WiFi 802.11 Fundamentals

altran

Part of Capgemini

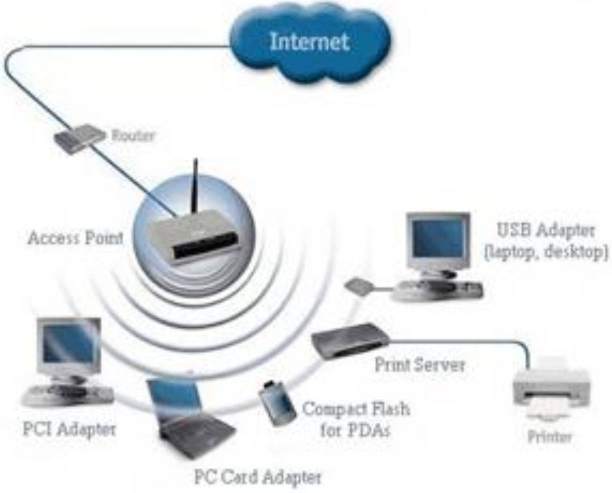
Agenda

- Wi-Fi Technology Overview and Standards
- 802.11n, 802.11ac and 802.11ax
- Wi-Fi Infrastructure (Access Point) architecture
- Wi-Fi authentication & Security
- - Wi-Fi Hotspot 2.0/Offload, WPA2, WPA3?, SIM-AKA, Wi-Gig
- Other usage - Wi-Fi Direct, Location services

Wi-Fi Technology Overview and Standards

Wi-Fi Introduction

“There was small bands of unused spectrum in 900 MHz, 2.4 Mhz and 5.8 GHz. FCC made it unlicensed for public innovation …it turned out to be a very forwarded thinking decision as Wi-Fi as indoor internet access is the de facto access today with more Wi-Fi devices than human population on earth. Wi-Fi uses unlicensed spectrum in 2.4 GHz and 5.8 GHz”

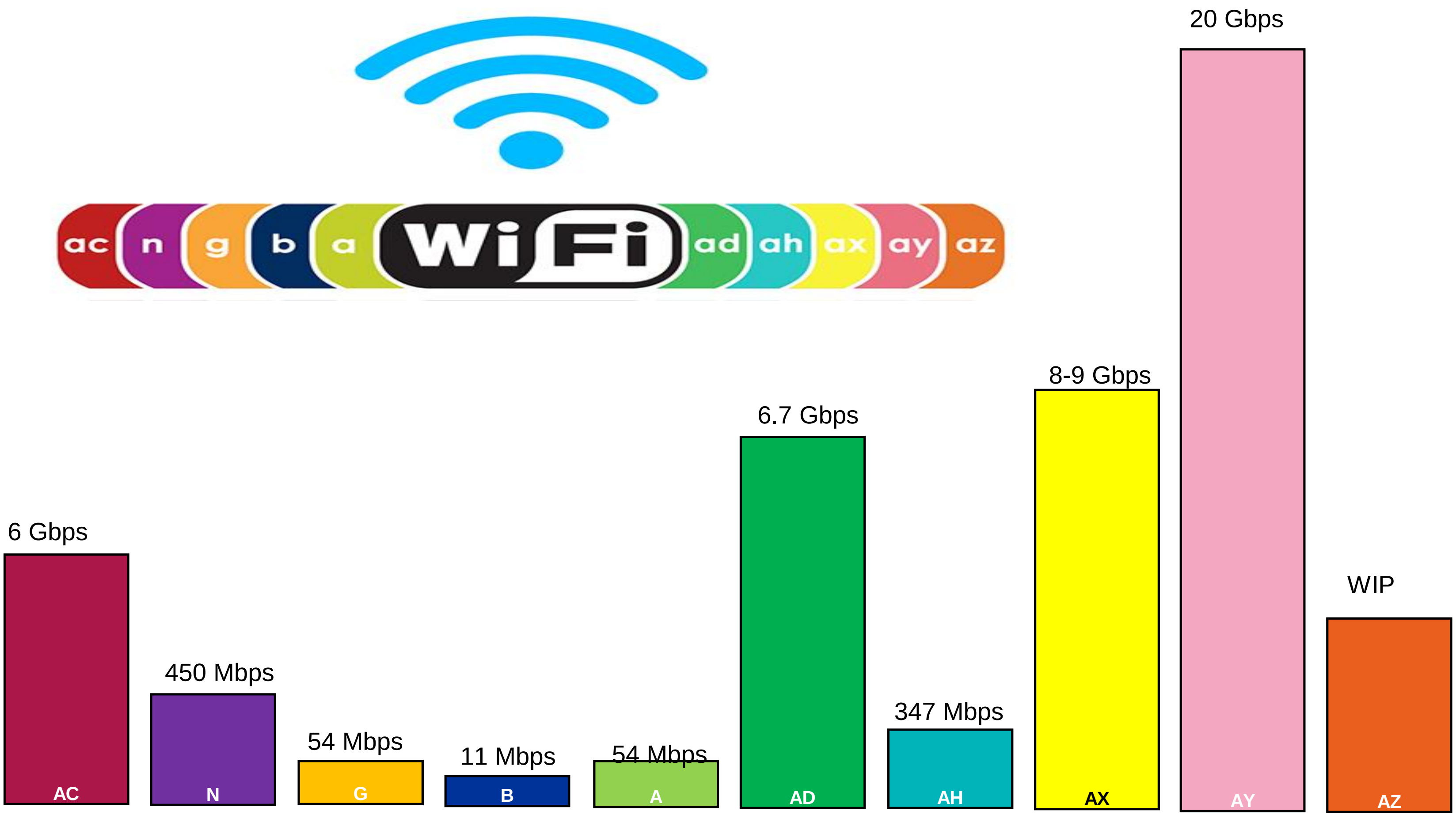


Wireless technology that provides connectivity to end-client devices wirelessly through radio-waves, to the network/internet.

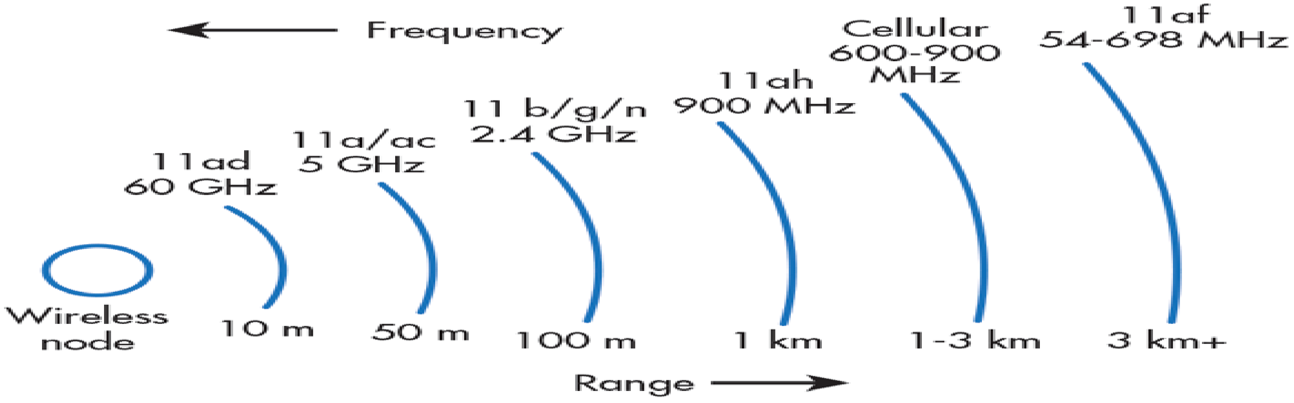
Uses the unlicensed spectrum

Wi-Fi Standards Overview

Standard	Year	Throughput Max	Frequency band	Order	Modulation	Bandwidth	MIMO
802.11a	1999	54 Mbps	5 Ghz	64 QAM	OFDM	20 Mhz	1X1
802.11b	1999	11 Mbps	2.4 Ghz	-	DSSS	20 Mhz	1X1
802.11g	2003	54 Mbps	2.4 Ghz	64 QAM	OFDM	20 Mhz	1X1
802.11n	2009	65-450 Mbps	2.4/5 Ghz	64 QAM	OFDM	20 / 40 Mhz	> 3X3
802.11ac	2013	0.290 - 3.6 Gbps	5 Ghz	256 QAM	OFDM	20/40/80/160 Mhz	> 4X4
802.11ax	2018	0.6 - 8 Gbps	5 Ghz	1024 QAM	OFDMA	20/40/80/160 Mhz	> 8X8

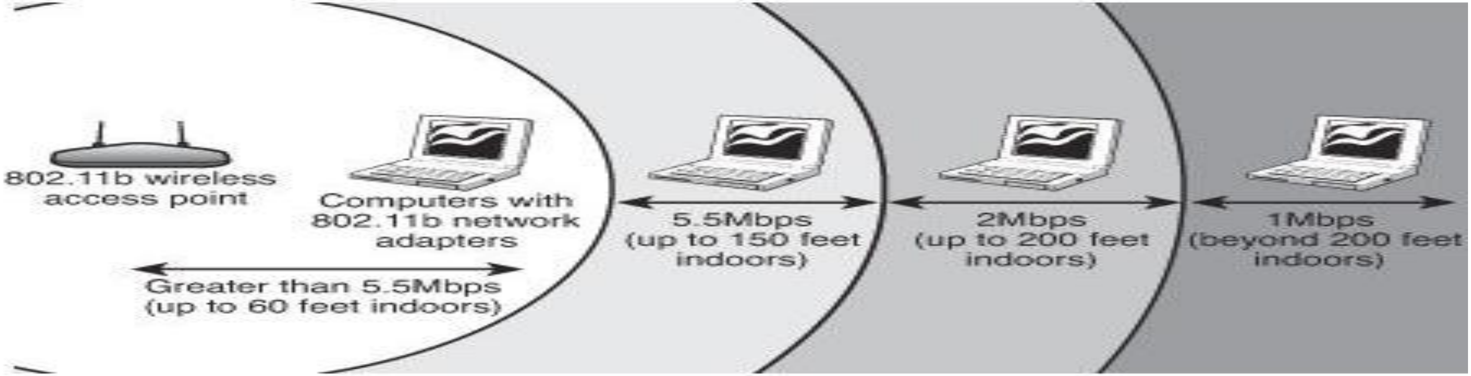

ac
n
g
b
a
WiFi
ad
ah
ax
ay
az
6 Gbps
AC
450 Mbps
N
54 Mbps
G
11 Mbps
B
54 Mbps
A
6.7 Gbps
AD
347 Mbps
AH
8-9 Gbps
AX
20 Gbps
AY
WIP
AZ

ac
n
g
b
a
WiFi
ad
ah
ax
ay
az


Frequency
11ad
60 GHz
11a/ac
5 GHz
11 b/g/n
2.4 GHz
11ah
900 MHz
Cellular
600-900
MHz
11af
54-698 MHz
Wireless
node
10 m
50 m
100 m
1 km
1-3 km
3 km+
Range

802.11b/g

- 802.11b uses DSSS – Spread spectrum and provide theoretical maximum of 11 Mbps
- Provides longer distance and operates at 2.4 Ghz (maximum of about 300m)
- It is more noise as it shares the spectrum with Bluetooth (e.g cordless phones)
- 802.11g arrived in 2003, improved bandwidth using OFDM, operated at 54 Mbps and backward compatible


802.11b wireless access point
Computers with 802.11b network adapters
Greater than 5.5Mbps (up to 60 feet indoors)
5.5Mbps (up to 150 feet indoors)
2Mbps (up to 200 feet indoors)
1Mbps (beyond 200 feet indoors)

802.11ac

- Uses OFDM Modulation scheme with QAM upto 256
- Operates at 5 GHz
- Allows bonding 40 MHz, 80 MHz and 160 MHz
- MIMO - 4X4
- Adaptive Beam forming
- MU-MIMO in the downlink side
- Implemented in two phases – WAVE-1 and WAVE-2

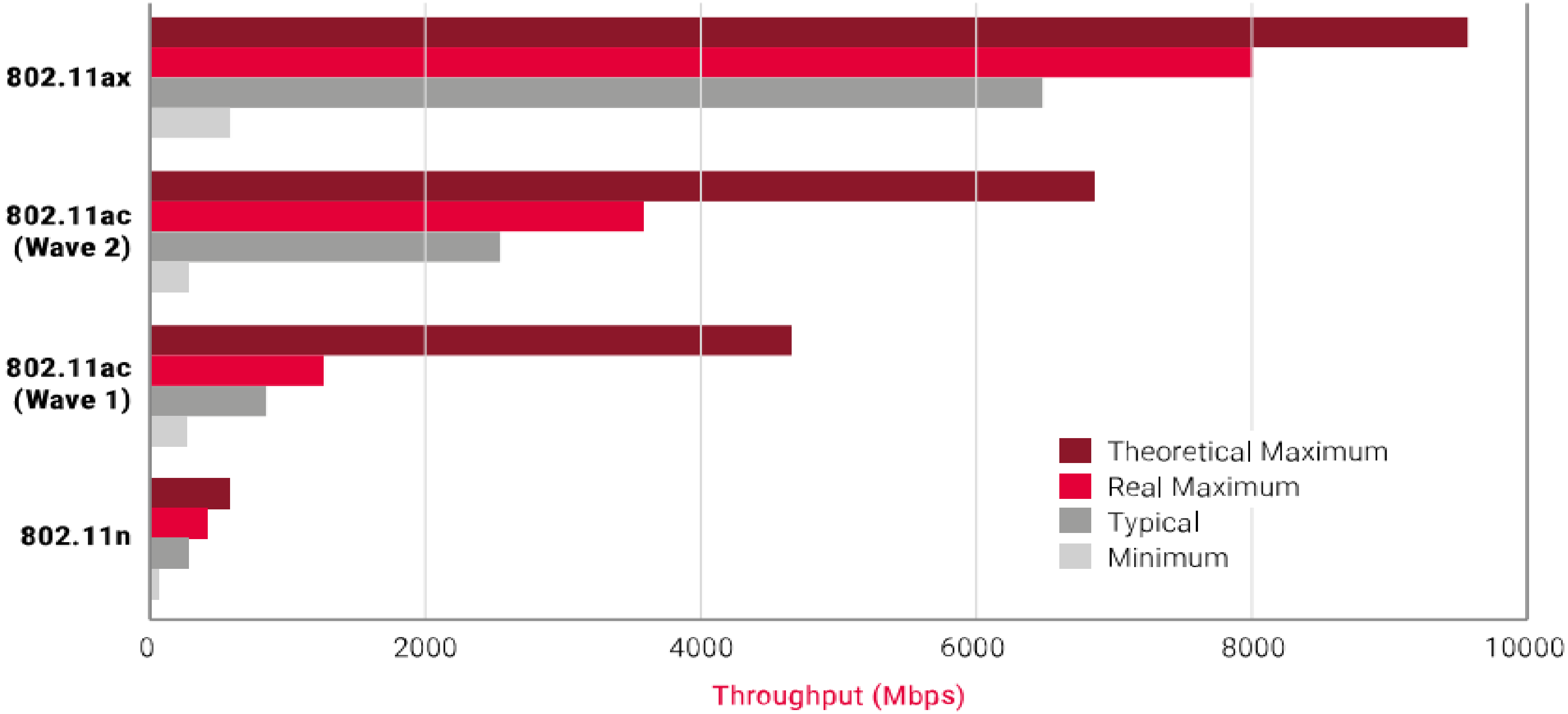
- Wave1 Salient features
- Adjacent Channel Bonding
- MIMO
- Theoretical Speeds up to 5 Gbps
- 20 MHz, 40MHz, 80 MHz support

- Wave2 Salient features
- All WAVE1 features
- Non Adjacent Channel Bonding 80+80 support (160MHz support)
- MU-MIMO
- Theoretical Speeds up to 9 Gbps

802.11ax

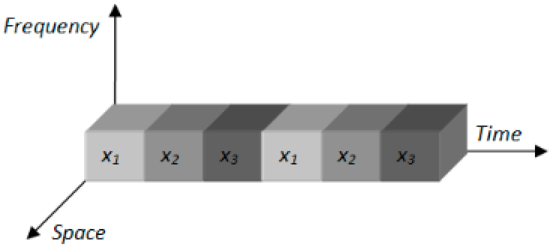
- Uses OFDMA Modulation scheme with QAM upto 1024
- Operates at both 2.4/5 GHz
- Allows bonding 20MHz, 40 MHz, 80 MHz and 160 MHz
- MIMO - 4X4
- Adaptive Beam forming
- MU-MIMO in both Uplink and Downlink side

Speed comparison for 802.11n/ac/ax

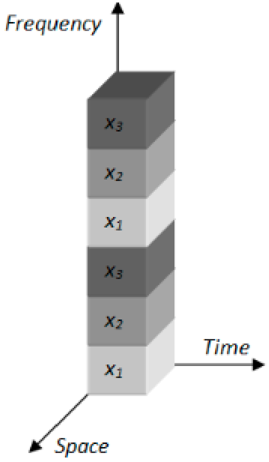


Diversity

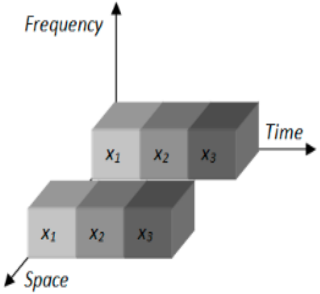
- Diversity techniques are based on the assumption that the probability that multiple statistically independent fading channels simultaneously experience deep fading is very low.
- There are various ways of realizing diversity gain, including the following ones:



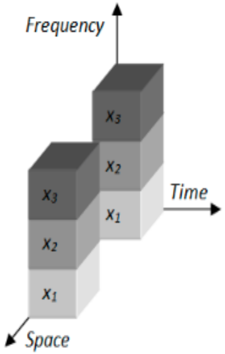
Time diversity



Frequency diversity

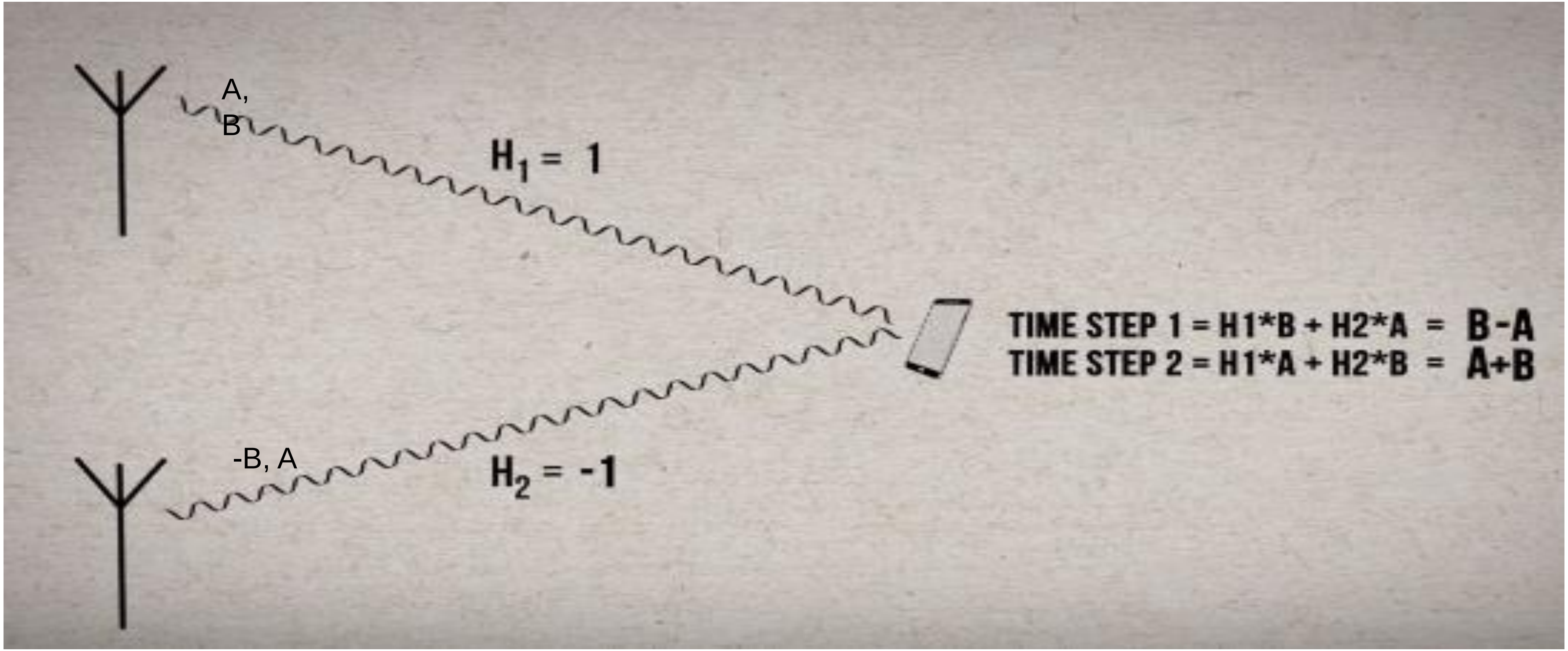


Space-time diversity



Space-frequency diversity

Space Time Block Code


A,
B
H_1 = 1
-B, A
H_2 = -1
TIME STEP 1 = H1*B + H2*A = B-A
TIME STEP 2 = H1*A + H2*B = A+B

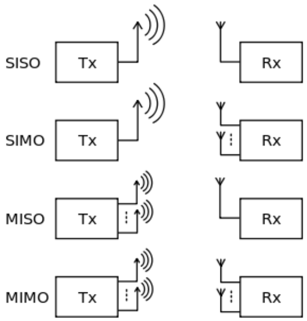
B – A = 0, A + B = 2 => A = 1, B = 1 and so on. H1 and H2 are fading characteristics

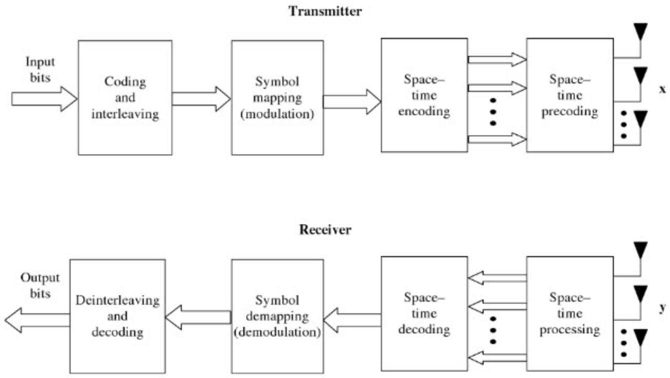
Rx is typically small and hence multiple antenna is used at the AP

MIMO

- Multiple Input Multiple Output or MIMO , is a method for multiplying the capacity of a radio link using multiple transmit and receive antennas to exploit multipath propagation.
- Multiple-in Multiple-out takes advantage of spatial multiplexing to increase wireless bandwidth and range.
- MIMO algorithms send information out over two or more antennas and the information is received via multiple antennas as well.
- MIMO systems provide a precise capacity gain over conventional single antenna RF systems, along with more reliable communication.

- A MIMO system has multiple radio chains each of which is a transceiver with its own antenna.
- A radio chain refers to the hardware necessary for transmit/receive signal processing.
- A radio chain is just a transceiver, antenna, and any hardware needed to process the signal

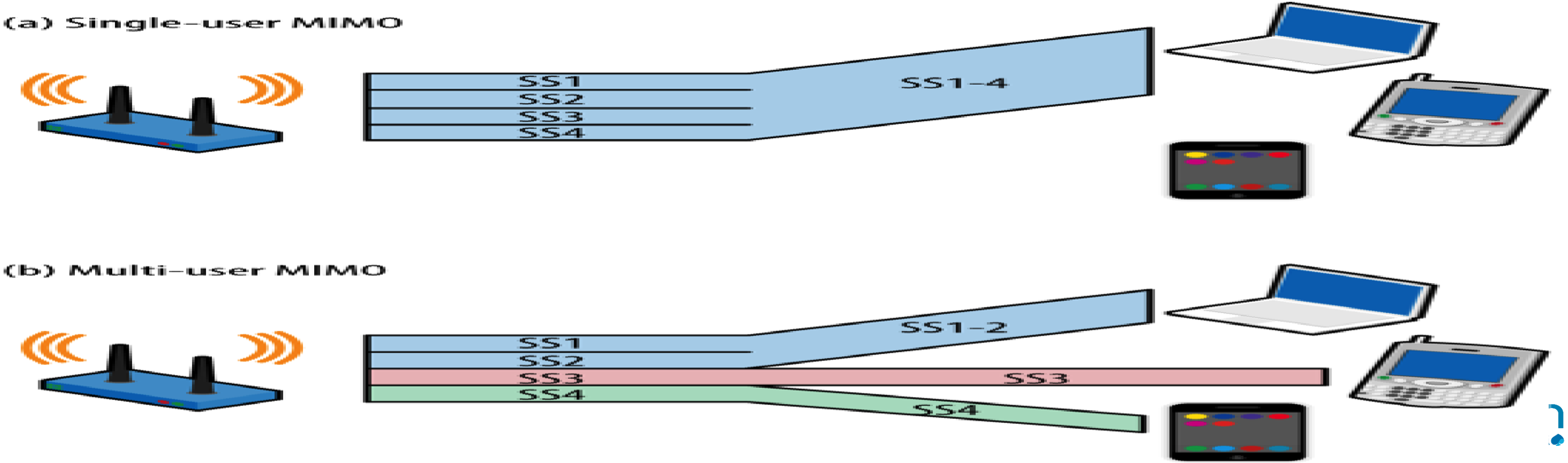




Basic Block Diagram of MIMO System

MU-MIMO

- Multi-user, multiple-input, multiple-output technology allows a Wi-Fi AP to communicate with multiple devices simultaneously.
- This decreases the time each device has to wait for a signal and dramatically speeds up network.
- MU-MIMO will increasingly improve Wi-Fi experience.
- Requires functionality to be updated both AP and station



Beam forming, Adaptive Beam forming

- Beamforming is all about focusing a Wi-Fi signal in a specific direction.

- Traditionally, when your router broadcasts a Wi-Fi signal, it broadcasts the data in all directior

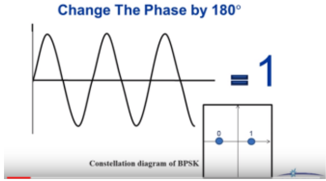
- With beamforming, the router determines where your device — laptop, smartphone, tablet, or whatever else — is located and projects a stronger signal in that specific direction (hence longer range).

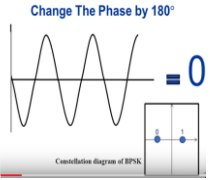
- **Explicit beamforming** is based on the transmitter and receiver exchanging information about the characteristics of the radio channel to wring out maximum performance based on measurements

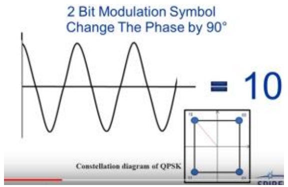
- **Implicit beamforming** is based on inferences of channel characteristics when frames are lost. Typically used for backward compatible stations which does support explicit beam forming.
- To change the radiation pattern on a frame-by-frame basis, smart antennas are controlled electronically.

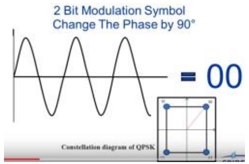
Smart antennas (also known as adaptive array antennas, digital antenna arrays, multiple antennas and, recently, MIMO) are antenna arrays with smart signal processing algorithms used to identify spatial signal signatures such as the direction of arrival (DOA) of the signal, and use them to calculate beamforming vectors which are used to track and locate the antenna beam on the mobile/target.
How Null Data packet helps in beam forming?

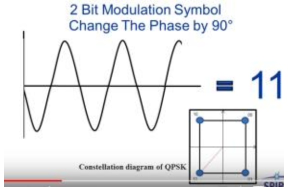
QAM

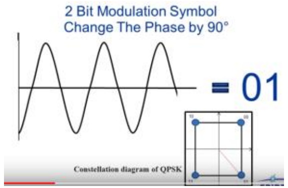

Change The Phase by 180°

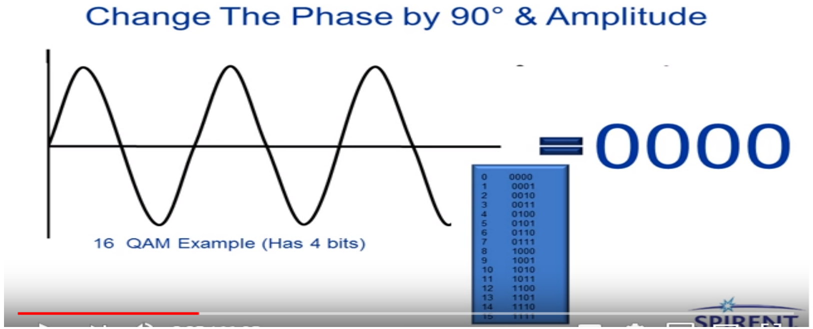

Change The Phase by 180°


2 Bit Modulation Symbol
Change The Phase by 90°


2 Bit Modulation Symbol
Change The Phase by 90°

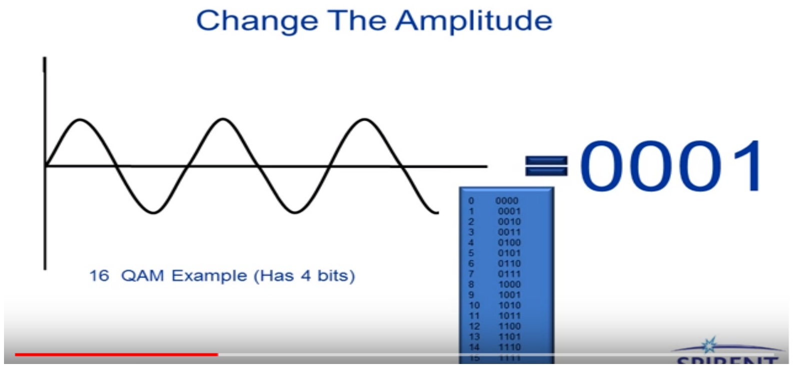

2 Bit Modulation Symbol
Change The Phase by 90°


2 Bit Modulation Symbol
Change The Phase by 90°


Change The Phase by 90° & Amplitude

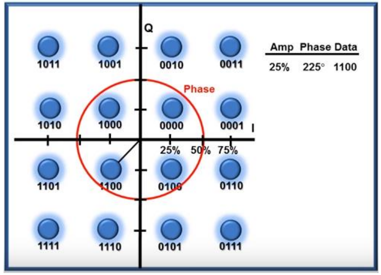
16 QAM Example (Has 4 bits)

0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111


Change The Amplitude

16 QAM Example (Has 4 bits)

0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111



Amp	Phase	Data
25%	225°	1100

- Vary Amplitude and phase to represent a symbol
- Upto 1024 QAM has been realized in Wi-Fi 802.11ax

OFDM/OFDMA

-reduces ISI
-minimizes the effect of multipath fading
-results in bandwidth saving

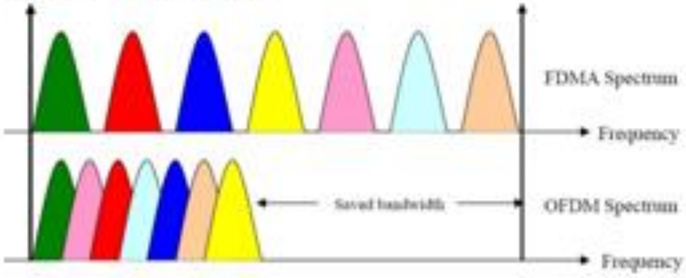
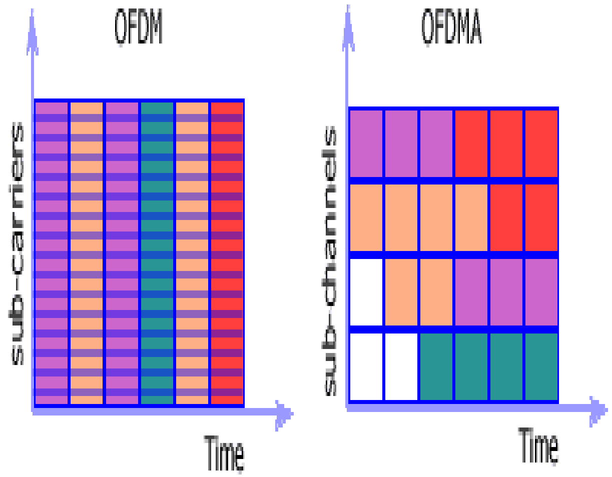
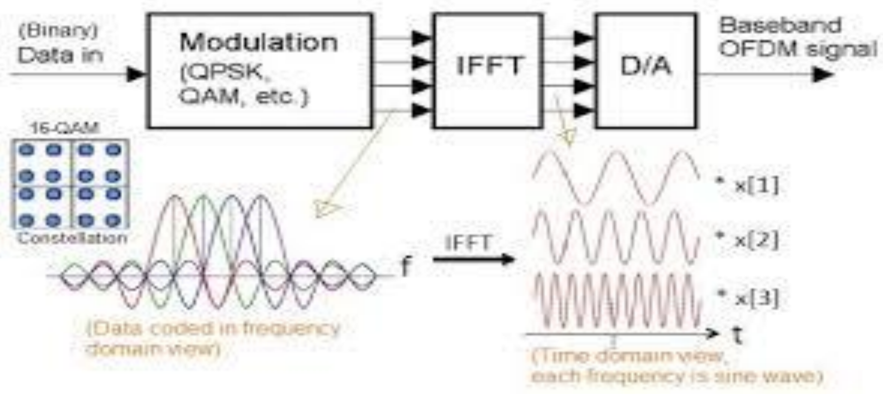
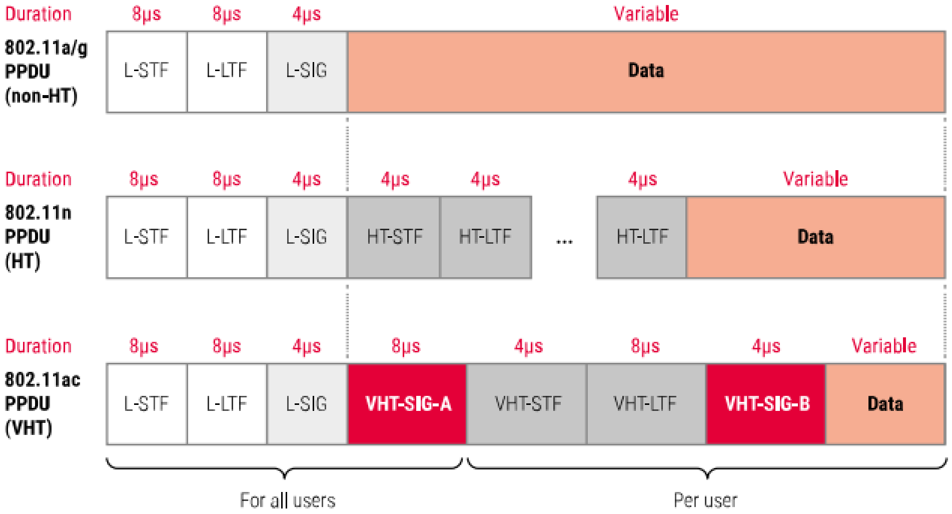


Figure : Bandwidth comparison of OFDMA and FDMA




(Binary) Data in
Modulation (QPSK, QAM, etc.)
IFFT
D/A
Baseband OFDM signal
16-QAM
Constellation
f
IFFT
x[1]
x[2]
x[3]
t
(Data coded in frequency domain view)
(Time domain view, each frequency is sine wave)

How backward compatibility of standards is achieved?



Duration	8µs	8µs	4µs	Variable
802.11a/g PPDU (non-HT)	L-STF	L-LTF	L-SIG	Data

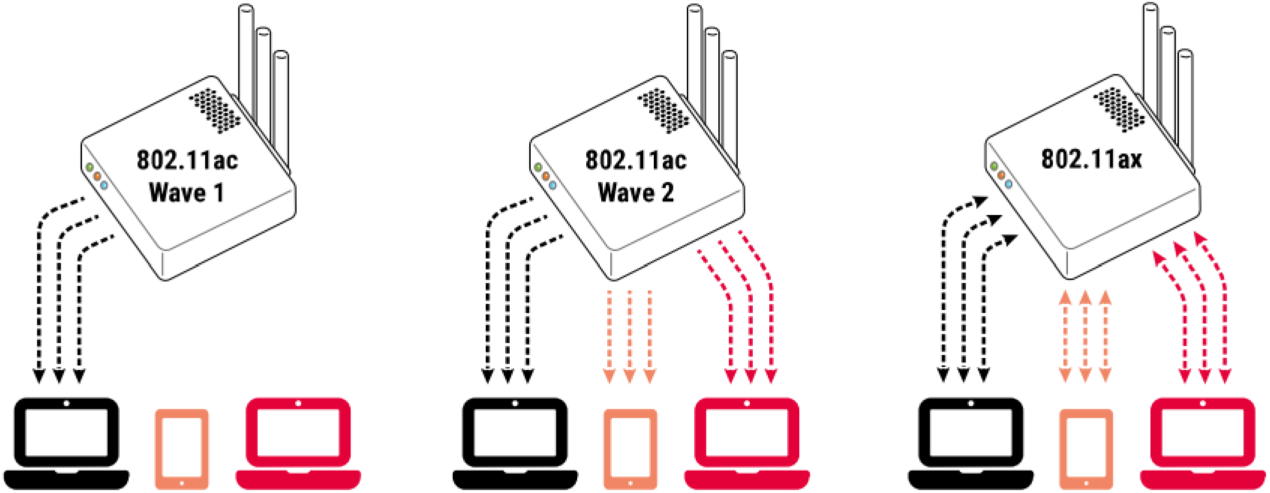
Duration	8µs	8µs	4µs	4µs	4µs		4µs	Variable
802.11n PPDU (HT)	L-STF	L-LTF	L-SIG	HT-STF	HT-LTF	...	HT-LTF	Data

Duration	8µs	8µs	4µs	8µs	4µs	8µs	4µs	Variable
802.11ac PPDU (VHT)	L-STF	L-LTF	L-SIG	VHT-SIG-A	VHT-STF	VHT-LTF	VHT-SIG-B	Data

For all users

Per user

MIMO comparison for 802.11ac-wave1/ac-wave2/ax

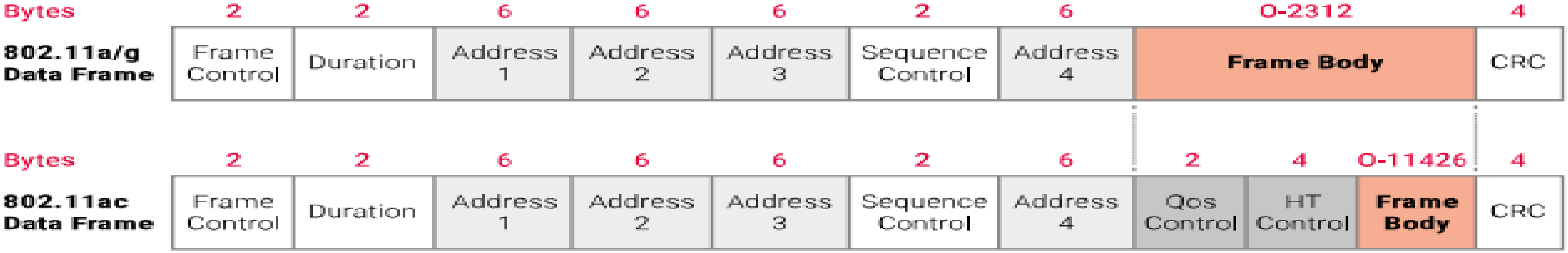


SU-MIMO One User
Downstream only

MU-MIMO
Multiple User
Downstream only

MU-MIMO
Multiple User Bi-directional

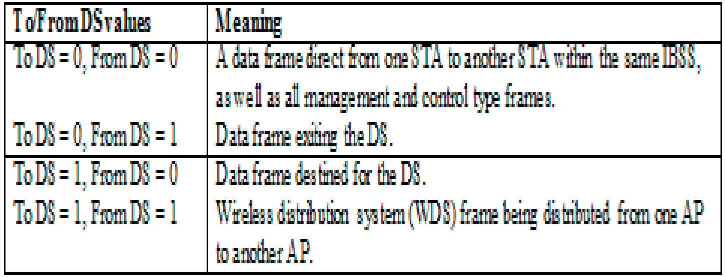
Wi-Fi Data Frame Format



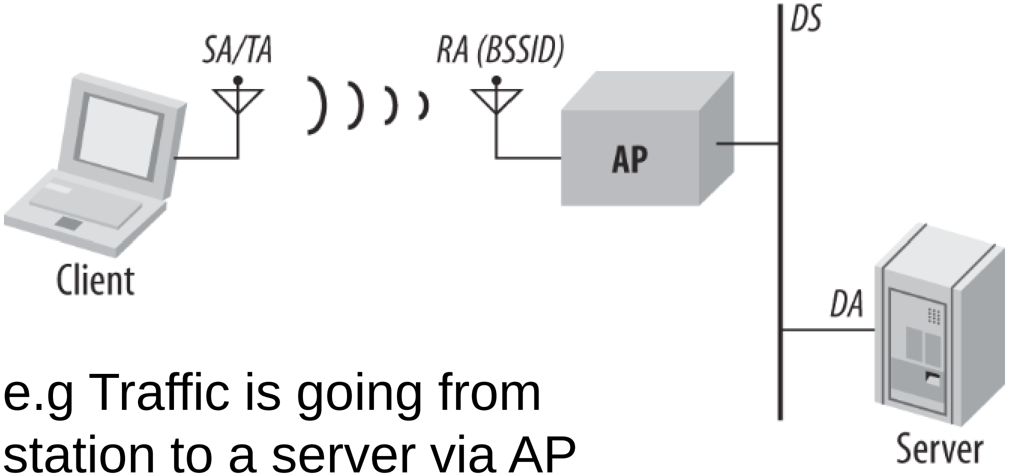
Bytes	2	2	6	6	6	2	6	0-2312	4
802.11a/g Data Frame	Frame Control	Duration	Address 1	Address 2	Address 3	Sequence Control	Address 4	**Frame Body**	CRC

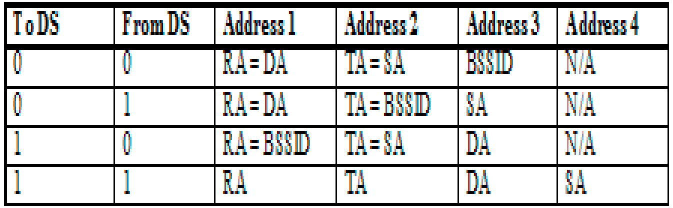
Bytes	2	2	6	6	6	2	6	2	4	0-11426	4
802.11ac Data Frame	Frame Control	Duration	Address 1	Address 2	Address 3	Sequence Control	Address 4	Qos Control	HT Control	**Frame Body**	CRC

- Transmitter Address (TA)
- Receiver Address (RA)
- Source Address (SA)



To/From DS values	Meaning
To DS = 0, From DS = 0	A data frame direct from one STA to another STA within the same IBSS, as well as all management and control type frames.
To DS = 0, From DS = 1	Data frame exiting the DS.
To DS = 1, From DS = 0	Data frame destined for the DS.
To DS = 1, From DS = 1	Wireless distribution system (WDS) frame being distributed from one AP to another AP.

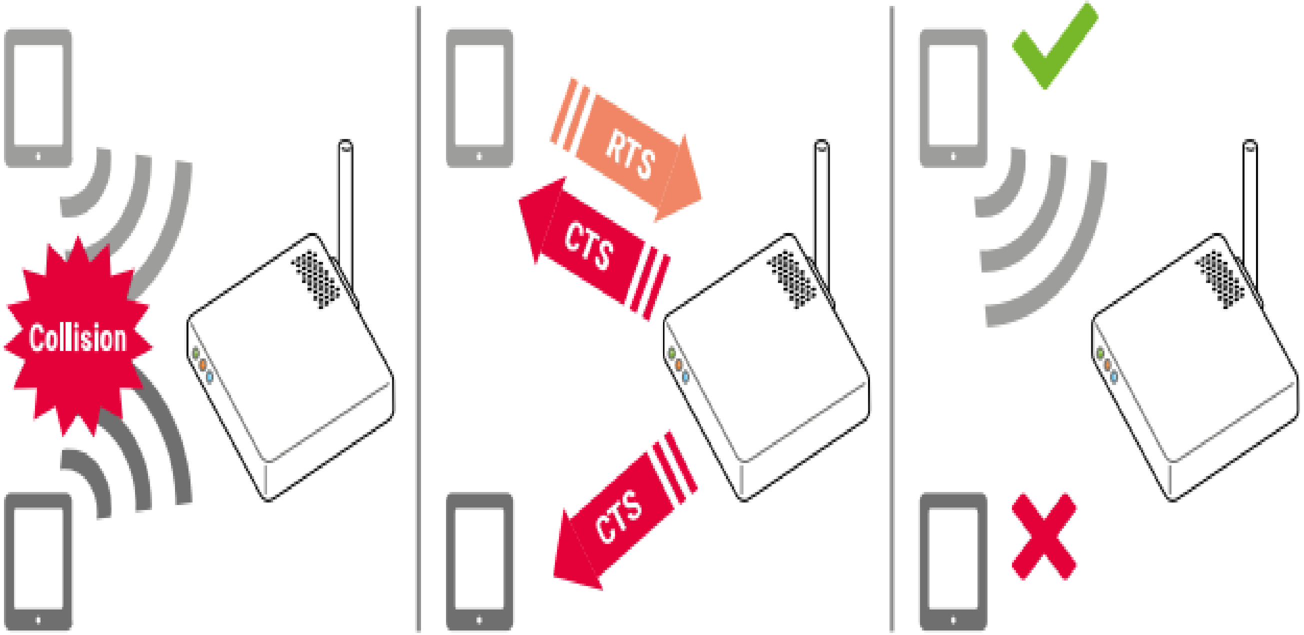




To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA = DA	TA = SA	BSSID	N/A
0	1	RA = DA	TA = BSSID	SA	N/A
1	0	RA = BSSID	TA = SA	DA	N/A
1	1	RA	TA	DA	SA

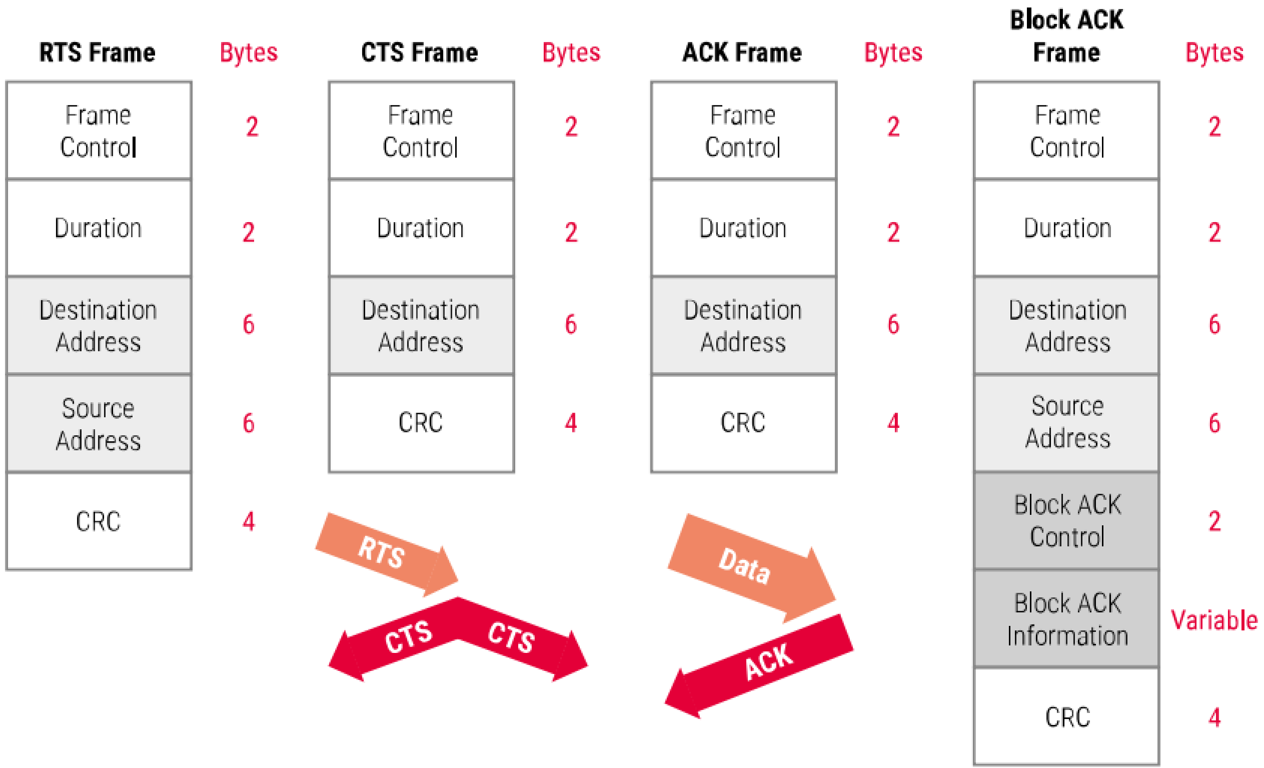
e.g Traffic is going from station to a server via AP

Collision avoidance – CSMA-CA “Ask permission before speaking”



RTS/CTS is sent at maximum power, minimum speed and maximum redundancy so that is backward compatible across 802.11bgn for 2.4 GHz and 802.11a/ac/ax in 5GHz

Control Frames



RTS Frame	Bytes
Frame Control	2
Duration	2
Destination Address	6
Source Address	6
CRC	4

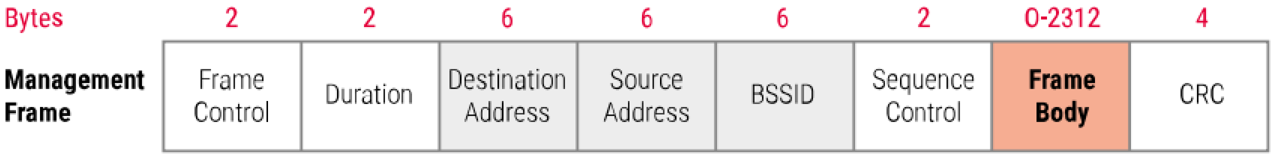
CTS Frame	Bytes
Frame Control	2
Duration	2
Destination Address	6
CRC	4

ACK Frame	Bytes
Frame Control	2
Duration	2
Destination Address	6
CRC	4

Block ACK Frame	Bytes
Frame Control	2
Duration	2
Destination Address	6
Source Address	6
Block ACK Control	2
Block ACK Information	Variable
CRC	4

Block Ack Request and Contention Free-End are other control blocks – less used

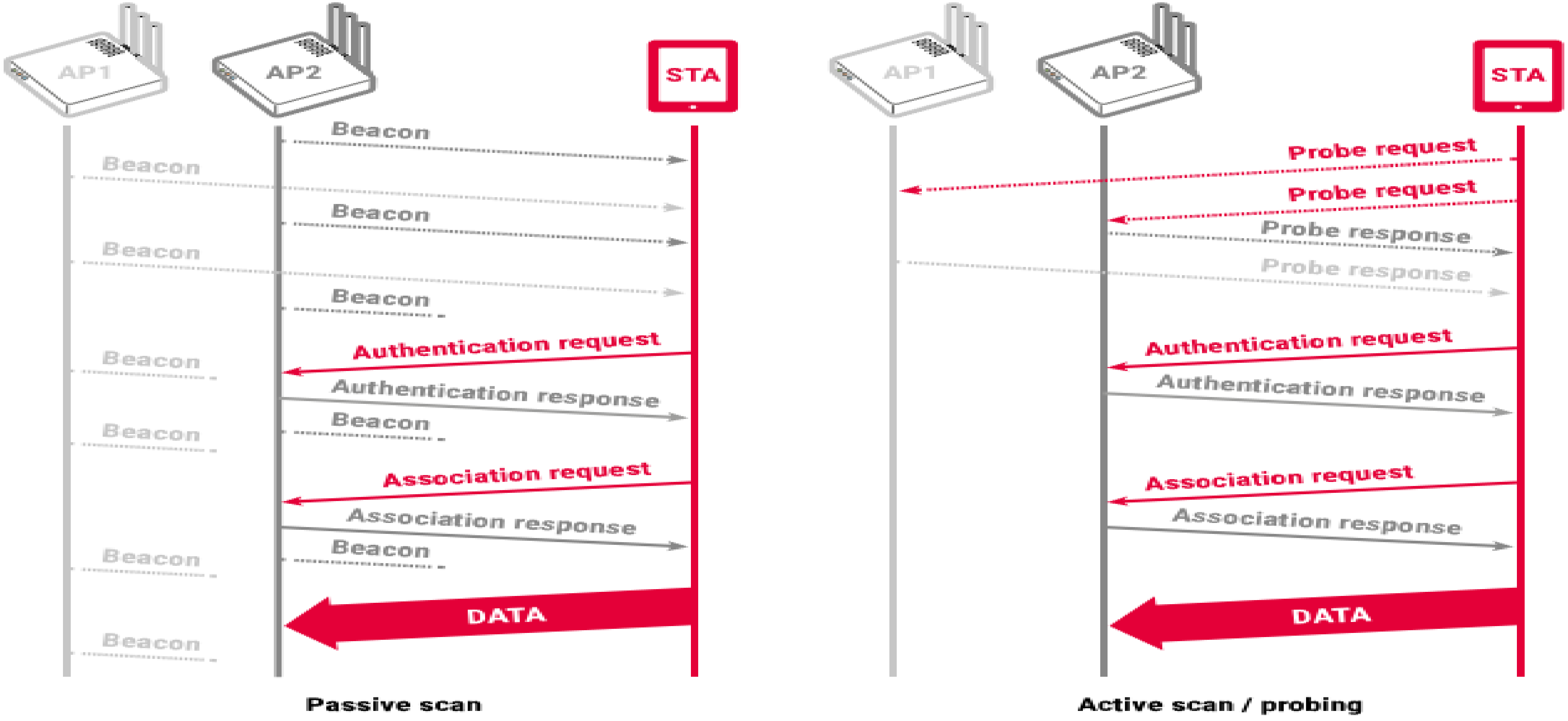
Management Frames



Bytes	2	2	6	6	6	2	0-2312	4
Management Frame	Frame Control	Duration	Destination Address	Source Address	BSSID	Sequence Control	**Frame Body**	CRC

- Beacon and Probe response: timestamp, beacon interval, capability information, SSID, supported rates, physical parameter sets, and traffic indication map
- Probe request : SSID and supported rates
- Authentication Request and Response : Authentication algorithm, transaction sequence number, status code, and challenge text (for some types)
- Association Request : Capability information, listen internval, SSID, and supported rates
- Association Response : capability information, status code, association ID, and supported rates.
- Deauthentication and Disassociation : Status code
- Reassociation request, Reassociation response and Action frames are other management frames – rarely used.

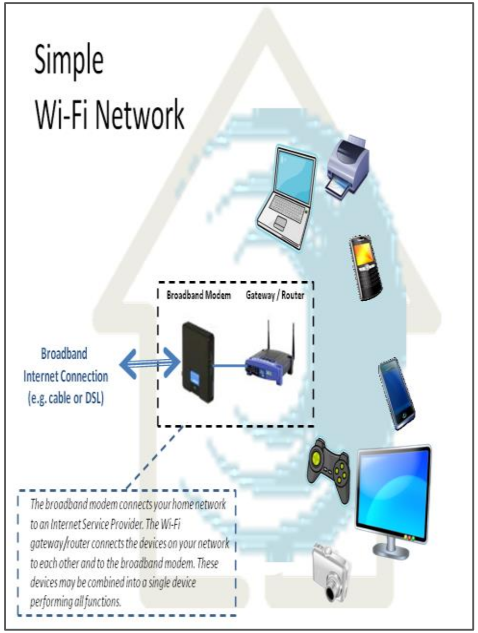
Active and Passive Scan



altran
Part of Capgemini

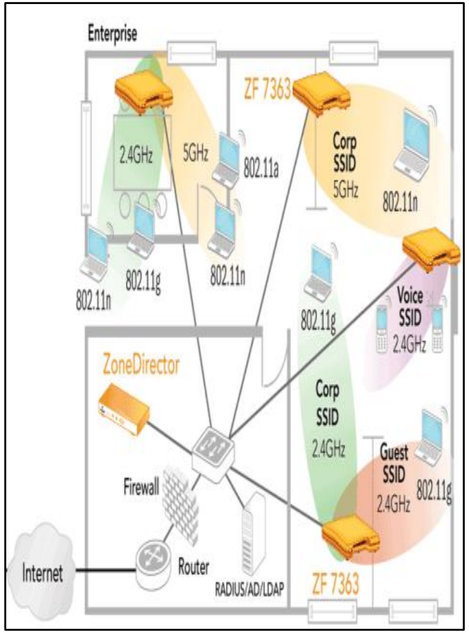
Wi-Fi Network Deployments (1 of 7)

HOME

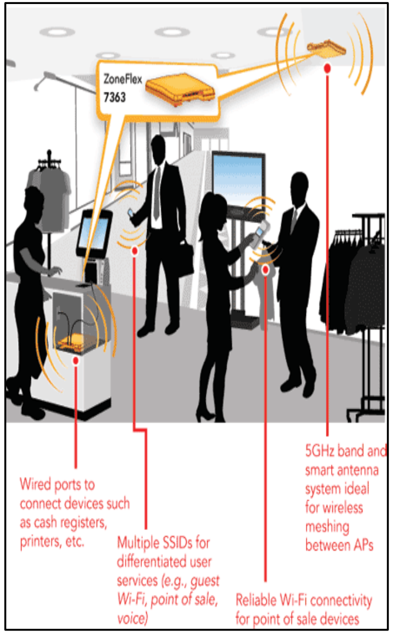


The broadband modem connects your home network to an Internet Service Provider. The Wi-Fi gateway/router connects the devices on your network to each other and to the broadband modem. These devices may be combined into a single device performing all functions.

ENTERPRISE



BRANCH-OFFICE/ RETAIL



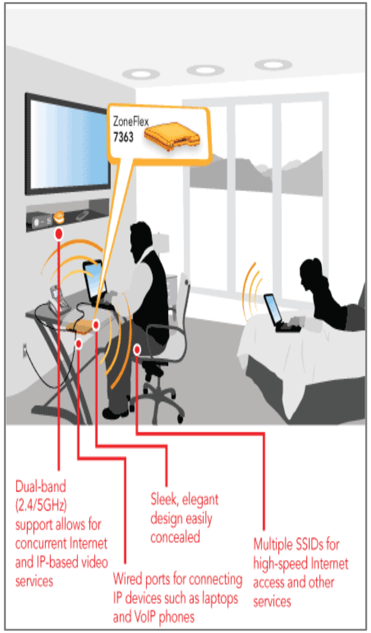
Wired ports to connect devices such as cash registers, printers, etc.

Multiple SSIDs for differentiated user services (e.g., guest Wi-Fi, point of sale, voice)

Reliable Wi-Fi connectivity for point of sale devices

5GHz band and smart antenna system ideal for wireless meshing between APs

HOTEL ROOM



Dual-band (2.4/5GHz) support allows for concurrent Internet and IP-based video services

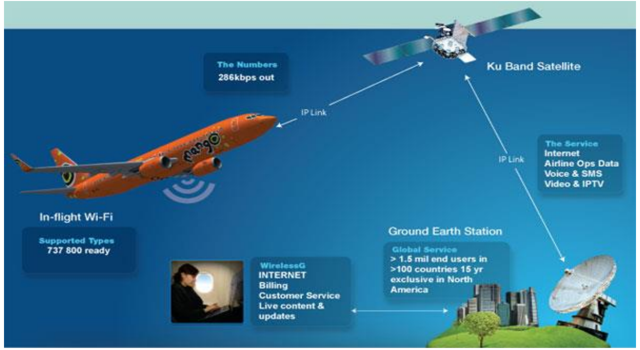
Wired ports for connecting IP devices such as laptops and VoIP phones

Sleek, elegant design easily concealed

Multiple SSIDs for high-speed Internet access and other services

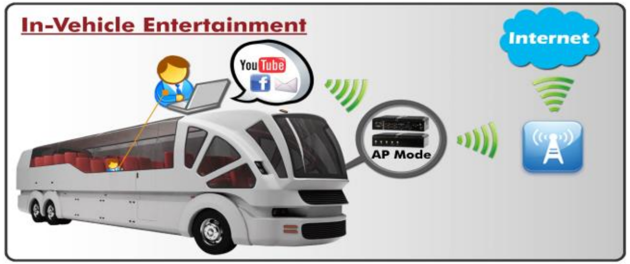
Wi-Fi Network Deployments (2 of 7)

IN-FLIGHT



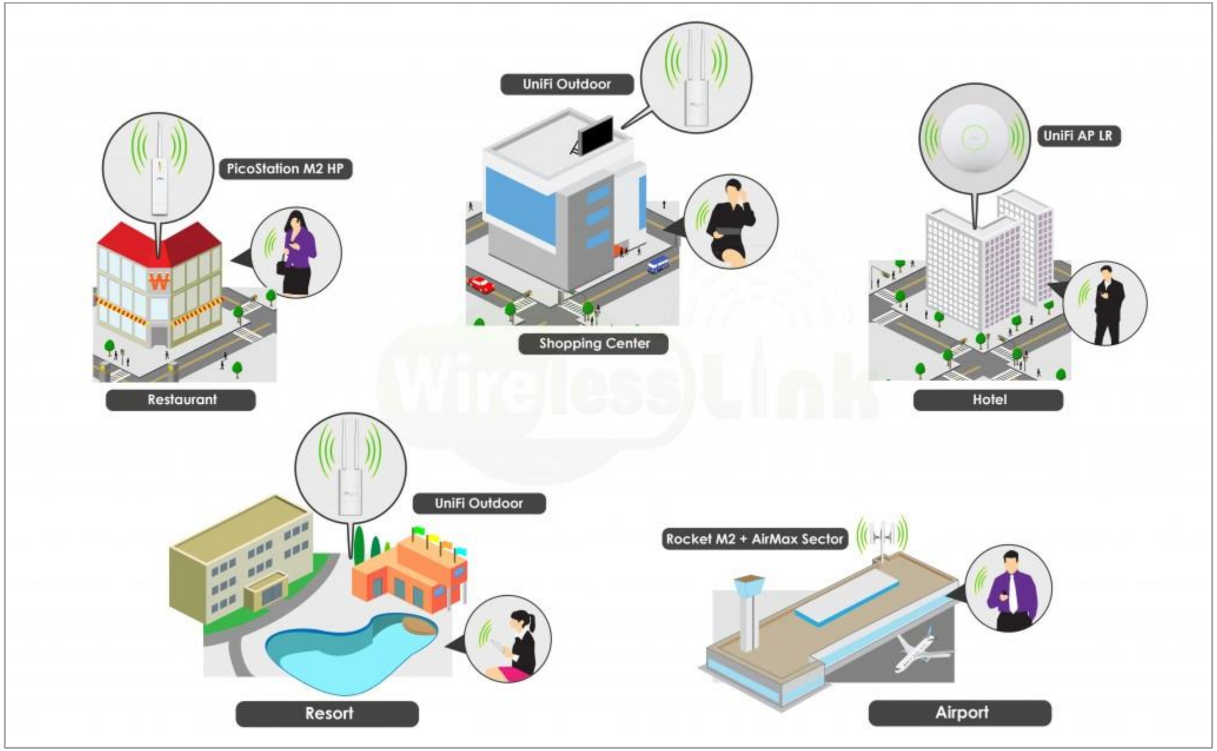
INDUSTRIAL WI-FI

IN-VEHICLE

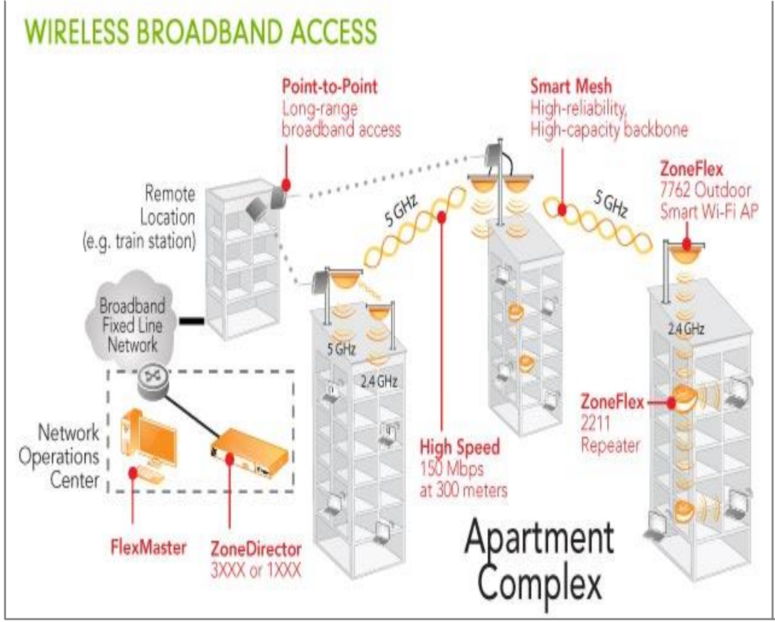
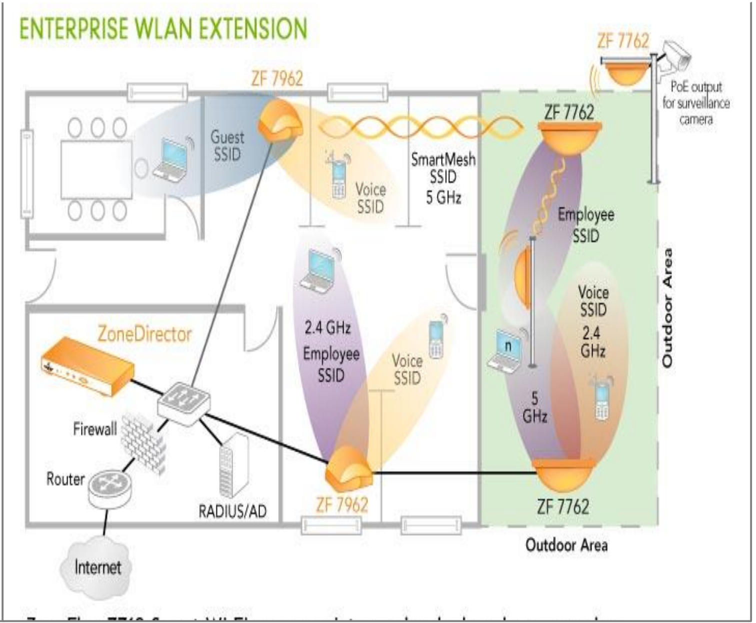


Wi-Fi Network Deployments (3 of 7)

PUBLIC HOTSPOTS

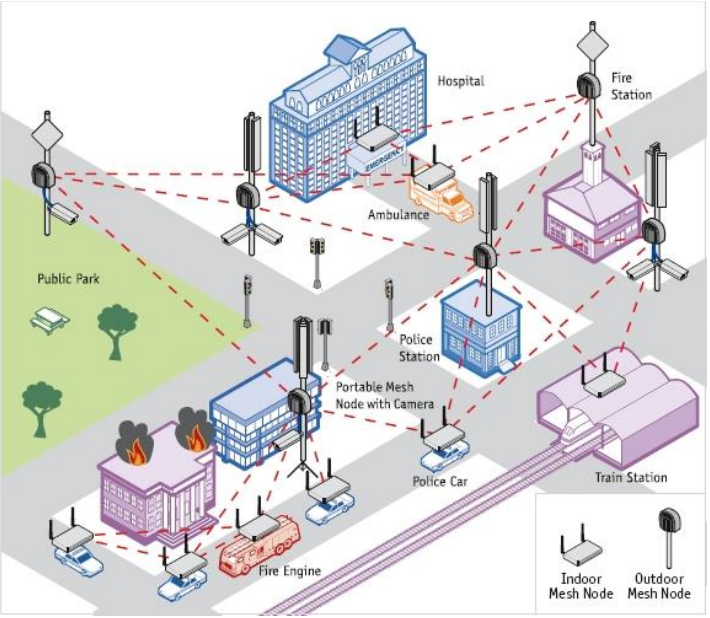


Wi-Fi Network Deployments (4 of 7)

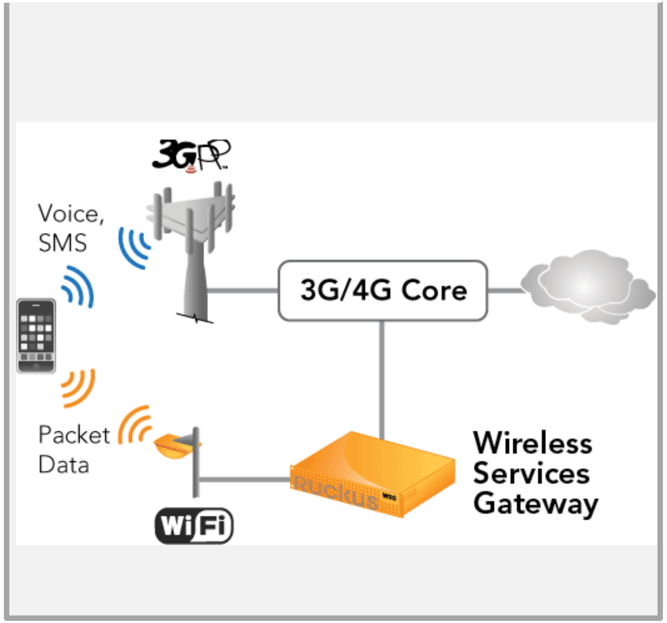
APARTMENT COMPLEX – WIRELESS BROADBAND ACCESS	ENTERPRISE WLAN – OUTDOOR EXTENSION
	

Wi-Fi Network Deployments (5 of 7)

PUBLIC SAFETY NETWORKS

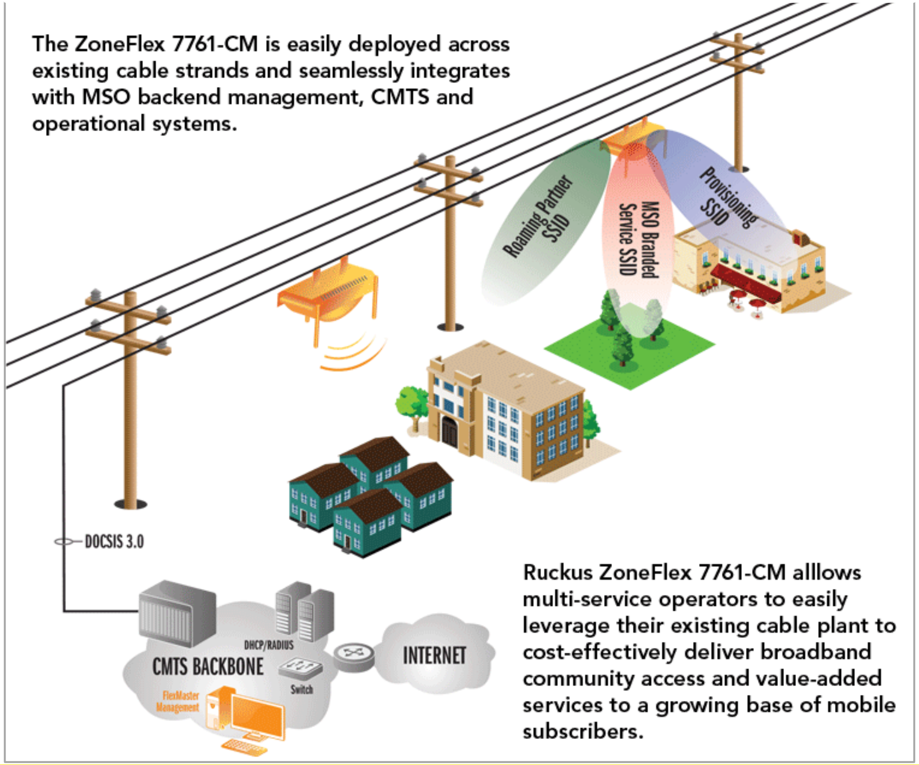


Wi-FI OFFLOAD (CARRIER WI-FI)



Wi-Fi Network Deployments (6 of 7)

CABLE MSO’S WI-FI SERVICE

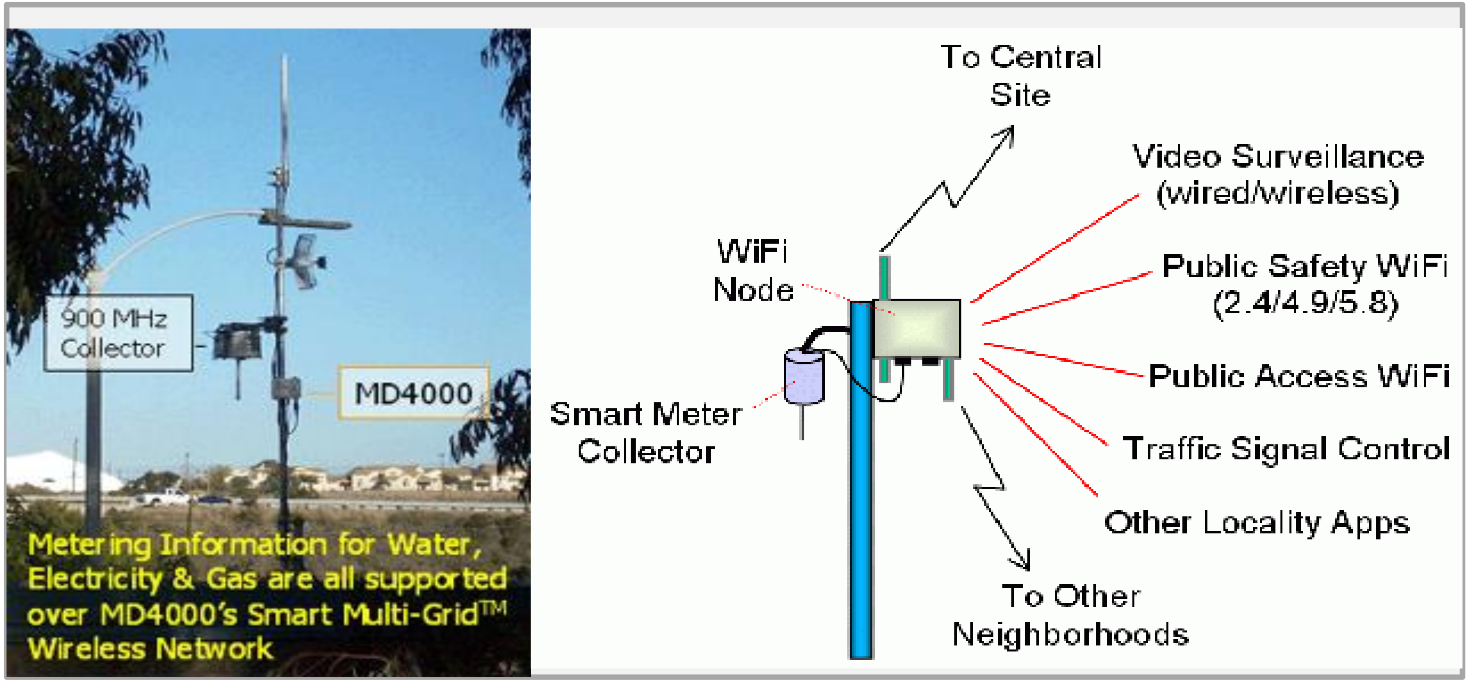


The ZoneFlex 7761-CM is easily deployed across existing cable strands and seamlessly integrates with MSO backend management, CMTS and operational systems.

Ruckus ZoneFlex 7761-CM alllows multi-service operators to easily leverage their existing cable plant to cost-effectively deliver broadband community access and value-added services to a growing base of mobile subscribers.

Wi-Fi Network Deployments (7 of 7)

SMART UTILITY NETWORKS



Metering Information for Water, Electricity & Gas are all supported over MD4000's Smart Multi-Grid™ Wireless Network

WLAN Network Equipment & Functions

Access Points, Cable Modems

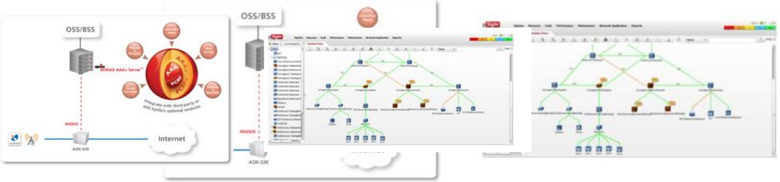
- Provides Access to the client devices over radio interface, Switches user traffic between the Radio nwk and the wired nwk.
- Connects to the wired network on the uplink side

WLAN Controller, Offload Gateway

- Provides the control logic to the APs
- Offload Gateway : Offloads data-traffic from Mobile to WiFi network

Wi-Fi Integrated Small Cell

- Carrier Grade AP with LTE Small Cell integrated



AAA Server , WLAN Management

- WLAN Management : for Provisioning, SW Upgrade, Diagnostics
- AAA Server : for Authentication, Authorization & Accounting) Server

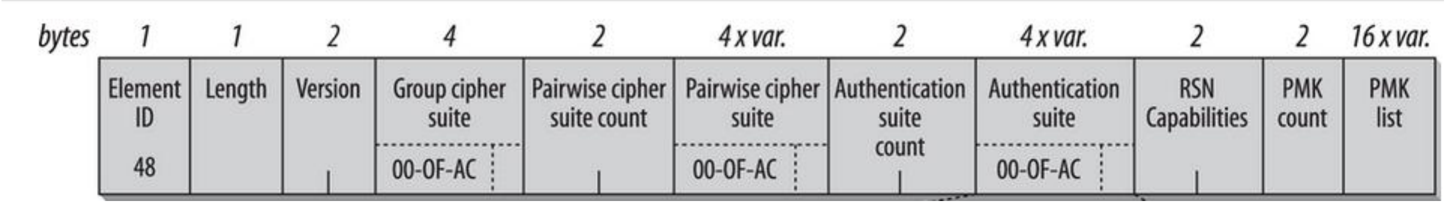
Wi-Fi Security

Introduction: IEEE 802.11i

- IEEE 802.11i defined to properly secure wireless LANs (2004)
- Defines a Robust Security Network (RSN)
- Called WiFi-Protected Access 2 (WPA2) by WiFi-Alliance
- Two types of Authentication available in WPA2 (PSK and enterprise)
- WPA2-PSK (Used in the case of personal/home networks)
- WPA2-ENTERPRISE (Used in the case of office networks)
-

RSN Elements in Beacon Frames

- The trigger point in any wireless connection (Open or WPA2 authentication) is the advertisement of the beacon frames.
- An RSN Information Element is sent in the beacon frames to differentiate between the open authentication and WPA2 authentication.
- The key elements in this field are Group Cipher, Pairwise cipher suite and authentication suite.
- Group cipher – Two different types (TKIP and CCMP)
- Pairwise cipher – Two different types (TKIP and CCMP)
- Authentication suite – Two different types (PSK and 802.1X(Enterprise))



bytes	1	1	2	4	2	4 x var.	2	4 x var.	2	2	16 x var.
	Element ID 48	Length	Version	Group cipher suite 00-0F-AC	Pairwise cipher suite count	Pairwise cipher suite 00-0F-AC	Authentication suite count	Authentication suite 00-0F-AC	RSN Capabilities	PMK count	PMK list

IEEE 802.11i: Pre-Shared Key (PSK)

Usually a single pre-shared key for entire network
Involves 4-way Handshake between the Client and AP
Password-to-Key Mapping

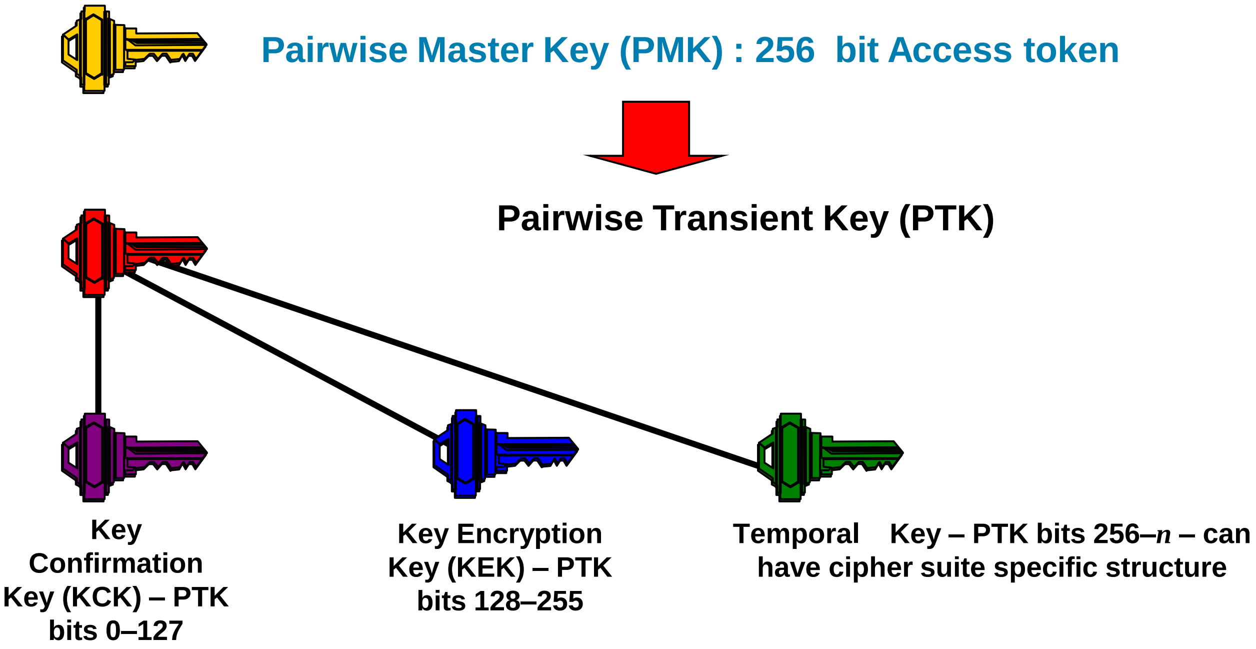
- PSK = PMK = PBKDF2 (Password, SSID, SSIDlength, 4096, 256)

Password-Based Key Derivation Function 2
Password – User given password
SSID – Name of the SSID (WLAN)
SSIDLENGTH – Length of the SSID
4096 is the number of iterations used in this process
256 is the length of the key in bits (32 hexbyte)

Sample PSK Value:
Password – abcdefgh (8-64 ascii characters)
SSID - RSNATEST
SSIDLEN - 8

PSK derived:
66159dc2975e09ba44db64175c7deb8f1a164a32983e7394ddd322be178abb02

802.11i Pairwise Key Hierarchy



Pairwise Master Key (PMK) : 256 bit Access token

Pairwise Transient Key (PTK)

Key Confirmation Key (KCK) – PTK bits 0–127

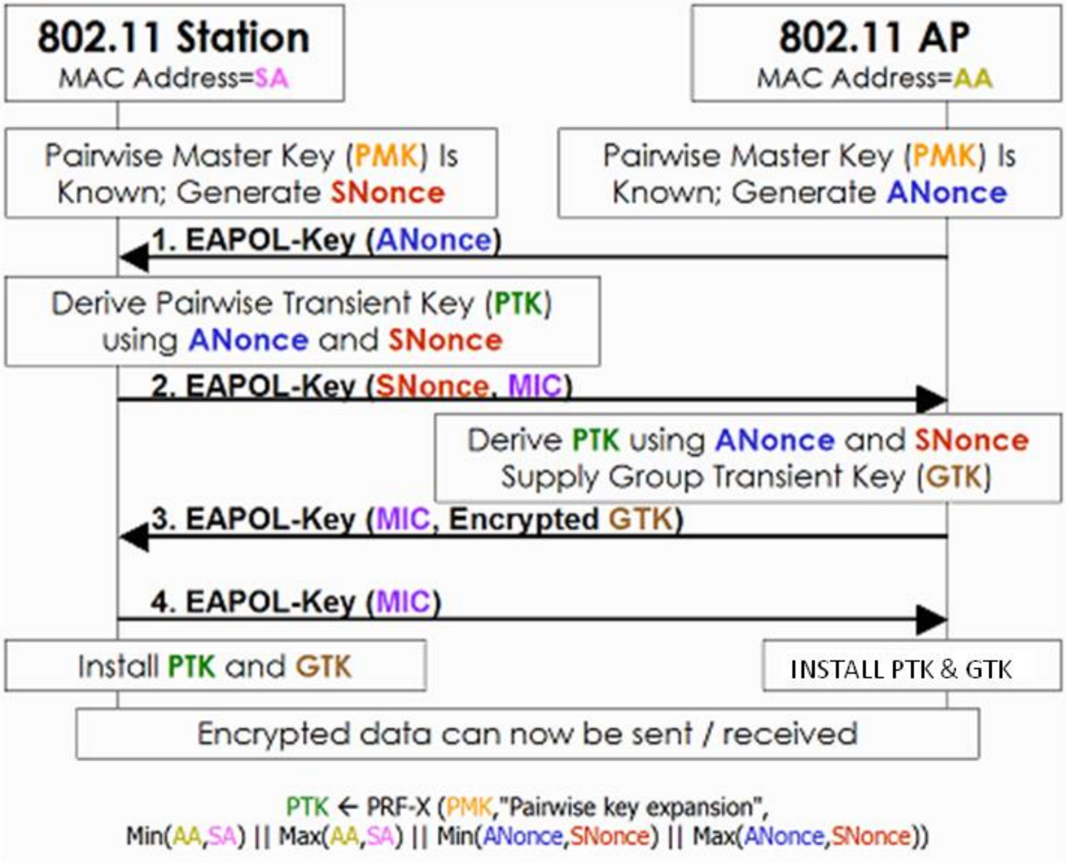
Key Encryption Key (KEK) – PTK bits 128–255

Temporal Key – PTK bits 256–n – can have cipher suite specific structure

Different types of keys used

- PMK -Pairwise Master Key. This is the trigger to the authentication process. In the case of PSK, PMK and PSK are both the same.
- **Pairwise Transient Key** (**PTK**) – Collection of operational keys:
  - **Key Confirmation Key** (**KCK**) – Used to verify MIC in the 4-way handshake
  - **Key Encryption Key** (**KEK**) – Used to encrypt and send the Transient Key (GTK)
  - **Temporal Key** (**TK**) – Final encryption key used to encrypt unicast data traffic.
- **Group Temporal Key (GTK):** Final encryption key used to encrypt broadcast and multicast traffic.

4-WAY HANDSHAKE



802.11 Station
MAC Address=SA

802.11 AP
MAC Address=AA

Pairwise Master Key (PMK) Is Known; Generate SNonce

Pairwise Master Key (PMK) Is Known; Generate ANonce

1. EAPOL-Key (ANonce)

Derive Pairwise Transient Key (PTK) using ANonce and SNonce

2. EAPOL-Key (SNonce, MIC)

Derive PTK using ANonce and SNonce
Supply Group Transient Key (GTK)

3. EAPOL-Key (MIC, Encrypted GTK)

4. EAPOL-Key (MIC)

Install PTK and GTK

INSTALL PTK & GTK

Encrypted data can now be sent / received

PTK ← PRF-X (PMK,"Pairwise key expansion",
Min(AA,SA) || Max(AA,SA) || Min(ANonce,SNonce) || Max(ANonce,SNonce))

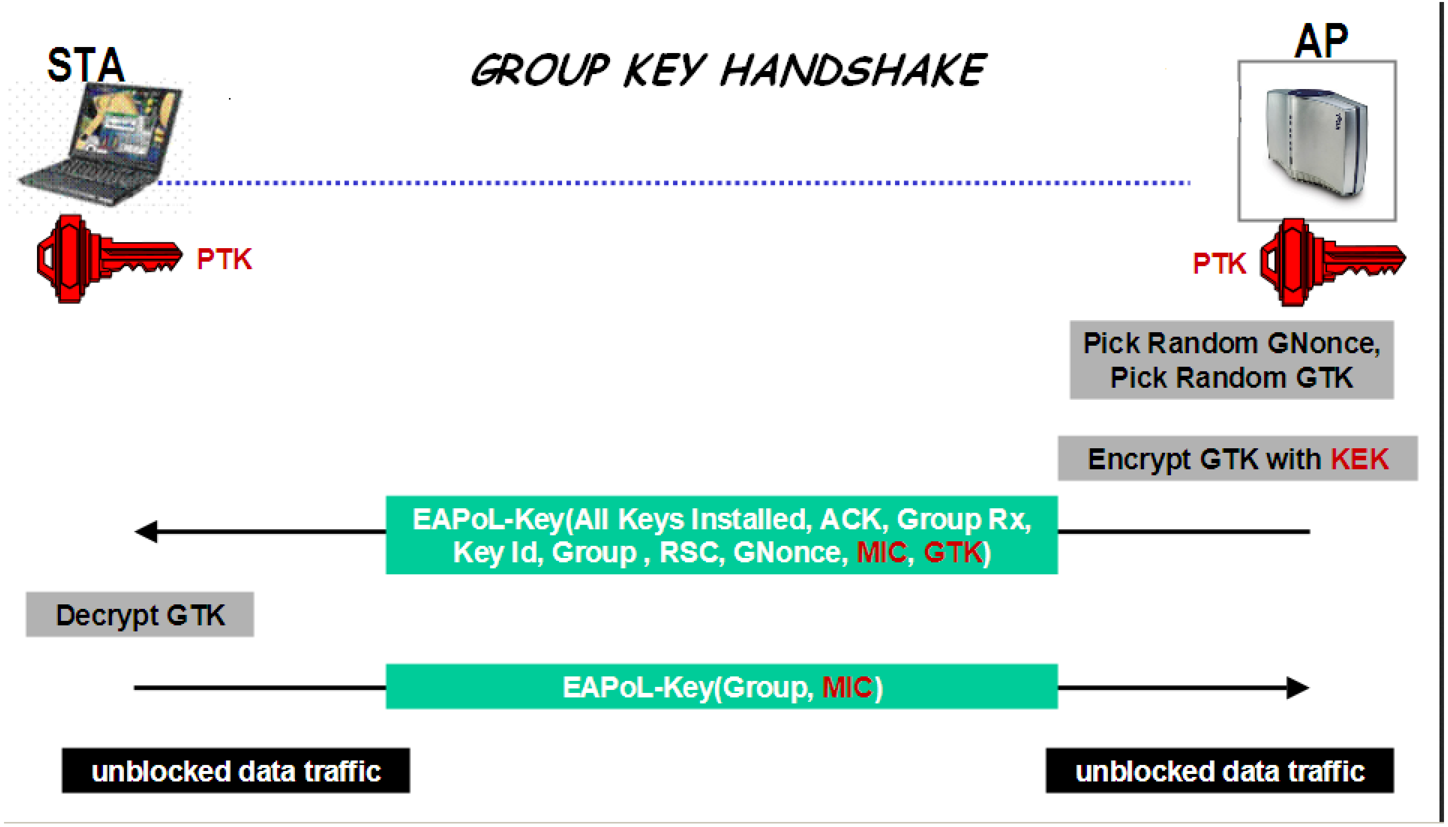
4-WAY HANDSHAKE

- The 4-way handshake is a 4 frame exchange between the supplicant and the authenticator.
- Using a pseudo-random function (PRF) the 4-way handshake will create the Pairwise Transient Key (PTK) by combining the PMK, an authenticator nonce, a supplicant nonce, the authenticator's MAC address (AA), and the supplicant's MAC address (SPA).
- PTK = PRF (PMK + ANonce + SNonce + AA + SPA)
- Message 1: The authenticator sends its ANonce to the supplicant. The supplicant now has all the information needed to generate the PTK using the pseudo-random function. The PTK protects the unicast data traffic.
- Message 2: The supplicant will send its SNonce to the authenticator. The authenticator now has all the information needed to generate a matching PTK using the pseudo-random function.
- Message 3: The authenticator generates the GTK from the GMK and transfers the GTK to the supplicant. The GTK is encrypted using the PTK and a secure exchange takes place. The GTK protects the broadcast and multicast traffic.
- Message 4: An acknowledgement that the client has successfully installed the PTK and GTK.

2-WAY GROUP KEY HANDSHAKE

- PTK and GTK are installed at the end of 4-way handshake.
- There needs to be a refreshing mechanism that refreshes the GTK.
- GTK refreshing can be done via two methods.
- Time Based (After certain amount of time. Default: 24hrs)
- Packet Based(After certain number of packets)
- We are supporting only time Based. User can configure the time after which the GTK refreshing can be done.
- GTK refreshing involves two handshake messages being exchanged between the Station and the Authenticator.

GROUP KEY HANDSHAKE



STA

AP

PTK

PTK

Pick Random GNonce,
Pick Random GTK

Encrypt GTK with KEK

EAPoL-Key(All Keys Installed, ACK, Group Rx,
Key Id, Group , RSC, GNonce, MIC, GTK)

Decrypt GTK

EAPoL-Key(Group, MIC)

unblocked data traffic

unblocked data traffic

2-WAY Group key handshake

- The Authenticator generates a new GTK. It encapsulates the GTK and sends an EAPOL-Key frame containing the GTK (Message 1)
- On receiving the EAPOL-Key frame, the Supplicant validates the MIC, decapsulates the GTK and installs GTK.
- The Supplicant then constructs and sends an EAPOL-Key frame in acknowledgment to the Authenticator. (Message 2)
- On receiving the Message 2, the authenticator

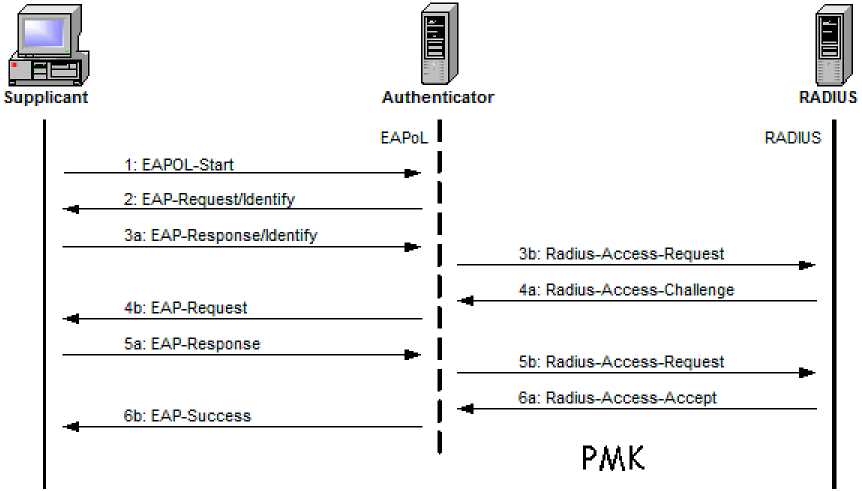
  installs the GTK.

Vulnerabilities of WPA2-PSK

- The same algorithm is used to generate the PMK key always. It is not dynamically calculated
- PSK - PMK = PBKDF2 (Password, SSID, SSIDlength, 4096, 256)
- In the above algorithm, if the inputs are known then the PMK can be found out using hacking mechanisms.
- For example, if the PSK, SSID and SSIDlength are known, Password can be found out, as the algorithm to generate the key is known.
- Password length is between 8 -64 ascii characters only
- To overcome these drawbacks, WPA2- ENTERPISE is used

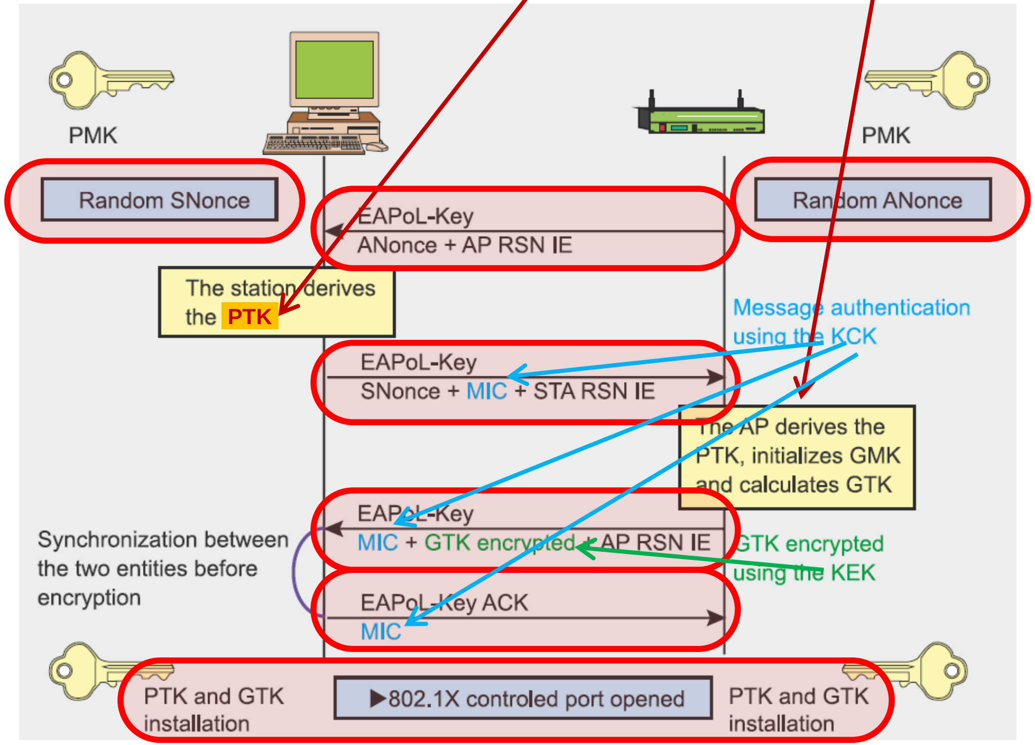
IEEE 802.11i: WPA2- ENTERPRISE

- Difference lies in the way how PMK gets generated.
- In PSK, the PMK is generated, using the alogrithm as mentioned earlier
- PSK = PMK = PBKDF2 (Password, SSID, SSIDlength, 4096, 256)
- In the case of WPA2-ENT, the PMK is generated and given by an External Radius Server. In the below image, PMK is received from the Radius Server in the Radius-Access-Accept message



4-WAY HANDSHAKE

PTK = EAPoL-PRF(PSK, ANonce | SNonce | AP MAC Addr | M’s MAC Addr)



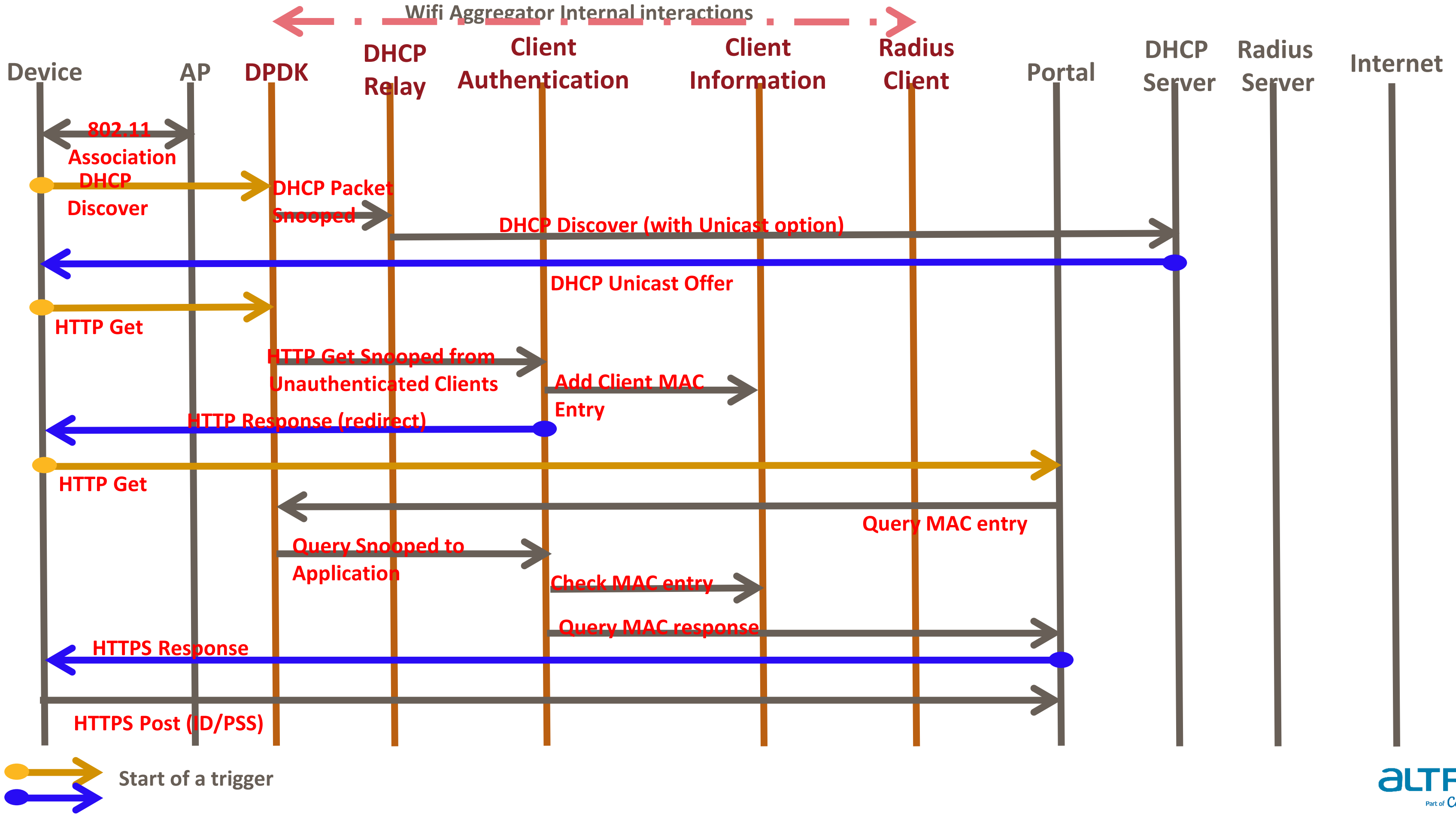
PMK
PMK
Random SNonce
Random ANonce
EAPoL-Key
ANonce + AP RSN IE
The station derives the PTK
Message authentication using the KCK
EAPoL-Key
SNonce + MIC + STA RSN IE
The AP derives the PTK, initializes GMK and calculates GTK
EAPoL-Key
MIC + GTK encrypted + AP RSN IE
GTK encrypted using the KEK
Synchronization between the two entities before encryption
EAPoL-Key ACK
MIC
PTK and GTK installation
▶802.1X controled port opened
PTK and GTK installation

IN A NUT SHELL

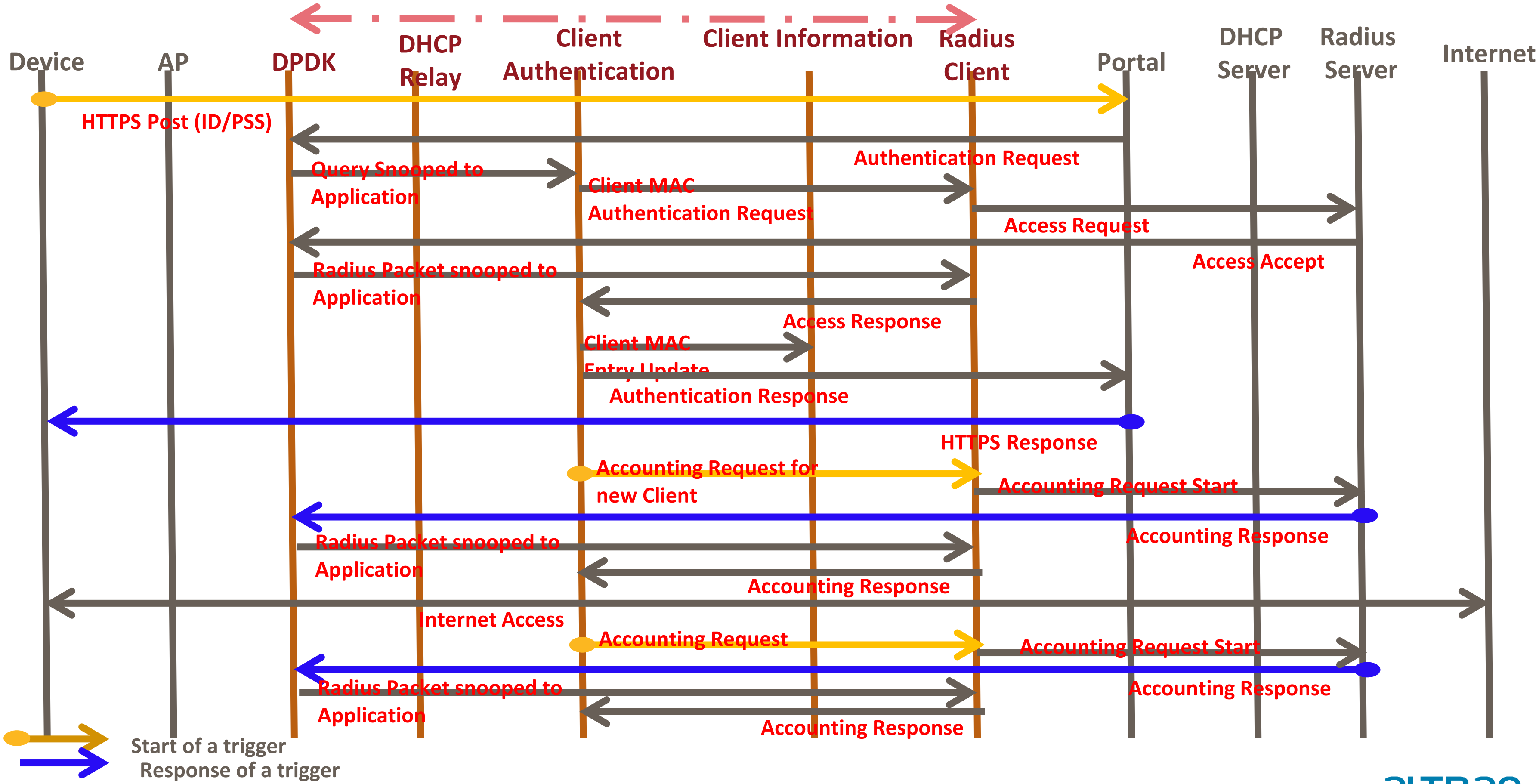
802.11i provides

- Data confidentiality; ensures only authorized parties can access the information
- Authentication; provides proof of genuineness of the user
- RSNA-PSK and RSNA-ENT are widely used authentication methods in the present world and in the near future

Captive Portal



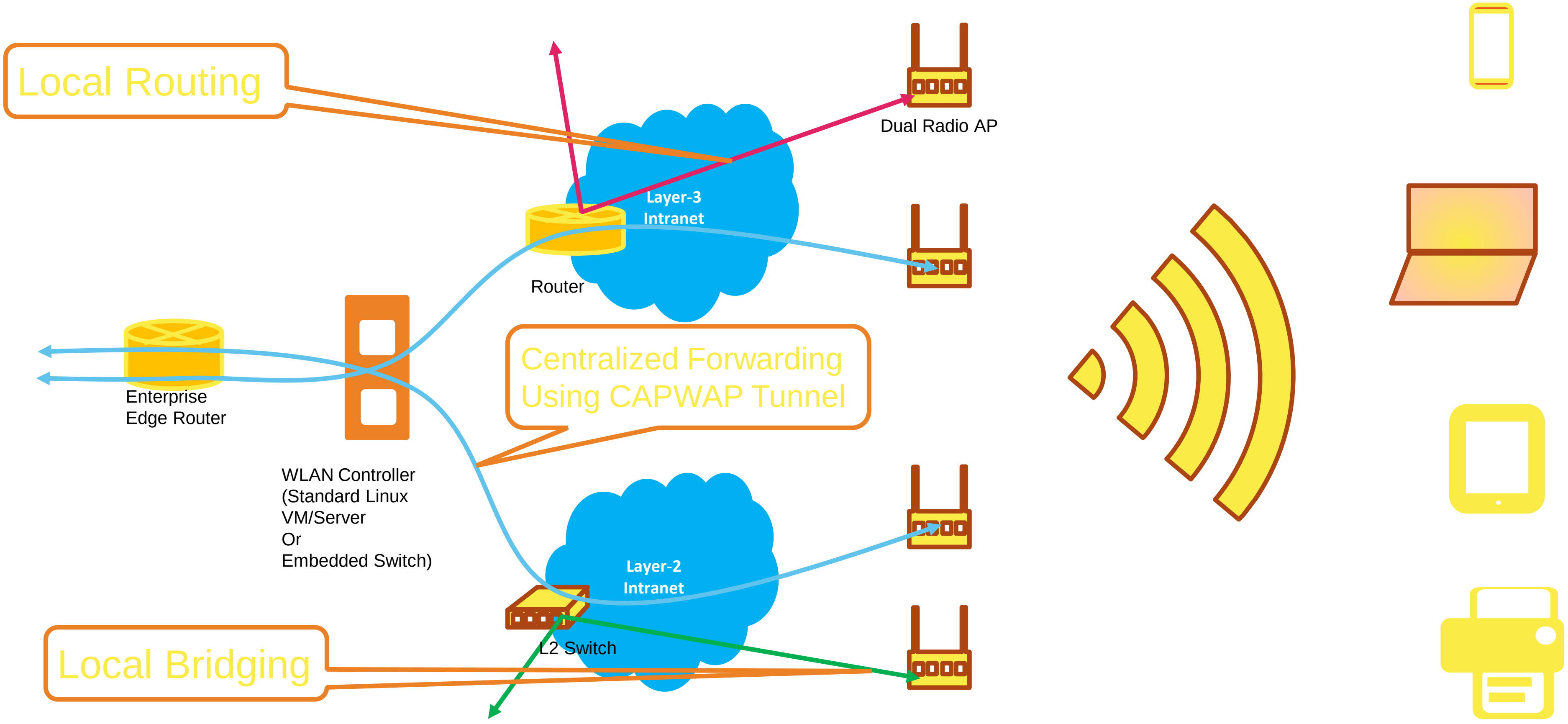
Captive Portal



altran Part of Capgemini

Infrastructure Wi-Fi

Enterprise Deployment

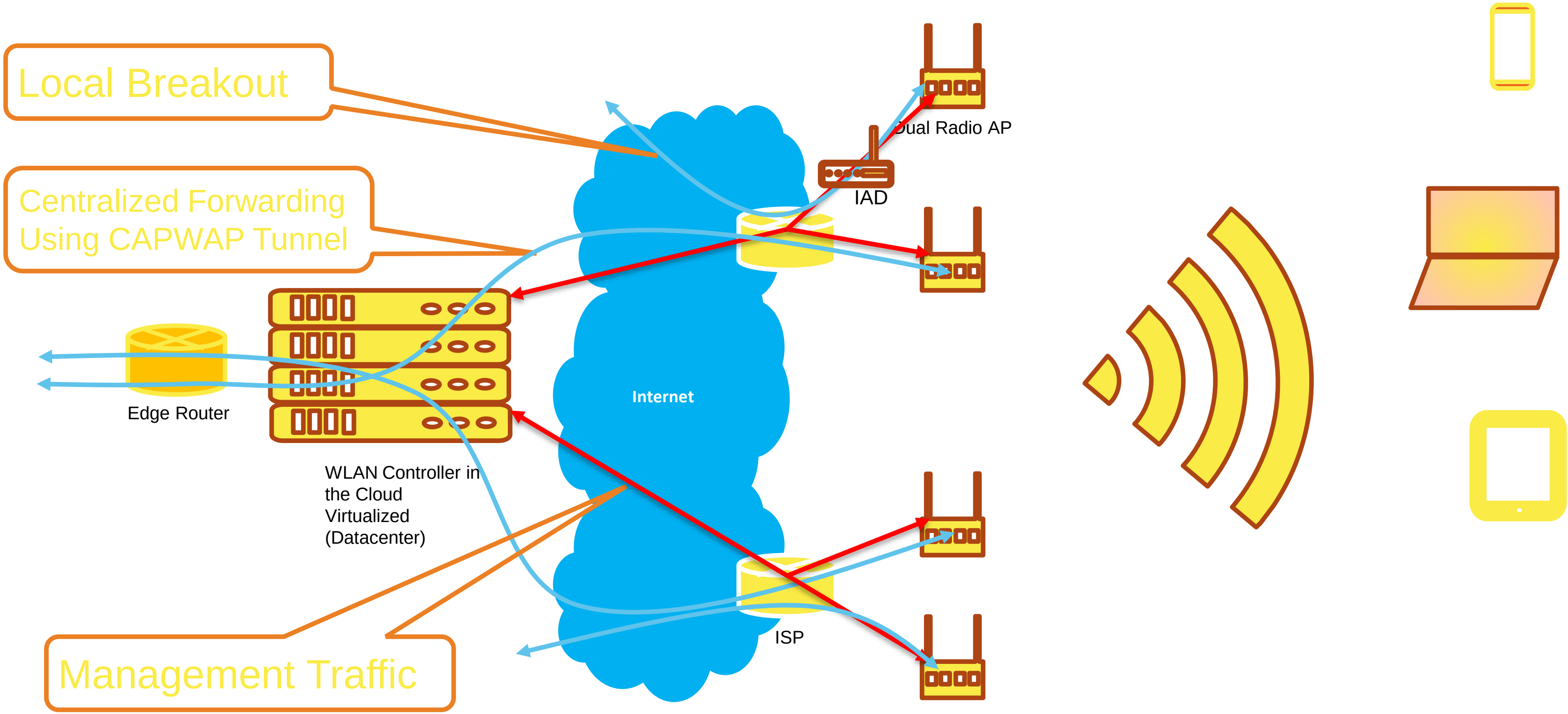


Local Routing

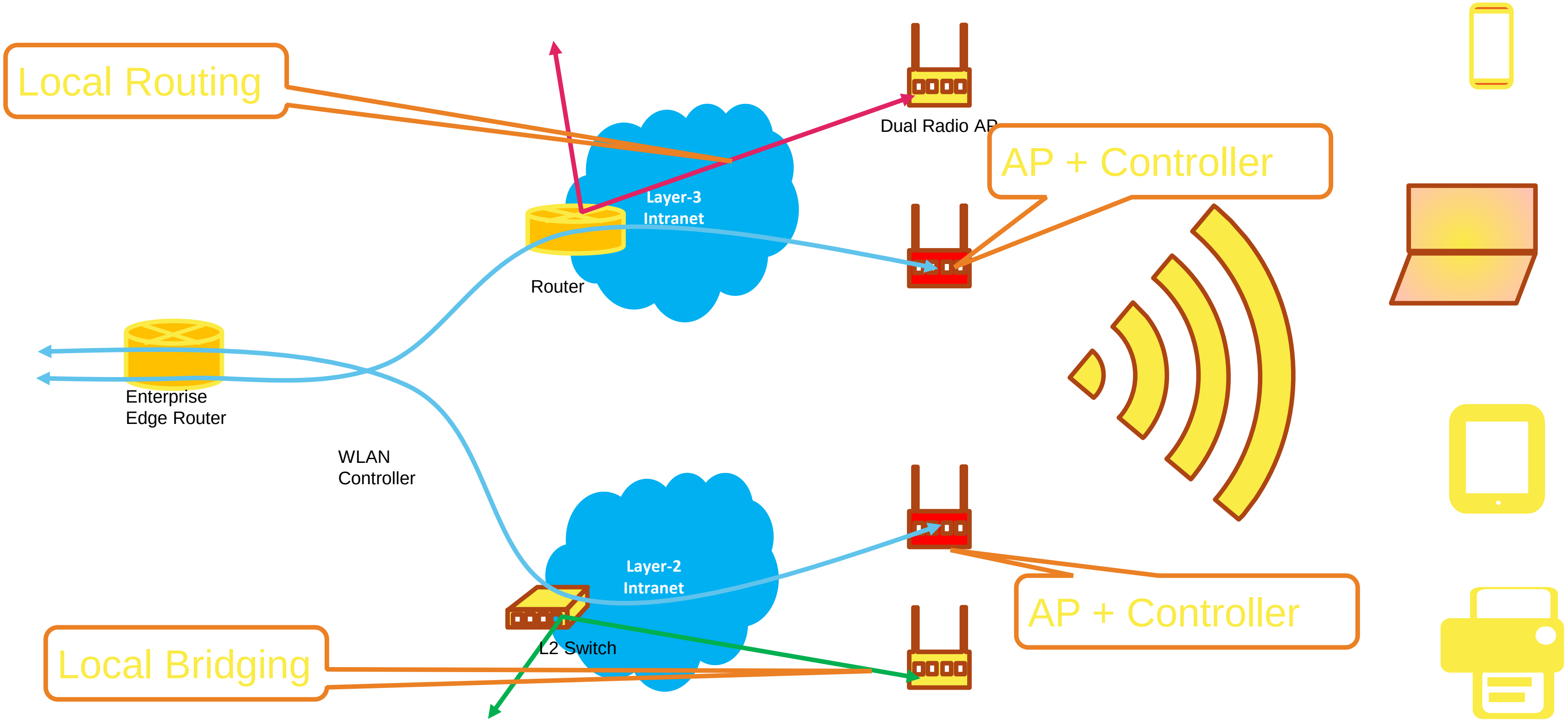
Centralized Forwarding Using CAPWAP Tunnel

Local Bridging

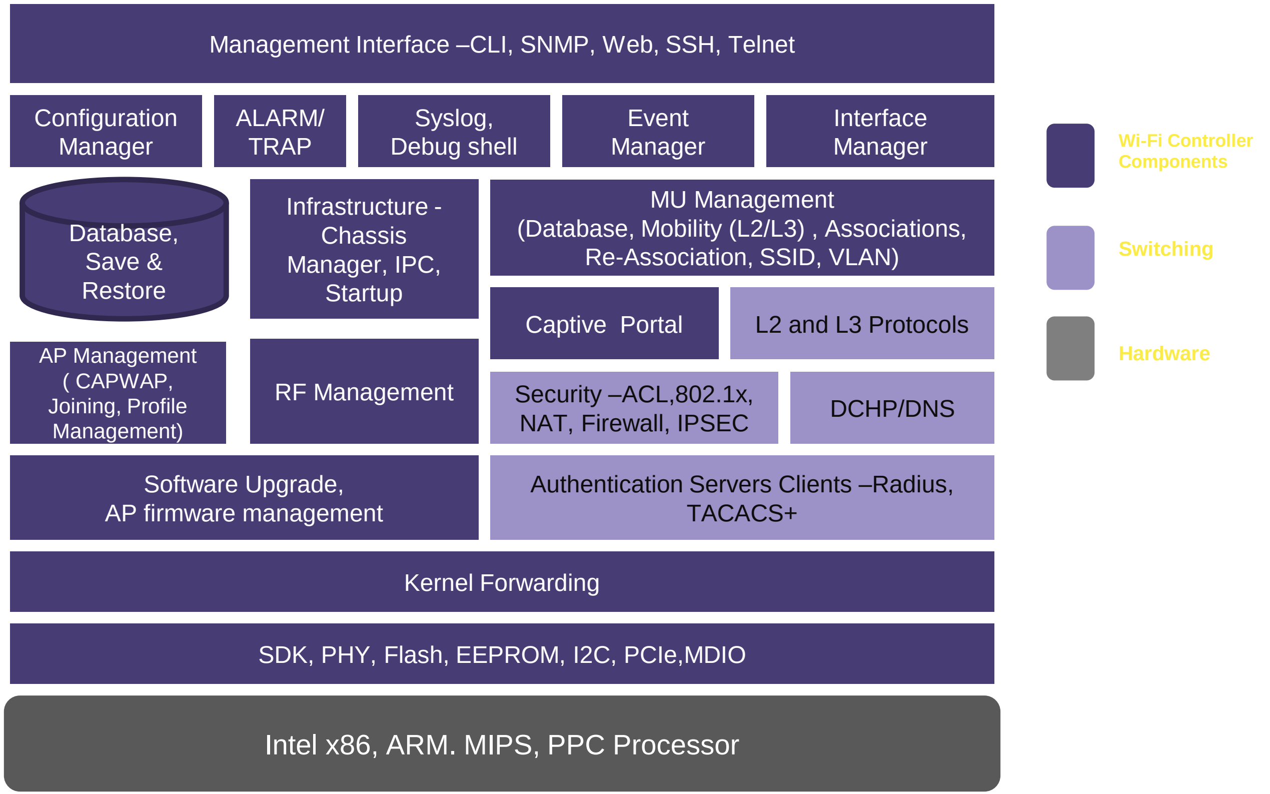
Cloud Deployment


Local Breakout
Centralized Forwarding Using CAPWAP Tunnel
Dual Radio AP
IAD
Edge Router
Internet
WLAN Controller in the Cloud Virtualized (Datacenter)
ISP
Management Traffic

Controller Less Access Point Deployment



Aricent's Wi-Fi Controller Software Architecture



Management Interface –CLI, SNMP, Web, SSH, Telnet

Configuration Manager

ALARM/ TRAP

Syslog, Debug shell

Event Manager

Interface Manager

Database, Save & Restore

Infrastructure - Chassis Manager, IPC, Startup

MU Management (Database, Mobility (L2/L3) , Associations, Re-Association, SSID, VLAN)

Captive Portal

L2 and L3 Protocols

AP Management (CAPWAP, Joining, Profile Management)

RF Management

Security –ACL,802.1x, NAT, Firewall, IPSEC

DCHP/DNS

Software Upgrade, AP firmware management

Authentication Servers Clients –Radius, TACACS+

Kernel Forwarding

SDK, PHY, Flash, EEPROM, I2C, PCIe,MDIO

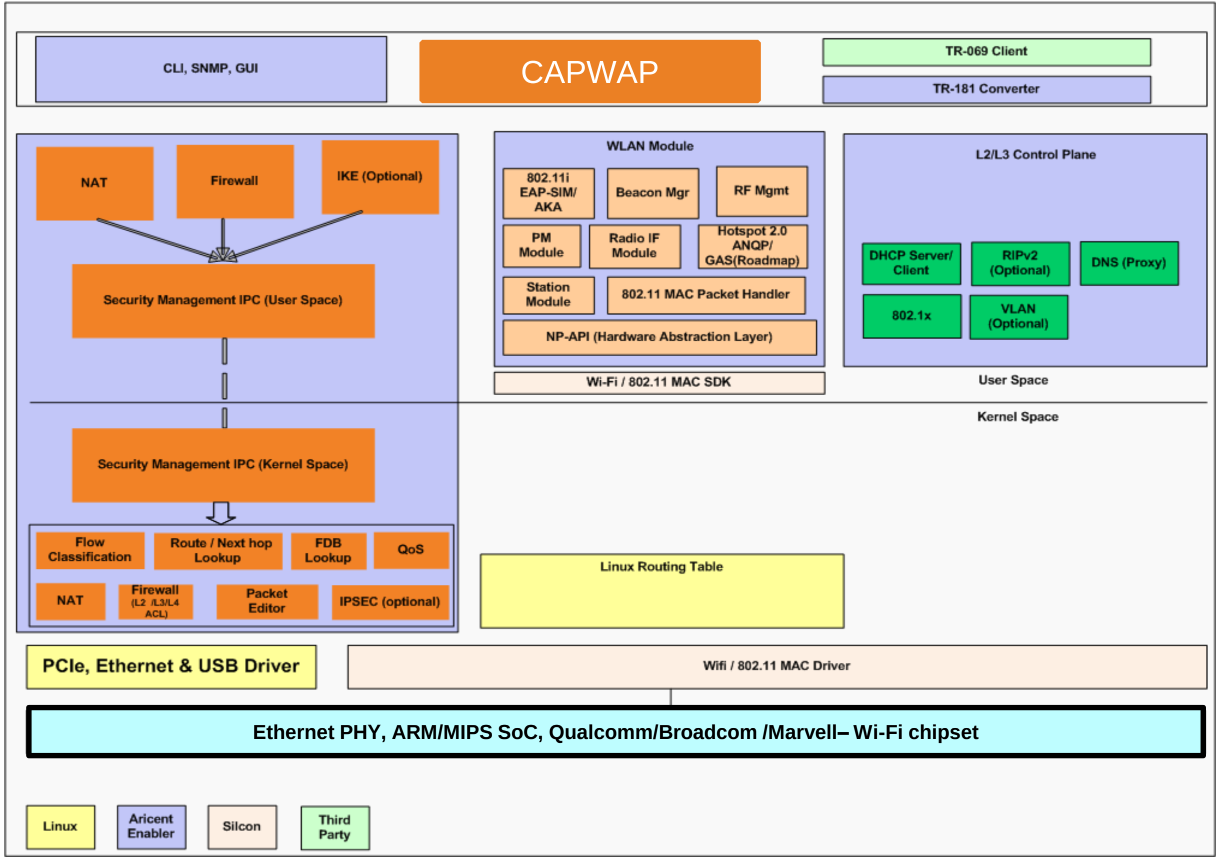
Intel x86, ARM. MIPS, PPC Processor

■ Wi-Fi Controller Components

■ Switching

■ Hardware

High Level Software Architecture –



CLI, SNMP, GUI

CAPWAP

TR-069 Client

TR-181 Converter

NAT

Firewall

IKE (Optional)

Security Management IPC (User Space)

Security Management IPC (Kernel Space)

Flow Classification

Route / Next hop Lookup

FDB Lookup

QoS

NAT

Firewall (L2 /L3/L4 ACL)

Packet Editor

IPSEC (optional)

WLAN Module

802.11i EAP-SIM/ AKA

Beacon Mgr

RF Mgmt

PM Module

Radio IF Module

Hotspot 2.0 ANQP/ GAS(Roadmap)

Station Module

802.11 MAC Packet Handler

NP-API (Hardware Abstraction Layer)

Wi-Fi / 802.11 MAC SDK

L2/L3 Control Plane

DHCP Server/ Client

RIPv2 (Optional)

DNS (Proxy)

802.1x

VLAN (Optional)

User Space

Kernel Space

Linux Routing Table

PCIe, Ethernet & USB Driver

Wifi / 802.11 MAC Driver

Ethernet PHY, ARM/MIPS SoC, Qualcomm/Broadcom /Marvell– Wi-Fi chipset

Linux

Aricent Enabler

Silcon

Third Party

Hotspot 2.0

Goals

- **Make Wi-Fi access seamless and transparent**
- **Remove manual end-user intervention**
- **Enable network/device to make decision automatically**
- **Services come to end-user rather have end-user look for them**

Use Cases

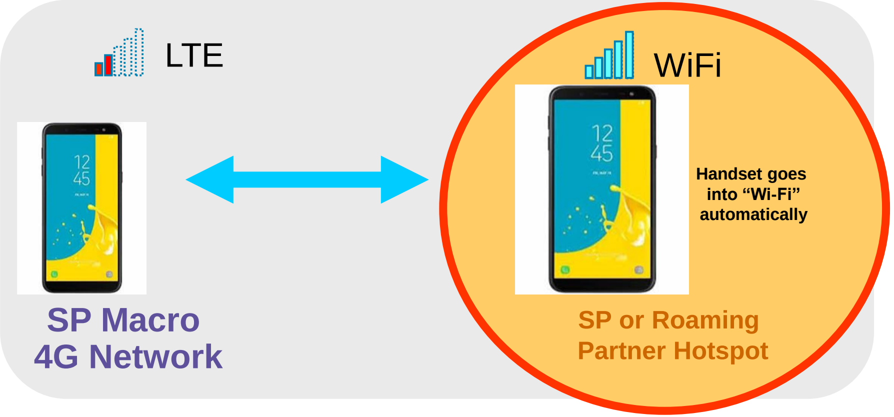
Seamless Data Connectivity

Hotspot 2.0:
Turn it on and Get Access

- Turn it on and seamlessly get access
- Access can be 4G or Wi-Fi
- No manual end-user interaction
- No need to program SSIDs, store SSIDs, maintain SSIDs, search for SSIDs, etc.

Seamless Data Roaming

Subscriber with Wi-Fi Data Plan Seamlessly Connects to Hotspot

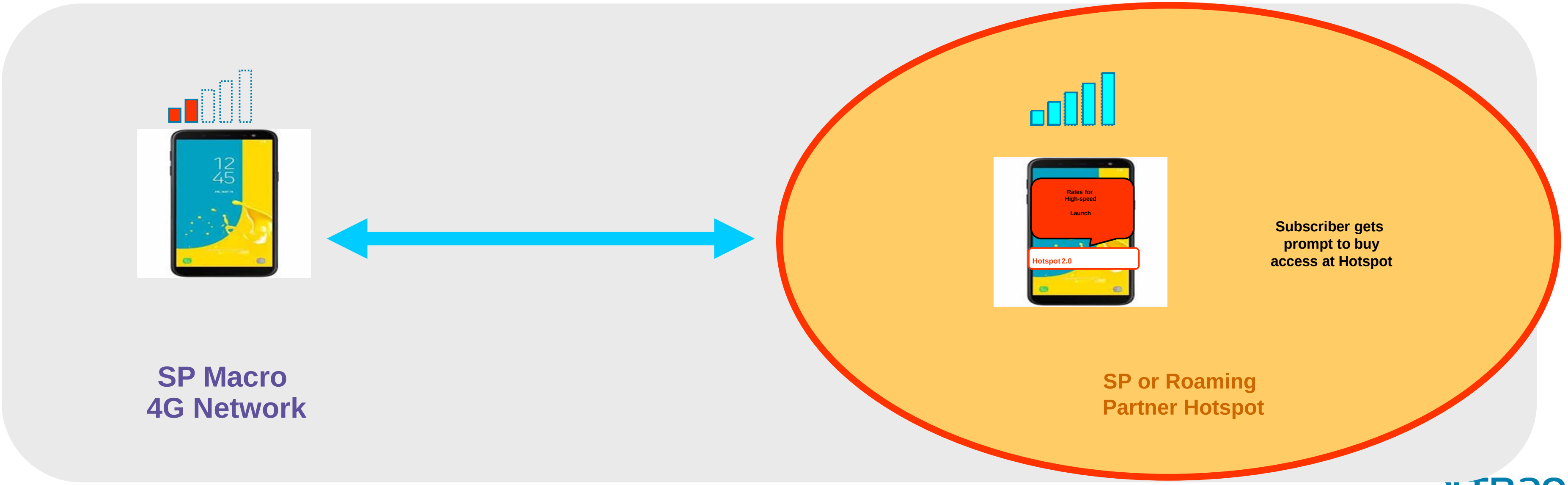


LTE
WiFi
Handset goes into “Wi-Fi” automatically
SP Macro 4G Network
SP or Roaming Partner Hotspot

Use Cases

Online Sign-up

Example: Subscriber Without Data Plan Gets Prompt for One



Subscriber gets prompt to buy access at Hotspot

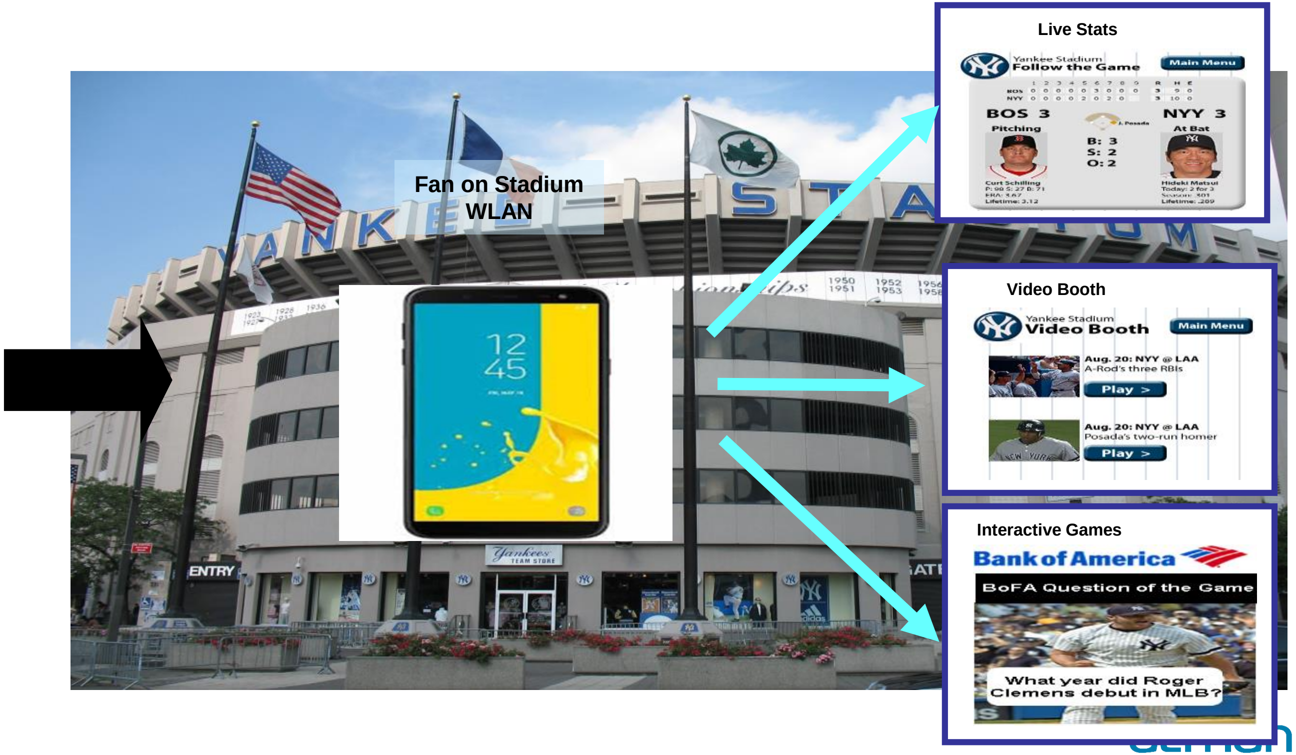
SP Macro 4G Network

SP or Roaming Partner Hotspot

Use Cases

Guest Access

Example: Consumer



Fan on Stadium WLAN

Live Stats

Yankee Stadium
Follow the Game

Main Menu

	1	2	3	4	5	6	7	8	9	R	H	E
BOS	0	0	0	0	0	3	0	0	0	3	9	0
NYY	0	0	0	0	2	0	2	0		3	10	0

BOS 3 | NYY 3

Pitching | At Bat

J. Posada

B: 3
S: 2
O: 2

Curt Schilling
P: 98 S: 27 B: 71
ERA: 3.67
Lifetime: 3.12

Hideki Matsui
Today: 2 for 3
Season: .301
Lifetime: .289

Video Booth

Yankee Stadium
Video Booth

Main Menu

Aug. 20: NYY @ LAA
A-Rod's three RBIs

Play >

Aug. 20: NYY @ LAA
Posada's two-run homer

Play >

Interactive Games

Bank of America

BoFA Question of the Game

What year did Roger Clemens debut in MLB?

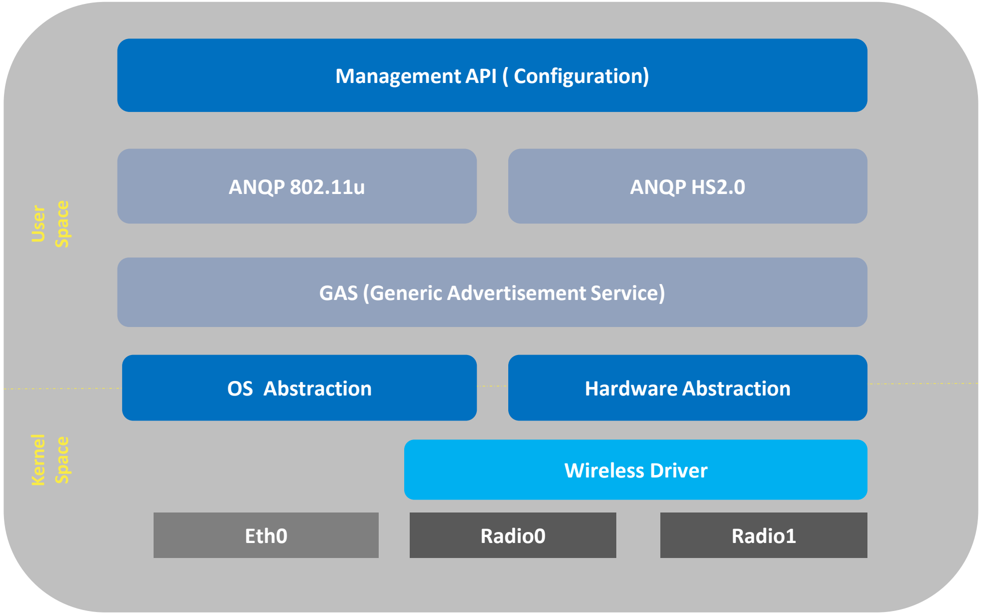
Hotspot 2.0 Architecture

Hotspot (1.0) Challenges

- Complicated Login Procedure
- Problems with Time Limited Credentials
- Time consuming hotspot selection
- Hotspots Operated by Roaming Partners
- Various Security Threats to the Hotspots
- Ability to bring Cellular user experience to Hotspot Users
- Industry divided/proprietary solutions on interworking with external networks

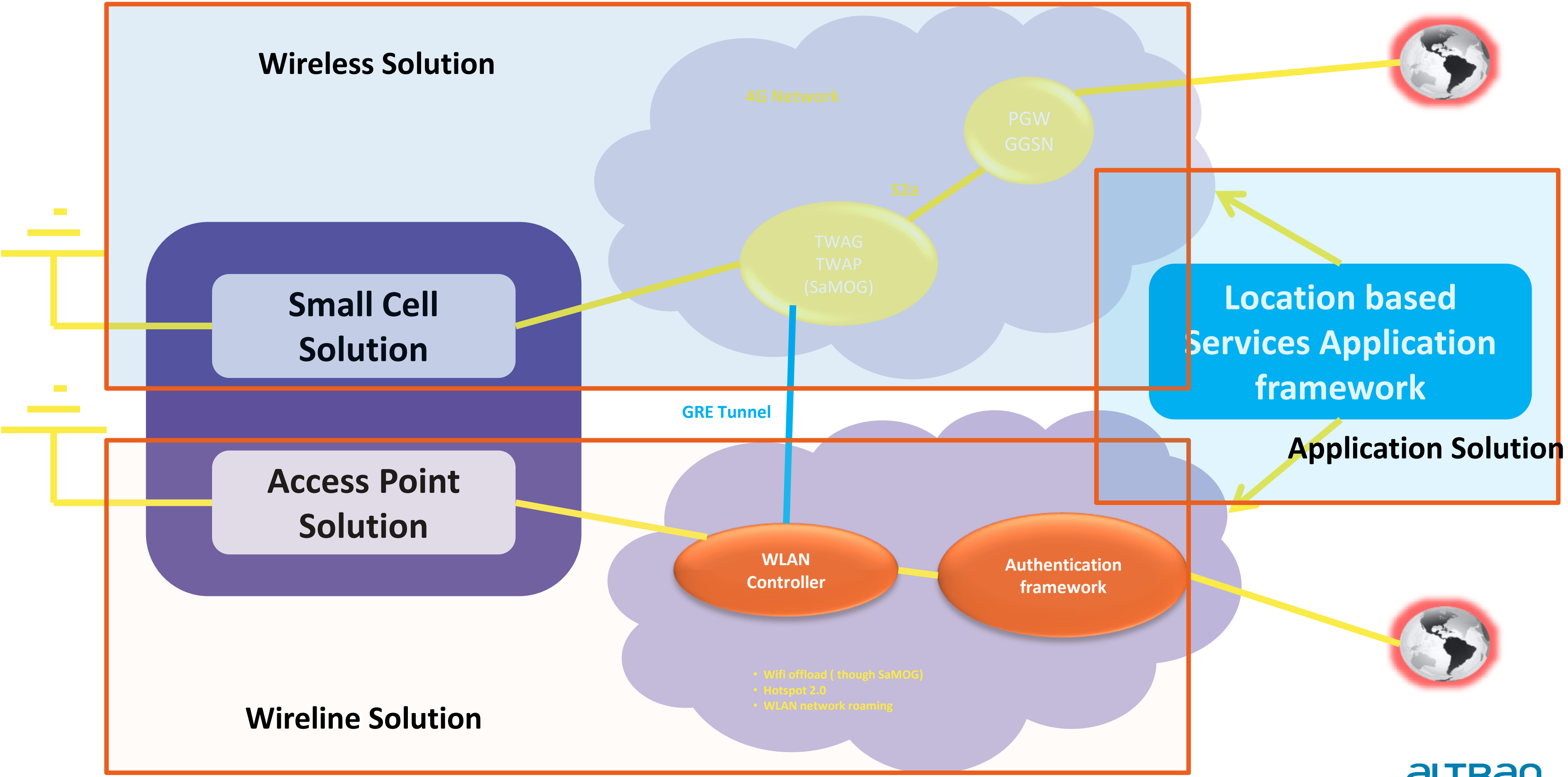
Solution –Hotspot 2.0

- Service Provider Wi Fi Architecture
- 3G-like end-user experience to Wi-Fi authentication and roaming
- IEEE 802.11u Standard Compliant Solution
- Enable service providers to better manage and monetize their hotspots.
- Stronger EAP based Authentication
- Standard based Service Discovery
- Based on WPA2-Enterprise



Aricent Solution for Hotspot 2.0

Wi-Fi Offload



Wireless Solution

4G Network

PGW
GGSN

S2a

TWAG
TWAP
(SaMOG)

Small Cell Solution

GRE Tunnel

Access Point Solution

WLAN Controller

Authentication framework

- Wifi offload (though SaMOG)
- Hotspot 2.0
- WLAN network roaming

Wireline Solution

Location based Services Application framework

Application Solution

802.11ad Overview

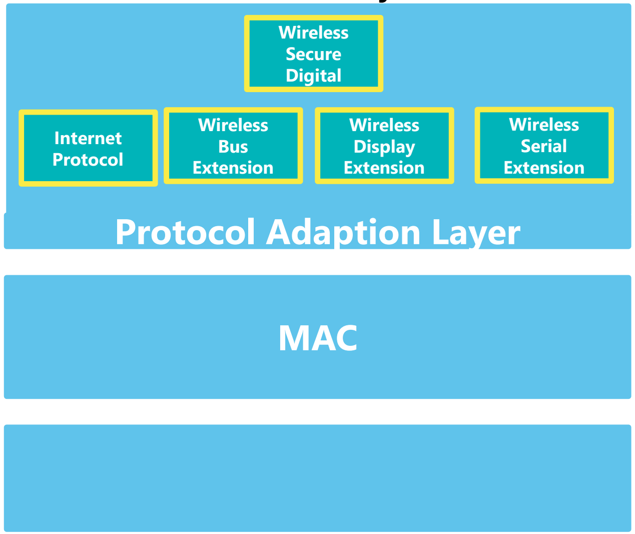
802.11ad – Technology

- The multi-gigabit wireless communication technology is based on IEEE 802.11ad, the standard wireless communications in 60 GHz. The 60 GHz band has more spectrum available than the 2.4 GHz and 5 GHz bands, allowing for wider channels to support faster data rates of up to 7 Gbps using low power modulation schemes, making it ideal for in-room connectivity to support demanding multimedia applications. (In-Room simply because 60 GHz transmission has large attenuation through physical barriers.)
- The key trigger for 60 GHz use are –
  - Wireless Display / Audio
  - In-room Video Application
  - Upload / Download & Docking
  - The wide adoption of tri-band chipsets to create concurrent 2.4/5/60 GHz devices running 802.11ac/n and 11ad (802.11ac and 802.11ad are compatible at the MAC or Data Link layer, and differ only in PHY)
  - At 60 GHz and the lightly licensed bands above, growth in "line of sight" backhaul for smalls cells and Wi-Fi hotspots.
  - 60GHz has a shorter range and thus other networks are less likely to intercept / interfere and thereby makes it more secure.

802.11ad – Technology

- 57-66 Ghz band
- Throughput up to 7 Gbps
- Beamforming
- P2P & LoS technology

Protocol Layers



Wireless Secure Digital

Internet Protocol

Wireless Bus Extension

Wireless Display Extension

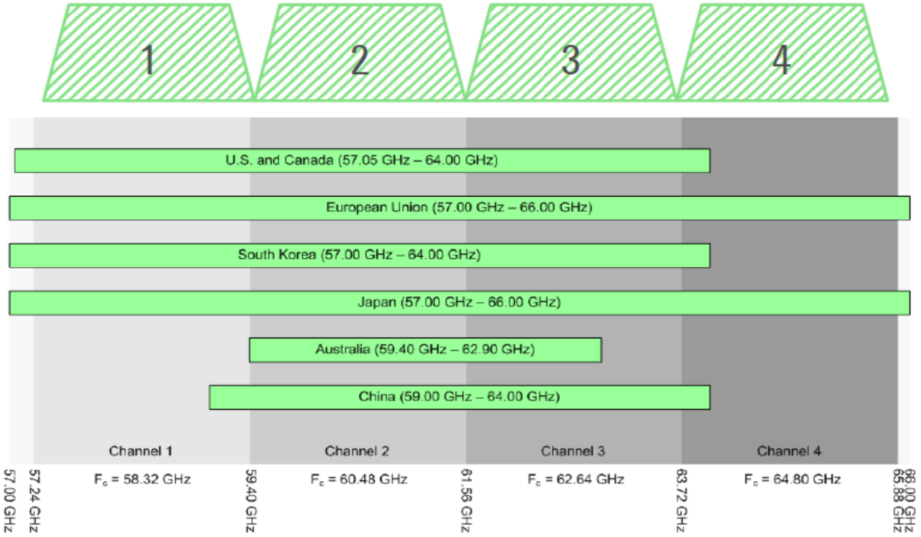
Wireless Serial Extension

Protocol Adaption Layer

MAC

* Optional

60 GHz Channel Plan by Region



Mandatory MCS PHY rates

- Single Carrier PHY : mcs 1-12
- Low power single carrier PHY : mcs 25-31
- OFDM PHY : mcs

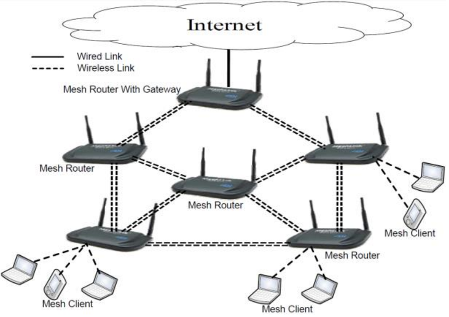
Use Cases

Wireless Docking and Display

Wireless PC

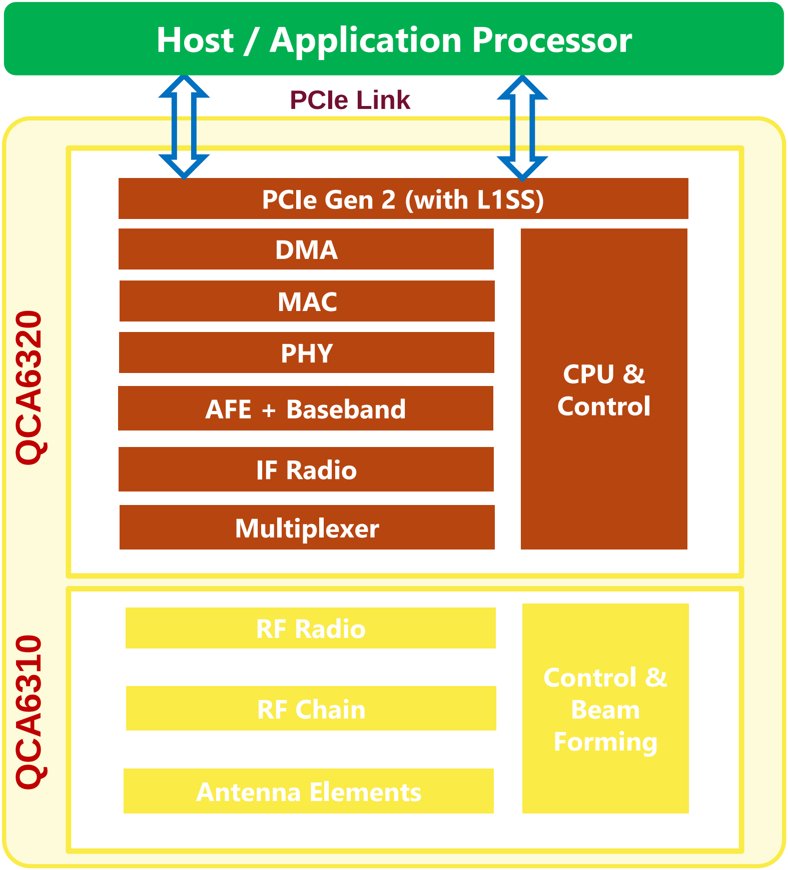
Rapid Upload / Download

Mesh Backhaul



HDTV distribution

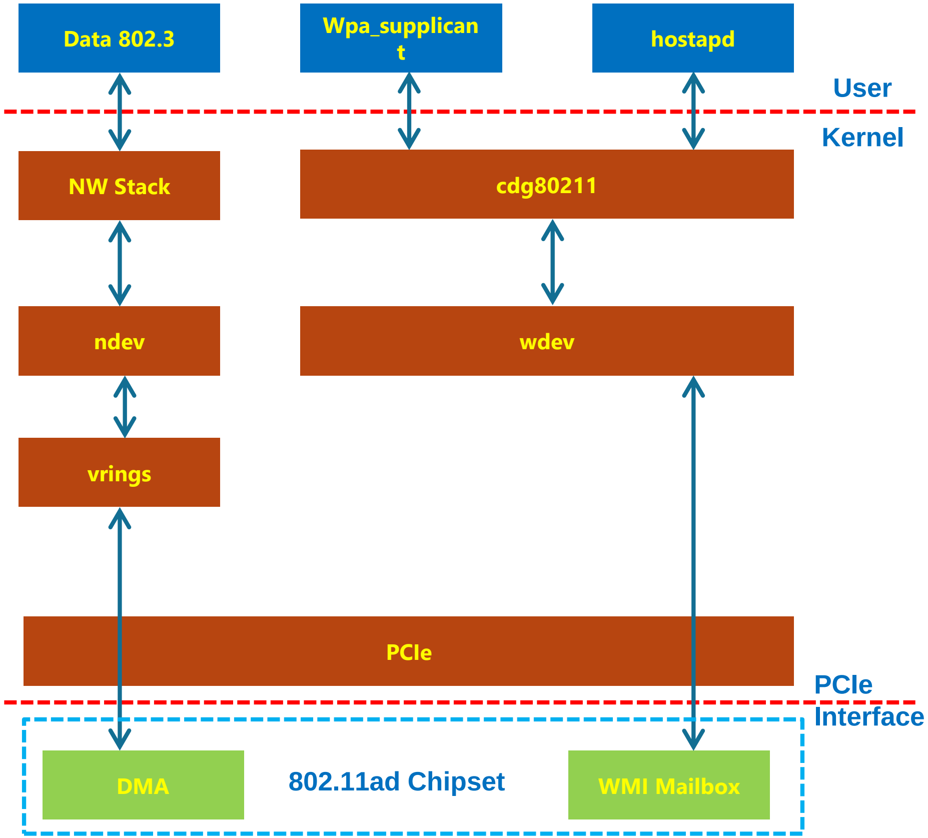
Qualcomm QCA6310 & QCA6320 Architecture



- **L1SS** – Per PCIe spec, L1 state can be utilized to reduce power consumption by controlling the PCIe configuration bit via software. However it is found to be not sufficient due to other factors such as leakage etc. Hence additional L1 state called L1SS (L1 sub-states) has been defined. L1 sub-states adds two “pseudo sub-states,” called L1.1 and L1.2, to the LTSSM, which can be used to turn off additional analog circuits in the PHY. L1.1 allows the common-mode voltage to be maintained, while L1.2 allows all high-speed circuits to be turned off.
- **QCA6320** – 28nm HPM (High Performance Mobile) Baseband. Implements 802.11ad 4.6 GBPS device. Off Load engine. PCIe Host Interface, 15GHz IF Interface (Data, Control & DC)
- **QCA6310** – The QCA6310 is 60GHz RFIC solution. During TX it gets a 15 GHz IF signal from QCA6320 802.11ad MAC processor and up converts it to a 60 GHz signal and during receive, it receives 60 GHz signal and down converts it to a 15 GHz signal going to QCA6320.

The QCA6320 when combined with QCA6310 (the RFIC) will communicate over 60 GHz frequency at 4.6 GHz speed using Single Carrier transmission. It supports large Antenna Chains (up to 32 Antennas) and also implements Beam Forming technology.

Linux Driver for Interfacing App Processor with QCA6320/6310

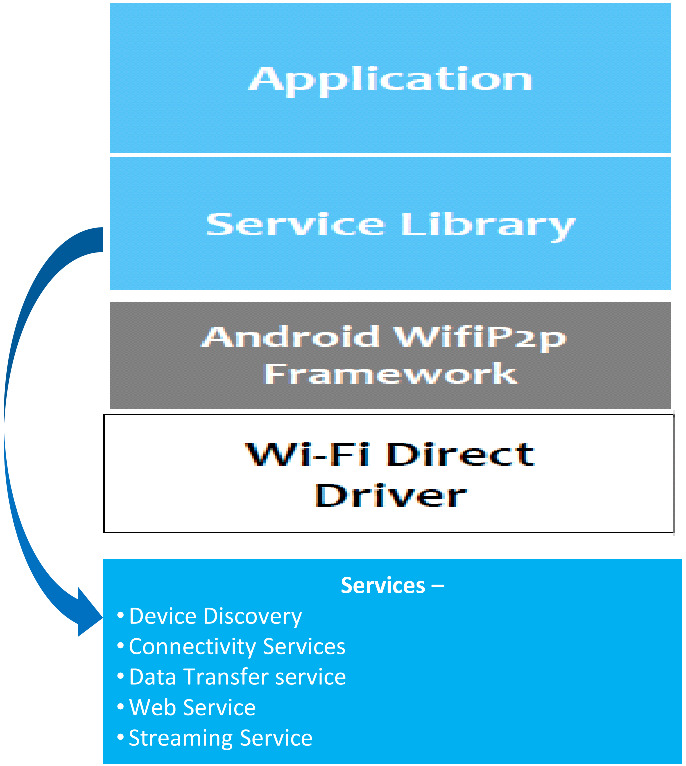


- For integration with the host Application Processor, platform specific driver module is required which will work along with the 802.11ad driver. Amongst the other things, this driver will perform are - PCIe enumeration and PCIe Suspend / Resume using the PCIe Root Complex driver.
- The Driver will have to be registered with the Linux PCIe Framework.
- The driver will use standard cfg80211 and NetDev APIs for Control & Data Paths.
- Control Path with the card is done through WMI (Wireless Module Interface) commands and events. The Host Driver will access the mailbox within the 802.11ad device memory. There are 2 similar mailbox structures: one for **host** → **card** commands, and one for **card** → **host** events.
- Data Path - DMA using 'Vring' structures. Vring in consistent memory, hold descriptors that points to the data buffers. Card to write status back to the descriptor.
- The Chipset Firmware flashing may not be required. In the current version, firmware stored in the flash memory on the Chipset and not downloaded by the driver. Firmware flashing required for the upgrade only. Need to check this aspect.
- The driver uses cfg80211 framework, but not mac80211 as the MAC is inbuilt into the 802.11ad chipset.

Wi-Fi Direct

Wifi Direct

- WiFi-Direct a “peer-to-peer” mode
- WiFi that does not require transmissions via a separate access point
- Wi-Fi Direct builds upon the successful IEEE 802.11 infrastructure mode and lets devices negotiate who will take over the AP-like functionalities
- P2P GO and client functionality is dynamic and is negotiated at the time of initial network setup
- Default Wi-Fi Direct uses WPA2PSK as security standard
- Multiple devices, tablets provide support for Wifi P2P framework
- Innovative Service creations, APIs and facilitation for rapid application development



Services –

- Device Discovery
- Connectivity Services
- Data Transfer service
- Web Service
- Streaming Service

Indoor Positioning System

Key Features of Indoor Positioning (1/2)

Tracking:

The solution facilitates position tracking using the following ways:

Bluetooth low energy (BLE)-based location tracking on Android and iOS platforms. WiFi-based location tracking using WiFi trilateration and fingerprinting to track the location. Network-based location tracking using GMLC node in the network to determine location

Floor Map Integration:

Displays 2D floor map images with Cartesian co-ordinates. Admin interface to upload the floor map. Provision to Integrate with third-party indoor maps. Multi-Floor detection.

Point of Interest (POI) Setup:

Option of adding/updating a new POI, which can be defined either by providing X and Y co-ordinates or by marking point, radius and labels in the floor map. POIs are of two types — access points (beacons, WiFi and BLE) and areas (entry door, exit door, pantry, conference rooms and cubicle).

Navigation:

Option to navigate from current location to desired POI. This is achieved using floor map, compass, accelerometer, algorithm and/or WiFi-based location and device sensors.

Key Features of Indoor Positioning (2/2)

Content Definition:

Option to upload content types - images, text, videos and html. Option to edit content using a rich text editor.

Dynamic Messaging using Rule Engine:

Option to display dynamic content to users depending upon physical location, IN and OUT movements, demographics and device types.

Alerts and Notifications:

Supports alerts and notifications through text messages, emails and push notifications.

Security:

Highly secured solution mandating use of login credentials and role-based access. Also, with multi-tenancy feature, each tenant has its unique, secured set of data elements, but application infrastructure is shared.

Indoor Positioning **Solution Architecture**

Indoor positioning solution enables our enterprises to track and trace the user or an asset inside the building or closed area where satellite-based tracking is not accurate enough

Protocols

WiFi Fingerprinting & Trilateration

Beacons

Network Integration

Modules

Proximity Sensing
Ambient Location
Absolute Location

Content Definition

Floor Map Integration

Rule Engine

Inertial Navigation
Point to Point Nav

Alerts and Notification

Repository

Multi-Tenant
User Profile
User Movement
Logs
Floor Data
Events
Content

altran

Part of Capgemini