SMART CAMPUS DESIGN using DHCP & RFID

A PROJECT REPORT

Submitted by

PRANAY KAISTHA (RA2111030010123)

Under the Guidance of

Mrs.D.Saveetha

Assistant Professor, Department of Computational Intelligence

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE ENGINEERING

with specialization in cyber security

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TECHNOLOGY SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR – 603 203

NOVEMBER 2023

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR – 603 203

BONAFIDE CERTIFICATE

Certified that this Course Project Report titled **"SMART CAMPUS DESIGN using DHCP & RFID"** is the bonafide work done by **PRANAY KAISTHA (RA2111030010123** Certified further, that to the best of my knowledge the work reported herein does not form part of any other work.

SIGNATURE
Mrs. D.Saveetha
Assistant Professor

Department of Network and communications
SRM Institute of Science and Technology
Kattankulathur Campus, Chennai-603203.

SIGNATURE
Dr. Annapurani Panaiyappan.K
Head of The Department
Department of Network and communications
SRM Institute of Science and Technology
Kattankulathur Campus, Chennai-603203.

SIGNATURE OF INTERNAL EXAMINER

SIGNATURE OF EXTERNAL EXAMINER

Department of Computational Intelligence

SRM Institute of Science and Technology

Own Work Declaration Form

Degree/ Course **:** B.Tech in Computer Science and Engineering with a specialization in cyber security

Student Names **:** PRANAY KAISTHA

Registration Number **:RA2111030010123**

We hereby certify that this assessment compiles with the University's Rules and Regulations relating to Academic misconduct and plagiarism, as listed in the University Website, Regulations, and the Education Committee guidelines.

We confirm that all the work contained in this assessment is our own except where indicated, and that we have met the following conditions:

- Clearly references / listed all sources as appropriate
- Referenced and put in inverted commas all quoted text (from books, web, etc.)
- Given the sources of all pictures, data etc. that are not my own

- Not made any use of the report(s) or essay(s) of any other student(s) either past or present
- Acknowledged in appropriate places any help that I have received from others (e.g., fellow students, technicians, statisticians, external sources)
- Compiled with any other plagiarism criteria specified in the Course handbook / University website

I understand that any false claim for this work will be penalized in accordance with the University policies and regulations.

DECLARATION:
I'm aware of and understand the University's policy on Academic misconduct and plagiarism and I certify that this assessment is my / our own work, except where indicated by referring, and that I have followed the good academic practices noted above.

ACKNOWLEDGEMENT

We express our humble gratitude to **Dr. C. MUTHAMIZHCHELVAN**, Vice-Chancellor, SRM Institute of Science and Technology, for the facilities extended for the project work and his continued support.

We extend our sincere thanks to Dean-CET, SRM Institute of Science and Technology, **Dr. T.V. GOPAL**, for his invaluable support.

We wish to thank **Dr. REVATHI VENKATARAMAN**, Professor & Chairperson, School of Computing, SRM Institute of Science and Technology, for her support throughout the project work.

We are incredibly grateful to our Head of the Department, **Dr. R. ANNIE UTHRA,** Professor, Department of Computational Intelligence, SRM Institute of Science and Technology, for her suggestions and encouragement at all the stages of the project work.

We would also like to register our immeasurable thanks to our Faculty Advisor,

Dr. M. MAHESHWARI, Assistant Professor, Department of Computational Intelligence, SRM Institute of Science and Technology, for leading and helping us to complete our course.

Our inexpressible respect and thanks to our guide, **Mrs. R. VIDHYA**, Assistant Professor, Department of Computational Intelligence, SRM Institute of Science and

Technology, for providing us with an opportunity to pursue our project under her mentorship. She provided us with the freedom and support to explore the research topics of our interest. Her passion for solving problems and making a difference in the world has always been inspiring.

We sincerely thank the Computational Intelligence Department staff and students, SRM Institute of Science and Technology, for their help during our project. Finally, we would like to thank parents, family members, and friends for their unconditional love, constant support, and encouragement.

TABLE OF CONTENTS

ABSTRACT

This report delves into the Smart Campus Simulation Project, a pioneering initiative showcasing the potential of Computer Networking technology within a university campus environment. A key focus of the project is the Dynamic Host Configuration Protocol (DHCP), which plays a central role in streamlining network configuration and bolstering security. By automating IP address allocation, DHCP simplifies the complex task of network provisioning, replacing manual configurations with a dynamic system that ensures seamless connectivity for various computer devices.

The report highlights how DHCP optimizes resource allocation, contributing to resource conservation and cost reduction. The smart campus simulation project also aims to showcase the potential of this technology in a larger-scale setting, particularly in a university campus environment. The project involves creating a complex network and layout, which allows for deeper interactions between devices, and provides us with more options for future exercise expansion. The simulation features various devices, such as RFID access control management and an intelligent sport field watering solution, which highlights the practical applications of the technology.

The project also aims to provide us with a more comprehensive understanding of IoT technology and its potential applications. By simulating a university campus environment, the project seeks to prepare us for the future of IoT technology, where the integration of different IoT devices and networks would become increasingly common.

Overall, the smart campus simulation project aims to provide us with a practical and comprehensive understanding of Networking & IoT technology and its potential applications in a larger- scale setting. By showcasing the benefits in a university campus environment, the project aims to prepare us for the future of networking, where the integration of different IoT devices and networks will become increasingly prevalent.

OBJECTIVE

Objectives of the DHCP Protocol in the Smart Campus Simulation Project:

- **Efficient IP Allocation:** Automate IP address allocation forseamless device connectivity.
- **Network Scalability:** Easily accommodate new IoT devices as the campus network expands.
- **Enhanced Security:** Implement access control to distinguish authorized from unauthorized devices.
- **Resource Optimization:** Optimize resource usage for sustainability and cost reduction.
- **Simplified Administration:** Streamline network management for operational efficiency.
- **Preparation for IoT Integration:** Provide insights for seamless, secure IoT integration in the future.
- **Monitoring and Analysis:** Collect data for network health, issueidentification, and security incident response.
- **Documentation and Reporting:** Create comprehensive documentation for network administrators and stakeholders.

The project aims to demonstrate the potential of IoT technology in a larger-scale setting like a university campus by showcasing examples of RFID access control management and an intelligent sport field watering solution. The project also aims to create a more complex network and IoT layout, allowing for deeper interactions between IoT devices and providing us with more options for future exercise expansion. Overall, the objective is to prepare us for the future of networking technology by providing them with a practical and comprehensive understanding of its potential applications.

CHAPTER 1

INTRODUCTION

1.1 General

The Smart Campus Simulation Project represents a pioneering venture into the realm of Computer Networking, specifically within the intricate landscape of a university campus. This report offers a comprehensive insight into the project's central focus on the Dynamic Host Configuration Protocol (DHCP) and its pivotal role in establishing an efficient, secure, and scalable network infrastructure within this dynamic environment.

1.2 Purpose

DHCP emerges as a linchpin in the Smart Campus simulation, facilitating network configuration in a landscape brimming with diverse devices. By automating the allocation of IP addresses, DHCP simplifies the intricate task of provisioning a network in a large-scale campus setting, replacing manual configurations with a dynamic system that ensures seamless connectivity for a myriad of devices, ranging from smartphones to IoT sensors.

1.3 Scope

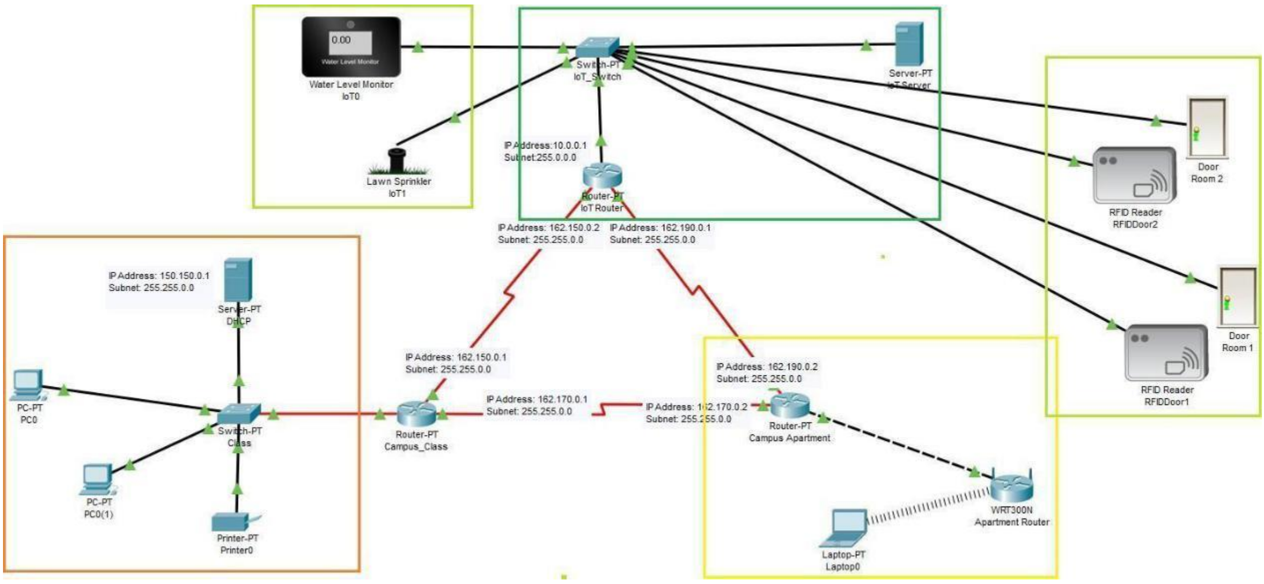
The project's primary themes include strengthening security measures and optimizing resource allocation. DHCP plays a crucial role in these aspects, with a keen emphasis on access control management, distinguishing between authorized and unauthorized devices, and thereby bolstering the overall security infrastructure of the campus network. Moreover, DHCP demonstrates its resource efficiency by adeptly allocating IP addresses in various scenarios, including the management of intelligent sport field watering systems. The project demonstrates its practical applications through examples of RFID access control management. This not only fosters resource conservation but also contributes to cost reduction, which is of paramount importance in the sustainability of the campus infrastructure.

In summary, this report delves into the multifaceted role of DHCP within the Smart Campus Simulation Project, offering a comprehensive exploration that prepares us for a future where the integration of diverse IoT devices and networks within higher education institutions becomes not only seamless but also secure and resource efficient.

CHAPTER 2

PROPOSED METHODOLOGY

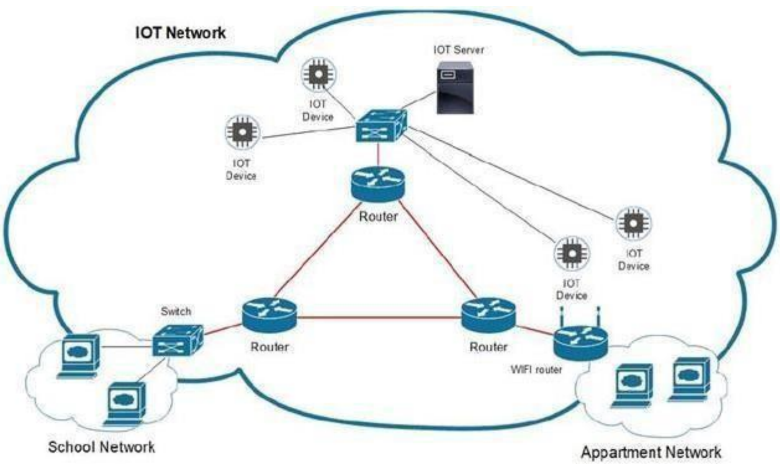
Smart Campus Topology



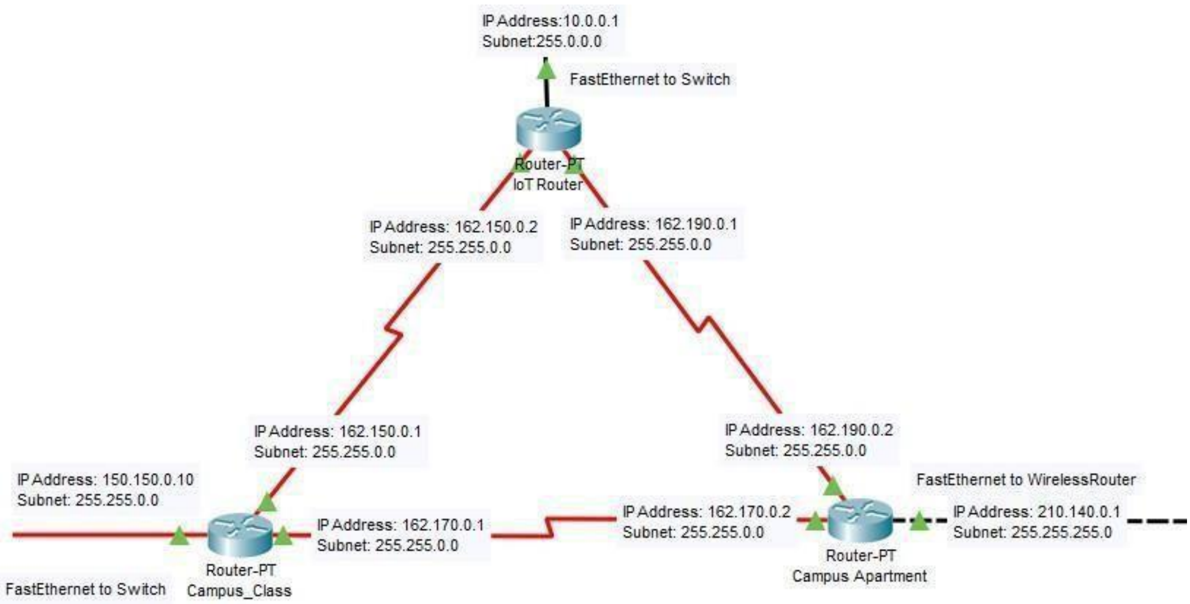
Network Layout

The network layout in this exercise is more complex compared to previous lab exercises. This network topology includes:

- Backbone router network
- Traditional switch-based classroom wired network
- Wireless LAN for the apartment buildings
- Dedicated IoT network based also on switch.



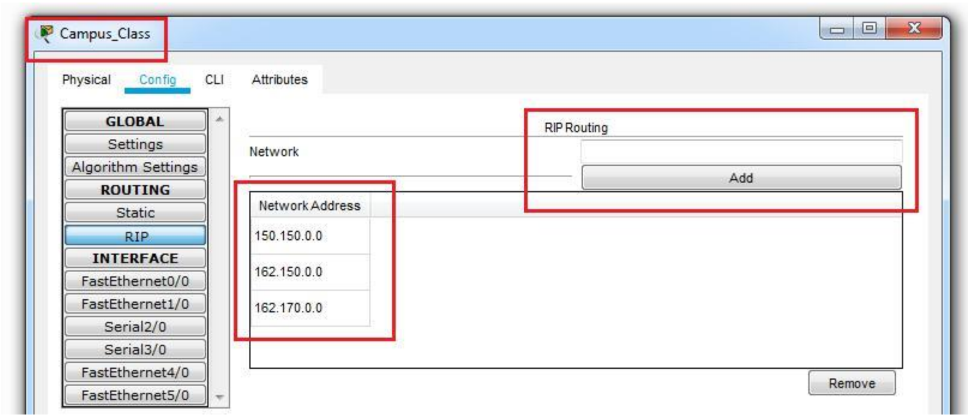
Part 1: Backbone Router Network

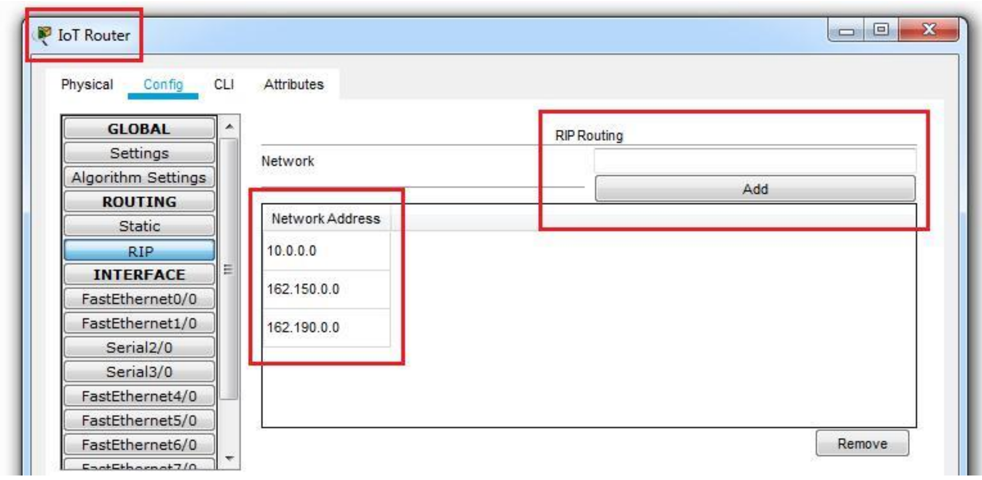


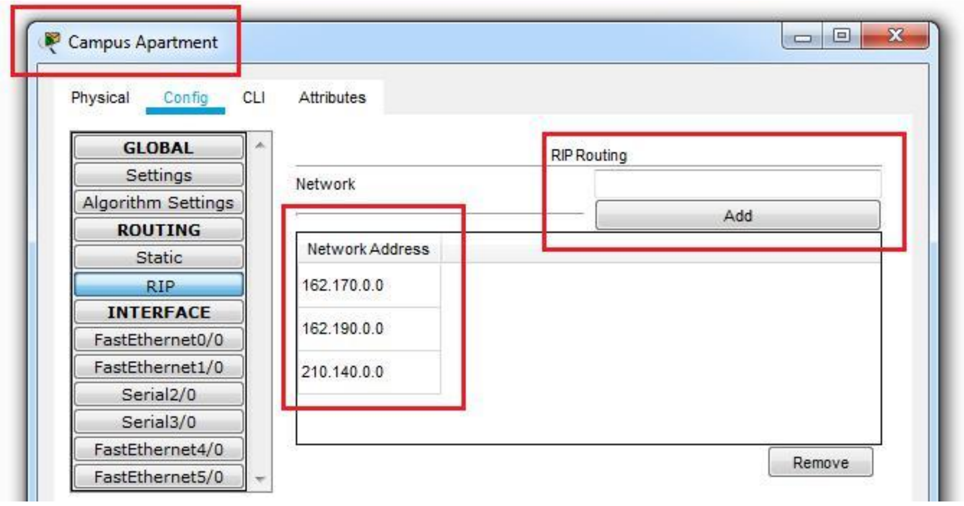
1. Set the router interface IP addresses as follows:

Router Name	Interface	IP Address	Subnet
Campus Class	FastEthernet to Switch	150.150.0.10	255.255.0.0
	Serial 2/0	162.150.0.1	255.255.0.0
	Serial 3/0	162.170.0.1	255.255.0.0
Campus Apartment	FastEthernet to Wireless Router	210.140.0.1	255.255.0.0
	Serial 2/0	162.190.0.2	255.255.0.0
	Serial 3/0	162.170.0.2	255.255.0.0
IoT Router	FastEthernet to Switch	10.0.0.1	-
	Serial 2/0	162.150.0.2	255.255.0.0
	Serial 3/0	162.190.0.1	255.255.0.0

2. Implement RIP protocol on all the three routers as shown below:



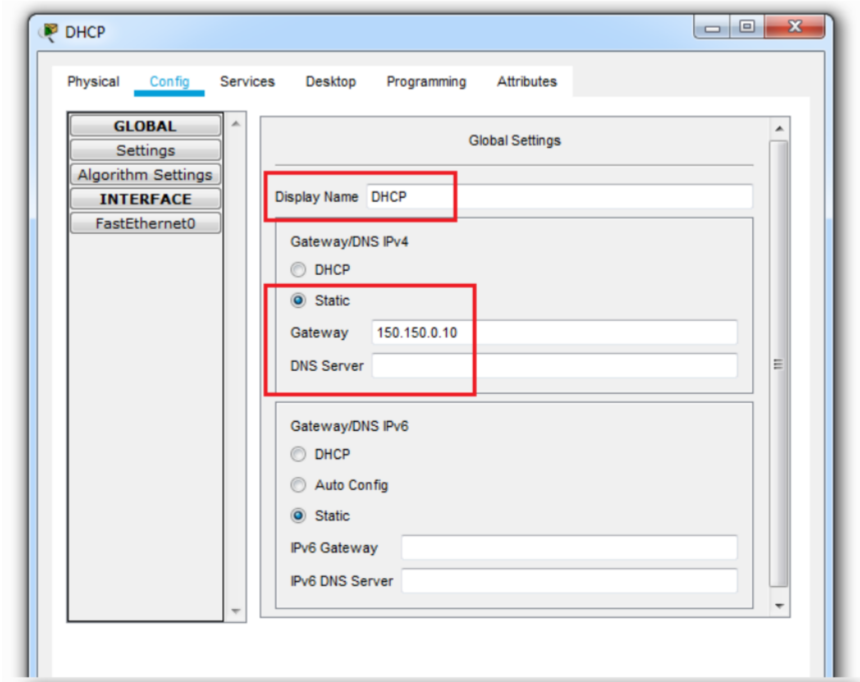

IoT Router
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
FastEthernet6/0
RIP Routing
Network
Add
Network Address
10.0.0.0
162.150.0.0
162.190.0.0
Remove

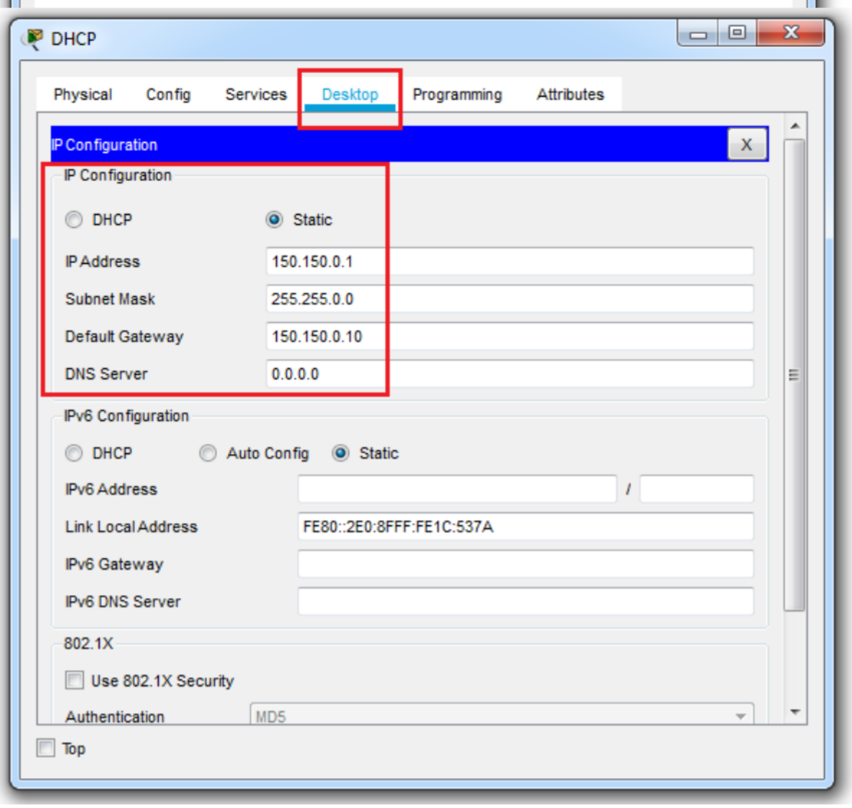

Campus Apartment
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
RIP Routing
Network
Add
Network Address
162.170.0.0
162.190.0.0
210.140.0.0
Remove

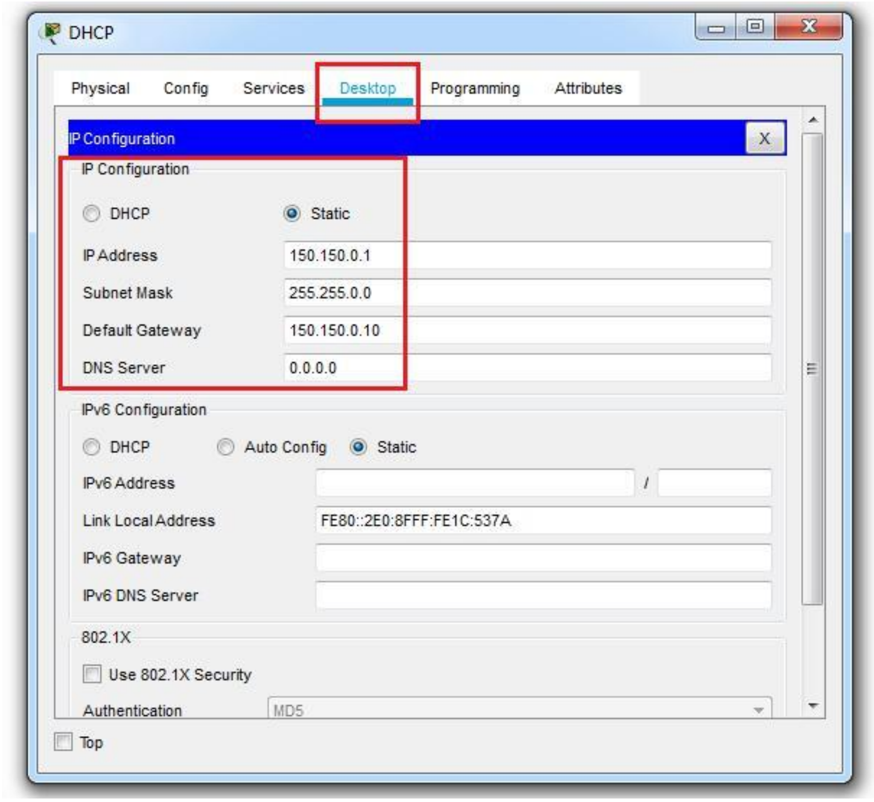
Part 2: Setting up Campus Class Network

1. Add devices as shown in the above diagram.

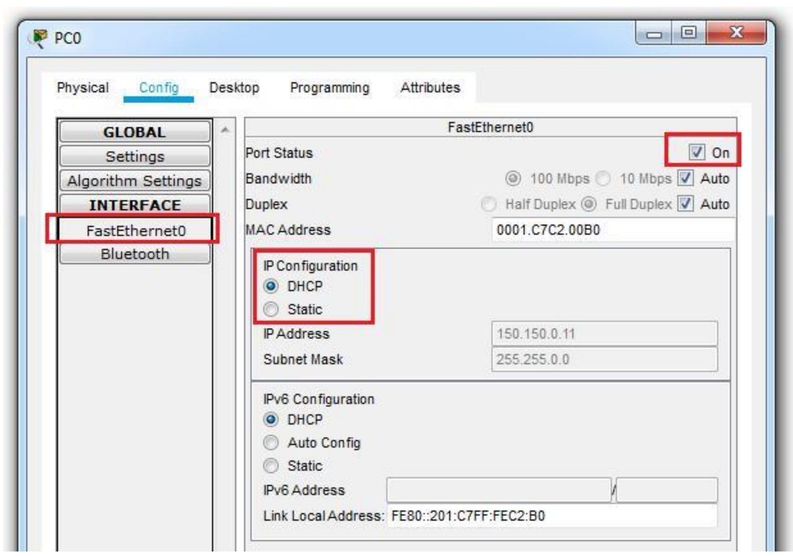
2. Setup a DHCP server. A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. Therefore, once a DHCP server is configured, there is no need to add IP Addresses to the remaining client devices.



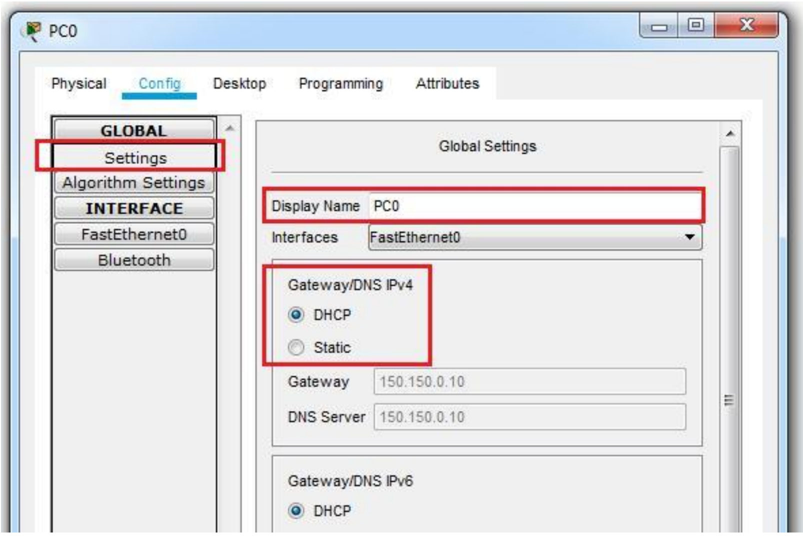




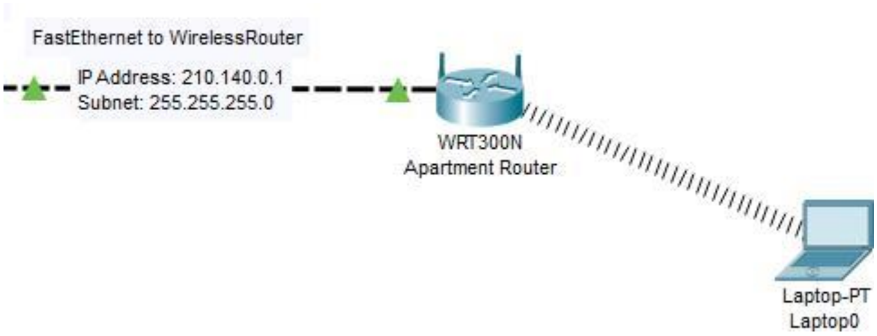
3. For all the devices, turn on the connected port and refresh the DHCP option. The port is allocated an IP address by the server.



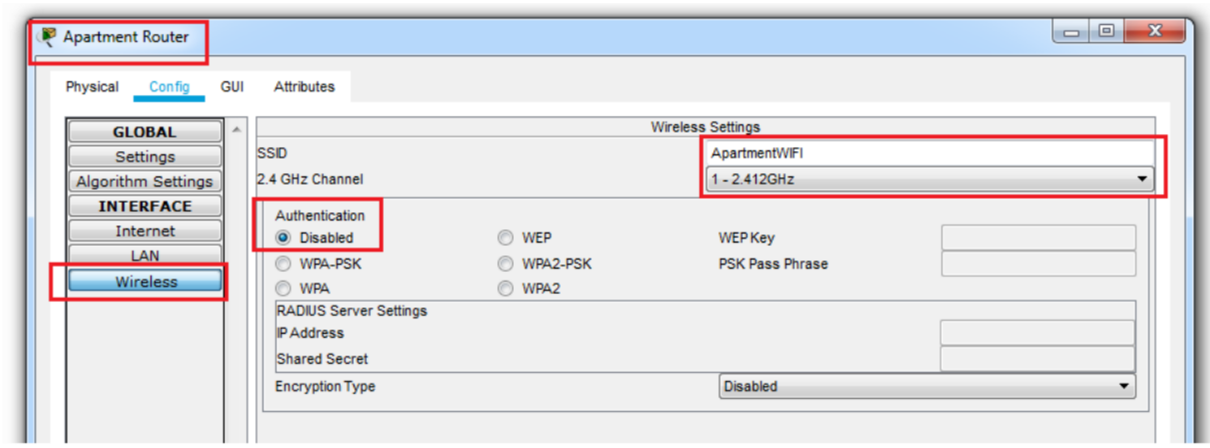
4. For all the devices, refresh the DHCP option in the settings. The Gateway and DNS IP Address configured in the DHCP server will appear.

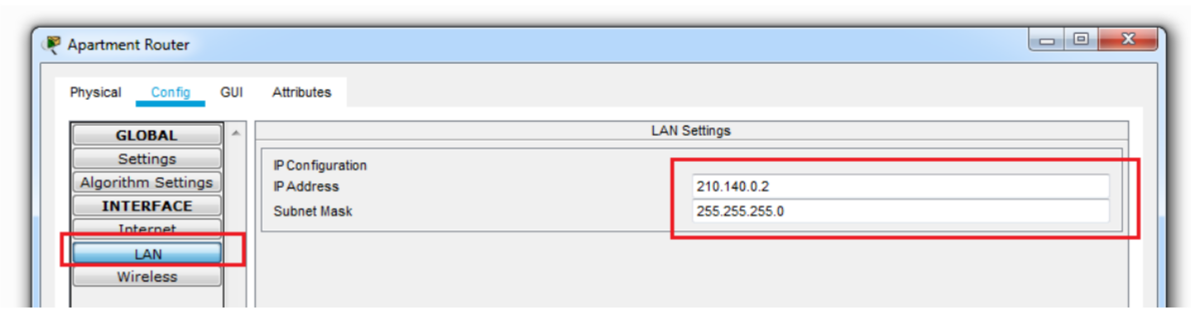


Part 3: Setting up Campus Apartment Network



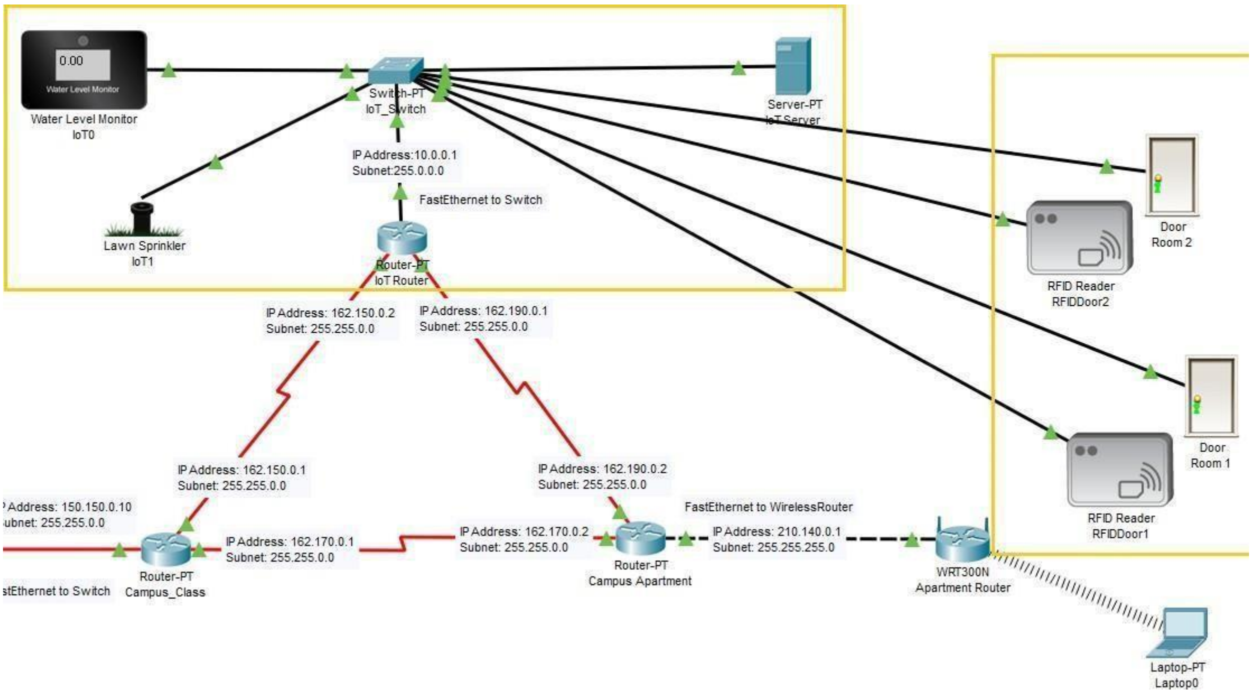
1. Setup the wireless router WRT300N as shown below. We set up a wireless network through which various devices can connect.





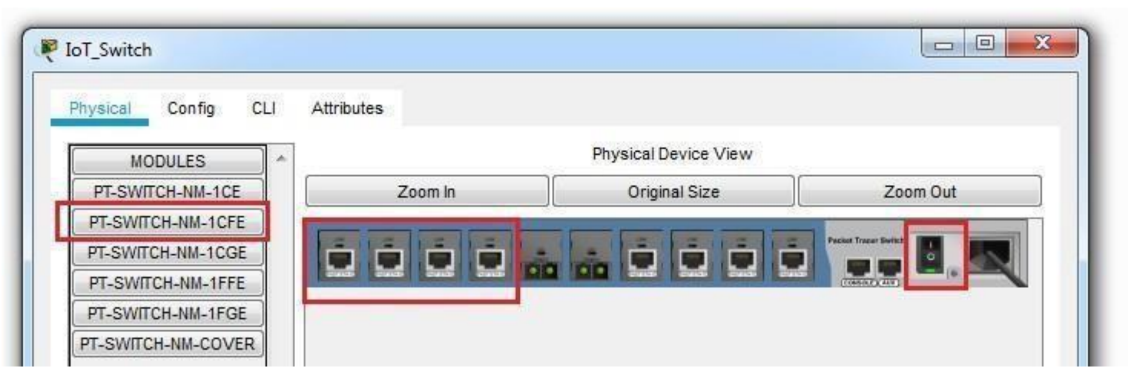
Part 4: Setting up IoT Network

Setup the wireless router WRT300N as shown below. We set up a wireless network through which various devices can connect.

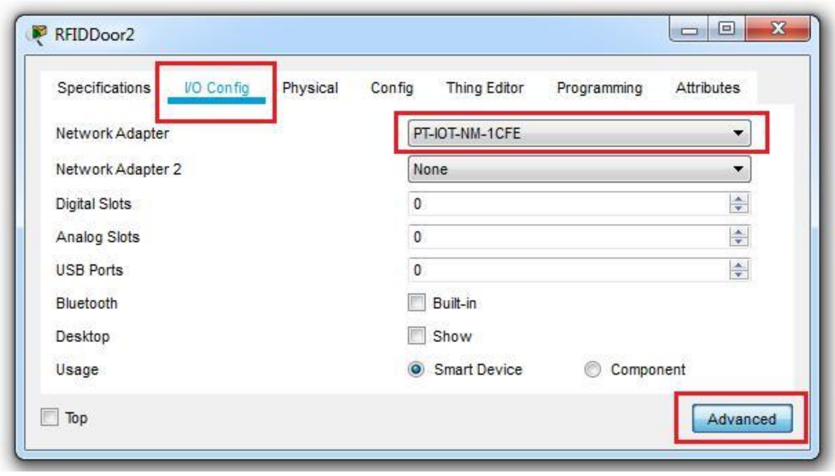


However, you will find that the switch does not have enough FastEthernet port to connect all devices. Therefore, we add the ports to the switch as follows:

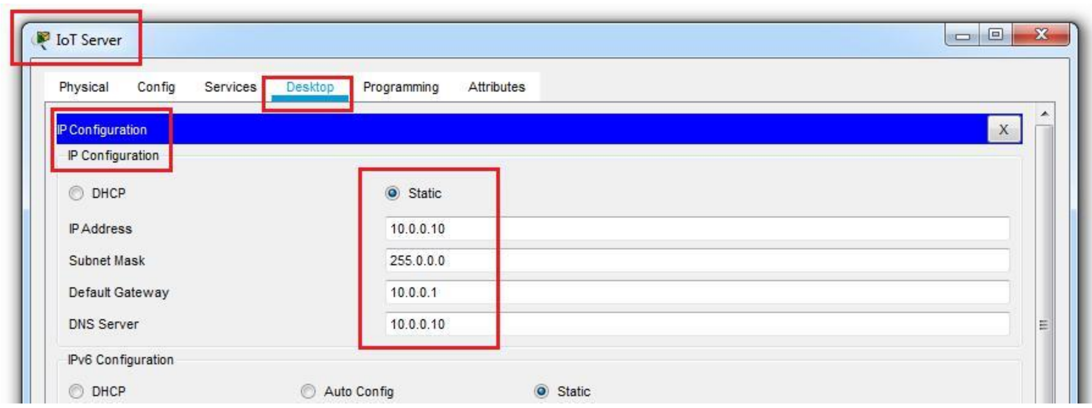
1. Shut down the switch. Drag the PT-SWITCH-NM-1CFE to the empty slots on the right side of diagram.



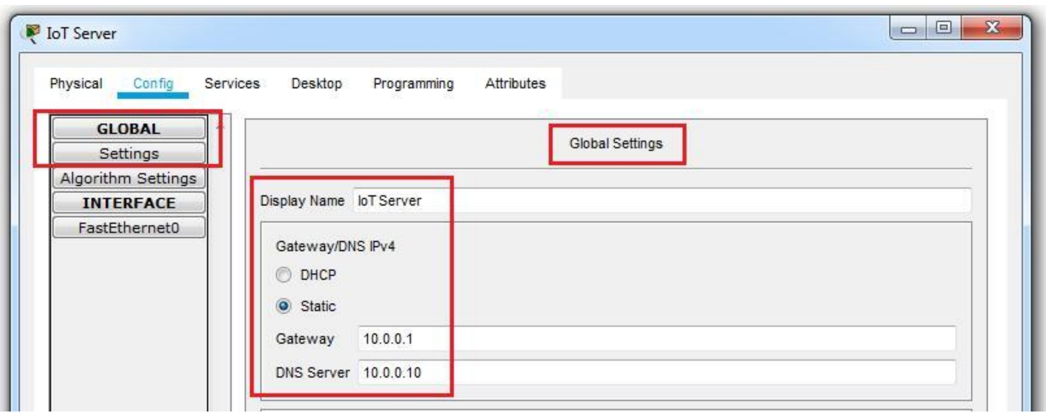
2. Make sure the IoT devices have FastEthernet ports. If not use the Advanced button on every IoT device. That will provide an I/O Config option, where you can change the port connectivity type.



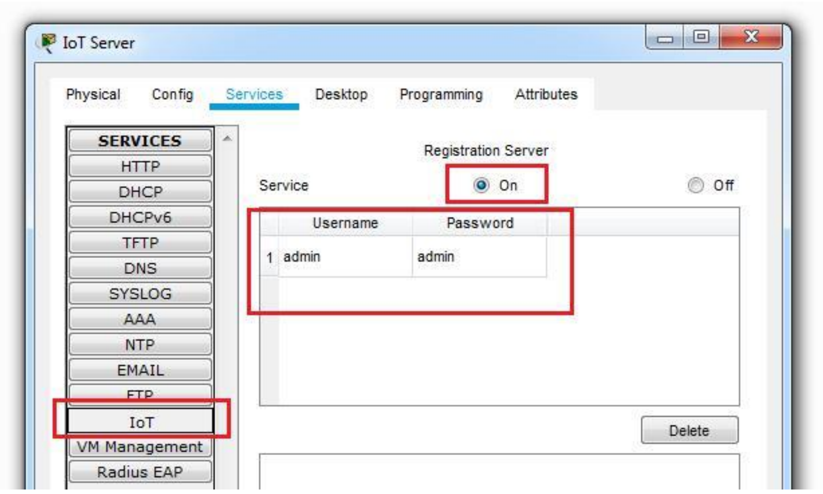
3. After adding all the devices and auto cabling them, we start with configuring the devices.
4. First, we configure the IoT Server. Add IP Address to the IoT Server as shown below.



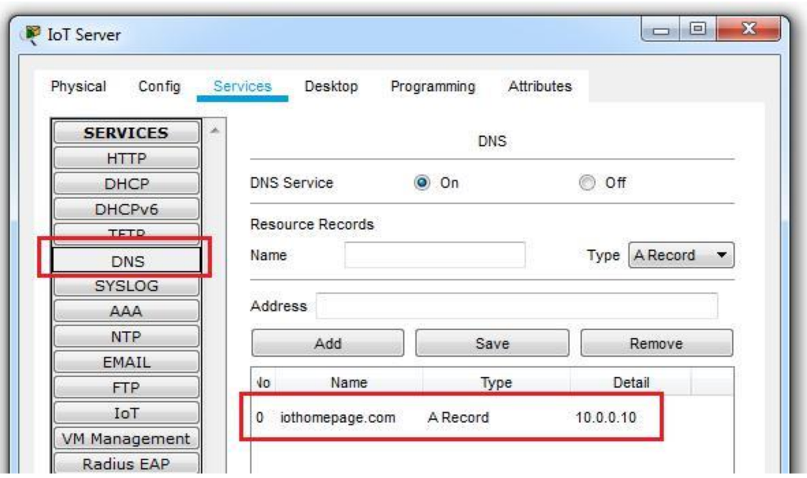
5. In Global Settings, configure the Name, Gateway IP and the DNS IP.



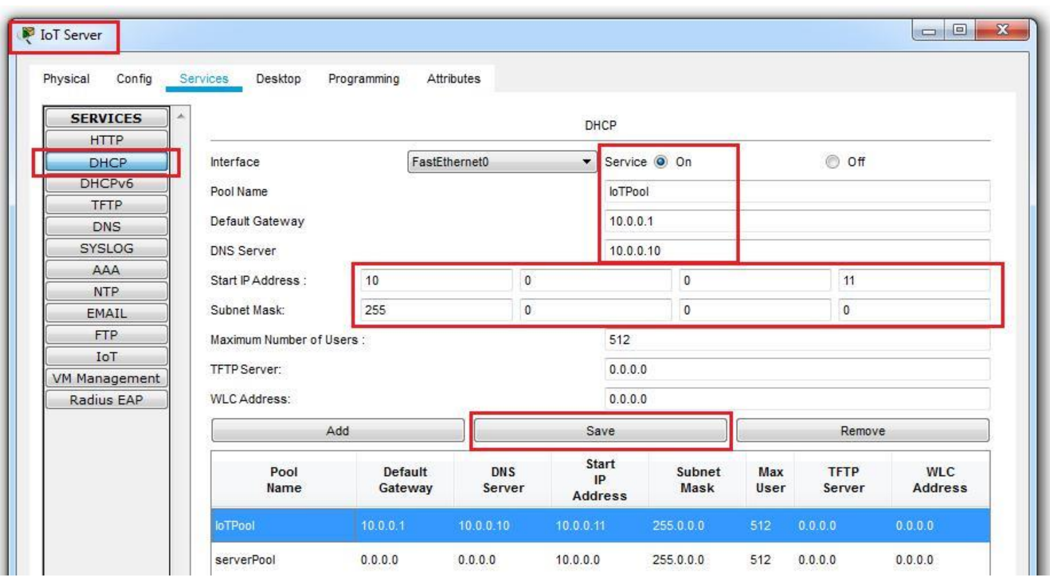
6. Add IoT Registration services as performed in previous labs.



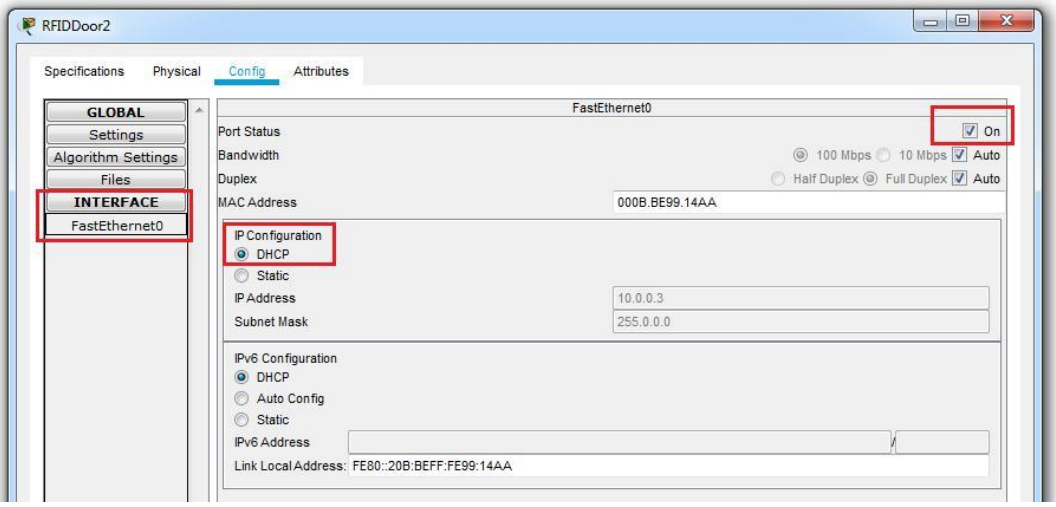
7. Add DNS services on the IoT Server.

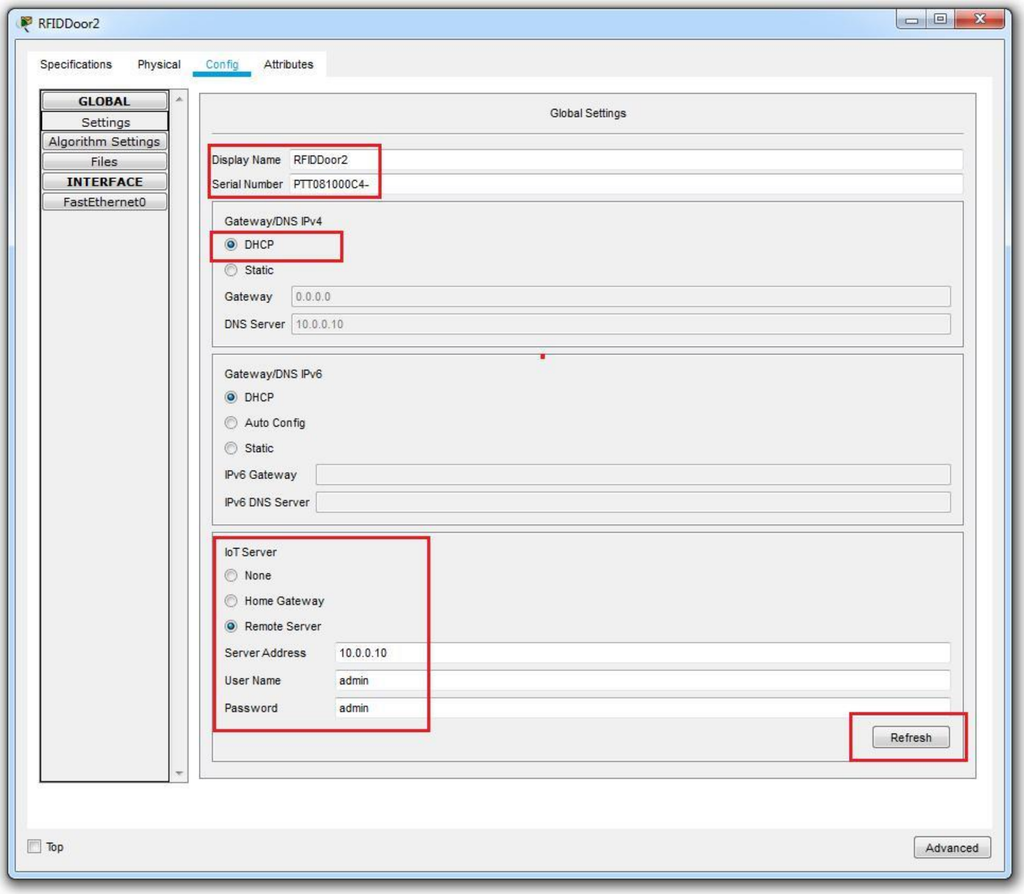


8. Add DHCP service on the IoT Server so it can assign IP addresses to IoT devices.

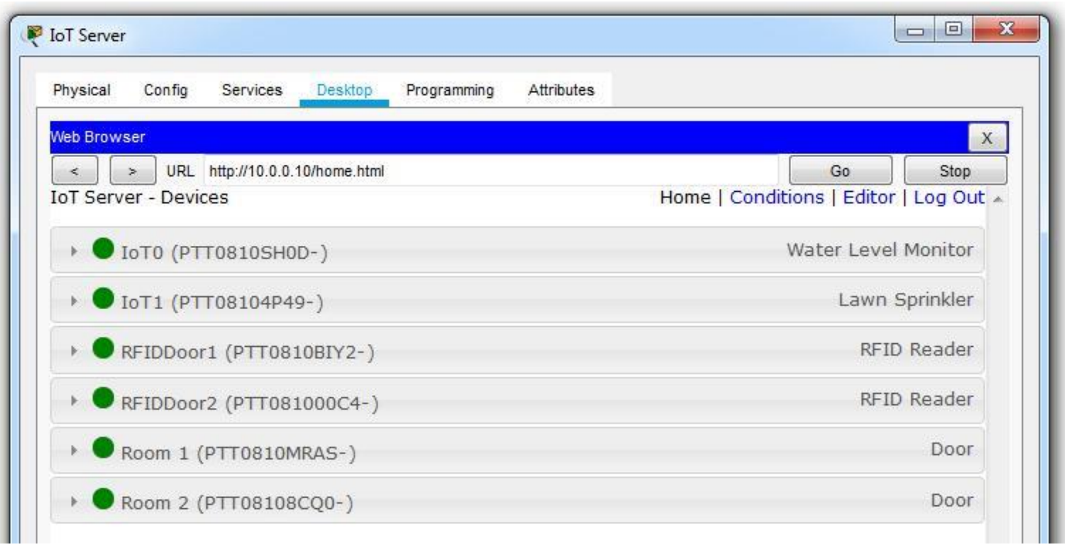


9. Add DHCP service on the IoT Server so it can assign IP addresses to IoT devices.





10. When all the devices are properly connected, the devices will show up in the IoT Registration Service. The Registration service can be accessible using the Web Browser and IP address 10.0.0.10

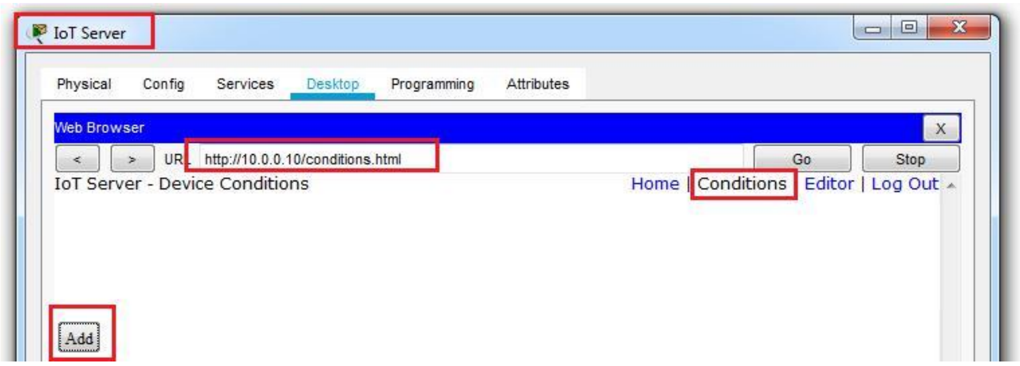


Part 5: Adding IoT Device Conditions

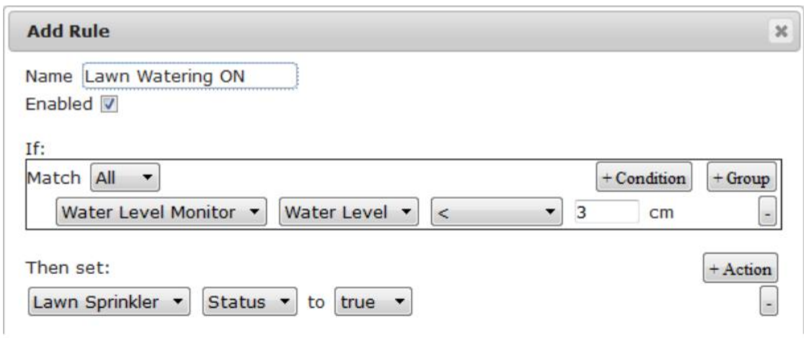
There are 2 ways to add IoT Conditions.

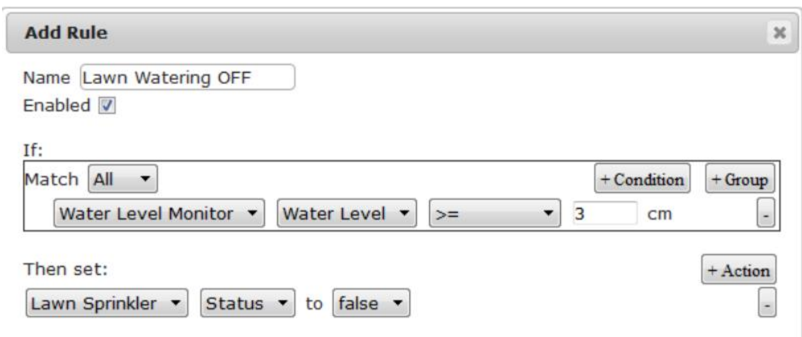
- Add a micro-controller, connect the devices, and program the conditions.
- Add the conditions in the IoT Registration Server.

We will use the second approach as we do not need to change the topology.



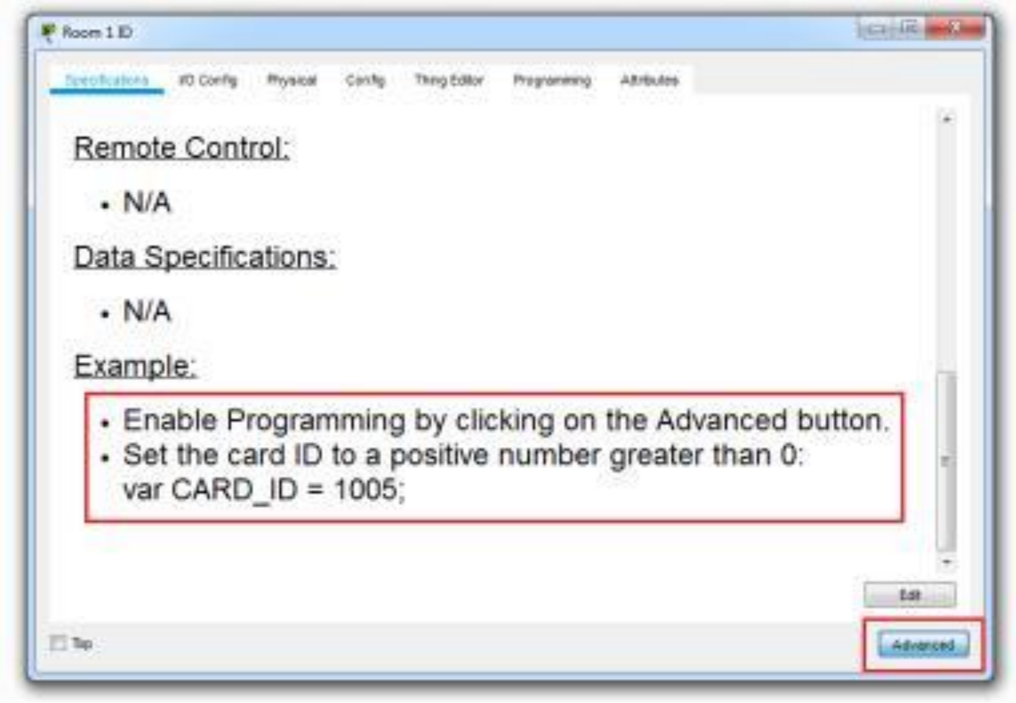
1. Add conditions for Lawn Sprinkler ON and OFF.





2. We now add RFID cards for the Apartment Doors

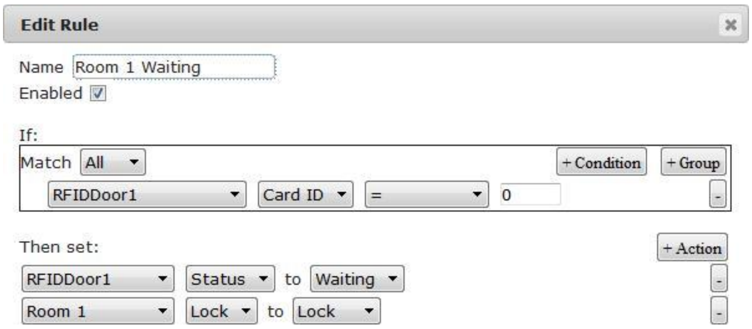
3. Configure the above RFID cards as follows:



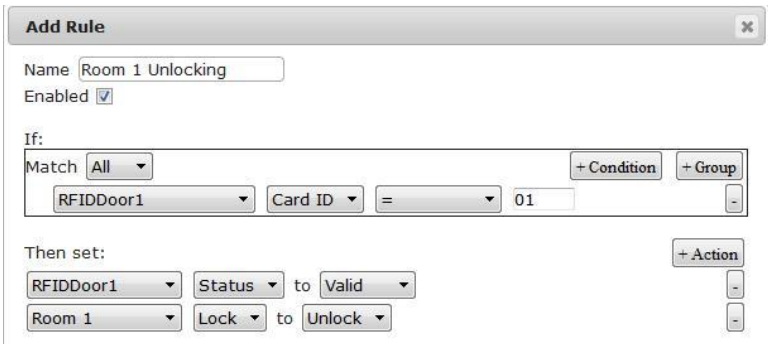
4. Select the Programming option and double click on RFID Card (Python)

5. Double click on the main.py. And change the value of Card_ID to 01. Click Run. Similarly add 02 and 03 to RFID Card 2 and 3 respectively.

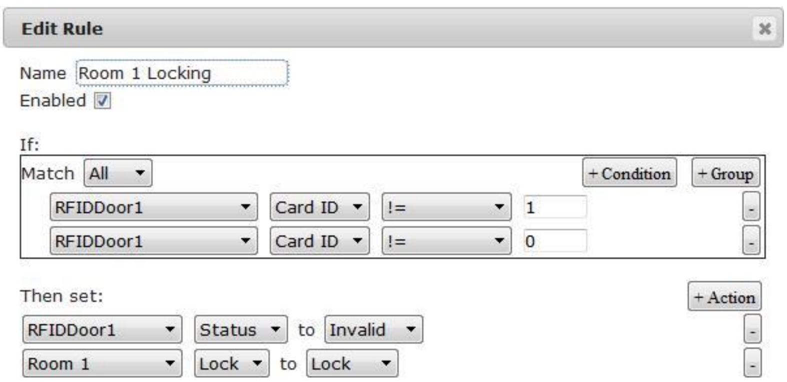
6. We now configure the RFID Reader. Add the following conditions in the Condition section in the IoT Registration Service website. Perform the following for all the RFID readers:
   - We first set all the RFID into a waiting mode and set room doors to lock status.



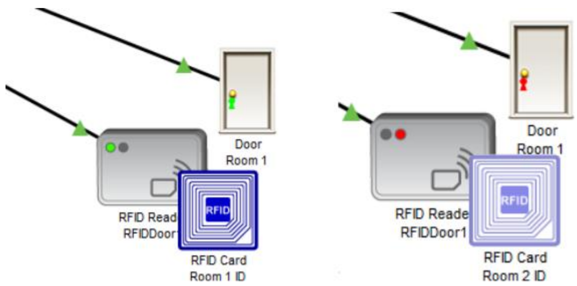
   - We set the unlocking conditions for the door.



   - We set the locking conditions for the door.



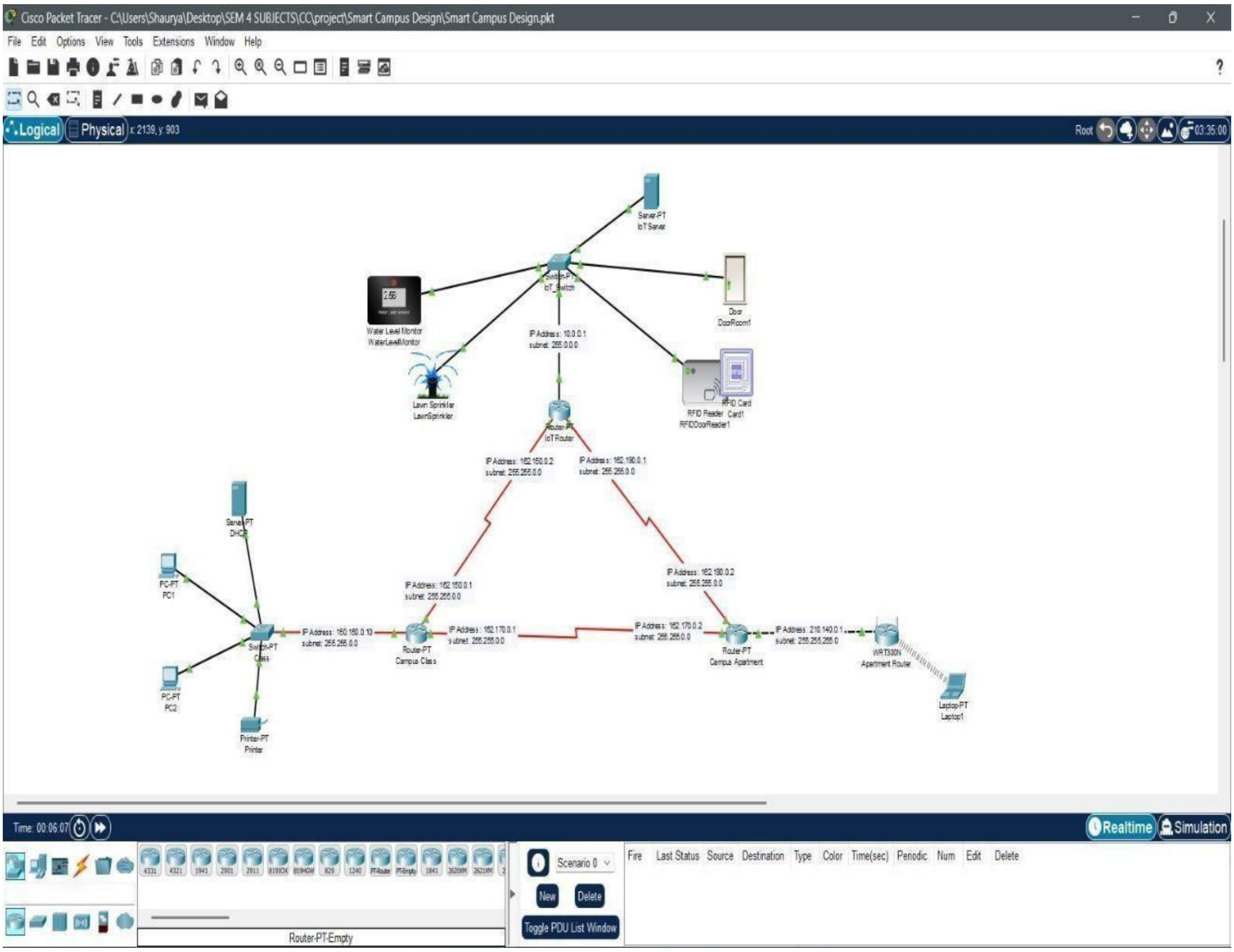
   - The door will unlock with proper RFID Card



CHAPTER 3

IMPLEMENTATION

Here is a real-time simulation of how the Smart-Campus Network can be implemented using Dynamic Host Control Protocol & Radio-Frequency Identification in Cisco Packet Tracer tool.



CHAPTER 4

RESULTS

4.1 Inference

The DHCP Protocol plays a pivotal role in the Smart Campus Project, addressing a range of critical objectives. By efficiently automating IP address allocation, it ensures that the diverse array of devices on the campus network can connect seamlessly, simplifying network administration and reducing the potential for errors. This scalability promotes future growth, allowing for the integration of more devices as needed without complex reconfiguration.

4.2 Future Scope

The emphasis on enhancing security through access control strengthens the campus's overall security infrastructure, safeguarding sensitive data and resources. Simultaneously, resource optimization, particularly in applications like intelligent sport field watering, contributes to sustainability by conserving resources and reducing operational costs. Moreover, monitoring and analysis tools ensure network health and security incident response, while comprehensive documentation and reporting serve as valuable resources for network administrators and stakeholders.

4.3 Conclusion

This project is a multifaceted strategy that aims to create a dynamic, secure, and efficient IoT environment within the university campus. It serves as a practical and valuable learning experience for us to gain a comprehensive understanding of networking technology and its potential applications in a larger-scale setting like a university campus. These objectives collectively contribute to the project's success and its readiness for the evolving landscape of IoT technology.

CHAPTER 5

REFERENCES

1. Chen, J., & Wu, H. (2019). Smart Campus: From Vision to Reality. Journal of Software Engineering and Applications, 12(6), 250-263. https://doi.org/10.4236/jsea.2019.126018

2. Fan, J., Wang, S., & Chen, G. (2018). An IoT-based Campus Security System. In 2018 17th IEEE International Conference on Communication Technology (ICCT) (pp. 1303-1307).https://doi.org/10.1109/ICCT.2018.8539584

3. Khan, A., & Nizamuddin, N. (2019). IoT-based Intelligent System for Water Management of Agriculture Fields. International Journal of Emerging Technologies in Learning (iJET), 14(14), 105-116. https://doi.org/10.3991/ijet.v14i14.10753

4. Lu, Y., & Liu, X. (2017). Research on IoT technology application in university campus environment. In Proceedings of the International Conference on Education, Management and Systems Engineering (EMSE 2017) (pp. 290-297). Atlantis Press. https://doi.org/10.2991/emse-17.2017.55

5. Wang, S., Jiang, J., & Wang, Y. (2018). IoT-based Intelligent Campus Energy Management System. In 2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 190-194). IEEE. https://doi.org/10.1109/CyberC.2018.00041

APPENDIX

Utilizing the Cisco Packet Tracer environment, the project made use of a wide range of complex parts and state-of-the-art technologies. The following crucial components were combined, making use of the simulation software's capabilities, to provide an extensive and dynamic network simulation:

Network Tracer from Cisco:

Serving as the project's main hub, Cisco Packet Tracer provided a powerful simulation tool for setting up and testing different network configurations. This setting made it easier to simulate actual network situations, which made it possible to integrate and test various technological components.

Identifying radio frequencies (RFID):

In order to facilitate the tracking and unique identification of things through radio-frequency communication, the project included RFID technology. RFID capabilities in the Cisco Packet Tracer simulation modelled object tracking and identification procedures.

Distributed Host Configuration Protocol, or DHCP:

Dynamic Host Configuration Protocol, or DHCP, was developed to automate network settings and IP address assignment. Cisco Packet Tracer was used to configure DHCP services. In order to ensure effective communication between network devices, this automation expedited the assignment of IP addresses and other network settings.

Water Level Monitor:

To replicate the tracking and measuring of water levels inside the network, a virtual water level monitoring system was added in the simulation. This part made it possible to keep an eye on the water levels in a mock environment.

RFID Reader:

An essential component of the project's simulation within Cisco Packet Tracer, RFID readers are used to read and analyze data stored on RFID tags. These readers replicated the procedure for obtaining and deciphering information from RFID tags.

The amalgamation of these innovative technologies and components within the Cisco Packet Tracer environment formed the backbone of the project, allowing for a comprehensive exploration and simulation of network configurations, object identification, automated network settings, and environmental monitoring.

PLAGIARISM REPORT

Dupli Checker

PLAGIARISM SCAN REPORT

12% Plagiarised	88% Unique	Date	2023-11-01
		Words	936
		Characters	7800

This Plagiarism Report was generated based on this documentation:

Matched Source

Similarity 50%
Title:submitted in partial satisfaction of the requirements for ...

https://escholarship.org/content/qt9b21d5jv/qt9b21d5jv_noSplash_cc3ca9b4d975e322e6a4f7290dbfab25.pdf

Similarity 50%
Title:jaipur.manipal.edu › foe › programsB Tech AI & ML at Manipal Univ Jaipur offers a cutting-edge ...
B Tech (Hons) Computer Science and Engineering with specialization in Artificial Intelligence & Machine Learning at Manipal University Jaipur. Check program details, eligibility, fee structure and scholarships at the Department of CSE, MUJ.
https://jaipur.manipal.edu/foe/programs/program-list/BTech-CSE-Artificial-Intelligence-and-Machine-Learning.html/

Similarity 17%
Title:18CSC206J-SEPM-Lab Report 1 .docx

https://www.coursehero.com/file/155139749/18CSC206J-SEPM-Lab-Report-1docx/

Similarity 17%
Title:Multi-disease classification model using deep neural ...

https://onlinelibrary.wiley.com/doi/10.1111/exsy.13335?af=R

Similarity 4%
Title:Chellammal Nallaperumal

https://srmist.irins.org/profile/306002