

Wi-Fi Technology Fundamentals



WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

Module-1

Introduction and History of WiFi

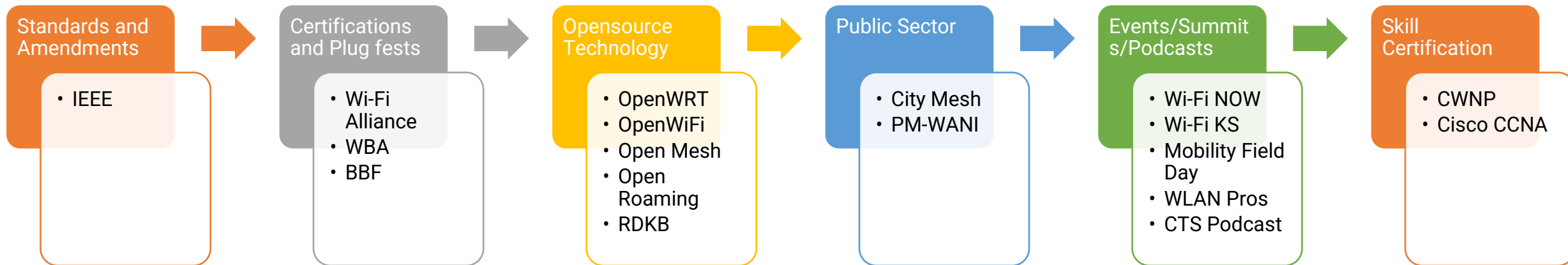
Session-1d

Basic Functional Building Blocks of a Wi-Fi Router

Last Session Recap.....



Module-1 Introduction and History of WiFi Session-1c WLAN Standards/Amendments and Alphabet Soup



How to Stay Connected?

Access Course Webpage



[Click here: Wi-Fi Technology Fundamentals Course \(candelatech.com\)](https://candelatech.com)

- ✓ Access course notes, slides, video recordings

Register to Get Updates



[Click Here: Registration \(zoho.in\)](https://zoho.in)

- ✓ Provide basic contact info to get calendar invites, reminders and updates about the material and sessions.

Join Whatsapp Group



[Click here: WhatsApp Group Invite](#)

- ✓ Provide basic contact info to get whatsapp messages about calendar invites, reminders and updates about the material and sessions.

Today's Session...



Module-1

Introduction and History of WiFi

Session-1d

Basic Functional Building Blocks of a WiFi Router

Wi-Fi Connection



Types of WiFi Routers/APs

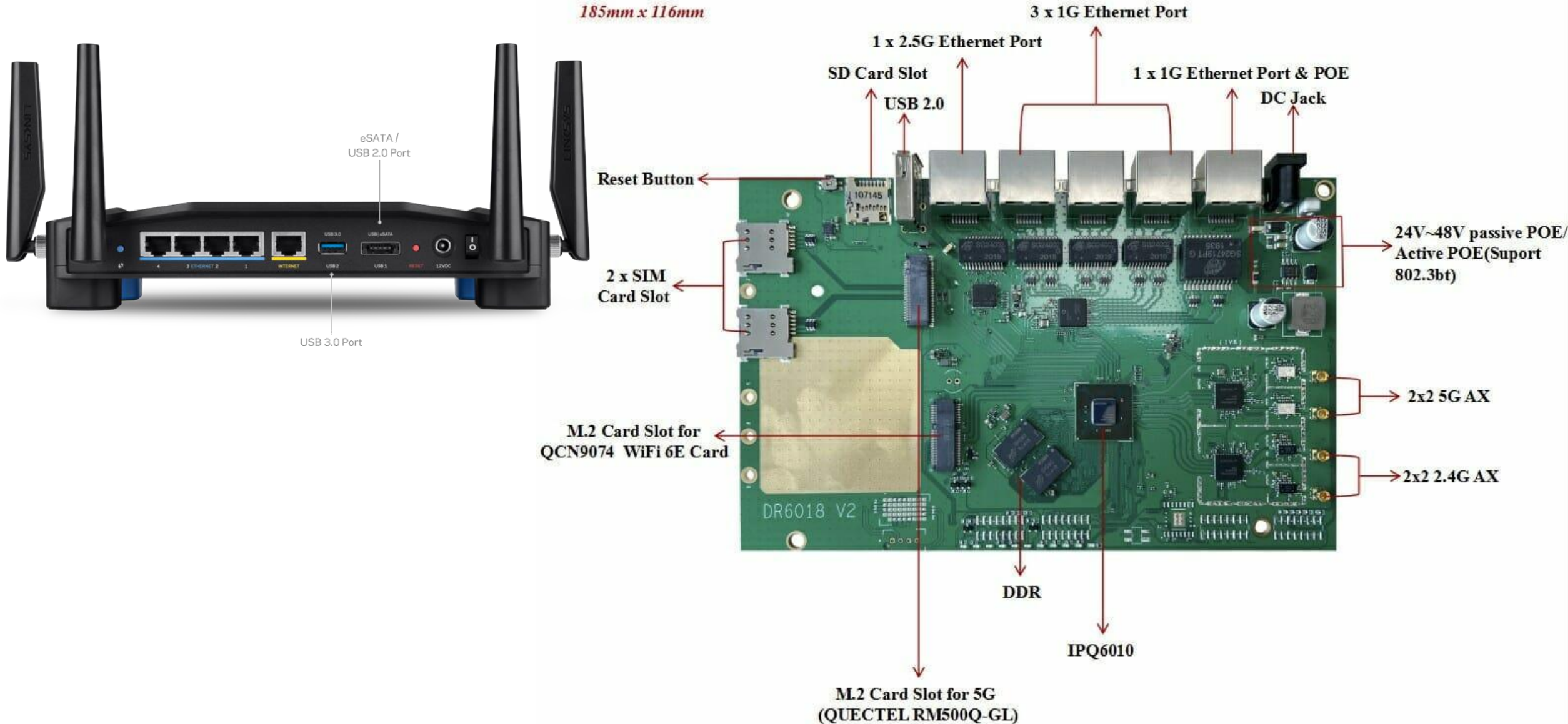


Residential
Wi-Fi Router

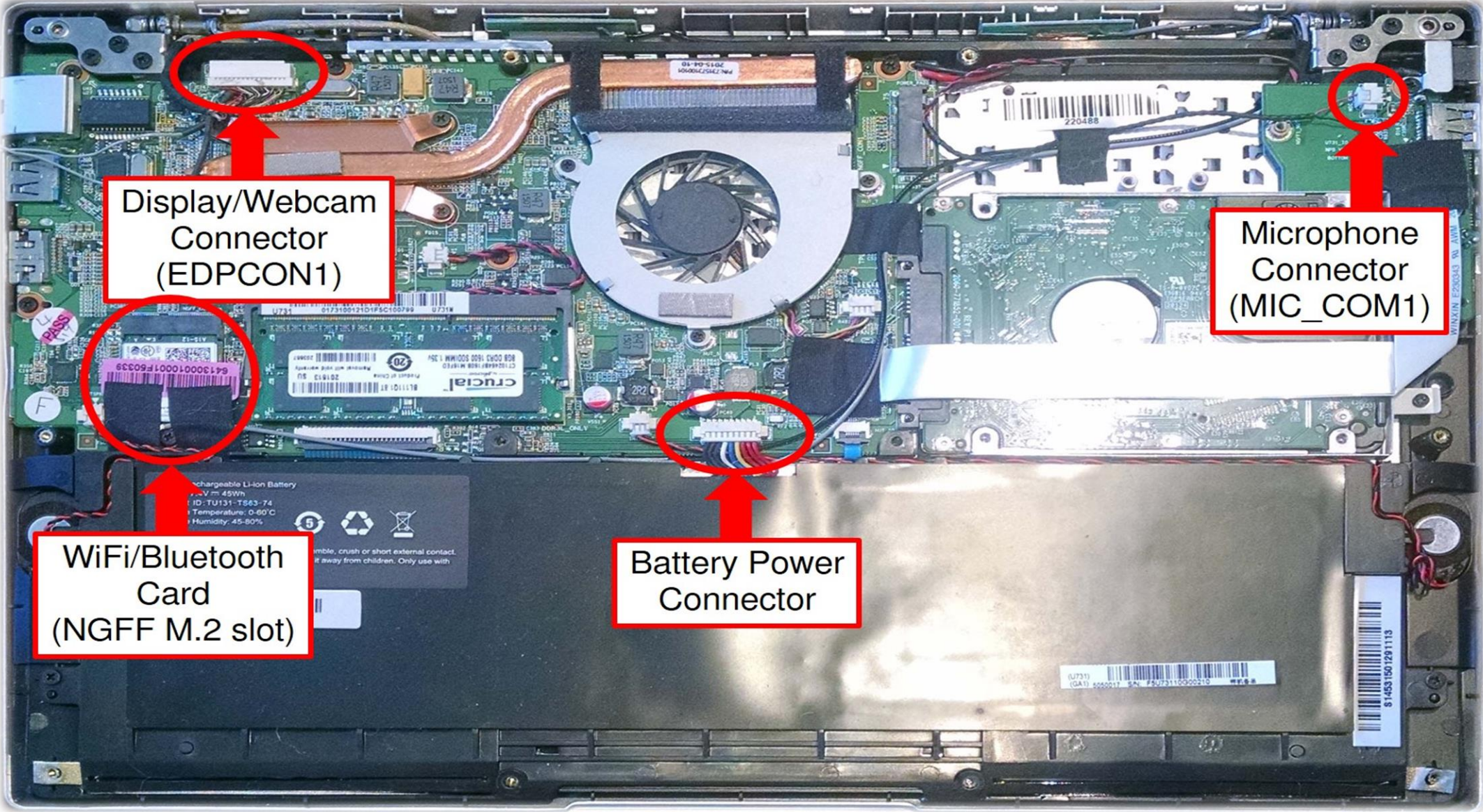


Enterprise
Wi-Fi Access Point

What is Inside the Wi-Fi Router?



WiFi Client



Display/Webcam
Connector
(EDPCON1)

Microphone
Connector
(MIC_COM1)

WiFi/Bluetooth
Card
(NGFF M.2 slot)

Battery Power
Connector

Inside the Wi-Fi Access Point

<https://fccid.io/MSQ-RTAX5600/Internal-Photos/Internal-Photos-5516748>

🔊 ☆ 📄

FCC ID.io

Blog

Search

External Photos

External Photos

Alternate Views:

PDF [Zoom]

Download [PDF]



3

of 43

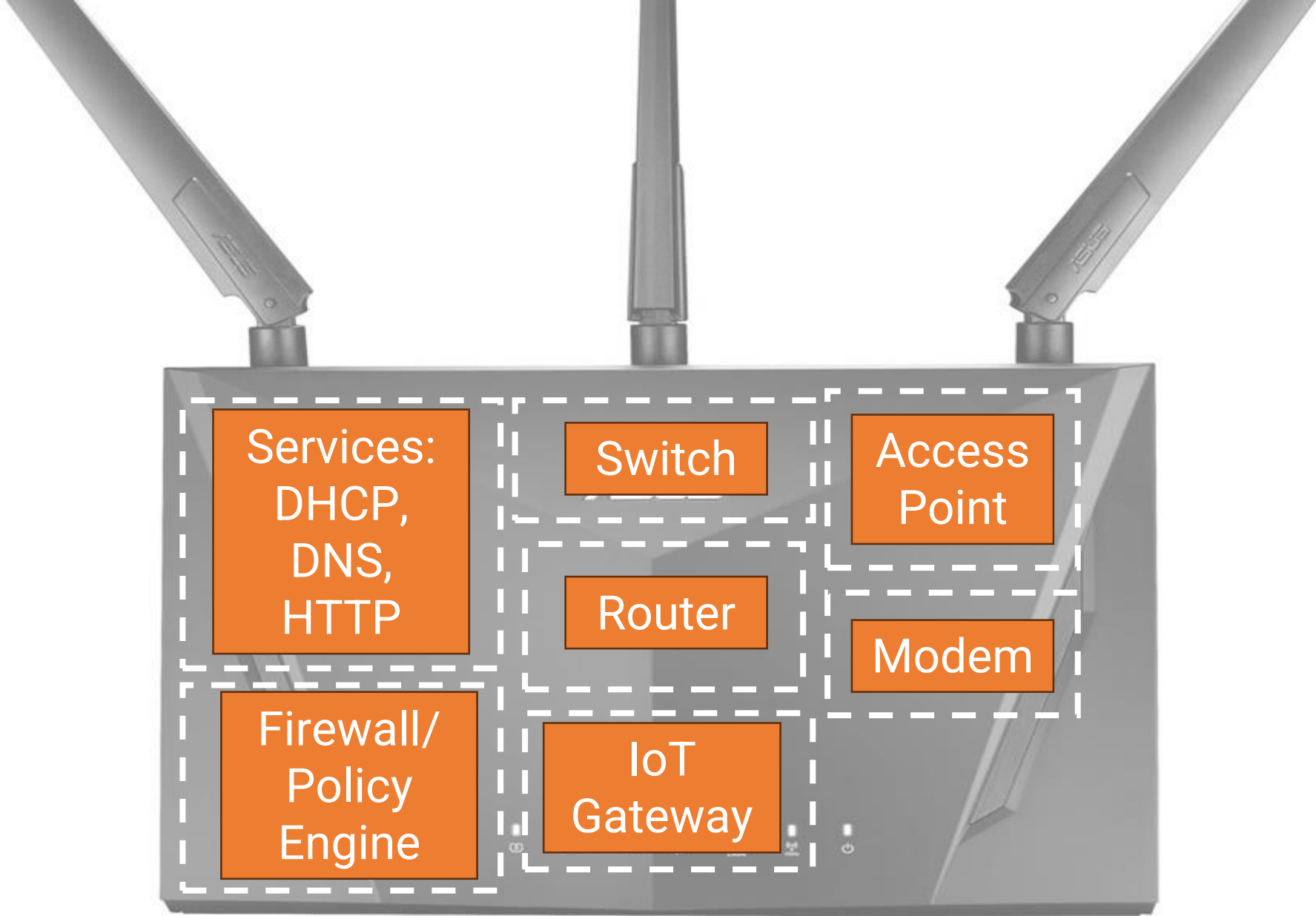


Automatic Zoom

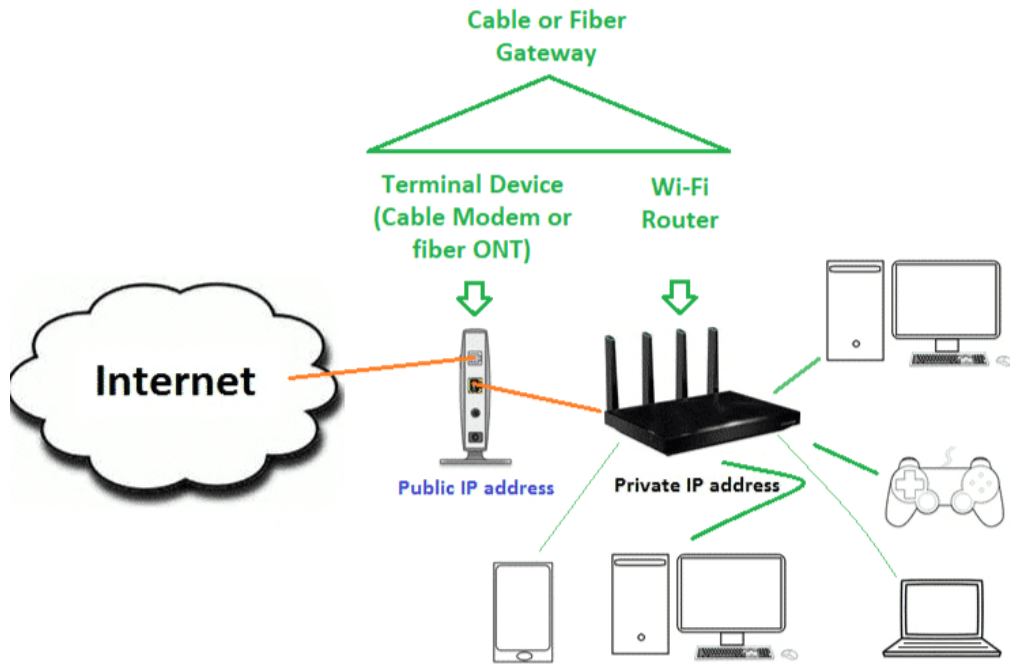


<https://fccid.io/>

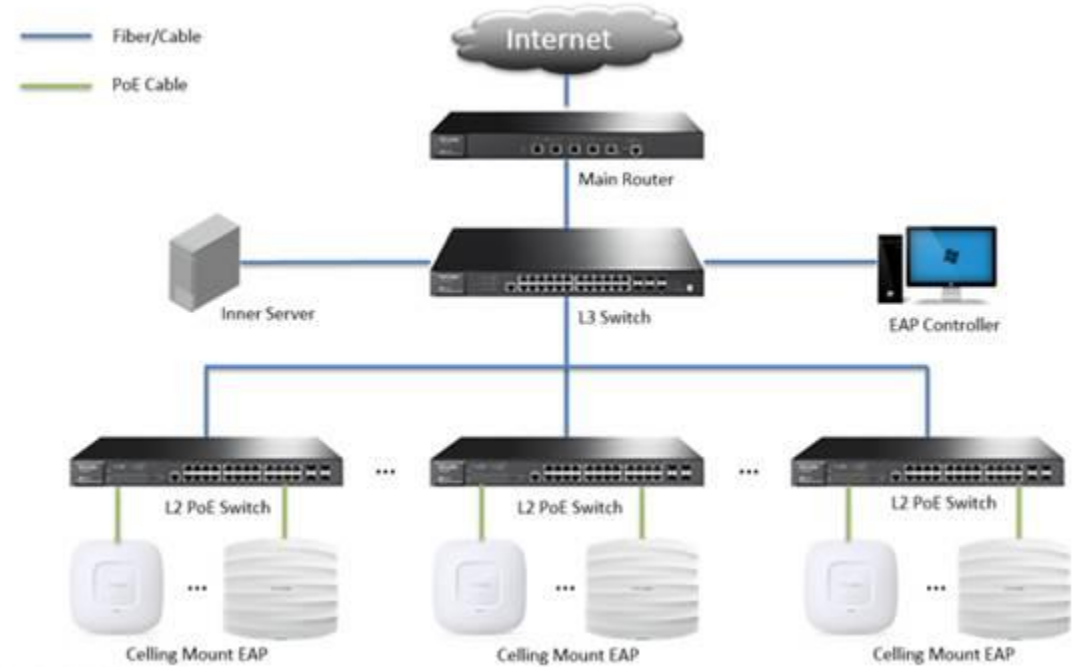
A Modern Day Wi-Fi Router



Types of WiFi Network Installations



Residential WiFi Network













Enterprise WiFi Network

The Configuration Interface of a Residential Router




The screenshot displays the configuration interface for the ASUS Rapture GT-AXE 11000 router. The interface is dark-themed with red accents. At the top, the router's name 'RAPTURE GT-AXE 11000' is prominently displayed, along with the 'REPUBLIC OF GAMERS' logo. A 'Logout' button and a language dropdown set to 'English' are visible in the top right. Below the header, the current 'Operation Mode' is 'Access Point (AP) mode' and the 'Firmware Version' is '3.0.0.4.388.23482'. The SSID settings are listed as 'ASUS_2G', 'ASUS_5G', and 'ASUS_6G'. A navigation sidebar on the left includes 'Quick Internet Setup', 'General' (with sub-items: Dashboard, AiMesh, Game Radar, WiFi Radar), 'Advanced Settings' (with sub-items: Network Map, Wireless, Guest Network, LAN, USB Application, AiCloud 2.0, Administration, System Log, Network Tools), and 'System Status'. The main content area is divided into several sections: 'Parent AP status : AP Mode' with a globe icon; a central network diagram showing 2.4 GHz, 5 GHz, and 6 GHz bands connected to a central router icon, with 'WPA2-Personal' security indicated; 'Clients: 0' with a 'View List' button; 'AiMesh Node: 0'; and two 'USB 3.0' ports, both showing 'No Device'. On the right, the 'System Status' panel is open, showing settings for three wireless bands: 2.4 GHz, 5 GHz, and 6 GHz. Each band has its own 'Network Name (SSID)', 'Authentication Method' (set to 'WPA2-Personal'), and 'WPA Encryption' (set to 'AES'). The 2.4 GHz SSID is 'ASUS_2G', 5 GHz is 'ASUS_5G', and 6 GHz is 'ASUS_6G'. The WPA-PSK key field is masked with dots.

Enterprise AP Configuration


-  Network San Francisco ▾
-  Network-wide
-  Security & SD-WAN
-  Switching
-  Wireless
-  Systems Manager
-  Cameras
-  Sensors
-  Insight
-  Organization

Health

UPLINKS

 2/2 healthy

SECURITY APPLIANCES

 2/2 healthy

SWITCHES

 8/9 healthy

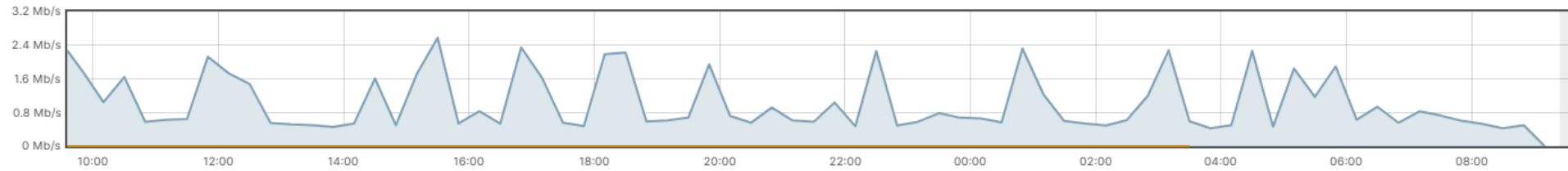
ACCESS POINTS

 9/9 healthy

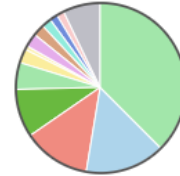
Clients

all ▾ for the last day ▾

10.46 GB (↓ 3.47 GB, ↑ 6.99 GB)



Applications















[More »](#)

Download as ▾

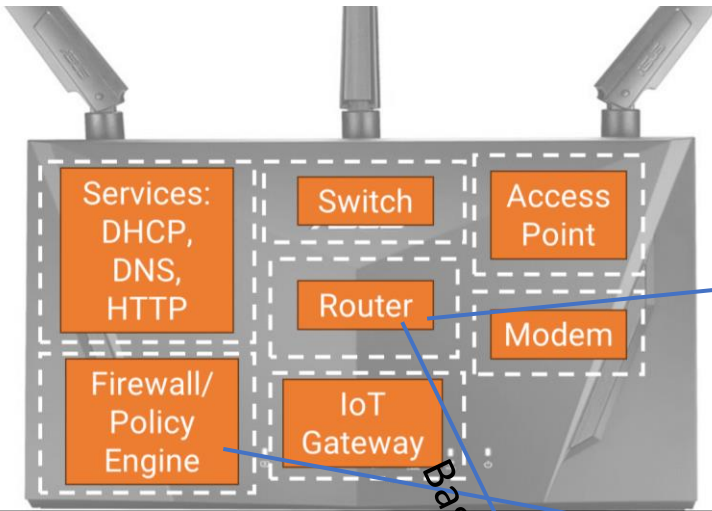
Policy ▾

Search... ▾

26 clients

<input type="checkbox"/>	Status	Description	Connected To	Usage	Performance	User	Port	VLAN	Policy	Recent SSID	Capable Wi-Fi standards	Onboarding	Capable channel width	Client type, OS	First Seen	802.1X policy	Systems Manager	IPv4 address	IPv6 address	IPv6 address
<input type="checkbox"/>		Samuel Morse	CAMPUS-SFO-1.1-MR46	7 KB	 100%			40	normal	CMP-CAMPUS-SFO-Lobby	802.11ac - 2.4 and 5 GHz	N/A 	80 MHz	Windows 10	Feb 1 18:51	normal		172.16.40.3		fe80:0:0:0:0:0:0:0:0
<input type="checkbox"/>		00:ce:39:c8:76:d9	CAMPUS-SFO-IDF1.1.1-MS390-24UX	51 KB	N/A 		4	10	normal			N/A 		Other	Sep 6 08:55	normal	Yes	169.254.87.53		
<input type="checkbox"/>		campus-sfo-1-6-cw9166i-cc9c3eec2640	CAMPUS-SFO-MDF1.1-MS425-16-CORE2	178.2 MB	N/A 				normal			N/A 		Meraki	Jul 12 13:20	normal		172.16.1.2		
<input type="checkbox"/>		a0:3d:6e:30:12:c7	CAMPUS-SFO-IDF2.1.1-MS355-	395.8 MB	N/A 		24	1	normal			N/A 		Other	Jun 10 11:24	normal		172.16.1.201		

Difference Between Wi-Fi Router and Access Point

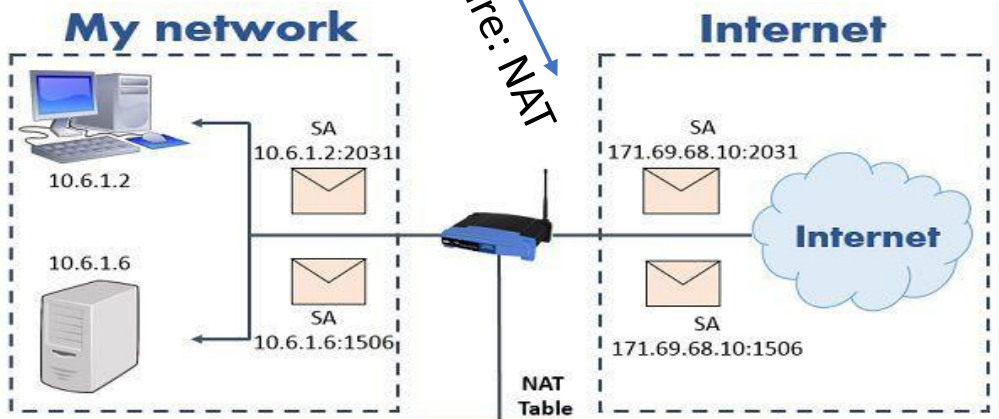


Basic Feature: DHCP

DHCP client DHCP server



Advanced Features



Inside Local IPv4 Address	Inside Global IPv4 Address
10.6.1.2:2031	171.69.68.10:2031
10.6.1.6:1506	171.69.68.10:1506
10.6.1.6:131	171.69.68.10:2032

Parental Control ✕

① Click "Edit", and name the device

Device Name: WQ-20151029DCJX Edit

② Setup Internet accessible time

Internet Accessible Time: 19:00 ~ 21:00

Repeat: Every Day Specified Days

Sun. Mon. Tue. Wed.
 Thur. Fri. Sat.

③ Setup repeat time of this function

④ Enable website limit

Website Limit:

⑤ Choose control mode

Access Control: Blacklist White List

Forbidden Websites:

⑥ Enter the key words of the website, and delimit them with ","

Please enter the key words of the websites, and separate them with ",". For example: "eHow,google" means that only ehow and google are forbidden.

⑦ Click "Save"

Save Cancel

What is Wireshark?




What is Wireshark?



by @SecurityGuill


What is Wireshark?




- Wireshark is the world's leading **network traffic analyzer**, and an essential tool for any security professional or systems admin. A network packet analyzer will try to **capture network packets** and tries to **display that packet data** as detailed as possible.

- This **free** software lets you analyze network traffic in **real time**, and is often the best tool for **troubleshooting issues** on your network.

Some features

- **Multiplatform** (Windows, UNIX/Linux, ...).
- Capture live packet data from a **network interface (or more)**. 
- Open **files containing packet data** captured with tcpdump/WinDUMP, & many **other packet capture programs**.
- Display packets with **very detailed protocol information**.
- **Filter & search** for packets on many criteria. Create various **statistics**.

Some reasons people use Wireshark

- Network administrators use it to **troubleshoot network problems**, monitoring, ...
- QA engineers use it to **verify network application**.
- Network security engineers use it to examine **security problems**.
- Developers use it to **debug protocol implementations**. 

What Wireshark is not

- Wireshark **isn't an intrusion detection system (IDS)**. It will not warn you when someone does **stranges things** on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might **help you figure out** what is really going on.
- Wireshark will not **manipulate things on the network**, it will only "measure" things from it. **Wireshark doesn't send packets on the network**.

 Follow @SecurityGuill on **Twitter** for more about **Infosec / Cybersecurity**

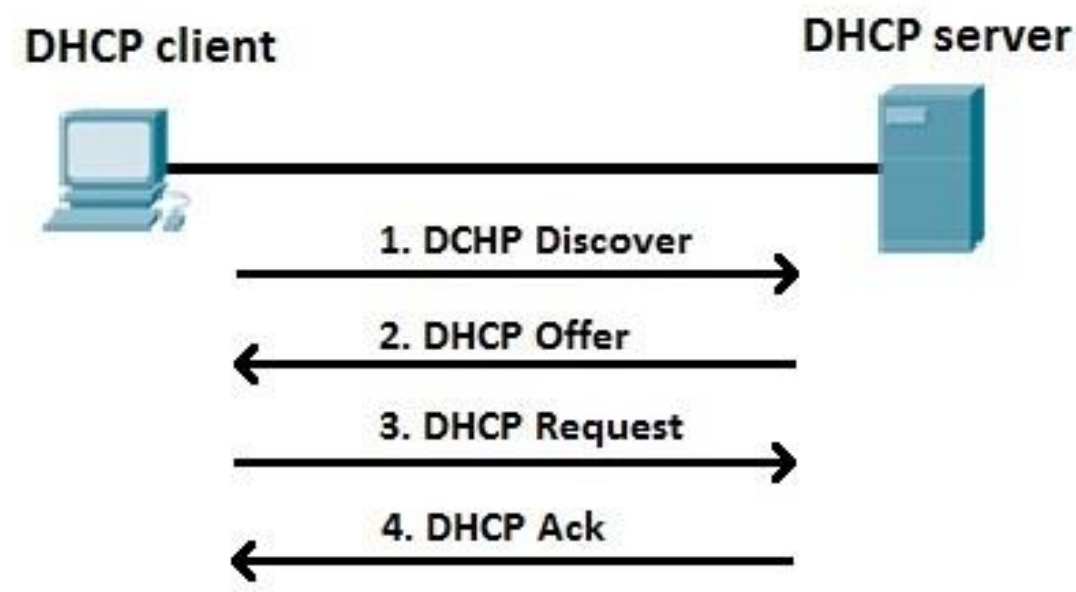
DHCP Packet Capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
19	0.266326	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction
28	0.282418	192.168.90.217	192.168.90.227	DHCP	352	DHCP Offer - Transaction
29	0.294187	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction
30	0.313803	192.168.90.217	192.168.90.227	DHCP	352	DHCP ACK - Transaction

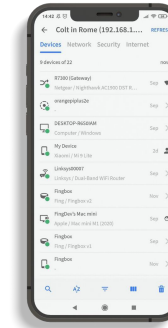
```
> Frame 29: 370 bytes on wire (2960 bits), 370 bytes captured
> Ethernet II, Src: d4:1b:81:3e:80:b5 (d4:1b:81:3e:80:b5), Ds
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Request)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x169f40cc
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: d4:1b:81:3e:80:b5 (d4:1b:81:3e:80:b5)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  v Option: (50) Requested IP Address (192.168.90.227)
    Length: 4
    Requested IP Address: 192.168.90.227
  > Option: (54) DHCP Server Identifier (192.168.90.217)
  > Option: (12) Host Name
  > Option: (81) Client Fully Qualified Domain Name
  > Option: (60) Vendor class identifier
```



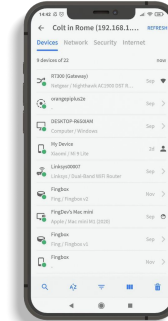
```
0000 ff ff ff ff ff ff d4 1b 81 3e 80 b5 08 00 45 00 ...
0010 01 64 ae 87 00 00 80 11 8b 02 00 00 00 00 ff ff ...d...
0020 ff ff 00 44 00 43 01 50 e1 19 01 01 06 00 16 9f ...D...
```


NAT/PAT Packet Capture

Public Network | Private Network

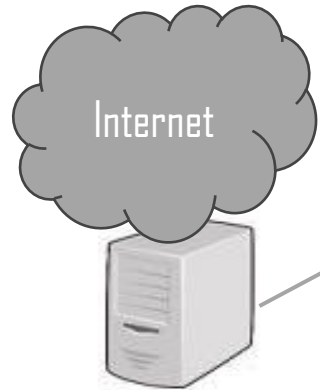


Private IP:
192.168.1.53



Private IP:
192.168.1.82

172.16.222.41	18.189.85.200	TCP	2962 32628 → 5201 [PSH, ACK] Seq=...
172.16.222.41	18.189.85.200	TCP	2962 32628 → 5201 [PSH, ACK] Seq=...
172.16.222.41	18.189.85.200	TCP	2962 32628 → 5201 [PSH, ACK] Seq=...
172.16.222.41	18.189.85.200	TCP	1514 32628 → 5201 [PSH, ACK] Seq=...
172.16.222.41	18.189.85.200	TCP	2962 32628 → 5201 [PSH, ACK] Seq=...
172.16.222.41	18.189.85.200	TCP	2962 32628 → 5201 [PSH, ACK] Seq=...
172.16.222.41	18.189.85.200	TCP	2962 32628 → 5201 [PSH, ACK] Seq=...
172.16.222.41	18.189.85.200	TCP	2962 32628 → 5201 [PSH, ACK] Seq=...
172.16.222.41	18.189.85.200	TCP	1514 32628 → 5201 [ACK] Seq=579...
172.16.222.41	18.189.85.200	TCP	1514 32628 → 5201 [PSH, ACK] Seq=...
172.16.222.41	18.189.85.200	TCP	2362 [TCP Window Full] 32628 → ...
172.16.222.41	18.189.85.200	TCP	194 [TCP Window Full] 32628 → ...
172.16.222.41	18.189.85.200	TCP	66 [TCP Keep-Alive] 32628 → ...
172.16.222.41	18.189.85.200	TCP	66 [TCP Keep-Alive] 32628 → ...
172.16.222.41	18.189.85.200	TCP	74 22898 → 5201 [SYN] Seq=0...
172.16.222.41	18.189.85.200	TCP	66 22898 → 5201 [ACK] Seq=1 A...
172.16.222.41	18.189.85.200	TCP	126 22898 → 5201 [PSH, ACK] Seq=...
172.16.222.41	18.189.85.200	TCP	2962 22898 → 5201 [PSH, ACK] Seq=...
172.16.222.41	18.189.85.200	TCP	1514 22898 → 5201 [ACK] Seq=295...
172.16.222.41	18.189.85.200	TCP	1514 22898 → 5201 [PSH, ACK] Seq=...
172.16.222.41	18.189.85.200	TCP	2962 22898 → 5201 [PSH, ACK] Seq=...
172.16.222.41	18.189.85.200	TCP	1514 22898 → 5201 [ACK] Seq=874...
172.16.222.41	18.189.85.200	TCP	1514 22898 → 5201 [PSH, ACK] Seq=...

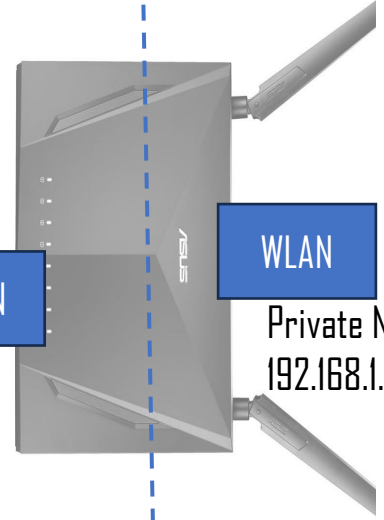


Server IP:
172.16.222.41

Public IP:
18.189.85.200

NAT Table

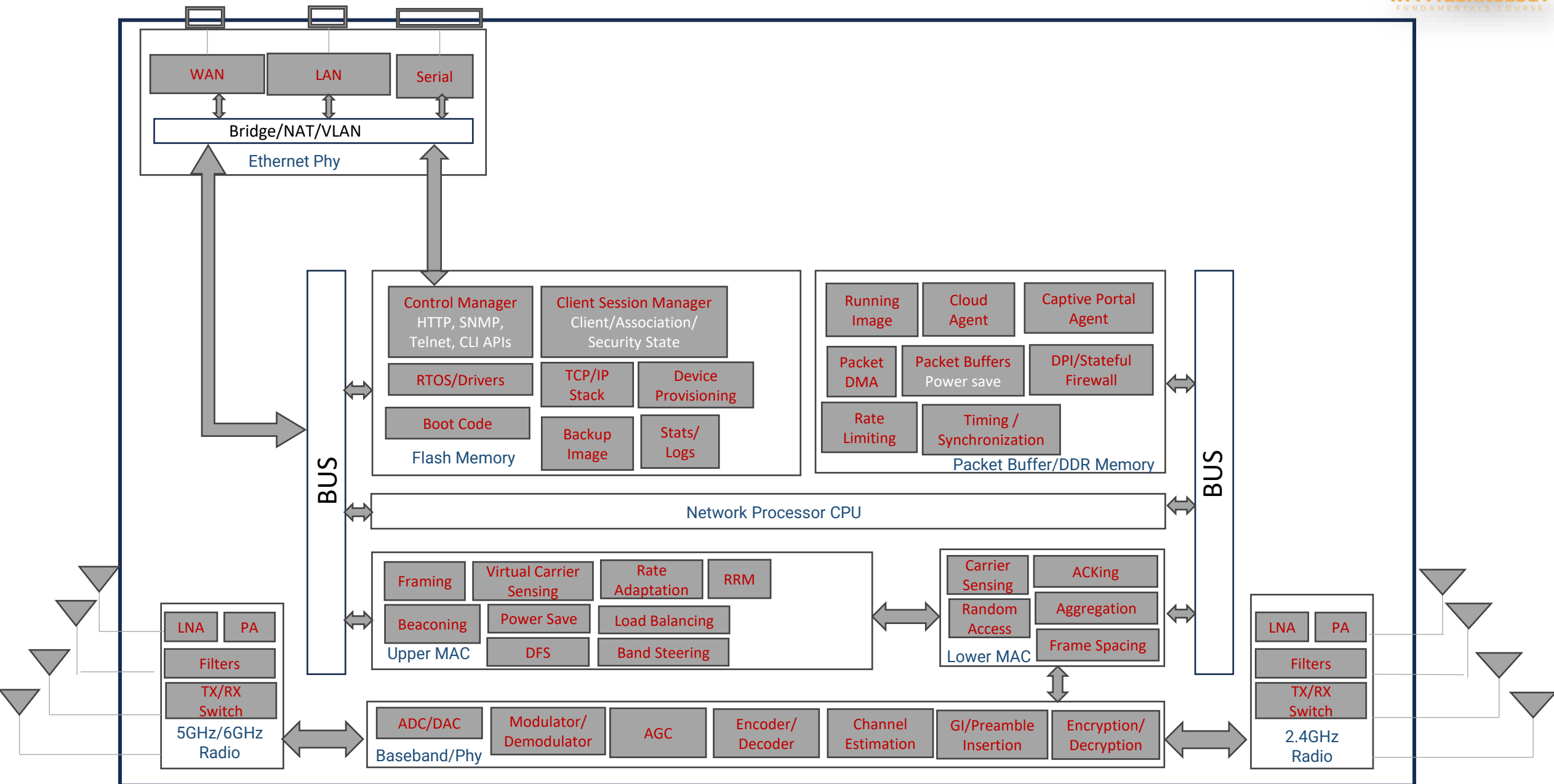
Public Address	Private Address
18.189.85.200:32628	192.168.1.53
18.189.85.200:22898	192.168.1.82



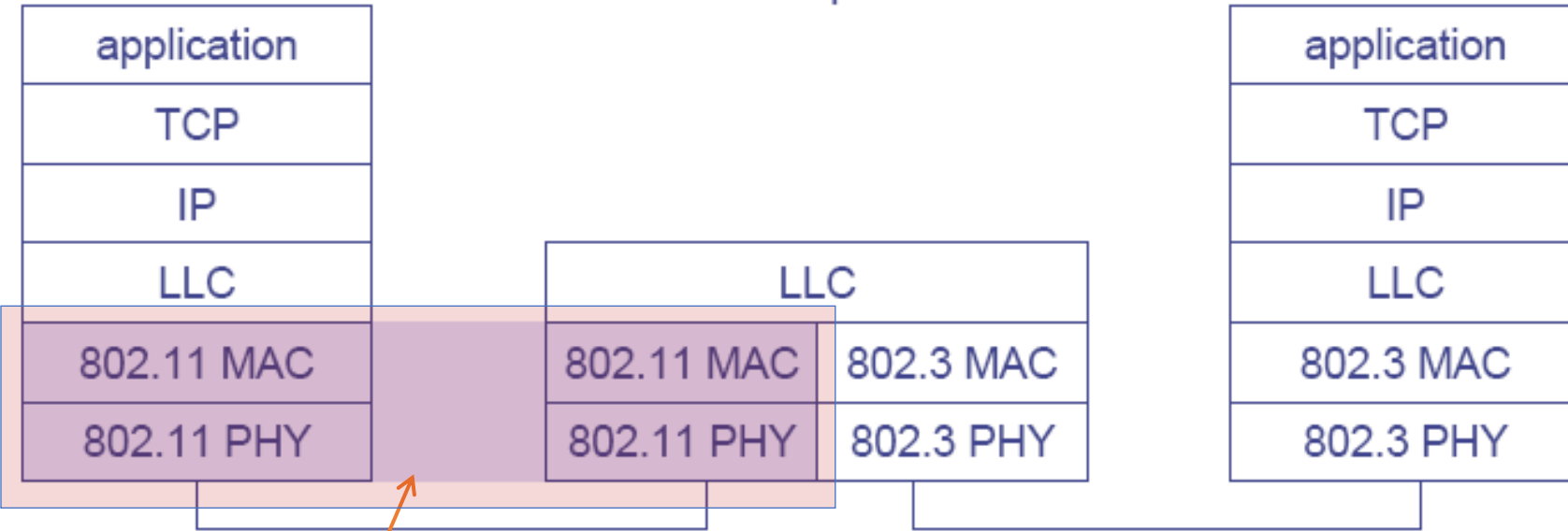
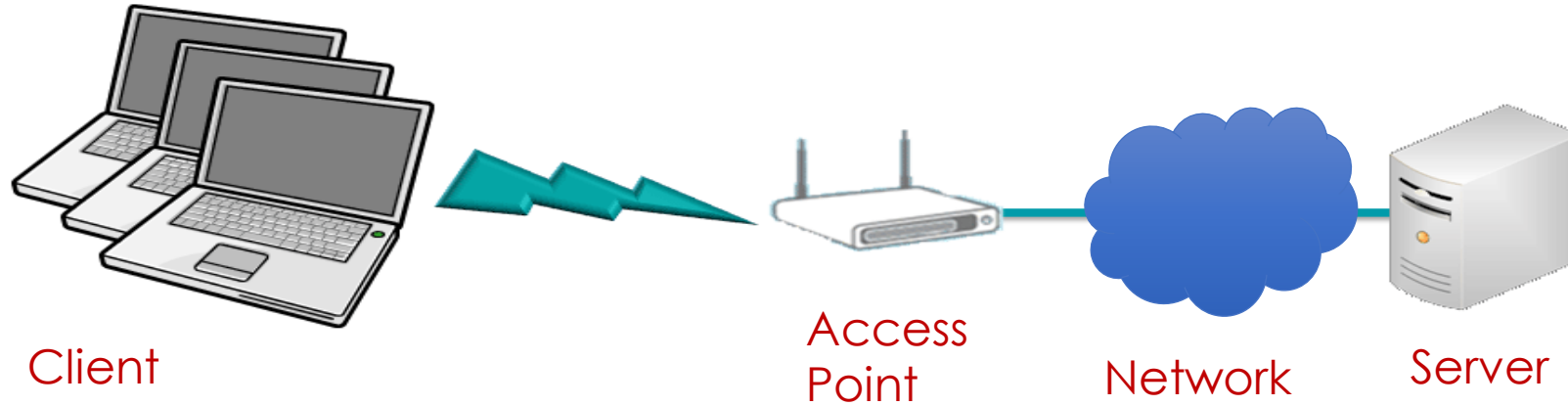
Private Network:
192.168.1.X

18.189.85.200	192.168.1.53	TCP	162 5201 → 32628 [ACK]
18.189.85.200	192.168.1.53	TCP	162 5201 → 32628 [ACK]
18.189.85.200	192.168.1.53	TCP	252 5201 → 32628 [ACK]
18.189.85.200	192.168.1.53	TCP	162 5201 → 32628 [ACK]
18.189.85.200	192.168.1.53	TCP	162 5201 → 32628 [ACK]
18.189.85.200	192.168.1.53	TCP	162 5201 → 32628 [ACK]
18.189.85.200	192.168.1.53	TCP	162 5201 → 32628 [ACK]
18.189.85.200	192.168.1.53	TCP	162 [TCP ZeroWindow]
18.189.85.200	192.168.1.53	TCP	162 [TCP ZeroWindow]
18.189.85.200	192.168.1.82	TCP	170 5201 → 22898 [SYN]
18.189.85.200	192.168.1.82	TCP	162 5201 → 22898 [ACK]
18.189.85.200	192.168.1.82	TCP	162 5201 → 22898 [ACK]
18.189.85.200	192.168.1.82	TCP	162 5201 → 22898 [ACK]
18.189.85.200	192.168.1.82	TCP	404 5201 → 22898 [ACK]
18.189.85.200	192.168.1.82	TCP	328 5201 → 22898 [ACK]
18.189.85.200	192.168.1.82	TCP	328 5201 → 22898 [ACK]
18.189.85.200	192.168.1.82	TCP	162 5201 → 22898 [ACK]
18.189.85.200	192.168.1.82	TCP	162 5201 → 22898 [ACK]

Anatomy/Functional Block Diagram of Enterprise WiFi Access Point



WiFi Infrastructure Network



WiFi AP Protocol Scope

Module 2
WLAN PHY

Module 3
WLAN MAC

Module 4
Security

Module 5
Advanced Topics

Module 6
Troubleshooting

Some References

What is Wireshark and how it works

<https://www.youtube.com/watch?app=desktop&v=Lb-PJl9u3z8>

Instant Demo of Enterprise Wi-Fi network Management

<https://meraki.cisco.com/form/instant-demo/>

FCC ID Website

<https://fccid.io/>

Wireshark Website

<https://www.wireshark.org/>

NAT and PAT explained

<https://www.youtube.com/watch?v=wg8Hosr20yw>

How DHCP Works

<https://www.youtube.com/watch?v=IUOVSIKj6GU>

Wireshark Masterclass

<https://www.youtube.com/watch?v=OU-A2EmVrKQ&list=PLW8bTPfXNGdC5Co0VnBK1yVzAwSSphzpj>



QUIZ!

TIME

Quiz 1c Results

Number of participants - 231



**Vysyaraju
Manideepika**

