2017-06-07

Improvement Proposal for Wireless Office Networks

Thesis for the Degree of Bachelor of Science, Computer Network Engineering

Mälardalen University
School of Innovation, Design, and Technology

Student: Simon Blomqvist
Examiner: Elisabeth Uhlemann
Supervisor at MDH: Svetlana Girs
Supervisor at NetEnt: Wilhelm Vöörtmann

Abstract

Wireless networks nowadays are more affordable and faster than ever and thus many companies incorporate wireless solutions into their networks. However, a lot of challenges are introduced with wireless implementations and knowing how to make the best use of one's equipment can lead to increased quality of experience, higher security, and improved manageability. The Stockholm based company NetEnt has recently moved into a new office and enhancements on its new wireless network are to be implemented throughout the year. Wireless networks are complex to implement and even if the installation works properly there are still improvements that could be made. The presumption is that such improvements could lead to increased delivery quality for NetEnt. Thus, the main goal of this thesis work is to create a proposal of improvements based on best practices for NetEnt. During the thesis work, an investigation has been conducted to find general wireless network recommendations and vendor specific best practices. Recommendations were found in areas such as 802.11 frequency bands and standards, forwarding architecture, security, and management. The study showed that few recommendations alone would make a significant difference, but together they could make a noticeable boost to the network. The recommendations were compared to NetEnt's network and an analysis of the differences was performed. The study showed that some advocated proposals were already met while other were planned to be implemented in a near future. The conducted analysis includes the remainder of best practices and is to be seen as a proposal of improvements, which is expected to help NetEnt's IT department to increase the overall condition of the network.

Table of Contents

1. Introduction

NetEnt is a leading provider of premium gaming solutions to the world's most successful online casino operators. 2017 is a year where NetEnt move and relocate its local key office. NetEnt's new office in Stockholm has a new wireless network where improvements will be implemented throughout the year. As NetEnt is a large and fast growing company whose share is listed on Stockholm Nasdaq, aspects like scalability, availability, security, and fast connection speed of the network are fundamental for its business and future growth. The importance of a good access network is crucial for any network but especially so for a large one. In a rapid growing company, such as NetEnt, scalability in the access network is paramount. If the preparation for future network demands is unsuccessful then the network is prepared to be unsuccessful. Furthermore, another key of a good access network is availability, therefore, aspects such as coverage and redundancy have to be taken into account. One more vital part of a good network is security, especially so in a wireless network since you never know who is listening. Access to the network needs to be secure in order not to create a back door into the network. High security is imperative to protect the network from malicious attacks and to keep sensitive data from leaking. Lastly one other high-priority element of an exceptional computer network is connection speeds. It goes without saying that a fast network is better than a slow one since productivity is affected by it. The previously mentioned topics are the motivations for why an investigation is important for a large enterprise wireless network.

1.1. Problem Formulation

Even if a wireless network function properly and no major issues arise there are still improvements that could be made. These improvements can seem small but together they can mitigate problems, save CPU resources and improve the overall quality of the network. The open office space that is NetEnt's office advocates for collaboration between the employees. The many group sessions and work on shared resources could gain from improved roaming and coverage. The employees need to be able to access the shared resources quickly, which might be large files, in order not to lower the productivity. An increase in throughput could therefore lead to increased productivity. Leakage of confidential data could possibly be harmful for the business; only authorized users should therefore have access to the network and possible dangers should be detected and eliminated. New threats arise every day and high security is a continuous mission, countermeasures for the threats are created at an equal rate and a network could always be improved by adopting them. The overall objective of this thesis work is to investigate key features of an efficient and secure enterprise wireless network and the possible improvements that could be done on NetEnt's new wireless computer network. The following questions must be answered to produce an improvement proposal for NetEnt:

- What are the general best practices for wireless local area networks in open office spaces?
- What are the characteristics and specifics of NetEnt's wireless network?
- Are there any vendor specific best practices which are relevant to NetEnt's network?
- How can NetEnt's wireless network be improved by adopting recommended best practices for wireless local area networks?

2. Methodology

The thesis work will be split in three main stages. The first stage is a thorough literature study on wireless communication for local area networks and computer networks. The study will be conducted in order to find state-of-the-art and state-of-practice in relevant areas such as network access security, wireless local area network (WLAN) environments, and wireless communication in general. The second part of the thesis work will include an inspection on NetEnt's current wireless computer network. Key elements of a wireless access network such as access point placement and the protocols and functions in use will be investigated. There will be much iteration between these steps since further studies might be required if unexpected technologies are met in NetEnt's network. The third and final part of the thesis work will consist of a comparison between the best practices of wireless access networks, which were studied in the first stage, and NetEnt's wireless network, which was investigated in the second stage. Possible improvements for NetEnt's network will be documented in detail. The final result of the entire work will therefore be a clear picture of what is good and bad about NetEnt's wireless access network and a list of recommendations for the possible changes that could be made together with their corresponding strengths and weaknesses. The method is visualized in Figure 1. The purpose of the literature study is to obtain an understanding of wireless technologies, gather information about general best practices and vendor specific best practices. Books and IEEE articles will be used to gain knowledge about technologies and general best practices. The vendor specific best practices and recommendations, in this case Aruba best practices, will be acquired by reading Aruba devices' and technologies' data sheets and verified reference design guides. The second stage, which is the investigation of the characteristics of NetEnt's wireless network, will be conducted by reading documentation and by interviewing IT personnel.

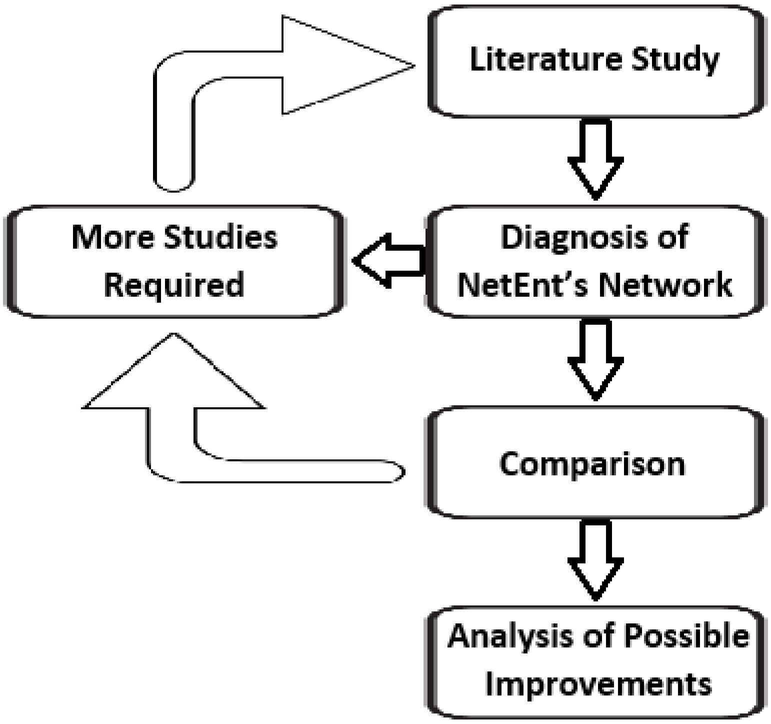

Literature Study
More Studies Required
Diagnosis of NetEnt's Network
Comparison
Analysis of Possible Improvements

Figure 1 Thesis Work Process Steps.

3. 802.11 Wireless Communication

Wireless communication uses radio frequencies to send traffic to its destination. Specific radio frequency spectrum ranges have been reserved for wireless networks and they have different characteristics. The Institute of Electrical and Electronics Engineers (IEEE) have released standards which utilize these frequencies to send data frames. The following sections will briefly cover those topics to give the reader a better understanding of the report.

3.1. Radio Frequencies

The most commonly used frequency range in wireless local area networks is the 100 MHz wide 2.4 GHz – 2.5 GHz band, also known as the scientific band. It is the primary band for wireless devices and is also used by for example microwave ovens, which has led to it being extremely overcrowded [1]. As defined in the IEEE 802.11-2012 standard, the band is divided into 14 channels, where the width of the channels depends on the technology used by the 802.11 transmitter. The channels' center frequencies only have a distance of 5 MHz and therefore the frequency spaces overlap. There are different combinations for non-overlapping channels, the most commonly used combination is using the channels 1, 6, and 11. Local rules in Sweden have limited the band to 83.5 MHz, 2.4 GHz – 2.4835 GHz, according to the Swedish Post and Telecom Authority. To increase wireless throughput, the 5 GHz bands can be used. In Sweden, there are 5 license free bands reserved for wireless networks ranging from 5.15 GHz – 5.35 GHz and 5.47 GHz – 5.725 GHz. This brings a total of twenty non-overlapping 20 MHz channels to use for communication in a wireless network (if 802.11ac is used, or nineteen channels otherwise). Although the network speed is improved with the use of a 5 GHz band, the range and penetration of physical objects declines [2]. Some of the 5 GHz band's frequencies are also reserved for other types of traffic such as military communication [3]. Those other types of traffic can interfere with a wireless network's traffic and a function known as *Dynamic Frequency Selection* (DFS) must be used. This function will switch channels when radio interference is detected [4].

3.2. 802.11 Standards

This thesis deals with local area networks and the most commonly used standard for WLANs is IEEE 802.11. IEEE's task groups have published many standards ever since the first one which was released in 1997. Previously one would see the 802.11a, 802.11b, or 802.11g standards but since these are considered legacy they will not be discussed any further. The two most common radio standards seen today are the IEEE 802.11n and the 802.11ac. The 802.11n standard included many enhancements, compared to the legacy standards, that increased data rates and thereby gave a higher throughput. An example of such an enhancement is the *multiple-input multiple output* (MIMO) technology which takes advantage of several antennas to increase throughput and gives a greater range. The standard also introduced the capability of 40 MHz channels which greatly increases data rates. 802.11n can be used on both the 2.4 GHz and 5 GHz frequency bands. The second most commonly seen radio standard, 802.11ac, provides Gigabit speeds with its major enhancements. It introduced improved MIMO, called *multiuser* MIMO (MU-MIMO), which was a massively anticipated technology that allows communicating with several clients simultaneously. It should be noted that the clients participating in the communication need to be MU-MIMO compatible and that MU-MIMO is possible by determining the physical location of the clients. The implication of this is that client density could potentially cause disturbances. Other improvements are better modulation, more spatial streams, and wider channels. The channels can be 80 MHz or 160 MHz, which will skyrocket the data rates, but the downgrade is that the small frequency space of the 2.4 GHz band is not sufficient and only the 5 GHz band can be utilized [2], [5].

Given the high popularity of IEEE 802.11 networks, a lot of equipment compatible with the standard have been developed by different vendors. Some of the main companies producing IEEE 802.11 hardware are Cisco Systems, Aruba Networks, Aerohive Networks, and Juniper Networks [2]. However, in this thesis the main focus will be on Aruba's proprietary functions and equipment since NetEnt has chosen its products for the company's network.

3.3. 802.11 Communication Recommendations

A great deal of time should be invested in the selection of channel width. Even though a wider channel provides the possibility for higher data rates, it would also mean fewer channels. This could cause interference for environments with a high density of access points. In 2.4 GHz networks the channel width should always be 20 MHz, as for a multiple access point environment there would simply not be enough channels otherwise. For 5 GHz networks the situation is a little more complex and more thought need to be put into the decision. A 160 MHz band would only have two channels, which works in an environment with a maximum of two access points. For offices with more than two access points, 80 MHz is preferred as this solution would provide five channels which works perfectly fine for enterprise offices. Recall, that the 5 GHz band shares some frequency ranges with other types of radio communication. If the DFS function constantly would have to change channels for the access points, then five channels would not be enough and a channel width of 40 MHz should be used. The amount of possible radio interference should be assessed before the final decision is made [6]. Another matter to consider is the fact that every device does not support all channels on the 5 GHz band. Clients could potentially experience loss of connection in certain areas of the office, therefore, it is important to identify which channels that are supported by the network's client devices [7].

Aruba has developed a set of tools, named *Adaptive Radio Management* (ARM), that dynamically select channels for the access points. ARM makes use of data that the access points obtain through their occasional scanning. Based on the gathered data, ARM choses channels for the access points to avoid interference and adjusts the transmit power to mitigate coverage holes [6]. When using ARM, there are certain considerations to be taken into account on the recommendation of Aruba. ARM has a parameter called ideal coverage index, which ensures that access points do not transmit on too high power. The default value for this parameter is 10 but the recommended value is 6. The free channel index parameter helps ARM to select a new channel, it is recommended to increase the parameter's value to 40 for the 2.4 GHz band. ARM has a back off timer which does not allow an access point to change channel until it is expired, to avoid frequent channel changes it should be increased to 1800 seconds. The parameters error-rate-threshold and error-rate-wait time should be increased to 70% and 90 seconds respectively. These parameters check how much error rate there is on a channel and the period of time before an access point will change channel after an error [7].

4. Wireless Local Area Networks

In today's local area networks, it is possible for users to connect to local resources, network services, and to the Internet wirelessly. Typically, in wireless enterprise deployments, several access points are connected to a wired backbone network, serving as a bridge between the wireless and the wired network. The data packets used by wireless networks are translated by the access points or by a controller, controllers will be explained later in this section, into Ethernet frames which are then forwarded onto the wired network. The communication between access points and clients is half-duplex, meaning that only one radio can send traffic at a time. Collisions and other problems might occur because of this and some of the following sections will discuss technologies and best practices that mitigate bad network behavior. Access points can be categorized into two different types, controller-based access points, also known as thin access points, and autonomous access points. Autonomous access points are considered legacy devices and today it is more likely to see thin access points in wireless networks. Thin access point deployments use a controller to control the wireless network in a centralized manner. The controller configures and manages the access points and traditionally forwards the data traffic. The access points and the controllers communicate using a tunnel protocol, typically *Control and Provisioning of Wireless Access Points* (CAPWAP) but some vendors use proprietary protocols. For data traffic, it is common to use the *Generic Routing Encapsulation* (GRE) protocol but CAPWAP can be used for that as well [2].

4.1. Access Point Recommendations

Access points should be placed on the ceiling approximately 15 meters apart from each other in a honeycomb patter as this will ensure optimal coverage, as depicted in Figure 2. If both the 2.4 GHz and 5 GHz band is to be used together it is recommended to disable the 2.4 GHz on some access points. The reason for this is that, as previously mentioned, the 2.4 GHz band has longer range as well as fewer channels. If 2.4 GHz radios are as closely deployed as 5 GHz radios should be, the network would be more susceptible to co-channel interference. To evaluate which radios should be disabled, site survey tools need to be utilized. One could for instance use Aruba's VisualRF function which visualizes the access points' coverage zones. To support the high speeds that 802.11ac provides it is recommended to have gigabit connectivity between access points and access switches. When it comes to the cabling itself, it is advocated to use Cat 6a cables if it can be afforded, otherwise use the Cat 5e cables [6]. Though it should be mentioned that some research has shown that Cat 6a does not increase performance proportionally to the price raise. At the same time the implementation of Cat 6a cables could still be financially justified if the network has time sensitive functions, such as voice and video, or as a mean to meet future network demands and possibilities [8].

The image is missing in the electronic edition for copyright reasons

Figure 2 Honeycomb Pattern Deployment [6].

As specified earlier, access points should not be deployed too far from each other, there is a correlation between a device's distance from an access point and signal quality. Therefore, less complex modulations must be used at greater distances [2], [7]. Since different data rates utilize different modulation types, radios use a process known as *dynamic rate switching* (DRS), which shifts the data rate up or down depending on the distance to the other radio. There are several reasons for why this is not desirable, besides the obvious of decreased throughput. A consequence of networks being half duplex is that if one client that was unfortunate enough to be downgraded by the DRS process to data rates of 1 or 2 Mbps, then all other clients connected to the same access point as the previously mentioned client would have to wait until that slow transmission has been finished. The large coverage zone that comes with the lowest data rates can also create hidden nodes in that specific zone. A hidden node is a client that one or several other clients cannot hear, which could result in that several clients transmit at the same time resulting in a collision, which in its turn can drive retransmission rates up to 20 percent if not more. It is a recommended best practice to turn off low data rates to mitigate the previously mentioned problems and to help with roaming problems. Although access points' coverage would decline, the overall throughput of the network would be kept high. Smaller coverage areas are also good if users will use personal mobile devices on the network, for example phones or tablets. These small devices generally have lower signal strength than a laptop and can experience dead spots throughout the network if the coverage areas are too large. It is now such a commonplace for employees to bring their personal devices to work that a term for it has been coined, *bring your own device* (BYOD) [2]. Several additional difficulties come with this new trend, the best ways to manage them will be covered in another section.

In a wireless network, there are two ways for a client to discover an access point, passive scanning or active scanning. In passive scanning, the client passively listens for beacon frames that are regularly sent by the access points. If the client is configured to connect to a received beacon's network, then it will try to determine which access point has the best signal and then start an association process with that one [2]. When using passive scanning, it is recommended to adjust the beacon rate. Like for normal traffic, the transmit range for beacon frames are determined by their data rate. To mitigate roaming issues, it could be beneficial set the beacon rate to a higher value than the default. It is important that the beacon rate is not set too high, as it might happen that some clients cannot receive traffic at such high rates. Administrators should have a good understanding of what kind of client devices that are to connect to the network to adjust the beacon rate correctly [7]. In active scanning, the access points do not send out beacons continuously [2], instead the clients actively send out probe requests for a specific *service set identifier* (SSID), which is an identifier for a specific wireless network [9]. Access points in the vicinity that support the specific SSID will answer with a response frame that mostly contains the exact information as a beacon frame. Since the client that conducts active scanning actively searches for access points with the best signal, it can typically perform roaming faster and more efficiently [2]. Like for passive scanning, it is recommended to adjust how far from the access points clients can be located to be associated. This is done by instructing access points not to answer a probe request unless the *signal-to-noise ratio* (SNR) is higher than a specified threshold. The threshold value should only be adjusted after careful analysis by an engineer, however a guideline is that it should be less than 3 decibels lower than Aruba's ClientMatch's sticky SNR parameter [7]. This parameter and other ClientMatch recommendations will be covered in greater detail in the following paragraph.

The ClientMatch function, which is a part of ARM, ensures that access points are load balanced, changes clients' associations to the most optimal access points and can also enforce which frequency band clients should use [6]. Aruba recommends that clients should change access point association when the SNR reaches 18 decibels, this is the sticky SNR parameter that was previously mentioned. It is also recommended to increase the load balancing threshold to 30 clients and the band steering of 2.4 GHz band clients to -10 decibel-milliwatt. During failed steering events the client is blocked by all radios except the designated one, it is advocated to reduce the restriction timeout to 3 seconds [7]. Clients should also be steered to use the 5 GHz band using the *prefer 5 GHz* mode [10] however equal access should still be provided, meaning that no client is prioritized based on which band or 802.11 standard they use [6].

4.2. General Wireless Local Area Network Recommendations

A controller should have the capacity to send and receive large amount of traffic since in a lot of cases all wireless data traffic flows through the controllers. Therefore, redundant 10 GBps links from access switches and controllers to distribution or core switches should be implemented [6]. Increasing the speed between devices in the network can be done in several ways. A port could be upgraded to a faster one with gigabit speed. This solution has limited scalability since there is a limit on how much speed a port can provide and it is also the most expensive method. Another more scalable approach is to bundle several links together to work as one with the use of Etherchannel [11]. Lastly, one could improve load balancing in the network by moving the layer 2/3 border [12] to the access switches. If a dynamic routing protocol was implemented on the access switches, it would not only allow dynamic load balancing but also decrease the time of convergence for the network by up to five times. The convergence time would be decreased since some routing protocols, such as *Open Shortest Path First* or *Enhanced Interior Gateway Routing Protocol*, perform faster calculations than *Spanning-Tree Protocol* [13].

Aruba recommends a flat single VLAN solution for wireless users to simplify the network. Since a large VLAN creates a large broadcast domain, it is also recommended to drop all broadcast and multicast traffic. Some broadcast traffic is essential though, such as DHCP and ARP. The function AirGroup can allow specific multicast or broadcast traffic that is needed in an organization. Since multicast is sent at lower data rates in wireless networks, as stated in the 802.11 standard, *Dynamic Multicast Optimazation* (DMO) can be used to convert multicast traffic into unicast traffic. DMO uses a threshold to determine if traffic should be converted or sent as is. If the number of multicast receivers exceeds the threshold, then traffic would not be converted and throughput would be downgraded for the wireless network. The default threshold value is 6 but it is advocated to set it to the number of clients that are expected to be associated to each access point. It should be mentioned that DMO requires *Internet Group Management Protocol* (IGMP) snooping to function. Even if DMO is enabled the data rate of potential multicast traffic should be optimized to the highest possible common rate [6], [7].

5. Wireless Local Area Network architecture

A scalable solution provides many benefits for a network. Not only is it more economic but also more efficient and less of an administrative burden. This section will describe and evaluate scalability of the two most commonly seen architectures.

5.1. Centralized Architecture

The most commonly seen wireless architectures in modern networks are the traditional centralized architecture and the trendier distributed architecture. In the centralized method, all planes of operation, i.e. data, management and control, reside in controllers and the access points only handle some time-sensitive operations. Controllers are typically located in the core layer of the network but different vendors suggest different solutions. As seen in Figure 3, a client sends wireless frames to the access point which forwards the data traffic inside a tunnel to the controller. The controller will then translate the frame into an Ethernet frame, also called 802.3 frame, which will be directed to the wired network [2].

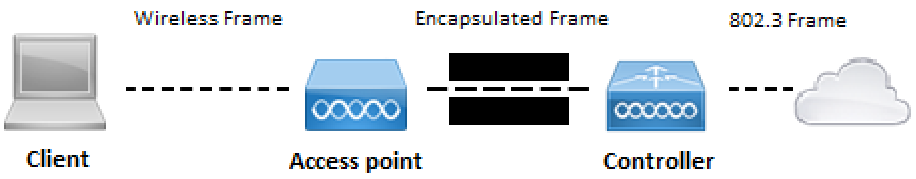


Figure 3 Centralized architecture.

5.2. Distributed Architecture

With newer wireless technologies with higher throughput, such as 802.11ac, controllers might not have the capability to forward all user data in an efficient manner. In the distributed architecture, all the data forwarding and 802.11 to 802.3 frame translations reside on the access points, as shown in Figure 4 [2].

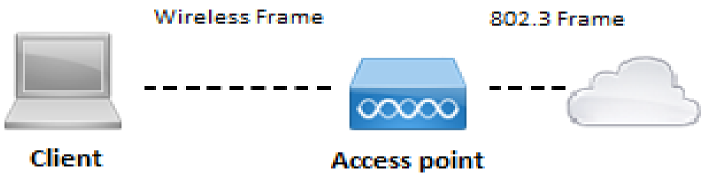


Figure 4 Distributed architecture.

The management plane is still centralized with the use of a controller and control plane mechanisms are cooperatively used by the access points with help of proprietary protocols. Access points must cooperate for functions like roaming to work. The distributed architecture can be viewed as a more scalable one since it is cheaper only having to buy access points instead of both access points and wireless controllers if the network were to grow. Also, in a centralized architecture, if a data forwarding device, in this case a wireless controller, were to fail it could be considered a major network failure even if several redundant devices existed in the network. On the contrary, a similar failure in a distributed network would probably not have a huge impact on data forwarding [2]. This architecture has been embraced by a lot of vendors and some, such as Aerohive Networks which is a competitor of Aruba [14], have designed all of their wireless network solutions based on the distributed forwarding architecture.

5.3. Forwarding Mode Recommendations

Even though there are a few advantages with the distributed architecture, some vendors' proprietary functions only work in a centralized method. For instance, Aruba, which recommends the use of their Tunnel mode for campus networks. In this mode, all data and control traffic is sent to the controller in an encrypted GRE tunnel. The data traffic goes through the firewall and is monitored and filtered according with the firewall policies. Aruba's distributed forwarding mode is only recommended for branch offices with a small number of users and without a controller of their own [6]. Many features are not supported in Aruba's distributed architecture, such as layer 3 mobility, rate limiting for multicast and broadcast and captive portal [15]. The controllers should be implemented in the active-active redundancy model, which is when both devices forward traffic simultaneously [16].

For the centralized architecture, together with 802.11ac, there are certain considerations to be aware of. 802.11ac aggregates frames into, so called, jumbo frames, which can be 4500 bytes large or even larger. "Normal" Ethernet frames are not larger than 1500 bytes and frames with more bytes are fragmented. To achieve the highest performance of the network when using a centralized method, such as Aruba's Tunnel mode, it is important that the intermediate devices support jumbo frames [6].

6. Wireless Network Security

Proper security is a requirement for wireless networks as data is transmitted freely in the air and the wireless section can be a portal to the entire network. A good defense should include proper authentication that only lets authorized users gain access to the network. Even though authentication keeps out a lot of unauthorized traffic in a wireless network, it is crucial to have a second line of defense against threats. Unauthorized clients could gain access to the network via a rouge access point. A rouge access point could be an authorized employee's phone or laptop that has set up an ad-hoc network, an unauthorized user could then potentially connect to the network through the employee's device. This is very common and large companies often find several rouge access points in their networks. If a rouge access point is under control of an attacker, legitimate users connecting to that access point could become victims of a man-in-the-middle attack. This could have serious consequences since an attacker could obtain passwords and other confidential information. Another form of attack that could be inflicted on a wireless network is a *denial of service* (DOS) attack, these attacks are meant to disable network services [17]. There should also be security measures implemented to handle employees and guests bringing their own devices [2].

6.1. Wireless Authentication Recommendations

In 2004 IEEE released the framework 802.1x for wireless network access. The standard authorizes users to either be allowed to send traffic through a port or be denied. To authenticate users, the *extensible authentication protocol* (EAP) is let through the port, the client and an authentication server can then exchange authentication credentials. There are several different EAP methods, some of which are more secure than others. One commonly used method is the *protected* EAP (PEAP) which supports various methods within a secure *transport layer security* (TLS) tunnel [2]. A TLS tunnel shields traffic from eavesdropping and tampering, if implemented correctly [18]. With PEAP the authentication server is authenticated with a digital certificate, clients on the other hand can be authenticated in many ways, for example with username and password. Another EAP method, EAP-TLS, authenticates both the user and the server with digital certificates within a secure TLS tunnel. It is considered one of the strongest authentication methods but can be quite complex. EAP-TTLS extends the concepts of EAP-TLS and functions similarly to PEAP. It utilizes a TLS tunnel to encapsulate another version of EAP authentication, but unlike PEAP it supports far more authentication methods and unlike EAP-TLS it is more flexible. There are EAP methods that are not protected by a TLS tunnel, but they are highly unsecure and can let anyone eavesdrop on authentication credentials and therefore jeopardize the network. If the complexity of the implementation does not scare one off then EAP-TLS is a good choice and will provide very secure authentication [2], [17], [19].

6.2. Wireless Intrusion Prevention System Recommendations

To protect a wireless network from attacks such as rouge access points and DOS, a *wireless intrusion prevention system* (WIPS) can be used. Rouge access points can be detected by a WIPS which can countermeasure them with a DOS attack to render the communication between a rouge access point and users useless. Malicious DOS attacks are harder to prevent, usually only detection of them is possible. However, a WIPS detection mechanism could help in locating the source of a DOS attack and manually eliminating it. It is also a good idea to have a WIPS solution for the wired network since rouge access points can be found there as well [17]. A WIPS does not only protect the network against rouge access points and DOS attacks, but also analyses traffic to find malicious data. The system utilizes signatures that are a collection of rules that can help detect severe security threats. If a threat is identified, the system will take automated actions to mitigate the problem and possibly notify administrators. WIPS is built upon an older system known as *Intrusion Detection System* (IDS), which is a system that passively conducts deep analysis on copies of traffic to find harmful activities. Even though an IDS system cannot prevent dangerous traffic on its own, it can e.g. send a message to a switch telling it to deny certain traffic. WIPS is considered to be more scalable and a safer option than IDS but it is recommended not to exclude one for the other, the two systems should cooperate and complement each other [20].

Aruba controllers have an implemented WIPS solution, which together with Aruba Airwave and RFProtect, which will be covered later, creates a vigilant defense for a wireless network. The WIPS solution provides three different access point modes, *Access Point* (AP) mode, *Air Monitor* (AM) mode and *Spectrum Monitor* (SM) mode. The AP mode is the only mode that serves clients and is the standard mode. The AP mode can detect rouge access points on its channel and it will perform off channel scanning every 10 seconds to detect rouge access points on other channels. The standard mode can contain rouge access points but it should be mentioned that it is a best effort attempt, meaning it will only contain rouge access points if they are on the same channel as the access point in question. If the access point has no clients connected to it, it is possible to configure the access point to change the channel to contain a detected rouge access point. The AP mode will also perform spectrum analysis on its channel to detect non-WI-FI interference, such as microwaves. Access points configured using the AM mode are dedicated to wireless security and will not serve clients. They are very effective at containing rouge access points and will search for them on all regulatory channels and even on some rare channels. The SM mode is designed for spectrum analysis and will search each regulatory channel every second to find wireless interference. SM access points can be a good tool when troubleshooting the network and could help a troubleshooter find causes of disturbance. Most enterprises only need the standard AP mode but if there is a wish to uphold high security and availability then AM and SM access points could be a good implementation. The Aruba WIPS solution can also detect wired rouge access points by cooperating with access points. In order to contain wired rouges all client facing VLANs have to be trunked to all access points which will perform ARP poisoning on the rouge device. Aruba AirWave can also be used to detect wired rouge access points; this will be discussed in a following section. Included in the Aruba WIPS solution there is an IDS system which can detect malicious data traffic. When configuring this, Aruba recommends to start with a small list of threats to detect. Too large of a list could overwhelm administrators with too many alerts and fails. Not only can the IDS system detect attacks against the network infrastructure but also attacks against client devices, which are generally more vulnerable [21]. Most of these functions, such as advanced rouge access point containment and IDS, require the RFProtect license to function. As seen in Figure 5 there is an abundance of extra features that are granted with the RFProtect module [22].

The image is missing in the electronic edition for copyright reasons

Figure 5 ArubaOS Base versus RFProtect [22].

6.3. Controller Firewall Recommendations

Aruba *Policy Enforcement Firewall* (PEF) is a function that enforces access policies, *Quality of Service* (QoS) and provides stateful firewall instances for every user. PEF uses identity-based policy controls to identify a connecting device and user. When the identity of the user and the specification of the device is learned, they can be placed in a specific class which will determine the policy which will be applied to the user. The policies can deny or restrict certain applications or websites that are deemed to be unnecessary personal traffic, which is important in order to prioritize essential corporate data. Other QoS tasks are also provided by the PEF to let the IT department implement advanced prioritizing. PEF also restricts some broadcast and multicast protocols that eat up a lot of bandwidth. In addition, PEF protects users by denying malicious files and URLs from being accessed [23], [24]. PEF is also essential for some of Aruba's BYOD features [25], this will be discussed in the following section.

6.4. Bring Your Own Device Recommendations

When employees bring their personal devices to work, it is not only a coverage concern, that was mentioned in a previous section, but also a network security issue and thus a *mobile device management* (MDM) solution might be needed. A MDM solution can manage both *company-issued devices* (CID) and personal devices. For CIDs, a MDM solution could, for example, keep a hardware and software inventory control. It could also give administrators the ability to remotely wipe devices' data if they were stolen or lost. When a personal device that is enrolled in the MDM solution accesses the network, it could be given certain restrictions, for example it might lose the ability to take pictures within the company's building. Another good reason to use a MDM solution is the possibility to provision digital certificates. A digital certificate is a form of digital ID that can be used for authentication. It works great with the network access authentication framework 802.1x. It is easy to install certificates for windows laptops just using active directory *group policy objects* (GPO), but for apple laptops and mobile phones it is not equally simple since GPOs cannot be used by them. MDM solutions offer the function over-the-air provisioning which can easily provision a digital certificate, making an otherwise hard task very simple. Employees are not the only ones who bring their own devices, a lot of companies have guests, such as customers or consultants. These guests sometimes require Internet connectivity to do their work. It is highly recommended that guests are much more restricted than employees. Guests should have their own SSID and virtual local area network to separate them from all other traffic on both the wireless and wired mediums. Another important component is the guest firewall policy, which should only permit connectivity for guests to fundamental network services, e.g. DHCP and DNS, and the Internet. Guests should not be able to communicate directly to each other, isolating the guest clients prevents peer-to-peer attacks which could possibly give an attacker a higher level of access to the network. Another common practice is to limit the data rate of guest clients to ensure that most of the bandwidth is reserved for the employees. The rate limit of guest user traffic is typically limited to 1024 Kbps. When guests and employees bring their personal devices, it must be guaranteed that the device has not been compromised, in form of a virus, worm or malware, before it is allowed to connect to the secure network. *Network access control* (NAC) evaluates the health of a device to determine if there are any potential risks with allowing it to access the network. NAC performs a so-called posture assessment and checks that the device's security software is operational and up-to-date and that the state of the operating system is acceptable. If the device is deemed as a risk it is not allowed access until certain requirements are fulfilled. On CIDs, an agent can be installed to automatically update the device to make sure that the requirements are satisfied [2].

Aruba offers a great solution for BYOD with the ClearPass system. ClearPass offers everything that was previously mentioned, such as guest access, certificate provisioning, user device hardware and software inventory control, user device health checks, and role- and device-based access control [26]. Captive portal is a feature that is designed for integration with the ClearPass guest access function. It is a layer 3 authentication method which redirect guests to a captive portal page when they attempt to access a web page. The captive portal page has various functions, such as authentication, providing use policies and self-registration. It is more common to use proper authentication with a username and password than self-registration, though that requires a guest provisioning system. Guest provisioning allows non-IT professionals, commonly receptionists, to create temporary guest user accounts. PEF is required for guest specific user roles and captive portal requires that a centralized architecture is used [25].

7. Management

To know which equipment and features that should be implemented into a network is one of the most important tasks of a good network, but it is equally important to manage and monitor the implemented elements. The following sections will briefly cover some common management tools.

7.1. AirWave

The Aruba AirWave is a management tool for wired and wireless infrastructure. It monitors the network and can alert the IT administration about different end-user failures, such as time, response, DHCP and name resolution failures. AirWave can provide mapping of the radio frequency environment, which give administrators an accurate picture of who is in the network, where they are and how their network connection is performing. The mapping feature can for example be a great tool for locating rouge access points or other threats. AirWave collaborates with the Aruba WIPS to detect and mitigate rouge devices and wireless intrusions [27]. With the use of SNMP, AirWave polls switches and routers for bridge forwarding tables and *Address Resolution Protocol* (ARP) tables to detect rouges. The program can even determine several operating systems of rouge devices which could aid in finding the malicious device [22]. It is recommended to poll these devices every 12 hours [28].

7.2. Management Recommendations

Simple Network Management Protocol (SNMP) is one of the handiest tools for monitoring and management. It is supported by nearly every vendor and is used to poll networks' devices for environment and performance data. SNMP agents, which reside on the network's devices, can also send event triggered data to a centralized database. SNMP can be used to push configurations but it is rarely needed, therefore, it is recommended to only allow read-only access. SNMP access should also be limited to the SNMP database to improve security. Lastly, SNMP version 3 should always be used, since it is the only version that supports authentication, encryption and integrity. SNMP version 2's communities should not be confused as proper authentication, it is sent as plain-text meaning anyone could intercept and read it [11], [29].

8. NetEnt's Wireless Network

NetEnt has approximately 500 employees and an office occupying three floors. The demand of mobility is accommodated with 78 access points that are deployed in an adapted honeycomb pattern, Figure 6, and two controllers. As their access point of choice, NetEnt have implemented Aruba's AP-315. It is a dual-band access point utilizing both the latest 802.11ac on the 5 GHZ band and 802.11n on both the 5 GHz and 2.4 GHz bands. With 802.11n the access points can provide two spatial streams to increase reliability and range. 802.11ac can provide four spatial streams and MU-MIMO for MU-MIMO compatible clients. With the use of MU-MIMO, the access point can communicate simultaneously with up to three clients, with two spatial streams for one client and one spatial stream each for the other two clients; some other combinations are also available. The access point can support 255 associated clients per radio, i.e. 255 802.11n clients and 255 802.11ac clients [30]. The wireless local area network controllers in use are the Aruba 7205 Mobility Controller. One controller can support up to 256 access points, 8192 concurrent devices and provides 12 Gbps of throughput [31]. As their access switch, NetEnt's has implemented the Aruba 2920 switches. These are layer 3 switches which support static routing and the routing protocol RIP [32]. For monitoring, the administrators utilize OP5 and AirWave, and SNMP version 2 is used together with Syslog to gather information from network devices.

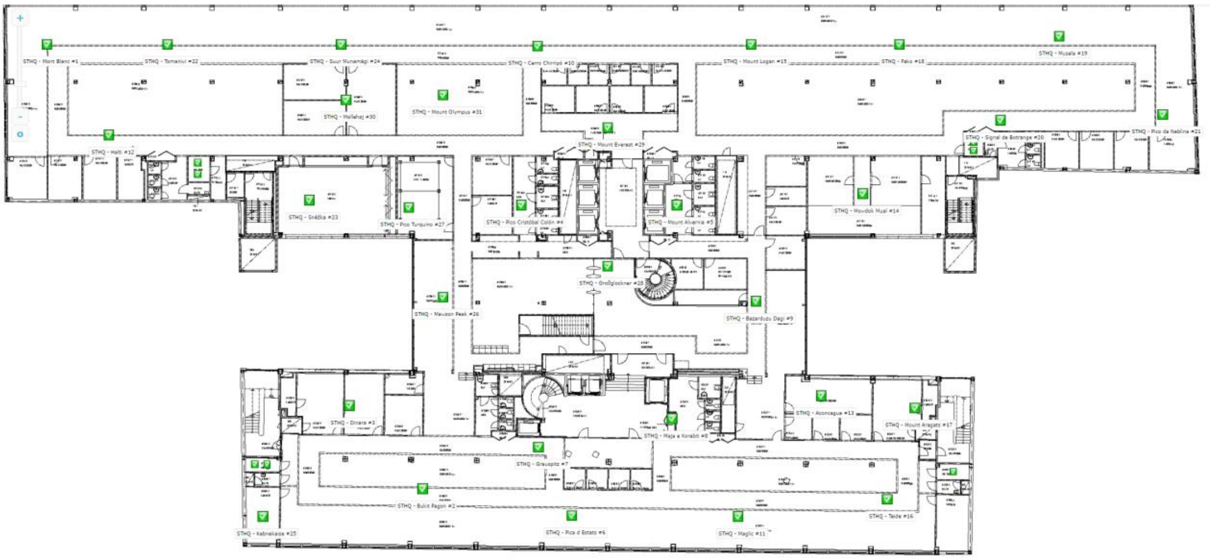
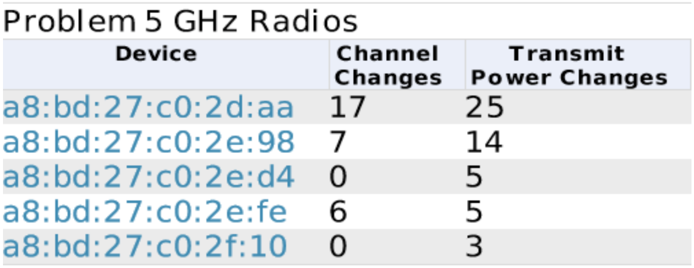


Figure 6 NetEnt's Office Floor 7

The tables in the office are deployed in a manner to evenly distribute wireless traffic over the access points and employees are encouraged to connect to the wired network whenever possible. During peak hours, the wireless network has 500 to 600 associated client devices. Most of the users, about 500, use the 802.11ac and the other users use 802.11n and are divided between the two bands. The bands themselves are left at their default setting, the 2.4 GHz being 20 MHz wide and the 5 GHz being 40 MHz. At this moment, ClientMatch is not enabled, which leaves the administrators with no control over which band or 802.11 standard the clients use to communicate and the choice is completely left to the client devices. Although ARM seems to be enabled, since, as seen in Figure 7, access points can dynamically change channels and adjust their transmit power, the ARM parameters are mostly left at their default. Since most settings have been left at default it is assumed that no data rates have been disabled. Employee users associate with access points with passive scanning, the access points send out beacons with the data rate of 12 Mbps.



Problem 5 GHz Radios

Device	Channel Changes	Transmit Power Changes
a8:bd:27:c0:2d:aa	17	25
a8:bd:27:c0:2e:98	7	14
a8:bd:27:c0:2e:d4	0	5
a8:bd:27:c0:2e:fe	6	5
a8:bd:27:c0:2f:10	0	3

Figure 7 Health Report of NetEnt's Access Points

Motivated by the sake of simplicity, NetEnt have a distributed architecture, utilizing Aruba’s bridge mode. Thereby, the controllers only have a management role in the network. The controllers are implemented in an active-standby setup, if the active one were to fail the standby controller would take over. To ensure that the network has the best possible chance of handling its traffic, Cat 6a cabling has been implemented. The active controller is connected to a core switch with a 1 GBps port while standby controller is located in the data center. The access switches use Etherchannel bundles to connect to the core switch.

Employee users are currently authenticated with 802.1x with PEAP-MS-CHAP version 2 as their EAP method, it is planned to implement EAP-TLS in the future. Currently, there is no MDM solution in place, but NetEnt’s IT team has the intention to implement the ClearPass system. An additional security feature to the authentication is a back off timer of 3 minutes if a user fails to write the correct password 3 times in a row. There is a separate SSID that guests can gain access to with a PSK, they are limited to only browsing the Internet. When it comes to rouge access points, the administrators can detect them but there are no counter measures in place. Since the PEFNG license is a requirement for the Aruba bridge mode, it is evidently that it is installed.

9. Analysis of NetEnt's Wireless Network and improvement recommendations

NetEnt's network has modern equipment that supports advanced technologies and is overall a good wireless network with high availability. However, there are still improvements that could be made to increase security and make the network more robust. The following sections will provide an analysis of NetEnt's network and describe proposed improvements.

9.1. 802.11 Frequency Bands

The two bands' channel widths are left at their default setting which raises an interesting discussion about possible changes and their benefits and shortcomings. The 2.4 GHz band should never have another channel width than 20 MHz since that would leave too few channels, but the 5 GHz band could potentially have a channel width of 80 MHz which would increase the amount of traffic that could be sent at once immensely. On the other hand, since some access points have many channel changes it could also be advantageous to leave the channel width at its default for stability's sake. Throughout the following sections there will be suggestions for how to decrease the amount of channel changes, if that could be achieved then it would be highly recommended to change the channel width. One solution to the frequent channel changes could be ARM's back off timer, mentioned in section 3.3. The timer makes sure that channel changes do not occur in too close proximity of each other. The back of timer parameter and the other parameters mentioned in section 3.3 should be changed to their recommended values.

Even though it is good that most of the users use the 5 GHz band, it does not seem to be the IT department's choice since 802.11n devices can choose to use the 2.4 GHz band. The likely cause of this is probably that ClientMatch is not enabled which would give administrators control of such issues. It should be encouraged to use the 5 GHz band, which offers higher throughput. Though, if the channel width of the 5 GHz band was changed to 80 MHz, it would be better to steer 802.11n clients to the 2.4 GHz band. This is because otherwise the network would probably experience more collisions since 802.11n cannot have 80 MHz as its channel width [33]. ClientMatch has many other features, recommendations for parameter changes are mentioned in section 4.1.

9.2. Security

Even though NetEnt uses PEAP-MS-CHAP as their EAP method for 802.1x authentication, which is a very secure option, it is planned to implement EAP-TLS. EAP-TLS is considered to be one of the most, if not the most, secure EAP methods. So, NetEnt has it handled when it comes to authentication, or soon to be handled. To easily provision digital certificates for EAP-TLS, NetEnt will implement ClearPass. ClearPass is a great MDM solution and can meet many BYOD requirements. NetEnt's IT team considers that guests are handled poorly at the moment and would like to implement a guest provisioning system. This is a more secure guest handling system than PSK and it would not burden the administrators with additional work. It is important to mention that guest provisioning requires captive portal which in turn requires a centralized architecture. It is also a prerequisite to have PEF, which is already implemented in the network, to have guest user roles. It is unclear what settings PEF have but it is presumed that it is not used to optimize traffic, this should be investigated by NetEnt's IT department. It is also fruitful to rate limit how much traffic guests can send, this would ensure that important employee traffic, which often uses more advanced programs than guests, is prioritized.

The presence of rouge access points or non-WIFI interference could be a reason for the previously mentioned frequent channel changes. As a part of the WIPS solution, some cheap and simple access points could be implemented to operate in the AM and SM modes. This would help in containing rouges and to discover and help eliminating interference. RFProtect should be implemented for more advanced features as seen in Figure 5. This would not only make the network more secure but could also decrease the amount of channel changes which would allow the use of the 80 MHz channel width.

Even though AirWave is installed it does not help with the discovery and containment of rouge access points, it should be configured to cooperate with SNMP as described in section 7.1. Since SNMP version 2 has many security issues, it is advocated to use version 3 which offers proper authentication and encryption.

9.3. Miscellaneous

The manner in which the access points have been deployed is in accordance with the recommended best practice, i.e. in a honeycomb pattern and approximately 15 meters apart. This will contribute to good coverage throughout the network. It is presumed that the 2.4 GHz band is enabled on every access point. If it were discovered that there were a lot of co-channel interference on the 2.4 GHz band, then the band could be disabled on some access points. The access points and the connected access points have high speed interfaces and the cables in between are Cat 6a, which is all in accordance with Aruba's recommendations. Since the access points are closely deployed it could be beneficial to disable lower data rates. This would ensure that the throughput would not decline significantly and roaming issues would be mitigated when users move around. Lastly, the association process between clients and access points could be made more efficient by using active scanning. Though, this is not a best practice and neither scanning method is favored over the other, but it could be tested as it may produce good results.

The controller, or preferably controllers, should have redundant 10 GBps interfaces connected to the core switches. Though, this is only a recommendation when a centralized forwarding architecture is used. But since a centralized forwarding architecture is also a recommendation by Aruba, both should be implemented. This will ensure that many important Aruba features can be used, see [15] for more information. The two controllers should work in an active-active setup, which would let both devices forward traffic simultaneously. Recall that jumbo frames need to be activated on intermediate devices to achieve the highest performance of the network. As mentioned in section 4.2, the convergence time of the network could be decreased if routing were implemented on the access switches. The access switches in use only support RIP as routing protocol [32], which does not converge particularly fast [34]. Therefore, that is not a recommended change for NetEnt's network. Since broadcast and multicast traffic is sent at lower data rates, it is highly recommended to drop all nonessential traffic and convert necessary traffic to unicast with DMO.

The table placement policy and preferment of wired connections makes it clear that there is an effort to minimize the traffic load of the wireless network and to distribute wireless traffic evenly over the access points. These policies should decrease congestion which would give associated clients more time on the medium. Lastly, it could be good to mention that NetEnt's wireless network lacks proper documentation, resulting in that the network is highly dependent on its technicians to remember how the network is set up. It would be easier to find areas that are prone to improvement if the network's details were written down as well as the motivations for different choices.

10. Conclusions

The overall goal of this thesis work was to gather best practices for wireless networks and propose improvements for NetEnt’s new wireless installation. The thesis work started with a literature study which gave the student fundamental knowledge of wireless communications and networks. The study focused on 802.11 frequency bands and standards, 802.11 forwarding architectures, security, and management. The second stage was the overview of NetEnt’s wireless network. Since the network lacked proper documentation the investigation came down to interviews and viewing logging and health reports. Some of the interviews were verbal and made up most of the interpretations about the network. There was much iteration between these stages which led to that the literature study dwelled into details about vendor specific protocols and features. Lastly, the thesis work ended with a comparison between general and vendor specific recommendation and NetEnt’s network. Some recommendations were met, some other were planned by NetEnt’s IT team to be implemented in the future, and then there were a couple of best practices that were not met and not a part of the IT department’s future plans.

From these steps, it was discovered that several different improvements could be made on NetEnt’s wireless network. To increase data speeds, the channel width could be changed, higher frequency ranges could be used, broadcast and multicast traffic could be converted to unicast, and the lower data rates could be disabled. To save network resources, unnecessary traffic and guest user traffic should be filtered or limited. Higher security could be achieved if rouge access points were contained, latest versions of protocols were used, and if a centralized forwarding architecture were used that would allow more security features.

These proposals are expected to help NetEnt’s new office prepare for today’s and future demands. This will be accomplished by mitigating security and communication issues while at the same time keeping the data throughput high and CPU usage low.

11. References

[1] T. Murakami, Y. Matsumoto, K. Fujii, A. Sugiura and Y. Yamanaka, "Propagation characteristics of the microwave oven noise interfering with wireless systems in the 2.4 GHz band," *14th IEEE proceedings on Personal, Indoor and Mobile Radio Communications,* vol. 3, pp. 2726-2729, 2003.

[2] D. Coleman and D. Westcott, Certified Wireless Network Administrator, Indianapolis: John Wiley Sons Inc, 2014.

[3] The Swedish Post and Telecom Authority, "PTS Spectrum Orientation Plan," 12th October 2012. [Online]. Available: https://pts.se/upload/Ovrigt/Radio/draft-orientation-plan-121011.pdf. [Accessed 23th January 2017].

[4] D. Qiao and S. Choi, "New 802.11h mechanisms can reduce power consumption," *in IT Professional,* vol. 8, no. 2, pp. 43-48, 2006.

[5] A. F. Rochim and R. F. Sari, "Performance comparison of IEEE 802.11n and IEEE 802.11ac," in *2016 International Conference on Computer, Control, Informatics and its Applications (IC3INA)*, Tangerang, pp. 54-59, 2016.

[6] Aruba, a Hewlett Packard Enterprise company, "Aruba 802.11ac Networks Validated Reference Design," 2015. [Online]. Available: http://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/61/1/Aruba%20802.11ac%20Networks%20VRD.pdf. [Accessed 28th February 2017].

[7] Aruba, a Hewlett Packard Enterprise company, "RF and Roaming Optimization for Aruba 802.11ac Networks," 2015. [Online]. Available: https://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/28/1/RF%20and%20Roaming%20Optimization%20for%20Aruba%20802.11ac%20Networks.pdf. [Accessed 8th March 2017].

[8] B. K. Soorty, S. S. Kolahi, N. Chand and Z. Qu, "Performance Comparison of Category 5e vs. Category 6 Cabling Systems for both IPv4 and IPv6 in Gigabit Ethernet," *10th IEEE International Conference on Computer and Information Technology,* pp. 1525-1529, 2010.

[9] J. Vasseur and A. Dunkels, Interconnecting Smart Objects with IP: The Next Internet, Burlington: Morgan Kaufmann Publishers, 2010.

[10] Aruba, a Hewlett Packard Enterprise company, "Aruba 802.11n Networks," 2012. [Online]. Available: http://www.arubanetworks.com/vrd/80211nNetworksVRD/wwhelp/wwhimpl/js/html/wwhelp.htm. [Accessed 11th March 2017].

[11] R. Froom and E. Frahim, Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: CCNP SWITCH 300-115, Indianapolis: Cisco Press, 2015.

[12] J. D. Day and H. Zimmermann, "The OSI Reference Model," *in Proceedings of the IEEE,* vol. 71, no. 12, pp. 1334-1340, 1983.

[13] Cisco Systems, Inc, "High Availability Campus Network Design Routed Access Layer using EIGRP or OSPF," 2005. [Online]. Available: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a00805fccbf.pdf. [Accessed 28th February 2017].

[14] Aerohive, "About Aerohive Networks," Aerohive, [Online]. Available: http://www.aerohive.com/company/about/. [Accessed 25th April 2017].

[15] Aruba, a Hewlett Packard Enterprise company, "Behavior and Defaults," n.d. [Online]. Available: http://www.arubanetworks.com/techdocs/ArubaOS_61/ArubaOS_61_UG/Defaults.php. [Accessed 30th March 2017].

[16] Aruba, a Hewlett Packard Enterprise company, "Aruba Mobility Controllers," 2012. [Online]. Available: http://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/14/1/Aruba%20Mobility%20Controllers-%20PDF.pdf. [Accessed 11th May 2017].

[17] S. Wilkins and T. Smith, CCNP Security Secure 642-637 Official Cert Guide, Indianapolis: Cisco Press, 2011.

[18] S. Turner, "Transport Layer Security," *in IEEE Internet Computing,* vol. 18, no. 6, pp. 60-63, 2014.

[19] G. C. Cristescu, V. Croitoru and V. Sorici, "Implementing an AAA-RADIUS solution based on EAP," in *2016 12th IEEE International Symposium on Electronics and Telecommunications (ISETC)*, Timisoara, pp. 81-86, 2016.

[20] Cisco Network Academy, "CCNA Security 1.1: Implementing Network Security," Cisco Press, Indianapolis, 2012.

[21] Aruba, a Hewlett Packard Enterprise company, "Working with Intrusion Detection," n.d. [Online]. Available: http://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyles/New_WIP/Intrusion_Detection.htm#new_wip_1365762209_1012568. [Accessed 24th February 2017].

[22] Aruba, a Hewlett Packard Enterprise company, "Wireless Intrusion Protection (WIP)," 2014. [Online]. Available: http://www.arubanetworks.com/assets/tg/TG_WIP.pdf. [Accessed 23rd February 2017].

[23] Aruba, a Hewlett Packard Enterprise company, "Aruba Policy Enforcement Firewall," n.d. [Online]. Available: http://www.arubanetworks.com/assets/ds/DS_PEF.pdf. [Accessed 22nd February 2017].

[24] Aruba, a Hewlett Packard Enterprise company, "Aruba 802.11n Networks," 2011. [Online]. Available: http://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/15/1/Aruba%20802.11n%20Networks.pdf. [Accessed 30th March 2017].

[25] Aruba, a Hewlett Packard Enterprise company, "Guest Access with ArubaOS," 2012. [Online]. Available: http://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/25/1/Guest%20Access%20with%20ArubaOS.pdf. [Accessed 30th March 2017].

[26] Aruba, a Hewlett Packard Enterprise company, "ClearPass Deployment Guide," 2015. [Online]. Available: https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/51/1/ClearPass_Deployment_Guide.pdf. [Accessed 30th March 2017].

[27] Aruba, a Hewlett Packard Enterprise company, "Aruba Airwave: Centralized Visibility and Management for Multivendor Access Networks," n.d. [Online]. Available: http://www.arubanetworks.com/assets/ds/DS_AW.pdf. [Accessed 27th February 2017].

[28] Airwave Wireless, Inc, "AirWave RAPIDS Best Practices Guide," 2006. [Online]. Available: http://www.airwave.com/support/knowledge-base/support/supportdocs/RAPIDS_Best_Practices623.pdf. [Accessed 27th February 2017].

[29] W. Stallings, "SNMPv3: A security enhancement for SNMP," *in IEEE Communications Surveys,* vol. 1, no. 1, pp. 2-17, 1998.

[30] Aruba, a Hewlett Packard Enterprise company, "Aruba 310 Series Access Points," n.d. [Online]. Available: http://www.arubanetworks.com/assets/ds/DS_AP310Series.pdf. [Accessed 22nd February 2017].

[31] Aruba, a Hewlett Packard Enterprise company, "Aruba 7200 Series Mobility Controllers," n.d. [Online]. Available: http://www.arubanetworks.com/assets/ds/DS_7200Series.pdf. [Accessed 22nd February 2017].

[32] Aruba, a Hewlett Packard Enterprize company, "ARUBA 2920 SWITCH SERIES," n.d. [Online]. Available: http://www.arubanetworks.com/assets/ds/DS_2920SwitchSeries.pdf. [Accessed 4th April 2017].

[33] M. Park, "IEEE 802.11ac: Dynamic Bandwidth Channel Access," in *2011 IEEE International Conference on Communications (ICC)*, Kyoto, pp. 1-5, 2011.

[34] S. Yang and Z. Z. Yong, "RIP Internet Protocol Failure Analysis and Research," in *2012 International Conference on Industrial Control and Electronics Engineering*, Xi'an, pp. 1221-1224, 2012.