
WI-FI TECHNOLOGY
FUNDAMENTALS COURSE
Module 4: Security in Wi-Fi
Session 4d:
SEAMLESS CONNECTIVITY/
HOTSPOT 2.0/ OPEN ROAMING

Wi-Fi Security in a Single Location

- Secure a single location, such as a home or office.
- Not intended for cross-organizational use or large-scale networks.
- Easy setup and management: Suitable for non-technical users.
- Wide compatibility: Supports most modern Wi-Fi devices.
- Strong security: Provides sufficient protection for typical home and small office needs.

Authentication:

- WPA Personal: Common security protocol for home and small office networks.
- Pre-Shared Key (PSK): Password shared between router and authorised devices.
- Device authentication: Requires obtaining PSK from router, either manually or through WPS.

Data Protection:

- Strong encryption: Ensures secure data exchange between devices and router.
- Potential vulnerabilities: Attackers can attempt to crack PSK or exploit weaknesses in WPS.

Drawbacks:

- Limited scope: Not ideal for complex networks with multiple locations or users.
- Security vulnerabilities: PSK cracking and WPS weaknesses can be exploited by attackers.

Day in the Life of a Mobile Device

Problem:

- Connecting to Wi-Fi in public places is tedious and insecure.
- Users must manually select and connect to networks, and the process varies from venue to venue.
- Open authentication is used, which is not secure.
- Venues want users to connect to their Wi-Fi networks so they can track user activity and push targeted ads.

Solution:

- Seamless and secure onboarding to Wi-Fi networks.
- Use of multiple networks simultaneously to increase bandwidth.

Technologies:

- Hotspot 2.0: It is a standard that provides secure and seamless onboarding to Wi-Fi networks. It uses a variety of methods, including EAP-TLS and DNS redirection, to authenticate users and connect them to the network.
- Open Roaming: It is a framework that allows users to roam between different Wi-Fi networks without having to manually select and authenticate to each network. It uses a variety of methods, including EAP-TLS and RADIUS, to authenticate users and connect them to the network.

Wi-Fi Offload:

Wi-Fi offload and Hotspot 2.0 offer a solution to the growing problem of network congestion. By seamlessly transitioning users between cellular and Wi-Fi networks, these technologies provide a better user experience, reduced costs for providers, and a more efficient use of resources. As data usage continues to increase, Wi-Fi offload and Hotspot 2.0 are expected to play a critical role in the future of mobile networking.

Problem:

- Cellular networks are overloaded with increasing bandwidth usage.
- Users demand faster speeds for activities like watching movies on their phones.
- Cellular network providers want to offload traffic to Wi-Fi to reduce costs and improve performance.

Solution:

- Wi-Fi offload: Seamlessly transfers data from cellular networks to Wi-Fi networks.
- Hotspot 2.0: A technology that enables smooth and secure roaming between different Wi-Fi networks.

How it works:

1. User's phone connects to a cell tower.
2. Cellular network providers offload the user's traffic to a Wi-Fi network in the vicinity.
3. The Wi-Fi network is advertised using Hotspot 2.0 technology, providing information about available networks, fees, speed, and venue details.
4. User's phone connects to the chosen Wi-Fi network.
5. User is authenticated using the same credentials as their cellular network.
6. Data is transmitted through the Wi-Fi network, providing faster speeds and lower costs for the cellular network provider.

It provides:

- Reduced network congestion: Offloads traffic from cellular networks, improving performance and reliability.
- Cost savings: Reduces expenses for cellular network providers.
- Improved user experience: Provides faster data speeds for users.
- Seamless connectivity: Users experience smooth transitions between cellular and Wi-Fi networks.

Examples:

- A user watches a movie on their phone while travelling. Their phone automatically switches from the cellular network to a Wi-Fi network in the train station, providing a faster connection.
- A user visits a coffee shop and connects to the free Wi-Fi network using Hotspot 2.0 technology. They are automatically authenticated and enjoy a fast and secure connection.

Public Hotspot

- Easier to connect and use compared to traditional Wi-Fi networks.
- Seamless roaming between different public hotspots.
- Collaborative efforts between network providers offer improved user experience.
- Public hotspots are becoming increasingly common in various locations like airports, coffee shops, and libraries.
- Network discovery, registration, provisioning, and usage are facilitated through public hotspot technology.

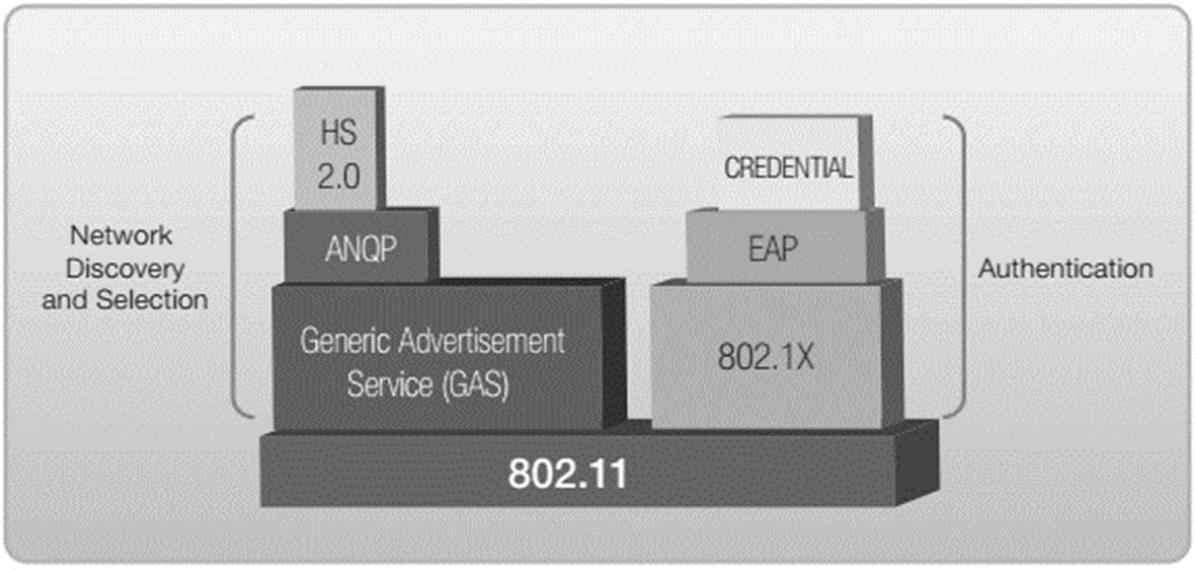
Hotspot 2.0 (Passpoint) and Terminology

- Hotspot 2.0 is based on the 802.11u standard.

- Hotspot 2.0 uses EAP methods for authentication.
- Hotspot 2.0 uses ANQP to exchange information between devices, access points, and networks.
- Hotspot 2.0 uses GAS to transport ANQP frames.
- Hotspot 2.0 includes Radius servers, Tria servers, and IdPs.

Terminology:

- 802.11u: A protocol that enables inter-networking between external networks.
- Access Network Query Protocol (ANQP): A protocol used by devices, access points, and networks to exchange information about available networks.
- Generic Advertisement Service (GAS): A Layer 2 transport mechanism used to carry ANQP frames.
- EAP-TTLS: An authentication protocol used in Hotspot 2.0.
- Radius server: A server that provides authentication, authorization, and accounting services for network users.
- Tria server: A server that provides trusted network access services for Hotspot 2.0.
- Identity provider (IdP): A provider that provides identity verification services for Hotspot 2.0 users.



How it works:

1. A device scans for Hotspot 2.0 networks.
2. The device uses ANQP to query the access point for information about available networks.
3. The device selects a network and authenticates using EAP-TTLS.

4. The device is granted access to the network.

802.11u Information Elements in a Beacon Frame

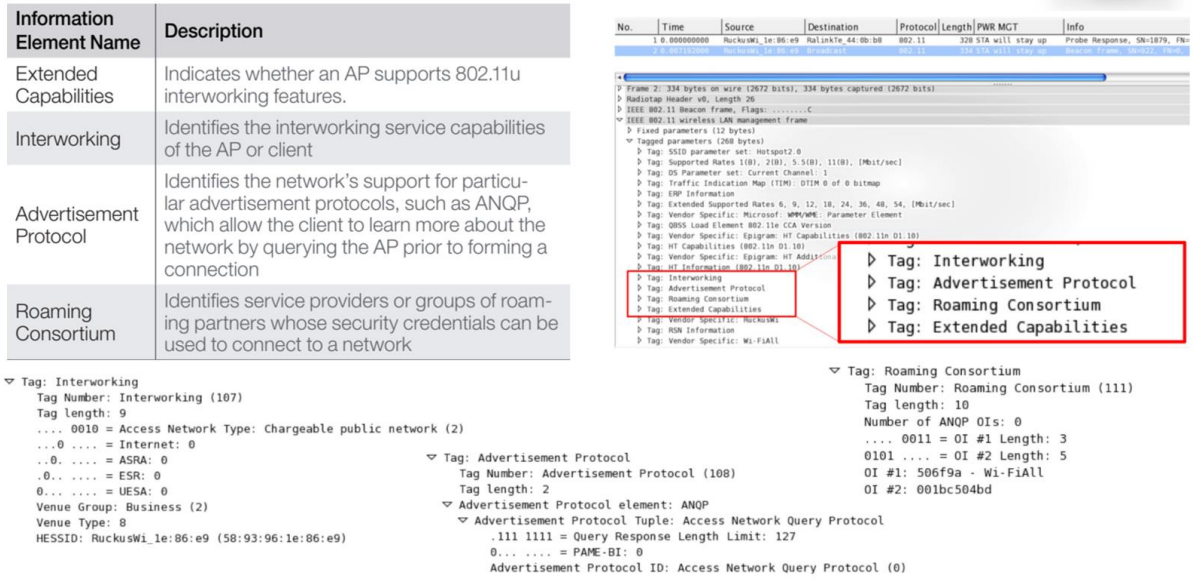
- 802.11u information elements in beacon frames play a critical role in Hotspot 2.0 networks. They enable access points to advertise multiple networks, provide clients with detailed network information, facilitate seamless roaming, and enhance network security.
- Standard Information Elements: SSID, supported rates, ERP information elements, QBSS, HT, VHD, EHD information elements, etc.
- Hotspot 2.0 Information Elements: Interworking Information Element (IIE), Advertisement Protocol Information Element (APIE), Roaming Consortium Information Element (RCIE), Extended Capabilities Information Element (ECIE)

Benefits:

- Multiple Network Advertisement: Enables advertising multiple networks on a single access point, increasing user choice and flexibility.
- Enhanced Network Discovery: Provides clients with detailed information about available networks, simplifying network selection.
- Seamless Roaming: Facilitates seamless roaming between different networks by utilising roaming consortium information.
- Improved Security: Allows clients to authenticate with their service provider before connecting, enhancing network security.

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



The image shows a Hotspot 2.0 enabled access point beacon frame containing the following 802.11u information elements:

- Interworking Information Element (IIE):
  - Access Network Type: Chargeable public network (2)
  - Number of ANQP OIS: 0
- Advertisement Protocol Information Element (APIE):
  - Advertisement Protocol: Access Network Query Protocol (108)
- Roaming Consortium Information Element (RCIE):
  - Tag Number: Roaming Consortium (111)
  - Tag Length: 10
- Extended Capabilities Information Element (ECIE):
  - Tag Number: Extended Capabilities (107)
  - Tag Length: 9

This information indicates that the access point is advertising a chargeable public network that supports ANQP and is part of a roaming consortium.

Access Network Query Protocol (ANQP)

ANQP is a protocol used by devices, access points, and networks to exchange information about available networks. It is used in Hotspot 2.0 networks to allow clients to discover and select the best network for their needs.

It provides:

- Improved network discovery: ANQP provides clients with detailed information about available networks, including their service providers, roaming partners, security capabilities, and other details. This helps clients to select the best network for their needs.
- Seamless roaming: ANQP can be used to facilitate seamless roaming between different networks. For example, if a user is traveling and their device is connected to a Hotspot 2.0 network, ANQP can be used to discover and connect to a network from the same service provider in a different location.
- Enhanced security: ANQP can be used to enhance network security by allowing clients to authenticate with their service provider before connecting to a network. This helps to prevent unauthorized access to networks.

How it works

ANQP uses a request-response messaging mechanism. A client device sends an ANQP request message to an access point to query information about available networks. The access point then responds with an ANQP response message that contains the requested information.

The ANQP request and response messages can contain a number of information elements, including:

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

Example

The following is an example of how ANQP might be used to discover and connect to a Hotspot 2.0 network:

1. A user device scans for Hotspot 2.0 networks.
2. The device discovers a Hotspot 2.0 network and sends an ANQP request message to the access point to query information about the network.
3. The access point responds with an ANQP response message that contains information about the network, such as the service provider, security capabilities, and roaming partners.
4. The device selects a network based on the information provided in the ANQP response message.
5. The device authenticates with the network using the appropriate authentication method.
6. The device connects to the network and begins exchanging data.

The Generic Advertisement Service (GAS)

The Generic Advertisement Service (GAS) is a fundamental component of Hotspot 2.0 networks. It plays a crucial role in facilitating seamless and secure connectivity by enabling:

- Advertisement of multiple networks: Allows access points to advertise various operator networks on a single physical access point, offering users more choice and flexibility.
- Enhanced network discovery: Provides detailed information about available networks, simplifying user selection.
- Seamless roaming: Facilitates seamless roaming between different networks by utilizing roaming consortium information.
- Improved security: Enables clients to authenticate with their service provider before connecting, enhancing network security.

Components:

The GAS framework operates using two main components:

- GAS Request/Response: This frame exchange process allows clients to query access points for specific information about available networks.
- Framing format: Utilizes 802.11 Action frames to transport advertisement service frames efficiently over the Wi-Fi air interface.

Information Elements:

Several information elements are carried within the GAS framework, providing valuable details about available networks:

- Interworking Information Element (IIE): Provides information about the available access network types (e.g., cellular, Wi-Fi), network costs, and venue type.
- Advertisement Protocol Information Element (APIE): Indicates the network's support for specific advertisement protocols like ANQP, allowing clients to query the access point for further details before connecting.
- Roaming Consortium Information Element (RCIE): Identifies service providers or roaming partners whose credentials can be used for network access.
- Extended Capabilities Information Element (ECIE): Provides additional network information like supported rates and channels.

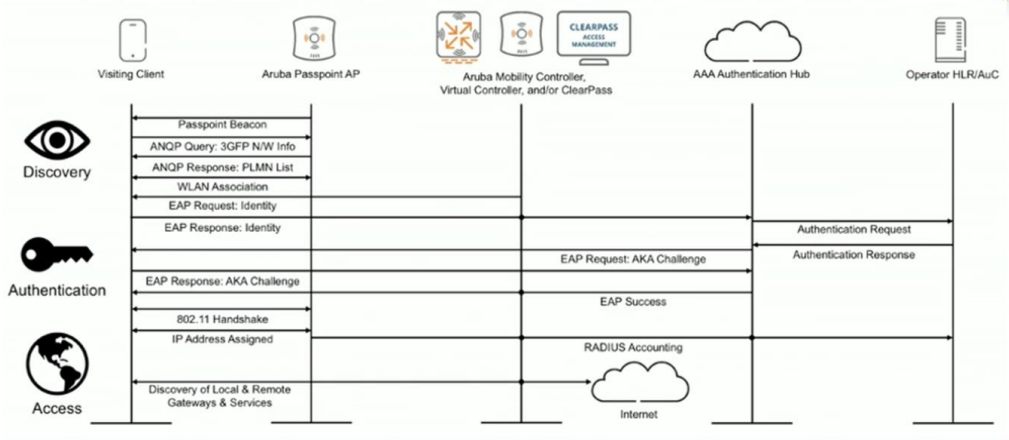
It provides:

- Increased user convenience: Offers a broader range of network options and simplifies network selection through detailed information.
- Improved network utilisation: Enables efficient allocation of resources by directing users to the most suitable network.
- Enhanced security: Provides secure authentication mechanisms to protect user data and network integrity.
- Reduced network congestion: Optimizes network traffic by directing users to less congested networks.

How it works:

1. Client discovery: Client scans for Wi-Fi networks and identifies Hotspot 2.0 networks through beacon frames.
2. GAS query: Client sends a GAS request frame to the access point requesting information about specific networks.
3. GAS response: Access point responds with a GAS response frame containing the requested information elements.
4. Network selection: Client analyzes the received information and selects the network that best meets its needs.
5. Access and authentication: Client initiates network access and performs authentication based on the selected network's protocol (e.g., EAP-SIM or EAP-AKA).

Passpoint Discovery and Authentication



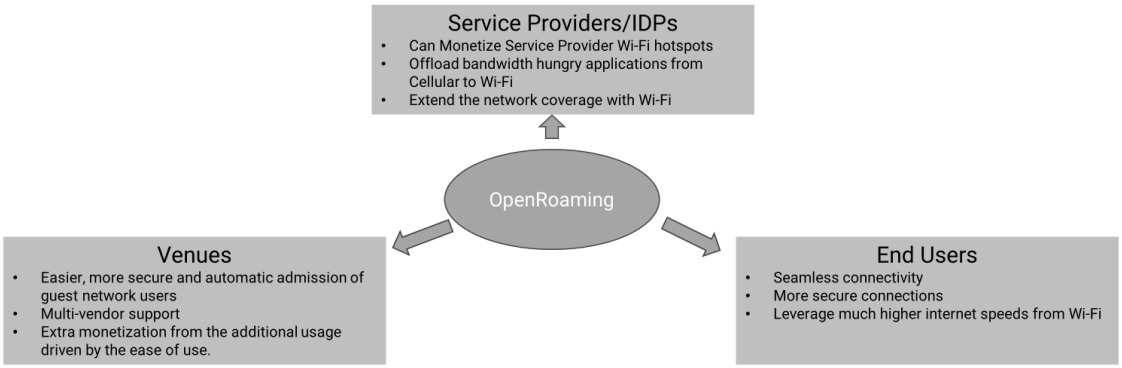
- **Seamless Connectivity**: Unlike conventional Wi-Fi, where manual selection and authentication are needed, Passpoint automates these processes.
- **Enhanced Security**: Passpoint networks use enterprise-grade security protocols, significantly improving over the often less secure traditional hotspots.
- **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.

Open Roaming:

Open roaming is a technology that enables seamless and secure connectivity between users and various Wi-Fi networks provided by different operators, eliminating the need for manual network selection and re-entry of credentials.

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.

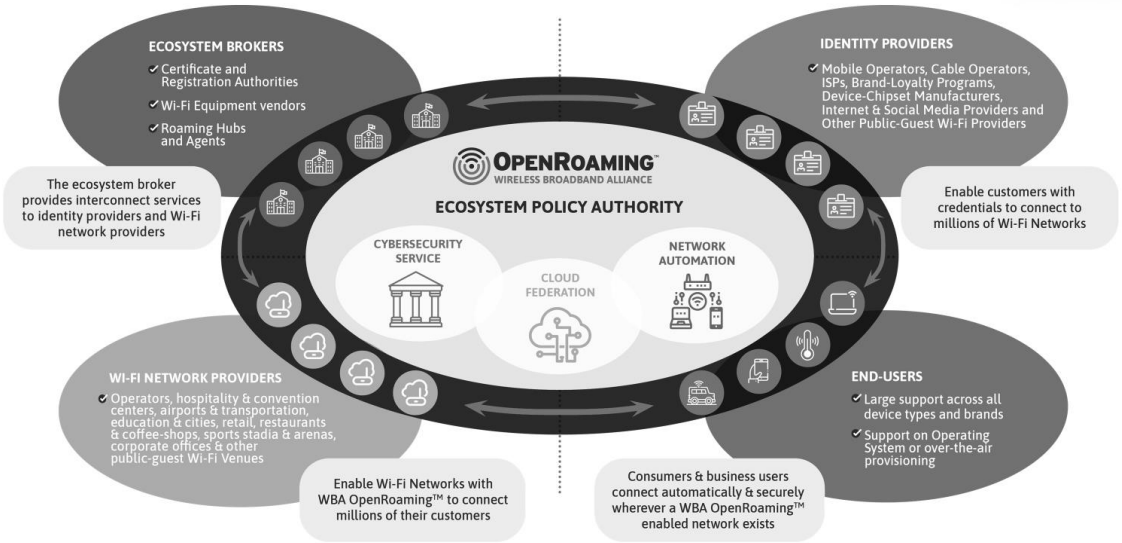


Open Roaming Ecosystem:

The open roaming ecosystem consists of several stakeholders working together to ensure seamless and secure connectivity. These include:

- Identity providers (IdPs): Verify user identity and issue credentials.
- Mobile network operators (MNOs): Provide cellular network access and manage user subscriptions.
- Wi-Fi network providers: Deploy and manage Wi-Fi networks participating in the ecosystem.
- Ecosystem brokers: Facilitate communication and data exchange between stakeholders.
- Users: Carry devices that support open roaming and utilize the service.

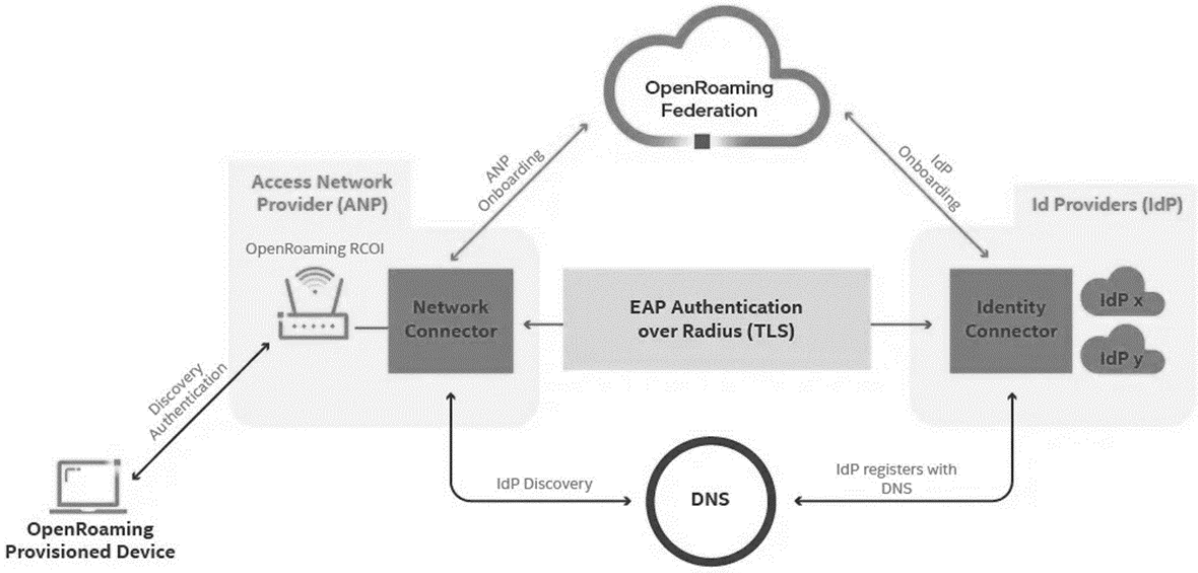
Open Roaming Ecosystem



How Open Roaming Works:

1. Device discovery: The user device scans for and identifies Wi-Fi networks enabled for open roaming.
2. Access request: The device sends an access request to the Wi-Fi network.
3. Identity verification: The Wi-Fi network forwards the request to the relevant IdP for user identity verification.
4. Authorization: If the user identity is valid, the IdP grants authorization to access the network.
5. Network access: The device establishes a connection with the Wi-Fi network and begins using internet services.

Throughout the process, secure communication protocols ensure data privacy and integrity.



Benefits:

- Seamless connectivity: Users move between networks without interruption.
- Improved user experience: No need for manual network selection or credential re-entry.
- Increased network utilisation: Encourages use of available Wi-Fi networks, offloading cellular traffic.
- Enhanced security: Robust security mechanisms protect user data and network infrastructure.
- Monetization opportunities: Operators and network providers can generate revenue through various models.

Challenges:

- Standardisation: Different vendors may implement open roaming differently, leading to compatibility issues.
- Security concerns: Robust security solutions are crucial for data protection and network security.
- Inter-operator agreements: Collaboration between stakeholders is essential for seamless roaming.