Ministry of Higher Education and Scientific Research

Faculty of Sciences of Monastir

Mini Project: Fundamentals of Networks

"From Idea to Smart Home:

Design and Configuration of a Computer Network"

Date: 30/04/2024

Full Name: Med Yassine Khlif

GENERAL INTRODUCTION

GENERAL INTRODUCTION

Going beyond a mere collection of connected devices, IoT weaves a complex web of interactions between physical objects and the digital world, opening endless possibilities to transform our way of life and interaction with the environment.

At the core of this approach lies a sharp combination of several technological domains: network management, cloud storage, full-stack development, and intelligent embedded systems equipped with sensors. This vision drives the project, where I had the privilege to design an innovative network architecture, offering everyone complete control of their home, wherever they are, anywhere in the world.

To explore this project, we will simulate its architecture using "Cisco Packet Tracer," network modeling tools. This simulation will allow us to visualize the functioning of our network, test various configurations, and address any potential issues. By simulating interactions between connected devices, IoT gateways, and cloud servers, we will refine our design to ensure its effectiveness and reliability.

With this innovative approach, we aspire to redefine the boundaries of home connectivity and pave the way for an era where technology transcends traditional borders, where every object becomes an opportunity for enhancing and enriching our daily lives.

CHAPTER 1:

NETWORKS

CHAPTER 1:

NETWORKS

Introduction to Computer Networks

In today's digital landscape, computer networks play a crucial role in facilitating communication and information sharing among devices and users. This exploration aims to closely examine the various types of networks and the fundamental components that make them operational.

Types of Networks:

Local Area Network (LAN):

LANs are confined to limited areas such as offices, homes, or campuses. They offer fast speeds and low latency, perfect for internal communications within an organization.

Wide Area Network (WAN):

WANs cover vast geographical areas, often connecting multiple LANs together. They use technologies like leased lines or the Internet to provide connectivity over long distances.

Metropolitan Area Network (MAN):

MANs cover extensive urban areas, connecting multiple sites within a city. They facilitate communication and resource sharing at the city level.

Virtual Private Network (VPN):

VPNs establish secure connections over public networks, allowing remote users to access private resources securely.

Wireless Networks:

These networks use technologies such as Wi-Fi to enable wireless connectivity between devices, offering deployment flexibility.

Peer-to-Peer (P2P) Networks:

P2P networks allow individual devices to connect directly to each other to share resources without going through a central server.

Network Components:

Nodes:

Nodes are the devices connected to the network, such as computers, servers, printers, switches, routers, phones, etc. Each node has a unique address that allows it to be identified on the network.

Transmission Media:

Transmission media are the physical or wireless means by which data is sent from one node to another. This can include Ethernet cables, optical fibers, radio waves, satellites, etc.

Network Equipment:

Network equipment includes the hardware devices that enable the network's operation. These include routers, switches, hubs, gateways, Wi-Fi access points, repeaters, etc.

Network Protocols:

Network protocols are sets of rules and conventions that determine how data is transmitted and received between network nodes. Common protocols include TCP/IP, UDP, ICMP, HTTP, etc.

IP Addresses:

IP (Internet Protocol) addresses are unique numerical identifiers assigned to each node on an IP network. They allow data to be routed to the correct destination.

MAC Addresses:

MAC (Media Access Control) addresses are unique identifiers assigned to each network card. They are used at the data link layer to identify devices connected to the local network.

Structured Cabling:

Structured cabling includes the cables and connectors used to connect different network equipment. It provides a physical infrastructure for data transfer.

Network Services:

Network services are software that provides specific functionalities to users and applications, such as file sharing, printer sharing, Internet access, email, etc.

In this smart home network infrastructure project, a variety of networks and components are used to facilitate communication between different devices. LANs enable internal exchanges, while WANs ensure connection to the Internet. Physical components include coaxial cables, copper cables, routers, switches, servers, modems, and default home gateways. Smart devices connect wirelessly to the home gateway to access the Internet. This combination of networks and components ensures smooth and efficient communication within the smart home and with external services.

CHAPTER 2:

PROPOSED

ARCHITECTURE

CHAPITRE 2:
ARCHITECTURE PROPOSÉE

To create a network infrastructure enabling communication between different components of the smart home model, both within the local network and with external networks and services, it's crucial to choose the appropriate type of cabling for each connection. To do so, we need to establish a breakdown of relationships between each component in the model:

Cell Tower and CO Server: The cell tower connects to the central server (CO) via a Coaxial cable for its high bandwidth, reliability, ability to cover long distances, and compatibility with existing infrastructures, thus establishing the link between the wireless network and the central network infrastructure.

CO Server and Router: The connection between the CO server and the router is made through a Copper Coss-Over cable to establish a direct link, thus eliminating the need for an intermediate switch. The router then acts as the Internet service provider. By connecting to the router, the CO server functions as a gateway connecting the local network to the broader Internet. This setup allows the router to efficiently route data between the local network and the Internet, facilitating access for local network users to online resources, and vice versa.

Router and Switch/Cloud: The connection between the router and the switch/cloud is typically made using a Copper Straight-Through cable to maintain a standard wiring configuration. The router is connected to both the switch and the cloud component. The switch facilitates communication between local servers and devices, while the cloud component represents the connection to the Internet. This configuration allows the router to effectively direct

traffic between the local network and the Internet, while ensuring smooth communication between various devices in the local network.

Switch and Servers (DNS and IoE): The switch connects to the Domain Name System (DNS) server and the Internet of Things (IoE) server. The DNS server resolves domain names into IP addresses, allowing devices to access websites and services by name. The IoE server manages communication between smart devices and facilitates their integration into the network.

Cloud and Modem: The cloud component connects to the modem via a Coaxial cable, which links the local network to the broader internet infrastructure, enabling communication with external networks and services.

Modem and Default Home Gateway: The modem typically connects to the default home gateway using a Copper Straight-Through cable, serving as a central hub for all smart devices in the home network. This gateway manages communications between devices in the home network and the external network.

Smart Devices and Home Gateway: All smart devices connect wirelessly to the home gateway, allowing them to communicate with each other and access the internet via the gateway.

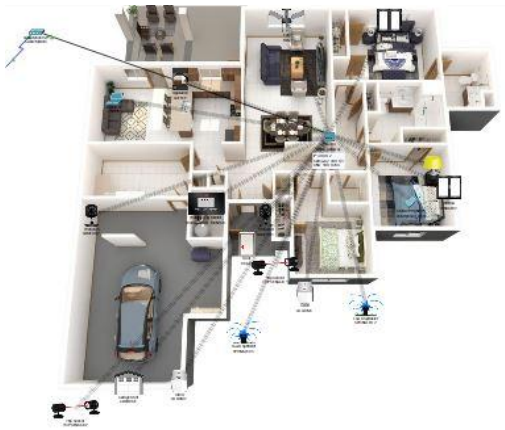
CHAPTER 3:

SIMULATION

CHAPTER 3:
NETWORK SIMULATION

In this section, you will provide all the configurations made and the connectivity tests using the "ping" command.

In our network, all components share the same server address, allowing users to control their devices from an IoT monitor. We have set up a configuration with a central server where all IoT devices communicate.



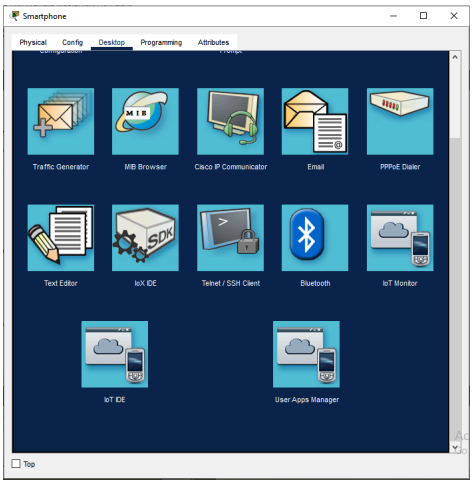
When we ping the server address (10.0.0.253), we assess the connectivity between our device connected to the Internet and this central server. Receiving a response confirms its availability.

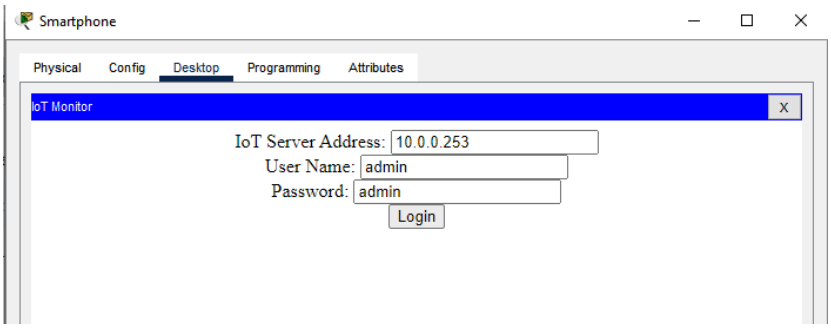
```
C:\>ping 10.0.0.253

Pinging 10.0.0.253 with 32 bytes of data:

Reply from 10.0.0.253: bytes=32 time=78ms TTL=126
Reply from 10.0.0.253: bytes=32 time=27ms TTL=126
Reply from 10.0.0.253: bytes=32 time=16ms TTL=126
Reply from 10.0.0.253: bytes=32 time=13ms TTL=126

Ping statistics for 10.0.0.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 78ms, Average = 33ms
```

All IoT devices are connected to the gateway, thus facilitating data exchange and control by the user via the IoT monitor interface.

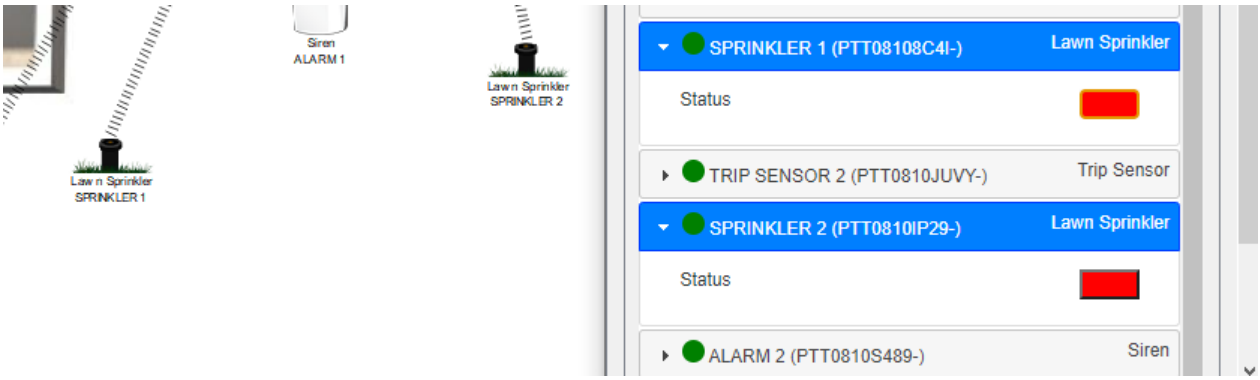
Now, we will verify if the user can control these devices from their home using their device. To do this, they need to access the "IoT Monitor" tab, enter the IP address of the IoE server, and then provide the required credentials (username and password). Finally, they just need to click "Login" to establish the connection to the server.

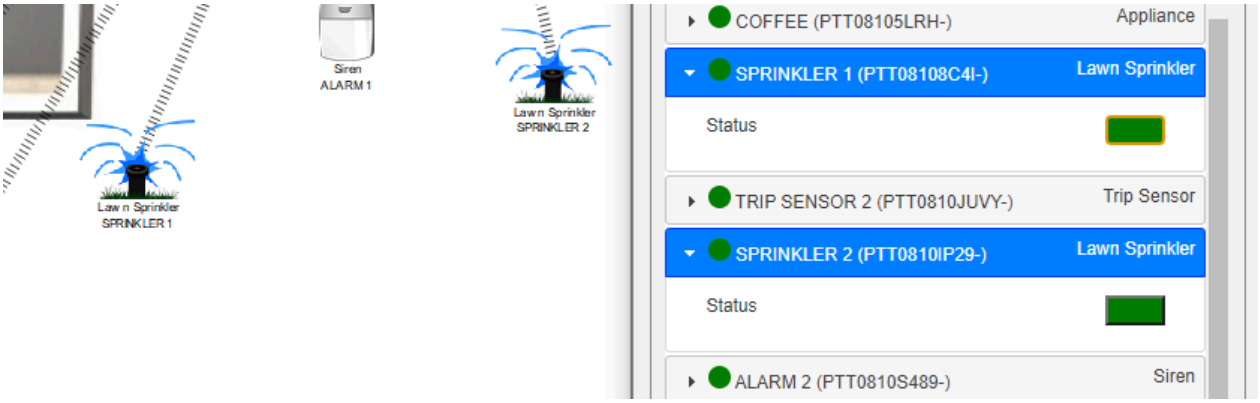
Desktop > IoT Monitor > Provide the IP address of the IoE server > Enter credentials > Login.





It is clear that they have access to all connected devices and can modify their operation. For example, one can water the lawn outside the house.





To configure the router, we need to follow these essential steps:

1. Assign an IP address to each connection: Ensure that every device connected to the network has an IP address to enable smooth communication.
2. Configure DNS and IoT servers: Provide appropriate IP addresses, and gateways, and ensure that DNS and IoT services are activated to facilitate domain name resolution and connectivity of IoT devices.
3. Implement DHCP (Dynamic Host Configuration Protocol): Automatically assign IP addresses to devices connected to the network, simplifying IP address management and ensuring continuous connectivity.

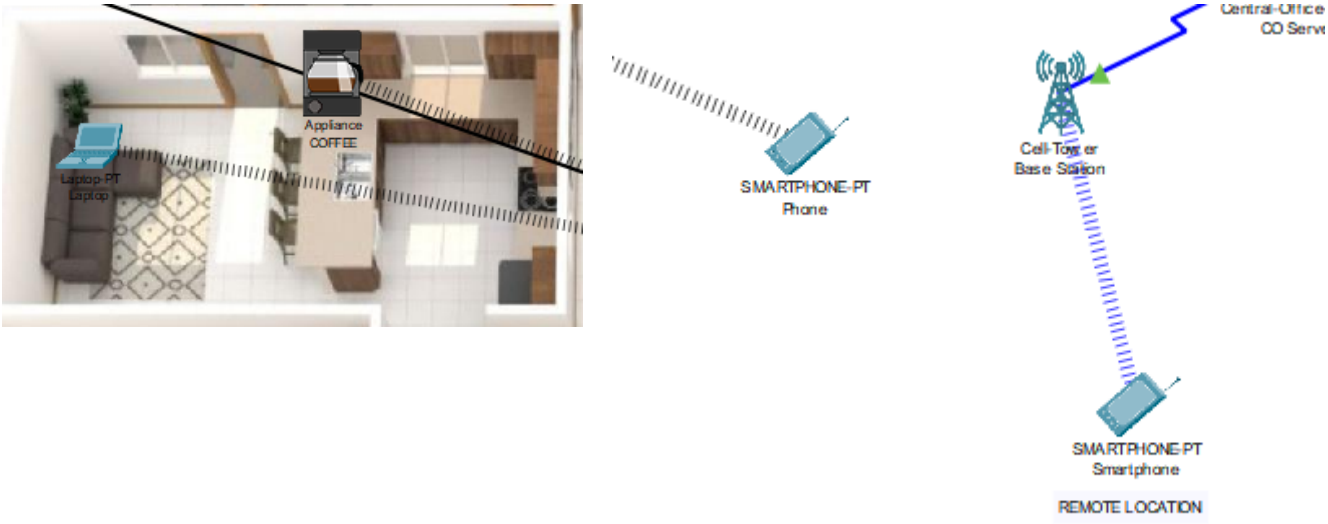
To implement DHCP on the server side and other sides (cloud and modem), follow these configuration commands:

```
enable
Config t
(config)# ip dhcp pool ---Name---
(config)# network ---IP--- ---Subnet Mask----
(config)# default-router ---Router Gateway---
(config)# dns-server ---DNS Server IP---
```

Connect and configure connections

For each device you need to control, you should access **Config > IoT Server > Provide the IP address of the IoE server > Enter the username and password.**

The user can control these devices from anywhere, even outside their home and over long distances. This scenario is highlighted by connecting three devices to the Internet.



CONCLUSION

CONCLUSION

In conclusion, this smart home represents much more than just an ambitious network infrastructure project; it embodies a revolution in the evolution of home connectivity. By innovatively merging cutting-edge technologies such as network management, cloud storage, full-stack development, and the use of intelligent embedded systems, it paves the way for a new era where technology truly becomes ubiquitous and transformative. This smart home goes beyond a mere collection of connected devices; it symbolizes a bold vision where every aspect of our daily life is enhanced and enriched by the convergence of the physical and digital worlds. Its impact extends far beyond its walls by redefining the standards of home connectivity, opening new vistas for innovation and progress in numerous fields. Empowering individuals to control their environment wherever they are in the world, creates an unprecedented user experience and heralds an era of endless possibilities.

In a constantly evolving world, this smart home catalyzes change, integrating advanced technological solutions into our daily lives, enabling us to tackle environmental, social, and economic challenges with confidence and creativity, thus paving the way for a future where technology becomes the engine of our collective progress. Ultimately, this project embodies the promise of a future where connectivity becomes ubiquitous, where every object becomes an opportunity for improvement and enrichment, and where every individual can shape their environment according to their own needs and desires. With this smart home, we stand on the brink of a revolution that transcends traditional boundaries and opens the door to a new era of endless possibilities.