Wi-Fi Technology Fundamentals

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

Module-4

Security in Wi-Fi

Session-4d

Seamless Connectivity/Hotspot2.0/Open Roaming

Last Session Recap……

Module-4

Security in Wi-Fi

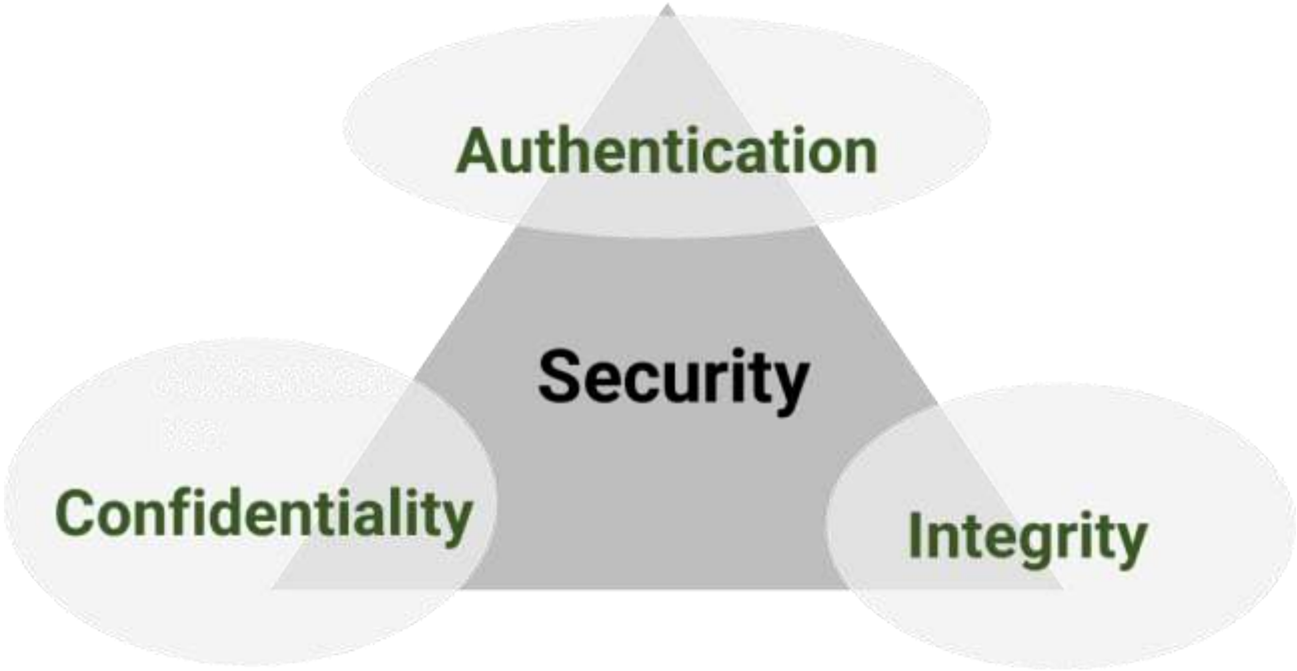
Session-4c

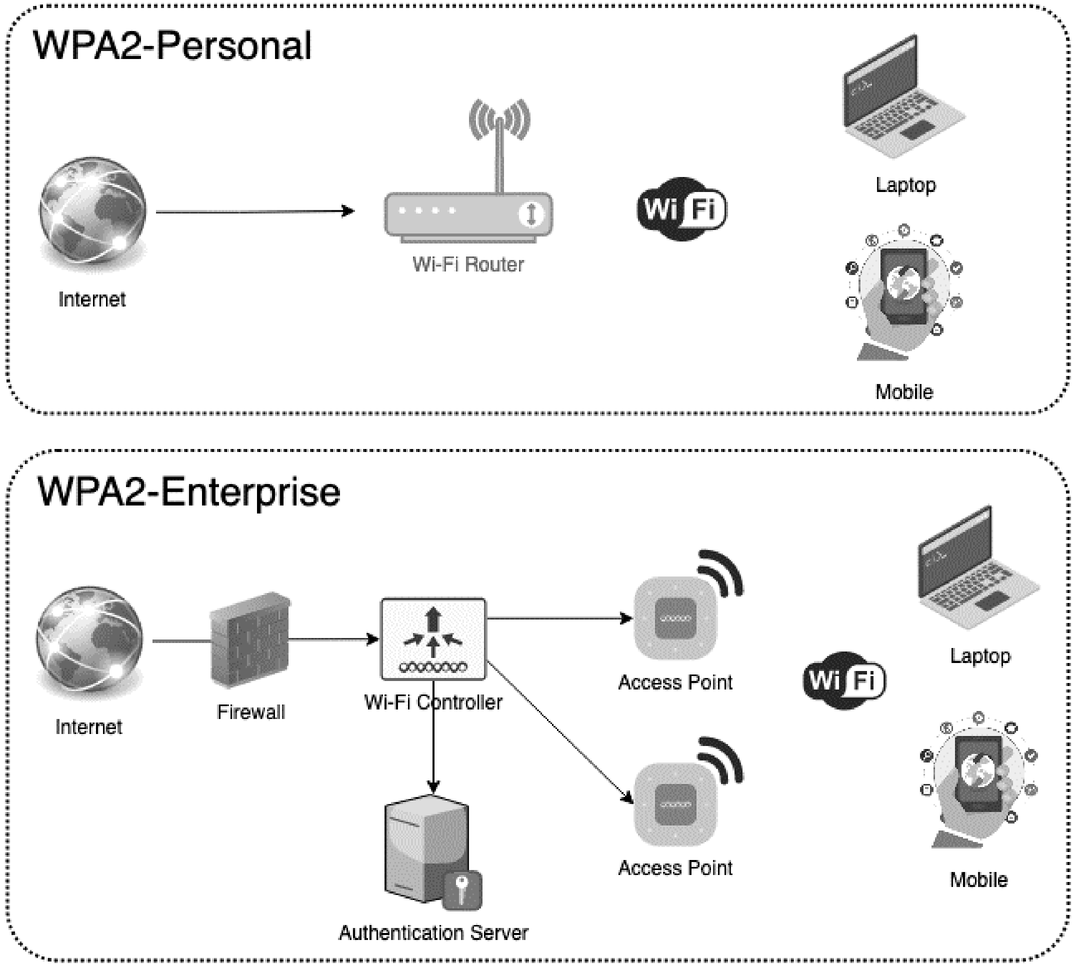
Attacks and Vulnerabilities

- ✓ Wireless Eavesdropping (Passive Attacks)
- ✓ Wireless Jamming
- ✓ Rogue Access Points
- ✓ WEP/WPA Cracking
- ✓ Evil Twin Attacks
- ✓ Deauthentication/Disassociation Attacks
- ✓ Man-in-the-Middle Attacks
- ✓ Replay attacks

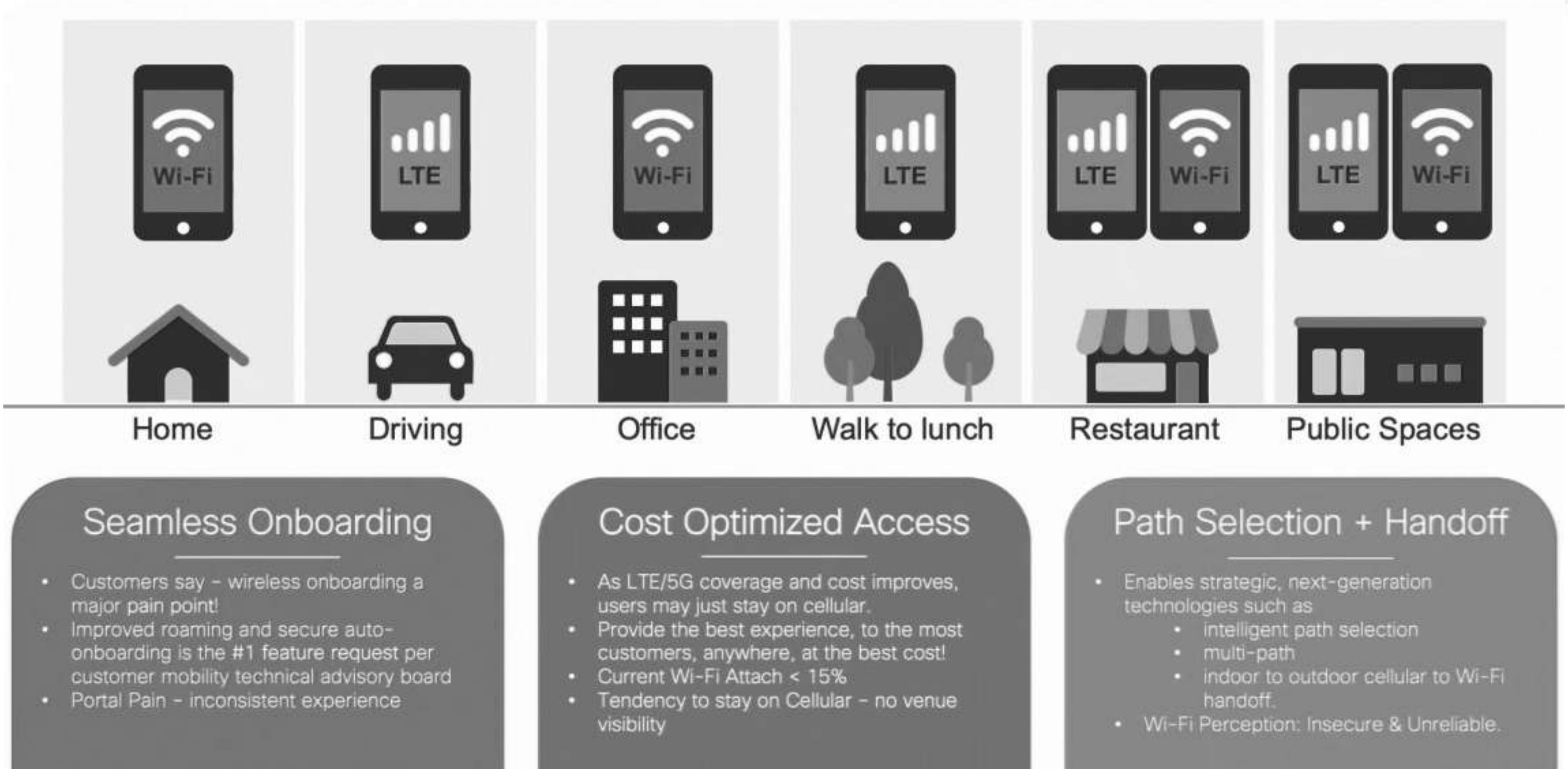
Wi-Fi Security in a Single Location

- Security problem confined to a single location or a group of locations within a single organization.
- Pre-shared Key based security in homes.
- Server based security in enterprises.





Day in the Life of a Mobile Device



Seamless Onboarding

- Customers say – wireless onboarding a major pain point!
- Improved roaming and secure auto-onboarding is the #1 feature request per customer mobility technical advisory board
- Portal Pain – inconsistent experience

Cost Optimized Access

- As LTE/5G coverage and cost improves, users may just stay on cellular.
- Provide the best experience, to the most customers, anywhere, at the best cost!
- Current Wi-Fi Attach < 15%
- Tendency to stay on Cellular – no venue visibility

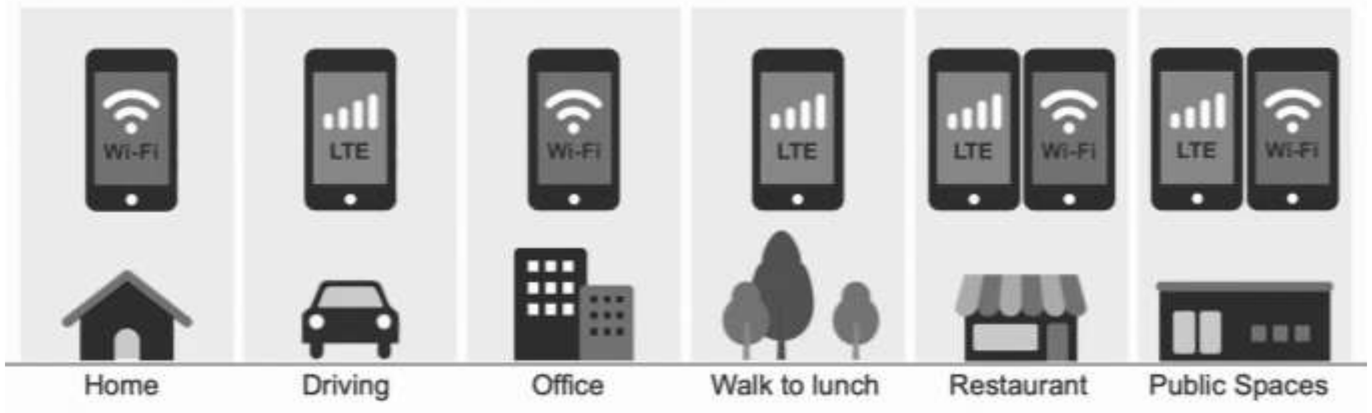
Path Selection + Handoff

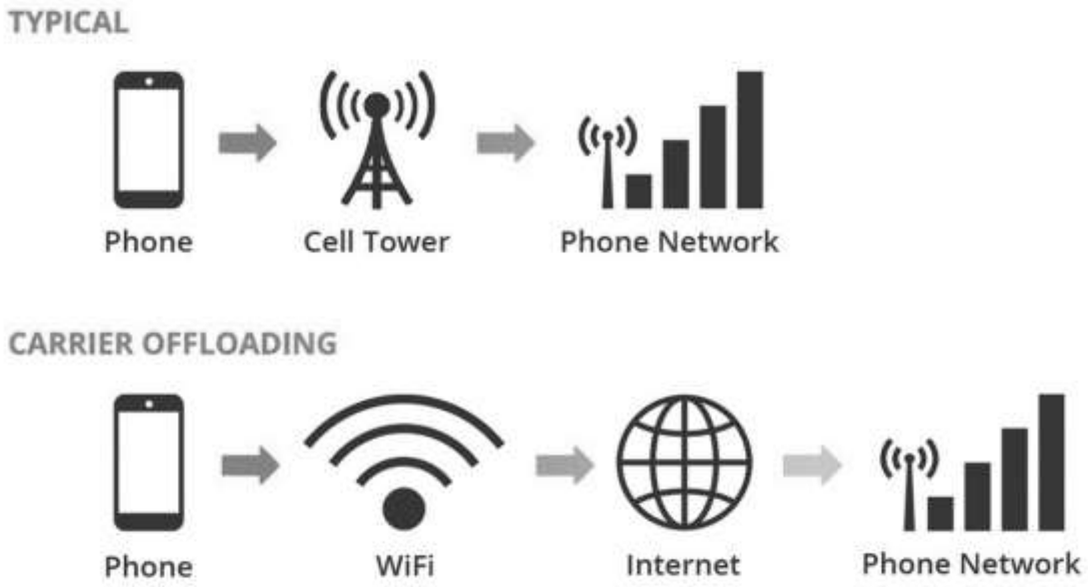
- Enables strategic, next-generation technologies such as
  - intelligent path selection
  - multi-path
  - indoor to outdoor cellular to Wi-Fi handoff.
- Wi-Fi Perception: Insecure & Unreliable.

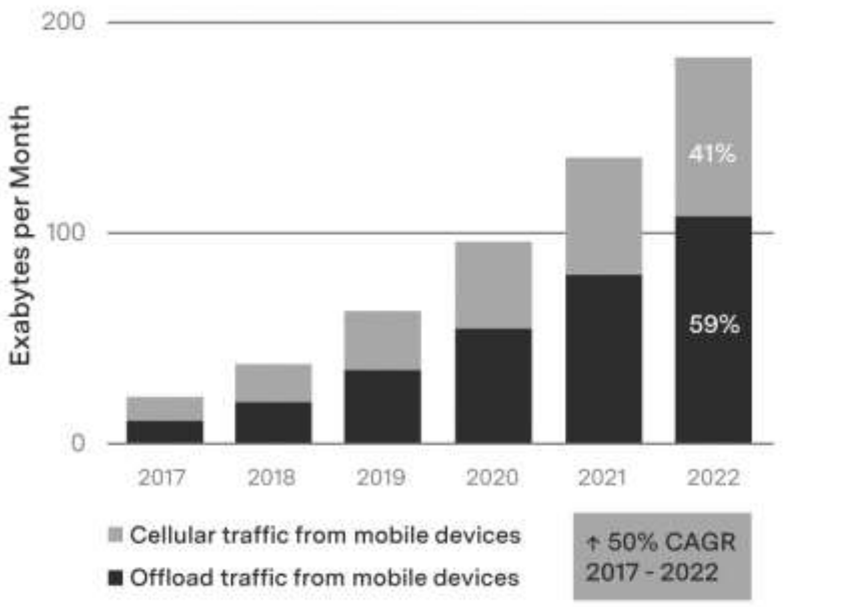
Cisco Presentation: https://www.youtube.com/watch?v=rW5I6csmF1o

WiFi Offload

- Usage of Wi-Fi is not limited to just homes and offices.
- A user would like to use the same mobile devices at public locations where public Wi-Fi networks are available.
- Cellular Service providers are not able to meet the bandwidth demand on costly and limited licensed spectrum and hence prefer offloading to WiFi
- Over 50% of cellular traffic in recent times is being offloaded to WiFi.
- The user should be able to seamlessly and securely move between cellular and WiFi





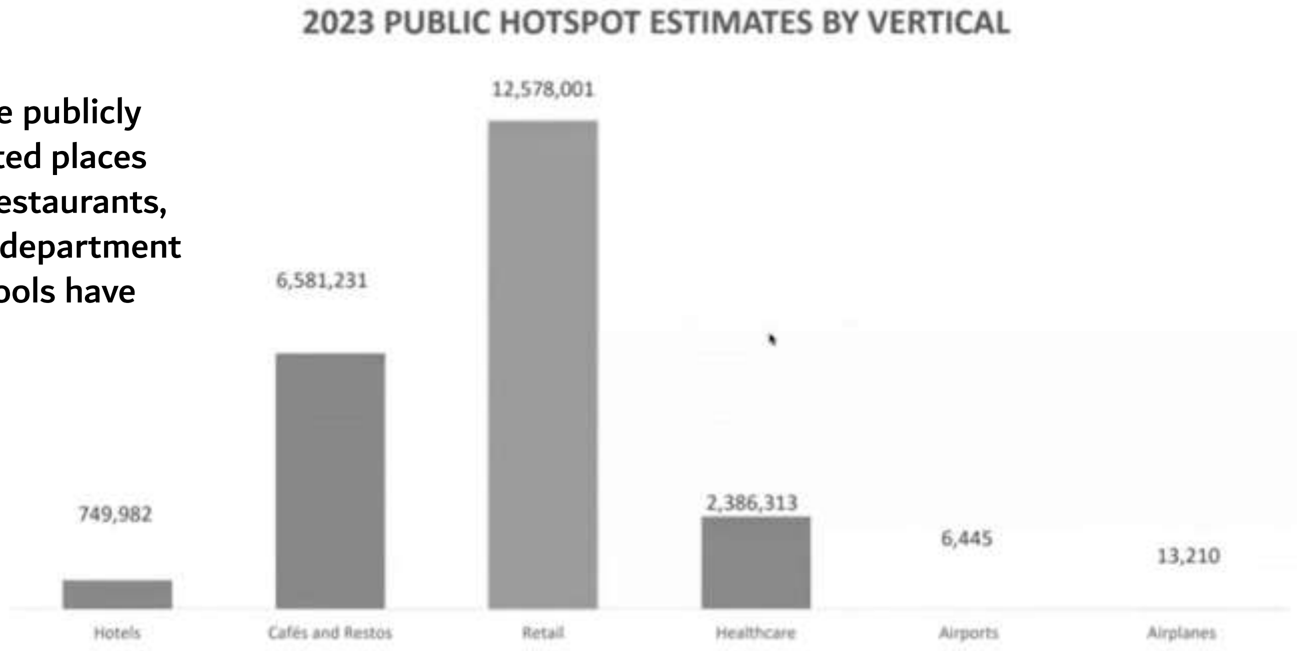


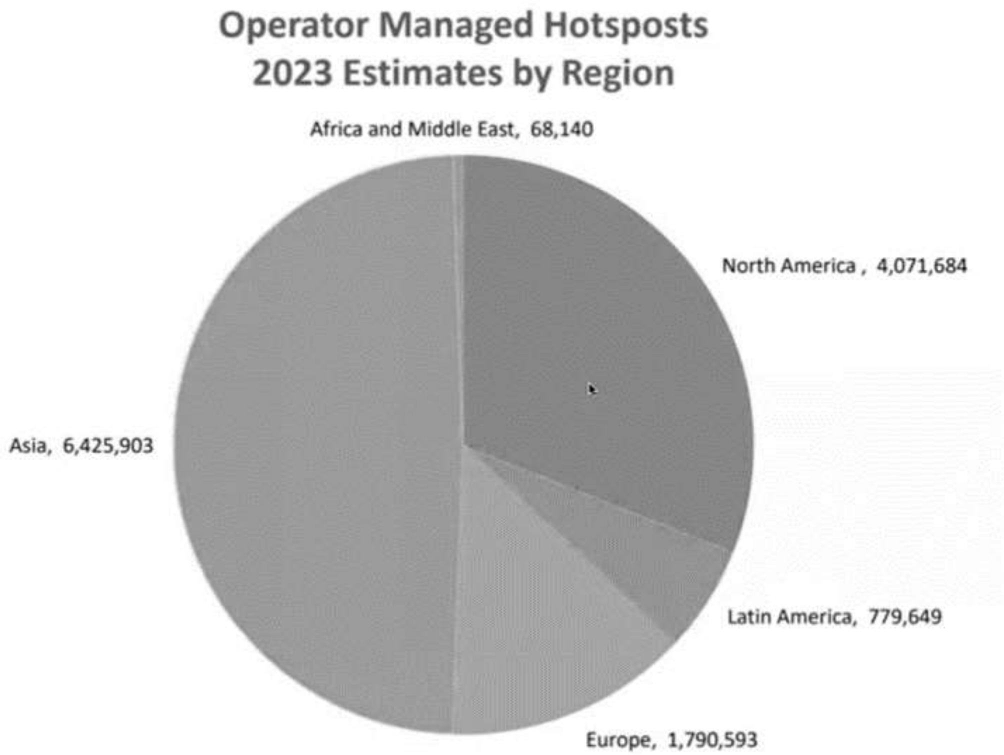
1 Exabyte = quintillion bytes = 1,000,000,000,000,000,000

Source: Cisco Mobile Devices Forecast 2019

Public Hotspots

A hotspot is any location where Wi-Fi broadband network access is made publicly available through a WLAN. Hotspots are often located in heavily populated places and typically have a short range of access. Hotspots are often found at restaurants, train stations, airports, libraries, coffee shops, bookstores, fuel stations, department stores, supermarkets and other public places. Many universities and schools have wireless networks in their campus


2023 PUBLIC HOTSPOT ESTIMATES BY VERTICAL


Operator Managed Hotsposts 2023 Estimates by Region

https://www.youtube.com/watch?v=o7DPRa9uIUs

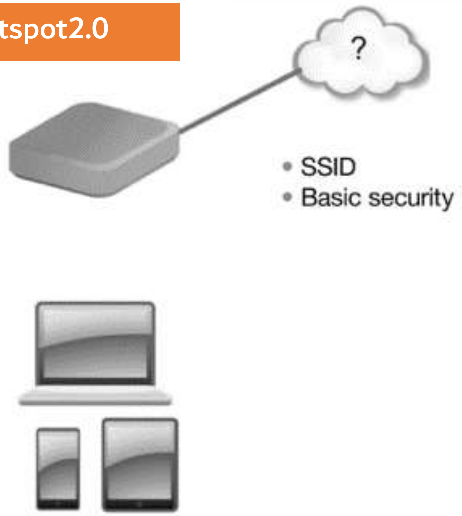
Hotspot 2.0 (Passpoint)

- Enables seamless roaming among WiFi networks and between WiFi and cellular networks.
- The HS 2.0 specification is based on a set of protocols called 802.11u.
- When an 802.11u-capable device is in range of at least one Wi-Fi network, the device automatically selects a network and connects to it if the authentication to the network is done once before.
- Network discovery, registration, provisioning, and access processes are automated so that the user does not have to go through them manually in order to connect and stay connected.

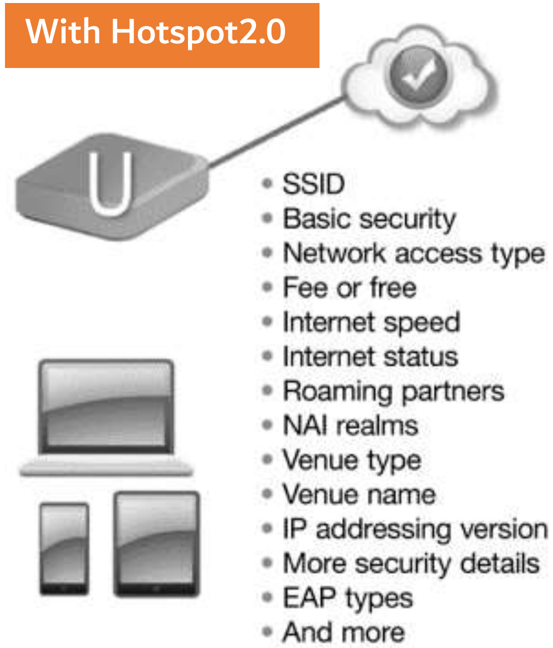
Advantages of Hotspot 2.0

- Public Hotspots Become Easier and More Secure
- Multiple Network Providers Can Work Together
- Encryption is Mandatory with provides high level of security
- Allows for policy enforcement and QoS implementations

Before Hotspot2.0

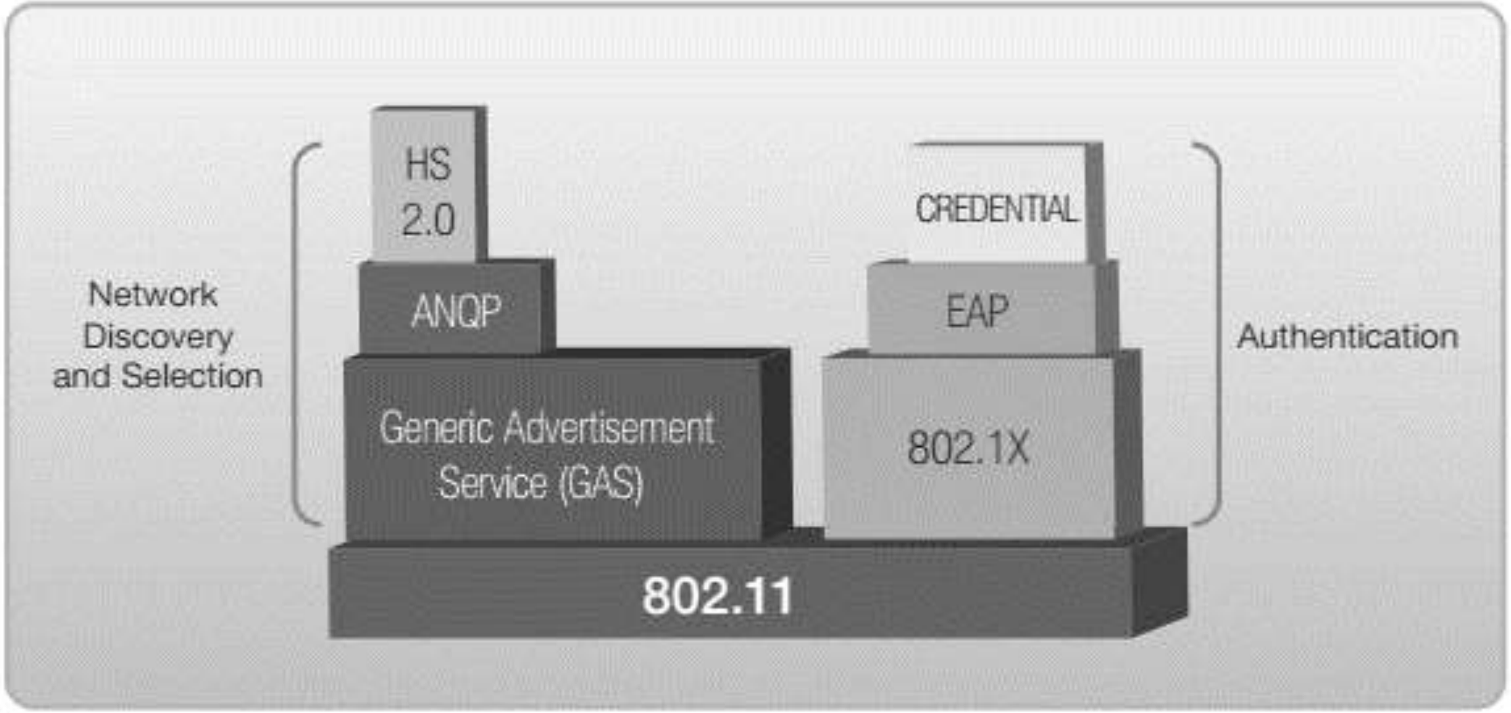


With Hotspot2.0



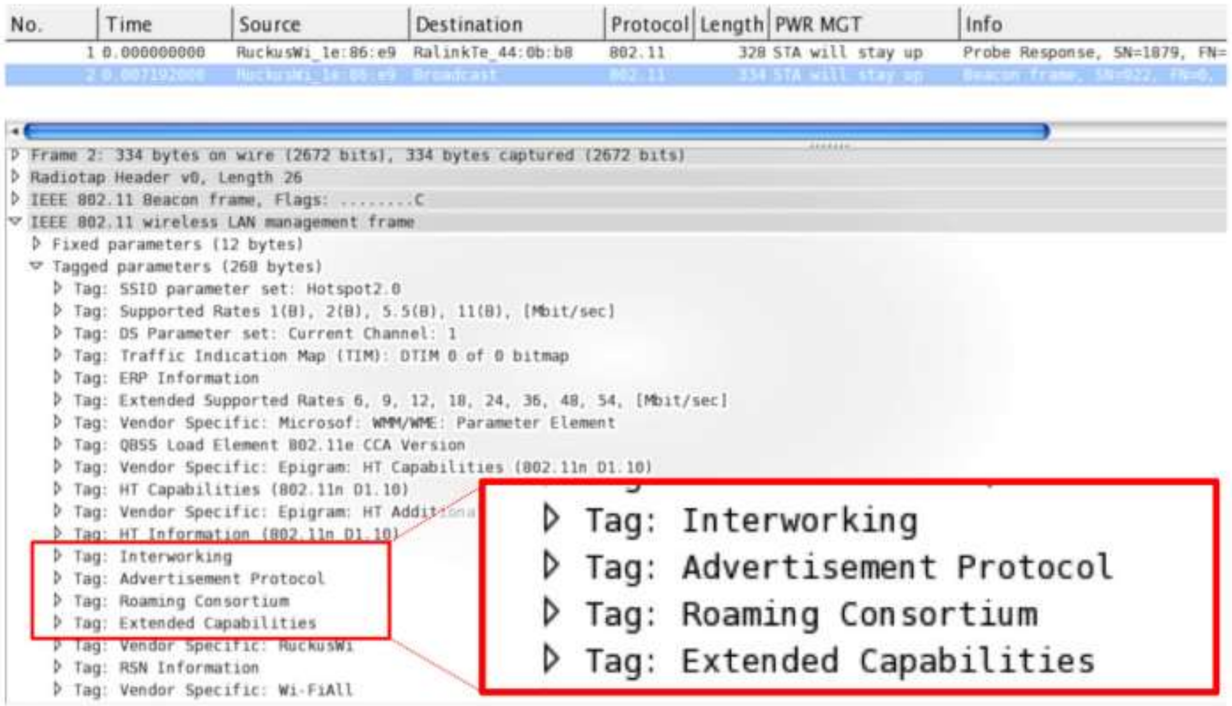
Hotspot 2.0 Terminology

- **802.11u –** The 802.11 standard extension from IEEE for improving internetworking with external networks
- **Hotspot 2.0 -** also known as Wi-Fi Certified Passpoint, is a standard based on 802.11u that is developed by the WiFi alliance for public-access Wi-Fi that enables seamless roaming among Wi-Fi networks and between Wi-Fi and cellular networks
- **Access Network Query Protocol (ANQP) -** is a query and response protocol used by a mobile device to discover a range of information, including the hotspot operator's domain name , roaming partners accessible via the hotspot along with their credential type and EAP method supported for authentication, IP address type availability and other metadata useful in a mobile device's network selection process.
- **Generic Advertisement Service (GAS) -** provides for Layer 2 transport ANQP frames between a mobile device and a server in the network prior to authentication. The access point is responsible for the relay of a mobile device's query to a server in the carrier's network and for delivering the server's response back to the mobile.
- **802.1X -** defines the encapsulation of the Extensible Authentication Protocol (EAP) over wired IEEE 802 networks and over 802.11 wireless networks which is known as "EAP over LAN" or EAPOL
- **EAP -** is an authentication framework that provides some common functions and negotiation of authentication methods called EAP methods
- **AAA server-** is a server program that handles user requests for access to computer resources and, for an enterprise, provides authentication, authorization, and accounting services.
- **Identity provider (IDP) -** is a system entity that creates, maintains, and manages identity information for principals and also provides authentication services to relying applications within a federation or distributed network.


Network Discovery and Selection
HS 2.0
ANQP
Generic Advertisement Service (GAS)
CREDENTIAL
EAP
802.1X
Authentication
802.11

802.11u Information Elements in a Beacon Frame

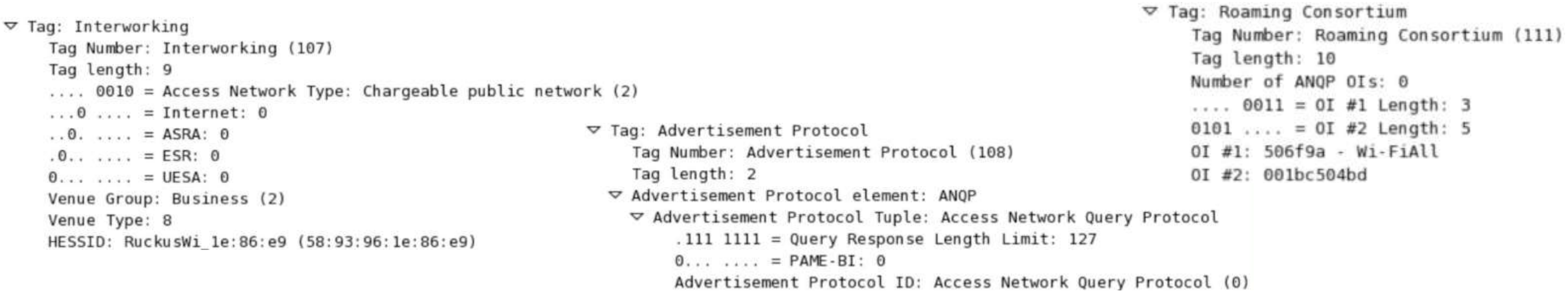
Information Element Name	Description
Extended Capabilities	Indicates whether an AP supports 802.11u interworking features.
Interworking	Identifies the interworking service capabilities of the AP or client
Advertisement Protocol	Identifies the network's support for particular advertisement protocols, such as ANQP, which allow the client to learn more about the network by querying the AP prior to forming a connection
Roaming Consortium	Identifies service providers or groups of roaming partners whose security credentials can be used to connect to a network



```
No.  Time         Source             Destination        Protocol Length PWR MGT            Info
   1 0.000000000  RuckusWi_1e:86:e9  RalinkTe_44:0b:b8  802.11      328 STA will stay up   Probe Response, SN=1879, FN=
   2 0.007192000  RuckusWi_1e:86:e9  Broadcast          802.11      334 STA will stay up   Beacon frame, SN=922, FN=0,

▷ Frame 2: 334 bytes on wire (2672 bits), 334 bytes captured (2672 bits)
▷ Radiotap Header v0, Length 26
▷ IEEE 802.11 Beacon frame, Flags: ........C
▽ IEEE 802.11 wireless LAN management frame
  ▷ Fixed parameters (12 bytes)
  ▽ Tagged parameters (268 bytes)
    ▷ Tag: SSID parameter set: Hotspot2.0
    ▷ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    ▷ Tag: DS Parameter set: Current Channel: 1
    ▷ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▷ Tag: ERP Information
    ▷ Tag: Extended Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    ▷ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
    ▷ Tag: QBSS Load Element 802.11e CCA Version
    ▷ Tag: Vendor Specific: Epigram: HT Capabilities (802.11n D1.10)
    ▷ Tag: HT Capabilities (802.11n D1.10)
    ▷ Tag: Vendor Specific: Epigram: HT Additional
    ▷ Tag: HT Information (802.11n D1.10)
    ▷ Tag: Interworking
    ▷ Tag: Advertisement Protocol
    ▷ Tag: Roaming Consortium
    ▷ Tag: Extended Capabilities
    ▷ Tag: Vendor Specific: RuckusWi
    ▷ Tag: RSN Information
    ▷ Tag: Vendor Specific: Wi-FiAll
```

```
▷ Tag: Interworking
▷ Tag: Advertisement Protocol
▷ Tag: Roaming Consortium
▷ Tag: Extended Capabilities
```



```
▽ Tag: Interworking
    Tag Number: Interworking (107)
    Tag length: 9
    .... 0010 = Access Network Type: Chargeable public network (2)
    ...0 .... = Internet: 0
    ..0. .... = ASRA: 0
    .0.. .... = ESR: 0
    0... .... = UESA: 0
    Venue Group: Business (2)
    Venue Type: 8
    HESSID: RuckusWi_1e:86:e9 (58:93:96:1e:86:e9)
```

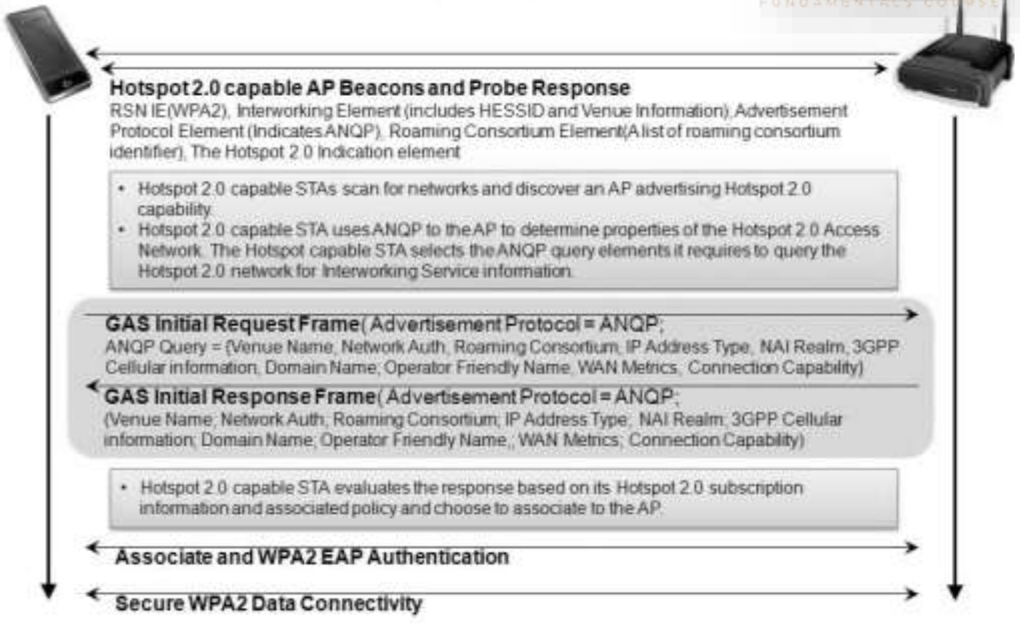
```
▽ Tag: Advertisement Protocol
    Tag Number: Advertisement Protocol (108)
    Tag length: 2
  ▽ Advertisement Protocol element: ANQP
    ▽ Advertisement Protocol Tuple: Access Network Query Protocol
        .111 1111 = Query Response Length Limit: 127
        0... .... = PAME-BI: 0
        Advertisement Protocol ID: Access Network Query Protocol (0)
```

```
▽ Tag: Roaming Consortium
    Tag Number: Roaming Consortium (111)
    Tag length: 10
    Number of ANQP OIs: 0
    .... 0011 = OI #1 Length: 3
    0101 .... = OI #2 Length: 5
    OI #1: 506f9a - Wi-FiAll
    OI #2: 001bc504bd
```

Access Network Query Protocol

ANQP messages are used to exchange information between the wireless client and the AP. There are three types of ANQP messages:

Request messages: These messages are sent by the wireless client to request information from the AP. A request message includes a list of information elements that the client is interested in.
Response messages: These messages are sent by the AP in response to a request message. A response message includes the requested information elements.
Notification messages: These messages are sent by the AP to notify the client of changes to the available networks or their capabilities.



Hotspot 2.0 capable AP Beacons and Probe Response
RSN IE(WPA2), Interworking Element (includes HESSID and Venue Information), Advertisement Protocol Element (Indicates ANQP), Roaming Consortium Element(A list of roaming consortium identifier), The Hotspot 2.0 Indication element

- Hotspot 2.0 capable STAs scan for networks and discover an AP advertising Hotspot 2.0 capability
- Hotspot 2.0 capable STA uses ANQP to the AP to determine properties of the Hotspot 2.0 Access Network. The Hotspot capable STA selects the ANQP query elements it requires to query the Hotspot 2.0 network for Interworking Service information.

GAS Initial Request Frame(Advertisement Protocol = ANQP;
ANQP Query = (Venue Name, Network Auth, Roaming Consortium, IP Address Type, NAI Realm, 3GPP Cellular information, Domain Name; Operator Friendly Name, WAN Metrics, Connection Capability)

GAS Initial Response Frame(Advertisement Protocol = ANQP;
(Venue Name; Network Auth; Roaming Consortium; IP Address Type; NAI Realm; 3GPP Cellular information; Domain Name; Operator Friendly Name,; WAN Metrics; Connection Capability)

- Hotspot 2.0 capable STA evaluates the response based on its Hotspot 2.0 subscription information and associated policy and choose to associate to the AP.

Associate and WPA2 EAP Authentication

Secure WPA2 Data Connectivity

ANQP Information Elements

ANQP messages include information elements that provide details about the available networks and their capabilities. These elements are organized into categories that include:

Capability Information: This category includes information elements that describe the capabilities of the AP and the network, such as the supported authentication and encryption methods.
Network Authentication Type: This category includes information elements that describe the authentication methods used by the network.
Operating Class: This category includes information elements that describe the frequency band and channel number used by the network.
Roaming Consortium: This category includes information elements that describe the roaming agreements between networks.
Emergency Services: This category includes information elements that describe the emergency services available on the network.
Venue Name: This category includes information elements that describe the name and location of the venue where the network is located.
Geographic Location: This category includes information elements that describe the geographic location of the network.
Hotspot 2.0: This category includes information elements that describe the Hotspot 2.0 service and the available service providers.

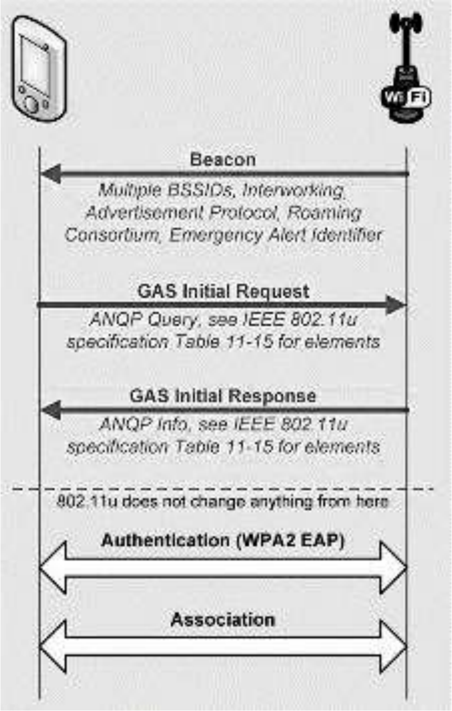
https://www.telecomtrainer.com/anqp-access-network-query-protocol/

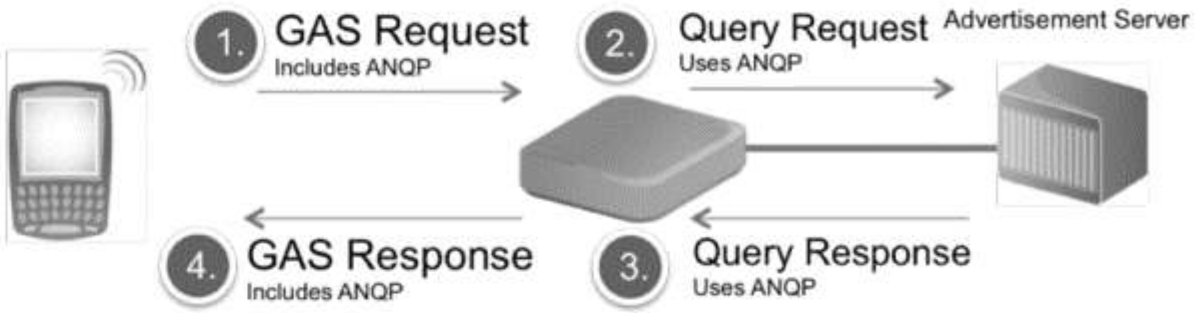
The Generic Advertisement Service (GAS)

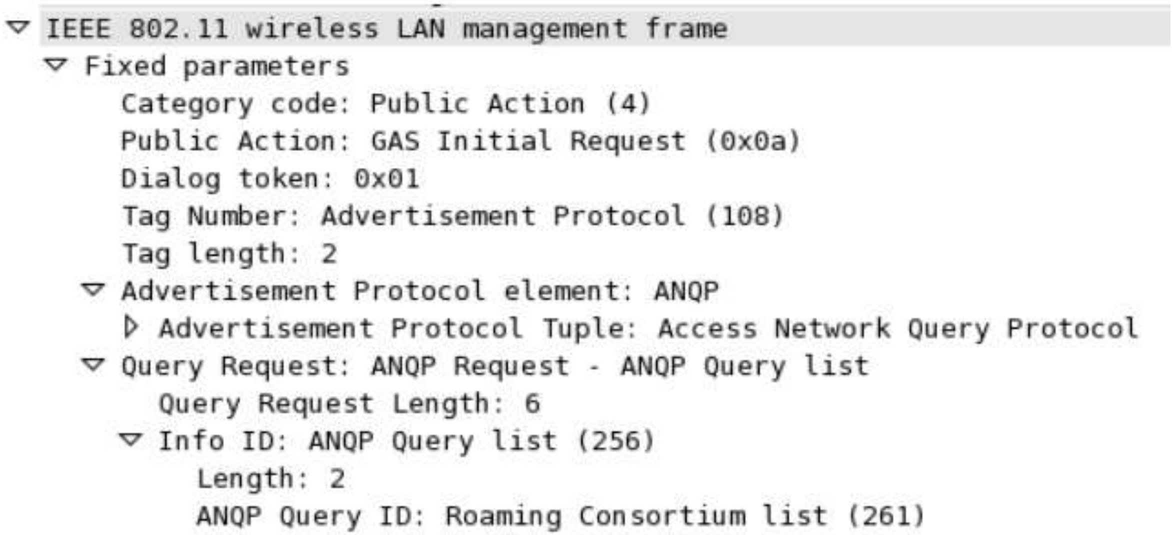
The Generic Advertisement Service (GAS) is a framework that provides transport for advertisement services like ANQP. When a client must query the AP using an advertisement protocol, it uses GAS to do so.

GAS provides a frame exchange process (GAS Request/Response) and a framing format (using 802.11 Action frames) for the advertisement services.

GAS Action frames contain fields used by the transported advertisement protocol to fulfill its purposes, as we will show later. One reason GAS is used is that prior to association, mobile devices have not obtained an IP address

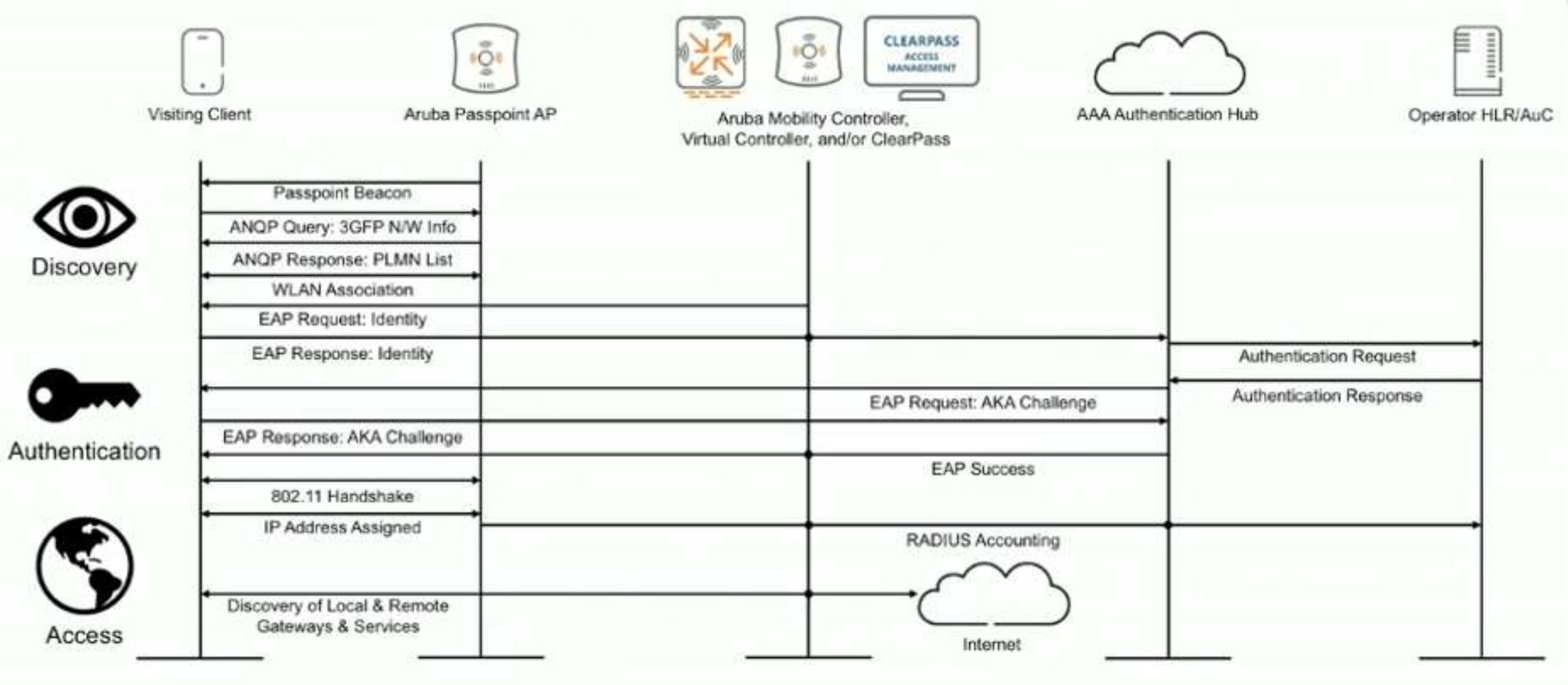

Wi Fi
Beacon
Multiple BSSIDs, Interworking, Advertisement Protocol, Roaming Consortium, Emergency Alert Identifier
GAS Initial Request
ANQP Query, see IEEE 802.11u specification Table 11-15 for elements
GAS Initial Response
ANQP Info, see IEEE 802.11u specification Table 11-15 for elements
802.11u does not change anything from here
Authentication (WPA2 EAP)
Association





```
▽ IEEE 802.11 wireless LAN management frame
  ▽ Fixed parameters
      Category code: Public Action (4)
      Public Action: GAS Initial Request (0x0a)
      Dialog token: 0x01
      Tag Number: Advertisement Protocol (108)
      Tag length: 2
    ▽ Advertisement Protocol element: ANQP
      ▷ Advertisement Protocol Tuple: Access Network Query Protocol
    ▽ Query Request: ANQP Request - ANQP Query list
        Query Request Length: 6
      ▽ Info ID: ANQP Query list (256)
          Length: 2
          ANQP Query ID: Roaming Consortium list (261)
```

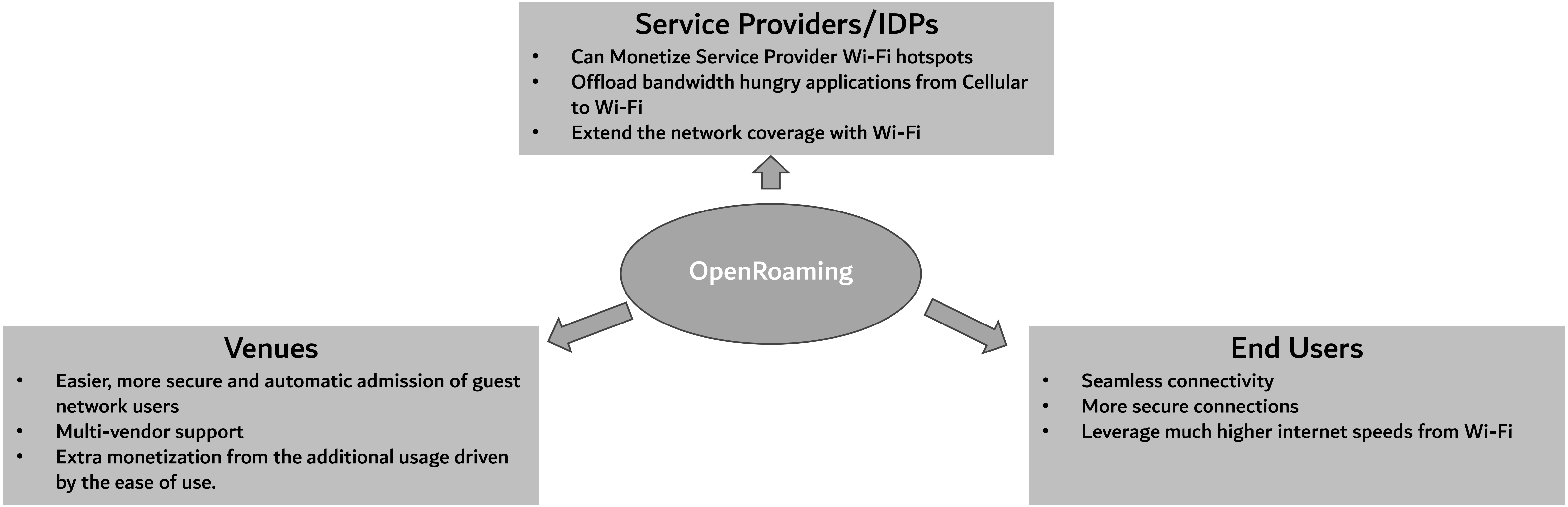
Passpoint Discovery and Authentication



- **Seamless Connectivity**: Unlike conventional Wi-Fi, where manual selection and authentication are needed, Passpoint automates these processes.
- **Enhanced Security**: Passpoint networks use enterprise-grade security protocols, significantly improving over the often less secure traditional hotspots.
- **Efficient Roaming**: Passpoint supports seamless roaming, allowing devices to switch between Wi-Fi networks without the need for re-authentication.
- **User Experience**: The automated, secure, and seamless nature of Passpoint translates into a superior user experience, with less frustration and more productivity.

OpenRoaming

- OpenRoaming is a WiFi roaming federation.
- With OpenRoaming the end user can use the existing user credentials like username/passwords, certificates, Mobile SIMs to automatically connect to any Wi-Fi network around the world that is operated by any member of the Federation.



Service Providers/IDPs

- Can Monetize Service Provider Wi-Fi hotspots
- Offload bandwidth hungry applications from Cellular to Wi-Fi
- Extend the network coverage with Wi-Fi

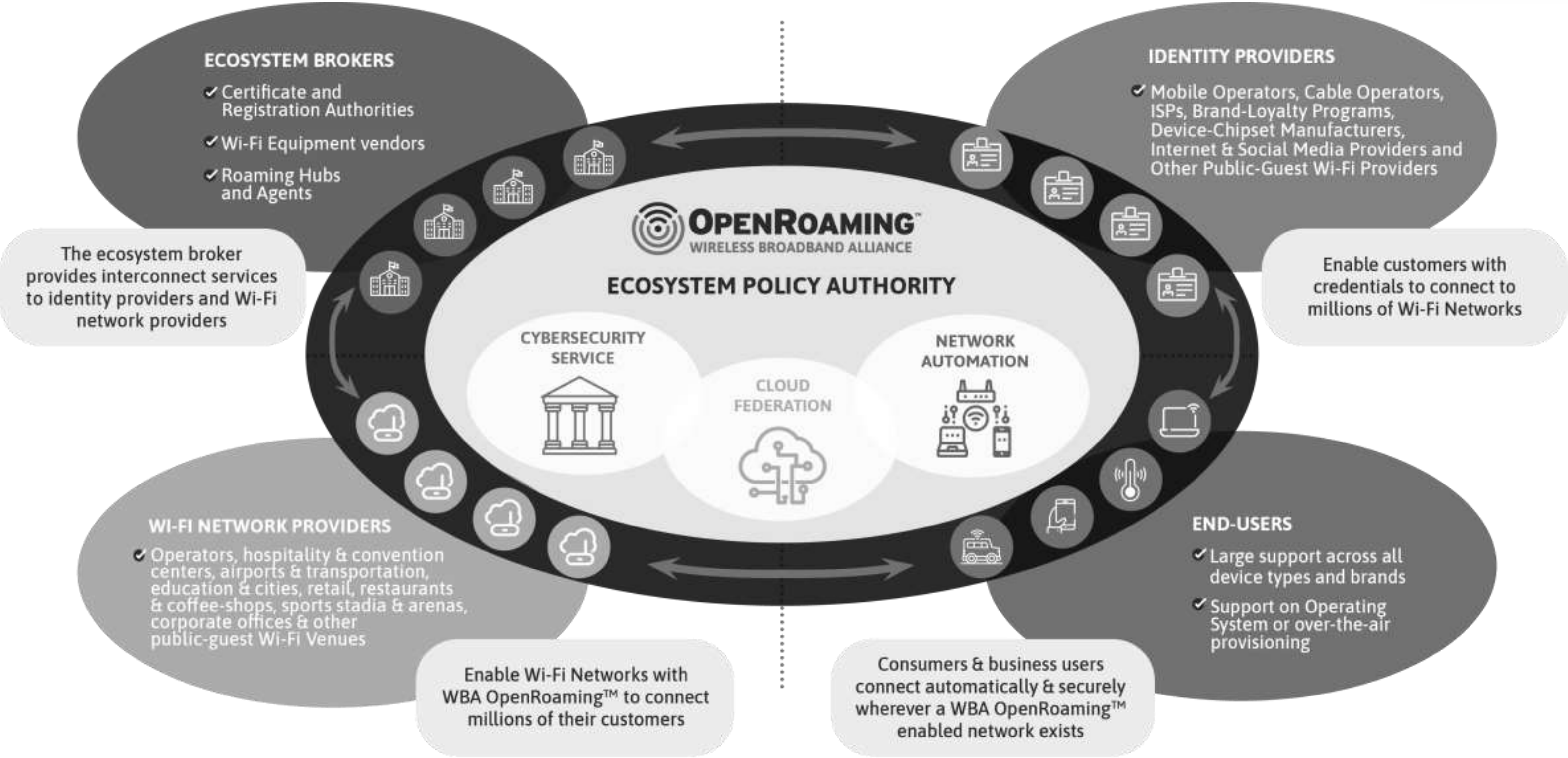
Venues

- Easier, more secure and automatic admission of guest network users
- Multi-vendor support
- Extra monetization from the additional usage driven by the ease of use.

End Users

- Seamless connectivity
- More secure connections
- Leverage much higher internet speeds from Wi-Fi

Open Roaming Ecosystem



ECOSYSTEM BROKERS

- ✓ Certificate and Registration Authorities
- ✓ Wi-Fi Equipment vendors
- ✓ Roaming Hubs and Agents

The ecosystem broker provides interconnect services to identity providers and Wi-Fi network providers

IDENTITY PROVIDERS

- ✓ Mobile Operators, Cable Operators, ISPs, Brand-Loyalty Programs, Device-Chipset Manufacturers, Internet & Social Media Providers and Other Public-Guest Wi-Fi Providers

Enable customers with credentials to connect to millions of Wi-Fi Networks

OPENROAMING™ WIRELESS BROADBAND ALLIANCE

ECOSYSTEM POLICY AUTHORITY

WI-FI NETWORK PROVIDERS

- ✓ Operators, hospitality & convention centers, airports & transportation, education & cities, retail, restaurants & coffee-shops, sports stadia & arenas, corporate offices & other public-guest Wi-Fi Venues

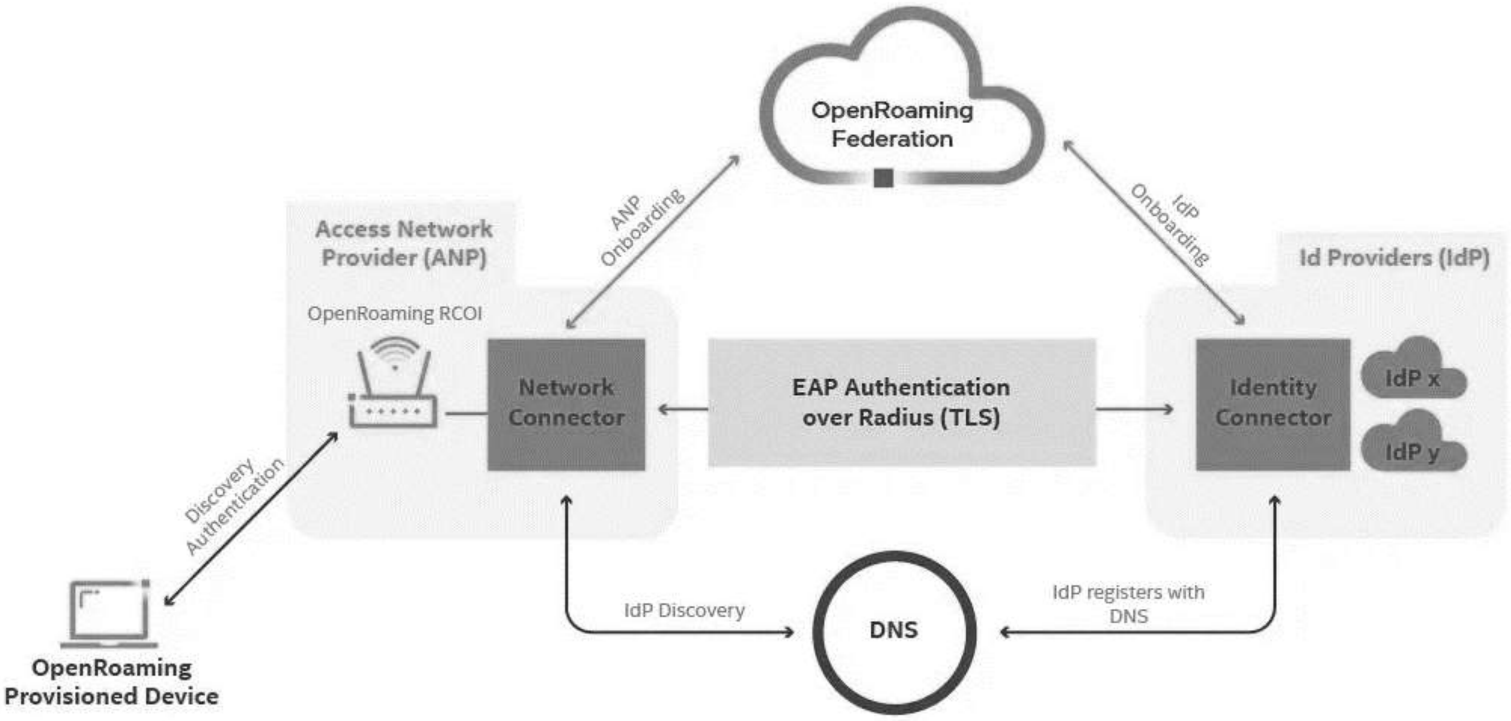
Enable Wi-Fi Networks with WBA OpenRoaming™ to connect millions of their customers

END-USERS

- ✓ Large support across all device types and brands
- ✓ Support on Operating System or over-the-air provisioning

Consumers & business users connect automatically & securely wherever a WBA OpenRoaming™ enabled network exists

How OpenRoaming Works



- When a verified user enters an area where a Wi-Fi network with OpenRoaming is enabled, their device automatically sends an access request.
- The Wi-Fi network responds with an authentication request.
- The consumer's device then responds with their identity information, which is typically a UserID associated with a particular identity provider in the OpenRoaming network.
- The user's identity is then forwarded to that identity provider, who verifies the user's information.
- After IDP successfully authenticates the user, a confirmation message is sent back to the Wi-Fi Access Network Provider.
- At that point, the user is verified and authenticated, and they can begin accessing the internet.
- This process is done without any user input and everything is completed in the background.
- This enables a much more seamless transition among different public Wi-Fi networks.

https://medium.com/intel-tech/technology-d2673bef3dc1

References

A Detailed Look at 802.11u and Hotspot 2.0 Mechanisms

https://www.commscope.com/globalassets/digizuite/1528-1358-wp-how-interworking-works.pdf

Cisco OpenRoaming to Better Bridge Between Mobile and Wi Fi Networks
https://www.youtube.com/watch?v=rW5I6csmF1o

Part1: WiFi Technology Fundamentals – Basics

Module1: Introduction and History of Wi-Fi	
Tue – 26th Sept 2023	Session1a: Evolution of WiFi WiFi Generations, Residential/Enterprise WiFi Applications, Business Evolution
Thu – 28th Sept 2023	Session1b: WiFi Network Topologies Infrastructure/Mesh/Bridge/Adhoc Modes, Backhaul Mechanisms, Deployment Use cases
Tue – 3rd Oct 2023	Session1c: WLAN Standards and Amendments Alphabet Soup IEEE Standards Bodies, WiFi Alliance, Standards and their extensions
Thu – 5th Oct 2023	Session1d: Basic Functional building blocks of a WiFi AP/Router PHY, Baseband, Lower MAC, Upper MAC, various Interfaces, key functional blocks

Module2: WLAN PHY Layer	
Tue – 10th Oct 2023	Session2a: Frequency Allocation ISM and UNII Bands, unlicensed spectrum allocation, channels, Channel BW
Thu – 12th Oct 2023	Session2b: Modulation/Coding, MIMO Basics Basics of Digital Modulation and Coding, Multipath, MIMO, OFDMA, Spectral Efficiency
Tue – 17th Oct 2023	Session2c: MCS Table, PHY Data Rates PHY Data rates, MCS Table, Theoretical Throughput
Thu – 19th Oct 2023	Session2d: PHY Headers and key functions PHY Headers, PCLP and PMD Sub Layers, Key PHY layer functions

Module3: WLAN MAC Layer	
Tue- 24th Oct 2023	Session3a: Basic AP Management and Control Functions Beaconing, BSSID, Scanning, Basic Service Set and its Capabilities
Thu – 26th Oct 2023	Session3b: MAC Framing, Headers and Key Functions MAC headers and key functions, Management/Control/Data Frames
Tue – 31st Oct 2023	Session3c: Carrier Sense and Medium Access Physical/Virtual Carrier Sensing, DCF, Random Backoff, Interframe Spacing, EDCA Parameters
Tue- 7th Nov 2023	Session3d: Data Transfer and Aggregation Data Transfer, Medium Overhead, Aggregation, Admission Control

Module4: Security in Wi-Fi	
Tue- 14th Nov 2023	Session4a: Various WiFi Security Protocols Security basics, WEP, WPA/WPA2/WPA3, Enterprise/Personal, Captive Portal, WPS
Tue- 21st Nov 2023	Session4b: Basics of Authentication and Encryption EAP Methods, TKIP/CCMP, 802.1x connection, Key Generations, 4-way Handshake
Tue – 28th Nov 2023	Session4c: Attacks and Vulnerabilities DoS Attacks, Man in the Middle Attacks, Cracking Security Keys, PMF
Tue – 5th Dec 2023	Session4d: Seamless connectivity/Open Roaming Open Roaming Technology, WiFi to Cellular Handover, EAP-SIM/AKA

Exam Prep, Exam and Certificates	
Tue–12th Dec 2023	Optional Interactive Q/A session – Exam Prep Week
Tue–19th Dec 2023	Online Exam
Thu–28th Dec 2023	Presenting the Excellence, Merit and Participation Certificates.

Q&A

?
QUIZ!
TIME

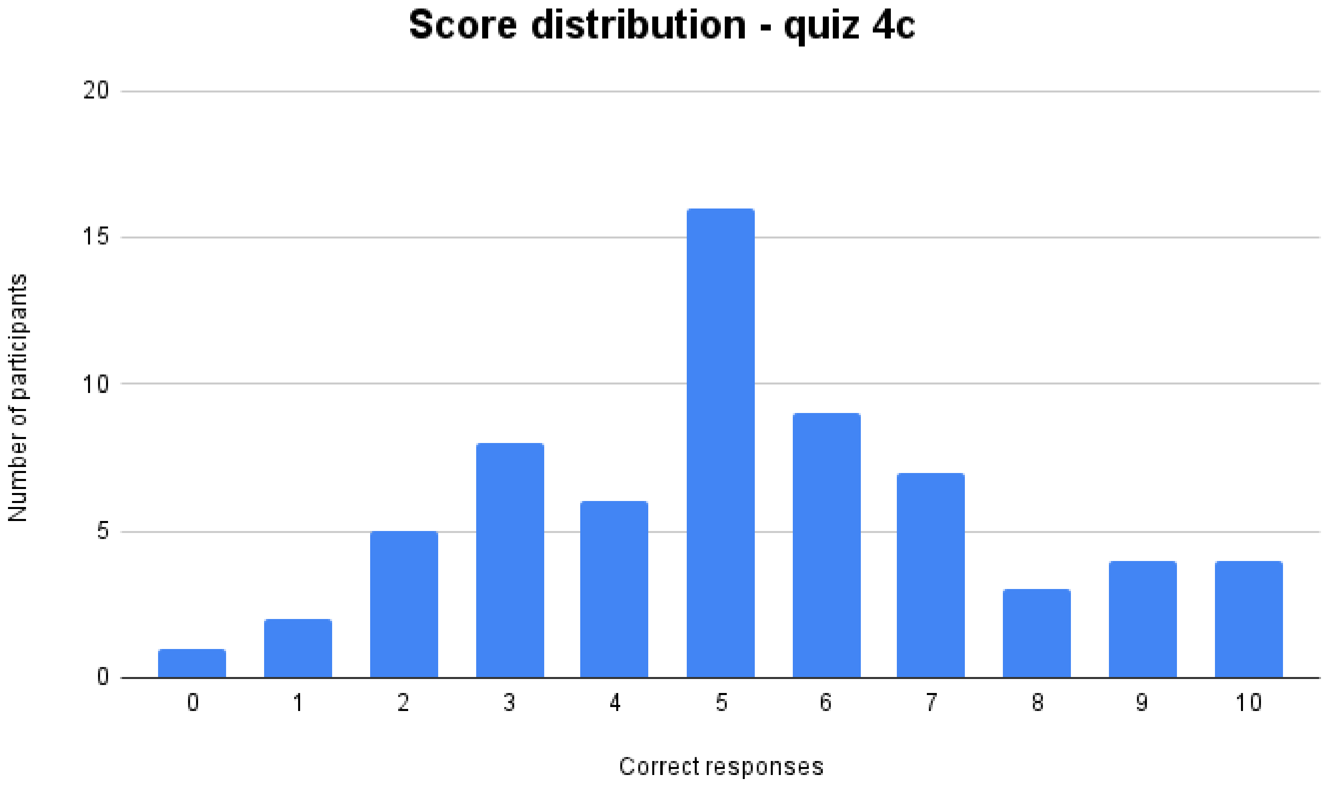
Quiz 4c Results

Winner

Madhu R

INDIA

Number of participants - 65


Score distribution - quiz 4c
Number of participants
Correct responses