International Journal of
Applied Mathematics,
Electronics and Computers
ISSN: 2147-8228 http://ijamec.atscience.org

Advanced Technology and Science

Original Research Paper

Long Range Wireless Point to Point Link Network on 5 GHz Frequency Band with VoIP

Rida Khan *[1], Rumsha Ansari [2], Arslan Ayoub[2]

Accepted 3rd September 2016

Abstract: 802.11 Wi-Fi technology is commonly used for creating wireless access networks with a maximum range of one hundred meters. With careful planning and proper antennas, this same technology can also be used to make point to point links up to several kilometres. Since, it is not always feasible and wise to run cables over long distances to connect different networks, therefore, wireless links may turn out to be cost effective alternative to their counterpart wired links while creating long distance networks and providing network scalability. Wi-Fi-based point to point links can therefore be used to connect two local area network (LAN) segments, which besides being cost-effective, provides network scalability and other advantages such as high speed, centralized and easier management and high throughput for line of sight (LOS) applications. A Wi-Fi-based point to point link can extend the range of wireless LAN by a few hundred feet to few miles which can further be increased by using highly directional antennas for point to point links, while serving as a backup network in different organizations. So, we have designed a soft private branch exchange (PBX) system for a university campus or organization, facilitating voice over internet protocol (VoIP) calls and instant messaging, employing the idea of Wi-Fi- based point to point links. Moreover, we have also analysed the quality of service (QOS) of the given setup in terms of data rate and connectivity using bandwidth test and ping test respectively, for both transmission control protocol (TCP) and user datagram protocol (UDP) scenarios.

Keywords: Wireless Point to Point Bridge Link, LAN segments, Soft PBX, VoIP, Instant Messaging, QOS.

1. Introduction

Many rural regions in developing and developed countries with low user densities do not have good connectivity solutions with a low budget. In low density environments, people are usually clustered around small localities, with large distances among these clusters. The example of such environments is a large enterprise situated in premises, with different departments or buildings at a distance or possibly villages or sub-urban areas. In such cases, traditional options to provide connectivity are not economically viable [1].

Fibre optics can be a very good choice for long distance backbone networks. It provides good reliability but it is not suitable for network scalability. Besides its installation and maintenance costs are quite high. So in case of low density environments and intranet connectivity, they turn out to be expensive and resources are wasted as well. Satellites technologies are very efficient for broadcast traffic, but when it comes to bidirectional internet and intranet access and interactive communications, they tend to be severely limited in throughput and costly. Traditional microwave links can scale in throughput but generally require licensing and hence are expensive to be utilized. Networks with base station model such as Worldwide Interoperability for Microwave Access (WiMAX) and cellular networks like General Packet Radio Service (GPRS) and Code Division Multiple Access (CDMA) consist of expensive base stations, which do not cover enough users in low-density regions and hence lead to the waste of resources [2].

Wireless mesh networks are generally established using the 802.11 Wi-Fi technology and serve to provide internet access in high user density environments. These wireless mesh networks provide full coverage of the region using Omni-directional Access Points (APs) over a range of about one hundred meters. But mesh networks suffer from two major short comings when scaled to larger areas. First, an increase in number of APs in the growing network with Omni-directional antennas leads to increased interference in over-lapping cells. Second, the use of low gain Omni-directional antennas increases the hop length, resulting in a decrease in throughput [2]. Thus, it can be implied that for low density of users, traditional approaches that provide full coverage or require wiring of sites are not feasible. The alternative is to cover only those few places where connectivity is required, by employing long distance wireless point to point links. Such links can be employed using Wi-Fi for low cost and ease of configurability. Hence, the best solution for internet access and intranet communications in low density environments and some organizations is using Wi-Fi in bridge mode providing point to point and point to multipoint links [1].

Wi-Fi-based point to point links have proved to be the cost effective alternative to their counterpart wired networks to provide communication over long distances, especially in rural areas and within an enterprise or premises. Wi-Fi-based point to point links are relatively cheap and provide a number of

[1] *Telecommunication Engineering Department, Istanbul Technical University, Campus, Ayazaga, Istanbul/Turkey*
[2]*Telecommunication Engineering Department, Mehran University of Engineering and Technology, Pakistan*
** Corresponding Author: Email: rida.khanoct@yahoo.com*
Note: This paper has been presented at the 3rd International Conference on Advanced Technology & Sciences (ICAT'16) held in Konya (Turkey), September 01-03, 2016.

advantages such as network scalability, high speed, centralized and easier management and high throughput for Line of sight (LOS) applications. Wi-Fi-based point to point links can extend the range of wireless local area network (WLAN) by a few hundred feet to a few miles, by segmenting it, using highly directional antenna and adequate planning for these point to point links. They can also serve as a backup network in different organizations.

Therefore, in this paper, we propose the idea of Wi-Fi-based point to point links for any type of low density environment with voice over internet protocol (VoIP) and instant messaging services in a soft private branch exchange (PBX) system. We setup a server to enable these applications at one end of the soft PBX system and configure the APs to enable Wi-Fi-based point to point links for providing services at the other end of the soft PBX system. Furthermore, we also analyse the quality of service (QOS) of the given setup in terms of data rate and connectivity using bandwidth test and ping test respectively, for both transmission control protocol (TCP) and user datagram protocol (UDP) scenarios.

The rest of the paper is organized as follows. In Section II, related terminology used in this paper is discussed and Section III puts light on the system model. Section IV explains the soft PBX system and Section V presents observations. Section VI finally concludes the paper.

2. Related Terminology

2.1. Wireless Bridges

We use wireless bridges in our system to connect network segments using point to point links. LAN would be flooded with unnecessary traffic if the messages are broadcasted to every destination in that network thus bridges are usually used for the segmentation of LAN and interconnection of LAN segments. A bridge network solution does not necessitate difficult configurations, like IP routing. The bridge network manages LAN segments and creates a single subnet for the entire network. Bridges work at the data link layer of the Open System Interconnection (OSI) model. Bridges learn which addresses are on which network segment and develop a forwarding table so that subsequent messages can be forwarded to the right network segment. Bridges examine the incoming packets and look up the forwarding table for their destination media access control (MAC) address. If the destination MAC address is found in the forwarding table, the packet is forwarded to the corresponding port and if the destination MAC address is not found in the same segment, the bridge restricts the transmission [3].

Wireless bridges are same in functionality and used to connect two LAN segments via a wireless interface such as a radio link, to facilitate connectivity and data transfer between them. Wireless bridges are commonly used to interconnect wired network segments such as an Ethernet network via wireless link. In simple terms a wireless bridge is a device that allows two network segments of users to transparently communicate to one another over long distances without wires. They can be used to connect areas that are geographically apart like a remote building to the main building up to 30 miles, using proper antennas and LOS. Connecting two locations wirelessly through a wireless bridge is much more cost effective than the installation and maintenance of a wired network whether it is fiber optics or copper, for the same purpose. Wireless bridges provide connectivity when it is difficult to wire the sites. Moreover, with wireless bridges, network scalability can be performed very easily by just providing another AP working in the bridge mode at the place of interest [4].

2.2. Wireless Aps

Wireless access points (APs or WAPs) are specially configured nodes on WLANs. These are the network devices used to connect multiple wireless devices to wired LAN, for accessing internet. APs act as a central transmitter and receiver of WLAN radio signals. APs used in home or small business networks are generally small, dedicated hardware devices featuring a built-in network adapter, antenna, and radio transmitter. APs support 802.11 wireless communication standards. Usually, WAPs operate in "root mode", a point to multipoint configuration in which the AP relays frames between many 802.11 stations and an adjacent Ethernet LAN. However, WAPs also have bridging mode that can be configured for connecting LAN segments in point to point link configuration. Wireless bridges relay frames between LAN segments using the same 802.11 wireless communication standards [4].

2.3. FCC Rules for 802.11 Standards

Since, Wi-Fi 802.11 standard operates in an unlicensed Industrial scientific and medical (ISM) band therefore, the signals operating over that band can interfere with each other. So, there are some rules defined by FCC to cope up with it that put some limitations on the power or Effective Isotropic Radiated Power (EIRP) of the signals radiated on this band. These rules are different for 2.4 GHz and 5 GHz operating frequencies of ISM bands as well as for point to point and point to multipoint topologies. In this project, a point to point link is established between LAN segments operating on the 5 GHz band within the limitations defined by FCC, which state that. "For maximum transmitted power of 30dBm, a directional antenna gain of 23dBi can be used with no reduction of transmitter power output in point to point links. However, if directional antenna gain increases greater than 23dBi, a 1dB reduction in peak transmitter power is required for each 1dBi increase in antenna gain greater than 23dBi" [5].

2.4. Fresnel Zone Clearance in Point to Point Links

We use 5 GHz ISM band to establish point to point link in our system that falls in the microwave region of electromagnetic spectrum. Microwave links are generally used for LOS communications as microwaves are highly directional and travel in straight lines. But the energy of microwaves is not pencil thin. They spread out the farther they get from the antenna. The area that the signal spreads out is called Fresnel Zone. If there is an obstacle in the Fresnel zone, part of the radio signal will bent away from the straight line path which will result in the reduction of the amount of radio frequency (RF) energy reaching the receiving antenna. Fresnel zones can also be viewed as the concentric ellipsoids surrounding the transmitter, receiver and the LOS between them. The first Fresnel zone is the region where the microwave transmission energy is the most intense and it is the closest to the direct line between transmitter and receiver, as shown in Fig. 1.

The obstruction in the first Fresnel zone can even lead to link failures. Therefore, the Fresnel zone clearance is the most crucial phenomenon while designing the microwave point to point link. In order to provide a lossless communication via point to point microwave link, the radius of the first Fresnel zone should be 60

per cent clear of any obstruction. This Fresnel zone clearance can be achieved by adjusting the antenna heights at both the transmission and reception ends [6].

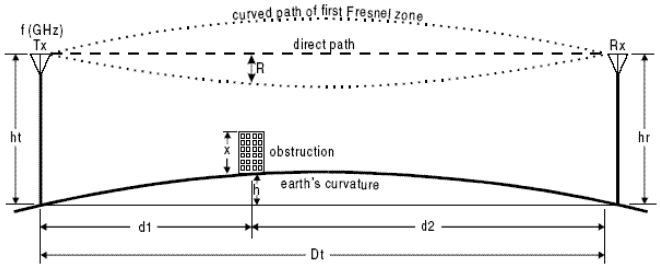

Figure 1. Fresnel Zones.

2.5. Devices for Point to Point Link

We use MikroTik SXT 5HnD devices to connect LAN segments with a point to point bridge link. These are low cost, versatile and high speed devices, operating at 5 GHz frequency of ISM band. The devices include many important features such as support for 802.11a/n wireless standard, transmitter power of 26dBm, built-in 16dBi dual chain antenna, 10/100 Ethernet port and others. These devices have their own proprietary wireless protocol, named as Nv2 for use with 802.11 wireless chips. Nv2 protocol is specifically based on Time Division Multiple Access (TDMA) technology for long range point to point links instead of Carrier Sense Multiple Access (CSMA) technology for 802.11 devices. Nv2 protocol in AP enables to control media access by dividing time in fixed size slots. These slots are dynamically allocated in downlink (data sent from AP to clients) and uplink (data sent from clients to AP) portions, based on queue state on AP and clients. Nv2 is different from 802.11 as the media access is scheduled by AP. AP controls that how much time is used by every client and time is assigned to clients according to some policy not according to contention based methods like in 802.11 standards. Also propagation delay is reduced in Nv2 as there are no per frame acknowledgements. Nv2 implements frame aggregation and fragmentation to maximize the assigned media usage and reduce per frame overhead. The devices also include high throughput (HT) to enable the use of MIMO feature of 802.11n standard used in the device. With HT chains 0 and 1 enabled at the transmitter and receiver sides, 2 by 2 antenna diversity and spatial multiplexing can be achieved which significantly increases the throughput of the device. With "HT guard interval" option, the length of guard interval can be adjusted to minimize the inter symbol interference while maintaining the desired throughput [9].

3. System Model

The point to point microwave bridge link is established to connect the LAN segments in the two buildings that are 1km apart in the campus. For proper transmissions the two antennas should be properly aligned and should have a clear LOS with 60 percent of the Fresnel zone unobstructed. From the site survey, it was observed that there are obstructions between the two departments so the antennas are needed to be mounted at a considerable height to get an unhindered path. The system model in Fig. 2 shows how different devices are connected to establish the point to point link between LAN segments and provide intranet connectivity as well as internet access. The AP at one side of the link is configured as the bridge or AP while on the other side, it acts as the client. The client is connected to a switch/router to which wired device (such as PCs) as well as wireless devices (like laptops, phones) can connect and use the wireless link. The AP at the other end is also connected to a switch/router to which the IP PBX sever is attached for VoIP communication and instant messaging. Other wired or wireless devices can also connect to it for intranet communication. The switches/routers transfer the VoIP calls/instant messages within a LAN segment and the APs (configured in AP or bridge mode) transfer the VoIP calls/instant messages to the other LAN segment. Ethernet cables and Power over Ethernet (POE) adapter are used for interface and power.

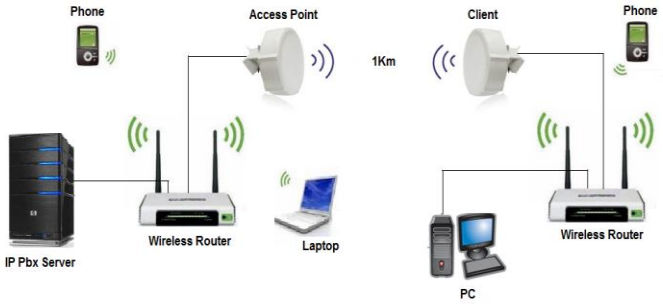

Figure 2. System Model for Wireless Point to Point Bridge link.

3.1. Configuration of Devices

We use two RouterBoard SXT G-5HnD access points to establish the link. One of them is configured as a bridge (AP) and other as a station bridge (client). The devices are graphically configured using Winbox software/ application. After logging into the devices at both AP/client end, both MAC and IP addresses are configured first and then their identities are defined as AP or client.

Wireless point to point link is created at both AP and client by defining different interfaces with address resolution protocol (ARP) enabled. The wireless characteristics of the point to point link such as band, channel width, frequency and wireless protocol are set to be 5 GHz, 20 MHz, 5180 MHz and Nv2 respectively at both AP and client end of the LAN segment. The manual transmit power is set to 30dBi as per FCC rules requirement at the client end. All HT chains are enabled at both AP and client ends to provide MIMO feature and the guard interval is kept 800ns to avoid inter symbol interference and get a more stable link. After setting the wireless point to point link, it is necessary to make bridge configurations at both ends of the LAN segment. At both AP and client side, rapid spanning tree protocol (RSTP) is used to prevent bridging loops and two interfaces are defined, one for the point to point bridge link and the other for connecting to the particular LAN segment. We use Dynamic host configuration protocol (DHCP) to provide automatic IP address to the devices, connected to each LAN segment for soft PBX call and instant messaging. The configuration is made on AP device that is connected to the soft PBX server. A static IP is defined for the gateway DHCP and the rest of the IP addresses are allocated dynamically from the DHCP pool for a maximum lease time of 3 days.

4. Soft PBX

PBX is a telephone switching system owned by a company that manages incoming and outgoing calls for the company's internal users. Companies lease only one line and have many people using

it, with each one having a phone at the desk with different number, called extension. PBX automatically sends incoming calls to the required extensions. A PBX hence can switch calls within the organization and can also connect to the Public switched Telephone Network (PSTN) for calling outside the organization. A conventional PBX can be costly as it requires copper wires and other hardware equipment. Soft PBX (also called IP or virtual PBX) is a telephone system used for the sending voice over the internet protocol (IP) network and is same in application as the conventional PBX but functions differently. It is based on a computer PBX software and voice over internet protocol (VoIP) instead of relying on the traditional telephone hardware and copper circuits. A soft PBX system uses a single network for data traffic and voice calls, both encapsulated in IP packets and then transferred over the network, unlike conventional PBX. The major part of the soft PBX is handled by the software so they are relatively inexpensive. A soft PBX system consists of three components; phones, soft PBX server and an optional VoIP gateway. Phones should capable of supporting VoIP. Soft PBX software installed in PC can serve the purpose of a soft PBX server. VoIP gateways are optional and are used to connect to the external land line PSTN. The users in soft PBX register their session initiation protocol (SIP) address, very much like extensions in conventional PBX, with the soft PBX server, which maintains a database of all its users and their corresponding SIP addresses. The VoIP telephone calls are established modified and terminated using the IP telephony protocol SIP. To make a call, the server is requested to establish a connection. When the called party's number is dialled, the IP address of the phone is mapped to the corresponding SIP address and then it is sent to the destination. The calls to and from PSTN are routed via VoIP gateway. If the call is to be made outside the soft PBX network, the server directs it to the gateways from where it is sent towards the PSTN. Similarly the calls from PSTN are directed to the server via the gateway and the server then sends them to the appropriate destination [8].

4.1. For VoIP Calls

For VoIP calls, we use Asterisk which is open source soft PBX software that can use both traditional Time Division multiplexing (TDM) technology and packet voice protocols (VoIP and Voice over Frame relay). Asterisk acts as a full featured PBX, supporting virtually all conventional call features on SIP phones like Caller ID, Call waiting, Call forward/busy, Call forward/no answer, Voice mail, Least cost routing, Call conferencing and many more. Asterisk supports three VoIP protocols, two industry standards and one specifically for Asterisk. Inter-Asterisk exchange (IAX) is the de-facto standard for Asterisk networking. The other protocol used by Asterisk is Session initiation Protocol (SIP) which is an Internet Engineering Task Force (IETF) standard for VoIP. The last one is H.323 which is an International Telecommunication Unit (ITU) standard for VoIP. Asterisk provides seamless and transparent translation among so many codecs and file formats such as A-law, u-law, GSM 6.10, MP3, PCM, VOX and LCP-10 [9]. In order to configure soft PBX, we download and install Asterisk10 along with its packages on Ubuntu Linux operating system. SIP file is edited to define SIP clients, codecs used, mailbox addresses and other options. We set different extensions for each SIP client or user under the context of phones and a shared password is used to authenticate each phone. The user reachability checks are performed every 60seconds. Out of all codes available, we use only u-law, A-law and GSM codes in our soft PBX system. Mailbox is used for the voice mail messages such that the voice mails for the user having extension 101 will be saved at 101@default. Dial plan file is created to handle incoming and outgoing calls such that the commands are executed in the following order: when there is a call for some extension, direct the call to that extension. After 20s the called party is asked to leave their message which will be saved at extension@phones. The server is then directed to play an audio file and then hang-up the call. A separate file for voicemail is made with a separate extension such that the called party is directed to the main voice mail system to check the voice mails if there are any. All files are reloaded after their configuration.

4.2. For Instant Messaging

Open fire version 3.8.0 server is used in the project to facilitate instant messaging which uses the only widely adopted open protocol for instant messaging; that is Extensible Messaging and Presence Protocol (XMPP) (also called Jabber). Jabber is an open, Extensible Mark-up Language (XML)-based protocol for instant messaging written in Java. The server is also compatible with the Asterisk 10 server used for VoIP calls in the system. Concisely, open fire is a freeware open source server that provides instant messaging, broadcast messaging, offline messaging and group chat. Open fire also provides a higher degree of security to the end user as the clients are connected to the server using the Secured Sockets Layer (SSL) secured connection so; the traffic streams in both directions are encrypted. The server also provides a way of authentication to its clients for improved security using a different user ID and password for each client. Whenever a client is registered to the server, the user ID and password for that instant messaging service are stored in encrypted form on the server and are used for client authentication. Open fire is based on the protocol that runs on Java so open fire requires Java Run time Environment (JRE) and Java development Kit (JDK) to operate. Open fire also requires MySQL server to make its user accounts database [10]. Therefore, first the latest versions of Oracle JRE/JDK are installed on the Linux server and then MySQL database server and client packages are installed. When the MySQL server and client packages are installed, the database or user accounts are ready to be set. MySQL has its own user accounts which are not related to the user accounts on the Linux machine for VoIP calls. By default, the root account of MySQL server is empty so, root accounts along with the passwords are defined. A new MySQL database is created for Open fire with a new username and password. After that Open fire 3.8.0 is downloaded, installed and configured. For the configuration of Open fire, first administrator account is setup with email and password and then the administrator account is used to create users/clients with their corresponding usernames, email addresses and passwords.

5. Observations

Once the point to point bridge link is established and it is working properly, it becomes important to analyse the QOS provided by the link for the VoIP calls and instant messaging services. The key parameters to estimate the QOS of any network are its delay, bandwidth or data rate and packet loss. These parameters are

tested one by one over the link to observe QOS by the link for each service. The results are indicated in Fig. 3 and Fig.4 for bandwidth test and Fig.5 and Fig. 6 for ping test at both AP and client ends.

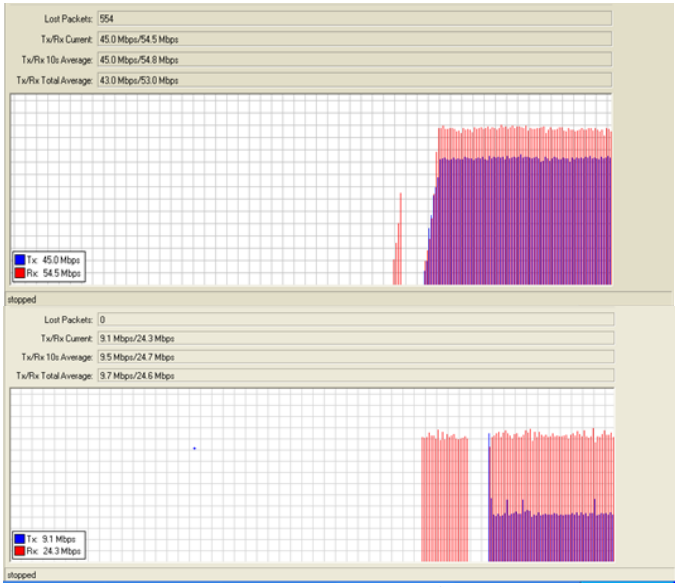

Figure 3. Bandwidth Test at AP for UDP and TCP.

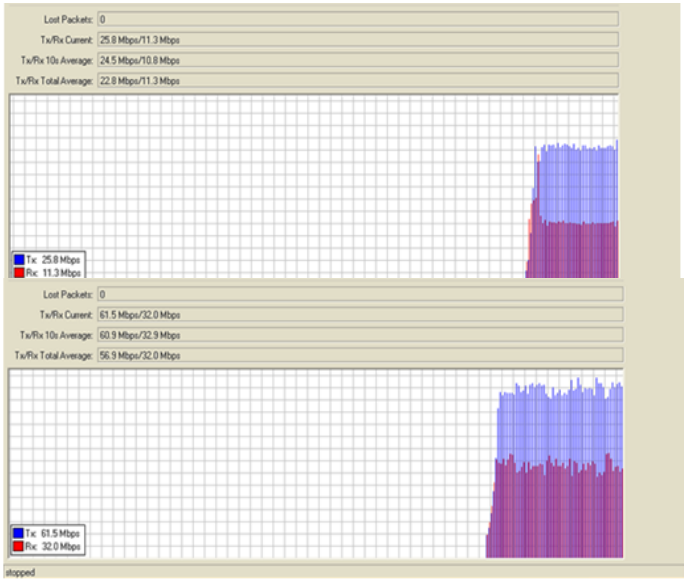

Figure 4. Bandwidth Test at client for UDP and TCP.

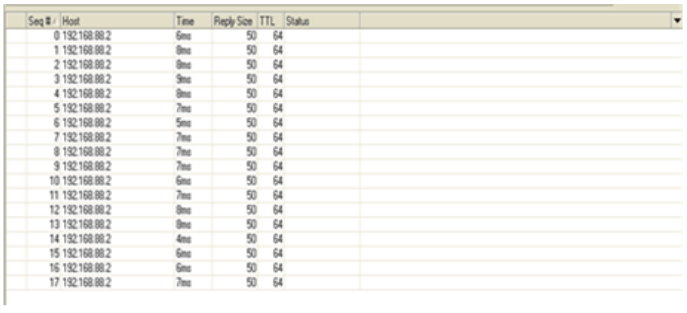

Figure 5. Ping Test at AP.

Seq #	Host	Time	Reply Size	TTL	Status
0	192.168.88.1	3ms	50	64	
1	192.168.88.1	27ms	50	64	
2	192.168.88.1	10ms	50	64	
3	192.168.88.1	32ms	50	64	
4	192.168.88.1	16ms	50	64	
5	192.168.88.1	14ms	50	64	
6	192.168.88.1	4ms	50	64	
7	192.168.88.1	16ms	50	64	
8	192.168.88.1	32ms	50	64	
9	192.168.88.1	21ms	50	64	
10	192.168.88.1	32ms	50	64	
11	192.168.88.1	9ms	50	64	
12	192.168.88.1	20ms	50	64	

Figure 6. Ping Test at client.

5.1. Bandwidth Test

Bandwidth test is done to get the bandwidth and data rate of the link in both directions that is transmit and receive, at both AP and the client. Bandwidth test also gives the packet loss at an instant when some particular number of packets is sent. Bandwidth test is done in two different scenarios of TCP and UDP as they provide different results in terms of data rate and packet loss. Bandwidth test performed at the AP device gives the results shown in Fig. 3. Results are taken for UDP as well as TCP in both directions when the transmitted and received packet sizes are 1500 bits. The QOS analysis for UDP shows that the data rate at the transmission is 45 Mbps and at the reception is 54.5 Mbps giving the total data rate of about 99.5 Mbps in both directions that can adequately make several voice calls and data transmissions simultaneously. For a packet size of 1500 bits per packet, almost 66,333 packets are transmitted per second in both directions at a bidirectional data rate of 99.5 Mbps, out of which 554 packets are lost at an instant. Therefore, the packet loss is never exceeding 1 percent which is optimum for voice calls and data transmission. For TCP, it can be clearly seen that the packet loss is 0 since TCP is a connection oriented reliable protocol in which each transmitted packet is acknowledged and none of the packet is lost. However, due to multiple acknowledgements, the data rate is significantly reduced to 9.1 Mbps at the transmission side, 24.3 Mbps at the reception side and a total data rate of 39.4 Mbps in both directions. But the data rate is still enough to send multiple voice calls and data files simultaneously. Bandwidth test performed at the client device gives the results presented in Fig. 4. The results for UDP show that the data rate at the transmission side is 61.5 Mbps and at the reception is 32 Mbps, giving a total data rate of 93.5 Mbps in both directions that is optimum for making several voice calls at the same time and the packet loss is seen to be zero even for UDP protocol. The results for TCP protocol at the client side show that the effective data rate is reduced to 25.8 Mbps at the transmission side and 11.3 Mbps at the reception side summing up to a total data rate of 37.1 Mbps in both directions. The packet loss is zero for the same reason of reliability.

5.2. Ping Test

Ping is an acronym for the word “Packet internet gofer”. Ping works over Internet Control Message (ICMP) protocol that checks for the relative connectivity in the network. So, ping test is performed to check the connectivity of the link and an average delay that it takes for a packet to be sent to a destination and receive a packet in response from the destination. Ping test is performed at both the AP and client devices to check connectivity and delay at both ends. Ping test is performed at AP to check its connectivity with the client.

Ping test performed at the AP device gives the results, as depicted in Fig. 5. As seen from the ping statistics of the packets sent and ping replies, it is clear that the average delay is not exceeding above 7ms that is quite appropriate for making several voice calls and data transmissions simultaneously. The continuity in ping replies also assures the reliability of the link for making voice calls. Ping test at the client is performed to check its connectivity with the AP client and delay in packet transmission and reception. Ping test made at the client device gives the results, as shown in the Fig. 6. The results show that the minimum delay of the link for transmission and reception of packets is 3ms and average delay is 18ms. This delay is a little greater than the delay observed in the ping test performed at the AP device but still satisfies the QOS requirements for voice calls and instant messaging.

6. Conclusion

In this work, we have used wireless point to point bridge link to connect LAN segments located separated 1km apart and provide VoIP and instant messaging service using soft PBX in both LAN segments. Although wireless bridge link operating in an unlicensed band and can suffer from interference and lack of reliability, but these shortcomings can be adjusted with proper planning of the link. Wireless bridge link can offer outstanding advantages such as cost effectiveness, suitable data rate, easier installation, easier trouble shooting and scalability for low density environments.

References

[1] Wireless Revolution. (2016) Wireless Revolution on Economist.[Online].Available:http://www.economist.com/node/9080024.

[2] Point to Point Broadband Wireless for Enterprise. (2016) White paper on Point to Point Broadband Wireless for Enterprise.[Online].Available:http://www.motorolasolutions.com/content/dam/msi/docs/business/solutions/industry_solutions/education/motowi4/_documents/static_files/ne_wb_enterprise_wp_us_r4_new.pdf.

[3] Jeffrey S. Beasley, Networking, 2nd ed., New Mexico State Univ., USA: Prentice Hall, 2008.

[4] Understanding Wireless Bridging and WDS. (2016) on Connect802.[Online].Available:http://www.connect802.com/wireless_bridging.html.

[5] FCC Rules. (2016) the fcc-rules on afar tutorials. [Online].Available: http://www.afar.net/tutorials/fcc-rules.

[6] Fresnel Zone. (2016) Fresnel Zone on Digital Air Wireless. [Online].Available:http://www.digitalairwireless.com/wireless-blog/recent/fresnel-zones-what-are-they-and-why-are-they-so-important.html.

[7] Mikrotik. (2016) Wireless Workshop on Mikrotik. [Online].Available:http://mum.mikrotik.com/presentations/US12/uldis.pdf.

[8] IP PBX. (2016) IP PBX on Asterisk Applications. [Online].Available:http://www.asterisk.org/get-started/applications/pbx.

[9] Mark Spencer, "Introduction to the Asterisk Open Source PBX," Libre Software Meeting, France, Linux Support Services Inc., 2002.

[10] Openfire. (2016) Openfire 4.0.2 on igniterealtime. [Online].Available:https://www.igniterealtime.org/projects/openfire.