the gateway device now, we are going to change the routing by making the IoT devices think that attacker device is gateway it will help us to make the routing changes and to perform all the required changes related to our IoT device. We are going to use IP address of gateway but MAC address of attacker PC to think IoT devices that attacker PC is our gateway for this we have use ARP -s command.

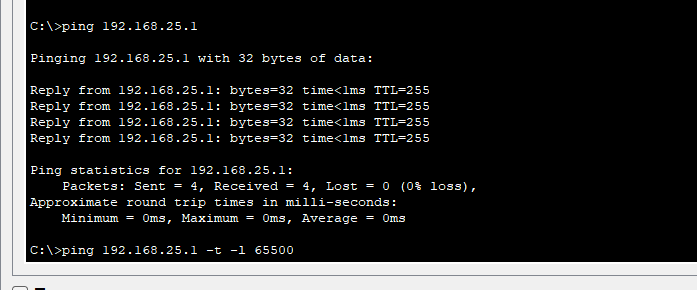
A screen shot of a computer

Description automatically generated

* **Sniffing the traffic:**
* We have added a sniffer for sniffing the traffic or data packets that are sent or received throughout the whole connection this could help us to manipulate the packets if it is required.****
* **DoS (Denial of Service) Attack:**

1. **ICMP Flood Attack:** We are going to send continue ping or ICMP request to the home gateway to keep it busy and deny the upcoming service to fulfil current service which could make the IoT network slower in response.

-t makes the ping continuous.

-l 65500 sets the size of the packet to the maximum allowed (65,500 bytes), increasing the load on the target.

1. **Monitoring the effect of DoS attack:**

We can use sniffers to monitor the packets. We can see how our packets got disturbed by sending too much traffic to our router which could result in denying the service for the users. Also by accessing the web interface of our gateway router to identify how its performance got disturbed.

**Analyzation for Preventing Security Attacks:**

To safeguard the Smart Office from security attacks, several measures can be implemented:

**Mitigating Man-In-The-Middle (MITM) Attacks**

1. **Secure Communication Protocols:**
   * Use HTTPS and other secure communication protocols to encrypt data transmissions between devices.
2. **Network Segmentation:**
   * Segment the network to isolate critical devices, reducing the impact of potential intrusions.
3. **Regular Software Updates:**
   * Ensure all devices are regularly updated with the latest security patches and firmware.
4. **Strong Authentication:**
   * Implement strong authentication mechanisms, such as two-factor authentication, for accessing IoT devices and the network.
5. **ARP Spoofing Detection:**
   * Use tools and techniques to detect and prevent ARP spoofing, such as dynamic ARP inspection.

**Preventing Denial of Service (DoS) Attacks**

1. **Rate Limiting:**
   * Implement rate limiting on the home gateway and critical devices to mitigate the effects of an ICMP flood attack.
2. **Firewall Configuration:**
   * Configure firewalls to block excessive ICMP requests and filter traffic from suspicious sources.
3. **Intrusion Detection Systems (IDS):**
   * Deploy IDS to monitor network traffic and identify unusual patterns indicative of a DoS attack.
4. **Traffic Analysis:**
   * Regularly analyze network traffic to detect and respond to potential attacks promptly.

**Conclusion**

In this IoT project, we simulated a Smart Office environment using Cisco Packet Tracer, implementing various IoT devices and examining their functionalities. By performing security attacks such as MITM and DoS, we identified vulnerabilities and explored methods to prevent such attacks. Through proper configuration, regular updates, and robust security measures, we can significantly enhance the security and efficiency of IoT systems in a smart office setup.