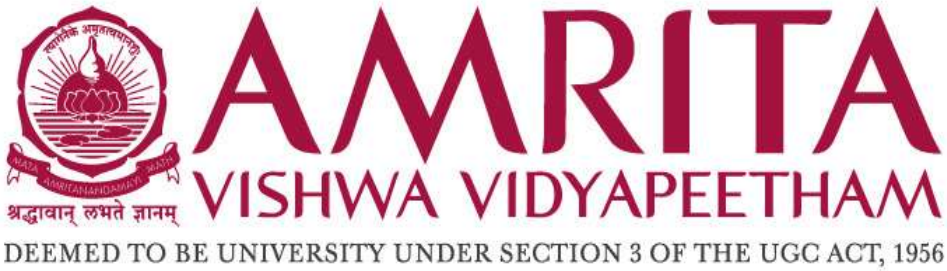
A Project

Submitted in partial fulfilment of the completion of

the course 19CCE304 Computer Networks

TEAM 09

S. No.	Name	Roll No.
1	B Ambareesh	CB.EN.U4CCE20006
2	Narendran S	CB.EN.U4CCE20036
3	Narun T	CB.EN.U4CCE20037
4	Pabbathi Greeshma	CB.EN.U4CCE20040
5	Santosh	CB.EN.U4CCE20053



BACHELOR OF TECHNOLOGY

COMPUTER AND COMMUNICATION ENGINEERING

AMRITA VISHWA VIDYAPEETHAM

COIMBATORE CAMPUS (INDIA)

Academic Year – 2022-23

Faculty In-Charge – Dr Gandhiraj R.

Developing a Network Design for a Smart Airport using Cisco Packet Tracer

B Ambareesh
B.Tech. Computer and Communication Engineering.
Amrita School of Engineering
Coimbatore, India
cb.en.u4cce20006@cb.students.amrita.edu

Narun T
B.Tech. Computer and Communication Engineering.
Amrita School of Engineering
Coimbatore, India
cb.en.u4cce20037@cb.students.amrita.edu

Narendran S
B.Tech. Computer and Communication Engineering.
Amrita School of Engineering
Coimbatore, India
cb.en.u4cce20036@cb.students.amrita.edu

Pabbathi Greeshma
B.Tech. Computer and Communication Engineering.
Amrita School of Engineering
Coimbatore, India
cb.en.u4cce20040@cb.students.amrita.edu

Santosh
B.Tech. Computer and Communication Engineering.
Amrita School of Engineering
Coimbatore, India
cb.en.u4cce20053@cb.students.amrita.edu

ABSTRACT – The fast-changing world is evolving towards automation rapidly every day, and a good network system is inevitable anywhere to properly manage an automated system. Before implementing a network system, it is necessary to visualize and learn a protocol to understand the system in depth and identify its issues. Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. It helps network developers design prototype models and provides a virtual network simulation platform that helps simulate projects and observe their efficiency in the real world. In this research, the authors have developed a prototype of the network design of an airport using a Cisco Packet Tracer. The process that depicts how the network system will work in real life is explained and the simulation of data transmission is provided.

KEYWORDS – Data Transmission, Networking System, Network Design, Cisco Packet Tracer, Virtual Network Simulation

I. INTRODUCTION

Computer networks are a demanding and important topic for any kind of networking and data communication. Nowadays, the need for developing a proper networking system for any infrastructure like offices, schools, airports, universities etc. is rapidly increasing to conduct their day-to-day work. This work is based on developing a network design prototype for an airport. It can vary from organization to organization since every organization implements a different network system as the interior and exterior do not match one another. To conduct this work, we have chosen to use Cisco Packet Tracer as it is a compact software by which researchers can develop models like the real world and can implement the necessary changes required. Packet Tracer also supports virtual network simulation. For these large numbers of advantages, researchers have chosen to use Packet Tracer.

The objectives of working on this project are as below:

- Gathering knowledge about computer network
- Learning Cisco Packet Tracer in depth
- Getting experience in how real-life projects work
- Learning about networking systems and network design
- Developing a prototype of network design, suitable for an airport.

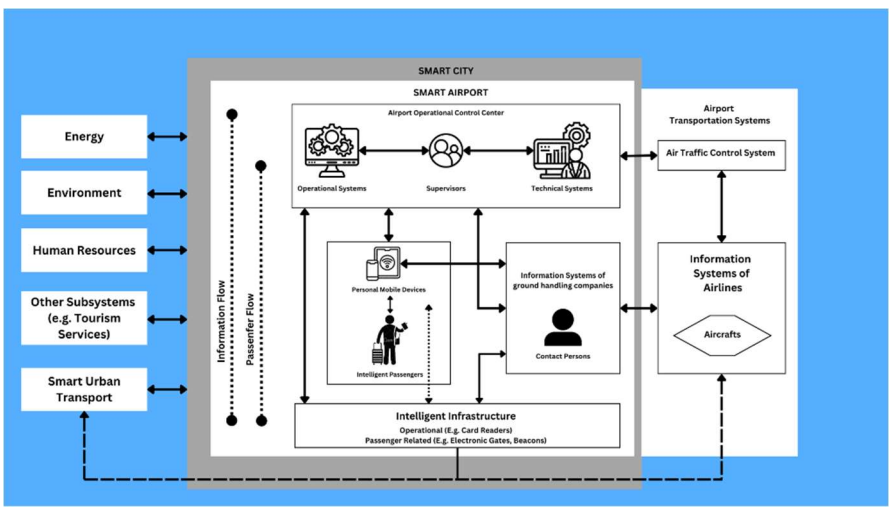


Figure 1 – Smart Airport Visualization

II. NOVELTY

1. Exploring The Security Challenge:
   - While security systems share the goal of protecting the flying public, most operate independently within an airport.
   - The existing and new technologies from multiple vendors operate on individual networks, each requiring separate equipment installation, expensive cabling, and ongoing maintenance.
   - As additional security systems come on board, the number of networks could go higher still. The lack of unification makes it difficult to share information within the airport and with external local and federal authorities.

2. From Chaos to New Order:
   - Regaining the confidence of air travelers will take a combination of improved security measures and devices; return of consumer confidence; and streamlined systems that allow data correlation and information sharing.
   - A quick, coordinated security network that allows information sharing between the airlines, airport and security personnel, and law enforcement authorities would prevent many of the airport terminal closures and flight delays that have recently plagued air travelers.

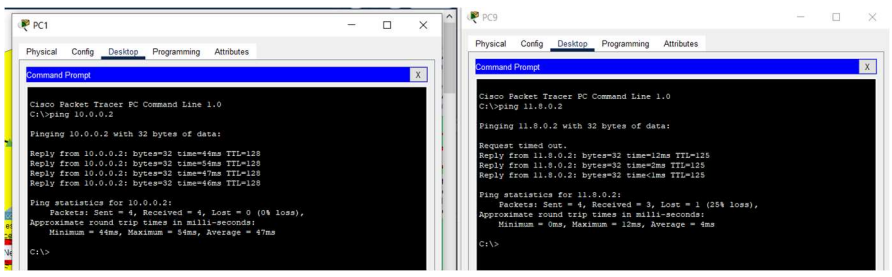


Figure 2 – Difference in Round Trip Time

3. Applying Existing Technology in a New Way:
   - Much integration work still needs to be performed, and this task is made more difficult with the wide variety of proprietary communications protocols currently in use by security applications.
   - Consolidation of development around current communications standards will speed the integration of applications and provide new opportunities to share data.

Job	Number of People	Annual Pay (in Rupees)	Cost per Year (in Rupees)
Environmental Monitoring	8	2,64,000	21,12,000
Airport Maintenance	8	1,60,000	12,80,000
Basic Security and Surveillance	10	3,00,000	30,00,000

4. Integrated Solutions:
    - As airports tackle the job of deploying security technologies, they need to consider solutions from multiple vendors. These include vendors in the categories of video surveillance, access control, biometrics, other security technologies, and systems integrators to pull the solution together.
    - A critical component of an integrated security environment is a network architecture that is built on industry standards and leverages common tools and designs to serve as a unified platform for security applications.

5. Unifying Video Surveillance:
    - One of the major problems with current analogue video systems is that there are a wide variety of industry standards in use, many of which are highly proprietary.
    - Systems from different vendors, operating on widely varying standards, are difficult, if not impossible, to integrate. As systems are purchased over the years, each new vendor or technology solution must operate on its network.
    - Complex Problem, Simple Solution – Multiple vendors have come together to design a smart, streamlined solution that integrates analogue-based systems onto the digital common network infrastructure.
    - Digital Advantages – In a digital networked CCTV model, a camera is located near a switch that directs it onto the common network infrastructure, thereby allocating 80 per cent of the investment to active elements and only 20 per cent to cabling.

The main contributions of this work are as follows:

- We analyse the various IoT applications found in contemporary smart airports, the methods utilised for their development and their vulnerabilities.
- We propose a network architecture for contemporary smart airports, focusing on the network architecture of the installed IoT devices.
- We investigate security and privacy issues present in contemporary smart airports, with a focus on their networks.
- We provide a study of security solutions for smart airports, including vulnerability analysis and risk mitigation strategies.

III. METHODOLOGY

In this research, we develop a network design that includes an airport's basic components.

1. Air Control Room:
    - To make the Arrival Room secure, we can perform static routing (a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic) to control the data transmission system.
    - With this system, only the Arrival and Departure Room employees can retrieve data from the Air Control Room.

2. Arrival Room:
    - In the Arrival Room, there are two parts. The first one is for the employees and the other one is for the guests. Here, both parts are divided through two different routers.
    - The router for the employees can transmit data to the Air Control Room so that the employees can be informed of flight updates and other necessary data from air control. And guests cannot transmit data to/from the Air Control Room for security purposes.

    (i) *Employee Department* –
        - The PCs can communicate directly with the Air Control Room through the router. The Default Gateway IP is the IP for the router connecting the PCs with the Air Control Room.
        - The default gateway should be the same in all the PCs as all are transmitting data through the same router. And the Subnet will be auto-generated according to the IP class.

    (ii) *Guest Department* –
        - The guest department has a wireless router connected to a guest router. This wireless router is connecting the end devices of the guests.
        - The Wi-Fi router can transmit data in any range between 0-250 meters and it will use 2.4 GHz of the wireless channel to avoid conflict.
        - The Arrival_Guest_Router is connected to two devices through two ports. The ethernet port is connected to the Wi-Fi router and supplies the internet to it. And the serial port is connecting the server through the arrival router.

3. Departure Room: Same as Arrival Room.

4. Security Room: There are two servers in the Security Room. These servers are connecting two switches that are connected with motion detector security cameras.

    (i) *Internet of Things (IoT) Devices* –
        - There is an individual working motion detector-operated security camera in both the Arrival and the Departure Room. When the motion detector is off, the camera does not work and vice-versa.
        - When someone walks near the motion detector, it sends a signal to the camera to be turned on. It is a power-efficient way to install security cameras.
        - This model needs a registration server to work properly. Live feedback can be seen by logging into the registration server by entering the correct username and password.
        - It shows that this model of installing security cameras is pretty safe and secure. In addition, the data can be found on the servers in the Security Room as the servers are collecting and storing the data.

    (ii) *Server Room* – There are mainly three basic servers in the server room. These servers collect and store data coming from the air control, the arrival and the Departure Room.

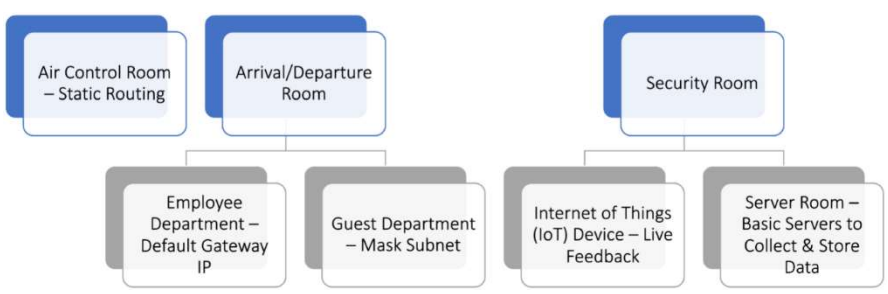


Figure 3 – Hierarchical Representation of Methodology

IV. RESULTS AND ANALYSIS

1. Air Quality Check:

- Construct a simple air quality monitoring system using Packet Tracer.
- Choose the components to construct the system – Home Gateway, Smartphone, Carbon Monoxide Detection, Windows and Siren.
- Set the authentication mode and passphrase in the home gateway.
- Connect all the IoT components and the smartphone to the home gateway. Set the remote IoT server by entering the server address, username and password. Set the network adapter to 'PT-IOT-NM-1W'.
- In the web browser of the smartphone, enter the IPv4 Address. Log in with the assigned username and password.
- All the components connected to the circuit can be viewed here. Automate the system using conditions/editor.
- Create actions by defining rules on the server.

Name	Condition	Actions
Low-Risk	CO Sensor Level > 0.02	Set Window 1 On to true Set Window 2 On to true
High-Risk	CO Sensor Level > 0.03	Set Alarm On to true
No-Risk	CO Sensor Level < 0.01	Set Window 1 On to false Set Window 2 On to false Set Alarm On to false

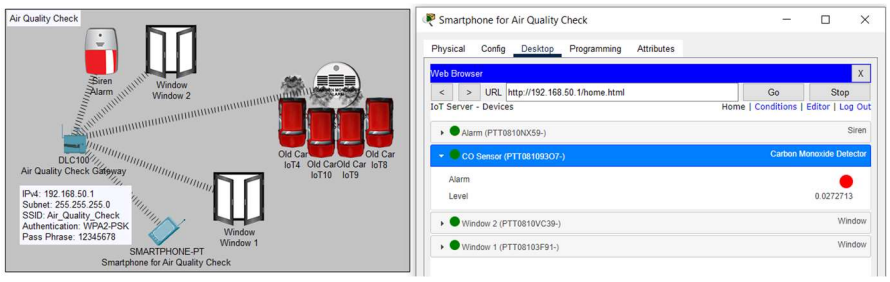


Figure 4 – Air Quality Check

2. Lounge for Staff Only (Employee Department):

- Use Cisco packet tracer for Radio-Frequency Identification (RFID) enabled door access mechanism, Bluetooth technology to connect various devices and access IoT-enabled devices from a smartphone.
- Choose the components to construct the system – Server, Switch, Router, Smartphone, Home Gateway, Door, RFID Reader, RFID Card, Light, Bluetooth Speaker and Portable Music Player.
- Register the IoT devices with the server. Select the network adapter as 'PT-IOT-NM-1CFE' for the door lamp and 'PT-IOT-NM-1W' for other IoT devices.
- Automatically choose the connection type to connect necessary devices with cables.
- Configure the router by navigating to the required interface and assign the IPv4 address and subnet mask in the IP configuration.
- Turn on the port status and enable the DHCP server to assign the IP address to the IoT devices.
- Configure the IP address to the server along with the subnet mask and default gateway, i.e., the router's IP address.
- Enable IoT services on the server to act as a registration server for the IoT devices. Create an IoT account.
- Register each IoT device with the server. Select the mode of gateway/DNS IPv4 as DHCP and remote IoT server by specifying the server address, username and password.
- Create actions by defining rules on the server.

Name	Condition	Actions
RFID-Valid	RFID Reader Card ID = 1001	Set RFID Reader Status to Valid
RFID-Invalid	RFID Reader Card ID != 1001	Set RFID Reader Status to Invalid
Door-Open	RFID Reader Status is Valid	Set Door Lock to Unlock
Door-Lock	RFID Reader Status is Invalid	Set Door Lock to Lock

- Assign an ID to the RFID Tag, by default, the value is 1001. Disable wireless and enable Bluetooth interfaces in both the music player and speaker. Disable wireless and 3G/4G for the smartphone.
- Discover both the devices nearby, select the devices and pair them. Connect the IoT devices wirelessly with the home gateway by connecting to the SSID and authentication passphrase of the home gateway.

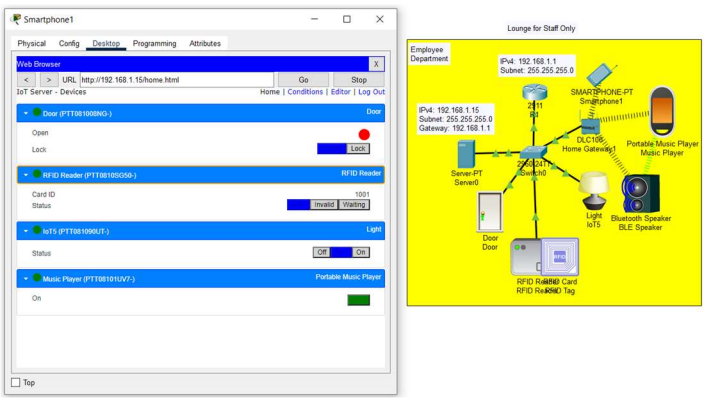


Figure 5 – Lounge for Staff Only (Employee Department)

3. Lounge for Travelers Only (Guest Department):

- Choose the components to construct the system – Home Gateway, Switch, Router, Server, PC, Smartphone, Laptop, Door, Lamp, Webcam, Window, Fan and Air Conditioner.
- Connect to the required components with a straight-through copper wire and make a note of the IP addresses as you move along.
- For the router, enable the port status and configure the IPv4 address and subnet mask. Enable the DHCP server to assign the IP address of the IoT devices.
- Assign the LAN IPv4 address to the home gateway, and configure the IP in static mode with the default gateway (router's IP).
- In the wireless settings, assign the SSID, coverage range to 1000 meters and authentication mode to WEP with the passphrase.
- Assign the IPv4 address, subnet mask and default gateway for the PC. Enable IoT services on the server to act as a registration server for the IoT devices.
- Create an IoT account. For each of the IoT devices, configure the static default gateway and remote IoT server with the server address, username and password.

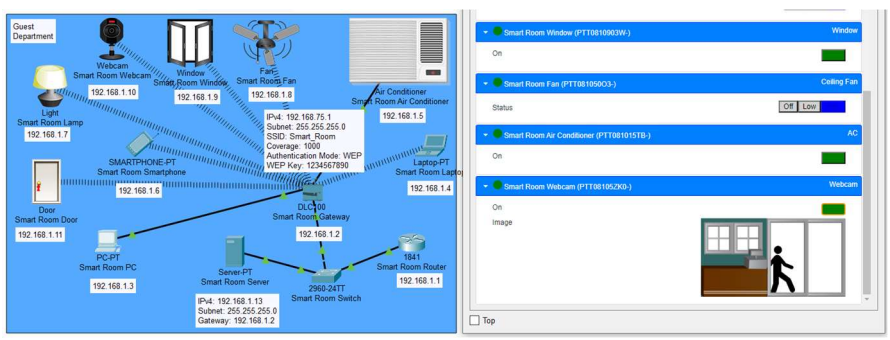


Figure 6 – Lounge for Travelers Only (Guest Department)

4. Smart Garden:

- Configure a lawn sprinkler and monitor the water level by using a sensor with an IoT registration server.

- Choose the components to construct the system – Server, Home Router, Laptop, Lawn Sprinkler and Water Level Monitor.
- Connect the IoT server and wireless router with a copper straight-through cable and assign the IP address, subnet mask and default gateway to the server.
- Configure the wireless router and assign the IP address, network name (SSID), security mode, encryption and passphrase.
- Connect the laptop wirelessly with the server by adding the wireless NIC in the physical device view. Provide the SSID, authentication mode and passphrase in the wireless interface.
- Configure the lawn sprinkler and water level monitor by setting the network adapter to 'PT-IOT-NM-1W' and provide the configuration settings with the same as for the laptop.
- Turn ON the IoT services in the server and assign the username and password for the account creation. Register the IoT devices with the remote server by providing the same username and password.
- Create actions by defining rules on the server.

Name	Condition	Actions
Turn-ON-Sprinkle	Water-Level Water Level <= 10.0 cm	Set Sprinkle Status to true
Turn-OFF-Sprinkle	Water-Level Water Level > 11.0 cm	Set Sprinkle Status to false

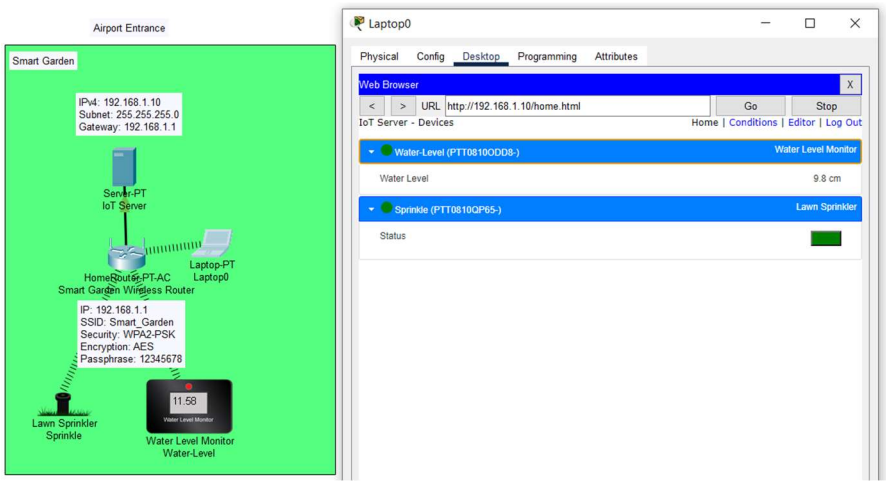


Figure 7 – Smart Garden

5. Boarding Area:
    - Smoke and fire detection systems use automatic functions to detect the occurrence of an event that may result in a fire.
    - Receive a sign from a fireplace sensing smoke and mechanically transmit it to the fireplace siren panel. The fire siren panel activates sprinklers and opens all windows and doors.
    - Choose the components to construct the system – Smartphone, Home Gateway, Siren, Switches, Windows, Doors, Smoke Detectors, Fire Sprinklers and an Old Car.
    - Create the boarding layout and place all the components in appropriate places. Configure all components with the home gateway and connect them with a switch.
    - Access all the sensor devices from the smartphone by connecting them with the required username and password.
    - Create actions by defining rules on the server.

Name	Condition	Actions
On	Match any: • G Sensor Level > 0 • K Senor Level > 0 • B Sensor Level > 0	Set G Door On to true Set G Sprinkler Status to true Set K Sprinkler Status to true Set K Window On to true Set K Door Lock to Unlock Set B Window On to true Set B Sprinkler Status to true Set B Door Lock to Unlock Set Siren On to true
Off	Match all: • B Sensor Level <= 0 • K Senor Level <= 0 • G Sensor Level <= 0	Set Siren On to false Set B Sprinkler Status to false Set K Sprinkler Status to false Set G Sprinkler Status to false

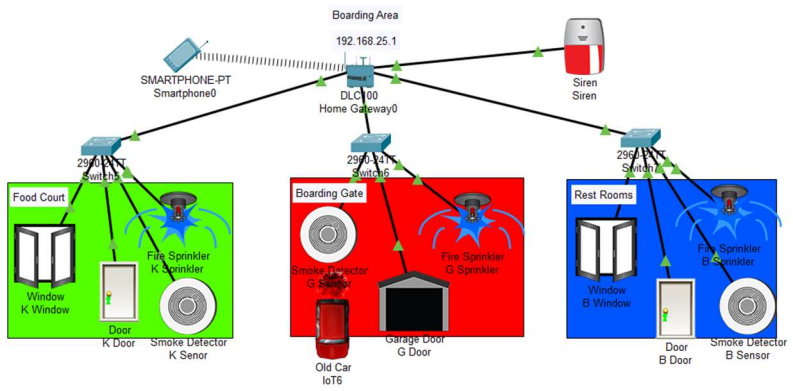


Figure 8 – Boarding Area

6. Highly Restricted Areas:
    - Choose the components to construct the system – Home Gateway, Smartphone, Door, Motion Detector, Siren and Webcam.
    - Note the IP address of the gateway and set SSID, authentication mode and passphrase.
    - For all the IoT devices, select Home Gateway in IoT Server and set the network adapter to 'PT-IOT-NM-1W'. Configure the wireless interface to the gateway.
    - Open the web browser on the smartphone and log in to the home gateway. All the components connected to the system can be accessed here.
    - Create actions by defining rules on the server.

Name	Condition	Actions
Person-Present	Security Room Motion Detector On is true	Set Security Room Webcam On to true Set Security Room Siren On to true
No-Person	Security Room Motion Detector On is false	Set Security Room Webcam On to false Set Security Room Siren On to false

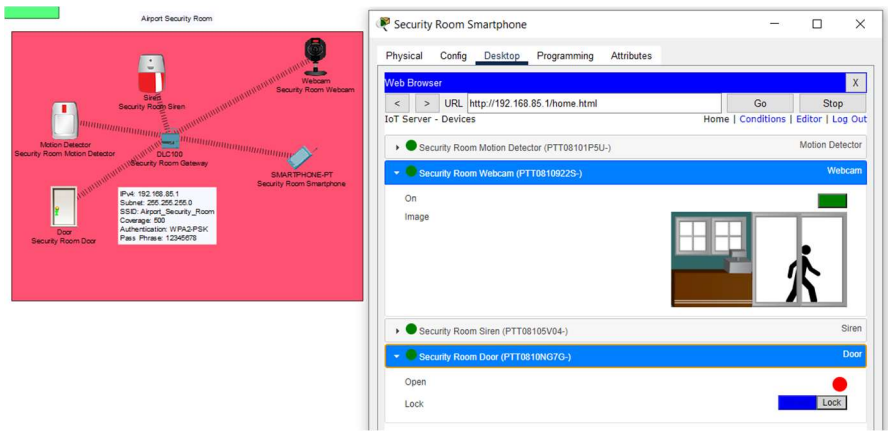


Figure 9 – Highly Restricted Areas

7. Secured Airport Communications:
Setup Pre-requisite – Integrate LAN and PAN steps to form WAN. Further steps include the following,

a) Create topologies for two separate wireless local area networks (WLANs).
   - Configure the wireless interface on each device with the IP address in the WLANs.
   - Set Wired Equivalent Privacy (WEP) key on each device in the WLANs.

b) Connect the two WLANs with a wired backbone network and configure the IP address on each device in the wired network.

c) Check communication between,
   - Wired Devices
   - Wireless Devices
   - Wired and Wireless Devices

d) Outputs generated include,
   - Successful ping responses between different devices.
   - Sample screenshots of WEP key setting and IP address configuration.

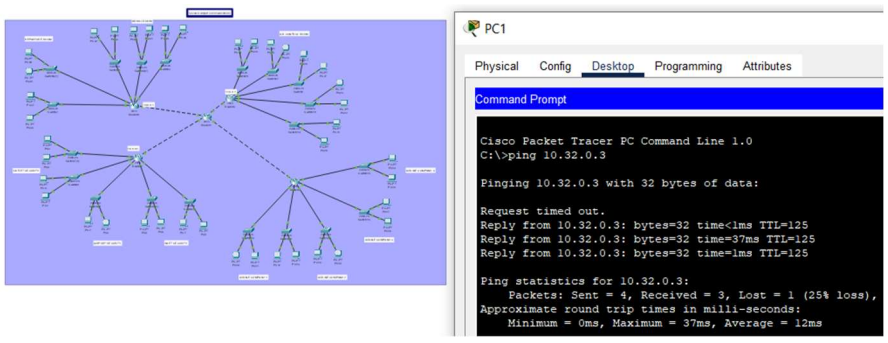


Figure 10 – Air Control Room (Static Routing)

8. Air Control Room – Network Address Translation (NAT)
   - NAT allows a single device, such as a router, to act as an agent between the Internet (public network) and a local (private) network. This means only a single, unique IP address is required to represent an entire group of computers.
   - In static NAT, a private IP address is mapped to a public IP address, where the public address is always the same IP address (i.e., it has a static address). This allows an internal host such as a web server, to have an unregistered (private) IP address and still be reachable over the internet.
   - Configure the IP address on the interface in both routers, PCs and the server.
   - Ping to the server from PC1 and then, configure static NAT.

STEP – I	STEP – II	STEP – III
configure terminal	int serial 0/0/0	ip nat inside source static 192.172.1.1 1.0.0.1
int fastEthernet 0/0	ip nat outside	ip route 0.0.0.0 0.0.0.0 serial 0/0/0
ip nat inside	ex	ip nat inside source static 192.172.1.2 1.0.0.1
ex		ip route 0.0.0.0 0.0.0.0 serial 0/0/0

   - Ping command on both PCs and check connectivity.

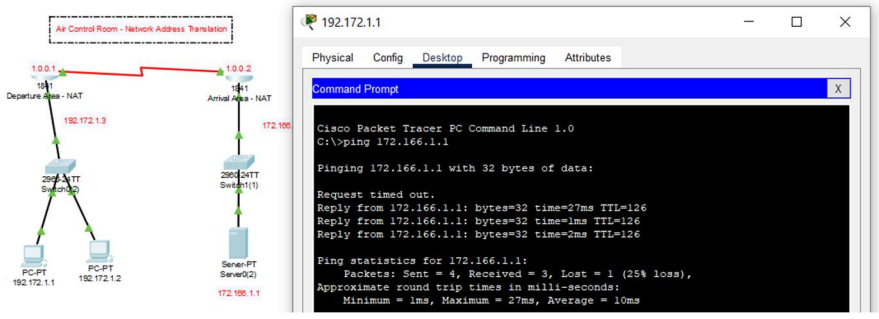


Figure 11 – Air Control Room (NAT)

V. CONCLUSION

In this work, a prototype of network design for an airport has been successfully developed and tested in the real-time simulation mode available in Cisco Packet Tracer. This prototype has been developed in such a way that ensures faster data transmission and secured network connections. In addition, this network design makes sure that any unwanted data transmission cannot happen. All these implementations help to develop smooth network connections as well as make the network design secure enough to operate. We have ensured successful connectivity among all the devices in this network system.

VI. REFERENCES

Serial Number	Base Paper	Cisco Documentations	Journals & Conference Papers	Packet Tracer YouTube Tutorials	
				Video Name	URL
1	Ahmed Imran KABIR & Sriman MITRA & Suraya AKTER & Md Rakibul ISLAM & Soumya Suhreed DAS, 2022. "Developing a Network Design for a Smart Airport Using Cisco Packet Tracer," Informatica Economica, Academy of Economic Studies - Bucharest, Romania, vol. 26(1), pages 25-38.	Airport Network Integration Eases Costs, Improves Security, And Enhances Operations, Cisco Systems, Inc.	N. Koroniotis, N. Moustafa, F. Schiliro, P. Gauravaram and H. Janicke, "A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports," in IEEE Access, vol. 8, pp. 209802-209834, 2020, DOI: 10.1109/ACCESS.2020.3036728.	Air Quality Check (or) Environment Monitoring System using Packet Tracer | IoT Application	https://www.youtube.com/watch?v=4ht5FojLI7I&t=449s&ab_channel=TechnoBrunch
2		Cisco Intelligent Airport Wireless (Wi-Fi) Network Solution, White Paper, Cisco Systems, Inc.	Rajapaksha, Aruna & Jayasuriya, Nisha. (2020). Smart Airport: A Review on Future of the Airport Operation. Global Journal of Management and Business Research. 20. 10.34257/GJMBRAVOL20IS3PG25.	Cisco Packet Tracer - RFID, Bluetooth, Smartphone	https://www.youtube.com/watch?v=cPewlj0kEtk&t=340s&ab_channel=DrSKhan
3		Cisco Technology Helps Keep Passengers, Plans, and Luggage on Schedule at Sydney Airport, Business Case, Cisco Systems, Inc.	Alghadeir, Abdullah and Sakran, Hasan Al-, Smart Airport Architecture Using Internet of Things (September 30, 2016). International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-4, Issue-5, September 2016.	Configuration of Wireless Heterogeneous Network using Cisco Packet Tracer	https://www.youtube.com/watch?v=UZwB7JTgYCc&ab_channel=Dr.ShubhangiKharche
4				How to Configure a Smart Home Design in Cisco Packet Tracer | IoT Devices Configure | End Devices	https://www.youtube.com/watch?v=vjPWanGskek&ab_channel=ProgrammingFrog
5				IoT Device Programming using Packet Tracer with Sensors and Actuators	https://www.youtube.com/watch?v=RH1az9-GxoY&t=698s&ab_channel=KayalvizhiJayavel
6				Smart Garden in Packet Tracer	https://www.youtube.com/watch?v=DdeXrsMFnq4&t=7s&ab_channel=HaiderTech
7				Smart Security System using Packet Tracer | IoT application | Anti-Theft System using Packet Tracer	https://www.youtube.com/watch?v=42DCkx36Uv8&ab_channel=TechnoBrunch
8				Static NAT Configuration in Cisco Packet Tracer 2019	https://www.youtube.com/watch?v=pErjl9WA1V8&t=919s&ab_channel=KrishnoDey