

## Efficient Building to Building Communication

Jonathan White, Aaron Arthurs  
*University of Arkansas*  
{jlw09, ajarthu} @uark.edu

### Abstract

*In this experiment, we examine several aspects of building to building communications. The attributes that we are concerned with are the length of the link between the buildings (varying between a few meters to a few kilometers), the type of the link (wired 100BaseT Ethernet, frame relay, Token Ring, and wireless Ethernet), and general topology of the connection (either switch or router based connection).*

*Different link types have very different characteristics at different distances. Some of these characteristics aren't well known, and if a business wants to have effective communication between sites, they need to know how their performance will be affected as different variables change. We hope to present information that would be useful to businesses that are planning to make a building to building link.*

### 1. Introduction

The demand for efficient communication is a must in today's data oriented society. Corporations are faced with several choices when coordinating their network. Several goals come to mind for networks such as low cost, high thru-put, reliability, and scalability. For small businesses, a network may be contained within a single office while for large corporations, a network may (and typically does) span multiple sites. The distance between each site varies from neighboring buildings to international communications.

Two problems arise when establishing connection between each site; both problems are directly related to the distance of the connection. One problem is intrusion or unwanted disclosure of information. The other problem is having an erratic/unpredictable connection. The latter problem is influenced by long distance and an inappropriate type of link (as there are many different types of links available). Corporations need information about the performance drop off for various link types as the distance between buildings gets larger.

Besides connecting several sites together, there is also the problem of distributing the connection throughout a site. For an existing site, wired resources tend to be limited, if

not costly to have installed. Also, setting up wireless connections may be difficult depending on the site's building material (e.g. thick concrete blocking high-frequency signals). For a new site, the network topology must be planned ahead of time.

The information about maximum run lengths is quite extensive in the literature. Companies have been running long lines for years, and the maximum run lengths for the various protocols is fairly established. For example, the maximum run length in 10BaseT Ethernet is 100 meters, for 10BaseF using fiber optic cables, the maximum run length is 2000 meters [3]. For Token Ring, the maximum length is 45 meters for unshielded twisted pair, and 101 meters for shielded wires [5]. FDDI runs can extend for a much greater distance, up to 100 kilometers [4]. Wireless protocols vary greatly in the distance that they can provide. Using off the shelf equipment, typically distances that can be traversed are in the .5 to 1 mile range. However, much larger distances in the 25 mile range have been done [6].

Under OPNET Modeler 9.1, we will construct multiple scenarios based on a network cluster connected to another network cluster. Performance and reliable connections will be measured using OPNET's simulator. The scenarios will include varying distances between the two clusters, Ethernet, T1, Frame Relay, SONET, 801.11b/g wireless, and VPN connection types, and hub/switch/router-type inter-connecting nodes in each cluster.

For simplicity, only one parameter (i.e. distance, link type, cluster inter-connecting devices) will vary while observing connection speeds and collisions. For example, given the distance is 100 meters and switches are used, compare the speed and number of collisions between an Ethernet and wireless connection.

Companies have so many options to choose from when deciding on a building to building link. Information about how different protocols suffer at different lengths would be a great benefit. For example, how efficient is 10BaseT Ethernet at links greater than a kilometer? We hope to answer these questions and more.

This paper is organized as follows. In section 2, we present information regarding Token Ring. Section 3 covers FDDI and section 4 covers wired Ethernet. Section 5 covers wireless Ethernet. Section 7 contains a chart that summarizes how the differing link types suffer at different distances. Finally, we conclude our research in Section 6 and we present our works cited in section 8.

## 2. Token Ring

The Token Ring technology was developed by IBM in the 1970's. It is a token passing network; meaning that only the station that has the token has the right to transmit. If the station that receives the token has nothing to transmit, it simply passes the token to the next station. Each station can hold the token for some predefined maximum time. Token Ring was designed this way to eliminate collisions between packets.

If a station does wish to transmit a packet, it alters the first bit of the token, appends its information and transmits this information to the next station on the ring. The next station examines the destination, and it will forward the packet to the next station in the ring if it isn't the final destination. There are control bits in the packet's header to ensure that no packet goes around the ring forever. While an information frame is circling the ring, no other tokens are allowed to be on the network. Token Ring does use a priority system that allows certain stations to use the network more frequently. This is done by using a priority field in the packet's header. A station that has a priority equal to or greater than the priority value in the token that is being passed can set a bit in the token to reserve the token for the next pass around the ring.

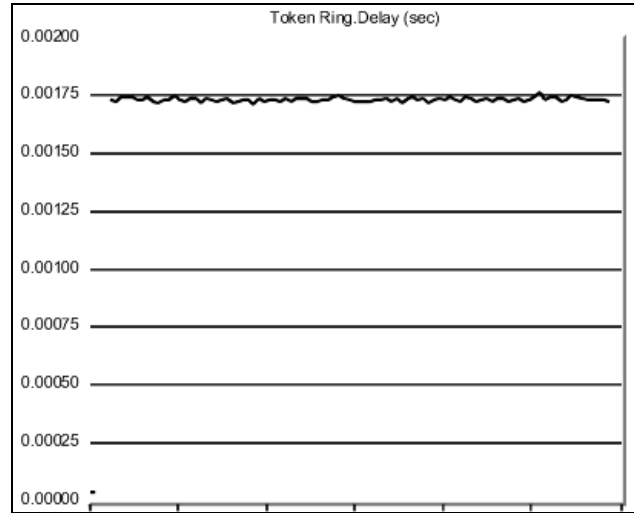
IBM's Token Ring is nearly identical to the IEEE 802.5 specification. In fact, the specification was modeled after Token Ring. The major differences are that Token Ring specifies a star as a topology and twisted pair as the physical medium. The IEEE 802.5 specification doesn't specify this. Token Ring support a data rate of 4.16 Mbps, making it one of the earliest broadband technologies.

One of the advantages of Token Ring is that it is deterministic, meaning that it is possible to calculate the maximum time that will pass until a station can transmit. Token Ring also has several reliability features that make Token Ring ideal for networks in which the delay must be predictable and the operation of the network must be very robust.

From our simulations, we found several problems with Token Ring as a business to business communication

link. We didn't really expect Token Ring to be a viable option, as from the get go we knew that it didn't support a high data rate and also that it would only run over twisted pair copper.

Using OPNET, we did confirm that Token Ring produced almost no collisions. This was a benefit.



**Figure 2.1: Delay is fairly constant in Token Ring. This example is for a link that is 100 meters in length.**

However, we also found that Token Ring was very slow and had a large delay as the link between buildings got larger. Token Ring produced the largest delay all of the technologies we tested. Also, since the data rate was only 4.16 Mbps, we didn't get a high throughput. Token Ring is not a viable option for building to building communication.

## 3. FDDI

The Fiber Distributed Data Interface (FDDI) technology was developed in the mid 1980's to fill a need in the network backbone area. In the mid 1980's, high end engineering workstations were beginning to tax the bandwidth of existing networks that were based on Ethernet and Token Ring. Also, network reliability had become more of an issue as mission-critical applications were moved from large mainframe computers to networks. FDDI has several characteristics that fit these needs.

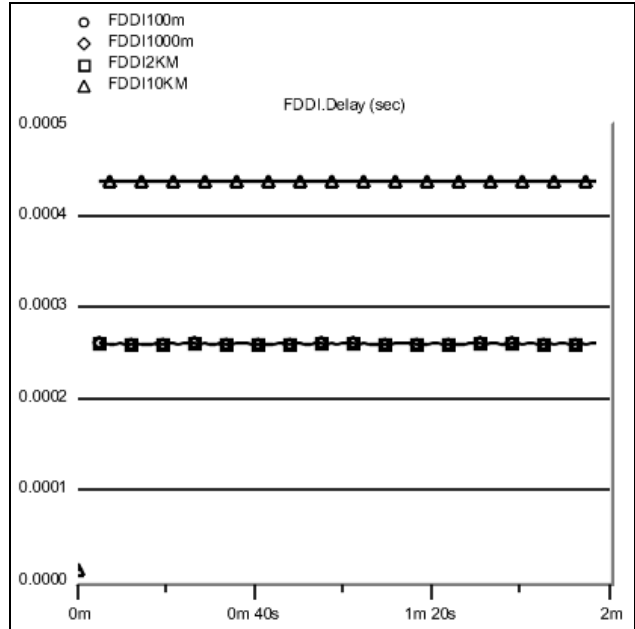
FDDI specifies a 100 Mbps token passing, dual-ring LAN that uses fiber optic cable as the transmission medium. FDDI supports very large distances between stations; up to 2 kilometers for multimode fiber optic cable, and as far as 10 KM for single mode fiber. This was a great benefit for the designer who wished to network together buildings that were separated by a large distance.

FDDI uses a dual-ring architecture consisting of a primary and a counter rotating secondary ring. The primary ring is used to send and receive packets during normal operation and the secondary ring remains idle as a backup. The secondary ring is only used if there is a fault in the primary ring. When a single device fails, devices on either side of the failure wrap around, forming a single ring. Devices still on the ring operate as normal. FDDI only provides fault tolerance against a single failure. When 2 or more failures occur, the FDDI ring segments into 2 or more independent rings.

FDDI specifies the physical and media access layers of the OSI model. This provides high-speed connectivity between upper layer protocols such as TCP/IP. In this way, it is similar to Ethernet and Token Ring.

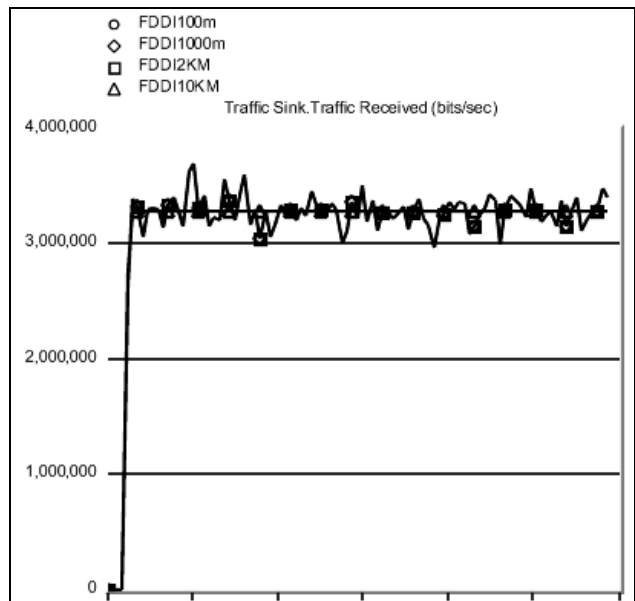
FDDI is unique in that it defines several ways in which devices can attach to the ring. A single-attachment station (SAS) attaches only to the primary ring through a concentrator. If an SAS device fails, it has no impact on the ring. A dual-attachment station (DAS) has ports that attach to both the primary and secondary rings. A failure in a DAS does affect the ring as a whole. A concentrator is the building block of an FDDI network. It attaches to both the primary and secondary rings and ensures that the ring doesn't fail when a device like a PC powers down.

We simulated an FDDI environment in OPNET, and we were very pleased with the results and a building to building communication link. As the following graph shows, the delay was constant for the 100 meter to 2 kilometer range. Only when much greater distances were traversed (10 Km) did the delay begin to fluctuate. See Figure 2 for the graph. The delay was also fairly constant for the lower distances, due to FDDI being a token passing technology. The delay was also very small.



**Figure 3.1: FDDI Delay Note that the delay is fairly constant for distances less than 10 Km.**

FDDI also supported a high data rate across a large link. In fact, the data rate didn't really go down as the distance of the link increased. It fluctuated by about 7 percent, but this was not really noticeable. Figure 3 shows the results we obtained from OPNET. Note that at greater distances, the traffic received fluctuates, but it is still close to the maximum amount.



**Figure 3.2: FDDI Traffic Received Rate**

In conclusion, FDDI seems to be a great technology for a building to building or building to WAN communication link. From our research, we have found it to be reliable, and it is very capable of sustaining a high data rate at large distances.

#### 4. Wired Ethernet

The choice of physical layer protocol is 100baseT. Two topologies are used: a single mid-switch, and a dual mid-switch; also, the following distances are used: 100, 500, and 10000 meters. In each topology, the two nodes communicate via a hub to the switch system using the following traffic generation parameters. Each node is always in the "ON" state (packet generation is allowed), uses exponential interarrival times (.005 seconds), and uses a constant packet length of 1000 bytes. Based on the traffic generation parameters, the data rate transmitted by each node is calculated by Equation 4.1, which results to 1.6 Mbps.

$$\text{Equation 4.1: Individual\_Data\_Rate} = \text{Packet\_Size} * 8 * (1 / \text{Interarrival\_Time})$$

Under ideal conditions, the data rate received by each node is 1.6 Mbps; furthermore, because two packet-generating/receiving nodes (a.k.a. end nodes) are involved, the aggregate data rate is twice the individual data rate (3.2 Mbps or 400 packets/second). The same holds true for other measurements such as end-to-end delay and packets sent.

$$\text{Equation 4.2: Aggregate\_Data\_Rate} = \text{Number\_End\_Nodes} * \text{Individual\_Data\_Rate}$$

The connection from each node to its hub is set to negligible; that is, the propagation speed is set to the speed of light ( $300 \times 10^6$  meters/second) and the propagation delay is set to zero. In contrast, the connection from each hub to the switch has minimum propagation speed ( $0.585 * \text{speed of light}$  or  $175 \times 10^6$  meters/second) and has propagation delay directly related to the distance of the wire.

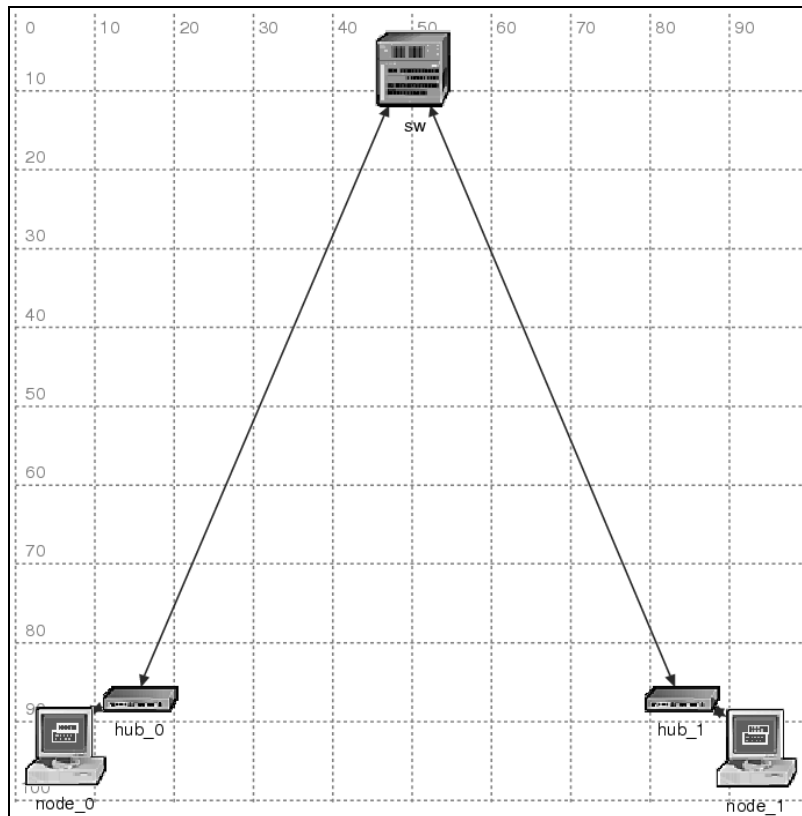
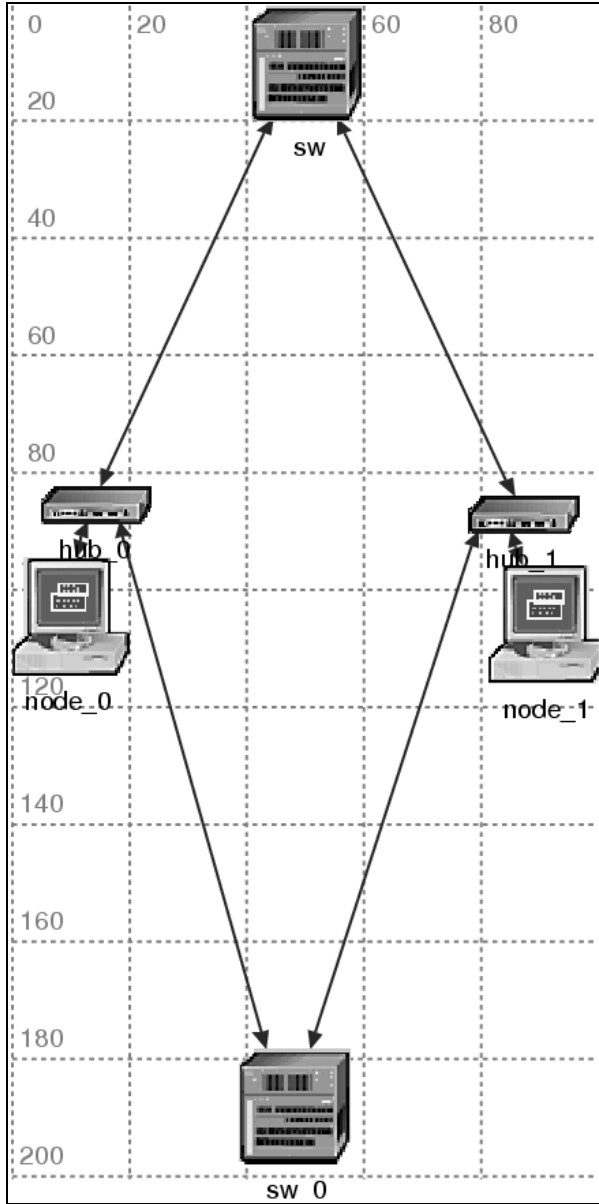


Figure 4.1. 100 meter, single-switch system, wired Ethernet

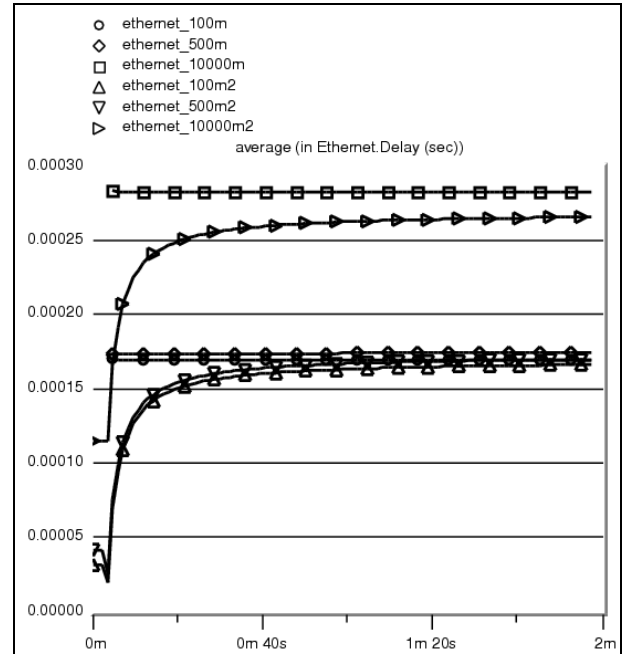


**Figure 4.2. 100 meter, dual-switch system, wired Ethernet**

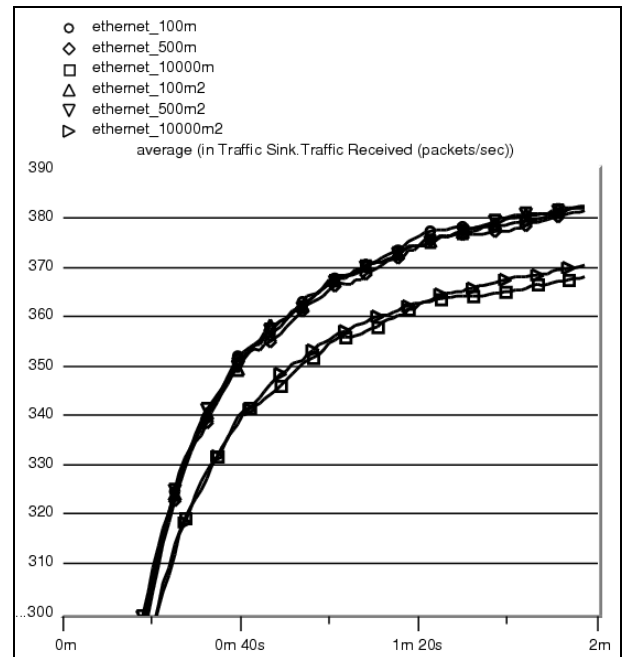
After simulating each scenario, the following measurements are made and compared. The first measurement observed is the end-to-end delay. Figure 4.3 shows the average delay between node\_0 and node\_1 over a 2-minute interval. Note that the naming convention for each scenario is ‘ethernet\_<DISTANCE>[2<if dual-switch>]’ (e.g. ‘ethernet\_500m2’ means 500 meter distance per hub-to-switch link and is dual-switched).

The end-to-end delay certainly increases as the distance increases. However, the delay is greater for single-switch than dual-switch. The difference in delay

between single and dual-switch increases as the distance increases. For example, there is a significant gap at 10000 meters between the delay of the single and dual-switch topologies.



**Figure 4.3. Average aggregate-delay for each wired scenario.**



**Figure 4.4. Average aggregate-traffic rate received for each wired scenario.**

Another measurement observed is the aggregate traffic rate received (in packets/second), shown in Figure 4.4. Again, distance affects this measurement in that increased distance reduces the traffic rate received. There is, on the other hand, a small (if not, negligible) difference in traffic rate between the two switch topologies. Using the simulation results, one form of utilization can be calculated using Equation 4.3. In the case of ‘ethernet\_10000m’, the traffic rate utilization of the network at two minutes is about 92% (368 packets/second divided by 400 packets/second).

Equation 4.3:  $Utilization\_Traffic\_Rate = Traffic\_Rate\_Received / Traffic\_Rate\_Sent$

A slight variation of traffic quantity considered is the aggregate traffic received (in packets), shown in Figure 4.5. Distance still has the same impact as with the aggregate traffic rate received, but at 10000 meters, the traffic received in the dual-switch topology is somewhat higher than the single-switch network. Another form of utilization is derived in Equation 4.4. Based on simulations, the average, aggregate traffic sent is found to be 480 packets at each time. As an example, the traffic utilization of ‘ethernet\_10000m’ at two minutes is about 95% (459 packets / 480 packets); whereas, ‘ethernet\_10000m2’ at 2 minutes has a traffic utilization of 96% (463 packets / 480 packets).

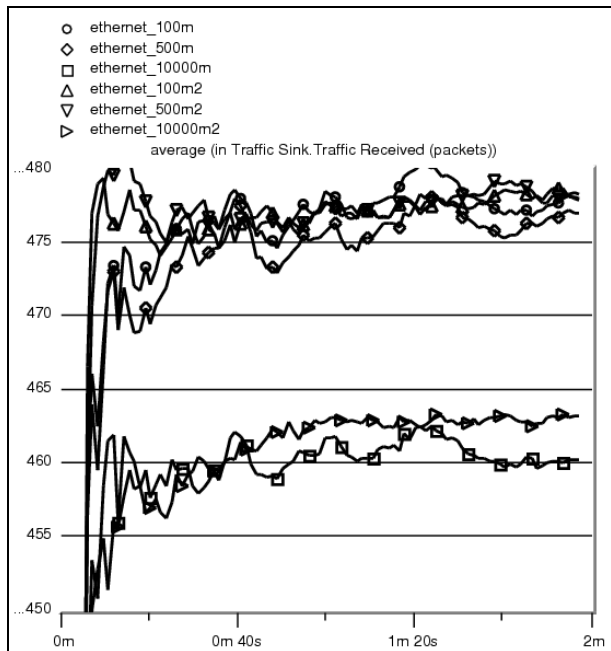


Figure 4.5. Average aggregate-traffic received for each wired scenario.

Equation 4.4:  $Utilization\_Traffic = Traffic\_Received / Traffic\_Sent$

One final observation made is the number of collisions detected by each end node, shown in Figure 4.6. Once again, increased distance increases collision count. However, the distance also affects which topology results with more collisions. In the case of 10000 meters, the single-switch topology shows a higher collision count as compared to the dual-switch topology. As for the case of 500 meters, the dual-switch network results with higher collision counts than the single-switch network.

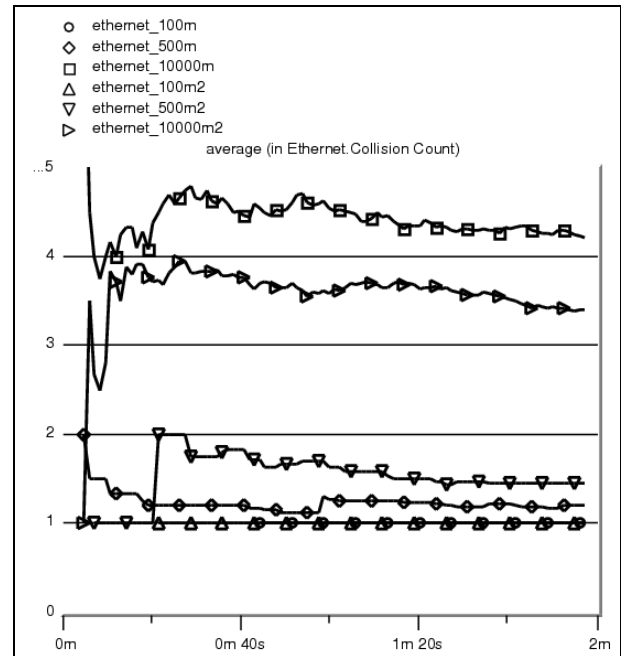


Figure 4.6. Average number of collisions detected by each end node for each wired scenario.

To conclude the results found for wired Ethernet, the dual-switch topology outperforms the single-switch topology only at a large distance (10000 meters in this case). At a small distance, the single-switch network is preferred.

### 5. Wireless Ethernet

For wireless Ethernet (wireless-LAN), two wireless-enabled end nodes send/receive packets; packet generation is set the same as in Section Wired Ethernet. The physical characteristics of each end node are similar to the 802.11b standard (see Figure 9.3). Frequency hopping spread spectrum (FHSS) is chosen because it is more resilient to interference than direct sequence spread spectrum (DSSS) [6]. The resilience to

interference is important because of the long distances between end nodes.

The scenarios are created such that they vary by distance and the middle node, if present. Using an ad hoc structure, the two end nodes are separated by distances of 100, 1300, and 2000 meters. The middle node, which has the same physical characteristics as the end nodes, is placed halfway between. Furthermore, the middle node's packet generation is set to either 'on' or 'off' in separate scenarios (i.e. the middle node either generates its own packets or simply reflects incoming packets).

The measurements taken in the simulations are different from the wired Ethernet simulations because of the wireless technology. One quantity taken is the number of collisions detected. For wired Ethernet and some radio systems, CSMA/CD (carrier sense multiple access with collision detection) is used [2]. For wireless Ethernet, the IEEE 802.11 MAC layer specifications are based on the CSMA/CA (carrier sense multiple access with collision avoidance) scheme [1]. With this in mind, the simulations measure the number of retransmission attempts by each node in place of collision detection for the wireless Ethernet scenarios.

Besides the difference in the technology used the idea of whether the middle node is present or not affects whether the aggregate measurements are justifiable or comparable with other scenarios. For instance, the aggregate traffic rate received adds the traffic rate

received by each end node as well as the middle node; however, this analysis is mainly concerned with the traffic rate received by the end nodes only. For this matter, only the quantities taken for one of the end nodes are compared.

To illustrate the behavior of the aggregate measurements taken, Figure 5.3 shows the average aggregate traffic rate received in the network. The 100 and 1300 meter scenarios average around 380 packets/second when the middle node is not generating/receiving packets or is not present. When the middle node is generating/receiving packets, the aggregate traffic rate received jumps up to around 565 packets (nearly a 49% increase). This is due to a combination of the end nodes receiving traffic from the middle node and the middle node receiving traffic from the end nodes.

Moving on to the individual quantities measured, Figure 5.4 illustrates the average retransmission attempts by each node ('node\_0' is used as the reference end node). For 2000 meters, the retransmission attempts are significantly higher when the middle node is not generating/receiving packets or is not present. This is due to some of the traffic being sent by each end node to the middle node when it is in the 'on' state. When the middle node is in the 'off' state, then end nodes transmit to each other only. However, the retransmission attempts are higher for 100 and 1300 meters when the middle node is turned on, possibly from interference from the middle node.



Figure 5.1. Two-node wireless topology.

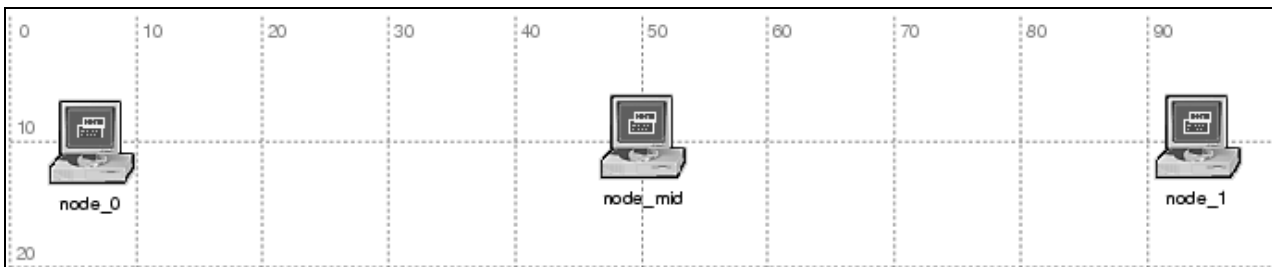


Figure 5.2. Two-node wireless topology with middle repeater (either packet-generating or not).

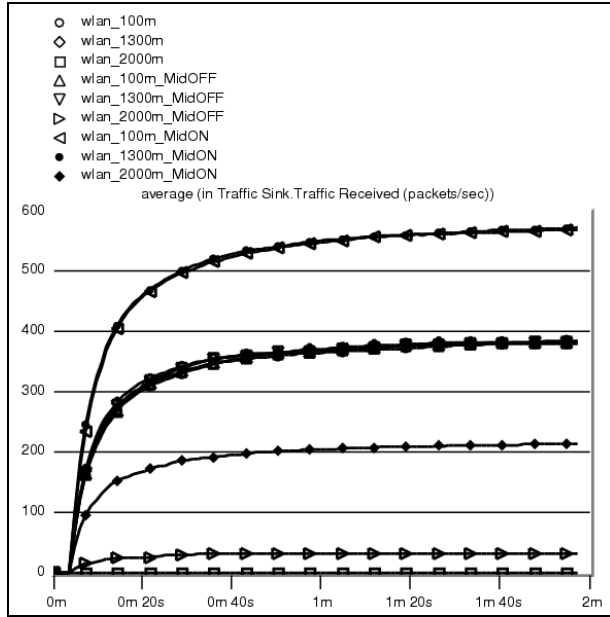


Figure 5.3. Average aggregate-traffic rate received for each wireless scenario.

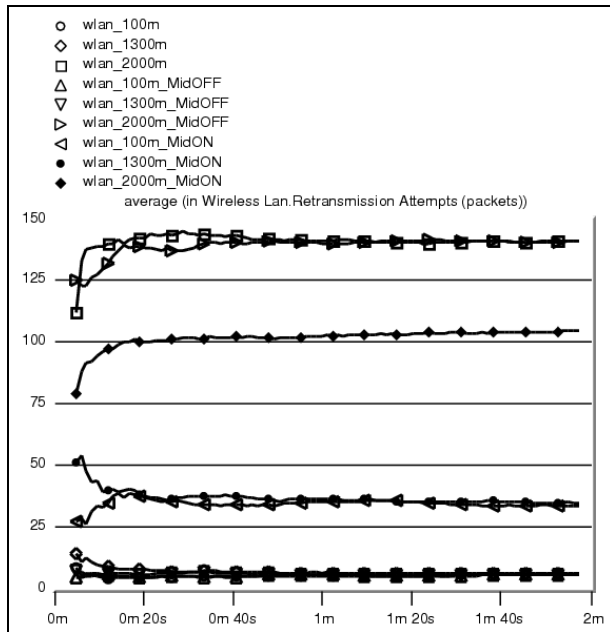


Figure 5.4. Average number of retransmission attempts made by each node for each wireless scenario.

Taking a look at Figure 5.5, the 100 and 1300 meter scenarios show more throughputs when the middle node is not present or when the middle node is in the ‘on’ state. For 2000 meters, there is throughput only when the middle node is turned on. An interesting observation is the fact that including a middle that is turned off reduces the throughput by an average of 50%.

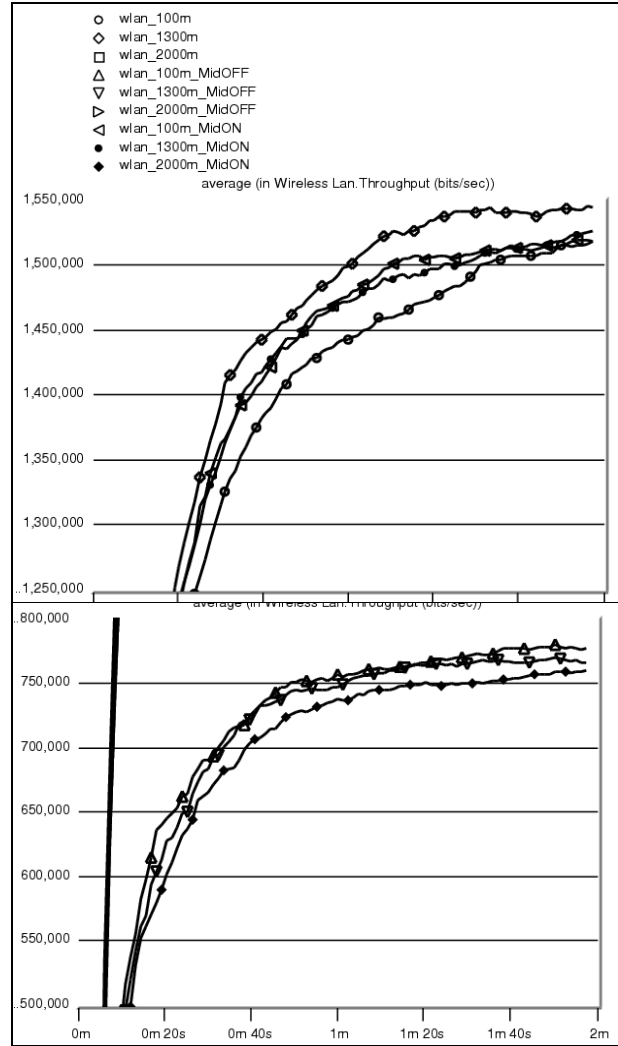


Figure 5.5. Average throughput of each node for each wireless scenario (wlan\_2000m and wlan\_2000m\_MidOFF have a throughput of 0 bps).

Another measurement observed is the average dropped packet rate of each end node (Figure 5.6). Only at 2000 meters does the dropped packet rate show a non-zero value. Among the 2000 meter scenarios, the scenario with the middle node turned off shows the lowest dropped packet rate.

A final quantity measured is the average load of each end node, which represents the average number of packets queued in each node’s receive buffer at that time (Figure 5.7). The same behavior results as with the dropped packet rate; the 2000 meter scenarios show much less performance than the other distances. Also, the 2000 meter scenario with the middle node turned off has a higher load than the other 2000 meter scenarios.

Based on the given physical characteristics, distances greater than 1300 meters may not allow for strong enough

connections among the end nodes (at least for wireless-LAN). In addition, if a middle node should exist (e.g. a building in between two buildings), having the middle node will give better performance, but less reliability (i.e. retransmission attempts).

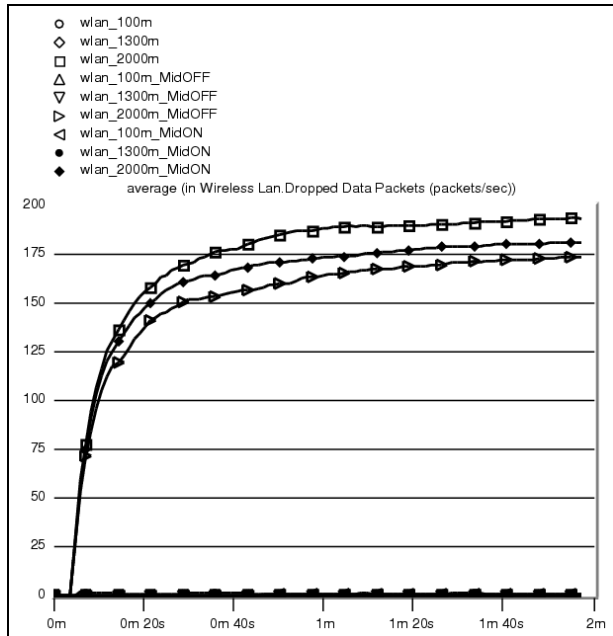


Figure 5.6. Average dropped packet rate of each node for each wireless scenario.

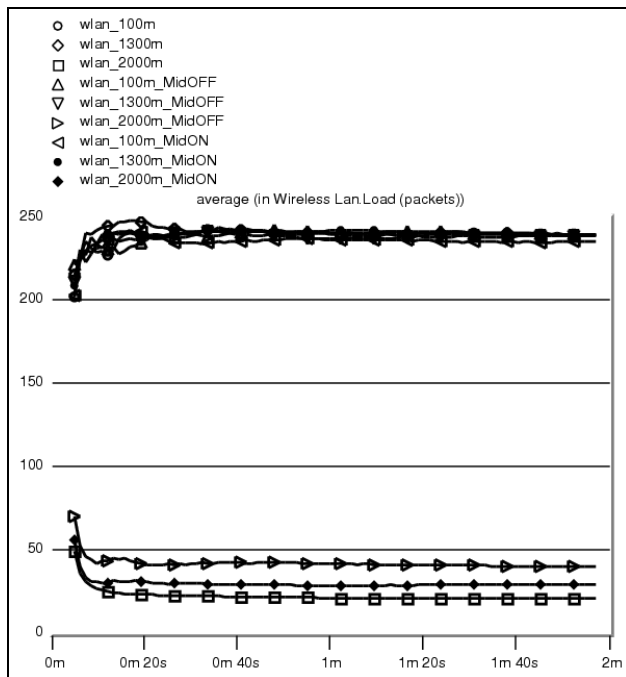


Figure 5.7. Average load of each node for each wireless scenario.

## 6. Conclusions

From our experiments, we found several interesting facts that corporations should be aware of when designing a building to building link.

First of all, businesses should try to use a fiber link whenever possible. Fiber supports such a greater data transmission rate as opposed to copper wire and wireless radio transmissions that it is well worth the investment in the wiring, if a high data rate is desired.

Companies also should be very wary about using Token Ring as their building to building link. Token Ring would be good in several environments where constant delay is a plus, but it really isn't fast enough to support a business link. Also, Token Ring suffers at large distances and it really can't be used across large distances.

FDDI, on the other hand, is a token passing technology that can be used for building to building links. FDDI is very fault tolerant, and it also supports a data rate that is suitable for organizations. If a company is looking for a token passing link, they should choose FDDI.

If Ethernet is chosen instead, a wired connection is preferred because it is more reliable and better performing than a wireless connection. On the other hand, a wireless connection may be more feasible and less costly.

### 7. Table of Recommendations

Technology	Data Rate	Cost per PC	Advantages	Disadvantages
<i>Token Ring</i>	4.16 Mbps	\$400. \$150 per NIC and \$250 for cabling.	Delay is deterministic	Slow, not good over long distances.
<i>FDDI</i>	100 Mbps	\$300 - \$1000 for NIC plus cabling.	Deterministic delay, high reliability, high data rate.	Expensive. Being supplanted by Ethernet.
<i>Ethernet (wired)</i>	Varies, typically 10/100 Mbps or 1 Gbps	Inexpensive; \$10 - \$150 for NIC plus cabling.	Least expensive, highest data rates possible, most common	Cabling must be ran
<i>Wireless Ethernet (WLAN)</i>	Varies, typically used is from 1 – 11 Mbps.	NIC is inexpensive. Other equipment ranges in price.	Can be used where others can't, can have a high data rate.	Not as fast as other technologies, not as reliable either.

### 8. References

[1] Aguayo, Daniel et. al. Link-level measurements from an 802.11b mesh network, in: *Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications*, Portland, Oregon (August 2004) 121-132.

[2] Bellamy, John C. *Digital Telephony Third Edition*. John Wiley & Sons, New York (2000).

[3] Computer Technology Documentation Project, 'Ethernet Standards',

<http://www.comptechdoc.org/independent/networking/guide/nethwethernet.html>, 2004.

[4] Fiber Distributed Data Interface [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/fddi.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/fddi.htm), Cisco Press, 2002.

[5] TokenRing/IEEE-802.5 [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/tokenrng.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/tokenrng.htm), Cisco Press. 2002.

[6] Wireless Communications. [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/wireless.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/wireless.htm). Cisco Press, 2002.

### 9. Addendum

Attribute	Value
└name	node_0
└model	ethernet_station
└x position	6.2
└y position	93.4
└threshold	0.0
└icon name	terminal
[-] Traffic Generation Parameters	(...)
└Start Time (seconds)	constant (5.0)
└ON State Time (seconds)	constant (1000)
└OFF State Time (seconds)	constant (0)
[-] Packet Generation Arguments	(...)
└Interarrival Time (seconds)	exponential (.005)
└Packet Size (bytes)	constant (1000)
└Segmentation Size (bytes)	No Segmentation
└Stop Time (seconds)	Never
└altitude modeling	relative to subnet-platform
└condition	enabled
└financial cost	0.00

Figure 9.1. End-Node's attributes for wired Ethernet.

Attribute	Value
└name	sw <-> hub_0
└model	100BaseT_adv
└transmitter a	sw.hub_tx_0
└receiver a	sw.hub_rx_0
└transmitter b	hub_0.hub_tx01
└receiver b	hub_0.hub_rx01
[+] Background Utilization	(...)
└Propagation Speed	Minimum Propagation Velocity
└arrowheads	head and tail
└ber	0.0
└color	#850000
└condition	enabled
└cost	0.0
└data rate	100,000,000
└delay	Distance Based
└ecc model	ecc_zero_err_bgutil
└error model	error_zero_err
└financial cost	0.00
└line style	solid
└packet formats	ethernet_v2
└propdel model	dpt_propdel_bgutil
└symbol	none
└thickness	1
└txdel model	eth_hub_txdel_bgutil
└user id	0

Figure 9.2. 100BaseT Link's attributes for wired Ethernet.

Attribute	Value
└name	node_0
└model	wlan_station_adv
└Destination Address	Random
[+] Traffic Generation Parameters	(...)
└Wireless LAN MAC Address	Auto Assigned
[-] Wireless LAN Parameters	(...)
└Rts Threshold (bytes)	None
└Fragmentation Threshold (bytes)	None
└Data Rate (bps)	11 Mbps
└Physical Characteristics	Frequency Hopping
└Packet Reception-Power Threshold (...)	7.33 E-14
└Short Retry Limit	7
└Long Retry Limit	4
└Access Point Functionality	Disabled
[-] Channel Settings	(...)
└Bandwidth (Khz)	1,000
└Min Frequency (Mhz)	BSS Based
└Buffer Size (bits)	256000
└Max Receive Lifetime (secs)	0.5
└Large Packet Processing	Drop
└BSS Identifier	Not Used
[+] PCF Parameters	Disabled

Figure 9.3. Wireless node's attributes.