NETWORK PROVIDER WI-FI
– THE WHOLESALE BUSINESS MODEL

APTILO NETWORKS WHITE PAPER

By Anders Emilsson, VP Sales EMEA

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Managed Wi-Fi is an unexploited business opportunity for service providers and network providers. There is a growing trend worldwide where more and more service providers, network providers and enterprises are deploying managed Wi-Fi services for their subscribers and guests to use when visiting venues and when travelling.

This paper will explain how a network provider can leverage their ownership of a Wi-Fi network by selling wholesale services to service providers and enterprises.

Plenty of network providers have deployed successful Wi-Fi networks and developed innovative business models the last few years, in all parts of the world. The regional cable and fixed-line operators in North America have developed a cooperative business model by sharing their common Wi-Fi "assets." Network providers in Europe, Africa and Asia are launching "neutral" wholesale networks in their respectively markets.

A Wi-Fi network is a great asset for doing sustainable business with service providers and enterprises by offering wholesale services. The business models, actors, go-to-market strategies and service offerings will be explored further in this white paper.

1 BUSINESS MODEL

The business model of public Wi-Fi involves several actors, where the original source of revenue is either the consumer who pays to use the Wi-Fi service, or the enterprise or venue owner who uses Wi-Fi to attract customers, guests and visitors to spend time at their venue. Public Wi-Fi access may also be financed by online marketing where commercial products are promoted through the web portal, e-mail, SMS or an app.

The network provider owns the network and has invested in infrastructure and site acquisition for several years in order to build good coverage at relevant places. The network provider will sell network capacity to service providers and enterprises that, in turn, sell or give Wi-Fi access to their subscribers, guests and visitors.
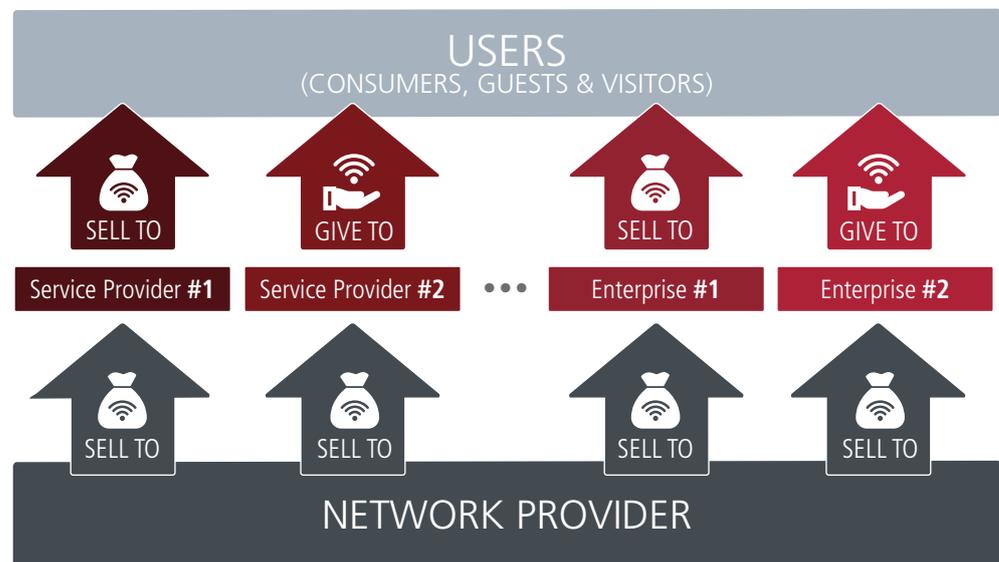

Figure 1. The business model and business relationship

A key success factor is to offer the end-user an attractive, relevant and intuitive experience when they access the Wi-Fi service. Users tend to otherwise abandon Wi-Fi, which will limit the uptake.

The user will normally login to public Wi-Fi through the device browser and a captive portal. This login process is a great opportunity to engage the user with a relevant message and/or survey. These messages and the portal design may be tailored to each location and/or location type. The portal design and content may either be controlled by the network provider, the service provider or the venue owner (enterprise).

Users may also login automatically through a secure SSID (802.1x). We will see more of this as Hotspot 2.0 with Passpoint certified devices and access points become more commonplace. The need for the user engagement possibilities mentioned above will however remain the same.

2 THE USER

People today have their devices always connected, and expect the connection to work flawlessly at home, in the office and on the road. They also have more than just a smartphone, often carrying a laptop and a tablet that are non-SIM devices as well. Wi-Fi is key to giving users a high performing and reliable internet connection, devices are therefore designed to always prefer Wi-Fi before any other network technology.

Guest Wi-Fi needs to be available at venues for visitors, travelers and guests to enjoy the time they spend at the venue. Users do not care how and from whom they get Wi-Fi access. They just use the best and easiest connection to internet they can find.

2.1 THE USER EXPERIENCE

The user experience is mainly decided by the intuitive and appealing user journey through the captive portal at the time of login, registration and payment. In operator neutral networks, the network provider will always host the initial captive portal page except when the network provider sold a dedicated SSID to the service provider. The network provider's captive portal will present the available services and service providers available at this location and on this SSID.
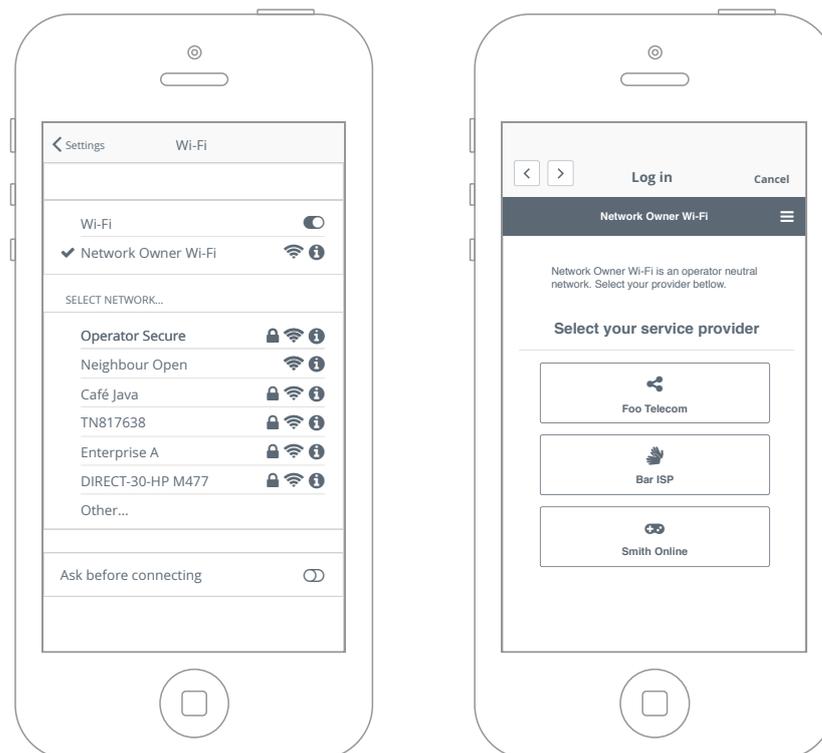

Figure 2. The user selects the network provider's SSID, "Network Owner Wi-Fi," and is thereafter presented service providers who sell services at this location. In this case there are three service providers: Foo Telecom, BAR ISP and Smith Online.

The user will select their "home" service provider with whom the user initially registered their subscription, or a new unregistered user may select temporary internet access which is offered through for instance a bank card or voucher payment.

After selecting the service provider, the user will be directed to the selected service provider's portal page where available services, login methods and registration alternatives are presented.
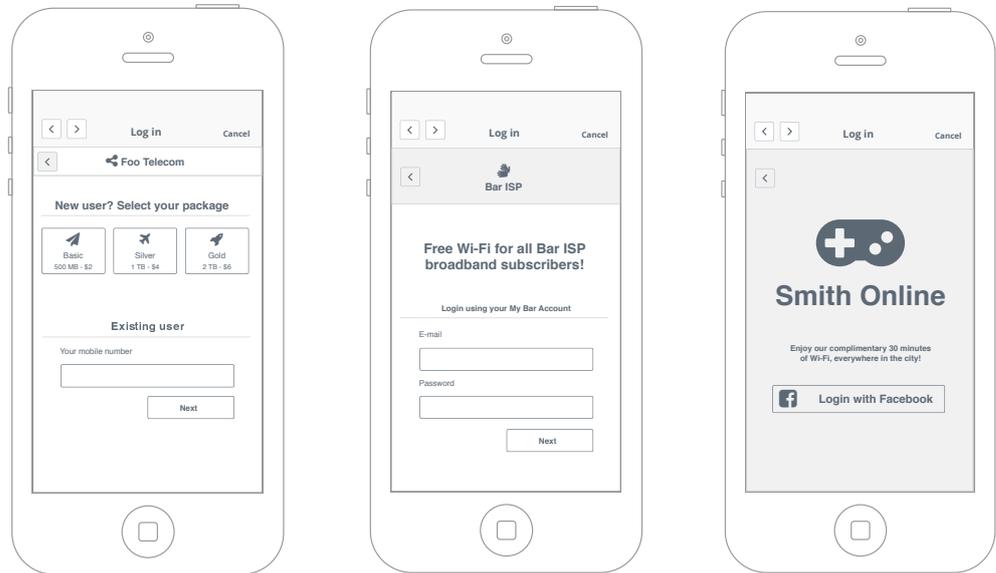
Figure 3. Each service provider will present their respective portal page where available login and payment options are offered to the user.

The user will manually select the login method and, if applicable, insert the login credentials to obtain internet access.

The initiative called "Hotspot 2.0" or "Passpoint" from Wi-Fi Alliance extended with a roaming framework from Wireless Broadband Association (WBA) will enhance the service provider selection to become fully automatic. The user device will, through this new standard, have a predefined service provider set in the preferences and the Wi-Fi network will broadcast a list of all service providers that are available on each SSID. This allows the device to automatically connect to the preferred service provider, even when the Wi-Fi access network is shared between service providers.

Hotspot 2.0 is still not implemented in most Wi-Fi networks and user devices, but is estimated to be broadly deployed within a few years.

2.3 LOGIN METHODS

Users typically rank Wi-Fi services based on their login simplicity, performance and user experience. Price is naturally another metric that is evaluated. When the service is free of charge, i.e. when the venue owner covers the costs just to attract users to spend time at their venue, the user's expectations for simplicity and quality is still the same. Wi-Fi should just be there and it should work!

There are several ways a user may access the Wi-Fi service, and the methods are not only designed for the purpose of the user, but also for the purpose of the venue owner, service provider and network provider to engage with the user to promote relevant and location-based offers and marketing campaigns.

The interests of user engagement and marketing varies between different types of venue owners and verticals. The strongest drive to engage with users through the Wi-Fi service is typically from the retail, hospitality and transportation segments, and from stadiums. The drive from enterprises, institutions and schools to engage with users is less, but it does exist.

The variety of access methods includes the following where one or maximum two methods should be available at a location. Regardless of the access method, the method must be perceived as easy and intuitive to the user, or he will choose other alternatives.

Some methods are designed for maximum user engagement and analytics, while other methods are designed primarily for simple access for the user. Some are designed for user charging and some are for sponsored or promotional access where the venue owner or a sponsor usually pays for the service.

The captive portal is typically branded with promotional information from the venue owner, from the service provider or a mixture of both. Each captive portal may be tailored to each location.

CAPTIVE PORTAL LOGIN METHODS AND THEIR BENEFITS

MANUAL LOGIN. This method is typically used for subscribers who have user credentials through their service provider, often bundled with a mobile subscription or with residential broadband subscriptions. The service is either charged prepaid with online top-up or postpaid through e.g. a monthly invoice.

VOUCHER LOGIN. The service provider or venue owner may sell Wi-Fi access through a printed voucher check, where the user is typically given access to Wi-Fi for e.g. one hour, four hours etc. The user purchases the voucher at Venue reception or in the store.

SMS VALIDATION. This access method is for mobile subscribers who are charged on their mobile phone bill or by mobile quota. It can also be used just to verify the user's identity and to capture their mobile number. The user inputs their mobile number and receives an SMS with a link and a code. The user get access by simply clicking on the link or type the code into the captive portal.

EMAIL VALIDATION. This access method is similar to SMS validation with the link and code distributed through an e-mail rather than an SMS. The user may be charged through a subscription (typically a residential broadband subscription). It can also be used just to verify the user's identity and to capture their e-mail.

CREDIT CARD PAYMENT. Unknown temporary users, who could be any users with local or international residence, may register and purchase temporary access online using a credit card, Paypal or any other online payment method.

FACEBOOK LOGIN. A user may access through Facebook login using their Facebook credentials. This will give the service provider and/or venue owner access to demographic information about the user, extracted from Facebook, to generate a tailored engagement with the user with promotional offers and targeted advertisements. The Wi-Fi access is normally sponsored by the venue owner or service provider.

MICRO SURVEY. A user may click through a micro survey before gaining access to Wi-Fi. This survey will give the service provider and/or venue owner access to information about the user, to engage with the user with relevant offers and directed advertisements. The Wi-Fi access is normally sponsored by the venue owner or service provider.

SPONSORED LOGIN. The user may need to view commercial information such as a short film to be given Wi-Fi access free-of-charge. The access to Wi-Fi is sponsored by this supplier of commercial information.

CLICK & CONNECT. This method is probably the simplest way for the user to access Wi-Fi, but gives the venue owner or service provider no opportunity for any granular marketing campaigns or offerings. This method is typically used at locations where the venue owner pays for the access, e.g. an enterprise or conference location.

3 THE SERVICE PROVIDER

A service provider is an expert in packaging, marketing and selling consumer services, either as private or as business subscriptions. The service provider may naturally also have its own network, but the reason to have its own network is primarily to control the production quality and cost of the consumer services.

A typical service provider could be a cable or fixed-line operator or an internet service provider, or it could be a mobile operator. These operators are working in a highly competitive market where the key metrics to maintain a solid business is the customer churn rate and the ARPU level. Their target is to acquire and keep as large a portion of the consumer market as possible and to keep users at the higher end of the charging plans.

Differentiation is the key to success for operators where service quality, network coverage (mobile operators), price and value-added services are what separate them from "everyone else." Public Wi-Fi as a complement to residential broadband or to mobile data is an attractive value-added service that is commonly used by operators to diversify against competition.

Another example is global service providers like Boingo and iPass who are specialized in offering Wi-Fi services to travellers worldwide and therefore always interested in buying Wi-Fi capacity from network providers.

3.1 MOBILE OPERATORS

Mobile operators are selling mobile voice and data subscriptions to consumers as either prepaid or postpaid. The mobile operator also operates its own mobile macro-network (MNO=Mobile Network Operator) or leases capacity from another mobile operator's network (MVNO=Mobile Virtual Network Operator). Good network coverage, capacity and quality are the core competitive advantages for a mobile operator, combined with their subscription price.

A mobile operator's main cost is customer acquisition. Their business target is to maximize customer uptake and minimize customer churn to competition (churn rate). At the same time, the mobile operator's goal is to maximize average revenue per customer (ARPU) to maintain healthy business margins.

A mobile operator, therefore, always wants to offer improved network coverage, capacity and quality, and wants to include value-added services to diversify towards competitors. Wi-Fi is one key element to achieving both of these things, and is the perfect network technology to give their subscribers solid indoor coverage, and good performance and capacity in dense areas. Wi-Fi evidently reduces the churn rate and increases the ARPU.

Mobile subscribers are typically given a bundled subscription that includes both mobile access on their 3GPP macro-network, and Wi-Fi access in selected high-density areas.

This Wi-Fi access can be seamless and fully automated by using their SIM cards for accessing Wi-Fi. It could also be a manual and branded experience for the subscribers where they must login to Wi-Fi using a captive portal. The business model differs somewhat between these two access methods where the seamless access is typically charged the same way as in the mobile macro network and the portal access may be co-sponsored in different ways by venue owners or third-party advertisers.

With the right Wi-Fi service management system in place, the seamless and automated access to Wi-Fi may be combined with location-based notifications/marketing via e.g. SMS or email.

The Wi-Fi network provider may offer the mobile operator access to the Wi-Fi network through SMS-based login (open SSID) and may also offer a dedicated secure SSID (802.1x) to the mobile operator for automated and seamless SIM authentication. The number of SSIDs is due to radio protocol limitations a limited resource in Wi-Fi networks and cannot always be used as a differentiator between operators and service providers. A few SSIDs may however be sold to high-profile service provider customers.

3.2 CABLE AND FIXED-LINE OPERATORS

Cable and fixed-line operators offer residential broadband services to consumers aka triple-play services consisting of voice, TV and data to the home. While this has been a sound and profitable business for many years, it is now starting to erode into a pure single-play service of broadband data only. Cable/fixed-line operators are therefore looking for ways to enhance their offerings to the home, and are interested in the business-to-business segment as well.

One step many cable/fixed-line operators have already taken is to offer mobile subscriptions to their residential customers, transforming their triple-play into a quad-play offering. This is normally achieved through an agreement with a mobile operator where mobile capacity is leased and the cable/fixed-line operators pay the mobile operator per minute of voice and per MB of data. This is often a costly and sometimes even risky business case for the cable/fixed-line operator, since the cost model to the mobile operator is seldom back-to-back with the revenue model with the consumer, with the cable/fixed-line operator taking a business risk.

Cable/fixed-line operators have been looking into Wi-Fi for several years, and many of them have already deployed a community Wi-Fi through the residential broadband services. This means that home customers who are part of the community can use their Wi-Fi anywhere in the area, from their home to their neighbor's homes, and to selected public places, essentially transforming their Wi-Fi to an "on-the-go" service. Each and every user session on Wi-Fi will bring down the business risk with their mobile operator agreement, since traffic in Wi-Fi is much less costly than traffic in the mobile network.

In addition, consumers prefer Wi-Fi and look for Wi-Fi. It is usually faster and more reliable than the mobile network in indoor locations, and devices and apps are designed to prefer Wi-Fi over cellular mobile networks. Also, people use non-SIM-enabled "Wi-Fi only" devices to a high extent such as tablets and laptops.

A network provider that has a good Wi-Fi network with coverage in relevant places would therefore be of great value to the cable/fixed-line operator.

3.3 GLOBAL SERVICE PROVIDERS

There are a variety of global service providers that are interested in expanding their network coverage through partnerships with local network providers. These service providers include mobile operators such as Lyca Mobile, and niche Wi-Fi service providers like Boingo and iPass.

The network provider typically charges these service providers per time volume (tariff per minute) but may also agree on a flat-rate model in case the fixed charge is on and acceptable level.

4 THE ENTERPRISE

Enterprises and other verticals all have a need for Wi-Fi access for guests, visitors and customers.

There is a variety of verticals that need to offer guest Wi-Fi, each with its unique tweak and taste. Verticals of obvious interest are:

VERTICALS

RETAIL   HOSPITALITY, HOTELS   TRANSPORTATION   ENTERPRISE

STADIUMS   EDUCATION & MDU   HEALTHCARE   TRANSPORTATION HUBS
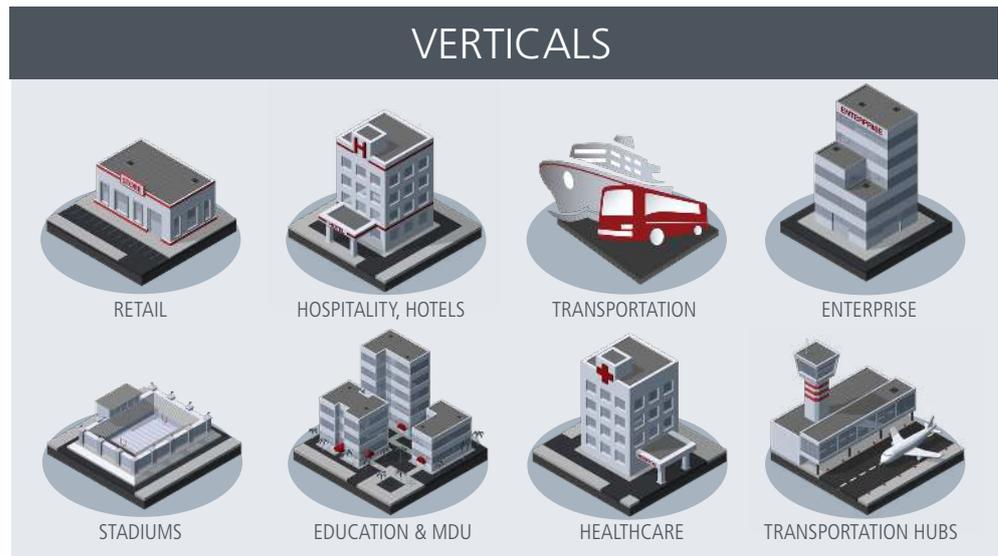
Commercial venues see their visitors and guests as their main source for business, and they have a somewhat common driver to offer these people guest access to the internet. Consumers will expect Wi-Fi when visiting retail and hospitality venues. Transportation and stadiums are growing segments as well.

Enterprises, institutions and corporations have a different driver for offering guests and visitors internet access. They typically offer visitors and consultants guest Wi-Fi within the conference and office areas, and employees of enterprises want to bring their own devices to the office (BYOD) to be used for both private and professional purposes. It is less important for these actors to do sophisticated customer engagements and campaigning.

5 THE NETWORK PROVIDER

A typical network provider is a network operator who has infrastructure assets like an IP-based fiber backbone, wired or wireless local loop and FTTH/FTTC, and who has an ongoing wholesale business or is planning to launch one. The network owner has knowledge and experience from deploying physical infrastructure and capacity in and between cities, and sells last-mile services to service providers and Internet backhauling services to enterprises and other verticals.

The network provider also knows how to operate large-scale networks and how to control network quality, capacity and availability for their customers, and how to manage thousands of network elements that form the service layer on top of the physical infrastructure.

The network provider may expand its business offerings by adding Wi-Fi on top of the infrastructure and/or backhaul services, and offer Wi-Fi wholesale to service providers and enterprises.

5.1 SERVICE DEPLOYMENT SCENARIOS

The Wi-Fi service, including the Wi-Fi service management system with features such as captive portal, user database and the AAA, can be fully hosted by the network provider. The service provider does not need to own any technology apart from what is potentially needed for management of customer relations and marketing campaigns.

The service provider may though, for different reasons, want to use their existing user database and AAA. The main reason is for their existing users to use their existing login credentials such as loyalty program identity, SIM card or my-pages credentials to access Wi-Fi.

Some service providers would also like to have their own captive portal. Their main driver is to have the flexibility to do their own marketing campaigns and to better control customer engagement and analytics.

There are also service providers that are looking for a "white label" network capacity, where it looks like it is the service provider's own network. In order to achieve that, they need to have their own dedicated SSID.

RESOURCE OWNERSHIP				
RESOURCE	SCENARIO 1 Fully hosted by Network Provider	SCENARIO 2 Service Provider, User Database	SCENARIO 3 Service Provider, User Database, Captive Portal	SCENARIO 4 Service Provider, Dedicated SSID
Wi-Fi Network	Network Provider	Network Provider	Network Provider	Network Provider
SSID	Network Provider	Network Provider	Network Provider	Service provider
WAG	Network Provider	Network Provider	Network Provider	Network Provider
IP-Backbone	Network Provider	Network Provider	Service provider	Service provider
AAA	Network Provider	Service provider	Service provider	Service provider
User Database	Network Provider	Service provider	Service provider	Service provider
Captive Portal	Network Provider	Network Provider	Service provider	Service provider

The four deployment scenarios are described in detail in the following chapters.

5.1.1 FIRST SCENARIO – FULLY HOSTED BY NETWORK PROVIDER

OVERVIEW

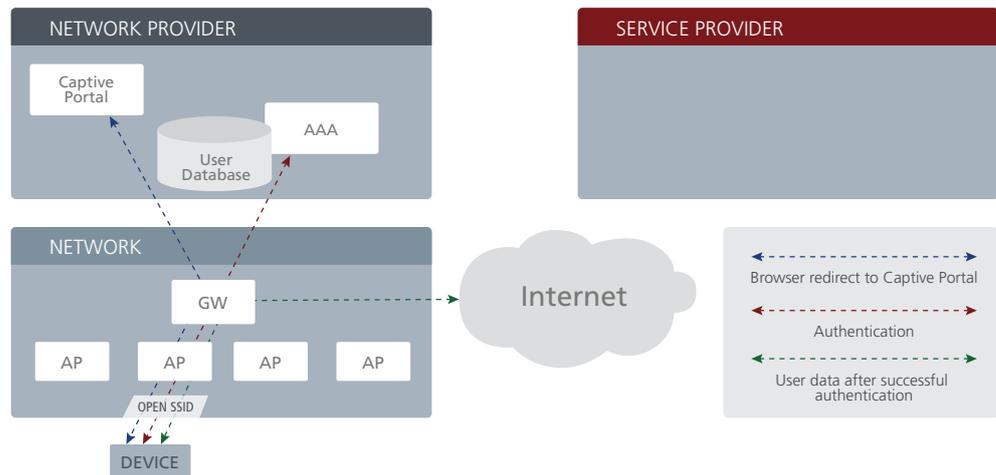### WI-FI SERVICE FULLY HOSTED BY THE NETWORK PROVIDER:

Figure 4. The Wi-Fi service is fully hosted by the network provider.

The **first** scenario (figure 4) describes the fully hosted service model. This means that the network provider facilitates with a full technical solution including the captive portal, the end-user charging, the user database, the AAA etc. The service provider owns its business case, brand and defines its service offerings, but does not need to make any investments in technology. The network provider will be responsible for the full service production environment, including creating and managing Wi-Fi accounts on behalf of the service provider.

TECHNICAL DETAILS

RESOURCE OWNERSHIP		
RESOURCE	NETWORK PROVIDER	SERVICE PROVIDER
Wi-Fi Network	✓	
SSID	✓	
WAG	✓	
IP-Backbone	✓	
AAA	✓	
User Database	✓	
Captive Portal	✓	

The user, who has a subscription account at a Service Provider, will visit a Wi-Fi location, attach to the Wi-Fi network through the Network Provider open SSID and will get an IP-address from the Wireless Access Gateway (WAG) through DHCP. Some user devices, typically smartphones and tablets, will thereafter scan Internet to determine whether the access to Internet is open or not, and in case it is not open, launch the native login-browser for authentication. Other devices,

12

typically laptops, will not evaluate the Internet connectivity and the user must therefore open a browser manually. The device will in both cases submit a http-request that will be re-directed, by the WAG, to the Captive Portal welcome page, where the user may select Service Provider. The user will thereafter be presented a login page hosted by the Network provider on behalf of the Service Provider, where the user may authenticate, register or purchase access to Internet.

The login page is a web-form containing one of several editable fields in which the user may insert user credentials such as username and password or an access-code. The user will insert the access credentials into the web-form and press the login button. The form will then be posted towards the WAG that will read the form and create a radius authentication request [1]). The request will be forwarded to the Network Provider AAA, where the credentials are verified towards the user-database. In case the user exist, is authorized to use Internet and has a valid quota for charging, the AAA will respond to the WAG with a radius-accept message to open the user session, or else will respond with a radius-reject in case the user is not authorized. The user traffic will be routed from the WAG through the Network Provider IP-backbone to reach the Internet.

The subscription may be either complimentary or charged for. Regardless, there may be a quota limitation of either time or traffic volume. The AAA will receive interim accounting information from the WAG and will thereby keep track of the time and data-consumption during the session. As the quota is consumed, the AAA will either send a radius-disconnect to the WAG who will terminate the user session, or a Change-of-Authorization (CoA) to the WAG who will change the session policy to a "re-direct" profile meaning the user can only access the Captive Portal and nothing else on the Internet. The user may in this state top-up the subscription quota or confirm another set of complimentary access.

---

1   Alternative login methods may be used depending on the type and vendor of the WAG.

5.1.2 SECOND SCENARIO – SERVICE PROVIDER USER DATABASE

OVERVIEW

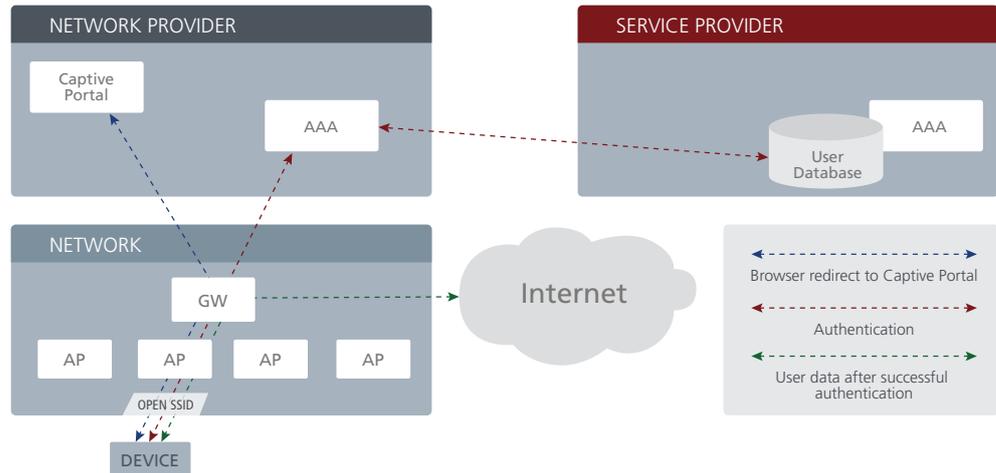### WI-FI SERVICE PARTLY HOSTED BY NETWORK PROVIDER:

Figure 5. The Wi-Fi service is hosted by the network provider except for the local user database and AAA located at the service provider.

The **second** scenario (figure 5) describes a partly hosted service model. The service provider has, in this scenario, its own user database and AAA solution and all authentications, and possibly also policy and charging, are done toward this AAA over typically the Radius protocol.

The benefits for the Service Provider with this scenario is the control of the user activation/deactivation, the service profiles and the service policy & charging of the end-user. A benefit is also the possibility for SSO where the user may use the same user credentials for Wi-Fi as is used for other services provided by the service provider.

TECHNICAL DETAILS

RESOURCE OWNERSHIP		
RESOURCE	NETWORK PROVIDER	SERVICE PROVIDER
Wi-Fi Network	✓	
SSID	✓	
WAG	✓	
IP-Backbone	✓	
AAA	(AAA-proxy)	✓
User Database		✓
Captive Portal	✓	

The user, who has a subscription account at a Service Provider, will visit a Wi-Fi location, attach to the Wi-Fi network through the Network Provider open SSID and will get an IP-address from the Wireless Access Gateway (WAG) through DHCP. Some user devices, typically smartphones

and tablets, will thereafter scan Internet to determine whether the access to Internet is open or not, and in case it is not open, launch the native login-browser for authentication. Other devices, typically laptops, will not evaluate the Internet connectivity and the user must therefore open a browser manually. The device will in both cases submit a http-request that will be re-directed, by the WAG, to the Captive Portal welcome page, where the user may select Service Provider. The user will thereafter be presented a login page hosted by the Network provider on behalf of the Service Provider, where the user may authenticate, register or purchase access to Internet.

The login page is a web-form containing one of several editable fields in which the user may insert user credentials such as username and password or an access-code.

The user will insert the access credentials into the web-form and press the login button. The form will then be posted towards the WAG that will read the form and create a radius authentication request [2]). The request will be forwarded to the Network Provider AAA proxy and forwarded to the Service Provider AAA, where the credentials are verified towards the user-database. In case the user exist, is authorized to use Internet and has a valid quota for charging, the AAA will respond back through the Network Provider AAA to the WAG with a radius-accept message to open the user session, or else will respond with a radius-reject in case the user is not authorized.

The user traffic will be routed from the WAG towards the Network Provider IP-backbone.

The subscription may be either complimentary or charged for. Regardless, there may be a quota limitation of either time or traffic volume. The Service Provider AAA will receive interim accounting information from the WAG through the proxy AAA and will thereby keep track of the time and data-consumption during the session. As the quota is consumed, the Service Provider AAA will either send a radius-disconnect to the WAG who will terminate the user session, or a Change-of-Authorization (CoA) to the WAG who will change the session policy to a "re-direct" profile meaning the user can only access the Captive Portal and nothing else on Internet. The user may top-up the subscription quota through the Captive Portal.

---

2   Alternative login methods may be used depending on the type and vendor of the WAG.

5.1.3 THIRD SCENARIO – SERVICE PROVIDER USER DATABASE AND CAPTIVE PORTAL

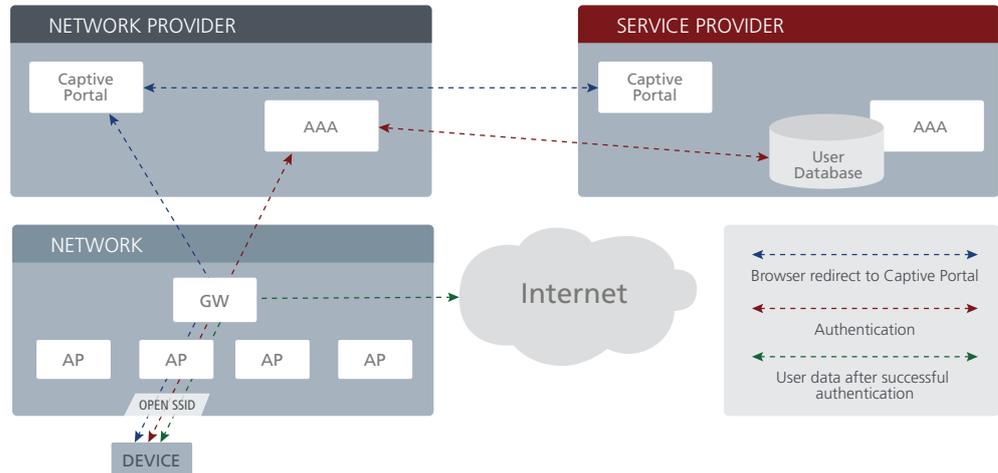OVERVIEW

WI-FI SERVICE PARTLY HOSTED BY NETWORK PROVIDER:

Figure 6. The Wi-Fi service is hosted by the network provider except the local user database, AAA and captive portal located at the service provider.

The **third** scenario (figure 6) describes the partly hosted service model where the captive portal is also owned by and located at the service provider's datacenter.

The benefits of having direct control of the captive portal is the direct control of the portal look and feel, messages on the portal pages, advertisements, and other user engagement flows. The portal may also be used for other services provided by the service provider, where the user e.g. may access the same e-wallet and top-up mechanism for Wi-Fi as is used for other services.

TECHNICAL DETAILS

RESOURCE OWNERSHIP		
RESOURCE	NETWORK PROVIDER	SERVICE PROVIDER
Wi-Fi Network	✓	
SSID	✓	
WAG	✓	
IP-Backbone		✓
AAA	(AAA-proxy)	✓
User Database		✓
Captive Portal	✓ Welcome Page	✓ Login Page

The user, who has a subscription account at a Service Provider, will visit a Wi-Fi location, attach to the Wi-Fi network through the Network Provider open SSID and will get an IP-address from the Wireless Access Gateway (WAG) through DHCP. Some user devices, typically smartphones and tablets, will thereafter scan Internet to determine whether the access to Internet is open or not, and in case it is not open, launch the native login-browser for authentication. Other devices, typically laptops, will not evaluate the Internet connectivity and the user must therefore open a

browser manually. The device will in both cases submit a http-request that will be re-directed, by the WAG, to the Captive Portal welcome page, where the user may select Service Provider. The user will thereafter be presented a login page hosted by the Service Provider, where the user may authenticate, register or purchase access to Internet.

The login page is a web-form containing one of several editable fields in which the user may insert user credentials such as username and password or an access-code.

The user will insert the access credentials into the web-form and press the login button. The form will then be posted towards the WAG that will read the form and create a radius authentication request [3]). The request will be forwarded to the Network Provider AAA proxy and forwarded to the Service Provider AAA, where the credentials are verified towards the user-database. In case the user exist, is authorized to use Internet and has a valid quota for charging, the AAA will respond back through the Network Provider AAA to the WAG with a radius-accept message to open the user session, or else will respond with a radius-reject in case the user is not authorized.

The user traffic will be policy routed from the WAG through the Service Provider IP-backbone to reach the Internet. On the Service Provider side, all traffic from the Wi-Fi network will be translated using Network Address Translation, in order for the packets to find their way back via the Service Provider uplink. In this scenario, all bandwidth for users belonging to the Service Provider will be consumed over the uplink of the Service Provider.

The subscription may be either complimentary or charged for. Regardless, there may be a quota limitation of either time or traffic volume. The Service Provider AAA will receive interim accounting information from the WAG through the proxy AAA and will thereby keep track of the time and data-consumption during the session. As the quota is consumed, the Service Provider AAA will either send a radius-disconnect to the WAG who will terminate the user session, or a Change-of-Authorization (CoA) to the WAG who will change the session policy to a "re-direct" profile meaning the user can only access the Captive Portal and nothing else on Internet. The user may top-up the subscription quota through the Captive Portal.

---

3   Alternative login methods may be used depending on the type and vendor of the WAG.

5.1.4 FOURTH SCENARIO – DEDICATED SSID

OVERVIEW
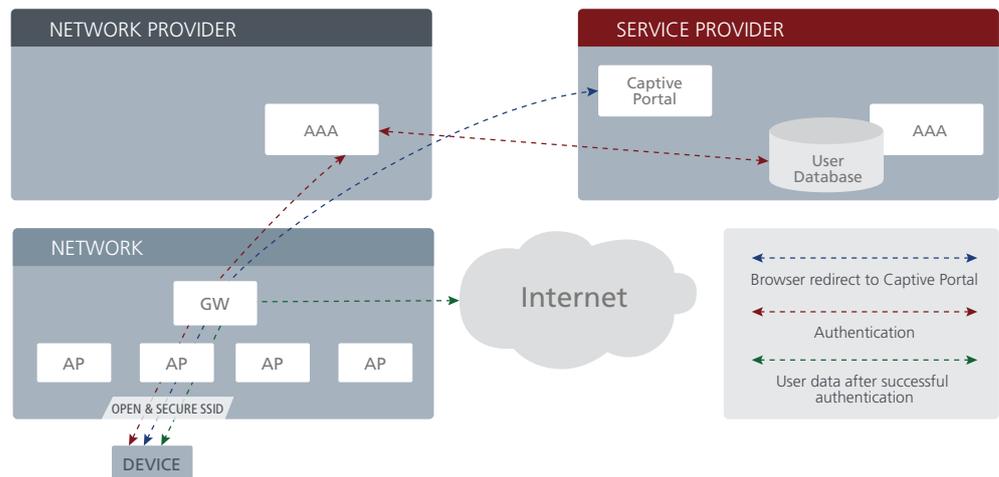SERVICE PROVIDER DEDICATED SSID :

Figure 7. The Wi-Fi service is hosted by the network provider except the local user database, AAA and captive portal located at the service provider. The network provider also offers the service porvider one or two dedicated SSIDs.

A fourth scenario is when the network provider sells a dedicated SSID to a service provider. This SSID may be made available at all the network providers' locations or just some of the locations, depending on the agreement between the network provider and the service provider.

Users may, through this SSID, be redirected directly to the service provider's captive portal without passing the network provider's captive portal. The access gateway may have different redirect policies per SSID at each location.

TECHNICAL DETAILS

RESOURCE OWNERSHIP		
RESOURCE	NETWORK PROVIDER	SERVICE PROVIDER
Wi-Fi Network	✓	
SSID		✓
WAG	✓	
IP-Backbone		✓
AAA	(AAA-proxy)	✓
User Database		✓
Captive Portal		✓

The user, who has a subscription account at a Service Provider, will visit a Wi-Fi location, attach to the Wi-Fi network through the Service Provider open SSID and will get an IP-address from the Wireless Access Gateway (WAG) through DHCP. Some user devices, typically smartphones and tablets, will thereafter scan Internet to determine whether the access to Internet is open or not,

and in case it is not open, launch the native login-browser for authentication. Other devices, typically laptops, will not evaluate the Internet connectivity and the user must therefore open a browser manually. The device will in both cases submit a http-request that will be re-directed, by the WAG, directly to the Captive Portal login page hosted by the Service Provider, where the user may authenticate, register or purchase access to Internet.

The login page is a web-form containing one of several editable fields in which the user may insert user credentials such as username and password or an access-code.

The user will insert the access credentials into the web-form and press the login button. The form will then be posted towards the WAG that will read the form and create a radius authentication request [4]). The request will be sent to the Network Provider AAA proxy and forwarded to the Service Provider AAA, where the credentials are verified towards the user-database. In case the user exist, is authorized to use Internet and has a valid quota for charging, the AAA will respond back through the Network Provider AAA to the WAG with a radius-accept message to open the user session, or else will respond with a radius-reject in case the user is not authorized.

The user traffic will be policy routed from the WAG towards the Service Provider IP-backbone.

The subscription may be either complimentary or charged for. Regardless, there may be a quota limitation of either time or traffic volume. The Service Provider AAA will receive interim accounting information from the WAG through the proxy AAA and will thereby keep track of the time and data-consumption during the session. As the quota is consumed, the Service Provider AAA will either send a radius-disconnect to the WAG who will terminate the user session, or a Change-of-Authorization (CoA) to the WAG who will change the session policy to a "re-direct" profile meaning the user can only access the Captive Portal and nothing else on Internet. The user may top-up the subscription quota through the Captive Portal.

The Service Provider SSID may also be a secure SSID encrypted with IEEE 802.1x for EAP-authentication. The secure SSID provides a seamless access in terms of, for the user perspective, an automated and and seamless authentication similar to 3GPP-networks. The authentication methods include EAP-SIM/AKA (using SIM-card credentials) and EAP-TTLS/PEAP (using username+password). EAP-SIM/AKA is fully automated from the first login, while EAP-TTLS/PEAP will require an initial insertion of the user credentials at the first login. The secure SSID and it's authentication methods suits well for operators who want to use Wi-Fi to offload their 3GPP-networks at dense areas and indoor where 3GPP macro-network coverage might be poor.

Note. The Service Provider may use its own WAG instead of the Network Provider WAG. This will require that the Network Provider must have tools in its Wi-Fi network to measure and calculate usage.

---

4   Alternative login methods may be used depending on the type and vendor of the WAG.

5.2 BUSINESS PARAMETERS IN THE NETWORK

There are a few business attributes in the network that will be an essential part of the value proposition to service providers and enterprises.

SSID

The first important business parameter in the network is the SSID(s). An SSID is the broadcasted network name of the Wi-Fi network that will become visible in the user device for access. The network could have several SSIDs commissioned in the network in parallel, i.e. one location could have several SSIDs at the same time. The user will see the possible networks (SSIDs) in the network list and select one to connect to. The network provider will need at least two types of SSIDs in the network, possibly more:

1. The Venue SSID which will be different from venue to venue. This SSID is typically called the name of the hotel, the name of the airport, the name of the stadium etc. This is an important part of the value proposition to the venues.

2. The Network Provider SSID for service providers. This SSID shall be available at all the locations of the network, and service provider customers will recognize this SSID and get familiar using it. This SSID is the key business value for selling Wi-Fi to service providers.

3. There may potentially be Service Provider SSIDs (unique per Service Provider) commissioned in the global network, but this is something a service provider should pay extra for since it increases their value greatly toward their consumer customers. A mobile operator may e.g. want their own SSID for Wi-Fi offloading.

LOCALIZED CAPTIVE PORTAL

The second important business parameter is location identity and the localized captive portal. There are three types of captive portals in the network:

1. The Venue captive portal is unique per enterprise customer. This captive portal is branded and designed with a look-and-feel decided by the venue owner. Users who select to access to the Venue SSID will be presented this captive portal.

2. The Network Provider captive portal is the common captive portal for service provider access where users may select the Service Provider from whom to buy access from. This captive portal will be the same in the global network so that users will recognize their Network provider's Wi-Fi service. It may include some location-unique welcome message. Users who select access to the Network Provider SSID will always be presented this captive portal. After selecting the service provider, the user will be presented with a captive portal look and feel unique to that service provider.

3. The Service Provider captive portal is a unique portal, offered by the Network Provider, to a specific service provider. This captive portal requires a Service Provider SSID and the look & feel is decided by the Service Provider.

5.3 SITE ACQUISITION

The network provider's main business asset is its mass of Wi-Fi locations in relevant and attractive places. These places are typically in high density areas and venues where many people spend time (with their devices). These locations are especially interesting if mobile networks can't offer sufficient bandwidth or coverage.

A business plan should always start with a location inventory:

1. Based on local understanding of the city or area, its citizens and visitors, their travelling paths and places where people spend time, prepare the list of attractive locations.

2. Categorize and rate these locations from their user relevance and business importance.

When you know the places of interest and have these categorized by priority, there are two ways to sign up attractive venues and locations with Wi-Fi:

1. Approach the venue owner of the location and offer them Wi-Fi coverage, a guest Wi-Fi with their own brand (Venue SSID, Venue Captive Portal), and a service provider service that spans across the Wi-Fi network (Network Provider SSID, Network Provider Captive Portal). This kind of venue owner should be charged a monthly fee for their own branded guest access, which may cover the full investment with margin.

2. Locations of priority, but without a clear commercial owner, could be deployed through an agreement with the municipality or real estate company.

5.4 NETWORK PROVIDER PROPOSITIONS TO SERVICE PROVIDERS

STANDARD PROPOSITION TO SERVICE PROVIDER (EXAMPLE)		
#1	NETWORK:	Full access to the network provider's Wi-Fi network (*Network Provider SSID*)
#2	CAPTIVE PORTAL:	Full access to the network provider's captive portal (*Network Provider Captive Portal*)
#3	LOGIN METHODS:	Two of the available authentication methods: • SMS verification • Manual login
#4	BUSINESS MODEL:	The Network provider will charge for the service both with a fixed monthly service fee and a flexible fee per GByte.

EXTENDED PROPOSITION TO MOBILE OPERATOR (EXAMPLE)		
#1	NETWORK:	• Full access to the network provider's Wi-Fi network (*Network Provider SSID*) • Unique secure SSID for mobile subscriber offloading with SIM authentication (*Service Provider SSID*)
#2	CAPTIVE PORTAL:	Full access to the network provider's captive portal (*Network Provider Captive Portal*)
#3	LOGIN METHODS:	Three of the available authentication methods: • SMS verification • Manual login • SIM authentication (EAP-SIM/AKA)
#4	BUSINESS MODEL:	• The Network provider will charge for the service both with a fixed monthly service fee and a flexible monthly fee per GByte. • A dedicated SSID (*Service Provider SSID*) will be charged a fixed monthly fee

5.5 NETWORK PROVIDER PROPOSITION TO ENTERPRISE

STANDARD PROPOSITION TO ENTERPRISE (EXAMPLE)		
#1	NETWORK:	Own SSID for guest access (Venue SSID)
#2	CAPTIVE PORTAL:	Own branded captive portal (Venue Captive Portal)
#3	LOGIN METHODS:	Two login methods of choice
#4	BUSINESS MODEL:	The Network provider will charge for the service both with a fixed monthly service fee and a flexible monthly fee per Access Point

6 ROAMING PARTNERSHIPS

Agreements can also be made with other network or service providers who have a Wi-Fi network of their own. These agreements are based on more mutual conditions where both parties bring network locations to the table.

As both parties in this way may add more relevant locations to their respective footprints, both parties may win from becoming more relevant to service provider and enterprise customers, and exchange coverage with each other. The party with the least relevant locations will naturally benefit the most, and the business agreement is a negotiation of who is bringing most value to the other party.
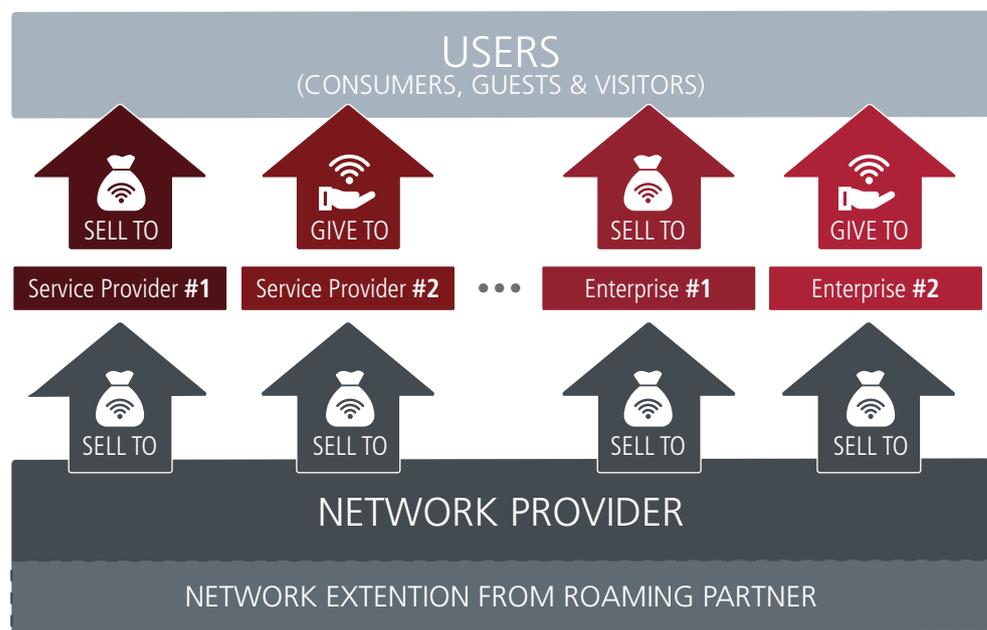

Figure 7. Adding coverage from roaming partnerships.

ABOUT APTILO

Aptilo Networks is a leading provider of carrier-class systems to manage data services with advanced functions for authentication, policy control and charging. We help service providers to create growth, save costs and reduce churn while increasing ARPU and customer loyalty through:

· Public Wi-Fi services
· Managed Guest Wi-Fi services to enterprises and venues
· Wi-Fi offload
· Wi-Fi Calling
· IoT services

The Aptilo Service Management Platform™ is the world's #1 Wi-Fi service control solution. It's been proven in large-scale deployments with 100+ operators worldwide, in partnership with leading vendors including Arris, Cisco, Ericsson, Fujitsu, HP, Nokia and Ruckus.

For more information, contact us at www.aptilo.com/contact-us/