Experiment-01

IMPLEMENTATION OF IOT DEVICES IN NETWORKING

AIM: To implement an IoT devices in networking using cisco packet tracer.

Software/Apparatus required:
packet tracer, End devices, Hubs, connectors.

Procedure:

Steps:

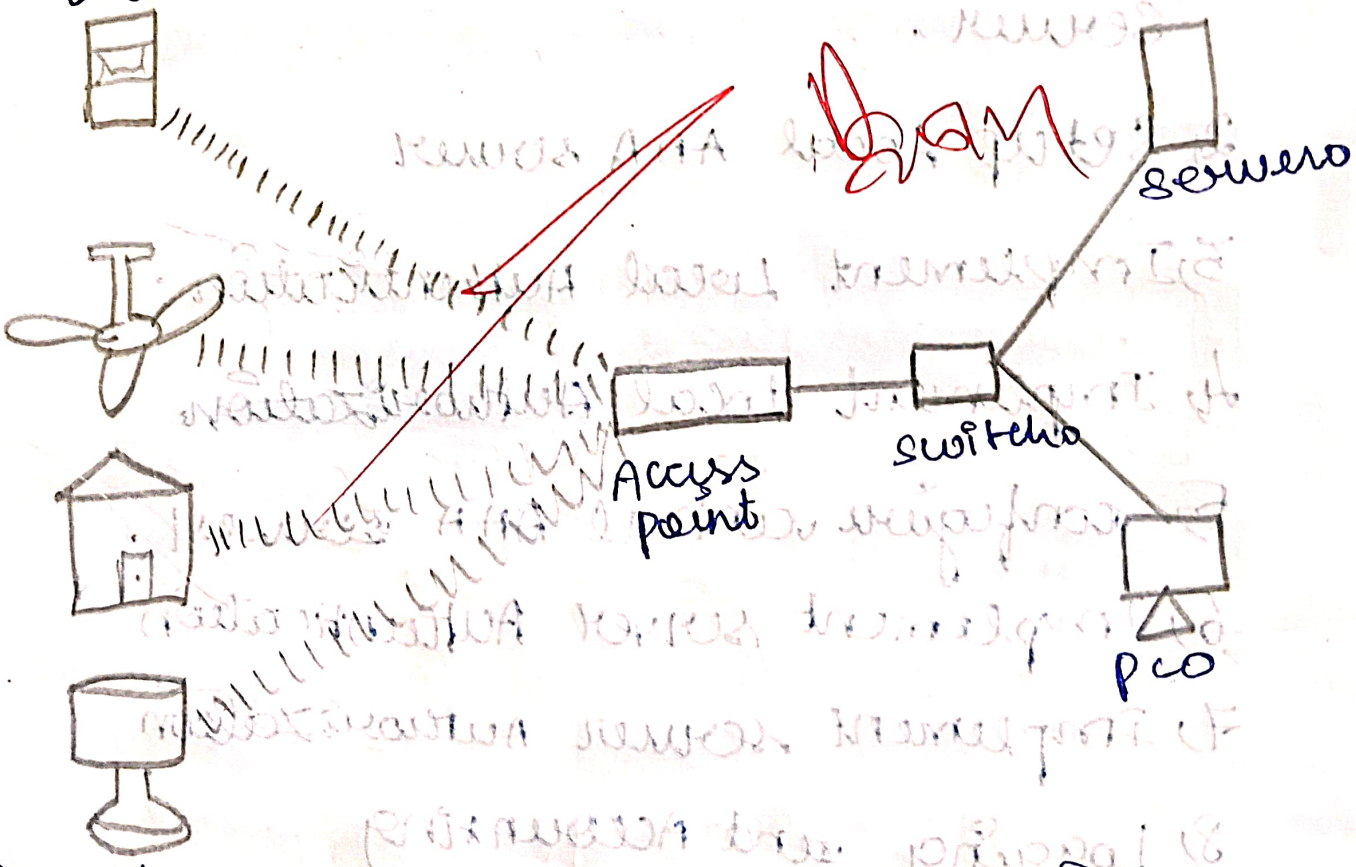
1) open cisco packet tracer and create a new project.
2) connect the router to the internet by dragging and dropping a cloud device from the Devices panel onto the workspace area.
3) Add an IoT devices to the network by dragging and dropping a device from the devices panel on the to the workspace area.

4) connect the IoT device to the ... an ethernet cable.

5) configure the IoT device by clicking on it and then clicking on the CLI tab.

6) Test the connectivity of the IoT devices by pinging it from the router or from another device on the network.

7) These are just general steps and the specifics of the implementation will depend on the specific IoT device and network configuration you want to create.



Result: Thus an IoT device in networking is implemented using cisco packet tracer.

J.S Jaseel
1925210116

Experiment - 22

IoT based AAA local and server authentication configuration.

Aim: Assigning an IoT based AAA local and server based authentication configuration.

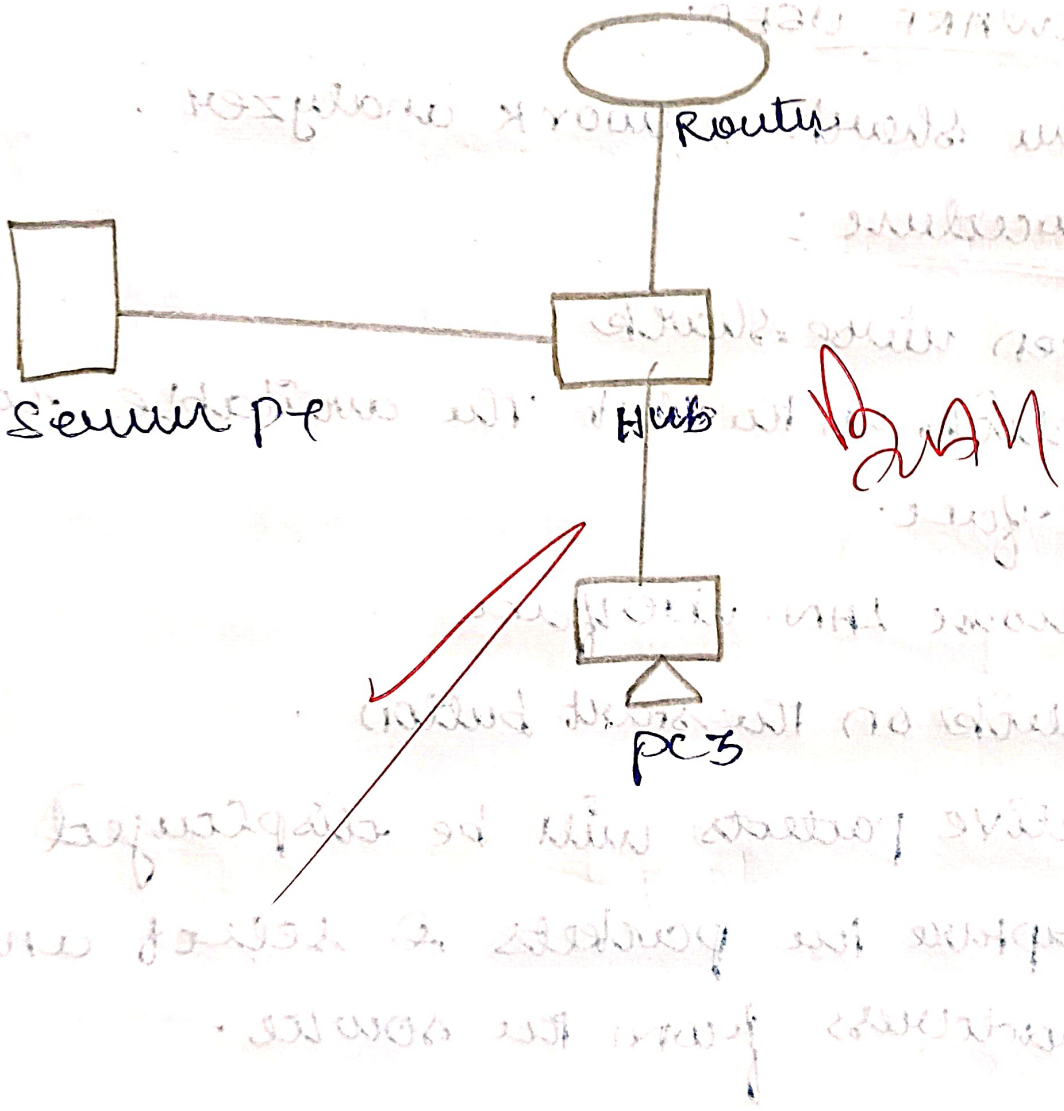
Software / Apparatus Required: packet tracer / End devices, Hubs, connections.

procedure:

Algorithm:

1) Define IoT devices and 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 encryption, secure measures such as encryption, secure communication protocols, and strong passwords policies to ensure the integrity and confidentiality of the authentication process



Result: IOC based AAA local and server based authentication is assigned successfully.

192524046

Experiment - 25

TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING 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.

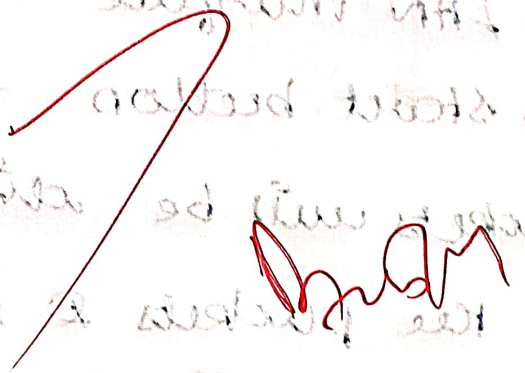
Procedure:

1) Open wireshark
2) click on the list the 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 IPV4 → ip addr : source address.

in the field name

8) select the double equals (==) from the relation and enter the selected ip source address & click on apply button.

10) 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.

192501406

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 IPV4 ip address source address in the field name.
8. Select the double equals (==) from the selection and enter the selected IP source address.

click on apply button.

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

Result: Hence, the capturing of packets using wireshark network Layer analyzer was for SMTP and ICMP.

Experiment - 25

NETWORK LAYER PROTOCOL HEADER ANALYSIS USING WIRE SHARK - ARP AND HTTP

Aim: To analyze capturing & transport layer protocol packet analysis using wire shark - ARP and HTTP.

SOFTWARE USED:

Wire shark network analyzer

Procedure:

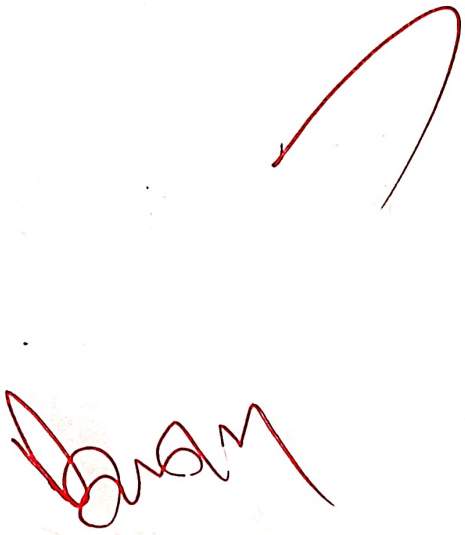
1) Open wire shark.
2) Click on list the available capture interface
3) Choose LAN interface.
4) Click on start button.
5) Active packets will be displayed.
6) Capture the packets & select any IP address from the source -

7) click on the expression and select IPV4 → IP addr source address in the field name.

8) select double equals (==) from the selection and enter the selected IP source address.

9) click on apply button.

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



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