July 2011

Wireless Testing Tool for Wireless Routers

Kavan K V

Department of CS&E, Sri Siddhartha Institute of Technology, Tumkur, India, kavankvsit@gmail.com

M. SIDDAPPA Dr.

Department of CS&E, Sri Siddhartha Institute of Technology, Tumkur, India, msiddu_ssit@rediffmail.com

Follow this and additional works at: <https://www.interscience.in/ijssan>

Part of the [Digital Communications and Networking Commons](#), and the [Electrical and Computer Engineering Commons](#)

Recommended Citation

K V, Kavan and SIDDAPPA, M. Dr. (2011) "Wireless Testing Tool for Wireless Routers," *International Journal of Smart Sensor and Adhoc Network*: Vol. 1 : Iss. 1 , Article 14.

DOI: 10.47893/IJSSAN.2011.1013

Available at: <https://www.interscience.in/ijssan/vol1/iss1/14>

This Article is brought to you for free and open access by the Interscience Journals at Interscience Research Network. It has been accepted for inclusion in International Journal of Smart Sensor and Adhoc Network by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

Wireless Testing Tool for Wireless Routers

Kavan K V¹, Dr. M.SIDDAPPA²

Department of CS&E, Sri Siddhartha Institute of Technology, Tumkur, India
E-mail: kavankvsit@gmail.com¹, msiddu_ssit@rediffmail.com²

Abstract- Wireless test tool is a powerful tool for wireless network monitor and analyzer for 802.11 a/b/g/n networks. Loaded with many user-friendly features, Wireless test tool for Wi-Fi combines performance and flexibility with an ease of use in the industry. Wireless test tool for Wi-Fi captures every packet on the air to display important information such as the list of access points, IP address etc. By providing this information, Wireless test tool for Wi-Fi can help you view and examine packets, network problems, and troubleshoot software and hardware.

Wireless test tool for Wi-Fi is a comprehensive and affordable tool for wireless LAN administrators, security professionals, network programmers, or anyone who wants to have a full picture of the WLAN traffic. It also test the Wi-Fi router and its capabilities like signal strength, Its data transfer in terms of throughput, bandwidth etc.

Keywords: Wi-Fi(Wireless-Fidelity), Throughput, Wireless router, Bandwidth, IEEE 802.11 a/b/g/n standards, Access point, IP address

I. INTRODUCTION

IP based wireless network usage is growing significantly among DOTs. Agencies are realizing that wireless links are an additional communications medium that can be added to their existing toolbox of services. Wireless can be used as a temporary solution or as a permanent one for certain areas where fiber or other wireline service is not realistic. As the use of wireless IP systems grows, agencies need methods for evaluating and comparing systems and architectures [2].

WiFi is the wireless way to handle networking. It is also known as 802.11 networking and wireless networking. The big advantage of WiFi is its simplicity. You can connect computers anywhere in your home or office without the need for wires. The computers connect to the network using radio signals, and computers can be up to 100 feet or so apart.

In this paper, we will discuss two different aspects of WiFi. First we will discuss the basic technology that makes WiFi networking possible. Then we will discuss the hardware you need to create a WiFi network, and help you understand how to set up and access a WiFi hotspot in your home.

A. Wi-Fi is Freedom

Wi-Fi, or Wireless Fidelity, is freedom: it allows you to connect to the Internet from your couch at home, a bed in a hotel room or a conference room at work without wires and Wi-Fi is a wireless technology like

a cell phone. Wi-Fi enabled computers send and

Figure 1. Example for Wi-Fi environment.

receive data indoors and outdoors anywhere within the range of a base station. And the best thing of all, it's fast. In fact, it's several times faster than the fastest cable modem connection.

B. Wi-Fi Connects You Anywhere

Imagine working on your laptop or checking e-mail from anywhere in your home. Imagine being able to connect to your office network from an airport or coffee shop. Imagine retrieving files or presentations from the corporate network, cruising the Internet or sending instant messages to co-workers—and doing it all from a conference room or the company cafeteria.

Now, imagine doing all these things easily and quickly - without worrying about finding a wired network connection. That is Wi-Fi. Imagine being able to move your entire office without losing your investment in networking installs, or to add new staff,

All without moving cables or installing complicated hubs and routers.

This paper objective was to develop a software tools that can be used to quantitatively measure bandwidth metrics

across wireless networks. These tools will either transmit real data traffic across a wireless network and measure the amount of data transmitted over time, or will simulate different types of traffic and estimate the bandwidth.

A repeatable methodology is required to accurately measure the Internet Protocols that are used for transferring data. These protocols include File Transfer Protocol (FTP), Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP). TCP and UDP are most often used when assessing the true available bandwidth, often referred to as payload bandwidth, across wireless links.

C Why Bandwidth

When assessing wireless networks there are many parameters that can be investigated. Many focus strictly on the wireless aspect when comparing and evaluating systems. Metrics such as signal-to-noise ratio (SNR), bit error rate (BER), and received signal strength indication (RSSI) are some of the parameters used in wireless technologies. These metrics are all important to the performance of a wireless network; however for this project it was decided that the useable bandwidth of a system is the most telltale metric for comparing systems. Wireless parameters such as SNR, BER, and RSSI all have an end effect on the bandwidth. Low signal strength or a large number of bit errors correlate to lower bandwidth. Therefore, the researchers opted to analyze bandwidth performances as an overall indicator of system performance.

The problem statement is to develop an software application that perform an testing operation on wireless router/modem and test the Wi-Fi router and its capabilities like signal strength, Its data transfer in terms of throughput, bandwidth etc.

The solution to the problem to design an application in Visual C# on windows XP platform such that the applications should detect an strength of a wireless router and test its capabilities like Signal strength, data transfer rate between two or more system located at different distance in the Wi-Fi network i.e., throughput which uses FTP protocol.

What can do with Wireless test tool for WiFi

- Scan the air for WiFi stations and access points.
- Capture 802.11a, 802.11b, 802.11g, and 802.11n WLAN traffic.
- View detailed IP connections statistics: IP addresses, ports, sessions, etc.
- Configure alarms that can notify you about important events, such as suspicious packets, high bandwidth utilization, unknown addresses, rogue access points, etc.

II. IEEE 802.11 ARCHITECTURE

Architecture Components An 802.11 LAN is based on a cellular architecture where the system is subdivided into cells. Each cell (called **Basic Service Set**, or **BSS**, in the 802.11 nomenclature) is controlled by a Base Station (called **Access Point** or, in short, **AP**).

Although a wireless LAN may be formed by a single cell, with a single Access Point, (and as will be described later, it can also work without an Access Point), most installations will be formed by several cells, where the Access Points are connected through some kind of backbone (called **Distribution System** or **DS**). This backbone is typically Ethernet and, in some cases, is wireless itself [1].

The whole interconnected Wireless LAN, including the different cells, their respective Access Points and the Distribution System, is seen as a single 802 network to the upper layers of the OSI model and is known in the Standard as **Extended Service Set (ESS)**.

The standard also defines the concept of a **Portal**. A portal is a device that interconnects between an 802.11 and another 802 LAN. This concept is an abstract description of part of the functionality of a “translation bridge”.

The following diagram shows a typical 802.11 LAN including the components described below:

Figure 2: A Typical 802.11 LAN

Even though the standard does not necessarily request it, typical installations will have the AP and the Portal on a single physical entity.

A IEEE 802.11 Layers Description

As any 802.x protocol, the 802.11 protocol covers the MAC and Physical Layer. The Standard currently defines a single MAC which interacts with three PHYs (all of them running at 1 and 2 Mbit/s) as follows:

1. Frequency Hopping Spread Spectrum in the 2.4 GHz Band
2. Direct Sequence Spread Spectrum in the 2.4 GHz Band, and
3. Infrared

Beyond the standard functionality usually performed by MAC Layers, the 802.11 MAC performs other functions that are typically related to upper layer protocols, such as

Fragmentation, Packet Retransmissions, and Acknowledges [1].

While these Collision Detection mechanisms are a good idea on a wired LAN, they cannot be used on a Wireless LAN environment for two main reasons:

1. Implementing a Collision Detection Mechanism would require the implementation of a Full Duplex radio capable of transmitting and receiving at once, an approach that would increase the price significantly.
2. In a Wireless environment we cannot assume that all stations hear each other (which is the basic assumption of the Collision Detection scheme), and the fact that a station wants to transmit and senses the medium as free doesn't necessarily mean that the medium is free around the receiver area.[7] [Patrick Wiederkehr, Hotspot logins with wi-fi devices]

B. The Authentication Process

Once the station has located an Access Point, and decides to join its BSS, it goes through the **Authentication Process**. This is the interchange of information between the AP and the station, where each side proves the knowledge of a given password.

Once the station is authenticated, it then starts the **Association Process**, which is the exchange of information about the stations and BSS capabilities, and which allows the DSS (the set of APs) to know about the current position of the station). A station is capable of transmitting and receiving data frames only after the association process is completed.

Roaming is the process of moving from one cell (or BSS) to another without losing connection.

This function is similar to the cellular phones' handover, with two main differences:

1. On a packet-based LAN system, the transition from cell to cell may be performed between packet transmissions, as opposed to telephony where the transition may occur during a phone conversation, this makes the LAN roaming a little easier, but
2. On a voice system, a temporary disconnection may not affect the conversation, while in a packet based environment it significantly reduces performance because retransmission is then performed by the upper layer protocols.

The 802.11 standard does not define how roaming should be performed, but defines the basic tools. These include active/passive scanning, and a re-association process, where a station which is roaming from one Access Point to another becomes associated with the new one **Keeping Synchronization** Stations need to keep synchronization, which is necessary for keeping hopping synchronized, and other functions like Power Saving. On an infrastructure BSS, this is achieved by all the stations updating their

clocks according to the AP's clock, using the following mechanism:

The AP periodically transmits frames called **Beacon Frames**. These frames contain the value of the AP's clock at the moment of transmission (note that this is the moment when transmission actually occurs, and not when it is put in the queue for transmission. Since the Beacon Frame is transmitted using CSMA rules, transmission may be delayed significantly).

The receiving stations check the value of their clocks at the moment the signal is received, and correct it to keep in synchronization with the AP's clock. This prevents clock drifting which could cause loss of synch after a few hours of operation.[9]

C. Security

Security is one of the first concerns that people have when deploying a Wireless LAN. The 802.11 committee has addressed the issue by providing what is called **WEP (Wired Equivalent Privacy)**.

Users are primarily concerned that an intruder should not be able to:

1. Access the Network resources by using similar Wireless LAN equipment
2. Capture Wireless LAN traffic (eavesdropping)

Preventing Access to Network Resources

This is done by the use of an Authentication mechanism where a station needs to prove knowledge of the current key. This is very similar to Wired LAN privacy, in the sense that an intruder needs to enter the premises (by using a physical key) in order to connect his workstation to the wired LAN.[10] [T. Jämsä, V. Hovinen, A. Karjalainen, J. Iinatti]

D. Eavesdropping

Eavesdropping is prevented by using the WEP algorithm which is a Pseudo Random Number Generator initialized by a shared secret key. This PRNG outputs a key sequence of pseudo-random bits equal in length to the largest possible packet which is combined with the outgoing/incoming packet producing the packet transmitted in the air.

The WEP is a simple algorithm based on RSA's RC4 which has the following properties:

1. **Reasonably strong:** Brute-force attack to this algorithm is difficult because every frame is sent with an Initialization Vector which restarts the PRNG for each frame.
2. **Self Synchronizing:** The algorithm re-synchronizes for each message. This is necessary in order to work in a connection-less environment, where packets may get lost (as any LAN).

III. FTP (File Transfer Protocol)

File Transfer Protocol (FTP) is a standard network protocol used to copy a file from one host to another over a TCP/IP-based network, such as the Internet. FTP is built

on client-server architecture and utilizes separate control and data connections between the client and server. Client applications were originally interactive command-line tools with standardized command syntax, but graphical user interfaces have been developed for all desktop operating systems in use today. FTP is also often used as an application component to automatically transfer files for program internal functions. FTP can be used with user-based password authentication or with anonymous user access.

The objectives of FTP, as outlined by its RFC, are:

- To promote sharing of files (computer programs and/or data).
- To encourage indirect or implicit use of remote computers.
- To shield a user from variations in file storage systems among different hosts.
- To transfer data reliably, and efficiently.

The protocol is specified in RFC 959, which is summarized below.

A client makes a TCP connection to the server's port 21. This connection, called the control connection, remains open for the duration of the session, with a second connection, called the data connection, opened by the server from its port 20 to a client port (specified in the negotiation dialog) as required to transfer file data. The control connection is used for session administration (i.e., commands, identification, passwords) exchanged between the client and server using a telnet-like protocol. For example "RETR filename" would transfer the specified file from the server to the client. Due to this two-port structure, FTP is considered an out-of-band, as opposed to an in-band protocol such as HTTP

The server responds on the control connection with three digit status codes in ASCII with an optional text message, for example "200" (or "200 OK.") means that the last command was successful. The numbers represent the code number and the optional text represent explanations (i.e., <OK>) or needed parameters (i.e., <Need account for storing file>). A file transfer in progress over the data connection can be aborted using an interrupt message sent over the control connection.

FTP runs over the Transmission Control Protocol (TCP). Usually FTP servers listen on the well-known port number 21 (IANA-reserved) for incoming connections from clients. A connection to this port from the FTP client forms the control stream on which commands are passed to the FTP server and responses are collected. FTP uses out-of-band control; it opens dedicated data connections on other

port numbers. The parameters for the data streams depend on the specifically requested transport mode. Data connections usually use port number 20.

In active mode, the FTP client opens a dynamic port, sends the FTP server the dynamic port number on which it is listening over the control stream and waits for a connection from the FTP server. When the FTP server initiates the data connection to the FTP client it binds the source port to port 20 on the FTP server.

In order to use active mode, the client sends a PORT command, with the IP and port as argument. The format for the IP and port is "h1,h2,h3,h4,p1,p2". Each field is a decimal representation of 8 bits of the host IP, followed by the chosen data port. For example, a client with an IP of 192.168.0.1, listening on port 49154 for the data connection will send the command "PORT 192.168.0.1". The port fields should be interpreted as $p1*256 + p2 = \text{port}$, or, in this example, $192*256 + 2 = 49154$.

In passive mode, the FTP server opens a dynamic port, sends the FTP client the server's IP address to connect to and the port on which it is listening (a 16-bit value broken into a high and low byte, as explained above) over the control stream and waits for a connection from the FTP client. In this case, the FTP client binds the source port of the connection to a dynamic port.

To use passive mode, the client sends the PASV command to which the server would reply with something similar to "227 Entering Passive Mode (127.0.0.1)". The syntax of the IP address and port are the same as for the argument to the PORT command.

In extended passive mode, the FTP server operates exactly the same as passive mode, however it only transmits the port number (not broken into high and low bytes) and the client is to assume that it connects to the same IP address that was originally connected to. Extended passive mode was added by RFC 2428 in September 1998.

While data is being transferred via the data stream, the control stream sits idle. This can cause problems with large data transfers through firewalls which time out sessions after lengthy periods of idleness. While the file may well be successfully transferred, the control session can be disconnected by the firewall, causing an error to be generated.

A. Remote FTP

Where FTP access is restricted, a remote FTP (or FTP mail) service can be used to circumvent the problem. An e-mail containing the FTP commands to be performed is sent to a remote FTP server, which is a mail server that parses

the incoming e-mail, executes the FTP commands, and sends back an e-mail with any downloaded files as an attachment. Obviously this is less flexible than an FTP client, as it is not possible to view directories interactively or to modify commands, and there can also be problems with large file attachments in the response not getting through mail servers. The service was used when some users' only internet access was via email through gateways such as a BBS or online service. As most internet users these days have ready access to FTP, this procedure is no longer in everyday use.

IV ADVANTAGES AND APPLICATIONS

The main Advantages are:

- **Expert Technology Services:** By partnering with Wireless Integrated you ensure a expert technology services for your WiFi Radio requirements. We help you select the right technology, offer wide product range and be successful in your High-Technology business
- **Low hardware cost:** Every WiFi Radio project seek very low cost of RF sensors, remotes and controllers along with assured range and performance. Products and designs from us shall cost you nearly 75% cheaper than market prices. We significantly reduce your Total Cost of Operations and guarantee range and performance.
- **Customized solutions:** Your large customers will ask for customization, addressing their unique problems and offer exclusive services. This will require you to have complete control over your infrastructure and ability to customize your products as per requirements. We offer this capability to you.
- **Software cost:** Most customers delay their RF automation plan because they are not able to get right range, performance, price and consultants for successful implementation. Wireless Integrated offer you all this in single package.

The main applications are:

- **Used in Modem Industries:** Wireless testing tool is used in many Wireless modem manufacturing company to test the various capabilities of modem like signal strength, Bandwidth, throughput etc.
- **Used in Simulation software:** Various simulation software provides wireless testing tool to test the connectivity and capability.
- **Used in Mobile manufacturing Industries:** Various mobile manufacturing Industries use wireless testing tool to test the handset capability and wireless connectivity.
- **Used by Various Service Provider:** Wireless testing tool are also used by various mobile

service provide to test the dataflow and also Internet service provider (ISP) uses wireless testing tool.

- **Used in WLAN Environment:** Wireless testing tool is used in various WLAN environments to test the WLAN features are working efficiently or not.

V. CONCLUSIONS

A reliable, repeatable methodology is required for comparing wireless networks. Agencies need tools in order to compare technologies and evaluate deployments. The methodologies developed in this project provide some options for DOTs and other agencies.

Wireless testing tools provide a straightforward method for quantifying the performance of wireless links across single and multiple hops. They do have some shortcomings in terms of mobile handoffs and how they measure UDP throughputs. Ping utilities such as HRPING provide a very high time resolution in order to properly evaluate wireless handoffs. The current tools are not the most user friendly and do require some post processing in order to extract useful data [2].

VI. REFERENCES

- [1] Pablo Brenner, "A Technical Tutorial on the IEEE 802.11 Protocol" BreezeCOM © 2007.
- [2] Dr. Aaron Schroeder "Wireless Testing Protocols", A research Project Report for Center ITS, A U.S. DOT University. (c)2006.
- [3] "Xirrus XN8 WI-FI Array" A device-level Performance and functional evaluation, © 2010 Tolly Enterprises.
- [4] "Enterprise wireless LAN competitive testing", Performance results of Industry, © 2008 Jones-Petric.
- [5] "A test report on WiMax based Broadband wireless access technology", © 2005 China Motion Telecom.
- [6] "Lab Testing report on 802.11 Wireless Optimization" (c) 2009 Miercom.
- [7] Patrick Wiederkehr, "Approaches for Simplified Hotspot logins with wi-fi devices", © 2009 ETH Switzerland.
- [8] L. Hentila, M. Narandzic, J. Meinila, "Measurement based parameter extraction for WINNER radio channel model, Proc. of the XXIX General Assembly of the International Union of Radio Science (Union Radio Scientifique Internationale-URSI), Chicago, USA, Aug. 07-16, 2008.
- [9] X. Zhao, J. Meinilä, L. Hentilä, T. Jämsä, P. Kyösti, J-P Nuutinen, "Effects of Noise Cut for Extraction of Wideband Channel Parameters", (Invited Paper) Proc. IEEE Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 07).
- [10] T. Jämsä, V. Hovinen, A. Karjalainen, J. Iinatti, "Frequency Dependency of Delay Spread and Path Loss in Indoor Ultra-Wideband Channels, Proc. The IET Seminar on Ultra Wideband Systems, Technologies and Applications, Savoy Place, London, UK, Apr. 20, 2006.