47464

PERFORMANCE EVALUATION OF A FRAME RELAY BASED IP ROUTER TO INTERCONNECT ETHERNET LANS

by

Roy Küçükateş

B.S. in Computer Engineering, Boğaziçi University, 1993

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science
in
Computer Engineering

Boğaziçi University

1995

PERFORMANCE MODELING OF A FRAME RELAY BASED IP ROUTER TO INTERCONNECT ETHERNET LANS

APPROVED BY

Assist. Prof. Dr. Cem Ersoy
(Thesis Supervisor) .....

Assist. Prof. Dr. Sina Balkır .....

Assoc. Prof. Dr. M. Ufuk Çağlayan .....

DATE OF APPROVAL 25.7.1995

ACKNOWLEDGMENTS

I am grateful to Dr. Cem Ersoy who proposed and helped me to complete the thesis and caused me to enter to the magnificent world of Computer Networks. I thank Dr. M. Ufuk Çağlayan for his significant contributions and helps to my thesis. I thank Dr. Sina Balkır for his careful review in my thesis jury. Special thanks to my room mate Oğuz Sinanoğlu for his significant help and patience during my thesis. Thanks to Sema Oktuğ, Albert Levi, Tuna Tuğcu and to members of Network Research Laboratory, NETLAB. Many thanks to undergraduate students Günay Arslan and Emre Çelebi for their help while installing Linux on my PC. I thank Boğaziçi University Research Fund and TÜBİTAK-BAĞ for providing the financial support of this work. Special thanks to my family and friends who tolerated me during my graduate studies. Special thanks to my fiancée and future wife Karin İnceyan for her patience during these thesis months. Finally, I thank Prof. Dr. Selahattin Kuru in the names of all the members of Boğaziçi University Computer Engineering Department who educated me to become an engineer.

ABSTRACT

Many organizations have a substantial number of computers in operation. All these computers were isolated from each other. Whereas, the jobs done on these machines were strongly correlated. In order to share the computing power and special hardware as the printing machines or extensive disk storage these computers have been interconnected with Local Area Networks (LAN). For geographically distant parts of organizations and companies, the local area networks, due to electrical limitations, are impossible to use. As a solution to this problem, interconnection of LANs over a Wide Area Network (WAN) is proposed and implemented. In this thesis, a gateway is proposed as an interconnection machine. The main communication protocol of nodes in LANs is taken as Internet Protocol (IP). LANs are consisting of well known implementations of IEEE 802.3 standards: Ethernet networks. As a WAN protocol Frame Relay (FR) is proposed. FR is chosen because of its speed compared to traditional communication methods. FR is not the fastest way for interconnection but an economical and sufficient method for the problem.

In this thesis, an IP router is proposed to interconnect LANs over FR service. The design is simulated and evaluated on a powerful computer network analysis tool, OPNET, implemented by using PCs and also the system's performance is measured. This thesis covers Ethernet, FR, Internet Protocol, Routers, Ethernet to FR routing problems, computer simulation results and the implemented system's performance measurement results.

KISA ÖZET

Bilgisayarlar birçok kurumlarda kullanılır. Bütün bu bilgisayarlar birbirinden yalıtılmıştı. Bunun yanında, bu makinelerde yapılan işler arasında kuvvetli bir bağ bulunmaktadır. Yazıcı ve disk kapasitesi gibi özel donanım veya işlem gücü yüksek makinelerin paylaşımı için bu bilgisayarlar yerel bilgisayar ağlarıyla birbirlerine bağlandılar. Yerel bilgisayar ağları, elektriksel kısıtlamalar nedeniyle, coğrafik olarak birbirinden uzakta bulunan alt kurumlar veya kurumların bölümleri için kullanılamıyordu. Bu probleme çözüm olarak yerel ağların bir geniş alan ağı ile birbirine bağlanması öne sürüldü ve uygulandı. Bu tezde, bağlantı makinası olabilecek bir yönlendirici öneriliyor. Haberleşen yerel ağlardaki bilgisayarların ana protokolü olarak Internet Protokolü (IP) seçilmiştir. Yerel ağlar IEEE 802.3 standardının en popüler uygulaması olan Ethernet ağlarıdır. Geniş alan ağı protokolü olarak Çerçeve İletimi önerilmiştir. Çerçeve İletiminin seçilmesindeki ana neden tarihi haberleşme protokollerinden hızlı olması. Çerçeve İletimi haberleşmede en hızlı metod değildir, fakat problem için yeterli bir çözüm olmasının yanında ekonomik olaması da dikkati çeker.

Bu tezde, yerel ağları Çerçeve İletimi üzerinden birbirine bağlayacak bir IP yönlendirici önerilmiştir. Tasarımın bilgisayardaki benzetimi ve başarımı etkili bir ağ analiz yazılımı olan OPNET'te incelenmiştir. Tasarım, kişisel bilgisayarlar kullanılıp uygulanmış ve oluşan sistemin başarımı incelenmiştir. Bu tez Ethernet'i, Çerçeve İletimi'ni, yönlendiricileri, Ethernet'ten Çerçeve İletimi'ne yönlendirme problemlerini, bilgisayar benzetimi neticelerini ve gerçekleştirilen sistemin başarım ölçümü neticelerini kapsar.

TABLE OF CONTENTS

Page

1. INTRODUCTION 1

2. OVERVIEW OF ETHERNET BASED LOCAL AREA NETWORKS 4

2.1 IEEE 802 & ETHERNET 4

2.1.1 IEEE 802 4

2.1.2 ETHERNET 5

2.2 MEDIUM ACCESS CONTROL (MAC) SUBLAYER 6

2.2.1 FRAME STRUCTURE 6

2.2.2 COLLISION 7

2.2.3 FUNCTIONS OF MAC SUBLAYERS 7

2.3 THEORETICAL AND REAL VALUES OF ETHERNET 8

2.4 TRAFFIC CHARACTERISTIC AND PERFORMANCE 9

3. FRAME RELAY (FR) OVERVIEW 10

3.1 COMMUNICATION CHARACTERISTICS OF FR 12

3.2 BENEFITS OF FR 14

3.3 FRAME STRUCTURE OF FR 15

3.4 PROTOCOL DETAILS 18

3.5 ELEMENTS OF FR 21

4. INTERNET PROTOCOL (IP) OVERVIEW 23

4.1 IP ADDRESSING 24

4.1.1 SUBNETS 26

4.2 IP RELATED PROTOCOLS 27

4.3 INTERNET PROTOCOL (IP) 32

4.4 TRANSMISSION CONTROL PROTOCOL (TCP) AND USER DATAGRAM PROTOCOL (UDP) 37

5. ROUTERS 39

5.1 IP ROUTING LOGIC 39

5.2 REQUIREMENTS FOR INTERNET GATEWAYS 43

5.3 ROUTE DISCOVERY PROTOCOLS 43

6. DESCRIPTION OF THE TEST SETUP 46

6.1 ETHERNET-FR ROUTING PROBLEMS 49

6.2 HARDWARE USED 51

6.3 SYSTEM'S SOFTWARE 52
6.4 POINT-TO-POINT PROTOCOL (PPP) 53
6.4.1 PACKET STRUCTURE OF PPP 53
6.5 PERFORMANCE EVALUATION METHOD 54

7. PERFORMANCE EVALUATION 56

7.1 PERFORMANCE MEASURES 57
7.2 MODELING SETUPS 58
7.2.1 SETUP 1.A 59
7.2.2 SETUP 1.B 59
7.2.3 SETUP 2.A 60
7.2.4 SETUP 2.B 60
7.2.5 SETUP 3 60
7.2.6 SETUP 4 60
7.2.7 SETUP 5.A 61
7.2.8 SETUP 5.B 61
7.3 SIMULATION RESULTS 61
7.3.1 SETUP 1.A 61
7.3.2 SETUP 1.B 62
7.3.3 SETUP 2.A 63
7.3.4 SETUP 2.B 65
7.3.5 SETUP 3 68
7.3.6 SETUP 4 70
7.3.7 SETUP 5.A 71
7.3.8 SETUP 5.B 72
7.4 TEST RESULTS 74
7.5 EFFECT OF FINITE BUFFER 77

8. CONCLUSION 83

8.1 FUTURE WORK 85

9. REFERENCES 87

10. INDEX 92

LIST OF FIGURES

Page

FIGURE 2.1 IEEE 802.3 FRAME FORMAT 6
FIGURE 3.1 MESH TOPOLOGY. 11
FIGURE 3.2 LOGICAL MESH TOPOLOGY 12
FIGURE 3.3. 2, 3 AND 4 OCTET ADDRESS FIELD STRUCTURES. 16
FIGURE 3.4 FRAME STRUCTURE OF FR. 17
FIGURE 3.6. TRANSMISSION OF A FRAME OVER PHYSICAL NETWORK 20
FIGURE 4.1. CLASS A, B, C ADDRESSES (FROM TOP,) CLASS D FOR MULTICAST AND CLASS E FOR FUTURE USE. 25
FIGURE 4.2. SUBNET ADDRESSING SCHEME IN IP. 27
FIGURE 4.4. THE ARP PACKET STRUCTURE. 29
FIGURE 4.5. ICMP ENCAPSULATION. 31
FIGURE 4.6. IP DATAGRAM FORMAT. 33
FIGURE 4.7. IP FRAGMENTATION AND REASSEMBLY LOGIC. 35
FIGURE 4.8. PROPOSED FRAGMENTATION AND REASSEMBLY LOGIC FOR FR. 36
FIGURE 5.1. DIRECT AND INDIRECT ROUTING IN IP. 40
FIGURE 5.2. THE STRUCTURE OF AN EXAMPLE NETWORK. 41
FIGURE 5.3. ROUTING ALGORITHM OF IP [2]. 42
FIGURE 6.2. LANS INTERCONNECTED THROUGH FR. 49
FIGURE 6.3. THE INTERCONNECTION GATEWAYS 52
FIGURE 6.4. PPP FRAME STRUCTURE. 54
FIGURE 7.1. SETUP 1.A'S RESULTING GRAPH. 62
FIGURE 7.2. SETUP 1.A'S RESULTING GRAPH. 63
FIGURE 7.3. THROUGHPUT FOR MTU = 270 AND 1500. 64
FIGURE 7.4. THROUGHPUT CONVERGENCE FOR MTU = 270 AND 1500 FOR 1500 BYTE/PACKET 65
FIGURE 7.5. THROUGHPUT FOR MTU = 270 AND 1500. 66
FIGURE 7.6. CONVERGENCE TO MAXIMUM THROUGHPUT FOR MTU = 270 AND 1500 FOR 1500 BYTE/PACKET 67
FIGURE 7.7. COMPARISON OF DIFFERENT WAN SPEEDS VS. DELAYS. 69
FIGURE 7.8. COMPARISON OF DIFFERENT WAN SPEEDS VS. THROUGHPUTS. 69
FIGURE 7.9. SIMULATION RESULTS FOR THE IMPLEMENTED SYSTEM. 71
FIGURE 7.10. THROUGHPUT VALUES FOR THE FASTER GATEWAY. 72
FIGURE 7.11. THROUGHPUT FOR FASTER GATEWAY. 74
FIGURE 7.12. MAXIMUM THROUGHPUT OF THE IMPLEMENTED SYSTEM. 76
FIGURE 7.13. QUEUEING MODEL OF THE GATEWAY 78
FIGURE 7.14. PROBABILITY OF BLOCKING FOR INCOMING PACKETS 80

FIGURE 7.15. PROBABILITY OF BLOCKING FOR OUTGOING PACKETS 81

LIST OF TABLES

	Page
TABLE 2.1 IMPORTANT FIXED PARAMETERS OF ETHERNET.	8
TABLE 2.2 IMPORTANT USER DEFINED PARAMETERS OF ETHERNET	8
TABLE 3.1. ADDRESS FIELD BITS AND THEIR MEANINGS	17
TABLE 4.1. ADDRESS CLASSES AND THEIR RANGE.	25
TABLE 4.2. ARP PACKET FIELDS AND THEIR MEANINGS.	29
TABLE 4.3. ICMP TYPE FIELD VALUES AND THEIR INTERPRETATIONS.	32
TABLE 4.4. IP DATAGRAM FIELD NAMES AND INTERPRETATIONS.	34
TABLE 5.1. GATEWAY G1'S IP ROUTING TABLE.	41
TABLE 7.1. SIMULATION RESULTS FOR SETUP 1.A.	61
TABLE 7.2. SIMULATION RESULTS FOR SETUP 1.A.	62
TABLE 7.3. THROUGHPUT FOR MTU =270 AND 1500	63
TABLE 7.4. THROUGHPUT FOR MTU =270.	64
TABLE 7.5. THROUGHPUT FOR MTU =1500.	65
TABLE 7.6. THROUGHPUT FOR MTU =270 AND 1500	66
TABLE 7.7. THROUGHPUT FOR MTU =270.	67
TABLE 7.8. THROUGHPUT FOR MTU =1500.	67
TABLE 7.9. SETUP 3 RESULTS.	68
TABLE 7.10. SIMULATION RESULTS FOR THE IMPLEMENTED SYSTEM.	70
TABLE 7.11. THROUGHPUT FOR MTU =270 AND 1500.	72
TABLE 7.12. THROUGHPUT FOR MTU =270.	73
TABLE 7.13. THROUGHPUT FOR MTU =1500.	73
TABLE 7.14. THROUGHPUT VALUES FOR DIFFERENT PACKET SIZES AND WAN SPEEDS.	75
TABLE 7.15 BUFFER SIZE VERSUS PROBABILITY OF BLOCKING FOR INPUT BUFFER	79

1. Introduction

Digital communication networks have started a new revolution by providing the technology that transports the data needed by a society in which information plays a key role. Many organizations already have a substantial number of computers in operation. All these computers were isolated from each other whereas the jobs done on these machines were strongly correlated. The management, then, decided to interconnect them to be able to share information, or more general, to share the resources. The goal was to make available all programs, data and equipment to anyone who has access to the network without regard to the physical location of the resource and the user. Another goal was to provide high reliability by having alternate resources of supply. In this manner, the user would not be dependent of one specific equipment. An additional goal is to save money. Small computers have a much better price-performance ratio than larger ones. This last forced designers to come up with powerful systems that would be given to each user and file servers and/or printers open to users over networks. This design caused to have many interconnected machines distributed in buildings. These networks are called Local Area Networks (LAN) [1]. One of the most attractive architectures for a local computer network is a shared, multiaccess bus with distributed control.

The networking research and development occurred in three stages. Before the 1960's the main question was, "How can we transmit bits across a communication medium efficiently and reliably?" The result was development in information theory and in signal processing. Coming to mid 1960's the emphasis shifted to packet switching and the main question became, "How can we transmit packets across a communication medium efficiently and reliably?" The result was improvements in packet switching technologies, in LANs and in statistical analysis of network response to load. From mid 1970's to the present, emphasis has centered on the network architecture and the question, "How can we provide communication services across a series of interconnected networks?" The result includes the development of internetwork technologies, protocol layering models, datagram and stream transport services, and the client-server interaction paradigm [2].

For some organizations that were located in more than one buildings and especially, for some which were spread across different cities and countries, the need for interconnection of their LANs became important. The data should be available for everyone in the organization. The solution was to interconnect the LANs over a Wide Area Network

(WAN). Many ways of LAN interconnection are designed and implemented today. Most of them use lower layers of the ISO's Open System Interconnection (OSI) model [1] since most networks use this model to communicate. During the thesis we will frequently deal with the second and third layers of the OSI model. The reader is assumed to know the OSI's seven layer structure, especially the Data Link Layer (DLL) and the Network Layer. The DLL in IEEE 802 LANs is divided into two sub-layers: Logical Link Control (LLC) and Media Access Control (MAC). A more detailed discussion about these layers can be found in [1]. The necessary layers for LAN and WAN protocols will be described in Sections 2 and 3.

Currently LANs can be interconnected by using either repeaters, bridges or routers. Each one has its advantages and complexities. Repeaters duplicate the packet coming from one side to the other. Bridges are a little more complex and "intelligent." They operate at the second layer of the OSI model. They examine the source and destination addresses of a packet and if the destination is at the other side of the bridge they forward the packet to the destination network. Routers are more complex. They operate at the third layer of OSI model. They can do protocol conversion, routing, error and control management, etc.

This thesis presents the logical structure and performance evaluation of a LAN interconnection device, namely, an Internet Protocol router (IP gateway). The gateway connects two LANs over a WAN protocol connection, namely, Frame Relay (FR).

During the study, the main goal was to study the performance an IP gateway interconnecting Ethernet LANs over a fast WAN protocol. While analyzing the performance, another goal was to discover the difficulties encountered during the design of such a system, the throughput of the whole system and the end-to-end delay for a typical packet coming or going between the communicating nodes. The interconnection is modeled on a network simulation tool to study the performance of the system. Some traffic scenarios and network setups are investigated and the behavior of the system is analyzed according to these setups. FR is compared with some available protocols and products on the market by using again the simulation tool. In the analysis part of the thesis, we studied the necessary buffer sizes of the gateways in different incoming data traffics and packet sizes in order to prevent buffer overflows and unnecessary buffer allocation.

In order to compare the performance of IP gateways with the computer simulation results, we configured two PCs as IP gateways. They were fully implementing TCP/IP protocol stack and were able to route datagrams. The gateways are located between a real network and a test segment which includes a host for data collection or generation. The gateway

machines were equiped with Ethernet cards as LAN interfaces and serial ports as WAN interfaces. The gateway PCs, running Linux as the operating system, were routing the test datagrams generated from one segment, either the real network segment or the test segment, to the other part if it was the destination of the datagrams (specified in the header part of the packets) over the serial link between them. A packet generation tool is designed in our laboratory to be able to send datagrams through the gateways to the other segment. A packet collection tool is designed, again in our laboratory, to collect routed datagrams over the destination segment. The final step during the configuration was to interconnect two gateways over their serial lines, which will be described in Section 6.4.

FR is chosen as the WAN protocol in the interconnection because a FR communication card for PCs is being designed and implemented in our Computer Networks Research Laboratory (Netlab), it is cheap compared to faster protocols (such as Asyncronous Transfer Mode) and because of its speed adventage compared to slower protocols such as X.25.

In Chapter 2, an overview of Ethernet based Local Area Networks is given and protocol details are discussed. Some important parameters for Ethernet are given in this section.

In Chapter 3, an overview of WAN technologies and FR is given. The reasons for choosing FR as an interconnection media are discussed.

In Chapter 4, Internet Protocol (IP) is discussed. The protocol is described in detail. The error management, addressing mechanism, address resolution protocol (ARP) are described.

In Chapter 5, routing and performance issues of routing in a multi network environment is overviewed. The routing in Internet is described in this Chapter.

Chapter 6 involves the setup details. The need for such a system is discussed in this section. Some future work are given.

In Chapter 7, the performance evaluation methods and environments, also the performance evaluation of the system is given. Tests done on the system and measurements are given here.

The last Chapter, concludes the thesis report.

2. Overview of Ethernet Based Local Area Networks

One of the most attractive architectures for a local computer network is a shared, multiaccess bus with a distributed control. LANs allow small departmental workgroups to share applications, expensive storage and printing resources in a localized environment. The approach used in CSMA/CD is based on radio-based Aloha packet switch network developed in the University of Hawaii [1]. In Aloha the terminals were equipped with packet radios and were communicating over a shared radio channel. There was no central controller of the channel, the control was shared by all stations. In pure Aloha a host transmits whenever it has data to transfer. Two terminals transmitting at the same time produce a collision. In a collision case both of the terminals wait a random amount of time and then retransmit. The maximum utilization of this network was only 18% [3], [4].

2.1 IEEE 802 & Ethernet

2.1.1 IEEE 802

IEEE has produced a set of standards for LANs known as IEEE 802 standard. The set includes standards for CSMA/CD, token bus and token ring. They all differ in physical and MAC layers, but at LLC they are compatible. Each IEEE 802 standard describes the following:

- **802.1**: introduction to the set of standards and definition of interface primitives
- **802.2**: description of upper part of DLL which uses the LLC protocol
- **802.3**: standard of 1-persistent CSMA/CD LAN
- **802.4**: standard of token bus LAN
- **802.5**: standard of token ring LAN

2.1.2 Ethernet

The Ethernet is the most widely used LAN system based on the CSMA/CD protocol. It also formed the basis for IEEE 802.3 standard. It is an architecture that provides best-

effort datagram service with error detection but not correction. It is a multiaccess, packet-switched network with no centrally controlled, passive broadcast medium that makes the communication difficult for the stations but reduces the possibility of total network crashes.

In Ethernet, and in all 1-persistent CSMA/CDs, the station listens the channel before transmitting. If the channel is busy it waits until the channel goes idle. If channel is idle it transmits with probability 1 (coming from 1-persistence). Two stations transmitting at the same time collide. At collision both stations stop transmitting and after waiting a random amount of time, they repeat the same job.

The ancestor of Ethernet is Abramson's ALOHA system in Hawaii. Later carrier sensing was added to it and a 2.94 Mbps CSMA/CD was built by Xerox to connect over 100 stations on a single 1 km long cable. This last was the first Ethernet. It was so successful that later, Xerox, DEC and Intel formed the standard for a 10 Mbps Ethernet. This, as described earlier, formed the basis for IEEE 802.3. The difference between IEEE 802.3 and Ethernet is that IEEE is a general standard for 1-persistent CSMA/CD systems for 1 to 10 Mbps speed and on various physical media.

Generally, two types of cable are used in Ethernet: "thick Ethernet" and "thin Ethernet." All 802.3 implementations, including Ethernet use Manchester encoding. [1]

Typical features of Ethernet can be described as follows:

- Simple,
- Cheap,
- Compatible,
- Addressing flexibility,
- Fair,
- Progressive,
- High speed,
- Low delay,
- Stable,
- Maintainable,
- Layered architecture.

2.2 Medium Access Control (MAC) Sublayer

This layer consists of the control functions of the station related to the shared communication medium. It describes the packet structure, retransmission method after the collision, etc.

2.2.1 Frame structure

The frame structure used by IEEE 802.3 is given in Figure 2.1.

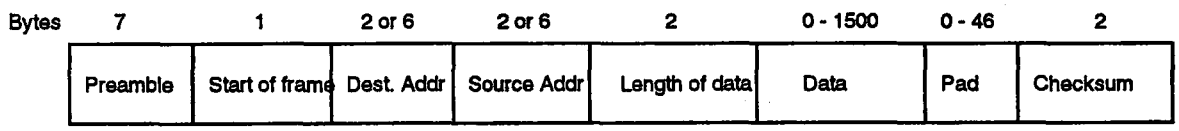


Figure 2.1 IEEE 802.3 frame format

Each frame starts with a **preamble** (7 bytes). They all contain the bit pattern 10101010. It enables the receiver synchronize its clock with the sender's. The **start of frame** byte contains the pattern 10101011. The following field is the **destination address field**. The standard allows only 2 bytes or 6 bytes addresses. But in 10 Mbps baseband standard only 6 bytes addressing is used. The length of data field contains information about the data

field of the frame, which is the following field. The **length of data** field must be between 0 and 1500 bytes. In order to distinguish valid frames from garbage 802.3 states that valid frames must be at least 64 bytes long. For this purpose the **pad** field is added. If the data field is less than 46 bytes the pad field is used to bring the length of the frame to 64 bytes. The last field is the **checksum** value field that is a cyclic redundancy check (CRC) value for the frame.

2.2.2 Collision

It was mentioned earlier about the collision of frames in a multiaccess medium. In such a case where there is no controller unit for the media there can be collisions. In CSMA/CD, more than one station transmitting at the same time cause collision. Any station detecting collision stops transmission, generates a noise burst in order to warn other stations. Wait a random time and begins transmission again. After the first collision the station waits either 0 or 1 slot time to begin retransmission. After second, it waits either 0, 1, 2 or 3 slots. After the i^{th} collision the random number is chosen from the interval 0 to 2^i-1. This algorithm is known as **binary exponential backoff**. [1]

2.2.3 Functions of MAC sublayers

The MAC layer consists of following sublayers. The functionality of the sub layers is given also.

- **Transmit data encapsulation**. Accepts data from LLC, calculates CRC and places to the appropriate field.
- **Transmit media access management**. Presents a serial bit stream to the physical layer, defers transmission when the line is busy, does collision detection and rescheduling of frame, manages the pad field and enforces collision by sending jam message.
- **Receive data decapsulation**. Performs CRC check, recognizes the address of the frame, presents data to LLC.
- **Receive media access management**. Receives the serial bit stream from physical layer, discard short frames (less than 64 bytes)

2.3 Theoretical and Real Values of Ethernet

The performance of Ethernet depends on many parameters. Some fixed parameters of the Ethernet are given in Table 2.1 in order to be able to understand the nature of the load on the network and the performance of it.

Table 2.1 Important fixed parameters of Ethernet.

Parameter	Value
Bit rate	10 Mbps
Max. propagation delay	Max. roundtrip delay between any two transmitter is 464 bit times.
Max. jam time	32-48 bit time to stop transmission after detecting the collision.
Slot time	512 bit times (51.2 microseconds)
Minimum packet length	64 bytes including header and FCS
Maximum packet length	1518 bytes
Number of hosts	100 per cable segment, 1024 for multi segmented Ethernet (totally)
Persistence	1-persistent

Besides fixed parameters, user defined parameters also affect the performance of the Ethernet. These parameters can be listed as follows (Table 2.2).

Table 2.2 Important user defined parameters of Ethernet

Parameter	Value
Packet length distribution	Bimodal. Most of them are either near max. or min. values
Actual number of hosts	Typically on the order of tens to a couple of hundred hosts
Packet arrival rate	Typically less than a few hundred of packets
Actual length of cable	May be far shorter than it is specified, e.g. a few hundred meters

For the theoretical analysis, some assumptions are made about Ethernet. These include the packet arrival distribution, topology, packet size, etc. The packet arrivals are modeled as a Poisson process, but the real traffic looks like brief packet trains after long silences. In an experiment, it is measured that 50% of all packets are followed by the next packet within 10 ms [3]. In theory, the analysis is done assuming after buffer overflow the arriving packets are discarded, whereas in the real network there exist flow-control mechanisms, so none of the packets are discarded. It is assumed that a master clock generates slot signals. In general, the minimum packet size (worst case) is used [5], [6]. Although, Ethernet provides a best effort delivery service, it does not guarantee the delivery of packets [3]. This must be checked by the upper layers.

2.4 Traffic Characteristic and Performance

The study on an Ethernet of 2.94 Mbps done by Shoch and Hupp [3] in 1980, reported seeing about 2.2 million packets per day, representing less than 1% utilization of the network capacity. Coming to the 1989, studies show that even in 10 Mbps Ethernet networks this utilization is exceeded. It is reported that in peak utilization hours the value exceeds 30% and in peak minutes more than 50% [7].

Many CSMA/CD networks have nonconstant packet lengths, and the lengths of packets transmitted before a waiting packet is retransmitted are an important factor in the delay experienced by that packet. The distribution of the packet length thus has a very serious effect upon the delay distribution [8]. Various performance, traffic characteristic and delay issues can be found in [3], [5], [6], [8].

3. Frame Relay (FR) Overview

The communication's nature is changing with the needs of business and researches. As the computing environment evolves from a host-centric model to a network-centric model, corporations are redistributing network processing and utilizing the increased intelligence of network endpoints. New protocols and communication methods are needed to take advantage of this competitive potential, creating new demands for faster and more effective networks. FR is here to meet these demands [9]. Packet switching was developed at a time when the error rate of long-distance transmissions exhibited a relatively high error rate compared to today's facilities. The solution was to add some fields to the header part of the frames so that the receiving station could correct the damaged frames. This reduced the data transmission rate of the protocols in favor of error correction. However, with modern technology the error rates are reduced. As a consequence, the new protocols do not need huge headers resulting in higher speed of communication [10].

Today's technology and applications transfer huge data and require fast protocols and lines. In order to interconnect LANs, the rates like X.25's 64 Kbps are no longer sufficient. Integrated Services Digital Network (ISDN) was developed as a solution to this new type of communication requirements. FR provides a communication speed up to 2.048 Mbps. The speed of FR is less than Asynchronous Transfer Mode (ATM) but the necessary hardware is cheaper. In FR, protocol processing overhead such as error correction and flow control operations is done at network end points. The intermediate nodes do not care about the flow control and error correction. They assume that the upper layers which are located at the end nodes take care of the error control. This behavior and the increased reliability of today's physical communication media made FR a more convenient way of cheaper and faster communication environment. FR, being a higher performance service compared to traditional packet switching is positioned by the four vendors (Northern Telecom, Digital Equipment Corp., StrataCom, Cisco) in the market as a LAN interconnection service [11], [12].

Providing LAN-to-LAN connectivity is emerging as a primary data application. The concept of connecting many LANs with bridges or routers is simple and easy to support when the number of LANs to interconnect is small. But, interconnecting becomes more and more difficult when the number increases, especially with the increasing need for networks and communication facilities. With traditional one-to-one connection methods

the cost of interconnection grows rapidly and becomes unmanageable. Such a physical mesh network can be seen in Figure 3.1. The alternative to this mesh topology is a logical mesh topology where the connection between any two router or bridge is transparent to the end-system. In this method the sites are directly connected to a network where logical mesh is transparent to the sites (Figure 3.2).

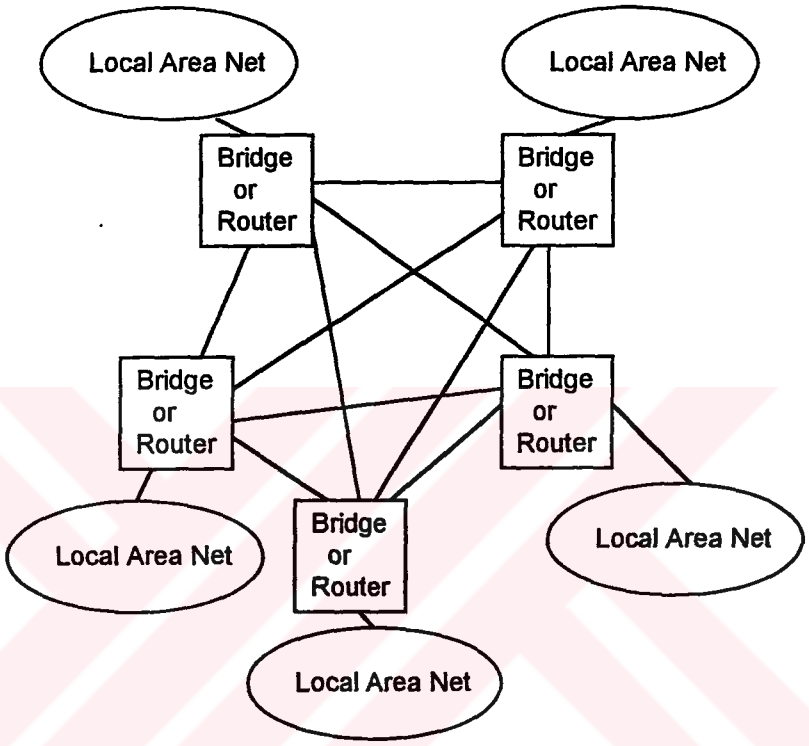


Figure 3.1 Mesh topology.

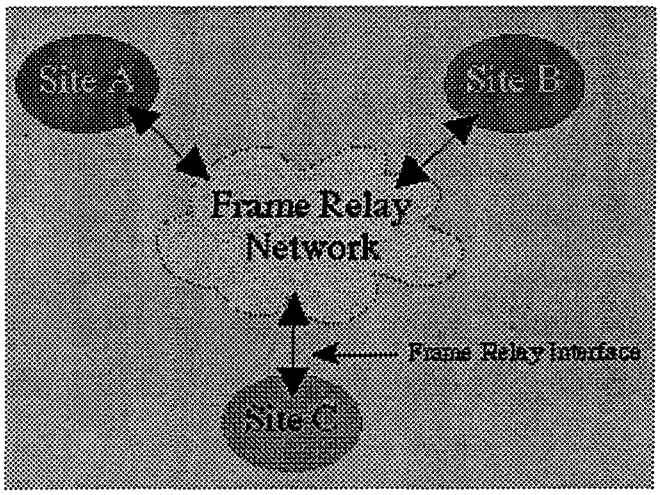


Figure 3.2 Logical mesh topology

Further introductory material can be found in [14] about FR standards, about comparison of FR and X.25 functions in [15]. An example setup: Telecom Finland FR service[16].

3.1 Communication Characteristics of FR

LANs have grown up from a conglomeration of PCs and intelligent workstations, thus pulling along with them the workstation applications with their expectations of quick response time and the ability to handle large quantities of data. The LAN pipeline, typically running at 4, 10 or 16 Mbps, is assumed to be available for these applications, so the applications typically transfer orders of magnitude more data per transaction than a typical terminal-to-mainframe transaction. Nevertheless, like their terminal-to-mainframe counterparts, the LAN applications are low duty cycle applications. They use their high LAN bandwidth intensively in bursts and then may be idle for long periods of time. The combined increase in computing power and the increased amount of information exchanged per transaction has resulted in greater application demand for high speed, low latency communications. While this may be provided by traditional dedicated-bandwidth services like T1/E1, the economics for installing a sufficient number of these circuits may be economically prohibitive.

The modernization of the public telecommunications infrastructure is quickly replacing analog facilities with high quality digital facilities often based on fiber optics. The results are increased bandwidth availability to end users for data communications and significantly reduced error rates over those experienced by analog transmission facilities. In fact, modern digital facilities can approach bit error rates of one in ten billion.

Nevertheless, today's telecom managers still face a multi-faceted problem. There is an explosion in the use of LANs. LAN-based applications are often developed at the user or department level rather than through a centralized Management Information System (MIS) group. Therefore, internetworking the growing number of remote LANs becomes even more complex. Increased bandwidth demands have resulted in higher speed, higher cost connections. To meet both the growth in data applications and the response times demanded by these applications, network bandwidth requirements are increasing. Networks must have the flexibility to handle the changing mix of traffic requirements characterized by bursty transmissions [9].

In traditional time division multiplexing and circuit switching (non-statistical methods) the network allocates a fixed amount of bandwidth (whether used or not) to the stations. Virtually all data has "silence" between transmissions. In fact, data transmissions are typically much more "bursty" than voice conversations as specified also in Section 2. Which means that in non-statistical methods a large amount of channel bandwidth is vasted. For bandwidth saving in FR, a mechanism called “bandwidth on demand” is used. In this method, the network allocates more bandwidth if the transmitter has a large burst of data to send [13].

Recent evolution in the communication technology showed that error detection, recovery and other protocol overhead is not necessarily required at the intermediate nodes. Thus, protocol processing can be left to the higher layers inherent in the transported data.

Further reading about network evolution and communication characteristics of FR can be found in [17].

3.2 Benefits of FR

The FR interface specification provides a signaling and data transfer mechanism between endpoints and the network. This interface allows communication bandwidth to be shared among multiple users, creating instantaneous bandwidth allocation on demand. Each frame (or packet) contains header information that is used to determine the routing of the data to the desired destination. This enables each endpoint to communicate with multiple destinations via a single access link to the network. Instead of fixed amounts of bandwidth allocated to the resource, FR traffic receives full bandwidth for short transaction bursts.

The benefits to the user of FR include [9]:

- **Reduced internetworking costs**, statistically multiplexed traffic from multiple sources over private backbone networks can reduce the number of circuits and corresponding cost of bandwidth in the wide area. Since FR provides multiple logical connections within a single, higher capacity physical connection, access costs are also reduced. Equipment costs may be lowered by reducing the number of port connections required to access the network. FR's DLCI addressing can allow a single FR access device to communicate as if directly attached to nearly 1000 other access devices [13].
- **Increased performance with reduced network complexity**, both by reducing the amount of processing (as compared to X.25) and by efficiently utilizing high speed digital transmission lines, e.g. statistical multiplexing and bandwidth on demand, FR can improve performance and response times of applications.
- **Increased interoperability via international standards**, FR's simplified link layer protocol can be implemented over existing technology. Access devices often require only software changes or simple hardware modifications to support the interface standard.

The advantage of FR is that the communication process is streamlined, protocol functionality at the user-network interface and the processing required by the internal network is reduced. As a result, a reduced delay and higher throughput is reached [10]. One of the additional advantages of FR over its competitors is the market demand. FR is seen by users as offering immediate solutions to real problems. One other advantage is its inherent simplicity. The FR frame is so straight-forward that equipment does not require years of engineering to be compatible [17]. Additional information about effectiveness of FR in public networks can be found in [18].

3.3 Frame Structure of FR

FR is a standardized interface protocol, as is X.25, and does not define the backbone switching protocols or topologies. The FR interface presents its data to the transmission network in a format which is consistent with LAP-D (Link Access Procedure on D channel) framing. The version of LAP-D specific to FR has been called LAP-D+, and LAP-F (Link Access Procedure for FRing services) and is generally being referred to now as LAP-E. The transmission network recognizes three core elements of LAP-E frames [13]:

- Frame delimiters (flags),
- Data Link Connection Identifier (DLCI), an addressing mechanism,
- Two-byte Cyclic Redundant Check (CRC) called Frame Check Sequence (FCS).

The packet structure of FR contain a header part, an information field (where the encapsulated data is) and a CRC field. The header part, in most common implementations include 2 octets, but 3 or 4 octet headers are also valid.

Various address field structures of FR can be seen in Figure 3.3.

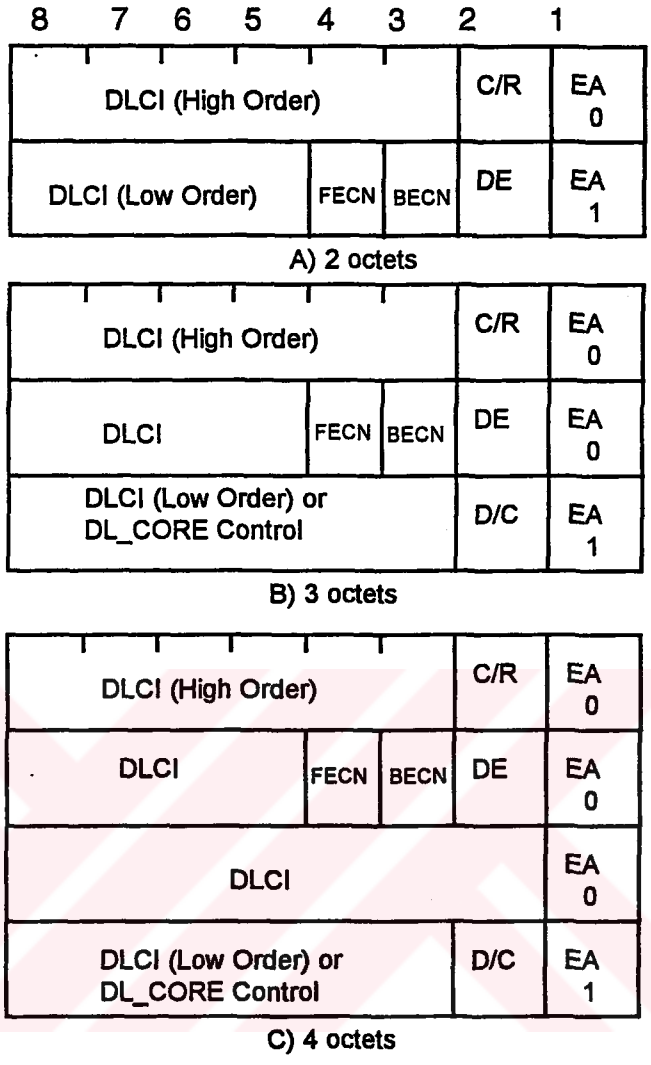


Figure 3.3. 2, 3 and 4 octet address field structures.

FR frames begin with a delimiting flag which contains the bit pattern 01111110 (7E Hex or 126 Decimal). In the specification the maximum Information Field is specified as 262 octets[12]. After the Information field the FCS value is placed. The frame ends with, again, a delimiting flag. The described frame structure can be seen in Figure 3.4.

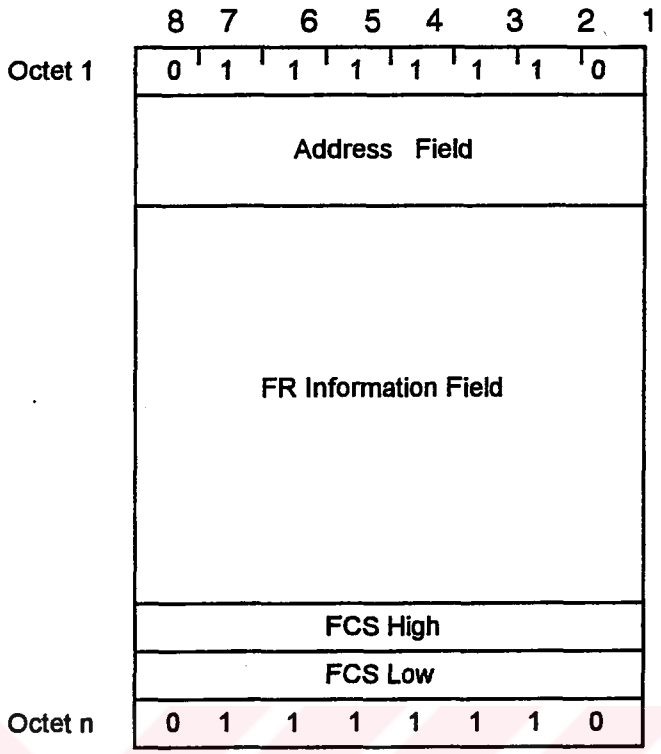


Figure 3.4 Frame structure of FR.

The meaning of the address field parts are presented in Table 3.1.

Table 3.1. Address Field bits and their meanings

Field	Meaning
DLCI	Data Link Connection Identifier. The virtual circuit number of the connection.
C/R	Command/Response. Contains 0 for command frames and 1 for response frames.
FECN	Forward Explicit Congestion Notification.
BECN	Backward Explicit Congestion Notification.
DE	Discard Eligibility. For congestion control. In congestion, frames having this bit set to 1 are suitable to be discarded.
D/C	DLCI/DL_CORE Control Indicator. Indicates whether the remaining six usable bits are DLCI bits or DL_CORE control information bits.
EA	Address Field Extension bit. If this value is reset to 0 the address field will continue in the next octet.

The address field of the frame can be one of the three choices shown in Figure 3.3. Although in the original specification the MTU (Maximum Transfer Unit) of FR is 270 octets [11] the revisited version of FR can support a maximum frame size of 1600 octets. [16] While the theoretical maximum is 4096 octets corresponding maximum integrity of FCS, the actual maximums are vendor specific [9].

The order of transmission of the frame: inside an octet bit 1 is the first bit to be transmitted.

Invalid frames for the protocol are the frames that are:

- not properly bounded by two flags,
- less than 5 octets between flags (e.g. frames not having an information field are considered invalid,)
- not consisting of an integral number of octets prior to zero bit insertion or following zero bit extraction,
- containing a FCS error,
- containing a single octet address field, or
- containing a DLCI that is not supported by the receiver.

3.4 Protocol Details

The communication in FR begins with a virtual connection establishment. Rather than requiring separate physical facilities for each conversation or connection, each communication frame contains a DLCI (Data Link Connection Identifier) that denotes which conversation "owns" that particular information or which is the connection on which the frame will travel. After the connection establishment the user device can send frames to the network (Figure 3.5). The frames contain addressing information that the network uses to determine the destination of the frame. The network device reads this information and routes the frame to the proper destination.

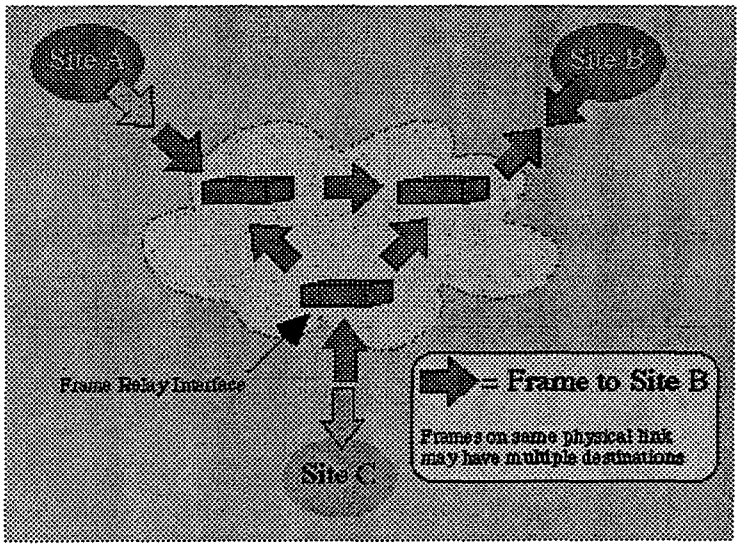


Figure 3.5. FR frames on the network.

Since FR is an interface specification only, the network may route the frames by whatever means the network builders and providers choose. In some cases, the frames are kept intact as they traverse the network. This is called "frame switching." In other cases, the frames are broken into smaller, fixed-length information units, or cells. The "cell switching" network passes the information along in small entities, then reassembles the cells into frames at the destination. These both methods are fully compliant with FR and common network architectures [9].

There are two methods of connection in FR that are very common: permanent virtual circuits (PVC) and the switched virtual circuits (SVC). In PVC, the network operator assigns the end-points of the circuit and the line behaves as a dedicated line. The intermediate nodes can change but the end-points remain the same. In SVC, the actual user of the circuit establishes a connection like a telephone call. He, specifies the destination he wants to connect and gets a DLCI number for the connection. The DLCI is permanent until the connection is closed. The advantage of these methods are that they, both, can support multiple connections over a single physical line. The specifications about the procedures of virtual call and permanent virtual circuit bearer services are I.462 (X.31) [11].

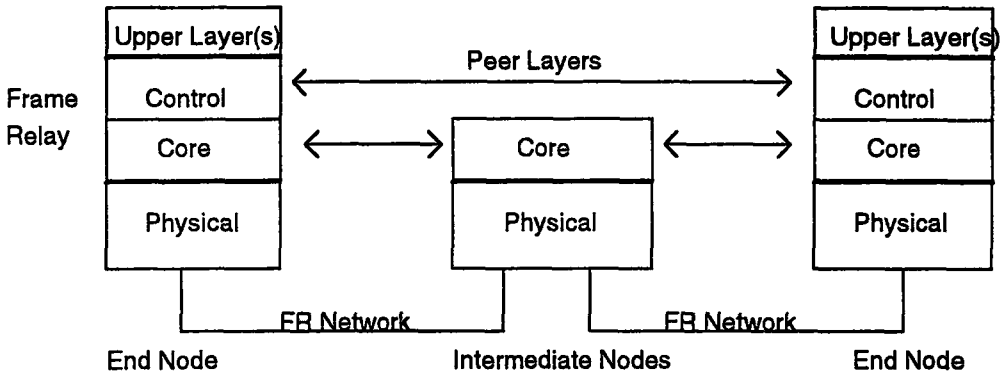


Figure 3.6. Transmission of a Frame over physical network

The stations using FR can make multiple permanent virtual circuits to different destination nodes and can send data by multiplexing the frames to different destinations at the same time. The FR communication layer consists of two sub-layers, namely Core and Control. The Core functions do not include flow control, frame acknowledge and error recovery since these functions are handled by the Control layer and performed at the end points. The transmission of a physical frame can be seen in Figure 3.6. FR speeds up the data transmission rate compared to the older communication protocols that have error recovery and flow control at each intermediate node [19].

The information field (I-field) contains the user data that is passed between devices over a FR network. The user data may contain various types of protocols (PDUs or Protocol Data Units) utilized by the access devices. The I-field may also include "multiprotocol encapsulation" according to IETF RFC-1294, an industry-standard mechanism for specifying which particular protocol is in the current I-field. With or without multiprotocol encapsulation, the protocol information sent in the information field is transparent to the FR network.

The FR interface is an access arrangement, similar to X.25, and is used at the edges, or periphery of the network. The terms of FR standards, LAP-D, LAP-E/Q.922 (LAP-F), and I.122, define PVC FR services. Q.931 standards define call setup procedures for SVC FR services. Link Access Procedure D (LAP-D) is a set of OSI Layer 2 (Link Layer) specifications for use with the ISDN [D Channel]; it is the basis for the FR standards for information transfer. LAP-D is defined by CCITT I.144/Q.921 standards. Link Access Procedure-Extended (LAP-E) or Link Access Procedure-FR (LAP-F), are names applied to an enhanced LAP-D specification, which is defined in the CCITT Q.922 standard.

FR uses only the core functions of Q.922, which include frame delimiting, alignment and transparency, frame multiplexing/demultiplexing using the address field, inspection of the frame to ensure that it consists of an integer number of octets and the inspection about max. and min. sizes of frames, FCS check, congestion control (via FECN/BECN) or Consolidated Link management (CLLM) [13], [15].

FR provides bandwidth on demand. The advantage of this behavior is that it can handle the congestion inside the network, also the bandwidth contention at the periphery of the network, optimize throughput, and enforce a system of fair sharing between multiple users.

More detailed discussion about traffic management in FR networks can be found in [20], LAN interconnection example over FR can be found in [21].

3.5 Elements of FR

FR networks are made up of three distinct elements: FR access equipment, FR switching equipment, and public FR services.

FR access equipment is the customer premises equipment (CPE) that uses FR to send information across the wide area. Access equipment may be bridges, routers, hosts, packet switches, specialized FR "PADs" or any other similar devices. In general, the same FR access equipment may be used either with private network FR switching equipment or with FR services.

FR switching equipments are devices that are responsible for transporting the FR compliant information offered by the access equipment. Switching equipment may be T1/E1 multiplexers, packet switches, or any specialized FR switching equipment that implements the standard interface and is capable of switching and routing information received in frame-relay format. As mentioned earlier, the actual transmission of the frames may be accomplished in either variable-length information units (frames) or fixed-length information units (cells). This equipment is used in the creation of private or public FR networks, as the underlying technology is identical.

Public service providers (carriers) offer FR services by deploying FR switching equipment. Both FR access equipment and private FR switching equipment may be connected to services provided by a carrier. The service provider maintains access to the network via the standard FR interface and charges for the use of the service.

Access to the FR service involves three elements: customer premises equipment (CPE), a transmission facility, and the network itself. The CPE may be any of the types of access equipment, such as a FR compliant router, or even a private network switch with a FR compliant interface [9].

4. Internet Protocol (IP) Overview

In 1969 DARPA (Defense Advanced Research Projects Agency) began a research and development project to create an experimental packet switching network: ARPANET. The goal was to create a communication technique that was robust, reliable and vendor-independent. In 1975, ARPANET was converted to an operational network, since many organizations were attached to it already and they were using it for daily data communications. After ARPANET was operational the basic TCP/IP protocols were developed. About the time that TCP/IP was adopted as a standard, the term Internet came into common usage. In 1983, ARPANET was divided into two: MILNET and a new, smaller ARPANET. The name of these combined nets is Internet [22].

Internet protocol is the building block of the network. It is located at the Internet Layer that corresponds to the third layer of ISO OSI model, namely the Network Layer. IP is a connectionless protocol. The error detection and recovery are left to the upper layers. The functions of the protocol include:

- Defining the basic unit of transmission: datagram;
- Defining the Internet addressing scheme;
- Moving data between Network Access Layer and the Host-to-Host Transport Layer;
- Routing datagrams to remote destinations over connected lines;
- Performing fragmentation and reassembly of datagrams in necessary cases.

IP is quite similar to the ISO 8473 (the Connectionless Network Protocol or CLNP). Many of the ISO 8473 concepts were derived from IP.

IP is an example of a connectionless service. It permits the exchange of traffic between two host computers without any prior call setup. Since IP is a connectionless protocol, it is possible that datagrams could be lost during data transfer. These datagram losses can be due to maximum buffer size of a gateway that is responsible to catch a packet from one network and route it to the other. If the gateway cannot allocate buffer space to the coming datagrams, it loses the due to 'buffer overflow.'

In the following sub-sections the IP addressing mechanism, IP address to physical address mapping mechanism (ARP), discovering its own IP address mechanism (RARP), Internet Control Message Protocol (ICMP), IP protocol, Transmission Control and User Datagram

Protocols (TCP and UDP) will be described. While data passing from host to host, it is important that hosts use the same notation for data bytes. The need for a standard byte representation comes from the constraint of being vendor independent protocol. Since different architectures use different data presentations. TCP/IP protocols solve the byte-order problem by defining a network standard byte-order that all machines must use for binary fields in IP packets. Source hosts convert bytes from local byte-order to network byte-order and transmit their packets, destination hosts, in their turn, convert the network byte-order to their local byte-order. The internet standard for byte-order specifies that integers are sent most significant byte first (Big Endian style).

The assigned numbers to protocols and every kind of numbers related to network protocol implementations can be found in [23].

4.1 IP Addressing

A communication system is said to supply universal communication service if it allows any host to communicate with any other. Internet, which is a universal communication system, provides a globally addressing method to be able to identify hosts attached to it. Host identifiers are classified as names, addresses and routes. IP layer uses the binary addresses as host identifiers, since it is easier to handle in computers. Each host, in a communication medium, is identified with a physical address. Physical addresses are assigned by the physical communication equipment providers. They are also unique numbers. However, it is difficult to give routing decisions according to the physical address of a host (the cause will be described in the Routing Section). These addresses are not groupable and there is no address relation between the hosts located in the same segment. Therefore, IP layer uses its own addressing scheme, and classes for the connected hosts.

IP networks use 32 bit address to uniquely identify a host computer and the network to which the host is attached. The IP address is formed of two parts: the network address and the host address in the network.

IP addresses are classified according their formats. Four formats are permitted:

- Class A

- Class B
- Class C
- Class D

In practice, IP addresses are of the first three formats. The address structures of the 4 classes and a 5th class for future use are given in Figure 4.1.

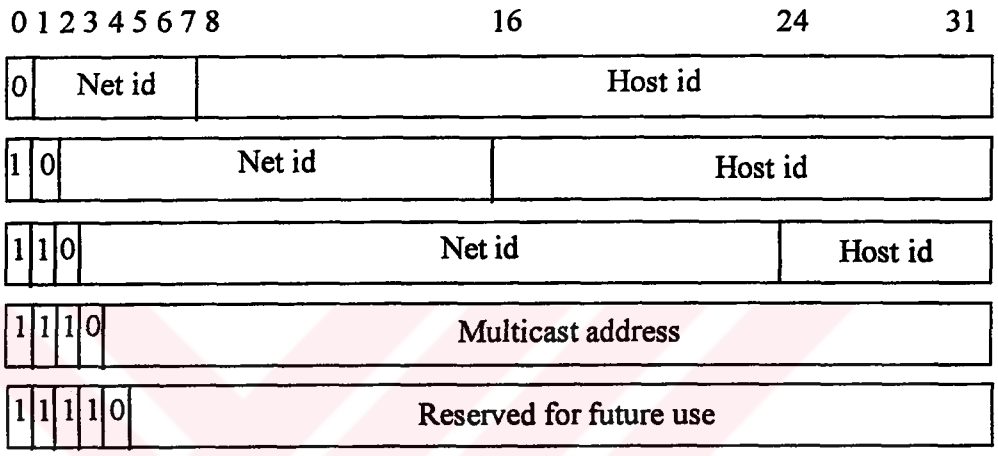


Figure 4.1. Class A, B, C addresses (from top,) Class D for multicast and Class E for future use.

Class A is given for systems that have large number of hosts attached to. They use 7 bits as network number and 24 bits for host number in the network. Class B addresses are for intermediate size networks. For the network ID 14 bits are assigned, and the remaining 16 bits for host Ids. Class C networks are small size networks. 21 bits are assigned for the network ID and 8 bits for host IDs. Finally, Class C addresses are reserved for multicasting. Multicasting is broadcasting on a limited area. The address values, number of possible networks and hosts are given in Table 4.1.

Table 4.1. Address classes and their range.

Class	Network Address Values	Max. Number of Nets	Max. Number of Hosts
A	0-127	126	16,777,124
B	128-191	16,384	65,534
C	192-223	2,097,152	254
D	224-254		

Max. number of networks, for class A is 128-2, since the numbers 0 and 127 are reserved.

For convenience, the IP addresses are used in decimal notation and '.' (dots) as separators. For example, 11000001 10001100 11000100 1010000 is written as 193.140.196.80. This address corresponds to a Class C network where its first 21 bits (following class identifier bits) are for network number and following 8 bits for host number in that network.

Network addresses that contain all bits equal to 0 mean *this network*. According to the standard, any host id consisting of all 1s is reserved for broadcast. However, broadcasts are implemented only on networks that physically support broadcasts. An address with all host id bits set to 1 causes a hardware broadcast on hardware broadcast supporting networks.

The weakness of IP addressing is that a host must change its IP address if it changes the network it used to be, since the routing of information packets is done according to host addresses.

Hosts, in IP, can have more than one connection to the system. In this case it can have more than one IP addresses. Such hosts are called multi-homed hosts.

The class A network address, 127.0.0.0 is reserved for loopback and is designed for testing and inter-process communication on the local machine. It does not appear on any network, moreover, gateways that encounter this address in a data packet, discard the packet.

To ensure that the network portion of the address is unique, all Internet addresses are assigned by a central authority, the Network Information Center (NIC).

4.1.1 Subnets

Subnets are sub-divisions of a network. It is possible to divide a network into local subnets. The easiest way of understand a subnet is to realize that a site is assigned a Class B address. In fact, the site contains two or more physical networks. In subnets, only local gateways know that the entire network consists of two or more subnets. The exterior gateways are unaware of the local sub-divisions. The major component of subnets is the subnet mask. Subnet mask is a number that defines the physical network id part in the host part of an IP address. In subnets, some bits from the host id field are reserved for the physical sub-network id. The subnet address structure can be seen in Figure 4.2.

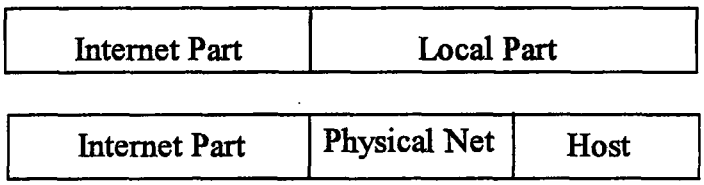


Figure 4.2. Subnet addressing scheme in IP.

The physical net part is specified with the subnet mask. Each subnet must have its subnet mask to have its own physical subnet address. The subnet mask contains all 1s for the Internet part and 1s for the physical network id bits in the local part. For example, a netmask assigned as 11111111 11111111 00011000 01000000, selects the first two bytes, 2 bits from the third byte and 1 bit from the fourth byte as the net portion of the address. Although, netmasks are flexible to choose any bits within the local part it is recommended that sites use contiguous subnet masks and that they use the same mask throughout an entire set of physical nets that share an IP address.

4.2 IP Related Protocols

Address Resolution Protocol (ARP) ARP is used to map IP addresses to physical addresses. The IP packets that are encapsulated or inserted into the data fields of lower layers must be forwarded to the physical connection of the destination machine. Therefore, the lower layer should know the appropriate address for the corresponding layer (peer layer) of the destination host. The data packet from IP layer that has a source IP address and a destination address in its header is inserted in a lower layer packet that is going to be send to the network. Figure 4.3 describes the situation.

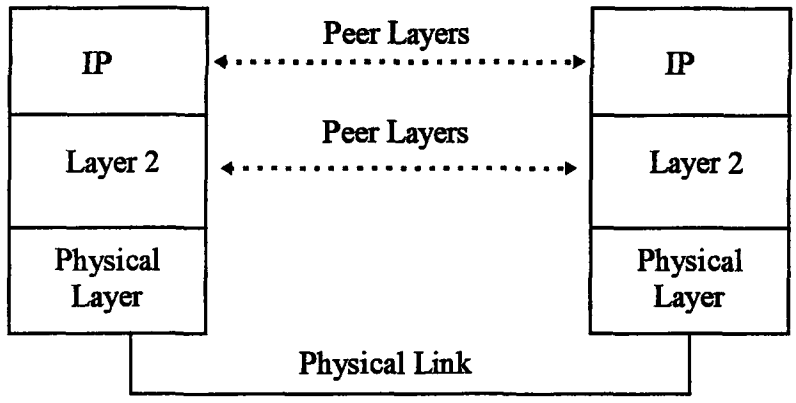


Figure 4.3. Peer layers communication logic

Each layer presented in Figure 4.3 can send packets to its peer layer on the other side of the network by knowing peer's address. If the IP layer wants to send a packet to its peer layer it must provide its lower layer with the data packet and the destination's Layer 2 address. Since the physical data packet is transmitted from the physical layer, all upper layers must pass their communication packets to the layers below. To discover the destination's Layer 2 address, the ARP is used. In ARP, the source host keeps an IP to physical address mapping table that it discovers from the incoming packets or by broadcasting an ARP request packet. In this packet, the source puts its physical address, IP address, the destination host's IP address and an empty field for the destinations physical address to be filled by the destination host. After preparing the ARP request packet it broadcasts this packet. When the packet is caught by the destination host, it updates its ARP tables according to the packet coming from the sender, since that packet carries source's physical layer address. After updating local ARP tables, the destination host fills the destination hardware address field in the packet and sends it to the source host. Other hosts, that receive the ARP packet as well, update their ARP tables, but do not respond to the sender.

The ARP packet structure is seen in Figure 4.4.

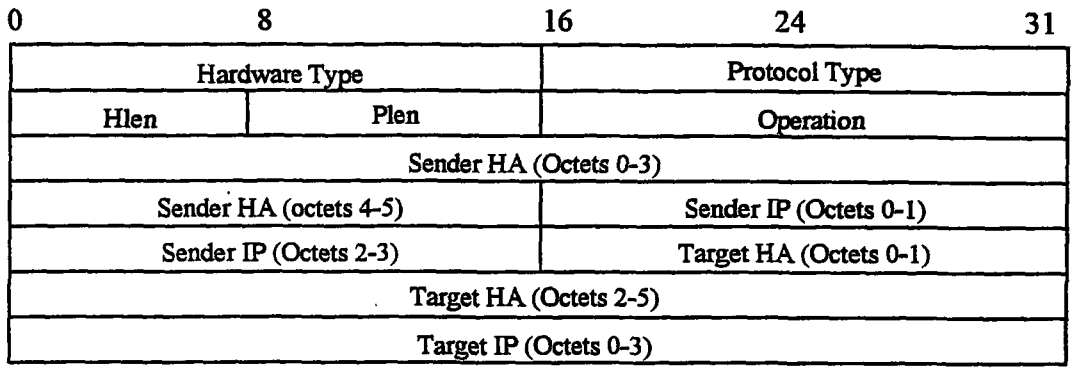


Figure 4.4. The ARP packet structure.

The explanations of the packet fields are described in Table 4.2.

Table 4.2. ARP packet fields and their meanings.

Name	Description
Hardware Type	The hardware interface type for which the sender seeks an answer. For Ethernet the value is equal to 1.
Protocol Type	Type of high-level protocol address the sender is supplied. 0x800 Hex for IP addresses
Operation	1 for ARP Request 2 for ARP Response 3 for RARP Request 4 fro RARP Response
Hlen	Hardware address length.
Plen	High-level protocol address length
Sender HA	Sender's hardware address
Sender IP	Sender's IP address
Target HA	Target's hardware address
Target IP	Target's IP address

ARP requests are sent to discover the physical addresses of the hosts that are on the same physical network, to the hosts that are directly connected to the same network. However, some gateways may use a modified version of ARP that is called Proxy ARP. In Proxy ARP, the sender broadcasts an ARP request packet to a destination that is not on the same physical network. In this case, the sender is unaware of being physically different networks. The gateway that is directly connected to both of the hosts, the sender and the

receiver, responds to the source's ARP request as if it has the destination IP address it is searching. After having the packet from the source, it forwards it to the destination host.

Detailed information about ARP can be found in [24].

Reverse Address Resolution Protocol (RARP) RARP is used for IP hosts that discover their IP address at boot time from a RARP server. The packet structure of RARP is the same as ARP's. IP addresses are stored in local disks of the hosts, they do not change in most of the time. However, if the host is a diskless machine, it cannot store its IP address. It broadcasts a RARP packet containing only its physical address. The RARP server, which is located on the same network, responds to the request by sending the IP address of the diskless machine.

Internet Control Message Protocol (ICMP) Internet protocol provides an unreliable, connectionless datagram delivery service. A datagram is forwarded by special devices called routers (or gateways) from net to net until it gets to its final destination. In a case of an error in a gateway some datagrams may be lost or cannot be forwarded due to congestion, gateway buffer overflow, etc. In such cases, gateways inform the source of the datagram about the action taken by the gateways, so that the sender knows what happened to the datagram and it can be able to correct the situation (by retransmitting over the same route or another route to the destination).

Failures occur more common is the following cases:

- disconnected communication lines and/or processors,
- destination machine is temporarily or permanently disconnected from the network,
- time-to-live of the packet expires,
- intermediate gateways are so congested that they cannot service incoming traffic.

To allow gateways in an internet to report errors or provide information about unexpected circumstances, ICMP protocol is added to the TCP/IP protocol stack. It is a required part of IP and must be implemented in all implementations of IP. ICMP provides communication between IP software on one machine with the other IP software on the other side of the network. It does only report the error. The correction of the error is left to the sender. On the other hand, errors, more generally, occur due to senders. Therefore, ICMP is used to inform only the end nodes, the intermediate nodes are not informed. Direct result of this behavior is that ICMP cannot be used to inform intermediate gateways about the situation, they only forward the ICMP information packet to the right place.

ICMP packets are encapsulated (or inserted) into IP datagrams. It is not an upper layer protocol, it is the required part of IP layer. Therefore, ICMP packets require two levels of encapsulation. The encapsulation of ICMP is shown in Figure 4.5.

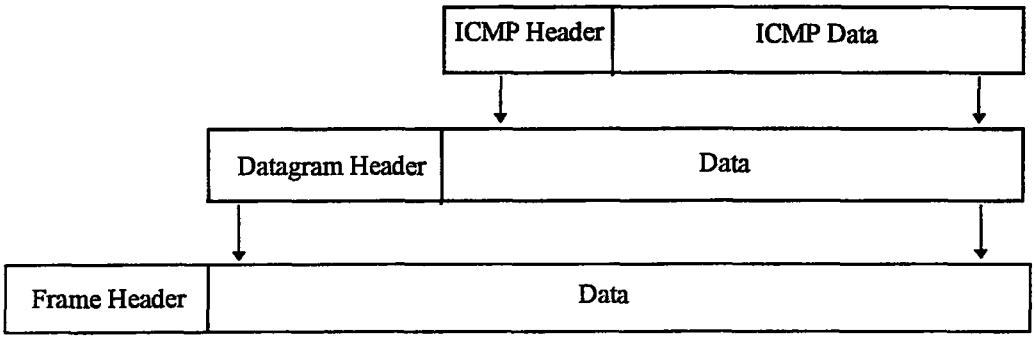


Figure 4.5. ICMP encapsulation.

Each ICMP message contains its own format, they all begin with the same three fields:

- TYPE: an 8-bit integer value that identifies the message,
- CODE: an 8-bit field that provides further information about the message type,
- CHECKSUM: a 16-bit checksum value of the ICMP packet.

ICMP messages that inform about errors always include the header and the first 64 data bits of the datagram causing a problem. The ICMP TYPE field defines the meaning of the message along with the format of the packet. Possible TYPE field values and their meanings are given in Table 4.3.

Table 4.3. ICMP TYPE field values and their interpretations.

Type Field	ICMP Message Type
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect (change a route)
8	Echo Request
11	Time Exceeded for a Datagram
12	Parameter Problem on a Datagram
13	Timestamp Request
14	Timestamp Reply
15	Information Request (obsolete)
16	Information Reply (obsolete)
17	Address Mask Request
18	Address Mask Reply

More detailed information about ICMP can be found in [25], [2], [26].

4.3 Internet Protocol (IP)

Internet Protocol is a building block of the network. It is located at the Internet Layer that corresponds to the third layer of ISO OSI model, namely the Network layer. IP is a connectionless protocol. The error detection and recovery are left to the upper layers. The functions of the protocol include:

- Defining the basic unit of transmission: datagram;
- Defining the Internet addressing scheme;
- Moving data between Network Access Layer and the Host-to-Host Transport Layer;
- Routing datagrams to remote destinations over connected lines;
- Performing fragmentation and reassembly of datagrams in necessary cases.

The purpose of IP layer can be stated as to pass data packets coming from the upper layer to the lower layer in order to send it over physical communication media, and on the other side of the network, to pass data packets coming from the lower layers to the fourth layer. IP, while passing data packet from the upper layer to the DLL, encapsulates the upper layer packet into IP datagram's data field part. Assigns the destination IP address according to the request coming from the upper layer, while assigning the destination address it discovers also the DLL address of the next gateway that will take the packet and route to the appropriate path.

The Internet datagram is the name of the communication packet used in IP layer. The structure of the packet consists of a HEADER and DATA parts. The structure of datagram looks like a physical frame structure, but the main difference is that in IP datagram the source and destination addresses are IP addresses. The datagram format can be seen in Figure 4.6.

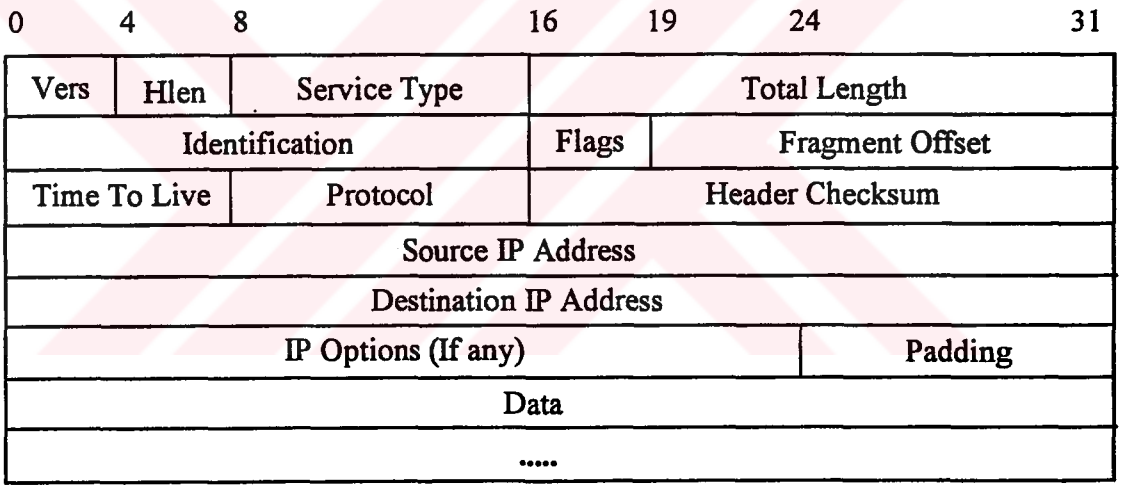


Figure 4.6. IP Datagram format.

Datagram fields and their meanings are described in Table 4.4.

Table 4.4. IP Datagram field names and interpretations.

Field	Meaning
Vers	The version of IP protocol that was used to create the datagram. Current value is 4.
Hlen	Header Length Field. Gives the datagram header length measured in 32-bit words. The most common header length is 20 octets and has a Hlen field equal to 5.
Service Type	Specifies the precedence of the datagram, the type of transport the datagram desires (options are high throughput, low delay, high reliability).
Total Length	Gives the total IP Datagram size measured in octets including header and data fields.
Identification	Contains a unique integer that identifies the datagram.
Flags	Controls the fragmentation.
Fragment Offset	Specifies the offset in the original datagram of the data being carried in the fragment, measured in units of 8 octets.
Time To Live	Specifies how long, in seconds, a datagram will remain in the internet system.
Protocol	Specifies which high-level protocol was used to create the message being carried in the Data area of the datagram.
Header Checksum	A checksum value to ensure the integrity of header values.
Source IP Address	Sender's IP address.
Destination IP Address	Receiver's IP address.
IP Options	For network testing and debugging. It is variable length field.
Padding	Represents bits containing 0 that may be needed to ensure the datagram header extends to an exact multiple of 32 bit words.
Data	Encapsulated layer 4 packet. (Or ICMP message).

The datagram size, according to Total Length field can be up to 2^{16} octets. However, IP datagrams, while passing over various communication media and protocols, can be divided into smaller parts or 'fragments.' This process is called fragmentation. The fragmentation can be done because of underlying protocol's Maximum Transfer Unit (MTU) size. For example, according to Q.922 standard, the FR frame structure cannot carry packets whose size is more than 262 octets. Over such media, the IP datagram is fragmented by the

intermediate gateway (or the host itself) and the whole packet is carried in fragmented form. The reassembly of fragmented packets, is and should be done at the destination host. In case of fragmentation, the host that does the fragmentation, divides the data part of the datagram, inserts copies of the whole datagrams header fields (according to Identification, Flags and Fragment Offset values) and sends these new datagrams over the network that has a lower MTU. Each time the packets encounter a network that has lower MTU value than the datagram's size, are fragmented, this goes until all the fragments reach to their final destination. The fragments are reassembled there and the originally sent datagram is passed to the upper layer by the IP at the final destination.

The fragmentation of IP datagrams is the main time consuming factor in header processing. Some methods are designed and implemented to overcome the delay due to datagram fragmentation in IP layer. Their primary purpose is to keep unaware the IP layer from the lower MTU of the underlying network protocol and handling fragmentation of IP datagrams easier. Such proposals where the WAN protocol used as the second layer of OSI is FR can be found in [27], [19].

The fragmentation is shown in Figure 4.7.

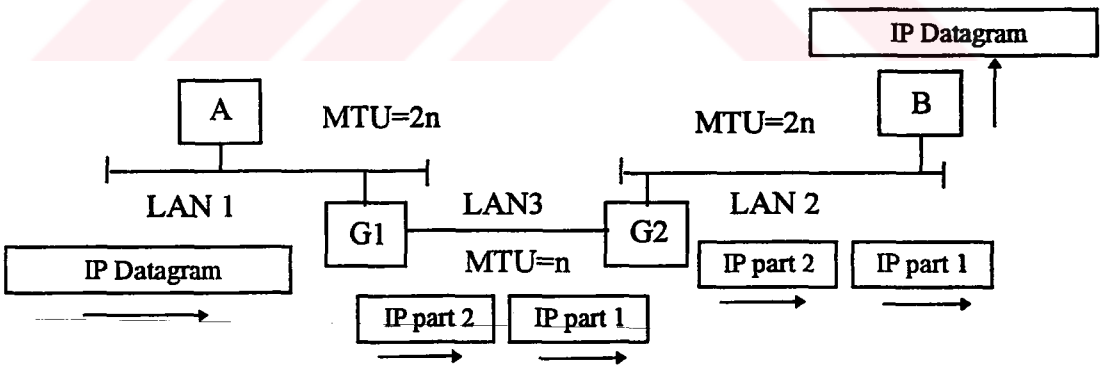


Figure 4.7. IP fragmentation and reassembly logic.

In the example figure (Figure 4.7) Host A sends a packet whose size is greater than *n* but less than *2n*. The gateway G1 fragments the datagram into datagrams whose sizes are less than *n*. Gateway G2, passes the datagrams without reassembling them. The reassembly is done at the IP layer of Host B and the original datagram is passed to upper layers. The proposed methods in [27] and [19] are to reassemble datagrams at the end nodes of LAN 3. LAN 3 is considered to behave as a FIFO queue and there is no alternate routes from G1 to

G2 that is the case in FR. Their fragmentation and reassembly logic can be seen in Figure 4.8.

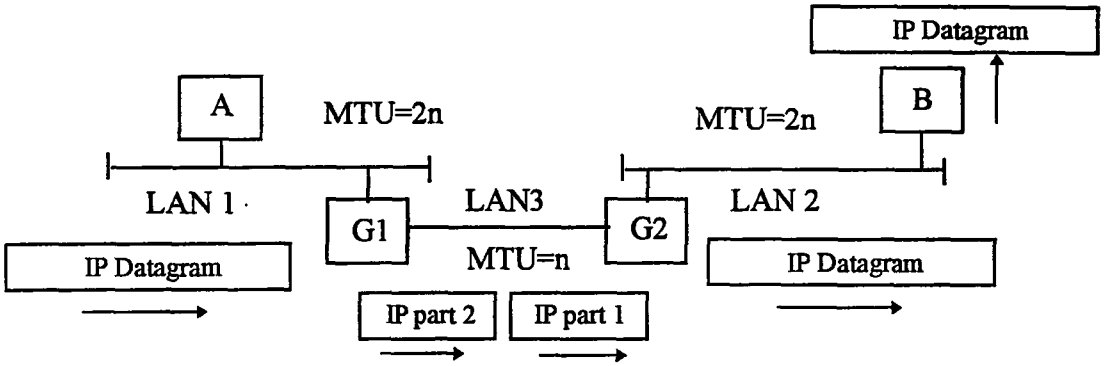


Figure 4.8. Proposed fragmentation and reassembly logic for FR.

While debugging the network one can want to record route from source to destination, or enforce gateways to route datagrams over a specified path. For this purpose, Options field is used. For more detailed information about broadcasting IP datagrams refer to [29], [30]. IP checksum computation algorithms can be found in [31]. IP datagram reassembly algorithms are presented in [32].

Communication in IP can be described as follows. A datagram delivery request comes from the upper layer. The data packet and the destination address are given by the upper layer. The IP layer looks to the network id part of the destination address. If the destination node's address is found in local routing tables, IP can deduce from that entry the next gateway's or host's segment id or physical port id. The routing table contains some recently communicated network ids, physical port numbers from where the datagram will be send, next gateway's id (if there are intermediate gateways along the path) and the distance measure to the destination. If the network number cannot be found in local routing tables, the datagram is sent to a default gateway that is assumed to know the right path to the destination. After deciding the intermediate (or final) node on the same physical network that is on the path to the destination, the datagram should be passed to the second layer with the physical address to send it over physical network. At this step, the ARP module is used to map IP addresses to physical addresses. A request is made by IP to the ARP module to have the physical address. If the IP address entry is found in the ARP tables the corresponding address is returned to IP. The address mapping is transparent to the IP layer and is carried by ARP module. Which means that, if the entry is

not found in the table ARP should broadcast an ARP request and discover the necessary address and then to respond the IP layer.

When the IP layer gets a datagram from the second layer it checks whether the datagram is destined to itself or it should be passed to another network. If the destination is itself then necessary header checks are performed and the data part of the datagram is sent to the upper layer. The routing logic of IP will be mentioned in Section 5.1.

4.4 Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

TCP and UDP are two protocols that are located over IP layer and correspond to Transport Layer of OSI. IP is responsible to carry datagrams from the source host to the destination host. It does not know what is the application that sends the datagram, and to which application the datagram is sent. However, in multi-tasking hosts more than one process can send message to a same host but to different applications running on. TCP and UDP are both designed to send messages to applications on an IP host. UDP provides protocol ports used to distinguish among multiple programs executing on a single machine. UDP uses the underlying IP protocol to transport a message from machine to another, and provides the same unreliable, connectionless datagram delivery semantics as IP. It does not send acknowledgments for the received packets and does not provide feedback to control the rate at which information flows between the machines. Thus, UDP messages can be lost, duplicated or arrive out of order. Furthermore, packets can arrive faster than the receiver can process them.

TCP provides a reliable, connection oriented service. It can be characterized with:

- Connection-oriented data management,
- Reliable data transfer,
- Stream-oriented data transfer,
- Push functions,
- Resequencing,
- Flow control (sliding windows,)
- Multiplexing,
- Full duplex transmission,
- Precedence and security,

- Graceful close.

Although the protocol stack is known as TCP/IP but TCP can function independently from the IP. TCP layers are not required parts of IP gateways. Detailed information about UDP can be found in [33]. TCP is described in [34].

5. Routers

The interconnection of heterogeneous networks is accomplished by dedicated processors, i.e., the gateways, attached to each network. The gateways are the interface between the local and the long haul networks. They perform the necessary protocol conversion, implement flow control algorithms and route packets over the long haul network. Additionally, they behave as buffers between networks with different transmission rates [35].

Previous studies showed that network use grows exponentially with time. The cause of this growth in use is the exponentially increasing number of hosts attached to Internet. Detailed investigation results about growth trends can be found in [36]. To respond to the growing network usage, new protocols and new communication methods are investigated. More intelligent and fast communication equipments, faster WAN protocols are being used to interconnect fast LANs. Since, the interconnection of a large number of LANs through a virtual-circuit WAN raises several performance issues due to the effects of bandwidth mismatch (e.g. 10 Mbps Ethernet LANs over 64 Kbps X.25 links), protocol mismatch, and large propagation delays [4].

The routing on Internet became one of the most important issues in internetwork communications. IP routers have to be more intelligent and faster. In Section 5.1, the routing logic of internet protocol is described. Requirements for Internet gateways are mentioned briefly. Some of the route discovery methods are explained.

5.1 IP Routing Logic

In a packet switching system, routing means finding the path to the destination. Any machine that makes this kind of decision is called a router. IP routing is analogous to this routing concept. IP hosts, while sending datagrams to the destination hosts chose paths over which the datagram will be delivered, we deduce from this explanation that all IP hosts are, in a manner, IP routers. However, in Internet there are computers that are

dedicated to only routing of other hosts' datagrams. These dedicated routers have more than one physical connection to different networks, they are multi-homed machines, e.g. they have more than one IP address. Throughout this thesis such kind of computers are referred as IP routers and devices that have only one IP address are referred as IP hosts. IP routers that do protocol conversions while passing datagrams from one physical network to another one are called gateways.

There exist two forms of routing:

- Direct routing,
- Indirect routing.

The direct routing is done when both the source and the destination are located on the same physical network and there is no intermediate machine(s) to forward the datagram from the source to the destination. This forms the basis of internet. Indirect routing occurs when the source and the destination are not located on the same physical network. In this case, the sender must pass the datagram to an intermediate gateway to deliver it to the receiver machine's physical network. Direct and indirect routing can be seen in Figure 5.1.

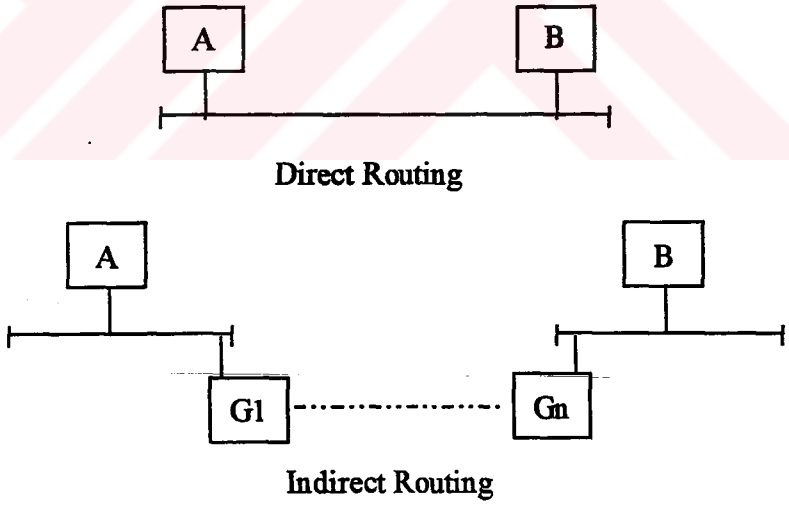


Figure 5.1. Direct and Indirect routing in IP.

A host while sending a datagram can easily decide the type of routing. If the destination has the same network address as the source's then it is on the same physical network. In case of subnets, the network address plus the subnet part is considered. The host, before sending a datagram, decides the routing method, if the destination is located on the same physical network it encapsulates the datagram into a physical frame, maps the destination

IP address to a physical address and delivers the packet to the network. The direct routing is the final step in every kind of datagram transmission. Even if the source does indirect routing to the destination, the final gateway will do direct routing.

Indirect routing is more difficult then the direct one. In this case, the source encapsulates its datagram in a physical frame, the datagram contains the destination IP address, however, the physical frame is destined to a gateway that is closer to the destination than the source. The gateway receives the frame, extracts the datagram from the frame, assigns the next hop's address to forward the datagram. The final gateway does direct routing.

Routing in IP is done by using routing tables. A routing table consists of 'destination network numbers' and 'next gateway address to that network' entries. The network ids are more efficient to keep in these tables since it would be very difficult and redundant to keep all the host addresses. The entries in the routing table shown only the next gateway, to which there is a physical connection. Thus, the gateways do not know all the path from the source to destination. All the information kept by the gateways serves to forward locally the datagram to the correct next intermediate node. This method is known as table driven routing. The gateways are responsible to keep their tables up-to-date. The entries in the table must be minimal (according to cost measure considered) routes to the destination networks. A gateway and its routing table will explain the logic (Figure 5.2 and Table 5.1).

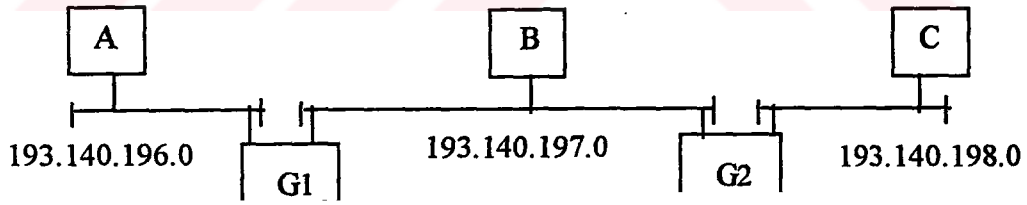


Figure 5.2. The structure of an example network.

Table 5.1. Gateway G1's IP routing table.

Destination Networks	Next Hop
193.140.196.0	DIRECT
193.140.107.0	DIRECT
193.140.198.0	193.140.197.2 (G2's address)

Datagrams coming to G1 from the host A destined to host C will be forwarded to gateway G2 according to routing table. If the datagram was destined to B. Then the datagram would be delivered directly to B by the gateway G1.

A way of keeping the routing table small is to consolidate multiple entries into a default entry. Default routing is useful when a site has a small set of local addresses and only one path to the rest of the whole Internet. In such routing tables, only the local addresses are kept and for the rest of the whole network a default route entry is inserted. That default entry contains, as a next hop, the address of the gateway that provides the connection with the rest of the world. However, it is possible to have host-specific route entries in the table. The entry contains the host address and again the next hop address.

IP routing logic can be described by the following algorithm (Figure 5.3).

```
Route_IP_Datagram(Datagram, Routing_Table)

Extract destination IP address, Id, from datagram

Compute IP address of destination network, In

If In matches any directly connected network address send datagram over that network
      (resolve Id to physical address, encapsulate datagram and send the frame);

else if Id appears as a host-specific route then route datagram as specified in the table;

else if In appears in routing table then route datagram as specified in the routing table;

else if a default route has been specified then route datagram to the default gateway;

else declare a routing error;
```

Figure 5.3. Routing algorithm of IP [2].

5.2 Requirements for Internet Gateways

An Internet gateway is an IP-level router that performs the following functions[37]:

- Conforms to specific Internet protocols (IP, ICMP, ARP, etc.),
- Interfaces two or more packet networks and implement necessary functions required by the network, such as encapsulation/decapsulation of IP datagrams, sending/receiving datagrams according to MTU sizes of that network, IP to physical address mapping, responding to the network flow control and error indication,
- Receives/forwards Internet datagrams,
- Chooses a next-hop destination for each IP datagram based on its routing table,
- Supports an interior gateway protocol (IGP) to carry out distributed routing and reachability algorithms with the other near gateways,
- Provides system support facilities (loading, debugging, status reporting, exception reporting and control).

The protocols needed in gateways are listed as follows:

- Internet Protocol IP,
- Internet Control Message Protocol (ICMP),
- Exterior Gateway Protocol (EGP),
- Address Resolution Protocol (ARP),
- Constituent network access protocols,
- Interior Gateway Protocol (IGP),
- Monitoring protocols,
- Internet Group Management Protocol (IGMP) (experimental).

Detailed information about the listed elements can be found in a very structured manner in [37].

5.3 Route Discovery Protocols

Internet gateways are classified as core and noncore gateways. Core gateways are those that are under the control of a single authority, Internet Network Operation Center

(INOC). Noncore gateways are not administrated by INOC. When ARPANET was first implemented it was a single backbone network. When it is converted to Internet, many gateways attached LANs to the backbone and others. Gateway-to-Gateway Protocol (GGP), was used between the core gateways to share routing information about attached LANs. Each gateway had complete information about the other gateway's routing. After the growth of Internet it became unnecessary to hold all the routing information. To divide this problem, gateways are given responsibility to keep local information within an autonomous system. An autonomous system can be described as a system consisting of local LANs and gateways. In a case where datagrams are destined to the exterior of the local system, the gateways chose an interior gateway that is connected to an exterior gateway to forward the datagram. This method brought two kinds of gateways: Interior and Exterior gateways. This led to two kinds of routing information passing protocol: External Gateway Protocol (EGP) and Internal Gateway Protocol (IGP). Thus, it is not unusual to see gateways implementing both protocols [26].

There exist several IGPs. The most commons are the Routing Information Protocol (RIP), the Hello Protocol, Open Shortest Path First (SPF) Protocol (OSPF). One of the most widely used IGP is RIP. The popularity of RIP is not because of being the best method, but, it is the result of Berkeley distributing routed software along with their popular 4BSD UNIX systems. RIP was being used and developed before a formal standard was written. An RFC [38] is written after many implementations of RIP.

RIP is a vector-distance routing protocol. It classifies IP hosts into two: active machines and passive machines. Active machines are the gateways that send their routing tables to the others. Passive machines are the hosts that listen to the routing updates, change their own routing tables but do not send to the others. An active gateway broadcasts its routing table at every 30 seconds. The sent table consists of IP network numbers and according hop counts to reach that network from the broadcasting gateway. The hop count is the number of gateways to pass along the path to the network specified. However, hop count is not a good metric, since both slower and faster protocol networks are considered as 1 hop and are considered as equal length paths.

By using RIP, gateways learn the routing tables of their neighboring gateways. They update their routing tables according to this information. An entry is modified whenever a better path is discovered. Eventually, all gateways learn the optimal (?!) routes to the remaining part of the network. RIP does not update an entry until the new hop metric is strictly less then the existing one. The routing table entries are kept for 180 seconds, if a new RIP update does not come for the entry up to 180 seconds, the entry is considered as a

lost network connection and is discarded from the table. The timer is updated every time a RIP update is received.

RIP must handle 3 kinds of errors caused by the underlying algorithm: detection of routing loops, prevention of instabilities by using a low value for the maximum possible distance (16), and, the vector-distance protocol used by RIP creates a slow convergence or count to infinity problem. Choosing small infinity (16) helps limit the slow convergence, but does not eliminate it [2]. There exist methods to solve the slow convergence:

- Split horizon update,
- Hold down method,
- Poison reverse.

RIP messages are encapsulated within UDP packets and are sent to UDP port 520.

An example to IGP is Interior Gateway Routing Protocol (IGRP) developed in the mid-1980s by Cisco Systems, Inc. IGRP uses a combination of metrics, internetwork delay, bandwidth, reliability, and load. The weighting factors of these metrics are set by the system administrator to calculate optimal routes. The Extended IGRP (EIGRP) is an enhanced version of IGRP that combines the advantages of link state protocols with the advantage of distance–vector protocols. EIGRP incorporates the Diffusing Update Algorithm (DUAL).

6. Description of the Test Setup

LANs have been designed for communicating machines that are close to each other. These local networks operate using data rates of a few Mbps. The use of remote bridges, routers, gateways to interconnect physically distant Local Area Networks has become increasingly popular because of the need to interconnect these distant network islands. There are various ways of connecting these LANs including private line, circuit switching and traditional packet switching. FR is a well-suited and economical method for interconnection of this kind of LANs. A remote bridge example connecting LANs over FR is given in [39]. The WAN speed of FR is more suitable then the traditional X.25's 64 Kbps speed. The performance comparison of FR with various protocols will be given in the Section 7. Moreover, the performance of the system can be compared with [39] and [40] as they are not presented in Section 7.

There are three alternatives for linking LANs into wide-area networks [41]:

- Circuit switching,
- Leased line,
- Packet switching.

In this thesis, a FR based network is proposed as a LAN interconnection method that is a better way compared with older packet switching methods like X.25. The purpose of this thesis is to evaluate the performance of an IP gateway linking LANs over FR protocol. During the logical design and the test phase some Ethernet to FR routing problems, incompatibilities between different types of protocols are investigated and some useful solutions to these problems are proposed.

The FR based router system is a functional and standalone system. However, it can be used as a part of a FR switch system which is being designed in Netlab.

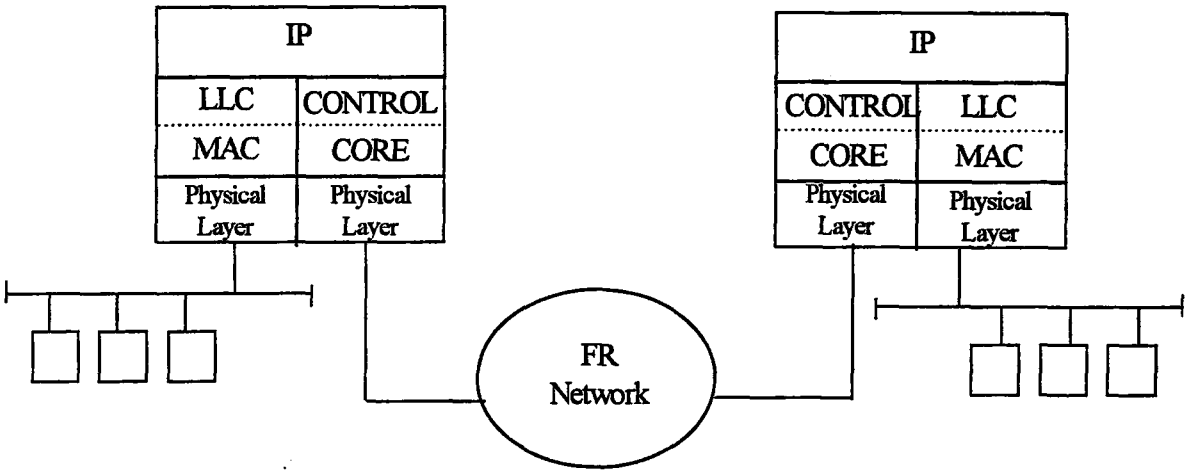


Figure 6.1. The test environment

When two high-speed networks, such as two Ethernet segments, are connected through a high-speed point-to-protocol, such as FR, a service called packet switching is required at the link layer. A packet consists of a sequence of bits, and is the basic unit of physical communication. A switch is a computer which transfers packets from one network to another according to destination information stored in the packet headers. A switch interconnecting high-speed networks is called a high-speed packet switch.

A high-speed packet switch must be a high-performance computer which is capable of receiving packets incoming from a high-speed network, storing these packets in buffers when necessary, and transmitting packets to the destination lines. All the above capabilities require a high processing power, a large memory, a real-time operation of the switch software, etc. The system must also be designed such that it will have more then one lines from where high speed packets are coming. One of the ways to reach to a high-processing power and a large memory is a multi-processor system with a large memory distributed among the processors.

The FR test bed, in the Computer Networks Research Laboratory of Computer Engineering Department of Boğaziçi University, seen in Figure 6.2, is interconnecting five physically disconnected and geographically distant LANs, namely four Ethernet LANs and an AppleTalk LAN. The test bed consists of an FR switch connected to several PCs and Macintoshes through 2 Mbps FR lines. The switch is a VME bus based multiprocessor system which has the power and memory required to be a hardware platform for a high-speed packet switch. Since the communication between LANs is on IP protocol and the IP layer is located at the third layer of OSI, the switch will only have to interpret FR headers coming from IP gateways or hosts.

The gateways, seen in the Figure 6.2 (described in more detail in Figure 6.1), will do protocol translation between Ethernet and FR In the original design, the gateways have Ethernet boards and FR ISA bus interface boards mounted into their slots. These PCs will route IP packets from the Ethernet segments they will be directly connected to with Ethernet boards, to the FR switch, to which they will be connected with FR ISA bus interface boards, and vice versa. The FR boards used in PCs are being designed by Oğuz Sinanoğlu as his M.S. thesis [42]. The DL Core layer software is designed by Albert Levi as his M.S. thesis [12], but it is not tested yet because of the lack of FR boards up to the moment.

Macintoshes will be used as end-user terminals and/or Ethernet-to-FR gateways. One of the Macintoshes will be a frame relay to AppleTalk router which will allow a Mac network to be connected to a FR switch. There will be also a Macintosh Quadra which will be used as FR to Ethernet gateway.

The FR switch is connected to the Computer Networks Research Lab Ethernet LAN. Thus, it will be able to perform the switching of IP packets from the Ethernet segment it will be directly connected to FR links and thus to the gateway PC, which will be a LAN-to-LAN internetworking process.

To run on the hardware mentioned above, driver software will be developed to drive the FR interface boards. On top of a basic FR communication facility, the upper layers of a FR software will be incorporated and, the FR ISA bus interface boards will be configured either as a FR end-user interface or as a network interface of a high-speed packet switch.

Among the test bed hardware mentioned above, the FR ISA bus interface board has been designed and developed in our laboratory [42].

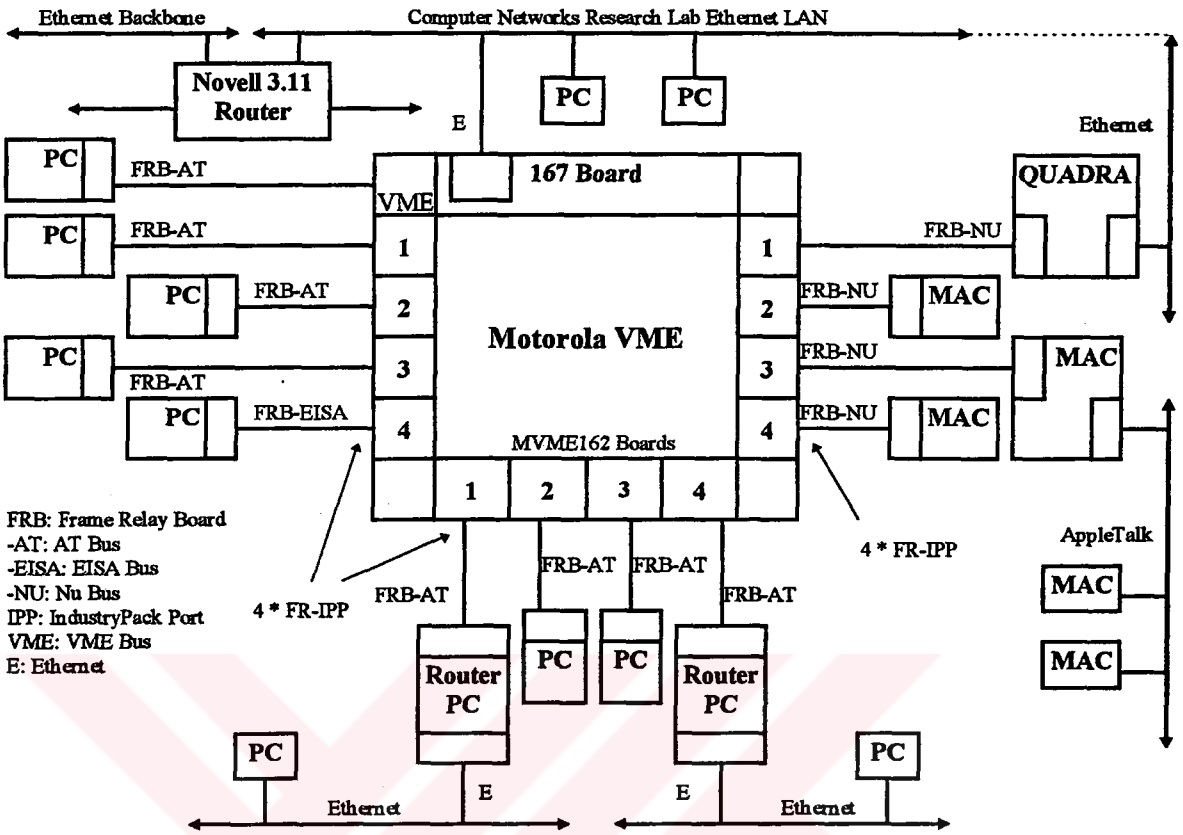


Figure 6.2. LANs interconnected through FR.

6.1 Ethernet-FR Routing Problems

The primary goal is to interconnect more than one LAN over a FR network. The gateways here is designed to route only IP datagrams. The number of communicating computers is increasing and these computers require huge data transfers in the fastest manner. FR is chosen as the communication medium since it is more efficient than X.25 and other older connection-oriented protocols. There are three types of basic problems while interconnecting two LANs over FR. These are due to the connection orientedness of FR, communication speed differences, MTU incompatibilities. As we know, Ethernet is a 10 Mbps network and FR is a 2.048 Mbps network. The packets are broadcasted in Ethernet, it is connectionless. However, in FR we need to establish a virtual circuit from the source to destination each time we send a packet. However, the connection establishment takes

lots of time, especially when time-to-live of the IP datagram is considered (the IP datagram has 16 seconds to reach its final destination before it is discarded by the intermediate gateways.) The last problem is the MTU of two networks. Ethernet has an MTU of 1514 bytes/packet, whereas FR has a MTU of 270 bytes/packet.

The data transfer rate difference between two networks is an important issue. However, it is not a significant problem since all IP packets on the Ethernet side are not required to be send to the other LAN through FR. The only implication of this speed difference is that the Ethernet side of the gateway has to have a relatively larger buffer compared to the FR side. It is observed in [50] that the external traffic, that is the traffic over the LAN which is destined to the exterior LANs, is varying between 54.20 % and 95.92 % of the whole traffic. The worst case in this interval is the highest limit, since around 95 % portion of the whole Ehernet traffic is to be carried from one LAN to the other, which is more time consuming then the 54 % case. Again in [50], it is considered that 87 % of the external traffic was TCP/IP datagrams. It is specified that the 12 % of non-IP traffic had no effect on the results of their analysis and external IP traffic was practically identical to the external traffic. In Section 7.5, we will concentrate on the sizes of the necessary buffers that will be used by the gateways. The external IP traffic will be taken as 95 % of the whole datagrams.

The connection type difference, also, is not a significant problem. The gateway, at the boot time, can make the necessary permanent virtual circuit connections (according to its recent tables) and keep the circuits permanent until the system shutdown. If a new circuit is needed, it can establish one and keep it permanent.

The biggest problem in the design is due to the fragmentation of packets. The gateway will have to fragment most of the IP datagrams coming from the Ethernet side. The fragmentation code becomes the most crucial part of the gateway software. The communication protocols that have MTUs less than that of FR, need to have IP datagrams fragmented into even smaller parts. For example, in ATM with a data packet size of 53 bytes, the gateway has to fragment an IP packet 5 times more than FR. This increases datagram processing time of the gateway that is the most crucial issue in terms of its performance. One solution to this problem is proposed in RFC 1490 [27]. Another solution to this problem is an intermediate fragmentation layer proposal (given in the Section 8) for identical gateways. This last solution proposes an additionnal layer located between IP and FR layers. The gateway, while establishing the connection with the others, detects the 'identical' gateways, namely the gateways that have the same intermadiate fragmentation (and reassembly) layer. After the connection establishment, they both fragment IP

datagrams before FR encapsulation and reassemble them before passing it to the IP layer at the end node of the FR network. This process takes less time because it does not do IP fragmentation that is the most time consuming part of the datagram routing. The proposed model can be seen in Figure 4.8, in Section Internet Protocol.

6.2 Hardware Used

We measured the performance of the prototype of our IP gateway using two PCs, equipped with the necessary communication boards, because of the limitations in our hardware prototype development ability. These gateways connect LANs over their serial ports with a 9600 bps communication speed. This speed is, of course, not sufficient for LAN interconnection. However, this speed and the serial ports are used for functional testing of the system. The first gateway configuration consists of a motherboard containing 486DX2-66 Mhz CPU, 16 Mb of RAM, 256 Kb cache memory, LAN interfaces which are National 83901 based 16 bit Ethernet cards (as many as needed), the FR interface is designed to consist of a Motorola 68302 based communication card which is separately being designed and implemented in our laboratory [42]. However, because of the unavailability of the final product it could not be implemented on the PC, but the serial port is used to be able to simulate FR and measure performance of the gateway. The second gateway configuration consists of a motherboard containing 386 SX 25 Mhz CPU, 4 Mb of RAM, 128 Kb cache memory, LAN interfaces which are National 83901 based 16 bit Ethernet cards (as many as needed), and again the serial port for the point-to-point communication protocol.

The gateways' buffer sizes are large enough compared with other implementations that are designed and tested [4]. They can dynamically grow due to the operating system run on the machines (will be described in the next subsection). However, the gateways' service rate is less than that of the dedicated gateways due to the operating system overhead and internal bus of the PCs. The structure of the implemented system can be seen in Figure 6.3.

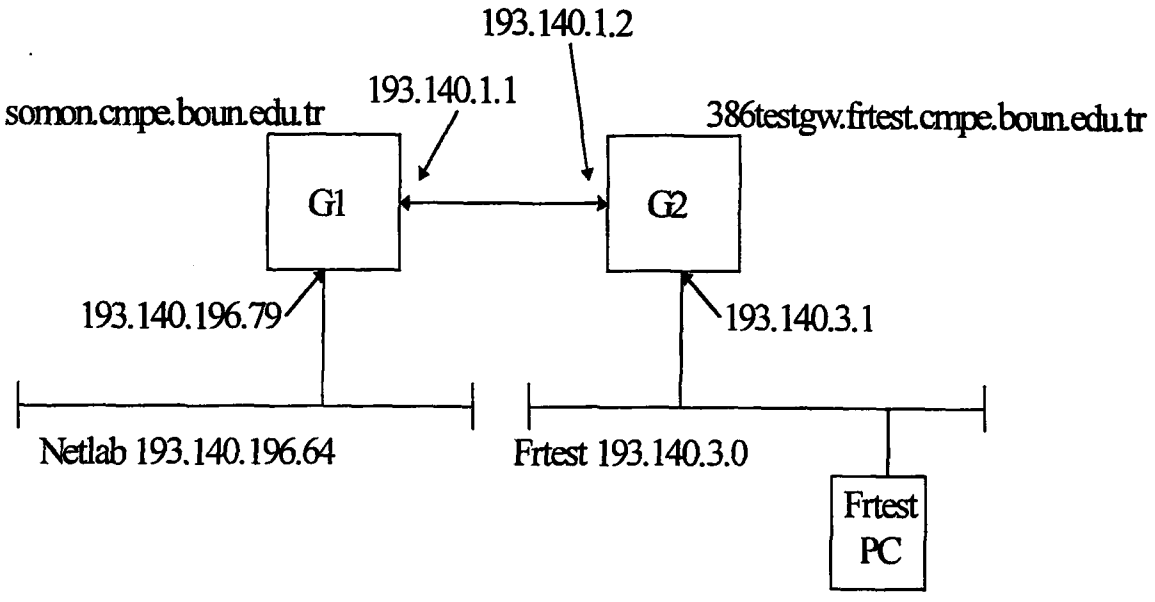


Figure 6.3. The interconnection gateways

6.3 System's Software

The gateway system consists of a Linux server. Linux is a UNIX clone for 386/486-based PCs written from scratch by Linus Torvalds with assistance from a loosely knit team of hackers across the Net. It aims towards POSIX compliance. It has all the features expected in a modern fully-fledged UNIX, including true multitasking, virtual memory, shared libraries, demand loading, shared copy-on-write executables, proper memory management and TCP/IP networking. It is distributed under the GNU General Public License [43].

As an IGP, Linux uses RIP protocol, a daemon *routed* is executed by the operating system in order keep its routing tables up-to-date. For the WAN connection of the gateway machines their serial ports and the PPP protocol are used because of the lack of FR boards.

6.4 Point-To-Point Protocol (PPP)

PPP provides a method for transmitting datagrams over serial point-to-point links. It has three main components[45]:

- A method for encapsulating datagrams over serial links,
- A Link Control Protocol (LCP) for establishing, configuring and testing the data-link connection,
- A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

PPP provides an encapsulation protocol over both bit-oriented synchronous links and asynchronous links with 8 bits of data and no parity. Links must be full duplex, may be either dedicated or circuit-switched. PPP uses HDLC as a basis for the encapsulation. It also provides for multiplexing of different network-layer protocols simultaneously over the same link. It is intended that PPP provide a common solution for easy connection of a wide variety of hosts, bridges and routers. It uses HDLC Frame Check Sequence for error detection.

PPP provides a Link Control Protocol (LCP) to automatically agree upon the encapsulation format options, handle varying limits on sizes of packets, authenticate the identity of its peer on the link, determine when a link is functioning properly and when it is defunctioning, detect a looped-back link and other common misconfiguration errors and terminate link.

PPP does not require the use of modem control signals, such as Request to Send (RTS,) Clear to Send (CTS,) Data Carrier Detect (DCD,) and Data Terminal Ready (DTR). It uses the principles, terminology and frame structure of ISO's High-level Data Link Control (HDLC) procedures.

6.4.1 Packet Structure of PPP

The packet structure of PPP is given in Figure 6.4.

Flag 01111110	Address 11111111	Control 00000011	Protocol 16 bits	Information	FCS 16 bits	Flag 01111110

Figure 6.4. PPP frame structure.

For asynchronous links, between message frames, if the line is idle, Inter-frame fill sequence (continuous 1bits) are transmitted. For synchronous links, the Flag Sequence should be transmitted during inter-frame time fill.

Please refer to [44] for more detailed information about the protocol.

In the thesis, PPP is chosen for two reasons as a WAN protocol:

- It is a point to point protocol that functions like a permanent virtual circuit. It has a call setup procedure. It is full duplex.
- It interconnects PCs by using their serial ports. It does not need any additional hardware.

Because of the lack of FR cards and software in our lab, we interconnected two LANs over a PPP link. The gateways are configured to establish necessary PPP connections during their system boot. 386testgw (seen in Figure 6.3), during its system boot establishes a PPP connection to Somon. They both keep the line open until one of them is rebooted or closes the PPP connection. The serial ports of the PCs are set to 9600 bps. The PPP link is controlled by a PPP Deamon *pppd*, and the log messages are written to /etc/ppp/ppp-log file.

6.5 Performance Evaluation Method

The necessary performance tests and measurements are made by using two methods: computer simulation and real setup performance measurement. During the computer simulation a powerful network simulation tool OPNET [45] is used. In computer simulation, the whole TCP/IP gateway model is modified to model the designed network model. The protocol stack is fully implemented and some additions to the source code are

made in order to get the necessary performance measures (will be described in Section 7). The simulation is performed because of the lack of real measurement tools, such as protocol analyzer and FR communication boards.

The real measurementsare taken in Computer Networks Research Laboratory (NETLAB) by using the setup given in Figure 6.3. However, a more realistic measurement of the system should be done by using FR communication cards. A physical layer driver software for the card should be designed and implemented for Linux environment. Afterwords, DL Core and Control layers and the interface between FR and IP layers should be implemented, which can be a future work.

The measurements are performed by sending IP datagrams by a host. The packets are destined to the *FrTestPc* which is located on the other LAN. The sending machine runs a packet sender software is designed and coded in our lab by Bahar E. Baran [53]. *FrTestPc* is responsible to catch and count the packets routed by *Somon* and *386TestGw*. The packet catching software, also, is designed and coded in NETLAB by Ali A. M. Kalufya [54]. This last, when run on the frtestpc, it counts the number of Ethernet packets broadcasted to the segment in 15 sec intervals. The throughput of the system is measured by dividing the number of packets captured to the number of intervals times 15. The measurement is done on a real network. The sender machine is located on a network where there is normal LAN traffic. This last means that the gateway located at the real network side has to filter all the incoming packets from the packets that are to be forwarded. For that reason somon (486 DX2 66) is located on that segment (see Figure 6.3) since it is faster than the 386testgw machine. The packet sizes, generation speeds and distributions are descirbed in Section 7.3.

The OPNET models of the setups described in Section 7 were full TCP/IP implementations (C codes) of the real gateway machines. The model is exactly the same of Figure 6.3. The end nodes are running applications that communicate with each other over TCP. The first machine continuously sends datagrams to the second according to a distribution. Some probes are inserted to the code of the model to be able to monitor the total number of datagrams, the packet number in the gateway queues and the total delay of transmitted packets. The second machine collects datagrams and sends acknowledgments to the first machine over the gateways.

7. Performance Evaluation

In this Section, the major performance issues of the IP router are described and performance results are given. The performance of interconnected networks is highly dependent on the performance of the gateways. Since the finite storage capability and packet forwarding capacity of gateways effects the throughput, it has to be considered for the analysis of interconnected networks [35]. However, in our case, the finite storage of gateways is so large that it can be thought as infinite buffers. Among many performance issues of IP gateways are the communications costs, throughput, average-delay of datagrams, the probability of packet loss, etc. However, the issues depend on the medium the gateway is located. For example, one would like to reduce the cost of an expensive connection media. Or, one would like to reduce the average delay of the packets if the applications need low average delay of the packets. Or, it can be to lower the rate of packet loss on the networks. We concentrated on the delay of the packets over the network and the throughput of the gateways. The OPNET simulations were run for different WAN speeds, different Maximum Transfer Units (MTU), different load generation speeds and packet sizes.

The performance of the system is evaluated by using two different methods: simulation and measurement. The need of using two different methods comes from the lack of FR communication cards and a FR link. In the simulation phase, we modeled the system on OPNET and got performance measures of the system under various traffics that was impossible to get such measures without a protocol analyzer and FR cards on a real network environment. One of these measures that was impossible to take was consisting of average end-to-end delay. However, it is available in OPNET. The measurement phase is performed on real networks. The gateway machines were real PCs. However, the FR side of the gateways were replaced with low speed (compared with FR) serial ports. The measurement is performed just to have an idea about the performance of PCs under real network load and by increasing the serial line speed to see the increase in throughput. The purpose here was to prove that the low throughput values for the system was because of low WAN speed and that the gateways are able to support heavier traffic load if they were equiped with FR boards. The simulation and measurement result, as they will be seen in Section 7.3 and Section 7.4 are compleating each other. More comment about the results of these methods will be given in Section 7.4.

One of the most important issues to consider here is the fragmentation of IP packets coming from Ethernet part and destined over FR network (datagrams whose lengths are greater than MTU of FR). In such cases, the fragmented IP packets will be delayed more (than the unfragmented packets) by the gateways that will result in some cases to internal buffer overflows and/or packet losses. FR communication equipments are theoretically designed to have MTU = 270 bytes/packet but there exist commercial implementations that have MTU = 1500 bytes/packet just to reduce the fragmentation task due to packet size differences between LAN protocols and FR. While the theoretical maximum is 4096 octets corresponding to the maximum integrity of FCS, the actual maximums are vendor specific [9]. The simulation considers these cases to test the performance differences between the theoretical and implemented equipments.

In this study, one simulation is performed to be able to compare two different WAN speeds, namely FR and the conventional RS232C port (port's speed is taken as 9600 bps) of a PC in different gateway buffer sizes for a fixed packet size and MTU. This last case was simulated to indicate the increased rate of performance with FR. One last simulation was performed to examine the packet loss rate for different network traffic load routed over the gateway.

Before going into further detail about the performance evaluation results brief information about performance measures and evaluated setups are given.

7.1 Performance Measures

The performance of an Ethernet network was described in Section 2. All the fixed or user dependent parameters that affect the Ethernet's performance are given again in Section 2. However, it is important to mention about how these parameters affect the performance. The packet length distribution for Ethernet is specified as bimodal with near to the maximum or minimum values [5]. This assumption is correct for IP, too. Except in cases where packet traffic has internetwork characteristics, i.e. the LAN and gateways are on the path of an ftp data transfer, and the maximum MTU of one of the networks on the path is less than Ethernet. In this case most of the packets arrive with fixed length equal to the MTU of the intermediate network. The number of hosts becomes one of the important performance affecting parameter if they become active, e.g. they want to send messages.

The arrival rate of packets is again an important parameter that has a strong relation with the throughput and the buffer overflow characteristics of the gateways. The performance of a network is a multidimensional analysis, it covers measures such as average delay, throughput, channel capacity, fairness, stability, end-to-end response time, so on [5], [49].

The performance measurement can be done in three ways: through mathematical analysis, system simulation and measurement. In this thesis, the system simulation and measurement are performed as performance evaluation methods. For both cases, an understanding of the nature of traffic in the target system and selection of an appropriate random traffic model are critical to the success of the modeling enterprise. Various traffic models and their nature are given in [46]. The Poisson models are mentioned as the oldest traffic models. They are well suited for analytical results but in real life the traffic's nature does never fit into Poisson process. However, the ability of superposition of independent Poisson process and the memoryless property of Poisson makes it, still, popular. The Poisson arrival, being unrealistic for a real network, should be substituted by a self-similar Ethernet traffic as specified in [52]. However, it is known that the beginning times of the packet batches are Poisson distribution. So, one other possibility for packet interarrival distribution could be the Batch Poisson process where the beginning times of packet batches and the number of packets in the batch are distributed as Poisson processes.

The performance measures in such a work should be the throughput of the entire system and of the gateway, the average end-to-end delay characteristics and queue-length behavior of the network [6], [8], [47]. Such work for LAN interconnection with bridges can be found in [48].

7.2 Modeling Setups

It is important to be aware of the trade-off between the model detail and the simulation execution time. Frugal modeling is often called for, i.e., modeling that includes only those network functions that have appreciable impact on the desired performance metrics. However, when an IP gateway is considered, all of the routing functions play an important role on the gateway throughput. The IP gateway has a dynamically changing routing table, ARP table, it discards datagrams if the time to live field is expired, so on. Therefore, the IP and MAC layers must be fully implemented in such a work. Performance evaluations may

consist of only queueing models and analysis over them as in [46] and in [35], but in this work, the model is implemented in detail, up to the source code of IP gateway by modifying and developing the example models of OPNET for simulation. Performance evaluation of the system is measured by continuously sending datagrams between interconnected LAN's over gateways. During simulation, the buffer sizes are taken very small compared to the original system and overflow characteristics are inspected. However, the buffer constraints are not as crucial as in [35] because of the implemented system's enormous dynamic buffer. A minimum input and output buffer size is calculated for the gateway in Section 7.5.

During the simulation, the packet interarrival times are taken as exponentially distributed with various mean values taken from a recent work on wide area TCP connection characteristics and growth trends of it [36], [51]. The packet sizes are taken as either deterministic [5], or random with [6], [8] exponential distribution or uniform distribution. The data is captured by the end nodes by operating Ethernet cards in the promiscuous mode [3], and by using a 'tcpdump' filter on Linux machines. The gateway packet service rates are taken from the real gateway PCs by measurement method.

The simulation setups and performance measures are presented in the following subsections:

7.2.1 Setup 1.a

The goal of this setup is to measure the throughput with different packet sizes. Simulation was done for exponentially distributed packet sizes equal to 100, 250, 350, 1500 bytes/packet, these values are the most common values and are the fragmentation boundary for FR. Four different buffer sizes were considered: 200K, 250K, 300K, 350K. The WAN protocol's MTU = 270, line speed 2 Mbps. Packet interarrival time was exponentially distributed.

7.2.2 Setup 1.b

The goal of this setup is to measure throughput with different packet sizes. Simulation was done for fixed packet sizes equal to 64, 250, 350, 1500 bytes/packet, these values are the most common values and are the fragmentation boundary for FR. Four different buffer sizes were considered: 200K, 250K, 300K, 350K. The WAN protocol's MTU = 270, line speed 2 Mbps. Packet interarrival time was exponentially distributed.

7.2.3 Setup 2.a

The goal of this setup is to find the relation between packet generation speed throughput's convergence to its maximum value. For packet generation speeds (Poisson dist). 40, 51, 68, 112, 167 and 203 packets/sec that are measured data values between 1990 to 1993 [9.] MTUs in this setup were 270 and 1500. Packet sizes were exponential with mean 100 bytes, exponential with mean 1500 bytes. WAN speed 2 Mbps.

7.2.4 Setup 2.b

The goal of this setup is to find the relation between packet generation speed throughput's convergence to its maximum value. For packet generation speeds (Poisson dist). 40, 51, 68, 112, 167 and 203 packets/sec are measured data values between 1990 to 1993 [36]. MTUs in this setup were 270 and 1500. Packet sizes were fixed 64 bytes and 1500 bytes. WAN speed 2 Mbps.

7.2.5 Setup 3

The goal of this setup is to measure the delay vs. link speed. For Poisson packet generation speed with mean 200 packets/sec, exponential packet size (mean 250 bytes). MTU = 270 bytes. WAN link speeds 9600 bps (the implemented setup's speed), 19200 bps (a modem's speed), 64 Kbps (X.25), 384 Kbps (a commercially available multiprotocol communication card, Eicon), 2 Mbps FR.

7.2.6 Setup 4

The goal of this setup is to measure the delay vs. packet generation speed. Designed to check the effects of different packet sizes on the implemented system. WAN speed equals to 9600 bps. MTU equal 1500 bytes/packet, packet sizes are exponential with mean 100, 250 bytes.

7.2.7 Setup 5.a

The goal of this setup is to measure the throughput vs. packet generation speed. This setup is designed to check the increase in performance by increasing the processing power of the gateways by 10 times. MTU equal 270 and 1500 bytes/packet, packet sizes are exponential with mean 100 bytes/packet.

7.2.8 Setup 5.b

The goal of this setup is to measure the throughput vs. packet generation speed. This setup is designed to check the increase in performance by increasing the processing power of the gateways by 10 times. MTU equal 270 and 1500 bytes/packet, packet sizes are exponential with mean 1500 bytes/packet.

7.3 Simulation Results

The results of the computer simulations by using OPNET are given in the tables and graphs of this section.

7.3.1 Setup 1.a

Constant values for the simulation:

- WAN Speed = 2 Mbps
- MTU of FR = 270 bytes
- Packet generation speed from LAN 1 (from source) Poisson with mean = 200 packets/sec
- Packet sizes are exponential

The results of the simulation can be seen in Table 7.1 and Figure 7.1.

Table 7.1. Simulation results for setup 1.a.

Packet Sizes (bytes/packet)	Gw Service Rate (Packets/sec)	Throughput (Packets/sec)
100	370	184
250	313	125
300	245	92
1500	157	22

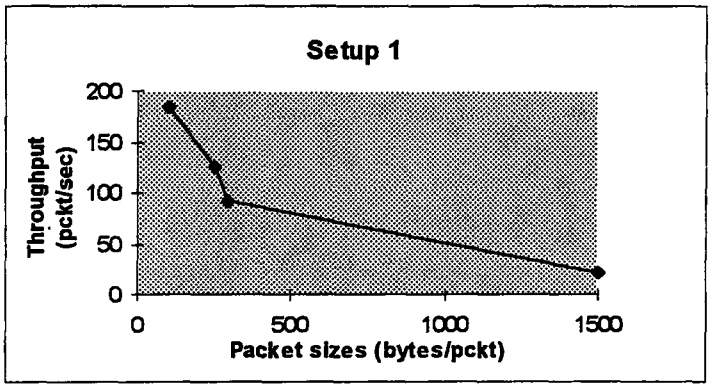


Figure 7.1. Setup 1.a's resulting graph.

The sharp decrease around 250 and 300 byte/packet sizes, is caused by the fragmentation done at IP layer due to MTU of FR (270 bytes/packet). The simulation showed the same behavior for 4 different buffer sizes since the buffers were too large, but smaller than the implemented system.

7.3.2 Setup 1.b

Constant values for the simulation:

- WAN Speed = 2 Mbps
- MTU of FR = 270 bytes
- Packet generation speed from LAN 1 (from source) Poisson with mean = 200 packets/sec
- Packet sizes are fixed

The results of the simulation can be seen in Table 7.2 and Figure 7.2.

Table 7.2. Simulation results for setup 1.a.

Packet Sizes (bytes/packet)	Gw Service Rate (Packets/sec)	hroughput (Packets/sec)
64	370	180
250	313	104
300	245	83
1500	157	20

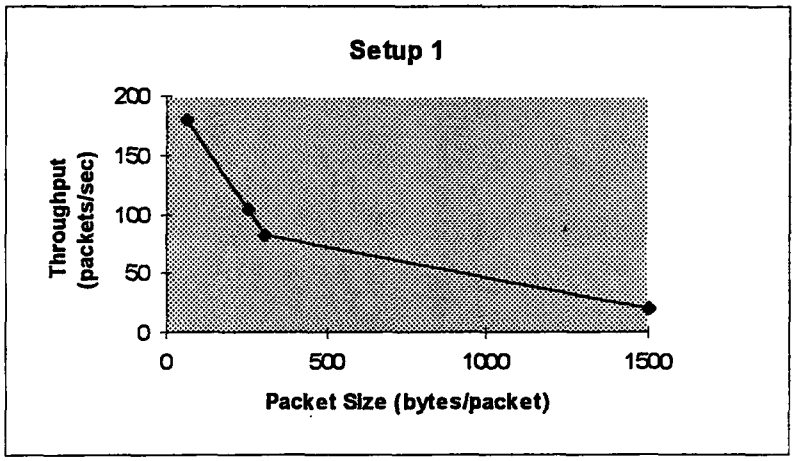


Figure 7.2. Setup 1.a's resulting graph.

The sharp decrease around 250 and 300 byte/packet sizes, is caused, again, by the fragmentation done at IP layer due to MTU of FR (270 bytes/packet). The simulation showed the same behavior for 4 different buffer sizes. The fixed packet sized model behaves very similar to the exponential packet sized one.

7.3.3 Setup 2.a

Constant values for the simulation:

- WAN Speed = 2 Mbps
- MTU of FR = 270 and 1500 bytes
- Buffer size = 300 Kbytes
- Packet size distribution: Poisson with mean = 100 bytes/packet

The results of the simulation can be seen in Table 7.3 and Figure 7.3.

Table 7.3. Throughput for MTU =270 and 1500

Pckt. Gen. Speed (Packets/sec)	Throughput (Packets/sec)
40	40
51	51
68	66
112	112
167	167
203	183

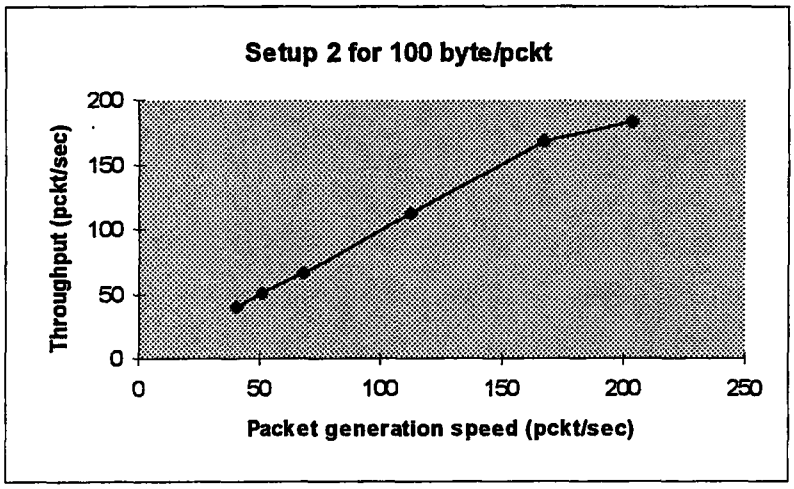


Figure 7.3. Throughput for MTU = 270 and 1500.

The results for MTU = 270 and 1500 are the same since the packets are not fragmented yet.

The same setup for 1500 bytes/packet is presented below.

Constant values for the simulation:

- WAN Speed = 2 Mbps
- MTU of FR = 270 and 1500 bytes.
- Buffer size = 300 Kbytes
- Packet size distribution: Poisson with mean = 1500 bytes/packet

The results are as follows (Table 7.4, Table 7.5, and Figure 7.4).

Table 7.4. Throughput for MTU =270.

Pckt. Gen. Speed (Packets/sec)	Throughput (Packets/sec)
40	21
51	21
68	21
112	21
167	21
203	21

Table 7.5. Throughput for MTU =1500.

Pckt. Gen. Speed (Packets/sec)	Throughput (Packets/sec)
40	39
51	48
68	59
112	66
167	66
203	66

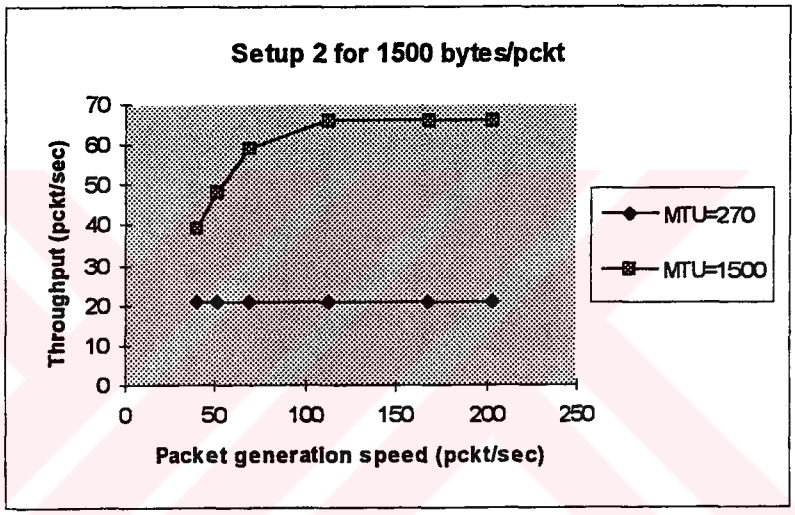


Figure 7.4. Throughput convergence for MTU = 270 and 1500 for 1500 byte/packet

As seen in Figure 7.4, the fragmentation is the main slowing and time consuming factor in the setup. Also, in MTU = 1500 the fragmentation is not done, which improves the throughput, but up to the point where the service time of the gateway becomes the main limiting factor of the throughput.

7.3.4 Setup 2.b

Constant values for the simulation:

- WAN Speed = 2 Mbps
- MTU of FR = 270 and 1500 bytes
- Buffer size = 300 Kbytes
- Packet size distribution: fixed 64 bytes/packet

The results of the simulation can be seen on Table 7.6 and Figure 7.5.

Table 7.6. Throughput for MTU =270 and 1500

Pckt. Gen. Speed (Packets/sec)	Throughput (Packets/sec)
40	40
51	51
68	68
112	112
167	167
203	188

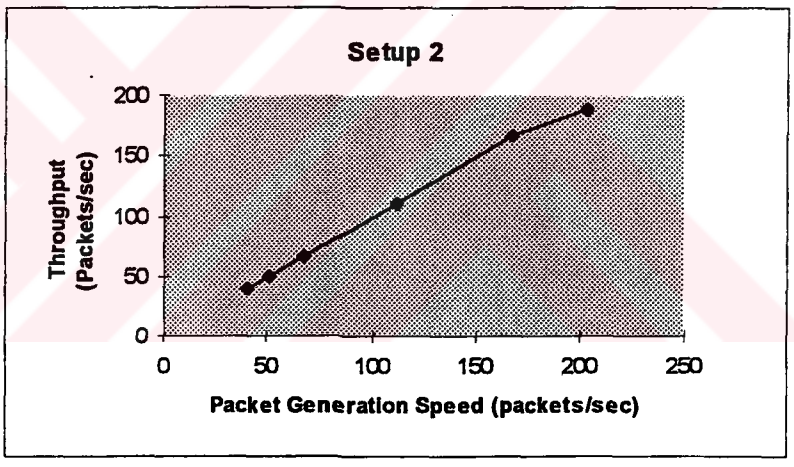


Figure 7.5. Throughput for MTU = 270 and 1500.

The results for MTU = 270 and 1500 are the same since the packets are not fragmented.

The same setup for 1500 bytes/packet is presented below.

Constant values for the simulation:

- WAN Speed = 2 Mbps
- MTU of FR = 270 and 1500 bytes.
- Buffer size = 300 Kbytes
- Packet size distribution: fixed 1500 bytes/packet

The results are as follows (Table 7.7, Table 7.8, and Figure 7.6).

Table 7.7. Throughput for MTU =270.

Pckt. Gen. Speed (Packets/sec)	Throughput (Packets/sec)
40	20
51	20
68	20
112	20
167	20
203	20

Table 7.8. Throughput for MTU =1500.

Pckt. Gen. Speed (Packets/sec)	Throughput (Packets/sec)
40	40
51	51
68	62
112	63
167	63
203	63

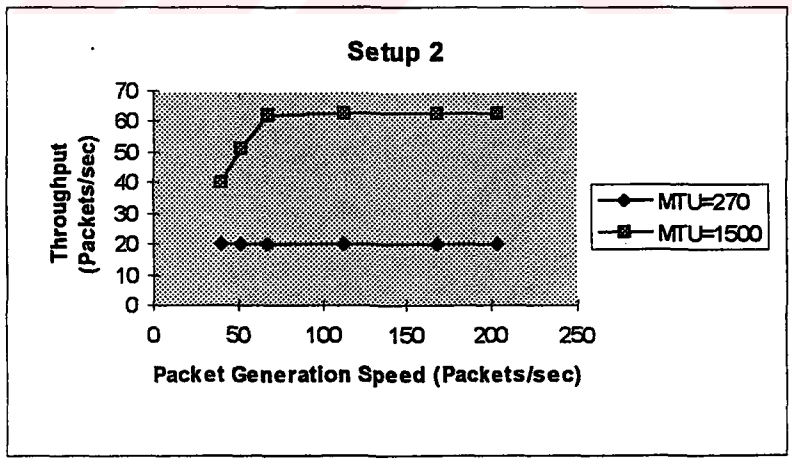


Figure 7.6. Convergence to maximum throughput for MTU = 270 and 1500 for 1500 byte/packet

As seen in Figure 7.6, the fragmentation is the main slowing factor in the setup. In the Table 7.7 it is shown that the gateway is processing at most 20 packets/sec because of the fragmentation overhead. Also, in MTU = 1500 the fragmentation is not done, which improves the throughput, but up to the point where the service time of the gateway becomes the main limiting factor of the throughput.

7.3.5 Setup 3

The main issue here is to compare different WAN speeds. Constant values for the simulation are:

- MTU = 270 bytes
- Packet size (exponentially distributed) = 250 (In order to ignore the effect of the fragmentation)
- Packet generation speed (Poisson) = 200 packet/sec.

For this setup the simulation results are given in the graphs in Figure 7.7, Figure 7.8 and in Table 7.9.

Table 7.9. Setup 3 results.

WAN Speed	Delay (msec)	Throughput (Packets/sec)
9600 bps	17000	5
19200 bps	4000	10
64 Kbps	1180	30
384 Kbps	146	124
2 Mbps	140	125

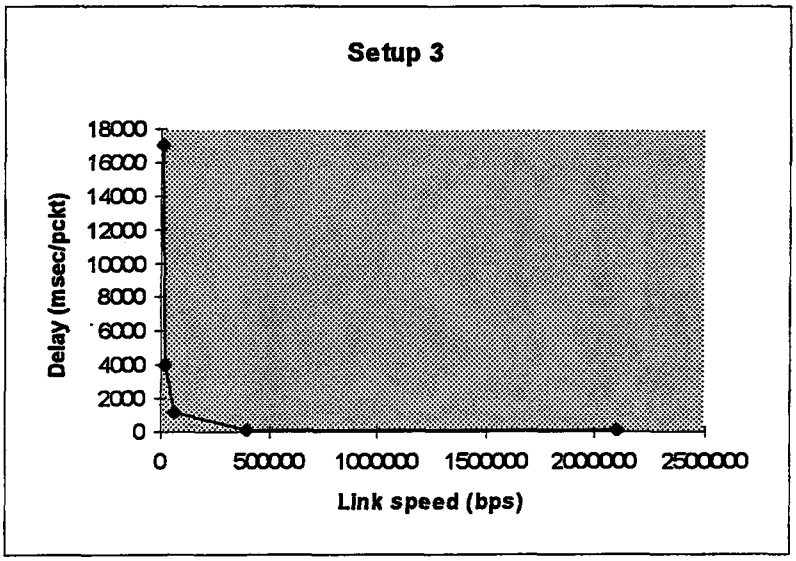


Figure 7.7. Comparison of different WAN speeds vs. delays.

The delay, as expected, decreases from 17 sec to 140 msec as we increase the speed of the WAN protocol. However, again, the service rate of the router plays an important role after the WAN speed 384 Kbps, since, the line converges to a delay of 140 msec after 384 Kbps.

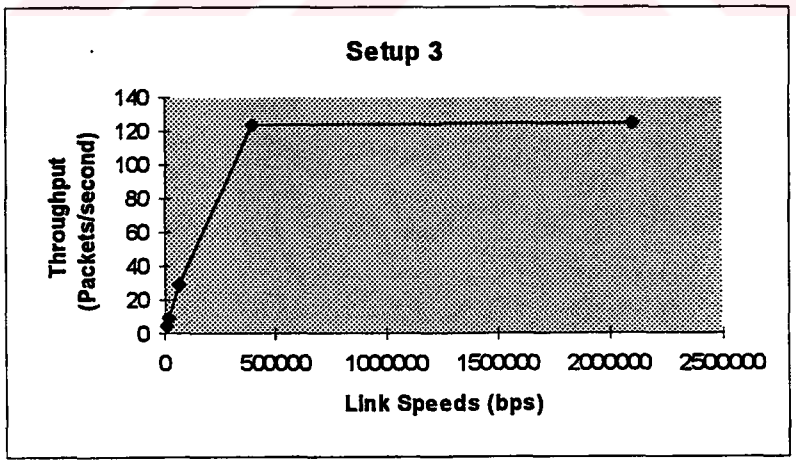


Figure 7.8. Comparison of different WAN speeds vs. throughputs.

As it can be seen from the graph in Figure 7.8, the throughput converges after the 384 Kbps WAN speed. This convergence is due to the packet service rate of the gateway.

Which means that with faster gateway service rate, we could increase the throughput and FR would not be the bottleneck of the communication setup.

7.3.6 Setup 4

This setup is designed to see the performance of the implemented system. The simulation is designed to compare the simulation results with the real system which consists of two PCs running Linux operating system. They are connected over their serial ports by using point-to-point (PPP) protocol. The results consists of only the simulation of the setup because of the lack of FR communication equipments in the laboratory and also the lack of a protocol analyzer that would serve to measure the performance of the whole system. The setup is designed to show the delays encountered at different packet generation speeds.

Constant values for the simulation:

- MTU = 1500 bytes
- WAN speed = 9600 bps

For this setup the simulation results are given in the graph of Figure 7.9 and in Table 7.10.

Table 7.10. Simulation results for the implemented system.

	Packet size = 100 bytes	Packet size = 250 bytes
Packet Gen. Sp. (packets/sec)	Delay (sec)	Delay (sec)
40	27	16
51	27	16
68	27	16
112	27	16
167	27	16
203	27	16

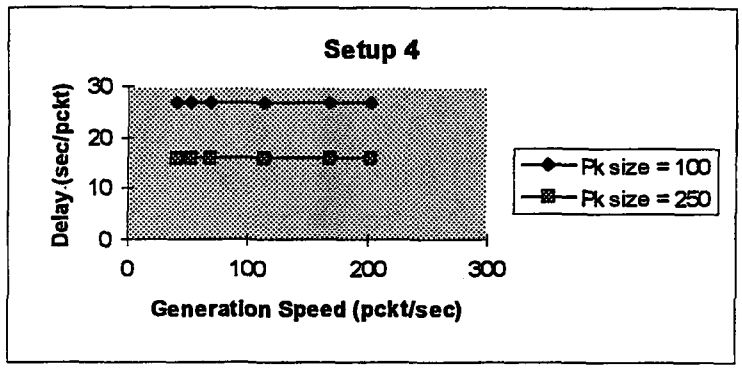


Figure 7.9. Simulation results for the implemented system.

As it can be deduced from the graph, the gateway always loses packets and the packets are always delayed at this line speed. The cause of this is the slowness of the WAN speed (9600 bps) at the first rank but also as we have seen from previous setups that after the critical value of the link speed, the gateway's service rate becomes the bottleneck for the communication. The gateway's performance could be measured in lower packet generation speeds (which will be done on the real system) in order to have meaningful results, but the main issue in these tests was to measure the behavior of the setups on a real network environment of average load (measured in [28]). All the values are taken from real measurements during 1990-1993.

7.3.7 Setup 5.a

This setup is designed to see the performance of a dedicated gateway that is 10 times faster than the PC's speed. In the implemented system, the main bottleneck was the service rate of the gateway per packet. The slowness of the PCs were because of the operating system overhead at the first rank and the slowness of the internal bus of the machine. This simulation is designed to measure the throughput of such a faster gateway with packet size 100 bytes/packet (exponentially distributed) and Poisson arrivals with 40, 51, 68, 112, 167 and 203 packets/sec.

Constant values for the simulation:

- MTU = 270 and 1500 bytes
- WAN speed = 2 Mbps
- Packet size = 100 bytes/packet (exponential)

For this setup the simulation results are given in the graph of Figure 7.10 and from the Table 7.11.

Table 7.11. Throughput for MTU =270 and 1500.

Pckt. Gen. Speed (Packets/sec)	Throughput (Packets/sec)
40	40
51	50
68	68
112	110
167	160
203	186

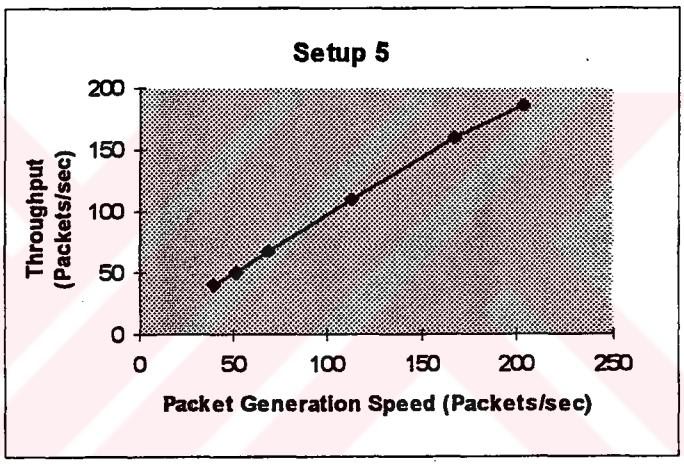


Figure 7.10. Throughput values for the faster gateway.

The graph proves that the gateway's speed was the bottleneck of the implemented system and the WAN speed of FR is sufficient for the specified packet generation speeds. This simulation is done for small packets of 100 bytes/packet. The next setup will show the effect of fragmentation on such a fast gateway.

7.3.8 Setup 5.b

Throughput vs. packet generation speed. The faster gateway will have to route in this setup packets of size 1500 bytes (exponentially distributed). The MTU value is taken as 270 and 1500 bytes/packet, the purpose of the setup is to investigate the effect of fragmentation on the gateway's throughput performance. The packets are fragmented at MTU = 270 bytes

value (the standard) and not fragmented at MTU = 1500 bytes (vendor specific implementations).

Constant values for the simulation:

- MTU = 270 and 1500 bytes
- WAN speed = 2 Mbps
- Packet size = 1500 bytes/packet (exponential).

For this setup the simulation results are given in the graph of Figure 7.11 and in Table 7.12 and Table 7.13.

Table 7.12. Throughput for MTU =270.

Pckt. Gen. Speed (Packets/sec)	Throughput (Packets/sec)
40	40
51	49
68	52
112	53
167	54
203	54

Table 7.13. Throughput for MTU =1500.

Pckt. Gen. Speed (Packets/sec)	Throughput (Packets/sec)
40	40
51	50
68	66
112	100
167	120
203	125

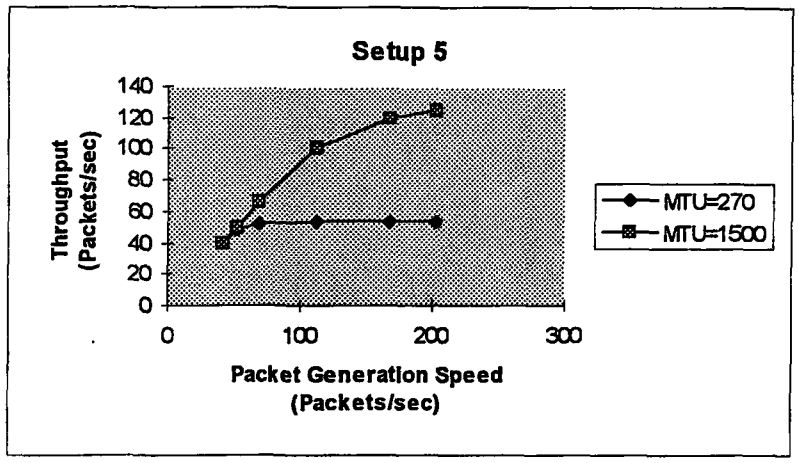


Figure 7.11. Throughput for faster gateway.

The graph represents the bottleneck of MTU over gateway's packet processing speed. The throughput of the gateway slows down to 54 packets/sec with the fragmentation.

As a conclusion for LAN interconnection the MTU=1500 bytes/packet of FR gives better performance than the MTU=270 bytes/packet. This is obvious that increasing the MTU from 270 to 1500 would give a better performance but there is still future work on this subject. For example, the fragmentation at FR layer would be a good subject to investigate. Another proposal would be an intermediate layer between FR and IP that would do only the fragmentation in necessary cases.

7.4 Test Results

The implemented system's test results are given in this Section. The tests are done in the same configuration as OPNET. The tested system can be seen in Figure 6.3. The packets are generated from a source PC located at Netlab segment. For all tests the generator was generating fixed sized packets with exponential interarrival times. The tests are done for packet sizes equal to 100, 250, 500, 1500 bytes. Packet generation speed is taken small since two gateways were not identical (Refer to Section 6.2). The bottleneck of the system was the serial line speed of the PCs used. However, because of enormous buffer sizes there was no lost packets in the system. All the packets sent from one side and were received

from the other side of the interconnected LANs (they were delayed but received). As it is specified above the reason of this is the enormous buffer size of the gateways, but in a *normal* and/or *bursty* traffic load the gateway will have buffer overflows very often.

Various serial line speeds are tested on the WAN side of the gateways. The tested values are as follows:

- 9600 bps
- 19200 bps
- 38400 bps
- 48000 bps
- 52800 bps
- 57600 bps
- 115000 bps

The gateway machine supported up to the WAN speed of 38400 bps. The throughput values for different packet sizes (fixed) and different packet generation speeds are given in Table 7.14 and Figure 7.12.

Table 7.14. Throughput values for different packet sizes and WAN speeds.

	Throughput (Packets/sec)			
WAN Line Speed (bps)	100 bytes/pkt	250bytes/pkt	500bytes/pkt	1500bytes/pkt
9600	5	2	1	0.33
19200	10	4	2	0.66
38400	20	7.8	4	1.33

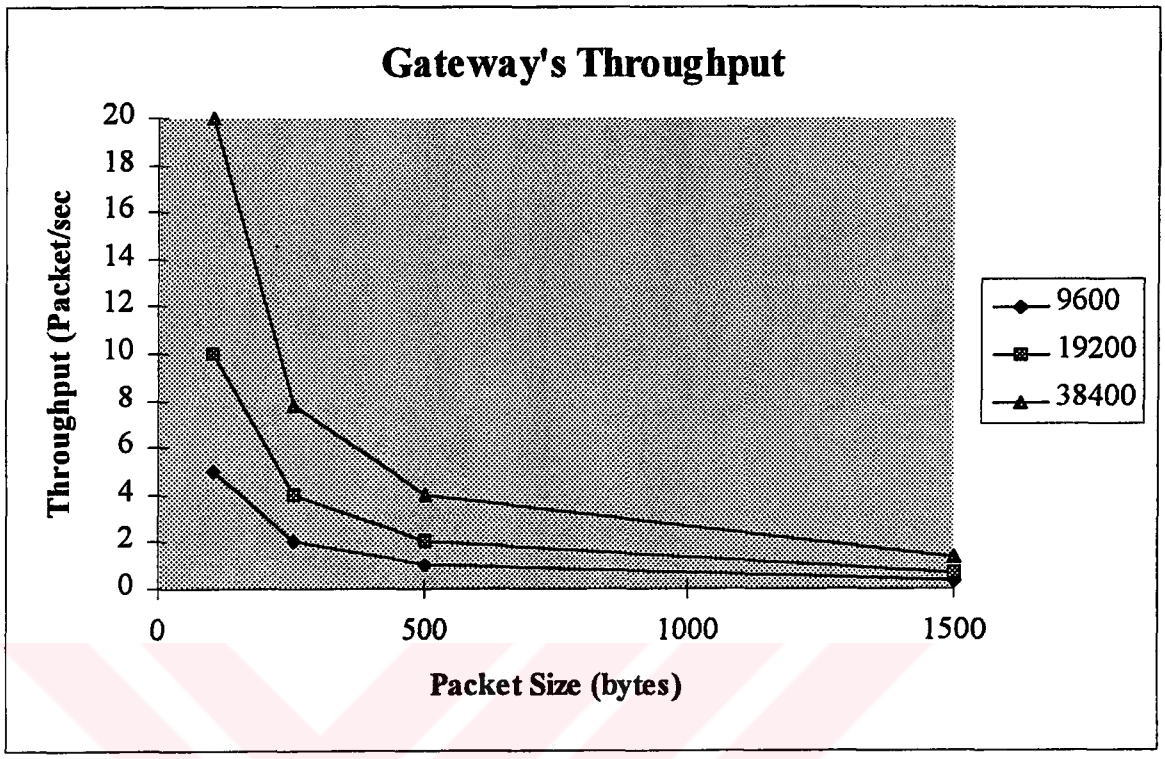


Figure 7.12. Maximum throughput of the implemented system.

The measured system consists of two gateway machines and two test machines located at different LANs as shown in Figure 6.3. The gateways are connected through their serial ports with a point to point protocol called PPP. The speed of the serial ports of gateway machines are set to 9600, 19200 and 38400 bps that are very small compared to FR's 2 Mbps speed. In this testing, it is shown that because of slow line speed on WAN side of gateway machines, the system cannot pass the limit of 20 packets/sec throughput that decreases with the increased packet sizes. This is proven by the increasing throughput with the increasing line speed of the system. The main bottleneck of the test system is the slow line speed of the serial port of PC. This is obvious, since there exists an enormous speed difference between Ethernet and the serial port. As a conclusion, a PC machine would give better performance and throughput on the system with a FR communication card as shown in the OPNET simulation results. However, the main issue in this thesis is not measuring the performance of a PC but the performance of a dedicated gateway machine, and also another issue is to investigate the difficulties encountered while designing such a system.

It is reported that a PC AT of 16 Mhz can route IP packets of 1500 bytes/packet up to 4.1 Mbps over Ethernet LANs. This performance is reached with WD8003E 8-bit Ethernet cards. Which means that an AT machine can do the routing of a heavily loaded Ethernet

LAN (4/10 of the whole bandwidth used). The software *pcroute* can be obtained from anonymous ftp [55]. This information proves that a PC can do the routing of an Ethernet LAN especially over FR. Also, a PC is well suited for the whole FR switch design (Figure 6.2).

Some work should be done about the IP fragmentation process especially when connection oriented WAN protocols are used between gateways. The bottleneck of the IP router is the fragmentation process. Because in the routing process, the gateway processes only the header of the datagram (that is 20 octets in general), but during the fragmentation process gateways have to process the whole packet. In order to improve the performance of the gateway, we should improve the fragmentation speed of the machine or we should not let the gateway fragment most of the packets by choosing WAN interconnection protocols with the same MTU as the Ethernet. The performance of a gateway can be improved by connecting it to networks where the gateway will not have to fragment packets because of the MTU compatibility between different networks. That was the main reason where the gateway's performance was improved in the setups that used MTU of FR equal to 1500 bytes/packet.

The performance measures in this study could be more accurate and several other issues could be investigated if we could test the system with a protocol analyzer. The real system's testing with FR boards and software will be possible after the availability of the necessary hardware [42] and software drivers.

7.5 Effect of Finite Buffer

The buffer sizes that are required by the gateways are calculated in this section. The gateways are modeled as M/M/1/m queues. Where m is the buffer size of the port buffers of the IP gateway. The system, seen in Figure 7.13, represents the gateway and the FR link.

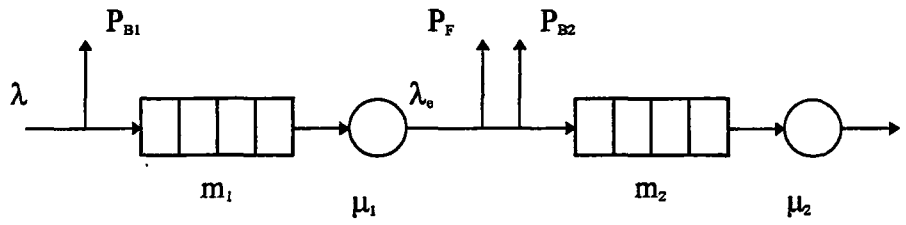


Figure 7.13. Queueing model of the gateway

m_1 and m_2 are the buffer sizes of the input buffer and the FR link buffer accordingly expressed as packets.

P_{B1} and P_{B2} are the blocking probabilities due to limited buffer sizes.

P_F is the probability of filtering. In our example, 5 % of the Ethernet traffic is filtered and 95 % is routed over FR link (according to [50]).

λ represents datagram arrival rate (in this example it is taken as 200 packets/sec, Poisson distribution).

λ_e is the effective arrival rate and is given as,

$$\lambda_e = \lambda(1-P_{B1}) \qquad (7.1)$$

μ_1 and μ_2 are the gateway's and the FR line's service rates (as packet/sec).

$\mu_1 = 3700$

$\mu_2 = 174$

Our aim is to calculate first the necessary buffer size m_1 for the input port so that there will be no buffer overflow. No buffer overflow means a negligible blocking probability (P_{B1} and P_{B2} are less than 10^{-10}.) Then the necessary output buffer size m_2 will be calculated according to $\lambda_e(1- P_F)$ which is the remaining part after the filter operation.

ρ is the utilisation and,

$$\rho = \frac{\lambda}{\mu} \tag{7.2}$$

P_n is the probability of having n packets in the waiting queue and is given as follows [51]:

$$P_n = \frac{(1-\rho)\rho^n}{1-\rho^{n+1}} \quad \text{for } \rho<1 \tag{7.3}$$

It is known that,

$$P_B = P_m \qquad \text{where } m \text{ is the buffer size} \tag{7.4}$$

The input buffer blocking probability versus the buffer size graph is given in Figure 7.14 and the plotted values are in Table 7.1.

Table 7.1. Buffer size versus probability of blocking for input buffer

m	λ=40	λ=51	λ=68	λ=112	λ=167	λ=203
1	0.010695187166	0.013596374300	0.018046709130	0.029380902413	0.043185932247	0.052011273379
2	0.000115610278	0.000187374368	0.000331559281	0.000888577584	0.001945410887	0.002845471672
3	0.000001249839	0.000002582721	0.000006093485	0.000026896760	0.000087798674	0.000156092050
4	0.000000013512	0.000000035600	0.000000111988	0.000000814172	0.000003962789	0.000008563896
5	0.000000000146	0.000000000491	0.000000002058	0.000000024645	0.000000178861	0.000000469857
6	0.000000000002	0.000000000007	0.000000000038	0.000000000746	0.000000008073	0.000000025779
7	0.000000000000	0.000000000000	0.000000000001	0.000000000023	0.000000000364	0.000000001414
8	0.000000000000	0.000000000000	0.000000000000	0.000000000001	0.000000000016	0.000000000078
9	0.000000000000	0.000000000000	0.000000000000	0.000000000000	0.000000000001	0.000000000004

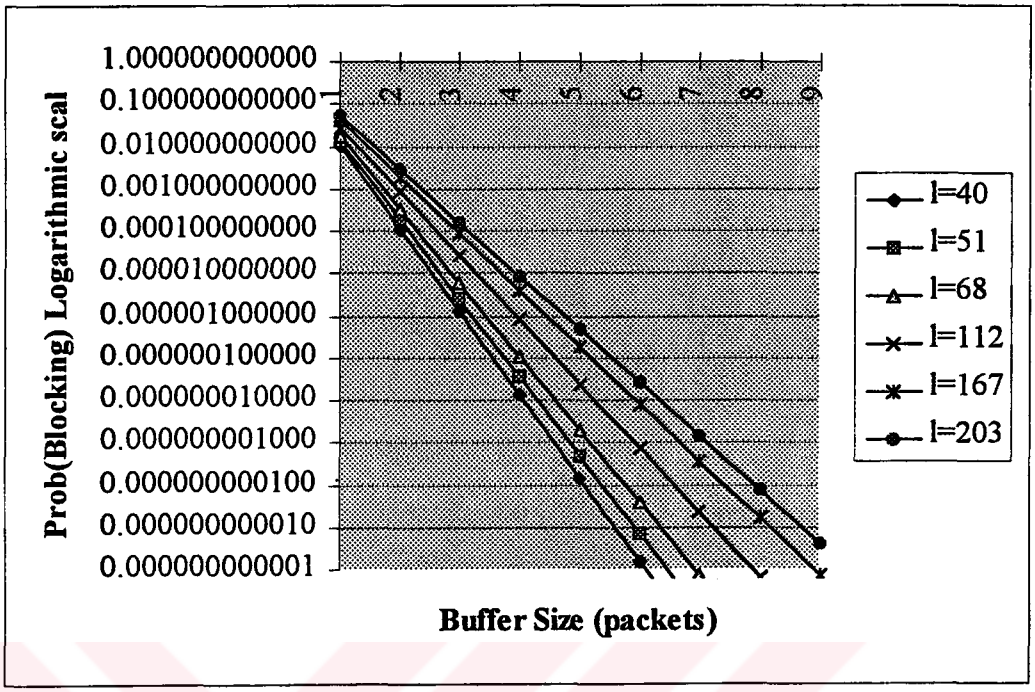


Figure 7.14. Probability of blocking for incoming packets

As it can be seen from Table 7.1 and Figure 7.14, a buffer of 8 packets is sufficient for the case. A buffer of 12000 bytes is sufficient for the maximum amount of incoming packet traffic for 1993 [9] (see Section Setup 2). This value is tested and approved by using OPNET Modeller and it did not give any buffer overflow for input buffer for a buffer size of 9 packets (1 for the MAC layer and 8 for IP).

For a buffer of 8 packets the blocking probability is negligible and,

$$\lambda_e = \lambda \tag{7.5}$$

The incoming traffic to the FR line buffer is,

$$\lambda(1-P_B) \tag{7.6}$$

However, in bursty traffic or in real cases this size for the input buffer may not be sufficient because this kind of traffic is more complex and more detailed models are needed as specified in [50].

The exterior traffic (in worst case) was specified as 95 % of the whole traffic observed on Ethernet according to [50]. Thus,

$$P_r = 0.05 \tag{7.7}$$

Considering the filtering, λ values for FR link buffer become, 38, 49, 65, 107, 159 and 193 packets/sec.

The input buffer blocking probability versus buffer size graph is given in Figure 7.15.

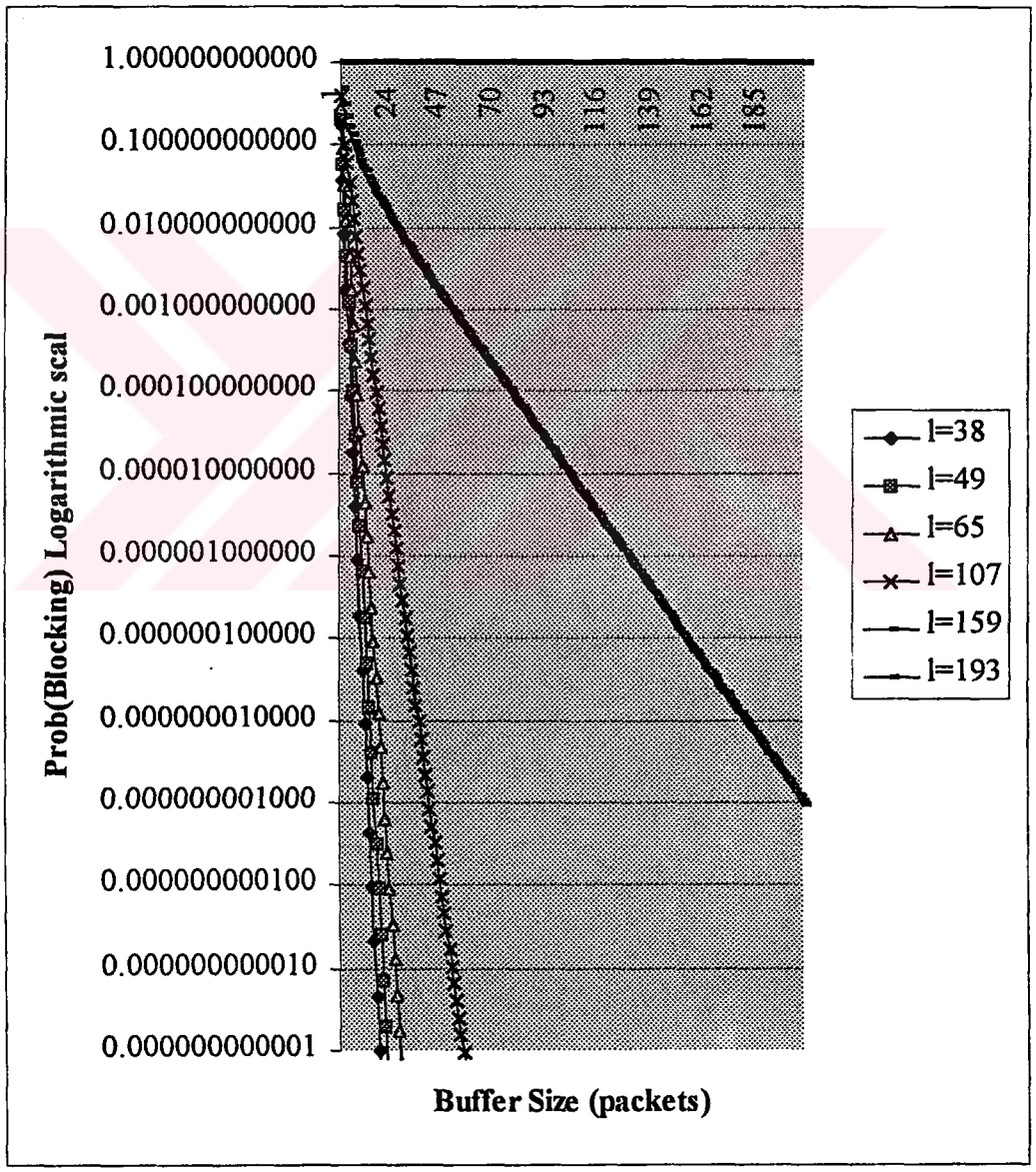


Figure 7.15. Probability of blocking for outgoing packets

As seen from the above graph, the blocking probability for 1500 bytes packets at the packet generation rate of 193 packets/sec is around 1 and does not decrease. The main reason of this situation is the line speed of FR. Since, FR can give a service of μ_2 =174 packets/sec (packet sizes are (fixed length) 1500 bytes/packet, and the line speed is 2 Mbps) there will be output buffer overflows. This is the point where the constraint ρ<1 is not satisfied and λ_2, the input traffic to the FR line in the gateway (95% of the 203 packets/sec input traffic to the gateway),

$$\lambda_2 > \mu_2 \tag{7.8}$$

This is an unstable system and the blocking probability is equal to 1.

In the OPNET model of the setup, the FR speed is raised to 10 Mbps to be able to measure the necessary input buffer of IP layer, since it is proven above that the FR line buffer will be unsufficient for loaded internetwork traffic and will be the bottleneck of the system. When it is raised to 10 Mbps the input buffer and the performance of the server will be measured easily.

8. Conclusion

This thesis presents the performance evaluation of a LAN interconnection device, namely, an Internet Protocol router (IP gateway). The gateway connects two LANs over a WAN protocol connection, namely, FR . In this work, a well known Local Area Network: Ethernet, a Wide Area Network: FR, LAN interconnection aspects, routing and performance evaluation of interconnected LANs are studied.

Today's faster applications need faster communication protocols. With the changing nature of the communication data, the interconnection became more crucial. With the increased need to transfer real time data, the performance of interconnection devices becomes increasingly important. This thesis, proposes an economic and faster method compared to traditional methods such as X.25. FR is a better solution than X.25, but not faster than ATM (Asynchronous Transfer Mode). However, FR is more economical than ATM.

One of the research purposes was to study Ethernet to FR routing problems. It is discovered that there are three types of basic problems while interconnecting two LANs over FR. These are due to the connection orientedness of FR, communication speed differences and MTU incompatibilities. As we know, Ethernet is a 10 Mbps network and FR is a 2.048 Mbps network. The packets are broadcasted in Ethernet, it is connectionless. However, in FR we need to establish a virtual circuit (in our case a permanent virtual circuit) from the source to destination. The last problem is the MTU of two networks. Ethernet has an MTU of 1514 bytes/packet, whereas FR has a MTU of 270 bytes/packet.

The data transfer rate difference between two networks is an important issue. However, it is not a significant problem since all IP packets on the Ethernet side are not required to be send to the other LAN through FR. The only implication of this speed difference is that the Ethernet side of the gateway has to have a relatively larger buffer compared to the FR side (a buffer size calculation for the gateway can be found in Section 7.5.) The connection type difference, also, is not a significant problem. The gateway, at the boot time, can make the necessary permanent virtual circuit connections (according to its recent tables) and keep the circuits permanent until the system shutdown. This is proposed instead of establishing a new connection for each transfer need over FR and closing the connection after the transfer. If a new circuit is needed, it can establish one and keep it permanent.

As a solution to the fragmentation problem of packets, while passing from the Ethernet side to the FR side (especially, for packets whose sizes are greater than MTU of FR) a second layer fragmentation is proposed by [27]. Another method can be proposed for only fragmentation. This new method is to introduce an inter-layer fragmentation layer between IP and FR layers. This proposal is given in Section 8.1 since it has not been implemented in this thesis, but proposed in [19].

Finally, the complete system is simulated in a powerful network simulation tool OPNET. The formed model in OPNET was a full implementation (including the source code) of TCP/IP protocol stack and Ethernet. The source codes of the example models are modified to be able to have the necessary performance measure results that were lacking in the example models. In this phase, average end-to-end delay and throughput variables are added to the appropriate place in the code. The interconnected network system is tested under various scenarios. These scenarios are designed to study the effect of packet size on the throughput of the gateways, the effect of packet generation speed on the throughput of the gateways. One scenario was designed to study the delay behaviour of the routed datagrams under different WAN interconnection protocol speeds. Delay characteristic of datagrams is studied when the WAN protocol speed is 9600 bps, this last is performed to compare the simulation and measurement results. A last simulation setup is designed to study the effect of increase in performance by increasing the processing power of the gateway.

The real system measurements are also given to compare with the simulation results. The real system measurements are implemented with the moderate facilities provided by the Computer Engineering Department. Because of the lack of a protocol analyzer the real measurements are lacking to be accurate.

In all these setups, it is found that, the speed of FR is offering a better price-performance result compared to older protocols. This is due to less protocol overhead and high speed offered by FR. The MTU of FR is specified in standards as 270 bytes/packet, this value is found to be the bottleneck in Ethernet LAN interconnection. The reason was the huge MTU difference between Ethernet and FR, and that the gateway was always fragmenting datagrams bigger than 270 bytes. This last was the most time consuming factor in the routing phase. A new, non-standard MTU value is studied under different packet size traffic and found to be more suitable for Ethernet LAN interconnection. This new value is the same MTU value as the Ethernet (1500 bytes/packet). When this MTU value is used the gateways will not have to fragment the datagrams and in this manner the throughput will be increased. However, in the thesis a new intermediate fragmentation layer to the FR

side is proposed. This is proposed to be used in standard FR, MTU=270 . This intermediate layer is proposed to make the datagram fragmentation to prevent the fragmentation of packets in IP layer (which is more time consuming then simple fragmentation).

The packet size is a bottleneck in the system, since while being transmitted over FR line big packets are delayed more. However, in gateways the bigger the packet the smaller is the delay. Which means that more data is carried by the packet but the processing speed is the same with smaller datagrams, this is a performance increasing factor. The packet generation speed also is affecting the performance of the system. In heavy traffic loads with large packets the gateway was suffering to route them due to insufficient FR speeds. However, these big and continuous traffic is not very often in real network environment and packet loses are controlled with TCP protocol.

The measurement phase is performed to show the effect of the line speed's effect of the throughput and the delay. The delay of the packets are found to be big as given in Setup 4 results, which proves the validity of the OPNET results.

8.1 Future Work

As a future work, the inter layer fragmentation module can be implemented and tested for increased or decreased performance. The multiprotocol interconnect over FR can be implemented and measured to be able to compare with the inter layer module.

Another future work can be the modeling of the whole university's computer network on OPNET and as an exterior gateway the proposed system can be used. Performance evaluation of the gateway and FR can be compared with the current values presented in the thesis.

The system with FR cards and drivers can be evaluated by using a protocol analyzer to give more accurate results. Since a protocol analyzer would be very useful for taking accurate measurements.

Full FR Protocol should be implemented after the serial communication card is finished.

A dedicated IP Router design would be a interesting study for the Ethernet to FR LAN interconnection. Since a dediaceted router does not have to deal with a multitasking operating system overhead and other processes.

It is known that packet traffic is very often modelled as a Poisson process, in fact, the behaviour of LAN traffic is burstier than the Poisson Model. It is shown in [52] that the Ethernet traffic is self-similar. The gateway can be simulated with a self-similar Ethernet traffic model for more realistic results.

9. References

1. Tanenbaum, A. S, *Computer Networks*, 2nd Ed, Prentice-Hall International, New Jersey, 1989.

2. Comer, D. E, *Internetworking with TCP/IP*, Vol. 1, 2nd Ed, Prentice-Hall International, New Jersey, 1991.

3. Shoch, F. S., and J. A. Hupp, "Measured Performance of an Ethernet Local Network,"Vol.23, No. 12, *Communications of the ACM*, pp. 711-721, December 1980.

4. Rodrigues, M. A., and V. R. Saksena, "Performance Analysis of a LAN/WAN Bridging Architecture",Vol. 9, No. 2, *IEEE Journal on Selected Areas in Communications*, pp. 265-270, February 1991.

5. Boggs, D. R., J. Mogul, C. A. Kent, "Measured Capacity of an Ethernet: Myths and Reality," *ACM SIGCOMM*, pp. 222-234, 1988.

6. Gupta, S. And K. W. Ross, "Performance Modeling and Optimization of Interconnected Ethernets," *Proceedings of the IEEE INFOCOM*, pp. 1353-1359, 1991.

7. Fowler, H. J., and W. E. Leland, "Local Area Network Traffic Characteristics, with Implications for Broadband Network Congestion Management," Vol. 9, No. 7, *IEEE Journal on Selected Areas in Communications*, pp. 1139-1149, September 1991.

8. Beuerman, S. L., and E. J. Coyle, "The Delay Characteristics of CSMA/CD Networks," Vol. 36, No. 5, *IEEE Transactions On Communications*, pp. 553-563, May 1988.

9. FR Forum, FR: Networks for Tomorrow and Today, 1995.

10. Stallings, W., *Local and Metropolitan Area Networks*, 4. Ed., Macmillan Publishing Co., New York, 1993.

11. Datapro Research Group, "Technology Overview: FR", *Datapro Reports on PC & LAN Communications*, pp. 717 101-116, March 1991.

12. Levi, A., "Development of FR Software for High Speed Packet Switched Networks," M.S. Thesis, Boğaziçi University, 1993.

13. Cavanagh, J. P., "Applying the FR Interface to Private Networks," *IEEE Communications Magazine*, pp. 48-64, March 1992.

14. Rahnema, M., "FRing and the Fast Packet Switching Concepts and Issues," *IEEE Network Magazine*, pp. 18-23, July 1991.

15. Stallings, W., "Faster Packet Networks," *Byte*, pp. 172-181, November 1991.

16. Heinanen, J., "FR as a Multiprotocol Backbone Interface," *Computer Networks and ISDN Systems*, pp. 363-369, 1992.

17. Taylor, S. A., "Frame Transport Systems," *IEEE Communications Magazine*, pp. 66-70, March 1992.

18. Ali, M. I., "FR in Public Networks," *IEEE Communications Magazine*, pp. 72-78, March 1992.

19. Küçükateş, R., C. Ersoy, "Interconnecting local area networks over FR," *Proceedings of the ninth International Symposium on Computer and Information Sciences*, Belek-Antalya, 7-9 November 1994, pp. 377-384, 1994.

20. Platt, A., and M. J. Morse, "Traffic Management in FR Networks," *Computer Networks and ISDN Systems*, pp.305-316, 1992.

21. Marsden, P., "Internetworking IEEE 802/FDDI LAN's Via the ISDN FR Bearer Service," Vol. 79, No. 2, *Proceedings of the IEEE*, pp. 223-229, February 1991.

22. Hunt, C., *TCP/IP Network Administration*, O'Reilly & Associates Inc., Sebastopol, 1992.

23. Reynolds, J., J. Postel, "Assigned Numbers," *Network Working Group Request for Comments 1010*, 1987.

24. Postel, J., "Multi-LAN Address Resolution," *Network Working Group Request for Comments 925*, 1984.

25. Postel, J., "Internet Control Message Protocol," *Network Working Group Request for Comments 792*, 1983.

26. Black, U., *TCP/IP and Related Protocols*, MC Graw Hill, New York, 1992.

27. Bradley, T., C. Brown, A. Malis, "Multiprotocol Interconnect over FR," *Network Working Group Request for Comments 1490*, 1993.

28. Paxson, V., "Empirically Derived Analytic Models of Wide-Area TCP Connections," Vol. 2, No. 4, *IEEE/ACM Transactions on Networking*,pp. 316-336, August 1994.

29. Mogul, J., "Broadcasting Internet Datagrams," *Network Working Group Request for Comments 919*, 1984.

30. Mogul, J., "Broadcasting Internet Datagrams in the Presence of Subnets," *Network Working Group Request for Comments 922*, 1984.

31. Braden, R., D. Borman, C. Partridge, "Computing the Internet Checksum," *Network Working Group Request for Comments 1071*, 1988.

32. Clark, D. D., "IP Datagram Reassembly Algorithms," *Network Working Group Request for Comments 815*, 1982.

33. Postel, J., "User datagram Protocol," *Network Working Group Request for Comments 768*, 1980.

34. Postel, J., "Transmission Control Protocol," *Network Working Group Request for Comments 793*, 1980.

35. Liebeherr, J., and I. F. Akyildiz, "Performance Analysis of Gateways with Buffer Constraints," *Proceedings of the IEEE INFOCOM*, pp. 1204-1212, 1990.

36. Paxson, V., "Growth Trends in Wide-Area TCP Connections," *IEEE Network*, pp. 8-17, July/August 1994.

37. Braden, R., and J. Postel, "Requirements for Internet Gateways," *Network Working Group Request for Comments 1009*, 1987.

38. Hedrick, C., "Routing Information Protocol," *Network Working Group Request for Comments 1058*, 1988.

39. Lamont, J., and M. H. Hui, "Some Experience with LAN Interconnection via FRing," *IEEE Network Magazine*, pp. 21-24, September 1989.

40. Zhang, X., and R. H. Deng, "Gateway Design for LAN Interconnection via ISDN," *Computer Networks and ISDN Systems*, pp. 43-51, 1990.

41. Derfler, F. J. Jr., "Linking LANs" *PC Magazine*, pp. 183-205, March 1993.

42. Sinanoğlu, O., "Development of a Frame Relay Communication Interface," MS Thesis, Boğaziçi University, 1995.

43. It can be found in, ftp.boun.edu.tr, under the directory /pub/slackware.

44. Simpson, W., "The Point-to-Point Protocol (PPP) for the Transmission of Multi-protocol Datagrams over Point-to-Point Links," *Network Working Group Request for Comments 1331*, 1992.

45. Mil 3, Inc., *OPNET Modeler*, 1994.

46. Frost, V. S., and B. Melamed, "Traffic Modeling for Telecommunications Networks," *IEEE Communications Magazine*, pp. 70-81, March 1994.

47. Bux, W., and D. Grillo, "End-to-End Performance in Local-Area Networks on Interconnected Token Rings," *Proceedings of the IEEE INFOCOM*, pp.60-68, 1984.

48. Exley, G. M., and L. F. Merakos, "Throughput-Delay Performance of Interconnected CSMA Local Area Networks," Vol. SAC-5, No. 9, *IEEE Journal on Selected Areas in Communications*, pp. 1380-1390, December 1987.

49. Mitchell, L. C., and D. A. Lide, "End-To-End Performance Modeling of Local Area Networks," Vol. SAC-4, No. 6, *IEEE Journal on Selected Areas in Communications*, pp. 975-985, September 1986.

50. Leland, W. E., M. S. Taqqu, W. Willinger, and D. V. Wilson, "On the Self-Similar Nature of Ethernet Traffic (Extended Version),", Vol. 2, No. 1, *IEEE/ACM Transactions on Networking*, pp. 1-15, February 1994.

51. Banks, J, and J. S. Carson, *Discrete-Event System Simulation*, Prentice-Hall, Inc., New Jersey, 1984.

52. Paxson, V., and S. Floyd, "Wide-Area Traffic: The Failure of Poisson Modeling," *ACM SIGCOMM*, pp. 257-268, 1994.

53. Baran, E. B., "Generating Data Traffic on Ethernet LAN," CmpE 492 Project Report, Boğaziçi University, 1995.

54. Kalufya, A. A. M., "Development of an Ethernet Based Traffic Monitor," CmpE 492 Project Report, Boğaziçi University, 1995.

55. Morrison, V., "PCROUTE - an IP routing program from the IBM PC", ftp.bilkent.edu.tr/pub/PC/Comm/pcrte224.zip.

10. Index

A

Aloha 4, 5
ARP 27, 43
Arpanet 23
ATM 10
Average Delay 58

B

Backbone Networks 14
Bandwidth On Demand 13, 14
Bandwidth Saving 13
Baseband 7
Best-effort Datagram Service 5
Big Endian 24
Binary Exponential Backoff 7
Bridges 2, 10, 58
Broadcast 5
Bursty 13

C

Cell Switching 19
Channel Capacity 58
Circuit Switching 13
Collision 4, 7
Communication Bandwidth 14
Connectionless Service 23
Connection-oriented 37
Control Management 2
Core 20
Core Gateways 43
Correction 5
CRC 7
CSMA/CD 4
Cyclic Redundancy Check 7

D

Data 7
Datagram 23, 32, 33
Delay Issues 9
Direct Routing 40
Distributed Control 4
DL Control 20
DLCI 14, 18

E

E112
EGP 43, 44
EIGRP 45
Encapsulation 31
Error Detection 5, 13
Error Management 2
Error Rates 10, 13
Error Recovery 13
Ethernet 4, 5, 8
Exponential Distribution 59

F

Fairness 58
Flow-control Mechanisms 9
FR Standards 12
Fragment 34
Fragmentation 50
Frame Relay 2, 10
Frame Switching 19

G

Gateway 2
GGP 44

H

HDLC 53
Hold Down Method 45

I

I.144/Q.921 20
ICMP 30, 43
IEEE 802 4
IGP 43, 44, 52
IGRP 45
Indirect Routing 40
INOC 44
Interconnection 10
Internet Protocol 2, 23
Internetworking 13
IP 43
IP Routing 39
ISDN 10

L

LAN-to-LAN Connectivity 10
LAP-D 15, 20
LAP-D+ 15
LAP-E 15
LAP-E/Q.922 20
LAP-F 15, 20
Linux 52
LLC 4
Local Area Networks 1, 4
Logical Link Control 2

M

MAC 4, 7
Media Access Control 2
Medium Access Control 6
Mesh Topology 11
Milnet 23
MTU 18, 34, 49, 56
Multiaccess 5
Multiaccess Bus 4

N

Netmask 27
Noise Burst 7

O

One-to-one Connection 10
OPNET 54
OSI 2
OSPF 44

P

Packet Arrival 9
Packet Radios 4
Packet Service Rate 59
Packet Switching 10
Packet-switching 5
Pad 7
Performance of Ethernet 8
Permanent Virtual Circuits 19
Poison Reverse 45
Poisson 58
Poisson Process 9
PPP 53, 76
Preamble 7
Protocol Conversion 2
Pure Aloha 4

Q

Q.922 ..... 20, 34
Q.931 20

R

RARP 30

Repeaters 2
Response Time 58
Response Times 13
RIP 44, 52
Routed 52
Router 2, 10, 39
Routing 2, 39

S

Shared Radio Channel 4
Split Horizon Update 45
Stability 58
Statistically Multiplexing 14
Subnets 26
Switched Virtual Circuits 19

T

T1 12
TCP 37
TCP/IP 23
Thick Ethernet 5
Thin Ethernet 5
Throughput 56, 58
Time Division Multiplexing 13
Token Bus 4
Token Ring 4
Traffic Characteristic 9

U

UDP 37
Uniform Distribution 59
UNIX 44

V

Vector-distance Routing 44
Virtual Circuit 49

W

Wide Area Network 1

X

X.25 ..... 10, 12

List of Acronyms

Acronym	Stands For
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BECN	Backward Explicit Congestion Notification.
C/R	Command/Response
CLLM	Consolidated Link Management
CLNP	Connectionless Network Protocol
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CRC	Cyclic Redudancy Check
CSMA	Carrier Sense Multiple Access
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear to Send
D/C	DLCI/DL_CORE Control Indicator
DARPA	Defense Advanced Research Projects Agency
DCD	Data Carrier Detect
DE	Discard Eligibility
DLCI	Data Link Connection Identifier
DLL	Data Link Layer
DTR	Data Terminal Ready
DUAL	Diffusing Update Algorithm
EGP	Exterior/External Gateway Protocol
FCS	Frame Check Sequence
FECN	Forward Explicit Congestion Notification
FR	FR
GGP	Gateway-to-Gateway Protocol
HDLC	High-level Data Link Control
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronical Engineering
IGMP	Internet Group Management Protocol
IGP	Interior/Internal Gateway Protocol
IGRP	Interior Gateway Routing Protocol
INOC	Internet Network Operation Center
IP	Internet Protocol
ISDN	Integrated Services Digital Network

ISO	International Standard Office
LAN	Local Area Network
LAP-D	Link Access Procedure on D channel
LAP-F	Link Access Procedure for FRing services
LLC	Logical Link Control
MAC	Media Access Control
MIS	Management Information System
MTU	Maximum Transfer Unit
NIC	Network Information Center
OSI	Open System Interconnection
OSPF	Open Shortest Path First Protocol
PC	Personal Computer
PDU	Protocol Data Unit
PPP	Point to Point Protocol
PVC	Permanent Virtual Circuits
RAM	Random Access Memory
RARP	Reverse Address Resolution Protocol
RFC	Request For Comment
RIP	Routing Information Protocol
SVC	Switched Virtual Circuits
TCP	Transmisiion Control Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network