EXPERIMENT - 21

IMPLEMENTATION OF IoT DEVICES IN NETWORKING

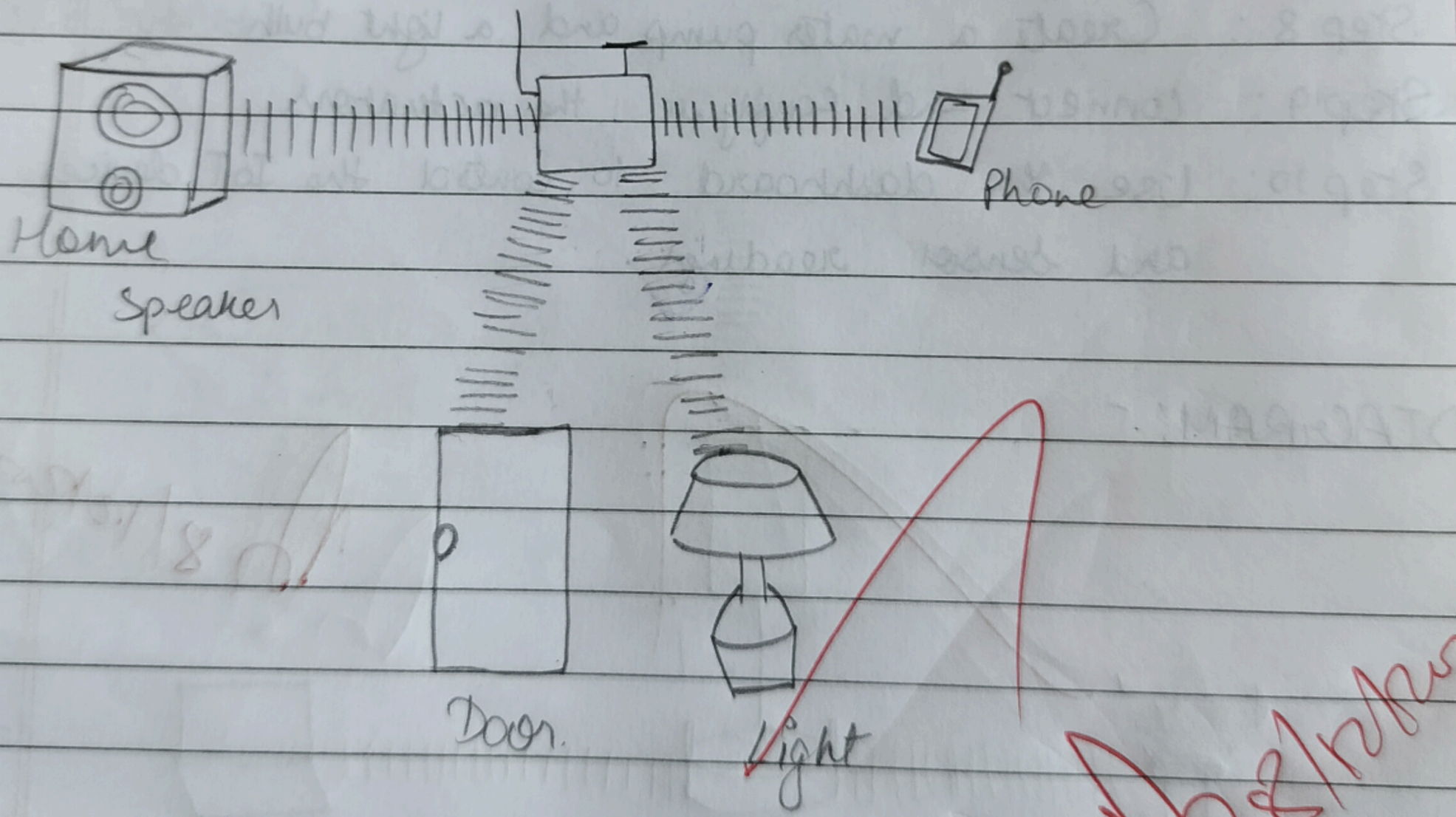
AIM:-

To implement an IoT device in networking using Cisco Packet Tracer.

PROCEDURE:-

Step 1: Open Cisco Packet Tracer.
Step 2: Connect router to internet
Step 3: Add an IoT device to the network.
Step 4: Connect the IoT device to the router using ethernet cable.
Step 5: Configure the devices.
Step 6: Test the connectivity.

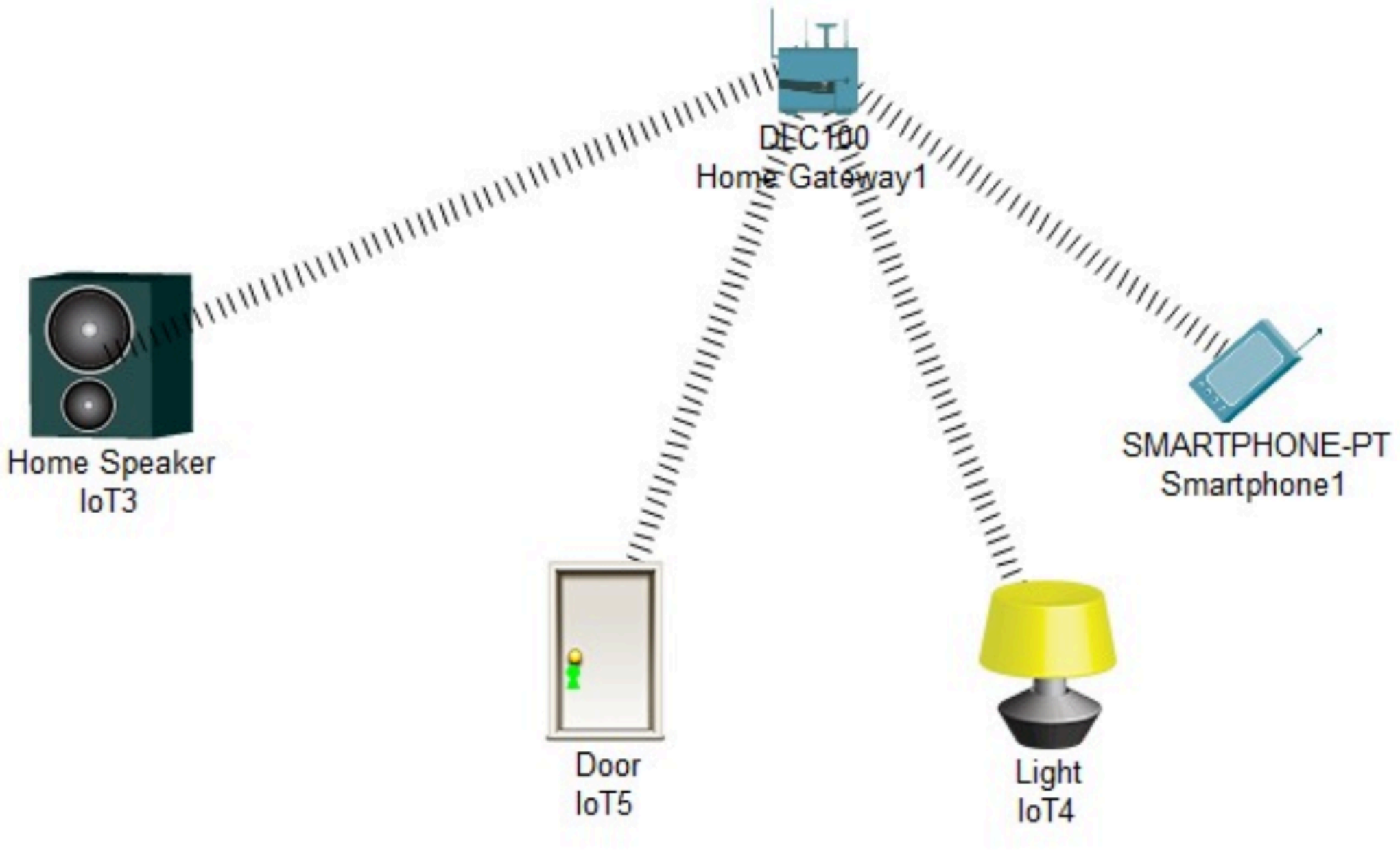
DIAGRAM:-



RESULT:-

Thus an IoT device in networking is implemented using Cisco Packet Tracer successfully.

implementation of iot devices in networking



EXPERIMENT - 22.

IoT based AAA LOCAL AND SERVER BASED AUTHENTICATION CONFIGURATION.

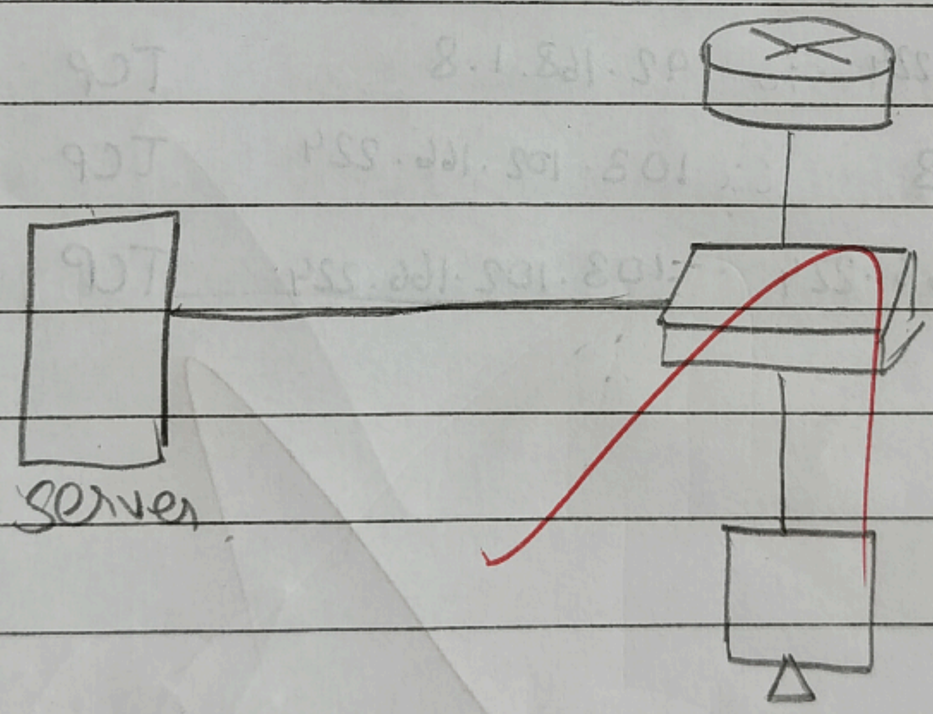
AIM:-

Designing an IoT based AAA local and server based authentication configuration

PROCEDURE:-

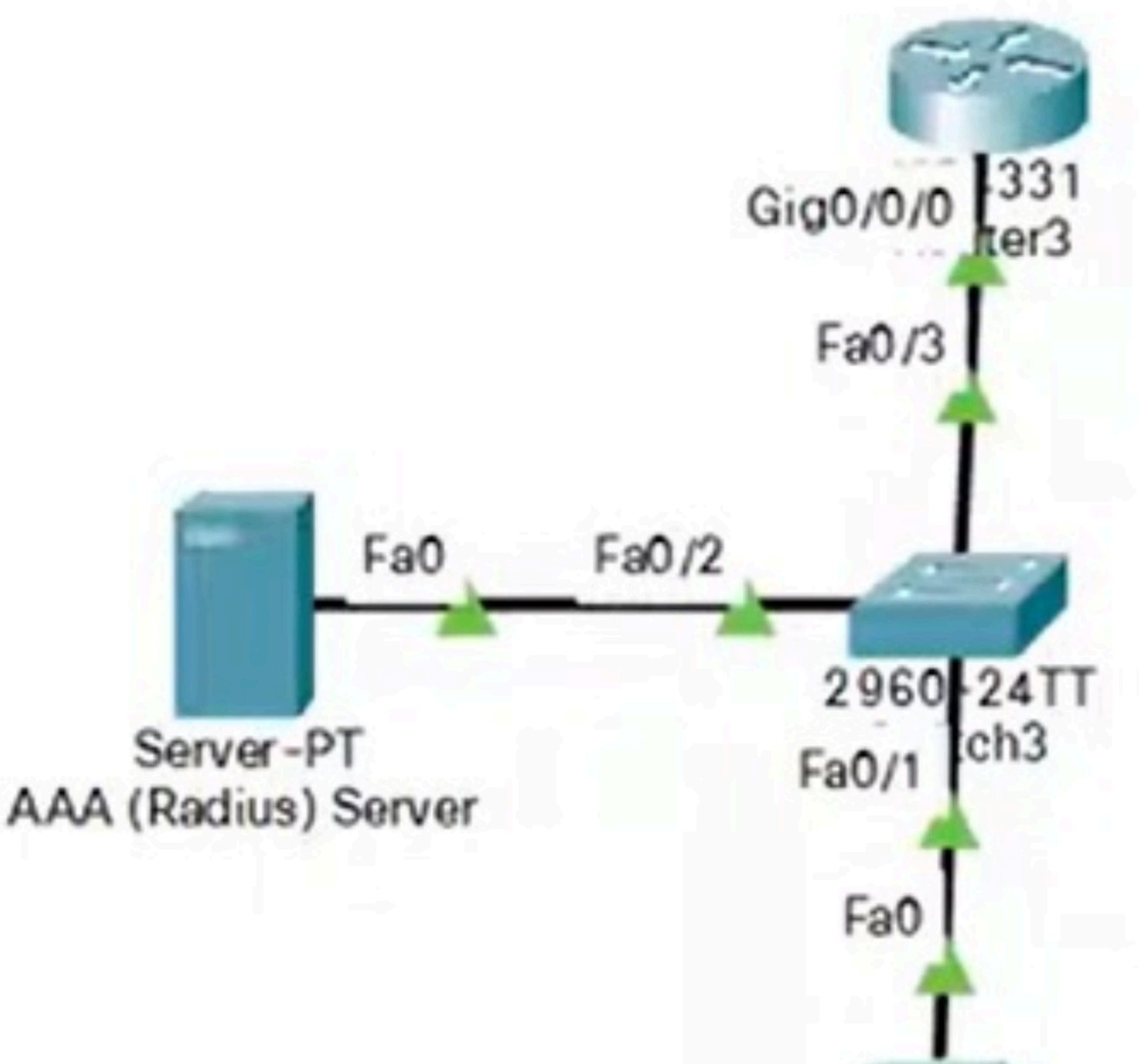
Step 1 : Define the components.
Step 2 : Setup Local AAA server
Step 3 : Implement Local Authentication
Step 4: Implement local Authorization
Step 5: Configure Central AAA server.
Step 6: Implement Server Authentication
Step 7 : Logging & Accounting
Step 8 : Revocation & Updates.

DIAGRAM:-



RESULT :-

IoT based AAA local and Server based authentication designed successfully.


Gig0/0/0
331
ter3
Fa0/3
Fa0
Fa0/2
Server-PT
AAA (Radius) Server
2960-24TT
ch3
Fa0/1
Fa0
PC-PT
PC3

EXPERIMENT-23

TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING ~~WHERE~~ WIRESHARK - TCP AND UDP.

AIM:-

To analyse capturing of Transport Layer protocol header analysis using wire-Shark_TCP and UDP.

PROCEDURE:-

Step 1: Open wire Shark.
Step 2: Capture interface and choose which LAN
Step 3: Click start - active packets will be displayed
Step 4: Capture packets & select IP address.
Step 5: Select IPV4 source address
Step 6: Select double equals and enter IP address
Step 7: Click apply, all packets will be filtered.

DIAGRAM:

Time	Source	Destination	Protocol	Length
9970 166.922419	192.168.1.8	103.102.166.224	TCP	66
9999 166.962098	103.102.166.224	192.168.1.8	TCP	66
10000 166.962230	192.168.1.8	103.102.166.224	TCP	54
10004 166.963204	103.102.166.224	103.102.166.224	TCP	66

RESULT:-

Hence, the capturing of packets using wire shark. for TCP and UDP was analyzed.

tcp and ip.addr == 103.102.166.224

No.	Time	Source	Destination	Protocol	Length	Info
9970	166.922419	192.168.1.8	103.102.166.224	TCP	66	51853 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
9999	166.962098	103.102.166.224	192.168.1.8	TCP	66	443 → 51853 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1436 SACK_PERM=1 WS=512
10000	166.962230	192.168.1.8	103.102.166.224	TCP	54	51853 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
10004	166.963204	192.168.1.8	103.102.166.224	TLSv1.3	1845	Client Hello
10012	167.001519	103.102.166.224	192.168.1.8	TCP	66	[TCP Window Update] 443 → 51853 [ACK] Seq=1 Ack=1 Win=42496 Len=0 SLE=1437 SRE=1792
10013	167.001519	103.102.166.224	192.168.1.8	TCP	54	443 → 51853 [ACK] Seq=1 Ack=1792 Win=40960 Len=0
10014	167.002031	103.102.166.224	192.168.1.8	TLSv1.3	2958	Server Hello, Change Cipher Spec, Application Data
10015	167.002083	192.168.1.8	103.102.166.224	TCP	54	51853 → 443 [ACK] Seq=1792 Ack=2905 Win=65280 Len=0
10016	167.002294	103.102.166.224	192.168.1.8	TLSv1.3	273	Application Data, Application Data, Application Data
10019	167.048396	192.168.1.8	103.102.166.224	TCP	54	51853 → 443 [ACK] Seq=1792 Ack=3124 Win=65280 Len=0
10021	167.081877	192.168.1.8	103.102.166.224	TLSv1.3	118	Change Cipher Spec, Application Data
10022	167.119792	103.102.166.224	192.168.1.8	TLSv1.3	596	Application Data, Application Data
10023	167.119901	192.168.1.8	103.102.166.224	TCP	54	51853 → 443 [ACK] Seq=1856 Ack=3666 Win=64768 Len=0
10929	212.130364	192.168.1.8	103.102.166.224	TCP	55	[TCP Keep-Alive] 51853 → 443 [ACK] Seq=1855 Ack=3666 Win=64768 Len=1
10930	212.170711	103.102.166.224	192.168.1.8	TCP	66	[TCP Keep-Alive ACK] 443 → 51853 [ACK] Seq=3666 Ack=1856 Win=42496 Len=0 SLE=1855 SRE=1856
11245	234.784161	192.168.1.8	103.102.166.224	TCP	54	51853 → 443 [FIN, ACK] Seq=1856 Ack=3666 Win=64768 Len=0
11298	234.823949	103.102.166.224	192.168.1.8	TLSv1.3	78	Application Data
11299	234.823949	103.102.166.224	192.168.1.8	TCP	54	443 → 51853 [FIN, ACK] Seq=3690 Ack=1857 Win=42496 Len=0
11300	234.824012	192.168.1.8	103.102.166.224	TCP	54	51853 → 443 [RST, ACK] Seq=1857 Ack=3690 Win=0 Len=0

```
> Frame 9970: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{FD08F7C8-F41E-4707-A969-6CABA5EC29EC}, id 0
> Ethernet II, Src: 90:10:57:ba:d2:90 (90:10:57:ba:d2:90), Dst: GXIntern_64:e8:68 (b4:3d:08:64:e8:68)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 103.102.166.224
> Transmission Control Protocol, Src Port: 51853, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  b4 3d 08 64 e8 68 90 10  57 ba d2 90 08 00 45 00   ·=·d·h·· W·····E·
0010  00 34 48 1a 40 00 80 06  00 00 c0 a8 01 08 67 66   ·4H·@··· ······gf
0020  a6 e0 ca 8d 01 bb f5 6a  2e 4d 00 00 00 00 80 02   ·······j .M······
0030  ff ff d0 1d 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                             ··
```

EXPERIMENT-24

NETWORK LAYER PROTOCOL HEADER ANALYSIS USING WIRE SHARK - SMTP & ICMP

AIM:-

To analyze capturing of Transport Layer Protocol header analysis using wire shark.

PROCEDURE:-

Step 1: Open wire shark and click on list the available capture interface

Step 2: Choose LAN and click start.

Step 3: Active packets will be displayed.

Step 4: Capture packets & select any IP Address

Step 5: Click on the expression and select IPV4.

Step 6: Select the double equals click apply

Step 7: All the packets will be filtered.

DIAGRAM:-

Time	Source	Destination	Protocol
25034 642.951030	192.168.1.8	142.251.43.36	ICMP
25035 642.956389	142.251.43.36	192.168.1.8	ICMP
25060 643.982005	192.168.1.8	142.251.43.36	SMTP
25061 643.988526	142.251.43.36	192.168.1.8	SMTP

RESULT:-

Hence, the capturing of packets using wire-shark for SMTP & ICMP has been analyzed.

icmp and ip.addr == 142.251.43.36

No.	Time	Source	Destination	Protocol	Length	Info
25034	642.951030	192.168.1.8	142.251.43.36	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 25035)
25035	642.956389	142.251.43.36	192.168.1.8	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=118 (request in 25034)
25060	643.982085	192.168.1.8	142.251.43.36	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 25061)
25061	643.988526	142.251.43.36	192.168.1.8	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=118 (request in 25060)
25062	644.999388	192.168.1.8	142.251.43.36	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 25063)
25063	645.005737	142.251.43.36	192.168.1.8	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=118 (request in 25062)
25064	646.031194	192.168.1.8	142.251.43.36	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 25065)
25065	646.036506	142.251.43.36	192.168.1.8	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=118 (request in 25064)

```
> Frame 25034: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{FD08F7C8-F41E-4707-A969-6CABA5EC29EC}, id 0
> Ethernet II, Src: 90:10:57:ba:d2:90 (90:10:57:ba:d2:90), Dst: GXIntern_64:e8:68 (b4:3d:08:64:e8:68)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 142.251.43.36
> Internet Control Message Protocol
```

```
0000  b4 3d 08 64 e8 68 90 10  57 ba d2 90 08 00 45 00   ·=·d·h·· W·····E·
0010  00 3c b3 ea 00 00 80 01  00 00 c0 a8 01 08 8e fb   ·<······ ········
0020  2b 24 08 00 4d 4f 00 01  00 0c 61 62 63 64 65 66   +$··MO·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```

EXPERIMENT - 25

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

AIM:-

To analyse capturing of Transport Layer Protocol header analysis using wire - Shark - ARP and HTTP.

PROCEDURE:-

Step 1: Open Wire-Shark.
Step 2: Click list available interface, Choose LAN
Step 3: Click start Button, active packets will be displayed
Step 4: Capture the packets and select any IP
Step 5: Select '==' and click apply
Step 6: All packets will be filtered using source data.

DIAGRAM:-

Time	Source	Destination	Protocol	Length
62.151593	SamsungE_e 2:95:b2	90:10:57:ba:d2:90	ARP	42
72.151638	90:10:57:ba:d2:90	SamsungE_e 2:95:b2	ARP	42
26 16.795501	GxIntern_64:e8:68	90:10:57:ba:d2:90	HTTP	288
27 16.795539	90:10:57:ba:d2:90	GxIntern_64:e8:68	HTTP	288

RESULT:-

Hence, the capturing of packets using wire Shark was analysed for ARP and HTTP.

arp

No.	Time	Source	Destination	Protocol	Length	Info
6	2.151593	SamsungE_e2:a5:b2	90:10:57:ba:d2:90	ARP	42	Who has 192.168.1.8? Tell 192.168.1.4
7	2.151638	90:10:57:ba:d2:90	SamsungE_e2:a5:b2	ARP	42	192.168.1.8 is at 90:10:57:ba:d2:90
26	16.795501	GXIntern_64:e8:68	90:10:57:ba:d2:90	ARP	42	Who has 192.168.1.8? Tell 192.168.1.1
27	16.795539	90:10:57:ba:d2:90	GXIntern_64:e8:68	ARP	42	192.168.1.8 is at 90:10:57:ba:d2:90
30	22.834972	a6:23:33:67:b1:f9	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.5
49	31.131239	SamsungE_e2:a5:b2	90:10:57:ba:d2:90	ARP	42	Who has 192.168.1.8? Tell 192.168.1.4
50	31.131282	90:10:57:ba:d2:90	SamsungE_e2:a5:b2	ARP	42	192.168.1.8 is at 90:10:57:ba:d2:90

```
> Frame 7: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{FD08F7C8-F41E-4707-A969-6CABA5EC29EC}, id 0
> Ethernet II, Src: 90:10:57:ba:d2:90 (90:10:57:ba:d2:90), Dst: SamsungE_e2:a5:b2 (b8:bc:5b:e2:a5:b2)
> Address Resolution Protocol (reply)
```