Alternative business models for visitors in office buildings

Joonas Ojala
joonas.ojala@hut.fi
+358 50 3449916

Abstract

There has been much discussion about different WLAN (Wireless Local Area Networks) business models. WLAN has been well accepted as a technology and there is a clear user-demand for it, but still many of the current market approaches have failed. WLAN has been typically made available as complementary service to customers of coffee shops, hotels, airports and many other public places as well, but creating profits from this kind of business model has turned out to be very challenging. New kinds of business models have emerged, and in this paper I will research alternative business models for visitors in office buildings. Nowadays most companies are offering WLAN for their visitors for free, but in this paper I will discuss about the alternative solutions.

1 Introduction

New WLAN hotspots (access points) are introduced all the time. Whether the WLAN service is offered by WISP (Wireless Internet Service Provider) or some other party, like public place owner (airport, café etc.), has clear implications on the business model. Selling WLAN access to consumers has been surprisingly difficult, and WISPs have been forced to develop new kinds of approaches. It is been suggested if WISPs should become more “WOSP-ish” (Wireless Outsourced Service Provider), and start offering more WLAN services for companies instead of creating dense public hotspot network.[7] According to recent studies, 64 percent of businesses intend to increase WLAN deployment during the next 12 months.[4] The question is just – are equipment vendors the only ones who will profit, or can there be something for WISPs as well?

Before evaluating the different business models for visitors in office building in chapter 4, we look at some technical aspects of WLAN. Different standards are shortly introduced, and also the technological challenges are briefly discussed in chapter 2. WLAN is not yet a mature product, and though it can offer seamless wireless connectivity, many problems must be addressed before enterprises are willing to make large-scale investments on WLAN. Normal consumers can more likely tolerate for example some security or network management issues, but companies are expecting mature products. Thus I introduce some technological challenges which must be overcome.

2 Technology Overview

2.1 Standards

802.11b is the most widely used standard nowadays among the 802.11 (the first IEEE’s WLAN standard) WLAN standard family. **Wi-Fi** (Wireless Fidelity) is more popular name for the 802.11b standard, which specifies a data rates up to 11 Mbps and uses 2.4-GHz ISM (Industrial, Scientific, and Medical) frequency band and DSSS (Direct Sequence Spread Spectrum) technology.

801.11a specifies data rates up to 54 Mbps and uses 5-GHz UNII (Unlicensed National Information Infrastructure) band and OFDM (Orthogonal Frequency Division Multiplexing) technology for transmission. Though 801.11a offers higher transmission speeds, it has not become very popular – probably for the reason that it is not compatible with most widely used 802.11b standard.

801.11g runs in the 2,4-GHz ISM band (like 801.11b), but it uses the same transmission technology – OFDM – as 801.11a and thus can operate with data rates up to 54 Mbps. 801.11g is backward-compatible with 801.11b, and may potentially become the most popular WLAN standard in the near future.

802.1x concentrates on WLAN security aspects. 802.1x defines port-based network access control, which provides mutual authentication between a network and its client.

802.11i, also known as WPA2, adds more security services to 801.11 WLAN standard family by specifically addressing issues concerning both the media access control (MAC) and physical layers of wireless networks. Authentication schemes in 802.11i are based on 801.1x. WPA2 (and its first version, WPA - Wi-Fi Protected Access) addresses the problems of the original 802.11b security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses.[9]

2.2 Technological challenges

WLAN technology has been widely accepted, but before it can fully break trough there are several challenges to overcome. These challenges include authentication, security, coverage, management, location services and interoperability.

Authentication must occur before user can access the network resources. Authentication must be very smooth operation, and not require active user participation. Problem with hotspots is that several access methods exist: while one hotspot requires user to login using web-based user interface, another uses client software that must be installed beforehand. This creates problems when users are swapping between hotspots, and probably forces user to remember multiple username and password combinations. This raises some questions about global user identity databases, which do not currently exist, but could help in case of multiple authentication domains. There could also be a business opportunity for credit card companies which already possess huge customer databases, and could offer authentication and bulling services. Finally, authentication mechanism must be secure from the user's and service provider's point of view.

Wireless-hop security: data privacy must be guaranteed to WLAN users and network must be protected from malicious users. Higher-layer security protocols like SSH, SSL and VPN offer security under all WLAN infrastructures, but are not enough for several reasons: average users do not necessarily understand how they should be used, user authentication is done before any secure tunnels exist, and finally, wireless-hop security allows network service provider to protect against unknown, potentially malicious users. 802.1x and 802.11i standards try to address solutions both to authentication and wireless-hop security challenges. Security questions related to the paper topic will be discussed more in chapter 3.

Coverage can be, especially indoors, poor with WLANs. Radio frequency range and multipath interference limit the user mobility within a hotspot. If network service providers want to offer uninterrupted connectivity to roaming users, they must find ways to increase the density of hotspot coverage.

Network performance and QoS are important issues with WLAN, where the user behavior patterns are different from normal LAN. Network service providers must be able to provide enough capacity and coverage, and to do so, they must understand mobile user behavior. Though traffic pattern studies in enterprises have been implemented ([2]), this issue needs more research.

Network management can be difficult once hotspot coverage starts to grow. Installing new access points to various parts of network can require site specific radio frequency measurements and thus consume resources, and also make the network management more challenging.[1] With newest technology network management can be made easier by using central repository for configuration settings and security standards. These properties allow deploying enterprise-grade WLAN more effectively.[10]

Location and context-awareness could be utilized much more effectively than they are now.[1] Location specific information and advertisements could be offered to users, and if WLAN access points would be aware of each other it could be utilized in many ways: failure of one access point would make the nearby access point automatically adjust their power levels to provide coverage in exposed area, the location of wireless device could measured using triangulation, and in enterprise-grade WLANs rogue access points could be identified. Of course all this will require more advanced network management software.[10]

3 WLAN in enterprises

Before alternative business models for visitors in offices are further discussed, we study what kinds of concerns arise when WLAN access is granted for the quests. The question is not about just letting the visitors access the Internet, but we must also consider the technology that is used and especially concentrate on the chosen security solution.

Security issues have been the biggest showstopper in enterprise WLAN adoption – studies show that 95 percent of companies consider security to be among the top five concerns in adopting WLANs.[4] Threats like a denial-of-service attack using radio frequency jamming, passive eavesdropping attack, session-hijacking vulnerabilities, rogue access points and – of course – malicious visitors exist, but with good policy control it is possible to produce secure systems. In case of granting the access for visitors, the security aspect is even more emphasized.

Usually unsecured visitor hotspot service in run alongside company‘s secure internal network. Visitor network is logically tied to a termination point in company's demilitarized zone (DMZ), which resides outside the company's firewall. In this kind of WLAN environments quest users are not any bigger threat to internal systems than normal Internet users.[8]

Another way to run WLANs is one where everyone – whether company's own personnel or visitors – is connected to single wireless network. Especially for larger sites this would be beneficial, because there would be fewer transmitters interfering each others, and less administrative tasks to take care in case of upgrades to access points. Initial configuration would be more time-taking and require special knowledge, but by using VLANs and multiple SSIDs (Service Set Identifier that identifies access point) for different user communities single wireless network can be implemented.[3]This kind of approach is closely related to idea where company's network – either WLAN or LAN – is fully public, and company's personnel must access company servers trough firewalls. Studying this idea further is left for future papers.

4 Business models

WLAN business models are under constant evaluation and criticism. No model has yet proved its superiority, and new models for different types of situations – home, public, office – are continuously developed and studied ([5], [14]).

In following chapters I have defined four different business models that could be used in case of visitors in offices. Almost no research exists from this field yet, and most of the models are based on some existing service offerings.

Before specifying some alternative business models for visitors in office buildings, I have defined some general success criteria for WLAN business models in chapter 4.1. Also different stakeholders of value chain are identified.

4.1 General success criteria

Successful WLAN business model must provide value for all stakeholders: end user, network service provider, and building and premise owner.

From the end user's perspective WLAN must be easy to use, economic, and provide fast access in a transparent (device and access technology independent) manner.

Network service providers (WISPs) benefit when they have reliable and robust third-party authenticating entity, they have established peering agreements with other providers for seamless billing, and they are able to adapt varying resource and performance demands of the users.

Premise and building owners can gain profits when they have established business agreements with network service providers for installation, maintenance, monitoring, and support, and they are able to make network access an everyday utility for the end users.[1]

4.2 Free WLAN

Most companies that possess WLAN capabilities are offering WLAN for their visitors free, if the security policies just allow it. WLAN (or normal LAN) connectivity is considered useful for the business – it is a part of client and partner relationship management.

Companies are either renting WLAN service (equipment, installation and maintenance) from network service provider or taking care of all operations by themselves. If network service provider is renting the service, there is an evident business case for WISPs (we could also use term WOSP that was mentioned in introduction). If company is taking care of everything by itself, it should be aware of the resources this requires. It is most likely more economic – and also secure – to rent the service from WISP.

From the visitor's perspective this model is clearly best possible. Especially if user management is implemented in an efficient way, and either visitor's host or someone in the lobby or waiting area is able to grant a temporary access for the user.

4.3 WISP collects profits

Companies might have difficulties in justifying WLAN charge for their visitors, because as stated, in most cases Internet connectivity is offered free for the visitors – and seen as a part of client or partner relationship management. To be better able to justify the costs, company can outsource the WLAN, and let the WISP setup the WLAN service and gain profits. Most likely also company would have to participate to setup costs, and if company wants to use the WLAN for internal purposes it should pay some fees.

For user, this model is not optimal, and most likely decreases user's network usage. On the other hand, if service would be bundled for example to user's normal broadband or WLAN subscription, user would be more likely to use service. This kind of approach would give vantage to dominant WISPs.

4.4 Company generates revenue

Companies can also profit from their visitors, but this will most likely demand some kind of co-operation with WISPs. Network setup and maintenance would be done together with WISP, and also billing would require co-operation. The model would be quite similar to the one that was presented in previous chapter, but in this case the company and network service provider would share the profits. This kind of model might not happen in case of office buildings, but on the other hand, the model would encourage the company to really market their WLAN service (maybe not to visitors only?).

4.5 Enterprise community

Companies can also form enterprise communities, and let the members use each others WLANs. This model would also require WISP-like administrative layer that would offer both WLAN setup and maintenance services, and tools for user and network management.

From user's point of view this kind of service would be very beneficial, because it would allow wireless connectivity for free from various sites. Eventually this model is not very different from the model where WISP operates several company sites and allows users to access Internet through all of them. These kinds of models utilize the network effect, and should be interesting from dominant WISPs point of view.

4.6 Comparison of business models

Presented business models are compared from each stakeholder's (identified in chapter 4.1) point of view in table 1.

Table 1 Comparison of business models

	End user (visitor)	Network service provider (WISP)	Premise owner (company)
Free WLAN	service free, encourages usage	outsourcing the service generates opportunities, bundling LAN and WLAN?	costly, must consider co-operating with WISP
WISP collects profits	service charged, decreases usage	expensive set-up (if company not involved), good profits if service widely used	cheap if visitors widely use the service, set-up cheaper
Company generates revenue	service charged, user might not accept	chance to co-operate with company, percentual share for usage	generates profits if service is widely used, set-up more expensive
Enterprise community	service free, multiple sites increase usage	no opportunity, community though requires some kind of administrative layer	probably cheaper than WISP's offering, good option if large community

5 Case examples – Finland

I have identified two alternative business models for visitors in offices in Finland. The concept of offering something else than free access to visitors is very new, and before it can be fully evaluated, more market data is required.

The first case – Sonera HomeRun – is incumbent telecommunications operator’s offering, which is targeted also for public (airports, cafés etc.) hotspot users. In HomeRun case only network service provider (Sonera) gains profit from visitors.

The second case – SparkNet – is a enterprise community where companies can join. SparkNet generates income from selling business solution packages. SparkNet also sells user accounts for non-members.

5.1 Sonera HomeRun

Sonera is offering its WLAN service as a supplementary service to user’s current subscription or as a separate subscription. By purchasing Sonera HomeRun, subscriber is allowed to access Internet through various public hotspots in Finland and abroad. Pricing scheme for Sonera HomeRun is presented in table 2, and hotspot statistics in table 3.

Table 2 Sonera HomeRun price list (19.10.2006)

Sonera HomeRun	
Connection charge, €	6,73
Monthly charge, €/month	3,36
Usage charge in public service area, €/min	0,26
Usage charge in public service area, €/month/subscription (unlimited use)	80
Usage charge in own corporate service area, €/min	-

Table 3 Sonera HomeRun hotspots in Finland and other courties (19.10.2006)

Hotspot type	**Sites in Finland**	**All sites**
Hotels and conference centers	149	601
Airports and train stations	25	49
Restaurants and cafés	9	112
Motorway services	9	47
Exhibitions and sport grounds	8	27
Companies	**20**	**93**
Public places	9	115

In addition to Sonera HomeRun, Sonera is offering Sonera HomeRun Corporate Service Area for companies. This solution allows companies to offer WLAN to their visitors without a risk of granting temporary access for visitors to company LAN – WLAN is totally separated from company’s LAN. For company’s own employees service is free, but visitors are charged according to used time, unless they are monthly subscribers of Sonera HomeRun. Inside corporate service area companies are also able to set startup page of internet explorer – and thus offer some additional information about the company. Additional charges related to Sonera HomeRun Corporate Service Area are presented in table 4.[12]

Table 4 Sonera HomeRun Corporate Service Area price list (19.10.2006)

Sonera HomeRun Corporate Service Area	
Site survey and radio planning, €/service area	588,66
Installation charges, €/base station	126,14
Introduction of portal service, €/service area	462,52
Maintenance/base station, €/month	84,09
ADSL Internet connection, €/month	183,33

Sonera's corporate service area offering is mainly targeted to smaller companies who do not want to operate their own WLAN, but still offer WLAN service for their visitors and own personnel. Companies having corporate service area cannot gain profits from visitors, all subscriber fees go to Sonera. Corporate service area can be also seen as a supplementary service to Sonera HomeRun, which is priced to attract only mobile business users. By getting companies to invest on corporate service area, Sonera is also trying to increase its subscriber base for Sonera HomeRun.

Subscriber achieved value of Sonera HomeRun is clearly affected by the count of hotspots – more hotspots available, more value for the user. On the other hand, count of hotspots is very closely related to subscriber count – more subscribers allow establishing more hotspots. This is a difficult dilemma for WISPs to solve, and one solution could be roaming agreements.[11] From table 2 it can be seen that only few (20) companies (sites) have so far invested in Sonera HomeRun Corporate Service Area.

5.2 SparkNet

SparkNet is a user community where companies can join by selecting one of SparkNet's business or enterprise solutions. Prices of these solutions are varying according the case, and they include for example tools for web based user management. SparkNet users can also join OpenSpark community, which is a community of approximately 2000 private users.

The basic concept of OpenSpark and SparkNet is that once company have joined the community, they must offer company's WLAN service to all other SparkNet and OpenSpark users, but they are mutually able to utilize other users' WLANs as well. So far approximately 200 companies have joined SparkNet.[6][13]

6 Conclusions and future work

Alternative business models for visitor in office buildings need further studying and market data. Empirical study about the current state of visitor WLANs in office buildings would also be beneficial.

In this paper I have suggested few possible business models that could be used. The most promising ones offer value for all stakeholders: user, premise owner (company) and network service provider.

Free of charge model cannot be ignored, because most companies are using it and it is seen as a beneficial part of client or partner relationship management. Whether the visitor pays or not, is clearly an important question, but probably even more should be emphasized how the WLAN service is implemented and sold. Should WLAN be part of company LAN, should the WISPs bundle WLAN and LAN offerings, should it be used also for company' internal purposes, and who should take care of it? If companies are managing their WLANs by themselves, they must be aware of resources and costs it takes. When companies are ready to do large-scale WLAN investments, there should be a market opportunity for WISPs that are able to offer solutions that can handle all security, and network and user management issues.

References

[1] Balachandran, A. et al: "Wireless Hotspots: Current Challenges and Future Directions", Mobile Networks and Applications 10, 2005

[2] Balazinska M. et Castro, P.: "Characterizing mobility and network usage in a corporate wireless local-area network", in: Proc. MobiSys'03, May 2003

[3] Betts, B.: "Providing Wi-Fi access for guests", TechWorld, April 25 2005

[4] Gartner Inc.: "Gartner Survey Shows that Corporate Wireless LAN Deployment is Increasing, But Security is a Major Concern", July 5th 2006, www.gartner.com, referred 19.10.2006

[5] Hämäläinen, S.: "Business models based on facilities bundling: success criteria", Seminar on Networking Business, TKK Networking Laboratory, 2006

[6] Kuosmanen, J.: "New Business Models for Public Wi-Fi Services", presentation on Telecommunication Forum 2006, Helsinki University of Technology, September 26 2006

[7] Metrinomics: "New WLAN Report Calls On WISPs To Be More 'WOSP-ish'", July 16th 2003, www.metrinomics.com, referred 19.10.2006

[8] Molta, D.: "Market Analysis: WLAN Security", Network Computing, June 23, 2005

[9] Park, J. S. et Dicoi, D: "WLAN security: Current and Future", IEEE Internet Computing, September 2003

[10] Richards, K.: “Enterprise WLAN is Growing Up”, Software Magazine, August 2005

[11] Smura, T.: “Roaming Considerations for Finnish Public WLAN Market”, Innovation Dynamics in Mobile Communications, Helsinki University of Technology, 2004

[12] Sonera HomeRun, www.sonera.fi, referred 19.10.2006

[13] SparkNet, www.sparknet.fi, referred 19.10.2006

[14] Tallberg, M.: “P2P-based Roaming Between Home WLAN Hotspots”, Seminar on Networking Business, TKK Networking Laboratory, 2006