aptilo
an Enea company

CARRIER
WI-FI

WHITE PAPER

Wi-Fi in the 5G Era

Strategy Guide for Operators

APRIL
2021

WWW.APTILO.COM

Wi-Fi and 5G are perfectly complementary for delivery of mobility (5G) and high-capacity indoor coverage (Wi-Fi) - which is why the time for operators to embrace Wi-Fi as a strategic technology of choice is now.

But it can be a challenge to navigate in this rapidly changing landscape, both in terms of technology and business strategies. It occurred to us that operators lack a strategy guide for Wi-Fi in the 5G era. And so we decided to write one.

This is the world's first strategy guide for operators who know that they will be required to rethink and renew their Wi-Fi strategies to address the challenges of the next decade.

In this paper we dig into the business models and technical architectures that allow service providers to extract maximum value from vastly improved new Wi-Fi technology. We also zoom in on how new Wi-Fi technology will converge with 5G.

Navigation
The number of pages may appear daunting. But fear not - you can click on any section or on the table of contents on the next page to navigate to the individual sections. You can also speed up your reading by clicking on the summary symbols. And you can always get back to the table of contents again by clicking on the Aptilo logo at the top of each page.

To get more information on a subject, you may also click on the following symbols:

Click to get to a section in this document

Click to go to a web page

THE AUTHORS

Claus Hetting
CEO & Chairman Wi-Fi NOW
CEO HETTING Consulting

Jonas Björklund
CTO
Aptilo Networks

Johan Terve
VP Marketing
Aptilo Networks

1

Carrier Wi-Fi's role in 5G

- The challenges of profitable 5G
- Break organizational silos
- How Wi-Fi complements 5G

SUMMARY

2

Wi-Fi Technology Developments

- Wi-Fi 6
- Hotspot 2.0/Passpoint
- Captive Portal API
- Multipath TCP

SUMMARY

3

Wi-Fi Industry Initiatives

- WBA OpenRoaming™
- Google's Orion Wi-Fi
- Telecom Infra Project

SUMMARY

4

Carrier Wi-Fi Strategies

- How to build a carrier Wi-Fi footprint
- Wi-Fi monetization strategies

SUMMARY

5

Wi-Fi and 5G Convergence

- Opportunities today
- 5G and Wi-Fi integration
- Opportunities for the future with ATSSS

SUMMARY

6

Enea Solutions for Wi-Fi and 5G

- Aptilo Carrier Wi-Fi
- Aptilo IoT Connectivity
- Enea 5G solutions

SUMMARY

1

Wi-Fi and 5G are perfectly complementary for delivery of mobility (5G) and high-capacity indoor wireless services (Wi-Fi). The time for operators to embrace Wi-Fi in their strategies is now.

Carrier Wi-Fi's role in 5G

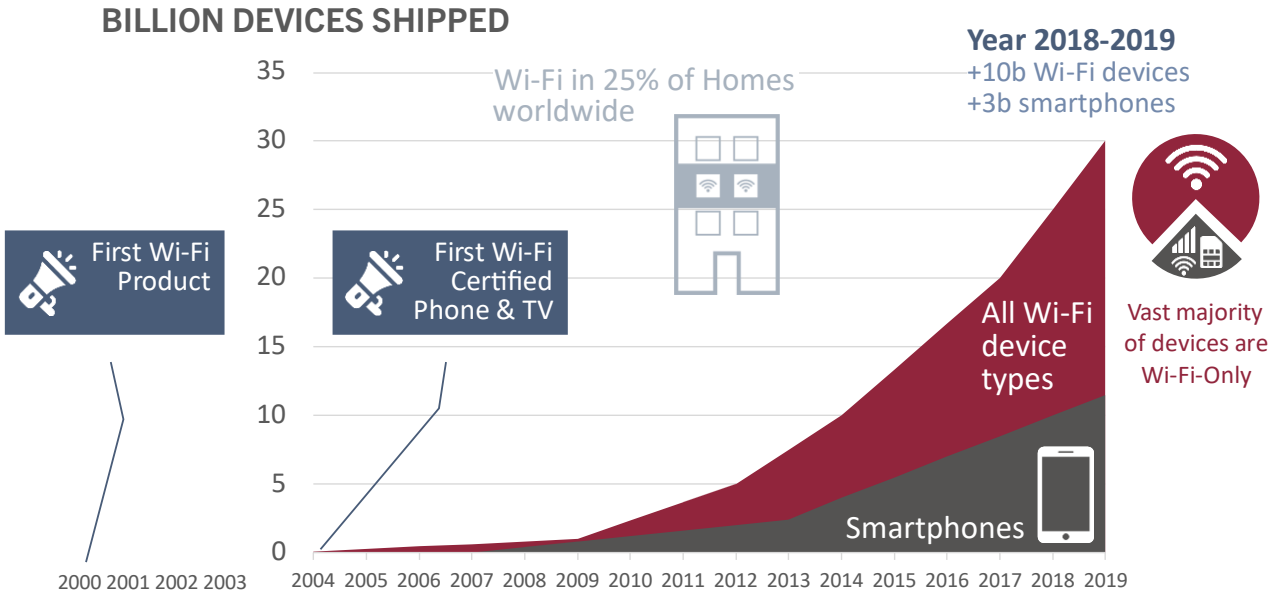
"Why Carrier Wi-Fi Is Even More Relevant in the 5G Era"

The challenges of profitable 5G

The world is firmly on the road to ubiquitous 5G networks and services - but how will service providers pull off investing in new networks while sustaining even modest growth rates and staying profitable under current market conditions? That is one of the mobile telecom industry's most pressing questions.

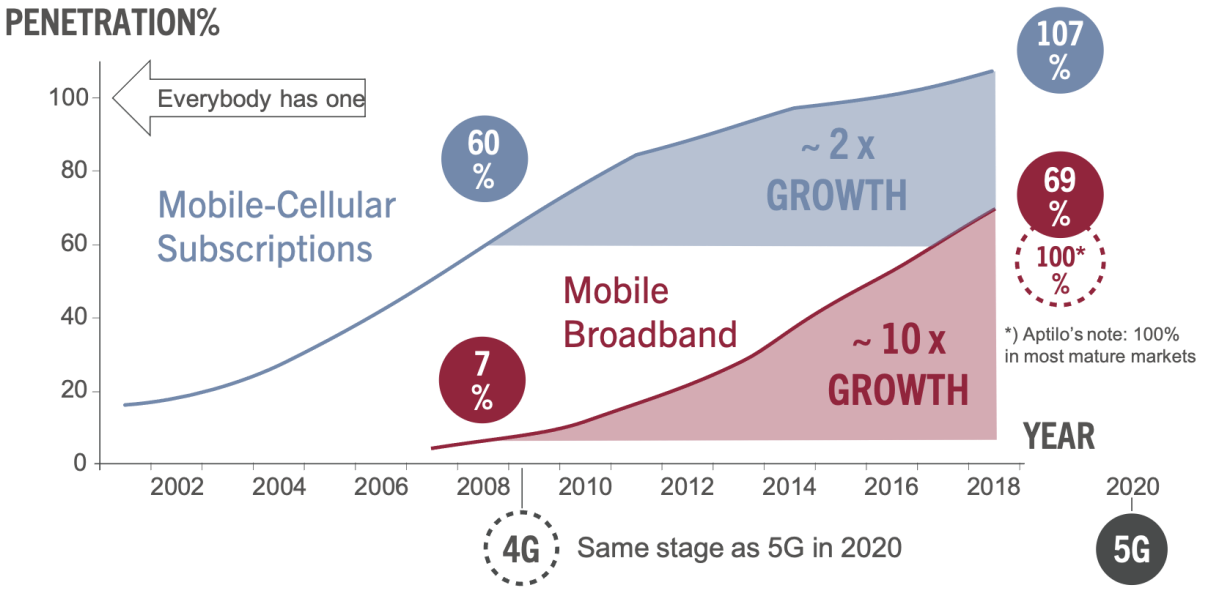
While the global 5G industry will be ramping up over the next many years to serve billions of IoT devices, private or public 5G networks for industry, self-driving cars, remote surgery, and more - the real challenge is what to do now to keep both current and future network costs as low as possible.

We believe one important component of profitable services in the 5G era is carrier Wi-Fi in all its forms.



In 2019 - 20 years after Wi-Fi technology was given its name - the 30 billionth Wi-Fi device shipped. When 4G launched in 2009, some people thought that Wi-Fi would be superseded by mobile technology. Now in the 5G era, people have become wiser. Strategy Analytics predicts that 17 billion Wi-Fi devices will be in use by 2030 - and that is only within homes.
Source : Wi-Fi Alliance

"4G had 2x growth in cellular services and 10x growth in mobile broadband to build ROI on. 5G will not have that luxury."



Global penetration of mobile-cellular telephone and mobile broadband subscriptions.
Source: ITU World Telecommunication / ICT indicators database.

When 4G was about at the same level of maturity as 5G is today - which was at around 2008 or so - global mobile broadband penetration stood at about 7%. Today, penetration stands at 69% globally with mature markets fully saturated.

Mobile operators who invested in 4G technologies had a lot to build their return-on-investment (ROI) on. They doubled the number of cellular subscriptions and mobile broadband traffic grew by a factor of ten. Now that everybody already has a subscription, what revenue sources will pay for 5G rollout? New 5G services of course, where IoT is one of the most promising opportunities.

But will it be enough?

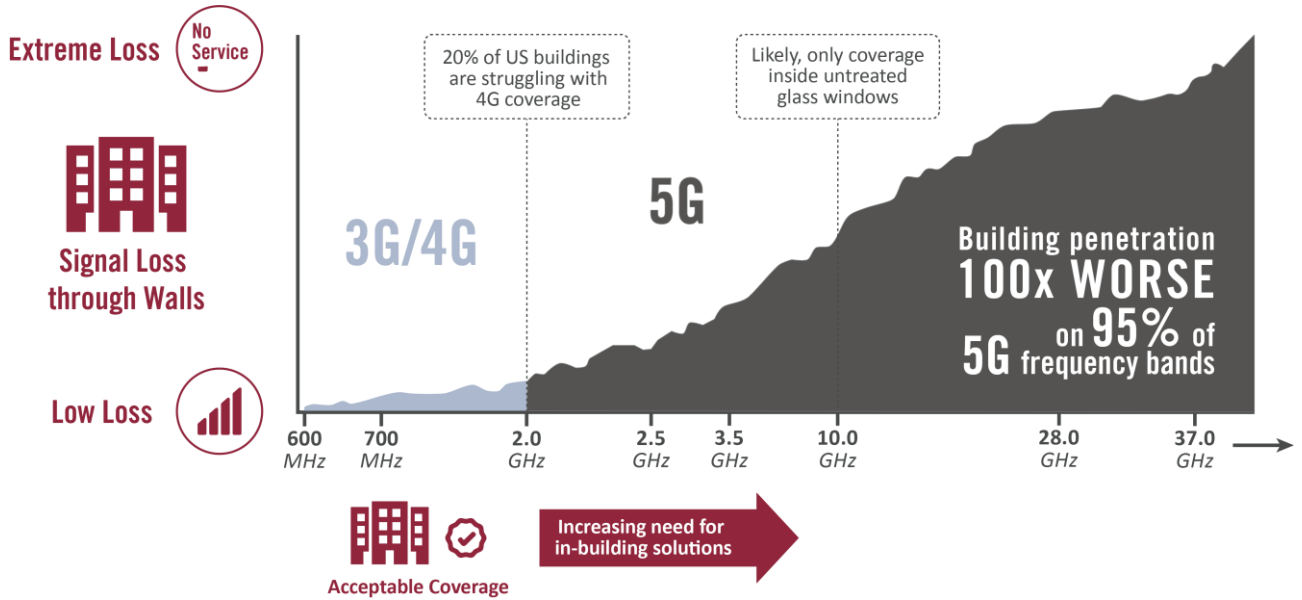
Mobile operators have every reason to begin looking for other cost-effective ways to deliver their services.

It also remains to be seen if mobile operators will be able to increase their Average Revenue Per Unit (ARPU) when 5G is deployed at scale. Many will probably see a flattening as opposed to declining ARPU trend as a major victory. At least initially, most consumers may not be in immediate need of higher data rates - and when they are, they are increasingly unlikely to accept paying more for faster services.

At the same time, consumers will continue expect unlimited data bundles and high service quality. Uncapped mobile broadband data bundles will fuel the need for operators to actively offload traffic to Wi-Fi. Back in the day when users had to pay for every megabyte of data, operators knew that users were desperately looking for Wi-Fi networks to connect to wherever they went. Once users were no longer connected to the operator's network, they were considered irrelevant and out of reach. In a world with unlimited cellular subscriptions - or practically unlimited with very high data volume allowances - operators can no longer take this passive approach.

This is the commercial reality facing mobile operators today.

Add to this the technical challenges that mobile operators face with 5G: Because most 5G services operate at relatively high radio frequencies, getting indoor coverage right by beaming in radio signals from the outside is a significant challenge. In the near field of an antenna (within 1-2 m) the so-called coupling loss reduces the signal by 75% (-6 dB) for every doubling of the frequency. In addition to simple path loss the signal will meet obstacles on its way and must finally penetrate the walls of the building itself.



One of the biggest 5G challenges is building sufficient indoor coverage. The chart above shows the increasing loss in signal as the cellular frequency increases. Building penetration is 100x worse than 3G/4G on 95% of the 5G frequency bands.
Source: Datapoints taken from Colin Berkshire, Talking Points Insider, April 2019.

The indoor coverage challenge already exists in the case of 4G. For example: 20% of buildings in the US are struggling with proper indoor coverage. The problem is exacerbated in the case of 5G because of the higher frequency bands involved. Initially 3.1-4.9 GHz is a commonly used frequency range but 5G will also employ the millimetre band above 30 GHz and at such frequencies, line of sight is required for signal reception. Already at the 5G frequency of 10 GHz the only indoor coverage option is to place your receiving device as close to an untreated pane of glass windowpane as possible. Energy-conserving glass used in many new buildings or other forms of treated glass panes will effectively attenuate the signal making indoor coverage more or less impossible.

Break organizational silos

"Make the most of your Wi-Fi assets"

As approximately 80 percent of wireless data traffic is consumed indoors, 5G will drive an unprecedented need for densification of base stations and indoor solutions. The only reasonable conclusion is that operators must use all technologies and spectra available to satisfy their subscribers' insatiable demand for data.

Aptilo believes that Wi-Fi is the perfect complement to 5G for indoor coverage. Wi-Fi is also an essentially untapped resource that many operators are working with already and thus have at their disposal. This is of course especially the case among operators whose current organizational structures are a result of mergers between fixed and mobile service providers.

Regretfully it is still often the case that staff responsible for fixed and mobile services continue to work in separate organizational departments or 'silos'. For example: While mobile teams deploy indoor cellular solutions at a venue such as a shopping mall, the fixed services team has already been to the same location to deploy Wi-Fi.

To win in a fiercely competitive market such disparate departments should instead come together with the single goal of delivering the absolute best subscriber experience using both technologies.

Parts of the mobile industry leadership has been skeptical towards adopting Wi-Fi as carrier-grade technology because it has been viewed as a best-effort service as a result of lack of scheduling mechanisms and the use of unlicensed spectrum.

Fortunately, Wi-Fi technology is right now evolving at such a rapid pace that we believe wireless connectivity in general is on the cusp of fundamental change - a paradigm shift. Soon the Wi-Fi quality shortcomings of the past will be firmly relegated to the history books.

Instead, Wi-Fi will - at least in the case of indoor connectivity - be leading the market in speed, capacity, latency, and overall quality by a wide margin.

How Wi-Fi complements 5G

"We believe that carrier Wi-Fi is the perfect complement to cellular in the 5G era principally for the following four reasons"

1. New Wi-Fi technology with the same scheduling capabilities as cellular and lots of new unlicensed spectrum provides a massive boost to Wi-Fi connectivity speed, capacity, and quality - and as always, Wi-Fi equipment is exceedingly cost efficient.

2. As discussed, most 5G operating frequencies penetrate poorly to the indoors and will need Wi-Fi as a complement to deliver seamless indoor coverage and capacity - and we know that 80% or more of the smartphone traffic is already now consumed indoors.

3. Wi-Fi is the dominant IoT technology by a wide margin with around 80% of all IoT devices connecting via short-range technologies such as Wi-Fi.

4. Carrier-grade service management solutions including seamless engagement/monetization methods and SIM or certificate-based Passpoint connectivity are mature, effective, and ready to be adopted by MNOs and ISPs everywhere.

At Aptilo Networks we never understood why there would ever be a conflict nor any real competition between Wi-Fi and 5G. On the contrary, the two technologies complement each other perfectly: One is for mobility and wide area coverage (5G), the other for high-performance and high-capacity connectivity indoors (Wi-Fi). And we cannot think of a single reason why operators should not use all the tools at their disposal to maximize profitability.

In October 2020, Aptilo was acquired by Enea, one of the world's leading suppliers of innovative software for telecommunication and cybersecurity. Enea is now one of the very few vendors in the world offering solutions both within the Wi-Fi and 5G domain.

Learn more in the last chapter about how we help service providers to create innovative services and cut cost in their operations.

SUMMARY

Why Carrier Wi-Fi Is Even More Relevant in the 5G Era

- **The time for operators to embrace Wi-Fi as a strategy is now.**
  - Wi-Fi and 5G are perfectly complementary for delivery of mobility (5G) and high-capacity indoor wireless services (Wi-Fi).
- **5G will not have the luxury of experiencing subscriber growth of 4G**
  - 4G experienced 2x growth in cellular services and 10x growth in mobile broadband on which to build ROI.
  - According to ITU the penetration of mobile broadband is 69% globally – we believe it is 100% in most mature markets.
- **Penetration through buildings is 100x worse on 95% of 5G frequency bands**
  - Already today – at cellular frequencies of around 2 GHz - 20% of US buildings are struggling with 4G indoor coverage.
  - At cellular frequencies of 10 GHz you will likely only achieve coverage in close proximity to untreated windowpanes.
- **80% of wireless data traffic is consumed indoors**
  - 5G will drive an unprecedented need for base station densification and indoor solutions. Why not use Wi-Fi?
- **Vast majority of devices are only Wi-Fi-capable**
  - In 2019 - 20 years after Wi-Fi technology was given its name - the 30 billionth Wi-Fi device was shipped.
  - Strategy Analytics predicts that 17 billion Wi-Fi devices will be in use by 2030 - and that is only within homes.
- **Operators must break organizational silos between cellular and fixed**
  - Mergers between fixed and mobile service providers means many operators own Wi-Fi as an underutilized asset
  - The fixed side can many times offer indoor coverage through their B2B Wi-Fi services at attractive venues.
  - New Wi-Fi technology (Wi-Fi 6) has the same scheduling capabilities as cellular and lots of new unlicensed spectrum.

2

Wi-Fi Technology Developments

The confluence of a new Wi-Fi 6 standard and huge amounts of new 6 GHz spectrum has created unprecedented opportunities for Wi-Fi service providers. The Passpoint standard has finally approached the tipping point to a mass market and Multipath TCP is next.

"These game-changing opportunities are available starting today"

Wi-Fi 6

During the past couple of years, the Wi-Fi industry has been blessed with a series of extraordinary developments. Firstly, a new and vastly improved Wi-Fi standard (Wi-Fi 6) has been introduced into the world. Secondly - and perhaps even more importantly - a large or, depending on country, very large swath of new spectrum has been allocated to unlicensed use. Each on its own such developments would likely produce surges in growth and innovation, as well as torrents of new business opportunities. But the timely confluence of the two leads us to believe that the next few years will be characterized by an even more radical transformation: Something akin to a paradigm shift in connectivity.

A paradigm shift in connectivity

This means that Wi-Fi performance - including capacities, data rates, latency, and more - as well as Wi-Fi's ubiquity and already broad applicability are likely to expand by orders of magnitude. Wi-Fi has in the course of the past twenty years grown to dominate the indoor wireless space regardless of whether you measure market presence by traffic volumes, numbers of devices, or number of coverage locations.

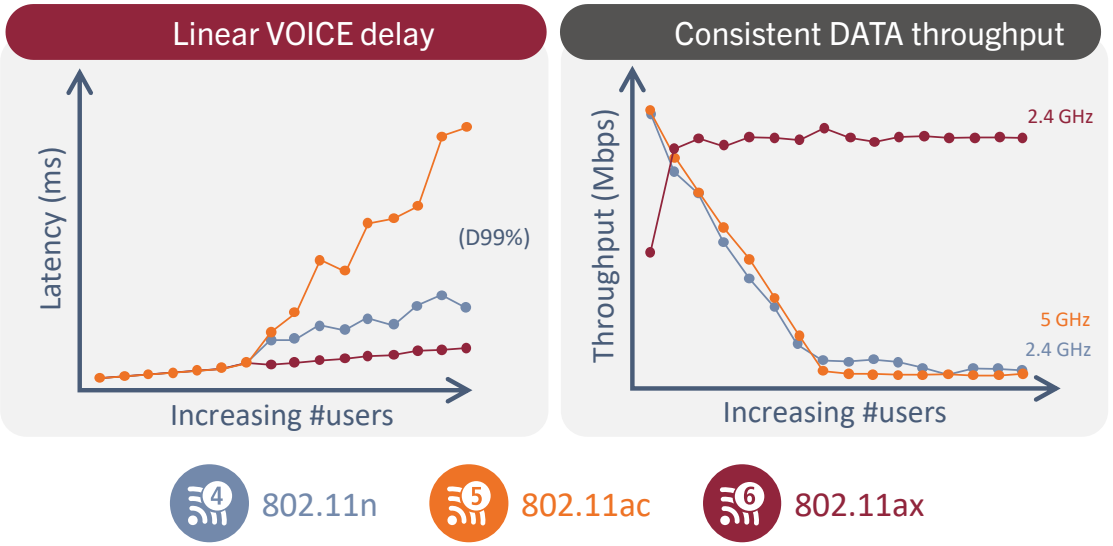
The coming decade will see an unprecedented expansion of Wi-Fi's dominant position as well as a slew of new applications. Both will be driven by an abundance of new spectrum as well as powerful - and highly affordable - new Wi-Fi technology.

A new kind of performance boost: Wi-Fi 6

For the first time in wireless technology history Wi-Fi will be capable of delivering a quality of service on par with that of cellular networks.

Wi-Fi 6 is the newest generation of certified Wi-Fi™ technology. Wi-Fi 6 is by a wide margin the most comprehensive and expansive reengineering of a Wi-Fi standard ever. In fact, Wi-Fi 6 comprises so many new features and performance boost that we have thus far only scraped the surface of what this new connectivity standard in time could bring to market in terms of innovative new use cases and improvements on existing applications.

Perhaps the most important Wi-Fi 6 feature is Orthogonal Frequency Division Multiple Access (OFDMA), which includes cellular-style scheduling. What in the past has been somewhat of an Achille's Heel for Wi-Fi - meaning the rapid deterioration of data rates and latency as the number of connected devices increases - will soon be a thing of the past. OFDMA and scheduling brings deterministic performance to Wi-Fi for the first time, which means that Wi-Fi services (for example those provided by ISPs) can be designed and deployed to comply with SLAs.



Wi-Fi 6 (802.11ax) delivers a consistent and linear voice delay when the number of users increase, making it ideal for applications such as voice over Wi-Fi, real-time video conferencing, and more. While data rates of previous Wi-Fi standards quickly deteriorate as a function of number of users or devices, Wi-Fi 6 delivers consistent data throughput. **Source: Cisco.**

Wi-Fi 6

- OFDMA
- 160 MHz Channels
- 1024QAM modulation
- Up to 4x faster uploads
- Up to 6x faster downloads
- Up to 4x better coverage
- Up to 6x better battery life

OFDMA also offers multiple other benefits: Wi-Fi 6 Access Points can serve many more devices and delivers up to four times the data transmission capacity of previous generation systems. Another benefit is the ability of Wi-Fi 6 to extend the range of Wi-Fi services at low data rates rendering it very useful for IoT.

Wi-Fi 6 comprises a long list of other valuable features and functions including UL (uplink) MU-MIMO, 160 MHz channels,1024QAM modulation, and more. Altogether the Wi-Fi 6 standard is designed to deliver a giant leap forward in high-density connectivity performance and not least in performance quality. This means Wi-Fi service providers will be able to deliver a vastly improved Quality of Experience (QoE) to consumers and professional users at venues such as transportation hubs, stadiums, and malls as well as for the 'carpeted enterprise', hospitality, and MDUs.

In short: Everywhere where there are people congregating, Wi-Fi will be there - and Wi-Fi 6 will make the service much, much better.

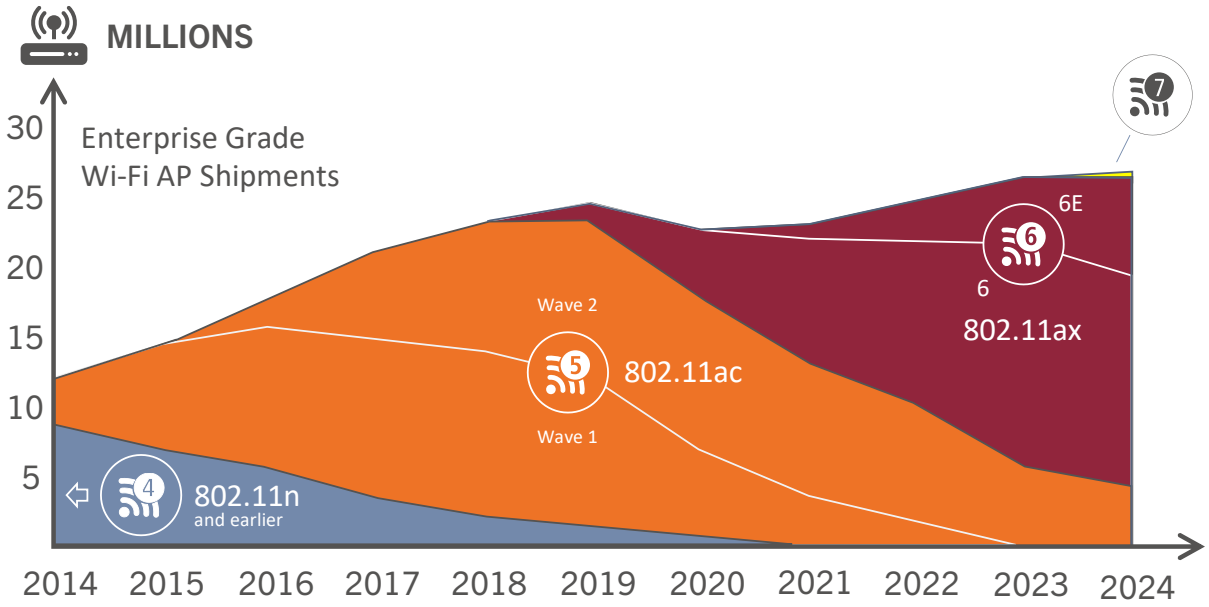
Last but not least: There is no doubt that Wi-Fi 6 will also deliver enormous value within the home and - for example - for industrial applications.

New spectrum & Wi-Fi in the 6 GHz band (Wi-Fi 6E)

Pristine 6 GHz spectrum will boost Wi-Fi speeds by at least a factor of four and capacities by even more with latencies as low as 2 milliseconds. This constitutes a paradigm shift in connectivity.

Wi-Fi 6 is in itself a big quality and data rate improvement over existing Wi-Fi services, most of which currently are still based on the Wi-Fi 5 (802.11ac, 5 GHz services) or even Wi-Fi 4 (802.11n, 2.4 GHz) legacy standards. Now add to this Wi-Fi 6E, an opportunity for the new standard to operate in the pristine 6 GHz band. The connectivity experience will improve by an order of magnitude in speed and quality.

It is also well documented that the rate of market penetration and rollout of both devices and access points supporting the Wi-Fi 6 standard has thus far well exceeded the pace of all previous standards. Within a couple of years, industry analysts expect the vast majority of enterprise-grade Wi-Fi access points to be Wi-Fi 6 capable.



The rate of Wi-Fi 6 market penetration will be very fast, as evidenced by the curve above. By 2023 analysts expect the vast majority of enterprise-grade access points to be Wi-Fi 6-capable.
Source: 650 Group.

Wi-Fi on 6 GHz triples available band

The 6 GHz Wi-Fi story is recent - and the date April 23, 2020, will be forever etched into the annals of wireless and technology history. On this date the commissioners of US telecom regulator FCC (Federal Communications Commission) voted unanimously five to zero in favor of releasing 1.2 GHz of pristine 6 GHz spectrum to Wi-Fi.

Since then, several other countries have followed suit. It is largely expected that most countries in the world will release some parts of the 6 GHz band as unlicensed spectrum in the course of the next few years. In the US the full 6 GHz band (including a section of band extending into 7 GHz) can already be used for indoor Wi-Fi services (for so-called Low Power Indoor or LPI services).

The huge new band allocation more than triples available Wi-Fi band in the US and will close to double available bands within the EU. In the US a total of seven 160 MHz-wide Wi-Fi channels will be available, while in Europe that number will be three (see the channel allocation table below). This means that Wi-Fi devices - including smartphones, tablets, laptops, etc. - will soon be operating at multiple gigabits per second of speed over Wi-Fi.

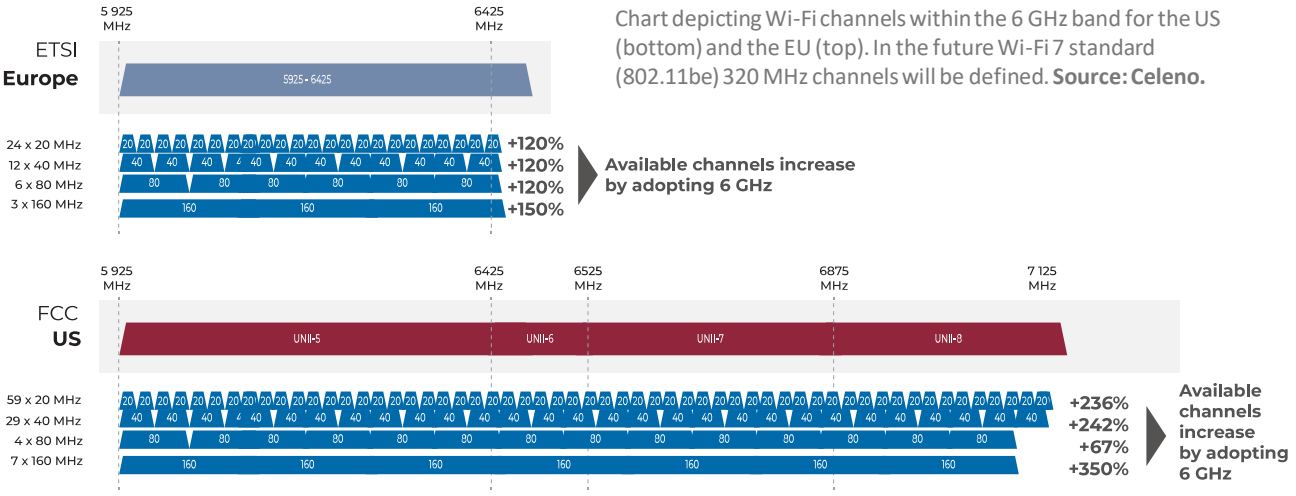


Chart depicting Wi-Fi channels within the 6 GHz band for the US (bottom) and the EU (top). In the future Wi-Fi 7 standard (802.11be) 320 MHz channels will be defined. **Source: Celeno.**

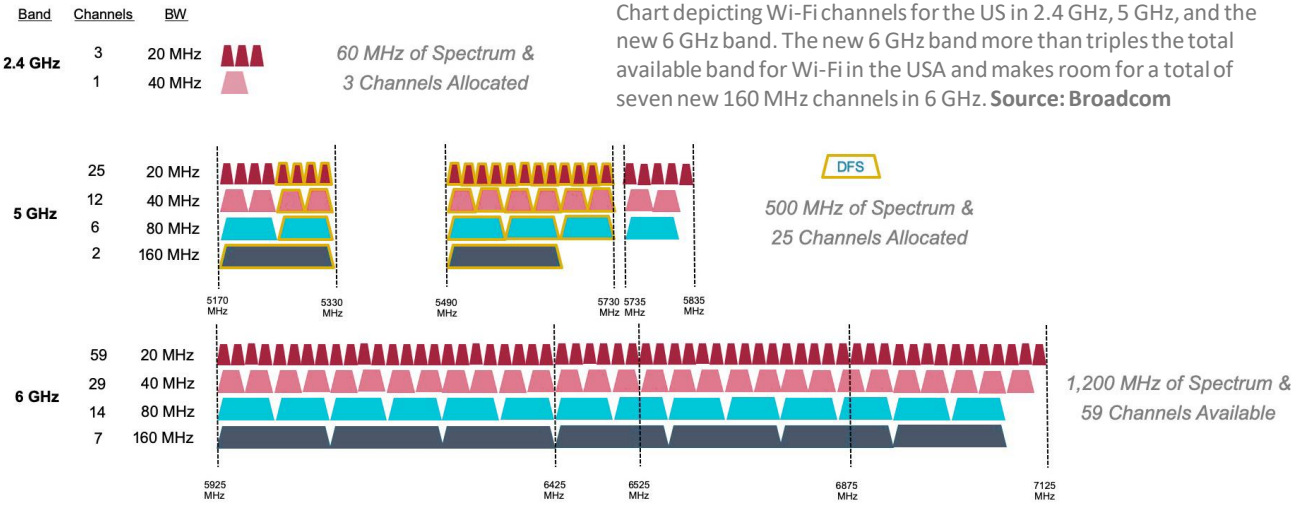


Chart depicting Wi-Fi channels for the US in 2.4 GHz, 5 GHz, and the new 6 GHz band. The new 6 GHz band more than triples the total available band for Wi-Fi in the USA and makes room for a total of seven new 160 MHz channels in 6 GHz. **Source: Broadcom**

One important aspect of Wi-Fi 6 in the 6 GHz band - dubbed Wi-Fi 6E by the Wi-Fi Alliance - is that only Wi-Fi 6E is certified to operate in the said spectrum and hence no legacy Wi-Fi systems will be around to generate interference within the new band. The quality of 6 GHz Wi-Fi services will therefore likely be close to that of cellular - except several multiples faster than most current wide-area coverage 5G data rates (with the exception of localized and outdoor mmWave-based 5G)[1].

The interference-free 160 MHz channels in Wi-Fi 6E means that smartphones and other mobile devices will be able to operate at peak theoretical speeds of more than 2 Gbps or - says chipset maker Broadcom - up to 1.4 Gbps at a distance of 7 meters non-line-of-sight from a Wi-Fi 6E access point.

In new enterprise deployments the adage 'eighty is the new twenty' will apply for Wi-Fi 6E: Standard 6 GHz Wi-Fi deployments will use 80 MHz channels instead of the usual 20 MHz channels applied today. This is because permitted power levels (in the US) are defined in such a way that there is no penalty for using wider channels and hence no real reason not to use them. As a result, average enterprise Wi-Fi data rates will be at least quadrupled.

Wi-Fi 6E technology will in addition deliver latencies as low as 2 milliseconds, which - as a starting point - will enable much more responsive and 'immersive' connectivity experiences, initially for gaming, fast video conferencing, AR/VR, and more and eventually for innovative new wireless enterprise applications.

In summary: Based on 480 MHz to 1200 MHz of new unlicensed (free) spectrum, Wi-Fi 6E will, depending on country-specific regulations, deliver multi-gigabit Wi-Fi speeds and capacities that by a wide margin will outperform current cellular systems indoors. And now - for the first time in Wi-Fi history - the application of Wi-Fi 6 and 6E technology using OFDMA, means the quality of Wi-Fi services will be similar to that of cellular.

6 GHz Wi-Fi by Country

Status as of April 2021	Used in 6 GHz band		Used for	
	500 MHz	1.2 GHz	ILP	VLP
USA		Full	●	
Brazil		Full	●	●
UK	Lower		●	
South Korea		Full	●	
Chile		Full	●	
UAE	Lower		●	
Saudi Arabia		Full	●	
EU states	Q2 2021		●	●

ILP = Indoor Low Power
VLP=Very Low Power

[1] Current 5G data rates are somewhat of a mixed bag of numbers depending on disparate frequency allocations across countries and continents. In the US wide-area and lower band 5G data rates typically range from 50-60 Mbps while millimeter wave 5G by Verizon delivers up to 500 Mbps but only over a very limited area (as reported by OpenSignal, June 2020). The millimeter wave 5G signal will generally not penetrate to the indoors. In other countries – such as Korea – up to 350 Mbps of 5G speed have been reported. Wi-Fi 6E peak data rates for smartphones are expected to exceed 2 Gbps with typical speeds reaching more than 1 Gbps even under non-line-of-sight conditions within the home.

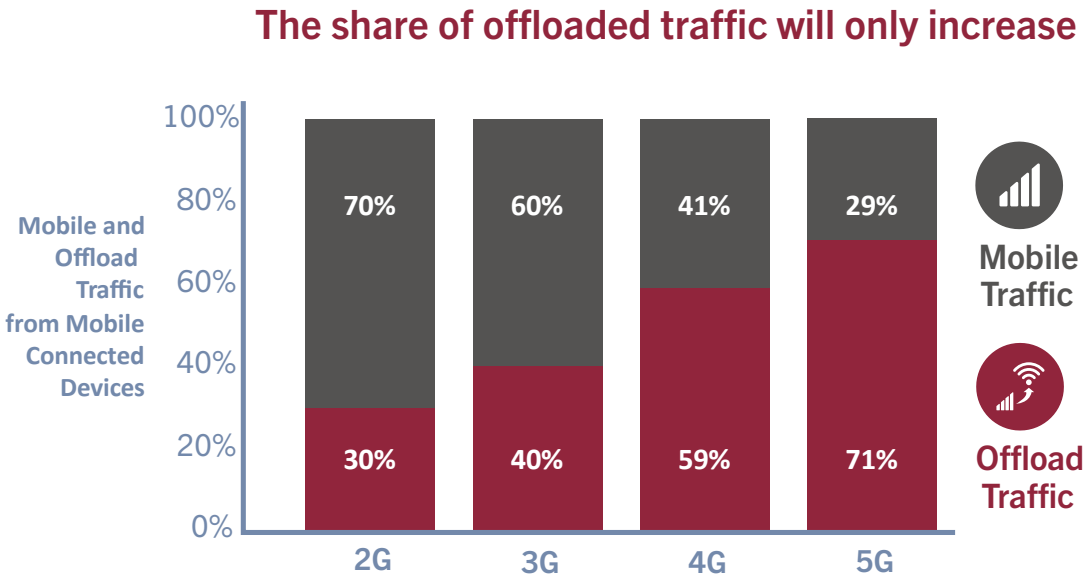
The rationale & market need for Wi-Fi 6 & Wi-Fi 6E

Rapid evolution and availability of new technology and new spectrum is making carrier Wi-Fi inevitable as a strategic technology of choice for service providers everywhere.

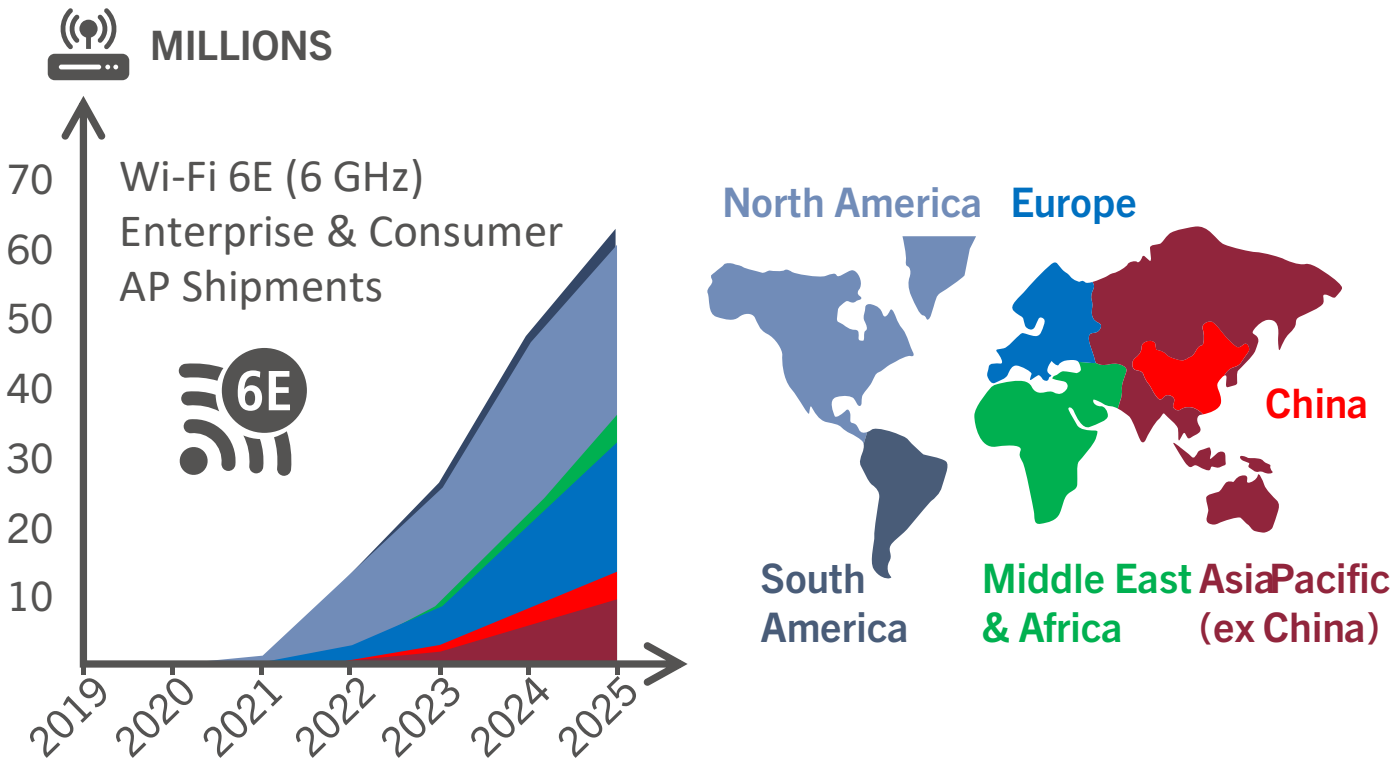
The idea that Wi-Fi is the dominant indoor wireless technology is not new. But we believe that Wi-Fi's dominance will be even more pronounced in the 5G era.

It is well known that device data consumption continues to rise particularly as the result of the increased popular demand for video streaming and - more recently perhaps - the explosive demand for collaborative work applications, such as video conferencing. More than this, research suggest (see figure) that the need for mobile networks to 'offload' traffic to Wi-Fi will substantially increase in the 5G era.

In some countries - such as the UK, Japan, and Germany – 'Wi-Fi offload' percentages (meaning the percentage of smartphone traffic delivered over Wi-Fi networks of any kind) are already well above 80%. In connection with the US decision to allocate all of the 6 GHz band to Wi-Fi, the FCC cited the need for offload from 5G networks as an important contributing factor in their decision.



The increasing percentage of traffic 'offloaded' from mobile networks to Wi-Fi networks as a function of the cellular generation. **Source: Cisco.**



Most analysts believe Wi-Fi 6 and Wi-Fi 6E technology will be ramped up quickly and indeed faster than previous generations of Wi-Fi, specifically because work-from-home connectivity today is business critical for ISPs and consumers. Such factors will continue to play important roles as drivers of renewed connectivity demand as will the continued growth in number of devices in the home as well as data consumption.

The next phase in the ramp-up and deployment of new Wi-Fi technology will then be enterprise and carrier-grade APs and supporting systems. This evolution will happen a little later but also in parallel with the mass-market deployment of home Wi-Fi 6 and Wi-Fi 6E gateways and systems.

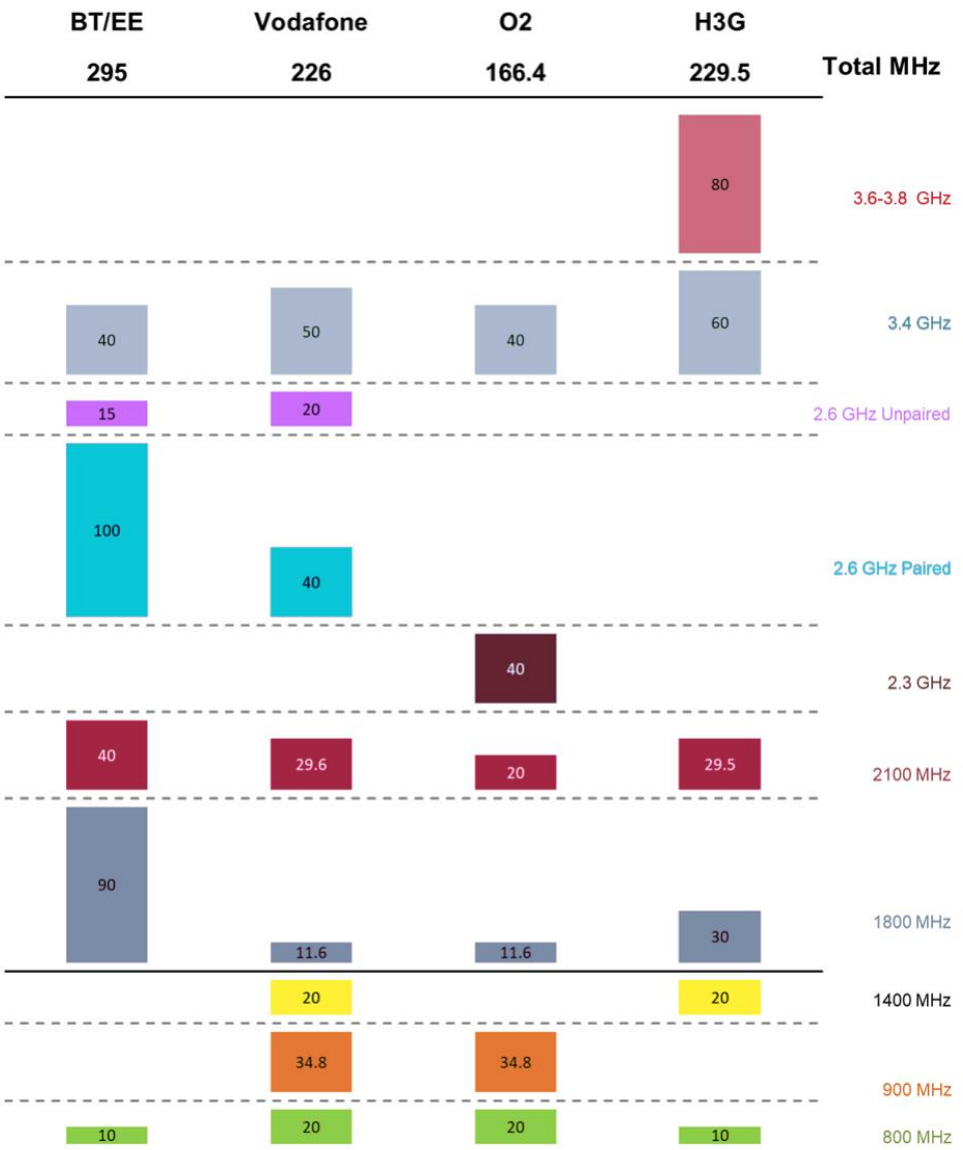
In general, the IEEE 802.11 standardization working group is now aiming for a Wi-Fi technology renewal cycle of five years, which means full market penetration of Wi-Fi 6 and Wi-Fi 6E into the enterprise and service provider Wi-Fi markets will sharply rise and come to completion around 2025-26.

Meanwhile it is critical to understand that the availability of pristine new unlicensed spectrum has made the case for carrier Wi-Fi hugely more compelling. Have a look - for example - at the graphic to the right picturing the total licensed spectrum holdings for mobile operators. The analysis uses the UK as an example.

The most amount of licensed spectrum is held by BT and totals 295 MHz while H3G is in second place totaling 229.5 MHz. None of the UK's mobile operators hold more than 300 MHz of total licensed spectrum - and most hold much less.

The UK recently released 500 MHz of pristine - meaning unused by legacy Wi-Fi - unlicensed spectrum in the lower 6 GHz band. That slice of Wi-Fi spectrum alone is around double the amount of licensed band that most UK mobile operators hold at this time. Add to this the existing 5 GHz and 2.4 GHz Wi-Fi bands - and we contend that it is becoming increasingly difficult for operators to reject the strategic use of carrier Wi-Fi services. Mobile and fixed operators need to embrace carrier Wi-Fi today to stay competitive.

In countries where the full 1.2 GHz of 6 GHz spectrum (up to 7.2 GHz) has been released - including the US, Korea, Brazil, Saudi Arabia, and the Republic of Chile thus far - the situation is even more extreme. The total amount of unlicensed spectrum available (some of it available for outdoor use as well) could be up to 10 times as much as the licensed spectrum holdings of a single mobile operator.



Hotspot 2.0 and Passpoint: Secure carrier Wi-Fi services

As one of the most important tools in the Wi-Fi toolbox, Passpoint including SIM authentication is enabling carrier-grade quality and highly monetizable Wi-Fi services.

Outstanding Wi-Fi 6 and Wi-Fi 6E radio technology capable of delivering very high-quality wireless connectivity is an excellent starting point. But for service providers, such capabilities must be transformed into user-friendly, secure, well-defined, and preferably carrier-class high-speed wireless data services.

To that end the Wi-Fi industry has developed the Hotspot 2.0 standard, nowadays more commonly referred to by its equipment certification name of Passpoint™.

Once provisioned on the phone or other Wi-Fi device, Passpoint technology allows users to connect securely, instantly, and automatically to public (or enterprise) Passpoint-capable Wi-Fi networks for example at public venues such as airports, stadiums, transport hubs, on aircraft, and so on. Passpoint technology also facilitates roaming onto Wi-Fi networks belonging to other service providers or third parties given that roaming agreements with the subscriber's home service provider exist.

Passpoint

- 802.11u
- ANQP
- 802.1x Wi-Fi
- WPA2/WPA3
- EAP Auth.

A Passpoint-capable network is defined by supporting the following functions:

- The network (Wi-Fi access point) should broadcast its capabilities and available services using 802.11u and a protocol called ANQP
- The network must use 802.1x-based authentication and WPA2 or WPA3 for over-the-air encryption
- Support for EAP-SIM/AKA (SIM-identity based) or EAP-TLS/TTLS (certificate-based methods usually for non-SIM devices) authentication
- Optional Wi-Fi roaming with home operator billing

An important component is the capability of Passpoint services to deliver 'Wi-Fi offload'-type services based on credentials stored in the subscriber's SIM. This means that carrier Wi-Fi services can be integrated into the total service offering of the mobile operator. Read more about this in our Wi-Fi and Cellular convergence section.

In essence Passpoint is designed to create a carrier-grade Wi-Fi service with a familiar and seamless user experience similar to that of cellular networks.

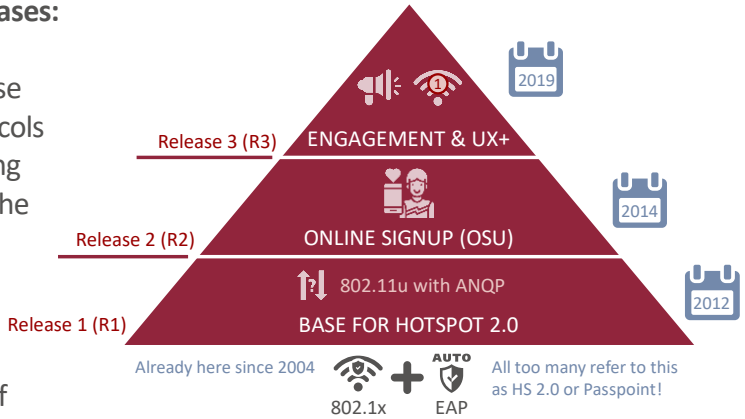
Note however that EAP-SIM/AKA authentication and mobile core integration can also be comfortably be applied outside of the full Hotspot 2.0/Passpoint specification. Aptilo Networks was already providing such solutions long before the release of the first Passpoint-capable devices. This also means that EAP-based authentication (SIM/AKA and TLS/TTLS) is not equivalent to Passpoint as such.

In the USA, Passpoint-capable Wi-Fi services and roaming are fairly readily available for example on the Boingo Wi-Fi network deployed at many airport locations and on some public Wi-Fi networks provided by US cablecos, for example on the former Time Warner Cable public Wi-Fi network today owned and operated by Charter Communications. Today, both Android and iOS operating systems natively support Passpoint, and many phones provided by US carriers are pre-provisioned to support Passpoint services.

In Europe and elsewhere, Passpoint-capable Wi-Fi services are less common but available from some major carriers in the form of EAP-SIM/AKA enabled 'Wi-Fi offload' convergent mobile services. Most enterprise-grade Wi-Fi access points are certified according to the Passpoint specifications.

Passpoint exists in three sequential releases:

Passpoint Release 1 (R1): The first release was introduced in 2012 and all the protocols and standards mentioned above, including 802.11u and ANQP, were included with the ability to discover Passpoint enabled networks and automatically connect to the optimal one.



Challenges still remain for onboarding of new devices. Users need to provision Passpoint R1 credentials manually by downloading a special file that contains profile and credential information. Many service providers use an app to make this process seamless for the user. More or less all mobile phones and laptops supports Passpoint RI. This includes Apple iPhones, although Apple has never formally certified them.

Passpoint Release 2 (R2):
Released in 2014 this version included the important Online Sign-Up (OSU) server allowing new users to create an account and in a user-friendly way provision Passpoint credentials at the point of access. This enables easy ad-hoc sign-up of new users, where they can select the service provider of choice if several options exist. To ensure that the server is trusted, the client validates the OSU server certificate. Either SOAP-XML or OMA-DM messages over HTTPS are then used for secure communications between the client and the provisioning servers.

Passpoint R2 requires a separate SSID for Online Sign-Up, either an open SSID or a so-called OSEN (OSU Server-only Authenticated L2 Encryption Network). This version also includes enhanced policy control for service providers. Device support is very limited.

Passpoint Release 3 (R3): R3 was released in 2019 but has not yet been implemented in a single device (as of April 2021). This version includes several new ANQP protocol elements and improvements in the interaction between operators and end-users. While previous versions have focused entirely on automatic connection and onboarding of the users, Passpoint R3 aims to enhance captive portal functions, by leveraging ANQP messaging.

For the first time Passpoint allows operators to offer B2B customers a tool to engage with visitors. They can do this through a Venue URL, which displays information about the Wi-Fi service and at the same time provides offers and local promotions. The R3 version also includes features for end-users to approve terms and conditions as well as charges for the Wi-Fi service.

Aptilo believes that Passpoint R3 may have attempted to push the user engagement features one step too far. Deploying these features through ANQP, locally in the access points, will make it harder to maintain central control especially in a multi-vendor deployment scenario. Because of the challenges in management and lack of device support there is a risk that R3 will never be implemented in carrier Wi-Fi networks.
Passpoint R3 also makes roaming much quicker and easier as the client can indicate, to a Wi-Fi access point, its membership of a roaming consortium.

Security is further improved in R3 with support up WPA3-Enterprise whereas R2 and R1 only supports up to WPA2-Enterprise. It is also possible to use the same SSID for both the actual Wi-Fi service (WPA2/WPA3) and the online sign-up (OSEN) functionality.

Strategies for deploying Passpoint in the real world

As of April 2021, no handsets support the latest R3 release of the standard. Some Android-based phones are R2 certified, but many are quite old. For example, the latest phone certified for R2 from Samsung is the Galaxy 5S (November 2016). In addition, smartphone vendors usually customize the Android platform to match own product requirements. So, just because it works with one vendor it doesn't mean that it works with another.

The Passpoint certification from Wi-Fi Alliance only certifies the radio protocols. In practice this means that new releases from R2 and above which include more complex service-related features cannot be guaranteed to work. At Aptilo we have experienced this through the testing conducted by the Wireless Broadband Alliance (WBA).

Conversely, it is probably true that devices with R2 support that have not been Passpoint certified also exist, just as R1 is supported in iPhones without official certification.

But as a service provider you cannot rely on so many unknown parameters.

On a more positive note, it is generally true that the vast majority of smartphones, tablets and laptops now support at least Passpoint R1. It is therefore advisable for operators to create and deploy Wi-Fi services based on R1, possibly with an extension for selective use of R2.

One thing is for certain: Operators who wait for new standards to be fully deployed and for mobile device manufacturers to adopt them risk waiting for a very long time. It is not only the complexity of the technology that decides whether a handset manufacturer develops support for standards like Passpoint R2/R3 or not and thus the wait could go on forever. Fortunately, there is no reason to delay the introduction of carrier-grade Wi-Fi services.

In the next section we will discuss how Passpoint R1 together with the new Captive Portal API may be the interim solution that in the end becomes the permanent pragmatic solution for Passpoint enabled networks.

Captive Portal API: A Pragmatic Approach to Passpoint

The new (September 2020) Internet Engineering Task Force (IETF) Captive Portal API, RFC8908, and RFC8910, is very promising.

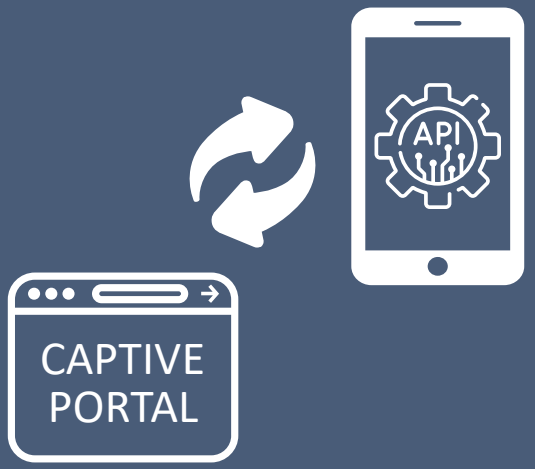
The Captive Portal API will not only improve the user experience in connection with traditional Captive Portal implementations. We believe that the Captive Portal API - in combination with Passpoint R1 - has the potential to deliver much of the user experience that Passpoint R2 and R3 were designed to accomplish.

The adoption of Captive Portal API among handset manufacturers has also been fast. Google was first to support the Captive Portal API for Android 11 and Apple soon followed with support in iOS14 and macOS Big Sur. With a critical mass of supporting devices in place, adoption across all the major operating systems appears imminent.

The Captive Portal API gives service management platforms, such as the Aptilo Service Management Platform™ (SMP), greater control of the Captive Portal flows for traditional hotspots. As a result, users will experience a more reliable service than ever before.

The overall user experience will also benefit hugely by the Captive Portal API. We have traditionally designed Access Gateways to intercept the user web request and redirected it to a Captive Portal.
With the Captive Portal API, the gateway does not need to intercept such requests. Instead, when users join the Wi-Fi network and receive an IP address via DHCP (or Router Advertisement in IPv6), the DHCP server also provides the URL to the Captive Portal API. This will trigger the device to query the API to determine if it is in captive mode or not.

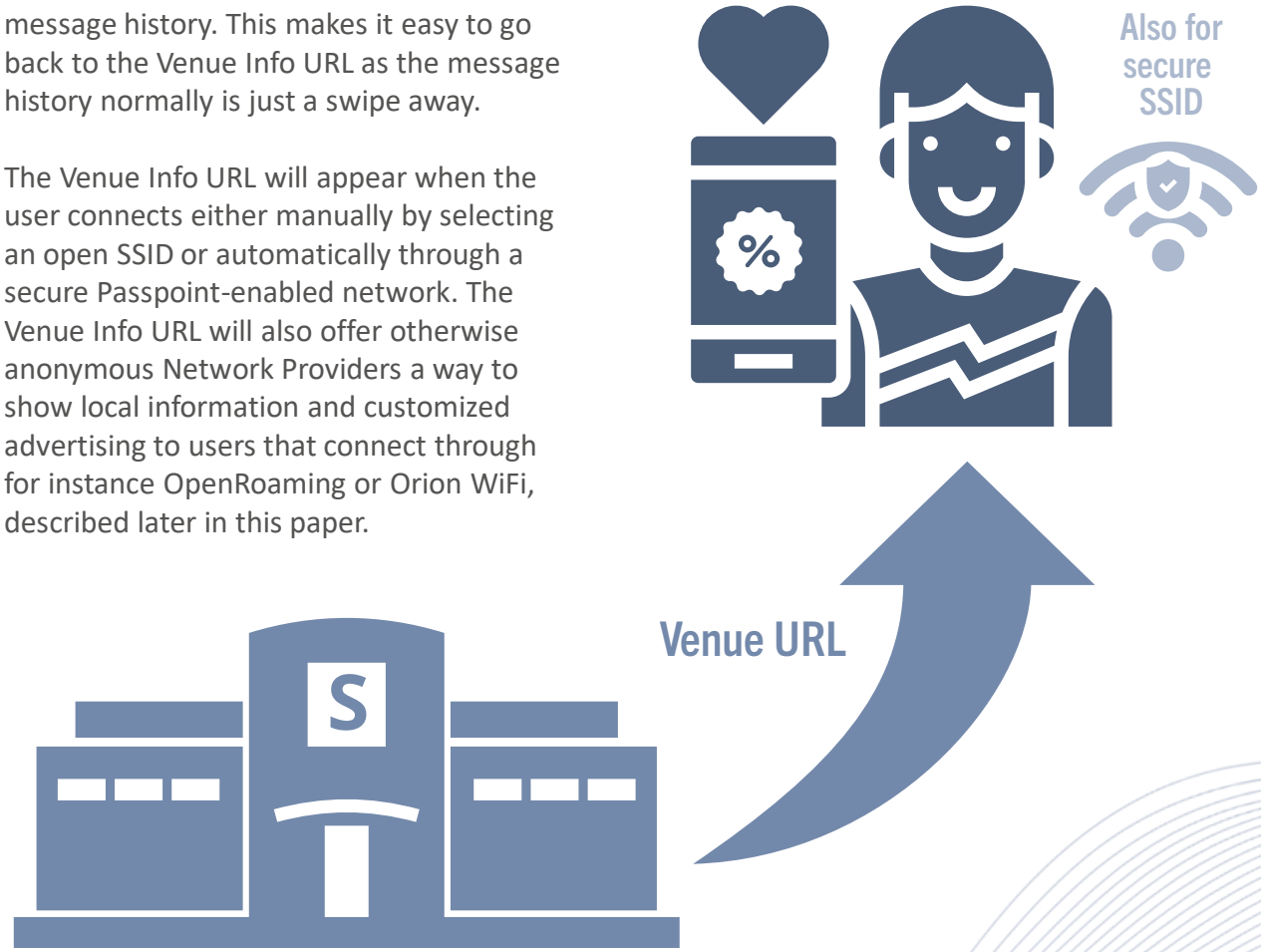
If the API states the device is in captive mode, the device will open the Captive Network Assistant (CNA) browser to log in. And, if the API states the device is not in captive mode, the device will proceed directly to Internet.



By using a standardized interaction between the device and the captive portal, the device can now reliably determine both its state and auxiliary information such as the remaining session time or data. This allows the device to take action before it reaches the limits, allowing the user to extend the session in a controlled way. This provides a smoother interaction between the device and the Wi-Fi service management system. Previously, with the guesswork of device-only captive portal detection and system-only control, the device was unaware of what was happening after authentication. This could cause sessions that appear to freeze after session time or data running out.

Another benefit of the Captive Portal API is that it can also provide a Venue Info URL. This is an excellent tool allowing service providers to empower their B2B customers to engage with users locally with information and offers. In current implementations the user receives the link to the Venue Info URL via an on-screen system message appearing as a text alert available during the session. The message remains on their lock screen and in their message history. This makes it easy to go back to the Venue Info URL as the message history normally is just a swipe away.

The Venue Info URL will appear when the user connects either manually by selecting an open SSID or automatically through a secure Passpoint-enabled network. The Venue Info URL will also offer otherwise anonymous Network Providers a way to show local information and customized advertising to users that connect through for instance OpenRoaming or Orion WiFi, described later in this paper.



Build from Passpoint R1

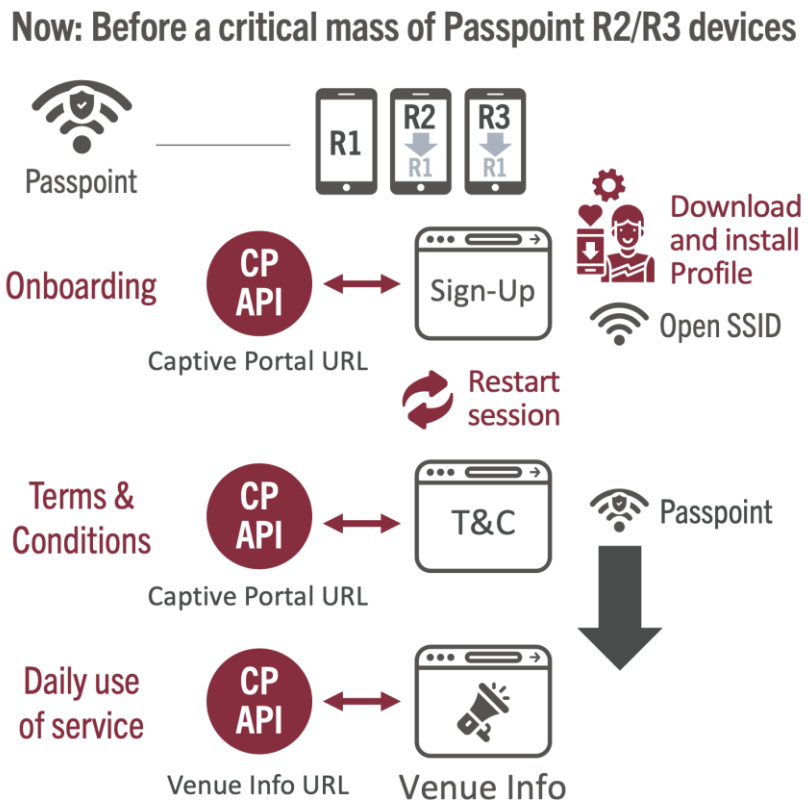
The fact that the Captive Portal API also works on secure Passpoint-enabled networks (802.1x), and that the concept of the Venue Info URL has many similarities with the Venue URL specified in Passpoint R3, opens up for new possibilities.

Aptilo believes that the Captive Portal API in combination with Passpoint R1 will deliver much of the user experience that Passpoint R2 and R3 were designed to accomplish.

It would make no sense to build special signup flows for the very few, if any, devices that support an end-to-end Wi-Fi service based on Passpoint R2/R3.

Devices that have not yet been provisioned for Passpoint R1 by other means, such as through a SIM-profile (EAP-SIM/AKA) or App (EAP-TLS/TTLS), will have to be provisioned ad-hoc through a sign-up portal over an open SSID or in advance via another connection.

The user will then download and install the Passpoint profile in his or her device with support from device specific instructions at the portal. The next time the user connects he or she will automatically connect through Passpoint on a secure SSID (802.1x). The Captive Portal API can then be used for approval of terms and conditions for new users or for existing users, if there is a need for an update. The Venue Info URL can also optionally be used to display venue specific information and promotions.



Add Passpoint R2-R3 Later

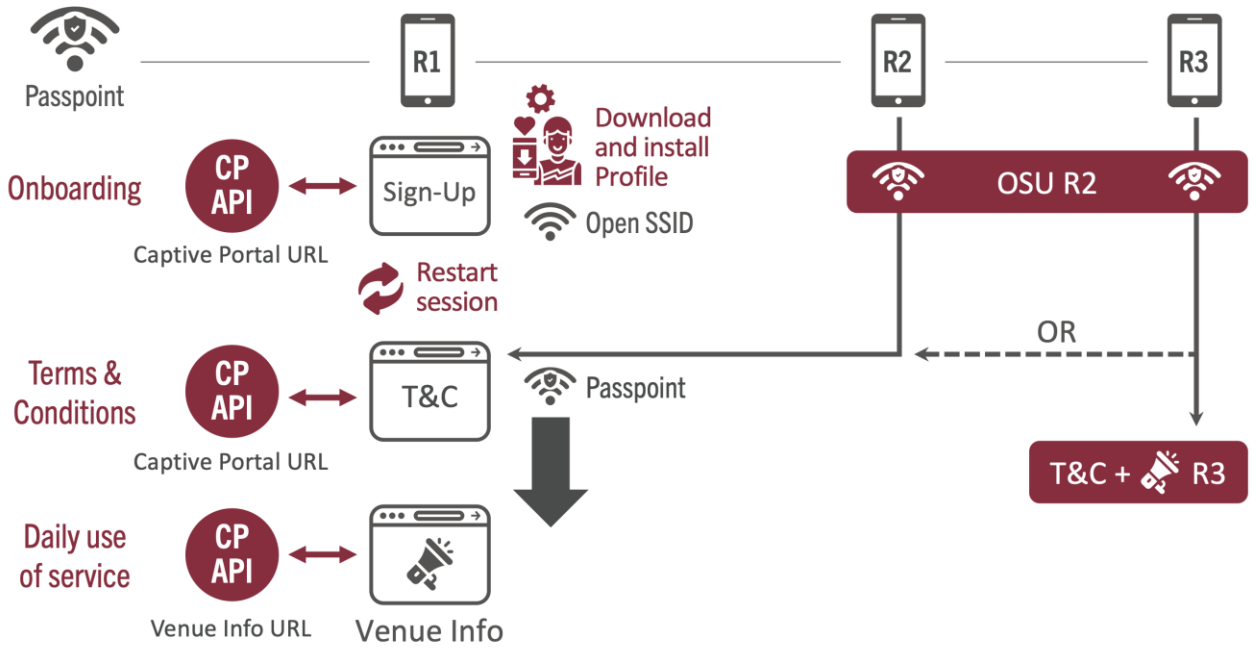
Support for Passpoint R2/R3 can be added later when, or if, a critical mass of device support has been achieved.

Note that the approval of terms and conditions has purposely been moved from the sign-up page to the first connection on the Passpoint-enabled network. This means that the process can also be used for already provisioned devices and devices with Passpoint R2 support. Users of Passpoint R1, that sign-up at the site, will see this as almost one flow since the session can be terminated right after a user has installed the profile. A user will then immediately return as pre-provisioned.

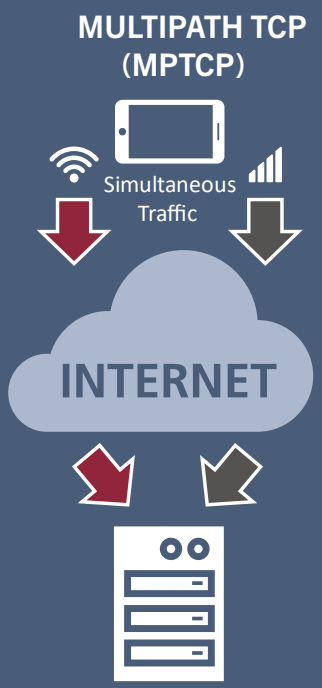
Online signup through the R2 online signup server (OSU) has many benefits to users once there is sufficient device support.

It remains to be seen if the benefits of Passpoint R3 terms and conditions and user engagement features will be significant or if it would be more beneficial to use the same processes as with Passpoint R1/R2 capable devices (dotted line in the figure).

Later: When there is a critical mass of Passpoint R2/R3 devices



A pragmatic approach to Passpoint. Start with Passpoint R1 and then add support for R2 and R3 when there is a critical mass device support. Utilize the Captive Portal API to fill the gaps in functionality.



Multipath TCP : Simultaneous use of Cellular & Wi-Fi

So-called Multipath TCP (MPTCP) technology allows IP data traffic to flow simultaneously over Wi-Fi and 5G networks. The result are higher data rates, much improved quality overall, and gapless handovers between Wi-Fi and cellular.

However, MPTCP requires support both in the device and the application server or web page it is connected to. This signifi-cantly slows down the deployment of this technology.

The only example of an existing commercial MPTCP implementation is proprietary and resides within Apple's iOS and infrastructure.

Apple uses MPTCP to make sure certain apps - currently Siri, Maps, and Music - run as responsively as possible by applying both Wi-Fi and mobile data services together and interchangeably. A couple of years ago Apple made their version of MPTCP available for developers via an API and thus far at least Amazon has chosen Apple's MPTCP function for their Alexa app.

There's also now a standardized 3GPP function utilizing MPTCP called ATSSS. Read more about this in our Cellular and Wi-Fi Convergence chapter.

SUMMARY

Game-Changing Wi-Fi Technology Developments

Wi-Fi 6 – A paradigm shift in connectivity

- Wi-Fi 6 features orthogonal frequency division multiple access (OFDMA), which includes cellular-style scheduling.
- OFDMA brings deterministic performance to Wi-Fi for the first time, especially in dense areas with many users.
- Up to 4x faster upload, 6x faster download, 4x better coverage and 6x longer battery life.
- The rate of Wi-Fi 6 market penetration will be very fast, by 2023 most enterprise-grade access points will be Wi-Fi 6-capable.

Wi-Fi 6E – running on 6 GHz, will triple the available Wi-Fi spectrum

- The availability of pristine new unlicensed spectrum has made the case for carrier Wi-Fi hugely more compelling.
- There will be no interference with legacy Wi-Fi as the 6 GHz band is reserved for Wi-Fi 6E only.
- Enterprise Wi-Fi data rates will be at least quadrupled, and latency will be as low as 2 ms.

The share of offloaded traffic will only increase with 5G

- According to Cisco the share of offloaded traffic to Wi-Fi will go from 59% in 4G to 71% in 5G.

Build on Passpoint R1: A pragmatic approach to Passpoint (Hotspot 2.0)

- Passpoint provides a secure and seamless user experience with automatic login (EAP) at encrypted 802.1x Wi-Fi networks.
- In April 2021, all devices supports Passpoint release 1 (R1). A handful devices supports release 2 (R2) and none release 3 (R3).
- Aptilo suggest to use Passpoint R1 in combination with the new IETF Captive Portal API to achieve much of the R2/R3 features.

Multipath TCP (MPTCP): Simultaneous use of Cellular & Wi-Fi

- Apple already uses MPTCP for Siri, Maps, and Music.
- 3GPP has standardized use of MPTCP in their ATSSS standard (more about that in section 5).

3

The industry is moving in the direction of new technology and new business models enabling more and better Wi-Fi everywhere - including for carriers and enterprises.

Wi-Fi Industry Initiatives

Industry initiatives for cost-effective ubiquitous Wi-Fi

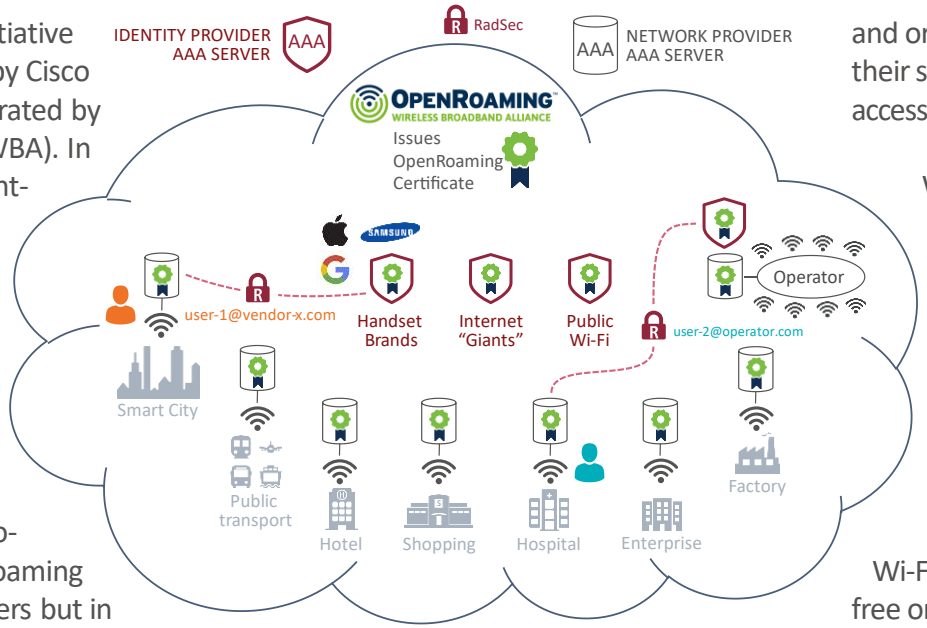
Meanwhile the growing mass market popularity of Wi-Fi as well as its giant leap of evolution to Wi-Fi 6 and Wi-Fi 6E is driving renewed interest in Wi-Fi roaming, mobile offload, and more.

New initiatives are indicators of an industry-wide desire to bring Wi-Fi and mobile services together for the benefit of service providers, consumers, and the ecosystem as a whole. And although similar initiatives have existed before, we believe that this time there are more compelling reasons for them to succeed.

OpenRoaming by Wireless Broadband Alliance

OpenRoaming is a Wi-Fi roaming initiative originally conceived and launched by Cisco but since taken over and today operated by the Wireless Broadband Alliance (WBA). In essence OpenRoaming is a Passpoint-based roaming scheme bringing together 'identity providers' and 'network providers' into a so called open roaming federation.

'Identity providers' can be any organization providing accounts for users. The most common and most numerous types of identity providers within the context of OpenRoaming are fixed and mobile service providers but in principle anyone providing a user account can also be an identity provider. Both Samsung and Google are identity providers and OpenRoaming is enabled by default in all Samsung devices from Galaxy S9 and in Google Pixel phones with Android 11 and above. Apple is largely expected to follow suit. OpenRoaming is a game changer for the live deployment of Passpoint. The industry-wide Passpoint project has been in the works since 2014, but the issue has always been provisioning of Passpoint profiles.



Now finally, Passpoint is pre-enabled in devices from the factory (for OpenRoaming). With this, Passpoint has the potential to achieve mass-market success also in practice, at least for the settlement-free use case within OpenRoaming.

Other potential identity providers could in theory be Internet giants like Facebook, Amazon, or Netflix and public networks such as WiFi4EU and Eduroam. Such companies and organizations would then be able to offer their subscribers auto-connect and secure access to Wi-Fi at participating Wi-Fi networks.

Within the OpenRoaming framework the term 'network providers' is used to describe the participating venues or service providers who own and operate Wi-Fi networks. 'Network providers' can be anything from major carrier Wi-Fi footprints to hotel chains, malls, airports, or congress centers.

Wi-Fi roaming within OpenRoaming can be free or paid - the details are up to the roaming partners to agree upon. The goal of OpenRoaming is to build renewed popular support - among carriers and venues - for ubiquitous Wi-Fi roaming and Passpoint.

We also see a use case for OpenRoaming together with Aptilo's Zero-touch Wi-Fi IoT Connectivity invention, more on that in the Wi-Fi IoT section.

Native support in Samsung, Google and likely soon Apple

Google's Orion WiFi

In the late summer of 2020 Google's Area 120 - an in-house technology incubator at Google - launched Orion WiFi. The concept behind Orion WiFi is simple: Public venues of any kind - restaurants, cafes, malls, congress centers, and so on - can receive payment for making their Wi-Fi available to mobile operator subscribers.

Orion WiFi uses Passpoint for secure auto-connect to venue Wi-Fi networks as well as the RadSec protocol (RADIUS over TCP & TLS). One technical requirement is that the venue Wi-Fi network supports Passpoint, which means that SMB or consumer-grade Wi-Fi equipment without Passpoint for the time being will not work with Orion WiFi.

The idea is that a person with a smartphone (subscribers of participating MNOs) can walk into an Orion WiFi participating venue and auto-connect to the Wi-Fi service.

The venue will be paid for providing the service by the person's service provider - but probably not only based data volume. It is likely that other factors such as quality and location will affect the amount paid although Google has not thus far released the specifics.

For now (April 2021), Orion WiFi is only available in the US and only works if you are a Google Fi or Republic Wireless mobile subscriber. The excellent news is that this a new effort to create a platform where nearly any venue can sign up to a service that will pay them to offload mobile data onto their own Wi-Fi network. If the scheme turns out to be a success, Orion WiFi may seed the ground for wider adoption of such types of Wi-Fi & mobile convergent services based on Passpoint or similar technologies.

TELECOM INFRA PROJECT

Telecom Infra Project: Disaggregating Wi-Fi technology

Meanwhile other industry initiatives are aiming at breaking open the markets for Wi-Fi hardware, software, and services for the purpose of driving up the availability of Wi-Fi networks and costs down.
Can hardware and software for Wi-Fi infrastructure be disaggregated - meaning can the two be made independent or even open sourced? If you ask the Wi-Fi subgroup of the Telecom Infra Project (TIP) the answer is yes.

The TIP 'Open Wi-Fi Infrastructure' project is working to remove the lock-in effects of proprietary Wi-Fi hardware and software, and architectures in general, with a view to reducing network costs and increasing ubiquity. Thus far the collaborative project - which is widely supported by Facebook - is mostly working to develop disaggregated residential Wi-Fi services architectures. TIP is also working on improved collaborative schemes to facilitate mobile and Wi-Fi convergence including Wi-Fi offload.

The work by TIP may eventually lend itself well to reducing the cost and complexity of deploying carrier Wi-Fi networks.

Wi-Fi Industry Initiatives

Industry initiatives for cost-effective ubiquitous Wi-Fi

- New initiatives are indicators of an industry-wide desire to bring Wi-Fi and mobile services together for the benefit of service providers, consumers, and the ecosystem.
- Similar initiatives have existed before but we believe that this time there are more compelling reasons for them to succeed.

OpenRoaming by Wireless Broadband Alliance (WBA)

- OpenRoaming is a Passpoint-based roaming scheme bringing together 'identity providers' and 'network providers' into a so-called open roaming federation. For the user, roaming is as seamless as in cellular networks.
- Participating parties do not need to know each other, AAA servers trust each other through a certificate issued by the WBA.
- Both Samsung and Google are identity providers and OpenRoaming is enabled by default in all Samsung devices from Galaxy S9 and in Google Pixel phones with Android 11 and above. This is a game-changer for mass-deployment of Passpoint.

Google Orion WiFi

- Restaurants, cafes, malls, congress centers, and others are paid for making their Wi-Fi available to mobile operator subscribers
- For now (April 2021), Orion WiFi is only available in the US and if you are a Google Fi or Republic Wireless mobile subscriber.

Telecom Infra Project (TIP): Disaggregating Wi-Fi technology

- The TIP 'Open Wi-Fi Infrastructure' project is working to remove the lock-in effects of proprietary Wi-Fi hardware and software.
- Thus far the collaborative project - which is widely supported by Facebook - is mostly working to develop disaggregated residential Wi-Fi service architectures.

4

Operator managed Business-to-Business (B2B) Wi-Fi is the foundation for carrier Wi-Fi both in terms of monetization and to gain a valuable Wi-Fi footprint for subscribers.

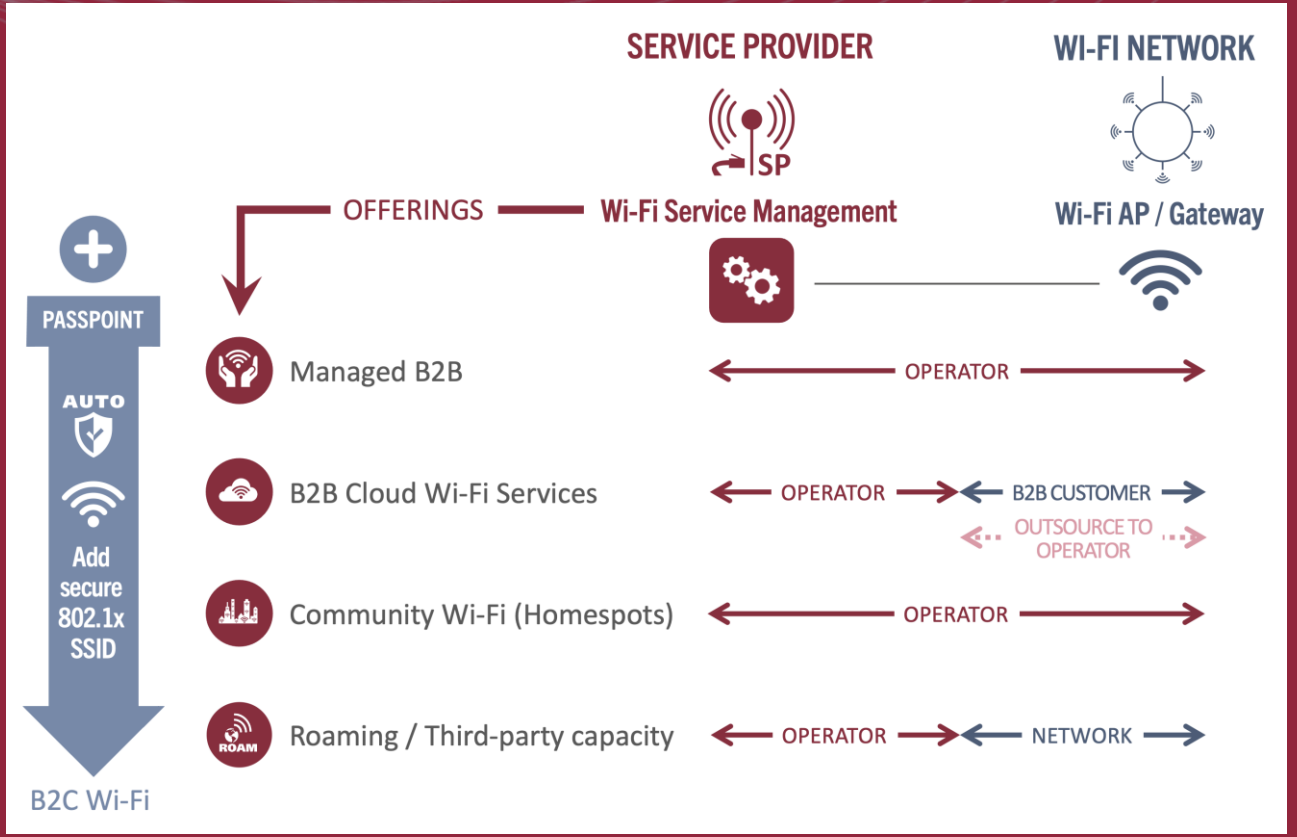
Carrier Wi-Fi Strategies

How to build a carrier Wi-Fi footprint

Carrier Wi-Fi footprints, or Wi-Fi network coverage, can be built or created in a number of ways of which the most common are shown in the figure.

As such the methods are independent and are often used in combination. Aptilo Networks today serves operator customers who are using several of the methods concurrently to build a Wi-Fi footprint.

Operators can use this footprint and add a secure and Passpoint enabled SSID for their own subscribers.



Operator Managed B2B or B2C Wi-Fi

This is a fully operator-owned and managed Wi-Fi network. In this case the operator owns and manages everything including on-premise Wi-Fi infrastructure, services, on-boarding, operations, etc. As an example, Aptilo recently provided the Kingdom of Bahrain's Batelco with a service management platform, the Aptilo SMP, for Batelco themselves to deliver top-quality managed venue Wi-Fi services (B2B and B2B2C) to their clients.

An example of a B2C network of this type is that of Telkom Indonesia, a giant telco operating some 400,000 Wi-Fi access points (including homespots) serving more than 70 million users (this figure includes businesses).

Telkom Indonesia has been using Aptilo service management solutions for six years and counting. Good examples of effective operator managed B2B Wi-Fi service offerings include the small business Wi-Fi services of Aptilo clients NOS Portugal and Swisscom.

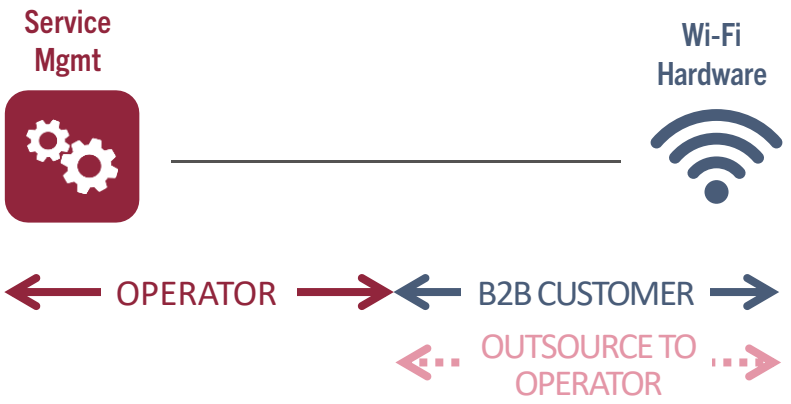
For the most part, managed B2B services provide excellent, high margin revenues.

Operator B2B Cloud Wi-Fi Services

Here the operator provides tools - meaning Cloud-based Software-As-A-Service-type Wi-Fi service management - for operation of managed enterprise Wi-Fi, while the B2B customer owns and retains his or her own Wi-Fi infrastructure.
This type of approach is often used for instance in the case of guest Wi-Fi services.

The approach is required when operators want to extend their coverage footprint and business scope simply because most venues already own and operate their own Wi-Fi networks.

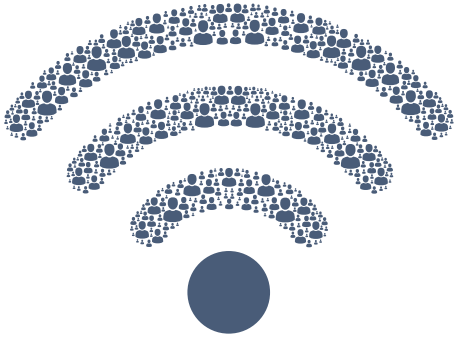
Conversely, in some cases Aptilo clients have acquired the Wi-Fi network equipment belonging to certain important customers and locations so as to convert the service to a fully operator managed B2B Wi-Fi.



Community Wi-Fi (Homespots)

'Homespots' or community Wi-Fi means that Wi-Fi-capable residential gateways (terminating fibre, DSL, or cable connections in the home) are configured to double as public Wi-Fi hotspots in addition to fulfilling their primary role of delivering residential Wi-Fi services. Such schemes - which are or have been popular with US cablecos in particular - are relatively quick ways of building huge Wi-Fi hotspot networks spanning millions of locations.

Homespot services are commonly used for 'Wi-Fi offload' of mobile data from for example cableco MVNO subscribers.



For example: Spectrum Mobile - the MVNO services arm of US cableco Charter Communications - uses such a scheme to keep their subscribers connected on Charter-owned 'homespots' as much as possible.

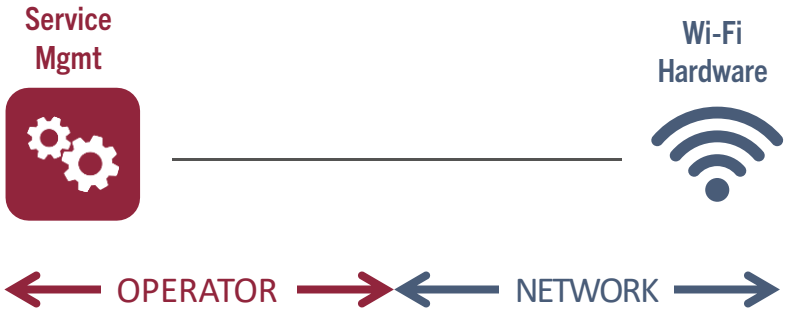
Some service providers also configure their business customers' Wi-Fi to serve multiple functions: Wi-Fi for the business at which it is installed as well as for public Wi-Fi.

ROAM

Third-party Wi-Fi Services & Roaming

Operators with or without own Wi-Fi networks can also choose to partner with third-party Wi-Fi service providers to allow their subscribers access to specific Wi-Fi service footprints, for example for international travel or Wi-Fi services in the London Underground, with 3UK enabled by Aptilo SMP and using Virgin Media's network, and so on. Some third parties can also provide roaming onto extensive airport Wi-Fi networks, for example.

Aptilo Networks is currently contributing to the ongoing international collaborative work on the Wireless Broadband Alliance's OpenRoaming initiative (discussed above) which at some point may allow the means for mobile subscribers to roam onto Wi-Fi services at stadiums, malls, or even onto the properties of certain hotel chains.



Operator Wi-Fi monetization strategies

Based on twenty years of Wi-Fi industry evolution, carrier Wi-Fi monetization strategies are both well-known and evolving continuously to match B2B and B2C needs. Aptilo has been actively participating in this service evolution process from the start.

So how do you monetize Wi-Fi? The question has loomed large for years particularly since, from a consumer point of view, Wi-Fi is typically offered as a free amenity. This does however not mean that service providers cannot monetize Wi-Fi services. Apple founder Steve Jobs once elegantly pointed out that “if you’re not paying for the product, you are the product.” And this is indeed true specifically for Wi-Fi.

The service provider will receive significant revenues from venues that want to provide carrier-grade Wi-Fi to guests or workers in order to stay competitive and relevant. Users receive the free service in return for their engagement with the brand and as a result of surrendering some personal details. The service providers may even agree to subsidize the B2B Wi-Fi service at particularly attractive venues in return for securing valuable indoor Wi-Fi footprint for use by their own subscribers.

For years operator managed Wi-Fi has been a specialized but growing telecom market segment. Most Wi-Fi monetization strategies and methods are not new but in coming years we expect them to grow both in value and importance as they are boosted in particular by the mass-market arrival of new Wi-Fi technology.

This strategy is driven by the continuous increase in demand for quality Wi-Fi services by businesses everywhere. Hardly a public or private venue exists without the need for Wi-Fi and so business clients can now benefit by offering their clients and staff top-quality carrier-grade Wi-Fi delivered by expert service providers.

Operator B2B Wi-Fi

B2B Wi-Fi offers not only a significant revenue stream but also a needed service 'stickiness' that keeps businesses and consumers coming back. Aptilo believes B2B Wi-Fi is a business-critical contribution to an all-encompassing 5G strategy, which also includes high-speed, low-latency indoor services delivered over Wi-Fi.

Businesses want to provide an easy-to-use, high-quality Wi-Fi service for their visitors. In many cases venue owners see value in using Wi-Fi as a means of engaging with their guests and clients, for example by asking clients to create and verify accounts or by presenting them with Internet access sponsorship options, coupon offers, and so on.

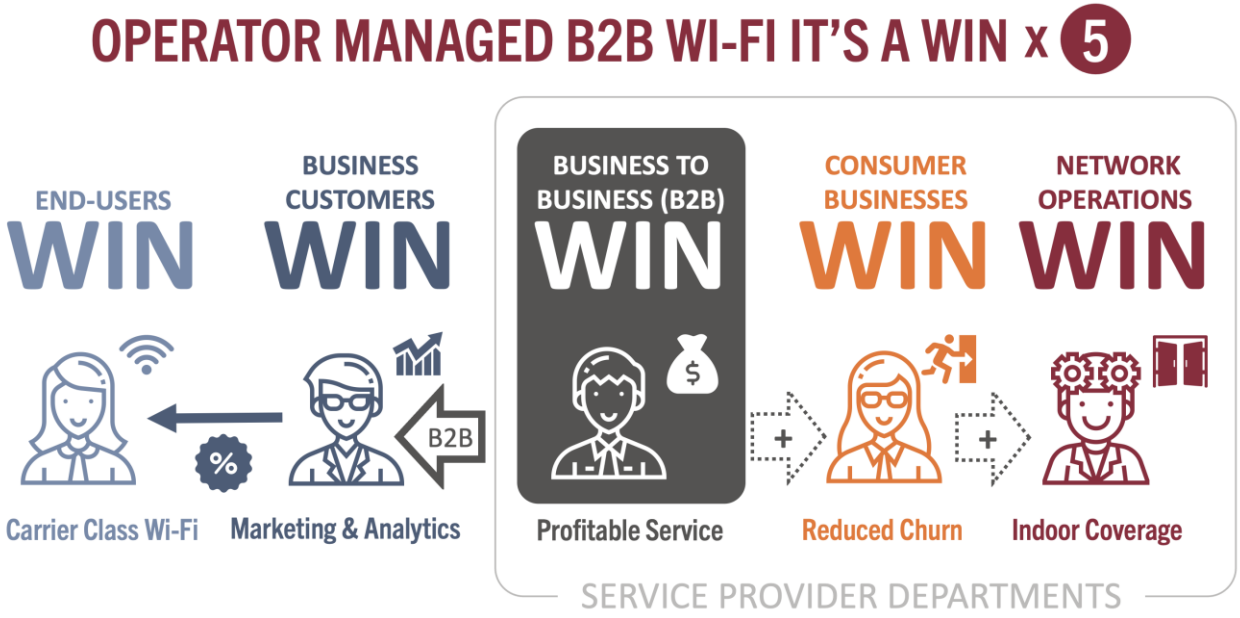
In some cases, venues will still request payment for Wi-Fi services often according to a 'freemium'-type business model. In other cases, venues may accept guests accessing their network via Passpoint-based auto-connect Wi-Fi either for free or via a paid settlement agreement between operators.

It is a well-established fact that venue owners benefit from collecting and analyzing Wi-Fi data. The data can then be used for marketing of the venues' products and services. Care must be exercised so as to act only in accordance with GDPR or other relevant privacy regulations.
When operators provide such sophisticated Wi-Fi-based tools to businesses they are typically also engaging their clients at the decision-making level, which in turn is conducive to building stronger, higher-value, and more fruitful client relationships.

All of these things are not easy for business owners to accomplish on their own. In most cases they are best provided by experts – meaning operators.

If operator B2B Wi-Fi doubles as a service offered to consumers, then both operators and consumers will benefit from the high-capacity deep indoor wireless coverage - provided of course that Wi-Fi networks are built in accordance with carrier-grade quality standards. The same applies for any businesses relying on the indoor coverage.

Last but not least: Mobile operators can in some cases leverage the strong demand for Wi-Fi from businesses to introduce small cells or DAS systems into indoor locations owned by such businesses. In some instances, venue owners may more readily accept such installations when also provided with the quality Wi-Fi that their businesses and their guests need. In this way operator B2B Wi-Fi can also become an indirect means of achieving better indoor cellular coverage.



B2B Wi-Fi is a win x 5. The service provider's B2B department gets a profitable service, business customers get analytics and a tool to engage their visitors, and visitors get a carrier class Wi-Fi service.
If an additional SSID or Passpoint service is implemented for the operator's subscribers, then the consumer department will receive the benefits of reduced churn and network operations will get much needed indoor coverage.

Operator Home Wi-Fi

Residential Wi-Fi delivered by ISPs is right now one of the most significant growth opportunities not just in Wi-Fi but within all of the tech world. A big driver is the need for much better home connectivity to accommodate an avalanche of devices. More and more individuals are transforming their homes into work-from-home offices.

Most ISP-delivered home Wi-Fi services are today managed with simple WPA2 or WPA3 passkey access although in more sophisticated cases smart home services are delivered to Wi-Fi devices at the endpoints. For example: A smart home Wi-Fi configuration app can provision not only Internet connectivity but many other services, such as parental controls, security monitoring, motion detection, and more.

In a few relatively new use cases the classic world of residential Wi-Fi (as provided by ISPs) and public Wi-Fi (such as managed services enabled by Passpoint or SIM-based authentication) are to some extent merging.

These include for example Wi-Fi services offered at MDU (Multi Dwelling Unit) housing complexes such as senior living facilities, long-stay resorts and condominiums, college campuses, and more.

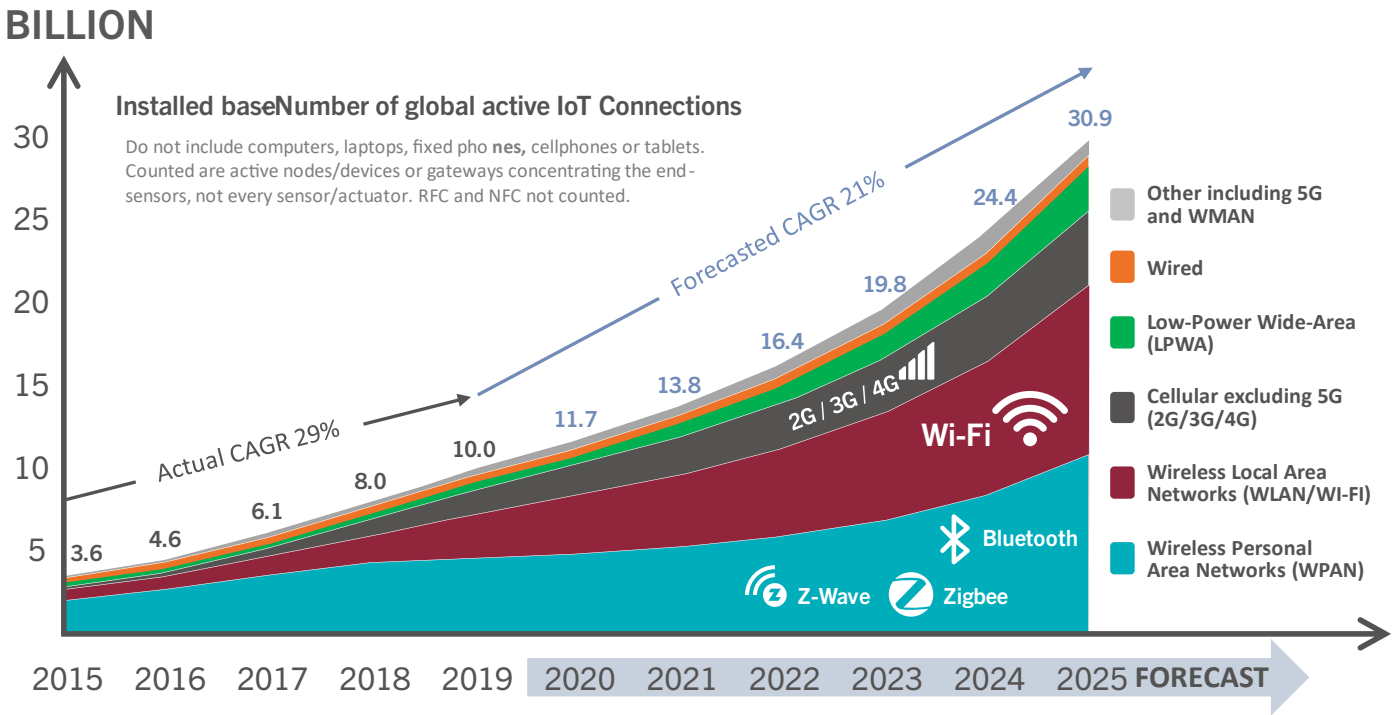
Wi-Fi services for MDUs - because they are often deployed to cover a wide area similar to classic campus Wi-Fi - often require carrier-grade authentication and service management so that guests and residents can enjoy high-quality, secure, and reliable Wi-Fi services anywhere on the property and on any connected device they choose.

We believe the service provider industry in coming years will see new products or even new companies emerge to serve many such specialized MDU (or new emerging enterprise) segments. Many such new business opportunities will be driven by the hugely improved and more sophisticated Wi-Fi technology and services based on Wi-Fi 6 and Wi-Fi 6E.

Wi-Fi-based IoT

The opportunity for operators to deliver connectivity services for IoT devices has long been touted as one of the most important growth segments in telecom. And the number of wireless IoT devices in need of connectivity is indeed growing at an impressive rate. As shown in the figure, IoT Analytics forecasts a growth of the installed base from 10.0 billion in 2019 to 30.9 billion in 2025. Ericsson's slightly more conservative estimate predicts a growth from 12.6 billion units in 2020 to a whopping 26.9 billion in 2026.

But here is a perhaps lesser-known fact: By far the largest proportion of IoT devices – approximately 7.5 billion out of a total of 11.7 billion units as of 2020 to be exact, see the figure above - are short-range, non-cellular devices. According to IoT Analytics, Wi-Fi-based IoT devices represent a third of all IoT devices in 2020 and is one of the fastest growing tech product segments.



Growth in connected IoT devices including Wi-Fi IoT (WLAN).
Source: IoT Analytics

The number of Wi-Fi-based IoT devices is expected to increase to more than 7 billion by 2025. This number of course includes devices for the smart home, devices operated by businesses, and even machinery and automation-type devices for industrial applications.

Connecting billions of IoT devices with secure and reliable carrier-grade Wi-Fi services is clearly a big business opportunity. But it is also a significant challenge for any service provider because the IoT device market is notoriously fragmented and dominated by proprietary solutions. The secure and automatic onboarding of masses of IoT Wi-Fi devices - many of which are 'headless' without a user interface - has proven less than easy.

Thankfully there are new tools and platforms that allow service providers to achieve effective automatic onboarding. Aptilo's Zero-Touch Wi-Fi IoT Connectivity™ solution uses certificates (x.509) that already exists in devices to auto-connect Wi-Fi IoT devices to Wi-Fi right out of the box. Aptilo has partnered with Amazon Web Services (AWS) IoT Core to deliver an end-to-end, massively scalable Wi-Fi IoT onboarding solution.

The solution also lends itself well to the OpenRoaming concept described previously. In this case the Zero-Touch service can act as an 'identity provider' for IoT devices allowing any enterprise, IoT solution provider, or operator to sign up for the service. The end result would be the onboarding and auto-connection of IoT devices not only within their own network but also within the extended coverage footprint enabled by the OpenRoaming federation.

Because we encourage the industry to participate in this initiative, we have chosen not to patent the Zero-Touch innovation. We believe that the time is now for operators to invest in massively scalable and standardized onboarding for Wi-Fi IoT.

For more about the Aptilo solution, go to the last section or also to Aptilo's web (link below).

SUMMARY

Carrier Wi-Fi

- **Business-to-business (B2B) Wi-Fi is the foundation for building an indoor Wi-Fi footprint**
  - Community Wi-Fi and roaming agreements / third-party networks are other options.
  - We advise operators to add a secure Passpoint-enabled connectivity across all these networks for subscribers.
- **B2B Wi-Fi services are 'sticky'**
  - They offer significant revenue streams but also 'stickiness' that keeps businesses and consumers coming back.
  - Aptilo believes B2B Wi-Fi is a business-critical contribution to an all-encompassing 5G strategy.
- **B2B Wi-Fi services are a win x 5**
  - End-users get Carrier-class Wi-Fi, Venue owners get marketing and analytics, operator B2B department get significant revenues, consumer department gets reduced churn and network operations gets indoor coverage.
- **By far the largest proportion of IoT devices use short range technologies such as Wi-Fi**
  - Approximately 7.5 billion out of a total of 11.7 billion IoT units as of 2020 are short-range and non-cellular.
- **Wi-Fi is one of the fastest growing IoT segments**
  - The number of Wi-Fi-based IoT devices is expected to increase to more than 7 billion by 2025.
- **Manual onboarding of Wi-Fi IoT devices is a potential showstopper for a mass-market**
  - Aptilo's Zero-Touch Wi-Fi IoT Connectivity initiative will make onboarding automatic. This is not a proprietary solution; We encourage the industry to follow suit.

5

Wi-Fi & Cellular Convergence

Business and technical consolidation trends all point in the same direction: Mobile and fixed networks are coming together - for the benefit of everyone in the industry and consumers.

Wi-Fi and Cellular Convergence: Opportunities today

While Wi-Fi and cellular is on a gradual path to technical convergence there can be no question that corporate fixed-cellular convergence aka consolidation has been happening for a long time already. Some years ago, dominant mobile operators trended towards acquiring cable and fiber operations. More recently fixed service providers and cablecos have either acquired mobile operators or have become MVNOs themselves.

All of this is seeding the ground for technology and services convergence in addition to the more obvious corporate consolidation.

But, as already discussed, if real technical Wi-Fi and mobile (5G) convergence is to happen service providers also need to break free from conventional organizational 'silos' and compartmentalized thinking on what technologies do and do not belong to mobile and fixed wireless services, respectively.

At Aptilo Networks we believe there is significant untapped business potential in breaking such operator 'silos' in order to achieve real progress in service and technological convergence.

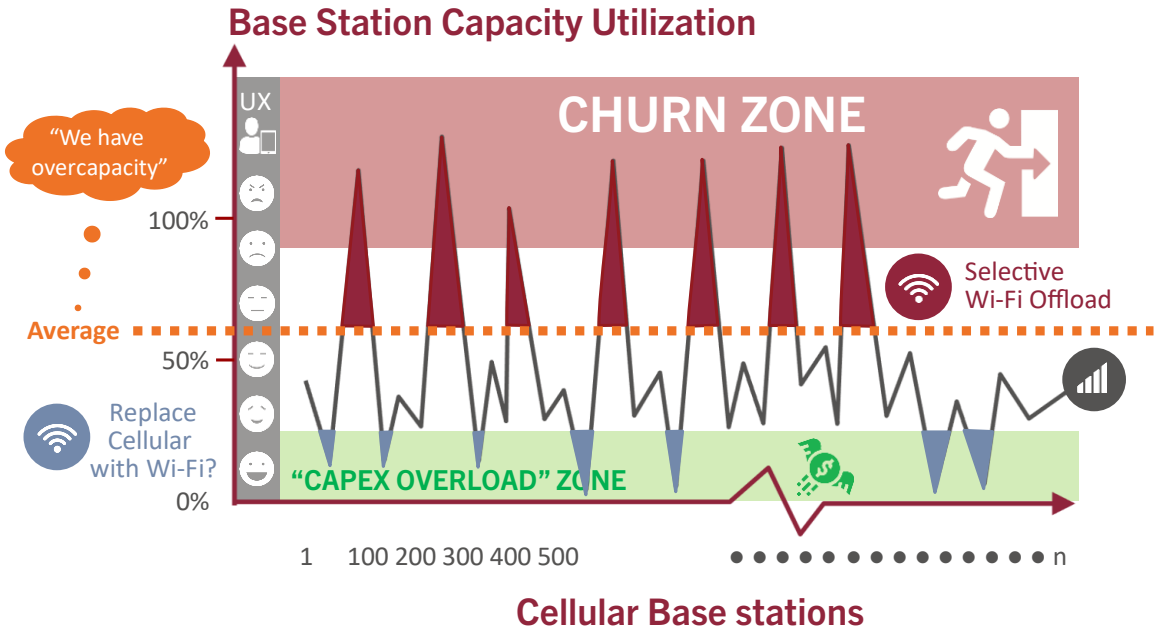
Some of these opportunities do not need big infrastructure investments nor do operators need to wait for new convergence (3GPP) standards or equipment to emerge.

Mobile network traffic data may indicate overcapacity. But that is often only true as a high-level average. There will always be some cell sites suffering from congestion and some only serving a handful of subscribers. Selective Wi-Fi offload is the answer: Build Wi-Fi capacity where it is needed most and of course always for indoor coverage.
If regulations allow it, mobile operators may even take the bold step to replace cellular with Wi-Fi at some locations.

Here is our suggested list of reasonably simple network changes that would create a 'Wi-Fi offload' service and hence a quick new source of revenue for operators:

- Create an additional SSID (network name) supporting the 802.1x protocol on all of your existing Wi-Fi footprint.
- Enable SIM-based Wi-Fi services authentication (using the EAP-SIM/AKA protocol).
- Introduce selective offloading of mobile traffic to Wi-Fi at various locations.

By introducing the right configurations and by provisioning devices correctly, such a scheme would create an additional layer of mobile network capacity using Wi-Fi. But this would of course also require that mobile and fixed parts of the operator organization collaborate.

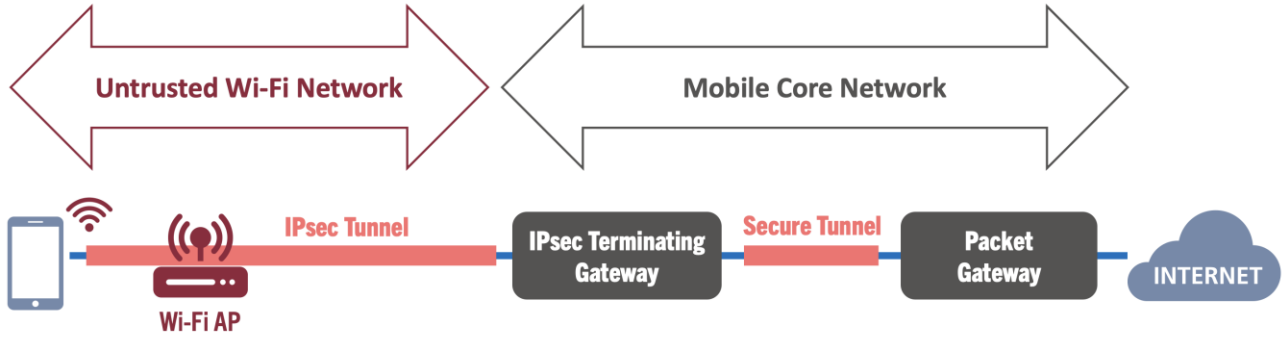


Wi-Fi and Cellular Convergence: 5G and Wi-Fi integration

5G introduces *new* network architectural concepts for Wi-Fi integration with the mobile core (non-3GPP access). In this section we first explore the basic concepts of trusted and untrusted Wi-Fi access and then point out what is *new* within 5G.

The 3GPP standard primarily offers two main strategies to integrate Wi-Fi networks with the mobile core: Trusted and untrusted non-3GPP (Wi-Fi) access.

Untrusted non-3GPP (Wi-Fi) Access



Untrusted non-3GPP (Wi-Fi) access was first introduced in the Wi-Fi specification in 3GPP Release 6 (2005). At that time Wi-Fi access points featuring advanced security features were rare. Hence Wi-Fi was considered open and unsecure by default. Untrusted access includes any type of Wi-Fi access that the operator has no control over such as public hotspots, subscribers' home Wi-Fi, and corporate Wi-Fi. It also includes any Wi-Fi that does not provide sufficient security mechanisms such as authentication and radio link encryption.

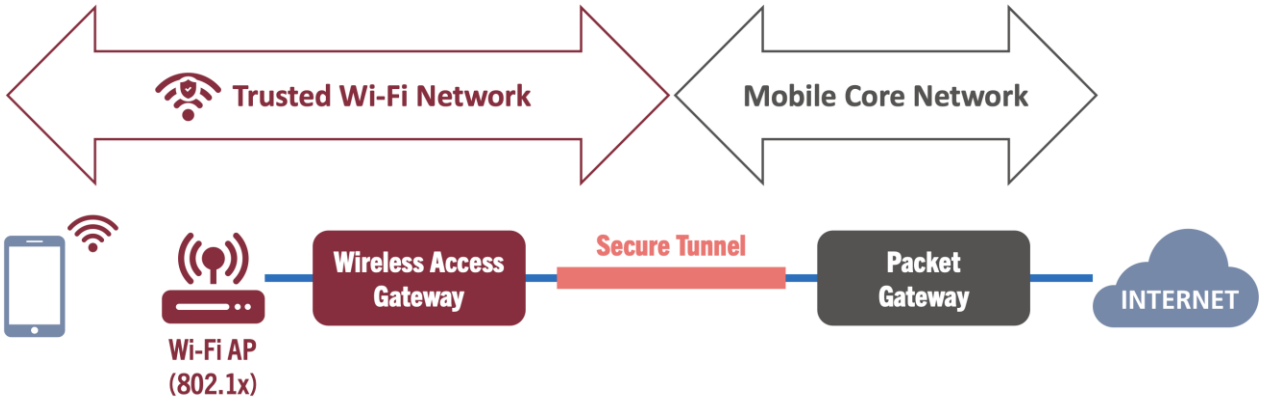
The untrusted model requires no changes to the Wi-Fi network but has an impact on the device side because it requires an IPsec client to be reside on the device. The device is connected through a secure IPsec tunnel directly to an IPsec Terminating Gateway in the Mobile Core, which in turn is connected through an encrypted tunnel to the Packet Gateway. The Packet Gateway is used for both cellular and Wi-Fi traffic.

This integration on the core network side also means that Wi-Fi service management platforms, such as the Aptilo Service Management Platform™ (SMP), must interface with mobile core network HLR/HSS/AMF for SIM Authentication (EAP-SIM/AKA/AKA' or 5G-AKA). This provides the same level of authentication security as in the cellular network. It may also be a requirement to interface towards mobile core network policy functions. In addition to authentication of the device, the SIM authentication process produces cryptographic keys. These keys are used for IPsec tunnel establishment and for encryption in the secure Wi-Fi network (802.1x).

Trusted non-3GPP (Wi-Fi) Access

Trusted non-3GPP (Wi-Fi) access was first introduced with the LTE standard in 3GPP Release 8 (2008). Trusted access is often assumed to be operator-built Wi-Fi access with encryption (enabled by 802.1x) in the Wi-Fi radio access network (RAN) and a secure authentication method (EAP). However, it is always up to the home operator to decide what is to be considered trusted.

In the case of trusted access, the device (UE) is connected through a Wireless Access Gateway in the Wi-Fi core. This Wireless Access Gateway is in turn connected through a secure tunnel directly with the Packet Gateway, used also for cellular traffic, in the Mobile Core.



Trusted and Untrusted Wi-Fi Network Integration to 5G Core

Let us now focus on the new architecture for integration with 5G Core (5GC). Go here for more information about the integration options for the 3G and 4G Core.

Standardization and network technology history tells us that not all functions in a standard will be deployed in real networks. They will not be implemented by vendors and service providers unless there are good commercial reasons for it.

The 3G and 4G versions of Wi-Fi data plane integration is a good example of this. The vast majority of mobile operators have focused on local break-out of Wi-Fi traffic from their secure Wi-Fi networks (802.1x).

With no operational rationale or commercial reasons to back-haul Wi-Fi traffic to the Mobile Core operators have opted to use secure SIM-based authentication, sometimes combined with policy control from the Mobile Core. There is no reason to exert extra load on the Mobile Core when all required policies for Wi-Fi can be applied locally.

Device manufacturers also control much of what is possible and implemented. It took almost 10 years for device manufacturers to decide to implement the IPsec client needed for untrusted Wi-Fi access. In their view it simply took that long for a good commercial reason to materialize.

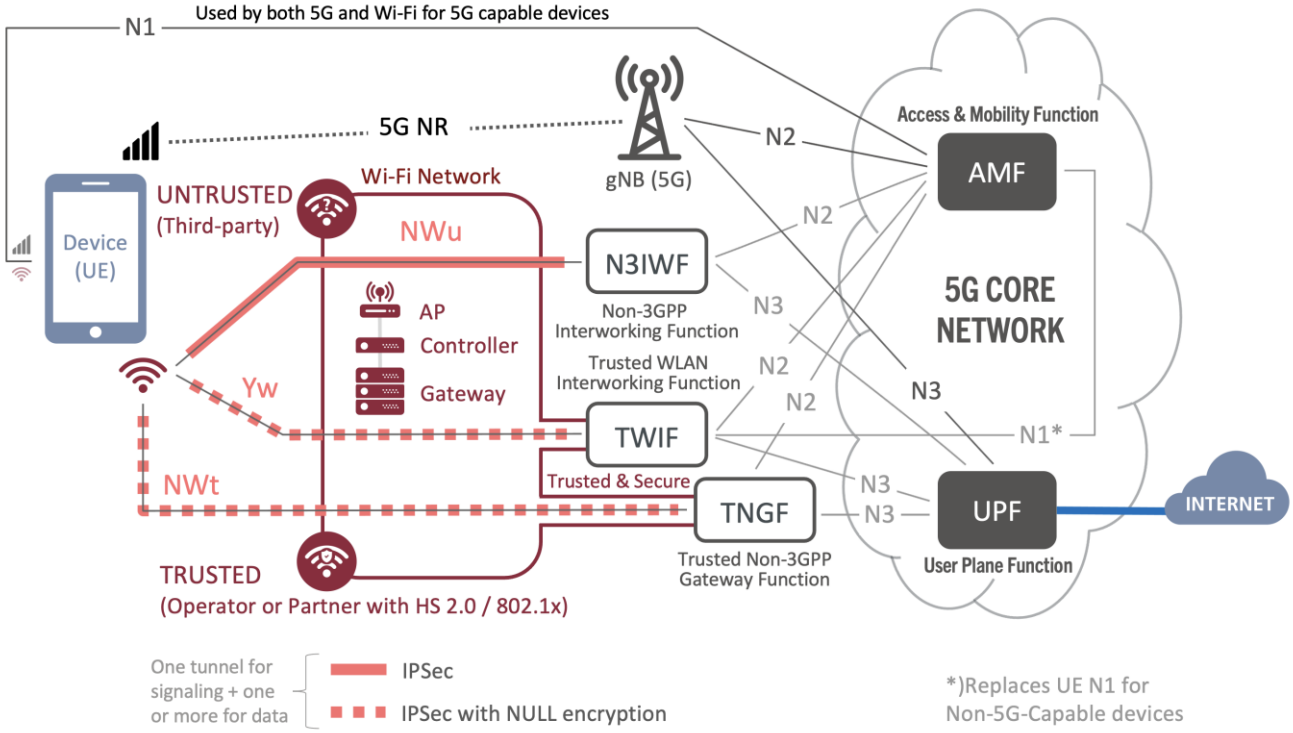
This reason came in the form of Wi-Fi Calling, which was in their own and their customers' best interest.

So, are operators likely to implement the 5G 3GPP standards for Wi-Fi access in the future? We believe so, and there are a few reasons for that. But such implementations will take time. First - as already discussed in this paper - operators more than ever need to embrace Wi-Fi in the 5G era. Secondly, a new breed of carrier grade Wi-Fi (Wi-Fi 6) is here. Thirdly, the new Access Traffic Steering, Switching & Splitting (ATSSS) 3GPPP standard will finally give operators a good reason to backhaul traffic to the Mobile Core.

Function	3G	4G	5G
Wireless Access Gateway	WAG	TWAG	TNGF
IPsec Termination	TTG	ePDG	N3IWF
Packet Gateway	GGSN	P-GW	UPF

Note that these are just "functions" and may be delivered as one combined solution, deployed as containerized functions, or the same virtual or physical gateway node."

TRUSTED AND UNTRUSTED WI-FI INTEGRATION TO 5G CORE



The simplified diagram shows Wi-Fi service integration with new service-based 5G Core (5GC) introduced in 3GPP release 15 (untrusted) and 16 (trusted).

The first thing to observe is that this architecture is Radio network (RAN) agnostic since both the Cellular and Wi-Fi access are using the same interfaces (N1-N3).

The N1 is a control plane interface between the device (UE) and the Access and Mobility Function (AMF). It is primarily used to transfer information about the connection, mobility, and session from the UE to the AMF.

This interface is used both for Cellular and Wi-Fi (for 5G Capable Devices) and it is physically transported the same way to the AMF as shown by the N2 interface.

The N2 is the control plane interface between the access network and the 5G Core. It is primarily used for connection management, UE context and Protocol Data Unit (PDU) session management, and UE mobility management.

The N3 is the data plane interface between the access network and the User Plane Function (UPF) in the 5G Core. The UPF is the packet gateway transporting data to the internet.

For Cellular, N2 and N3 connect the base station (gNB) with the AMF. For Wi-Fi, they connect the non-3GPP interworking and gateway functions (N3IWF, TNGF, TWIF) with the AMF.

5G introduces a new principle for non-3GPP access: Simultaneous connections via cellular and Wi-Fi are now possible by using multiple non-access stratum (NAS) connections over the N1 interface. This is a prerequisite for the new ATSSS standard and the same authentication procedures, EAP-AKA' and 5G-AKA, are used for both Cellular and Wi-Fi.

A new protocol, EAP-5G has been introduced in order to support NAS messages over Wi-Fi networks. The IKEv2 and EAP-5G protocols are used to establish an IPsec tunnel for signaling during the registration procedure between the device and the interworking and gateway functions. The EAP-5G protocol is then used to encapsulate NAS messages over the IKEv2 protocol.

Another interesting new principle is the use of IPsec also for trusted Wi-Fi networks. Why would you want to use an IPsec connection - albeit with null encryption to avoid double encryption - in a secure Wi-Fi network? It turns out that implementations in devices and gateways with dual support for both trusted and untrusted access will probably be easier to implement in this case. Add to this the benefits of a fixed anchor point in the Mobile Core to facilitate mobility and ATSSS.

Let's now examine the new functions for non-3GPP access. Again, please note that these functions are not the same thing as physical gateways. In practice, these functions could all reside in the same gateway.

The control plane (N1-N2) could also be provided by one vendor while the data plane (N3) is provided by another.

The Non-3GPP Interworking Function (N3IWF) is the IPsec tunnel terminating node for 5G similar to the ePDG for integration with the 4G Core. It is located in the Mobile Core and communicates with the Access and Mobility Function (AMF) control plane over the N1 and N2 interface. For the data plane it communicates with the User Plane Function (UPF) over the N3 interface.

The trusted non-3GPP Gateway Function (TNGF) is for 5G the equivalent to the Wireless Access Gateway (WAG) used for trusted access to the 4G Core. The TNGF is located in a trusted environment, often the Wi-Fi network, and communicates with the Access and Mobility Function (AMF) control plane over the N1 and N2 interface. For the data plane it communicates with the User Plane Function (UPF) over the N3 interface. As discussed, the device and the TGNF is connected using an IPsec tunnel with null encryption.

The trusted WLAN Interworking Function (TWIF) is a new 5G function for interoperability with legacy devices. This is to resolve the contingency that some devices may support 5G SIM authentication but do not support 5G NAS signaling over trusted Wi-Fi access. These devices lack the support for the EAP-5G and IKEv2 protocols. 3GPP refer to such devices as non-5G-Capable over WLAN (N5CW). The TWIF contains the NAS protocol stack and exchanges NAS messages with the AMF on behalf of this type of devices.

The TWIF is located in a trusted environment, often the Wi-Fi Network, and communicates with the Access and Mobility Function (AMF) control plane over the N1 and N2 interface. For the data plane it communicates with the User Plane Function (UPF) over the N3 interface.

Just as in the case of TNGF, the device is connected with the TWIF using an IPsec tunnel with NULL encryption.

Opportunities for the future: Smarter connectivity – ATSSS

The new Access Traffic Steering, Switching & Splitting (ATSSS) function is the 'Holy Grail' of mobile data offloading, but its complexity and reliance on device support means it will likely take years to come to market.

Will new and better technology and standards for automatic network selection and intelligent convergence between mobile and Wi-Fi services be developed for the mass market of the future? The short answer is probably yes. We will address one of them here, namely the newly released Access Traffic Steering, Switching & Splitting (ATSSS) as introduced in 3GPP release 16.

But the answer is also that for the most part such technologies - including Passpoint with SIM authentication - already exist. These may not be ideal but are still extensively field-proven and work well enough to have already been implemented by dozens of major carriers.

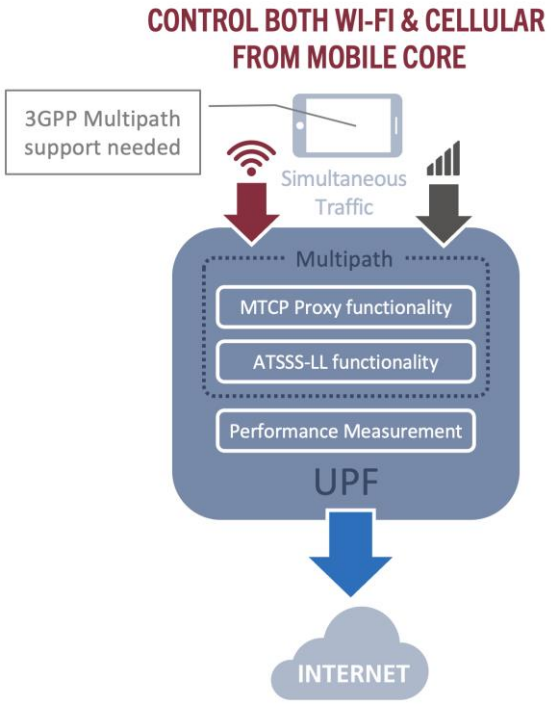
Operators actively choosing Wi-Fi offload as a strategy and who want more granular control, often include so-called connectivity manager clients (apps or hidden clients) on the device. Such solutions can be quite sophisticated depending on to what extent the app, and hence the operator, can access and control the communication layer in the device's operating system.

The capability of such apps or hidden clients must include at least the solutions to the following current imperfections in switching between Wi-Fi and mobile network access:

- Avoiding unintentional 'walk-by' switchover to public Wi-Fi which could produce a poor user experience or even intermittent loss of connectivity.

- Policies and thresholds should automatically reject or accept handoff to Wi-Fi and/or back to cell sites if either is congested.

ATSSS – Smarter Connectivity Natively in Device



Wouldn't it be a great step up in performance and quality of experience if a phone natively could aggregate the data streams from Wi-Fi and cellular into one stream and perhaps even intelligently steer and switch traffic between the two?

We think yes - and fortunately, the 3GPP seems to think so as well since they have introduced ATSSS as part of the 3GPP Release 16 standard for 5G.

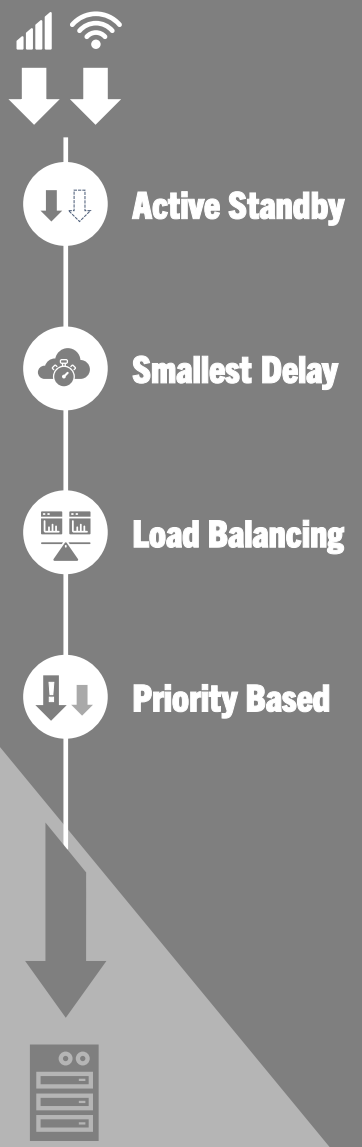
ATSSS uses the so-called Multipath TCP (MPTCP) technology described earlier to allow IP data traffic to flow simultaneously over Wi-Fi and 5G networks. The results are higher data rates, much improved quality overall, and even gapless handovers between Wi-Fi and 5G. Since very few application and web servers supports MPTCP, the ATSSS specifies a MTCP Proxy implemented in the 5G core User Plane Function (UPF). It also specifies a ATSSS low layer functionality (ATSSS-LL) to support other protocols such as UDP.

The introduction of ATSSS is very good news for advanced Wi-Fi service management platforms such as Aptilo SMP, as it makes policy management so much more complex.

Let's examine the three "S" in ATSSS:

- **Steering:** Choosing the best available network based on speed, cost and latency.
- **Switching:** Moving seamlessly between 5G and Wi-Fi networks.
- **Splitting:** Splitting the traffic over 5G and Wi-Fi, the split can be set by policies.

ATSSS Steering Modes



These functions, the three “S”, translate to four ATSSS standard steering modes that need to be supported in the device and in the Mobile Core (UPF).

Active Standby: One access network - cellular or Wi-Fi - is the active (default) access network. The traffic is routed over this access network until it becomes unavailable, in which case traffic switches over to the other access network. When the active access network is available again, the traffic is switched back.

Smallest Delay: Traffic is sent over the access network with the smallest delay. The Performance Measurement Function (PMF) determines the latency of each network connection. The underlying multipath protocol can also provide measurements.

Load Balancing: This specifies a fixed percentage for the fraction of the traffic that should connect over the 3GPP network with the rest of the traffic sent on the non-3GPP network. This mode only applies to QoS flows with non-guaranteed bit rate (non-GBR).

Priority Based: Traffic is transmitted over a specified high priority access network (Wi-Fi or cellular). If this access network becomes congested, the traffic overflows onto the other access network. If the high priority access network becomes unavailable, traffic switches to the other access network (as in Active Standby). The determination of congestion is implementation specific.

Another factor that adds to the complexity in policy management is the large number of stake holders. A real-world deployment of ATSSS will need to cater to:

- Service provider policies
- Policies set by the user
- Device vendor policies
- App provider policies
- Enterprise IT policies

We think that ATSSS is a very promising standard. It is at some extent the ‘Holy Grail’ of mobile data offload and with ATSSS, operators may finally find a good reason for backhauling Wi-Fi traffic all the way to the mobile core.

No Reason To Wait for ATSSS

But for ATSSS to reach mass market, device support is crucial. An example of a related standard that never achieved any market penetration at all is 3GPP ANDSF, which was a useful concept but in the end was never implemented natively in any device.

It may take quite a few years more for ATSSS to come to market – or alternatively, proprietary forms of largely the same function incorporated by Apple or others may in the end supersede the 3GPP's attempts. The ATSSS concept has already been tested successfully by Korea Telecom using a proprietary solution.

In either case there is a good likelihood that Wi-Fi and 5G data streams will find new ways of complementing each other - including using aggregation & gapless handovers - on the transport layer.

Meanwhile all the benefits of known and field-proven systems for cellular and Wi-Fi convergent services, remain available to any operator who wishes to apply vastly improved Wi-Fi technology as a part of their network strategy today. Passpoint and EAP-SIM based solutions are readily available and can possibly be complemented with an app for more granular control. In other words: Even though a more systematic 3GPP-based approach to convergence may emerge in coming years, there is no reason to wait. Excellent convergence solutions exist today.

Opportunities are here today!

SUMMARY

Wi-Fi & Cellular Convergence

- **Mobile and fixed networks are coming together**
  - More recently fixed service providers and cablecos have either acquired mobile operators or have become MVNOs themselves.
  - Convergence opportunities do not need big infrastructure investments nor need to wait for new 3GPP standards or equipment.
- **But we have overcapacity in our cellular network…**
  - That statement will only be true on average as there will always be service areas suffering from congestion and bad coverage.
  - Selective Wi-Fi offload is the answer. Operators are advised to add a secure 802.1x SSID across their Wi-Fi networks and to actively build secure Wi-Fi at congested locations and for indoor coverage.
- **Two standard options for non-3GPP (Wi-Fi) Access – with backhauling to mobile core**
  - **Untrusted:** A secure IPsec tunnel is established between the device and a gateway in the mobile core.
  - **Trusted:** The device is in a trusted secure Wi-Fi network, connected with the mobile core through a trusted gateway.
- **Standards will only be implemented if there are good commercial reasons for it**
  - Most mobile operators today are using SIM authentication and then just non-standard local break-out and policy control.
  - The non-3GPP access which backhauls traffic to the mobile core is mainly used for Wi-Fi Calling, using the untrusted method.
- **New concepts for non-3GPP (Wi-Fi) Access in 5G**
  - 5G is built to be radio (RAN) agnostic. Wi-Fi interworking nodes use the same interfaces to mobile core as 5G base stations.
  - IPsec tunnels are used also for trusted non-3GPP (Wi-Fi) access, but they are null encrypted.
  - The new Access Traffic Steering, Switching & Splitting (ATSSS) is the ‘Holy Grail’ of mobile data offloading, but its complexity and reliance on device support means it will likely take years to come to market. ATSSS is using Multipath TCP to provide simultaneous and optimal connectivity over Wi-Fi and cellular.

6

Enea is one of the very few vendors offering solutions both in the Wi-Fi and 5G domain. This allows us to serve our carrier customers even better and with a unique value proposition.

Enea Solutions for Wi-Fi and 5G

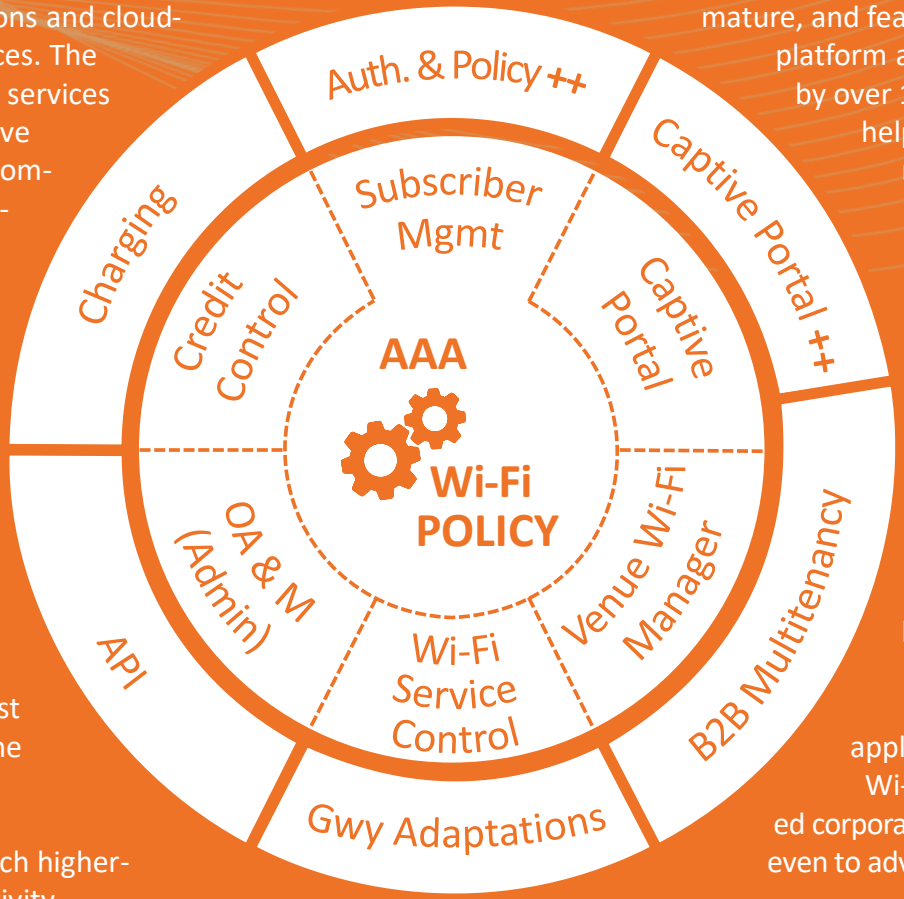
Enea business unit Aptilo – Solutions for Carrier Wi-Fi

Aptilo Networks is one of the world's leading providers of Wi-Fi service management solutions and cloud-based IoT connectivity control services. The company has delivered software and services to more than 100 operators that serve tens of thousands of enterprise customers, and hundreds of millions of end-users and devices.

In October 2020, Aptilo was acquired by Enea one of the world's leading suppliers of innovative software for telecommunication and cybersecurity.

Aptilo has for two decades been the industry's leading provider of carrier-class Wi-Fi service management solutions. In this section we give an overview of some of the most important solutions we provide in the Wi-Fi space.

As a new era of much faster and much higher-quality Wi-Fi 6 and Wi-Fi 6E connectivity approaches , the good news is that a field-proven, mature, and feature-rich Wi-Fi service management platform already exists. This platform is trusted by over 100 service providers and is ready to help you convert any or all of the aforementioned new Wi-Fi service opportunities into profitable, commercial reality. It is called the Aptilo Service Management Platform - or simply the Aptilo SMP™ - and it forms the core of all Aptilo carrier-class Wi-Fi solutions.



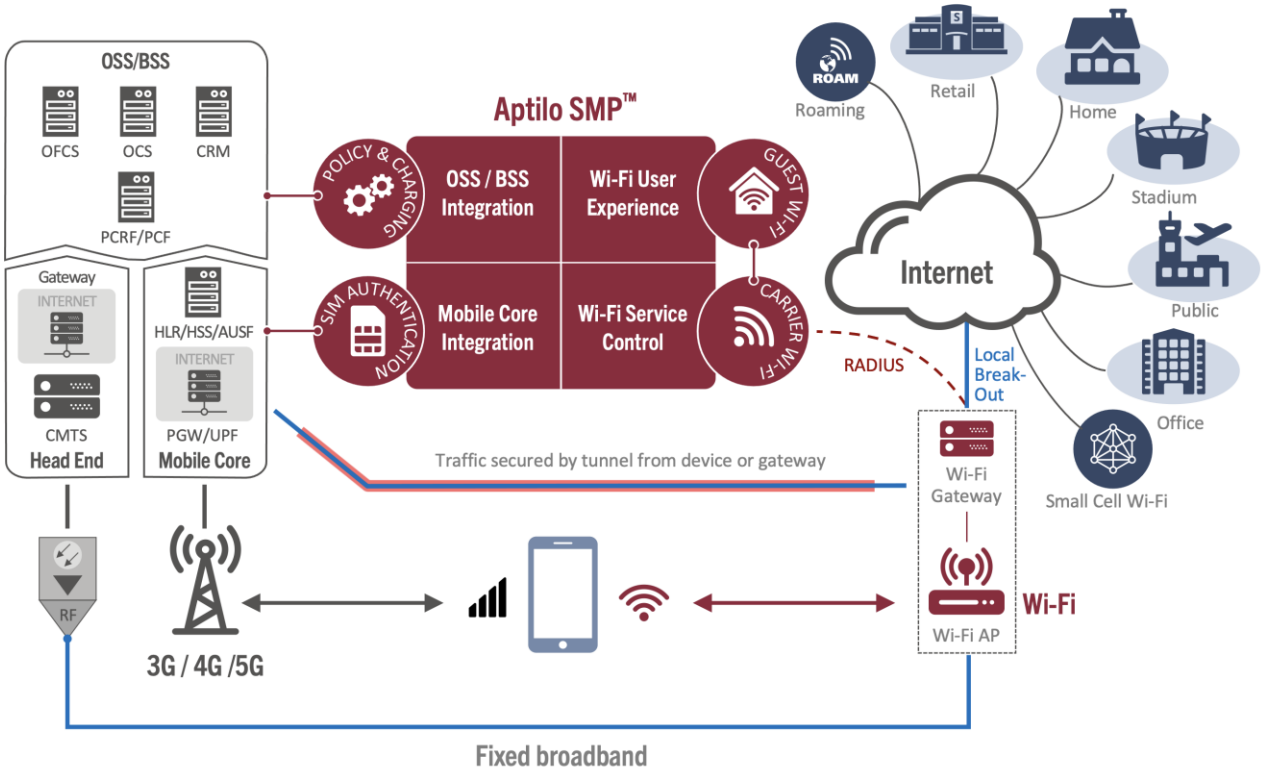
The Aptilo SMP - which includes a AAA, a policy server, a subscriber management module, captive portal management, charging, analytics, and more – has been designed to serve as a highly scalable carrier-class Wi-Fi services platform. It will apply equally well to multitenancy guest Wi-Fi use cases for enterprises, managed corporate Wi-Fi, carrier Wi-Fi offloading, and even to advanced IoT connectivity management.

Aptilo SMP™

Aptilo SMP is vendor agnostic so that you are free to select any or any combination of your preferred Wi-Fi AP vendors for your Wi-Fi projects - and in the process even apply a competitive bid process to drive down Wi-Fi AP costs. Here is a brief overview of how the Aptilo SMP becomes your primary tool capable of addressing many of the new Wi-Fi business opportunities detailed in this paper:

Aptilo SMP with SIM Authentication is the mobile offload function that allows carriers to authenticate and offer Wi-Fi access to mobile subscribers based on credentials stored in their SIM cards. Aptilo SMP also offers all the service management functions required to deliver fully compliant Passpoint network services. It is also possible to perform integrations towards core network policy functions and OSS/BSS subsystems.

Aptilo SMP Venue Wi-Fi Manager comprises everything you need to create and manage compelling carrier-class B2B Wi-Fi services for thousands of business customers from the same scalable platform. This includes multi-tiered management of networks, locations, captive portals, user flows, Wi-Fi analytics, marketing functions as well as a host of authentication and payment options. It is also possible to add our award-winning and



GDPR compliant functionality for personal data and consent management.

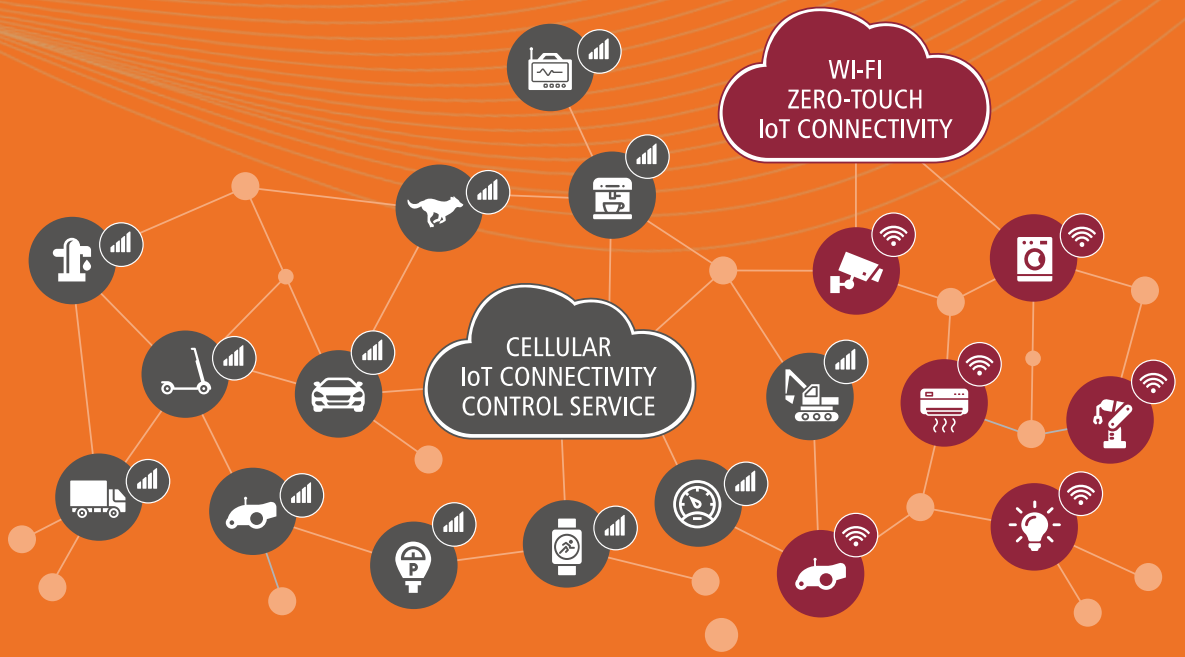
Aptilo Virtual Service Provider solution provides service providers with a highly standardized and scalable way to sell managed corporate LAN and Wi-Fi services. B2B clients become 'virtual service providers' (VSPs) and will themselves serve their tenants across many physical locations. Service providers can leverage one infrastructure and one SSID while still allowing each of their B2B customers to act as Virtual Service Providers, managing daily operations towards their own business or residential customers (tenants). Tenants get their own private Wi-Fi networks with secure access to internal networked resources such as printers and servers, just as if they had their own network. Ideal Virtual Service Provider examples include real estate owners, co-working offices, apartments (MDUs), and shopping malls.

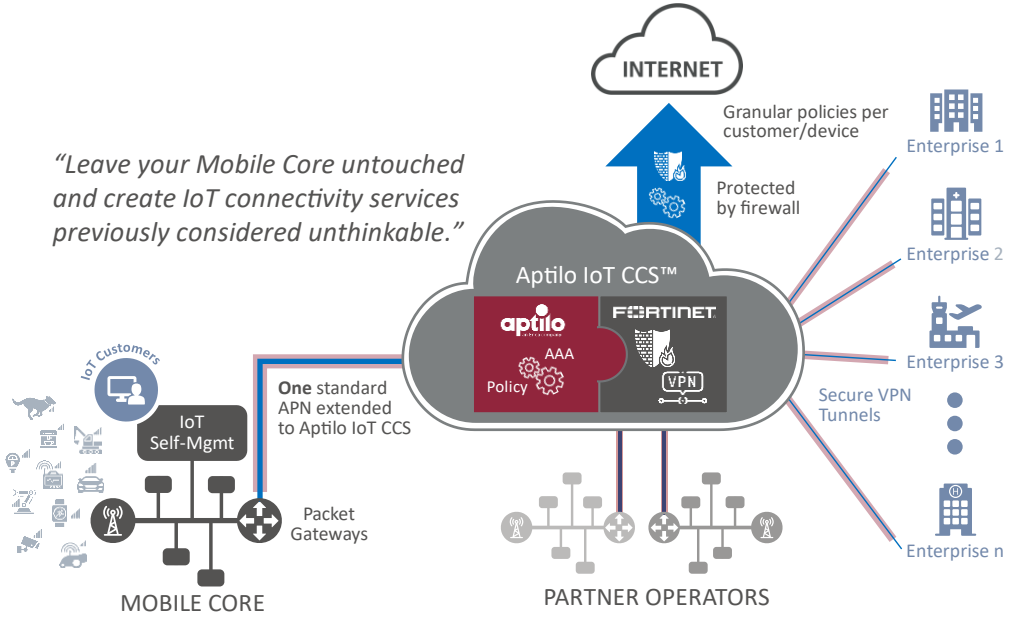
All functions mentioned above feature a high degree of B2B customer self-management.

Enea business unit Aptilo – Solutions for IoT Connectivity

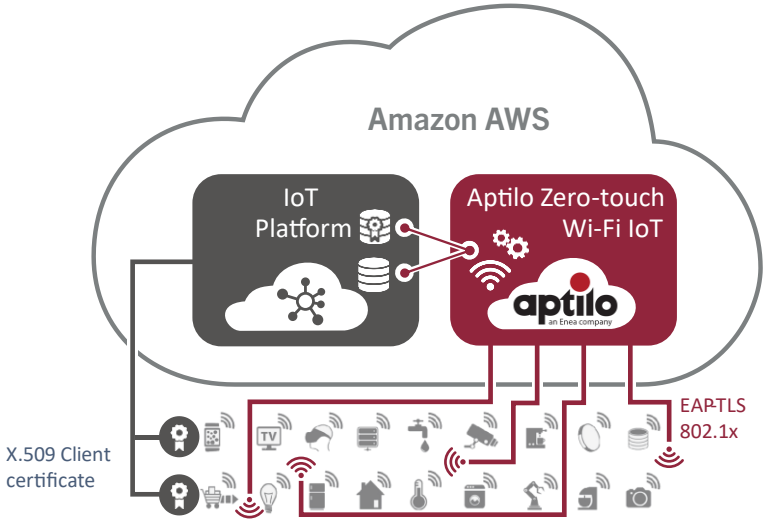
Aptilo has been closely associated with Wi-Fi so it is a lesser-known fact is that the flexible policy engine of the Aptilo SMP also can be applied as a policy function (PCRF) for cellular networks. One such example is the operator Hutchison 3 Scandinavia: Since 2012 they have been using the Aptilo SMP to control services for their 2.2 million subscribers.

We have also leveraged this capability to create ground-breaking IoT connectivity control solutions for both cellular- and Wi-Fi-based IoT. In this area we are primarily offering our solutions as cloud-based services on Amazon AWS.





"Leave your Mobile Core untouched and create IoT connectivity services previously considered unthinkable."



Aptilo IoT Connectivity Control Service™ (IoT CCS) is a unique cloud-native solution from Enea. It adds a flexible layer of IoT security and policy control on top of any mobile infrastructure. Delivered as a service on Amazon AWS, mobile operators can go beyond traditional IoT connectivity and provide secure, unified and programmable global IoT connectivity. They can allow customers to control authentication, security, policies and global connectivity from a single user interface. Manual setup of a secure private connection (APN) typically takes weeks. With Aptilo IoT CCS multitenancy virtual APN in place, enterprises can create their own APN connections in a matter of minutes.

Aptilo Zero-touch Wi-Fi IoT Connectivity™ uses existing device certificates to auto-authenticate and connect Wi-Fi IoT devices to a Wi-Fi network. Devices will securely auto-connect to the Wi-Fi network when switched on for the first time and will continue to auto-connect as required. The solution interfaces with IoT platforms, currently Amazon Web Services (AWS) IoT Core, for access to databases with x.509 certificates, used for secure management of the device. If the certificate matches, the device is granted access to the secure 802.1x Wi-Fi network through EAP-TLS authentication. A prerequisite is that the device is trying to connect to a ZeroTouch SSID or Passpoint service. Aptilo is actively working with IoT chipset vendors such as Esspresif to implement this as a default feature.

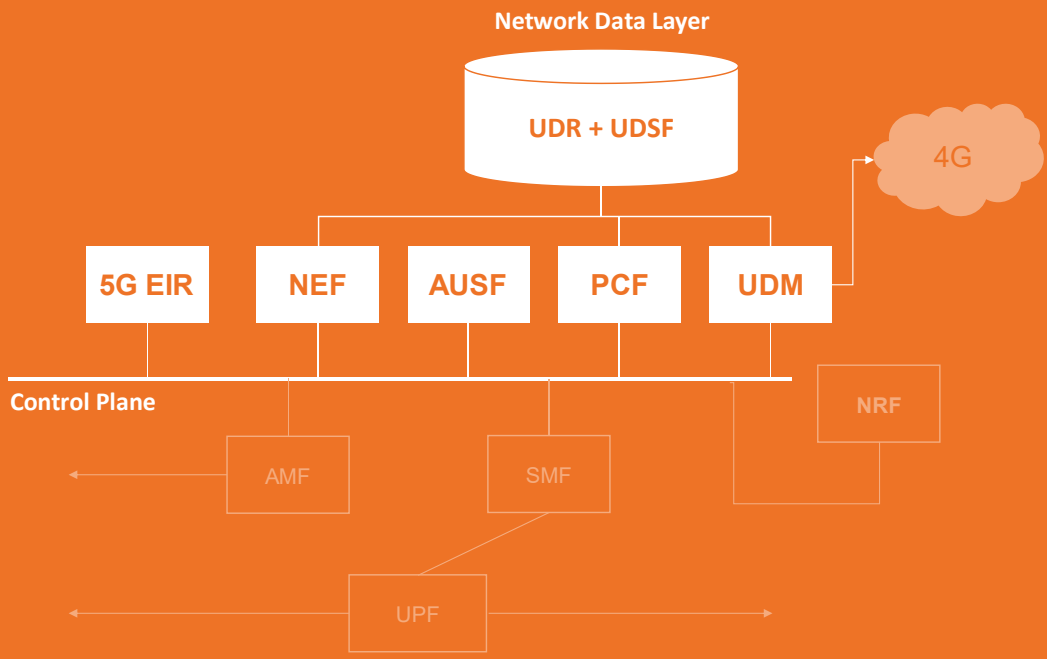
Enea 5G Solutions

Avoid vendor lock-in with the cloud-native 5G functions from Enea.

Enea's complete 5G Data Management portfolio stores and manages data across all 5G core and edge functions, supporting multi-vendor 4G/5G interworking. Our cloud-native suite spans the common network data layer (NDL), scaling the control plane with critical 3GPP functions including UDM, UDR, UDSF, AUSF, PCF and EIR.

The platform agnostic architecture provides support for any PaaS, private cloud, and public cloud deployment.

With Private 5G networks fueling a dramatic growth in Industry 4.0 and related initiatives, the demand for 5G core solutions with smaller footprint, faster deployment and proven track-record has never been greater. To address this market Enea offers the *Enea 5G MicroCore*.



5G Network Data Layer that solves the problem of vendor lock-in

Enea Stratum - Cloud Native 5G Network Data Layer (UDR | UDSF)

Stratum provides a cloud native data manager built for 5G, NFV and IoT. It provides performance and scale required to build telco clouds that can deliver low latency applications & services, scale to billions of devices and integrate with the Internet Ecosystem using secure REST APIs. Stratum solves the problem of vendor lock-in by collapsing all your vendor data silos into one common Network Data Layer.

Stratum is a foundation on which to deliver best in class network functions for 4G and 5G; it enables local and edge deployment providing standard 3GPP UDR/UDSF capability with hybrid storage options for all types of data.

Stratum scales on demand, consistently delivering performance and resilience (offering six 9's reliability on three 9's x86 hardware). 3GPP Network functions and existing applications can be easily on-boarded to access any data, anywhere, anytime.

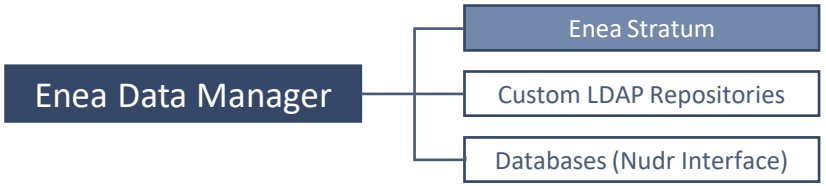
Enea Unified Data Manager (UDM)

The Enea Unified Data Manager (UDM) is a hardware-agnostic, cloud-native network function for 5G and 4G data management. The software performs the 3GPP functions of Unified Data Management (UDM) in 5G networks and interoperates with any Home Subscriber Server (HSS) in 4G. The solution is a critical component in multi-vendor and multi-generation network architectures, reflecting the call for a highly automated and open architecture, thereby, providing subscriber keys for authentication and encryption of all user equipment.

As a key solution, UDM is redefining both networking and data management. Enea UDM provides authentication credentials, user identification, access authorization, registration, and subscription management.

It allows seamless services for converged consumer broadband, IoT apps at the edge, and for private networking with true cloud-native apps in an externalized state.

Support for Backend Systems



Cloud-Native Management of 5G and 4G Subscriber Data

Enea 5G Policy Control and AAA

Enea Policy Manager (PCF)
Enhanced Subscriber and Device Experiences with Full Control of Network Utilization

The Enea Policy Manager is an independent, best-of-breed software product providing the functionality of the 5G Policy Control Function (PCF) as standardized by 3GPP. It manages QoS, gating and charging for all voice, broadband data and IoT use-cases. Both static and dynamic policies allow the service provider to quickly implement their business logic in an easy manner, ranging from simple to most complex scenarios without limits. With the integrated Policy Builder new uses-cases can be defined easily, leading to a significantly improved time-to-market.

The cloud-native Policy Manager can be deployed in containerized and virtualized environments and configurations including geo-redundancy. The 5G PCF is a fully cloud-native product.

The Enea Policy Manager can be deployed as a 4G PCRF or a 5G PCF or a combo-node consisting of both allowing a smooth transition from 4G to 5G.

Enea Access Manager
Authentication and Authorization on Cloud Scale for all System Generations and Access Networks

The Enea Access Manager provides the AAA and AUSF functions in 4G and 5G networks respectively, with authentication and service access capabilities. The highest standards of security and reliability are essential for cloud-native solutions and provided with this product. The Enea Access Manager is cloud native from initial design and builds on more than 15 years' experience delivering subscriber applications to Tier 1 network operators. With an architecture optimized for virtualization and cloud deployments, the Enea Access Manager provides the high availability and scaling capabilities required for 5G services.

It also supports all use cases based on 4G and Wi-Fi access.

Enea 5G Equipment Identity Register (5G-EIR)
The Enea 5G-EIR is a key solution for authentication of mobile devices in the network, including IoT devices preventing misuse of network and abuse of paid services. The 5G-EIR is an independent network component coupled via Service Based Interfaces (SBI) that helps telecom operators protect their networks. As a solution, it provides a mechanism to restrict malicious user terminals in a mobile network. For operators the solution allows separation of devices and contracts. So, when a listing needs to be done based on a request, the Enea 5G-EIR blocks only the device, rather than blocking all services to a subscriber. Through this way, subscribers can enjoy use of their paid services across their other devices, adding to trust of subscribers towards the operator.

SUMMARY

Enea Solutions for Wi-Fi and 5G

Unique value proposition in the 5G era

- Enea is one of the very few vendors offering solutions both in the Wi-Fi and 5G domain. This allows us to serve our carrier customers even better and with a unique value proposition.

Enea business unit Aptilo - Solutions for Carrier Wi-Fi

- The Aptilo Service Management Platform™ (SMP) is trusted by over 100 service providers and is ready to help you convert any or all of the aforementioned new Wi-Fi service opportunities into profitable, commercial reality.
- Aptilo SMP covers everything from SIM authentication and solid integration with the mobile core to multitenancy functions for B2B Wi-Fi which is essential to gain Wi-Fi footprint for 5G indoor coverage.

Enea business unit Aptilo - Solutions for IoT Connectivity

- Aptilo SMP also works as a policy function (PCRF) for cellular networks, one example is the operator Hutchison 3 Scandinavia.
- We leverage this capability to create ground-breaking IoT connectivity control services on AWS, for both cellular- and Wi-Fi.
- The Aptilo IoT CCS service for MNOs adds a flexible layer of IoT security and policy control on top of any mobile infrastructure.
- Aptilo Zero-touch Wi-Fi IoT Connectivity™ uses existing device certificates to auto-authenticate and connect Wi-Fi IoT devices.

Enea 5G Solutions

- Enea offers 5G functions both in the *Network Data Layer* (UDR + UDSF) and in the *Control Plane* (5G EIR, NEF, AUSF, PCF, UDM)
- Avoid vendor lock-in with the cloud-native 5G solutions from Enea which offers a clear separation between the network data layer and applications. Platform agnostic architecture that supports any PaaS, private cloud, and public cloud deployment.

ENEA

aptilo an Enea company | CARRIER WI-FI

About Aptilo Networks

Aptilo Networks, an Enea company, is one of the world's leading providers of Wi-Fi service management solutions and cloud-based IoT connectivity control services. The company has delivered software and services to more than 100 operators that serve tens of thousands of enterprise customers, and hundreds of millions of end-users and devices.

WWW.APTILO.COM

About Enea

Enea is one of the world's leading suppliers of innovative software for telecommunication and cybersecurity. Focus areas are cloud-native, 5G-ready products for data management, mobile video traffic optimization, edge virtualization, and traffic intelligence. More than 3 billion people rely on Enea technologies in their daily lives.

Enea is headquartered in Stockholm, Sweden, and is listed on Nasdaq Stockholm.

WWW.ENEA.COM