Title

Active Measurements on Wireless LAN

Authors

Ivan Maric
SRCE - University Computing Center
J.Marohnica b.b. , 10000 Zagreb, Croatia,
E-mail: ivan.maric@srce.hr

Mario Klobucar
SRCE – University Computing Center
J.Marohnica b.b. , 10000 Zagreb, Croatia,
E-mail: mario.klobucar@srce.hr

Igor Velimirovic
CARNet –Croatian Academic and Research Network
J.Marohnica b.b. , 10000 Zagreb, Croatia
E-mail: igor.velimirovic@carnet.hr

Abstract

CARNet (Croatian Academic and Research Network), in cooperation with FER (Faculty of Electrical Engineering and Computing) and SRCE (University Computing Center) has established a test wireless network, which connects several nodes using wireless local area network technology (Wireless LAN, IEEE 802.11b, DSSS). In order to test real transport characteristics of such established network, active measurements are performed. Connection is tested with IP/UDP traffic, generated with a software traffic simulator. Description of test bed is given in this paper, together with characteristics of transport system, plan of the test measurements and description of used tool (traffic generators, measurement techniques). Results of performed measurements are presented and analyzed, together with some conclusions.

Keywords

Wireless LAN, IP traffic measurement

1. Introduction

Since the Institute of Electrical and Electronics Engineers (IEEE) proposed standard for wireless LANs (IEEE 802.11 [1]) in 1997, many manufacturers deployed this standardized technology in area of wireless connectivity for data traffic. In 1999, IEEE 802.11b [2] standard proposed even higher data rates comparing to IEEE 802.11 (5,5 or 11 Mbps comparing to 1 or 2 Mbps) and it was clear that wireless technology has become very interesting solution for implementing network connectivity in the range from local area networks (LAN) to metropolitan area networks (MAN). Rapid growth of computer networks, operating over IP protocol (Internet) demanded some testing on how effectively those wireless networks can transport IP traffic, how reliable are those networks in terms of IP connectivity and what is really a useful bandwidth in terms of the IP traffic load.

CARNet (Croatian Academic and Research Network) in cooperation with FER (Faculty of Electrical Engineering and Computing) and SRCE (University Computing Center) implemented the test wireless network [4] connecting several nodes using wireless local area network technology. Plan of active measurements was established later. Several IP traffic generators were used to generate traffic load, in order to test wireless links up to their limits. Measurements have shown values of useful bandwidth (IP traffic load) and some other characteristics of links that are important for IP networks.

2. Description of technology, equipment and measuring techniques

Since the testing took place on the network that was already implemented and operational [4], there were some parameters that could not been changed, like number of devices in the network, distances between nodes, and so on. In this chapter description of the test network is given, followed by overview of used technology, device description and measuring techniques.

2.1 Wireless standard and operative modes

The technology that has been used to implement wireless LAN is described in IEEE 802.11b standard, built upon the 802.11 standard, working at the speed of up to 11 Mbps at 2.4 GHz band. This standard proposes functionality similar to standard wired Ethernet (IEEE 802.3), but because of specific medium access protocol - CSMA/CA (Collision Avoidance), compared to standard wired Ethernet - CSMA/CD (Collision Detection protocol) on MAC layer, the expected performance of traffic speed is lower. On the physical layer direct sequence spread spectrum (DSSS) is used, enabling speed of 11 Mbps. The frequency band used in this case (2.4 – 2.4835 GHz) is still unlicensed and available in Croatia.

Another important issue was security. IEEE 802.11 standard offers several layers of security, but it was important to implement encryption for the purpose of this testing, so WEP (Wire Equivalent Privacy) encryption was enabled on all devices during the testing. Therefore, devices are tested in the wireless network with the encryption turned on, as in real-life situations when security is demanded by end-users.

Two different operative modes were used: point-to-point (two devices with directional antennas) and point-to-multipoint (one Master device with omni-directional antenna and three other Slave devices with antennas directed to Master). Since one of the main goals of the testing was to compare two different devices included in implemented network, it was clear that devices should be compared only when operating in the same operative mode.

2.2 Equipment

Basic characteristics of two tested devices from different manufacturers are given in the Table 1:

Device	Manufacturer	Model	Encryption	Notes
A	Cisco	Aironet BRI340 Series 11Mbps WAN Ethernet Multipoint Bridge	128 bits (WEP)	Used in point-to-point operative mode
B	Lucent	WavePOINT II Wireless Bridge Orinoco ROR	64 bits (WEP)	Point-to-multipoint implemented with one omni-directional antenna on Master device

Table 1. Characteristics of tested wireless devices

As one of the main goals of the testing was to compare two different devices included in implemented network, it was clear that devices should be compared only when operating in equal operative mode. Device A was installed only in point-to-point configuration, so all comparisons between devices A and B were done analyzing results of point-to-point measurements. When device B operated in point-to-point mode, all other devices (of type B) in that segment were shut down, in order not to impact the measurements of two devices currently tested.

Device A was installed in the following configuration:

- Cisco-Aironet BRI340 Series 11Mbps WAN Ethernet Multipoint Bridge
- Aironet Yagi Mast Mount Antenna
- Aironet loss-low Antenna Cable
- Aironet Lighting Arrestor
- Aironet RP-TNC assembly

Device B was installed in the following configuration (on FKIT location omni directional antenna, on other locations directional antenna):

- Lucent Wireless Bridge Orinoco ROR
- Orinoco Card 11Mbps
- Antenna Lucent (omni directional or directional) OMNS10
- Lucent Pigtail cable
- Lucent Lighting Protector
- Lucent N-male connector
- Lucent Low Loss Cable

2.3 Traffic generators and measurement technique

Some simple software traffic generators were used to generate IP traffic. Those generators were standard PCs (Intel 486, Linux OS with program ***mgen*** *[3]*), but because of relatively weak processing power of PCs and some limitations of *mgen* program, the maximum speed of generated traffic did not exceed 8.5 Mbps. Since maximum values of actual transmitted traffic via wireless devices were well below that speed, that limitation was not a problem in this testing. Generated IP traffic was UDP, and several different values of packet size were used: 100, 200, 500, 1000 and 1400 bytes. Traffic generator tool (*mgen)* was configured in a way that for each packet size value, number of packets was increased in small steps, thus slowly increasing total traffic load. Here is a typical script that shows mgen generated traffic, in 60 seconds period, for packet size of 1000 bytes:

```
START 00:10:00
0      1  ON   192.168.100.10:10  PERIODIC  5   1000
60000  1  MOD  192.168.104.10:10  PERIODIC  8   1000
120000 1  MOD  192.168.104.10:10  PERIODIC  11  1000
180000 1  MOD  192.168.104.10:10  PERIODIC  14  1000
240000 1  MOD  192.168.104.10:10  PERIODIC  17  1000
300000 1  MOD  192.168.104.10:10  PERIODIC  20  1000
360000 1  MOD  192.168.104.10:10  PERIODIC  23  1000
420000 1  MOD  192.168.104.10:10  PERIODIC  26  1000
480000 1  MOD  192.168.104.10:10  PERIODIC  29  1000
540000 1  MOD  192.168.104.10:10  PERIODIC  32  1000
600000 1  MOD  192.168.104.10:10  PERIODIC  35  1000
660000 1  MOD  192.168.104.10:10  PERIODIC  38  1000
```

Measuring of transmitted and received packets was done on Ethernet switches for a specific segment of the network (specific interface). The number of received/transmitted packets has been collected via SNMP protocol in periodic fashion (every minute during the testing interval) and stored with a timestamp in the database for later analysis. Data was gathered using *scotty* [5] extension of TCL language [6]. The results were stored in mSQL database [7] using msqltcl [8] database interface.

2.4 Description of the test network

Two separate test beds were used. Device A was tested in the point-to-point operative mode, on location FER and FKIT. Device B was tested in the point-to-multipoint mode: Master (M) device was installed on location FKIT, and three Slave devices, on locations marked as PRAVO, ARHIV and IMO (see Figure 2). On Figure 1 the part of Zagreb city map is presented, with all locations specially marked:

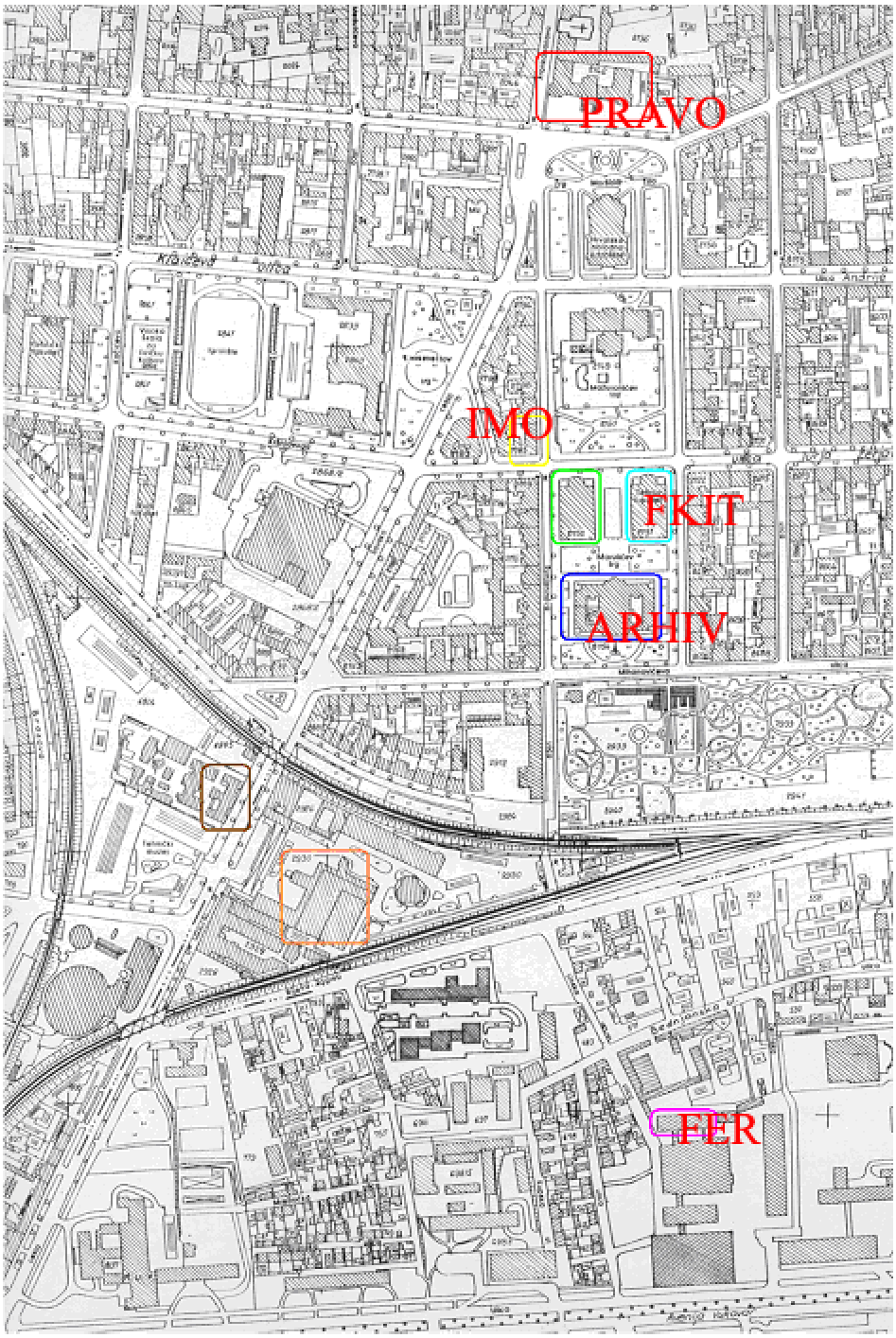


Figure 1. Zagreb city map with marked nodes of tested network

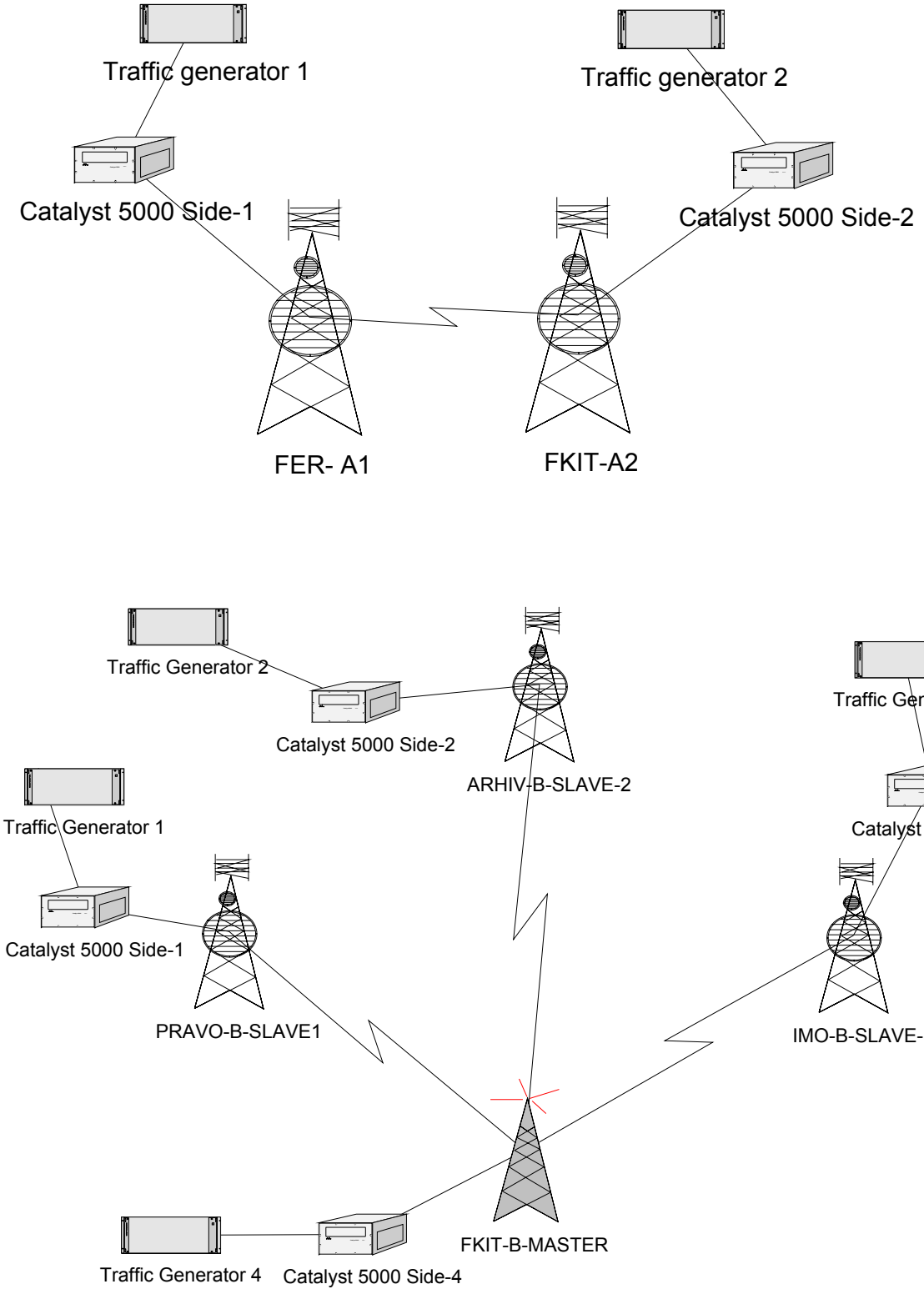
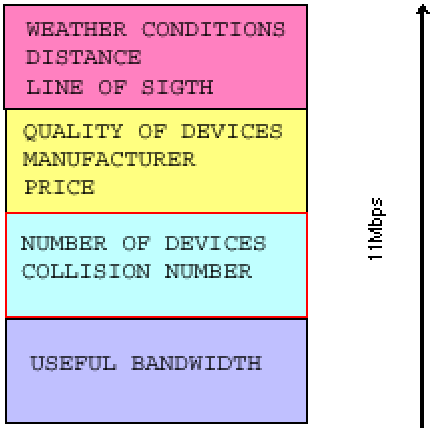


Figure 2. Test network scheme

The line of sight was established between all locations. Physical distances between locations were as follows (color of each location on Figure 1. corresponds to the color of location code name in a the Table 2):

Link	Distance (m)
FER-FKIT	620
FKIT –PRAVO	390
FKIT –IMO	130
FKIT –ARHIV	100

Table 2. Characteristics of wireless devices



Expected results: expecting the nominal speed of 11 Mbps is not realistic. The reasons are partly in specific medium and protocol on MAC layer (CSMA/CA), while other parameters are weather conditions, quality of equipment, number of devices connected in WLAN that share the same medium, etc.
The diagram shows some parameters that can limit actual transport speed.
From the diagram it is clear that some parameters are under the control of a network designer (type and quality of devices) but some parameters are predefined and are not under direct control (distances, weather and other conditions, number of nodes, etc.)

3. Results

Measurements were done in 3 separated tests as follows:

- Test in laboratory (device A)
- Test on location, point-to-point (device A)
- Test on location, point-to-multipoint (device B)

3.1 Test in laboratory (device A)

The first test was done in laboratory conditions. Measurement took place in a room, using device A (equipped with the standard antenna for home installation), with the distance between devices 3 meters. Measurements with small packet size did not reach full capacity of devices (for packet size of 100 bytes traffic generator was capable generating 2 Mbps max.). Devices were configured in a way that one device was set up as a Master device, and other device as a Slave device. In point-to-point operative mode maximal speeds of transmitted traffic were as follows:

- **7 - 7.5 Mbps** in one direction (traffic only in one direction, Master to Slave or Slave to Master)
- **3 Mbps** bi-directional (traffic in both directions, **6 - 6.5 Mbps** total amount of traffic)

In all tests when traffic in both directions was present (traffic generator on both side of wireless link generating UDP packets), some interesting results have been noticed. In a situation where total amount of traffic reached about 6 Mbps, Master device (previously set up by configuration) got priority, and was able to transmit more traffic towards Slave device than vice versa. This feature could be used on links with asymmetric traffic load, which is a typical situation on most links in CARNet network. Figure 3 shows results from the tests with traffic flow in both directions and packet size of 1400 bytes.

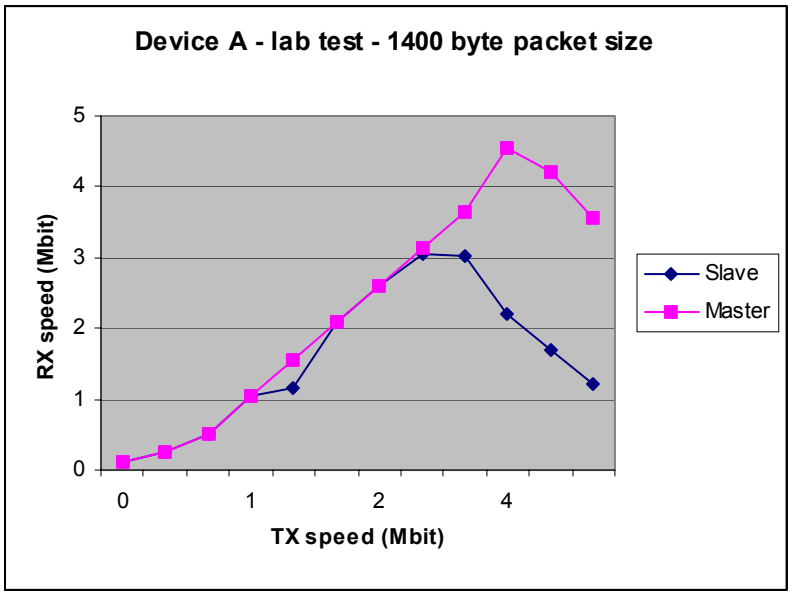


Figure 3. Results of device A testing in laboratory conditions, packet size 1400 bytes

3.2 Test on location, point-to-point (device A)

Measurements on installed equipment (devices on FER and FKIT) were done in 3 different modes:

- One direction from Master device (FER) to Slave device (FKIT), test mark M->S
- One direction, from Slave device to Master device, M<-S
- Both direction, from Master to Slave and vice versa, M<->S

Maximum traffic load transmitted in the whole WLAN (sum of all received packets) was up to **7 Mbps** (for packet size of 1000 and 1400 bytes) while minimal speed was **1.75 Mbps** (small packets, 100 bytes). The main reason for such difference is in encryption (128 bit), which influences traffic with smaller packets much more than traffic with bigger packets.
The summary of testing results (maximum transmission speed) for device A is presented on Figure 4.

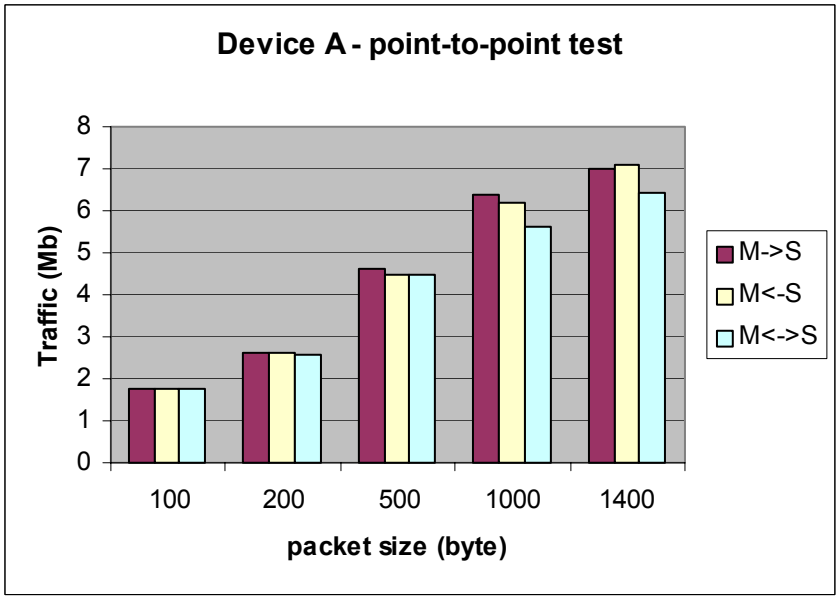


Figure 4. Point-to-point test – device A

3.3 Test on location, point-to-multipoint (device B)

Measurements were done on four devices: Master device on location FKIT (M) and 3 Slave devices (S, on locations PRAVO, ARHIV, IMO). Three different modes of traffic generation were used:

- One M and one S device (M->S, M<-S, M<->S) in point-to-point mode
- One M and two S devices (M->2S, M<-2S, M<->2S)
- One M and 3 S devices (M->3S, M<-3S, M<->3S)

Maximum traffic speed transmitted in the whole WLAN (sum of all received packets) was up to **4.4 Mbps** (for packet size of 200 bytes) while minimal speed was **1.8 Mbps** (packet size 1000 bytes).

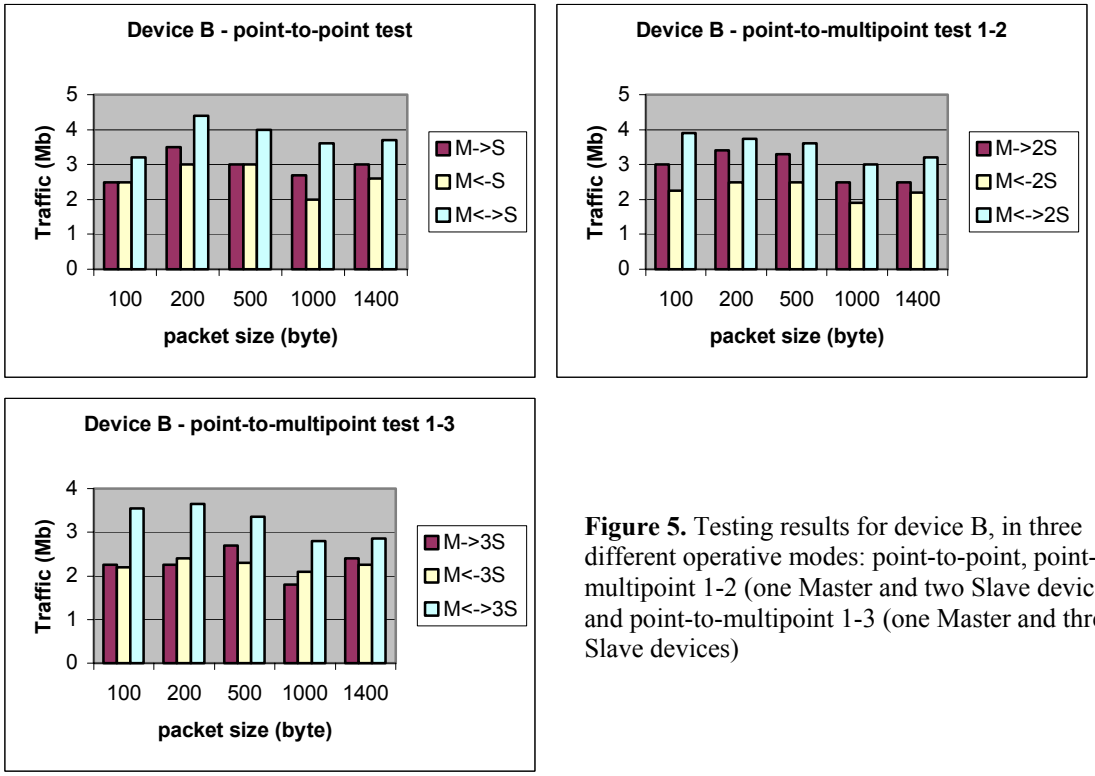


Figure 5. Testing results for device B, in three different operative modes: point-to-point, point-to-multipoint 1-2 (one Master and two Slave devices) and point-to-multipoint 1-3 (one Master and three Slave devices)

4 Result analysis

Comparison of two tested devices (A and B) is done only in point-to-point operational mode, since device A was implemented only in such a configuration. When comparing these two devices and measurement results, it should be kept noted that devices did not work in equal conditions: they were tested on different places with different antennas, but these parameters had to be taken as they were.

From the measurement results following conclusions can be extracted (Figure 4.):

1. Device A has shown much better transmit speed in all occasions. The only exception when device B had better results was in test with very small packets. The reason can be in different encryption technique used on each device: 128 bits encryption on device A vs. 64 bits encryption on device B.
2. Device A shows characteristic of priority balancing of the traffic to Master device, which can be advantage in real situation (asymmetric load). Device B shows no difference in load balancing between Master and Slave device.

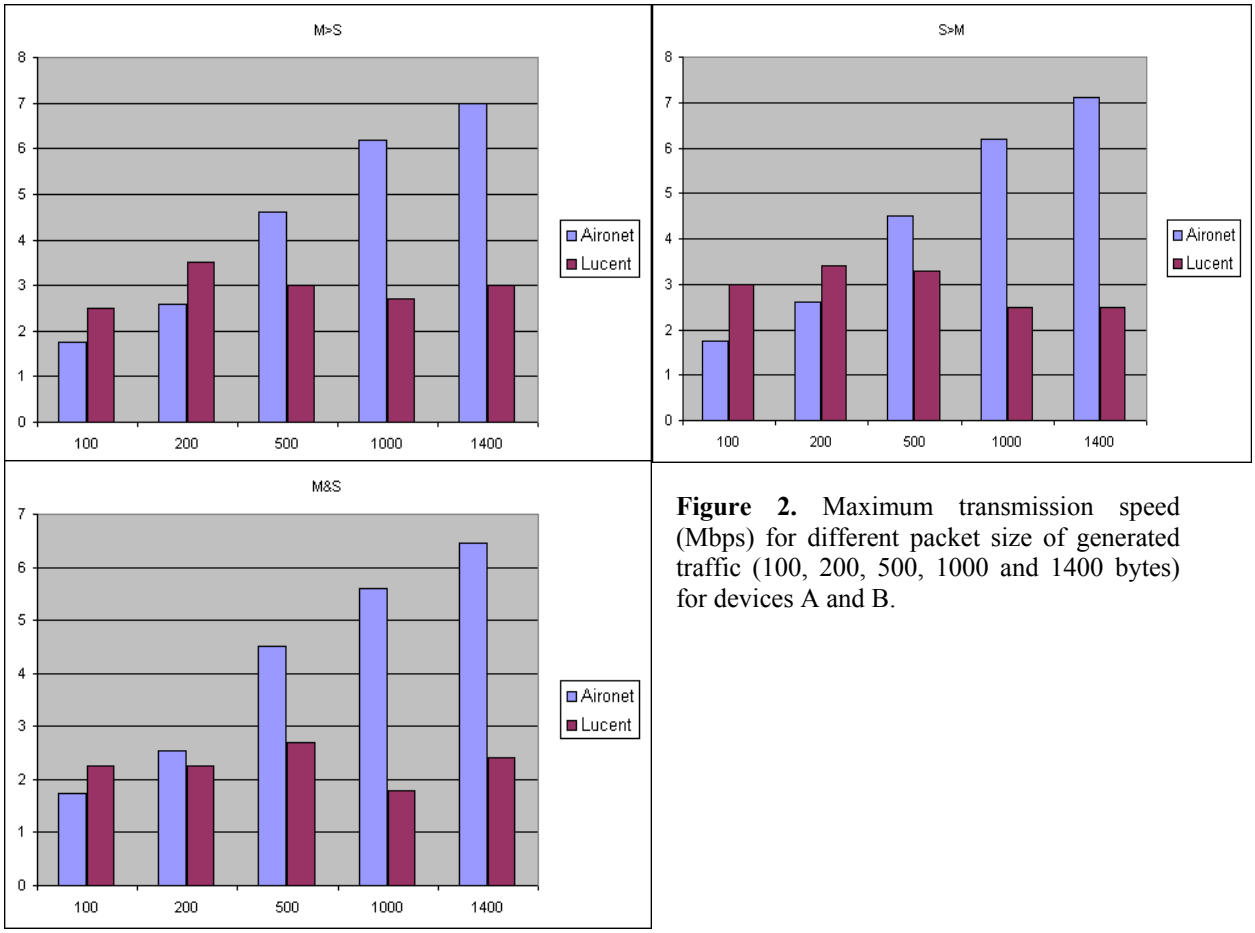


Figure 2. Maximum transmission speed (Mbps) for different packet size of generated traffic (100, 200, 500, 1000 and 1400 bytes) for devices A and B.

5 Future work

The focus of measurements described in this paper is how effectively can wireless links, built on IEEE 802.11b standard, transport IP traffic in the conditions of maximum traffic load.

Future work will be focused on time parameters (round trip time, response time, etc.) in order to see what are the limitations for time-sensitive applications like IP multicast, high quality voice and video over IP, etc. Especially, in order to test links on application level, some end-to-end testing will be performed, rather than node-to-node, as it was done in this measurements. Interoperability between different manufacturers is also an interesting topic for future research.

6 References

[1] IEEE Std 802.11, 1999 Edition (ISO/IEC 8802-11: 1999) IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Network - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, available at http://standards.ieee.org/reading/ieee/std/lanman/802.11-1999.pdf

[2] IEEE 802.11b-1999 Supplement to 802.11-1999,Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band, available at http://standards.ieee.org/reading/ieee/std/lanman/802.11b-1999.pdf

[3] "Multi-Generator" (MGEN) Toolset, The Naval Research Laboratory (NRL), available at http://manimac.itd.nrl.navy.mil/MGEN/

[4] D.Simunic, L.Flatz, B.Drilo, I.Maric: Idejno rjesenje izvedbe bezicne podatkovne povezanosti CARNet lokacija (project documentation of CARNet wireless test network, available at request, Croatian language only)

[5] Scotty - Tcl Extensions for Network Management Applications, available at http://wwwhome.cs.utwente.nl/~schoenw/scotty/

[6] TCL – Tool Command Language, available at http://www.tcltk.com

[7] Mini SQL (mSQL) lightweight relational database, available at http://www.hughes.com.au/products/msql

[8] msqltcl: Tcl/Tk interface to the Mini-SQL (mSQL) database server, available at http://www.soder-labs.com/msqltcl/

7 Vitae

Ivan Maric has been active in the area of computer networks since 1990. He received B. Sc. (1990) from the University of Zagreb. Since 1990 he has been working for SRCE (University Computing Center) at Croatian Academic and Research Network - CARNet, where he is responsible for development and operations. Currently he is Deputy Director and CTO of University Computing Center.

Mario Klobucar has been active in the area of computer networks since 1996. He received B. Sc. (1996) from the University of Zagreb. Since 1996 he has been working for SRCE (University Computing Center) at Croatian Academic and Research Network - CARNet. Currently he is the Head of Network Department of University Computing Center. Main area of his work is development, building and maintenance of the computer communication infrastructure.

Igor Velimirovic is the Chief of Network Monitoring and Measuring Department of CARNet – Croatian Academic and Research Network. He works for CARNet for the last 5 years, since he graduated on Faculty of Electrical Engineering and Computing. Main area of his work is network management, and main interests include performance management, especially active and passive measurements on IP networks.