

Implementing carrier Wi-Fi

An overview of design considerations

White Paper

This white paper highlights design considerations for carrier Wi-Fi® networks with the goal of detailing different Wi-Fi service models, taking into account the requirements and available features. The document can be used during design discussions as a guideline for Wi-Fi architectures where a Wireless LAN (WLAN) Gateway (GW) is part of the solution. The main focus of the paper is community Wi-Fi and hotspot integration, with a look as well at value-added services and mobility scenarios.

Contents

Carrier Wi-Fi motivators	3
Community Wi-Fi	4
Open SSID with portal	6
Closed SSID	6
Points of attention	9
Hotspot aggregation	11
Connectivity models	11
Transport options	13
Mobility	14
Inter-SSID	14
Inter-AP	15
Inter-WLAN GW	15
Inter-RAT	16
Value-added services	17
In-browser notification	17
Http one-time redirect	17
URL-based white-listing	17
Parental control	17
Deep Packet Inspection	18
Future evolutions	18
Network Functions Virtualization	18
Evolved packet data gateway	18
Conclusion	19
Acronyms	21
References	23

Carrier Wi-Fi motivators

Almost every mobile computing device from laptop to smartphone is Wi-Fi-enabled. Given the nearly ubiquitous presence of Wi-Fi hotspots inside and outside the home, Wi-Fi has become an integral radio access technology for most users on the move. This consumption of bandwidth by Wi-Fi users is so significant that service providers now consider Wi-Fi an attractive access technology. Fixed service providers can deploy it using their existing fixed network infrastructure to deliver a Wi-Fi canopy. For multiple systems operators (MSOs) or cable companies Wi-Fi is especially attractive. It allows them to offer wireless access to subscribers as part of a mobile broadband strategy, and also as a foundation on the operator's way to becoming a mobile virtual network operator (MVNO).

Historically, most public Wi-Fi offered by small retailers such as coffee shops, for instance, has been best effort, uncontrolled, and insecure. Service providers have to raise the bar for Wi-Fi access with extra focus on:

- Scale
- Performance
- Security
- Uniformity
- Wholesale options
- Seamless mobility
- And maybe interconnecting with the 3rd-Generation Partnership Project (3GPP) network.

All these specific characteristics are covered under the umbrella of what we refer to as carrier Wi-Fi.

This whitepaper will discuss a number of topics, including community Wi-Fi based on an open or closed service set identifier (SSID), as well as aggregation of new and existing hotspot infrastructures. Additionally, an integrated solution with the 3GPP network will offer seamless wireless access over different radio access types (RATs). By using Generic Routing Encapsulation (GRE) tunneling as a lightweight transport protocol to deliver Wi-Fi traffic over existing IP infrastructure, it allows the user equipment to anchor to a centralized WLAN GW in a uniform session context. Secure authentication can be offered with mutual EAP-methods (Extensible Authentication Protocol), where the choice of authentication method is based on the configuration of the user equipment (UE) or commercial agreement.

The goal of this white paper is to provide guidelines on designing a carrier Wi-Fi service focusing on operators of fixed networks although, optionally, they may be acting as an MVNO.

Community Wi-Fi

Community Wi-Fi opens up residential Wi-Fi for external users and offers these same residential subscribers free access to the community Wi-Fi service in return. This give-and-take arrangement creates a potentially huge Wi-Fi network and makes it available to all members of the greater Wi-Fi community. With the correct Wi-Fi core, (including the WLAN GW and AAA server), community Wi-Fi can be interconnected with any Wi-Fi hotspot deployment to further enlarge a service provider's Wi-Fi canopy. As well as including members of the community Wi-Fi, access can be granted to external subscribers, using on-line or membership subscriptions. There are mainly two variants of community Wi-Fi based on open and/or closed SSID. These are detailed below.

From the service provider's perspective, community Wi-Fi brings the following benefits:

- Creates or improves brand awareness as the region-wide SSID can carry the name of the service provider – in part or in full
- Community Wi-Fi members will benefit from an additional wireless access technology for overall improved customer experience
- Once residential subscribers get used to the community Wi-Fi service, it will result in increased loyalty and one more reason to stay with their current service provider
- Service providers can use the ubiquity of their Wi-Fi network to attract external subscribers to their network

Open SSID with portal

The most common community Wi-Fi deployment is based on an open SSID, with portal authentication. The open SSID is the easiest use case to deploy, but has some specific characteristics that need to be taken into account during service definition.

Security

The air interface is not encrypted. As a result, any device will be able to attach to the Wi-Fi network. Data traffic on open SSID can be monitored easily, so the risk of a malicious user trying to hi-jack an existing session has to be prevented on the WLAN GW.

Migrant users

Many devices are configured to automatically attach to Wi-Fi networks, but do not make use of the data connection. This has to be taken into account when dimensioning the subscriber scale. The presence of migrant users is heavily influenced by the locale of the Wi-Fi access point (AP); a hotspot next to a train station, for instance, will have many more migrant users than a rural home spot. In order to address a potentially large number of migrant users,

the WLAN GW should not initially consume the full set of resources such as accounting sessions, session specific resources like shapers and/or policers. Only after successful authentication, using a portal or smartphone application, should the UE session be upgraded to a full-fledged session, consuming the full set of resources.

Http redirect

Browsing sessions initiated on the UE must be intercepted and redirected to a captive portal.¹ To assure a practical redirection mechanism, white/blacklisting in combination with Application Assurance (AA), which incorporates Deep Packet Inspection (DPI) technologies, may be required on the WLAN GW. Application assurance will validate the http-flow to confirm it originates with a web-browser instead of another application. Http redirecting should also have the option to redirect towards a URL instead of an IP address, because the latter may vary over time and cause additional maintenance effort.

RADIUS change of authorization (CoA)

To upgrade a migrant UE or to remove an http-redirect from the UE session, Remote Authentication Dial-In User Service (RADIUS) CoA messages can be used. The messages can be instantiated by the authentication, authorization and accounting server (AAA server), captive portal, or any other RADIUS-capable back-office systems and will modify/remove the redirects or upgrade the UE session. Note that the originator of the RADIUS CoA message must be able to include the specific vendor-specific attribute (VSA).

Network address translation (NAT)

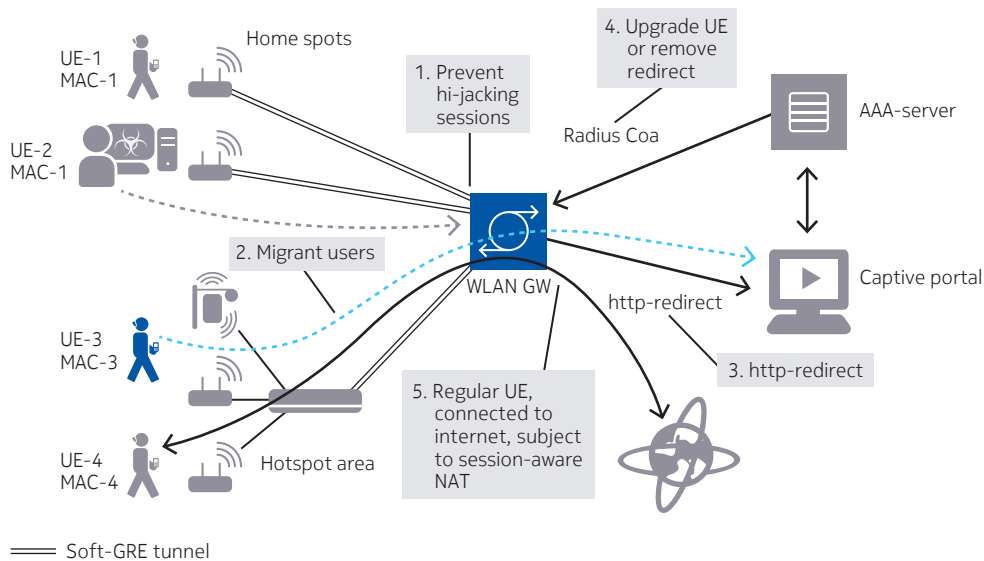
In most cases, private addresses are assigned to the UEs. Given the nature of Wi-Fi services, where UEs are often connected only for a short period of time, it is important to clean up all NAT bindings for a given UE when it disconnects from the carrier Wi-Fi service. This will mandate a correlation between the UE session and the NAT bindings.

Multi-access

The community Wi-Fi service can be delivered over a Residential Gateway (RG) acting as a Wi-Fi access point (AP), as well as hotspot infrastructure. Hotspot infrastructure can be positioned in locations where no RG is present (e.g., public places, event halls, sport stadium infrastructure) or can increase the footprint by adding APs in the urban area (e.g., street-cabinets, lamp posts). Figure 1 illustrates a community Wi-Fi implementation with open SSID annotated with call-outs.

¹ This does not apply to http traffic generated by a smartphone app in the background.

Figure 1. Community Wi-Fi with open SSID



The dynamic behavior of UEs can result in many pending UE sessions on the WLAN GW because a disconnected UE on an open SSID is neither detected by the WLAN GW nor by the back-end. As a result, there is a risk that a lot of resources are being consumed on the WLAN GW for idle UE sessions. To remove the idle UE sessions on the WLAN GW, the following mechanisms can be considered:

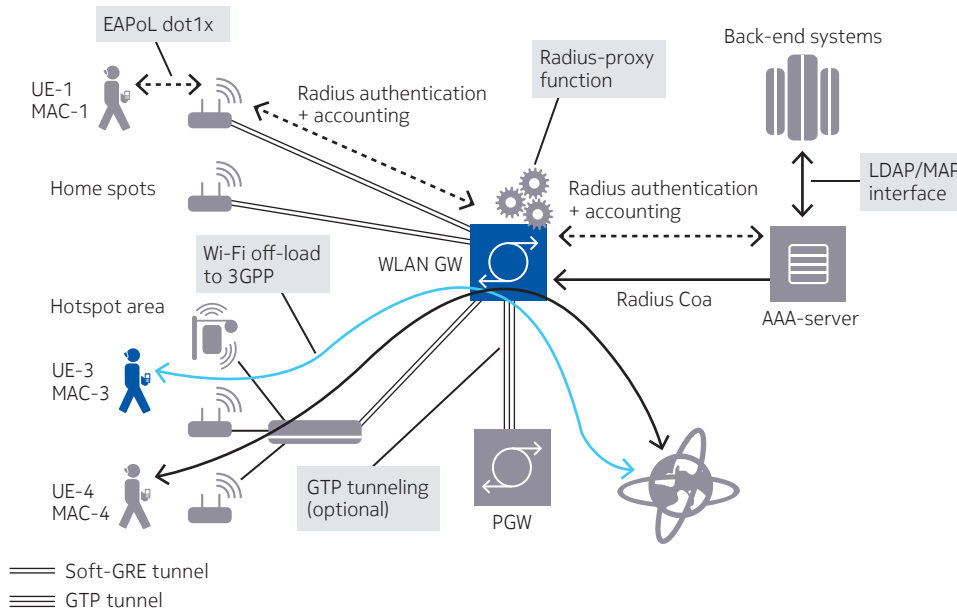
- Lower the Dynamic Host Configuration Protocol (DHCP) lease timers so that the session times out in minutes. Note that this may have a performance impact on the WLAN GW control plane and is not the optimal approach.
- Use the idle-timeout, returned by the AAA server as a VSA in the access-accept message to invoke the deletion of the UE session if no data traffic has been detected during a pre-defined period of time. Idle-timeout may not be a valid solution in all cases, because availability is restricted to specific scenarios.
- If an external traffic-monitoring device can detect idle data traffic from a UE, the AAA server informed by this traffic monitoring system can send a RADIUS disconnect-request message to the WLAN GW to delete the related UE session context.

Closed SSID

Closed SSID or “enterprise mode,” based on IEEE 802.1x/EAP authentication, can also be used for community Wi-Fi. Encryption of the air interface is a big advantage, as well as seamless authentication based on mutual EAP authentication methods, which avoids cumbersome login procedures through captive portals. While community Wi-Fi based on closed SSID is the preferred

solution, it can be perceived as being a more complex approach. The higher amount of control plane activity – a byproduct of the EAP authentication – can necessitate the greater engineering of the UE and WLAN GW control plane, as well as the performance of back-office systems, (including the AAA server). Figure 2 highlights the closed SSID model, illustrating all the building blocks.

Figure 2. Community Wi-Fi with closed SSID



In Figure 2, we see UE-1 being authenticated by EAP over LAN (EAPoL), which results in RADIUS communication between the home spot access point and the AAA server where the WLAN GW acts as RADIUS-proxy server. Once authenticated, a UE, such as UE-4 in the figure, can connect to the internet directly or, optionally, using a 3GPP network tunnel based on General Packet Radio Service (GPRS) Tunneling Protocol (GTP), or, in the case of UE-3 in the figure, between WLAN GW and the Packet Gateway (PGW). The AAA server will need to contact one or more back-office systems to validate the UE credentials.

Some specific characteristics important for a closed SSID deployment, are discussed below.

Authentication methods

Different EAP-authentication methods can reside on the same SSID allowing for authentication flexibility, where some UEs will authenticate based on username and password (e.g., EAP-PEAP) while others can authenticate based on a SIM-card (e.g., EAP-SIM, EAP-AKA, EAP-AKA'). When using EAP with a strong EAP type, such as Transport Layer Security (TLS) or the Protected Extensible Authentication Protocol (PEAP), both the client and

the server use certificates to verify their identities to each other. Certificates must meet specific requirements both on the server and on the client for successful authentication. Without using certificates, the closed SSID may be perceived as insecure by users, which needs to be avoided.

PMK caching

Pairwise master key (PMK) caching is in many cases enabled by default and will result in a UE re-connecting to a closed SSID without full RADIUS-based authentication, and data packets may arrive on the WLAN GW without any session awareness since there was no prior authentication. The WLAN GW will contact the AAA server to validate the incoming data-packets, (either regular IP packets or DHCP messages) and then allow or deny access.

Avoiding too many rejects for a given UE

A given UE may be rejected on the closed SSID after a number of failed attempts to connect. An example could be a one-time or short-life username/password that was wrongly entered on the UE. The risk here is that the UE clears the credentials and the end user does not reinitiate the process of entering the username/password again. This can lead to a perceived poor user experience.

Combined EAP authentication and authorization

The WLAN GW can act as RADIUS-proxy server and cache the necessary session parameters from the access accept message, which gives it the necessary information to build the UE-session context upon receiving the next DHCP message and combine the authentication and authorization phase into a single action.

Distributed mode for the RADIUS and AAA server

Given the potentially dynamic behavior of UEs in a shared Wi-Fi zone when there are a lot short duration connections and sessions do not last long, a higher number of RADIUS control messages can be expected. To help manage with this dynamic behavior, consideration should be given to deploy the RADIUS-proxy-server and the AAA server in a distributed mode.

Data retention and lawful intercept

Data-retention and lawful intercept (LI) can be provided on a WLAN GW by adding information on the outside/public IP-address as part of the RADIUS accounting messages and installing a tap on a per-UE basis.

GTP tunneling to the PGW

This is optional and can be invoked by the AAA server adding the necessary attributes in the access-accept messages. This offers a lot of flexibility as the decision to connect to the 3GPP network can be based on a commercial agreement, technical reasons, or even geographical location.

Selective IP traffic offload (SIPTO)

This allows the WLAN GW, based on traffic characteristics, to perform local break-out of traffic to defined IP service networks or to the internet. Data subject to SIPTO will be identified for each UE by an ingress access control list (ACL). Thus, the WLAN GW is capable of redirecting traffic per flow per UE away from the PGW, which optimizes resource consumption on the PGW and avoids sending obsolete data streams to the mobile core.

Differences between UE

It is even more important in a closed SSID implementation to be aware of the specific behaviors of UE brands or operating system versions (iOS, Windows or Android) as they may implement authentication and handle mobility slightly differently.

When a UE disconnects from a closed SSID, the AP will detect it and send an accounting stop message to the AAA server. The AAA server can decide (or not) to disconnect the UE from the WLAN GW in order to free up resources and close the session from a data-retention perspective. Optionally, the WLAN GW can decide to disconnect the UE as well, in case it is acting as RADIUS-proxy server and interprets the accounting stop message as a trigger to clear the UE session.

Noteworthy points

Irrespective of the SSID type (open or closed), there are some additional points that need to be considered during the community Wi-Fi design phase.

Service level agreement enforcement

Service Level Agreement (SLA) enforcement is required; service providers need to guarantee their residential subscribers that community Wi-Fi traffic passing through its RGs will not interfere with their private data bundling and premium services, such as telephony, video on demand or broadcast TV.

How and where to apply the SLA enforcement is a subject for debate. One can enforce the SLA per UE or AP on the WLAN GW, or a consideration can be determined to implement the SLA on the broadband network gateway (BNG), which is hosting the RG. The latter approach depends on the granularity of the capability of the BNG to distinguish between private data and community Wi-Fi traffic and prioritize accordingly.

Finally, there is the quality of the air interface, which is largely based on the distance between the UE and AP and can heavily impact the available bandwidth per UE. It is probably the most important influencing factor on quality of experience (QoE). Upstream (from UE to network), the AP may perform some level of traffic classification and/or scheduling, depending on vendor-specific implementations. However, probably the main focus of SLA enforcement is on the downstream direction (from network to UE).

Multi-SSID

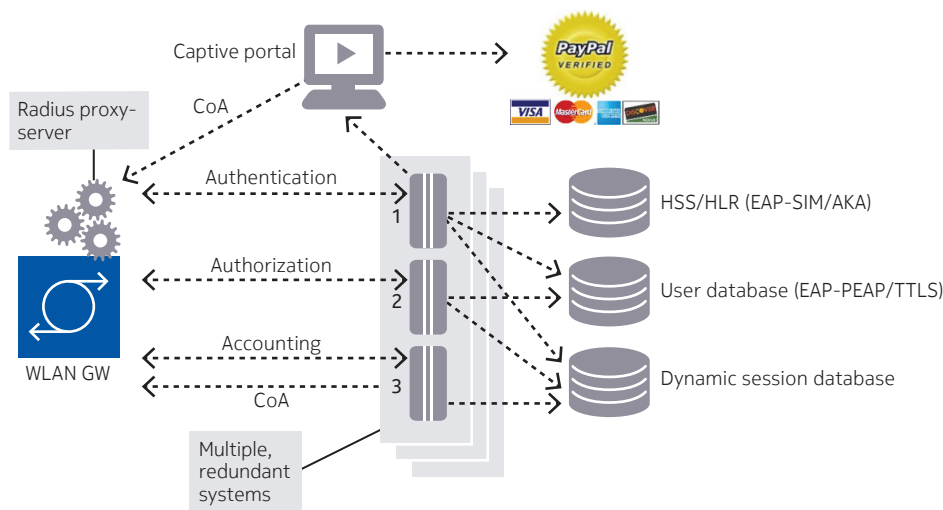
Community Wi-Fi can also be offered with a combination of open and closed SSID or multi-SSID. This allows for a secure service using seamless authentication on the closed SSID and open SSID for visiting subscribers with access using a captive portal. Traffic from each SSID can be separated and represented by a dedicated VLAN ID behind the GRE header of the transport tunnel.

AAA server

The AAA server is a crucial building block in the end-to-end solution; it takes care of the authentication (e.g., different EAP-methods), authorization (e.g., returning SLA profiles, IP-address) and accounting (e.g., data retention). All three functions can be combined on a single system or multiple systems, depending on the existing infrastructure or design recommendations. As previously discussed, a closed SSID may require a higher amount of RADIUS control plane messaging, which needs to be managed best by the AAA server. This demands a carrier-grade and, preferably, a distributed system.

Note that in the majority of use cases, the AAA server needs to maintain a dynamic session database. The database is mainly needed for closed SSID scenarios where PMK caching is involved, or in case multiple devices are allowed to connect using the same credentials.

Figure 3. AAA server layout



Hotspot aggregation

Current Wi-Fi deployments can be based on vendor-specific implementations, often with architectural customizations, as well as specific maintenance requirements per hotspot region. This results in hotspot islands that act independently. With a common WLAN GW, the Wi-Fi service becomes uniform and more centralized resulting in OPEX reduction. This section highlights the specific characteristics and requirements of hotspot aggregation on a WLAN GW.

Uniform service model

The common WLAN GW anchors all the UEs available on the related hotspots based on a uniform session framework. This clearly has advantages for a more flexible service offering, as well as OPEX reduction.

RADIUS back-end

The common WLAN GW(s) communicate(s) with a single AAA server (or set of AAA servers). This results in a common interface between the WLAN GW and AAA server, avoiding customizations on a per-hotspot basis. Subscriber provisioning will be more efficient and simpler as it only needs to be performed on a single location, accessible by the AAA server.

Uniform UE sessions

All UEs will be anchored on the WLAN GW and tied to a UE session. This UE session has a common set of parameters and features, independent of the access network, avoiding customization based on the type of hotspot or hotspot vendor.

Wholesale/retail service offering

With common WLAN GW(s), along with UE-session uniformity, easy and efficient implantation of a wholesale/retail service model is allowed. A retailer SSID can be implemented across the regions and all visitors can be back-hauled and anchored onto the common WLAN GW(s). Each retailer can be represented by a dedicated VPN on the WLAN GW, allowing for a clear isolation of traffic and features per retailer.

Connectivity models

Connecting different hotspot types and vendors to the WLAN GW results in multiple connection models. Selection of the appropriate model is driven by vendor specifications or design requirements. The connection models are illustrated in Figure 4.

Model 1

This model is based on a classic hotspot where all APs are connected to a Wireless Access Controller (WAC) taking care of the Radio Frequency (RF) management, Opportunistic Key Caching (OKC), and the RADIUS proxy

function. All data is transported over the GRE tunnel initiated on the WAC to the WLAN GW. This model is interesting in the following cases:

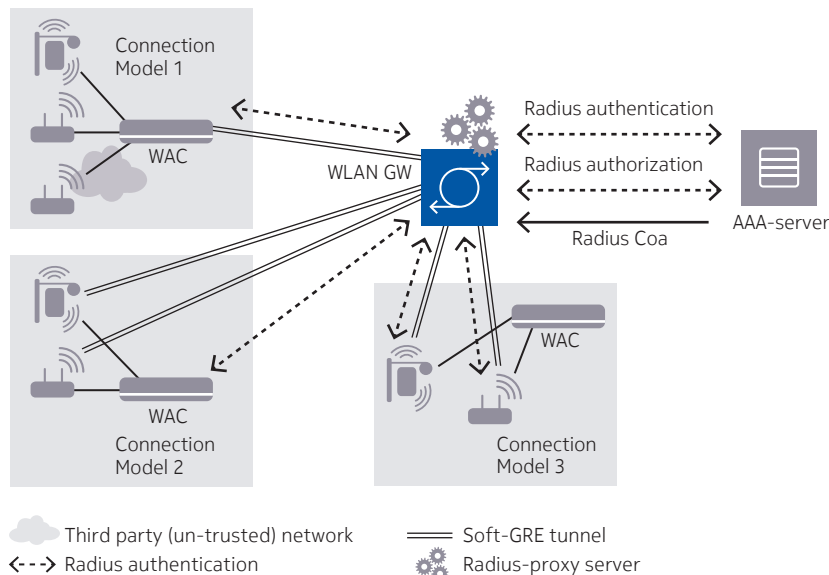
- When APs are covering a dense area, the WAC also takes care of the connectivity between the APs based on physical connections or Wi-Fi meshing
- In case the APs are connected to a third-party or untrusted network, it may be advantageous to benefit from potential proprietary data encryption between the APs and WAC.
- Where required, existing hotspots can be integrated by supporting GRE on the WAC without impacting the end actual AP itself.

Model 2

If the APs are not required to send all data traffic to the WAC, it is possible to instantiate the GRE tunnel directly from the AP to the WLAN GW. From the control plane perspective, the WAC still acts as RADIUS-proxy server and performs the majority of control plane functions, including OKC, RF management, and Operations, Administration and Management (OAM) functions.

The main advantage of this model is that the WAC does not require high-density, high bandwidth interfaces, which helps manage the WAC platform performance requirements and costs, along with aiding the virtualization of the WAC.

Figure 4. Connectivity models



Model 3

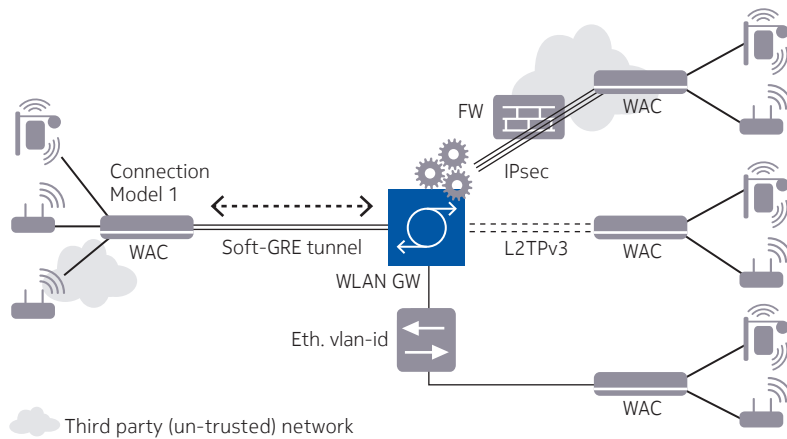
In scenarios where the APs are spread geographically – for instance, to increase the home-spot footprint – it is very efficient, if the AP directly communicates with the WLAN GW via RADIUS and all user data traffic to the WLAN GW is transported over a GRE tunnel. In this case, the function of the WAC is mainly reduced to RF management (if needed) and OAM functions.

Transport options

Multiple transport options are available as well. Although it is clear that GRE tunneling has many advantages, other transport options may be required for specific reasons.

Aside from selecting the transport tunneling mechanism, it is very important to investigate the Maximum Transmission Unit (MTU) size between the AP and WLAN GW, with the goal to prevent IP fragmentation and/or re-assembly, as much as possible. The MTU size is dependent on the underlay network and the capabilities of the access infrastructure, which may introduce specific implementations during architectural discussions. Transport options, described below, are illustrated in Figure 5.

Figure 5. Transport models



GRE

As indicated earlier, GRE is a simple lightweight protocol, suitable to transport Ethernet traffic over an IP network. This is a perfect match for residential gateways because the performance impact is limited, compared to other tunneling techniques. GRE encapsulation is supported on both IPv4 and IPv6, depending on the characteristics of the underlay network.

IPsec

Where the AP/WAC has to communicate to the WLAN GW over a third-party or un-trusted network, IPsec may be required to encrypt the data traffic. Also, GRE packets may face difficulties passing the NAT process, sometimes a requirement for IPsec tunneling. Note that IPsec tunnels can be used to natively transport the Ethernet frames from the SSID or to GRE tunnel packets. The latter allows the IPsec and GRE tunnels to be split between different NEs.

Ethernet

To prevent costly or complex changes to existing infrastructure, the WLAN GW should be able to connect access networks over Ethernet. The Ethernet connectivity between the WAC and the centralized WLAN GW can be based on switches, cross-connects, or Virtual Leased Lines (VLLs).

Layer-2 Transport Protocol version 3 (L2TPv3)

L2TPv3 is considered an alternative protocol to GRE for transporting Layer-2 traffic over IP. A potential advantage of L2TPv3 over GRE is the presence of a UDP header, allowing the tunneling mechanism to easily traverse a NAT process between the AP and the WLAN GW.

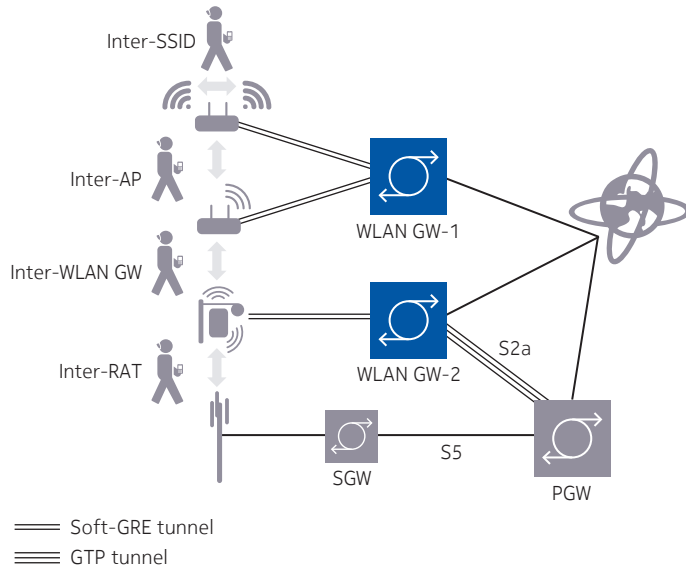
Mobility

Along with a uniform service model and seamless authentication, mobility is another advantage of a carrier Wi-Fi service. Smooth, seamless, and secure mobility increases the subscriber's QoE and makes the service more attractive. However, careful consideration should be given to ensure an optimal user experience and service quality.

Inter-SSID

Where multiple SSIDs are transported over the same tunnel mechanism, using a VLAN ID as an identifier, mobility from a specific SSID to another one on the same AP (tunnel) has to be handled properly on the WLAN GW. Especially when moving from one open to another open SSID, it is important for the WLAN GW to verify if the UE has been disconnected on the original SSID before attaching to a new one. Sending a unicast Address Resolution Protocol (ARP) request to the UE on the original SSID allows verification of the presence of the UE. In normal operations, there will not be a reply to the ARP request, because the UE has disappeared. If a reply is received, the mobility event can be seen as an attempt to hi-jack a session and should not be allowed.

Figure 6. Mobility scenarios



Inter-SSID mobility may not be perceived as “seamless” by the user because a new IP address will be assigned and portal authentication may be required, causing some potential disruption to some applications.

Inter-AP

Separate anchoring of UEs and transport tunnels on the WLAN GW allows for seamless inter-AP mobility. This is because moving from one AP to another has no impact on the anchored UE session; only a change of transport tunnels takes place. Seamless inter-AP mobility preserves the IP-address, with no impact on running applications.

It should be noted that, in some scenarios, inter-AP mobility is not recommended for security, commercial, or for other considerations. For instance, there may be different mobility requirements for open SSID compared to closed SSID.

Inter-WLAN GW

Mobility between WLAN GWs may occur as the result either of crossing geographical boundaries or geo-redundancy, that is, where a neighboring or standby WLAN GW takes over the functionality. In this case, the UE connects without user interaction for seamless connectivity, but this mobility may impact some services and applications, because a new UE context is created with a different public IP address (new NAT bindings).

Seamless inter-WLAN GW mobility for geo-redundancy can be achieved in a few ways:

1. The AP sends ICMP packets to detect if the WLAN GW is reachable. If not, it sends the Wi-Fi traffic over another GRE tunnel to the standby WLAN GW.

2. In the case where both WLAN GWs advertise the same GRE tunnel destination address, the network metrics decides on which WLAN GW the GRE tunnels will terminate. This is often referred to as Anycast routing and is the most simple approach. Even so, it requires a stable underlay network because network instabilities may cause GRE tunnels to terminate on the wrong WLAN GW, a situation that needs to be prevented.
- 3 In a pure active-standby scenario, only the active node advertises the GRE destination address. Once the standby WLAN GW detects the withdrawal of the specific route, it concludes that the active WLAN GW is no longer reachable and starts advertising the same address to attract the GRE traffic. This option allows for efficient usage of public addresses because the same outside IP-address pool can be re-used by both active and standby WLAN GW, since only a single one is active at any time.

All three of the above mechanisms are functionally equal. The preferred one to implement will be based on network characteristics and functional requirements. Crossing geographic boundaries can be achieved by assigning a specific IP-address as a GRE destination per region or an Anycast IP-address for all APs, which are regionally routed to the correct WLAN GW. Optionally, both mechanisms can be combined with the active-standby mechanism per WLAN GW.

Inter-RAT

Mobility between Wi-Fi and 3GPP networks is an interesting approach to merge the two networks (mobile and fixed). This helps provide a seamless wireless access from a subscriber's perspective. There are a few ways to offer inter-RAT mobility:

1. **3GPP MAPCON** (Multiple Access PDN Connectivity): the network assigns a different IP address to the RAN connection than to the Wi-Fi connection, and the continuity of Transmission Control Protocol (TCP) applications is achieved through the use of MultiPath TCP (MPTCP) clients and servers. However, this offers no solution for conversational applications (voice) and non-buffered streaming (live TV or radio), which typically rely on UDP.
2. **3GPP Release 12**, which evolves S2a-based Mobility over GTP, requires an additional control protocol between the AP and WLAN GW, called the Wireless LAN Control Protocol (WLCP).
3. **Hybrid access** is a mechanism where the UE connects both to the RAN and Wi-Fi, and the WLAN GW sets up a GTPv2 tunnel to the PGW, which binds both S2a and S5 interface to a single session. The PGW can assure that downstream traffic is sent over the S2a interface (if this is present), because many UE's by default prefer the Wi-Fi interface over the cellular interface for sending and receiving data (assuming both are operational). In this scenario, it is mandatory to delete the GTPv2 tunnel between the WLAN GW and PGW once the UE has disconnected from the Wi-Fi network.

This will bring in specific requirements on the AP/WAC and WLAN GW during the service design phase.

Option 3 is the option to offer seamless inter-RAT mobility between the Wi-Fi and cellular network with IP-address preservation until the commercial availability of option 2. Option 1 can offer inter-RAT mobility, but without IP-address preservation.

Value-Added-services

On top of internet connectivity, a carrier Wi-Fi solution can offer additional services, referred to as Value-Added Services (VAS). Although not mandatory, it may be interesting to consider them during the service design phase, as they may be implemented in consecutive phases.

The following is a short summary of some example VASs.

In-browser notification

This mechanism will insert unsolicited, clientless, in-browser messages to inform the subscriber on connectivity or location-specific information, as well as commercial offers and other kinds of notifications. Notifications are targeted per subscriber/UE and can be enforced on the WLAN GW by a RADIUS CoA message. In-browser notifications are less disruptive than http-redirects and are mainly there to grab the subscriber's attention while browsing the internet.

Http one-time redirect

Another use case based on the in-browser notification is an intelligent implementation of one-time http-redirects. Given that many apps on smartphones communicate with servers using HTTP, it is crucial to apply the one-time redirect to a real browsing session, not just any HTTP flow.

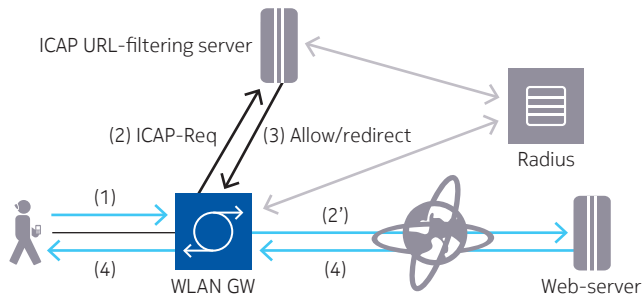
URL-based white-listing

Wi-Fi hotspots may allow free access to sponsored content, which can be achieved by URL-based white-listing. If a UE browsing the sponsored content then chooses to call up un-sponsored content, it will be redirected to a portal where access can be granted after authentication (payment portal most likely).

Parental control

The public nature of Wi-Fi hotspots will most likely require some kind of parental control to prevent opening inappropriate content. For this reason, an Internet Content Adaptation Protocol (ICAP) interface is required on the WLAN GW, to perform the necessary actions on a per subscriber basis while keeping the scaling and performance requirements in mind. Figure 7 illustrates the message flow of an ICAP interface on the WLAN GW. Note that parental control can also be achieved by URL-based black-listing.

Figure 7. ICAP interface



Deep packet inspection

In general, DPI or application awareness may be achieved by embedded functionality on the WLAN GW or on a dedicated system connected to the WLAN GW. Depending on specific requirements, or the presence of DPI systems in the network, the preference may or may not be to integrate it into the WLAN GW.

Future evolutions

Although Wi-Fi as an access technology has been available for several years, evolution can still be expected in the near future. The following topics will influence upcoming Carrier Wi-Fi services.

Network functions virtualization

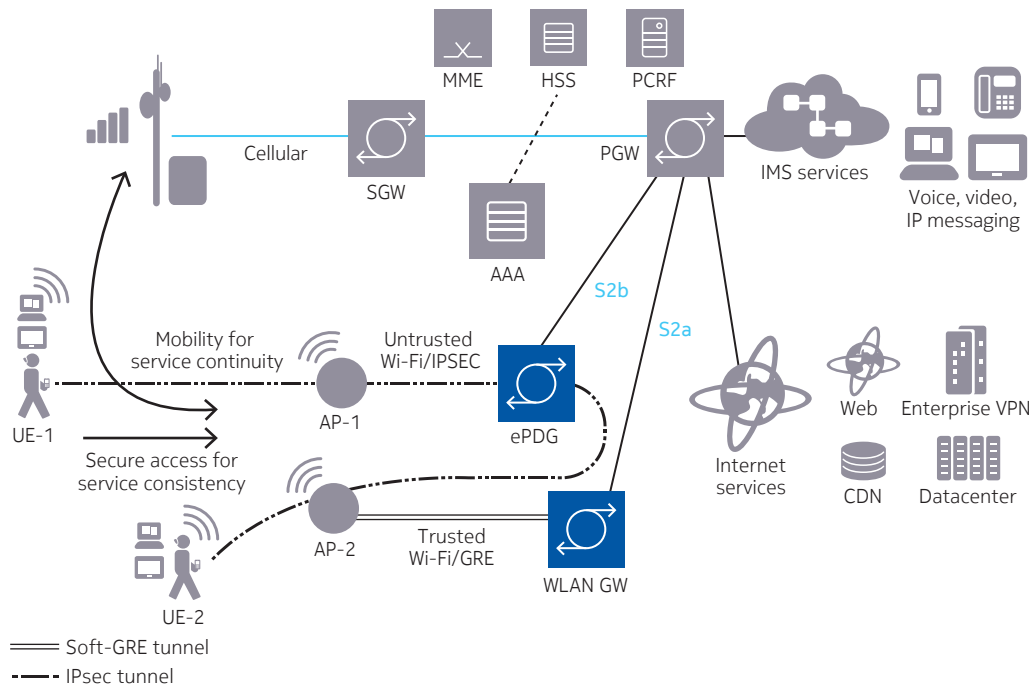
Although network functions virtualization (NFV) may not be appropriate for every network function, in the case of carrier Wi-Fi services, NFV may wish to be considered for the following reasons:

- The performance impact can be more on the control plane than the data plane, especially given the dynamic behavior of the UE. This can be in contrast to residential triple-play services, where HD VOD and HD BTV are heavy consumers of data plane bandwidth.
- The number of Wi-Fi subscribers varies significantly over time. Peak hours are defined at intervals throughout the day or short-term but intense events, such as concerts or sporting events. This pattern of demand is easier to manage in a flexible, virtualized cloud environment where resources could be allocated on a temporal and demand basis.

Evolved packet data gateway

The introduction of always-on IPsec clients on UE devices and versions of popular mobile OSs will speed up the introduction of evolved Packet Data Gateway (ePDG) in Carrier Wi-Fi solutions. Although a WLAN GW, which supports the trusted wireless access gateway (TWAG) capability, is able to handle secure connections, the ePDG will be the anchor point of the encrypted tunnels initiated by these IPsec-enabled UE devices.

Figure 8. WLAN GW (TWAG) and ePDG



As illustrated by UE-2 in Figure 8, the communication between the UE and ePDG can be over any kind of Wi-Fi connection, as well as existing community Wi-Fi services.

Conclusion

Carrier Wi-Fi, which leverages building blocks available in most fixed networks, is a valuable additional service to offer subscribers. Although many field-proven carrier Wi-Fi services have already been operating for years, evolving Carrier Wi-Fi so that it can improve the service compared to traditional Wi-Fi service, will create significant differentiation for service providers.

A number of topics require further investigation as part of re-setting subscribers' expectations of a carrier Wi-Fi service. These will result in specific requirements for the carrier Wi-Fi service design.

- **Carrier-grade behavior of WLAN GW and AAA server:** a carrier Wi-Fi service can go beyond the best-effort internet connection offered by small retailers, but the WLAN GW and AAA server will need to address the carrier-specific nature of the service.
- **QoE needs monitoring:** a best-in-class approach to maintaining a higher standard of service is not to rely on customer feedback, but to launch time-based, automated end-to-end tests to verify the health of the service.

- **EAP authentication overhead:** the dynamic behavior of UEs may result in much control plane activity on the network. This needs to be taken into consideration when defining scaling requirements.
- **UE-specific profiles:** the variety of UE types and different OS versions is large, and innovation is continuous in this field. As a result, regular testing of a wide range of UEs on the Carrier Wi-Fi service will be mandatory.
- **Value-added services:** one of the potential differentiators of a carrier Wi-Fi solution compared to best-effort internet connectivity is the option to deliver VAS. This may be valuable to all parties, including the service provider, retailer, and end customer.
- **Evolving technology and markets:** this is an area of rapid innovation and changing consumer expectations and behaviors, so it is critically important to keep an eye on upcoming technologies and emerging market trends.

Acronyms

3GPP	3rd-Generation Partnership Project
AAA	Authentication Authorization and Accounting
ACL	Access Control List
AP	Access Point
ARP	Address Resolution Protocol
BNG	Broadband Network Gateway
BTV	Broadcast TV
CGN	Carrier-grade NAT
CoA	Change of Authorization
COB	Close of Business
DHCP	Dynamic Host Configuration Protocol
DPI	Deep Packet inspection
EAP	Extensible Authentication Protocol
EAPoL	EAP over LAN
ePDG	Evolved Packet Data Gateway
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GTP	GPRS Tunneling Protocol
HD	high definition
HTTP	Hypertext Transport Protocol
HW	Hardware
ICAP	Internet Content Adaptation Protocol
LI	Lawful Intercept
LSN	Large-Scale NAT
MAPCON	Multiple Access PDN Connectivity
MNO	Mobile Network Operator
MPTCP	Multipath TCP
MSO	Multiple System Operator / cable company
MTU	Maximum Transmission Unit
MVNO	Mobile Virtual Network Operator
NAT	Network Address Translation

NFV	Network Functions Virtualization
OAM	Operations, Administration and Management
OKC	Opportunistic Key Caching
OPEX	Operating Expense
OS	Operating System
PEAP	Protected Extensible Authentication Protocol
PDN	Packet Data Network
PGW	Packet Gateway (3GPP)
PMK	Pairwise Master Key
QoE	Quality of Experience
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RAT	Radio Access Type
RF	Radio Frequency
RG	Residential Gateway
SIM	Subscriber Identity Module
SIPTO	Selective IP Traffic Offload
SLA	Service Level Agreement
SSID	Service Set Identifier
SIPTO	Selective IP Traffic Offload
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TWAG	Trusted Wireless Access Gateway
UDP	User Datagram Protocol
UE	User Equipment
URL	Uniform Resource locator
VAS	Value-add-services
VLAN ID	Virtual LAN Identifier
VLL	Virtual Leased Line
VOD	Video on demand
VoWi-Fi	Voice over Wi-Fi



VSA	Vendor-Specific Attributes
VPN	Virtual Private Network
VSA	Vendor Specific Attributes
WAC	Wireless Access Controller
WLAN GW	Wireless LAN Gateway
WLCP	Wireless LAN Control Protocol

References

- RFC 3931: Layer 2 Tunneling Protocol – version 3
- RFC1701: Generic Routing Encapsulation (GRE)
- RFC2784: Generic Routing Encapsulation (GRE)
- RFC2865: Remote Authentication Dial In User Service (RADIUS)
- RFC2866: RADIUS Accounting
- 3GPP TS 23.402, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture Enhancements for Non-3GPP Accesses
- IETF Layer 2-Aware NAT. draft-miles-behave-l2nat-00. March 4, 2009.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: PR1606020720EN (July)