Monitoring and ensuring WLAN performance

Report

Produced by FUNET

Author(s): Wenche Backman

September 2010

Document No: GN3-NA3-T4-WLAN-monitoring
Version / date: 14.06.2010
Original language: Finnish
Original title: "WLAN-verkon valvonta ja toiminnan varmistaminen"
Original version / date: 1.0 of 17.09.2009
Contact: wenche.backman (at) csc.fi

Funet bears responsibility for the content of this document. The work has been carried out by Funet but ideas and feedback has been received from the working group on wireless systems and mobility led by Funet (MobileFunet) as part of a joint-venture project within the HE sector in Finland.

The translation of this report has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 238875, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3)'.

Table of Contents

Executive Summary

This report contains a survey of the alternatives available for the monitoring of WLANs, taking into consideration the fixed network, access points and, in particular, the air interface. The information was mainly gathered from the manufacturers' product descriptions; no practical experiments were conducted for this report. Commercial products can be divided into three groups:

- Products based on data from base stations and the fixed network
- Products based on site survey
- Comprehensive solutions covering both the fixed network and the air interface

Of the comprehensive solutions, 7signal Sapphire presents itself as an extremely promising solution for continuous WLAN monitoring covering the fixed network, access points and the air interface. A current first-rate solution for WLAN management and monitoring would be one where controller functions are utilised for access point configuration and management and information security control and Sapphire is used for ensuring quality from the end-user perspective.

Other, more inexpensive solutions do exist and there is certainly no lack of advanced site survey tools. Moreover, it is possible, at least in theory, to significantly improve the level of network monitoring by deploying dedicated scripts to access points.

1 Introduction

The monitoring of Wireless Local Area Networks (WLAN) has traditionally been carried out using the same approach employed in the monitoring of fixed local area networks. In other words, the focus is solely on data obtained from the fixed network. Network infrastructure elements are generally monitored individually, which makes it difficult to perceive the bigger picture. Moreover, WLANs have been set up on the best-effort principle without Service Level Agreements. As a result, network reliability cannot be ensured and locating and solving problems becomes difficult. A best-effort solution such as Ethernet is well suited to file transfer, but less so to voice and video applications, which involve the need to consider network lag and jitter in addition to performance. This report examines ways for improving WLAN quality and discusses both current and future solutions.

Today, WLAN monitoring in campus areas is performed using controllers or by monitoring stand-alone base stations using ping or, in advanced cases, base station scripts. In a controller-based WLAN, base station status is generally observed by monitoring and processing SNMP Trap messages. In addition to allowing monitoring, controllers improve network quality through centralised channel partitioning and transmit power control. Controllers and scripts are used to monitor the network up to the base stations and to obtain the status of the air interface provided by the base stations. Traditionally, the service quality experienced by the user or the user's terminal has received little attention, even though air interface scanning has been performed to a certain extent. Scanning provides a better picture of disturbances and problems at the air interface than base station data, but only enables the examination of current status. Furthermore, scanning detects gaps in coverage areas, improving network quality.

2 SNMP and related products

SNMP (*Simple Network Management Protocol)* is used to communicate with network devices in order to ensure network performance. More information on SNMP can be found in references [1] and [2]. The SNMP manager monitors the SNMP agent by making queries or by retrieving and reacting to alarm messages. Identified on the basis of their numeric OID (Object Identifier), the parameters monitored at the agent are displayed as a tree structure. At the agent the parameters and the corresponding OID values are collected into the MIB (Management Information Base), which also contains read/write rights as well as a short description of each parameter.

Of SNMP messages, the one mainly connected to network monitoring is Trap, in which the SNMP agent, i.e. the device, informs the SNMP manager of status changes and alarms. Network monitoring using SNMP Trap messages is a conventional way of monitoring changes in the network. SNMP is supported by most hardware, such as WLAN controllers and derived applications.

There is a range of software, often free, for both Windows and Linux platforms for the collection and visualisation of data obtained using SNMP. A list of available products can be found on the following websites, for example:

- http://wlan-snmp-software.qarchive.org/
- http://www.snmptools.net/software/

3 Commercial products for monitoring and control

Commercial products for WLAN monitoring and control can be divided into three groups. The first group is WLAN controllers offered by major manufacturers. These include functions for WLAN monitoring mainly on the basis of base station data. The second group includes traditional methods for examining WLANs on the air interface, for example, by measuring the signal strength and noise level of the local air interface or by testing elements of the fixed network infrastructure via the air interface. The third group comprises products that have recently emerged in the market which are used to obtain an overall picture of the operation of the WLAN, taking into consideration the fixed network, access points and the air interface.

In controller-based WLANs, which belong to the first group, the objective is to obtain an overall image of the network to enable the improvement and monitoring of signal quality. Controllers provide constant data on access points and their surroundings for monitoring purposes, but the service level experienced by the terminal receives little attention. In the second group, local site surveys performed with wireless terminals reveal coverage areas, noise levels, the Signal-to-Noise-Ratio (SNR) as well as any information security gaps. This provides accurate, momentary data on the quality of the air interface, but the method is not suitable for continuous monitoring. Site surveys can, however, be a good complement to monitoring achieved with controllers. If the WLAN is not controller-based, site surveys are a straightforward method for checking network quality. Site surveys collect vast amounts of data on the radio interface and the packets on the interface: retransmissions taking place in the network in particular are an indicator of current performance [3]. Each retransmission, regardless of the reason, consumes network resources unnecessarily. Transfer speeds are also important indicators, as low transfer speeds are used in places where the signal quality is poor. The causes for poor signal quality include low signal strength and high noise level.

3.1 Products based on data from base stations and the fixed network

The **Cisco WCS** (Wireless Control System), [4], was mainly developed for the control and monitoring of several Cisco WLAN controllers, but also includes features for collecting and visualising data from the air interface. WCS is browser-based, and allows the monitoring of signal strength, current channel allocation and used transmit power. For purposes of network troubleshooting, WCS provides information on noise levels, terminals, controllers, access points, information security and, to an extent, performance. Location of terminals is also possible. Integration of WCS with the Cisco Spectrum Expert will provide even more detailed data on the disturbances on the air interface. WCS improves information security by detecting RF attacks, such as Denial of Service (DoS), and unauthorised access points. Monitoring is programmable to generate an alarm automatically in the event of attacks. WCS also includes functions for the debugging of network problems encountered by individual terminals, but data on transfer speed for the entire network is not available.

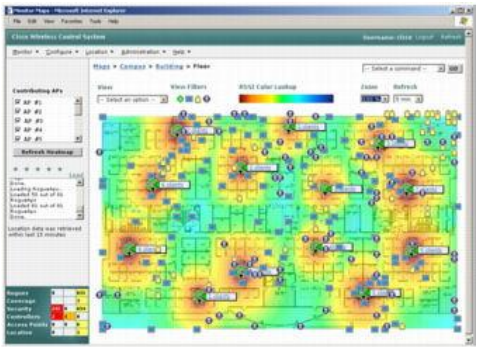

Figure 1. One of the network views provided by WCS [5].

AirWave's **Wireless Management Suite** [6] includes several modules for WLAN monitoring and control. Part of Arube Networks, AirWave specifically provides operations solutions for multi-vendor environments. It is claimed to support over 90% of the WLAN equipment of different manufacturers, and enables the monitoring and control of autonomous access points in addition to controller-based solutions. According to Arch Red, the product's distributor in Finland, the product is used by the Tampere University of Technology, the University of Oulu and the City of Tampere, among others.

One of the products included in Wireless Management Suite is the AirWave **Management Platform** (AMP), which is used for the management of multi-vendor WLAN systems. AMP enables centralised software updates and configuration and the specification of different settings for different hardware. Reporting tools are also included in the software.

For the monitoring of the air interface AirWave has developed the **VisualRF** module, which can be utilised to check signal strength and channel partitioning. It should be remembered, however, that the transfer speed used is more indicative of the network quality experienced by the user than signal strength and noise level alone.

In addition to the above-mentioned modules, AirWave's software includes the **RAPIDS** module for the detection of unauthorised access points. Detection covers both the air interface and the fixed network.

Motorola has the **RF Management Suite** for the management and monitoring of a network consisting of autonomous access points [7]. The product slightly resembles Cisco's controller and WCS.

3.2 Products based on site survey

Motorola AirDefense Mobile, [8], can be installed on laptops running Windows XP or 2000 with an Atheros-based 802.11 a/b/g network card, such as Netgear (WAG511) or Cisco (CB21AG).
The tool allows monitoring of traffic on the WLAN and terminal connections as well as diagnostics for troubleshooting. Focusing heavily on information security, the product has more than 175 various types of alarms, including alarms for rogue access points and misconfigured devices. AirDefense Mobile can be combined with Motorola AirDefense Enterprise, which is covered in more detailed in the next chapter.

Unlike AirDefense, Motorola **SiteScanner**, [10], is based specifically on the monitoring of network performance and coverage. SiteScanner can be used to measure factors such as data rates, signal strength and noise level at selected sites. Traffic generated by terminals can also be used to measure delay, jitter and retransmissions, if a receiving server has been specified and connected to the network. The product requires the Windows XP operating system. The supported network cards are presented in reference [10].

AirMagnet WiFi Analyzer, [11], is another laptop-based software allowing thorough examination of the air interface. The software includes features for the monitoring of both the radio interface and the fixed infrastructure, such as data rate and the rate of performance of DHCP and ping commands. Monitoring of signal strength and noise level is also possible, along with the control of network information security by identifying misconfigured devices and devices sending unencrypted data. Locating is also possible. WiFi Analyzer runs on both Windows and Mac operating systems but is only compatible with certain network cards.

The product is said to be extremely easy to use, offering an intuitive user interface and tools for the rapid troubleshooting of common network problems without the need to check individual packets [3]. AirMagnet also has the **VoFi Analyzer** for checking voice quality and for troubleshooting voice-over-WLAN problems [12]. Analysis on encrypted networks is also possible. The software enables the monitoring of significant Mean Opinion Scores (MOS) [13], used to determine the voice quality achievable at a certain point in time by checking which codec can be used.

Another popular WLAN analyser is the **WildPackets OmniPeek** [14], which enables the thorough analysis of packets sent over the air interface. The product is designed for the on-site troubleshooting of problems on the radio interface. Therefore, it naturally displays the access points and terminals as well as statistical data on traffic, including utilisation rate and number of retransmissions. According to [3] it is the best tool for troubleshooting problems on the air interface with its versatile functions and particularly extensive filtering properties.

Wireshark, [15], is an open source software for Windows and Linux computers for the analysis of network protocols. Wireshark allows the straightforward analysis of traffic on the computer in question, but is not so well suited to the comprehensive analysis of WLANs. Analysis of control and beacon frames requires use of the monitoring mode, which is not supported by all operating systems, adapters and drivers. Furthermore, physical variables are not available, including the channel used, signal strength and used data rate, which is critical in performance analysis. It is claimed that the capture of retransmissions requires multi-stage configuration [3]. Wireshark's user-friendliness can be considerably improved by combining it with AirPcap USB adapter [16], which is a commercial solution. This will also enable the analysis of physical-level data, such as the signal strength of individual frames and used data rate. The combination can be further complemented with the Pilot software by CACE Technologies [17], offering additional functions for visualisation.

MetaGeek offers the **Wi-Spy** product suite, with DBx as its most advanced component [18]. DBx is a spectrum analyser operating in the 2.4 and 5 GHz frequency ranges, allowing the selection of the optimal channel for autonomous access points and the identification of the noise level caused by nearby access points. The benefits of the product in controller-based environments are perhaps unclear. MetaGeek has also developed an open source scanner for WLANs which enables the establishment of the MAC addresses, SSIDs, channels and signal strengths of terminals connected to the network.

TamoSoft's **CommView**, [19], is a product for network monitoring and analysis enabling the analysis of access point and terminal signal strength, packets on the air interface and connections being used.

3.3 Comprehensive solutions

Differing from the other monitoring software, **7signal Sapphire**, [20], offers quality of service monitoring from the end-user perspective. Network performance is monitored automatically round the clock. 7signal claims the product to be the first end-to-end quality monitoring software combining the monitoring of wireless and fixed network infrastructure [21]. The claim is true at least in the respect that other monitoring software often lacks a comprehensive monitoring perspective, focusing only on selected parts, such as individual network elements in the case of SNMP software and the current air interface in the case of wireless site survey tools. WLAN controllers also fail to monitor quality of service.

Sapphire works through the installation of Eyes to monitor the network. Exploiting Power over Ethernet (PoE), the Eyes are connected to the fixed network and constantly monitor the network either actively or passively. Active measures include attach command polling and the time taken by authentication, DHCP server performance (the time taken to obtain an IP address) as well as HTTP and FTP transfers and downloads, usually using test files of 2-10 Mb in size. In addition to the Eyes, the fixed network is also equipped with the Sonar Server which functions as an endpoint for HTTP and FTP services. Active tests also include a VoIP test examining the codec used and the MOS values [13]. Passive tests include the measurement of signal strength and noise level as well as the measurement of the codec used in connection with voice. Monitoring can be done using the web-based user interface, but the application can also be configured to send e-mail or SNMP Trap messages when faults are detected.

Sapphire requires a degree of investment as one Eye can only monitor around 6-12 access points. Each Eye costs approximately EUR 2,000; the Sonar Server is priced on the basis of the number of Eyes and installed on an RHEL server. Sapphire has been developed especially for WLAN quality monitoring and does not include features for identifying unauthorised access points, for example. The operation of Sapphire is illustrated in Figure 2**.**

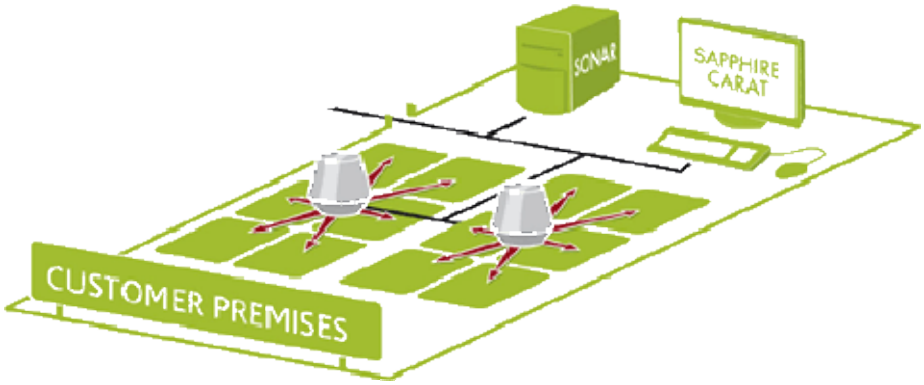

Figure 2. Sapphire operation.

Motorola **AirDefense Enterprise**, [9], enables round-the-clock network monitoring using sensors. In addition to sensors, the system comprises a server. The system can be used to monitor WLAN traffic for purposes of eliminating security threats, ensuring compliance with security policy, the detection of rogue access points, and performance monitoring. The locating of terminals is also possible.

Madge has a product called **WLAN Probe Monitor**, [22], which offers the same type of solution as 7signal Sapphire and Motorola AirDefense. However, Madge focuses only on information security and requires the installation of probes, which resemble the Eyes used by Sapphire. Madge products enable the monitoring of rogue access points, unauthorised terminals and networks, SSIDs on the air interface and attempted intrusions.

4 Ensuring network quality

In the academic sense, the ensuring of WLAN performance is based on the optimal distribution of radio resources. Owing to centralised channel partitioning and transmit power control, controller-based network solutions are clearly more powerful in this respect than networks comprised of autonomous access points.

Other methods also exist for optimising network performance. For example, the bandwidth used by visitors can be adjusted to ensure sufficient resources for proprietary users. Determination of the Quality of Service (QoS) is also possible. WLANs use QoS priority levels Voice, Video, Best Effort and Background. Cisco's controller, for example, enables the specification of data rates and share of bandwidth for all of these. The network can be configured to better support, for example, voice traffic (VoWLAN) by increasing data transfer rates and by allocating a large share of bandwidth to a selected service. However, depending on the number of users, these adjustments will cause the data rates of other users to drop when voice is transmitted over the network.

It is also possible to add access control to the network to protect existing connections from network overload. For example, Cisco's controller allows access control based on both bandwidth use and load levels.

In theory, the noise level of WLANs could be lowered by adjusting output power in the same way as on mobile phone networks. This would mean that the transmit power of both the access point and the terminal would be lower in cases where the distance between the two is short. In practice, WLAN power can only be adjusted to enter sleep mode when traffic is low to save battery power.

Network development and optimisation are also part of the measures taken to ensure network quality. The data provided by site survey tools can be utilised here, for example, for the location of any coverage gaps.

5 Network testing

Signal strength alone is not a particularly comprehensive indicator of network quality. The inclusion of the Signal-to-Noise ratio will result in slightly more information about the network. The best picture of the network quality experienced by the user is probably obtained by monitoring data rates and, in connection with VoIP, voice quality. Further information on quality can also be obtained by examining network performance in connection with processes relating to a user connecting to the network (association, authentication and obtaining of IP address).

The MobileFunet working group, which consists of Funet representatives and communications specialists from universities in Finland, could collaborate to develop a test used to measure the performance of WLAN networks. The test could examine the data rate per square metre by measuring a specified number of points (e.g. 0.1 points/m^2). The following should also be taken into consideration:

- Network ability to serve several users simultaneously (possibly using iperf with parallel data streams)
- Voice quality on VoIP

6 Measures for monitoring and ensuring WLAN performance

The solutions adopted for monitoring and ensuring WLAN performance depend on the starting points. If autonomous access points are used, these could be fitted with scripts used to relay the parameters of the air interface, noise level, etc. to the monitoring software. The script should take into consideration the fact that different access point manufacturers use different operating systems, which leads to different types of opportunities. Linksys, for example, currently uses the closed operating system VxWorks [23], but all access points in the OpenSpark user community use OpenWRT [24]. The operating system of Cisco devices (Cisco IOS) supports the sending of SNMP Trap messages to the server, and base stations based on OpenWRT can also be configured to send SNMP Trap messages. However, many manufacturers refuse to reveal their operating system, and monitoring using methods other than ping is not possible without editing the manufacturer's source code.

If the WLANs are controller-based, the network could be checked periodically using site surveys in addition to the data obtained from the controllers. Users could also be instructed to notify problems: for example, Aalto University in Finland has positive experiences of a feedback system.

The terminals of administrators could, where possible, be fitted with scripts used to notify the suitable monitoring software of problems in quality of service. Fault reports should at minimum include date and time, the names or MAC addresses of surrounding access points as well as signal levels. If the WLAN of the campus area already has a locating service in place, this could be exploited in this connection. A similar script could possibly be introduced for regular users, too: when quality of service deteriorates, a popup message could ask the user if he or she wishes to send a message containing location data to the network administrator. This would not have to take place in real time: the report could be sent when network quality improves or the next time the user logs on to the fixed network.

A further alternative would be to develop a script to monitor the quality of service of the air interface by relaying messages between access points. The transfer speed used to send a simple message from one access point to another and the other parameters of the message could provide important information on the quality and noise level of the air interface at that time. This requires that the distance between the access points is not too great, that is to say there should be no gaps in coverage. In such a solution the access points would provide normal service to the WLAN terminals for most of the time, but could be instructed (using a script, for example) to send messages to each other at certain intervals.

The quality monitoring concept of 7signal Sapphire is excellent; the implementation of this concept could create a network where monitoring and troubleshooting are easier than before. However, the "Eyes" required are expensive, and as access points have the ability to send and receive messages and monitor service quality, if only partially, it would be interesting to attempt service quality monitoring using messages sent between access points.

CSC/Funet could assist Funet's member organisations in the monitoring of WLANs and in ensuring their performance by evaluating, through practical testing, the AirMagnet WiFi and VoFi Analyzers as well as the WildPackets OmniPeek, which have received good reviews [3]. If possible, CSC/Funet could also evaluate the 7signal Sapphire as well as the AirWave Wireless Management Suite as a multi-vendor environment management and monitoring solution.

The MobileFunet working group could share scripts developed and implemented for monitoring purposes, if such scripts exist. Also, experiences of the monitoring software of different manufacturers could be listed on the Funet wiki page WLANVerkonHallintaJaYllapito [25]. Experiences of the features of the various controllers would also be valuable. MobileFunet could also jointly develop tests for the measurement of WLAN quality.

7 Summary and conclusions

New networks are generally built to consist of controllers, making the monitoring of at least the fixed network elements significantly more straightforward than in networks consisting of autonomous access points. Monitoring of the air interface is usually performed by monitoring network quality locally.

This report contained a survey of the alternatives available for the monitoring of WLANs, taking into consideration the fixed network, access points and, in particular, the air interface. The information was mainly gathered from the manufacturers' product descriptions; no practical experiments were conducted for this report. Commercial products can be divided into three groups:

- Products based on data from base stations and the fixed network
- Products based on site survey
- Comprehensive solutions covering both the fixed network and the air interface

Of the comprehensive solutions, 7signal Sapphire presents itself as an extremely promising solution for continuous WLAN monitoring covering the fixed network, access points and the air interface. A current first-rate solution for WLAN management and monitoring would be one where controller functions are utilised for access point configuration and management and information security control and Sapphire is used for ensuring quality from the end-user perspective.

Other, more inexpensive solutions do exist and there is certainly no lack of advanced site survey tools. Moreover, it is possible, at least in theory, to significantly improve the level of network monitoring by deploying dedicated scripts to access points.

In future CSC/Funet could focus on the evaluation of products and, together with MobileFunet, on the development of a network quality test. Members of MobileFunet are also encouraged, where possible, to share any scripts they have deployed as well as to share their experiences of monitoring software through the Funet wiki.

References

[1] http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

[2] http://www.rane.com/note161.html

[3] B. Miller, “Choosing the Right Analyzer for Your WLAN,” Expert Reference Series of White Papers, Global Knowledge, July 2009.

[4] http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.pdf

[5] http://www.digitalairwireless.com/cisco_wireless_networks.asp

[6] http://www.airwave.com/products/

[7] http://www.motorola.com/Business/US-EN/Business+Product+and+Services/Software+and+Applications/WLAN+Management+and+Security+Software/RF+Management+Software_US-EN

[8] http://www.airdefense.net/products/admobile/

[9] http://www.airdefense.net/products/enterprise.php

[10] http://www.motorola.com/Business/US-EN/Business+Product+and+Services/Software+and+Applications/Network+Design+Software/SiteScanner+Software_US-EN

[11] http://www.airmagnet.com/products/wifi_analyzer/

[12] http://www.airmagnet.com/products/vofi_analyzer

[13] http://en.wikipedia.org/wiki/Mean_opinion_score

[14] http://www.wildpackets.com/products/distributed_network_analysis/omnipeek_network_analyzer

[15] http://www.wireshark.org

[16] http://www.cacetech.com/products/airpcap.html

[17] http://www.cacetech.com/products/cace_pilot.html

[18] http://www.metageek.net/products/wi-spy-dbx

[19] http://www.tamos.com/products/commwifi

[20] http://www.7signal.com/

[21] http://www.7signal.com/files/7signal_in_Telecom_Trends.pdf

[22] http://www.madge.com/products/products-wireless.aspx

[23] http://linux.fi/wiki/WLAN-tukiasemat

[24] http://fi.wikipedia.org/wiki/OpenWRT

[25] https://info.funet.fi/wiki/BCP/WLANVerkonHallintaJaYllapito

Sites accessed on 17 September 2009.

Glossary

DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
FTP	File Transfer Protocol
Funet	Finnish University and Research Network
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
MAC	Medium Access Control
MIB	Management Information Base
MobileFunet	a working group on wireless systems and mobility led by Funet
MOS	Mean Opinion Scores
OID	Object Identifier
PoE	Power over Ethernet
QoS	Quality of Service
RF	Radio Frequency
RHEL	Red Hat Enterprise Linux
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise-Ratio
SSID	Service Set Identification
VoIP	Voice over IP
VoWLAN	Voice over WLAN
WCS	Wireless Control System
WLAN	Wireless Local Area Networks