Experiment-6

Implement Wi-Fi Security (WPA2, IP based, MAC Based)

Date: 30-9-24

AIM

Implement Wi-FI Security (WPA2, IP based, MAC Based).

PROCEDURE

Step-1: Switch On the D-Link Router and connect PC using a cable

Step-2: Run IP address of router in any browser

Step-3: Choose the Internet Connection Type

Step-4: Set wireless network name

Step-5: Setup wireless security mode

Step-6: Click Wireless Settings WPA2 Personal set the password Save

Step-7: Go to Network and Internet and connect to the wi-fi-DLink.

Step-8: open browser and check internet is accessible or not.

SOURCECODE

- Connect computer's LAN to wifi Routerhost Port.
- Connect -Ethernet cable (white wire) to Router.

first port and CPU Ethernet Port.

- Now connect the plug of the wifi Router plug and turn on the switch.
- Go to Control Panel > Network & Internet > Network & sharing Center > Change Adapter settings > Ethernet > Properties > Select TCP/IPV4 OK and close
- Go to google and enter the router IP address.
- Login directly.
- Go to wireless, you will get the details.

You can edit the wifi name in Name (SSID) and in security options choose WPA 2-PSK (AES) you can edit the password in Preshared Key. click on apply.

- Get a device and connect to wifi using password.
- Go to status. After connecting check the Active client table under the Active client table you will find source MAC address

first port and CPU Ethernet Port.

- Now connect the plug of the wifi Router Plug and turn on the switch.

- Go to Control Panel > Network & Internet > Network & sharing Center > Change Adapter Settings > Ethernet > Properties > Select TCP/IPV4 OK and close

- Go to google and enter the router IP address.

- Login directly.

- Go to wireless, you will get the details.

You can edit the wifi name in Name (SSID) and in security options choose WPA 2-PSK (AES) you can edit the password in Preshared Key. Click on apply.

- Get a device and connect to wifi using password.

- Go to status. After connecting check the Active client table under the Active client table you will find source MAC address

destination MAC address, copy both the addresses and remove colons.

• Now in the phone search in chrome and see the connectivity.

• Now go to Advanced and Mac filter change to deny and outgoing. Enter the source and incoming destination MAC addresses and Add

OUTPUT

If there are any existing under current MAC filter Table remove them. Now it will get blocked.

• You can test it by searching something in the device.

• You can now allow by clicking on allow and add for outgoing and incoming.

Experiment-6

Implement Wi-Fi Security (WPA2, IP based, MAC Based)

Date: 30/11/24

[M]

plement Wi-FI Security (WPA2, IP based, MAC Based).

ROCEDURE

ep-1: Switch On the D-Link Router and connect PC using a cable

ep-2: Run IP address of router in any browser

ep-3: Choose the Internet Connection Type

ep-4: Set wireless network name

ep-5: Setup wireless security mode

ep-6: Click Wireless Settings WPA2 Personal set the password Save

tep-7: Go to Network and Internet and connect to the wi-fi-DLink.

tep-8: open browser and check internet is accessible or not.

SOURCECODE
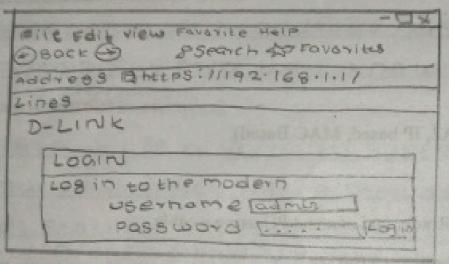
Step1: open control panel, click on Network and Internet, next click on Network and Sharing Centre.

step 2: In network and Sharing centre, select change/adapter settings click on it.

Step3: click on Ethernet, Click properties, Select Internet protocol version 4 (TCP/IPv4) click OK.
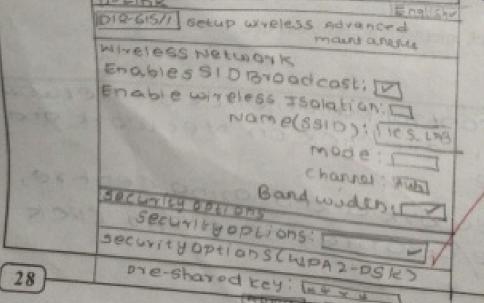
Step 4: Select the IP address of wifi rout-er in the Google chrome Tab.

Step 5: The username will be Admin there is default password. Now click on login button.

```
                                          - □ ✕
File Edit View Favorite Help
← Back →        ₽Search ☆ Favorites
Address ⊡ https://192.168.1.1/
Lines
   D-LINK
     ┌──────────────────────────────────┐
     │ LOGIN                            │
     ├──────────────────────────────────┤
     │ Log in to the modern            │
     │    username [admin]             │
     │    password [········] [Login]  │
     └──────────────────────────────────┘
```

Step 6: The information about the router device.

Step 7: Now, select the wireless tab on the menu.

Step 8: modify the name of the device, Change the password click apply button.

```
D-Link                                      English
[DIR-615/1] setup wireless Advanced
                            maintenance
  Wireless Network
  Enables SID Broadcast: ☑
  Enable wireless Isolation: ☐
           Name(SSID): [ICS LNS]
                 mode: [    ]
              Channel: [Auto]
           Band width: [    ]
   Security options
      security options: [    ]
   security options (WPA2-PSK)
      pre-shared key: [#####]
      [Apply] [Save]
```

Step 9: Select go to Advance tab, select mac filters

Step 10: Default policy will be default allow, change it to the deny state both incoming and outgoing policy.

Step 11: copy the source and Destination mac address from the Status tab by removing the colon symbol.

Step 12: click on advance tab select mac filters and paste the source and Destination mac address and select the deny button for both incoming and outgoing policy.

D-LINK

Advanced

MAC Filtering

Default Policy

MAC Filter

Outgoing Default Policy: ⊙Deny ⊙allow

Incoming Default Policy: ⊙Deny ⊙allow

Apply changes

Add Filter

Direction [outgoing▾]
Action ⊙Deny ⊙allow

Source MAC [_____]

Destination MAC [_____]

[Add]

Current MAC Filter table

Select	Direction	SourceMAC	Destination MAC	
☐	Outgoing	cD:18:93:16e:26	H	allow
☐	Incoming	cD:18:93:6e:126	H	deny

🔍 cmrit hyderabad 🌵 📷

All   Images   Maps   News   Videos

CMR Institute of
Technology

Institute of technology
in Telangana

CMR

(Overview)   (Packages)   (Rankings)

📞   ↗   ◁   🕐

calls   Direction   share   website

Step 13: click on Add button.

Step 14: Information is available in curr-
-nt mac Filter Table.
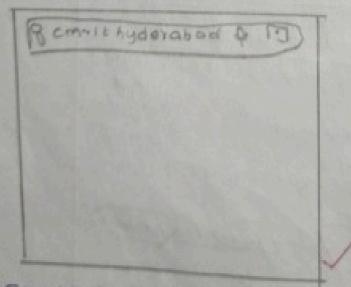
Step 15: After applied the mac based
filter, check the mobile device
connected through WiFi-Route

D-LINK   Select Language [English]

	MAC Filtering
	Default policy
MAC FILTER	

[Apply changes]

Add Filter
  Direction [Outgoing v]
    Action ⊙Deny ○Allow
    Source MAC: [   ]
    Destination MAC: [   ]

[Add]

Current Mac Filter Table

Select	Direction	Source MAC	Destination MAC	Action
☐	outgoing	c0:18:03:be:fb:2b	00:15:e0:25:t	deny
☐	outgoing	c0:18:03:be:fb:2b	7c:25:90:de	allow
☐	Incoming	c0:18:03:be:fb:2b	7e:25:90:	deny

cmrit hyderabad

Step 17: For IP Filter select the option IP/Port
Filter.

Step 18: By default it will be permit, select
Deny option

Step 19: In direction select with direction down
Step 20: paste source ip address and destina Stream?
-tion ip address, in status tab.
Step 21: click on Apply changes.

D-LINK   Select Language [English]

IP/Port Filtering

IP/Port Filter

Default Action Status
outgoing Default Action ⦿permit ○deny
Incoming Default Action ○permit ⦿deny

Rule configuration
Protocol [TCP]
Rule Action ⦿permit ○deny

OUTPUT

Current Filter Table
Rule Protocol Source IP/mask DestIP DPort Direction
      195.168.02/ 192.118.0.0 enable   ACSd
deny IP 255.255.255.155 255.255.255.45 upstream [✓] [delete]
      192.168.0.2/
permit IP 255.255.255.03 255.255.255 down
      192.168.0.2/   Stream [✓] [delete]
deny ip 192.118.0.2/ 255.255.25 upstream [✓] [delete]
deny tcp 255.255.255.155   255.255.255 down
      192.118.47/   255- 255.255 Down [✓] [delete]

Step 22: IP based wi-fi secure provide to the
connected device.

D-Link   Select Language
                               [English ✓]

ActiveClient Table

ActiveClient Table

Active wired client Table

name   ipAddress   MAcad
ausvru   192.168.0.2   -dres
                          Co.18.03:
                          be:76:26

Active wireless client Table

Name   IP Address
godmi-10-folora   192.168.0

Mac address
76:35:80:du:2e:81

[Refresh]