WHITE PAPER

# Software-Defined Community Wi-Fi:

## *Key Advantages and How to Get Started*

April 30, 2015

# Table of Contents

# Executive Summary

Fixed-line Internet Service Providers (ISPs) are deploying community Wi-Fi for a variety of reasons — to reduce churn, offload mobile data, some even to generate new incremental revenue [1]. All these reasons can be traced back to a single theme: staying relevant in a *Mobile First* future.

In this white paper, we explain how fixed-line ISPs with remotely managed residential gateways can use Anyfi Networks' **Carrier Wi-Fi System** to create amazing Wi-Fi user experiences for subscribers on the go — experiences that inspire loyalty and build customer relationships. Our analysis is focused on user experience and **key advantages**, using the currently most deployed community Wi-Fi architecture (the so-called Soft-GRE architecture) as a reference point, and the Wireless Broadband Alliance's (WBA) gap analysis [2] as the problem statement.

We conclude that the **key advantages** of Anyfi Networks' **Carrier Wi-Fi System** — **Dynamic Shaping of Guest Traffic**, advanced radio link-level **Admission Control**, intelligent **Steering of Home Users to Home Wi-Fi**, **Infrastructure-Initiated Hand-Over**, detailed **Quality of Service Monitoring**, **Trustworthy End-to-End Security** and **Standard Interfaces** — all combine to enable user experiences on par with 3G and 4G, without any client-side software or even a change of settings.

In later chapters we introduce the Software-Defined Wireless Networking (SDWN) architecture that underpins our **Carrier Wi-Fi System** and explain its grounding in **Software-Defined Networking** (SDN) principles. We also introduce *Anyfi.net software*, a small software component that can easily be integrated into almost any residential gateway, rendering it compatible with Anyfi Networks' **Carrier Wi-Fi System**.

In the closing chapter we explain how to get started with the free evaluation version of the **Carrier Wi-Fi System**, available for download as a **Virtual Network Function** (VNF). We also show how *Anyfi.net software* can be installed on many community Wi-Fi routers in just a few minutes, enabling ISPs to build proofs of concept (PoCs) and deploy small-scale field trials.

# User Experience

Regardless of why you are deploying community Wi-Fi, your success hinges on providing a the best possible user experience for guests, while at the same time prioritizing the primary home Wi-Fi user experience.

In this chapter we outline four user experiences, highlighting the **key advantages** of basing your community Wi-Fi service on our **Carrier Wi-Fi System**. In the next chapter we will then go into more detail on how these **key advantages** are implemented.

## Fixed-Line Subscribers in Their Own Home

Several key advantages of the **Carrier Wi-Fi System** combine to safeguard the primary fixed-line subscriber's user experience in his or her own home.

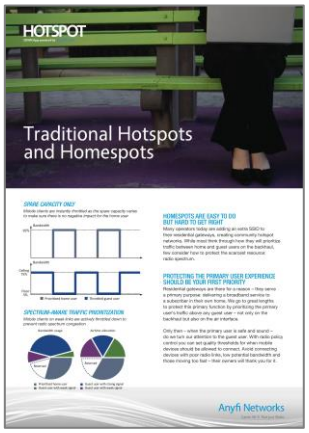
First, *Anyfi.net software* provides spectrum-aware **Dynamic Shaping of Guest Traffic**. This means that the operator can precisely control to what extent guest users can impact home users, both on the WAN connection and on the Wi-Fi air interface. With adaptive link-level **Admission Control** there is no need to worry about subscribers living in busy areas, e.g., close to a public attraction. If a gateway is too busy serving the home user (or a large number of guests) it will simply not present the network to new devices, making it impossible to even find.

Second, in the Soft-GRE architecture devices sometimes connect to the public network even when the subscriber is at home. In our architecture the Controller has a global view of the network and can **Steer Home Users to Home Wi-Fi** when within radio range of their own home gateway.

These processes are, of course, entirely invisible to the end-subscriber. From a pure end-user perspective, your community Wi-Fi service may not be detectable at all when the subscriber is in his or her own home.

## Traditional Homespots

In the traditional homespot or hotspot user experience, guest users connect to a separate operator-branded Wi-Fi network, distributed through all gateways. Once connected, guests are met by a captive portal where they can authenticate by entering a user name and a password.




**SDWN App: HOTSPOT**

HOTSPOT is an SDWN App for centrally terminated carrier Wi-Fi networks of the more traditional kind.

Related materials:

- Solution Brief
- Solution Presentation

If the network is left open, then the perhaps most noticeable benefit of our **Carrier Wi-Fi System** lies in the improved quality of service offered by adaptive link-level **Admission Control**: Guest devices will not connect too early to Wi-Fi, when the radio link (or the backhaul, for that matter) cannot support an acceptable user experience.

As guests move within the coverage area, their devices will roam from gateway to gateway, with **Infrastructure-Initiated Hand-Over** if necessary. When the signal gets too weak to support a meaningful quality of experience, then the **Admission Control** will withdraw the service, and the community Wi-Fi network will no longer be visible to that specific device. The same happens if a meaningful quality of service cannot be delivered for any other reason, e.g., the home user starts streaming an HD video from his or her home NAS, consuming all available spectrum.

Guests also benefit from the **Dynamic Shaping of Guest Traffic** implemented in *Anyfi.net software*. Instead of being limited to a static bandwidth limit, guests can use the majority of radio spectrum and backhaul bandwidth available (up to the *ceiling*), as long as this does not adversely affect a primary home user. But it is of course possible to limit the bandwidth available to a specific guest device: just integrate towards existing OSS/BSS systems through **Standard Interfaces** such as RADIUS.

Some additional benefits become apparent if the operator opts to add Wi-Fi security. End subscribers on the go will see noticeably faster authentication and **Seamless Hand-Overs With Key Caching**.

Security-conscious operators and end subscribers will also benefit greatly from the **Trustworthy End-to-End Encryption**, knowing that subscriber data stays encrypted all the way from the mobile device to the operator's Wi-Fi core (and, of course, back again in the egress direction). This means that data privacy and integrity is ensured — even against an attacker who is in control of the visited access point — without any negative impact on performance. Throughput well in excess of 25 Mbps is easily achieved even on an entry-level residential gateway.

Advanced **Quality of Service Monitoring** benefits end-users indirectly: when the ISP knows where the weak spots in their network are they can address them, by installing access points to augment the community Wi-Fi network, or even by directing marketing in such a way that the community Wi-Fi coverage is improved.

## Seamless Home Wi-Fi on the Go

One of the strong points of SDN is that it allows for **Scalable Network Virtualization**. The operator therefore has the option of allowing fixed-line subscribers to seamlessly connect to their own home Wi-Fi networks remotely, through other subscribers' gateways.

The user experience in this use-case is more or less identical to regular home Wi-Fi: Devices connect and authenticate automatically, even the first time they connect on the go. There is no registration process, no software to install on the mobile device, not even any settings to change — it just works.

One of the benefits of allowing subscribers to connect to their own home Wi-Fi remotely is automatic and secure remote access to the home LAN. It may seem like this benefit comes at the expense of an additional round-trip to the home gateway, even for Internet-bound traffic. But this is not so. An Optimizer can be inserted into the Wi-Fi over IP tunnel, so that Internet-bound traffic is broken out centrally in the network. This avoids the unnecessary round-trip to the home gateway and ensures encrypted throughput well in excess of 25 Mbps for Internet-bound traffic.

Guests will, of course, benefit from the same key advantages described above: **Dynamic Shaping of Guest Traffic** ensures that guests get as much bandwidth as possible (without impacting a home user); and **Infrastructure-Initiated Hand-Overs** ensure mobility on par with 3G or 4G within the coverage area. Subscribers can, for example, start a VoIP call in their home (connected to their regular home Wi-Fi) and walk out the door and down the street, without losing the call as their device is handed over from gateway to gateway.

With this approach there is no need for a captive portal to authenticate users; they are automatically authenticated using the WPA passphrase already stored in their device. But there may still be a business need to interact with the end-subscriber, e.g. for online billing. The Optimizer is designed to interface with existing OSS/BSS systems on **Standard Interfaces** such as RADIUS. This allows e.g. a model where low tier subscribers can only connect one device to the community Wi-Fi network, and will be prompted to upgrade their subscription to a higher tier if they attempt to connect with a second device.

Advanced **Quality of Service Monitoring** benefits end-subscribers in this use-case too. When the ISP knows where the weak spots in their network are they can address them.

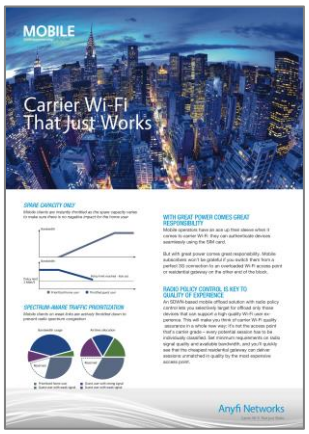

**SDWN App: SIMPLE**

SIMPLE is an SDWN App for seamless guest access and community Wi-Fi.

Related materials:

- Solution Brief
- Solution Presentation

# Secure Mobile Wi-Fi Offload




**SDWN App: MOBILE**

MOBILE is an SDWN App for secure mobile Wi-Fi offload with QoS integration towards the 3GPP network.

Related materials:

- Solution Brief
- Solution Presentation

In this use case, mobile data is offloaded from a cellular 3G or 4G network, onto a SIM-authenticated Wi-Fi network distributed through all residential gateways. This is where Anyfi Networks' **Carrier Wi-Fi System** really shines.

Adaptive **Admission Control** ensures that devices are only switched over to Wi-Fi when the radio link can support a high quality of service, and that they are switched back to the mobile network if Wi-Fi quality falls below an acceptable level. Every aspect that can affect quality of service is taken into account — radio link quality, backhaul capacity as well as spectrum availability and contention with other offloaded "guests" or fixed-line home users.

**Dynamic Shaping of Guest Traffic** ensures that guests can use the majority of radio spectrum and backhaul bandwidth available (up to the *ceiling*), as long as this does not adversely affect a primary home user.

Also note that **Admission Control** and **Dynamic Shaping of Guest Traffic** interact. For example, if a home user suddenly starts streaming an HD video from an NAS on the LAN, then *Anyfi.net software* will immediately throttle the offloaded "guest" to protect the radio airtime needed to stream the video. If the dynamically computed "guest" throttle limit falls below the **Admission Control** quality requirement, then the offloaded "guest" will be forcefully disassociated from the Wi-Fi network on the radio link level. The "guest" device will then scan for alternative access points, which again will only be visible if the quality requirement can be met there. If no access point with sufficient quality can be found, the device will return to 3G or 4G. None of this behavior requires any additional software on the mobile device.

Lastly, **Trustworthy End-to-End Security** ensures that even the most security-conscious operators can leverage their (fundamentally non-trusted) residential gateways as a trusted non-3GPP access.

It should also be noted that this **Trustworthy End-to-End Security** does not come at the expense of performance. If we look in the ingress direction for a moment, we will see that IEEE 801.11 frames are encrypted on the mobile device using the standard AES CCMP block cipher (implemented in fixed silicon) and are then transmitted over the air to the visited residential gateway. It may be tempting to assume that these frames must be decrypted there, in the residential gateway's Wi-Fi chipset, but in our architecture the access point does not even know the encryption key. Instead, *Anyfi.net software* encapsulates the raw encrypted IEEE 802.11 frames in UDP/IP packets and forwards them to a Gateway in the operator's Wi-Fi core. The

Gateway then decrypts the data, again using hardware acceleration (Intel AES-NI instruction set or Octeon NPU). None of this behavior requires any additional software on the mobile device.

Tunneling of raw IEEE 802.11 frames brings an additional benefit for "guests": **Seamless Hand-Over With Key Caching** ensures a significantly reduced authentication and reauthentication delay. Remember, the encryption keys are derived between the mobile device and Gateway, and as the mobile device roams from (visited) access point to access point, it will typically stay connected to the same Gateway. This means that encryption keys can be cached, and that a full IEEE 802.1X (re-)authentication can be avoided in most cases. To benefit from this key advantage, the mobile device must support Opportunistic Key Caching (OKC), Pairwise Master Key Security Association (PMKSA) caching or IEEE 802.11r Fast Transition. Most mobile devices do support at least one of these mechanisms.

By integrating the cellular and Wi-Fi data planes (over the 3GPP S2a interface), it is possible to ensure session continuity in the switch-over between cellular and Wi-Fi. This allow for an "almost always best-connected" user experience where mobile devices are switched over to Wi-Fi only when a high quality of experience can be delivered there.

As a next step, we are currently looking into control plane integration between cellular and Wi-Fi, i.e., using dynamic per-device **Admission Control** quality thresholds computed (and regularly recomputed) based on the quality achievable on the cellular side. This type of real-time traffic steering between Wi-Fi and cellular can provide an "always best-connected" user experience, without any special requirements on the mobile device.

With SIM authentication there is no need for a captive portal to authenticate users, but there may still be a business need to interact with the end-subscriber, e.g. for online billing. The Gateway interacts with OSS/BSS systems on **Standard Interfaces** such as RADIUS and IEEE 802.3 bridged Ethernet. This allows e.g. a model where the bandwidth of low tier subscribers is restricted.

Advanced **Quality of Service Monitoring** benefits end-subscribers in this use-case too. When the ISP knows where the weak spots in their network are they can address them.

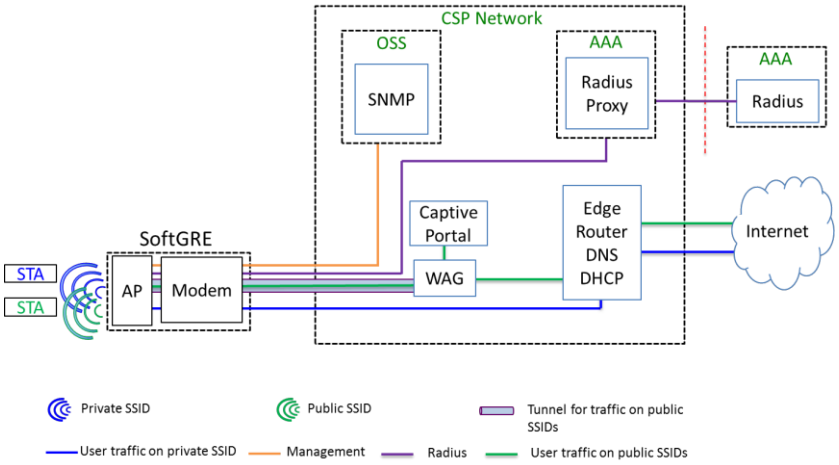
# Key Advantages

In this chapter, we go into more detail about how our **Carrier Wi-Fi System** realizes the **key advantages** referred to in the previous chapter. But we start with a brief introduction to the Soft-GRE architecture. Since this is the currently most deployed architecture for community Wi-Fi we have chosen it as a reference point.

## Soft-GRE as a Reference Point

The most commonly deployed architecture for community Wi-Fi today is the so-called Soft-GRE architecture. A "second SSID" (and perhaps third or even fourth) is broadcast from residential gateways, and the associated traffic is tunneled into the operator's Wi-Fi core over GRE on OSI Layer 2.

FIGURE 1
Illustration of the Soft-GRE architecture from the Wireless Broadband Alliance's recently published Community Wi-Fi White Paper [2].



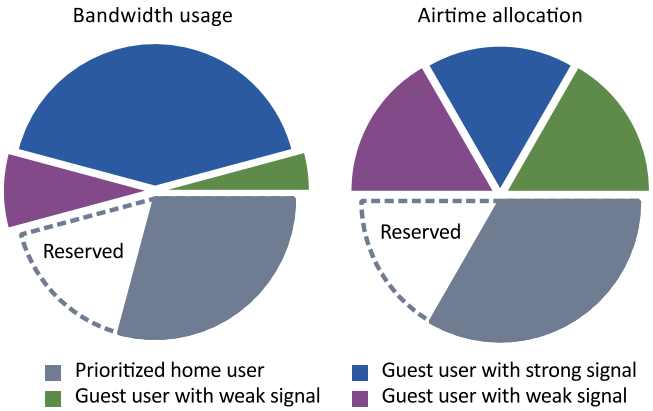

It is called "Soft-GRE" because the GRE tunnel termination point (labeled *WAG* in the figure) does not need to be configured with the IP addresses of all the residential gateways as end points; it simply learns them by examining incoming packets, much in the same way a switch learns which physical port a particular device can be found on. The Wireless Broadband Alliance (WBA) has published a white paper on the Soft-GRE architecture for community Wi-Fi, also outlining some its weaknesses [2].

## Dynamic Shaping of Guest Traffic

Protecting the primary home Wi-Fi user experience should be the first priority of any community Wi-Fi solution. In the classic Soft-GRE architecture this is, however, difficult.

For example, while it is relatively trivial to limit the bandwidth available to guest users by throttling at the GRE tunnel termination point (the *WAG*), it is still possible for a guest device to consume a large amount of radio spectrum. The reason is that the range of throughput that the IEEE 802.11 air interface can provide is huge, ranging from less than 1 Mbps to over 100 Mbps.

FIGURE 2
*Anyfi.net software* operates out of band with respect to the primary function of the gateway. Throttling is applied only to guests, ensuring that they do not negatively impact the home user (or each other). On the air interface, this means airtime fairness between guests and priority to the home user.

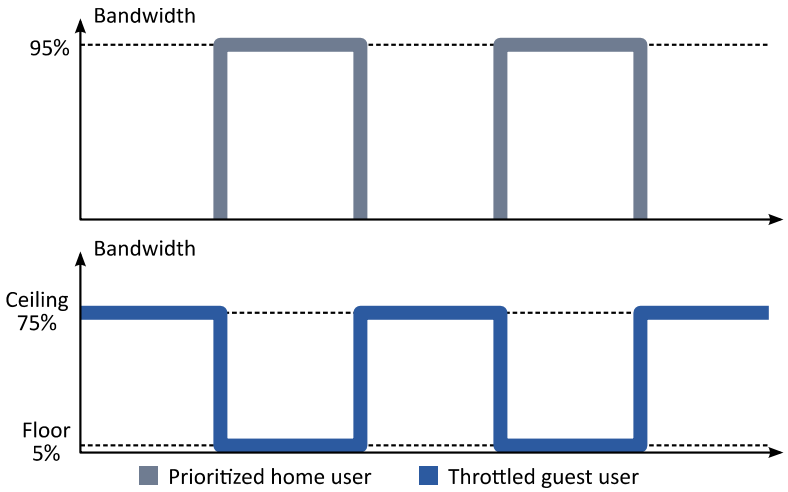



A guest device transferring data at a modest, 1 Mbps rate may thus be consuming anywhere between 1% and 100% of available radio spectrum, depending on the radio link modulation and transmission retry rate. This radio link quality information is unavailable at the GRE tunnel termination point, making informed traffic prioritization decisions impossible.

These problems can be mitigated to some extent within the classic Soft-GRE architecture, e.g., by disabling low modulation rates for the "second SSID". This reduces the dynamic range of air interface throughput, thereby increasing the effectiveness of static throttling, somewhat.

FIGURE 3

*Anyfi.net software* dynamically computes throttling limits based on the *floor* and *ceiling* parameters and the bandwidth use of the primary home user. The home user is prioritized on both the WAN connection and Wi-Fi air interface.




However, solving these problems requires radio management software on the gateway. In our architecture, the operator can configure a so-called *floor* and *ceiling*, which are essentially the minimum and maximum percentages of bandwidth that can be allocated to guests (without contention against the primary home user). These limits are then enforced by *Anyfi.net software* running on the gateway. The software takes both backhaul and radio spectrum use into account and adjusts throttling limits dynamically, several times per second. The results are minimal impact to the home user and airtime fairness between guests.

## Admission Control

Community Wi-Fi by its nature offers only limited coverage. As a simple consequence of geometry, such "spotty" networks will have a large proportion of fringe coverage where quality of service is low — in fact, often so low that no meaningful communication is possible. Unfortunately, many if not most devices will still attempt to connect to Wi-Fi in these situations, causing the average session quality in the classic Soft-GRE architecture to hover somewhere between poor and unusable.

This problem can be mitigated somewhat by disabling low modulation rates for the "second SSID". But disabling low modulation rates also reduces the coverage area and makes connections less reliable even within it, simply because the rate control algorithms in the mobile device and visited gateway can no longer fall back to lower, more robust rates even temporarily.

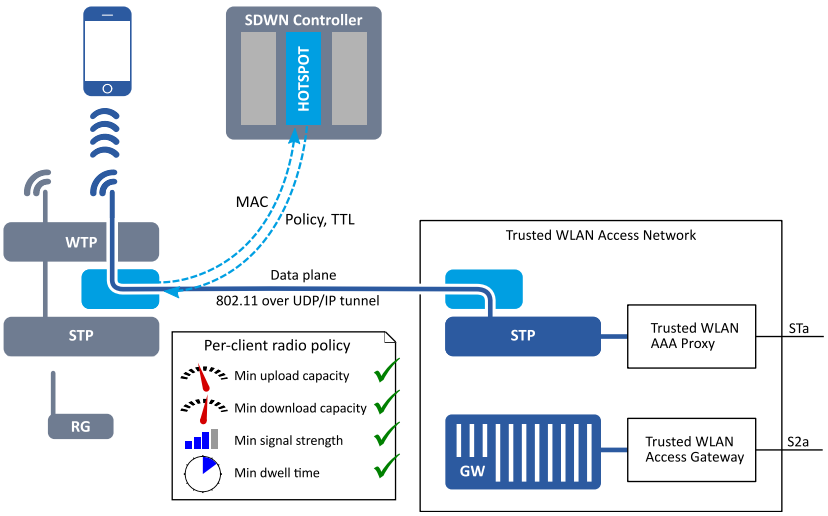
Another common mitigation approach is to statically limit the number of guest devices that can connect to a single gateway. But because quality of service correlates only weakly with the number of guest devices, this both prevents

sessions that would have been of acceptable quality and allows others that are of unacceptable quality. This approach also creates an unfortunate need to communicate the arbitrary limitation to the guest user ("too many guests connected — please try later"), something that cannot easily be implemented within existing standards.

In our architecture, the operator can configure so-called *radio policies* describing a minimum quality of service that must be met before a public network is presented to a device. A *radio policy* can, for instance, dictate that a certain network should only be presented if the bandwidth available to the device can be expected to surpass a certain level (in Mbps), and only if the device appears relatively stationary (i.e., its dwell time has exceeded a certain number of seconds).

FIGURE 4

*Radio policies* are configured into the Controller and distributed to visited access points through a lightweight DTLS/UDP/IP-based control plane protocol. Actual policy enforcement is implemented in *Anyfi.net software*, running on the visited access point itself.




Quality-of-service limits described in *radio policies* are enforced by *Anyfi.net software* running on the gateway, taking radio link quality, backhaul capacity, availability of spectrum and contention (with the primary home user as well as other guests) into account. The result is greatly improved average session quality, giving guests the most natural indicator of when quality cannot be met: The community Wi-Fi network simply will not be found.

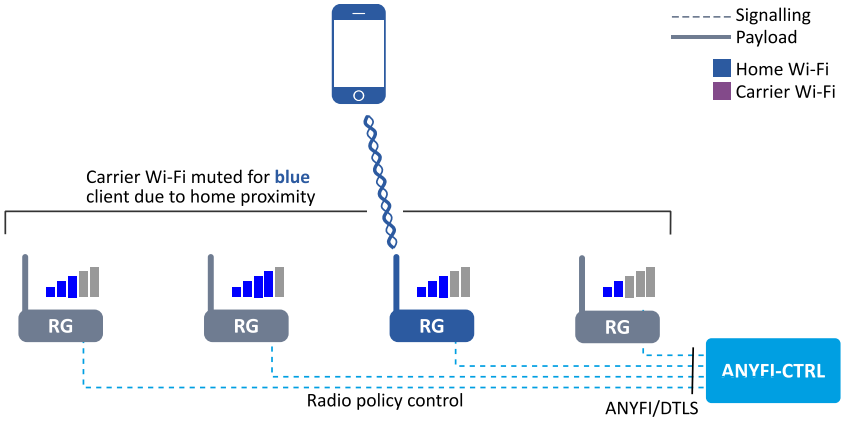
## Steering Home Users to Home Wi-Fi

Another problem is that if network selection is not managed in any way, then a fixed-line subscriber's mobile device may connect to the public "second SSID" even when that subscriber is in his or her own home. This results in subtle issues such as lack of local connectivity, higher latency and lower bandwidth. A less knowledgeable subscriber may not realize the cause of

such subtle problems, perhaps requiring assistance from customer support staff to resolve them (or simply assuming that this user experience is representative of the operator's fixed-line service).

Some operators attempt to mitigate this problem with custom modifications to the Wi-Fi subsystem in the gateway, e.g., blocking devices that have previously connected to the home Wi-Fi network from connecting to the community Wi-Fi signal of the same gateway. However, in areas with high subscriber density, a home user may then just as well connect to the community Wi-Fi signal coming from a neighbor's gateway.

FIGURE 5
The *radio policy* control built into *Anyfi.net software* is used to steer home users to home Wi-Fi.



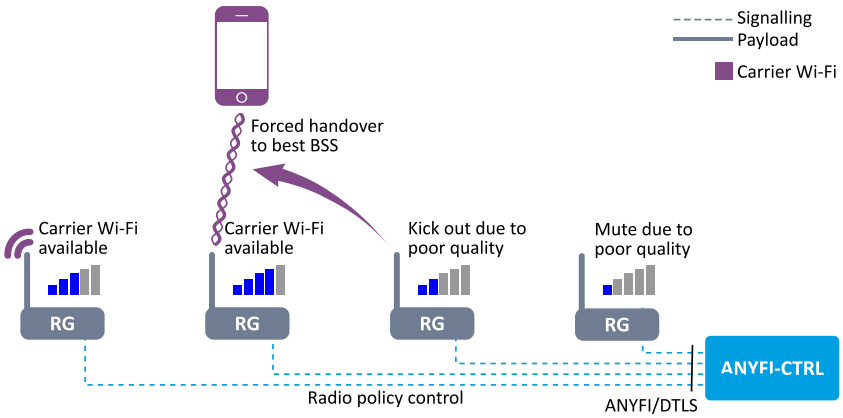

Solving this problem requires both radio management software on the gateway and coordination between gateways. In our architecture, the operator can configure so-called *alternate radio policies* to be applied in special cases, e.g., when the guest device is within radio range of its home network. The Controller detects such special cases by correlating information from multiple gateways, and distributes the appropriate *alternate radio policy* to the *Anyfi.net software* running in nearby gateways. Access to the community network can thus be suppressed in close proximity of the subscriber's own home.

## Infrastructure-Initiated Hand-Over

In the classic Soft-GRE architecture, there is no radio link-level coordination between access points, and access point selection is thus left entirely up to the mobile device. Unfortunately, many devices make poor choices under such circumstances, e.g., staying associated with a distant access point for too long, even after the radio link quality has fallen under acceptable levels and there are far better choices available.

FIGURE 6

The *radio policy* control built into *Anyfi.net software* can be used to solve the "device stickiness problem", by forcing devices to disassociate and scan for a better access point when quality of service falls below a predefined level.



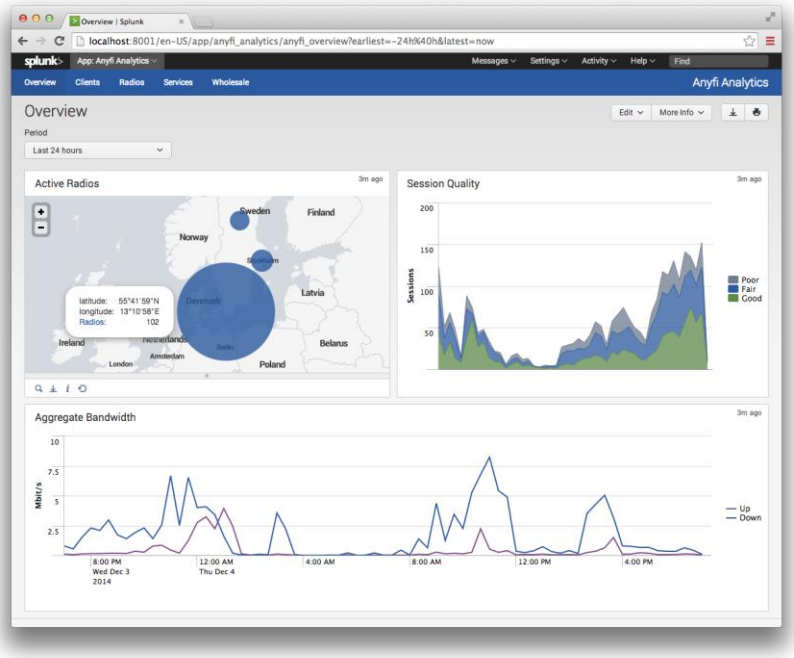

Solving this so-called "device stickiness problem" requires radio management software on the gateway. As we've outlined, our architecture allows the operator to (centrally) configure *radio policies*, ensuring that guest devices do not connect too early, before the radio link can support a reasonable quality of service. This *radio policy* can also dictate that guest devices be forcefully disassociated from the network (kicked out) if the quality of service later falls below the configured level. The guest device will then look for a new access point to associate with, and be gently steered toward good choices by the *radio policies* installed in other gateways.

## Quality of Service Monitoring

The classic Soft-GRE architecture offers very little insight into the quality of service delivered. Some operators attempt to address this with applications running on end-subscriber devices, but visibility is then limited to only those subscribers who have installed a particular app. It is also difficult to gain access to all relevant data (e.g., attainable bandwidth) on the device side without active testing.

FIGURE 7

The *radio link-level accounting* information collected by *Anyfi.net software* is aggregated in the Controller and can be further processed into dashboards and reports with a structured data analysis tool like Splunk.




In our architecture *Anyfi.net software*, running on the visited gateway, constantly collects per-session *radio link-level accounting* information. This includes aspects such as signal level in dBm, packet error rates and bandwidth consumed, but also more difficult to estimate aspects such as attainable bandwidth, i.e., the bandwidth that the guest device could have reached had it attempted to transfer a large amount of data.

Link-level accounting information is forwarded to the Controller then output in structured format on a SYSLOG interface — ideal for further processing into dashboards and reports with a structured data analysis tool such as Splunk.

Now, this is very different from traditional point-and-click Wi-Fi management solutions. In our architecture, everything is policy-controlled — only monitoring and reporting are graphical. This makes it feasible to scale the solution horizontally, well into the millions of access points.

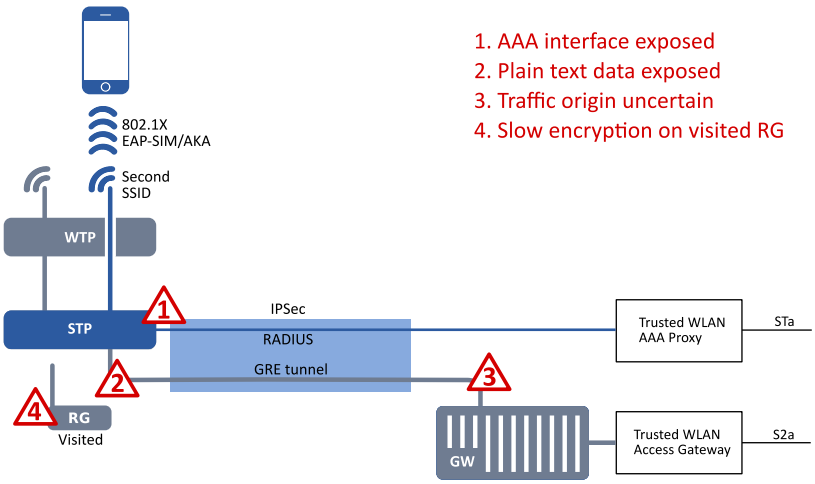
## Trustworthy End-to-End Security

Community Wi-Fi can be secured across the air interface, e.g., with WPA2 Enterprise and EAP authentication. In the classic Soft-GRE architecture, this encryption, however, terminates in the visited gateway, leaving clear-text data exposed inside the visited gateway itself and along the GRE tunnel to the operator's Wi-Fi core.

Some security-conscious operators mitigate this security problem by separately protecting the GRE tunnel, e.g., with IPSec. This, however, is quite costly in terms of performance because the user data plane traffic must be encrypted and decrypted on the visited gateway, often in software.

FIGURE 8

The classic Soft-GRE architecture has several security weaknesses. While IPSec on the backhaul offers some limited benefits, it cannot defend against an attacker in control of the visited access point. In other types of deployments, access points can often be physically protected to some extent, but for natural reasons this is impossible in community Wi-Fi networks.

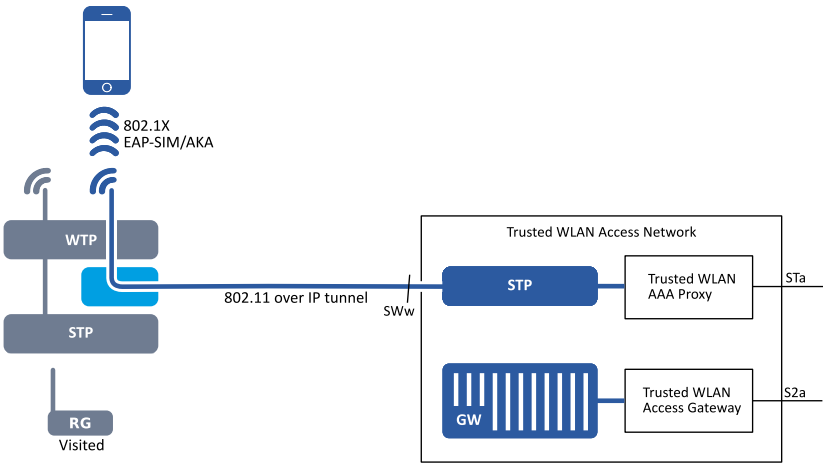



Complementing GRE with IPSec also does little to protect clear-text data (and other "secrets") in the RAM memory of the visited gateway itself. Accessing the RAM of a running residential gateway using only external tools may seem difficult but is, in fact, well within the reach of a skilled attacker [3].

There is also a counterintuitive but noteworthy drawback associated with securing the air interface in the Soft-GRE architecture: The RADIUS authentication interface must be exposed to residential gateways — perhaps millions of them. This risks breaking the mutual authentication property that all mobile network security rests on. If an attacker can access the RADIUS interface, then he or she can impersonate the network, and all the operator's subscribers become susceptible to man-in-the-middle (MITM) attacks. Hotspot 2.0 exacerbates this problem because gaining access to the RADIUS interface of one operator allows an attacker to impersonate all other operators within the same roaming consortium.

FIGURE 9

In our architecture, the air interface (3GPP SWw) security (WPA/WPA2/FT) is extended across the backhaul. The user data plane is thus encrypted end to end, leveraging hardware acceleration in both the mobile device and Gateway (Intel AES-NI or Cavium Octeon). This architecture ensures end-to-end confidentiality and integrity, with little or no impact on throughput.




In our architecture, on the other hand, the encryption is not terminated at the visited gateway. *Anyfi.net software* will instead forward the raw encrypted IEEE 802.11 frames across the backhaul, e.g., to a Gateway in the Wi-Fi core. Such forwarding does not require access to encryption keys, so even an attacker in complete control of the visited access point cannot eavesdrop on or modify guest communication. All security critical frame processing is performed in the Gateway, and the RADIUS authentication interface never has to extend beyond the operator's physically protected data center. This allows even the most security-conscious mobile operator to leverage inherently insecure access points as a trusted non-3GPP access.

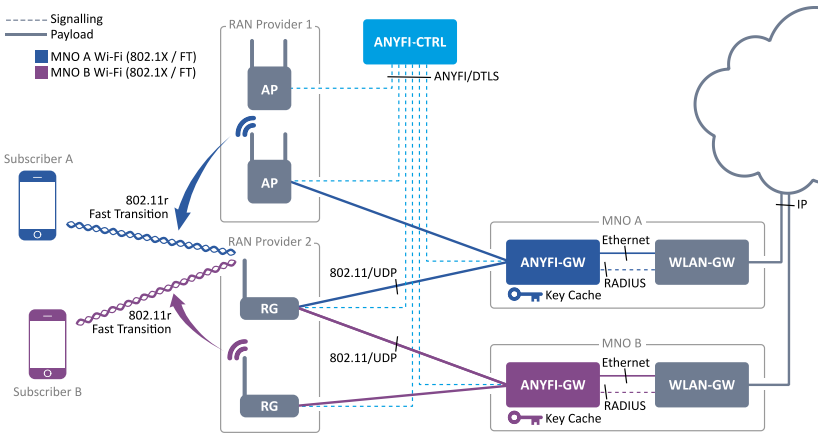
## Seamless Hand-Over With Key Caching

In the classic Soft-GRE architecture, each access point authenticates devices and derives encryption keys separately. This makes hand-over optimization with advanced key caching techniques such as Opportunistic Key Caching (OKC) and IEEE 802.11r Fast Transition difficult to implement.

In our architecture, IEEE 802.11 encryption keys are derived between a guest device and a Gateway in the Wi-Fi core, with the visited access point acting only as a remote radio head. The Controller will purposefully attempt to connect mobile devices to the same Gateway as they roam from access point to access point, thereby maximizing the effectiveness of key caching and reducing both hand-over delay and load on the AAA infrastructure. Both OKC and IEEE 802.11r Fast Transition are fully supported, even in combination with WPA2 Preauthentication and FT Over-the-DS.

FIGURE 10

In this example, two mobile operators leverage third-party Wi-Fi infrastructure for mobile offload. The confidentiality and integrity of subscriber data is cryptographically ensured, even against the radio access providers, while devices can still roam from access point to access point with IEEE 802.11r Fast Transition and/or OKC. Hand-over from a public access point operated by one entity to the guest access function of a residential gateway operated by another poses no particular problem.




Because the Gateway remains the termination point for the IEEE 802.11 protocol across the hand-over, it is also in a much better position to ease the transition, minimizing packet loss and ensuring a seamless user experience.

## Scalable Network Virtualization

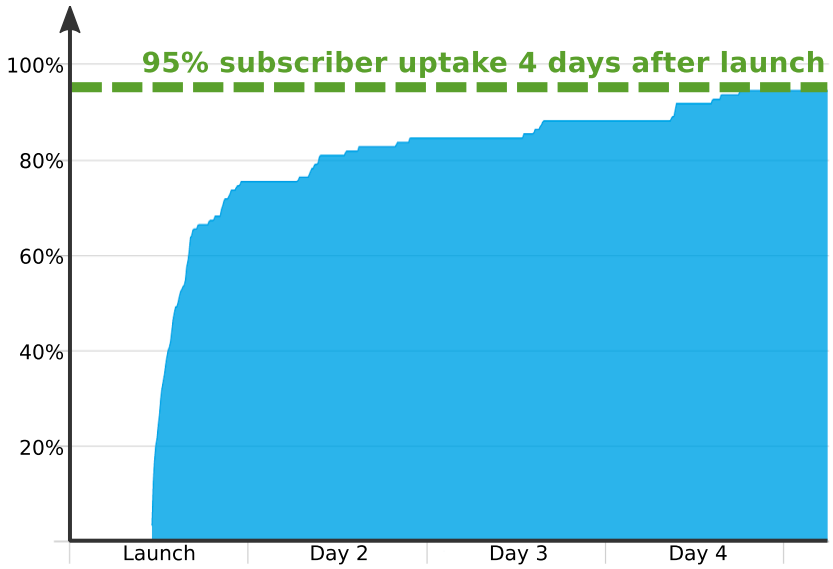
The business motives driving deployment of community Wi-Fi range from reducing fixed-line subscriber churn to offloading mobile data, improving indoor mobile coverage or even deriving entirely new revenue streams. In all cases, subscriber uptake is key: A community Wi-Fi solution is unlikely to drive down churn if nobody uses it.

In a typical Soft-GRE deployment, fixed-line subscribers connect to an open Wi-Fi network, are faced with a portal and need to register or sign in manually. In Western markets with well-developed 3G and 4G networks, only about 15%–20% of subscribers ever go through the trouble of doing so, even on a single device. The other 80%–85% simply are not reached.

Subscriber uptake can, however, be significantly improved if existing credentials are used for authentication, and devices can connect to the public network automatically, even the first time (zero sign-on). In this case you can expect well over 90% of subscribers to connect to the network, on multiple devices, multiple times a day.

FIGURE 11

This graph shows subscriber uptake of a home Wi-Fi anywhere service based on our SIMPLE solution. Of fixed-line subscriber households, 70% connected at least one mobile device to the community Wi-Fi **on launch day**. Four days after launch, 95% of fixed-line subscribers had connected at least one device. On average, each fixed-line subscriber household connected 3.3 mobile devices to the community Wi-Fi network within one week of launch, and the number of authenticated sessions was approximately 200 times as high as that of a comparable Soft-GRE network (not shown in the figure).




The classic Soft-GRE architecture can support such a zero sign-on user experience by using SIM authentication (optionally but not necessarily with Hotspot 2.0), but operators often hesitate to enable it due to the quality-of-service problems and the challenges we've discussed. Also, not all ISPs are mobile operators with SIM cards.

Release 2 of Hotspot 2.0 will partially reduce friction for non-SIM users by offering a standard way to provision credentials to mobile devices at the point of first connection. However, this will not provide a zero sign-on user experience — guest users will still need to manually register the first time they connect. It is also unclear when device support will be widespread enough to make this approach feasible in practice.

One of the strong points of SDN is its ability to provide scalable and robust network virtualization. This offers an interesting alternative to the distribution of new credentials: Simply make a network available that devices can connect to using existing credentials. We provide a complete solution (SIMPLE) based on this approach, making each subscriber's home Wi-Fi network available through every residential gateway or access point. The result is dramatically increased subscriber uptake, reduced churn and increased subscriber loyalty.

## Standard Interfaces

An important consideration when deploying a community Wi-Fi system is how easy it is to integrate with existing systems and infrastructure. In our

architecture, every component is carefully designed to fit into its surrounding environment using the standard interfaces of that particular domain. On the CPE side, the *Anyfi.net* software uses TR-069 for configuration and remote management. Our Gateway and Optimizer data plane components are designed to be connected to a standard WLAN gateway using RADIUS and Ethernet / VLAN / L2oGRE interfaces exactly like a regular access point. An operator can therefore reuse its existing infrastructure for AAA, IP address allocation, traceability and lawful intercept for the community Wi-Fi network.

FIGURE 12

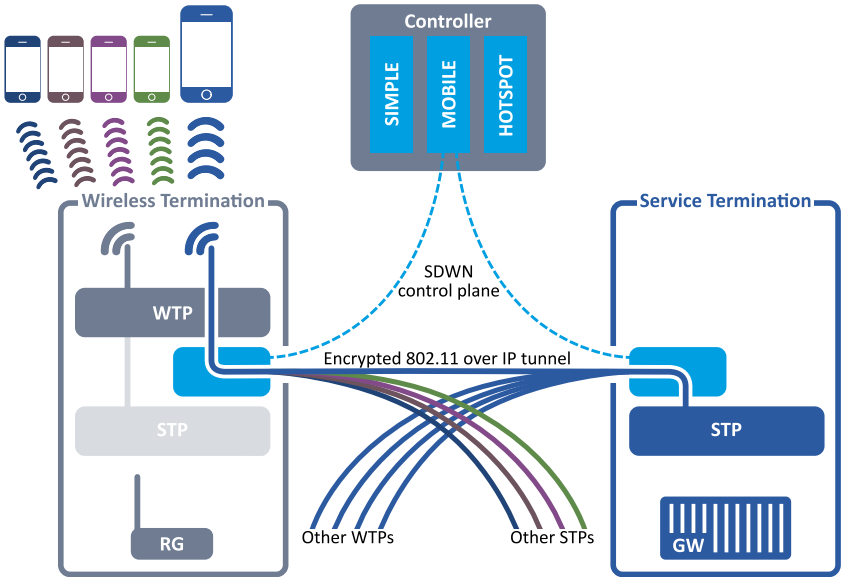
Every component in our Carrier Wi-Fi System provides standard interfaces to external systems to make integration with existing infrastructure as simple as possible. Even though the Gateway and Optimizer provides advanced functionality, they can be connected to a standard WLAN gateway just like a regular access point.

| | |
|---|---|
| **AIR INTERFACES** | |
| PHY | 802.11abgn (IEEE Std 802.11-2012) |
| Security | 802.11 RSN/WPA (IEEE Std 802.11i)<br>802.11 Fast Transition (IEEE Std 802.11r)<br>802.11 RSN Preauthentication (IEEE Std 802.11i)<br>802.11 PMKSA caching and Opportunistic Key Caching (OKC)<br>802.1X (IEEE Std 802.1X-2004)<br>EAP (RFC 3748) |
| **WIRED INTERFACES** | |
| Frame Format | Ethernet (IEEE Std 802.3) |
| Tunneling | VLAN (IEEE Std 802.1Q)<br>L2oGRE (RFC 1701, 2784) |
| **MANAGEMENT INTERFACES** | |
| CPE/APs | TR-069 (TR-069, TR-098, TR-181 Issue 2) |
| Core Products | SSHv2 (RFC 4250, 4251, 4252, 4253, 4254)<br>SNMP v2c (RFC 1901)<br>SYSLOG (RFC 5424) |
| **AUTHENTICATION INTERFACES** | |
| Methods | Pre-Shared Key (IEEE Std 802.11i)<br>EAP Pass-Through (RFC 3748) |
| Protocol | RADIUS Authentication (RFC 2865, 2869, 2548, 5247, 5080) |
| **AUTHORIZATION INTERFACES** | |
| Access Control | IP Filtering<br>HTTP Redirection<br>Bandwidth Limits<br>Dynamic VLANs |
| Protocol | RADIUS Authorization (RFC 2865, 2868, 4372 , 4849)<br>RADIUS Dynamic Authorization (RFC 5176)<br>RADIUS WISPr-Redirection-URL<br>RADIUS WISPr-Bandwidth-Max-Up/Down |
| **ACCOUNTING INTERFACES** | |
| Protocol | RADIUS Accounting (RFC 2866, 2869, 4372) |

# Architecture Overview

These key advantages and unique user experiences are achieved by partitioning the IEEE 802.11 stack into three parts: the *radio* that handles the low-level real-time aspects of the Wi-Fi protocol; a *service* that implements the higher layers of the stack; and a Controller that connects *radios* and *services* on demand. This makes it possible to assemble complete Wi-Fi stacks dynamically, depending on which *client* device happens to be within range of a particular *radio*.

FIGURE 13
Overview of our SDWN architecture, specifically designed for carrier Wi-Fi. Radio access (left) is clearly separated from service definition (right).




This architecture separates the control plane from the data plane, centralizing control plane decisions in the Controller, while the user data plane (and its security) remains distributed. In this way it is similar to other Software-Defined Networking (SDN) architectures of the overlay variety, e.g., Juniper's Contrail [4]. But we also introduce a second separation principle: the logical separation of *service* definition from *radio* access. We believe this should be the hallmark of a Software-Defined Wireless Networking (SDWN) architecture [5].

Below we give a brief introduction to the abstractions the architecture is built on.

## Client

A *client* is an abstract representation of a guest device. A *client* is identified by its MAC address (but typically authenticated using WPA, WPA2 or FT security mechanisms).

No additional *client* software is required for any of our solutions. Some solutions, however, require that *clients* be provisioned with a network profile before they can connect. Such provisioning is outside the scope of our solutions.

## Radio

A *radio* is an abstract representation of the IEEE 802.11 radio in an access point. A *radio* is identified by its hardware MAC address.

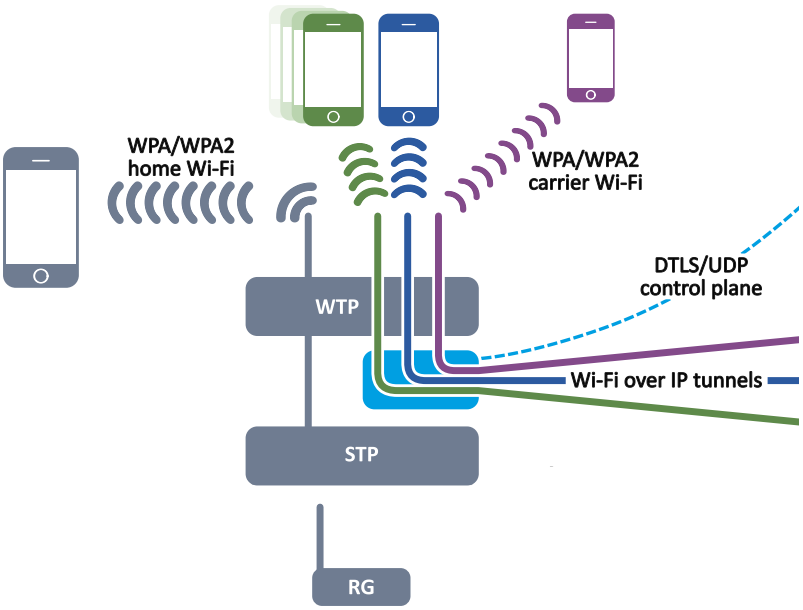
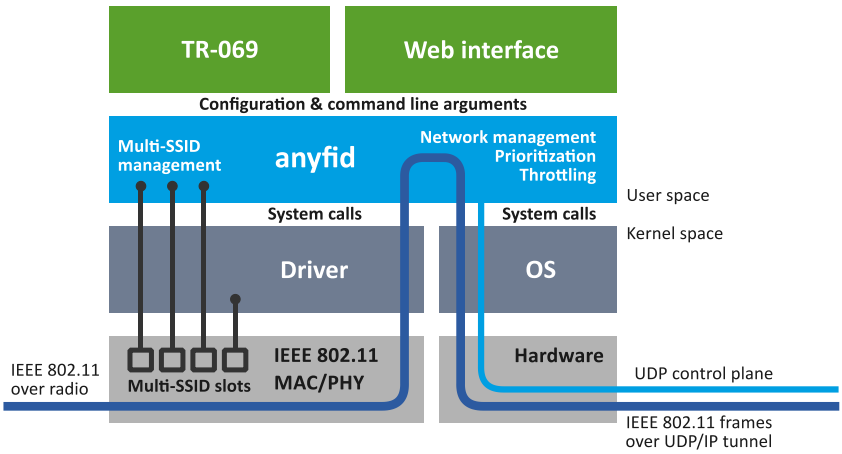



FIGURE 14
Overview of the *radio* management portion of *Anyfi.net software*, allowing the residential gateway to function as a *wireless termination point* (in addition to its normal function). Note that the software operates out of band with respect to the primary user (left). The DTLS-protected control plane connects the software to the Controller. Wi-Fi over IP tunnels carry (typically encrypted) IEEE 802.11 frames between *clients* and their trusted *services*.

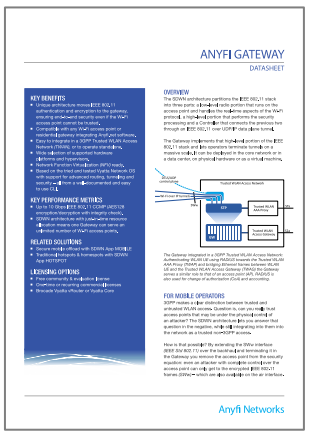
A *radio* typically serves a primary purpose outside the scope of our solution, e.g., it may provide home Wi-Fi for a fixed-line subscriber. We use only the spare capacity ("extra SSIDs", spare radio time and backhaul) of the *radio*, and we go to great lengths to ensure that we do not adversely affect its *primary function*.

We refer to an access point serving a *client* as the *wireless termination point (WTP)* for that particular *client*. It should be noted that this is a role that the access point plays in addition to its *primary function*.

FIGURE 15
Software architecture of a residential gateway integrating the *radio* daemon `anyfid`. This portion of the *Anyfi.net software* manages a pool of "extra SSIDs" used for guest access and can be enabled, disabled and configured through a Web interface and/or a TR-069 vendor extension.




Before the radios in an access point can be leveraged as a *radio* in our architecture, it must integrate *Anyfi.net software*. On a Linux-based residential gateway, this means running an instance of the user space daemon `anyfid`. The `anyfid` daemon manages a small set of "extra SSIDs", putting them under the control of the Controller for the purpose of serving *clients*.




**ANYFI GATEWAY**

The Gateway allows for central service definition and large-scale Wi-Fi over IP tunnel termination. It can be deployed as a virtual machine or on bare metal x86 hardware.

Related materials:

- Data Sheet
- Reference Guide
- Download

## Service

A *service* is an abstract representation of a Wi-Fi network, with properties such as an SSID; a set of security protocols (WPA, WPA2, FT) and associated cipher suites (TKIP, CCMP); and an authentication mechanism (PSK or EAP). Formally, all OSI Layer 3-7 processing can be seen as part of the service, including IP address assignment.

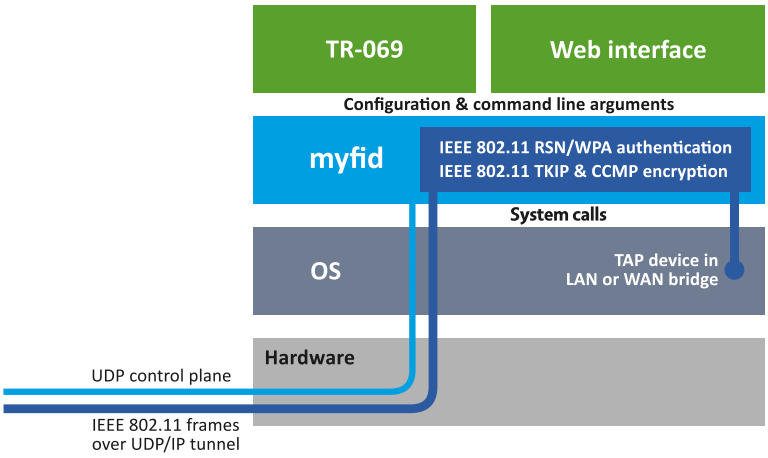
The SSID might seem like a natural identifier for a *service*, but within an SDWN architecture spanning millions of residential gateways, it may not necessarily be unique. We therefore identify a *service* by a Universally Unique Identifier (UUID) instead.

Just as a regular Wi-Fi network can have multiple access points, so too can a *service* have multiple *service termination points* (STPs). These are identified by an IP address and UDP port number where they are ready to receive IEEE 802.11 frames, coming in over the wired network instead of an air interface.

Before the Controller can provide *clients* with remote access to a Wi-Fi network, it must first be registered as a *service* with at least one *service termination point*. There are essentially two ways to accomplish this.

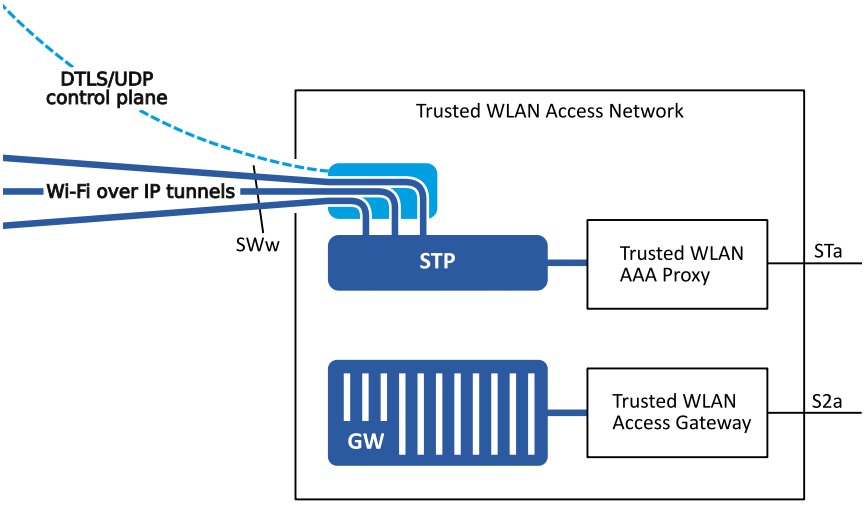
A regular Wi-Fi network such as a fixed-line subscriber's home Wi-Fi can be registered as a *service* by integrating *Anyfi.net software* in the gateway. On a Linux-based residential gateway, this means running an instance of the user space daemon `myfid`. The `myfid` daemon registers the local Wi-Fi network as a *service* in the Controller and serves as a *service termination point* for the same, without affecting the *primary function* of the gateway.

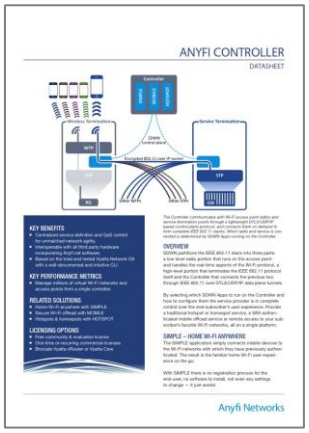
FIGURE 16
Software architecture of a residential gateway integrating the tunnel termination daemon `myfid`. This portion of the *Anyfi.net software* performs all security critical IEEE 802.11 frame processing and terminates the Wi-Fi over IP tunnels. The software can be enabled, disabled and configured through a Web interface and/or a TR-069 vendor extension.




Alternatively, an operator can use our Gateway product to terminate a large volume of Wi-Fi over IP tunnels in a Wi-Fi core. The desired Wi-Fi network settings (SSID, security, RADIUS servers, etc.) are then configured into one or several Gateways, which will register the corresponding *service* and *service termination points* in the Controller.

FIGURE 17
The Gateway is configured in much the same way as a Wi-Fi access point or WLAN controller. It will then register the corresponding service in the Controller and wait for inbound Wi-Fi over IP tunnels. When devices connect, they will be authenticated, e.g., through RADIUS, and their traffic bridged to an Ethernet interface for further (Layer 2-7) processing. The Gateway thus allows an operator to define a Wi-Fi service within the trusted and reliable environment of a data center, safe in the knowledge that radio access can be separately addressed later, using equipment from several different vendors.






**ANYFI CONTROLLER**

The Controller sets up Wi-Fi over IP tunnels between radios and services in much the same way as an overlay SDN controller. It can be deployed as a virtual machine or on bare metal x86 hardware.

Related materials:

- Data Sheet
- Reference Guide
- Download


**ANYFI OPTIMIZER**

The Optimizer enables central breakout of Internet-bound traffic with RADIUS authorization and accounting. It can be deployed as a virtual machine or on bare metal x86 hardware.

Related materials:

- Data Sheet
- Reference Guide
- Download

# Controller

The Controller connects *radios* and *services* on demand, forming complete IEEE 802.11 stacks that can serve nearby *clients*. It is also responsible for the distribution of *radio policies* and for aggregating *radio link-level accounting*. It communicates with other network elements through a lightweight DTLS-protected UDP/IP control plane protocol.

Which of the previously discussed user experiences will be realized depends almost entirely on the configuration of the Controller and the *control programs* running on it. We provide two built-in *control programs*.

The `hotspot` *control program* essentially makes a single *service* available through all (or a subset) of *radios*. This enables the traditional homespot user experience where guests connect to a separate operator-branded Wi-Fi network.

The `simple` *control program* instead makes a large number of *services* available specifically to *clients* who have previously connected to the corresponding local Wi-Fi networks. This enables the home Wi-Fi anywhere user experience, where every fixed-line subscriber can connect to his or her own home Wi-Fi network through every gateway.

Compared with the classic WLAN controller, our SDWN Controller is remarkably scalable. No user data plane communication ever passes through the Controller, and it is normally not even involved in authentication or key derivation. A single Controller running on a modern x86 rack mount server can easily scale to support millions of *radios* and *services*.

# Optimizer

The `simple` *control program* is often used to set up Wi-Fi over IP tunnels back to a visitor's own home gateway. Unfortunately, the wireless traffic must then traverse the visitor's home broadband connection twice, and be encrypted/decrypted on the home gateway (in software unless hardware AES acceleration is available). This will reduce throughput down to the upstream bandwidth of the home broadband connection, or the encryption throughput of the home gateway.

To avoid this, we have extended the architecture with a novel network element: the Optimizer. The Optimizer is automatically inserted into Wi-Fi over IP tunnels by the Controller. As soon as IEEE 802.11 authentication has been completed, the Optimizer receives an RSA-protected copy of the

temporal key (TK) from the *service termination point*. Using this encryption key, the Optimizer opens the Wi-Fi over IP tunnels and breaks out any Internet-bound traffic it finds.

# How to Get Started

In this chapter we show you how to quickly and easily get started with Software-Defined Community Wi-Fi using our free evaluation software and off-the-shelf commodity hardware.

To follow the steps below, you will need:

- commodity off-the-shelf Wi-Fi routers capable of running OpenWrt;
- an x86 64-bit system capable of running VMware ESXi or Oracle VM VirtualBox, to host the virtualized example Wi-Fi core; and
- one to five IP addresses, routable throughout your targeted coverage area (i.e., private addresses are fine for lab trials, but public addresses are needed for deployment in the field).

## Installing Anyfi.net Software in Access Points

*Anyfi.net software* has been designed to easily integrate into any Linux-based access point or residential gateway with a Wi-Fi chipset from Broadcom, Qualcomm Atheros, Ralink or Realtek. A production-quality integration on a typical target platform will, however, still require approximately two weeks of engineering time.

To make it easy to quickly get started with proof of concepts (PoCs) and small-scale trials, we have made our reference integration for OpenWrt publicly available [6]. This can be installed with only a few commands on just about any Wi-Fi router that runs OpenWrt Barrier Breaker or later. Step-by-step instructions are available at http://anyfi.net/openwrt/INSTALL.

## Choosing and Installing an Example Core

Our core products are delivered as virtual machines, built on the Vyatta Networking OS. This ensures a seamless migration to Network Function Virtualization (NFV) in the future, but also makes it easy to get started here and now.

We provide a number of example cores as starting points that can be downloaded at http://www.anyfinetworks.com/download, both in Open Virtual Appliance (OVA) format and as self-extracting archives of disk images and

provisioning scripts for automated provisioning on VMware ESXi or Oracle VM VirtualBox.

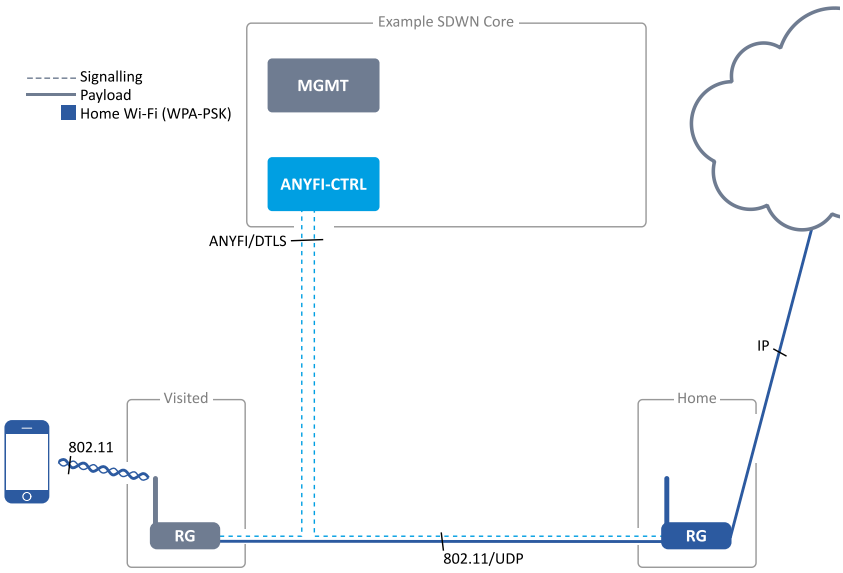
Each example core comes with a **Getting Started Guide**, providing detailed installation instructions and outlining the necessary basic configuration. By following the guide, you should have a working system up and running in about 30 minutes. Bundled with each core you will also find **Reference Guides** for each individual core product. These contain a complete command reference and discussion on more advanced and specialized configuration options.

## Seamless Home Wi-Fi on the Go Without Optimizer

This use-case is potentially the easiest to implement because the data plane remains entirely distributed The **Minimal Example Core** available for download from our website [7] is ideally suited for this use-case.

In this use-case, the Controller is configured to run the `simple` *control program*, which essentially provides remote access to the Wi-Fi networks that the client has in the past successfully authenticated.

FIGURE 18
The **Minimal Example Core** consists of just a Controller and a management machine. The latter can run Splunk to generate dashboards from radio-link level analytics and a TR-069 Automatic Configuration Server (ACS) to distribute and configure the *Anyfi.net software* in the residential gateways.




Since there is no Optimizer in this example core, the data plane will remain distributed, i.e., Wi-Fi over IP tunnels will carry encrypted *client* traffic from the visited access point to the home gateway, where it will be decrypted (with hardware acceleration if available). For a more advanced example with Optimizer, please see the **Advanced Example Core** introduced below.

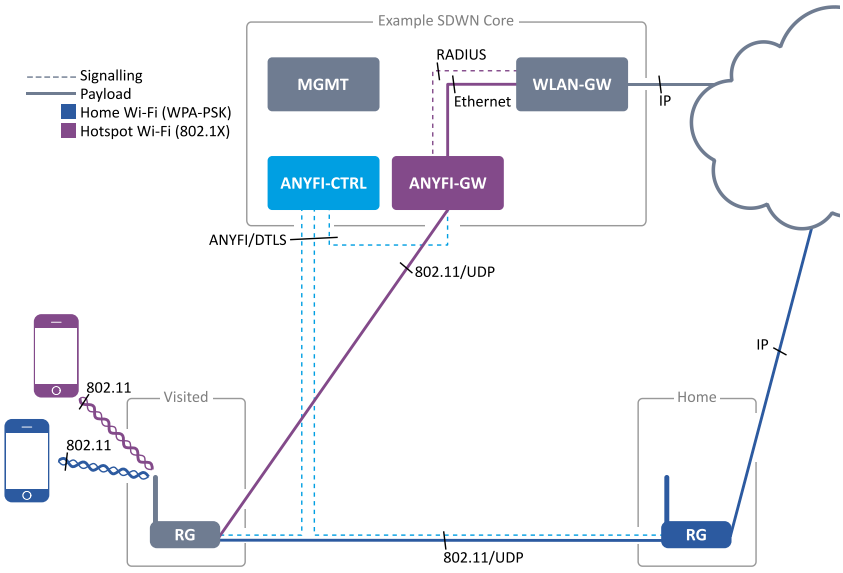
The **Getting Started Guide** for the **Minimal Example Core** will take you as far as a functional system. The Controller **Reference Guide** further details advanced topics such as configuring *radio* and *service* groups to restrict access to certain subscribers, *radio policies* to ensure quality of service on the go, and *alternate radio policies* steering *clients* to their own home gateway when within radio range.

## Traditional Homespots and Home Wi-Fi on the Go

One of the strengths of the SDWN architecture is that it allows solutions to be superimposed: Existing subscribers connect seamlessly and securely to their own home Wi-Fi networks while, e.g., mobile subscribers can connect to a centrally terminated operator-branded Wi-Fi network. The **Basic Example Core** available for download from our website [8] implements exactly this combined use case.

In this use case, the Controller is configured to run both the `simple` *control program* and the `hotspot` *control program*. The former will provide existing fixed-line subscribers with seamless and secure remote access to their own home Wi-Fi networks, while the latter will distribute an operator-branded traditional homespot network across all *radios* under management.

FIGURE 19
The **Basic Example Core** consists of a Controller, a Gateway, a WLAN gateway and a management machine. The latter two are not part of our product portfolio and would, in a production deployment, typically be replaced with third-party systems.




Since there is no Optimizer in this example core, the data plane will remain distributed for fixed-line subscribers, i.e., their Wi-Fi over IP tunnels will carry encrypted *client* traffic from their visited access points back to their home gateways. For a more advanced example with Optimizer, please see the **Advanced Example Core** introduced below.

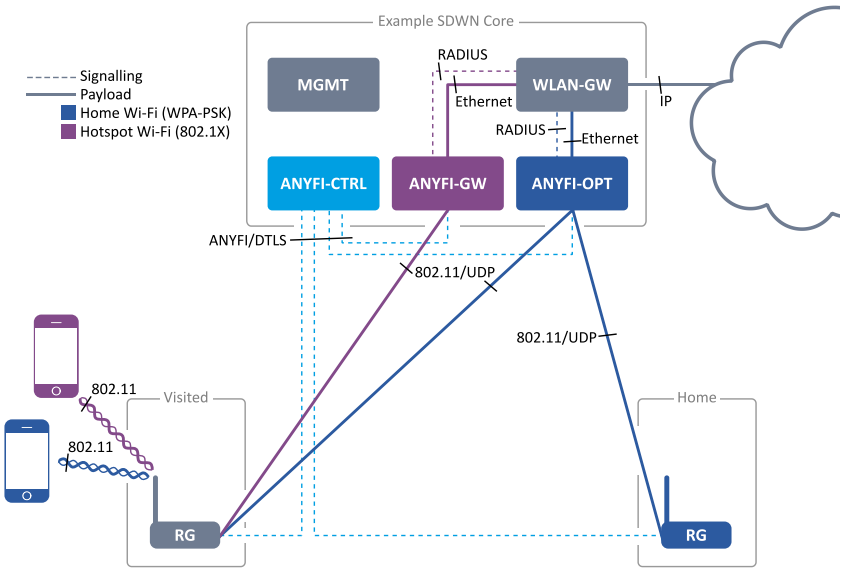
The **Getting Started Guide** for the **Basic Example Core** will take you as far as a functional system. The Controller **Reference Guide** further details advanced topics such as configuring *radio* and *service* groups to restrict distribution only to certain access points, *radio policies* to ensure quality of service on the go, and *alternate radio policies* steering *clients* to their own home gateway when within radio range. Turn to the Gateway **Reference Guide** to learn more about advanced configuration of the centrally terminated operator-branded Wi-Fi network: RADIUS authentication, authorization and accounting; bandwidth restrictions; dynamic VLAN assignment; WPA/WPA2 security settings; key caching and IEEE 802.11r Fast Transition; and similar.

## Advanced Example Core With Optimizer

The **Advanced Example Core** [9] contains all our core products: a Controller, a Gateway and an Optimizer. With this core, an operator can realize all the use cases and benefits detailed in this white paper, providing traditional homespots, secure mobile offload and seamless home Wi-Fi on the go.

In this example core, the Controller is configured to run both the `simple` *control program* and the `hotspot` *control program*. The former will provide existing fixed-line subscribers with seamless and secure remote access to their own home Wi-Fi networks (via an Optimizer), while the latter will distribute an operator-branded traditional homespot network across all *radios* under management.

FIGURE 20
The **Advanced Example Core** consists of a Controller, a Gateway, an Optimizer, a WLAN gateway and a management machine. The latter two are not part of our product portfolio and would, in a production deployment, typically be replaced with third-party systems.



In this example core, the data plane is centralized even for fixed-line subscribers: The Controller will automatically insert the Optimizer element into Wi-Fi over IP tunnels to ensure that Internet-bound traffic can be broken out and routed straight to the Internet. This avoids the unnecessary round-trip to the home gateway.

Notably, the Optimizer integrates into the Wi-Fi core on the same interfaces as the Gateway: Bridged Ethernet with DHCP address assignment and RADIUS for authorization and accounting. This allows the operator to use existing captive portal, lawful intercept and billing systems.

The **Getting Started Guide** for the **Advanced Example Core** will take you as far as a functional system. The Controller **Reference Guide** further details advanced topics such as configuring *radio* and *service* groups to restrict distribution only to certain access points, *radio policies* to ensure quality of service on the go, and *alternate radio policies* steering *clients* to their own home gateway when within radio range. Turn to the Gateway **Reference Guide** to learn more about advanced configuration of the centrally terminated operator-branded Wi-Fi network: RADIUS authentication, authorization and accounting; bandwidth restrictions; dynamic VLAN assignment; WPA/WPA2 security settings; key caching and IEEE 802.11r Fast Transition; and similar. Finally, the Optimizer **Reference Guide** details advanced configuration options related to the home Wi-Fi anywhere service: ensuring secure transfer of temporal keys (TKs) with RSA encryption; assigning breakout IP addresses with DHCP; and RADIUS for authorization and accounting.

# References


1 Tefficient: How Operators Use Wi-Fi to Strengthen Existing Business, December 2014. http://tefficient.com/how-operators-use-wi-fi-to-strengthen-existing-business/.

2 Wireless Broadband Alliance: Community Wi-Fi White Paper, September 2014. http://www.wballiance.com/resource-center/wba-white-papers/.

3 Scanlime - One Girl's Diary of Improvisational Engineering: DSi RAM Tracing, September 2009. http://scanlime.org/2009/09/dsi-ram-tracing/.

4 Juniper Networks: Contrail Open SDN NFV & Cloud Solutions. http://www.juniper.net/us/en/products-services/sdn/contrail/.

5 Anyfi Networks: Software-Defined Wireless Networking: Concepts, Principles and Motivations, May 2014. http://www.anyfinetworks.com/resources/anyfi-sdwn-concepts-whitepaper.

6 GitHub: OpenWrt feed for Anyfi.net software. https://github.com/anyfi/openwrt-anyfi.

7 Anyfi Networks: Minimal Example Core, Getting Started Guide and VM images. http://www.anyfinetworks.com/resources/anyfi-sdwn-core-minimal.

8 Anyfi Networks: Basic Example Core, Getting Started Guide and VM images. http://www.anyfinetworks.com/resources/anyfi-sdwn-core-basic.

9 Anyfi Networks: Advanced Example Core, Getting Started Guide and VM images. http://www.anyfinetworks.com/resources/anyfi-sdwn-core-advanced.