Universitat Oberta de Catalunya

Analysis and Design of a secure WLAN solution for Cobre Las Cruces

Student: Carlos Jiménez Barranco

ETIS at UOC

Consultant: Carlos Ares Angulo

June, 10th 2011

I want to dedicate this work to the people who really trust on me and daily bring me the chance to be a better person: My parents, my girlfriend Elena and some friends like Melissa, Jordi and Jose.

Also, special thanks to Jorge Rodríguez and Pablo Nebrera for this chance of developing such an interesting project and to Carlos Ares for his collaboration on the elaboration of the TFC.

Epigraph

After searching for an interesting TFC, Cobre las Cruces in conjunction with Eneo Tecnologia, gave us a chance to develop a project in the field of security in wireless environments.

Cobre Las Cruces is a renowned copper mining company located in Sevilla, with unexpected problems in wireless communications that have a direct affectation in production. Therefore, the main goals are to improve the WiFi infrastructure, to secure it and to detect and prevent from attacks and from the installation of rogue (and non-authorized) APs. All of that integrated with the current ICT infrastructure.

This project has been divided into four phases, although only two of them have been included into the TFC; they are the analysis of the current situation and the design of a WLAN solution.

Once the analysis part was finished, some weaknesses were detected. Subjects such as lack of connectivity and control, ignorance about installed WiFi devices and their localization and state and, by and large, the use of weak security mechanisms were some of the problems found. Additionally, due to the fact that the working area became larger and new WiFi infrastructures were added, the first phase took more time than expected.

As a result of the detailed analysis, some goals were defined to solve and it was designed a centralized approach able to cope with them. A solution based on 802.11i and 802.1x protocols, digital certificates, a probe system running as IDS/IPS and ligthweight APs in conjunction with a Wireless LAN Controller are the main features.

Keywords

SSID, 802.1x, 802.11i, WiFi, Rogue AP, Cisco Wireless LAN Controller (WLC), Lightweight Access Point (LAP), probe, Icinga, MAC address, RADIUS Server, Digital Certificate, signal level, aircrack-ng suite, WEP, WPA2, WLAN, PKI, analysis, design, flaw, security.

TFC's working area

Security

Contents

Illustrations Index

Index of Tables

Chapter 1 – Introduction

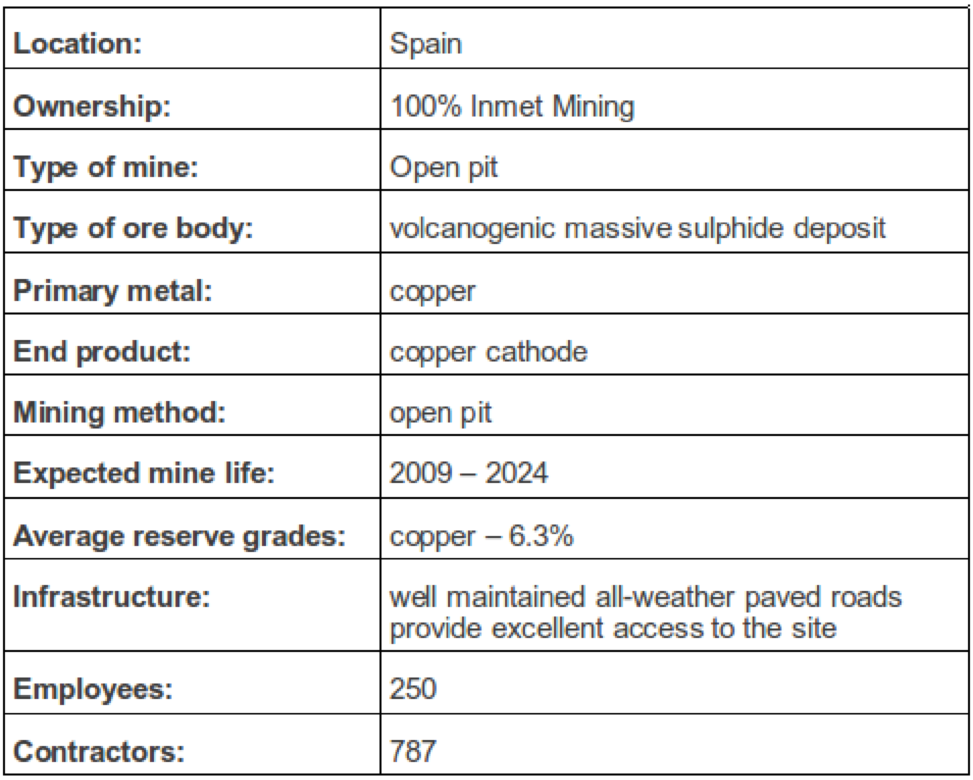
1. Environment where this TFC happens

1.1. About CLC

Las Cruces is an open pit mining operation and process plant located in the Sevilla Province of Southern Spain that uses leaching and electrowinning technology to produce copper cathode. It is owned and operated by Inmet Mining, who is a Canadian-based global mining company that produces copper and zinc and also owns and operates other mining operations in Turkey and Finland. Inmet also develops another project in Panama.

Illustration 1. Aerial view of CLC's plant and mine area

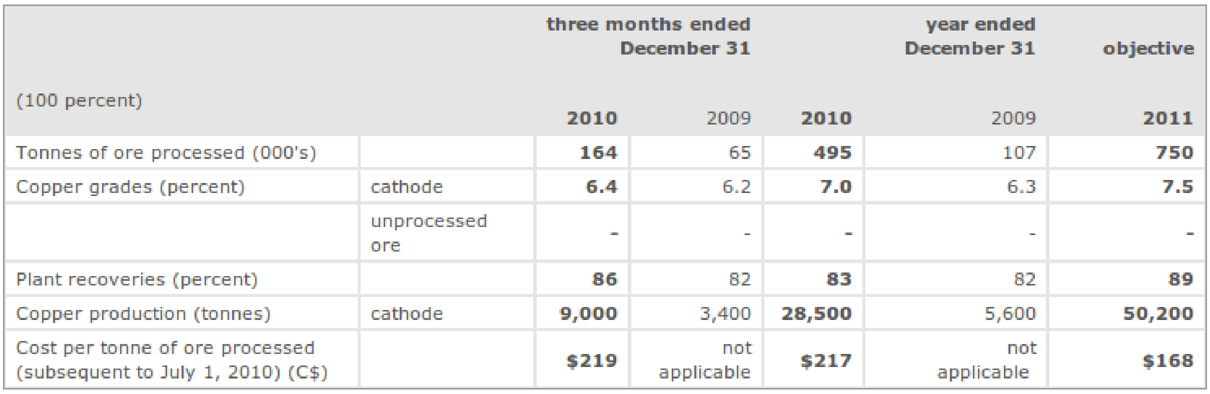
Cobre Las Cruces's plant is designed to produce approximately 72,000 tonnes of copper cathode per year which is shipped as final product. Inmet Mining has a 100 percent interest in Las Cruces. Additional information is shown in tables 1 and 2.



Location:	Spain
Ownership:	100% Inmet Mining
Type of mine:	Open pit
Type of ore body:	volcanogenic massive sulphide deposit
Primary metal:	copper
End product:	copper cathode
Mining method:	open pit
Expected mine life:	2009 – 2024
Average reserve grades:	copper – 6.3%
Infrastructure:	well maintained all-weather paved roads provide excellent access to the site
Employees:	250
Contractors:	787

Table 1. Data about Cobre Las Cruces's plant

Targets and results



		three months ended December 31		year ended December 31		objective
(100 percent)		**2010**	2009	**2010**	2009	**2011**
Tonnes of ore processed (000's)		**164**	65	**495**	107	**750**
Copper grades (percent)	cathode	**6.4**	6.2	**7.0**	6.3	**7.5**
	unprocessed ore	**-**	-	**-**	-	**-**
Plant recoveries (percent)		**86**	82	**83**	82	**89**
Copper production (tonnes)	cathode	**9,000**	3,400	**28,500**	5,600	**50,200**
Cost per tonne of ore processed (subsequent to July 1, 2010) (C$)		**$219**	not applicable	**$217**	not applicable	**$168**

Table 2. Targets and results of CLC

1.2. Technological field

Cobre las Cruces is a company with some special technological requeriments due to its specific business activity (copper mining and cathode production).

By the number of users it can be considered a large size company, but it also has an important industrial infrastructure working 24 hours a day, 7 days a week, where SCADA systems are a critical element. For this reason, communications with these systems are necessary to be up and running continuously and in an efficient way.

Systems infrastructure is mainly Microsoft based, with several corporate applications (i. e. ERP, Knowledge management, messaging and antivirus), a Windows Domain and several custom developed web applications. Otherwise, several Linux devices are being used in perimetral security and to allocate several of the new high demanding web applications. At this moment, IT department is moving from a physical server infrastructure to a virtualized and more redundant one.

With regard to the communications, it is a switched network, that has improved its performance and stability by the use of VLAN's and whose security has increased by the use of advanced firewalling and contents inspection technologies. It contains hundreds of wired and wireless devices and there are some wireless areas of influence. Moreover, VoIP technology is also fully integrated within this infrastructure.

Compared to other areas that are quite advanced, wireless part is certainly one of the “weaknesses”. After this project, the goal is to improve the wireless field so the IT department can have a global an accurate knowledge and control over all the wireless devices installed and can be notified as soon as something not allowed or just a change tries to be introduced in 2.4GHz frequency band.

Cobre las Cruces has security in mind for all the areas of its business, so IT Security is growing in importance daily. This is why some of the infrastructures developed in this project will be used with other systems (i. e. PKI and digital certificates for e-mail digital signature). Eventually, the main goal of all the securization process (not only this project) is to get a highly secure and redundant infrastructure with a central management point (i. e. events/alarms correlation, access control, policies deployment, vulnerabilities detection, IDS/IPS, etc.); therefore, solutions implemented in this project will be fully integrated with the Active Directory infrastructure and other architectures already installed or in progress.

2. Goals

2.1. Object and scope

The object of this project is to secure the wireless network infrastructure of an international mining company (Inmet Mining) with a subsidiary in Sevilla (Cobre las Cruces). Using Open Source software, it will include the analysis of the situation, the design, the implementation and a final evaluation of a solution based on 802.11i and 802.1x protocols and digital certificates, fully integrated with Active Directory and Icinga. Also, the implementation of a PKI and the deployment of a rogue AP's and attacks detection system with a centralized management.

According to that, the scope of the TFC will vary depending on the results of the first phase of the project: The analysis of the situation. Due to the duration of the full project and the duration of the TFC, this is why the TFC is intended to be a part of the full project.

The first aim was to include three of four parts (analysis, design and implementation). But eventually, only analysis and design phases were included. Actually, the initial idea was to include only the hidrometalurgic area (the production factory itself and the headquarters), but the customer requested us to add all the wireless communications of the company (Cobre Las Cruces), including all the mining area and other contractors in that area, so the total area of research became much larger. This included not only more devices and networks to identify, but to work on a solution to improve wireless communications with SCADA systems (telecontrol network) and CCTV IP systems, that are suffering similar problems as the devices located in the factory and in the headquarters area.

2.2. Professional and personal goals

This section explains the goals of this project from a professional and personal point of view. Both perspectives are connected due to the special situation of this project.

It is an initial six months long project in an important company. Also, this project obtained an scholarship and it is intended to be an opportunity for me to improve my professional career and to focus on IT security. Whereas, it will be the better way to put in practice many of the concepts learnt in ETIS and to elaborate a good TFC (not just to pass this subject). After finishing ETIS, I would like to continue working on IT Security and studying postgraduated courses in the same field, so this project I think that can be a good chance for me as an entry letter and for improving my professional career.

With aproximately 1000 workers, several network technologies an about 10 wireless areas of influence, the main goal is to homogenize that infrastructure and to implement a solution to get a centralized management of the network and its security. Initially, based on Open Source software.

The aim is to solve some problems of the customer: lack of connectivity, interferences between WiFi devices (APs, SCADA systems...), an excessive incidence response time and an important unknowledge about installed wireless devices, their localization and state. All of those problems have a direct affectation in production and their solution is a priority for CLC.

Also, another goals are the securization of the wireless network, the reduction of the attacks and the detection and prevention from installing rogue AP's. All of that integrated with the already created ICT infrastructure.

3. Approach and methodology

As stated in the previous section, this TFC is expected to be a part of a 6 months project in the form of a practical case of consulting in WiFi and mainly in Security fields. So we will differentiate between a main project for a customer and another project (contained into the first one) for the academic part; it is, the wellknown TFC.

The approach for the project is to divide it into 4 parts: the previous analysis, the design of a solution, the implementation of that solution and a final performance evaluation. Nonetheless, only the analysis and the design will form the TFC.

The methodology is to divide each main part into tasks and subtasks in order to make work easier to handle and able to plan it. With regard to the design stage, it shows an overall picture first and next a detailed explanation of each subpart within the global solution. In fact, the design will be a recursive task because is has been decided with the customer to do for each part separately. Then, until one part is not designed, approved by the customer and fully installed, the design of the next part does not start.

3.1. Tasks that form the project

This is the list of tasks under the two first phases of the project:

- Introduction
  - Introduction to the customer of the global idea of this project and some of the technologies in use.
- Analysis of customer's current situation
  - Knowledge of network topology and IT infrastructure.
  - Study of the signal levels detected on each working centre.
  - Inventory and tracking down of AP's and SSID's (updated with the inclussion of the new WiFi influence areas and the new technologies involved).
  - Updating of the information collected comparing it with a previous work done by several Engineering companies several months ago.
  - Wireless network assessment:

        - To gain access.
        - To obtain configurations and to analyze them
        - To find threats that can affect CLC's network security
    - Writing conclusions.
    - Evaluation of detected problems and improvements to deal with and presentation of the report.
- Design of a solution based on customer's real requirements:
    - Research about best technologies to solve issues mentioned in the analysis stage (i. e. cipher features).
    - Study of the technical specifications of the current networking devices in order to evaluate whether they can be used/adapted or not to the new solution.
    - Evaluation of the new devices required to purchase.
    - Study of PKI requirements and viability of its implementation
    - Writing of a report and presentation to the customer's CIO.
    - Modification (if necessary) to the previous design to include changes and/or requests made by the customer.
    - Acceptance of the approach by the CIO of CLC.

So far, for the implementation and evaluation parts there are no tasks defined due to the fact that we are currently waiting for the acceptance of the global project and several main parts. Then, implementation will have to be decided with the customer. Nonetheless, this is an approach of the general tasks to do in the implementation and performance evaluation phases:

- Implementation of the solution. Some of the expected tasks will be:
    - AP's standardization.
    - Define base line for the migration in order to avoid that users loss network connectivity
    - Implementation of a network authentication solution based on 802.1x protocol over 802.11i standard. Some tasks are:
        - Implementing RADIUS for authentication, autorization and accounting over a virtualized environment.

        - RADIUS integration with Active Directory infrastructure.
        - Deployment of PKI.
        - Migration to 802.11i solution (i. e. WPA2).
    - Use of separated areas for users and guests
    - Monitoring of new WiFi infrastructure
        - Icinga monitoring system integration.
    - Rogue AP's and attacks detection
        - Deployment of detectors in strategic positions over the customer's buildings and dependences.
- Evaluation of the performance
    - Execution of specific security and performance tests.
    - Data collecting.
    - Analysis of lacks and possible improvements
    - Making a report and delivering it to the customer

3.2. Requirements

Apart from the supervision of the TFC and the support offered by Carlos Ares (UOC Consultant), this project is supervised by the IT Director (CIO) of Cobre las Cruces and by the Development area Director of Eneo Tecnología, Pablo Nebrero, who is also the teacher of de US (Universidad de Sevilla) in charge of mentoring (together with Carlos Ares) this project. Furthermore, several ICT professionals of Eneo Tecnología will give their support in some parts of the implementation of this project.

It is important to mention that staff designated by the customer has been required to attend us during the access to the mining area and security clothes have been necessary too.

At the end, some users of Cobre las Cruces will be required during implementation and testing phases of the solution.

With regard to the technical requirements, several laptops, WiFi adapters with (omni) directional antennas and a signal amplifier have been necessary during the analysis phase. Additionally, software to study WiFi signal was required too (i. e. to view amplitude time variations) and to capture and analyze paquets in all of the channels of the 2.4GHz band (i. e. to detect hidden ESSID's or unexpected behaviour of stations or AP's). For the wireless assessment (basic penetration testing), a set of tools will be used (like all the included in BackTrack and WiFiWay Linux distros). Furthermore, several virtual machines will be necessary to install RADIUS and CA and some wireless and wired networking devices will be required too (i. e. Lightweight APs, a Wireless LAN Controller, some probe devices and switches).

4. Planning

A first attempt of getting a planning is based on the four phases that the project is divided into:

1. Analysis
2. Design
3. Implementation
4. Performance test

Initially, the purpose was to link every phase of the project with a delivery of the TFC. So, CA 2 (11/04/2011) would coincide with the presentation of the results of the analysis, CA 3 (02/05/11) with the design of the solution and CA 4 with a part of the implementation. Otherwise, we found an important unknowledge about the global wireless network infrastructure by the customer so it was difficult to establish a timming or schedule every subtask, mostly because the research task was greater than the initial idea (in environmental conditions quite different that those we are used to). In that way, the project has suffered some time variations, so eventually, the planning has been this:

- CA 1 (18/03/2011) → planning and state-of-the-art
- CA 2 (24/04/2011) → first part of the analysis phase
- CA 3 (19/05/2011) → second part of the analysis phase, updated with the WiFi network assessment and additional conclusions
- CA 4 (06/06/2011) → overall picture of the design phase

Depending on the acceptance of the proposed solution by CLC's CIO, the implementation of two of the parts that make up the solution (WiFi Network and Probe system IDS/IPS) would start on July. Consequently, the rest of the project (implementation and performance evaluation) is out of the scope of the TFC, due to a timing reason.

5. Next chapters

This document contains two additional chapters: one for the analysis part and another for the design of the solution.

In the analysis section, they are shown the results of an intensive signal study, an SSIDs detection process and their tracking down and a later inventory of all the main WiFi devices. Also, a wireless network assessment was done and the results are showed in the analysis part too. Eventually, all that gathered data was studied and the last part of this section suggests a set of conclusions to take into consideration about the wireless network infrastructure of the customer and mostly about its weackness.

The design part is the result of the previous study of the situation. In fact, some goals were defined in conjunction with the customer so it is shown a design to achieve all those goals. Initially, it is given an overall picture of the approach and later it is divided into some parts so that a more detailed explanation can be done of each one. Additionally, benefits of this solution are exposed too.

Chapter 2 – Analysis of CLC's current situation

1. Introduction to the analysis part

The goal of this section is to show the contents of the first phase of the four that form this project; it is, the analysis of the customer's current situation. Obviously, from a technical point of view and always focused on the wireless network infrastructure.

First of all, the tasks done up to now are introduced and explained in a brief way in order to concentrate in the conclusions. Additionally, the parts that make up this document are explained. It is important to mention that this document structure (with regard to the different sections used) is the same that the structure used for the report that was delivered to the customer, despite of the fact that customer's document was more extensive and it included confidential information that is not allowed to be shown in this document.

Also, the different sections explained here are used to show a sample of the results of the different tasks done (i. e. WiFi signal sampling and WiFi network assessment).

2. Tasks of the analysis part

This section lists the main tasks that make up the analysis of CLC's WiFi network current situation. All of those tasks have been done over most of the time we have been in the customer's facilities.

As a result, this document offers the final version of a two parts document delivered in CA 2 and CA 3 and shows the analysis stage done. Next, these are the tasks:

- Knowledge of network topology and IT infrastructure. Apart from a first introduction done at the beginning of this project, a deeper knowledge has been adquired during the daily work, by the achievement of the defined tasks and goals within the analysis phase. However, additional knowledge has been obtained during the design stage.

- Study of the signal levels. Sampling was taken in all the sites where there could be computers or other mobile devices with WiFi capabilities.

- Tracking down and inventory of the SSIDs and the main WiFi devices. Tracking down of the SSIDs has been fully accomplished (updated with the inclussion of new WiFi influence areas and the new technologies involved) and main WiFi devices (AP's, printers, Point to Point bridges...) have been found. Only a few devices situated in not allowed places (i. e. in operational zones) or whose access requires an special permission and equipment (i. e. work on heights) are still pending. Remaining information from another contractor was obtained.

- Updating of the information collected comparing it with previous works done by several Engineering companies. Customer gave us that information but there were few things to update due to the fact that the information contained in those reports was too different (perhaps outdated) from the current infrastructure. An appointment with technical managers of Ping Sistemas and ACT was eventually celebrated to collect extra information.

- Wireless network assessment. Based on SSIDs to evaluate, basic penetration tests were done. Within this task, the main goals were:

  - To find vulnerabilities that could allow to gain access to that network or WiFi device (i. e. nonsecure passwords or passphrases, vulnerable protocols in use, etc.).

  - To obtain configurations.

  - To detect threats that can affect CLC's network security.

- Writing conclusions. Based on the previous tasks and on the study of all the collected information, a thorough approach will be given.
- Evaluation of the detected problems and improvements to deal with and presentation of the report. Once the report was finished, it was delivered to CLC's CIO. In fact, a detailed document and a presentation was made to several people to show them the results of this phase and to decide the goals on the design phase.

3. Study of the signal levels

In this section, it is studied the use of the channels contained in 2.4 Ghz frequency range by the wireless networks detected in Cobre las Cruces.

It has been used a computer running as a probe device located in strategic points in every site. In this way, it was possible to offer a very accurate view of signal level received by stations (i. e. PC's).

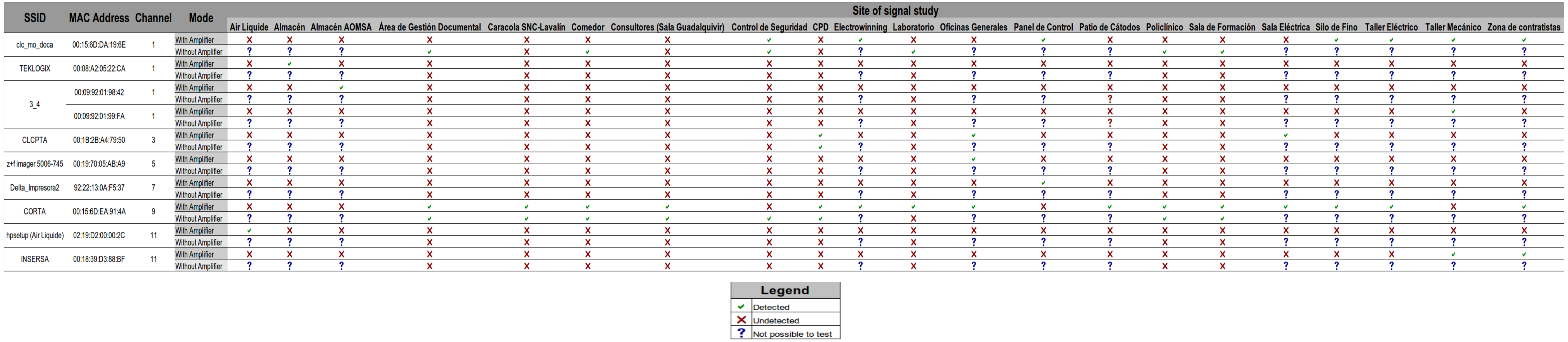
In order to accomplish it, several hardware and software tools have been required:

- Software:
  - inSSIDer 2
  - WiFi Analyzer (for android)
  - Ubuntu Linux 10.10 virtual machine
- Hardware:
  - External (usb) WiFi device: Edimax EW-7318USg
  - Omnidirectionnal 4dbi's antenna
  - WiFi amplifier (500 mW): Renasis BA24J

Using an usb WiFi device and a wireless signal amplifier, the main purpose is to show signal levels that almost every station would receive in most cases. Moreover, it is intended to compare it with the exceptional signal levels (amplified) that just a few WiFi devices would receive. In that case, they would be devices with a high power WiFi adapter (not very common). This comparison results highly important in places where different SSIDs could be detected in order to prevent channel overlapping.

It is important to take into account that this part of the study only deals with non hidden SSIDs. So it reflects the same as a computer would show in its list of available WiFi networks. Hidden networks and their effects are studied in the next section (“Tracking down and inventory of the SSIDs and the main WiFi devices”).

Sampling has been done in 22 sites and depending on physical distribution and the presence of machines that could cause interferences, additional strategic points for sampling have been defined within every site. In this way, a total of 40 points of sampling have been set.



SSID	MAC Address	Channel	Mode	Site of signal study																				
				Air Liquide	Almacén	Almacén AOMSA	Área de Gestión Documental	Caracola SNC-Lavalín	Comedor	Consultores (Sala Guadalquivir)	Control de Seguridad	CPD	Electrowinning	Laboratorio	Oficinas Generales	Panel de Control	Patio de Cátodos	Policlínico	Sala de Formación	Sala Eléctrica	Silo de Fino	Taller Eléctrico	Taller Mecánico	Zona de contratistas
clc_mo_doca	00:15:6D:DA:19:6E	1	With Amplifier	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✓	✓	✓	✓
			Without Amplifier	?	?	?	✓	✗	✓	✗	✓	✗	?	✓	?	?	?	✓	✓	?	?	?	?	?
TEKLOGIX	00:08:A2:05:22:CA	1	With Amplifier	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
			Without Amplifier	?	?	?	✗	✗	✗	✗	✗	✗	?	✗	?	?	?	✗	✗	?	?	?	?	?
3_4	00:09:92:01:98:42	1	With Amplifier	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
			Without Amplifier	?	?	?	✗	✗	✗	✗	✗	✗	?	✗	?	?	?	✗	✗	?	?	?	?	?
	00:09:92:01:99:FA	1	With Amplifier	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
			Without Amplifier	?	?	?	✗	✗	✗	✗	✗	✗	?	✗	?	?	?	✗	✗	?	?	?	?	?
CLCPTA	00:1B:2B:A4:79:50	3	With Amplifier	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗
			Without Amplifier	?	?	?	✗	✗	✗	✗	✗	✓	?	✗	?	?	?	✗	✗	?	?	?	?	?
z+f imager 5006-745	00:19:70:05:AB:A9	5	With Amplifier	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
			Without Amplifier	?	?	?	✗	✗	✗	✗	✗	✗	?	✗	?	?	?	✗	✗	?	?	?	?	?
Delta_Impresora2	92:22:13:0A:F5:37	7	With Amplifier	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
			Without Amplifier	?	?	?	✗	✗	✗	✗	✗	✗	?	✗	?	?	?	✗	✗	?	?	?	?	?
CORTA	00:15:6D:EA:91:4A	9	With Amplifier	✗	✗	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓
			Without Amplifier	?	?	?	✓	✓	✓	✓	✓	✓	?	✗	?	?	?	✓	✓	?	?	?	?	?
hpsetup (Air Liquide)	02:19:D2:00:00:2C	11	With Amplifier	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
			Without Amplifier	?	?	?	✗	✗	✗	✗	✗	✗	?	✗	?	?	?	✗	✗	?	?	?	?	?
INSERSA	00:18:39:D3:88:BF	11	With Amplifier	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
			Without Amplifier	?	?	?	✗	✗	✗	✗	✗	✗	?	✗	?	?	?	✗	✗	?	?	?	?	?

Legend	
✓	Detected
✗	Undetected
?	Not possible to test

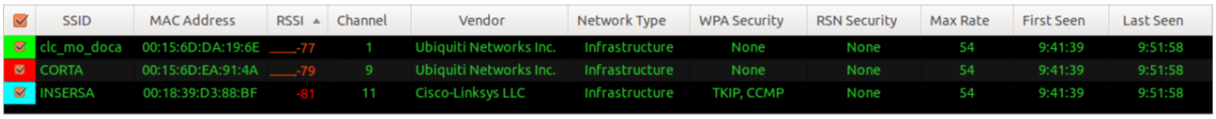
Table 3. The 21 most relevant places sampled and the main SSIDs detected

As seen in the table 3, 21 of 22 sites where showed. The office placed in av. El Garrobo is located in a village called Gerena and although it was sampled, it is not expected to there be people working so wireless received signal is less important. In fact, that sampling was just a request done by the customer. Obviously, it has no sense to compare SSIDs detected there to those detected in the hidrometalurgic plant, which actually are more important.

With regard to the use or not of a signal amplifier, it is important to take into consideration that this device was physically broken after some sampling. Therefore, only some sites got both measures. It was not possible to repair it or to buy a new one. One option could have been to delete measures using the amplifier, but we considered interesting enough to keep them in order to show differences among those places. Moreover, we talked about this subject with the customer and he considered it interesting enough to keep those measures as extra information.

Another subject to think about is that there were suspicious differences from using amplifier or not. Actually, there were places where signal of several SSIDs was detected in normal mode but not using the signal amplifier. The most common would have been to get much better signal power using the amplifier. But there were several AP's with such an unstable signal (i. e. “clc_mo_doca” SSID) so signal cuts were frequent (with or without amplifier).

Every sampling (with and without signal amplifier), has been done for 30 minutes, although the software only shows graphs of 10 minutes long. Over this time, information about SSID, signal power, channel, AP's MAC address and vendor, security, etc. is showed. Illustration 2 shows a sample of this output.



☑	SSID	MAC Address	RSSI ▲	Channel	Vendor	Network Type	WPA Security	RSN Security	Max Rate	First Seen	Last Seen
☑	clc_mo_doca	00:15:6D:DA:19:6E	-77	1	Ubiquiti Networks Inc.	Infrastructure	None	None	54	9:41:39	9:51:58
☑	CORTA	00:15:6D:EA:91:4A	-79	9	Ubiquiti Networks Inc.	Infrastructure	None	None	54	9:41:39	9:51:58
☑	INSERSA	00:18:39:D3:88:BF	-81	11	Cisco-Linksys LLC	Infrastructure	TKIP, CCMP	None	54	9:41:39	9:51:58

Illustration 2. Sampling done in the contractors' area (hut of the company Inselma)

Also, graphs about SSIDs detected on every channel (table 3) and signal time variation (table 4) have been created to show channel coincidences between different SSIDs and how link quality can vary over the time due to several reasons; it is, to show signal behaviour across time.

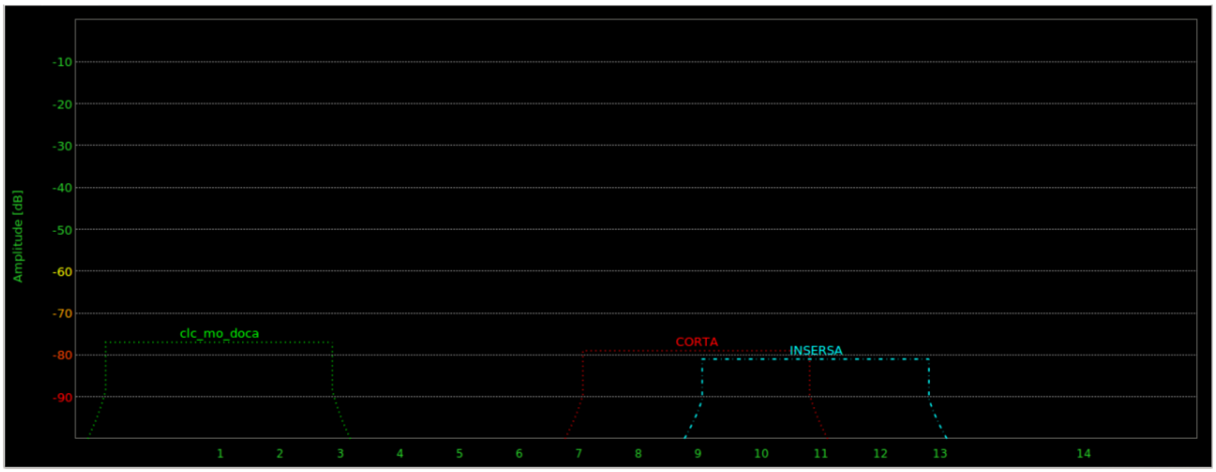


Illustration 3. SSIDs detected per channel in the contractors' area (hut of Inselma)

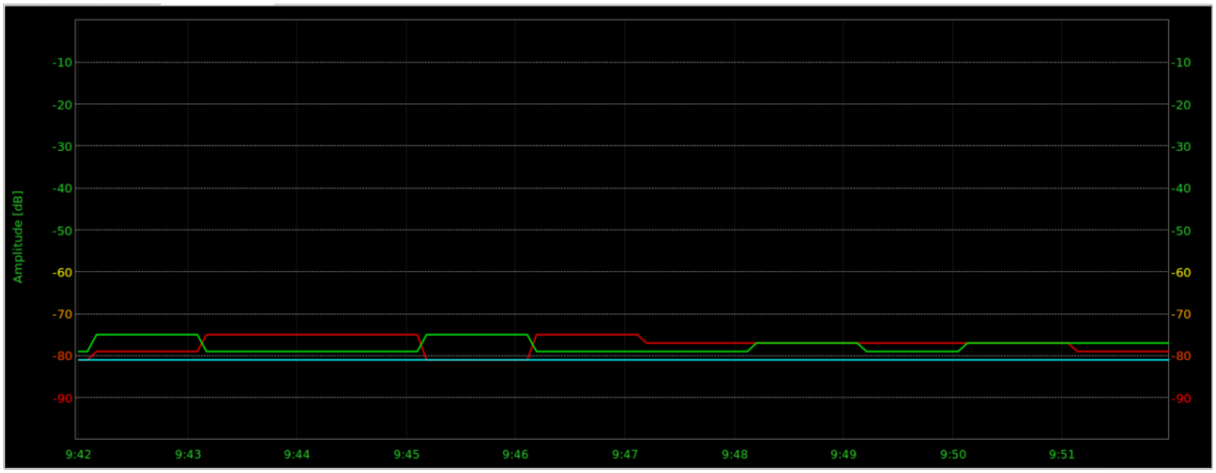


Illustration 4. Signal variations across time in the contractors' area (hut of Inselma)

Due to the frequent signal cuts and the unexpected signal behaviour of several SSIDs, many sampling have been done. As a result, 165 graphs have been generated for the customer's report to satisfy the needs of this part of the study. In every site section, an explanation about the obtained results has been given.

4. Tracking down and inventory of the SSIDs and the main WiFi devices

This section is divided into two subsections. The first one belongs to the task of SSIDs detection and the second to the tracking down of the signal source(s) and its corresponding inventory.

The main goal of this task is to detect any WiFi device acting as an AP or signal transmitter source in the area requested by the customer. Regardless it is a device running as a bridge or anything else with a WiFi adapter, a device owned by CLC or by a contractor, it is important to detect them to prevent wireless infrastructure from attacks, channel overlapping, interferences, unnecessary or malfunctioning devices and to detect lacks and limited WiFi coverage.

4.1. SSIDs detection

Unlike the previous section (study of the signal levels), which was done based on a per site sampling, SSIDs detection has been done based on a per area sampling. In this case, each sampling has taken between 1 and 3 hours long and the probe laptop has been placed in several points within each area to detect as many different SSIDs as possible. It has not been an static sampling, but in motion. Illustration 5 shows the area covered with this task.

To accomplish this part, these software and hardware tools have been used:

- Software:
  - WiFiway 2.0.1 operating system
  - Airmon-ng and airodump-ng
- Hardware:
  - Sony Vaio laptop with integrated WiFi adapter (based on chipset Intel 2200bg)

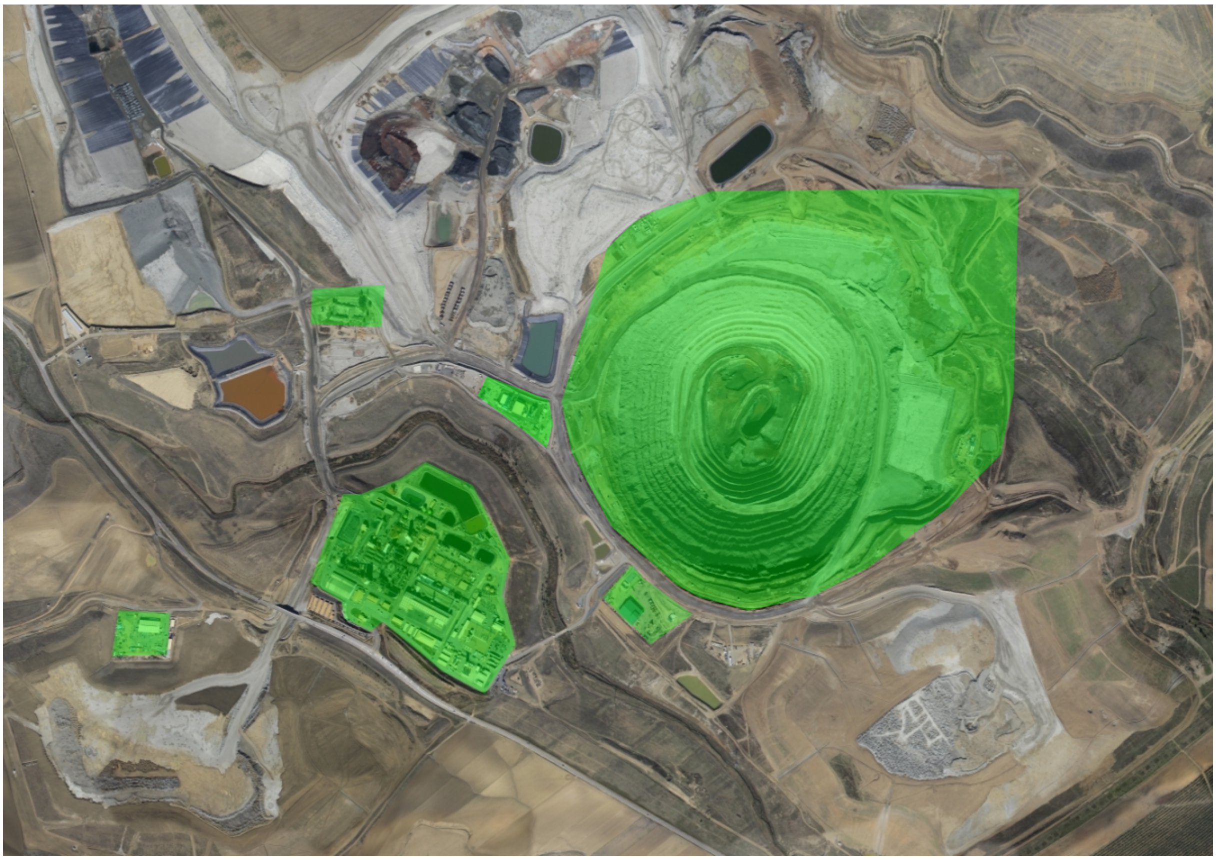
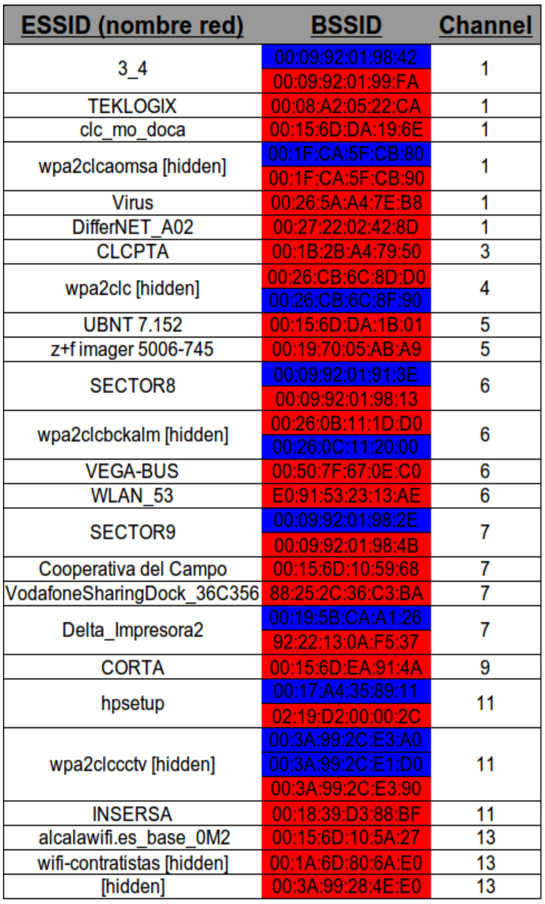
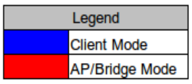


Illustration 5. Area covered with SSIDs detection

Capturing any WiFi packet, it was possible to get hidden and non hidden SSIDs and to extend results from the previous section. Consequently, at the end of this task, 6 main areas (25 subareas) have been sampled and 25 different SSIDs have been detected. 19 of them are non hidden SSIDs and 6 hidden. 5 of these 6 SSIDs have been discovered by the use of advanced packet capturing and analysis tools. Table 4 lists the result of the 25 detected SSIDs.



ESSID (nombre red)	BSSID	Channel
3_4	🟦 00:09:92:01:98:42 🟥 00:09:92:01:99:FA	1
TEKLOGIX	🟥 00:08:A2:05:22:CA	1
clc_mo_doca	🟥 00:15:6D:DA:19:6E	1
wpa2clcaomsa [hidden]	🟦 00:1F:CA:5F:CB:80 🟥 00:1F:CA:5F:CB:90	1
Virus	🟥 00:26:5A:A4:7E:B8	1
DifferNET_A02	🟥 00:27:22:02:42:8D	1
CLCPTA	🟥 00:1B:2B:A4:79:50	3
wpa2clc [hidden]	🟥 00:26:CB:6C:8D:D0 🟦 00:26:CB:6C:8F:90	4
UBNT 7.152	🟥 00:15:6D:DA:1B:01	5
z+f imager 5006-745	🟥 00:19:70:05:AB:A9	5
SECTOR8	🟦 00:09:92:01:91:3E 🟥 00:09:92:01:98:13	6
wpa2clcbckalm [hidden]	🟥 00:26:0B:11:1D:D0 🟦 00:26:0C:11:20:00	6
VEGA-BUS	🟥 00:50:7F:67:0E:C0	6
WLAN_53	🟥 E0:91:53:23:13:AE	6
SECTOR9	🟦 00:09:92:01:98:2E 🟥 00:09:92:01:98:4B	7
Cooperativa del Campo	🟥 00:15:6D:10:59:68	7
VodafoneSharingDock_36C356	🟥 88:25:2C:36:C3:BA	7
Delta_Impresora2	🟦 00:19:5B:CA:A1:26 🟥 92:22:13:0A:F5:37	7
CORTA	🟥 00:15:6D:EA:91:4A	9
hpsetup	🟦 00:17:A4:35:89:11 🟥 02:19:D2:00:00:2C	11
wpa2clccctv [hidden]	🟦 00:3A:99:2C:E3:A0 🟦 00:3A:99:2C:E1:D0 🟥 00:3A:99:2C:E3:90	11
INSERSA	🟥 00:18:39:D3:88:BF	11
alcalawifi.es_base_0M2	🟥 00:15:6D:10:5A:27	13
wifi-contratistas [hidden]	🟥 00:1A:6D:80:6A:E0	13
[hidden]	🟥 00:3A:99:28:4E:E0	13



Legend	
🟦	Client Mode
🟥	AP/Bridge Mode

Table 4. List of detected SSIDs, their operational channels and MAC

It is important to mention that this task has been done over several weeks and sampling on the same areas have been repeated several times in order to get the most accurate and up-to-date information. However, most of the changes in wireless network infrastructure were done without notice and still they are being made. So, there may be new SSIDs or WiFi devices not showed in this study. Currently, customer is conscious about this fact.

Compared to the signal study, several extra non hidden SSIDs have been detected in the same places. The main reason is that capturing of packets is different from signal study. The first one captures whatever it is detected, even a beacon every few minutes, while the second one studies signal based on other parameters and has other requirements (i. e. to receive a mininum number of packets per second), so it dismiss SSIDs because it is not able to get enough information in a regular basis to analyse those signals and to consider them valid networks.

Previous SSIDs list will be useful to set a baseline for next task: Tracking down and inventory of the main WiFi devices.

4.2. Tracking down and inventory of the main WiFi devices

With the information gathered in the previous section, tracking down of the main WiFi devices was done across the study areas. Also, it has been important the documentation collected from other networking Engineering companies (i. e. ACT and Ping Sistemas) that installed some WiFi infrastructures and from several departments of CLC that manage their own wireless network environment.

Some devices have been located visually during this task, but other devices have needed a more intensive tracking down. In fact, in some cases, special access has been required and even, some devices are still pending of inventory due to their inaccessibility. In a short time, it is expected to solve this subject with the customer for pending devices.

To accomplish this part, these software and hardware tools have been used:

- Software:
  - WiFiway 2.0.1 operating system
  - Airmon-ng and airodump-ng
- Hardware:
  - Sony Vaio laptop
  - External (usb) WiFi device: Edimax EW-7318USg
  - Directional 19 dbi antenna
  - Camera

As part of the inventory, local access to the device has been preferred whenever it has been possible. If not, remote access has been the alternative. However, there are a few located wireless devices for critical systems (i. e. SCADA and industrial electronic control systems) connected to independent networks whose access is restricted. So information will be provided by their engineers.

Once located the device itself, this is the obtained information:

- Vendor
- Model
- Serial Number

- MAC address of wireless interface
- MAC address of wired interface (if it exists)
- Management IP (if possible)
- SSID
- Location
- Owner (i. e. CLC or a contractor)
- State (switched on/off)

Also, several photos have been taken to show its location and a better view of the device. Illustrations 6 to 8 are a sample of the photos taken to several devices.

Illustration 6. Wireless devices used for security patrol

Illustration 7. Camera zoom: a Cisco AP and two directional antennas

Illustration 8. Photos of one end of a wireless point to point link

42 relevant WiFi devices have been located. 8 of them are switched off and inaccessible and the customer has been properly noticed about it. It is important to say that attending to the SSIDs information, there are several wireless networks/devices outside CLC, so their tracking down has not been possible. It has been reported to the customer.

This section contains a per site inventory of those WiFi devices, showing only fields such as Vendor, model, serial number, MAC WLAN, MAC LAN, ESSID and IP LAN for each device.

5. Wireless network assessment

This section deals with the results of the assessment done over the WiFi network infrastructure of Cobre Las Cruces.

The main goal on this work is to get an overall picture of the current infrastructure, mostly of the weaknesses from a point of view of ICT security, and to increase the knowledge obtained in previous sections within this analysis. For this reason, only a few basic penetration tests have been done and the configurations of the accessed WiFi devices have been checked.

Therefore, an intensive vulnerabilities assessment has not been done. In fact, once a vulnerability has been detected privileges scalation has not been tried or the attack of any critical system to take it over. Actually, this would be out of the scope of this project.

It is important to mention that tests that may involve any kind of denial of service have not been launched, so the detected vulnerabilities have not been exploited, althought exploits for those flaws are available over the Internet. Also, session hijacking and collecting of user personal information has been possible in several places in the infrastructure; however, just a few samples have been caught to show that vulnerability. We consider not necessary to pick up a larger amount of personal/confidential information.

In order to accomplish it, several hardware and software tools have been required:

- Software:
  - Ubuntu Linux 10.10 virtual machine
  - BackTrack Linux 5 virtual machine
  - Windows 7 virtual machine
  - WiFiway 2.0.1 operating system
  - Suite of tools aircrack-ng (airmon-ng, airodump-ng, aireplay-ng, packetforge-ng and aircrack-ng)
  - Nmap
  - Nessus
  - Wireshark
  - Cain & Abel

- Hardware:
    - Sony Vaio laptop with integrated WiFi adapter (based on chipset Intel 2200bg)
    - Asus F6V laptop with integrated WiFi adapter (based on chipset Intel WiFi Link 5100)
    - External (usb) WiFi device: Edimax EW-7318USg
    - Omnidirectionnal 4dbi's antenna

As previously mentioned, several techniques have been used to perform this assessment. The most important are packet sniffing, port scanning, banner grabing, arp spoofing/poisoning, Man in The Middle and social engineering among other.

It is important to mention that doing “ping” to a remote host (and obtaining the echo reply successfully) is a good sample of connectivity with that host. Nevertheless, ICMP traffic may be blocked between two hosts. Therefore, to get a connection against several ports (services) of a remote host is a better sign of access. Since that moment, to find out whether services are vulnerable can be checked.

With this assessment, it has been intended to detect several items:

- Use of vulnerable WiFi devices, regardless they are Point-to-Point links or APs.
- Use of weak protocols and/or ciphering algorithms.
- Lack of confidentiality in wireless communications.
- Lack of access controls between hosts from different network segments.
- Low management of events and errors generated by WiFi devices.
- Use of outdated devices and/or configurations.

Apart from a penetration test, another task has been collecting configuration files of WiFi devices in order to analyze them and to create a backup of that information.

According to the scope defined with the customer, 7 SSIDs (and their associated devices) have been audited:

- “clc_mo_doca”
- “CORTA”
- “WiFi-contratistas”
- “SECTOR9”
- “3_4”
- “SECTOR8”
- “CLCPTA”

This document explains the results of 4 of them. These SSIDs are considered good representatives of the different types of wireless network infrastructures found in CLC.

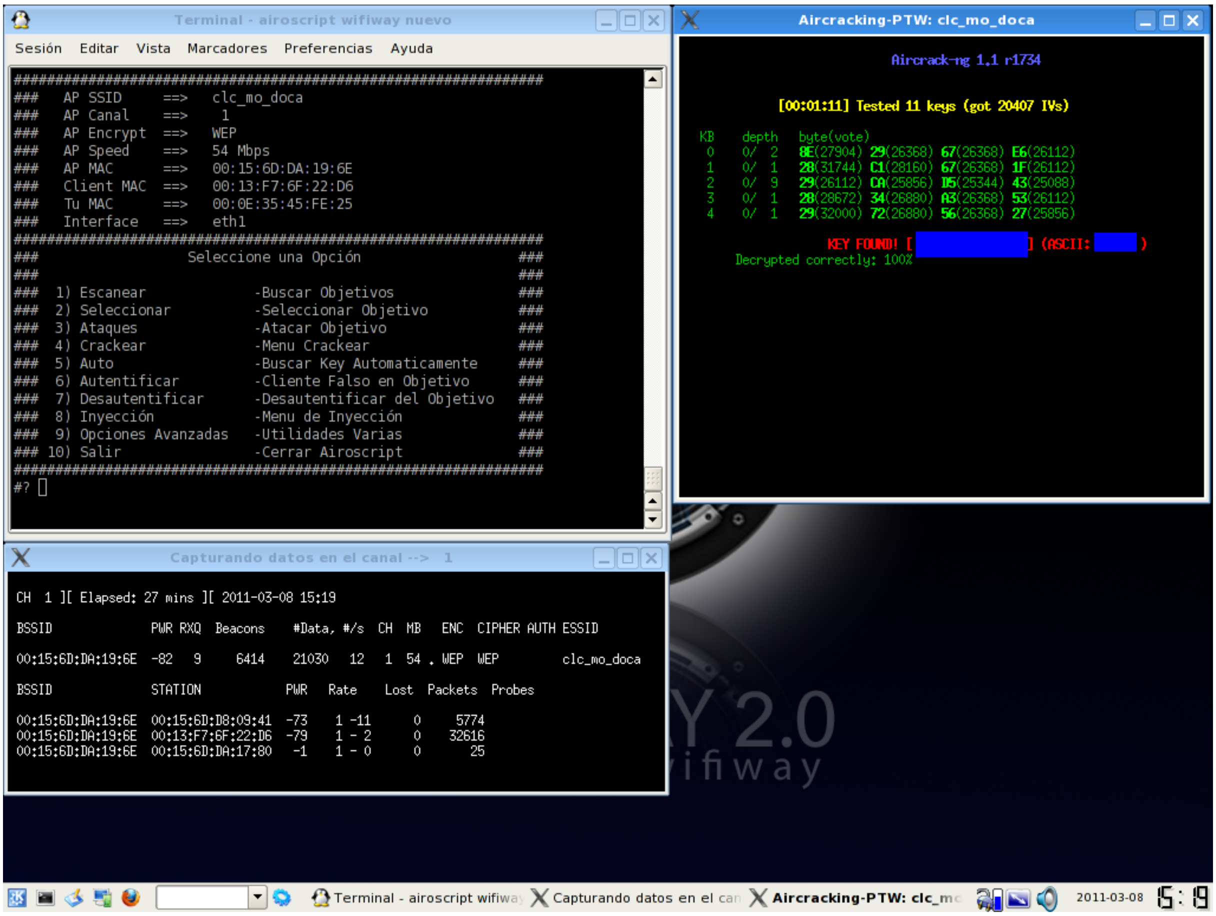
5.1. “clc_mo_doca”

This SSID belongs to the IP cams' system installed on several control access points (el Seroncillo and CLC's wharehouse). This infrastructure is no longer in use because it has been recently replaced by a new system.

In this case of study, the AP (located in the main control access area) was attacked to obtain the WEP key and to demonstrate the weak of WEP ciphering. Moreover the 64 bits choice (like in this case).

After WiFi sampling done in this area, several associated devices were found out. Then, we changed the MAC of our WNIC with one of those obtained in the sampling process in order to avoid possible MAC control access filtering and to improve the attack itself. The main goal was to obtain an ARP packet and to force reinjection of many packets per second in order to get a large amount of data packets containing initialization vectors.

As a result, after getting approx. 21000 data packets it was possible to obtain the key. It took less than 30 minutes. Illustration 9 shows the result of this operation.



Terminal - airoscript wifiway nuevo
Sesión Editar Vista Marcadores Preferencias Ayuda

```
#################################################################
###   AP SSID      ==>   clc_mo_doca
###   AP Canal     ==>     1
###   AP Encrypt   ==>   WEP
###   AP Speed     ==>   54 Mbps
###   AP MAC       ==>   00:15:6D:DA:19:6E
###   Client MAC   ==>   00:13:F7:6F:22:D6
###   Tu MAC       ==>   00:0E:35:45:FE:25
###   Interface    ==>   eth1
#################################################################
###                     Seleccione una Opción                 ###
###                                                           ###
###  1) Escanear              -Buscar Objetivos               ###
###  2) Seleccionar           -Seleccionar Objetivo           ###
###  3) Ataques               -Atacar Objetivo                ###
###  4) Crackear              -Menu Crackear                  ###
###  5) Auto                  -Buscar Key Automaticamente     ###
###  6) Autentificar          -Cliente Falso en Objetivo      ###
###  7) Desautentificar       -Desautentificar del Objetivo   ###
###  8) Inyección             -Menu de Inyección              ###
###  9) Opciones Avanzadas    -Utilidades Varias              ###
### 10) Salir                 -Cerrar Airoscript              ###
#################################################################
#? 
```

```
                         Aircrack-ng 1.1 r1734


              [00:01:11] Tested 11 keys (got 20407 IVs)

   KB    depth   byte(vote)
    0    0/  2   8E(27904) 29(26368) 67(26368) E6(26112)
    1    0/  1   28(31744) C1(28160) 67(26368) 1F(26112)
    2    0/  9   29(26112) CA(25856) D5(25344) 43(25088)
    3    0/  1   28(28672) 34(26880) A3(26368) 53(26112)
    4    0/  1   29(32000) 72(26880) 56(26368) 27(25856)

                   KEY FOUND! [ [redacted] ] (ASCII: [redacted] )
        Decrypted correctly: 100%
```

```
CH  1 ][ Elapsed: 27 mins ][ 2011-03-08 15:19

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:15:6D:DA:19:6E  -82   9     6414    21030   12   1  54 . WEP  WEP         clc_mo_doca

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:15:6D:DA:19:6E  00:15:6D:D8:09:41  -73    1 -11      0     5774
00:15:6D:DA:19:6E  00:13:F7:6F:22:D6  -79    1 - 2      0    32616
00:15:6D:DA:19:6E  00:15:6D:DA:17:80   -1    1 - 0      0       25
```

Illustration 9. WEP key obtained in a while with tools available over the Internet

5.2. “wifi-contratistas”

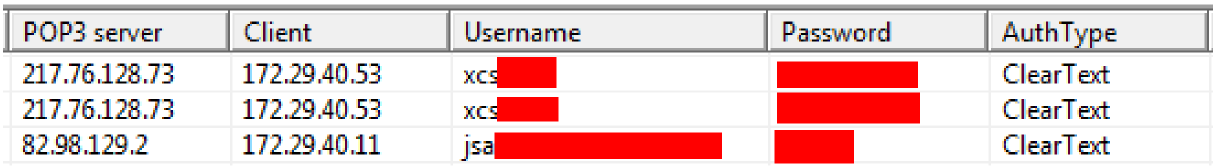
This SSID belongs to a Cisco AP that offers WiFi access to the users in contractors' area. The main goal on this device is to provide with Internet access to those users.

In this case, several flaws were discovered. Notice that this is a hidden SSID so there are many people not able to configure this kind of network by themselves (a part from asking IT staff). Additionally, IP configuration of this device was old so it was necessary to change several things in the routers and switches to gain access to this AP without service interruption.

Once we got access, we obtained running configuration to analyze it. Several issues were found and they may affect the common problems that users are experiencing to connect their computers and mobile devices to that network. For instance, it was reduced to 20 mW the maximum power transmission for clients to connect to this AP.

This network uses a 128 bits key to offer confidentiality. In this case, it was preferred to work on social engineering to obtain this key. Three people were asked and all of them gave us the passphrase (and even several extra keys for other WiFi networks available there). This shows how inefficient is the use of shared keys to protect communications.

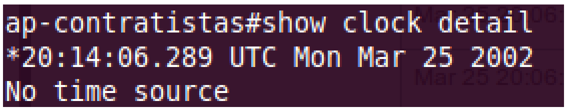
Once we got associated, using packet sniffing, arp spoofing, arp poison and man-in-the-middle techniques, it was possible to get confidential data transmitted in clear text (as seen in Illustration 10).



POP3 server	Client	Username	Password	AuthType
217.76.128.73	172.29.40.53	xcs[redacted]	[redacted]	ClearText
217.76.128.73	172.29.40.53	xcs[redacted]	[redacted]	ClearText
82.98.129.2	172.29.40.11	jsa[redacted]	[redacted]	ClearText

Illustration 10. User data (POP3 e-mail) obtained

With regard to the configuration of the device, it was detected that date and time values were incorrect.



```
ap-contratistas#show clock detail
*20:14:06.289 UTC Mon Mar 25 2002
No time source
```

Illustration 11. Date and time of an AP located in the contractors' area

Additionally, the method to cipher IOS's passwords was Cisco's weak algorithm (“type 7”). So it was easy to obtain the password in clear text using just a webpage. This is one example of a line found in the configuration file:

username apconxxx privilege 15 password 7 113910xxxxxxxxxxxxx

In this case, in few minutes it can be obtained the credentials of an user with administrive permissions.

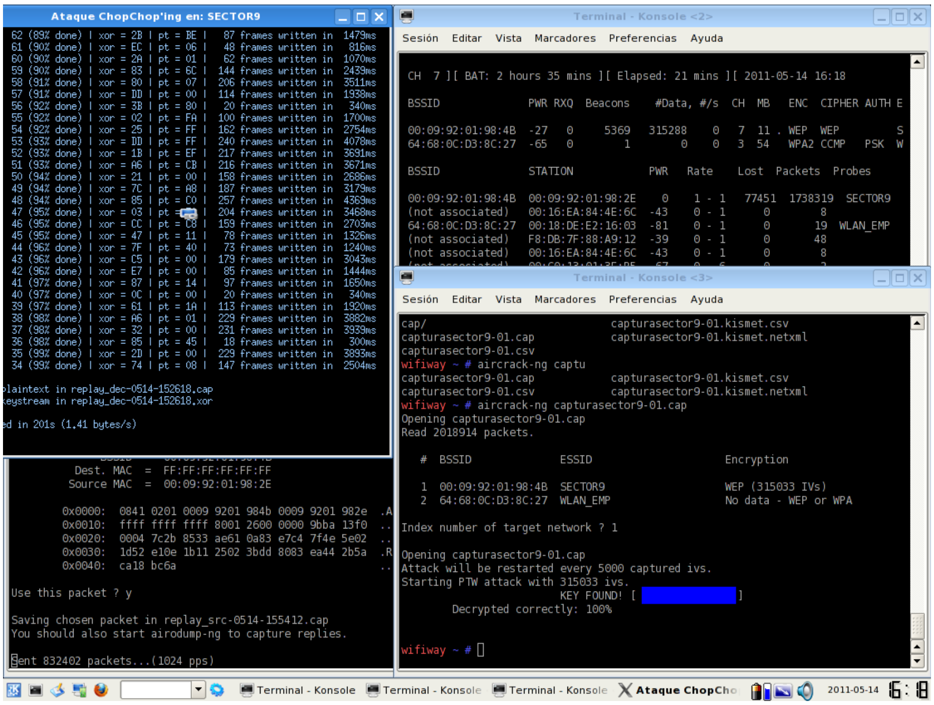
5.3. "SECTOR9"

This SSID belongs to a Point-to-Point link located in the mine area. This link is formed by two WiFi devices that connect two ends (water probes of the water treatment system).

Initially, this network was inoperative so we get access to one of the devices and we got to audit it. This assessment was quite exhaustive because it is such a critical infrastructure that the customer was very interested in knowing any possible flaw.

Some bugs were discovered. Some of them were due to an insecure configuration by default and another due to an obsolete firmware.

Communications were protected by a 64 WEP passphrase. Using an attack based on the creation of a weird packet and its reinjection it was possible to obtain a large amount of data packets containing initialization vectors and eventually to get the key in just 20 minutes. Illustration 12 contains several command lines with the tools used and the result.


Ataque ChopChop'ing en: SECTOR9
Terminal - Konsole <2>
Sesión Editar Vista Marcadores Preferencias Ayuda
Terminal - Konsole <3>
Sesión Editar Vista Marcadores Preferencias Ayuda
Terminal - Konsole
Terminal - Konsole
Terminal - Konsole
Ataque ChopCho
2011-05-14

```
 62 (89% done) | xor = 2B | pt = BE |   87 frames written in  1479ms
 61 (90% done) | xor = EC | pt = 06 |   48 frames written in   816ms
 60 (90% done) | xor = 2A | pt = 01 |   62 frames written in  1070ms
 59 (90% done) | xor = 83 | pt = 6C |  144 frames written in  2439ms
 58 (91% done) | xor = 80 | pt = 07 |  206 frames written in  3511ms
 57 (91% done) | xor = DD | pt = 00 |  114 frames written in  1938ms
 56 (92% done) | xor = 3B | pt = 80 |   20 frames written in   340ms
 55 (92% done) | xor = 02 | pt = FA |  100 frames written in  1700ms
 54 (92% done) | xor = 25 | pt = FF |  162 frames written in  2754ms
 53 (93% done) | xor = DD | pt = FF |  240 frames written in  4078ms
 52 (93% done) | xor = 1B | pt = EF |  217 frames written in  3691ms
 51 (93% done) | xor = A6 | pt = CB |  216 frames written in  3671ms
 50 (94% done) | xor = 21 | pt = 00 |  158 frames written in  2686ms
 49 (94% done) | xor = 7C | pt = A8 |  187 frames written in  3179ms
 48 (94% done) | xor = 85 | pt = C0 |  257 frames written in  4369ms
 47 (95% done) | xor = 03 | pt =    |  204 frames written in  3468ms
 46 (95% done) | xor = CC | pt = C8 |  159 frames written in  2703ms
 45 (95% done) | xor = 47 | pt = 11 |   78 frames written in  1326ms
 44 (96% done) | xor = 7F | pt = 40 |   73 frames written in  1240ms
 43 (96% done) | xor = C5 | pt = 00 |  179 frames written in  3043ms
 42 (96% done) | xor = E7 | pt = 00 |   85 frames written in  1444ms
 41 (97% done) | xor = 87 | pt = 14 |   97 frames written in  1650ms
 40 (97% done) | xor = 0C | pt = 00 |   20 frames written in   340ms
 39 (97% done) | xor = 61 | pt = 1A |  113 frames written in  1920ms
 38 (98% done) | xor = A6 | pt = 01 |  229 frames written in  3882ms
 37 (98% done) | xor = 32 | pt = 00 |  231 frames written in  3939ms
 36 (98% done) | xor = 85 | pt = 45 |   18 frames written in   300ms
 35 (99% done) | xor = 2D | pt = 00 |  229 frames written in  3893ms
 34 (99% done) | xor = 74 | pt = 08 |  147 frames written in  2504ms

plaintext in replay_dec-0514-152618.cap
keystream in replay_dec-0514-152618.xor

ed in 201s (1.41 bytes/s)
```

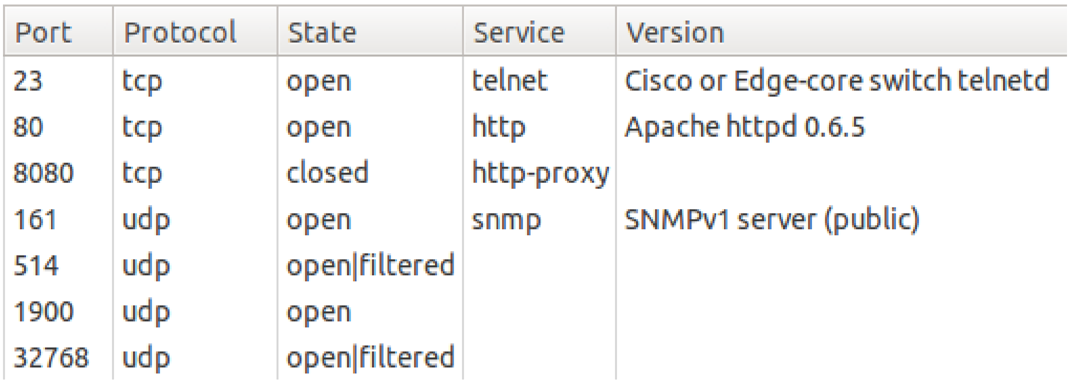
```
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:09:92:01:98:2E

        0x0000:  0841 0201 0009 9201 984b 0009 9201 982e  .A
        0x0010:  ffff ffff ffff 8001 2600 0000 9bba 13f0  ..
        0x0020:  0004 7c2b 8533 ae61 0a83 e7c4 7f4e 5e02  ..
        0x0030:  1d52 e10e 1b11 2502 3bdd 8083 ea44 2b5a  .R
        0x0040:  ca18 bc6a                                ..

Use this packet ? y

Saving chosen packet in replay_src-0514-155412.cap
You should also start airodump-ng to capture replies.

Sent 832402 packets...(1024 pps)
```

```
 CH  7 ][ BAT: 2 hours 35 mins ][ Elapsed: 21 mins ][ 2011-05-14 16:18

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

 00:09:92:01:98:4B  -27   0     5369   315288    0   7  11 . WEP  WEP         S
 64:68:0C:D3:8C:27  -65   0        1        0    0   3  54   WPA2 CCMP   PSK  W

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

 00:09:92:01:98:4B  00:09:92:01:98:2E    0    1 - 1   77451  1738319  SECTOR9
 (not associated)   00:16:EA:84:4E:6C  -43    0 - 1       0        8
 64:68:0C:D3:8C:27  00:18:DE:E2:16:03  -81    0 - 1       0       19  WLAN_EMP
 (not associated)   F8:DB:7F:88:A9:12  -39    0 - 1       0       48
 (not associated)   00:16:EA:84:4E:6C  -43    0 - 1       0        8
```

```
cap/                           capturasector9-01.kismet.csv
capturasector9-01.cap          capturasector9-01.kismet.netxml
capturasector9-01.csv
wifiway ~ # aircrack-ng captu
capturasector9-01.cap          capturasector9-01.kismet.csv
capturasector9-01.csv          capturasector9-01.kismet.netxml
wifiway ~ # aircrack-ng capturasector9-01.cap
Opening capturasector9-01.cap
Read 2018914 packets.

   #  BSSID              ESSID                     Encryption

   1  00:09:92:01:98:4B  SECTOR9                   WEP (315033 IVs)
   2  64:68:0C:D3:8C:27  WLAN_EMP                  No data - WEP or WPA

Index number of target network ? 1

Opening capturasector9-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 315033 ivs.
                       KEY FOUND! [ [redacted] ]
        Decrypted correctly: 100%


wifiway ~ # 
```

Illustration 12. 64 bits WEP passphrase got using a modified packet

Once associated, without using a fake MAC address, it was launched a port scanner to detect open ports (result in table 5).

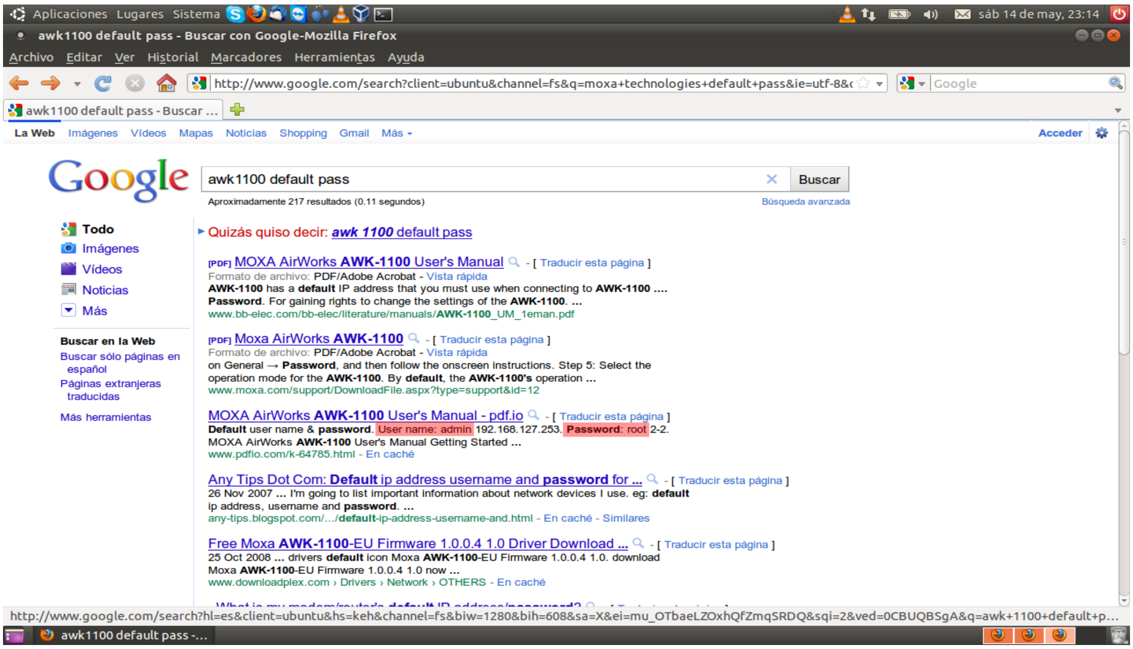


Port	Protocol	State	Service	Version
23	tcp	open	telnet	Cisco or Edge-core switch telnetd
80	tcp	open	http	Apache httpd 0.6.5
8080	tcp	closed	http-proxy	
161	udp	open	snmp	SNMPv1 server (public)
514	udp	open|filtered		
1900	udp	open		
32768	udp	open|filtered		

Table 5. List of open ports and services running

Port 80 was open and it had an obsolete Apache web server version. Current version is 2.2.18 so there is no support for version 0.6.5 and there may be exploits for detected vulnerabilities over the Internet.

Connection to port 80 was stablished using a web browser. Credentials were required but via Google (Illustration 13) it was possible to find the default user and password that were the valid credentials.



Aplicaciones Lugares Sistema
sáb 14 de may, 23:14
awk1100 default pass - Buscar con Google-Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Google
awk1100 default pass - Buscar ...
La Web Imágenes Vídeos Mapas Noticias Shopping Gmail Más
Acceder
Buscar
Búsqueda avanzada
Todo
Imágenes
Vídeos
Noticias
Más
Buscar en la Web
Buscar sólo páginas en español
Páginas extranjeras traducidas
Más herramientas
awk1100 default pass -...

http://www.google.com/search?client=ubuntu&channel=fs&q=moxa+technologies+default+pass&ie=utf-8&(

awk1100 default pass

Aproximadamente 217 resultados (0.11 segundos)

Quizás quiso decir: ***awk 1100*** default pass

[PDF] MOXA AirWorks **AWK-1100** User's Manual - [Traducir esta página]
Formato de archivo: PDF/Adobe Acrobat - Vista rápida
AWK-1100 has a **default** IP address that you must use when connecting to **AWK-1100** ....
Password. For gaining rights to change the settings of the **AWK-1100**. ...
www.bb-elec.com/bb-elec/literature/manuals/**AWK-1100**_UM_1eman.pdf

[PDF] Moxa AirWorks **AWK-1100** - [Traducir esta página]
Formato de archivo: PDF/Adobe Acrobat - Vista rápida
on General → **Password**, and then follow the onscreen instructions. Step 5: Select the operation mode for the **AWK-1100**. By **default**, the **AWK-1100's** operation ...
www.moxa.com/support/DownloadFile.aspx?type=support&id=12

MOXA AirWorks **AWK-1100** User's Manual - pdf.io - [Traducir esta página]
Default user name & **password**. User name: admin 192.168.127.253. **Password**: root 2-2.
MOXA AirWorks **AWK-1100** User's Manual Getting Started ...
www.pdfio.com/k-64785.html - En caché

Any Tips Dot Com: **Default** ip address username and **password** for ... - [Traducir esta página]
26 Nov 2007 ... I'm going to list important information about network devices I use. eg: **default** ip address, username and **password**. ...
any-tips.blogspot.com/.../**default**-ip-address-username-and.html - En caché - Similares

Free Moxa **AWK-1100**-EU Firmware 1.0.0.4 1.0 Driver Download ... - [Traducir esta página]
25 Oct 2008 ... drivers **default** icon Moxa **AWK-1100**-EU Firmware 1.0.0.4 1.0. download
Moxa **AWK-1100**-EU Firmware 1.0.0.4 1.0 now ...
www.downloadplex.com › Drivers › Network › OTHERS - En caché

http://www.google.com/search?hl=es&client=ubuntu&hs=keh&channel=fs&biw=1280&bih=608&sa=X&ei=mu_OTbaeLZOxhQfZmqSRDQ&sqi=2&ved=0CBUQBSgA&q=awk+1100+default+p...

Illustration 13. A successful search in Google for the default user/pass

Once gained access, configuration was checked and it was discovered that:

- MAC-based control access was disabled, although engineers that installed this device stated several times that it was enabled.
- Default SNMP values for read/write communities (public and private) were in use.
- System log was not enable so it was possible to display only the last 17 entries.
- This device had support for 64 and 128 bits WEP and WPA security, but just 64 bits WEP was used. 802.1x protocol was supported too, but it was not used.
- System log refreshing had a bug that allowed to increase one second the time of every log entry each time “Refresh” button was clicked. It was demonstrated that an automated system could modify considerably the real time of an event.

Apart from these flaws, a vulnerability test was launched and two medium risk vulnerabilities were detected in the web server:

- XXS (cross-site scripting) attack vulnerability.
- Cookie injection attack vulnerability.

It is important to mention that thanks to the work done up to now, it was possible to detect a not permitted access to several of the WiFi networks in the mine area. An station located in a contractor wharehouse was trying to get associated with this network. It was able to hack into other WiFi networks in the mine area with WEP security; therefore sampling done in previous sections has become a valuable proof of it. Currently, it is being investigated.

5.4. “CLCPTA”

This SSID belongs to a Cisco device running as AP in the headquarters. It offers WiFi access to the network and to Internet.

This case has no security so it illustrates how easy it is to spy communications between computers and to steal personal/confidential data without any kind of warning or restriction.

Association with this SSID was immediate and using arp spoofing and man-in-the-middle techniques with the aid of an sniffer it was possible to get sensible data. Initially, an arp scan was done to find all the hosts in that network segment. Then, with those previous techniques, several domain user credentials were obtained. It was possible to intercept netbios protocol messages between a desktop and a development server:

```
Source MAC address      :  00:1C:23:1F:36:53
Destination MAC address :  00:41:0A:31:72:A2

Source IP address      :      172.29.1.23
Destination IP address :      172.29.150.56
                           <<domainxxx>>

Protocol:               TCP
Source port:            1767
Destination port:       445    microsoft-ds

Transferred bytes: 22562

Account:
userxxx/userxxx:"":"":35E65C76AF4ACDB2000000000000000000000000000xxxxxx
Additional Info: DOMAIN: <<domainxxx>>
```

Another important data obtained was domain user of the Managing Director and several websites and images visited by this “VIP user”. It was clear text captured due to HTTP access.

Several hosts in different VLANs were accessed. Some of them are IP cams of CLC and contractors. It was possible to connect to a website to display and fully configure these IP cams. In the same network segment it was possible to launch a vulnerabilities test against a computer that manages access to CLC's facilities and two unpatched vulnerabilities were detected. Those bugs allow to execute remote code using SMB and RPC flaws.

Another network segment accessed was that where internal servers are located. A comprehensive network scan was done to discover the hosts and 9 critical servers were port scanned and their services fingerprinted. We considered not necessary to launch a vulnerabilities test against those computers in order to prevent any unwanted behaviour (i. e. DoS). Anyway, it was enough to show how that important network was accessible by anyone connected to “CLCPTA” non secure WiFi network.

6. Conclusions of the analysis

This section contains a set of conclusions after the work done up to now and all the data gathered about CLC's wireless network infrastructure.

It is not intended to act as a guideline or as a set of solutions for the problems detected, but a summary of the current situation of the wireless infrastructure and the main issues found during the analysis stage. In fact, it is expected that whoever that reads this document (mainly the technical people from the IT department) should be able to get a global idea about the environment and its strengths but mainly about its weaknesses.

Notice that due to a confidentiality policy, there are information and conclusions that cannot be showed in this document.

6.1. Overall picture

Wireless network infrastructure of CLC can be divided into 5 main environments:

- Wireless point-to-point links: used to link several areas or sites. There are 3 operational networks and 1 of them is a backup system of a fiber point-to-point link. Also, there is one additional link whose devices are currently switched off. One of those links is a WAN backup, so it is important to get it always up and ready to move from passive to active link whenever it is necessary.

- APs for WiFi networks: used to grant, on the one hand, access to CLC's network only for CLC's users and, on the other hand, access to Internet for contractors. There are two devices running as APs. One in the headquarters and another in the contractors' area. Both WiFi networks are important but not critical.

- Telecontrol wireless network: joined with a fiber based network, the WiFi part is used to extend that network range due to the fact that mine area is continuously getting larger. There are three WiFi links used by “SDR” system (system to manage water inside the mine). One link is currently switched off because it is a backup line between the mine and the production plant and the rest should be working to close the ring network topology, but they are currently inoperative because three of four WiFi devices are out of order. This is a critical network, mostly in case of the fiber line between the mine and the plant fails, because this system cannot be remotely managed.

- IP CCTV system: there are two CCTV systems. One to control several places in the mine area and another system to control customer facilities (i. e.

access, headquarters, etc.). Most of the cams are connected to a separated fiber network, but there are 6 cams (and additional cams pending of installation) conected through WiFi devices. A third system could be considered, but there are not WiFi devices connected there. All of those cams (wired and wireless) are IP devices.

- Other devices: Printers with WiFi adapter, barcode scanners and slide projectors. Most of them are used/owned by contractors. They are not monitored and usually installed according to temporary requirements.

Regarding to the detected problems, they are mainly due to 3 items:

- Unkwnoledge about what it is actually installed and working.
- Decentralized management of the WiFi infrastructures and just focused on satisfying the temporary needs.
- Use of old technologies and configurations with a low security level.

6.2. Management

According to whom it manages each wireless network infrastructure we can made 4 partitions:

- IT department: they only manage wireless point-to-point links and APs for WiFi networks. In fact, they have not a full knowledge about devices used in those links. In case of wireless failure, they get in touch with Ping Sistemas, that installed those communications systems. They manage incidences of devices from Mining department too.
- Mining department: they know about the existence of several cams in the mine area that are connected to a WiFi network but nothing else. They are worried about one cam used to monitor periodic controlled mine blowing up whose signal is received by the Chief of this department. The full system (cams and WiFi infrastructure) was designed and deployed by Doca Eléctricos, but the system is currently managed by Ping Sistemas. Complaints have increased because the system is not currently working and signal interruptions are common. They report incidences to IT department.
- Water treatment department: they have their own management about telecontrol network and its devices. Nobody has technical knowledge about what and how has been installed (with regard to WiFi devices). When they detect any problem that affects to the telecontrol network and the industrial

electronic control system, they get in touch with ACT, which is the company that installed and currently maintains all the system. Apart from several people of this department nobody from CLC knows about how this system works. Network devices are not monitored.

- Security patrol: they manage the set of cams with WiFi adapters. One part of the system was designed and deployed by Doca Eléctricos, but it has common technical flaws. Ping Sistemas has updated this system and installed new devices. This is the company to whom they directly report when there are technical failures. People from security patrol have knowledge about most of the current working devices, but not about the wired or wireless connection and whether they are connected to one SSID or another.

Up to now there is no person with a wide knowledge about which devices and how they are installed now. Each department manages its own incidences and reports technical issues to its contractor and then gets a solution for its problems in an isolated way. Also, it is important to mention that the company that manages switching, routing and networking security (Eneo Tecnologia) only monitors a few devices (such as Point-to-Point links and several IP cams) of those belonging to wireless networking.

There is no SLA defined with technological suppliers.

In CLC, technical issues are carried out in an autonomous way by several departments and mostly by companies different from CLC. Therefore, the customer has not an overall picture of his infrastructure and he relies on solutions given by other companies. In case of failure, how can someone decide about subjects connected to CLC's WiFi infrastructure knowing only the tip of the iceberg? Who does control quality of the work done by those technological contractors?

6.3. Technical issues

As seen in other sections, there is no control over WiFi devices installed in CLC. It involves that several departments get in touch with their own suppliers in order to install as many WiFi devices as required in that moment. And the same to solve problems. In the same way, unexpected WiFi devices can “appear” and “disappear” without knowing how their installation and uninstall can interfere over other critical wireless networks already running (i. e. channel overlapping). In fact, there is no central management over installed WiFi systems in CLC and it involves a lack of coordination and prevention from technical problems. Moreover, nobody alerts if someone install his/her own AP for a personal need.

Not important channel overlapping scenarios have been found, and situations where signal interferences could be something to have into account have been reported to the department responsible person. Also, the actions taken are detailed in the document that was delivered to the customer. The next illustrations (from 14 to 16) show detected WiFi signals from different SSIDs in some parts of CLC's facilities.

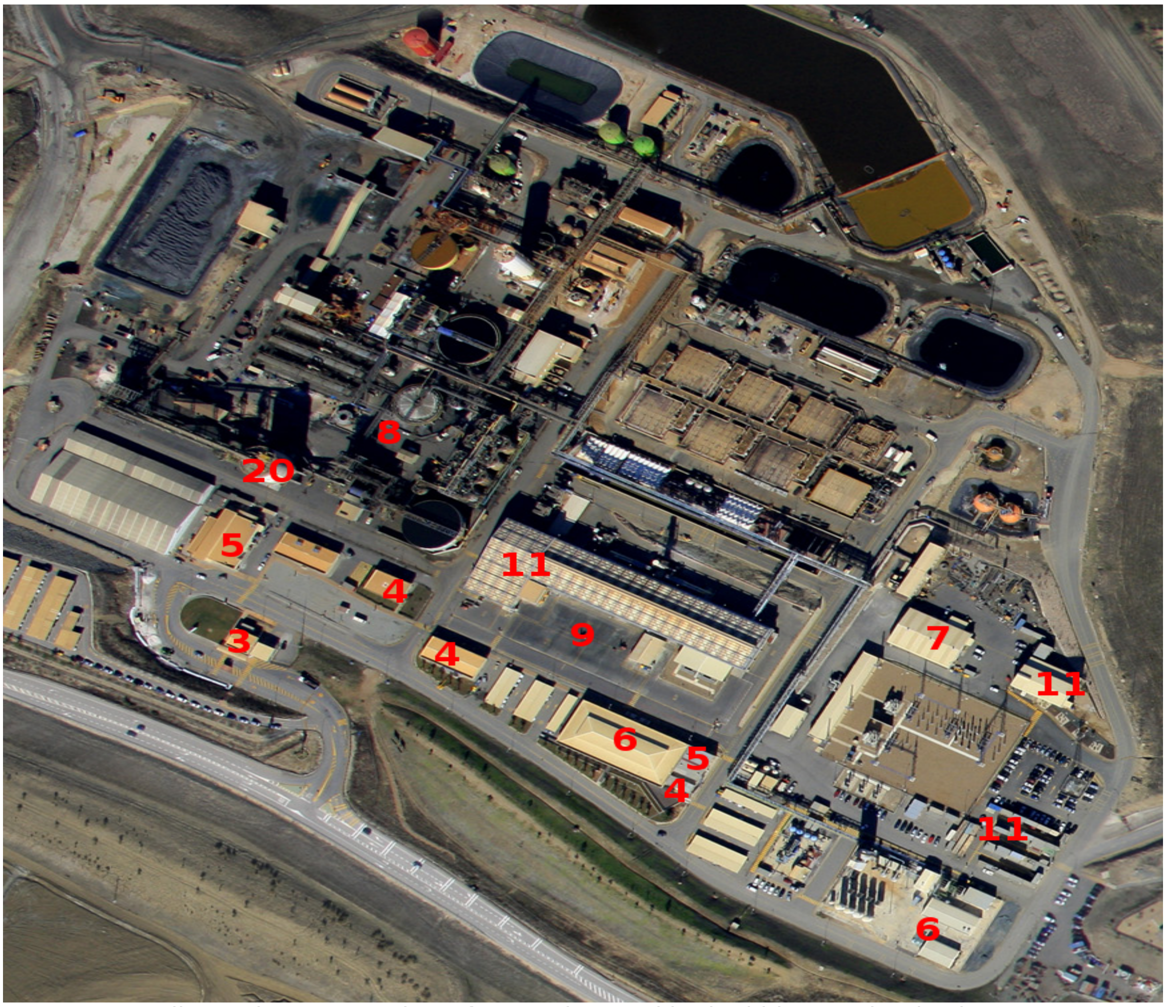


Illustration 14. Number of SSIDs detected in the hidrometalurgic plant

Illustration 15. Number of SSIDs detected in CLC's wharehouse

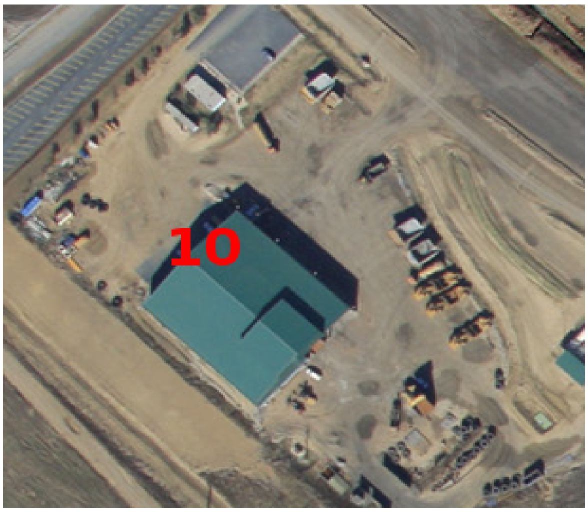


Illustration 16. Number of SSIDs detected in AOMSA's wharehouse

With regard to the WiFi AP installed in contractors' area, several incidences have been reported. In fact, that SSID is hidden as a security measure, signal power has been reduced to avoid interferences with other wireless devices and several parameters have been changed in the configuration to grant some control over that WiFi network. But users have problems to connect to that network, in some cases due to a coverage problem and in other cases due to the hidden SSID (users are not able to manually configure that network by themselves). Additionally, it has an outdated IP configuration (as the network with SSID “CLCPTA”) that hinders us from accessing to the device management console.

It has been detected that several wireless devices (i. e. Cisco and D-Link APs/bridges) are switched off, whereas other point-to-point links are down waiting for the repair of one or both end devices. In the same way, Doca Eléctricos installed Ubiquiti WiFi devices and gave outdated information, so technicians from Ping Sistemas have difficulties to access and/or to properly configure those devices. Those devices are used together with cams that currently are experiencing connectivity problems.

In the previous WiFi assessment section, it has been showed that WiFi network security has several threats. Next, there are a few examples:

- Ease for communications spying and user data theft. Every guest or user could pass oneself off as other person or to tap communications between two computers (i. e. using WiFi networks without confidentiality or WEP algorithms of 64 or 128 bits that are weak).

- Critical vulnerabilities detected in several hosts. Such as in a computer located in “Control de Seguridad”, with bugs solved by Microsoft several years ago but not patched yet.
- Unrestricted access to configuration and display of security patrol cams.
- Low maintenance and updating of WiFi devices. An example of it is the use of firmware with obsolete components, such as WiFi devices that link water treatment system in the mine area.
- Unrestricted access to other network segments for every user connected to a WiFi network. It has been demonstrated accessing from the WiFi network situated in the headquarters to several subnetworks and getting information of their hosts.
- Use of insecure configurations. For instance using default passwords to access to the management console of several devices.
- Repeating credentials to use and to configure different WiFi devices. By and large, each technological supplier has used the same credentials for each WiFi device he has installed. Those credentials have not been modified over the last years.
- Lack of WiFi intrussion detection and prevention systems. The users can attack WiFi security protocols (i. e. WEP) without generating any kind of event or alert. Furthermore, countermeasures are not done. The best example of it is just the fact of been able to accomplish all the tests done within the WiFi assessment using tools that everybody can dowload from Internet.
- Use of security policies based on hidding data. For instance, the network with SSID “WiFi-contratistas”. Its SSID is hidden and the password is private, but everyday less users ask for permission to IT department to connect their laptop to that network. Using social Engineering it has been showed that users share publicly that key to everybody that “requires” it. Therefore, use of shared keys is not a good way to maintain communications confidentiality.

Regarding to security, it is important to mention that some Point-to-Point links are quite secure (using WPA2, 802.1x based authentication and hidden SSIDs). This assures confidentiality in the communications. However, the configuration of these devices has not up to date password protection mechanisms or monitoring and event collecting systems. For instance, they use Cisco's ciphering algorithm to store IOS passwords (“type 7” identificated), which is weak, insted of MD5 hashes (“type 5” identified), that are not reversible.

And what about if a new WiFi device is installed without permission? What would be the effects of an undetected rogue AP used to gather personal information from users or confidential information from CLC?

At a sum, we consider that an heterogeneous wireless infrastructure may benefit in some cases, but in a corporate environment like this, it probably involves a higher response time in case of failure, security threats, a lesser knowledge of the inversion done and a problem of resources optimization.

Chapter 3 - Design of a WLAN solution

1. Introduction to the design part

The goal of this section is to show the contents of the second phase of the four that form this project; it is, the design of a Wireless LAN solution.

It starts with the main goals to be solved on this approach. Those items were collected during the interview with the customer where the results of the analysis stage were showed.

Once defined those goals, the design of the solution is showed. Then, the advantages of this design are listed and a summary of the parts that form this approach are given too. In fact, due to the design of such a complex solution, which embraces multiple technologies, it has been divided into several parts. This involves introducing the overall of the result (called “photo finish”) and later, the detail of each part.

This solution is given in a modular basis, so that each part is as autonomous as possible. It allows the customer to decide whether to accept a module or to change something else without affecting the rest. Therefore, once all the modules have been deployed all the pieces will fit together like a puzzle. Consequently, all the requirements (the goals) will be achieved and a highly secure WiFi environment will be guaranteed.

2. Goals to achieve

This section enumerates the main goals aimed to be achieved by the design of this solution. They were defined once the stage of analysis was finished and the report with the results was delivered to the customer. In fact, they are the result of the weaknesses and lacks detected in the current wireless network infrastructure.

As the customer stated, several of these goals are critical due to the threats showed in the assessment of the WiFi infrastructures.

Next, these are the goals:

- To provide the corporate users with WiFi access to CLC's network and to Internet.
- To provide the contractors and the guests users with access to Internet through WiFi.
- To deploy WiFi area of influence across only these 7 working centres:
    - Área de Gestión Documental
    - Oficinas Generales
    - Panel de Control
    - Sala de Formación
    - Taller Eléctrico
    - Taller Mecánico
    - Zona de Contratistas
- To create an user friendly infrastructure to connect to the WiFi network.
- To distinguish easily between corporate and non corporate users.
- To prevent all the wireless infrastructure from RF interferences and channel overlapping.
- To reuse as much as possible the already available WiFi devices.
- To grant confidentiality on the channel and environment used to transmit information, it is, the air.
- To unify security system across all the WiFi infrastructures currently available.

- To maximize the control over all the WiFi infrastructures in order to prevent against possible attacks and intrussions from inside/outside CLC's dependencies.
- To deploy a system to detect the rogue APs/stations. This system should provide the tools to define the policies for the countermeasures against those malicious devices.
- To prevent against the installation of non-authorized APs all around CLC's dependencies.
- To provide the contractors with a solution useful enough so that they gently move from their own AP with Internet access to the CLC's WiFi corporate solution. It is imperative to withdraw those APs not owned by the customer.
- To update devices and their configurations as much as possible so that the previously detected flaws can be solved.
- To establish a secure and automated system of data collecting and maintenance for the configurations of all the WiFi devices.
- To integrate the solution with the current customer's ICT infrastructure.
- To design a highly scalable and modular solution according to the state-of-the-art for this kind of systems.

3. Overall picture

This section shows the design of a secure WLAN solution for Cobre Las Cruces. This is the overall image of the proposed design that, as previously stated, it neither offers an exhaustive perspective of each technology in use nor the infrastructures affected. It will be done in the next subsection.

This solution, as showed in illustration 17, aims to be a combination of several state of the art technologies and security standards. These are a sample:

- Technologies involved:
  - WiFi sensors running as IDS/IPS
  - Multiple APs in a Lightweight AP – Wireless LAN Controller topology
  - Multiple SSIDs to differentiate between different user profiles
  - Digital certificates
  - Multiple WLANs to isolate traffic from/to insecure zones and to restrict access to several segments of the corporate network

- Security standards and protocols in use:
  - 802.11i → WPA2 protocol
  - 802.1x → RADIUS based authentication infrastructure
  - EAP → authentication method
  - AAA (authentication, authorization and accounting)
  - LWAPP / CAWAP protocol to manage lightweight access points

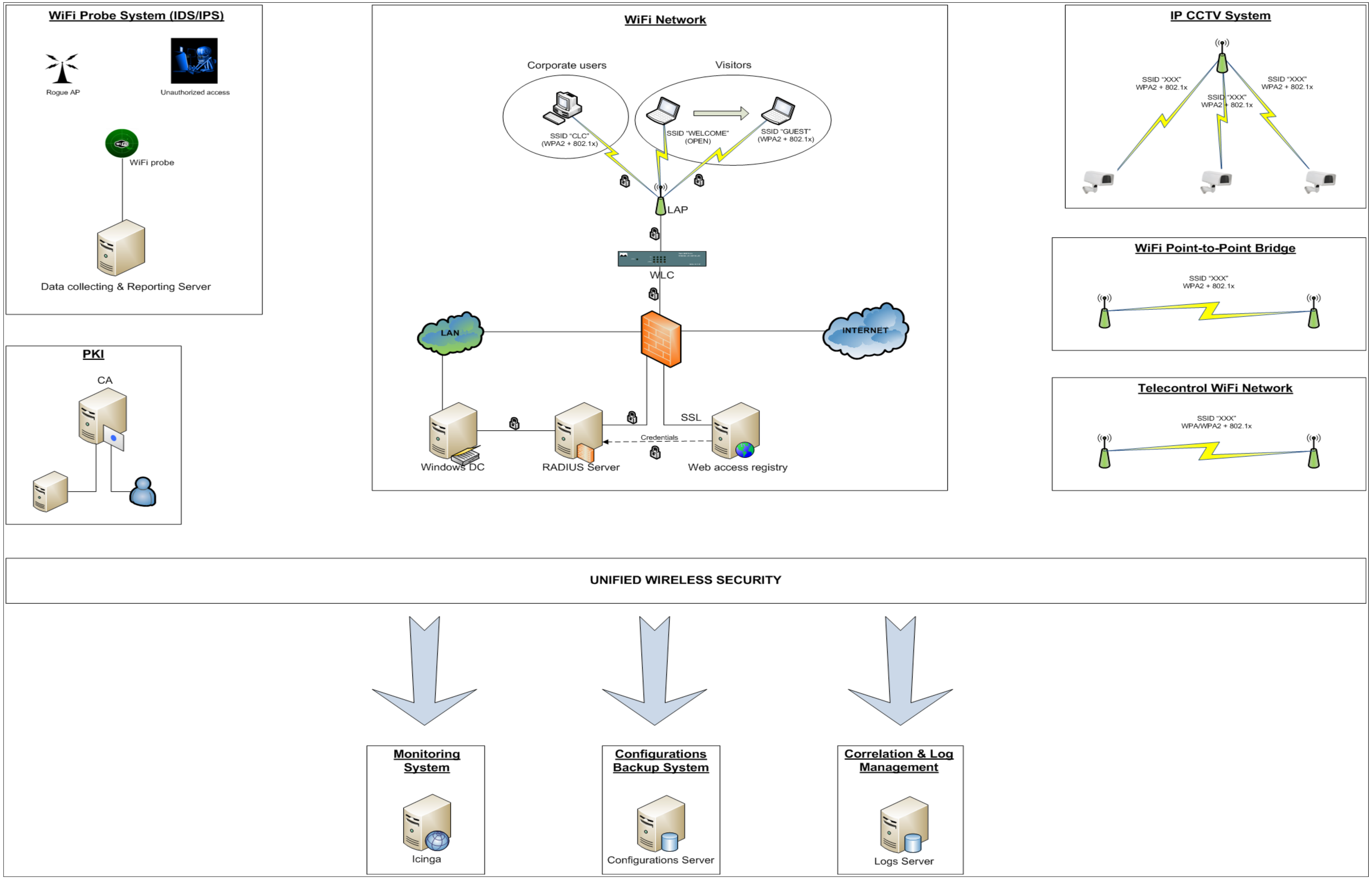


Illustration 17. Overall picture of the solution

3.1. Explanation of the design

The proposed design deals with 5 different WiFi infrastructures. Each one has its own particularities but all of them have been adapted to a global wireless solution. The main purpose is to offer an overall picture so that the customer is able to know which will be the result of this project. After that, in order to define how to arrive to this end, the design has been divided into some pieces and treated in a separated way. This allows to focus on each part in a more efficient way and to work on it as an autonomous item (eventually integrated with the rest). The modifications and the performance tests are preferred to accomplish in a more controlled infrastructure.

Apart from those WiFi infrastructures, there are additional technologies developed within this approach. Nonetheless, they will be showed as different modules (in the same way as the WiFi infrastructures). Therefore, it involves a total of 8 modules or “subprojects”. It is important to take into consideration that monitoring system is not an independent module because there is already a running system. So, integration into that system will be considered a part of each module.

Next, a brief explanation of each module:

- WiFi Network: this part will consist of a set of lightweight APs centrally managed by a Cisco Wireless LAN Controller. Autonomous APs will be upgraded to LAP mode. WPA2 and 802.1x will be used in order to gran confidentiality in the communications from end-to-end. EAP will be the preferred authentication mode using digital certificates. Three global SSIDs will be created: one for corporate users validating their credentials against a Windows Domain Controller and two SSIDs for visitors. One of those two will be an OPEN and isolated network used by default to allow guests to fill in a form (through an automated redirection to a local website) to ask for valid credentials to connect to the “official” guests WiFi network. Once a set of valid credentials are generated, the system updates a local database of credentials in the RADIUS Server and guests will be allowed to connect to the other SSID.

- WiFi Probe System (IDS/IPS): initially thought as a extension of the IDS/IPS system provided by the devices that form the WiFi network, a number of WiFi devices running as a probe will be deployed around CLC's dependencies, whenever the lightweight APs cannot be installed. They will detect rogue APs, unauthorized access (or just failed attempts to gain access) to the WiFi networks. Those devices will use a Linux based firmware (i. e. DD-WRT) and several scripts developed to detect and to report those events. A server will be used for data collecting and to create an automated reporting system and a centralized management point for all of the probe devices.

- PKI: a Public Key Infrastructure is required to deploy and manage per server and per user certificates to authenticate within the 802.1x infrastructure.

Additionally, this infrastructure will be used by the customer for other goals (i. e. messaging signature).

- IP CCTV System: there are two different CCTV deployments, so each one will require different measures. So far, the most insecure is the system that links cams installed in the mine area, so it will require a physical change of those WiFi devices. By and large, modifications in the current configurations will be required too.
- WiFi Point-to-Point Bridge: by and large, this is the most secure infrastructure. 802.11i standard is already in use so only a few changes will be required in the configuration of the devices. This infrastructure is already included in the monitoring system.
- Telecontrol WiFi Network: this critical infrastructure will require to deal with the Engineering company that maintains this infrastructure. An initial design to change the devices or to update the firmware will be proposed. The purpose is to reach WPA2 (or at least WPA) protocol for communications confidentiality and 802.1x for authentication. This design will include the installation of a local RADIUS server in that network and monitoring of all those devices.
- Configurations Backup System: running as an automated system for collecting and storage of configurations of all the WiFi devices (whenever it is allowed such as in the Cisco devices). It will be a central repository for those configurations. The task will be executed in an scheduled way to connect (i. e. via ssh) to the device and to obtain its configuration).
- Correlation and Log Management: a centralized server will become the point where all the devices will storage their logs and events. Having all of them in a central point will allow to manage and audit them in a efficient way.

Additionally to this items, there are a set of measures that have not been showed in the previous picture but they make up the overall picture:

- To update firmware of some of the WiFi devices.
- To securize the configurations of some of the devices to protect items such as privileged/administrative passwords.
- To define a corporate ICT security policy in order to prevent the arrival of vehicles carrying WiFi devices and the unauthorized and/or out-of-control installation of APs.

3.2. Advantages of this solution

This subsection lists the main pros provided by this solution. They are enumerated from an overall perspective, so they are expected to increase as a result of the detailed part of each module.

These are the advantages:

- Integration between each part of the design and with the already in use ICT infrastructure.
- Creation of a security baseline so each WiFi infrastructure has a common security by the use of specific technologies and protocols. It guarantees a high level of security by default.
- Confidentiality and non-repudation in communications.
- Prevention against identity spoofing and thieft in an 802.11 environment.
- Future vision to allow scalability and integration with new technologies in security and network management fields (i. e. PKI)
- Reuse of available WiFi devices, mostly Cisco and D-Link models. Those equipments that do not reach a minimum security level have been isolated and will be dealt with their supplier in order to find out a solution (i. e. to update their firmware).
- User friendly system. The main part of the infrastructure will be transparent for the end user and whenever user interaction is required, a detailed set of instructions will be provided (i. e. the web interface to create the valid credentials to connect to the guest WiFi network). The perspective of the end user has been one of the subjects taken into consideration over the design of this solution.
- Reduction of the time of response in case of failure of a WiFi device.

4. Detailed solution

This section consists on a detailed explanation of each part that makes up this approach.

It is important to mention that the main parts of this solution are the WiFi Network and the probe system. Therefore, they were showed to the customer and now they are pending of approval. If approved, a model will be created to show how they work. The rest of the solution is detailed in this section too, but not in such an exhaustive way.

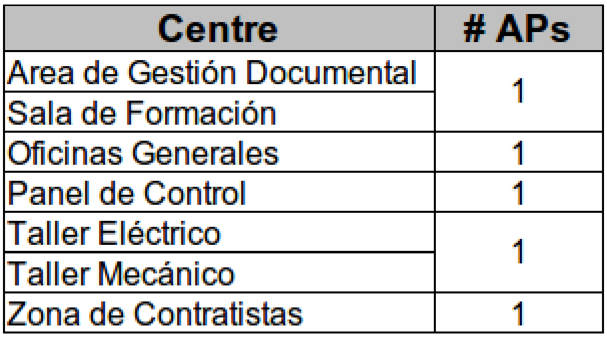
The module corresponding to the Publick Key Infrastructure is a primary subject that requires additional data gathering in order to design a corporate infrastructure able to be used by additional systems and services within the corporation. However, depending on the result of the two already delivered parts, the PKI will be designed or not.

4.1. WiFi Network

The goal on this part of the project is to get that 7 working centres have access to a global WiFi network.

It has been designed using multiple APs and based on the use of Lightweight Access Points (LAPs) managed in a centralized way by a device known as Wireless LAN Controller (WLC). Throught this device it will flow either control data (among devices) or user data.

Next (table 6), this is the distribution of the APs, taking into consideration all the available devices now (only Cisco equipments):



Centre	# APs
Area de Gestión Documental	1
Sala de Formación	
Oficinas Generales	1
Panel de Control	1
Taller Eléctrico	1
Taller Mecánico	
Zona de Contratistas	1

Table 6. Distribution of the APs by centre

This approach requires the use of 5 devices to connect the 7 working centres, as illustration 18 reflects. Due to the proximity between several buildings, it may be possible to use fewer.

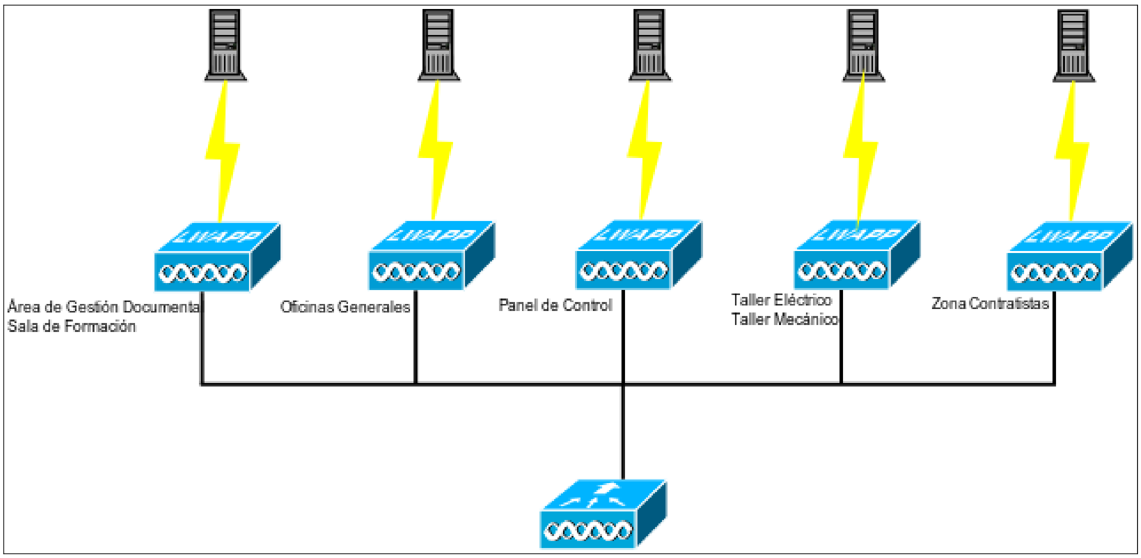


Illustration 18. Design based on 5 ligthweight APs and 1 Wireless LAN Controller

This approach considers the use of the protocols LWAPP and/or CAPWAP to manage the lightweight APs. It is important to mention that CAPWAP is already an standard so it is used by some vendors.

Already in use (and available) WiFi devices are running in autonomous mode, then it will be required to upgrade their Cisco IOS to a lightweight AP operational mode. All the models available (Cisco Aironet 1242 and 1310 series) in CLC support this upgrade.

As it can be appreciated, this design is scalable and it brings the opportunity to add new WiFi devices whenever it is necessary.

This solution uses several SSIDs to distinguish between different user profiles and several WLAN to create different network segments. Notice that the firewall (already in use) is a very important item within this design.

Corporate users

Illustration 19 shows the solution proposed for the corporate users profile.

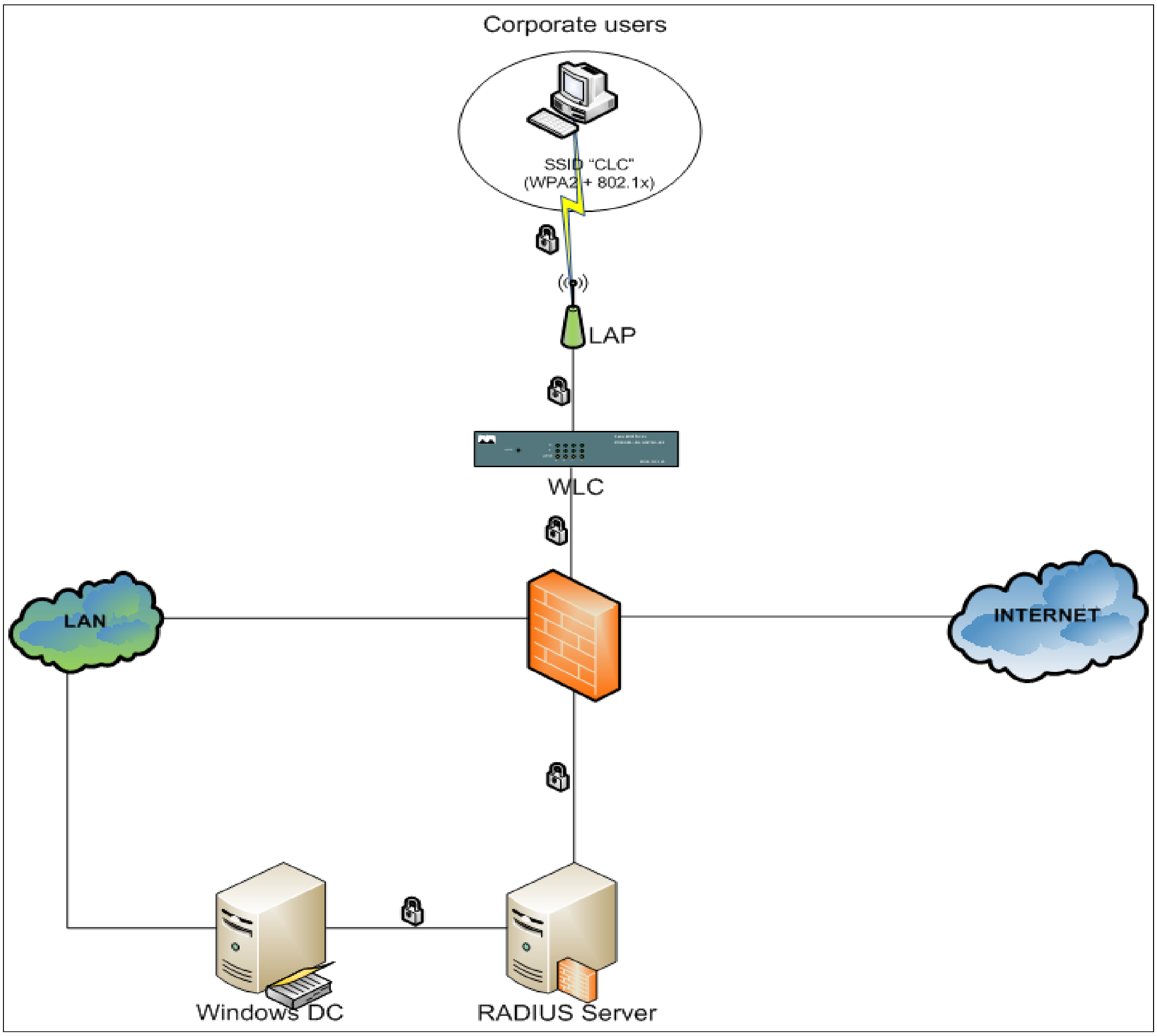


Illustration 19. Detail of the WiFi Network for corporate users

According to this solution, one possible SSID would be "CLC".

To cipher communications, the procol used would be WPA2, whereas authentication would be based on an implementation of the 802.1x protocol. Therefore, user would have to validate his credentials against a RADIUS server, which would verify them in Active Directory database; it is, a collection of users (and other objects) allocated in the Domain Controllers belonging to the Windows 2003 domain. In that way, EAP based would be the proposed method, using digital certificates, so that mutual device and user authentication would be granted. However, EAP extension must be analyzed in a more extensive way in order to decide about the use of one of the multiple choices. By now, EAP-TLS, EAP-TTLS and PEAP are the main candidates.

With this approach, communications are secured end to end and domain credentials are unique for each user and managed in a centralized way.

The deployment of this part of the project, based on the use of digital certificates at both ends, would require to design and to deploy a Public Key Infrastructure (PKI).

According to this part of the solution, once the host is associated and authenticated (and authorized), the user will have access to the CLC's network and to Internet.

Visitors (guest and contractor user)

For this kind of users, the proposed infrastructure is a bit different to that used for the corporate users, so that RADIUS server would not validate user credentials against Active Directory, but a local users database. Unlike the previous part, this infrastructure would not use digital certificates to verify identity of both entities, only the server part. Compared with the previous one, this approach relaxes security levels, but it is enough taking into consideration the cost of deploying certificates across visitors, that would be something inefficient.

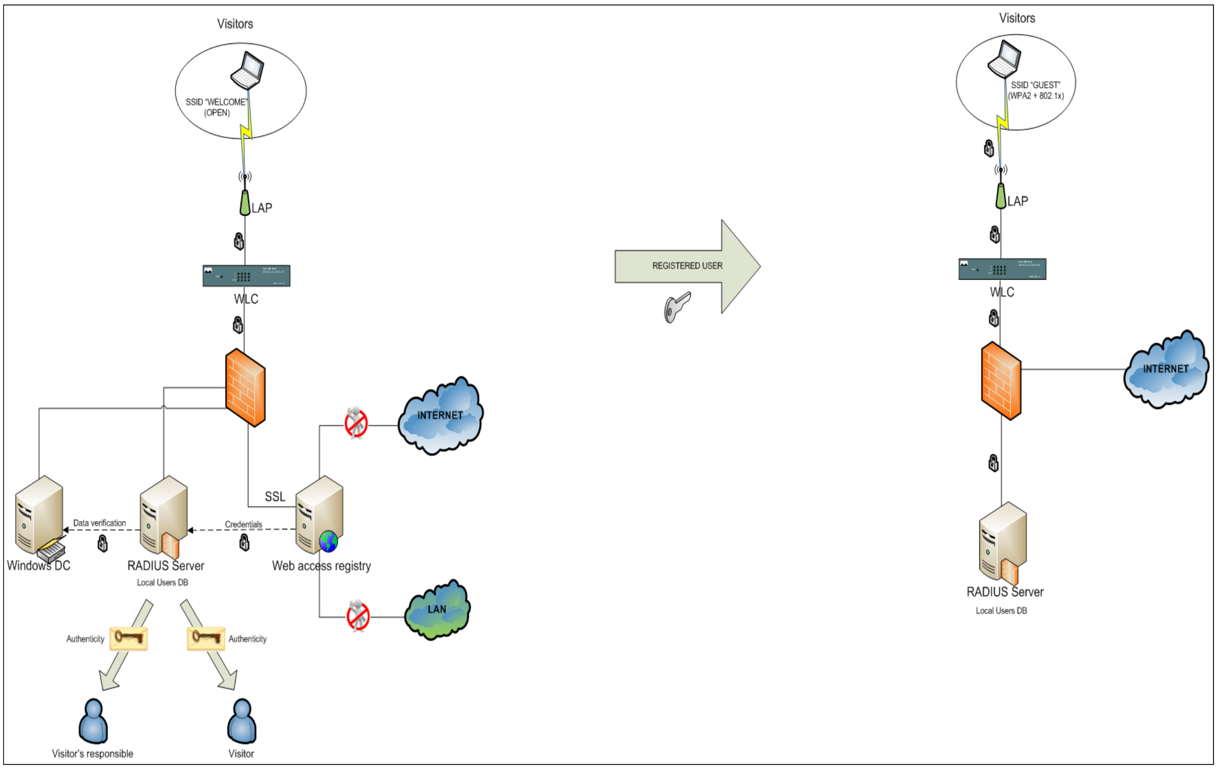


Illustration 20. Detail of the WiFi Network for visitors

This part of the solution relies on the use of 2 different SSIDs. The first one, called “WELCOME”, would have entry functions and no security at layer 2. Once associated, hosts would be allocated in an separated WLAN, totally undercontrol and without access to the LAN or to Internet. Then, opening a web browser would immediately redirect to a website to get a valid user and password. Some information would be required:

- Name and first name

- ID card number / Passport
- Company
- e-mail address
- Name and first name of the responsible person in CLC

With this information:

1. Web Server would generate a valid user and password pair.
2. Gathered data (and credentials) would be passed from the web server to the RADIUS server through a secure connection (i. e. SSH).
3. The RADIUS server would verify several parts of the gathered information (i. e. data of the responsible person in CLC against Active Directory). Then, there are two options:
   a) In case data is correct, RADIUS server would introduce gathered data (and user credentials) into its local database and it would notify the web server. Additionally, a notification e-mail would be sent to the responsible person and an e-mail with the new credentials and WiFi regulations would be sent to the visitor.
   b) In case data is not correct, RADIUS server would notify the web server and the new credentials would not been shown to the visitor. Web server would notify the user about the error.
4. Once data is confirmed and the web server notified, the visitor would see the new credentials displayed on the screen and he would be notified about connecting to the guest's SSID (“Guest”).

It is important to mention that registering website would use SSL (HTTPS), the server would be securized and monitorized and the code audited in orther to prevent from attacks (i. e. SQL injection). Also, each register attempt to create valid credentials would be registed in a local database in the webserver in order to maintain a list of requests.

Additionally, e-mails sent from the RADIUS server would use digital certificates to sign the e-mails. This measure would ensure sender authenticity and it would grant that nobody modifies the message. Ciphering to grant confidentiality has no sense because the e-mail sent to the visitor's responsible does not contain confidential information and the public key of the visitor is not available to cipher the message.

In case of failure during the creation of new credentials it is suggested to inform IT staff.

The third SSID ("Guest") would belong to a WiFi network configured to use WPA2 and 802.1x to securize communications end to end. Like in the corporate user's network, all actions done during the association phase would be registered.

Due to the fact that the secured "Guest" network would use temporal credentials, it would be necessary to define with the customer the duration.

Users connected to the "Guest" network would have only a controlled access to Internet.

4.2. WiFi Probe System (IDS/IPS)

This infrastructure consists on a set of WiFi devices compatible with DD-WRT Linux distro. They would be allocated in strategic places to act as a probe to detect and prevent from intrussions. Apart from an specific firmware, these devices would have a set of tools (i. e. aircrack-ng suite) and scripts developed to detect strange behaviours on the wireless network in several security related aspects. This is a sample of some of the issues that could be detected:

- Rogue APs used to obtain information from users.
- Non allowed devices running as APs installed for multiple purposes that could interfere with other wireless infrastructures.
- Client stations associated with a non allowed AP. It would involve a security breach.

This approach considers the deployment of 10 sensor devices around CLC's facilities (as shown in illustration 21). Nonetheless, once installed it could be necessary to move or to add a probe to improve the system performance.

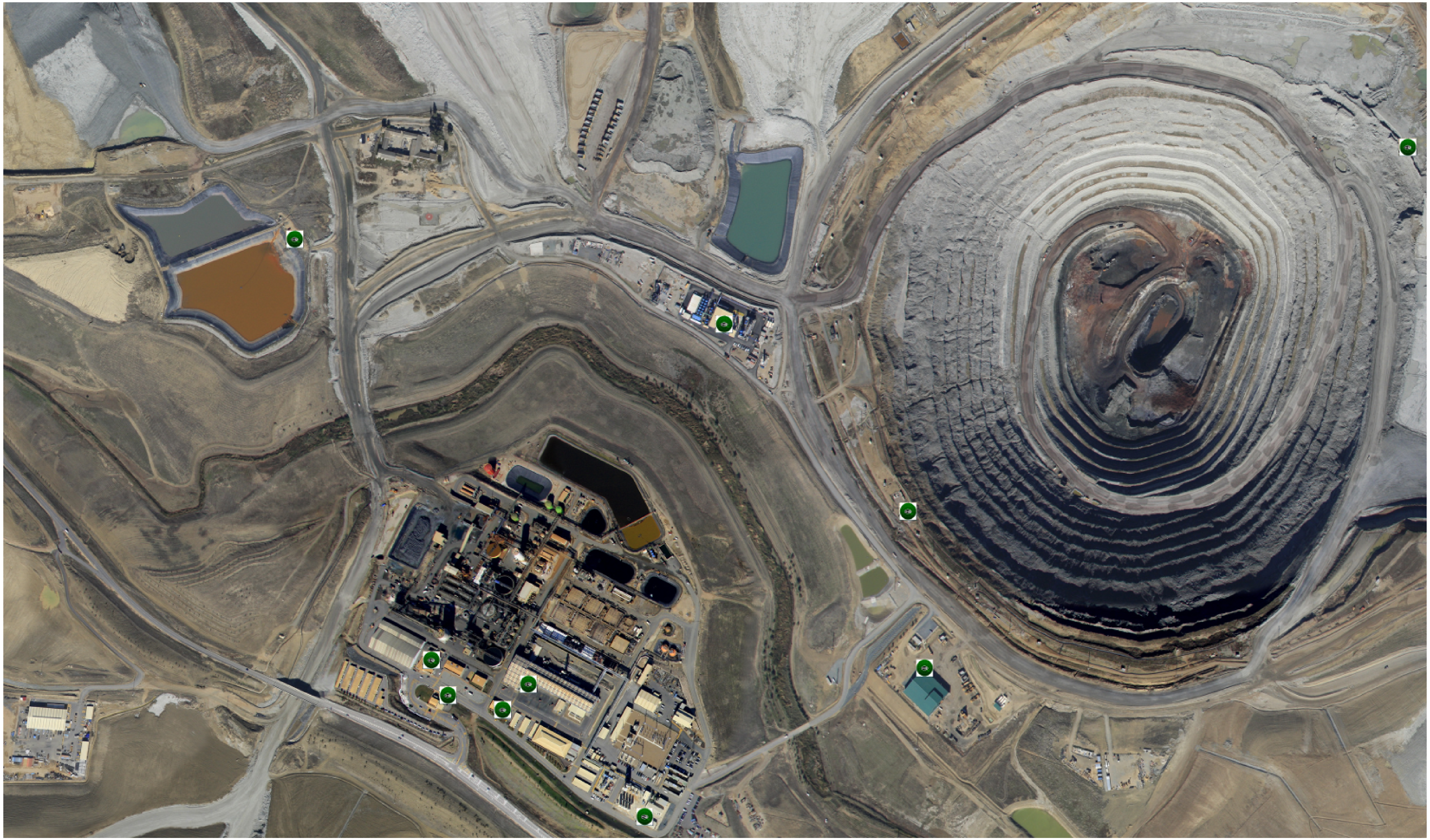


Illustration 21. Distribution of the 10 probe devices

With regard to the state and the alerts monitoring, it would integrate with the system already in use, called Icinga. However, it is suggested the installation of a dedicated server to storage data collected by these WiFi probes, so that an audit and/or analysis could be done whenever it is necessary. It would allow to detect anomalous behaviours. Illustration 22 shows the idea.

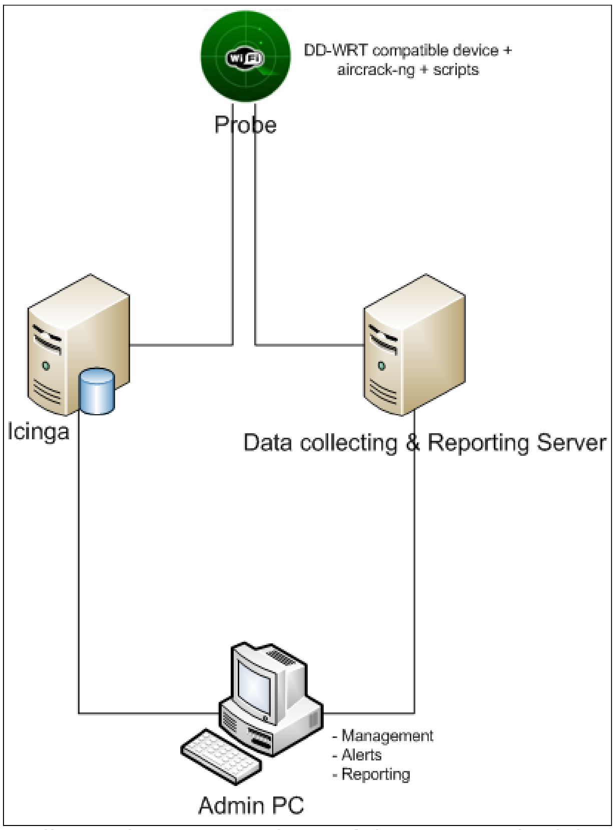


Illustration 22. Topology of the proposed WiFi Probe System

Integration between the WiFi Network and the Probe System

As previously stated, the devices that make up the infrastructure of Cisco ligthweight APs and WLC have security capabilities (i. e. Management Frame Protection). Therefore, the initial approach considers the probes as an extension of the WiFi network that would allow Cisco devices to widen detection and prevention capabilities to places where those devices have no WiFi range and, consequently, their security features have no effect.

The result of the deployment of the 15 devices is shown in the illustration 23.

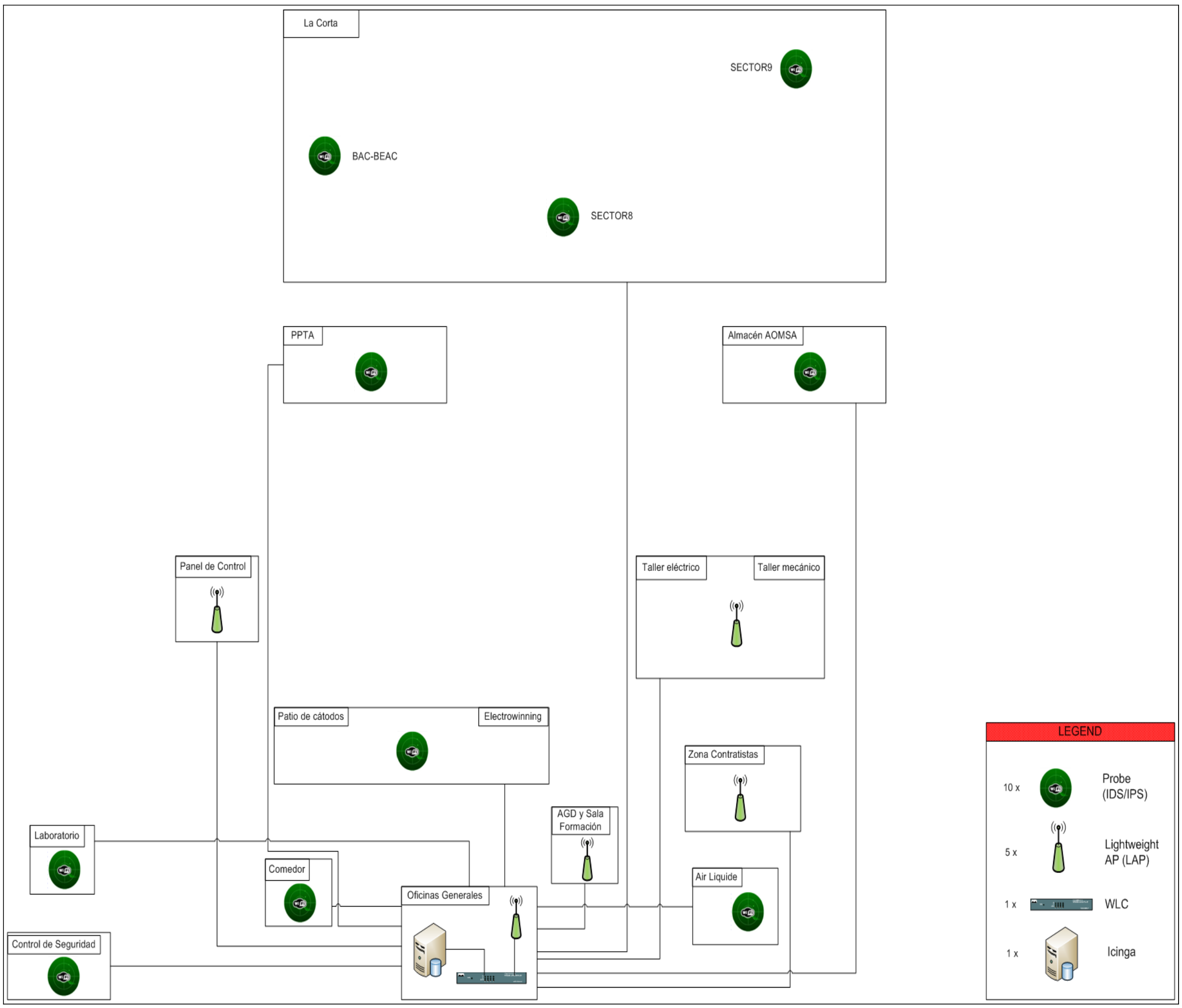


Illustration 23. Deployment and integration of the WiFi devices

With regard to the management and monitoring of both systems, they would be unified in an unique point, it is, the Icinga server. The Cisco WLC has its own monitoring possibilities, but it can join the current monitoring infrastructure by the use of SNMP. As a consequence, using Icinga as a central point, it would allow to create several maps with the precise position of those devices and their state. Therefore, it would be possible to obtain an overall picture and easily detect any failure or alarm and the location of the affected device. Look at illustration 24 for a sample of this integration.

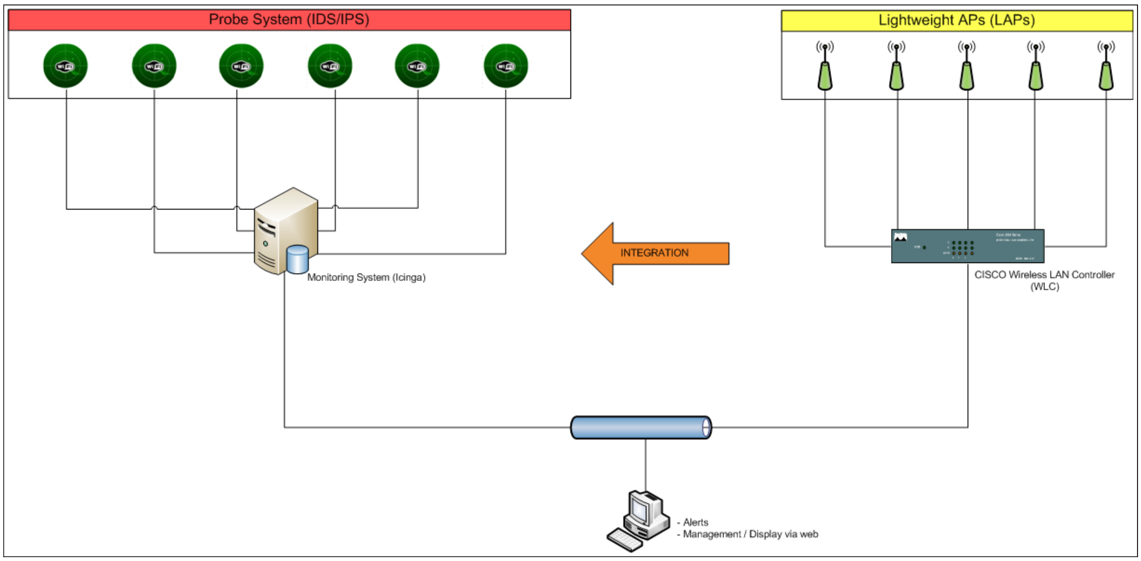

Probe System (IDS/IPS)
Lightweight APs (LAPs)
Monitoring System (Icinga)
INTEGRATION
CISCO Wireless LAN Controller (WLC)
- Alerts
- Management / Display via web

Illustration 24. Integration of both infrastructures into Icinga

4.3. Public Key Infrastructure (PKI)

According to the design of the solution, digital certificates are required in several parts, so a corporate certificate authority seems to be a must in CLC. Furthermore to the use of certificates for WiFi authentication purposes and thinking on future uses.

In this case, more information needs to be obtained in conjunction with the customer so that a proper infrastructure can be assessed and designed. This part (the PKI) is considered non futile and now we are not ready to offer a valid design of the infrastructure, therefore, just a few considerations are given about it.

In fact, the main issue is not just to install a CA integrated with Active Directory, because Microsoft Windows offers many guidelines to help on the creation of a CA in a “next... next” basis. The most important is to define the infrastructure itself and whether it will be really accepted by the users to save time and money. Some of the topics to think about would be:

- Technical requirements such as the authorities (the certificate, the registry, the validation and the timestamp) and the PKI products already available.
- Staff requirements such as the security responsible and the manager of the infrastructure.
- Procedural requirements such as the security procedures and the policies.

Additional subjects to have into account are CA's management model and type of acknowledgement required; so that the CA can be independent or based on a certificate from a root CA (i. e. Verisign), or managed by the IT crew or by another dedicated company (a hosted service).

4.4. IP CCTV System

As previously stated, there are currently two different infrastructures: one for the IP cams located in the access control to several parts of CLC and another for the IP cams in the mine area.

This part of the solution has not been analyzed in deep yet, but the main idea would be to deal with each system in a separated way because the current situation of each one is different from the other. However, both would reach equivalent security levels.

On illustration 25 it is displayed the location of the devices that make up each system.

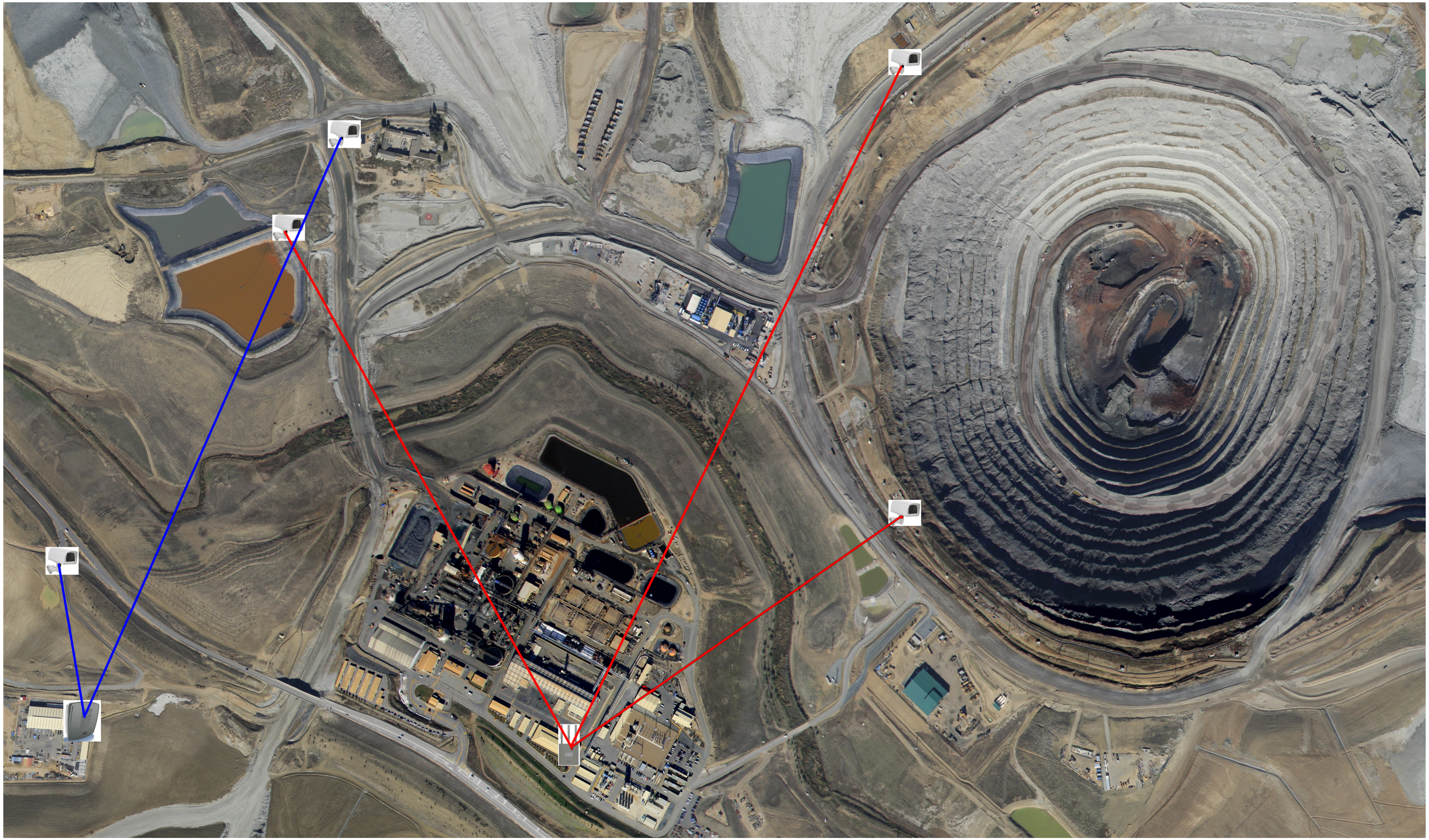


Illustration 25. Location of the devices that form each IP CCTV System

IP CCTV system for the access control

By now, this is one of the most up to date and secured WiFi infrastructures. It is formed by two autonomous AP (client mode) that connect IP cams to a third AP acting as the hub (or main) AP. They implement WPA2 and a local RADIUS server in the main AP to authenticate the other ends.

The solution would involve to integrate this solution with the LAPs – WLC topology proposed for the WiFi Network part, due to the fact that the three APs that form this system are Cisco models that support the lightweight operational mode. In fact, only the main AP would be updated to the new operational mode, while the other two AP would continue running as WiFi stations associated to the main one.

WPA2 would be used too and the RADIUS Server would be moved to a centralized one. Also, MFP would be enabled to take advantage of the security mechanisms of these devices.

This infrastructure would be used in a WLAN separated from those used for another infrastructures (i. e. WiFi Network). As a result, centralized security and management are granted.

IP CCTV system for the IP cams in la Corta

As shown in the Illustration, this system is formed by 3 IP cams connected each one to a WiFi device that is associated with a main AP at the headquarters. Unfortunately, this system has frequent techical problems and its solution requires an in depth analysis.

Based on the analysis done up to now, it is thought that the main AP is not the most convenient for this infrastructure because it cannot receive signal from the other ends with good power levels. One option would be to buy new Cisco APs, but a initial approach will be to reuse an available D-Link device with three independent radio interfaces. Each interface would have a directional antenna pointing to the other end.

As it was done with the other IP CCTV system, WPA2 and 802.1x would be implemented to secure communications. In this case, it would not be possible to integrate in the LAPs – WLC topology, but it would use the previous installed RADIUS server for a centralized management of the AAA protocol.

This system would be fully integrated with Icinga for monitoring tasks.

4.5. WiFi Point-to-Point Bridge

This infrastructure uses WPA2 and 802.1x to enforce communications security. In fact, it is quite similar to the implementation previously explained in the IP CCTV system for the access control, except that these devices are working in bridge mode while CCTV's APs work in AP and station/client mode. Therefore, a first approach would be quite similar to that. It would consider the upgrade of the APs to a lightweight operational mode in order to add them to the Wireless LAN Controller and to separate each bridge by the use of different WLANs. 802.1x would be implemented by using the centralized RADIUS server.

4.6. Telecontrol WiFi Network

Nowadays, this is an independent network so it will require to decide whether it must continue being an independent infrastructure. There are chances that it will continue working autonomously; therefore, the solution would be focused on increasing security levels.

There are 6 devices that form the WiFi part of this infrastructure but as shown in the WiFi assessment, they contain a very outdated and plenty of flaws firmware. Additionally, configuration contains several by default values that should be modified.

Consequently, the first action would be to upgrade the firmware. Then, to install a RADIUS server in that network and to configure each pair to use WPA2 and 802.1x (via that previously configured RADIUS server).

With regard to monitoring tasks, one option would be to install an additional server with Icinga only for people in charge of managing that infrastructure. Therefore, it would allow to monitorize wired and wireless network devices.

For IDS/IPS capabilities, it would be used the probe devices deployed in that area (as it was shown in the subsection “4.2. WiFi Probe System”). These devices belong to another network.

4.7. Configurations Backup System

This part of the solution is intended to offer a central repository where to safely pick up and storage the configurations of all the WiFi devices. However, the final goal is to extend this feature to all the wired and wireless network devices.

It would be enough with a virtual machine (with a Linux operating system) able to connect to each network device to download its configuration and to storage it in a folder structure pending of definition with the customer. A procedure would be decided to name each configuration file. The task would be executed in an scheduled way to connect (i. e. via ssh) to the device and to obtain its configuration.

This computer would be included into the corporate backup infrastructure. It is used Symantec Backup Exec, then a client program would be installed in this server to remotely backup the stored configuration files in an scheduled basis.

Eventually, this server would be added to Icinga for monitoring tasks.

4.8. Correlation and Log Management

Similar to the previous system of configurations backup, the idea is to have a centralized server (i. e. a virtualized one) to become the centralized point where all the devices would storage their logs and events. To accomplish it, all the network devices (wireless and even wired too) should be configured to output their events to an external host (traditionally it is used UDP port 514) and the syslogd (on the server) should be configured to accept remote logs. The protocol used would be the BSD syslog Protocol.

In this way, having all of them in a central point will allow to manage and audit them in a efficient way.

This machine would be added to Icinga for monitoring tasks.

Conclusions

The aim of this chapter is to be a section where to describe the conclusions of this TFC, but from a more personal perspective.

Initially, this project was a daunting adventure, full of new experiences, many tricky concepts and the use of English as the language to write it. Also, moving to a different city and working in a new company at the same time I studied some pending subjects sound very exhausting, but it was exciting even.

In fact, in Sevilla there were good personal reasons to live and the idea of this project for the TFC appealed to me. Additionally, I tend to think that this kind of opportunities only happen once at life. So I decided to accept this adventure.

Eventually, after some months of hard work and a positive thought, the course is almost finished and I have learned many technical and management related concepts. In fact, I must admit that security algorithms is a new subject (for me) to which I would like to invest more time to go into this topic in depth. Also, as far as I am concerned, this project is now even more ambitious than initially and, by and large, I think it can solve many of the problems detected in CLC and to improve several of its infrastructures.

Now, I certainly think that it has been a very gratifying experience. Moreover, several goals on this project have been already achieved and there are chances to continue after the schoolarship gets over to implement the full project. So, anything else?

Glossary

802.11i Security standard

It is an amendment to the original IEEE 802.11. The draft standard was ratified on 24 June 2004. This standard specifies security mechanisms for wireless networks. It replaced the short Authentication and privacy clause of the original standard with a detailed Security clause. In the process it deprecated the broken WEP. The amendment was later incorporated into the published IEEE 802.11-2007 standard.

IEEE 802.11i provides a Robust Security Network (RSN) with two new protocols, the 4-Way Handshake and the Group Key Handshake. These utilize the authentication services and port access control described in IEEE 802.1X to establish and change the appropriate cryptographic keys. The RSN is a security network that only allows the creation of robust security network associations (RSNAs), which are a type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-Way Handshake. It also provides two RSNA data confidentiality and integrity protocols, TKIP and CCMP, with implementation of CCMP being mandatory.

It supresses weaknesses of previous standards in user authentication and ciphering methods. It increases security in WLAN enviroments and it reduces complexity and roaming time of users from one access point to the other.

802.1x protocol

It is an standard mainly designed to offer authentication mechanisms to users on layer 2 (media access) in switched networks. Moreover, in wireless networks it uses dynamic keys for the association between a client station and the access point.

It brings confidentiality on media access (layer 2) because it creates a point to point connexion and prevents access on that port if authentication fails. It allows an strong authentication between a client and the access point.

AAA

In computer security, it stands for authentication, authorization and accounting:

Authentication refers to the process where an entity's identity is authenticated, typically by providing evidence that it holds a specific digital identity such as an identifier and the corresponding credentials. Examples of types of credentials are passwords, one-time tokens and digital certificates.

The authorization function determines whether a particular entity is authorized to perform a given activity, typically inherited from authentication when logging on to an application or service. Authorization may be determined based on a range of restrictions, for example time-of-day restrictions, or physical location restrictions, or restrictions against multiple access by the same entity or user. Typical authorizations in everyday computer life is for example granting read access to a specific file for authenticated user. Examples of types of service include, but are not limited to: IP address filtering, address assignment, route assignment, Quality of Service/differential services, bandwidth control/traffic management, compulsory tunneling to a specific endpoint and encryption.

Accounting refers to the tracking of network resource consumption by users for the purpose of capacity and trend analysis, cost allocation, billing. In addition, it may record events such as authentication and authorization failures, and include auditing functionality, which permits verifying the correctness of procedures carried out based on accounting data. Real-time accounting refers to accounting information that is delivered concurrently with the consumption of the resources. Batch accounting refers to accounting information that is saved until it is delivered at a later time. Typical information that is gathered in accounting is the identity of the user or other entity, the nature of the service delivered, when the service began, and when it ended, and if there is a status to report.

ARP poisoning

This technique consists of sending lots of ARP packets to a host in order to change a real MAC mapping with a different one, usually false, to take over the flow of traffic from/to that host (the host of the real MAC changed).

ARP spoofing

It consists of changing the MAC address of a computer to act as a different host.

Banner grabbing

Technique to get knowledge about running services from the banner once connection with the remote host is established.

Different WiFi areas for users and guests

It is a segmentation of a WLAN network using different SSID's. It allows to differentiate traffic from different hosts according to parameters like being a guest or a computer from within the CLC's network.

Once users have validated their credentials, they can gain full access to data and services in CLC's network; whereas the guests, allocated in an under control and monitorized WLAN, will access only Internet. This brings the advantage of safely isolate computers and users groups.

EAP

It is an authentication framework, not a specific authentication mechanism. It provides some common functions and negotiation of authentication methods called EAP methods. There are currently about 40 different methods defined. Methods defined in IETF RFCs include EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, EAP-AKA and EAP-AKA, and in addition a number of vendor specific methods and new proposals exist. Commonly used modern methods capable of operating in wireless networks include EAP-TLS, EAP-SIM, EAP-AKA, LEAP and EAP-TTLS.

Icinga

It is an enterprise grade Open Source monitoring system which keeps watch over networks and any conceivable network resource, notifies the user of errors and recoveries and generates performance data for reporting.

It is scalable and extensible and it can monitor complex, large environments across dispersed locations. Also, it is Open Source and it has an API based extensible architecture. It offers a dynamic web interface and supports a distributed system for redundant monitoring.

Intrusion and rogue AP detection systems

They are a set of hardware and/or software installed in strategic positions in the network to log events like failed/sucessful not permitted attempts of gainning access into the system, malicious traffic, a critical item within the network infrastructure suffering an attack, etc. Event logging allows to act in a preventive way and/or to respond actively to avoid other devices can be affected (i. e. with DoS attacs).

It is easily integrable with the current customer's network infrastructure and once it is parametrized it gives a large amount of information on real time about malicious actions, within a LAN and from Internet.

Maintenance of these devices is minimal and it considerably improves security levels and the control of the network infrastructure.

Man in The Middle

This technique has been used in conjunction with the arp spoofing technique to put an attacker computer between two target hosts, so that data traffic between those computers can be redirected through the attacker computer.

Management Frame Protection (MFP)

When management frame protection is enabled, AP adds message integrity check information element (MIC IE) to each management frame it transmits. Any attempt to copy, alter, or replay the frame invalidates the MIC. An AP, which is configured to validate MFP frames receives a frame with invalid MIC, reports it to the WLC.

Client MFP shields authenticated clients from spoofed frames, which prevents the effectiveness of many of the common attacks against wireless LANs. Most attacks, such as deauthentication attacks, revert to simply degraded performance when they contend with valid clients.

Packet sniffing

configuring NIC in promiscuous mode it can receive all packets on the WiFi frequency, regardless their destination.

Port Scanning

The act of systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.

Plublic Key Infrastructure (PKI)

It is a set of hardware and software, policies and security procedures to do criptographic operations safely (i. e. cipher, digital signature and non repudiation of electronical transactions). It also refers to the certification authority and to other components in electronical communications. Combined with 802.1x and 802.11i standards it allows to authenticate users and systems, to cipher data and to secure communications. In the same way, the use of digital certificates is an item that can be extended to messaging solutions (i. e. Microsoft Exchange) and fully integrated with Active Directory. It allows sender identification, digital signature and non repudation warranty (someone will be unable to deny at a later date that they have signed something).

RADIUS (Remote Authentication Dial-in User Server)

It is an AAA protocol (authentication, autorization and accounting) for network access or IP mobility services. On the other hand, it also refers to a server used to check whether that authentication/autorization information is correct. If credentials are valid, RADIUS server will authorize network access and it will deploy network resources (i. e. IP address). It logs events too. It validates credentials of computers attempting to connect to the wireless network. Also, it offers Active Directory integration capabilities. It logs and alerts of events like session log in/out, total transferred paquets, volume of trasferred data, reason of the session log out, etc.

SCADA

IT stands for supervisory control and data acquisition. It generally refers to industrial control systems: computer systems that monitor and control industrial, infrastructure, or facility-based processes, as described below:

- Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes.
- Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, Wind farms, civil defense siren systems, and large communication systems.
- Facility processes occur both in public facilities and private ones, including buildings, airports, ships, and space stations. They monitor and control HVAC, access, and energy consumption.

Service Set Identifier (SSID)

A service set identifier (SSID) is a name that identifies a particular 802.11 wireless LAN. A client device receives broadcast messages from all access points within range advertising their SSIDs. The client device can then either manually or automatically (based on configuration) select the network with which to associate. The SSID can be up to 32 characters long. As the SSID displays to users, it normally consists of human-readable characters. However, the standard does not require this. The SSID is defined as a sequence of 2–32 octets each of which may take any value.

It is legitimate for multiple access points to share the same SSID if they provide access to the same network as part of an extended service set.

Some wireless access points support broadcasting multiple SSIDs, allowing the creation of virtual access points, partitioning a single physical access point into several virtual access points, each of which can have a different set of security and network settings. This is not yet part of the 802.11 standard.

Social Engineering

This technique consists on obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information. Social engineering is successful because its victims innately want to trust other people and are naturally helpful. The victims of social engineering are tricked into releasing information that they do not realize will be used to attack a computer network.

Wireless LAN Controller (WLC)

This device is used in combination with Lightweight Access Point Protocol (LWAPP) to manage light weight access points in large quantities by the network administrator or NOC. The Wireless LAN controller is part of the Data Plane within the Cisco Wireless Model. The WLAN controller automatically handles the configuration of anywhere from 6 to 500 wireless access-points, depending on the model.

Wireless packet analysis hardware/software

It is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital wireless network or part of a wireless network. As data streams flow across the wireless network, the sniffer captures each packet and, if needed, decodes and analyzes its content according to the appropriate RFC or other specifications.

WPA2

It is a security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined this in response to serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy). WPA2 has replaced WPA. It implements the mandatory elements of 802.11i.

WPA2 provides support for all of the mechanisms available in WPA, as well as strong encryption and authentication support for infrastructure and ad-hoc networks. It reduces overhead in key derivation during the wireless LAN authentication exchange. Also, it supports opportunistic key caching to reduce the overhead in roaming between access points, as well as, pre-authentication, where a station completes the IEEE 802.1X authentication exchange before roaming. Overmore, it supports the CCMP encryption mechanism based on the Advanced Encryption Standard (AES) cipher as an alternative to the TKIP protocol.

Bibliography

This section lists the additional references (URLs, books, etc.) used within the TFC. Next, these are the most relevant:

Technical Specifications of the main WiFi devices

- http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6521/product_data_sheet0900aecd8031c844.html
- http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet09186a00802252e1.html
- http://www.dlink.es/cs/Satellite?c=Product_C&childpagename=DLinkEurope-ES%2FDLProductCarouselMultiple&cid=1197375189986&p=1197357768092&packedargs=locale%3D1195806681347&pagename=DLinkEurope-ES%2FDLWrapper
- Moxa AirWorks AWK-1100 User's Manual (First Edition) → http://www.bb-elec.com/bb-elec/literature/manuals/AWK-1100_UM_1eman.pdf
- Ubiquiti NS2 Datasheet → http://www.ubnt.com/downloads/ns2_datasheet.pdf

WEP Privacy

- http://www.configurarequipos.com/doc527.html

General information about modern WLANs

- http://www.perihel.at/wlan/wlanfacts.html
- http://es.wikipedia.org/wiki/DBm
- http://en.wikipedia.org/wiki/Service_set_%28802.11_network%29

WiFi Security assessment

- http://www.redeszone.net/seguridad-informatica/hackear-una-red-wifi-sin-clientes-conectados-aprende-a-hackear-una-red-wifi-sin-clientes-mediante-el-ataque-chop-chop/
- http://www.aircrack-ng.org/doku.php?id=es:packetforge-ng
- http://www.ifm.net.nz/cookbooks/passwordcracker.html

- http://www.tech-faq.com/decrypt-cisco-passwords.html
- http://books.google.es/books?id=4OszUcvlWrUC&pg=PA194&lpg=PA194&dq=open-wrt+rogue+ap&source=bl&ots=kVCk0TYq81&sig=O-2FFrTbKv4BGM5YpWDlVomj53M&hl=es&ei=FP_QTba7F4OzhAfdybDyDA&sa=X&oi=book_result&ct=result&resnum=5&ved=0CEgQ6AEwBA#v=onepage&q=rogue&f=false
- http://www.informit.com/articles/article.aspx?p=472323
- http://www.taringa.net/posts/info/8900842/Querias-localizar-senales-wifi_-Mira_.html
- http://bulma.net/body.phtml?nIdNoticia=2015
- http://geek00l.blogspot.com/2007/01/offline-pcap-analysis.html
- http://seguridadyredes.wordpress.com/2008/04/30/tshark-wireshark-en-linea-de-comandos-i-parte/
- http://www.aircrack-ng.org/

802.1x and EAP

- http://www.manual-wifi.com/802.1x.html
- http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
- http://www.blackhat.com/presentations/win-usa-03/bh-win-03-riley-wireless/bh-win-03-riley.pdf

802.11i

- http://www.networkworld.es/Seguridad-WLAN-802.11i-_Pros-y-contras/seccion-/articulo-169579

Wireless Distribution System (WDS)

- http://www.smallnetbuilder.com/wireless/wireless-howto/31191-everything-you-need-to-know-about-wireless-bridging-and-repeating-part-1-wds

Cisco Wireless Routers configuration

- https://help.ubuntu.com/community/CiscoConsole
- http://docstore.mik.ua/univercd/cc/td/doc/product/access/mar_3200/wlsnotes/cfpwrdat.htm
- http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00809d38a7.shtml

Cisco Wireless LAN Controller (WLC)

- http://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a008064a991.shtml
- http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps11630/data_sheet_c78-645111.html
- Cisco Wireless LAN Controller Configuration Guide, Release 7.0 (http://www.cisco.com/en/US/docs/wireless/controller/7.0/configuration/guide/c70cg.pdf)
- IRC channel #cisco at irc.ubuntu.com:8001

Security in a WLC and LAP topology

- http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008080dc8c.shtml

Cisco CleanAir Technology

- http://www.cisco.com/en/US/netsol/ns1070/index.html

Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode

- http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html#wp161111

Open Source LAN Controllers

- http://www.chillispot.info/features.html

LWAPP and CAPWAP

- http://datatracker.ietf.org/wg/capwap/charter/
- http://es.wikipedia.org/wiki/LWAPP
- https://learningnetwork.cisco.com/thread/6856

Public Key Infrastructure

- http://www.networkworld.es/Paso-a-paso_PKI-y-certificados-digitales/seccion-seguridad/articulo-134356
- http://web.ipsca.com/en/Products_PKI
- http://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica
- http://digi-sign.com/es/es/digi-ca/tipos%20autoridad%20certificadora

Remote Syslogs

- http://www.vicente-navarro.com/blog/2007/12/08/configurar-el-syslogd-para-que-acepte-mensajes-de-sistemas-remotos/
- http://www.debuntu.org/how-to-remote-syslog-logging-debian-and-ubuntu

Dictionaries

- Wordreference (online dictionnary) → www.wordreference.com
- Cambridge Advanced Learner's Dictionary (Third Edition, Cambridge University Press)
- Webopedia (online dictionary for words and sentences related to computer and Internet tecnology) → www.webopedia.com
- Wikipedia (online encyclopedia) → http://en.wikipedia.org