

## Experiment 21

### IMPLEMENTATION OF IoT DEVICES IN NETWORK

Aim: To implement IoT devices in networking using Cisco packet tracer.

Resources required:

Switches, routers, workstations and printer.

Internet connection, cable, patch cables.

Modem, telephone, telephone jack, telephone line, telephone cable.

Procedure:

1) Open Cisco packet tracer and create a new project.

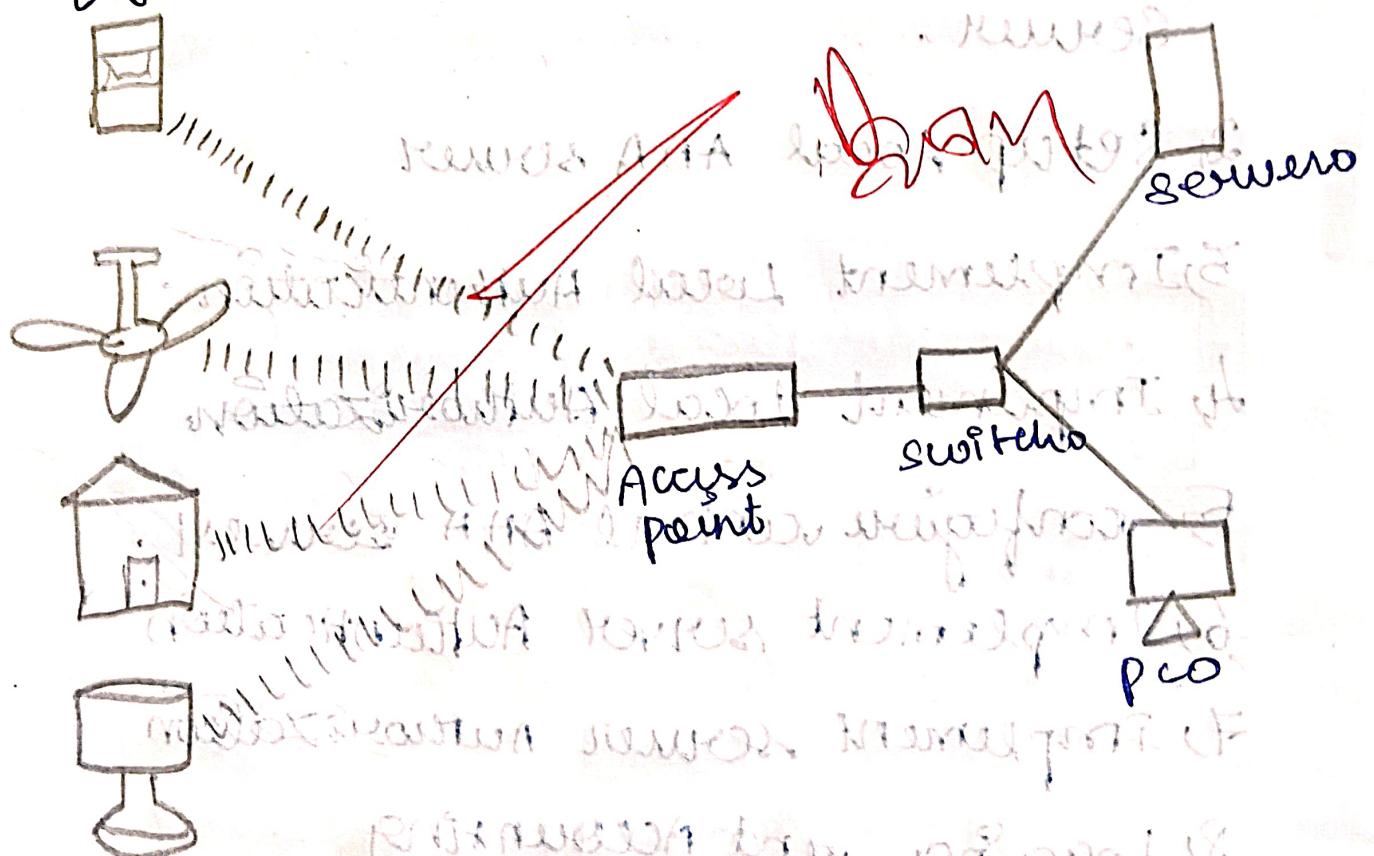
2) Steps:

1) open Cisco packet tracer and create a new project.

2) connect the router to the internet by dragging and dropping a cloud device from the devices panel onto the workspace area.

3) Add an IoT device to the network by dragging and dropping a device from the devices panel onto the workspace area.

- 4) connect the IoT device to the IoT service via an ethernet cable.
- 5) configure the IoT service by clicking on "configure IoT service" by clicking on the "edit" button and then clicking on "enable" and then clicking on "enable" and then clicking on "enable".
- 6) Test the connectivity of the IoT devices by pinging it from the Router or from another device on the network.
- 7) These were just general steps and the specifics of the implementation will depend on the specific IoT device and network configuration you want to create.



Results: Thus an IoT device in networking is implemented using Cisco packet tracer.

## Experiment - 22

Tel based AAA local and server authentication configuration

Aim: Designing range Tel based AAA local and server based authentication configuration.

Software/Apparatus Required:- packets

Procedure:

Algorithm:-  
1, Define Tel Tel deities record Local AAA server.

2) Setup Local AAA server

3) Implement Local Authentication

4) Implement Local Authorization

5) Configure central AAA server

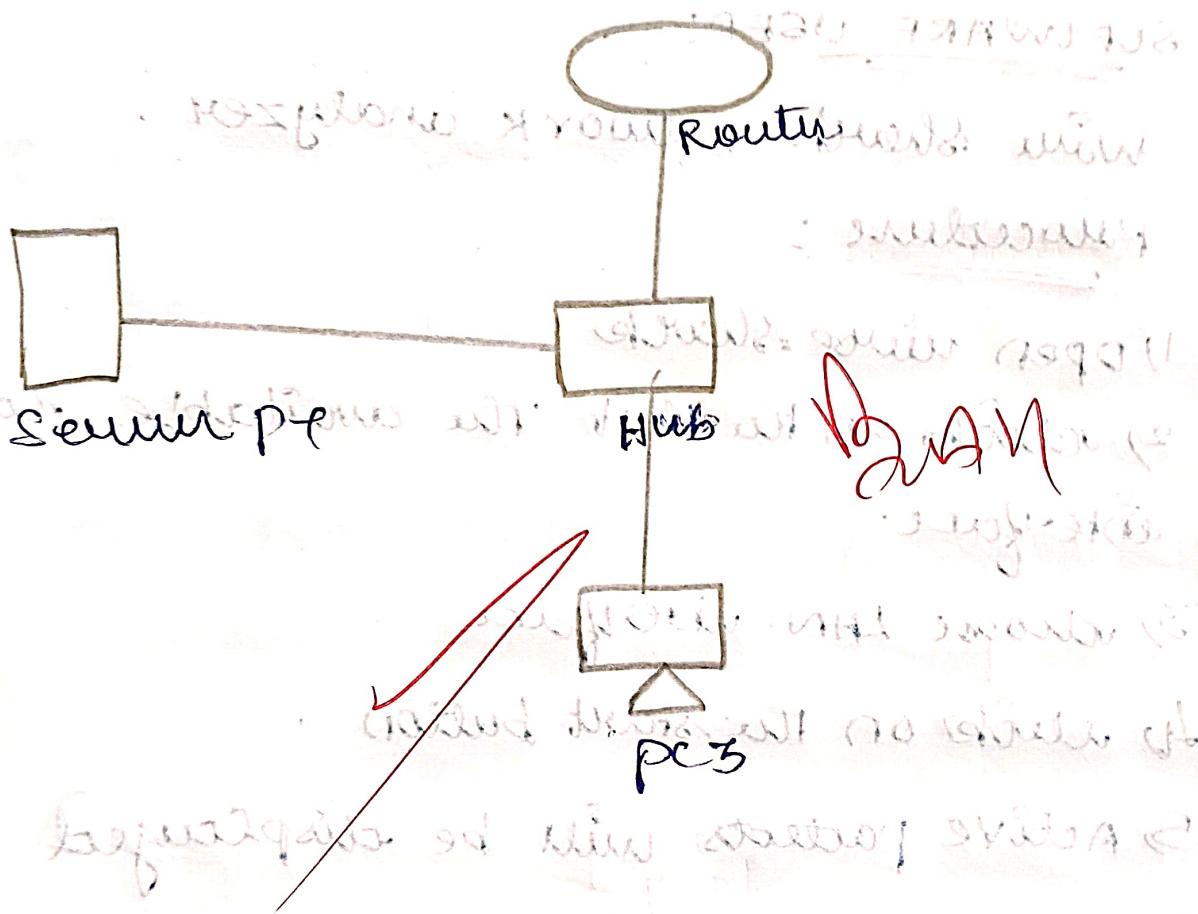
6) Implement server Authentication

7) Implement server Authorization

8) Logging and Accounting

9) Revocation and updates

Remember to implement appropriate security measures such as strong encryption, secure measures such as encryption, secure communication protocols, and strong passwords. policies to ensure the integrity and confidentiality of the authentication process.



Result: IoT based AAA, local and server

based authentication is assigned successfully.

Experiment - 25

TRANSPORT LAYER PROTOCOL HEADER ANALYSIS ~~WIRE SHARK~~ TCP and UDP

Aim: To analyze capturing of Transport layer protocol header analysis using wireshark - TCP and UDP.

### SOFTWARE USED:

wireshark network analyzer.

### Procedure :

- 1) Open wireshark
- 2) Click on the list of available capture interface.
- 3) choose LAN interface
- 4) click on the start button
- 5) Active packets will be displayed.
- 6) capture the packets & select any IP address from the source.
- 7) click on the expression and select IPVA → ip.addr == source address

8) After field name select the double equals ( $=$ ) from the selection panel enter the selected IP source address & click on apply button.

9) All the packets will be filtered using source address.

Result: Hence, the capturing of packets using Wireshark network analyzer was analyzed for TCP and UDP.

No. 10) For a connection using cable, if click with right mouse, went into

Result: Hence, the capturing of packets using Wireshark network analyzer was analyzed for TCP and UDP.

Experiment - 24

**NETWORK LAYER : Protocol Header Analysis**

using Wireshark - SMTP AND ICMP.

Aim: To analyze, capturing of Transport Layer protocol header analysis using Wireshark - SMTP and ICMP.

**SOFTWARE USED :**

1. open Wireshark.

2. click on list. the available capture interface

3. choose the LAN interface.

4. click on start button.

5. Active packets will be displayed

6. capture the packets & select any IP address from the source.

7. click on the expression and  $\text{IPV4} \rightarrow$   
add source address in the field  
name.

8.) Select the double equals ( $\equiv$ ) from the  
selection and enter the selected IP  
source address.

## Sniffer Configuration

click on apply button

All the packets will be filtered using source address.

Selected port number or name

Class selection: Selecting traffic types

• TCP/HTTP - Shows when

Selected frame type

Port filter creation shows when

• selecting

• Create new monitor

and then click on start monitor & configuration

configuration

• Selecting ports monitor

• monitor when do capture

• Selecting stop when do

stop capture

Port number & listening port supported

• 10000, 20000, 25000, 30000, 40000

Result: Hence, the capturing of packets using wireshark network layer analyzer was for smtp and icmp.

Experiment - 25NETWORK LAYER PROTOCOL HEADERS

ANALYSIS USING WIRE SHARK - ARP AND  
ICMP

Aim: To analyze capturing of Broadcast layer protocol header analysis using  
wire shark - ARP and ICMP.

SOFTWARE USED:

wire shark network analyzer

Procedure:

- 1) open wire shark.
- 2) click on list the available capture interface
- 3) choose LAN interface.
- 4) click on start button.
- 5) active packets will be displayed.
- 6) receive the packets & select any IP address from the source -



- 4) click on the expression and select  $\text{IPV4} \rightarrow \text{IP}$  address source address in the field name.
- 5) select double equals ( $= =$ ) from the selection and enter the selected IP source address.
- 6) click on apply button.
- 7) All the packets will be filtered using source address.



Ques 3

Result: Hence, the capturing of packets using wire shark network analyzer was analyzed for ARP and HTTP.