Abstract

In recent years, we note three phenomena in company networks. The increase use of convergent network architecture, the abundance of WiFi networks, and the stability of the ToIP (Telephony over IP) service and other multimedia applications. This article study the integration of the voice applications in the WiFi networks by using the strength of the convergent network architecture. We discuss different WiFi user needs such as the availability, the scalability, the security and the mobility. We focus on the QoS constraint and the competition between the voice and the data to access the media.

Keywords: WiFi, ToIP, Convergent network, Availability, Mobility, QoS.

1 Introduction

If we focus on the evolution of the company’s networks we notice two main orientations. The increasing demand on convergent network and the increasing use of WiFi networks. Convergent network is an IP network federating all company’s flows and applications namely the traditional data flow but also the voice one. This can be justified mainly by two causes. First, those networks provide a rich set of new services such as unified messaging and voice mail. These services are also easily customizable and every single program running on a PC platform can be interfaced with the network. Thus, these new services can be tailored to feet exactly the end user needs. Second, this convergence saves the company a huge effort and budget required for the deployment and the supervising of the company network. Concerning the deployment, the company can replace two or even more networks by only one. Concerning the configuration and supervision, the company substitutes many teams by only one team which is smaller due to the inborn intelligence of these networks.

We notice also an increasing demand on WiFi. In some installations especially recent ones, the WiFi occupies the entire access segment and the wired network only flood the collected wireless traffic. This can be explained by saving great money and effort required for installation. The company substitute cables stretching on all the campus by some AP. Especially for temporary networks, where the WiFi network deployment is easier. In addition, WiFi provides the mobility service which is appreciated by the users. This mobility enables new services which were not provided by the wired architecture such as the Telephony over WLan. Besides, WiFi became after the successive enhancements a mature and secure transport layer that its trusted by the most hard to please customer like bank and assurance.

In this paper, we present a voice over WiFi solution using a centralized network architecture. Voice applications may be a LAN multimedia application such as a voice conference or a telephony call. The remainder of this paper is
as follows. Section 2 presents the centralized WiFi architecture. Section 3 introduce the VoFi solution. Section 4 discuss three user needs: the availability, the scalability and the security. The QoS of the Physical layer is treated in the section 5. The section 6 presents a solution for different types of QoS of the layer 2.

2 Centralized WiFi Architecture

Using the distributed WiFi architecture, the end user is interfaced with the wired network by an Access Point (AP) called *fat*. This installation allows most of features of the layer 1 and 2 of the OSI model and also some advanced features like authentication, mobility, and policy rules. In centralized WiFi this big stack is split into two smaller one as shown in the figure 1. The AP is reduced to a simple antenna that handles the layer 1 and 2 of the OSI model. However, all the intelligence is concentrated on the WiFi controller that concentrates and monitors the APs. This controller is an IP switch running a special OS. The most important benefit brought by centralization is the accurate ease of configuring and monitoring the WiFi Park. In addition, the network administrator is not compelled any more to address each AP separately to change a radio parameters or to know the retransmission rate. He can uses a simple terminal to access to the main controller via the CLI or the controller Web interface to administrate all the APs or part of them, or pick out a traffic information. Besides, the APs which are linked to a single intelligent master, feel each others and cooperate especially to handle user’s roaming and efficiently share the Radio Spectrum.

3 VoFi Solution

The VoFi solution means a WiFi architecture that guarantees an efficient transmission of the voice. The most important application that the solution should support is the telephony. But other applications such as the LAN multimedia broadcasting may be included. To deploy a VoFi substructure, it is strongly recommended to adopt a centralized WiFi for three main reasons:

- Obviously a reliable WiFi network is a basic requirement of VoFi solution, and each strength of the WiFi network is also a strength for the VoFi solution.
- The company will use this network for all its traffic, so it claims a reliable and easily monitorable one.
- The centralization bring several profitable features required by VoFi application that cannot be provided by distributed architecture. Those required features will be discovered later in this document.

The VoFi solution should meet the user’s needs. Otherwise, it will be unable to easy penetrate the market. The employee’s claims can be summarized in five main points:

1. Availability: the telephony service is a critical one and all the company business relies on it, so it should be always available.
2. Scalability: since the user’s phone is expected to connect from every single point of the company, and since the company can be very large, the WiFi connection should cover the entire company. The company may require many AP and the WiFi architecture should scale well.
3. Security: this includes authenticity, confidentiality, and avoidance against layer one and layer two attacks such as man in the middle, impersonation, and jamming.
4. Mobility this don’t only mean the ability to connect from every where of the company but also the ability to roam between APs while communicating.
5. QoS: The voice must be clearly hearable without Jitter or Delay.

The next sections presents the VoFi solution based on the centralized architecture. Solutions for all five claims are introduced and discussed.

4 Availability, Scalability and Security

We previously present the advantages brought by centralization but we should’nt forget the risk it introduces. In fact, if the central component break down the entire network will also break down. For that we must make this critical component redundant in an active standby scheme. There are several methods to achieve this redundancy. One can either gives the AP a list of the controller’s IP address.
The AP will try to reach the next controller as soon as the first one will breakdown. A more elegant way to achieve the same task is to indicate to the AP a virtual IP address of the controller. This IP is in reality shared between two controllers via a VRRP[8] (Virtual Redundancy Router Protocol) channel.

Even if the number of AP managed by the controller can reach several hundreds, the VoFi solution should be scalable. Some centralized WiFi manufacturers like Aruba[5] and Trapeze[4] manage to afford these required number by increasing the number of controller in a master/local scheme. The master controller monitors the local ones and concentrates the intelligence.

To guarantee the user’s identity, an authentication server (radius[11, 10], LDAP[7]) is required. To grant access to the network for the authenticated users, a firewall embedded in the controller is required. In fact, with an external firewall, once the packets intermingle we can not differentiate between the packets generated on the wireless side and those generated on the wired side. However, an embedded firewall is able to determine the user that initiated each packet. Thus it is able to index the flows processing according to the user rather than the IP address or TCP port or other standard firewalling policies.

In traditional distributed WiFi network, when the user roam from one AP to another, he looses his session and is compelled to reauthenticate and eventually to get a new IP address. Such a poor performances are inconvenient for time-sensitive application like telephony. Using the centralization, changing AP is no more changing antenna. So that, all the information concerning the user including its authentication state remains in the controller. Thus, roaming which was a heard task in distributed network is non more a database update task. The user is never compelled to reauthenticate and a significantly hand off time is kept.

5 QoS of the Physical Layer

QoS is a more thorny issue. To handle it exhaustively, we will investigate all QoS degradation causes, then we will specify a fix for each cause. Note that Voice do not require great bandwidth but they are time sensistive. It is significantly affected if the delay and the jitter exceed tolerable limits. Thus, any cause of increase of the delay or the jitter is considered a source of voice quality degradation. Besides, Since the WiFi concerns only layer 1 and 2, so our investigation scope must be restricted to these two layers.

The first cause of degradation is the noise. What ever his source is, micro ovens, Bluetooth, DECT phone, or neighbouring office APs, the noise causes signal distortion. If this distortion exceeds reparable limit the transmission fails. The medium access algorithm makes the retransmission happens with an increasingly high and variable delay. The second cause is the non optimal channel distribution between the WiFi networks APs. This includes the share of a single transmission channel by many neighbouring APs. Since air is a shared medium, users associated with these APs cannot communicate independently. Each client must wait the end of current transmission before initiating his own one. This is similar to using only one AP. Non optimal channel distribution scheme includes also transmission of neighbouring AP on overlapping channels which is worst than sharing the same channel because overlapping signal is interpreted as a noise. The WiFi user initiates his transmission but it is likely to fail.

The fix of this second cause is to adopt an optimal channel and power transmission scheme. This can be performed manually in small networks, but as soon as the number of APs increase, it becomes a real hard task. We adopt an automatic frequency management which is introduced by some manufacturer like Aruba[5], Trapeze[4], and Colubris[3]. This radio frequency management is achievable only with a centralized solution. The general process can be summarized as follows: The AP is expected to stay stucked to its channel in order to handle the traffic of users associated with it. Nevertheless, it periodically affords some time slots to scan the other channels and then give a feed back to the controller of relevant information like the noise strength, the strength of the signal of other AP. The controller collects these information from all the APs and then returns back the configuration of channels and transmission power that allows AP to avoid noisy channel, avoid that neighbour AP transmit on the same channel or on overlapping channel. This method minimizes the interference, maximizes coverage and the available bandwidth for end users. This automated Radio Frequency management generally succeeds in fixing the layer 1 problems, but affording a reliable physical layer can be more challenging than this. At this time we use debugging tools like spectrum analysers, traffic generator and analyser.

6 QoS of the Layer 2

User competition: Since the air is a shared medium, a great number of users associated with the same AP will result on poor traffic efficiency with small bandwith and a great delay. We recommend a two-steps solution: first well designing the network then well exploiting it. Well designing the network includes affording sufficient number of AP for the available user and for the area to cover and also wise assignment of transmission channel and power. But this step remains insufficient. For example if three neighbouring APs are transmitting on three non overlapping channels but there is an AP with a slightly higher signal level. This AP will lure all the users and the other APs will stay unused. To avoid this situation, the controller should apply a load
balancing algorithm. This insures a fair distribution of the users over the APs.

Client data: If we have a small flash back on the QoS history we notice that the need for QoS arose with the development of convergent networks that federates many flows namely data, voice and video. Those flows have different requirements of bandwidth, delay and jitter. The main 3 claims of data are security, integrity and bandwidth. However, voice flow does not require a great bandwidth but it is very sensitive to latency and jitter. The task now is to put two flows, data and voice, having different requirements on the same medium and ensures that they contend for the medium in a way that guarantees for each flow its requirements. even though telephony concerns upper layers, lower layers should be well-adapted to Voice flow. This is important because the access to the media is not decided in the same way in Ethernet and in WiFi. Under big load conditions, all the flows are equally affected regardless of the type of data. The impact on user experience, however, depends a lot on the type of data and by the type of application. A one-second delay in sending a print job from a laptop to a printer is unlikely to be noticed by the user. However, a much smaller increase in latency may disrupt the conversation in a VoIP call, or may result in dropped frames or a frozen image on the screen. Although the QoS degradation of the telephony is noticeable only when data bandwidth consumption increases, it is wrong to intend to overcome this problem by only affording a greater bandwidth. In fact voice packets are short and very spaced from each other, so they do not need great bandwidth. What matters more is that the telephone be able to initiate his transmission as soon as it decides to. The figure 2 compares a QoS enabled network with another affording greater transmission speed but without QoS.

We notice that the voice packet wait less in the first network. The data-voice competition problem can be helped by segregating data and voice flows in treatment by introducing class of services (CoS). The communication chain contains three segments: telephone-AP, AP-Controller and controller-core. For the two last segments (i.e. wired side), there are many protocols of CoS that already proved their efficiency like DiffServ[6] or DSCP[9]. Generally, a centralized solution with an embedded firewall is able to detect mark and priorities the voice flow (SIP[12]/RTP[13], H323 ). But this happens after collecting the wireless traffic. On the telephone-AP segment(i.e. the wireless side), the only available CoS mechanism is the WMM (WiFi Multimedia) ratified by the WiFi alliance as a declaration of the 802.11e incoming protocol. The general concept of WMM is: higher the class of the user is, shorter is the sensing time of medium as idle before being able to transmit. Even if some centralized WiFi manufacturers implement this standard, we can not afford a WMM enabled wireless communication because no WiFi phone implements it. Note that like security, the CoS whether it is implemented from end to end or it is not even worth its name because the lack of CoS on one segment will cancel the CoS effort deployed on other segments. We can prove this assertion by a very simple experience shown in the figure 3.

We take two clients associated with one AP generating a TCP buffering sessions. When we disable the CoS on the wired side, we measure 15 Mbs of available bandwidth for each user. When we enable the CoS, there is roughly no changes in the measurement results. The same test with two wired users would have resulted on 100 Mbs vs 0 Mbs. In fact, the CoS prioritisation occurs after the collection of the wireless traffic, but if a client reserved the air, the other one must wait him finish. Since in legacy 802.11 protocol, users have equal chances to access the medium, the available bandwidth will be equal for these clients.

Many voice clients: Even without data clients, the WiFi network cannot process an infinity of call. However, there is an allowed limit of calls number that an AP can handle. This limit depends on the used telephone, the used codec, and the used band (a or b or g). As shown in the figure ??, when call number exceeds this limit all communications are affected and not only the ones above the limit. If you have twenty telephones trying to initiate a communication you have to choose between using fifteen usable calls and five blocked or redirected and 20 unusable calls. There are some manufacturers that developed load balancing algorithm that are specific to voice client. Those algorithms ensures that
an AP accepts only calls that it is able to handle correctly and redirect the other calls to neighbouring APs.

**Flow competition:** All the QoS degradation causes can be fully overcame or at least alleviated except the competition between voice and a heavy data flow. There are two types of competition to access the media that affect the voice quality: voice-voice competition and voice data one. The first can be helped with CAC (Call Admission Control) module of some manufacturers. But the second cannot be addressed since we cannot afford a CoS mechanism on the air. The WMM is planned to be adopted by most manufacturers. Till then, a solution could be eliminating the competition by using a channel for the voice and another one for the data. There are at least three ways to implement this.

The first solution is to use dual radio AP (i.e. AP supporting simultaneously the b/g) and a radio. Then, b/g band are used for the telephony and the a band for the client data. This scheme has some drawbacks. First, it is roughly a network duplication, which violates the convergence commitment. Second, the dual radio APs are more expensive. In addition, the cards supporting the a radio are also dual radio card and they are also more expensive. Third, we can not guess in the future which among voice and data will be translated to the a radio.

The second solution uses only the g radio and reserve special APs for the voice traffic that must be fixed on one channel to shorten the hand-off time while roaming. The remaining non overlapping channels will be distributed over the data APs by the calibration process. Once again, it is roughly a duplication of the network, so it violates the convergence aim and it is more expensive. Besides, reserving a g channel for the voice traffic will decrease the available bandwidth for data clients of 54 Mbs. The voice flow will use only a small portion of it.

The third solution uses four channels (1,5,9,13) rather than three channels (1,6,13). This attempt can be useful even outside the VoFi scope since it is intended to increase the available bandwidth. Overlapping channel is more noxious than occupying the same channel because the interference is interpreted as noise. If two clients of interfering channels transmit simultaneously, a collision will occur and they will renew their transmission but with greater contention window. This is only the case of two greatly overlapping channels.

This diagram 5 show the b/g channels and their corresponding central frequencies. Note that channels are separated by 5 Mbs. The bandwidth of the channel is 22 Mbs. So the channel 1 and 6 do not overlap. However the channel 1 and 5 overlap only for 1 MHz. An experience is done to test if this little interference prevents the wished increase of the available bandwidth. The table 1 summarizes this test.

<table>
<thead>
<tr>
<th>Card 1</th>
<th>throughput</th>
<th>retransmission</th>
<th>1 channel</th>
<th>3 channels</th>
<th>4 channels</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>throughput</td>
<td></td>
<td>26 Mbs</td>
<td>24 Mbs</td>
<td>20 Mbs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1%</td>
<td>3%</td>
<td>7%</td>
<td></td>
</tr>
<tr>
<td>Card 2</td>
<td>throughput</td>
<td></td>
<td>25 Mbs</td>
<td>23 Mbs</td>
<td>20 Mbs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1%</td>
<td>4%</td>
<td>8%</td>
<td></td>
</tr>
<tr>
<td>Card 3</td>
<td>throughput</td>
<td></td>
<td>28 Mbs</td>
<td>26 Mbs</td>
<td>22 Mbs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1%</td>
<td>3%</td>
<td>6%</td>
<td></td>
</tr>
<tr>
<td>Card 4</td>
<td>throughput</td>
<td></td>
<td>28 Mbs</td>
<td></td>
<td>22 Mbs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1%</td>
<td></td>
<td>6%</td>
<td></td>
</tr>
</tbody>
</table>

**Table 1. Interference between channels**

The retransmission rates were measured with an Aruba AP. This experience shows that with 3 channels the total bandwidth is 73 Mbs and with four channels the available bandwidth 84 Mbs. We gain 11 Mbs. Actually the expected raise of global throughput is more than 11 Mbs (it is almost 25 Mbs ie the efficient bandwidth of a channel). But the cause of this lower gain is that some of the Wifi cards are old and they do not respect all the 802.11 specifications.
As shown in the figure 6, the \( b \) mask is narrower than the \( g \) one. At 11 Mbs away from the central frequency, the card need a signal at -30 db from the peak. However with the \( g \) radio, at 11 Mbs the card need only -20 db than the peak signal. The increase of the retransmission rate results in the decrease of the throughput. The source of these suspects is mainly the increase of the retransmission rate that result in the decrease of the throughput as soon as the card is not only on the network but it coexists with two other clients although those clients are occupying non overlapping channels. To test if a Wifi card is compliant with the 802.11 specified mask we must trace its spectrum with a professional tool. The most trustful way to do it is to connect an antenna to a spectrum analyser and place it close to this card. There are PCMCIA and usb cards that enable a simple PC to analyse the radio spectrum of devices, the most known tools are AirMagnet[1] and Cognio[2].

Beyond the limitation of the solutions I proposed, these solutions succeeded in overcoming the QoS issue. After applying the precedent solution, the traffic of the voice client call on the Asterisk Server with ethereal was captured. The result present an average Jitter equal to 2 ms and the maximum Jitter is 4,2 ms. The call quality was very fine.

Figure 6. Transmit spectrum mask for the radio channels

7 conclusion

This article presents a VoFi solution suitable for all user group sizes. The main requirements gathered from employees claims that must be met by this solution are availability, scalability security, mobility and QoS. Availability can be help with the redundancy and fault tolerance mechanisms provided by the convergent network architecture. Security is provided by the firewall embedded in the controller and the encryption standards. Mobility is guaranteed by storing user authentication information in the central controller.

The QoS requirement is more complex to handle. The QoS degradation causes can be summarized in the competition to access the medium. Under big load, the competition for the media access that affects the voice quality has two components: voice-data and voice-voice. Voice and data have different requirements, the most important for voice are Delay and Jitter. The voice-voice competition component is overcome by the Call Admission Control modules of the controller. The voice-data competition component is generally addressed by the Class of Service techniques (CoS). However CoS implementation must be an end to end otherwise it will losses its efficiency. The only standard that monitor CoS on the air segment is the WMM. However, most existing phones do not support the WMM feature. We present three solution that eliminates the voice-data competition. The favorite solution consists of using four radio channels rather than three. Thus the data flow and the voice flow use different non-overlapping channels. In the mean time data users still have three channels to communicate on.

References