Harri Lapinoja

INTELLIGENT WIRELESS LOCAL AREA NETWORK MONITORING IN INDUSTRIAL ENVIRONMENT

INTELLIGENT WIRELESS LOCAL AREA NETWORK MONITORING IN INDUSTRIAL ENVIRONMENT

Harri Lapinoja

Master's Thesis

Fall 2013

Degree Programme in Information Technology

Oulu University of Applied Sciences

ABSTRACT

Oulu University of Applied Sciences
Master's Degree Programme in Information Technology

Author: Harri Lapinoja
Title of Thesis: Intelligent Wireless Local Area Network Monitoring in Industrial Environment
Supervisor: Kari Laitinen
Term and year when submitted: Fall 2013 Number of pages: 57

The research problem for this thesis was provided by Rautaruukki Oyj. The purpose of this thesis was to study how modern intelligent wireless local area network monitoring methods and tools could be used to improve WLAN monitoring and functionality at Ruukki Metals steel factory.

The research for this thesis was mainly done by studying research papers and articles but also by interviewing specialists and by participating in meetings and presentations. The research was concentrating on different monitoring methods for wireless local area networks and also on the features and characteristics of the selected monitoring software and Ruukki Metals steel factory network environment. The demonstration project was carried out to demonstrate and test the intelligent network monitoring in realistic conditions. The project environment was constructed for Ruukki Metals steel factory site in Raahe, it enabled the possibility to test the capabilities of the intelligent WLAN monitoring tool in an actual factory environment. As well as the existing WLAN network at Ruukki Metals factory, the demonstration project environment was assembled by using Cisco WLAN products. Cisco Prime Infrastructure software was selected as the monitoring tool for the project

The results of the research show that intelligent network monitoring tools are beneficial in monitoring wireless local area networks at a steel factory environment. By using intelligent network monitoring tools, network monitoring and managing becomes more efficient and the function of the network can be improved. Future research possibilities related to this research could relate to improving network monitoring and network reliability. For example effects of using directional antennas and dedicated spectrum analyzators as part of a network monitoring environment. Testing different antenna types and installation positions would provide useful information about what kind of impact they would have on interference tolerance and the range of access points.

Keywords:

Network monitoring, spectrum analysis, ICMP, SNMP, WLAN

TABLE OF CONTENTS

ABSTRACT **3**

TERMS AND ABBREVIATIONS **6**

PREFACE **9**

1 THE PURPOSE AND GOALS OF THE RESEARCH **10**

2 WIRELESS LOCAL AREA NETWORKS **11**

2.1 Wireless communications 11
2.2 Radio frequencies and spectrum allocation 12
2.3 Data transmitting in a radio channel 14
2.3.1 Path loss 14
2.3.2 Fading 14
2.3.3 Multipath propagation 15
2.4 802.11 16
2.4.1 802.11a 16
2.4.2 802.11b/g 17
2.4.3 802.11n 17
2.4.4 802.11s 18

3 WLAN MESH NETWORKS **19**

3.1 Advantages and challenges 19
3.2 Discovery and formation 20
3.3 Power management and synchronization 22
3.4 The medium Access Control in 802.11s 22
3.5 Congestion control 23
3.6 Security 23
3.7 Path selection 23
3.8 Known challenges 24
3.8.1 Multihop problem 24
3.8.2 Hidden node problem 25
3.8.3 Other issues 26

4 WIRELESS LOCAL AREA NETWORK MONITORING METHODS **27**

4.1 ICMP 27
4.2 SNMP 27
4.3 Sniffing 28
4.4 Spectrum analyzing 28
4.5 Intelligent network monitoring 29

5 NETWORK ENVIRONMENT AT RAAHE FACTORY **30**

5.1 Network structure 30
5.2 The challenges in a steel factory environment 32
5.3 Network devices at Raahe factory 33
5.4 Known issues 34

5.5 Network monitoring tools 35

6 RESEARCH AND RESULTS 37

6.1 Demonstration project..... 37

6.1.1 Installing and configuring the monitoring environment 39

6.2 Using the tools and acquiring data..... 45

6.3 Results 51

7 CONCLUSIONS..... 53

7.1 Future research possibilities 53

REFERENCES..... 55

TERMS AND ABBREVIATIONS

AODV	Ad Hoc On Demand Distance Vector. Routing protocol for mobile ad hoc networks.
ARP	Address Resolution Protocol. A protcol for resoluting network layer addresses to link layer addresses.
BGP	Border Gateway Protocol. Routing protocol.
CDP	Cisco Discovery Protocol. Used in Cisco network devices for network discovery.
DCF	Distributed coordination function. Used in 802.11 networks.
DFS	Dynamic frequency selection. Access points automatically selects the frequency channel with a low interference level.
CPU	Central Processing Unit. Hardware inside a computer that carries out the instructions of a computer program.
EDCA	Enhanced Distribution Channel Access. Used in WLAN mesh networks for channel access.
HWMP	Hybrid Wireless Mesh Protocol. The default path selection protocol for WLAN mesh networks.
Hz	Hertz. The physical measurement unit used to measure frequency. The unit was named after Heinrich Rudolph Hertz who was the first to prove existence of electromagnetic waves.
ICMP	Internet Control Message Protocol. ICMP is a protocol used by network devices to send error messages for example if the host cannot be reached.
IEEE	Institute of Electrical and Electronics Engineers. The

	world's largest professional association. The purpose of the association is to advance technical innovation and excellence.
IETF	The Internet Engineering Task Force. An organization which develops and promotes internet standards.
IP	Internet Protocol. A network layer protocol which transmits data packets according to their address.
ISM	Industrial, Scientific and Medical radio bands. International radio bands originally intended for industrial, scientific and medical use. Using these radio bands is free and does not require permission.
ITU	International telecommunication union. An agency of the united nation that is responsible for information and communication technologies.
LAN	Local Area Network. A small network.
MAN	Metropolitan Area Network. When two or more computers are connected to the same metropolitan area network it is called metropolitan area network. he size of the network is not static. The bigger the metropolitan area is the bigger is MAN.
MAP	Mesh access point. Mesh network access point which is connected only wirelessly.
Mbps	Megabits per second. A unit to measure transmission speed in a communication network.
MCCA	Mesh Coordinated Channel Access. A protocol used by mesh stations to avoid collisions and improve QoS.
MCF	Mesh coordination function. Used in WLAN mesh networks to coordinate mesh access points.
OSPF	Open Shortest Path First. A routing protocol.
PMK	Pairwise master key. Used for frame encryption.

QoS	Quality of service. Defines the quality of transmission.
RAP	Root access point. A mesh network access point which has a wired connection to the Internet and acts as a gateway to mesh access points.
RFC	Request for Comments. Rules developed by IETF and Internet Society for publications concerning technical development of internet.
SAE	Simultaneous Authentication of Equals. Security a algorithm.
SNMP	Simple Network Management Protocol. SNMP was originally developed for managing and monitoring IP-networks.
SSID	Service set identifier. A network identifier used with wireless local area networks.
TTL	Time-to-live. A mechanism that limits the life time of data in the network.
WAN	Wide Area Network. A network that covers a wide area. Can consist of multiple MAN and LAN networks. The most extreme example is the Internet.
WLAN	Wireless Local Area Network. WLAN standards are being defined by IEEE. Originally, WLANs were intended to be used in local environments such as offices and homes.
WMN	Wireless mesh network.

Preface

The research problem for this thesis was provided by Rautaruukki Oy. The research work for this thesis was done by searching various sources from the Internet, by studying published theses, literature and research papers, and by interviewing specialists. The research was mostly done at home but lot of time was also spent in libraries. The demonstration environment was built and configured at Ruukki Metals' steel factory in Raahe.

I would like to thank my supervisor Kari Laitinen for all his guidance during this research project. From Rautaruukki personnel I would like to thank Heikki Anttila for not only providing me the opportunity to work on this interesting project but also for all the help and guidance during this research. I would also like to thank Timo Elf for his professionalism and guidance with technical issues.

I would also like to thank my family, especially my wife Jenny, for the support and encouragement during my studies.

Oulu, Finland, September 2013

Harri Lapinoja

1 The purpose and goals of the research

This thesis is a research document and it is targeted at Ruukki Metals' IT personnel. Ruukki Metals is a part of Rautaruukki Oyj and produces special steel products. Ruukki Metals' steel factory is located in Raahe, Finland.

The usage of automation and information technology is constantly increasing in industrial processes and factories it means that devices need to be constantly connected to each others and the need for networking increases. Wireless networks are often an easier and more economical way of building new or expanding existing networks. At Ruukki Metals' factory WLANs are used for example in internal logistics, mobile machinery locationing and passage monitoring. As using WLANs has become more popular an effective network monitoring has become extremely important in ensuring the proper functioning of the network. The network monitoring tools that are currently in use at Ruukki Metals' steel factory do not provide enough information for network administrators to effectively monitor and solve network issues. Solving networking issues is usually quite time consuming and root causes will often stay unclear.

The target of this research was to investigate what kind of intelligent network monitoring methods and tools are available at the moment and how they can be used to improve network monitoring and network functionality at Ruukki Metals' factory. The high level research problem in this thesis was to make the WLAN at Raahe factory more reliable and effective. In order to reach this objective, detailed information about the network was needed to properly understand root causes for issues. This led us to a low level research problem which was to make the network monitoring and management at Raahe factory more effective. In order to test and demonstrate intelligent network monitoring methods and tools in practice, a small test network was built at Ruukki Metals' steel factory.

2 Wireless local area networks

The benefits of wireless data transfer such as lack of wiring and constant reachability have driven the growth of wireless networks. Wireless local area networks (WLAN) have become a popular way of constructing local wireless networks. The success of this technology is based on using the free ISM band at 2.4GHz and also the 5GHz band. Originally the WLAN connection was designed to be used only at homes and in offices with just few devices. Nowadays however also WLANs are commonly used in large environments such as factories and city wide metropolitan area networks (MAN). In order to understand the design and functionality of the network, it is important to understand the fundamentals of the wireless networking.

2.1 Wireless communications

Wireless communications and data transfer have fundamental differences compared to wired communication. When data is being transmitted through cables, one cable does not significantly interfere with other cables. However radio transmission situation is very different because it is much more challenging to prevent radio waves from distributing to the surrounding area. This means that two transmitters operating at the same frequency are interfering each other in an operation.

One of the most important standardization areas in wireless communication has been the frequency bands allocation. Without an international agreement, it would be close to impossible to have radio broadcasts or a wireless data transfer. ITU (International Telecommunication Union) is the key contributor in coordinating the global radio operations. ITU is a standardization organization working under supervision of the United Nations. It is nowadays responsible for

the whole ICT sector regulations, recommendations, data transfer coordination and harmonization of national regulations (Granlund 2001, 230.)

IEEE (Institute of Electrical and Electronics Engineers) is the world's largest professional association. The purpose of the association is to advance technical innovation and excellence. To archive this mission the association is organizing seminars and meetings. IEEE also publishes nearly a third of the world's technical literature in electrical engineering, computer science, and electronics. This includes more than 148 transactions, journals, and magazines published annually (IEEE 2013, date of retrieval 4.7.2013.) IEEE is also a leading developer of international standards for telecommunication. This includes 802.x standards which are fundamental to wireless communication.

ETSI (European Telecommunication Standards Institute) is an organization whose purpose is to produce data transmission recommendations for European countries. The recommendations published by IEEE are not compulsory but because they are composed by the communities that are actually using those recommendations, they are practical and necessary. Quite often ETSI recommendations have an impact on the development of European Union directives (Granlund 2001, 9.)

2.2 Radio frequencies and spectrum allocation

There are only limited amount of radio frequencies and in Finland the usage of radio frequencies is controlled by Viestintävirasto. The detailed tables of available radio frequencies can be found on Viestintävirasto's Internet page. In general the radio frequencies are being separated by the wave length as demonstrated in table 1.

TABLE 1. Radio frequencies (Wikipedia 2013, retrieval date 26.8.2013)

Frequency	Wavelength	Designation	Abbreviation
3 – 30 Hz	10^4 – 10^5 km	Extremely low frequency	ELF
30 – 300 Hz	10^3 – 10^4 km	Super low frequency	SLF
300 – 3000 Hz	100 – 10^3 km	Ultra low frequency	ULF
3 – 30 kHz	10 – 100 km	Very low frequency	VLF
30 – 300 kHz	1 – 10 km	Low frequency	LF
300 kHz – 3 MHz	100 m – 1 km	Medium frequency	MF
3 – 30 MHz	10 – 100 m	High frequency	HF
30 – 300 MHz	1 – 10 m	Very high frequency	VHF
300 MHz – 3 GHz	10 cm – 1 m	Ultra high frequency	UHF
3 – 30 GHz	1 – 10 cm	Super high frequency	SHF
30 – 300 GHz	1 mm – 1 cm	Extremely high frequency	EHF
300 GHz - 3000 GHz	0.1 mm - 1 mm	Tremendously high frequency	THF

All frequency bands, excluding ISM band (2400,000-2483,500 MHz) are subject to license. In addition, using some frequency bands require a permission from authorities.

2.3 Data transmitting in a radio channel

Radio waves are actually electromagnetic waves. Their energy appears as electric and magnetic fields. These fields appear together since a change in an electric field also causes a change to a magnetic field. When radio frequencies travel towards their destination, they will use different routes and have different amplitude at their destination. In an antenna the waves will be summed and the receiver sees only one signal. Since the phase difference between separate components affects greatly to the summation of the signal, the final difference between the transmitted and received signal depends on whether the summed signals will cancel or amplify each other. When comparing two parallel receivers, the amplitude of the received signal can have a difference of over dozens of decibels.

2.3.1 Path loss

Path loss means that the energy of the signal is decreasing. Path loss for radio waves can be calculated using the following formula.

$$L = 20\ \log_{10}\left(\frac{4\pi d}{\lambda}\right)$$

Where L is the path loss in decibels, λ is the wavelength and d is the transmitter-receiver distance in the same units as the wavelength (Wikipedia, retrieval date 4.7.2013).

2.3.2 Fading

Fading is divided into two parts. Fast fading and slow fading, which are

demonstrated in Figure 1. Slow fading means the change in the average of the received signal. This change results from an alternating terrain, blocking objects etc. Fast fading means that parts of the signal are being summed. This is caused by the movement of a transmitter and multipath fading.

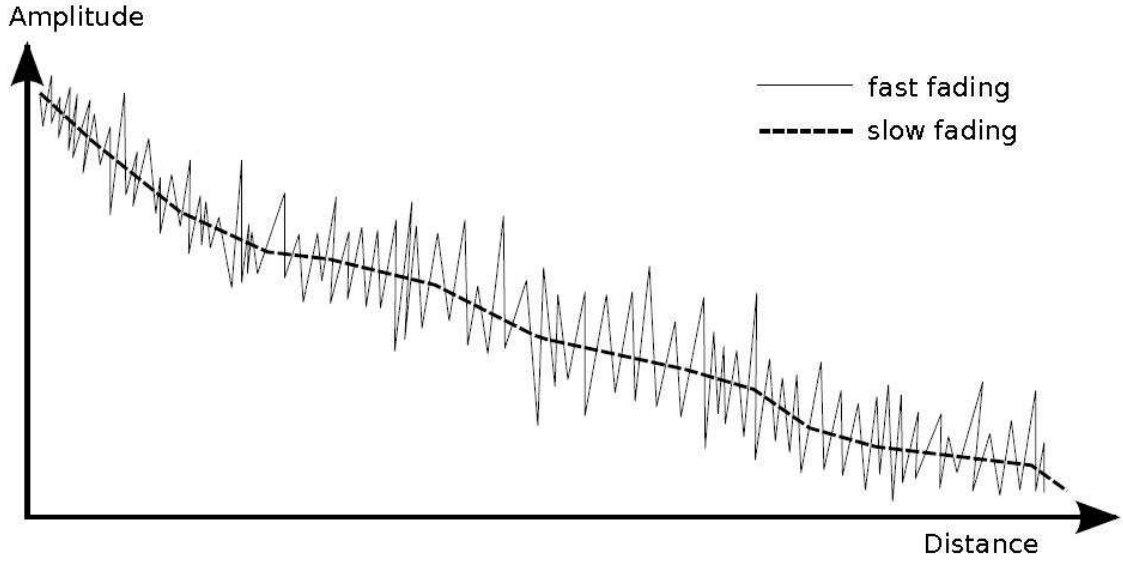

FIGURE 1. Fast and slow fading in respect to the distance. (Mahmood, F. 2013. retrieval date 13.9.2013).

2.3.3 Multipath propagation

Multipath propagation is a phenomenon of signal dispersion. This is a big challenge in wireless data transfer because a signal can bounce from objects, terrain, etc. and the same signal can use multiple paths and some signals can reach the destination travelling routes many times longer than others. This means that signals reach the destination at different times and with a different amplitude. Figure 2 demonstrates multipath propagation.

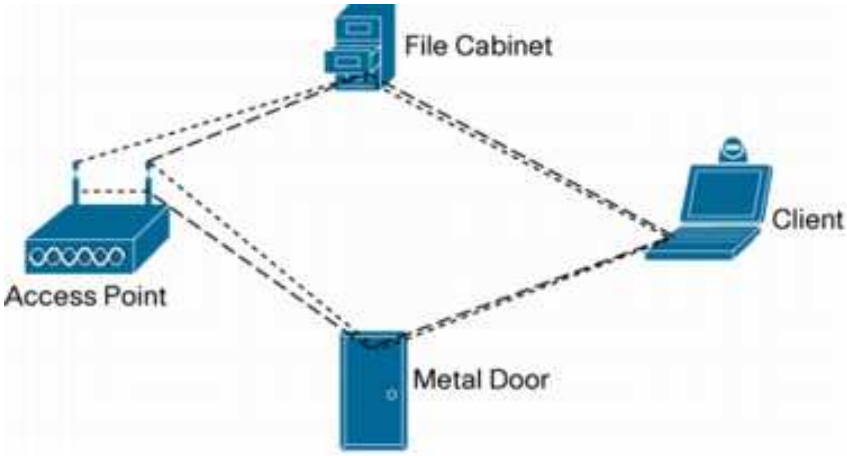

Figure 2 Multipath propagation. (Cisco Systems, Inc. 2013. Date of retrieval 13.9.2013)

2.4 802.11

802.11 is the IEEE standard for wireless local area communication. It was first introduced in 1997. It has since had many amendments. The most important ones concerning this thesis are briefly introduced below. (Granlund 2001, 230)

2.4.1 802.11a

802.11a defines 54 Mbps transmission speed using a 5-GHz frequency band (Granlund 2001, 238). Channel utilization of 802.11a is demonstrated in Figure 3. 802.11a was introduced in order to allow more bandwidth using a 5-GHz frequency band. However it was not as successful as 802.11b because of its smaller transmission range and more expensive network equipment (Wikipedia, retrieval date 26.8.2013.)

Channel Identifier	36	40	44	48	52	56	60	64		149	153	157	161
Center Frequency	5180	5200	5220	5240	5260	5280	5300	5320		5745	5765	5785	5805
Band	UNII-1				UNII-2					UNII-3			

Channel Identifier	100	104	108	112	116	132	136	140
Center Frequency	5500	5520	5540	5560	5580	5660	5680	5700
Band	New UNII-2 Channels							

220339

FIGURE 3. 802.11a channel utilization (Cisco Systems, Inc. 2013. Date of retrieval 13.9.2013).

2.4.2 802.11b/g

802.11b defines a transmission speed of 11 Mbps using the 2.4 GHz frequency band and 802.11g defines the transmission speed of 54 Mbps using the 2.4GHz frequency band (Granlund 2001, 240). Channel allocation of 802.11b/g is demonstrated in Figure 4.

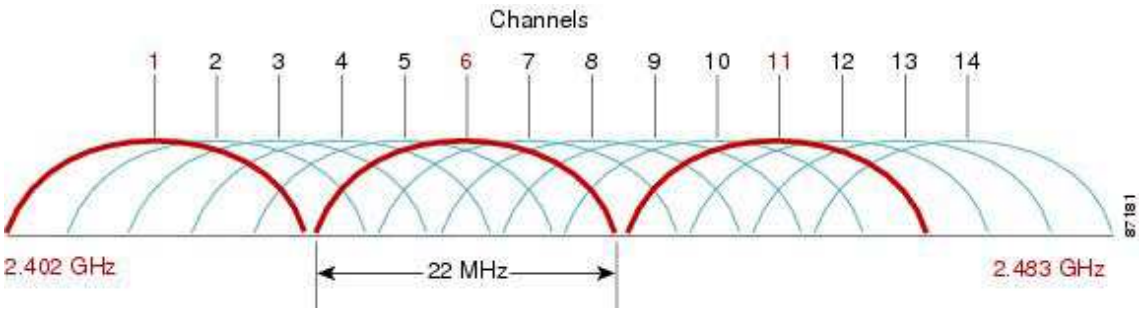

FIGURE 4. 802.11b/g channel allocation (Cisco Systems, Inc. 2013. Date of retrieval 13.9.2013).

2.4.3 802.11n

802.11n defines the usage of multi radio technology with 2.4 GHz and 5 GHz frequency bands. Multi radio technology means that 802.11n devices are able to use 2.4 GHz and 5 GHz bands. It is also possible to use three antennas in one device which enables using three different channels simultaneously. This can be used to increase the transmission bandwidth or range.

2.4.4 802.11s

802.11s introduces recommendations for WLAN mesh communication. It was released in 2011. WLAN mesh enables access points to form a connection between each other without wired links.

3 WLAN mesh networks

As the WLAN technology has been widely accepted for building WAN and MAN networks, the demand for new more economical ways to expand the networks has aroused. Traditional networks need wirings to all access points which increases building costs of the network. Using mesh technology is more economical because it makes it possible to remove the costly wiring between access points.

3.1 Advantages and challenges

Building traditional networks where all access points are connected to wires, is problematic for two main reasons. Building wide area networks with this technology is not cost efficient. Secondly the transmission power on unlicensed 2.4 GHz (802.11b/g/n) and 5 GHz (802.11a/h/j/n/ac) bands is regulated by laws which resolute to quite small cell sizes. The solution to the problem is a mesh network. Mesh networks have multiple advantages compared to traditional technology. The first benefit is obviously the increased flexibility over the wired networks. Wired access points need to be connected to a switch port after every 100 meters but with a mesh network, only the first access point may be wired and other access points are connected through it, even if they are moving objects. The benefit of flexibility is also that access points can have multiple paths for transmitting the data. With the Ethernet cable there is only one possible path, but with a wireless link any access point may be in range with many other access points and it can choose the best radio path. This possibility for any access point to be able to connect to one or several other access points is the very definition of a mesh network. The second benefit is that a mesh network is self-forming. This means that if an access point has multiple paths to a wired network, it automatically chooses the best path. Building up a mesh network may be as simple as adding new access points and making sure they

are in range of other access points. The third benefit is that a mesh network is self-healing. If an access point has several possible paths to a wired network, removing one access point from the mesh cloud would just simply force other access points to discover the best path to wired network. Figure 5 demonstrates the functionality of a mesh network and possible routes between nodes.

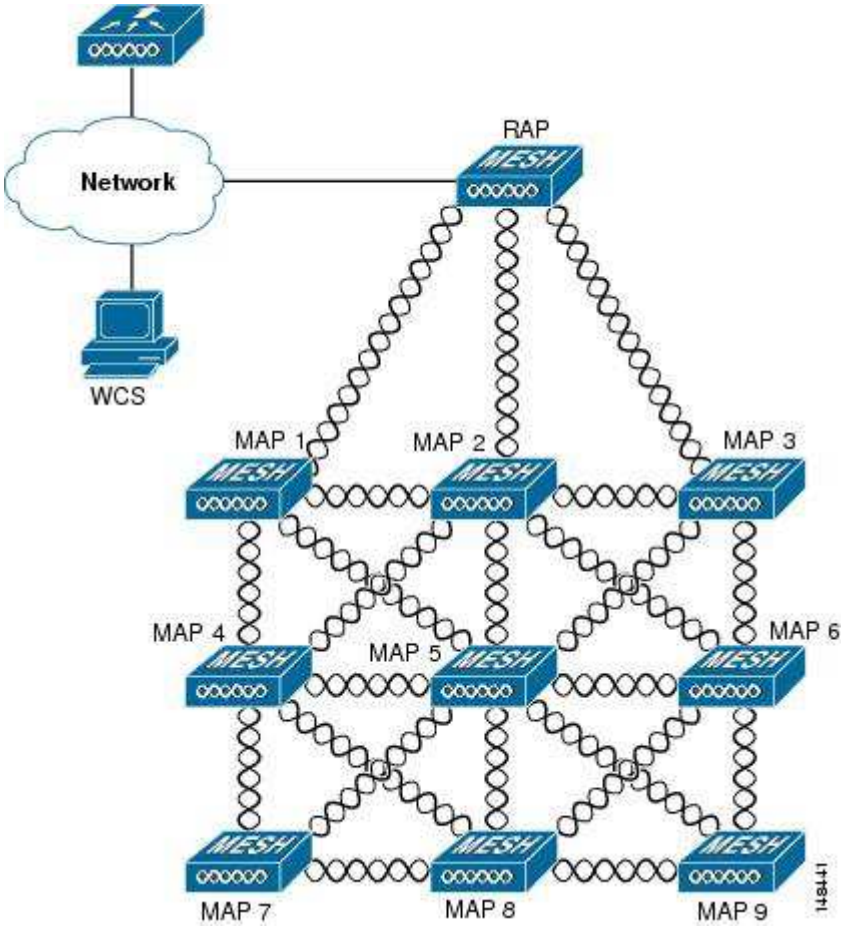

FIGURE 5. WLAN mesh network (Cisco Systems, Inc. 2013, date of retrieval 8.9.2013).

3.2 Discovery and formation

When a mesh station boots up, it needs to find out available networks. This is called discovery. When it finds a correct network it will try to join it. Mesh stations have two methods for detecting each other. Passive scanning (observation of beacon frames) or active scanning (probe frame transmission). 802.11 beacon frame contains information about the network and it is frequently

sent by access points. 802.11 probe frames are used when a new device wants to join the network. The mesh-specific beacon and probe frames contain a mesh ID (the name of a mesh), a configuration element that advertises the mesh services, and parameters supported by the transmitting mesh station. This functionality enables mesh stations to search for suitable peers (e.g. other mesh stations that use the same path selection protocol and metric). Once such a candidate peer has been identified, a mesh station uses the mesh Peer Link Management protocol to establish a peer link with another mesh station. Even when the physical link breaks, mesh stations may keep the peer link status to allow for quick reconnection (Hiertz et al. 2010, 106-107.)

Mesh stations use only a single transceiver. This means that a mesh operates in a single frequency channel only. However, with multi transceiver devices different frequency channel meshes can be unified into a single LAN. In figure 6 there is an example where multiple meshes operate in different frequency channels. Hiertz et al. explain the mesh formation in the figure as follows.

> "Mesh stations C, D, and E collocate within a device that has three independent transceivers. Incorporating an 802 bridge in the device, the collocated mesh stations interconnect and help to forward frames between their meshes. Consequently, a single WMN can be constituted." (Hiertz et al. 2010, 107)

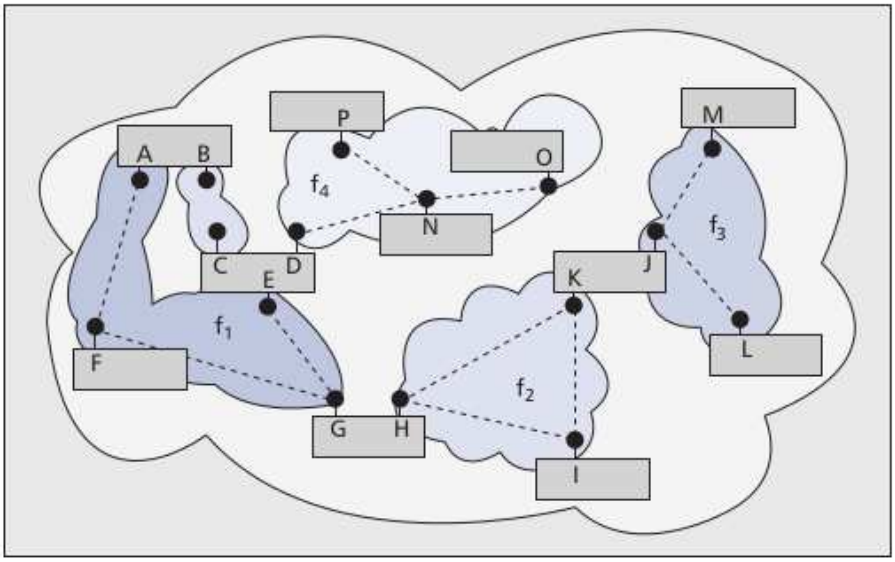

FIGURE 6. Mesh formation (Hiertz et al. 2010, 107)

3.3 Power management and synchronization

Synchronization and power saving features use a time reference that is provided by all beacon frames. Mesh stations using a power saving feature are either in deep or light sleep mode. When a mesh station is in light sleep mode, it will switch to full power whenever the mesh station itself or a neighbor is expected to transmit a beacon frame. When the mesh station is in deep-sleep mode, it will only wake up when transmitting its own beacon frames. During the awaking period of the mesh station that is following the beacon, it can be informed of the buffered traffic.

3.4 The medium Access Control in 802.11s

The medium access control in 802.11s has some differences compared to 802.11. Mesh stations implement the mesh coordination function (MCF) which has a mandatory and an optional scheme. MCF uses the contention-based protocol called Enhanced Distribution Channel Access (EDCA) for the mandatory part. EDCA is an improved version of the basic 802.11 distributed coordination function (DCF). When using the DCF, a station transmits a single frame of random size. Using the EDCA, a mesh station may transmit multiple frames, but the total transmission duration may not exceed the transmission opportunity limit. The targeted receiver acknowledges the successful frame reception. The EDCA also separates four traffic categories with different priorities in medium access. This provides a limited support of quality of service (QoS). In order to enhance QoS and help mesh stations to avoid collision, MCF describes an optional mesh Coordinated Channel Access (MCCA). When the MCCA transmission ends, mesh stations use EDCA for medium contention again (Hiertz et al. 2010, 108.)

3.5 Congestion control

In mesh networks a congestion control is very important as the mesh frame might have already traversed several hops to reach the congested mesh station. Sending same data several times will congest the network quickly. 802.11 networks rely on a carrier sensing technology for network access. The technology has been used in wired networks and it has been further developed in order to meet the requirements of wireless networks. 802.11 uses CSMA/CA-protocol (Carrier Sense Multiple Access/Collision Avoidance) as the basic technology for the congestion control and data transmit. In simple, the carrier sensing technology works so that the transmitting device listens to the radio frequency and transmits when the frequency is free (Granlund 2001, 242-245.)

Optionally 802.11s uses a management frame for the congestion control. The management frame indicates the expected duration of congestion and can request the neighboring mesh station to slow down (Hiertz et al. 2010, 108.)

3.6 Security

802.11s uses Simultaneous Authentication of Equals (SAE) algorithm for security between peers. Peers form a pairwise master key (PMK) which they use to encrypt their frame. SAE differs from the traditional 802.11 encryption also in a way that it does not rely on keying hierarchy. In pairwise encryption each link is secured independently. This also means that 802.11s does not provide the end-to-end encryption. A mesh station is required to renew its broadcast traffic key with every new peering established in order to broadcast traffic to all authenticated peers (Hiertz et al. 2010, 108.)

3.7 Path selection

All mesh stations inside a mesh use the same path metric and path selection

protocol. 802.11s defines a mandatory default scheme for both of them. Because it has an extensible framework, it can also be replaced by other solutions. Termed airtime metric is the default metric and it is indicating an overall cost of the link by taking into account date rate, overhead, and frame error rate of a test frame of size 1 Kbyte. Hiertz et al. explains path selection as follows.

> "The default path selection protocol, Hybrid Wireless mesh Protocol (HWMP), combines the concurrent operation of a proactive tree-oriented approach with an on demand distributed path selection protocol (derived from the Ad Hoc On Demand Distance Vector [AODV] protocol). The proactive mode requires a mesh station to be configured as a root mesh station. In many scenarios this will be a mesh station that collocates with a portal. As such, the root mesh station constantly propagates routing messages that either establish and maintain paths to all mesh stations in the mesh, or simply enable mesh stations to initiate a path to it. Mesh stations also rely on AODV when a root mesh station is unavailable. When no path setup messages are propagated proactively, however, the initial path setup is delayed. To allow for even simpler configuration, vendors may opt not to implement HWMP at all. As an example, a battery-limited handheld device may refrain from frame forwarding to minimize power consumption. Accordingly, it does not propagate path information and behaves like an end station. However, the device is still able to request the frame forwarding service from neighboring mesh stations" (Hiertz et al. 2010, 108-109.)

3.8 Known challenges

As all technologies WLAN mesh technology has also challenges. Some of the challenges are common to all wireless data transmitting such as signal fading and summing. The following represents the most important challenges of the WLAN technology.

3.8.1 Multihop problem

Every time a mesh access point connects to another mesh access point and acts as a router, it reserves a channel for the conversation between the two

access points. As the two access points reserve a bandwidth for their conversation, the available transfer capacity for payload is reduced. In early versions of WLAN mesh networks, only a band of 2.4 GHz was used and the result was that very few hops could be made because the data throughput would drop dramatically after each hop. The modern versions of the WLAN mesh networks are using multi radio technology. With this technology mesh access points are using a band of 5 GHz to discuss with each other and a band of 2.4 GHz to discuss with clients. This enables multiple hops without losing the throughput of the data.

3.8.2 Hidden node problem

Hidden node problem arises when a node is located between two access points in a way that the node is able to connect with both access points but the access points cannot detect each other. This would mean that without knowing from each other the access points might be transmitting in the same channel. This will interfere or even block the transmission. Usually, this is not a problem in an independent network but the issue arises when two wireless networks with different SSIDs are in the same range. This problem is best avoided by controlling the cell sizes of access points. This can be done by using directional antennas or by limiting the transmission power of the access point. Figure 7 illustrates hidden node problem.

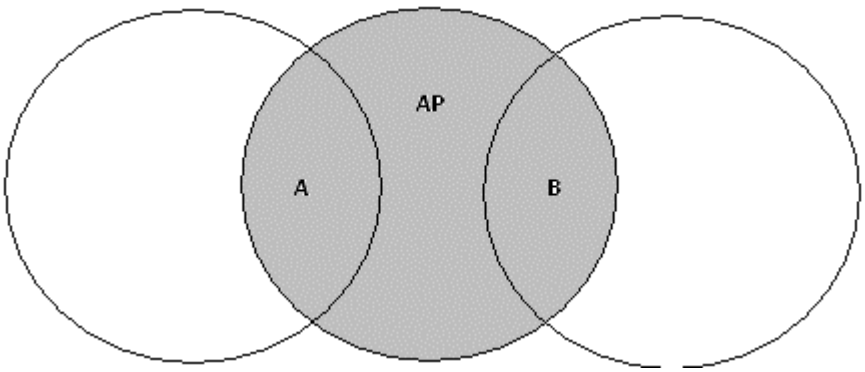

FIGURE 7 Hidden node problem (University of Adelaide 2013, retrieval date 14.8.2013).

3.8.3 Other issues

Some military and weather radars operate partially on the same 5 GHz frequency range than IEEE 802.11b/n devices. In Europe all 802.11 devices operating at a band of 5 GHz must contain a dynamic frequency selection (DFS) feature. This means that devices must be able to identify when a channel is being used by a radar and immediately stop listening the channel and leave it empty for a certain time.

4 Wireless Local Area Network monitoring methods

Several methods are available for monitoring wireless local area networks. WLAN networks are based on IP (internet protocol) technology which means that network monitoring methods such as ICMP and SNMP can be used in network monitoring. These methods are convenient as they do not need any additional hardware and network devices usually support these methods as standard. When more detailed information is needed such methods as vicinity sniffing and spectrum analyzing can be used.

4.1 ICMP

Probably the most commonly used protocol is Internet Control Message Protocol (ICMP). ICMP offers some commonly used utilities like ping and trace route. Ping operates by sending ICMP echo request packets to the target host and waiting for an ICMP response. Trace route also uses ICMP echo request packets and determines by using a time-to-live (TTL) value the amount of routers that are used in a route to the destination.

4.2 SNMP

Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that require administrative attention. SNMP presents management data in the form of variables in the managed systems. These variables may then be queried (and sometimes set) by managing applications. SNMP itself does not define which variables are accessible; Rather, SNMP uses an extensible design, where the available information is defined by Management Information Bases (MIBs) that

are often proprietary to individual vendors. MIBs describe the structure of the management data of a device subsystem in a hierarchical namespace containing Object Identifiers (OID). Each OID identifies a variable that can be read or set via SNMP.

SNMP was introduced in 1988 to meet the growing need for a standard for managing Internet Protocol (IP) devices. The main core of SNMP is a simple set of operation that provides the ability to query and set the state of some devices to network administrators. Although SNMP is capable of managing a wide variety of network devices (including but not limited to printers, personal computers, servers, power supplies, etc.), it is typically associated with routers and other network devices . Just as with other protocols, SNMP is defined by The Internet Engineering Task Force (IETF) using Request for Comments (RFC) specifications (Johnston 2009, 8.)

4.3 Sniffing

Vicinity sniffing has been considered to be the basic method and often the only reliable method for measuring the functionality of the wireless network. The basic idea and functionality of vicinity sniffing is to implement physical “sniffers” inside a transmission range of wireless network access point. Usually a sniffer is a laptop equipped with a wireless network card. The purpose is to capture all incoming and outgoing wireless traffic of the monitored device. Studies have shown that even though vicinity sniffing has been considered a reliable measurement method, the amount of captured data depends heavily on positioning of the sniffer (Johnston 2009, 11.)

4.4 Spectrum analyzing

Spectrum analyzing is used for measuring the radio frequency signals. Spectrum analyzing for wireless networks can be done by using spectrum

analyzers on a mobile platform such as a car. This way it is possible to measure signal strengths for the whole network coverage area. Nowadays it is also common for the access points to have spectrum analyzing capability features. Usually this means that access points are fitted with separate spectrum analyzing hardware. Spectrum analyzing is a good method for detecting interference and radio noise.

4.5 Intelligent network monitoring

Network monitoring is an important part of the flawless functioning of every network. Traditionally network monitoring tools provide only the very basic methods for monitoring the network. The tools are probably using only ping requests to check if access points or clients can be reached. These kinds of tools, however, provide very limited information about the network. Nowadays local area networks offer by default the possibility to use SNMP traps and the most modern systems also provide a spectrum analyzing capability. This has led to more sophisticated monitoring tools. However, the benefits of these tools are not yet necessarily broadly understood. Intelligent network monitoring can save a lot of costs by providing more detailed information to network operators or it can even be able to heal the network automatically. Naturally, this also affects the functioning of the network and data transmitting.

5 Network environment at Raahe factory

The following sections describe the wireless local area network environment at Ruukki Metals' steel factory in more detail. The network structure, devices, challenges, issues and currently used monitoring tools are being introduced.

5.1 Network structure

The network environment at Ruukki Metals' factory is using the LWAPP protocol based centralized network management model. The network structure is demonstrated in figure 8. The network is built using the Cisco technology. The production related network at Raahe factory is controlled with four Cisco controllers. The controllers are used to route the traffic of a WLAN network and also to handle the interface to the Internet. The network is built so that three controllers are in use simultaneously and one controller is at backup. The controllers are also able to replace each other so all four controllers are available constantly. An access point can connect to any controller but every access point has a predefined main controller and also a back up controller. There are three types of access points in use at the network. Local access points are connected directly to a wired network and they are mainly used inside buildings. Mesh access points are used to cover outside areas of the network. Some of the mesh access points are connected by a network cable and those access points can also act as access points to other mesh access points. The third type of access points are only connected through air link.

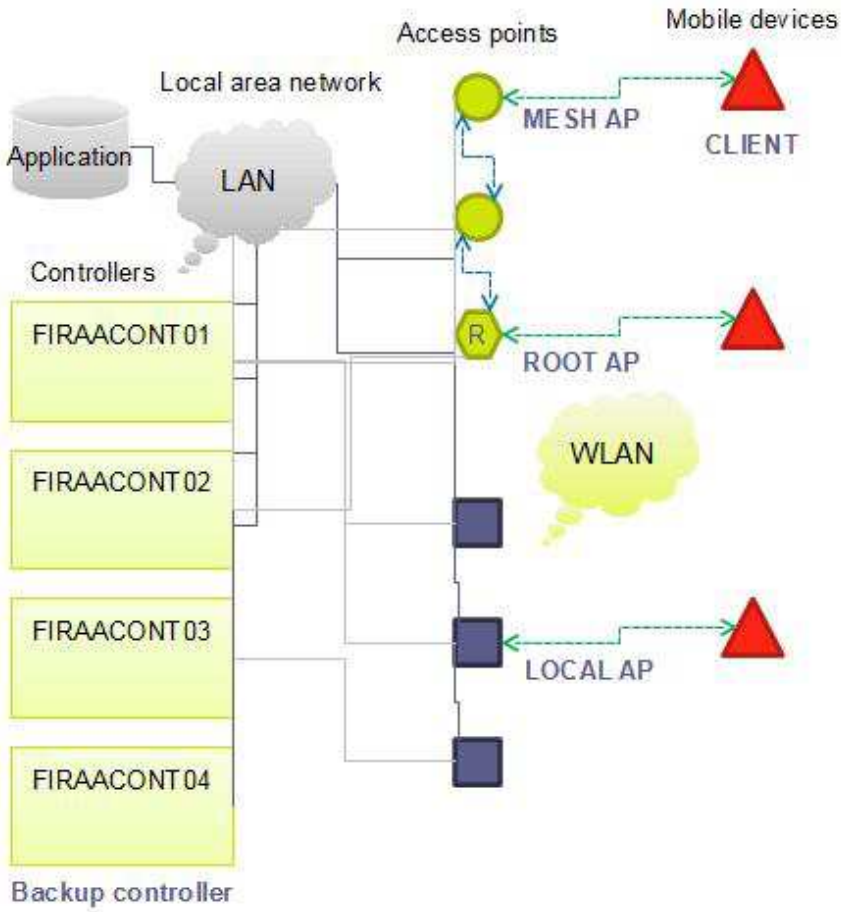

FIGURE 8. Ruukki Metals WLAN diagram (Anttila, H. 2012. Raahen tehtaan langattomat verkot, WLANit. Power point presentation 20.5.2013. Rautaruukki Oyj).

The network at Raahe steel factory has five bridge groups. The purpose of the bridge groups is to prevent clients from connecting to access points from different groups. The groups are geographically formed so that access points form small size network environments to a certain area of the factory and also that one separate area that is used for some certain process has its own bridge group. This way two bridge groups that are located next to each other do not interfere the functioning of the neighboring bridge group devices. If some mesh access point is not connected to a network it will automatically connect to the nearest root access point in the same bridge group. The access point will not connect to a root access point which belongs to another bridge group. However, data transmission routing is done by predefined controllers despite bridge groups (Anttila 20.5.2013, presentation.)

5.2 The challenges in a steel factory environment

Wireless communication methods, such as WLAN, are based on using radio frequencies. This means that steel factory environment introduces plenty of challenges for wireless communication. For example radio frequencies do not travel very well through metallic surfaces, which can cause signals to fade or reflect. A steel factory naturally has lots of metallic surfaces because the end product is steel. Storages may contain large quantities of steel products and steel products are also moved around the factory during the manufacturing process. In addition, large vehicles that in many cases are mobile are being operated and they may block signals from time to time. Large powerful machinery at product lines can also cause interference by causing radio frequency noise. For example, large electrical motors can cause interference to wireless communication. These challenges also mean that the positioning of the network devices is also one key factor in the proper functioning of the network. If access points are installed incorrectly they can become sensitive to interference and in the worst case that can be the source of interference. It is also possible that an incorrect installation may cause a physical breakage of the device.

In addition there is interference coming from the surrounding environment, for example the interference from radars. Utajärvi weather radar, figure 9, has been identified as one of the radar interference source.

Wireless local area network at a steel factory has to be able to cope with these challenges and perform reliably. In short, the wireless network must be able to cope with varying conditions and with as less maintenance as possible.

FIGURE 9. Utajärvi weather radar (Kaleva 2013, retrieval date 14.8.2013).

5.3 Network devices at Raahe factory

Quite often enterprise networks have been expanded in the course of time and in different cycles. This means that the network consists of many different type of devices which can belong to a whole different product family or generation. Making these devices working together can be challenging and usually compromises have to be made. For example, it is common that devices from different product families have varying features and some of those features can only be used with similar products. The WLAN network at Ruukki Metals' factory has also different types of devices. Some of the devices are of different type purely because they are meant for different purposes. For example, some devices are used inside buildings and some are used in open areas. This sets different kinds of demands, for example for shielding. The access point models used in the network are introduced in table 2.

TABLE 2. Access point types used at Ruukki Metals factory area.

Cisco Aironet LAP1242AG-E-K9	Used inside buildings. Supports IEEE 802.11a/b/g recommendations. Designed to challenging RF environments
Cisco Aironet LAP1510AG-E-K9	Outdoor WLAN mesh station. Supports 802.11b/g recommendations.
Cisco Aironet CAP1552E-E-K9	Outdoor WLAN mesh station with Cisco Clean Air capability. Supports IEEE 802.11n recommendation.

The access points are being controlled by four Cisco 4402–50 controllers. Three of these controllers are in use at the same time and one is a backup controller.

5.4 Known issues

The network is known to have issues with the functionality of the mesh access points. The access points might drop out of the network and are not able to join the network again for a long period. This leads to an improper functioning of the network and causes lots of work for network monitors. If an access point drops out of the network from time to time, it usually is not a severe issue for the network as mesh networks are self-healing. Also if two mesh stations drop out of the network far away from each other, it is not a problem. However, if two or more access points that are located next to each other lose connection to the network, the situation is very likely critical. Usually this means that some end

devices are being left without a connection and this might even cause the loss of data.

5.5 Network monitoring tools

At the moment network operators are using a combination of different tools. Some of the tools are manufactured specifically for the company. The tools are using mostly icmp requests for acquiring information from the network. These methods give only the very basic information about the network. An ideal situation would be to have one tool that would provide enough information to determine causes for possible networking issues. In figure 10 there is an example view of the Orion network monitoring tool. By using just a basic Ping command the tool determines if the access point is available or not.

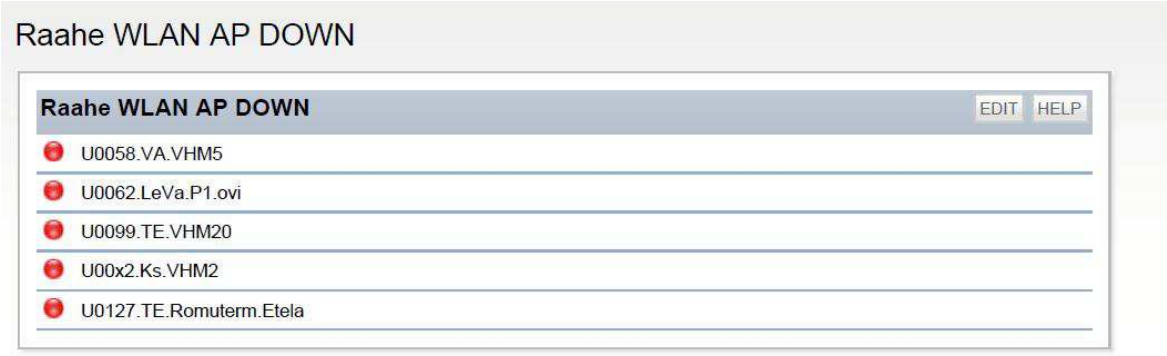

FIGURE 10. Ruukki Metals current network monitoring tools. AP down view.

In figure 11 there is another example view of the current monitoring tool. This view illustrates which access point has lost most packages.

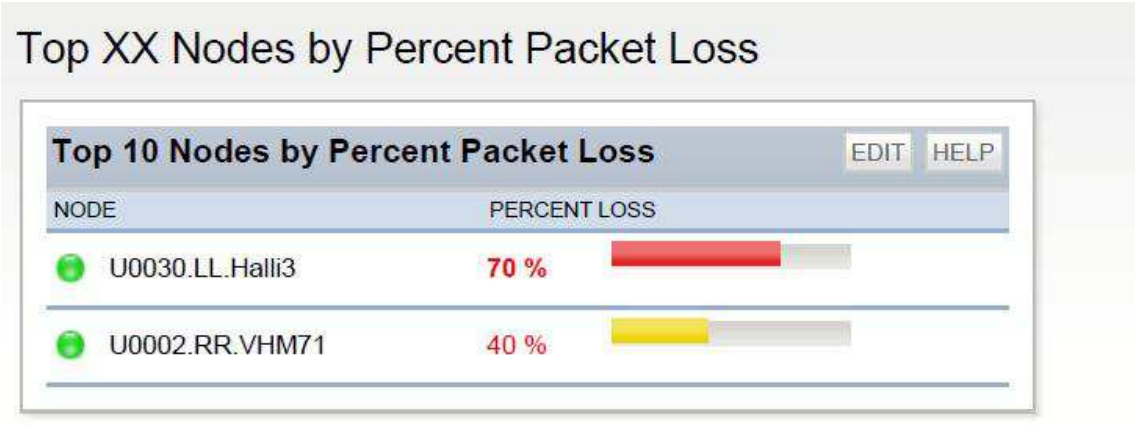

FIGURE 11. Current network monitoring tool, packet lost view

6 Research and results

The research for this thesis was mainly done by studying research papers and articles but also by interviewing specialist and by participating in meetings. The research concentrated on different monitoring methods for wireless local area networks and also on the features and characteristics of the selected software and network environment. A demonstration project was carried out to demonstrate intelligent network monitoring in a real life environment. The demonstration project and results are described in more detail in the following sections.

6.1 Demonstration project

The purpose of the demonstration project was to test intelligent network monitoring methods and tools in a realistic environment. This would also give the possibility to gather data and feedback from network administrators. While defining the demonstration project environment, a decision to use Cisco products was made, mostly because existing network is built by using Cisco devices and possible positive results from this research could be easily implemented to the existing environment. Also, several other facts were in favor of choosing Cisco software to be used in this demonstration project:

- The software was provided by the same manufacturer as the network devices that would be used in this project. It was likely that this would provide a better functionality of the system and also support was more easily available in case issues arose.
- The software had a 60-day free evaluation period which was enough for the purposes of this research.
- If the software was found to be useful, it would be easy to continue using it by just purchasing a license.

The demonstration project environment consisted of Cisco 1552E-series and Cisco 1522E-series wireless local area network access points, one server computer, which had an VmWare Esxi virtual server environment, a Cisco virtual controller and Cisco Prime Infrastructure software programs installed. Cisco 1552E-series access points, illustrated in figure 12, have a Cisco Clean Air capability. Clean air is a marketing name of Cisco technology for spectrum analyzing capabilities integrated in network devices. This technology was hoped to provide more information about the radio interferences in the factory area. It could also demonstrate how to use this information for intelligent wireless network monitoring.

Esxi is virtualization software for servers. It enables the virtualization of server's physical resources. By using virtual servers, it is possible to allocate resources effectively to multiple applications. It also combines physical resources from different locations to one or many different virtual machines. This makes using physical resources much more effective. In this demonstration project only one physical device was used as a server. The Cisco virtual controller is software that virtualizes network controller hardware. By using the software, it is possible to build a complete network without a dedicated controller device. The software is best suited to small networks where the amount of traffic is low and the controller performance is not an issue. Therefore, using the virtual controller in this demonstration project was suitable. The software comes with a 60-day evaluation license, which is also long enough for demonstration purposes. Cisco Prime Infrastructure is software for network monitoring and management. It is fully compatible with Cisco 1552E-series access points and provides a graphical interface for viewing radio spectrum utilization. The tool also uses SNMP to gather information about the network and comes with a logging feature. Logging gives more information about the network functionality and makes it possible to trace networking problems. Cisco Prime Infrastructure was also briefly tested with the actual production WLAN at the steel factory site.

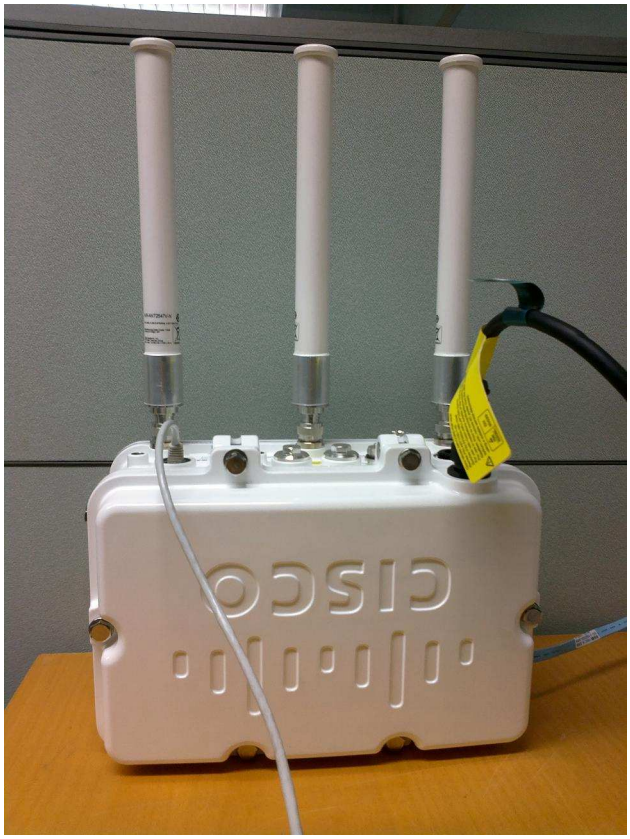

FIGURE 12. Cisco Aironet 1552E WLAN access point.

6.1.1 Installing and configuring the monitoring environment

Cisco provides a very detailed, easy to use guide of how to install the Cisco Prime Infrastructure and virtual controller software programs. The programs are installed on a virtual server and they require the VMWare Esxi environment as a platform for the installation.

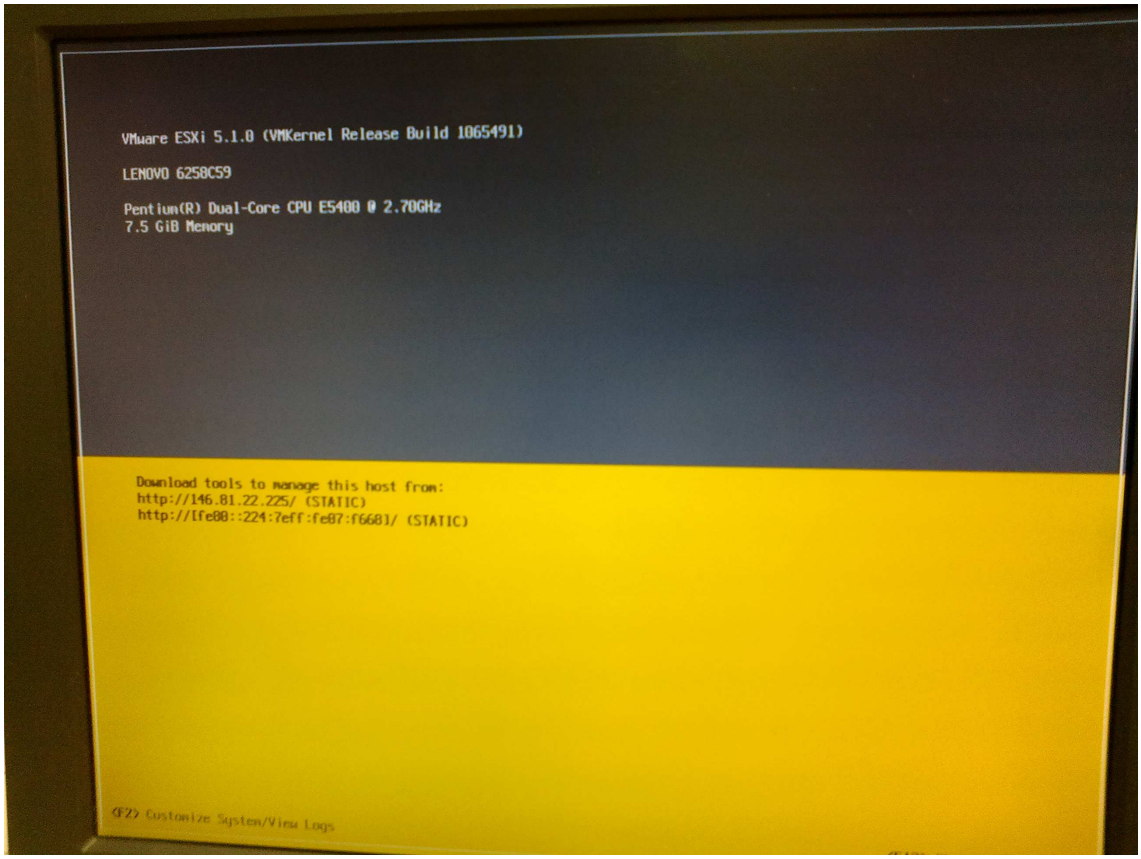

FIGURE 13. Esxi main menu.

Cisco Prime Infrastructure installation guide defines the minimum hardware requirements for a server and those requirements were used as a reference when selecting the server hardware. The server that met the requirements was available and was used for this project. Esxi is installed as a standalone installation and no other operating system can be installed on the same computer. After the installation, Esxi client software is used to configure the server and to allocate resources to virtual machines. Client software is also used to deploy .ova or .ovf -files which are open standards for packing virtual appliances. The main view of Esxi client software is illustrated in figure 14. The Cisco Prime Infrastructure and Cisco virtual controller are provided as ova-files. The software is installed by just opening the .ova-file Esxi client software.

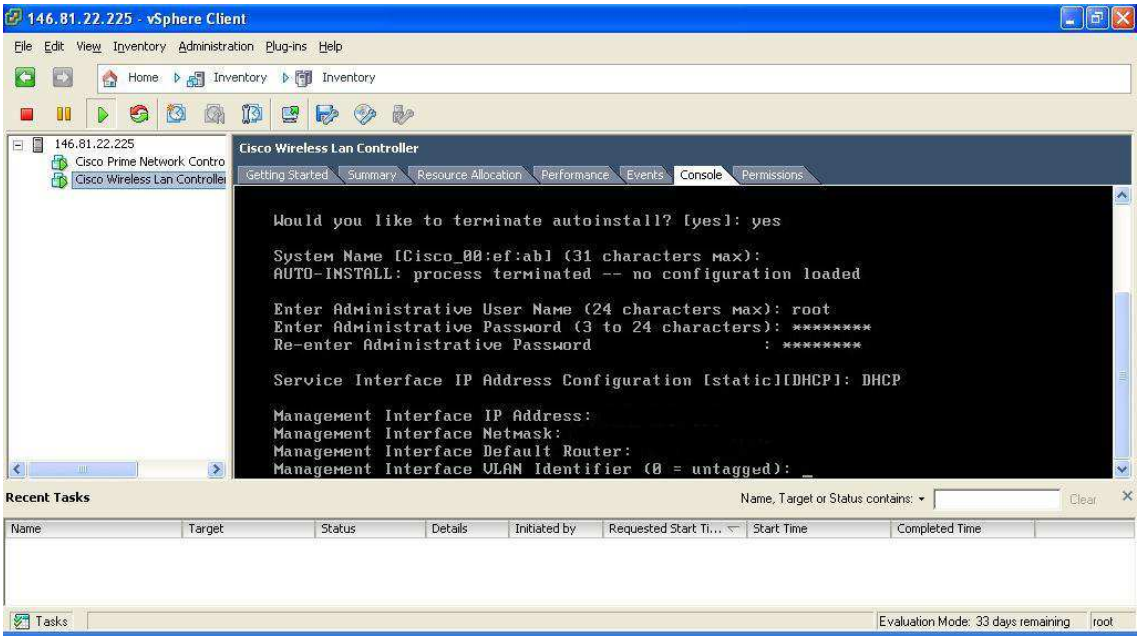

FIGURE 14. Esxi client.

The virtual controller software does not require as much hardware power as the Cisco Prime Infrastructure an and old desktop PC was used as a hardware platform. The virtual controller also requires Esxi installation and the software was similarly deployed from .ova file than the Cisco Prime Infrastructure. When the server is installed, it is first configured from a console with very basic network settings such as the IP address and so on. The Esxi main menu view is illustrated in figure 13. After initial setup, it is possible to use a browser to setup a more detailed setup of the controller. The virtual controller is accessed by a network browser. The login page which is illustrated in figure 15, has the same visual appearance as the login page of the physical controller.

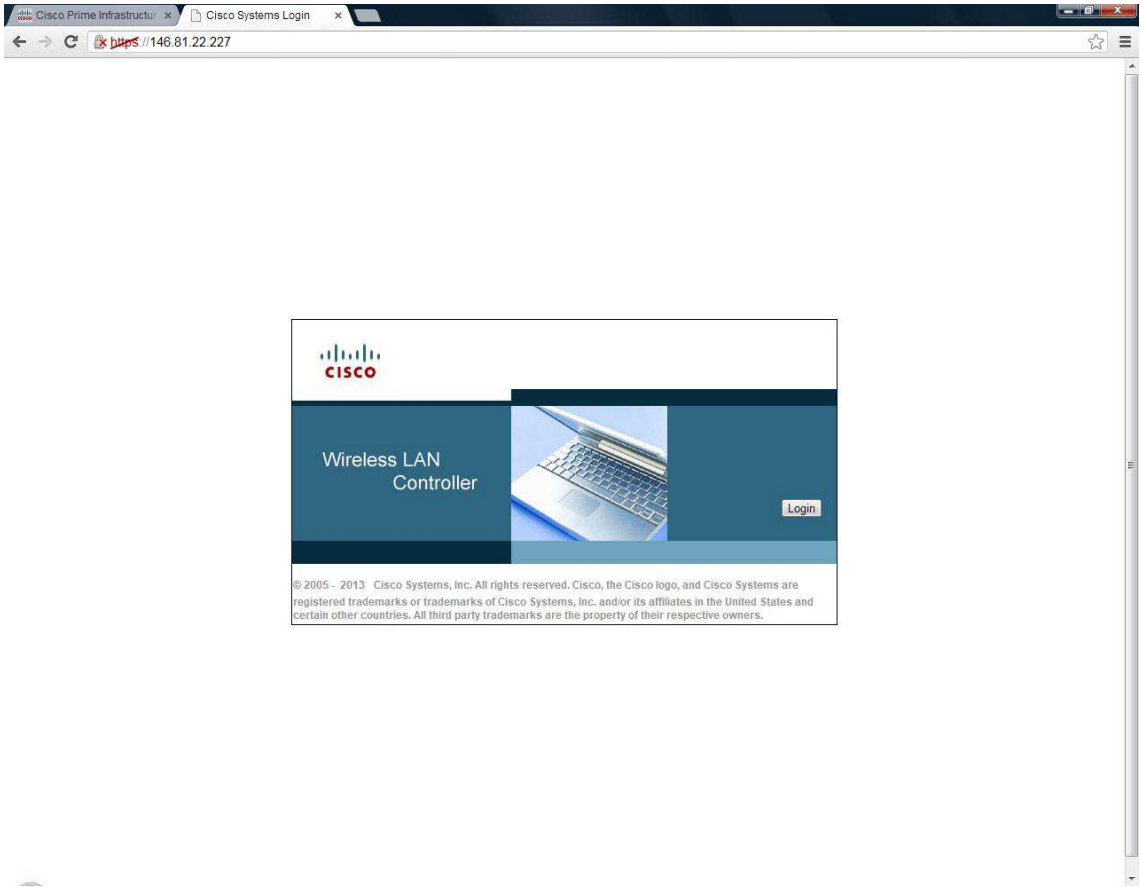

FIGURE 15. Cisco virtual controller login screen.

In this demonstration, a separate subnet was created for the devices that were used in this setup. When the controller is up and running, access points are able to join it. It is possible to filter access points so that only predefined access points are able to join a specific controller. With Cisco devices this can be done by using certificates. a user defines in the controller settings which certificate is used and which access points are allowed to the connect to controller. In addition, the user has to define the default controller to the access point. When access points are connected to a controller for the first time, they check from the controller that they have the correct software version. If the software is too old, the new software is automatically downloaded and installed from the controller. When the access points have correct software installed, they are ready to be used. Access points can then be managed from the controller web interface. As illustrated in figure 16, the main page shows a controller software version, connected access points and other useful information.

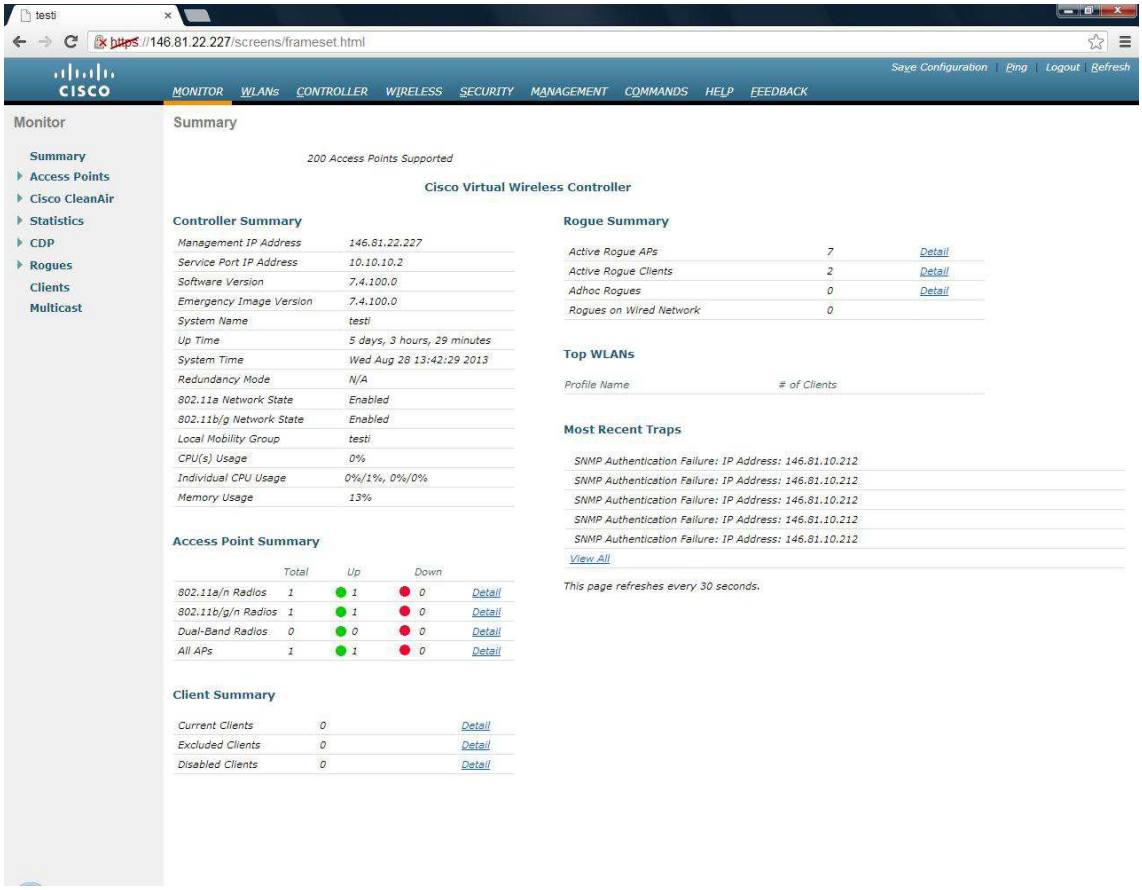

FIGURE 16. Cisco virtual controller summary page

The next step was the Cisco Prime Infrastructure software to discover the network. Discovering the network is an automated process and it can be done by using the "Quick discovery" -function from the software. The quick discovery view is illustrated in figure 17.

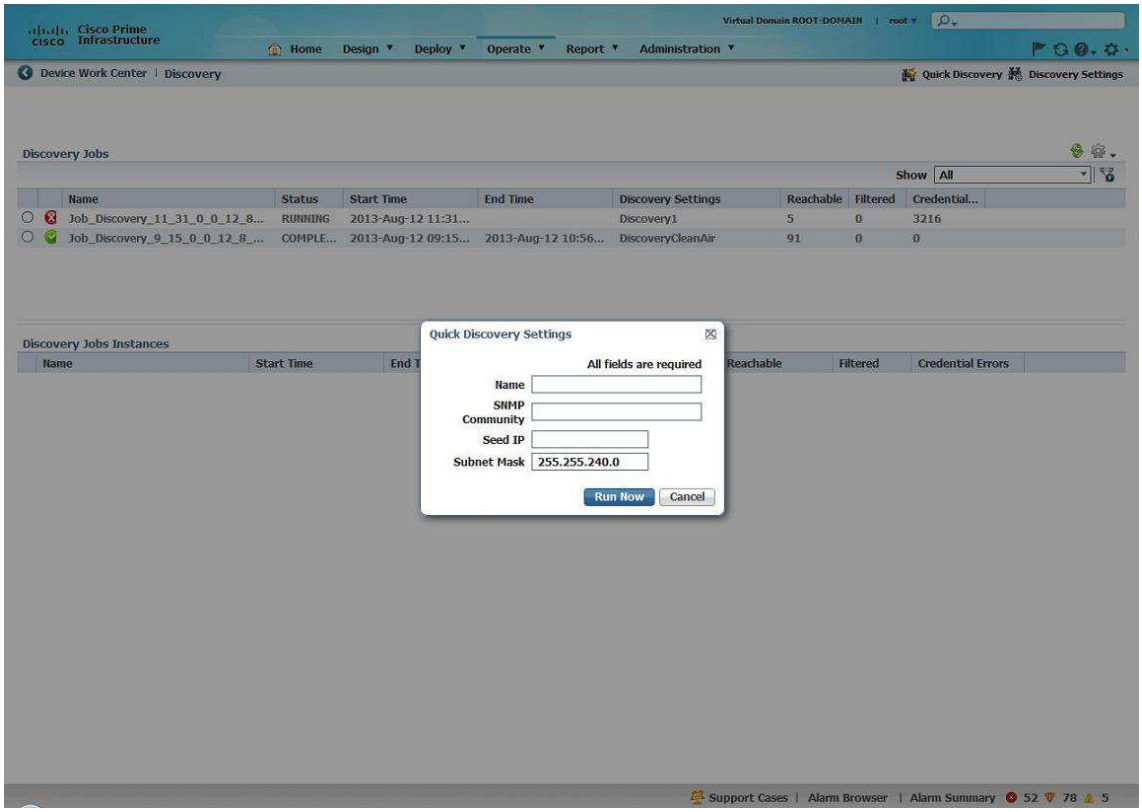

FIGURE 17. Cisco Prime Infrastructure network discovery view.

The user only needs to define the name for the discovery, an SNMP community string and a seed IP, which is the IP address that is used as a starting point for the discovery work. According to Cisco Internet pages, Cisco Prime uses six protocols to discover devices. The protocols are the following:

- Ping Sweep
- Cisco Discovery Protocol (CDP)
- Routing Table
- Address Resolution Protocol (ARP)
- Border Gateway Protocol (BGP)
- Open Shortest Path First (OSPF)

ICMP-Ping sweep is used to discover which addresses are being used. This very basic method does not provide any information about the device itself or

the location in the network. After ping sweep has discovered the reserved addresses, CDP is used to get network management applications to learn the device type and the SNMP agent address of the neighboring devices, and to send SNMP queries to those devices. If additional information is needed, more advanced methods are used to find out more detailed information about the network.

After the discovery is finished, the software will show all the devices it has found from the network and it is possible for the user to start monitoring the network status.

6.2 Using the tools and acquiring data

After the installations and configurations of the environment, we can begin the monitoring of the environment. The Cisco Prime infrastructure displays useful information right away on the main page. This view can be edited so that desired information is displayed on the main page. For example a controller and access point status can be observed quickly, as illustrated in figure 18.

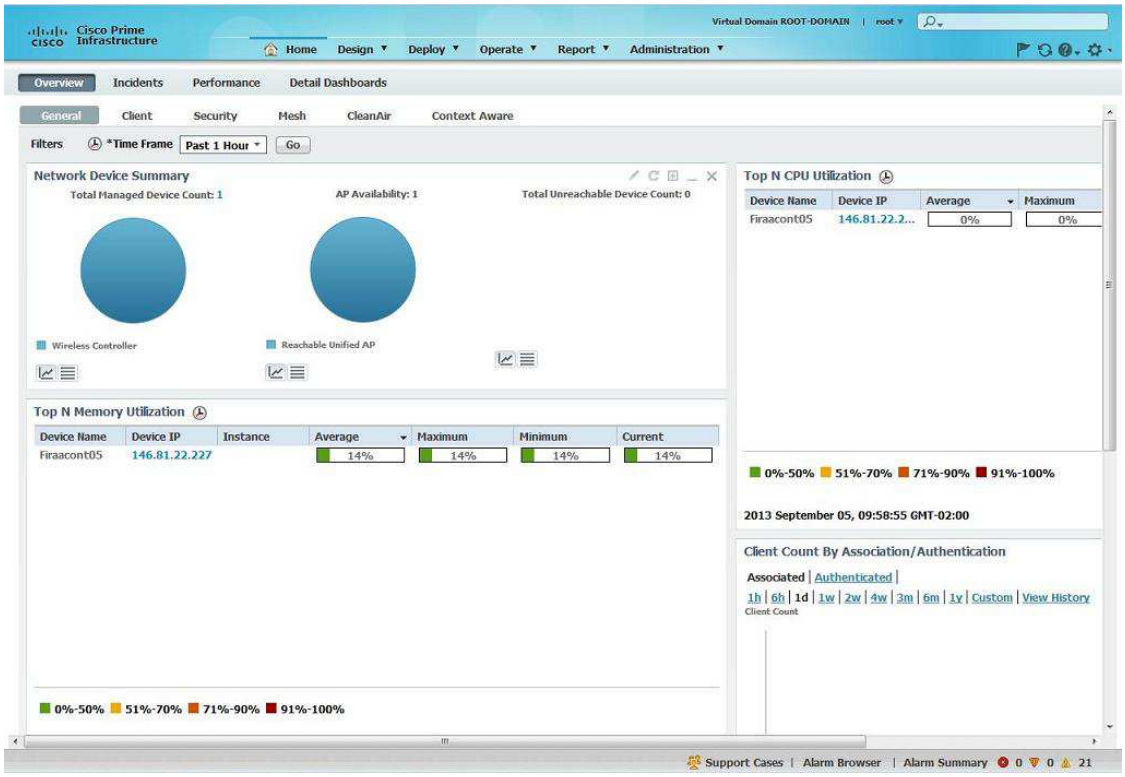

FIGURE 18. Cisco Prime Infrastructure main page.

One helpful feature in the Cisco prime infrastructure is maps. It is possible to add map images from outdoor and indoor areas. Access points can then be added to those maps to their physical locations. By using SNMP and other network management protocols, the Cisco prime infrastructure is able to display network information and the status of the access points. Network managers can then straight away view the status and state of those access points displayed on the maps. Different colors and shapes are used to display for example the status, RF maps and mesh relations of the access points. An example of RF maps is illustrated in figure 19.

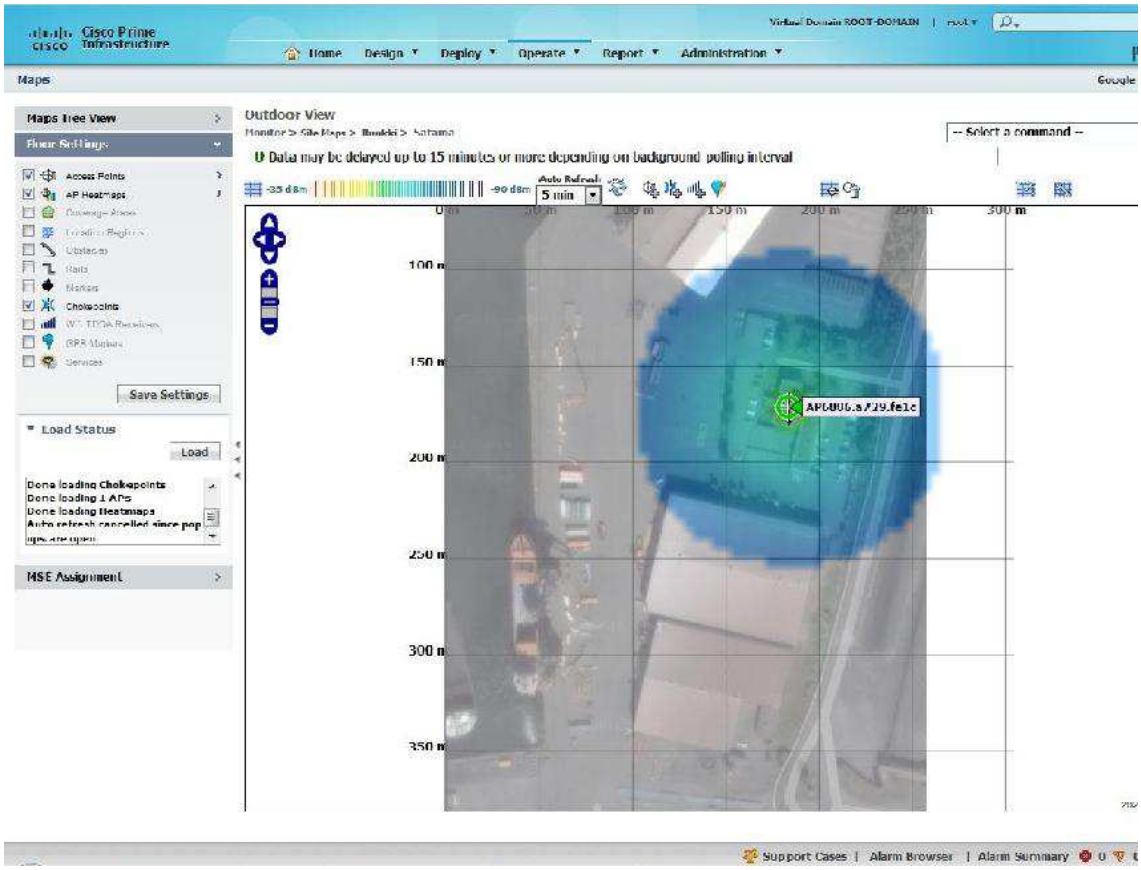

FIGURE 19. Cisco Prime Infrastructure heat map view.

A more detailed monitoring and configuring of the access points is also easy from the maps view. As illustrated in figure 21, by just clicking the access point image, a menu window is opened where information is easily available. A more detailed device monitoring and also configuring can be done from the device center view which is illustrated in image 20.

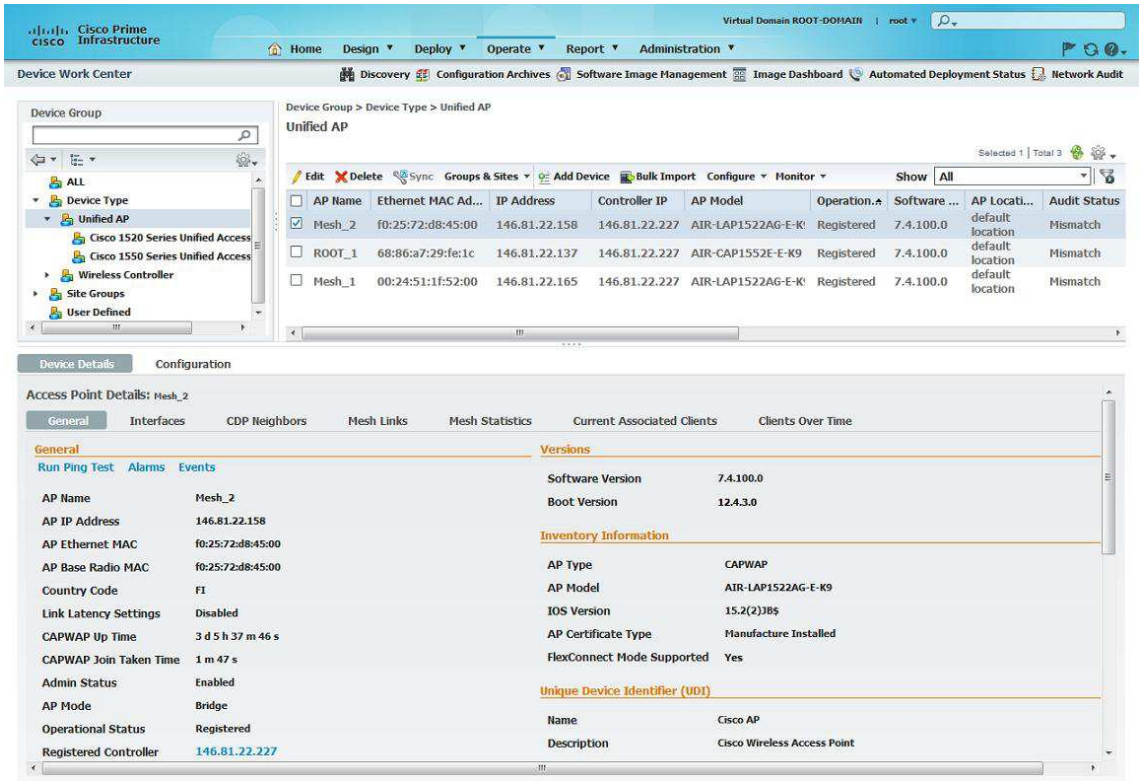

FIGURE 20. Cisco Prime Infrastructure device center view.

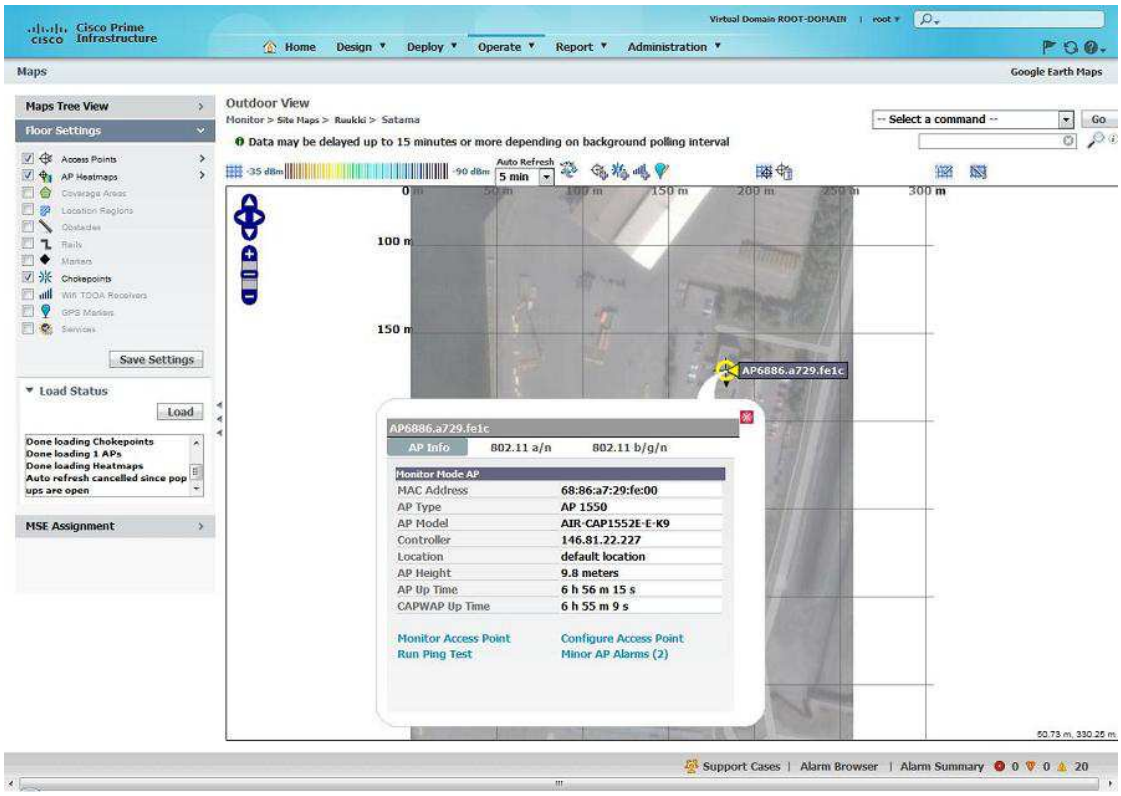

FIGURE 21. Cisco Prime Infrastructure maps view access point menu.

The clean air functionality provides information about the radio frequencies and interference. The Cisco prime infrastructure displays this information as charts. The tool was able to detect some radio interference in the area where access point was located. Clean air summary page view is illustrated in figure 22.

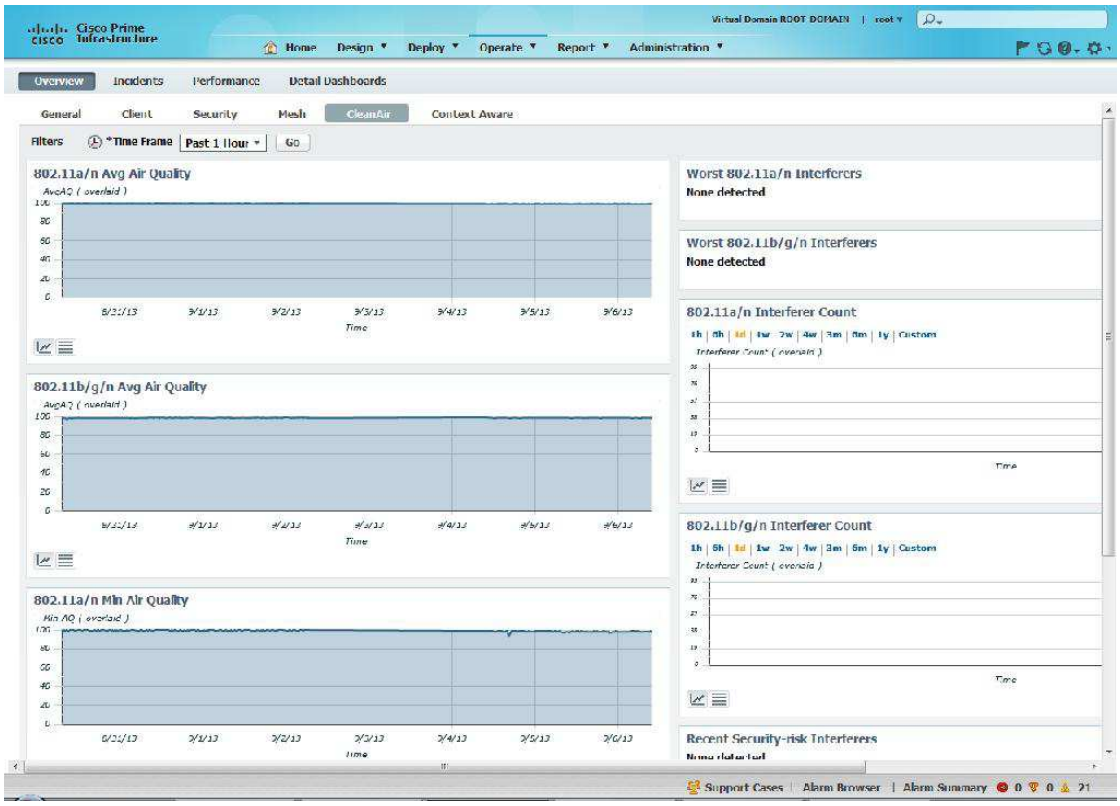

FIGURE 22. Cisco Prime Infrastructure Clean Air view.

An alarm feature is a very important feature in all monitoring applications. The Cisco Prime Infrastructure displays alarms on a notification bar at the bottom of the page as illustrated in figure 23. The bar is always visible, which means that a network administrator can easily view network alarms from any page of the tool. Alarms are divided into three categories according to their severity. Alarms are triggered by events. According to Cisco Internet pages, an event is an occurrence or detection of some condition in or around the network, such as a device reset, a port change and so on. Prime Infrastructure discovers events in the following ways:

- By receiving notification events and analyzing them; for example, syslog and traps.

- By automatically polling devices and discovering changes; for example, device unreachable.
- By receiving events when a significant change occurs in the Prime Infrastructure server; for example, rebooting the server.
- By receiving events when the status of the alarm is changed; for example when the user acknowledges or clears an alarm.

(Cisco 2013, retrieval date 2.10.2013). The alarm feature was investigated thoroughly because it would be a useful feature at Ruukki Metals' factory to be able to modify alarm parameters. By default the tool raises an alarm every time a device is dropped out of the network. It was investigated if it were possible to create an alarm when a specified access point drops out of network. Unfortunately, this kind of functionality was not found possible to achieve.

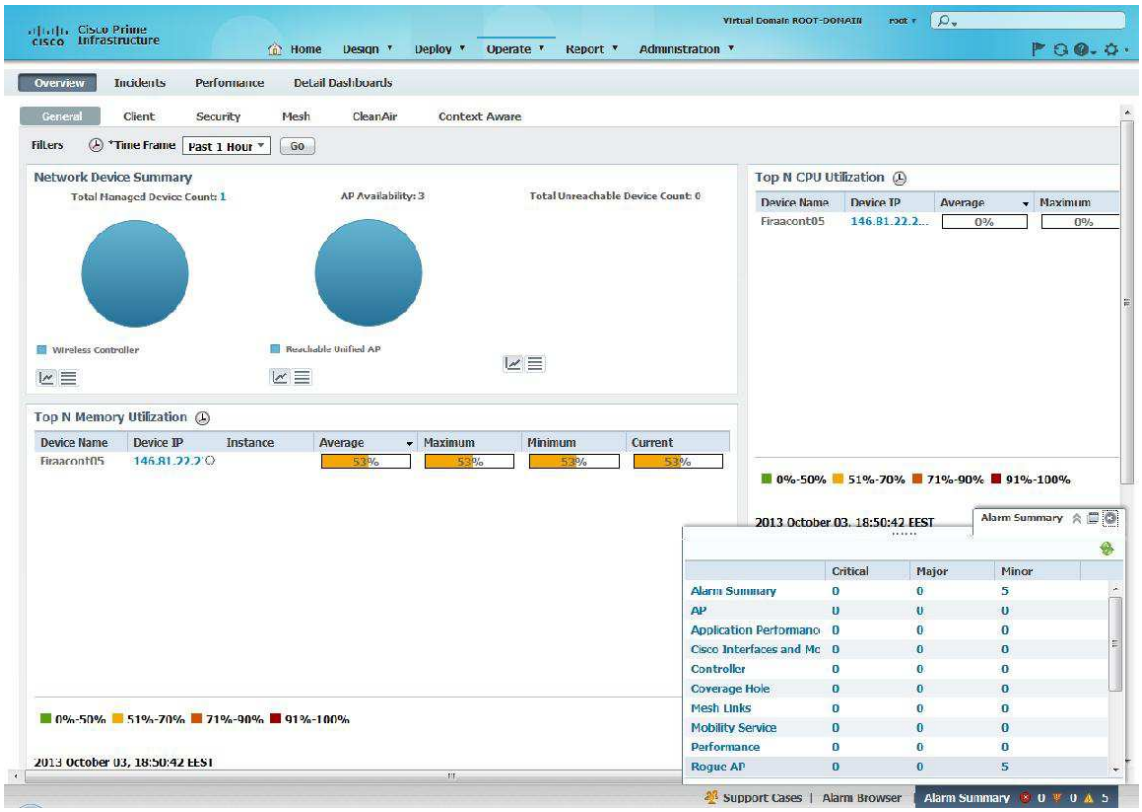

FIGURE 23. Cisco Prime Infrastructure alarm window.

The Cisco Prime Infrastructure user can also define which events will trigger alarm. This can be done by using templates as illustrated in figure 24. This feature is a good example of intelligent network monitoring. By defining custom

alarms, network administrators will get information which they consider useful. This increases efficiency by helping administrators to avoid unnecessary alarms.

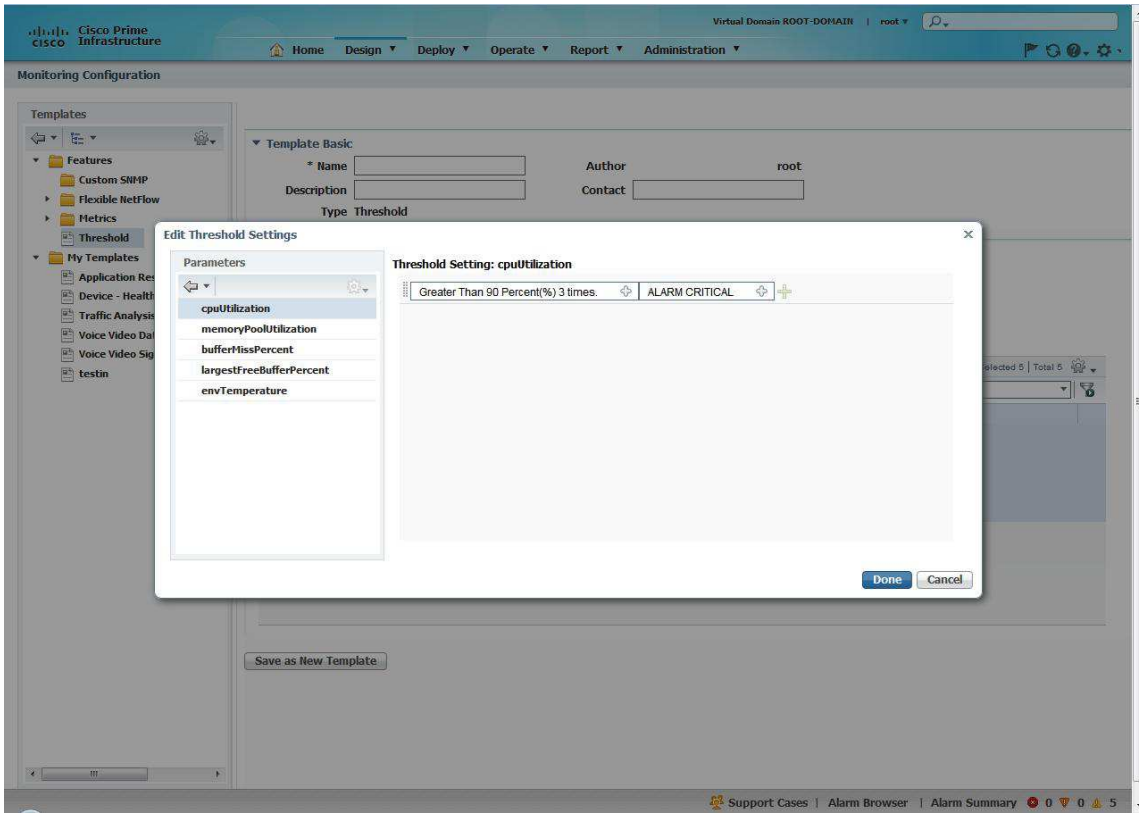

FIGURE 24. Cisco Prime Infrastructure alarm template.

6.3 Results

The following are the essential findings in the tests that were carried out:

- At first the Cisco Prime Infrastructure was installed and configured to the actual WLAN that is used at the factory site. Even though the tool was used only briefly, the network administrators were able to determine and solve one crucial networking issue: one controller was consuming more memory and CPU power than others. This could be viewed directly from the main page of the Cisco Prime Infrastructure, as illustrated in figure 18. The problem was solved by rebooting the controller. This improved the network performance and gave network administrators information on

what was causing the poor performance of the network.

- While the demonstration network was working, we were able to gather data from network interference. By using the Cisco Prime Infrastructure, the network administrators can easily monitor rogue WLAN devices. As illustrated in figures 21 and 22 the data of network interference is easily available. Unfortunately, time schedule of this thesis did not allow a thorough investigation of the network interference and networking issues but the gathered data will remain for Ruukki Metals' personnel to investigate. The benefits from Clean Air technology also remained unclear. The Cisco Prime Infrastructure provides air quality charts, but information was not as precise and detailed as it was hoped to be. Even though the network interference and issues could not be investigated more thoroughly the functionality of the monitoring tool was found useful and the investigation of network issues was faster with the Cisco Prime Infrastructure tool.
- One important aspect of the demonstration project was also to test the network devices that are newer model than those in use at the moment. Particularly the mesh functionality of the new models would have been interesting, but unfortunately the Cisco virtual wireless controller does not support the mesh functionality. However, during the demonstration project Cisco 1522AG access points were used with a virtual controller. In order to get access points connected to the virtual controller, they needed to have the same software version installed than the virtual controller was using. During this research the software version that the virtual controller was using was 7.4.100.0. The software installation was quite time consuming, because the software version, which the access points had, was much older and finding documentation to that software was difficult. After the installation, however, the access points were working well with the new software.

7 Conclusions

The purpose of this research was to investigate the usage and benefits of intelligent network monitoring in a steel factory environment. During the investigation I have studied several researches, studies and examples. This research has been truly interesting and given me understanding not only about intelligent network monitoring but also about the functionality of large and modern wireless local area networks. During this research I was able to extend my knowledge in network monitoring and WLAN technology. In addition to this I also got practical experience. During building and configuring the demonstration environment, I got experience from configuring wireless local area network devices and virtual servers. The fact that the demonstration network was assembled to Ruukki Metals steel factory gave understanding of the functioning of the network and daily routines of the network managers. Ruukki Metals' personnel's true professionalism and helpfulness had significant impact on the successfulness of this research. The results of the research show that using intelligent wireless local area network monitoring in a steel factory environment has many benefits. The software programs using intelligent network monitoring methods, such as the Cisco prime infrastructure, make network monitoring easier and problem solving faster. During the configuration of the demonstration project, the monitoring efficiency of the actual wireless local area network at Raahe factory was already improved and the root causes for some performance issues could be fixed. The results of the demonstration project also support the conclusions that with modern intelligent network monitoring tools it is possible to improve the functionality of the network and network monitoring at Raahe steel factory.

7.1 Future research possibilities

The usage of wireless local area networks is constantly increasing and new technologies are being developed. New technologies often promise to increase

efficiency and reliability. However, updating networks can be expensive and possible advantages should be investigated and planned carefully. Future research possibilities related to this research could relate to network monitoring improvements provided by a new technology. Due to limited time reserved to this research it was not possible to test some of the methods introduced in this paper for example, the effects of using directional antennas. The proper testing of directional antennas would require acquiring the hardware and installing and testing them in the actual network environment. Testing different antenna types and installation positions would provide useful information on what kind of impact they would have on interference tolerance and the range of the access points. The Cisco Prime Infrastructure supports the usage of dedicated spectrum analyzing hardware and implementing them as a part of the network would also be another interesting subject for a future research.

References

Anttila, H. 2012. Raahen tehtaan langattomat verkot, WLANit. Rautaruukki Oyj. Internal documents.

Cisco Systems, Inc. 2013. Cisco Prime Infrastructure 1.2 User Guide. Date of retrieval 2.10.2013. http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.2/user/guide/alarms.html

Cisco Systems, Inc. 2013. Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2. Date of retrieval 2.9.2013. http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf015.html

Cisco Systems, Inc. 2013. Cisco Prime Infrastructure 1.2 User Guide. Date of retrieval 2.9.2013. http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.2/user/guide/update_dev_inventory.html

Cisco Systems, Inc. 2013. Cisco ClientLink: Optimized Device Performance with 802.11n. Date of retrieval 13.9.2013. http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10092/white_paper_c11-516389_ns767_Networking_Solutions_White_Paper.html

Cisco Systems, Inc. 2013. Enterprise Mobility 4.1 Design Guide. Date of retrieval 13.9.2013. http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch3_WLAN.html

Cisco Systems, Inc. 2013. Enterprise Mobility 4.1 Design Guide. Date of retrieval 13.9.2013. http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch9_Voic.html

Cisco Systems, Inc. 2013. Cisco Wireless Mesh Access Points, Design and

Deployment Guide, Release 7.0. Date of retrieval 8.9.2013. http://www.cisco.com/en/US/docs/wireless/technology/mesh/7.0/design/guide/MeshAP_70.html

Hiertz, G. Denteneer, D., Max, S., Taori, R., Cardona, J., Berlemann, L., Walke, B., 2010. IEEE 802.11s: The WLAN Mesh Standard. IEEE. Pp. 104 - 111. Internal document. http://ieeexplore.ieee.org.ezp.oamk.fi:2048/stamp/stamp.jsp?tp=&arnumber=5416357

IEEE. 2013. At a glance. Date of retrieval 4.7.2013. http://www.ieee.org/about/today/at_a_glance.html

Johnston, R. 2009. Evaluating the use of SNMP as a wireless network monitoring tool for IEEE 802.11 wireless networks. Graduate school of Clemson university, Degree Master of Science Computer Science, Master's thesis. Date of retrieval 11.6.2013 http://people.cs.clemson.edu/~jmarty/projects/iTiger/Thesis.pdf

Granlund, K. 2001. Langaton tiedonsiirto. Jyväskylä: Docendo.

Kaleva Oy. 2013. Utajärven varma säätutka. Date of retrieval 14.8.2013. http://www.kaleva.fi/uutiset/galleriat/utajarven-varma-saatutka/4003/148482/

Mahmood, F. 2013. Mobile Radio Propagation Prediction forTwo Different Districts in Mosul-City. Date of retrieval 13.9.2013. http://www.intechopen.com/books/matlab-a-fundamental-tool-for-scientific-computing-and-engineering-applications-volume-2/mobile-radio-propagation-prediction-for-two-different-districts-in-mosul-city

The University of Adelaide. 2013. Optimisation WLAN for Broadband access. Date of retrieval 14.8.2013. http://www.eleceng.adelaide.edu.au/research/undergrad-projects/archive/WLAN-optimisation/ProjectMain/OptimisationTech/EffectOf.htm

Wikipedia. 2013. IEEE 2013. Date of retrieval 25.8.2013. http://fi.wikipedia.org/wiki/IEEE_802.11

Wikipedia. 2013. Path loss. Date of retrieval 4.7.2013. http://en.wikipedia.org/wiki/Path_loss

Wikipedia. 2013. Radio frequency. Date of retrieval 26.8.2013. http://en.wikipedia.org/wiki/Radio_frequency

Wikipedia. 2013. Radio frequency. Date of retrieval 4.7.2013. http://en.wikipedia.org/wiki/Radio_frequency

Ylitalo, A. 2008. Wireless Communication in Logistic Chain of Steel Products. University of Oulu, Department of Electrical and Information Engineering. Master's Thesis.