

**ANALYSIS OF DATA & COMPUTER NETWORKS IN
STUDENTS' RESIDENTIAL AREA IN UNIVERSITI TEKNOLOGI
PETRONAS**

By

SORAYA HANI BINTI ZAINALABIDIN

FINAL PROJECT REPORT

Submitted to the Electrical & Electronics Engineering Programme
in Partial Fulfillment of the Requirements
for the Degree
Bachelor of Engineering (Hons)
(Electrical & Electronics Engineering)

Universiti Teknologi Petronas
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

© Copyright 2006

by

Soraya Hani binti Zainalabidin, 2006

CERTIFICATION OF APPROVAL


ANALYSIS OF DATA & COMPUTER NETWORKS IN STUDENTS' RESIDENTIAL AREA IN UNIVERSITI TEKNOLOGI PETRONAS

by

Soraya Hani binti Zainalabidin

A project dissertation submitted to the
Electrical & Electronics Engineering Programme
Universiti Teknologi PETRONAS
in partial fulfilment of the requirement for the
Bachelor of Engineering (Hons)
(Electrical & Electronics Engineering)

Approved:



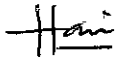
Mr. Azlan bin Awang
Project Supervisor

UNIVERSITI TEKNOLOGI PETRONAS
TRONOH, PERAK

June 2006

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.



Soraya Hani binti Zainalabidin

ABSTRACT

In Universiti Teknologi Petronas (UTP), most of the students depend on the Internet and computer network connection to gain academics information and share educational resources. Even though the Internet connections and computers networks are provided, the service always experience interruption, such as slow Internet access, viruses and worms distribution, and network abuse by irresponsible students. Since UTP organization keeps on expanding, the need for a better service in UTP increases. Several approaches were put into practice to address the problems. Research on data and computer network was performed to understand the network technology applied in UTP. A questionnaire forms were distributed among the students to obtain feedback and statistical data about UTP's network in Students' Residential Area. The studies concentrate only on Students' Residential Area as it is where most of the users reside. From the survey, it can be observed that 99% of the students access the network almost 24 hours a day. In 2005, the 2 Mbps allocated bandwidth was utilized 100% almost continuously but in 2006, the bottleneck of Internet access has reduced significantly since the bandwidth allocated have been increased to 8 Mbps. Server degradation due to irresponsible acts by users also adds burden to the main server. In general, if the proposal to ITMS (Information Technology & Media Services) Department for them to improve their Quality of Service (QoS) and established UTP Computer Emergency Response Team (UCert), most of the issues addressed in this report can be solved.

ACKNOWLEDGEMENTS

First and foremost, all praise to Allah s.w.t. for granting me the opportunity to complete my Final Year Project, satisfactorily. I am thankful to Universiti Teknologi Petronas for giving me a chance to do this analysis as my Final Year Project. But, my utmost gratitude and appreciation goes to my supervisor, Mr. Azlan b Awang for being there to guide me throughout the year providing his endless support and guidance.

For all the technician and staffs, especially Mr. Musa for being kind enough to provide technical support during Protocol Analyzer familiarization stage and Mr. Arfaishah from ITMS Department for all the crucial information supplied. For other UTP students, without their cooperation, this research will not be a success.

Once more, I would like to express my deepest gratitude to all contributors who helped me to complete this project.

Thanks a zillion.

TABLE OF CONTENTS

LIST OF TABLES	9
LIST OF FIGURES	10
LIST OF ABBREVIATIONS	12
CHAPTER 1 INTRODUCTION	13
1.1 Background of Studies	13
1.2 Problem Statement	13
1.3 Objectives	14
1.4 Scope of Studies	14
CHAPTER 2 LITERATURE REVIEW & THEORY	15
2.1 Literature Review	15
2.2 Theory	15
2.2.1 Local Area Network	15
2.2.2 Topology	16
2.2.3 Physical and Logical Technology	18
2.2.4 Network Protocols	19
2.2.4.1 OSI Model	19
2.2.4.2 TCP/IP Protocol Architecture	20
2.2.4.3 Data Encapsulation and Decapsulation	22
2.3 Network Performance	24
2.3.1.1 Bandwidth & Latency	24
2.3.1.2 Server Performance	24
2.3.1.3 Network Interface Card	25
2.3.2 Protocol Analyzer	26
2.3.2.1 Overview of Agilent Advisor	26
2.3.2.2 Features	27
2.3.2.3 The Expert Analyzer	27
2.3.2.4 Decodes	28
2.3.2.5 Capture Filters, Logging and Subnets	29
1.2.4.1 Active Tests and Traffic Simulation	29
CHAPTER 3 METHODOLOGY	30
3.1 Survey Methodology	31

3.2 Protocol Analyzer.....	32
3.2.1 Familiarization.....	32
3.2.2 Analysis	34
CHAPTER 4 RESULTS & DISCUSSION	35
4.1 Introduction	35
4.1.1 UTP Students' Residential Area.....	35
4.2 IP Addressing and its Allocation.....	36
4.3 Network Equipment Used	39
4.3.1 Passport 8600 Routing Switch.....	41
4.3.2 Nortel BayStack Portfolio.....	42
4.3.3 Nortel Business Policy Switch.....	43
4.3.4 Nortel : Designing the Network.....	43
4.3.4.1 Edge Switches	43
4.3.5 The Superiority of the Passport	44
4.4 Packet Captured and Analysis using Protocol Analyzer	45
4.4.1 Ethernet Header	46
4.4.2 IP Header	47
4.4.3 IGMP Header.....	50
4.5 Users' survey and feedback.....	51
4.5.1 Data Analysis.....	52
4.5.2 General Information.....	53
4.5.3 UTP Intranet & Internet.....	55
4.6 Application Runs and Bandwidth Consumption.....	61
4.6.1 E-Learning Portal.....	61
4.6.2 mIRC.....	61
4.6.3 Bulletin Board/Internet Forum	63
4.6.4 Radio Streaming	63
4.6.5 Gaming Server	64
4.7 UTP's Network Traffic Statistical Data	64
4.8 Degradation on Server Performance	71
4.8.1 mIRC Servers.....	71
4.8.2 Network Virus	71
4.8.3 Distributes Denial of Service.....	73
4.8.4 Proxy Server Abuse	74

4.9 Network Improvement	75
4.9.1 Internet Bandwidth	75
4.9.2 UTP Student Webmail	76
CHAPTER 5 CONCLUSIONS & RECOMMENDATIONS.....	78
5.1 Conclusions	78
5.2 Recommendations	78
5.2.1 Future Plans	79
5.2.1.1 Quality of Service.....	79
5.2.1.2 Establish UTP Computer Emergency Response Team (UCert)	79
REFERENCES.....	81
APPENDICES	82
Appendix A RFC 1180.....	83
Appendix B Product Brief : Passport 8600 Routing Switch	112
Appendix C Product Brief : Baystack 450 switches	113
Appendix D Product Brief: Baystack 470 switches	114
Appendix E Product brief: Business Policy switch.....	115
Appendix F Protocol Analyzer decodes analysis data	116
Appendix G UTP Network Survey	119

LIST OF TABLES

Table 1 UTP Students' Residential Area IP Addresses	37
Table 2 Survey group divisions.....	52
Table 3 Top Hosts by Packet Sent (External IP).....	65
Table 4 Top Hosts by Packet Sent (Internal IP).....	66
Table 5 Top Conversation between two hosts	67
Table 6 Top 10 Protocol Distribution	69

LIST OF FIGURES

Figure 1 Illustration of a bus technology which all computers attached to the same cable (network backbone).....	17
Figure 2 Illustration of tree topologies as an expansion of bus topologies	17
Figure 3 Illustration of the ring topology	18
Figure 4 Illustration of the star topology.....	18
Figure 5 Summary of OSI layers.....	20
Figure 6 Comparison of the OSI model and TCP/IP network architecture	21
Figure 7 Position of IGMP, ICMP, ARP and RARP protocol in Network Layer	21
Figure 8 Encapsulation steps.....	23
Figure 9 The protocol analyzer	27
Figure 10 Methodology Flow Chart.....	30
Figure 11 Survey Methodology.....	31
Figure 12 Illustration of UTP students' residential area	36
Figure 13 Screenshot of Local Area Network Connection Status for user in Village 4, Block B.....	38
Figure 14 Interconnectivity between routers in students' residential area to the Chancellor's Complex	39
Figure 15 Network equipment diagram for students' residential area.....	40
Figure 16 Passport 8600 Routing Switch.....	41
Figure 17 Passport 8600 Routing Switch in a Network Core	42
Figure 18 BayStack 450	42
Figure 19 BayStack 470	42
Figure 20 Business Policy Switch.....	43
Figure 21 Protocol Analyzer Decodes Summary	45
Figure 22 IP Datagrams.....	47
Figure 23 Encapsulation of IGMP message in an Ethernet Frame	51
Figure 24 Personal Computer ownership statistics of the students.....	53
Figure 25 Network connectivity statistics of the students.....	53
Figure 26 Network understanding statistics of the students.....	54
Figure 27 PC firewall usage statistics of the students.....	54
Figure 28 The UTP Intranet reliability survey	55

Figure 29 Internet accessibility statistics among the students.....	56
Figure 30 Internet connection speed during off-peak hour statistics	56
Figure 31 Internet connection speed during peak hour statistics	57
Figure 32 Students online duration statistics.....	58
Figure 33 PC idling statistics among the students.....	58
Figure 34 Network problems statistics among students.....	59
Figure 35 UTP Intranet security statistics	60
Figure 36 Protocol Distribution Tabulated Graph for 1 Week in Students' Residential Area.....	70
Figure 37 Virus report on the server	72
Figure 38 Report lodged by ISP to the ITMS Department	73
Figure 39 Proxy servers acting as mIRC proxy	74
Figure 40 Top File Hosting IP reported by ITMS Department.....	74
Figure 41 Traffic pattern before upgrading.....	76

LIST OF ABBREVIATIONS

1	ARP	: Address Resolution Protocol
2	ATM	: Automatic Teller Machine
3	BBS	: Bulletin Board System
4	BOOTP	: Boot Protocol
5	BPS	: Business Policy Switch
6	CAT 5	: Category 5
7	CRC	: Cyclic Redundancy Check
8	DDOS	: Distributed Denial Of Service
9	DHCP	: Dynamic Host Configuration Protocol
10	DNS	: Domain Name System/Service
11	DOS	: Denial Of Service
12	DS	: Distributes Services
13	FTP	: File Transfer Protocol
14	HLEN	: Header Length
15	ICMP	: Internet Control Message Protocol
16	IGMP	: Internet Group Message Protocol
17	IP	: Internet Protocol
18	IPV4	: Internet Protocol Version 4
19	IPV6	: Internet Protocol Version 6
20	ITMS	: Information Technology & Media Services Department
21	LAN	: Local Area Network
22	MAN	: Metropolitan Area Network
23	MTV	: Music Television
24	MYCERT	: Malaysia's Computer Emergency Response Team
25	NIC	: Network Interface Card
26	OSI	: Open System Interconnection
27	QOS	: Quality Of Service
28	RARP	: Reverse Address Resolution Protocol
29	RFC	: Request For Comments
30	RTCP	: Real Time Control Protocol
31	RTP	: Real Time Protocol
32	SCTP	: Stream Control Transmission Protocol
33	SMTP	: Simple Mail Transfer Protocol
34	TCP	: Transmission Control Protocol
35	TCP/IP	: Transmission Control Protocol / Internet Protocol
36	TELNET	: Terminal Emulation Program
37	TTL	: Time To Live
38	UCERT	: UTP's Computer Emergency Response Team
39	UDP	: User Datagram Protocol
40	UTP	: Universiti Teknologi Petronas

CHAPTER 1

INTRODUCTION

1.1 Background of Studies

The analysis aims to understand the users need, the issues, technology adopted and network utilisation in UTP Students' Residential Area. A survey among students about the current computer networking situation in Universiti Teknologi Petronas (UTP) has been carried out to obtain the statistics of networking issues in UTP. This study also gives an opportunity to the student on how to use a Protocol Analyzer for capturing, analysing and reporting the data traffic.

The topic discussed is related to the Data and Computer Networking class and throughout the year, the knowledge gained from the class as well as from the personal research do improves the author's understanding about computer networking. Familiarity with UTP existing computer networks and knowledge in computing will be an advantage while doing this study.

1.2 Problem Statement

In these past few years, UTP organization has expanded rapidly especially in the number of students. Due to the number of student increases, the demand for a better network services increases in UTP. Issues such as slow Internet access, worms and viruses distribution, network uptime versus downtime, and also network abuse by some irresponsible students are of interest to perform investigation and analysis.

1.3 Objectives

The objectives of the study are:

- i. To enhance knowledge in data and computer networking
- ii. To understand the networking technology employed in the university
- iii. To analyze the network utilization using Protocol Analyzer
- iv. To understand the user needs and their networks utilization
- v. To address every issues related to UTP network
- vi. To propose a solution to improve the UTP network

1.4 Scope of Studies

The scope of study is concentrated to the network in the student's residential area only since the area utilise the most of the UTP networks bandwidth. The study will include the network traffic overview, the technology applied for the implementation of networking topology in the area and most of the applications that utilize the networks. The study also gathers the student feedback about the current networks employed and information on issues related to UTP network.

CHAPTER 2

LITERATURE REVIEW & THEORY

2.1 Literature Review

Computer networks are everywhere, from the Auto-Teller Machine (ATM) to the telemarketers and the communication system. The user relies on the largest network in the world, the Internet, whenever there is a need to browse the Web or access email services. That is the outside world, but now networking have been applied in most of the universities in the world as a medium to share the academic resources efficiently, besides providing an ease to the students to access the resource centre from their own personal desktop.

2.2 Theory

In simplest term, a computer network is two or more connected computers. The actual physical connection between the computers can take a number of forms, which include physical cabling and connectivity strategies. There is more to networking computers, than just supplying a connection between the computers. There are also some basic rules related to the actual communication that must take place between the computers if they are going to be capable of exchanging data.

2.2.1 Local Area Network

A Local Area Network (LAN) consists of a shared transmission medium and a set of hardware and software for interfacing devices to the medium and regulating the orderly access to the medium. By introducing LAN, data that

need centralised facility can be accessible to a number of users, and there are some data that can be shared by the users[4].

By doing the sharing of information online, the efficiency of the works can be assured. LANs have the following parameters:

- They occupy only one physical location
- They have high speed data transfer rate, in UTP the data transfer rate is 100Mbps – Fast Ethernet LAN.
- All data travels on the local network wiring.

2.2.2 *Topology*

Topology is one of the elements of the LAN that determine the type of data that may be transmitted, the speed and efficiency of communication and even the kind of applications that can be supported. In context of a communication network, the term topology refers to the way in which the end points, or stations, attached to the network are interconnected. The common topologies for LAN are bus, tree, ring and star.

Bus Topology: Bus topology is characterised by the use of a multipoint medium. For the bus, all stations attach, through appropriate hardware interfacing known as tap, directly to a linear transmission medium, or bus. Full duplex operation between the station and the taps allows data to be transmitted and received by the bus. A transmission from any station propagates the length of the medium in both directions and can be received by all other stations. At each end of the bus is a resistor which acts like a terminator that absorbs any signal, thus removing it from the bus[4]. Diagram for bus topology can be referred in Figure 1.

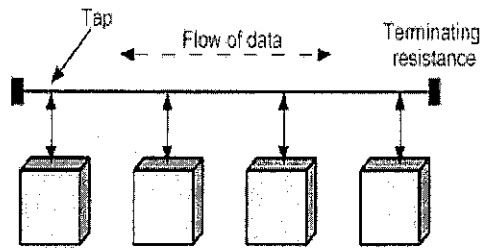


Figure 1 Illustration of a bus technology which all computers attached to the same cable (network backbone)

Tree Topology: As bus topology, tree topology is also characterized by its used of multipoint medium. The tree topology is a generalisation of the bus technology. The transmission medium is a branching cable without a closed loop, where branches started at the point named headend. Cables started at the headend, and it may have more branches. Again, a transmission from any station propagates throughout the medium and can be received by all other stations[4]. Diagram for tree topology can be referred in Figure 2.

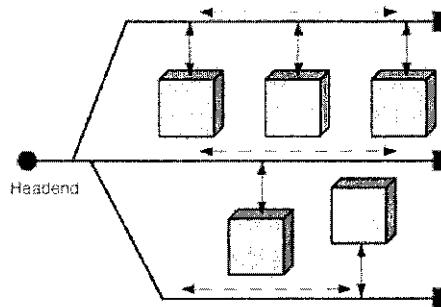


Figure 2 Illustration of tree topologies as an expansion of bus topologies

Ring Topology: In ring topology, the network consists of a set of repeaters joined by point-to-point links in closed loop. The repeater is capable of receiving data on one link and transmitting them. The links are unidirectional, so that data circulate around the ring in one direction only, clockwise or counter-clockwise[4]. Diagram for ring topology can be referred in Figure 3

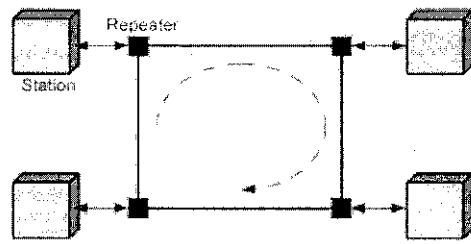


Figure 3 Illustration of the ring topology

Star Topology: In star topology, each station is connected to a common central node[4]. Diagram for star topology can be referred in Figure 4. Typically, each station attaches to a central node via two point-to-point links, one for transmission and for reception. UTP network is build based on this type of topology.

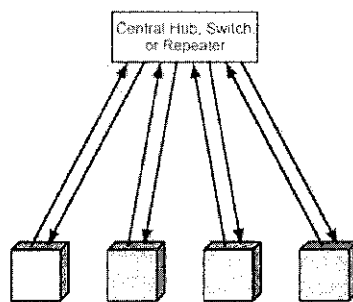


Figure 4 Illustration of the star topology

2.2.3 Physical and Logical Technology

Physical topologies are basically an arrangement of a medium such as cables and host in the network. A Network Interface Card (NIC) is used in every computer as a connection points to handles the communication with other devices in the network. Even though newer physical topologies such as star and ring have dominates the newer network installation, bus topologies can still be found in the older network installation.

In contrast with the physical topologies, logical topologies are largely abstract. Physical topologies can be observed through the arrangement of the devices, but the logical topologies are essentially the rules that are laid out for the devices to transmit their data; the protocols.

2.2.4 Network Protocols

After understanding the physical topologies, the next layer in the network model is the protocol. Network protocols consist of sets of rules for sending and receiving data across a physical network and the software that puts these rules into practice. Logical topologies instruct the hardware on how to packetize or to put into frame the data that need to be transmitted across the physical topology; hence the protocols translate the data between applications to the logical topologies.

2.2.4.1 OSI Model

Open Systems Interconnection (OSI) was first introduced in late 1970s that dominated data communication and networking world before 1990. OSI is defined as an open protocol that allows any two different systems to communicate regardless of their underlying architecture [1]. OSI aims to demonstrate how a communication between two different systems can be managed without adapting to the same hardware and software. OSI is actually not a protocol but just a model to understand and designed the network.

OSI model consists of seven layers, separated but interdependent layer. By understanding the OSI layer, it will provide a firm basic to explore the data communication world. In Figure 5 below, the definition of every layer in the OSI model are summarised.

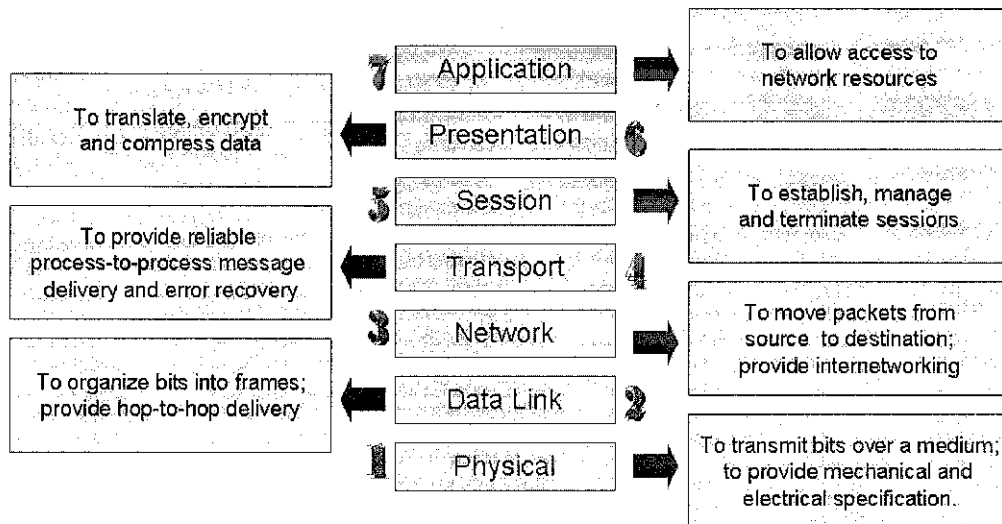


Figure 5 Summary of OSI layers

2.2.4.2 TCP/IP Protocol Architecture

Transmission Control Protocol/Internet Protocol (TCP/IP) is a term used to describe the hierarchy of protocol suite on which the Internet runs. The TCP/IP protocol architecture is the set of communications protocols that implement the protocol stack on which the Internet and most commercial networks run. It is sometimes called the TCP/IP protocol suite, after the two most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). TCP/IP is the most popular standard, mainly because it is an open standard; it is not own by any company.

The ideal model for communication architecture is the OSI layers. But, the TCP/IP layer can only be roughly fitted to the OSI model which describes a fixed set of 7 layers. Not all of the layers can fit well with IP based networking which really involves a varying number of layers depending on the design of the applications and the underlying network. Therefore, based on the OSI model the TCP/IP protocol architecture is developed to organize the communication task into five relatively independent layers.

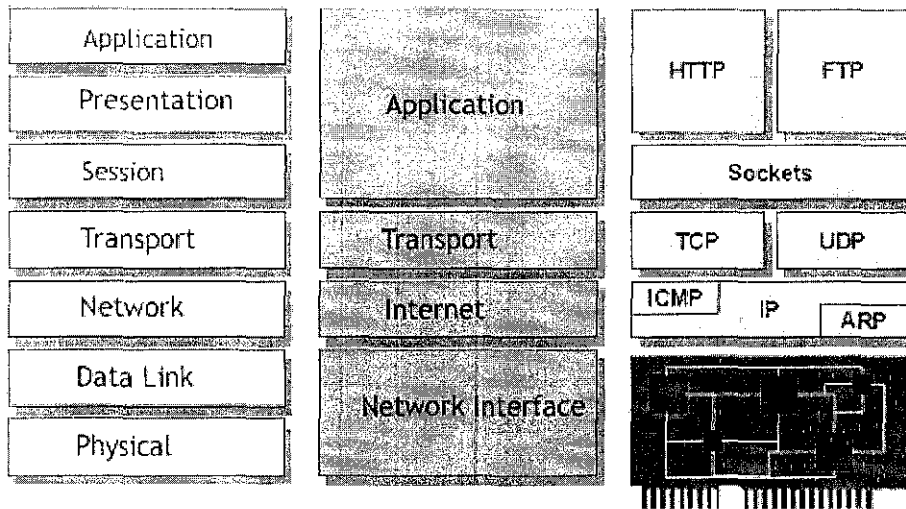


Figure 6 Comparison of the OSI model and TCP/IP network architecture

- **Physical and Data Link Layer**

In these two layers, TCP/IP does not define any specific protocol. It supports all protocols and standard, either in LAN, WAN or both.

- **Network Layer**

In this layer, TCP/IP supports the Internet Protocol (IP) with its four supporting protocols, which are ARP, RARP, ICMP and IGMP. Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP) are the protocols that are designed to perform dynamic mapping. The first maps logical address to a physical address and the second maps a physical address to a logical address. Internet Control Message Protocol (ICMP) is designed to compensate the IP protocol that lacks of mechanism for host and management queries. Internet Group Management Protocol (IGMP) is a protocol that manages group membership for a multicast router to distribute multicast packet to host or other routers.



Figure 7 Position of IGMP, ICMP, ARP and RARP protocol in Network Layer

- **Transport Layer**

The transport layer was initially represented by two protocols, User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). UDP and TCP are responsible for delivery of a message from a process or application to another process. A new transport layer protocol, Stream Control Transmission Protocol (SCTP) has been devised to handle new application such as Internet Telephony.

- **Application Layer**

A combination of session, presentation and application layer in OSI model results in the *application layer* in TCP/IP. The suite of applications that were specifically developed for TCP/IP is:

- Telnet
- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- Simple Mail Transfer Protocol (SMTP)
- Domain Name Services (DNS)
- Real-Time Protocol (RTP)
- Real Time Control Protocol (RTCP)
- Boot Protocol (BOOTP)
- Dynamic Host Configuration Protocol (DHCP)

2.2.4.3 *Data Encapsulation and Decapsulation*

During the third week in the second semester, a data packet traversing in UTP network has been captured for analysis purposes.

In computer networking, encapsulation is to append a header from an upper layer protocol into a lower layer protocol. When an application sends a message through UDP, it passes the message to UDP with a pair of addresses and data length. UDP will add the UDP header. The message will then be transmitted to IP with the UDP header and IP will append its own header. The data link layer receives the IP datagram, will add its own header and possibly a trailer and passes it to the physical layer. The physical layer will encode the bits

into electrical or optical signals and sends it to the remote machine. An overall encapsulation step is illustrated in Figure 8.

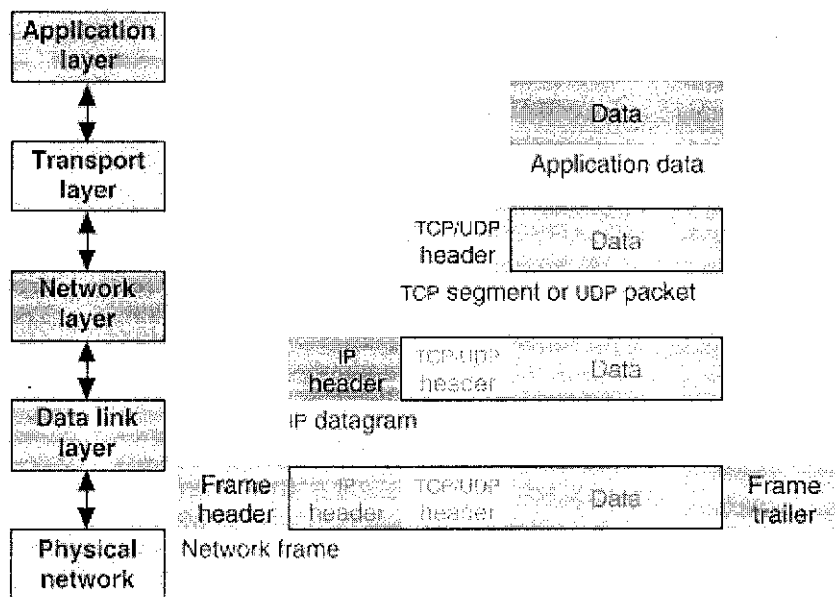


Figure 8 Encapsulation steps

Decapsulation will initiate when the message arrives at the destination host, the physical layer will decode the signal into bits and passes it to the data link layer. The outer layer of header and trailer that were appended will be checked by data link layer to detect any error. If there is no error, the header and trailer will be dropped and the datagram will be passed to IP. Again, error checking is performed by IP software and if there is no error, the header is dropped and the user datagram is passed to UDP. Using the checksum attached, the entire user datagram will be checked and an error-free message will be passed to the process along with the sender address. Basically, decapsulation is the reverse of encapsulation process in TCP/IP.

The terminologies used in this section are referred to TCP/IP terminology defined in RFC1180 attached in Appendix 1. A detail explanation on encapsulated message will be given in Chapter 4.

2.3 Network Performance

Computer networks are expected to perform well, since the effectiveness of data distribution over the network often depends directly on the efficiency of the networks that delivers the data. It is therefore important to understand the various factors that impact the network performance. As stated below, three major aspects which the network performance are measured will be discussed briefly.

2.3.1.1 *Bandwidth & Latency*

Network performance is measured in two fundamentals ways: bandwidth (throughput) and latency (delay). Bandwidth and throughput are two of the most confusing terms used in the networking. In some cases, bandwidth can be explained as the range of signals. But, in a communication link, bandwidth refers to the number of bits per second that can be transmitted on the link. As an example, the bandwidth of a Fast Ethernet is 100Mbps. In real world, there is no perfect communication link that will transmit data at its full capabilities. The actual number of bits that was transmitted on the link may only be half of its intended value. Therefore, the terms throughput is used to measure the performance of a system [2].

The second performance measure, latency is defined the duration that a message takes to travel from one end of a network to the other[2]. Latency is measured strictly in term of time. For example, a transcontinental network might have a latency of 24ms; that is it takes a message 24ms to travel from one end of Malaysia to other.

2.3.1.2 *Server Performance*

To be able to improve performance, part of the system that is slowing down the throughput must be determined. It could be:

- The speed of the processor
- The speed of the memory

- The speed of the disk system
- The speed of the network adapter system

This limiting factor is referred to as the bottleneck of the system.

2.3.1.3 Network Interface Card

Network Interface Card (NIC) typically fit into an expansion slot on a computer. In modern PCs, however most of the NIC is installed in the computer at the factory.

Functions performed by a NIC include:

- Providing a unique LAN address for the node.
- Performing the data link layer functions with other nodes appropriate to the physical connection and protocol used on the particular LAN
- Accepting protocol frames of information at full LAN speed and buffering them on the card until the computer is ready to process them
- Recognizing, examining the address information of, and ignoring received protocol frames that are not addressed to the node in which the NIC is installed
- Responding to certain management signals on the network, which might be inquiries about the status of the card or a recent communications load imposed on it or commands to stop communication on the network.

As NIC throughput have progressed from 10Mbps to 100Mbps and even 1Gbps, NIC have ceased to be the significant bottleneck in most networks.

2.3.2 Protocol Analyzer

A protocol analyzer, also known as a network analyzer is software or hardware or a combination of both, device that captured or received all the packets on the media, store them in a trace buffer and then show a breakdown of each of the packets by protocol in the order they appeared. Therefore, it can help to analyze all levels of the OSI model to determine the cause of the problem. Network analysis is the art of listening in on a network's communication to examine how devices communicate and determine the health of that network.

Protocol Analyzer is important because when network fails, the cause of the problems can not be visible. For that reason, the only way to determine the cause of the problems is by figuring it from the symptoms. It is better if the network failure can be predicted beforehand and actions can be taken to avoid the conditions that may lead to network failure.

In this project, the specific protocol analyzer that will be used throughout the semester is the Agilent Advisor Network Analysis. The Agilent Advisor has many capabilities in analyzing the network for the troubleshooting purposes. By pointing out the network state, areas of possible problems and network history, the network trends can be observed, thereby provided an ease to recognize the possible roots of network failure. All the network traffic, conversation and particular protocol interaction can also be analyzed too. If there are time constraints, the network statistics and network events can be logged to be processed and examined later.

2.3.2.1 Overview of Agilent Advisor

Agilent Advisor is a portable, full-featured network-analysis solution that allows users to install, support and maintain complex networks by providing features that makes troubleshooting any network segment quick and easy.

The Agilent Advisor is based on an upgradeable platform that allows users to add future testing capabilities easily and cost effectively. Variants and plug-in modules cater for a vast range of network topologies, including **10/100 Ethernet, Gigabit Ethernet, Token Ring, FDDI, ATM, WAN** technologies such as **ISDN, Frame Relay, X25, SNA, VoIP** and much more.

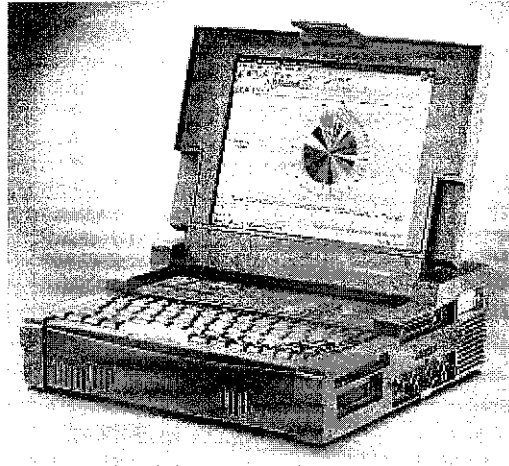


Figure 9 The protocol analyzer

2.3.2.2 Features

- i. Fast data capture and comprehensive decoding
- ii. Expert analysis.
- iii. Statistics and vital signs.
- iv. Multi-tasking and easy-to-use.
- v. Flexible for LAN/WAN/ATM testing.

2.3.2.3 The Expert Analyzer

The Expert Analyzer presents the big picture of your network showing utilization trends, error history, and connection statistics. When the Expert Analyzer is started, it automatically runs several measurements: Commentator, Protocol Statistics, and Node Statistics. These measurements are called “children” of Expert. Each of these measurements except Node Discovery can also be started by itself if Expert is not running.

- **Protocol Statistics:**
Shows utilization, average frame length and number of data link layer errors for each active protocol stack.
- **Protocol Vital Statistics:**
Shows thresholds and graph pertinent statistics for each active protocol stack.
- **Node Discovery:**
Shows currently active nodes detected on the network. The node can be sorted out based on their events, and an instant decode filter can be placed to or from that node.
- **Connection Statistics:**
For each active connection, the nodes involved, the protocols they are using and interesting statistics that apply to each connection can be observed.
- **Commentator:**
The Commentator stores up to 10000 each of alert, warning and normal events that can occur on your network. Events can be sorted by severity of the event, frequency of the event. Connections involved, nodes involved, as well as filtered by address or connections.

2.3.2.4 *Decodes*

The 'decodes' measurement displays in real time the contents of every frame and packet on the network. The information is presented in three inter-related sections: a summary line, a detailed English description of each field and a hex dump of the bytes of the frame. A display filter for specific addresses, protocols, port numbers, frame bytes or VLAN identification numbers can be implemented in the Decodes measurement.

2.3.2.5 *Capture Filters, Logging and Subnets*

The capture filters is used to store frames for processing by the various measurement. The capture buffer is a special kind of memory that can be written to very high rates of speed. Most Advisor measurements are fed by the frames in the capture buffer. The exceptions to this are Line Vital Statistics and some of the Protocol Vital Statistics counts. Capture filters can be defined to control which frames are allowed to enter the capture buffer. Log can be set up for data baselining and benchmarking. Subnet is used to tell the Advisor how to group the addresses in the networks.

1.2.4.1 *Active Tests and Traffic Simulation*

Active tests stimulate the network nodes and display responses. The active tests available are:

- IP PING
- IP ARP
- IP RARP
- IP Trace Route
- IP Active Network Discovery
- Novell Network List
- Novell View Nodes
- Novell Nearest Server
- Novell server List
- Novell Node Ping
- Novell Server Ping

Traffic generator is used to do performance testing. Parameters that can be defined for the performance testing are:

- % utilization
- Frame rate
- Frame size
- Time duration
- Number of frames sent
- MAC Addresses
- Network Layer addresses

CHAPTER 3

METHODOLOGY

In order to perform the study, several methods will be used. The flow chart below will explain the methodology applied in sequence.

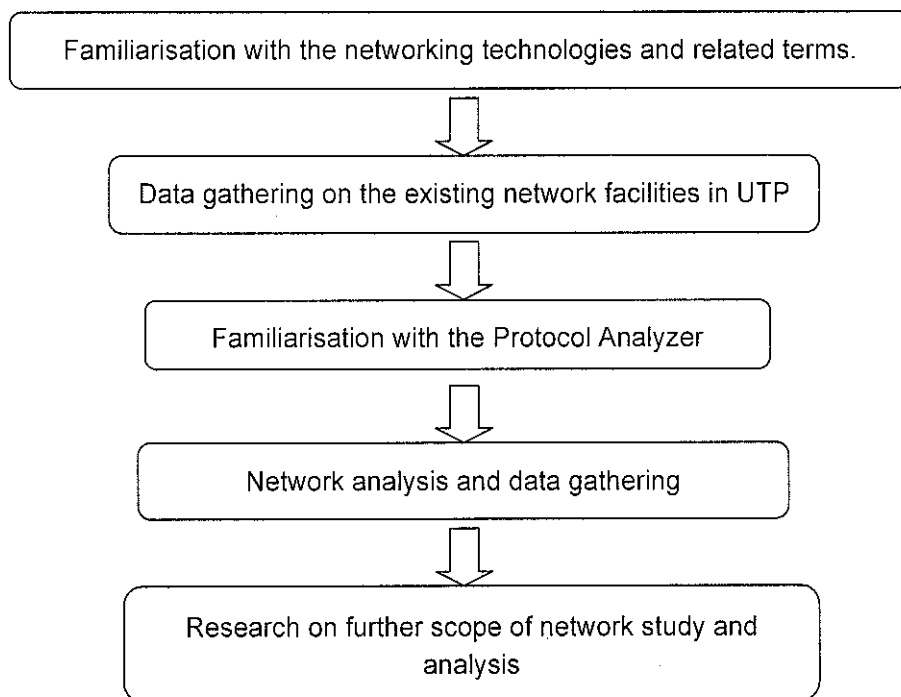


Figure 10 Methodology Flow Chart

The first stage is to study and understand the network technologies and concept for the ease of advanced research. The knowledge gained can therefore be applied in order to understand the network technologies adopted in UTP; this is the main purpose of the study besides gathering data about the network traffic and utilisation. After the current network concept has been grasped, advance research on network related technology will be carried out to optimise the networking capability and improve the network situation. But, according to the situation, the steps may be performed back and forth in order to obtain satisfactory results.

3.1 Survey Methodology

To survey people is to ask them to supply written answers to the questions provided. Survey can be used to receive answers from many people, more than what can be provided by interviewing. A survey also helps to determine basic facts or conditions and assess the significance or importance of facts. The methods to perform research by surveying method are as below:

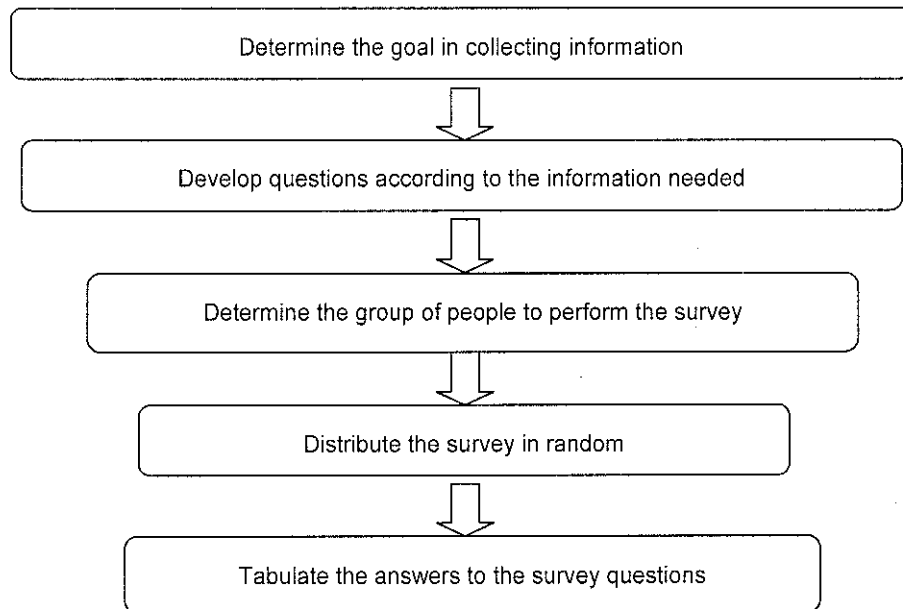


Figure 11 Survey Methodology

3.2 Protocol Analyzer

3.2.1 Familiarization

In order to use Protocol Analyzer to analyze the network, lab exercises provided in the training module are performed. The lab exercise consists of 7 modules, which are divided by the subtopics in the Protocol Analyzer manual. The modules are:

i. Lab 1: Expert Analyzer

This lab is mainly to be familiar with the Expert Analyzer's features and capabilities. The data that will be analyzed have been previously collected and then will be loaded to the capture buffer to be analyzed. The Expert Analyzer will work exactly the same way as when it is examining live data from a network.

ii. Lab 2: Commentator, Statistics and Node Discovery

This lab meant to introduce the students with the Commentator, Statistics and Node Discovery features in the Protocol Analyzer. The commentator can be configured to observe or to ignore any events in the network. The measurement taken can be set to STOP at any time when the command is triggered. The statistics of measurement in the Protocol Analyzer such as Protocol Stats, Connection Stats, Line Vital Stats, and VLAN Stats will give us the important information about the usage information for the network. The Node Discovery will keep track of names, addresses and events that occur on the nodes.

iii. Lab 3: Data Link Layer Errors

This lab will introduce the students on how would an error in the network be detected. In this case, a demonstration file of DLL errors will be loaded in the network. There are three measurements that deal

directly with DLL errors: MAC Node Statistics, Line Vital Statistics and Protocol Vital Statistics.

iv. Lab 4: Decodes

Decodes is a valuable troubleshooting tool because it can see every byte in every frame. Normally, Decodes features will not be used independently, but will be used after problems are detected by other measurements. The Decodes functions then will be used to drill into the problem. This lab is designed to show the students the troubleshooting tools that are available in Decodes.

v. Lab 5: Capture Filters, Logging and Subnets

This lab will implement the features of Capture Filters, set up the Advisor for data logging, set up the workspace options and set up custom subnet addresses for a network.

vi. Lab 6: Configurations, New Measurement and Printing

In this lab, the students will learn on how to configure and save new measurements, restore default measurement, how to set up a generic printer and how to get screenshots and other documentation from the advisor.

vii. Lab 7: PING and Traffic Generation

This lab objective is to understand and exercise some features of the Active Tests and the Traffic Generator. The Active Test will stimulate the network and then will monitor its responses by introducing IP and Novell PINGs to establish network connectivity. They can also be used to determine a degree of network latency since the elapsed time for the PING is displayed in the measurement result window. A transmit password will be asked during the first session of running Active Test.

3.2.2 *Analysis*

To start the analysis, the Protocol Analyzer must be connected to the network through one of the network port in the lab. There are two mode of connection available in the Advisor, as to connect the Protocol Analyzer to the “To Hub/Switch”. This is used to connect the equipment to a repeating hub port when the Protocol Analyzer is terminating the network link. The second option is to connect the Protocol Analyzer to the “To Node” port that will make the Protocol Analyzer operate in a pass through mode. During the analysis, the RJ-45 cable is connected to the “To Hub/Switch” port.

The Protocol Analyzer will then be turned on and the analysis software is executed. The Expert Analyzer module need to be started before the real-time network measurement could be initiated. The measurement duration is 15 minutes and then will be saved for future use. The reporting software are started to generate the intended report.

CHAPTER 4

RESULTS & DISCUSSION

4.1 Introduction

In order to present the analysis results, the data have been classified into several sections, which are:

- IP Addressing and its Allocation
- Network Equipment Used
- Packet Captured and Analysis using Protocol Analyzer
- User's Survey & Feedback
- Issues: Application Runs in the Network
- Issues: UTP's Network Traffic Statistical Data
- Issues : Degradation of Server Performance
- UTP's Network Improvement in 2006

4.1.1 UTP Students' Residential Area

In order to comprehend the scope of studies, the illustration of UTP Students' Residential Area is provided to provide a basic perspective of what will be presented in this chapter.

Students' Residential Area consists of 5 cluster of blocks, or better known as "Village" among the students. The first is Village 1 with 4 blocks, Village 2 with 3 blocks, Village 3 and 4 have the same design with 5 blocks each and finally Village 5 with 11 blocks. In the illustration, only 10 blocks are shown in Village 5 since there is another 1 block unoccupied. The UTP's Village will continue to expand as to accommodate the growing number of students in every intake each semester. Currently, the total numbers of students in all the residential area is about 5000 people.

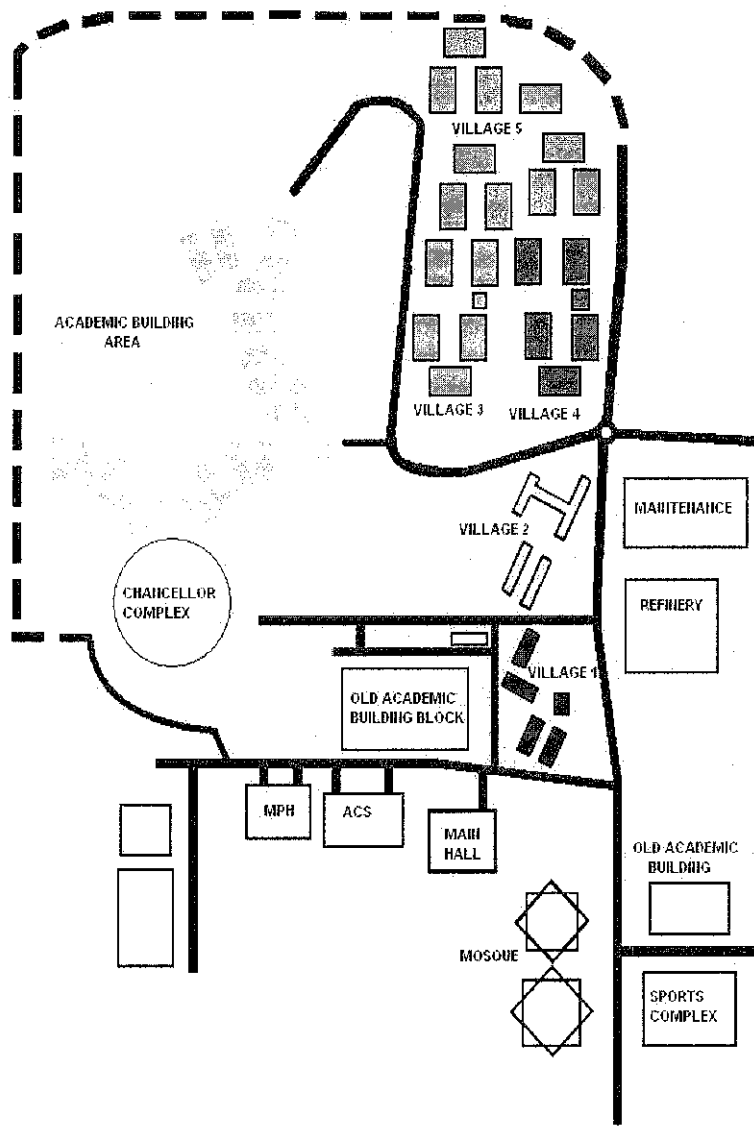


Figure 12 Illustration of UTP students' residential area

4.2 IP Addressing and its Allocation

Before going through the real-time network monitoring activities, the trend in computer networking in the students' residential area must be understood beforehand. This is to ensure that the findings obtained during the real-time network monitoring can be comprehended since UTP employed a unique system of IP addressing that enable users to determine the location of the network hub just by reading the IP. Below is the data gathered about the IP address assigned for each user in the blocks and their respective gateway IP.

Village	Building	User IP Address Range	Gateway IP
1	A	161.0.1.1 – 161.0.1.252	161.0.1.254
	B	161.0.2.1 – 161.0.2.252	161.0.2.254
	C	161.0.3.1 – 161.0.3.252	161.0.3.254
	D	161.0.4.1 – 161.0.4.252	161.0.4.254
2	A	162.0.1.1 – 162.0.1.252	162.0.1.254
	B	162.0.2.1 – 162.0.2.252	162.0.2.254
	C	162.0.3.1 – 162.0.3.252	162.0.3.254
	D	162.0.4.1 – 162.0.4.252	162.0.4.254
	E	162.0.5.1 – 162.0.5.252	162.0.5.254
3	A	163.0.1.1 – 163.0.1.252	163.0.1.254
	B	163.0.2.1 – 163.0.2.252	163.0.2.254
	C	163.0.3.1 – 163.0.3.252	163.0.3.254
	D	163.0.4.1 – 163.0.4.252	163.0.4.254
	E	163.0.5.1 – 163.0.5.252	163.0.5.254
4	A	164.0.1.1 – 164.0.1.252	164.0.1.254
	B	164.0.2.1 – 164.0.2.252	164.0.2.254
	C	164.0.3.1 – 164.0.3.252	164.0.3.254
	D	164.0.4.1 – 164.0.4.252	164.0.4.254
	E	164.0.5.1 – 164.0.5.252	164.0.5.254
5	A	165.0.1.1 – 165.0.1.252	165.0.1.254
		165.0.2.1 – 165.0.2.252	165.0.2.254
	B	165.0.3.1 – 165.0.3.252	165.0.3.254
		165.0.4.1 – 165.0.4.252	165.0.4.254
	C	165.0.5.1 – 165.0.5.252	165.0.5.254
		165.0.6.1 – 165.0.6.252	165.0.6.254
	D	165.0.7.1 – 165.0.7.252	165.0.7.254
		165.0.8.1 – 165.0.8.252	165.0.8.254
	E	165.0.9.1 – 165.0.9.252	165.0.9.254
		165.0.10.1 – 165.0.10.252	165.0.10.254
	F	165.0.11.1 – 165.0.11.252	165.0.11.254
		165.0.12.1 – 165.0.12.252	165.0.12.254
	G	165.0.13.1 – 165.0.13.252	165.0.13.254
165.0.14.1 – 165.0.14.252		165.0.14.254	
H	165.0.15.1 – 165.0.15.252	165.0.15.254	
	165.0.16.1 – 165.0.16.252	165.0.16.254	
I	165.0.17.1 – 165.0.17.252	165.0.17.254	
	165.0.18.1 – 165.0.18.252	165.0.18.254	
J	165.0.19.1 – 165.0.19.252	165.0.19.254	
	165.0.20.1 – 165.0.20.252	165.0.20.254	
K	165.0.21.1 – 165.0.21.252	165.0.21.254	
	165.0.22.1 – 165.0.22.252	165.0.22.254	

Table I UTP Students' Residential Area IP Addresses

The user IP address can be assigned manually in the computer network configuration setting or automatically by the DHCP server.

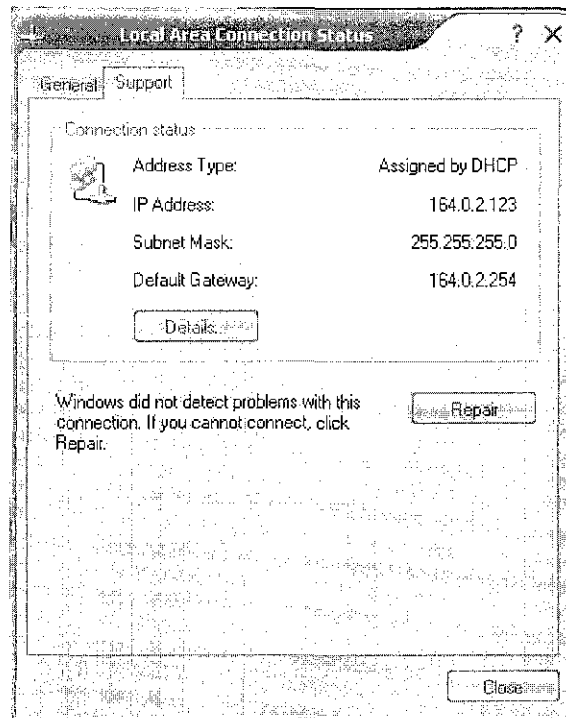


Figure 13 Screenshot of Local Area Network Connection Status for user in Village 4, Block B.

During the past few years, if a user wants to access the Internet, the user has to go through an Internet Proxy Server. In UTP currently there are 4 proxies, which are:

- i. 160.0.226.207
- ii. 160.0.226.208
- iii. 160.0.234.207
- iv. 160.0.234.208

The first two proxies can only be accessed in the academic area during office hour only, during the night, the proxies are left idle. But the remaining two proxies can be accessed both from academic area and students' residential area 24 hours a day.

Starting from January 2006, the need to go through UTP's Internet proxy server for users in the residential area is no longer a necessity. The user can access the Internet directly without any hassle in setting up the connection options in their browser. But, proxy services are still available for those who need it.

4.3 Network Equipment Used

There are several types of equipments that are important to build a network. In UTP, if a user wants to access the Local Area Network, the users must connect through a personal computer or laptop with a 10/100Mbps Network Interface Card to the network hub that is provided for each student in their room. The second equipment that comes in line is the switches located in the server room at the ground floor of each building. A router that is located at every Village's server room will connect all switches in the same Village to the Main Server in Information Technology & Media Services Department (ITMS) in Chancellor's Complex.

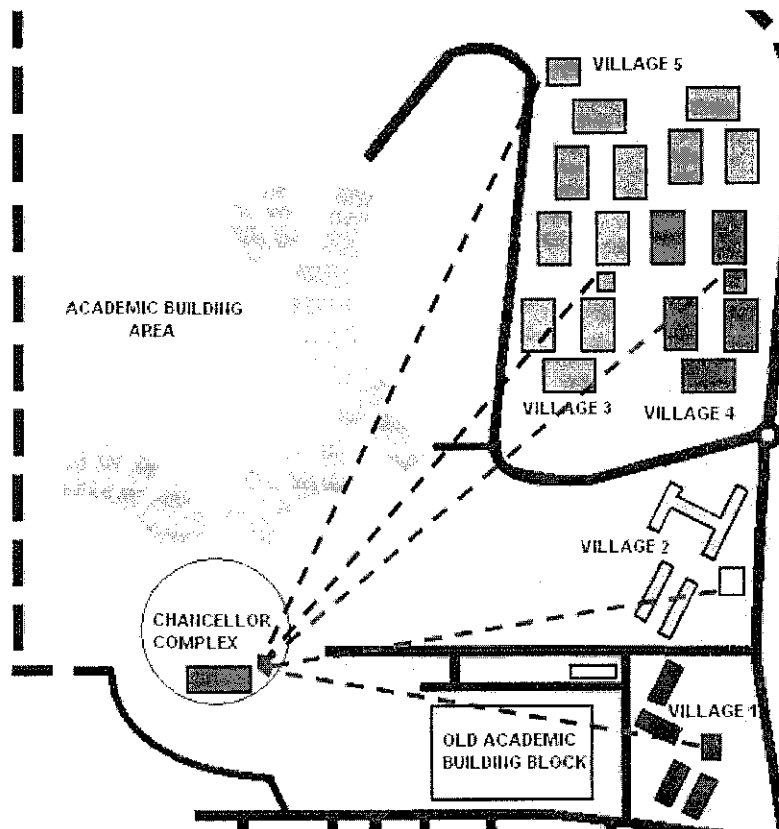


Figure 14 Interconnectivity between routers in students' residential area to the Chancellor's Complex

As being confirmed by ITMS representative, the switches models that are located in every building are Nortel Baystack Portfolio 450 and 470 for Village 1 and 2. Meanwhile, the switches used for the Village 3, Village 4 and Village 5 are Business Policy Switch, also by Nortel. The router model for every village is Passport 8600 Routing Switch and is located at the server room, near the cafeteria.

The 8600 routing switch module is specifically designed for use in the campus and building backbones, where higher performance, routing and MAN/WAN integration are required. For campus backbones burdened with unpredictable intranet traffic flows, the routing switches provide extensive gigabit Ethernet bandwidth to support policy-based traffic prioritization and graphic VLAN configuration [3].

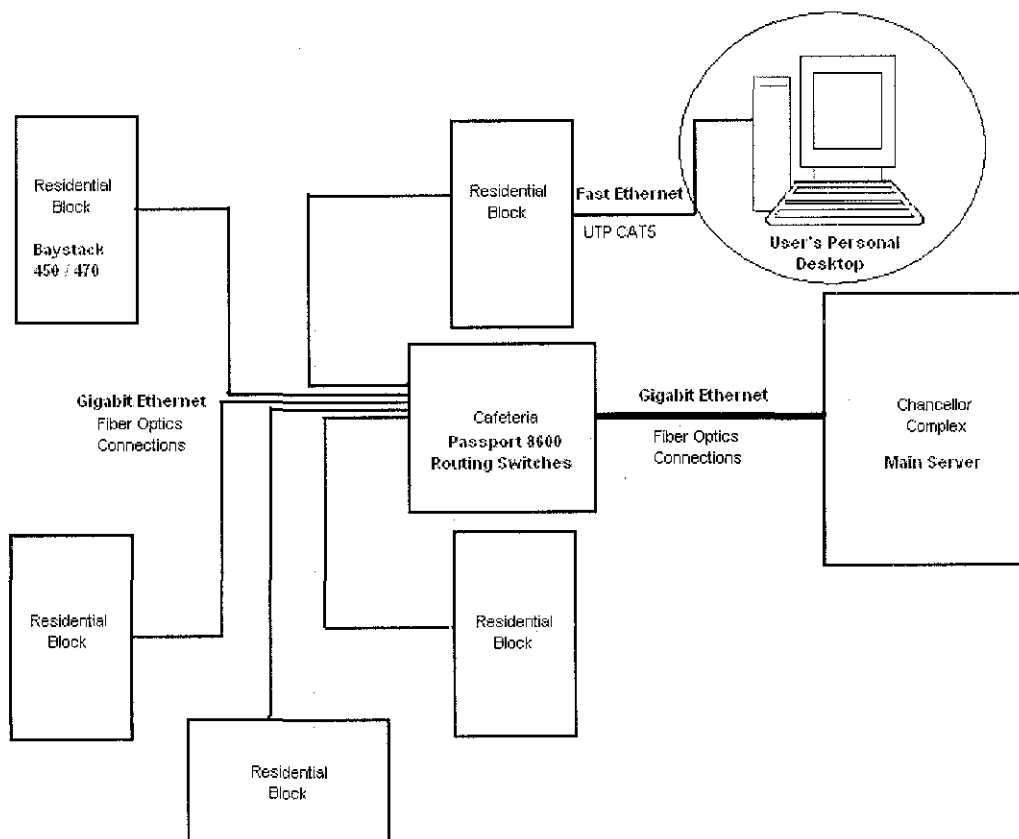


Figure 15 Network equipment diagram for each village in students' residential area

As stated in the diagram above, the connections between the Main Server to the routers, and from the routers to the switches are using fiber optics cable. From the students' connection, Unshielded Twisted Pair (CAT 5) are used.

4.3.1 *Passport 8600 Routing Switch*

The Nortel Networks Passport 8600 series Routing Switch is designed for high-performance enterprise networks. The Passport 8600 is deployed in campus and building backbones needing higher performance, routing, or metropolitan area network (MAN) connectivity. As a key component of the Nortel Networks Optical Ethernet solution, the Passport 8600 Routing Switch delivers Gigabit Ethernet performance and Quality of Service (QoS) for business-critical applications and services such as Internet telephony. The Passport 8600 series provides penalty-free QoS, features a fault-tolerant chassis, and provides a variety of 10/100, Gigabit Ethernet, Packet over SONET and ATM ports, as well as a high-performance infrastructure for core routing and switching. It also provides wire-speed switching and routing over fiber and copper media [3]. Product brief for Passport 8600 is attached in Appendix B.

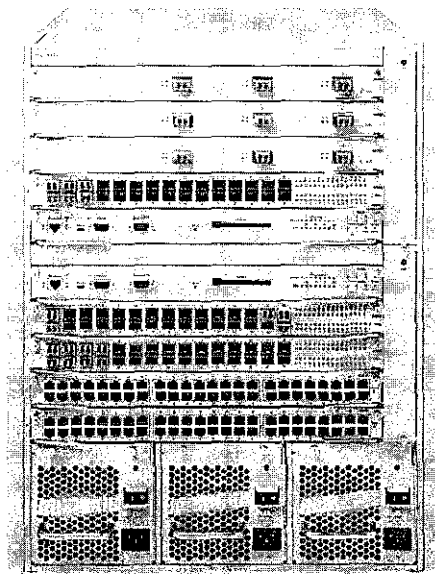


Figure 16 Passport 8600 Routing Switch

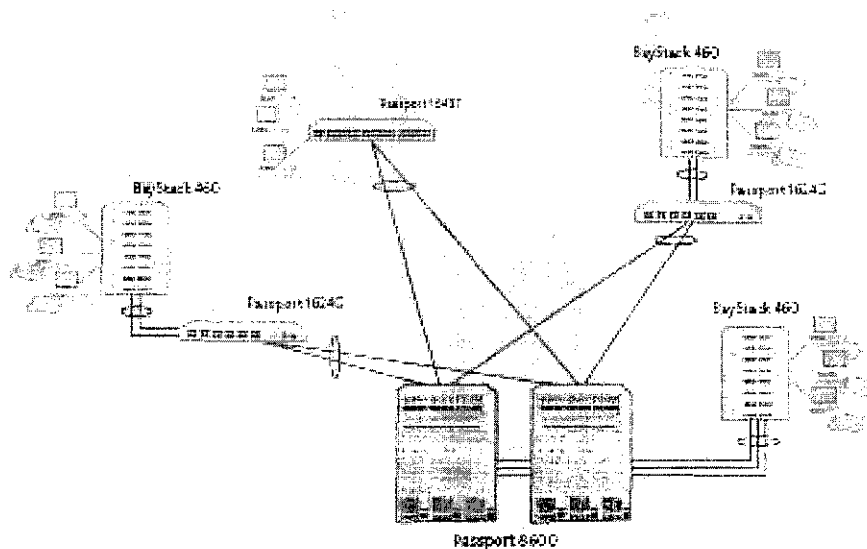


Figure 17 Passport 8600 Routing Switch in a Network Core

4.3.2 Nortel BayStack Portfolio

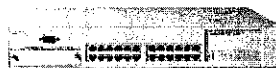


Figure 18 BayStack 450



Figure 19 BayStack 470

The Nortel Baystack portfolio or now known as Nortel Ethernet Switch portfolio provides small and medium businesses and large enterprises high-throughput networking at low ownership cost per port. A cascade stacking arrangement combines up to 8 mixed switch-type units, offering hundreds of ports in one managed entity, with no single point of failure. Product brief for BayStack 450 and BayStack 470 are attached in Appendix C and Appendix D, respectively.

4.3.3 Nortel Business Policy Switch

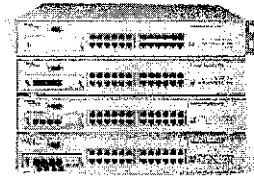


Figure 20 Business Policy Switch

The Nortel Business Policy Switch (BPS) is a 24-port, stackable 10/100 Mbps Ethernet Layer 2 switch that delivers Layer 2/3/4 packet classification and prioritization to the desktop. With Web-based management and advanced IP QoS, this LAN switch is targeted for resource-intensive and delay-intolerant applications in mid- to large-sized enterprises, such as voice over IP, video streaming, and e-commerce. Product brief for Business Policy Switch is attached in Appendix E.

4.3.4 Nortel : Designing the Network

Nortel Networks always recommends a two-tier network approach as opposed to other vendors (especially Cisco) that recommend three levels. The simple two-tiered backbone architecture from Nortel Networks limits the amount of different product platforms required, reducing cost by one third. The components of a classic Nortel Networks designed infrastructure consist of edge devices, including layer-2 switches that will house the workstations and servers, and core routing switches [3].

4.3.4.1 Edge Switches

The focal purpose of the edge switches is to provide desktop connectivity for users and servers and to aggregate all the traffic through high-speed connections back to the core. The edge switches are generally layer 2 switches, where intranet resides. The switches will function as intranets to provide the users with their desktop connectivity in the wiring closets. The types of users will affect the edge switches that will be chosen. For an example,

networks that have limited functionality administrators may use switches that don't have even VLAN capabilities. In a more complicated networking environment, even the edge switches must be high speed and filter the traffic according to specific organization policies [3].

4.3.5 *The Superiority of the Passport*

Based on the book by Bates & Kimmel on Nortel Networks [3], the advantage of Passport Technology employed by UTP's Network compared with other technologies are:

- Nortel Networks designed their products to switch at layer 2 and layer 3 at the same or extremely fast rates.
- Nortel Networks is the leader in providing low and consistent latency compared with other vendors which normally provided a high and unpredictable latency.
- Nortel Networks delivered high-density layer 3 gigabit Ethernet switches with advances features.
- The passport also features superior spanning tree support with Fast Start. With Fast Start, ports can come up instantaneously but still participate with the spanning tree if a loop is detected.
- The Passport is easier to manage and takes less time to configure because of its centralized management architecture.
- In term of cost, Nortel Network provides solution at 25% lower rates compared with other vendors.
- Nortel Networks is one of the leaders in the ISP market in many technology fields. Nortel Networks also offers an end-to-end solution, but it is not mandatory.

4.4 Packet Captured and Analysis using Protocol Analyzer

Using Protocol Analyzer, a network data from the Academic Area have been captured for the purpose of understanding its packet and frame contents. After using decodes feature in Protocol Analyzer, four frames have been captured and analyse.

Frame	Len	Absolute Time	Source	Destination	Prot	Description
1308	64	16:37:44.800534	160.0.226.2	239.255.255.254	ETHER IP IGMP	00-04-38-13-41-60 -> Intrnt-00-00-01 160.0.226.2 -> 239.255.255.254 Id=0000 Query Grpaddr:239.255.255.254
1309	64	16:37:44.899709	160.0.226.2	224.0.1.24	ETHER IP IGMP	00-04-38-13-41-60 -> Intrnt-00-00-01 160.0.226.2 -> 224.0.1.24 Id=0000 Query Grpaddr:224.0.1.24
3392	64	16:41:56.314742	160.0.226.2	239.255.255.254	ETHER IP IGMP	00-04-38-13-41-60 -> Intrnt-00-00-01 160.0.226.2 -> 239.255.255.254 Id=0000 Query Grpaddr:239.255.255.254
3393	64	16:41:56.413956	160.0.226.2	224.0.1.24	ETHER IP IGMP	00-04-38-13-41-60 -> Intrnt-00-00-01 160.0.226.2 -> 224.0.1.24 Id=0000 Query Grpaddr:224.0.1.24

Figure 21 Protocol Analyzer Decodes Summary

In this chapter, only Frame #1308 will be explained in detail. For the other three frames, the packet description is almost the same. The details can be obtained in the Appendix F.

Below is the frame detail information, as presented in the Protocol

Analyzer:

Record #1308 (From Hub To Node) Captured on 10.13.04 at 16:37:44.800534300 Length = 64
Runtime Frame# 1308

----- ETHER Header -----

ETHER: Destination: Intrnt-00-00-01 (01-00-5E-00-00-01)
ETHER: Source: 00-04-38-13-41-60
ETHER: Protocol: IP
ETHER: FCS: E2D21F08

----- IP Header -----

IP: Version = 4
IP: Header length = 20
IP: Differentiated Services (DS) Field = 0xC0
IP: 1100 00.. DS Codepoint = Class Selector Codepoint (48)
IP:00 Unused
IP: Packet length = 28
IP: Id = 0
IP: Fragmentation Info = 0x0000
IP: ..0. Don't Fragment Bit = FALSE
IP: ..0. More Fragments Bit = FALSE

```
IP: ...0 0000 0000 0000 Fragment offset = 0
IP: Time to live = 1
IP: Protocol = IGMP (2)
IP: Header checksum = 471F (Verified 471F)
IP: Source address = 160.0.226.2
IP: Destination address = 239.255.255.254
```

```
----- IGMP Header -----
IGMP: Message Type = Membership Query (17)
IGMP: Max Response Time = 5 (in 1/10 seconds)
IGMP: Header checksum = 0xFEFB (Verified 0xFEFB)
IGMP: Group Address = 239.255.255.254
```

As can be seen above, the first line displays the general information about the frame, which consist frame number, destination, capturing time and frame length. It is followed by Ethernet Header, IP Header and IGMP Header.

4.4.1 Ethernet Header

The Ethernet frame consists of these three parts.

- i. Address:
The address of the sender and or receiver
- ii. Error Detecting Code:
A Frame Check Sequence is often included for error detection
- iii. Protocol Control:
Additional information is included to implement the protocol functions listed in the section.

```
----- ETHER Header -----
```

```
ETHER: Destination: Inrnt-00-00-01 (01-00-5E-00-00-01)
```

- o The MAC address of the destination

```
ETHER: Source: 00-04-38-13-41-60
```

- o The MAC address of the source

```
ETHER: Protocol: IP
```

- o The type of protocol used

```
ETHER: FCS: E2D21F08
```

- The Frame Check Sequence

4.4.2 IP Header

IP provides an unreliable and connectionless datagram delivery service. It is unreliable because IP is a best effort service. If anything goes wrong, IP will simply discard the datagram and attempt to send an ICMP message back to the source. Reliability must be provided by the upper layers, e.g. TCP or UDP. It is connectionless because IP maintains no state information about successive datagrams. Each datagram is independent from all other datagrams. This means that datagrams can get delivered out of order.

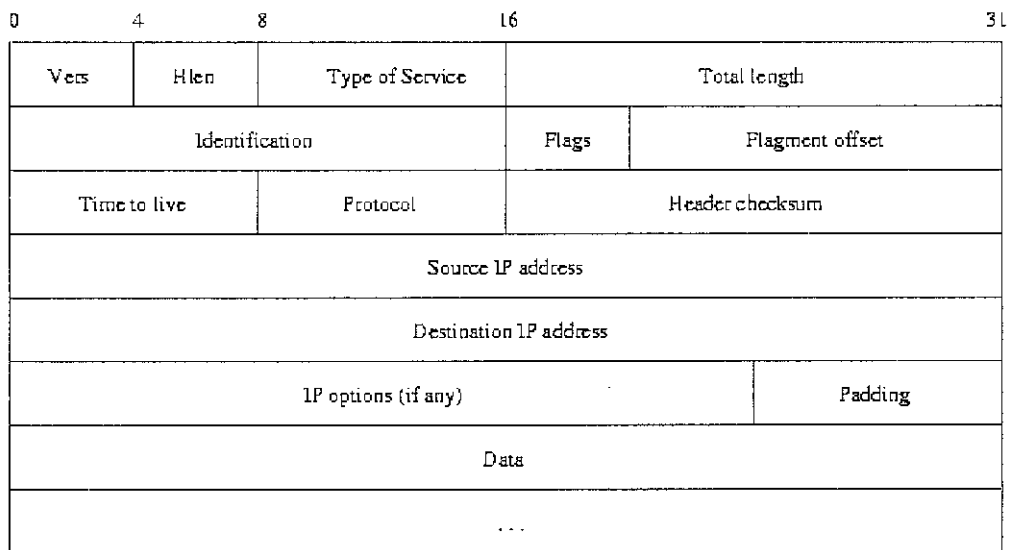


Figure 22 IP Datagrams

----- IP Header -----

IP: Version = 4

- This field defines the current version of IP implemented by the network station. Version 4 (IPV4) is the latest version, although IPV6 is being experimentally deployed.

IP: Header length = 20

- The Header Length Field (HLEN) defines the length of the IP header excluding the IP data field. Not all fields in the IP header must be used. The header length field contains the number of 32-bit words in the header. The shortest possible IP header is 20 bytes. Therefore, this field would contain a minimum entry of 5 (20 bytes = 160 bits; 160 bits/32 bits = 5). This field is necessary, because the header can be variable in length, depending on the IP Options field.

IP: Differentiated Services (DS) Field = 0xC0

IP: 1100 00.. DS Codepoint = Class Selector Codepoint (48)

IP:00 Unused

- Differentiated Services is a method of trying to guarantee quality of service on large networks such as the Internet. This field, previously called Service Type, is now called Differentiated Services. The interpretation of DS, the first 6 bits make up the codepoint subfield and the last two bits are not used. In the codepoint section, the bits in binary are 110 000. Since the 3 right-most bits are 0s, the 3 left-most bits are interpreted the same as the precedence bits in the service type interpretation. In other words, it is compatible with the old version.
- In the old version, the 3 left-most bits are called the precedence bits. The precedence defines the priority of the datagram in issues such as congestion. If router is congested and needs to discard some datagrams, those datagrams with lowest precedence will be discarded first.

IP: Packet length = 28

- This is the 16-bit field that defines the total length (header plus data) of the IP datagram in bytes. To find the length of the data coming from the upper layer, subtract the header length from the total length. The header length can be found by multiplying the value in the HLEN field by four.

$$\text{Length of data} = \text{Total length} - \text{Header length}$$

IP: Id = 0

- Identifies a group to which datagrams belong so that they do not get mismatched. The receiving IP layer uses this field and the source IP address to identify which fragments belong together.

IP: Fragmentation Info = 0x0000

IP: ..0. Don't Fragment Bit = FALSE

IP: ..0. More Fragments Bit = FALSE

- Flags field is a three bit field. The first bit is reserved. The second bit is called the do not fragment bit. If its value is 1, the machine must not fragment the datagram. If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host. If the value is 0, it can be fragmented if necessary. The third bit is called the more fragment bit. If its value is 1, it means the datagram is not the last fragment; there are more fragment after this one. If the value is 0, it means this is the last or the only fragment.

IP: ...0 0000 0000 0000 Fragment offset = 0

- The IP headers from each of the fragmented datagrams are almost identical. This field indicates the offset in bytes from the previous datagram that continues the complete datagram. In other words, if the first fragment has 512 bytes, this offset would indicate that the second datagram starts the 513th byte of the fragmented datagram. It is used by the receiver to reassemble the fragmented datagram. In this frame, it shows that there are no offsets.

IP: Time to live = 1

- In IPv4, time to live (TTL) is an 8-bit field in the Internet Protocol (IP) header. It is the 9th octet of 20. The time to live value can be thought of as an upper bound on the time that an IP datagram can exist in an internet system. The TTL field is set by the sender of the datagram, and reduced by every host on the route to its destination. If the TTL field reaches zero before the datagram arrives at its destination, then the datagram is discarded and an ICMP error datagram (11 - Time Exceeded) is sent back to the sender. The

purpose of the TTL field is to avoid a situation in which an undeliverable datagram keeps circulating on an internet system.

IP: Protocol = IGMP (2)

- The protocol field is used to indicate which higher level protocol should receive the data of the datagram (i.e., TCP, UDP, or possibly other protocol like IGMP for multicasting). This field allows multiplexing of many protocols over the same IP interface. In this frame, the protocol used is IGMP (2) which is Internet Group Management Protocol Version 2.

IP: Header checksum = 471F (Verified 471F)

- The header checksum field is a cyclic redundancy check (CRC) of 16 bits. The idea behind it is to ensure the integrity of the header. A CRC number is generated from the data in the IP data field and placed into this field by the transmitting station. When the receiving station reads the data, it computes a CRC number. If the two CRC numbers do not match, there is an error in the header and the packet will be discarded. Each router that receives the datagram recomputes the checksum because the TTL field is changed by each router that the datagram traverses.

IP: Source address = 160.0.226.2

IP: Destination address = 239.255.255.254

4.4.3 IGMP Header

Brief explanation on the definition of IGMP has been placed in Chapter 2. Detail explanation about the content of IGMP message is stated below:

----- IGMP Header -----

IGMP: Message Type = Membership Query (17)

- This 8 bit field defines the type of message. There are 3 types of message, Membership Query (0x17), Membership Report (0x16) and Leave Report

(0x17). The query message is a multicast using the multicast address 224.0.0.1 (all system in the subnet). All hosts and all routers will receive the message.

IGMP: Max Response Time = 5 (in 1/10 seconds)

- This 8 bit field defines the amount of time in which a query must be answered. The value is tenths of a second. The value is nonzero in query message.

IGMP: Header checksum = 0xFEFB (Verified 0xFEFB)

- This is a 16 bit field carrying the checksum. The checksum is calculated over the 8 byte message.

IGMP: Group Address = 239.255.255.254

The value is 0 for a general query message. The value defines the multicast address of the group in the special query, the membership report and the leave report message.

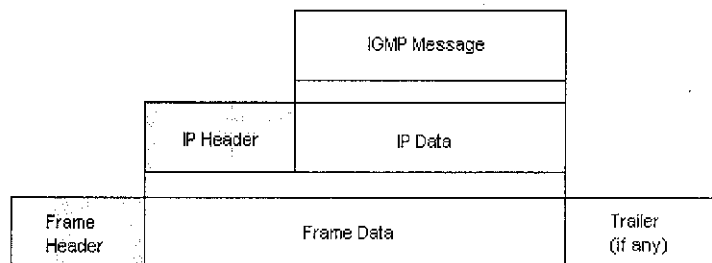


Figure 23 Encapsulation of IGMP message in an Ethernet Frame

4.5 Users' survey and feedback

For the purpose of surveying the UTP network from the student's point of view, 100 questionnaires have been distributed in random to the UTP students in September 2005. The main purpose of this questionnaire is to produce a statistic about the current service provided by the IT & Media Support department of UTP. The questions ranging from the student's general knowledge in networking, to their network utilization, applications launched major problems experiences and also include their recommendation to improve the current network situation.

100 students have participated in this survey and they are grouped into 4 divisions, which are:

Group	Gender	Standing Year	Total Number of Participants
A	Male	Year 1, 2 & 3	16
B		Year 4 & 5	22
C	Female	Year 1, 2 & 3	10
D		Year 4 & 5	52

Table 2 Survey group divisions

All of the participants reside in Village 3, 4 and 5. This survey focused more on the fourth and fifth year students because they have experience the network in a longer time, thus enable them to provide proficient answer according to their understanding. Sample of the questionnaires is attached in Appendix G.

4.5.1 Data Analysis

The questionnaire is divided into three division; Personal Information, General Information and UTP Intranet and Internet. The first division meant to separate the participants into three groups by gender, standing year and residential village. In the general information, the questions asked are related to the basic knowledge about computer ownership and basic knowledge about networking. The third column contained questions regarding the reliability, services provided, applications and other related questions.

4.5.2 General Information

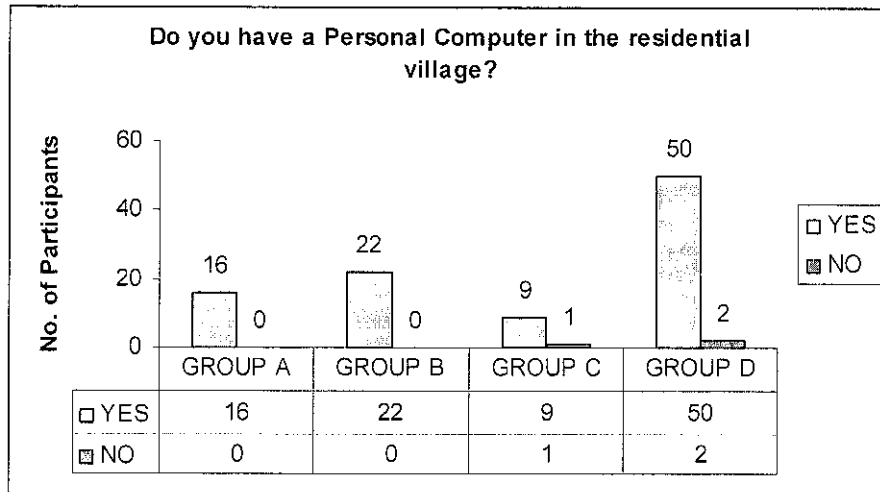


Figure 24 Personal Computer ownership statistics of the students

Referring to the Figure 24, the total number of students that owned a PC is 97% compared to 3% students' who did not own a PC. This shows that computer played an important role as a medium for education and also entertainment. Since Figure 25 also shows almost similar results, it can be concluded that every student that owned a PC will connect to the network through the intranet hub in the room.

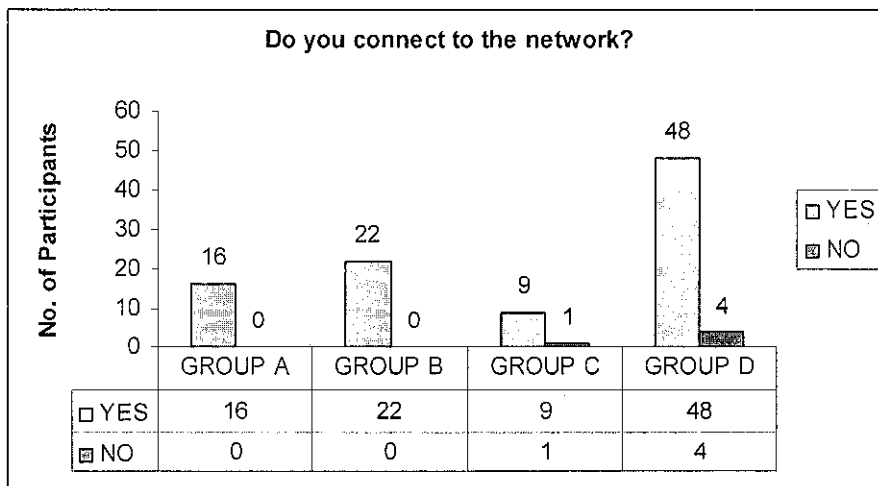


Figure 25 Network connectivity statistics of the students

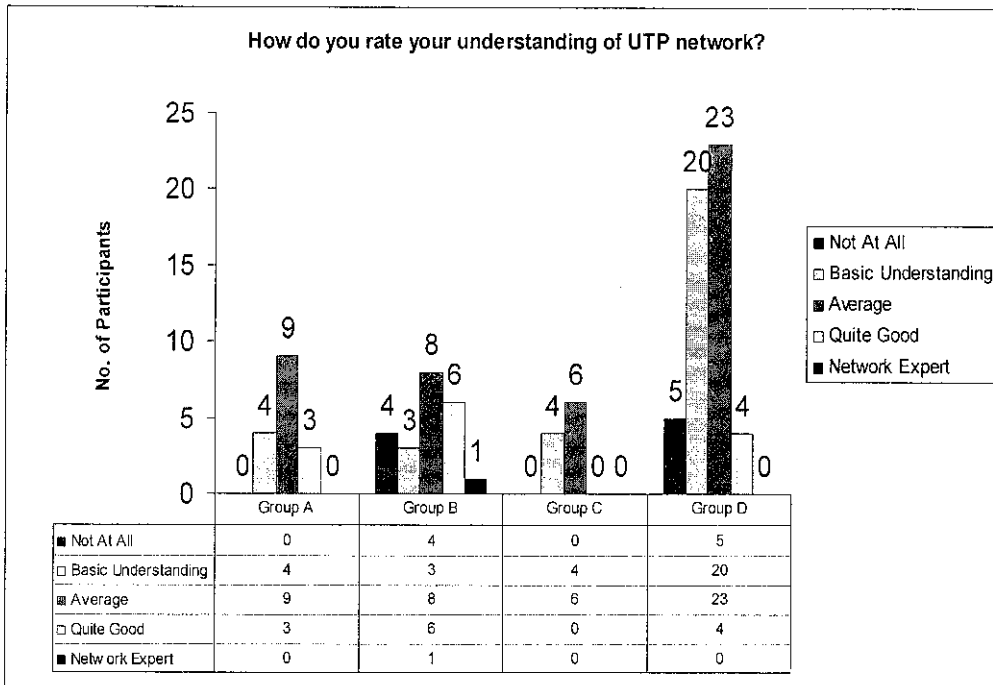


Figure 26 Network understanding statistics of the students

For Figure 26, the question is formed to get an overview at the level of network expertise between students. 46% of the students are having average rate of understanding about UTP network. The scope of understanding in this questions are the IP addressing between each blocks, basic connection topology and network applications.

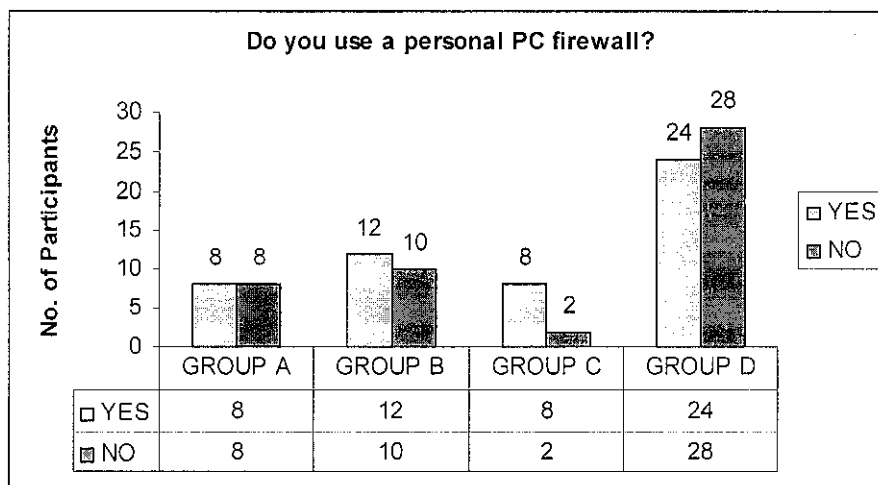


Figure 27 PC firewall usage statistics of the students

The question in Figure 27 simply asked about the awareness of network threat in the network. The results shown that 52% of the students used a PC firewall during connected to the network. Meanwhile, another 48% is simply connected without any protection. From the questionnaires answer, most of the students used Zone Alarm and Sygate Personal Firewall to manage their personal network security.

4.5.3 UTP Intranet & Internet

The purpose of the questions in this category are to rate the level of satisfactory about the current network, their own point of view about UTP network, problems experienced and recommendation.

The question in Figure 28 refers to UTP networks reliability. The scope of reliability in questions is about the consistency of the services provided. Most of the students' rate the reliability as "Bad", followed by "Adequate", "Very Bad" and only 12% of the students rated the reliability as "Good" or "Very Good". Since the statistics leans toward the negative side, it can be concluded that more than half of the students' do not satisfied with the services provided.

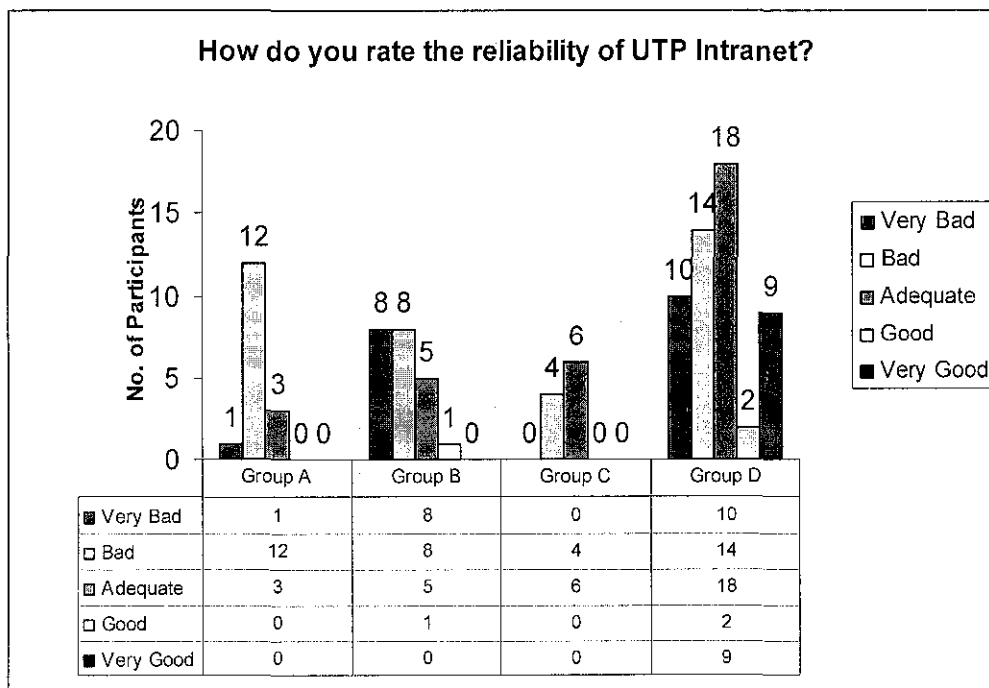


Figure 28 The UTP Intranet reliability survey

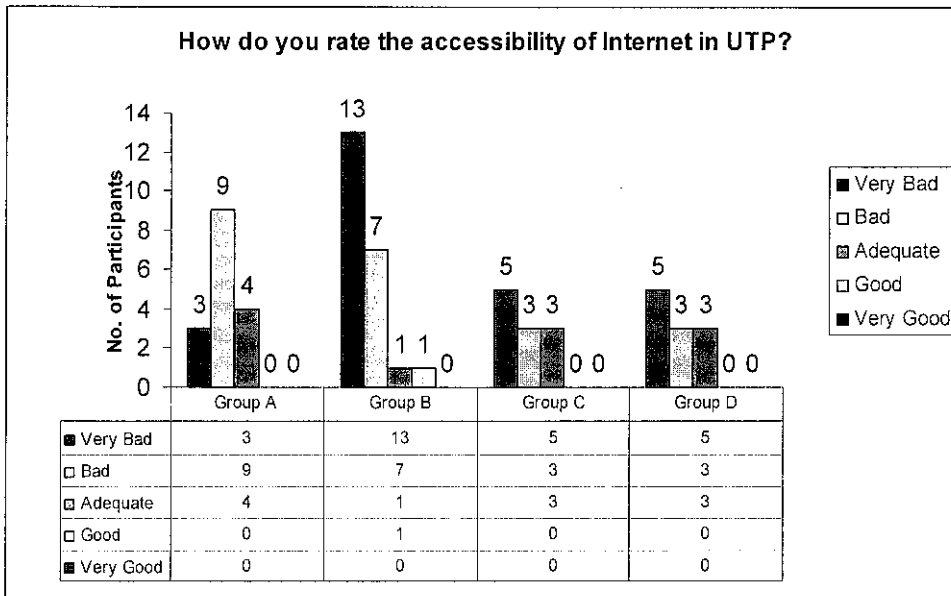


Figure 29 Internet accessibility statistics among the students

From Figure 29, within a glance a conclusion the Internet accessibility at the residential village is very low can be made because 99% of the students rate the accessibility at “Adequate” and below. This will limits the students from the Internet and also formed a barrier for the students to communicate through the internet by using e-mail or instant messenger.

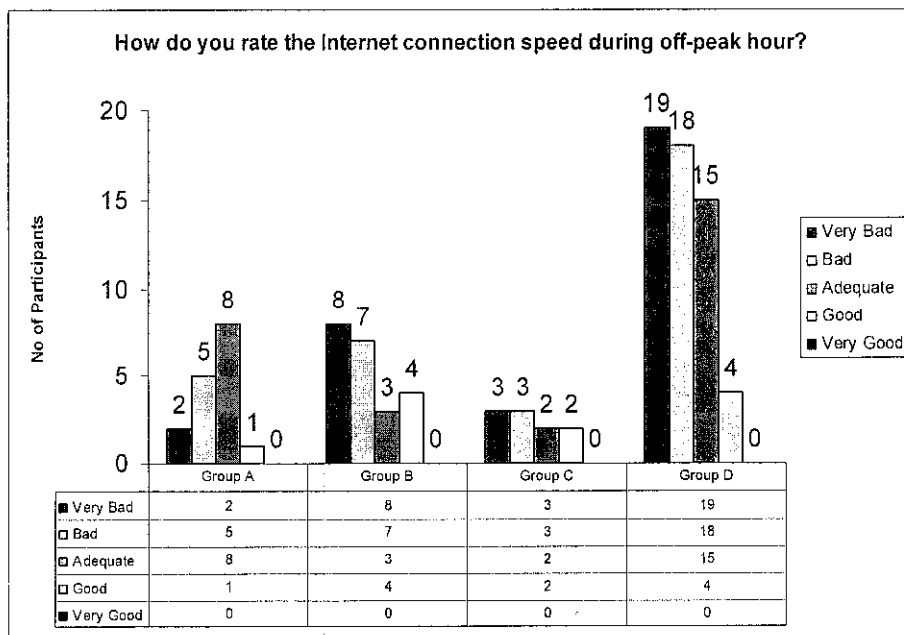


Figure 30 Internet connection speed during off-peak hour statistics

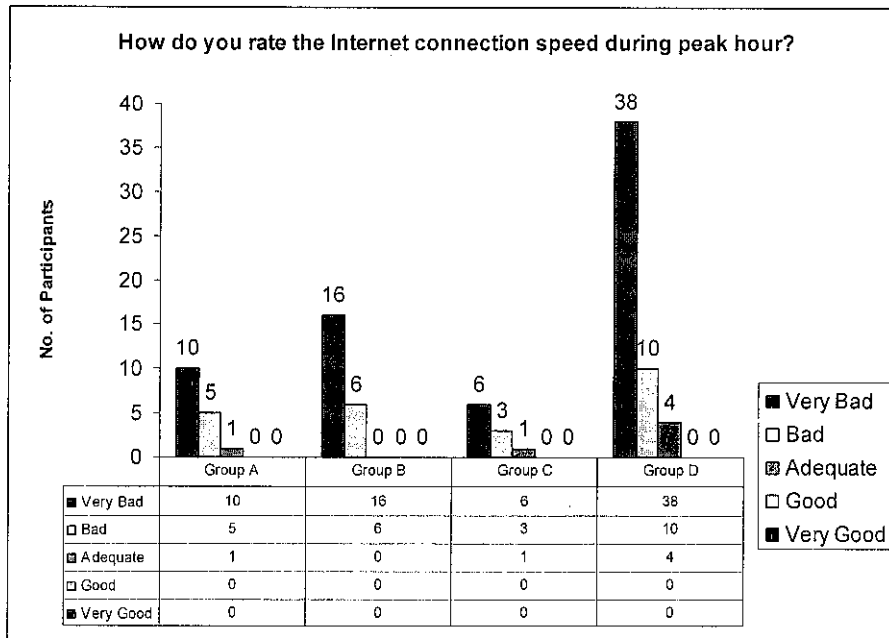


Figure 31 Internet connection speed during peak hour statistics

As being shown in Figure 30 and Figure 31, internet connection speed comparison between peak hour and off peak hour shown a slight difference where during peak hour, 70% of the students rated that the internet connection speed is very bad and 0% of the students rated the internet connection speed as “Good” and “Very Good”. During off-peak hour, the percentage of students that rated the internet connection speed is reduced to 32% but still 0% rated the connection as “Very Good”.

In the survey, the students are requested to state their view on the importance of Internet connections in UTP, most of the students stated that the internet is very important as an educational tool that provides vast choices of information, from numerable source. Most of the students connect to the internet to do research for their Final Year Project, surfing, emailing, and most of the international students stated that internet is their easiest way to communicate back to their home country.

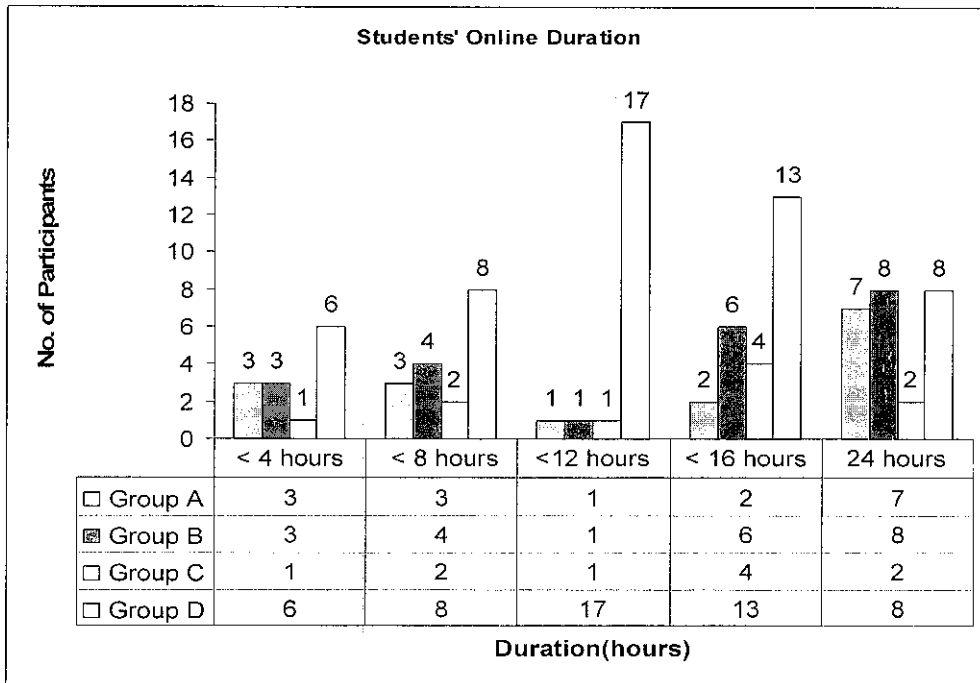


Figure 32 Students online duration statistics

From Figure 32, it can be concluded that most of the students connected to the network in a long duration, and sometimes even 24 hours straight without turning it off. This will contribute to the high network utilization. From figure 33 below, it also prove that 24% of students that never turning off their pc, by keeping it idle even during time that they are not in UTP. This will contribute to the unnecessary network traffic and bandwidth consumption.

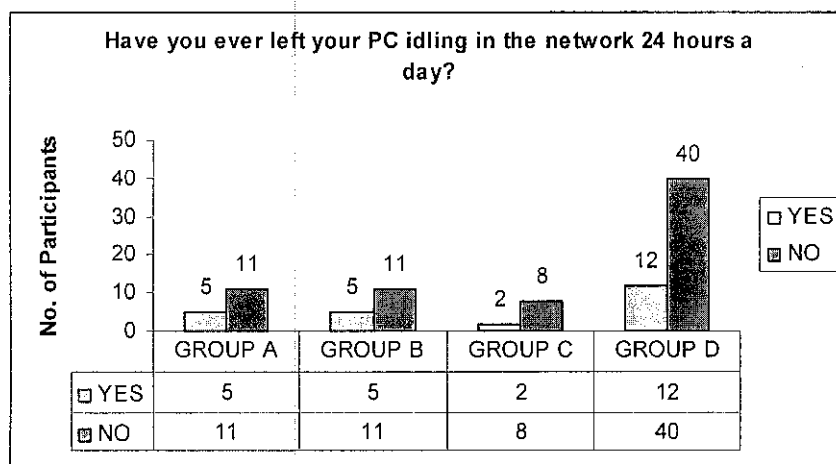


Figure 33 PC idling statistics among the students

From the question no. 7 (refer Appendix G), most of the students stated that most of the time, they will connect to the network to launch the mIRC program and also the internet browser.

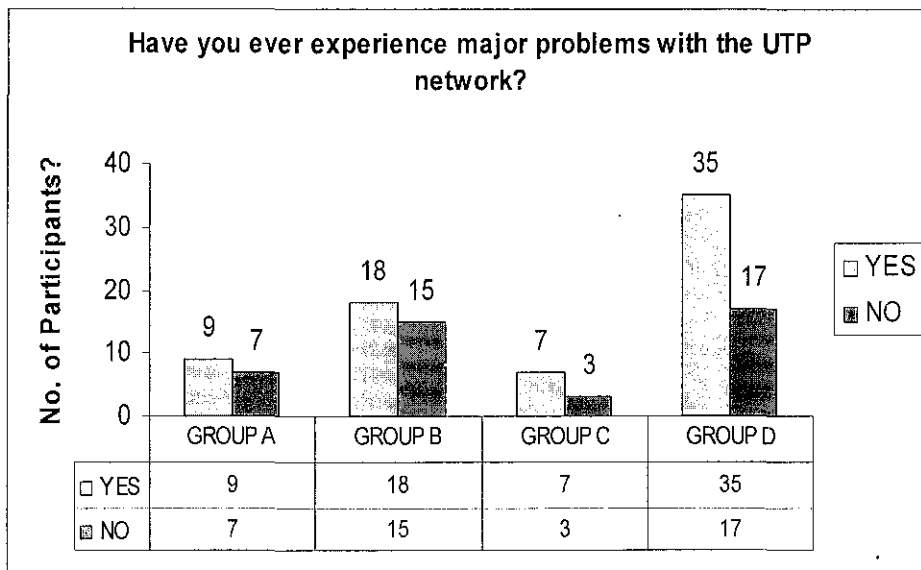


Figure 34 Network problems statistics among students

From Figure 34, it can be concluded that 69% of students in UTP have experience network problems. Most of the problems experienced by the students are about the worms that spread in the network and also about the Novell software that the network administrator used to manage the network. These occurrence will reduce the efficiency of the network, thus the students will have problems during connecting to the network.

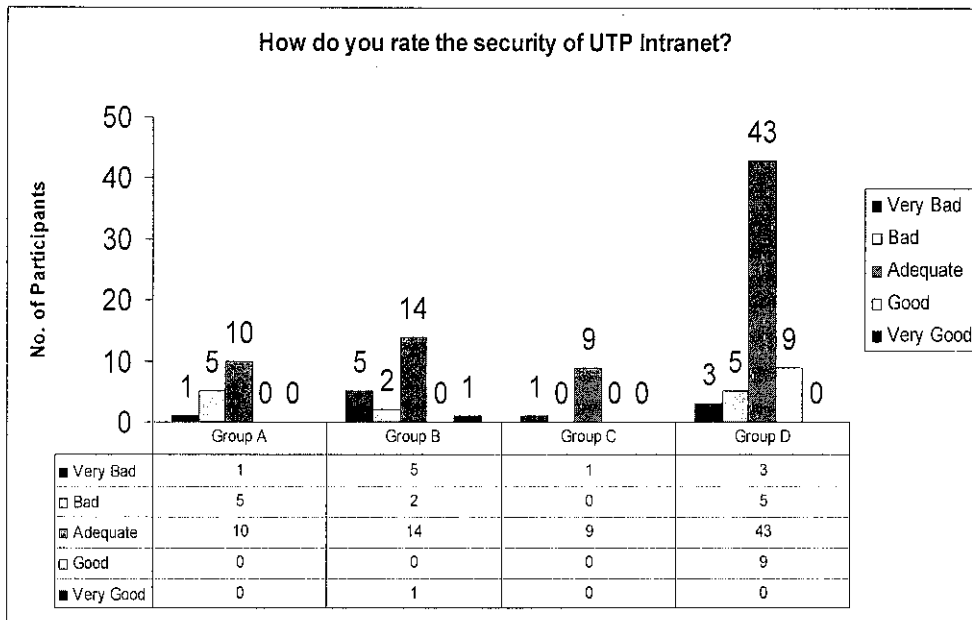


Figure 35 UTP Intranet security statistics

In Figure 35, most of the students rated that the security level is adequate. The questions main purpose is to observe the awareness of the students about viruses and worms distribution threat in the network.

At the last part of the questionnaires, most of the students recommend the network management to improve the current network situation to provide a better service. The students are expecting a faster network, a consistent service and less disruption. They also suggested that the network management reduce the setback of the internet by allowing wider choices of network utilization. The current intra-village connection is also a hindrance for the students in communicating, and it restricts the student to communicate with students that reside in other villages.

4.6 Application Runs and Bandwidth Consumption

In this report, some of the applications that monopolize the network bandwidth will be explained in depth. The applications are listed below:

- i. E-Learning Portal
- ii. mIRC
- iii. Bulletin Board/Internet Forum
- iv. Radio Streaming
- v. Gaming Server

4.6.1 E-Learning Portal

This portal is hosted by UTP for the ease of students to obtain information about the courses they enrolled for the semester. The information can be in the form of announcement, lecture materials, assignment, projects and also results. The website can be access by visiting <http://www.elearning.edu.my> via the Internet or the Local Area Network. Each student will have their own user ID and password to access the site, therefore no anonymous user can access the data hosted there.

4.6.2 mIRC



mIRC is a shareware Internet Relay Chat client for Windows, created in 1995 and developed by Khaled Mardam-Bey. This was originally its only use, but it has evolved into a highly configurable tool that can be used for many purposes due to its integrated scripting language. Other uses may include:

- IRC bot / channel management
- MP3 player
- Web page parser (usually for retrieving search results or headlines)
- DCC, HTTP, and IRC server

mIRC is highly popular, as it has been downloaded nearly eight million times from CNET's download.com service as of August 2005. Nielsen Net

Rankings also rated mIRC as among one of the top 10 most popular internet applications in 2003.

In UTP, the software has been unofficially one of the most important communication medium between the students in the residential area, and also utilizes by several users connected from the academic area. Several of the benefits of mIRC in the students' communication context are:

- i. Enhance communication easily among the students, irrespective of gender and race. It serves as a medium for virtual discussions more apparent and convenient, while eliminating the need for physical discussions.
- ii. Students have more liberty in transferring files and documents that are in need for immediate attention. It is very crucial for group based projects, assignments and laboratory reports that are given out throughout the semester.
- iii. mIRC network allow important announcements to be delivered to the respective students more effectively and have been proven to be a very good advantage to students especially to spread out news from lecturers and concerning academic information and news more quickly. Normal means or channels used to spread events and happening are less reliable at times thus a centralized source for students to check on any news and latest update within UTP is much needed.

There are 5 mIRC server located in the students' residential areas, in Block B Village 1, Block B Village 2, Block E Village 3, Block E Village 4 and Block C Village 5 respectively and are provided, managed and maintained by a group of students. Currently, every server can cater about 1000 to 2000 users at one time, depends on the server memory size. To connect to the server, fives addresses of server are listed below:

- | | | | | | |
|------|-----------|-----|-------------|-----------|----------------------|
| i. | Village 1 | IP: | 161.0.2.210 | DNS Name: | togakure.utpchat.net |
| ii. | Village 2 | IP: | 162.0.2.210 | DNS Name: | awaken.utpchat.net |
| iii. | Village 3 | IP: | 163.0.5.210 | DNS Name: | evilz.utpchat.net |
| iv. | Village 4 | IP: | 164.0.5.210 | DNS Name: | student.utpchat.net |
| v. | Village 5 | IP: | 165.0.5.210 | DNS Name: | soul.utpchat.net |

Recently, the inter-village connection has been blocked by the respective UTP IT Department due to the excessive bandwidth usage and this has been a major drawback. The current network situation did isolate the students' residential area into separate LANs according to their village. This shunned the students' from optimizing the software features effectively.

4.6.3 Bulletin Board/Internet Forum

A conventional bulletin board is a place where people can leave public messages, for example, to advertise things to buy or sell, announce events, or provide information. Bulletin boards are often made of a material such as cork to facilitate addition and removal of messages. But, in accordance with the technology advancement, an online bulletin board or Bulletin Board System(BBS) have been popular especially with the online community.

In UTP, one popular bulletin board or often called the 'UTP Grapevine' is hosted by the student to enable UTP student to involve in an online community that allow every students to voice out their opinions freely about any issues . UTP Grapevine also has all the featured as other bulletin board system describe above. UTP Grapevine can be accessed via <http://grapevine.utpchat.net> for LAN users or <http://www.myutp.org> via internet.

4.6.4 Radio Streaming

SHOUTcast is Nullsoft's Free Winamp-based distributed streaming audio system. It only needs an audio player, such as Winamp and the audio streaming are ready to be accepted. There are a number of students who inspire to be a radio DJ hosted this audio streaming application and the links are distributed freely in the mIRC.

4.6.5 Gaming Server

There is numerous numbers of online games in the world. In UTP, there are a number of students that hosted a server dedicated for this online gaming, such as Half Life: Counter Strike, Defence of The Ancients, Ragnarok, Need for Speed Underground 2 and even games like Solitaire and Monopoly. The gaming server often utilizes port number 27010 and above as their root of connections.

4.7 UTP's Network Traffic Statistical Data

This data was originally planned to be captured by the author using the Protocol Analyzer, but since there is some difficulty to access the Students' Residential Area network as a whole, the same data captured by ITMS has been used as a replacement. With the cooperation from the representative, a considerable number of information related to the UTP network traffic was obtained. The data was captured on 10am until 4 pm on 9 March 2006.

The data obtained includes:

1. Top Hosts by Packet Sent
2. Top Conversation by Packets
3. Protocol Distribution

From the brief analysis done, the data contained in described the host address and the packet counts. The host name is not provided; just the numbered address is given. So, the DNS for every address given need to be determined. The data is arranged according to the number of packet sent, with <http://www.oracle.com/technology/software/index.html> in the top most position. The information is mixed with the LAN addresses and the Internet addresses in the same page and for the detailed report later, the hosts name will be arranged according to their origins.

Name	Address	Count
download-oc-west.navisite.net	206.204.021.139	99,567
relay1.voice.tpe.yahoo.com	202.043.193.118	96,698
No Hostname	060.051.094.222	63,347
No Hostname	061.060.021.202	50,934
No Hostname	213.252.189.079	21,943
cds15.sjc.llnw.net	069.028.178.068	18,256
No Hostname	209.245.059.120	16,803
Web Proxy	066.090.101.058	14,417
163.000.001.075	163.000.001.075	14,322
cds2.sjc.llnw.net	069.028.178.012	13,457
061.200.083.062	061.200.083.062	13,349
75.67-18-200.reverse.theplanet.com	067.018.200.075	13,288
www.ovh.com	213.251.141.038	13,098
No Hostname	061.058.044.222	12,458
a202-187-31-42.deploy.akamaitechnologies.com	202.187.031.042	12,409
a202-187-31-45.deploy.akamaitechnologies.com	202.187.031.045	11,613
No Hostname	058.227.193.190	11,212
ns20324.ovh.net	213.251.134.046	11,018
Unable to resolve hostname (Dead)	218.111.236.171	10,861
a61-208-229-143.deploy.akamaitechnologies.com.128.229.208.61.in-addr.arpa	061.208.229.143	10,542
sourceforge.optusnet.com.au	211.029.132.142	9,076
Unable to resolve hostname (Dead)	130.237.111.123	9,019
066.249.093.176	066.249.093.176	8,558
196.035.064.036	196.035.064.036	8,309
No Hostname	066.045.235.228	8,244
165.000.004.234	165.000.004.234	7,688

Table 3 Top Hosts by Packet Sent (External IP)

If Table 3 and 4 just listed the highest number of packets sent by certain host, Table 5 will describe the conversation between two hosts, complete with its packet quantity exchanged in between. The Protocol Distribution contained a numerous number of protocols and a lengthy explanation will be needed to describe each one of them.

Name	Address	Count
Village 5, Block F	165.000.012.214	87,525
Village 5, Block A	165.000.002.068	83,197
Village 5, Block E	165.000.010.042	75,852
Village 5, Block C	165.000.005.005	74,647
Village 3, Block B	163.000.003.023	69,237
Village 5, Block E	165.000.010.028	68,939
Village 5, Block D	165.000.008.101	50,535
Village 5, Block D	165.000.007.087	39,391
Village 3, Block A	163.000.001.013	31,536
Village 5, Block E	165.000.009.040	17,135
Village 3, Block A	163.000.001.070	16,088
Village 3, Block A	163.000.001.009	15,241
Village 5, Block B	165.000.003.058	14,463
Village 3, Block A	163.000.001.075	14,322
Village 3, Block A	163.000.001.024	12,636
Village 5, Block B	165.000.002.080	11,533
Village 3, Block B	163.000.002.066	10,157
Village 3, Block E	163.000.005.026	10,150
Village 5, Block A	165.000.001.027	9,858
Village 3, Block B	163.000.002.084	9,811
Village 3, Block E	163.000.005.210	9,610
Village 3, Block B	163.000.002.001	9,477
Village 3, Block B	163.000.002.059	9,436
Village 3, Block B	163.000.002.043	9,263
Village 3, Block E	163.000.005.074	9,103
Village 5, Block B	165.000.004.234	7,688




Table 4 Top Hosts by Packet Sent (Internal IP)

Name A	Cnt A->B	Cnt B->A	Name B	Whois Database Referred
061.060.021.202	216,020	346,460	165.000.008.101	APNIC
209.245.059.120	64,794	4,987	165.000.007.087	APNIC
012.120.005.107	35,751	21,872	163.000.001.013	ARIN
069.028.178.068	36,471	3,950	163.000.001.075	ARIN
069.028.178.026	35,618	3,978	163.000.001.013	ARIN
069.028.178.040	31,790	6,007	163.000.001.013	ARIN
012.120.025.017	17,413	16,455	163.000.001.013	ARIN
069.028.178.069	26,150	7,118	163.000.001.013	ARIN
069.028.176.053	17,270	14,605	163.000.001.013	ARIN
012.120.045.017	27,188	3,482	163.000.001.013	ARIN
069.028.178.068	26,516	3,755	163.000.001.106	ARIN
069.028.178.020	19,409	3,585	163.000.001.013	ARIN
123.123.123.123	8,259	12,956	165.000.005.089	APNIC
130.237.111.123	19,319	0	163.000.002.084	RIPE
163.000.001.013	8,767	9,365	069.028.176.066	ARIN
163.000.001.013	8,600	9,152	069.028.176.059	ARIN
165.000.008.234	10,103	6,408	196.035.064.036	AFRINIC
066.045.235.228	12,299	1,703	165.000.007.087	ARIN
069.028.176.044	10,391	3,599	163.000.001.013	ARIN
163.000.001.013	4,617	5,028	069.028.176.062	ARIN
163.000.001.013	9,565	0	012.120.101.107	ARIN
062.067.057.031	7,393	2,105	163.000.001.070	RIPE
064.182.248.035	5,654	3,779	163.000.001.037	ARIN
196.035.074.227	8,643	600	163.000.001.045	AFRINIC
165.000.002.083	5,713	2,806	203.162.119.086	ARIN
163.000.001.013	4,107	4,169	069.028.176.060	ARIN
196.035.064.036	6,789	1,288	163.000.001.075	AFRINIC
196.035.064.036	5,764	1,736	163.000.001.046	AFRINIC
196.035.064.036	6,506	711	163.000.001.045	AFRINIC
066.028.206.168	3,837	2,884	163.000.001.070	ARIN
219.018.024.027	6,547	0	163.000.002.066	APNIC
163.000.001.013	2,771	3,395	066.152.098.202	ARIN
163.000.003.050	3,857	2,206	200.081.094.059	LACNIC
218.066.203.235	6,050	0	163.000.002.084	RIPE
067.018.200.075	4,503	1,437	165.000.002.080	RIPE
163.000.002.037	5,379	0	192.166.144.001	APNIC
069.028.176.051	2,714	2,592	163.000.001.013	ARIN
163.000.001.013	2,332	2,522	080.190.066.200	RIPE
081.165.171.211	4,209	115	163.000.003.017	RIPE
059.144.090.010	2,579	1,702	163.000.003.034	APNIC
069.028.176.039	2,973	1,261	163.000.001.013	ARIN
203.162.163.058	3,154	1,044	163.000.001.102	APNIC
163.000.001.013	1,967	2,012	069.028.176.054	ARIN
038.101.153.099	2,849	889	165.000.002.066	APNIC
069.028.176.050	2,013	1,409	163.000.001.013	ARIN
069.028.176.049	2,187	1,181	163.000.001.013	ARIN
062.075.244.211	1,901	1,462	163.000.001.034	ARIN

Table 5 Top Conversation between two hosts

From Table 3, it can be observed that a large number of packets originated from `xxxx-xxx-xxx-xxx.deploy.akamaitechnologies.net`. Further analysis on the packet conversation data also showed numerous conversations between the students PC and websites that contains `xxxx-xxx-xxx-xxx.deploy.akamaitechnologies.net`. The number of packets sends is also quite high.

Akamai Technologies, Inc. headquartered in Cambridge, Massachusetts, is a corporation that provides, among other services, global Internet content caching. Their customers include Yahoo!, AOL Radio, Symantec, Match.com, Google, Microsoft, FedEx, Xerox, iVillage, Apple Computer, Music Television (MTV), the United States Geological Survey, Reuters, Newegg.com, and XM Radio [7]. Even though most of the Akamai's customer seems reputable, there are some other spyware by other company that used the same service provider. The ITMS Department is aware of this spyware, but since most of the Akamai customers are important, they can't put a ban on Akamai's IP. This is one of the ways for spyware to penetrate into UTP's network.

Akamai Technologies, Inc.	
	
Type	Public (NASDAQ: AKAM )
Founded	1995
Location	Cambridge, Massachusetts, USA
Key people	George H. Conrades, Chairman Paul L. Sagan, President & CEO
Industry	Internet Software & Services
Products	Content and Application Delivery Application-Performance Services On-demand-managed services Business Performance-Management Services
Revenue	▲\$283.115 Million USD (2005)
Net Income	▲\$327.998 Million USD (2005)
Employees	784 (2005)
Website	www.akamai.com 

Protocol	Definition	Packets	Octets
HTTP	Hyper Text Transfer Protocol	22,034,178	2,711,489,449
HTTPS	Hyper Text Transfer Protocol (Secure)	8,501,700	1,869,077,825
NCP	NetWare Core Protocol	6,588,381	814,681,735
TCP-OTHER	Transmission Control Protocol	6,108,220	856,406,016
SAP-R3	Service Advertising Protocol	167,057	11,196,570
SMTP	Simple Mail Transfer Protocol	108,398	7,154,304
ENDPOINT-MAPPER	Remote Procedure Call Protocol	56,458	3,726,228
NETBIOS-SSN	Network Basic Input/Output System	30,227	2,031,940
FTP	File Transfer Protocol	28,535	1,895,659
MS-TERMINAL-SERVER	-	13,202	1,307,267
IRCU	Universal Internet Relay Chat	9,500	698,811

Table 6 Top 10 Protocol Distribution

From the table above, it can be concluded that HTTP and HTTPS protocol is the highest protocol employed in the UTP network. Both protocols are used for Internet browsing and instant messaging. In the next page is the tabulated graph related to the table above obtained from the ITMS Department.

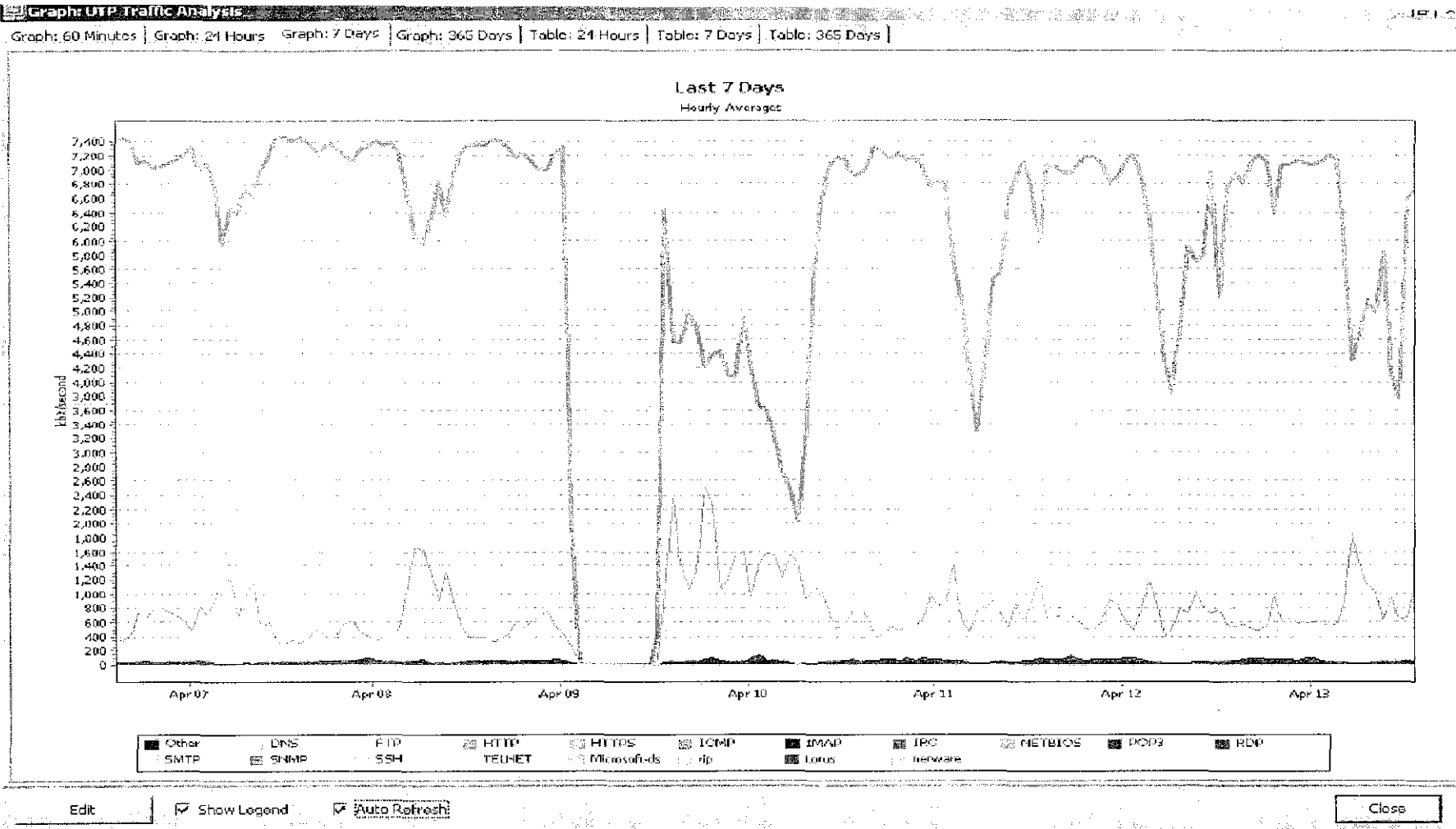


Figure 36 Protocol Distribution Tabulated Graph for 1 Week in Students' Residential Area.

4.8 Degradation on Server Performance

The server performance has been degraded due to congestion introduced by unnecessary and illegal activities. This non-education activities conducted over the network generate unnecessary traffic to the internal gateway, thus bottleneck occurs. Most of the unnecessary traffic sourced from large file transfer, such as movies, audio and games, and audio or video streaming.

Besides, a large number of users hosted file servers, also illegally. This file server does serve large files such as movies, audio files, application software, games and etc. It bombarded the network with excessive signals, messages and traffic.

4.8.1 *mIRC Servers*

By right, no servers are allowed outside the Data Centre and hosting mIRC server is regarded illegal. But, since the users need on user friendly communication medium is high, they hosted their own mIRC server, interconnecting all blocks in the residential area by using their own tunnelling method. The server is hidden from the Academic area and the mIRC administrator disables the file sharing functions for different village. Thus, the unnecessary traffic caused by file transfer is reduced and mIRC is only used as primary communication medium.

4.8.2 *Network Virus*

The network was flooded with network worms and virus that were distributed within the network, especially through insecure file sharing. The virus varies from the vital virus type that will create severe impairment to the end user's PC or the silent worm that will reproduce and redistribute itself until the network was

congested with its traffic. This problem occurs due to ignorance in basic network security knowledge. Most of the users infected do not realize they are the main distributor for the worms or virus until it is too late. To rectify this problems, the ITMS Department have urged every students to install and update their anti virus software. By keeping the virus definition up-to-date, any new viral attack can be discovered before it affect a larger system, such as the servers. To increase the security, nowadays most of the students install they own firewall software that will filter inbound and outbound traffic generated by their own PC.

Number	Date	Time	Origin	Service	Source	Destination
1185241	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	52.56.232.149
1185242	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	56.42.98.132
1185243	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	61.204.248.235
1185244	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	40.69.154.195
1185245	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	166.66.85.17
1185246	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	95.242.157.25
1185247	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	170.231.116.37
1185248	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	75.3.40.54
1185249	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	144.181.136.15
1185250	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	20.180.14.55
1185251	18Oct2005	8:05:15	utpfw2	TCP	microsoft-ds	72.79.144.224
1185252	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	115.73.32.58
1185253	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	5.295.124.231
1185254	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	15.144.155.155
1185257	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	60.165.193.189
1185263	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	24.211.102.174
1185264	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	79.353.165.175
1185270	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	183.146.229.138
1185271	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	155.149.150.139
1185272	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	121.94.49.124
1185274	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	81.202.182.76
1185275	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	86.151.179.121
1185276	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	112.214.717.24
1185277	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	161.15.250.185
1185278	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	94.12.36.4
1185290	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	115.176.178.143
1185290	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	165.221.227.239
1185291	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	210.175.85.118
1185282	18Oct2005	8:03:15	utpfw2	TCP	microsoft-ds	187.213.92.84

Figure 37 Virus report on the server

4.8.3 Distributed Denial of Service

The Internet Service Provider, Jaring have received a report about DDos attack generated from the users in UTP. A denial-of-service attack (also, DoS attack) is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

The other kinds of DoS rely primarily on brute force, flooding the target with an overwhelming flux of packets, oversaturating its connection bandwidth or depleting the target's system resources. Bandwidth-saturating floods rely on the attacker having higher bandwidth available than the victim; a common way of achieving this today is via Distributed Denial of Service (DDos). Other floods may use specific packet types or connection requests to saturate finite resources by, for example, occupying the maximum number of open connections or filling the victim's disk space with logs.

Report from Jaring:

DDoS Attack -SO/803747

Dear Sir,

We received below report. From our further investigations, the IP involved was one of the IPs under your organisation.

```
20050926 17:10:47      202.185.22.22 http://www.national-
anime.com/images/layout/layout_02.jpg
DIRECT/72.20.33.213 CLIENT_CLOSE/703795.22
20050926 17:13:56      202.185.22.22 http://www.national-
anime.com/images/layout/layout_02.jpg
DIRECT/72.20.33.213 SERVER_CLOSE/703790.54
20050926 17:16:59      202.185.22.22 http://www.national-
anime.com/images/layout/layout_02.jpg
DIRECT/72.20.33.213 SERVER_CLOSE/703790.54
20050926 17:25:18      202.185.22.22
```

Figure 38 Report lodged by ISP to the ITMS Department

4.8.4 Proxy Server Abuse

Since the inter-village ban introduced, the Internet proxy servers have been abused by users to transfer files between different village and it caused the Internet speed to be reduced due to wasted resources. Below is the report on most of the host that were highly engaged to the proxy servers.

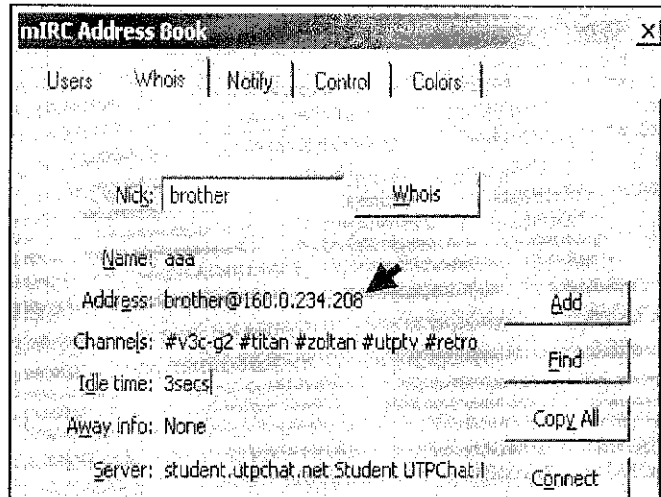


Figure 39 Proxy servers acting as mIRC proxy

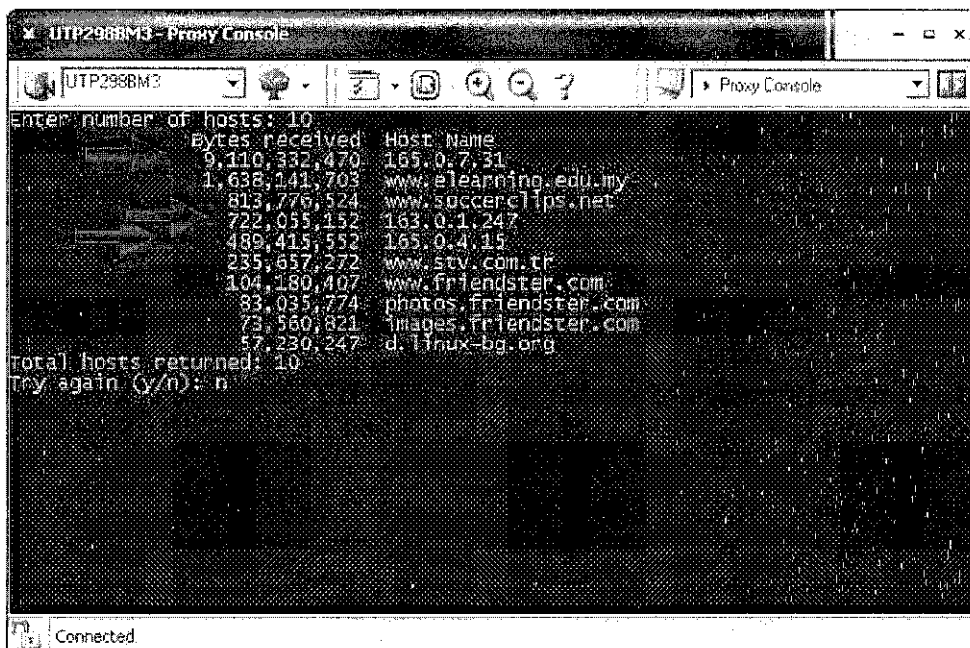


Figure 40 Top File Hosting IP reported by ITMS Department

The internal IP that did exploit the proxy servers was generated from Village 3 and Village 5 users. This explains the reasons why currently these two residential areas experienced restriction on the sizes of file transfer (less than 2Mb), packet drops for several protocols, and extreme filtering on websites browsed.

4.9 Network Improvement

4.9.1 Internet Bandwidth

In 2005, the Internet bandwidth provided was 2Mbps for the Academic building and 2Mbps for Residential area. During the time, the internet speed accessed by the students, especially in residential area was slow and many complaints have been lodged. Starting from 17th February 2006, the Internet bandwidth has been upgraded to 8Mbps for each Academic building and Residential area.

This improvement released the bottleneck in resources, thus increasing the network performance and users satisfaction. Below is the graph that will show the traffic pattern before the upgrading. It can be observed that the traffic level was constantly on the highest level with 100% usage due to downloading activities. The traffic pattern after server upgrading can be observed in Figure 36.

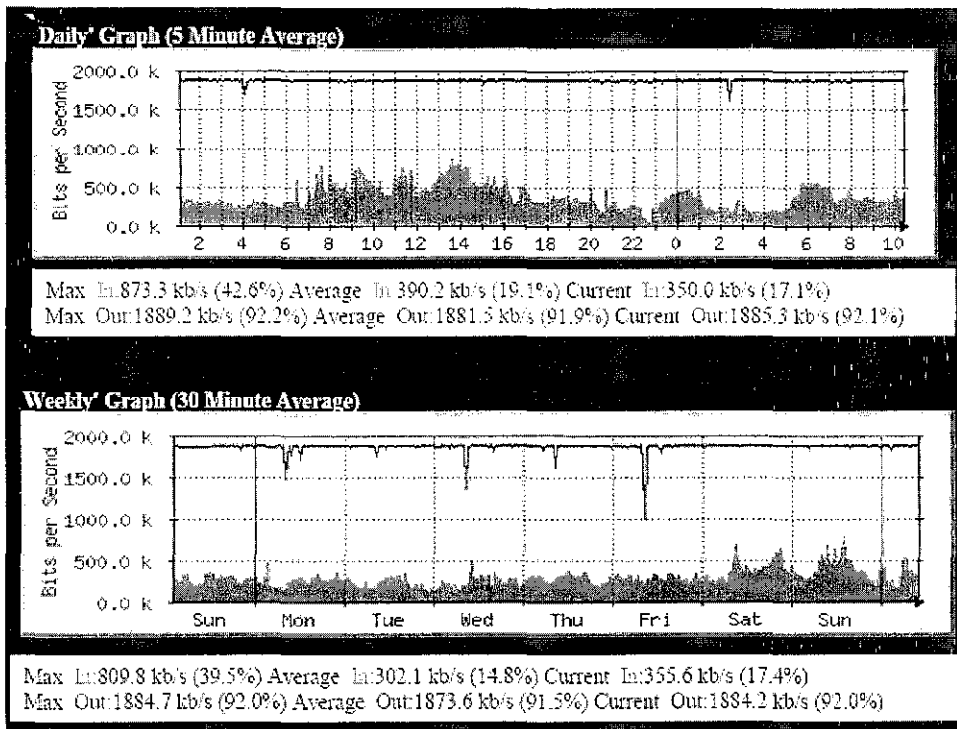


Figure 41 Traffic pattern before upgrading

4.9.2 UTP Student Webmail

This long awaited service has actually been formally introduced by the ITMS department starting from 20th April 2006. This email is accessible via LAN and Internet 24 hours per day, from anywhere the users are. The email capacity is 50Mb and the features provided is on par with other Email service provided elsewhere.

Information on Email ID :

Example :

Student Name : Soraya Hani Zainalabidin

Email address : soraya_hani@utp.edu.my

To login to web mail, this URL can be used: <http://mail.utp.edu.my>



UTP Webmail

Email Login

Username:

Password:

[Get your email ID](#)

Figure 8: UTP Webmail screenshot

CHAPTER 5

CONCLUSIONS & RECOMMENDATIONS

5.1 Conclusions

This project has completed without much hassle and all of its objectives have been fulfilled. From the author observation, the number of users does contribute to the type and numbers of issues come about in the networks. As the years goes by, the user's need keep changing and to remain up-to-date in this industry, a drive to keep improving and learning is very important. As a conclusion, satisfaction level will increase and network abuse will decrease if only the quality of service provided improved.

5.2 Recommendations

In order to cope with the ever-changing technology, UTP network must improve its efficiency. The current network utilization has advanced dramatically compared with the initial network utilization during the previous three or four years. Since the technology advancement is something that cannot be avoided or restricted, the network provider must also cope with the users demand and consumption.

Guidance and support from the management are more welcomed by the students rather than the rigid actions imposed on the students to reduce their network consumption. Thus, the creativity and effectiveness of the students to utilize the provided computer network restrained without chances to evolve.

5.2.1 *Future Plans*

In order to cope with the ever-changing technology, UTP network must improve its QoS, by improving the service provided to the users, thus optimised the networking facilities efficiently.

5.2.1.1 *Quality of Service*

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, and IP-routed networks that may use any or all of these underlying technologies. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail. QoS technologies provide the elemental building blocks that will be used for future business applications in campus, WAN and service provider networks.

5.2.1.2 *Establish UTP Computer Emergency Response Team (UCert)*

The idea for the foundation of UTP Computer Emergency Response Team (UCert) is developed based on the Malaysia's own MyCert (Malaysia Computer Emergency Response Team). Malaysian Computer Emergency Response Team (MyCERT) was formed on January 13, 1997 and started its operation fully on March 01, 1997. Operating from the Mimos Berhad office at the Bukit Jalil, Technology Park Malaysia, MyCERT provide a point of reference for the Internet community here to deal with computer security incidents and methods of prevention. MyCERT also works closely with the CERT Coordinating Centre, AUSCERT, besides other CERTs and the Malaysian Police, in dealing with security incident reports that we may receive [8].

For the UCert, the mission for the team is to address the concern of UTP's own Local Area Network. UTP's network will keep expanding as years come; therefore a special team to attend the network is highly recommended. The member of the team can be a combination of UTP's IT advisor and students. If the administration observed, UTP have quite a number of students that are talented and very interested in computer networking. Instead of letting them continue to abuse the network with their expertise, it is better to employ their knowledge in maintaining the security of the network. The collaboration of students and ITMS Department can provide a chance for those talented students to enhance their gift legally.

Functions

- UCert provides a point of reference of expertise on network and security matters
- UCert centralizes reporting of security incidents and facilitates communication to resolve security incidents
- UCert disseminates security information including system vulnerabilities, defence strategies and mechanism
- UCert acts as a repository of security related information, acquiring patches, tools and technique
- UCert also plays an educational role in educating the public with regard to computer security in University Teknologi Petronas.

REFERENCES

- [1] A. Forouzan, Behrouz, *TCP/IP Protocol Suite*, New York, McGraw-Hill Companies, 2006
- [2] L. Peterson, Larry & S. Davie, Bruce, *Computer Networks*, San Francisco, Morgan Kaufmann Publisher, 2003
- [3] Bates, R. J. & Kimmel, Zeecil, *Nortel Networks Layer 3 Switching*, New York, McGraw-Hill Companies, 2001
- [4] Stallings, William, *Data and Computer Communication*, New Jersey, Prentice Hall, 2004
- [5] Regan, Patrick, *Local Area Network* New Jersey, Prentice Hall, 2004
- [6] Agilent Advisor LAN Analysis Training Module
- [7] <http://en.wikipedia.org/wiki/Akamai>
- [8] <http://www.mycert.org.my/>
- [9] <http://www.nortel.com>

APPENDICES

APPENDIX A

RFC 1180

Network Working Group
Request for Comments: 1180

T. Socolofsky
C. Kale
Spider Systems Limited
January 1991

A TCP/IP Tutorial

Status of this Memo

This RFC is a tutorial on the TCP/IP protocol suite, focusing particularly on the steps in forwarding an IP datagram from source host to destination host through a router. It does not specify an Internet standard. Distribution of this memo is unlimited.

Table of Contents

1. Introduction.....	1
2. TCP/IP Overview.....	2
3. Ethernet.....	8
4. ARP.....	9
5. Internet Protocol.....	12
6. User Datagram Protocol.....	22
7. Transmission Control Protocol.....	24
8. Network Applications.....	25
9. Other Information.....	27
10. References.....	27
11. Relation to other RFCs.....	27
12. Security Considerations.....	27
13. Authors' Addresses.....	28

1. Introduction

This tutorial contains only one view of the salient points of TCP/IP, and therefore it is the "bare bones" of TCP/IP technology. It omits the history of development and funding, the business case for its use, and its future as compared to ISO OSI. Indeed, a great deal of technical information is also omitted. What remains is a minimum of information that must be understood by the professional working in a TCP/IP environment. These professionals include the systems administrator, the systems programmer, and the network manager.

This tutorial uses examples from the UNIX TCP/IP environment, however the main points apply across all implementations of TCP/IP.

Note that the purpose of this memo is explanation, not definition. If any question arises about the correct specification of a protocol, please refer to the actual standards defining RFC.

The next section is an overview of TCP/IP, followed by detailed descriptions of individual components.

2. TCP/IP Overview

The generic term "TCP/IP" usually means anything and everything related to the specific protocols of TCP and IP. It can include other protocols, applications, and even the network medium. A sample of these protocols are: UDP, ARP, and ICMP. A sample of these applications are: TELNET, FTP, and rcp. A more accurate term is "internet technology". A network that uses internet technology is called an "internet".

2.1 Basic Structure

To understand this technology you must first understand the following logical structure:

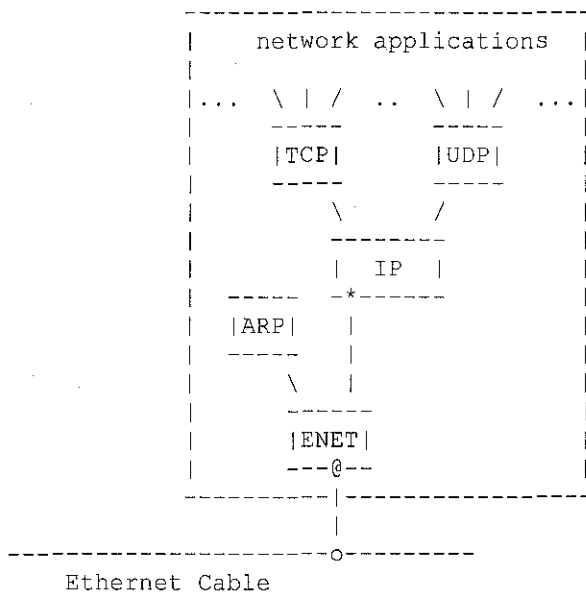


Figure 1. Basic TCP/IP Network Node

This is the logical structure of the layered protocols inside a computer on an internet. Each computer that can communicate using internet technology has such a logical structure. It is this logical structure that determines the behavior of the computer on the internet. The boxes represent processing of the data as it passes through the computer, and the lines connecting boxes show the path of

data. The horizontal line at the bottom represents the Ethernet cable; the "o" is the transceiver. The "*" is the IP address and the "@" is the Ethernet address. Understanding this logical structure is essential to understanding internet technology; it is referred to throughout this tutorial.

2.2 Terminology

The name of a unit of data that flows through an internet is dependent upon where it exists in the protocol stack. In summary: if it is on an Ethernet it is called an Ethernet frame; if it is between the Ethernet driver and the IP module it is called a IP packet; if it is between the IP module and the UDP module it is called a UDP datagram; if it is between the IP module and the TCP module it is called a TCP segment (more generally, a transport message); and if it is in a network application it is called a application message.

These definitions are imperfect. Actual definitions vary from one publication to the next. More specific definitions can be found in RFC 1122, section 1.3.3.

A driver is software that communicates directly with the network interface hardware. A module is software that communicates with a driver, with network applications, or with another module.

The terms driver, module, Ethernet frame, IP packet, UDP datagram, TCP message, and application message are used where appropriate throughout this tutorial.

2.3 Flow of Data

Let's follow the data as it flows down through the protocol stack shown in Figure 1. For an application that uses TCP (Transmission Control Protocol), data passes between the application and the TCP module. For applications that use UDP (User Datagram Protocol), data passes between the application and the UDP module. FTP (File Transfer Protocol) is a typical application that uses TCP. Its protocol stack in this example is FTP/TCP/IP/ENET. SNMP (Simple Network Management Protocol) is an application that uses UDP. Its protocol stack in this example is SNMP/UDP/IP/ENET.

The TCP module, UDP module, and the Ethernet driver are n-to-1 multiplexers. As multiplexers they switch many inputs to one output. They are also 1-to-n de-multiplexers. As de-multiplexers they switch one input to many outputs according to the type field in the protocol header.

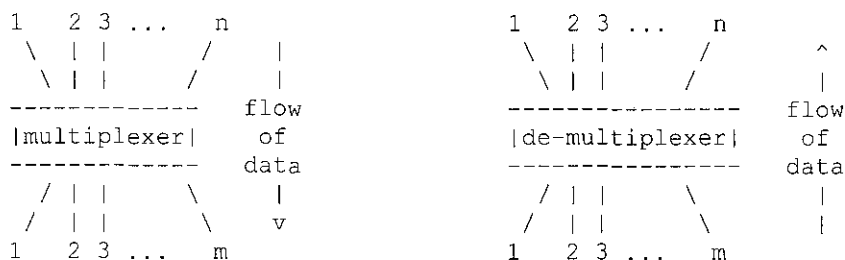


Figure 4. n-to-m multiplexer and m-to-n de-multiplexer

It performs this multiplexing in either direction to accommodate incoming and outgoing data. An IP module with more than 1 network interface is more complex than our original example in that it can forward data onto the next network. Data can arrive on any network interface and be sent out on any other.

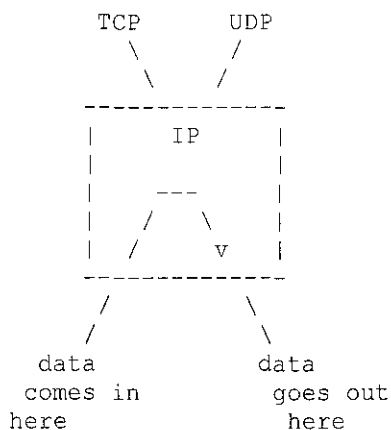


Figure 5. Example of IP Forwarding a IP Packet

The process of sending an IP packet out onto another network is called "forwarding" an IP packet. A computer that has been dedicated to the task of forwarding IP packets is called an "IP-router".

As you can see from the figure, the forwarded IP packet never touches the TCP and UDP modules on the IP-router. Some IP-router implementations do not have a TCP or UDP module.

2.5 IP Creates a Single Logical Network

The IP module is central to the success of internet technology. Each module or driver adds its header to the message as the message passes

down through the protocol stack. Each module or driver strips the corresponding header from the message as the message climbs the protocol stack up towards the application. The IP header contains the IP address, which builds a single logical network from multiple physical networks. This interconnection of physical networks is the source of the name: internet. A set of interconnected physical networks that limit the range of an IP packet is called an "internet".

2.6 Physical Network Independence

IP hides the underlying network hardware from the network applications. If you invent a new physical network, you can put it into service by implementing a new driver that connects to the internet underneath IP. Thus, the network applications remain intact and are not vulnerable to changes in hardware technology.

2.7 Interoperability

If two computers on an internet can communicate, they are said to "interoperate"; if an implementation of internet technology is good, it is said to have "interoperability". Users of general-purpose computers benefit from the installation of an internet because of the interoperability in computers on the market. Generally, when you buy a computer, it will interoperate. If the computer does not have interoperability, and interoperability can not be added, it occupies a rare and special niche in the market.

2.8 After the Overview

With the background set, we will answer the following questions:

When sending out an IP packet, how is the destination Ethernet address determined?

How does IP know which of multiple lower network interfaces to use when sending out an IP packet?

How does a client on one computer reach the server on another?

Why do both TCP and UDP exist, instead of just one or the other?

What network applications are available?

These will be explained, in turn, after an Ethernet refresher.

3. Ethernet

This section is a short review of Ethernet technology.

An Ethernet frame contains the destination address, source address, type field, and data.

An Ethernet address is 6 bytes. Every device has its own Ethernet address and listens for Ethernet frames with that destination address. All devices also listen for Ethernet frames with a wild-card destination address of "FF-FF-FF-FF-FF-FF" (in hexadecimal), called a "broadcast" address.

Ethernet uses CSMA/CD (Carrier Sense and Multiple Access with Collision Detection). CSMA/CD means that all devices communicate on a single medium, that only one can transmit at a time, and that they can all receive simultaneously. If 2 devices try to transmit at the same instant, the transmit collision is detected, and both devices wait a random (but short) period before trying to transmit again.

3.1 A Human Analogy

A good analogy of Ethernet technology is a group of people talking in a small, completely dark room. In this analogy, the physical network medium is sound waves on air in the room instead of electrical signals on a coaxial cable.

Each person can hear the words when another is talking (Carrier Sense). Everyone in the room has equal capability to talk (Multiple Access), but none of them give lengthy speeches because they are polite. If a person is impolite, he is asked to leave the room (i.e., thrown off the net).

No one talks while another is speaking. But if two people start speaking at the same instant, each of them know this because each hears something they haven't said (Collision Detection). When these two people notice this condition, they wait for a moment, then one begins talking. The other hears the talking and waits for the first to finish before beginning his own speech.

Each person has an unique name (unique Ethernet address) to avoid confusion. Every time one of them talks, he prefaces the message with the name of the person he is talking to and with his own name (Ethernet destination and source address, respectively), i.e., "Hello Jane, this is Jack, ..blah blah blah...". If the sender wants to talk to everyone he might say "everyone" (broadcast address), i.e., "Hello Everyone, this is Jack, ..blah blah blah...".

1. ARP

When sending out an IP packet, how is the destination Ethernet address determined?

ARP (Address Resolution Protocol) is used to translate IP addresses to Ethernet addresses. The translation is done only for outgoing IP packets, because this is when the IP header and the Ethernet header are created.

1.1 ARP Table for Address Translation

The translation is performed with a table look-up. The table, called the ARP table, is stored in memory and contains a row for each computer. There is a column for IP address and a column for Ethernet address. When translating an IP address to an Ethernet address, the table is searched for a matching IP address. The following is a simplified ARP table:

IP address	Ethernet address
223.1.2.1	08-00-39-00-2F-C3
223.1.2.3	08-00-5A-21-A7-22
223.1.2.4	08-00-10-99-AC-54

TABLE 1. Example ARP Table

The human convention when writing out the 4-byte IP address is each byte in decimal and separating bytes with a period. When writing out the 6-byte Ethernet address, the conventions are each byte in hexadecimal and separating bytes with either a minus sign or a colon.

The ARP table is necessary because the IP address and Ethernet address are selected independently; you can not use an algorithm to translate IP address to Ethernet address. The IP address is selected by the network manager based on the location of the computer on the internet. When the computer is moved to a different part of an internet, its IP address must be changed. The Ethernet address is selected by the manufacturer based on the Ethernet address space licensed by the manufacturer. When the Ethernet hardware interface board changes, the Ethernet address changes.

4.2 Typical Translation Scenario

During normal operation a network application, such as TELNET, sends an application message to TCP, then TCP sends the corresponding TCP message to the IP module. The destination IP address is known by the

application, the TCP module, and the IP module. At this point the IP packet has been constructed and is ready to be given to the Ethernet driver, but first the destination Ethernet address must be determined.

The ARP table is used to look-up the destination Ethernet address.

4.3 ARP Request/Response Pair

But how does the ARP table get filled in the first place? The answer is that it is filled automatically by ARP on an "as-needed" basis.

Two things happen when the ARP table can not be used to translate an address:

1. An ARP request packet with a broadcast Ethernet address is sent out on the network to every computer.
2. The outgoing IP packet is queued.

Every computer's Ethernet interface receives the broadcast Ethernet frame. Each Ethernet driver examines the Type field in the Ethernet frame and passes the ARP packet to the ARP module. The ARP request packet says "If your IP address matches this target IP address, then please tell me your Ethernet address". An ARP request packet looks something like this:

```

-----
|Sender IP Address   223.1.2.1       |
|Sender Enet Address 08-00-39-00-2F-C3|
-----
|Target IP Address   223.1.2.2       |
|Target Enet Address <blank>         |
-----

```

TABLE 2. Example ARP Request

Each ARP module examines the IP address and if the Target IP address matches its own IP address, it sends a response directly to the source Ethernet address. The ARP response packet says "Yes, that target IP address is mine, let me give you my Ethernet address". An ARP response packet has the sender/target field contents swapped as compared to the request. It looks something like this:

```

-----
|Sender IP Address   223.1.2.2   |
|Sender Enet Address 08-00-28-00-38-A9|
-----
|Target IP Address   223.1.2.1   |
|Target Enet Address 08-00-39-00-2F-C3|
-----

```

TABLE 3. Example ARP Response

The response is received by the original sender computer. The Ethernet driver looks at the Type field in the Ethernet frame then passes the ARP packet to the ARP module. The ARP module examines the ARP packet and adds the sender's IP and Ethernet addresses to its ARP table.

The updated table now looks like this:

```

-----
|IP address          Ethernet address |
-----
|223.1.2.1          08-00-39-00-2F-C3|
|223.1.2.2          08-00-28-00-38-A9|
|223.1.2.3          08-00-5A-21-A7-22|
|223.1.2.4          08-00-10-99-AC-54|
-----

```

TABLE 4. ARP Table after Response

1.4 Scenario Continued

The new translation has now been installed automatically in the table, just milli-seconds after it was needed. As you remember from step 2 above, the outgoing IP packet was queued. Next, the IP address to Ethernet address translation is performed by look-up in the ARP table then the Ethernet frame is transmitted on the Ethernet. Therefore, with the new steps 3, 4, and 5, the scenario for the sender computer is:

1. An ARP request packet with a broadcast Ethernet address is sent out on the network to every computer.
2. The outgoing IP packet is queued.
3. The ARP response arrives with the IP-to-Ethernet address translation for the ARP table.

4. For the queued IP packet, the ARP table is used to translate the IP address to the Ethernet address.

5. The Ethernet frame is transmitted on the Ethernet.

In summary, when the translation is missing from the ARP table, one IP packet is queued. The translation data is quickly filled in with ARP request/response and the queued IP packet is transmitted.

Each computer has a separate ARP table for each of its Ethernet interfaces. If the target computer does not exist, there will be no ARP response and no entry in the ARP table. IP will discard outgoing IP packets sent to that address. The upper layer protocols can't tell the difference between a broken Ethernet and the absence of a computer with the target IP address.

Some implementations of IP and ARP don't queue the IP packet while waiting for the ARP response. Instead the IP packet is discarded and the recovery from the IP packet loss is left to the TCP module or the UDP network application. This recovery is performed by time-out and retransmission. The retransmitted message is successfully sent out onto the network because the first copy of the message has already caused the ARP table to be filled.

5. Internet Protocol

The IP module is central to internet technology and the essence of IP is its route table. IP uses this in-memory table to make all decisions about routing an IP packet. The content of the route table is defined by the network administrator. Mistakes block communication.

To understand how a route table is used is to understand internetworking. This understanding is necessary for the successful administration and maintenance of an IP network.

The route table is best understood by first having an overview of routing, then learning about IP network addresses, and then looking at the details.

5.1 Direct Routing

The figure below is of a tiny internet with 3 computers: A, B, and C. Each computer has the same TCP/IP protocol stack as in Figure 1. Each computer's Ethernet interface has its own Ethernet address. Each computer has an IP address assigned to the IP interface by the network manager, who also has assigned an IP network number to the Ethernet.

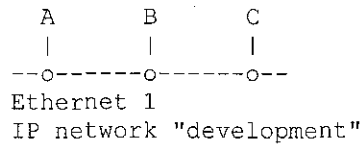


Figure 6. One IP Network

When A sends an IP packet to B, the IP header contains A's IP address as the source IP address, and the Ethernet header contains A's Ethernet address as the source Ethernet address. Also, the IP header contains B's IP address as the destination IP address and the Ethernet header contains B's Ethernet address as the destination Ethernet address.

address	source	destination
IP header	A	B
Ethernet header	A	B

TABLE 5. Addresses in an Ethernet frame for an IP packet from A to B

For this simple case, IP is overhead because the IP adds little to the service offered by Ethernet. However, IP does add cost: the extra CPU processing and network bandwidth to generate, transmit, and parse the IP header.

When B's IP module receives the IP packet from A, it checks the destination IP address against its own, looking for a match, then it passes the datagram to the upper-level protocol.

This communication between A and B uses direct routing.

5.2 Indirect Routing

The figure below is a more realistic view of an internet. It is composed of 3 Ethernets and 3 IP networks connected by an IP-router called computer D. Each IP network has 4 computers; each computer has its own IP address and Ethernet address.

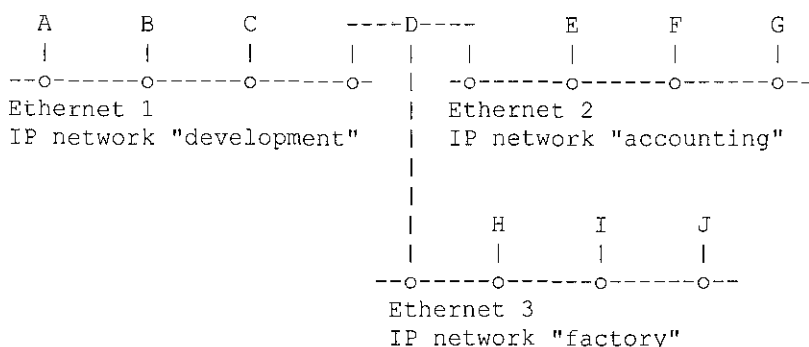


Figure 7. Three IP Networks; One internet

Except for computer D, each computer has a TCP/IP protocol stack like that in Figure 1. Computer D is the IP-router; it is connected to all 3 networks and therefore has 3 IP addresses and 3 Ethernet addresses. Computer D has a TCP/IP protocol stack similar to that in Figure 3, except that it has 3 ARP modules and 3 Ethernet drivers instead of 2. Please note that computer D has only one IP module.

The network manager has assigned a unique number, called an IP network number, to each of the Ethernets. The IP network numbers are not shown in this diagram, just the network names.

When computer A sends an IP packet to computer B, the process is identical to the single network example above. Any communication between computers located on a single IP network matches the direct routing example discussed previously.

When computer D and A communicate, it is direct communication. When computer D and E communicate, it is direct communication. When computer D and H communicate, it is direct communication. This is because each of these pairs of computers is on the same IP network.

However, when computer A communicates with a computer on the far side of the IP-router, communication is no longer direct. A must use D to forward the IP packet to the next IP network. This communication is called "indirect".

This routing of IP packets is done by IP modules and happens transparently to TCP, UDP, and the network applications.

If A sends an IP packet to E, the source IP address and the source Ethernet address are A's. The destination IP address is E's, but because A's IP module sends the IP packet to D for forwarding, the destination Ethernet address is D's.

address	source	destination
IP header	A	E
Ethernet header	A	D

TABLE 6. Addresses in an Ethernet frame for an IP packet from A to E (before D)

D's IP module receives the IP packet and upon examining the destination IP address, says "This is not my IP address," and sends the IP packet directly to E.

address	source	destination
IP header	A	E
Ethernet header	D	E

TABLE 7. Addresses in an Ethernet frame for an IP packet from A to E (after D)

In summary, for direct communication, both the source IP address and the source Ethernet address is the sender's, and the destination IP address and the destination Ethernet address is the recipient's. For indirect communication, the IP address and Ethernet addresses do not pair up in this way.

This example internet is a very simple one. Real networks are often complicated by many factors, resulting in multiple IP-routers and several types of physical networks. This example internet might have come about because the network manager wanted to split a large Ethernet in order to localize Ethernet broadcast traffic.

3.3 IP Module Routing Rules

This overview of routing has shown what happens, but not how it happens. Now let's examine the rules, or algorithm, used by the IP module.

For an outgoing IP packet, entering IP from an upper layer, IP must decide whether to send the IP packet directly or indirectly, and IP must choose a lower network interface. These choices are made by consulting the route table.

For an incoming IP packet, entering IP from a lower interface, IP must decide whether to forward the IP packet or pass it to an upper layer. If the IP packet is being forwarded, it is treated as an

outgoing IP packet.

When an incoming IP packet arrives it is never forwarded back out through the same network interface.

These decisions are made before the IP packet is handed to the lower interface and before the ARP table is consulted.

5.4 IP Address

The network manager assigns IP addresses to computers according to the IP network to which the computer is attached. One part of a 4-byte IP address is the IP network number, the other part is the IP computer number (or host number). For the computer in table 1, with an IP address of 223.1.2.1, the network number is 223.1.2 and the host number is number 1.

The portion of the address that is used for network number and for host number is defined by the upper bits in the 4-byte address. All example IP addresses in this tutorial are of type class C, meaning that the upper 3 bits indicate that 21 bits are the network number and 8 bits are the host number. This allows 2,097,152 class C networks up to 254 hosts on each network.

The IP address space is administered by the NIC (Network Information Center). All internets that are connected to the single world-wide Internet must use network numbers assigned by the NIC. If you are setting up your own internet and you are not intending to connect it to the Internet, you should still obtain your network numbers from the NIC. If you pick your own number, you run the risk of confusion and chaos in the eventuality that your internet is connected to another internet.

5.5 Names

People refer to computers by names, not numbers. A computer called alpha might have the IP address of 223.1.2.1. For small networks, this name-to-address translation data is often kept on each computer in the "hosts" file. For larger networks, this translation data file is stored on a server and accessed across the network when needed. A few lines from that file might look like this:

```
223.1.2.1    alpha
223.1.2.2    beta
223.1.2.3    gamma
223.1.2.4    delta
223.1.3.2    epsilon
223.1.4.2    iota
```

The IP address is the first column and the computer name is the second column.

In most cases, you can install identical "hosts" files on all computers. You may notice that "delta" has only one entry in this file even though it has 3 IP addresses. Delta can be reached with any of its IP addresses; it does not matter which one is used. When delta receives an IP packet and looks at the destination address, it will recognize any of its own IP addresses.

IP networks are also given names. If you have 3 IP networks, your "networks" file for documenting these names might look something like this:

```
223.1.2    development
223.1.3    accounting
223.1.4    factory
```

The IP network number is in the first column and its name is in the second column.

From this example you can see that alpha is computer number 1 on the development network, beta is computer number 2 on the development network and so on. You might also say that alpha is development.1, Beta is development.2, and so on.

The above hosts file is adequate for the users, but the network manager will probably replace the line for delta with:

```
223.1.2.4    devnetrouter    delta
223.1.3.1    facnetrouter
223.1.4.1    accnetrouter
```

These three new lines for the hosts file give each of delta's IP addresses a meaningful name. In fact, the first IP address listed has 2 names; "delta" and "devnetrouter" are synonyms. In practice "delta" is the general-purpose name of the computer and the other 3 names are only used when administering the IP route table.

These files are used by network administration commands and network applications to provide meaningful names. They are not required for operation of an internet, but they do make it easier for us.

5.6 IP Route Table

How does IP know which lower network interface to use when sending out a IP packet? IP looks it up in the route table using a search key of the IP network number extracted from the IP destination

address.

The route table contains one row for each route. The primary columns in the route table are: IP network number, direct/indirect flag, router IP address, and interface number. This table is referred to by IP for each outgoing IP packet.

On most computers the route table can be modified with the "route" command. The content of the route table is defined by the network manager, because the network manager assigns the IP addresses to the computers.

5.7 Direct Routing Details

To explain how it is used, let us visit in detail the routing situations we have reviewed previously.

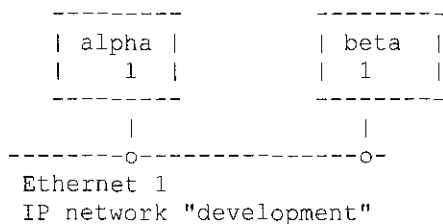


Figure 8. Close-up View of One IP Network

The route table inside alpha looks like this:

network	direct/indirect	flag	router	interface	number
development	direct		<blank>	1	

TABLE 8. Example Simple Route Table

This view can be seen on some UNIX systems with the "netstat -r" command. With this simple network, all computers have identical routing tables.

For discussion, the table is printed again without the network number translated to its network name.

network	direct/indirect	flag	router	interface	number
223.1.2	direct		<blank>	1	

TABLE 9. Example Simple Route Table with Numbers

5.8 Direct Scenario

Alpha is sending an IP packet to beta. The IP packet is in alpha's IP module and the destination IP address is beta or 223.1.2.2. IP extracts the network portion of this IP address and scans the first column of the table looking for a match. With this network a match is found on the first entry.

The other information in this entry indicates that computers on this network can be reached directly through interface number 1. An ARP table translation is done on beta's IP address then the Ethernet frame is sent directly to beta via interface number 1.

If an application tries to send data to an IP address that is not on the development network, IP will be unable to find a match in the route table. IP then discards the IP packet. Some computers provide a "Network not reachable" error message.

5.9 Indirect Routing Details

Now, let's take a closer look at the more complicated routing scenario that we examined previously.

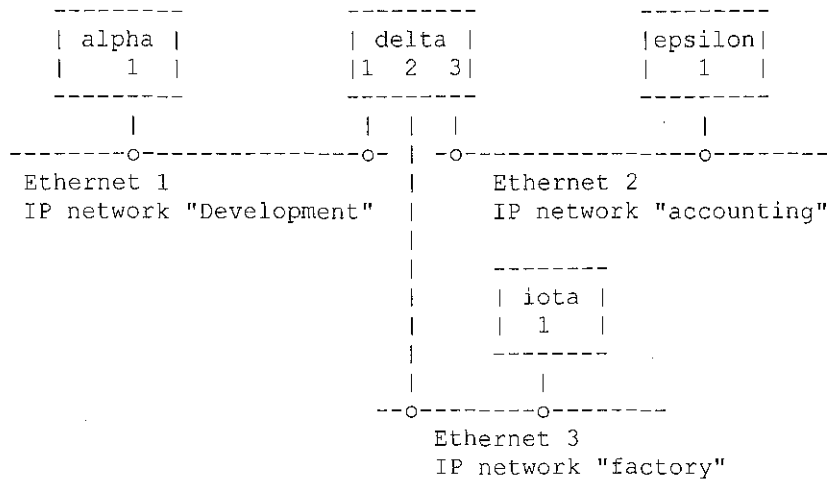


Figure 9. Close-up View of Three IP Networks

The route table inside alpha looks like this:

network	direct/indirect	flag	router	interface number
development	direct		<blank>	1
accounting	indirect		devnetrouter	1
factory	indirect		devnetrouter	1

TABLE 10. Alpha Route Table

For discussion the table is printed again using numbers instead of names.

network	direct/indirect	flag	router	interface number
223.1.2	direct		<blank>	1
223.1.3	indirect		223.1.2.4	1
223.1.4	indirect		223.1.2.4	1

TABLE 11. Alpha Route Table with Numbers

The router in Alpha's route table is the IP address of delta's connection to the development network.

5.10 Indirect Scenario

Alpha is sending an IP packet to epsilon. The IP packet is in alpha's IP module and the destination IP address is epsilon (223.1.3.2). IP extracts the network portion of this IP address (223.1.3) and scans the first column of the table looking for a match. A match is found on the second entry.

This entry indicates that computers on the 223.1.3 network can be reached through the IP-router devnetrouter. Alpha's IP module then does an ARP table translation for devnetrouter's IP address and sends the IP packet directly to devnetrouter through Alpha's interface number 1. The IP packet still contains the destination address of epsilon.

The IP packet arrives at delta's development network interface and is passed up to delta's IP module. The destination IP address is examined and because it does not match any of delta's own IP addresses, delta decides to forward the IP packet.

Delta's IP module extracts the network portion of the destination IP address (223.1.3) and scans its route table for a matching network field. Delta's route table looks like this:

network	direct/indirect	flag	router	interface number
development	direct		<blank>	1
factory	direct		<blank>	3
accounting	direct		<blank>	2

TABLE 12. Delta's Route Table

Below is delta's table printed again, without the translation to names.

network	direct/indirect	flag	router	interface number
223.1.2	direct		<blank>	1
223.1.3	direct		<blank>	3
223.1.4	direct		<blank>	2

TABLE 13. Delta's Route Table with Numbers

The match is found on the second entry. IP then sends the IP packet directly to epsilon through interface number 3. The IP packet contains the IP destination address of epsilon and the Ethernet

destination address of epsilon.

The IP packet arrives at epsilon and is passed up to epsilon's IP module. The destination IP address is examined and found to match with epsilon's IP address, so the IP packet is passed to the upper protocol layer.

5.11 Routing Summary

When a IP packet travels through a large internet it may go through many IP-routers before it reaches its destination. The path it takes is not determined by a central source but is a result of consulting each of the routing tables used in the journey. Each computer defines only the next hop in the journey and relies on that computer to send the IP packet on its way.

5.12 Managing the Routes

Maintaining correct routing tables on all computers in a large internet is a difficult task; network configuration is being modified constantly by the network managers to meet changing needs. Mistakes in routing tables can block communication in ways that are excruciatingly tedious to diagnose.

Keeping a simple network configuration goes a long way towards making a reliable internet. For instance, the most straightforward method of assigning IP networks to Ethernet is to assign a single IP network number to each Ethernet.

Help is also available from certain protocols and network applications. ICMP (Internet Control Message Protocol) can report some routing problems. For small networks the route table is filled manually on each computer by the network administrator. For larger networks the network administrator automates this manual operation with a routing protocol to distribute routes throughout a network.

When a computer is moved from one IP network to another, its IP address must change. When a computer is removed from an IP network its old address becomes invalid. These changes require frequent updates to the "hosts" file. This flat file can become difficult to maintain for even medium-size networks. The Domain Name System helps solve these problems.

6. User Datagram Protocol

UDP is one of the two main protocols to reside on top of IP. It offers service to the user's network applications. Example network applications that use UDP are: Network File System (NFS) and Simple

Network Management Protocol (SNMP). The service is little more than an interface to IP.

UDP is a connectionless datagram delivery service that does not guarantee delivery. UDP does not maintain an end-to-end connection with the remote UDP module; it merely pushes the datagram out on the net and accepts incoming datagrams off the net.

UDP adds two values to what is provided by IP. One is the multiplexing of information between applications based on port number. The other is a checksum to check the integrity of the data.

6.1 Ports

How does a client on one computer reach the server on another?

The path of communication between an application and UDP is through UDP ports. These ports are numbered, beginning with zero. An application that is offering service (the server) waits for messages to come in on a specific port dedicated to that service. The server waits patiently for any client to request service.

For instance, the SNMP server, called an SNMP agent, always waits on port 161. There can be only one SNMP agent per computer because there is only one UDP port number 161. This port number is well known; it is a fixed number, an internet assigned number. If an SNMP client wants service, it sends its request to port number 161 of UDP on the destination computer.

When an application sends data out through UDP it arrives at the far end as a single unit. For example, if an application does 5 writes to the UDP port, the application at the far end will do 5 reads from the UDP port. Also, the size of each write matches the size of each read.

UDP preserves the message boundary defined by the application. It never joins two application messages together, or divides a single application message into parts.

5.2 Checksum

An incoming IP packet with an IP header type field indicating "UDP" is passed up to the UDP module by IP. When the UDP module receives the UDP datagram from IP it examines the UDP checksum. If the checksum is zero, it means that checksum was not calculated by the sender and can be ignored. Thus the sending computer's UDP module may or may not generate checksums. If Ethernet is the only network between the 2 UDP modules communicating, then you may not need

checksumming. However, it is recommended that checksum generation always be enabled because at some point in the future a route table change may send the data across less reliable media.

If the checksum is valid (or zero), the destination port number is examined and if an application is bound to that port, an application message is queued for the application to read. Otherwise the UDP datagram is discarded. If the incoming UDP datagrams arrive faster than the application can read them and if the queue fills to a maximum value, UDP datagrams are discarded by UDP. UDP will continue to discard UDP datagrams until there is space in the queue.

7. Transmission Control Protocol

TCP provides a different service than UDP. TCP offers a connection-oriented byte stream, instead of a connectionless datagram delivery service. TCP guarantees delivery, whereas UDP does not.

TCP is used by network applications that require guaranteed delivery and cannot be bothered with doing time-outs and retransmissions. The two most typical network applications that use TCP are File Transfer Protocol (FTP) and the TELNET. Other popular TCP network applications include X-Window System, rcp (remote copy), and the r-series commands. TCP's greater capability is not without cost: it requires more CPU and network bandwidth. The internals of the TCP module are much more complicated than those in a UDP module.

Similar to UDP, network applications connect to TCP ports. Well-defined port numbers are dedicated to specific applications. For instance, the TELNET server uses port number 23. The TELNET client can find the server simply by connecting to port 23 of TCP on the specified computer.

When the application first starts using TCP, the TCP module on the client's computer and the TCP module on the server's computer start communicating with each other. These two end-point TCP modules contain state information that defines a virtual circuit. This virtual circuit consumes resources in both TCP end-points. The virtual circuit is full duplex; data can go in both directions simultaneously. The application writes data to the TCP port, the data traverses the network and is read by the application at the far end.

TCP packetizes the byte stream at will; it does not retain the boundaries between writes. For example, if an application does 5 writes to the TCP port, the application at the far end might do 10 reads to get all the data. Or it might get all the data with a single read. There is no correlation between the number and size of

writes at one end to the number and size of reads at the other end.

TCP is a sliding window protocol with time-out and retransmits. Outgoing data must be acknowledged by the far-end TCP. Acknowledgements can be piggybacked on data. Both receiving ends can flow control the far end, thus preventing a buffer overrun.

As with all sliding window protocols, the protocol has a window size. The window size determines the amount of data that can be transmitted before an acknowledgement is required. For TCP, this amount is not a number of TCP segments but a number of bytes.

8. Network Applications

Why do both TCP and UDP exist, instead of just one or the other?

They supply different services. Most applications are implemented to use only one or the other. You, the programmer, choose the protocol that best meets your needs. If you need a reliable stream delivery service, TCP might be best. If you need a datagram service, UDP might be best. If you need efficiency over long-haul circuits, TCP might be best. If you need efficiency over fast networks with short latency, UDP might be best. If your needs do not fall nicely into these categories, then the "best" choice is unclear. However, applications can make up for deficiencies in the choice. For instance if you choose UDP and you need reliability, then the application must provide reliability. If you choose TCP and you need a record oriented service, then the application must insert markers in the byte stream to delimit records.

What network applications are available?

There are far too many to list. The number is growing continually. Some of the applications have existed since the beginning of internet technology: TELNET and FTP. Others are relatively new: X-Windows and SNMP. The following is a brief description of the applications mentioned in this tutorial.

8.1 TELNET

TELNET provides a remote login capability on TCP. The operation and appearance is similar to keyboard dialing through a telephone switch. On the command line the user types "telnet delta" and receives a login prompt from the computer called "delta".

TELNET works well; it is an old application and has widespread interoperability. Implementations of TELNET usually work between different operating systems. For instance, a TELNET client may be on

VAX/VMS and the server on UNIX System V.

8.2 FTP

File Transfer Protocol (FTP), as old as TELNET, also uses TCP and has widespread interoperability. The operation and appearance is as if you TELNETed to the remote computer. But instead of typing your usual commands, you have to make do with a short list of commands for directory listings and the like. FTP commands allow you to copy files between computers.

8.3 rsh

Remote shell (rsh or remsh) is one of an entire family of remote UNIX style commands. The UNIX copy command, cp, becomes rcp. The UNIX "who is logged in" command, who, becomes rwho. The list continues and is referred to collectively to as the "r" series commands or the "r*" (r star) commands.

The r* commands mainly work between UNIX systems and are designed for interaction between trusted hosts. Little consideration is given to security, but they provide a convenient user environment.

To execute the "cc file.c" command on a remote computer called delta, type "rsh delta cc file.c". To copy the "file.c" file to delta, type "rcp file.c delta:". To login to delta, type "rlogin delta", and if you administered the computers in a certain way, you will not be challenged with a password prompt.

8.4 NFS

Network File System, first developed by Sun Microsystems Inc, uses UDP and is excellent for mounting UNIX file systems on multiple computers. A diskless workstation can access its server's hard disk as if the disk were local to the workstation. A single disk copy of a database on mainframe "alpha" can also be used by mainframe "beta" if the database's file system is NFS mounted on "beta".

NFS adds significant load to a network and has poor utility across slow links, but the benefits are strong. The NFS client is implemented in the kernel, allowing all applications and commands to use the NFS mounted disk as if it were local disk.

8.5 SNMP

Simple Network Management Protocol (SNMP) uses UDP and is designed for use by central network management stations. It is a well known fact that if given enough data, a network manager can detect and

diagnose network problems. The central station uses SNMP to collect this data from other computers on the network. SNMP defines the format for the data; it is left to the central station or network manager to interpret the data.

8.6 X-Window

The X Window System uses the X Window protocol on TCP to draw windows on a workstation's bitmap display. X Window is much more than a utility for drawing windows; it is entire philosophy for designing a user interface.

9. Other Information

Much information about internet technology was not included in this tutorial. This section lists information that is considered the next level of detail for the reader who wishes to learn more.

- o administration commands: arp, route, and netstat
- o ARP: permanent entry, publish entry, time-out entry, spoofing
- o IP route table: host entry, default gateway, subnets
- o IP: time-to-live counter, fragmentation, ICMP
- o RIP, routing loops
- o Domain Name System

10. References

- [1] Comer, D., "Internetworking with TCP/IP Principles, Protocols, and Architecture", Prentice Hall, Englewood Cliffs, New Jersey, U.S.A., 1988.
- [2] Feinler, E., et al, DDN Protocol Handbook, Volume 2 and 3, DDN Network Information Center, SRI International, 333 Ravenswood Avenue, Room EJ291, Menlow Park, California, U.S.A., 1985.
- [3] Spider Systems, Ltd., "Packets and Protocols", Spider Systems Ltd., Stanwell Street, Edinburgh, U.K. EH6 5NG, 1990.

11. Relation to other RFCs

This RFC is a tutorial and it does not UPDATE or OBSOLETE any other RFC.

12. Security Considerations

There are security considerations within the TCP/IP protocol suite. To some people these considerations are serious problems, to others they are not; it depends on the user requirements.

This tutorial does not discuss these issues, but if you want to learn more you should start with the topic of ARP-spoofing, then use the "Security Considerations" section of RFC 1122 to lead you to more information.

13. Authors' Addresses

Theodore John Socolofsky
Spider Systems Limited
Spider Park
Stanwell Street
Edinburgh EH6 5NG
United Kingdom

Phone:

from UK 031-554-9424
from USA 011-44-31-554-9424

Fax:

from UK 031-554-0649
from USA 011-44-31-554-0649

E-Mail: TEDS@SPIDER.CO.UK

Claudia Jeanne Kale
12 Gosford Place
Edinburgh EH6 4BJ
United Kingdom

Phone:

from UK 031-554-7432
from USA 011-44-31-554-7432

E-Mail: CLAUDIAK@SPIDER.CO.UK

APPENDIX B
PRODUCT BRIEF : PASSPORT 8600 ROUTING SWITCH



Product Brief

Passport 8600 Routing Switch

Applications that need a reliable, secure, and intelligent network include:

- IP Telephony
- Collaboration tools

Enterprise Resource Planning (ERP) and CRM

- Supply chain management
- Unified Messaging
- Call center—ACD

Delivering reliable, secure, and intelligent Ethernet connectivity for today's convergence applications

More companies are turning to technology to help boost their bottom line and increase employee productivity. Convergence provides a clear path for enabling applications to provide gains in employee productivity and decreases in reoccurring costs. By creating a unified communications network, enterprises can employ collaborative technologies to share resources within the entire organization, improve day-to-day operational processes, and more cost effectively communicate with customers, partners, and suppliers.

Converged solutions require reliable, secure, and intelligent networks. The ability of the network to handle multiple types of traffic, each with their own requirements, means performance, intelligence, and resiliency have to be built into the network:

- As more revenue-generating services are delivered over the network, resiliency becomes critical to an enterprise's success. Network uptime and availability affect the profitability of the enterprise.
- With the addition of multiple traffic types comes the need to be able to classify traffic intelligently. Understanding what traffic receives priority on the network and when becomes more important as the number of traffic types increases.
- With so much corporate information flowing across the network, including customer information, sales information, and corporate strategies, security in the network has become a priority worldwide. Security of data, access to the network, and the infrastructure are only a few of the areas being addressed today. Securing the network requires understanding how the business and network work together.

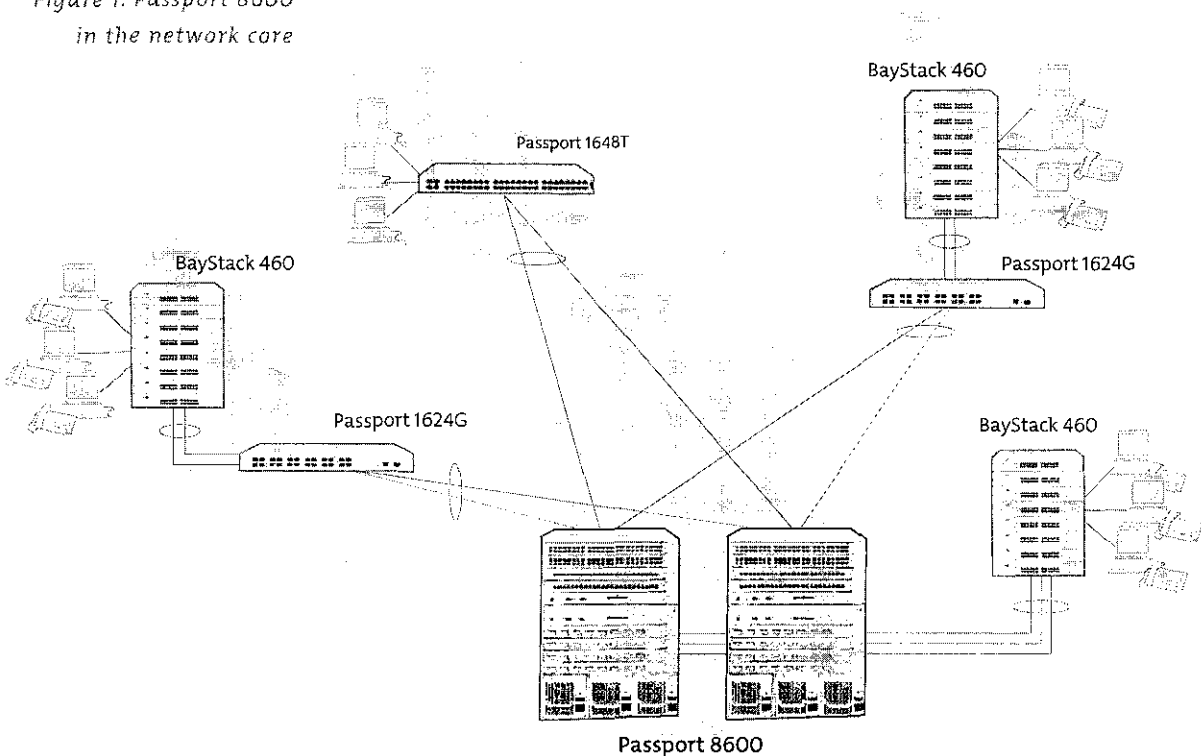
The Passport* 8600 Routing Switch delivers a proven and tested resilient, secure, and intelligent network solution. With the capability to deliver hundreds of millions of packets per second (Mpps) performance to the network core, the Passport 8600 Routing Switch combines high performance with intelligence and security. The Passport 8600 leverages technology from industry-leading products to create an integrated intelligence with the Alteon* Web Switch module, SSL Acceleration module, and the Switched Firewall module[†].

Delivering resiliency

Network resiliency is the most basic requirement when implementing a converged network. The network needs to be available to be able to support the applications whose ultimate promise is increasing the bottom line. The Passport 8600 addresses resiliency at multiple levels for maximum coverage. At the hardware level, the Passport 8600 provides hot swappable modules including fan trays and N+1 power supplies. The Passport 8600 software ensures resiliency for the network core with features like Split Multi-Link Trunking (SMLT), Routed Split Multi-Link Trunking (R-SMLT), Layer 3 redundancy, 802.3ad, and Remote Mirroring.

Connectivity within the network often relies on trunks or groups of ports connecting disparate areas of the network. The resiliency of these trunks can mean the difference between a highly available network and a network plagued with outages. Multi-Link Trunking support allows up to eight ports to be grouped into a single trunk, providing increased bandwidth and resilient connections. Split Multi-Link Trunking combines the increased bandwidth of MLT with industry-leading

Figure 1. Passport 8600 in the network core



cy. SMLT allows desktop or access switches to be dual homed/connected to Passport 8600s in the network core and have all links active. This innovative technology delivers a solution that provides increased bandwidth available from the wiring as well as sub-second failover. R-SMLT extends the reliability of SMLT to extended core networks. By providing subsecond failover for Layer 3 information, R-SMLT ensures converged applications are viable and maintainable throughout network work. The Passport 8600 also supports standard resiliency protocols like HSRP, Virtual Router Redundancy Protocol (VRRP), and Equal Cost Multi-pathing (ECMP). Both of these protocols work to ensure that users stay connected to the network and that the network provides the best bandwidth available along with the fastest convergence time.

These features, the Passport 8600 delivers increased available bandwidth, increased network availability, and resiliency designed for unified communications architecture.

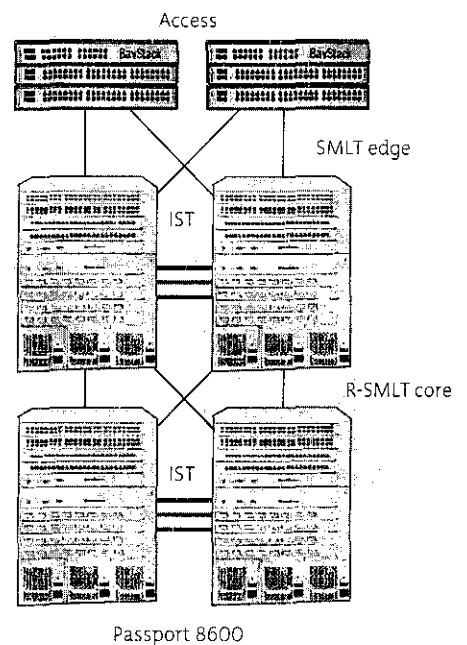
Intelligent networking

Network traffic is becoming more diverse and more prolific. Because of this trend, network devices need to be keenly aware of traffic types and be able to handle different types of traffic differently. This sense or awareness of differing traffic types combined with the ability to process each type differently is what sets intelligent networks apart from typical LANs. The Passport 8600 combines intelligence and performance to create a next-generation intelligent network solution.

In addition to built-in best-of-breed Layer 4-7 performance, the Passport 8600 is able to intelligently classify a variety of traffic types without affecting switch performance. Load balancing, SSL acceleration, and an integrated firewall allow the Passport 8600 to provide data center services for an entire network. Quality of Service (QoS) and traffic filtering ensure that bandwidth is allocated to the applications that need it the most. Filtering can also be used to provide security as well as manage bandwidth.

Speedy routing and non-blocking switch fabrics provide the performance needed for today's unified communication applications. With the capacity to scale up to 512 Gbps, the Passport 8600 is designed to scale as well as provide performance. Two active redundant switch fabrics provide seamless failover delivering maximum resiliency. The Passport 8600 supports up to 128 Gigabit Ethernet ports and provides connectivity for 10/100 Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet. It also supports Wavelength Division Multiplexing (WDM), ATM, and Packet over SONET. As network traffic increases, scalability and performance become even more critical for network core devices.

Figure 2. Reliability with SMLT/R-SMLT



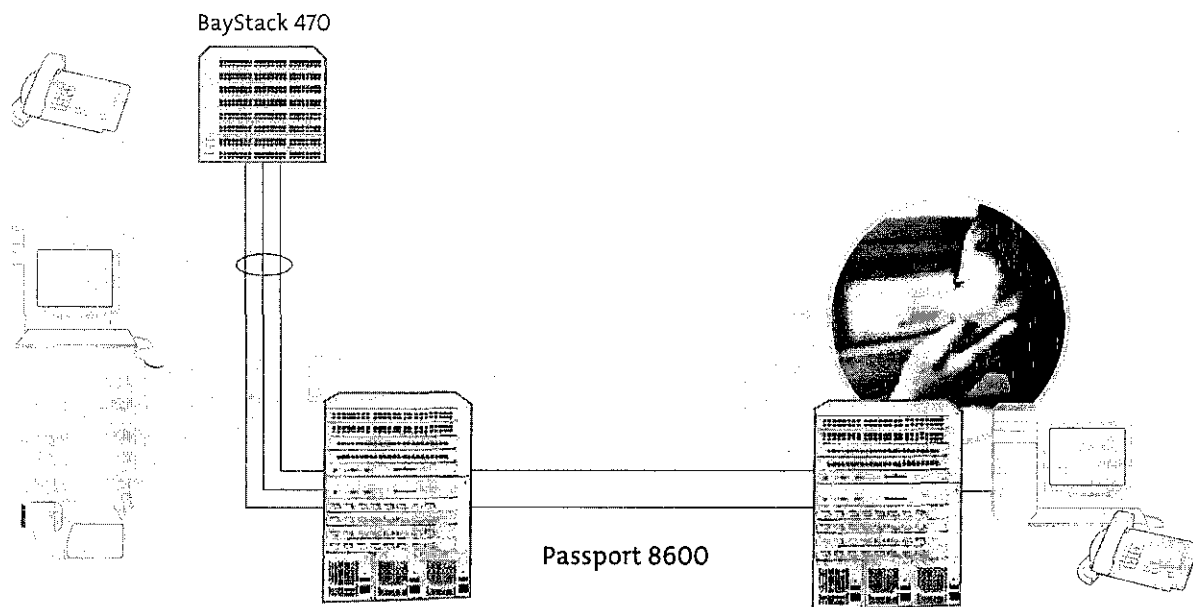


Figure 3. Convergence solution

Ensuring security

With voice, video, and data traveling across the network, there has never been a more urgent need for keeping the network secure. All devices on the network need to ensure network element security as well as data integrity. The Passport 8600 employs several layers of built-in security for both switch access and network data. Passwords, access policies, secure protocols, address and port filtering, routing policies, and DoS prevention mechanisms help ensure that the network and its data stay secure.

Firewall, VPN, and Intrusion Detection System (IDS) load balancing provide both security load balancing and redundancy for maximum effectiveness. Standardized secure protocols for access to the Passport 8600 like SNMPv3 and SSH are designed to ensure the switch stays secure from the inside out. VLANs provide a mechanism to logically separate traffic and are the first step towards ensuring disparate network traffic is not mixed. Support for authentication protocols like 802.1x EAP and RADIUS allow existing authentication systems to be used with the Passport 8600 with little network disruption. An integrated firewall means fewer security devices to configure, manage, and maintain. Fewer devices translates into less errors which means better security protection.

Summary

The Passport 8600 is a resilient, intelligent, secure solution that allows corporate networks to provide a truly unified communications network. Resiliency helps ensure that network resources are always available. Intelligence delivers bandwidth and performance for those applications that need it the most when they need it. Security helps ensure that the information traveling across your network remains secure and unaltered. Resiliency, intelligence, and security are the basic network building blocks that allow an enterprise to use their network to grow their business and provide a solid foundation for their future network growth.

switching and processing

switch fabric/CPU module—High-performance 256 Gbps Layer 2 and Layer 3 traffic switching. One per chassis; two for redundancy.

et

10GBASE-T/100BASE-TX Ethernet Routing Switch module (RJ-45)—Cost-effective switching/routing via 48 auto-sensing 10/100 ports, for high-density server farms and high-end wiring closets

et/Gigabit Ethernet

Routing Switch Module 8632TX—32-port mixed-media module for 10GBASE-T/100BASE-TX switching and routing, with two Gigabit Interface Converters (GBICs), used where high port density and minimal number of gigabit ports are required

hernet

100BASE-FX Fast Ethernet Routing Switch module (MT-RJ)—Cost-effective 10/100 switching and routing over long cable runs (kilometers over multimode fiber)

1 Gigabit Ethernet

1000BASE-SX Gigabit Ethernet Routing Switch module (MT-RJ)—Up to 128 Gigabit Ethernet ports per 10-slot chassis, for high-gigabit Ethernet

1000BASE-T Gigabit Ethernet Routing Switch module (RJ-45)—Gigabit Ethernet over Category 5 copper cabling, up to 128 Ethernet ports per 10-slot chassis, for high-density gigabit Ethernet

1000BASE-T Gigabit Ethernet Routing Switch module (RJ-45)—Gigabit Ethernet over Category 5 copper cabling, a low-cost for runs up to 100 meters

1000BASE-SX Gigabit Ethernet Routing Switch module (SC)—8 Gigabit Ethernet ports with SC connectors, for cost-effective switching and routing using multimode fiber

1000BASE-T Gigabit Ethernet Routing Switch module—Uses one or more plug-in GBICs for customers wishing to mix and match interface a single module using copper, multi-mode, or single-mode fiber. GBICs available in 1000BASE-T, short distance (SX), long distance extended distance (XD and ZX).

10 Gigabit Ethernet

100Gbit 10-Gigabit Ethernet Routing Switch modules—Auto sensing, fully featured LAN and WAN connectivity with the full capability and intelligence of the Passport 8600

100Gbit Packet over SONET

100Gbit MDA Baseboard—Supports up to either four ports of DS-3 or eight OC-3 or two OC-12 ports for ATM interface applications permanent virtual circuit VLAN bridging and routing, maintaining QoS prioritization

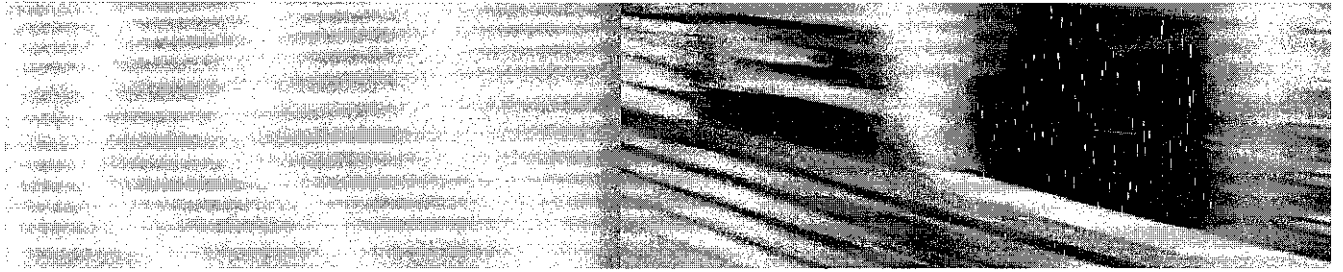
100Gbit S MDA Baseboard—Supports up to six OC-3 or three OC-12 ports for SONET interface applications such as routing/bridging sites with SONET ADMs, interconnecting sites with private/leased fiber connections, and IP over PPP connections

100Gbit Packet over SONET

100Gbit Packet over SONET Switching Module—4-port 1000BASE-SX Gigabit or 10GBASE-T/100BASE-TX scales to support over 4 million concurrent sessions of 2.4 million sessions per second with wire-speed filtering for over 48,000 security and policy services

100Gbit Packet over SONET Switching Module—Features 3,000 SSL sessions per second, 260 Mbps and 64,000 concurrent connections per module

1 in a future release.



The Passport 8600 is a resilient, intelligent, secure solution that allows corporate networks to provide a truly unified communications network. Resiliency, intelligence, and security are the basic network building blocks that allow an enterprise to use their network to grow their business and provide a solid foundation for their future network growth.

Nortel Networks is an industry leader and innovator focused on transforming how the world communicates and exchanges information. The company is supplying its service provider and enterprise customers with communications technology and infrastructure to enable value-added IP data, voice and multimedia services spanning Wireless Networks, Wireline Networks, Enterprise Networks, and Networks. As a global company, Nortel Networks does business in more than 150 countries. Information about Nortel Networks can be found on the Web at:

v.nortelnetworks.com

For more information, contact your Nortel Networks representative, or 1-4 NORTEL or 1-800-466-7835 from anywhere in North America.

Nortel Networks, the Nortel Networks logo, the globemark design, Alteon, BayStack, and Passport are trademarks of Nortel Networks. All other trademarks are the property of their owners.

© 2004 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for any errors that may appear in this document.

084-052604

In the United States:

Nortel Networks
35 Davis Drive
Research Triangle Park, NC
27709
USA

In Canada:

Nortel Networks
8200 Dixie Road,
Suite 100
Brampton, Ontario L6T 5P6
Canada

In Caribbean and Latin America:

Nortel Networks
1500 Concorde Terrace
Sunrise, FL 33323
USA

In Europe:

Nortel Networks
Maidenhead Office Park
Westcott Way
Maidenhead Berkshire SL6
3QH
UK

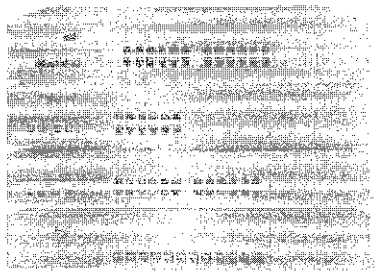
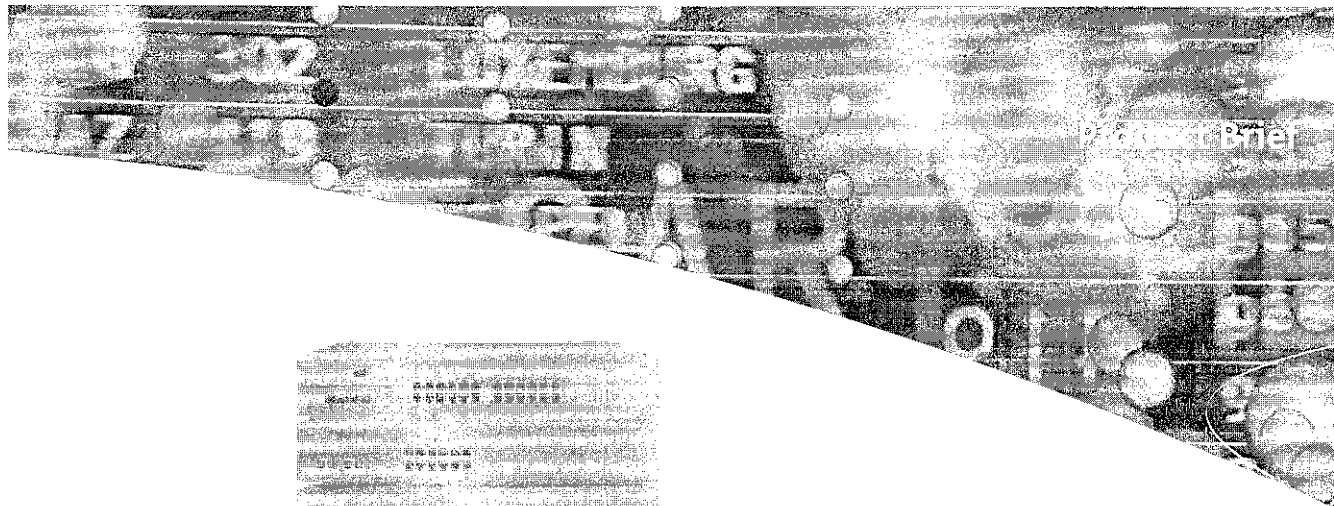
In Asia:

Nortel Networks
Level 5, 495 Victoria Avenue
Chatswood, NSW, 2067,
Australia
Phone: +61 2 8870 5200

NORTEL
NETWORKS

LESS WITHOUT BOUNDARIES

APPENDIX C
PRODUCT BRIEF : BAYSTACK 450 SWITCHES



BayStack 410 and 450 Switches

Stackable Up to
48 Ports and 224 Ports

Safe Cascade
Switching
Architecture

Multiple Uplink Options

BayStack* 410 and 450 Switches are stackable Ethernet switches featuring fail-safe stackability, flexible choices for high-speed uplinks, and advanced software features.

BayStack 450 Switches are designed to provide high-density, high-performance switching for enterprise wiring closets, and to provide fail-safe scalability and advanced traffic management for rapidly growing networks in demanding environments.

The BayStack 410-24T Switch is an affordable, stackable 10BASE-T switch solution for growing network environments and features fail-safe stackability with the BayStack 450 Switches.

BayStack 410 and 450 Switches also include advanced features such as VLAN trunking, priority queuing, and IGMP snooping. BayStack 450 Switches and Accelar* Routing Switches also provide network resilience and advanced management with MultiLink Trunking, LinkSafe* redundant uplink ports, RMON on every port, complete integration into Optivity* network management software, and easy-to-use GUI management.

NORTEL
NETWORKS™

How the world shares ideas.

defined in Table 1, BayStack 450 switches are available in 24- and 12-port configurations, each with a Media Independent Adapter (MDA) slot, as well as a cascade module slot. The BayStack 410-24T has 24 10BASE-T ports, one MDA slot, and one cascade module slot.

Features and Benefits

High-Speed Port Options

100BASE-FX and 10BASE-T/100BASE-TX ports for the BayStack 410 and 450 switches provide high-speed connections to your network center. Specifically for the BayStack 450 Switches, Gigabit Ethernet ports and ATM uplinks provide greater connections to the backbone.

Autosensing Every Port

Every port on the BayStack 450-12T and 450-24T Switches are equipped with autosensing technology to automatically detect and support the speed and mode of the connected device. As well as automatically detecting whether a connected device is operating at 10 Mbps or 100 Mbps and automatically adjusting to the

optimal speed, each switched port also automatically detects and supports full-duplex connections to servers, power-user endstations or other switches as well as half-duplex connections to legacy NICs or hubs. The BayStack 410-24T Switch is a cost-effective, stackable switch that supports 24 10BASE-T ports.

High-Density Fiber Ports

The BayStack 450-12F Switch has twelve 100BASE-FX mini MT-RJ ports, one MDA slot, and a cascade module slot. Up to eight BayStack 450-12F Switches can be stacked to achieve up to 128 100BASE-FX ports (with 4-port 100BASE-FX MDA on each switch). The BayStack 450-12F Switch can also be stacked with the BayStack 410-24T, 450-12T, and 450-24T Switches to accommodate flexible networks.

Redundant Cascade Stacking Architecture

Unlike other stacking switches, BayStack 410 and 450 Switches are designed with a fail-safe cascade stacking architecture (see Figure 1). Cascade cables connect up to 8 stacked switches into a self-healing configuration that protects the stack's connectivity by looping connection

signals back at a point of failure. In the unlikely event of a switch failure, all other units in a stack remain operational without interruption.

The redundant cascade stacking architecture is a safer, smarter alternative to current "matrix" stacking switches, which suffer from a single point of failure design flaw — should the base unit fail, all connectivity to all switches in the stack is lost.

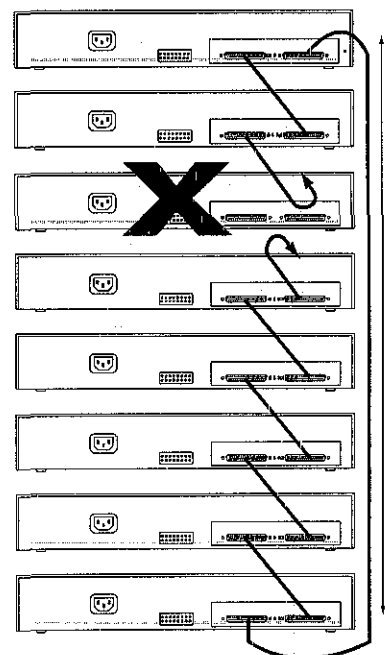
Wire-speed Throughput

2.5 Gigabit per second (Gbps) switching fabric and custom switching ASICs support full 802.1D-compliant MAC Layer frame forwarding and filtering across all ports at the peak rate of 3 million packets per second for the BayStack 450 Switches. The non-blocking architecture of the BayStack 410-24T Switch allows packets to be forwarded at 1 million packets per second.

Figure 1: In the unlikely event of a switch failure, the stack integrity is maintained: cascade signals loop back at point of failure.

Table 1: Port, MDA, and Stacking Module Slot Configurations of the BayStack 410 and 450 Switches.

BayStack Switches	Autosensing 10BASE-T/ 100BASE-TX Ports	MDA Slot	Cascade Stacking Module Slot
BayStack 450-12T	12	1	1
BayStack 450-24T	24	1	1
BayStack 410-24T	24 (10BASE-T only)	1	1
BayStack 450-12F	12 (100BASE-FX only)	1	1



Configured VLAN Support

Port-based or protocol-based VLANs can be established for each switch to extend the broadcast domain and segment network traffic.

Protocol-based VLANs allow switch ports to be assigned to a broadcast domain, independent of the protocol information within the packets. These VLANs can localize network traffic and assure that the correct protocol type packets are sent through the protocol-based VLAN ports.

Stacked VLAN Trunking

VLAN trunking is supported on every switch in the stack, allowing efficient transport of broadcast domains across switches.

Priority Queuing

Class-based priority queuing allows prioritization of multimedia or sensitive traffic, making possible coexistence of voice, video, and data on the same network.

Life Design Features

Redundant cascade stacking architecture. Each unit in the stack has a full copy of stack configuration so in the unlikely event of any unit failure, operation of the stack continues without affecting network connectivity.

Stacked uplinks (for BayStack 450 switches only) feature LinkSafe, which provides two different physical fiber connectors for each Gigabit uplink. In the event of a primary path failure, the traffic is automatically rerouted to the redundant path within microseconds, protecting critical Ethernet connections to servers or the network center.

Stacked Link Trunking can be implemented across the stack, where connections between individual devices (for example, between a BayStack 450 Switch and an Accelar 1200 Routing Switch) can be aggregated for both higher bandwidth

and redundancy. Should one port connection fail, other connections within the MultiLink Trunk assume the full traffic load seamlessly. MultiLink Trunking also allows servers and critical resources to be connected to different switches in the stack to achieve “Multi-Homing,” whereby link redundancy is extended to include unit redundancy, resulting in highly available critical resources (see Figure 2).

- Each switch includes a Redundant Power Supply Unit connection. Should the switch’s built-in power supply fail, the Nortel Networks RPSU (sold separately) will automatically supply power to the switch for uninterrupted operation.

MultiLink Trunking

Enables grouping of links between the switch and another switch or a server to provide higher bandwidth of up to 800 Mbps (when used with 10/100 ports or 100BASE-FX ports) or up to 8 Gigabits

per second (when used with Gigabit uplink ports on BayStack 450 Switches) with active redundant links. Trunked ports can span multiple units of the stack for fail-safe connectivity to mission-critical servers and the network center.

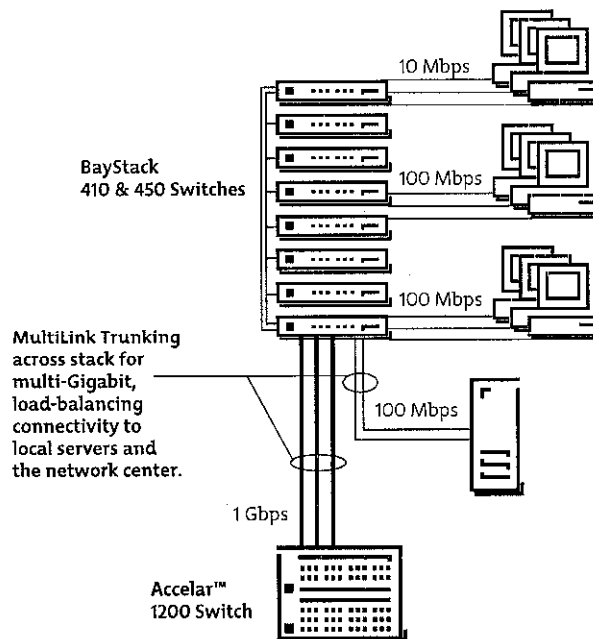
IGMP Snooping

The BayStack 410 and 450 Switches feature a new level of efficient IP MultiCast support by examining (‘snooping’) all IGMP traffic in hardware at line rate, and pruning unwanted data streams from affecting network or endstation performance.

Enterprise-sized MAC Address Table

BayStack 410 and 450 Switches support more than 16,000 MAC addresses per switch for deployment of large-scale enterprise networks with many attached devices and workgroups connected to each switch. (In a full 802.1Q environment, 32,000 MAC addresses are supported.)

Figure 2: High-density 10/100/1000 switching in the wiring closet, featuring fail-safe stackability and MultiLink Trunking for redundant connections to local servers and the network center.



Ports Spanning Protocol

BayStack 410 and 450 Switches include support for Spanning Tree Protocol (IEEE 802.1D), which detects and eliminates logical loops in the network. When multiple paths exist, the switch automatically places some ports on hold to form a network with the most efficient traffic pathways, avoiding the possibility of looping of frames.

Integrated into Optivity Network Management Software

BayStack 410 and 450 Switches feature support for Optivity network management software, enabling complete integration with Network Management Protocol (NMP) and RMON monitoring and management. Network administrators can manage their entire network, including all switches, and routers, from a single management station, dramatically reducing network total cost of ownership.

Web-Based GUI Management

BayStack 410/450 Switches can be configured and managed by using the Optivity Manager Software. Also, VLAN configuration software may be used for configuring and managing VLANs on any BayStack 410/450 and 450 switches. Both software can be downloaded free from the web site.

BayStack 410/450 Switches may also be managed by using Optivity NMS and NCS software.

In addition to above choices, an easy-to-use menu-driven interface can be accessed via console or Telnet for complete configuration and management for the BayStack 410 or 450 Switch.

Other Advanced Management Features

- Adjustable rate limits protect the LAN against broadcast or multicast storms that can severely limit performance.
- BootP and TFTP support allows centralized switch IP address assignment, software upgrades, and SNMP agent updates over the network.
- The RADIUS-based security feature uses the RADIUS (Remote Authentication Dial-In User Services) protocol to authenticate local console and TELNET logins.
- The Autotopology feature allows network topology mapping of other switches in the network.

BaySecure Secure LAN Access

BaySecure* allows authentication of all access, not only to the switches for management and configuration, but also access to the infrastructure through these switches. Integrated with DHCP and other IP services from Nortel Networks, this software feature limits access to the network to authorized and trusted users with full tracking of network connections.

Concurrent RMON on Every Port

This enables standards-based RMON managers and Optivity applications to manage the network, as well as the device, with four groups of RMON (Alarms, Events, History, and Statistics) on every port.

Enhanced Port Mirroring

Port mirroring enables detailed RMON 1 and RMON 2 analysis of switched traffic using the Nortel Networks StackProbe* or other external LAN analyzers connected to any port in the stack. Port mirroring copies packets flowing through a specified port and sends the replicated data to the probe for in-depth analysis of switched traffic patterns to trouble-shoot problems and optimize network configurations.

Recovery Configuration File Support

The configuration file feature allows for storing of switch or stack configuration parameters on a TFTP server. Configuration parameters can be retrieved automatically to configure a replacement switch or stack with the same configuration. For new installations or when a switch has failed, this feature saves time in reconfiguring another switch or stack.

RJ-45 Connectors Wired for MDI-X

All 10/100 autosense Ethernet port connectors are wired for MDI-X connections to other devices. Inexpensive straight-through unshielded twisted pair (UTP) cables can be used to provide switch connections to servers, desktops, and internetworking devices.

Technical Specifications

Technical Specifications for the BayStack 410 and 450 Switches.

Performance Specifications (64 byte packets)

Aggregate Throughput (BayStack 450 Switches)	3 million packets per second (pps)
Aggregate Throughput (BayStack 410-24T Switch)	1 million packets per second (pps)
Switched 10 Mbps Port Forwarding Rate	14,880 pps
Switched 100 Mbps Port Forwarding Rate	148,810 pps
Switched 1000 Mbps Port Forwarding Rate	1,488,100 pps
Latency	9 microseconds for minimum packet length at 100 Mbps

Work Protocol and Standards Compatibility

IEEE 802.3 CSMA/CD (ISO/IEC 8802-3)
IEEE 802.3i 10BASE-T (ISO/IEC 8802-3)
IEEE 802.3u 100BASE-TX (ISO/IEC 8802-3)
IEEE 802.1D MAC Bridges (ISO/IEC 10038)
IEEE 802.3z 1000BASE-SX and 1000BASE-LX
(Draft Standard ver. 3.1)
IEEE 802.1p (Prioritizing)
IEEE 802.1Q (VLAN Tagging)

Rate and Encoding

10 Mbps	Manchester encoding
100 Mbps	4B/5B encoding
1000 Mbps	8B/10B encoding

Optical Link Power Budget

1000BASE-SX	7.5 dB
1000BASE-LX MultiMode Fiber	7.5 dB
1000BASE-LX SingleMode Fiber	8.0 dB

Optical Cabling Distance Specification

1000BASE-SX on MMF (50 μ m)	550 m
1000BASE-SX on MMF (62.5 μ m)	260 m
1000BASE-LX on MMF (50 μ m)	550 m
1000BASE-LX on MMF (62.5 μ m)	550 m
1000BASE-LX on SMF (10 μ m)	5 km

Optical Cabling and 100BASE-FX Cabling Type

62.5/125 micron (core/cladding) MultiMode fiber

Optical Cabling and 100BASE-FX Connector Type

SC type connector for the Gigabit MDAs
and the 2-port 100BASE-FX MDA
MT-RJ type connector for the 4-port 100BASE-FX MDA
and the BayStack 450-12F Switch

Technical Specifications for the BayStack 410 and 450 Switches (continued).

Electrical Specifications

Operating Frequency	47 to 65 Hz
BayStack 410-24T Switch	Input Volt Amperes Rating 150 VA maximum Input Power 100 W maximum Input Voltage 100-240 VAC Input Current 1.5 to 1.6 A @ 100 VAC Thermal Rating 500 Btu/hr
BayStack 450-24T and 450-12F Switches	Input Volt Amperes Rating 200 VA maximum Input Power 140 W maximum Input Voltage 100 - 240 VAC Input Current 2.0 A @ 100 VAC Thermal Rating 478 Btu/hr
BayStack 450-12T Switch	Input Volt Amperes Rating 150 VA maximum Input Power 120 W maximum Input Voltage 100 - 240 VAC Input Current 1.5 A @ 100 VAC Thermal Rating 410 Btu/hr

Mechanical Dimensions

BayStack 450 Switches	(H) 2.77 in. x (W) 17.55 in. x (D) 15.0 in. [(H) 7.03 cm x (W) 44.07 cm x (D) 38.1 cm]
BayStack 410-24T Switch	(H) 2.77 in. x (W) 17.40 in. x (D) 13.50 in. [(H) 7.03 cm x (W) 44.20 cm x (D) 34.29 cm]

Weight

BayStack 450 Switches	11.6 lb (5.26 kg)
BayStack 410-24T Switch	7.63 lb (3.46 kg)

Environmental Specifications

Operating Temperature	32° to 104° F (0° to 40° C)
Storage Temperature	-13° to 158° F (-25° to 70° C)
Operating Humidity	85% maximum relative humidity, noncondensing
Storage Humidity	95% maximum relative humidity, noncondensing
Operating Altitude	10,000 ft (3,000 m) maximum
Storage Altitude	10,000 ft (3,000 m) maximum
Shock/Fall/Drop	ISO 4180-s, NISTA 1A
Vibration	IEC 68-2-6/34
Shock/Bump	IEC 68-2-27-29

: Technical Specifications for the BayStack 410 and 450 Switches (continued).

Electromagnetic Emissions

Meets requirements of

US	FCC Part 15, Subpart B, Class A
Canada	ICES-003, Issue-2, Class A
Australia/New Zealand	AS/NZS 3548:1995, Class A
Japan	V-3/97 04:1997, Class A
Taiwan	CNS 13438, Class A
EN 55 022 (CISPR 22:1985), Class A	
EN61000-3-2	1995
EN61000-3-3	1994
VCCI Class 1 ITE	
CE	

Electromagnetic Susceptibility

Electrostatic Discharge (ESD)

EC 801-2, Level 2

Radiated Electromagnetic Field

EC 801-3, Level 1

Critical Fast Transient/Burst

EC 801-4, Level 2

UL Agency Approvals

UL Listed (UL 1950)

CSA 22.2 #950 with D3 deviations

IEC 950/EN 60 950

UL-94-V1 flammability requirements for all PC boards

Ordering and Availability Information

: Ordering and Availability Information for the BayStack 410 and 450 Switches.

Number	Description	Comments
2214	BayStack 450-24T Switch 24 10BASE-T/100BASE-TX ports plus 1 MDA slot and 1 Cascade slot	
2215	BayStack 450-12T Switch 12 10BASE-T/100BASE-TX ports plus 1 MDA slot and 1 Cascade slot	
2216	BayStack 410-24T Switch 24 10BASE-T ports plus 1 MDA slot and 1 Cascade slot	
2219	BayStack 450-12F Switch 12 100BASE-FX ports plus 1 MDA slot and 1 Cascade slot	
3002	BayStack 400-2FX 2-port 100BASE-FX MDA	
3003	BayStack 400-4FX 4-port 100BASE-FX MDA	
3004	BayStack 400-4TX 4-port 10BASE-T/100BASE-TX MDA	

ii: *Ordering and Availability Information for the BayStack 410 and 450 Switches (continued).*

Number	Description	Comments
33005	BayStack 450-1SX 1-port 1000BASE-SX Single PHY MDA	For BayStack 450 Switches only.
33006	BayStack 450-1SR 1-port 1000BASE-SX Redundant PHY MDA	For BayStack 450 Switches only. Includes LinkSafe.
33007	BayStack 450-1LX 1-port 1000BASE-LX Single PHY MDA	For BayStack 450 Switches only.
33008	BayStack 450-1LR 1-port 1000BASE-LX Redundant PHY MDA	For BayStack 450 Switches only. Includes LinkSafe.
33010	BayStack 400-ST1 Cascade Module, 2.5 Gbps	Includes cascade cable. Order one per switch in a stack.
18001	BayStack 400-SRC Cascade Return Cable (1 meter)	Order one per stack of 3 units or more.
18002	BayStack 400-SSC Cascade Spare Cable (18 in.)	
18003	BayStack 350/450 Wall Mount Kit - Kit includes 2 wall mount brackets and two expansion brackets for stacking units up to two high.	
18004	BayStack 400-SRC Cascade Return Cable (3 meter)	

enth character (?) of the switch order number must be replaced with the proper code to indicate desired product nationalization. "A" – No power cord included. "B" – European "schuko" power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden. "C" – Power cord commonly used in the United Kingdom and Ireland. "D" – Power cord commonly used in Japan. "E" – North America power cord. "F" – Australia power cord, also commonly used in New Zealand and the People's Republic of China.



How the world shares ideas.

For more sales and product information, please call 1-800-822-9638.

United States
Nortel Networks
4401 Great America Parkway
Santa Clara, CA 95054
1-800-822-9638

Canada
Nortel Networks
8200 Dixie Road
Brampton, Ontario
L6T 5P6, Canada
1-800-466-7835

Europe, Middle East, and Africa
Nortel Networks
Les Cyclades - Immeuble Naxos
25 Allée Pierre Ziller
06560 Valbonne France
33-4-92-96-69-66

Asia Pacific
Nortel Networks
151 Lorong Chuan
#02-01 New Tech Park
Singapore 556741
65-287-2877

Japan
Nortel Networks
Shiroshima Jc Mori Bldg. 28F
4-3-1, Toranomon
Minato-Ku
Tokyo, 105 Japan
81-3-5402-7001

Caribbean and Latin America
Nortel Networks
1500 Concord Terrace
Sunrise, Florida
33323-2815 U.S.A.
954-851-8000

<http://www.nortelnetworks.com>

*Nortel Networks, the Nortel Network corporate logo, the Globemark, How the World Shares Ideas, Accelar, BaySecure, BayStack, LinkSafe, Oprivity, and StackProbe are trademarks of Nortel Networks. All other trademarks are the property of their owners. © 2000 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for any errors that may appear in this document.

APPENDIX D
PRODUCT BRIEF: BAYSTACK 470 SWITCHES

desktop

on effective

Product Brief

Nortel Networks BayStack 470 Switches

- High-density desktop connectivity up to 384 ports
- Cost-effective, plug-and-play with built-in stacking ports
- Two built-in GBIC uplinks for highest uplink capacity and flexibility
- Flexible stacking across different BayStack switches—a stack is managed as a single entity with a single IP address
- Simple software upgrades with single image for different switches
- Resilient connectivity for minimal network downtime
- Fail-safe stacking design assures continuous uptime
- Network availability with QoS features
- Secure access and data traffic protection
- Common look and feel minimizes training and installation costs

Part of the successful Nortel Networks BayStack* family, BayStack 470 Switches are stackable 10/100 Mbps Ethernet Layer 2 switches. BayStack 470 Switches include two built-in GBIC (Gigabit Interface Converter) uplink ports and built-in stacking ports in a compact, one rack-unit high design. They are designed to provide high-density desktop connectivity for mid-size and large enterprise customers' wiring closets.

BoSS (BayStack operating-system Switching Software) allows BayStack 470 Switches to stack with other BayStack switches. BoSS also simplifies software upgrades with a single image for different BayStack switches.

BayStack 470 Switches' comprehensive Quality of Service (QoS) features are designed to ensure connectivity and network availability by managing and prioritizing data traffic for maximum performance. These switches offer a scalable, resilient solution that minimizes capital and operational expenses. Their robust security features offer protection against unauthorized access to data traffic.

The BayStack 470 Switches are available in two models—the BayStack 470-48T Switch and the BayStack 470-24T Switch (*Figure 1*).

High-density, high-speed desktop switching

The BayStack 470-48T Switch features 48 10/100BASE-TX RJ-45 ports for desktop switching and two built-in GBIC ports for uplink. Port 47 and Port 48 offer configuration flexibility by allowing the network administrator to configure each port as either 10/100BASE-TX or make use of the built-in GBIC. Up to eight BayStack 470-48T Switches can be stacked to achieve up to 384 10/100 ports that can be easily managed as a single unit. The 2.56-Gbps cascading bandwidth offers dedicated bandwidth between switches without sacrificing any uplink ports. The uplink ports can be used for connections to backbone switches such as the Passport* 8600 Switch.

The BayStack 470-24T Switch offers 24 10/100BASE-TX RJ-45 ports for desktop switching and two built-in GBIC ports for uplink. All 26 ports may be used simultaneously. Up to eight BayStack 470-24T and 470-48T switches may be combined in a single stack for maximum flexibility.

The BayStack 470 Switches can also be stacked with BayStack 460-24T-PWR, BayStack 450, and BayStack Business Policy Switch. (BoSS 3.1 is the last revision to support the Business Policy Switch.)

Full autosensing on every port

Every UTP port on the BayStack 470 Switch is equipped with autosensing technology to automatically detect and support the speed and mode of a connected device. The ports determine whether a connected device is operating at 10 Mbps or 100 Mbps, and automatically adjust to the optimal speed. Each of the switched ports also automatically detect and support full-duplex connections to servers, power-user end-stations, or other switches, as well as half-duplex connections to legacy NICs or hubs.

Two built-in GBIC ports

BayStack 470 Switches have two built-in GBIC ports for dedicated uplink connectivity to network core switches such as the Passport 8600. This doubles the uplink bandwidth as GBIC ports are not required for stacking purposes. Using the Distributed Multi-Link Trunking, up to 16 GBIC or 10/100BASE-T ports are available for pure uplink connectivity in a full stack—the highest in the market.

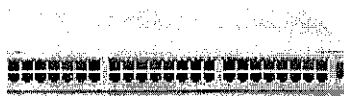
Innovative built-in stacking ports

BayStack 470 Switches have built-in stacking ports for simpler, quicker, and more cost-effective stacking, as cascade modules are not required. This unique stacking design frees up both of the uplink ports for dedicated connectivity to the backbone.

ack 470-24T



ack 470-48T



1. The BayStack 470 Switches

BayStack operating system Switching Software)

With the release of BoSS, Nortel Network became the first vendor to offer a single software image that can support four different switch types: BayStack 460-24T-PWR, BayStack Business Policy Switch, BayStack 470-48T, and BayStack 470-24T. BoSS simplifies network operations and provides the flexibility of stacking different switches in the same stack.

Unified network operations

BoSS simplifies network operations by reducing the number of steps required for switch software updates. With BoSS, you need to download only a single image from Nortel Networks for four different switch types. Loading the image to different switches is also greatly simplified. The image is loaded only to the base unit of the stack which automatically loads it to other switches in the stack. Finally, keeping track of the version number is much easier as only one version number needs to be remembered.

Stacking with other BayStack Switches

With BoSS, the BayStack 470 Switches are able to stack with other BayStack switches (Table 1). Two types of stacks are supported:

BayStack 470-48T can stack with any combination of BayStack 470-24T, BayStack Business Policy Switch, and BayStack 460-24T-PWR.

BayStack 470-24T can stack with any combination of BayStack 470-48T, BayStack Business Policy Switch, BayStack 470-24T-PWR, and BayStack 450.

Please be noted that the BayStack 470-24T cannot be stacked with BayStack 450.

BoSS protects customers' existing investment in BayStack 450 and BayStack Business Policy Switch stacks by allowing a feature-rich and cost-effective upgrade—such as the BayStack 470-24T—stack with the legacy stacks.

With BoSS, a maximum of eight switches can be stacked together in any valid configuration (Table 1).

BoSS 3.1 features

BoSS 3.1 is downloadable from the Web for free and includes support for the following new features, in addition to those supported in v3.0:

- Link aggregation
- Replacement feature
- Based policies
- 100 GbE support
- In-network advertisements (CANA)
- Configuration generator
- Network Time Protocol (SNTP)
- Encrypted message logging

Figure 2. Stacking with existing BayStack 450 or BPS stacks

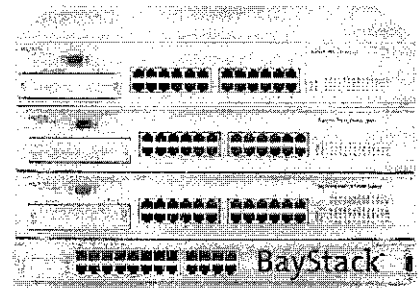


Table 1. Stacking matrix

	BayStack 460-24T-PWR	BayStack 470-24T	BayStack 470-48T	BayStack Business Policy Switch	BayStack 450
BayStack 460-24T-PWR with BoSS v3.1	Yes	Yes	Yes	Yes	Yes
BayStack 470-24T with BoSS v3.1	Yes	Yes	Yes	Yes	Yes
BayStack 470-48T with BoSS v3.1	Yes	Yes	Yes	Yes	No
BayStack Business Policy Switch with BoSS v3.1	Yes	Yes	Yes	Yes	Yes
BayStack 450 ¹	Yes	Yes	No	Yes	Yes

Note: ¹ BayStack 450 must have BayStack 450 software v4.2 or higher. BoSS v3.1 is the last revision that will support BayStack BPS.

802.3ad link aggregation

IEEE 802.3ad provides an industry-standard method for bundling multiple links together to form a single trunk between two networking devices. BoSS 3.1 supports both Dynamic Link Aggregation Group (LAG) trunks and MLT trunks. Once configured, the Link Aggregation Group or trunk group is managed by the Link Aggregation Control Protocol (LACP). BayStack supports both Link Aggregation and MLT groups. Up to six LAG or MLT groups are supported. The maximum number of active links per group is four. The link aggregation allows more than four links to be configured in one LAG. The first four high-priority links will be active links and the lower-priority link will be the standby link. When one of the active links goes down, the standby link will become active. This feature can be implemented by using Command Line Interface (CLI), Device Manager, or SNMP.

Unit replacement feature

In the unlikely event that a switch fails in a stack, the affected switch can easily be replaced without disrupting the stack. This feature provides the capability of upgrading a new unit with the configuration of the affected unit off-line, before adding the new unit to the stack. The configuration of the affected switch may be copied from the Trivial File Transfer Protocol (TFTP) server to the new switch. The new switch can then be inserted into the stack without requiring a reboot of the entire stack. This feature can be implemented by using menu, Web interface, or CLI commands.

User-based policies

This feature enables network services (i.e., QoS) to follow the user regardless of the PC logged into or the port connected to. The switch requires a user to be authenticated using EAP and sends username/password information to the Remote Authentication Dial-In User Service (RADIUS) server. The RADIUS server provides the user's role/group attributes to the switch that allows user access to the port with the default configuration. The switch then passes role/group/port information to the Optivity* Policy Services (OPS) server that configures the user port based on the specific policy information.

Custom Autonegotiation Advertisements (CANA)

This feature enables the network manager to tune the capabilities that a particular Ethernet port can advertise via autonegotiation. The capabilities include half-duplex and full-duplex modes with speeds of 10, 100, and 1000 Mbps. Autonegotiated Ethernet ports establish a connection based upon the highest common capabilities. This feature is implemented by using CLI commands and saves the network manager from having to go to each workstation and switch to configure a "fixed" speed.

ASCII configuration generator

The ASCII configuration generator allows the configuration settings of the switch to be displayed or saved to an external ASCII configuration file made up of a series of CLI commands. This editable ASCII configuration file can then be uploaded to a switch from an external file server.

The ASCII configuration file contains configuration settings for the following network management applications:

- Core applications (system information, topology, etc.)
- Internet Protocol
- Multi-Link Trunking (MLT)
- Port configuration

Spanning Tree configuration, including configuration of port priority and path cost
 configuration
 of Service (QoS)
 N

Network Time Protocol (SNTP)

Network Time Protocol allows the synchronization of the switch or stack's clock to time clock on the SNTP server. If the system (switch or stack) uses SNTP, then time is used to time-stamp system log (Syslog) messages. If SNTP is not in-use, system uses a time-stamp relative to boot time.

Enhanced message logging

Several features have been added for enhanced message logging. Log entries can now be time-stamped in real time when the SNTP is in use. With the remote logging feature, the switch has the ability to copy internal system log messages onto a remote Syslog server. Additionally, the *Show Logging* feature gives the administrator flexibility to view and sort log entries in forward or reverse manner.

Link Trunking

Link Trunking (MLT) enables grouping of links between the BayStack 470 and Passport 8600 switch or server to provide greater bandwidth with active redundant links. With networks unique Distributed Multi-Link Trunking (DMLT) feature, trunked ports connect multiple units of the stack for fail-safe connectivity to mission-critical servers and network center. This can provide greater bandwidth of up to 800 Mbps (when used with 100 ports) or up to 8 Gbps (when used with Gigabit uplink ports) with active redundant links in one trunk. Up to six trunks are supported per switch or stack (Figure 3).

Stack 470's ability to have multiple connections to a Passport 8600 core using the Split Multi-Link Trunking (SMLT) feature of the Passport 8600 provides customers to double their bandwidth with no extra investment. The Passport 8600 provides a self-managing network which delivers the performance and availability required by mission-critical applications. By combining the reliability of the Passport 8600 with the resilient trunking features of BayStack 470, such as DMLT and Distributed Multi-Link Trunking, Intel Networks has created the foundation of flexible networking solutions.

For example, an enterprise solution consisting of BayStack 470 Switch stacks connecting closets, collapsing in to the core switch (Passport 8600), providing high-density desktop connectivity and fault-tolerant connections to network and mission-critical servers (Figure 4).

Figure 3. Distributed Multi-Link Trunking across stack for higher bandwidth and fault tolerance

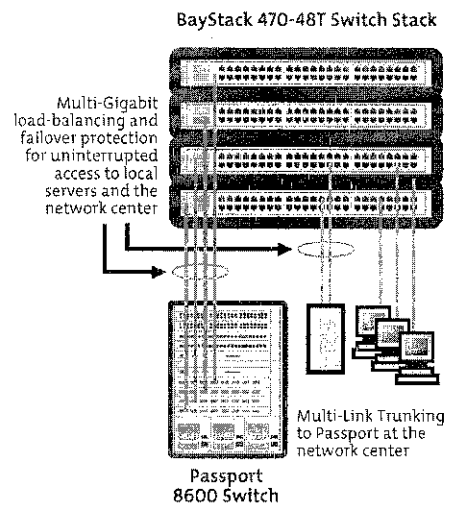
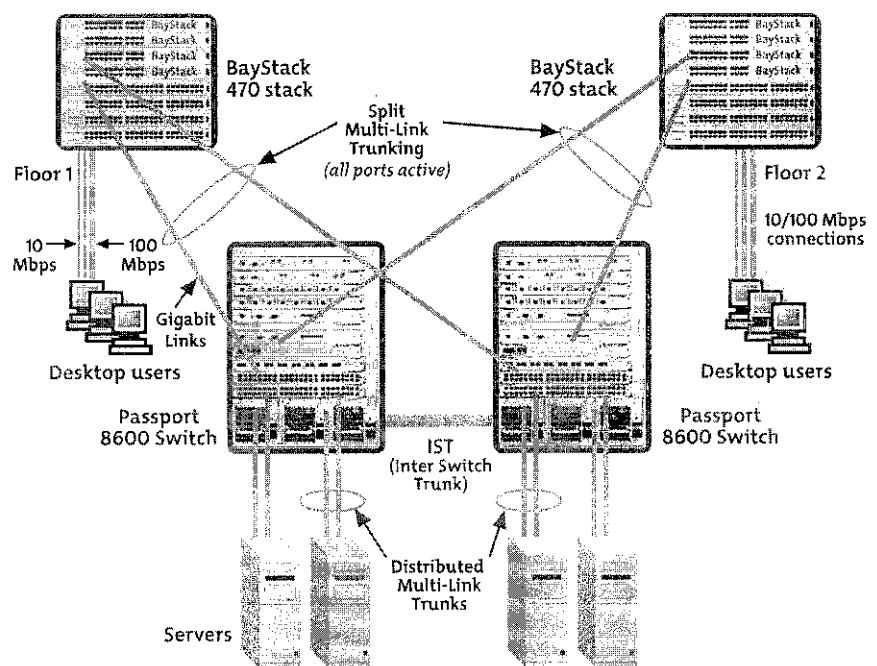


Figure 4. Split Multi-Link Trunking (SMLT)



Redundancy

With connectivity to the BayStack 10 Power Supply Unit (PSU), paired with a -48V DC-to-DC converter module, BayStack 470 Switches deliver redundant power supply (RPS) support crucial in mission-critical environments. The Uninterruptible Power Supply (UPS) capability is supported on the switch with BayStack 10 PSU.

Enhanced security

BayStack 470 Switches offer the highest level of security with features including Secure Shell (SSH), IEEE 802.1x based security (also known as Extensible Authentication Protocol - EAP), Simple Network Management Protocol (SNMPv3), IP Manager's list, MAC address-based security, and RADIUS authentication.

SSHv2 supports strong authentication and encrypted communications. It allows a user to log into the switch from an SSH client and perform a secure Telnet session using CLI commands. This feature is ideal for security conscious customers such as federal governments.

For added security, BayStack 470 Switches support the 802.1x-based security feature—EAP. Based on the IEEE 802.1x standard, EAP limits access to the network based on user credentials. A user is required to “login” to the network using a username/password; the user database is maintained on the authentication server (not the switch). EAP prevents network connectivity without password authorization for added security and control in physically non-secure areas. It is used where the network is not 100 percent physically secure or where physical security needs enhancement—for example, banks, trading rooms, or classroom training facilities. EAP supports client access to the network and interoperates with Microsoft Windows XP and other standards-based clients.

SNMPv3 provides user authentication and data encryption for higher security. It also offers secure configuration and monitoring.

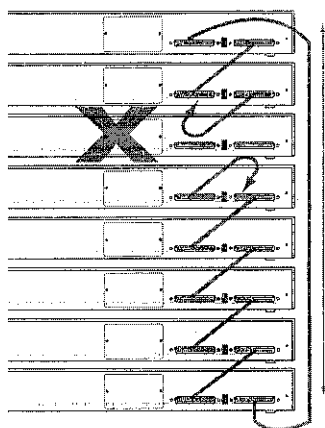
IP Manager List limits access to the management features of BayStack 470 Switches by a defined list of IP addresses, providing greater network security and manageability.

The BayStack 470 Switches feature BaySecure* MAC address-based security, which allows authentication of all access, not only to the switches for management and configurations but also access to the infrastructure through these switches. This software feature limits access to only network authorized and trusted personnel, including full tracking of network connections. With BaySecure, network access is granted or denied via proper MAC address (up to a maximum of 448) identification. In addition, with the Distributed Access List Security feature, network access is granted or denied on a per-port basis. BayStack 470 Switches also provide RADIUS authentication for switch security management.

Fail-safe stacking and resiliency

A key differentiator for BayStack 470 Switches is their resilient stacking feature. BayStack 470 Switches can stack up to eight units with a cascade stacking design, assuring continuous uptime even if a single switch in the stack should fail. A loop-back or cascade cable is used to seamlessly connect the entire stack to provide no single point of failure (*Figure 5*).

5. In the unlikely event of a failure, the stack integrity is maintained: cascade signals track at point of failure.



Look and feel

Stack switches, including the BayStack 470, have a common “look and feel” which reduces training costs. This allows the switches to be managed in a similar fashion via a variety of management tools. These tools include Web, Java™-based Device Manager Command Line Interface (CLI), menus, Optivity Network Management System (ONMS), Optivity Switch Manager (OSM), and Optivity Policy Services (OPS).

MAC addresses

BayStack 470 Switches support up to 16,000 MAC addresses per switch or stack, for use in a wide range of large-scale, enterprise networks with many attached devices and workstations, allowing for scalability and cost-effectiveness.

VLAN support

256 port-based VLANs can be configured per individual switch or per stack to define a broadcast domain and segment network traffic. The 256 VLANs can be spread across port-based and MAC source address-based VLANs (up to a maximum of 48 MAC address-based VLANs). The 256 VLANs can be on a standalone switch or across a stack. Protocol-based VLANs allow switch ports to be assigned to a broadcast domain based on the protocol information within the packet. These VLANs localize broadcast traffic and assure that the specified protocol type packets are sent only to the protocol-based VLAN ports.

Shared VLAN (SVL) and Independent VLAN Learning (IVL) are supported. With SVL, all VLANs in the switch share the same forwarding database. IVL allows individual VLANs to have separate forwarding databases within the switch, and it allows the switch to handle duplicate MAC addresses if the addresses are in different VLANs.

IGMP snooping

BayStack 470 Switches feature IP Multicast support by examining (‘snooping’) all Internet Group Management Protocol (IGMP) traffic in hardware at line rate, and pruning unwanted traffic to prevent it from affecting network or end-station performance.

Multiple spanning tree protocol groups

BayStack 470 Switches support multiple spanning tree groups (STGs). They support a maximum of eight STGs, either all in one standalone switch or across a stack consisting of up to eight BayStack 470 Switches. Multiple STGs provide multiple data paths, which can be used for load balancing and redundancy.

Command Line Interface (CLI)

CLI is used to automate general management and configuration of BayStack 470 Switches. The CLI may be used through a Telnet/Secure Shell session or through the serial console.

Configuration file

BayStack 470 Switches can download a user-editable ASCII configuration file from a Trivial File Transfer Protocol (TFTP) server. The ASCII configuration file can be loaded automatically at boot time or on-demand using the management systems (console menus). Once downloaded, the configuration file automatically configures the switch or stack according to the CLI commands in the file. This feature allows the flexibility of using command configuration files that can be used on several switches or stacks with minimal modifications.

Support for Spanning Tree Protocol

Built-in support for Spanning Tree Protocol (IEEE 802.1D) detects and eliminates logical loops in the network. When multiple paths exist, the switch will automatically place some ports on standby to form a network with the most efficient traffic pathways, avoiding the continual looping of frames.

Port mirroring

The port mirroring feature (sometimes referred to as 'conversation steering') allows the network administrator to designate a single switch port as a traffic monitor for a specified port. Port mirroring copies packets flowing into a specified port and sends the replicated data to the mirrored port for in-depth analysis of switched traffic patterns to troubleshoot problems and optimize network configurations. Additionally, an external probe device can be attached to the designated monitor port.

Advanced management features

BootP and TFTP support allows centralized switch IP address assignment, software upgrades, and SNMP agent updates over the network. The RADIUS-based security feature uses the RADIUS protocol to authenticate local console and TELNET logins.

LED indicators

The LED indicators on the front panel make it easy to monitor the switch and port status and help in isolating and diagnosing switch problems.

Auto MDI/MDIX

BayStack 470 Switches can be connected to a hub or another switch quickly and cost-effectively. Normally, a crossover cable is needed for this purpose, but with the BayStack 470 Switch, an inexpensive straight-through cable or a crossover cable can be used.

When a cable is connected to one of the 10/100 ports on the switch, the switch port automatically can detect the energy on the cable and configures itself. This feature makes configuration easier, as it eliminates the need for an MDI/MDIX port; any port may be used for connection to a hub or switch.

Network management

Web-based management

Web-based network management makes managing the BayStack 470 Switch stack easy with a Web browser. Summary, configuration, fault, statistics, application, administration, and support pages can be provided for the entire stack. Traffic classification and prioritization can be set via the Web-based QoS Wizard and advanced configuration tool. Real-time sampling provides up-to-date LED statistical information for stacked units. The Web interface also allows for static configuration of numerous parameters of the device.

On-box management

Network management begins with the device. BayStack 470 Switches support four groups of Remote Monitoring (RMON) on all ports and are SNMPv3 (Simple Network Management Protocol) compliant. RMON2 is supported via the port mirroring function using an external RMON2 probe. The SNMP agent software resides in the switch and uses the information it collects to provide management for all ports in the stack, providing comprehensive network monitoring capabilities. In addition, the agent also provides the ability to set up policy-based networks by supporting the Common Open Policy Support (COPS) protocol.

uration management

cess of configuration begins with a single device but finishes across multiple Java Device Manager (JDM) is the GUI device configuration tool for configuring device. It uses a common user interface and workflow that supports many Nortel s Ethernet switches. This commonality allows the network manager to become with one tool instead of multiple tools. Furthermore, JDM also supports SNMPv3, network managers to securely manage their network. Optivity Switch Manager 4.0 is a Java™-based, real-time, configuration management application for networks Ethernet products including BayStack 470 Switches. It enables network s to discover, view, and configure more than 500 network devices and their links on a topology map. Configuration is stored in Non-Volatile Random Access (NVRAM).

management and resolution

ativity Network Management System (ONMS), the network manager has quick the information required to manage and isolate all network events on BayStack ches. Tools such as Physical Topology View inform the network manager of how a r event is affecting the physical connectivity within the network. End Node ol provides the ability to locate a failing end node and, with one mouse click, access to the RMON statistics for the failing Ethernet port supporting that end ese solutions provide visual and statistical tools necessary to quickly resolve any event or to manage performance in real-time. The BayStack 470 Switches ‘syslog’ capability that helps in troubleshooting network issues.

/ of Service

Stack 470 Switch’s QoS features allow you to not just utilize bandwidth more effi- ptimizing existing network resources and capabilities, but also provide packet tion and marking at the edge of the network—simplifying the QoS deployment gregation and core of the network. By classifying, prioritizing, policing, and LAN traffic, networks can offer reliable connectivity and required bandwidth for critical applications like IP Telephony and mission-critical data applications to groups and users, and to individual devices.

of these applications, advanced QoS features support Internet Engineering Task (IETF) standard DiffServ QoS architecture—a packet classification based on the of packet header fields (voice, video, data), traffic policing, and remote sniffing.

ing function

: 470 Switches provide network availability for mission-critical applications, and users. This is done by classifying, prioritizing, and marking LAN IP traffic to eight hardware-based IP service class queues (on the Gigabit uplink ports) the following parameters:

o SCP marking

o source address/destination address or subnets

o JDP source/destination port/port range

o priority bits

o physical source port

o protocol ID (e.g., TCP, UDP, IGMP, ICMP, RSVP)

o type (e.g., IP, IPX)

o ! ID

The switches have the ability to read packets that have been marked from other devices such as the Passport 8600 Switch. The switches support Strict Priority Queuing as well as the Weighted Round Robin method. The Weighted Round Robin prevents normal priority traffic from being starved by expedited traffic (on a per packet basis).

QoS and policy management

QoS provides the ability to read, alter, prioritize, tag, or mark IP traffic based upon information imbedded in the Type of Service (ToS) field. Based on the IETF Committee's industry standards, BayStack 470 Switches provide the ability to prioritize traffic based upon the required level of service for a given transaction. This level of service can be marked in the embedded information inside each IP packet's ToS field. DiffServ is based upon the ToS field. BayStack 470 Switches have Application Specific Integrated Circuits (ASICs) to enable DiffServ Code points to be mapped to 802.1p. The QoS policies can be configured via the BayStack 470 Switch's built-in Web-based management tools to facilitate QoS or alternatively, Optivity Policy Services can be utilized for dynamic end-to-end enterprise-wide policy and QoS management—facilitated through the Common Open Policy Service (COPS) protocol.

Quality of Service provisioning

With Optivity Policy Services, policies can be created through a simple and intuitive drag-and-drop workflow. Optivity Policy Services is the Policy Decision Point in a DiffServ QoS implementation.

Further benefits include:

- Simple intuitive policy creation
- Ability to re-use common filter sets
- Provision of a network-wide view of policies currently being enforced
- Ability to avoid QoS provisioning errors
- Centrally managed DSCP and 802.1p queue mapping tables
- Saved time in provisioning the network—as thousands of CLI or Web transactions are reduced to a few simple actions

Simplified QoS

The BayStack 470 Switch supports Nortel Networks Service Classes (NNSC), which provide simplified QoS provisioning. NNSCs provide factory-default QoS configurations, eliminating the complexities often associated with QoS-enabled network deployments.

NNSCs provide default settings such as:

- DSCP marking per class
- DiffServ forwarding behavior (PHB) per class
- DSCP to queue mapping
- DSCP to 802.1p mapping
- Default scheduler per class

ifying the traffic and placing it into an NNSC, complex QoS configurations are simplified. NNSCs simplify the deployment of a QoS-enabled network with Nortel switching solutions. Using the Web-based interface, select the NNSC that best fits the type of traffic or application being classified on each Nortel Networks switching device and take advantage of the default QoS settings. This saves on provisioning time and, importantly, ensures that the QoS functions are provisioned consistently across the network.

These NNSCs are also supported on the Passport 8600 Routing Switch, BayStack 470 Switches, and BayStack Business Policy Switch.

traffic policing

Traffic policing enables provisioning of different levels of service by limiting traffic output at the ingress (incoming) port of the BayStack 470 Switch. For example, if a limit is set to a certain speed, such as 10 Mbps, all traffic above 10 Mbps will be dropped or marked with lower priority in the event of congestion. The bandwidth guarantee can be defined in increments as small as 1 kbps. Service providers will find this especially useful to control bandwidth to their customers.

traffic shaping

Traffic shaping offers the ability to smooth IP classified traffic from the Gigabit uplink of a single BayStack 470 Switch. While traffic policing is needed to provide different levels of service to data streams on the ingress ports, traffic shaping is needed to smooth traffic on the uplink connection from the BayStack 470 Switch to the network core, ensuring the most efficient bandwidth utilization. Service providers or carriers utilize this when they are selling Ethernet in place of the traditional Frame Relay, ISDN, or T1/E1 access solutions. Some enterprise customers use traffic shaping as a mechanism to limit bandwidth without having to swap out physical interfaces, leaving them open to grow.

primary

More than 100 years in telecommunications, Nortel Networks is uniquely positioned to help your business reduce cost by combining voice and data into an integrated system. Is there a chance on a vendor that only understands part of the equation? Let us show you how the BayStack 470 Switches, along with other Nortel Networks products, can increase your profitability, streamline your business operations, increase productivity, and help you gain the competitive edge.



Technical specifications

Table 2. BayStack 470 Switches technical specifications

Performance specifications

Switch fabric	2.56 Gbps
Frame forward rate (64-byte packets)	Up to 3.2 million packets per second (pps) maximum, learned unicast traffic
Memory	16 MB SDRAM
Port forwarding/filtering performance (64-byte packets)	For 10 Mbps 14,880 pps maximum For 100 Mbps 148,810 pps maximum
For 1000 Mbps	1,488,100 pps maximum
Address database size	16,000 entries at line rate (32,000 entries without flooding)
Addressing	48-bit MAC address
Frame length	64 to 1518 bytes (IEEE 802.1Q Untagged) 64 to 1522 bytes (IEEE 802.1Q Tagged)

Data rate 10 Mbps Manchester encoded or 100 Mbps 4MB - 5MB encoded

Interface options

10BASE-T/100BASE-TX RJ-45 (8-pin modular) with Auto MDI/MDIX

The BayStack 470 Switches support the following GBICs:

1000BASE-SX	Uses shortwave length 850 nm fiber optic connectors to connect devices over multimode (550 m or 1,805 ft) fiber optic cable
1000BASE-LX	Uses longwave length 1,300 nm fiber optic connectors to connect devices over single mode (5 km or 3.1 mi) or multimode (550 m or 1,805 ft) fiber optic cable
1000BASE-XD	Uses single mode fiber to connect devices over distances up to 40 km (31 mi), depending on the quality of the cable
1000BASE-ZX	Uses single mode fiber to connect devices over distances up to 70 km (43 mi), depending on the quality of the cable. The ports on this GBIC operate only in full-duplex mode.
1000Base-CWDM	Eight GBIC types with 1470-1610nm (in 20nm intervals) with LC connector to connect devices over distances up to 70km

LED indicators

Per-port status LEDs	10 or 100 Mbps port speed, Power over Ethernet detection, link status
System status LEDs	Power, system, RPSU, stack mode, base mode

Network protocol and standards compatibility

IEEE 802.3 10BASE-T (ISO/IEC 8802-3, Clause 14)
IEEE 802.3u 100BASE-TX (ISO/IEC 8802-3, Clause 25)
IEEE 802.3u Autosensing (ISO/IEC 8802-3, Clause 28)
IEEE 802.3x (Flow control on the Gigabit uplink port)
IEEE 802.1p (Prioritizing)
IEEE 802.1Q (VLAN tagging)
IEEE 802.3z (Gigabit)
IEEE 802.1D (Spanning Tree Protocol)
IEEE 802.3ad (Static/dynamic LACP)
IEEE 802.1s¹
IEEE 802.1w¹
IETF DiffServ

¹ Future software release

Technical specifications

2. BayStack 470 Switches technical specifications (continued)

Support

1 (IP); RFC 792 (ICMP); RFC 793 (TCP); RFC 783 (TFTP); RFC 826 (ARP); RFC 768 (UDP);
4 (TELNET); RFC 951 (Bootp); RFC 2236 (IGMPv2); RFC 1112 (IGMPv1); RFC 1945 (HTTP);
RFC 2138 (RADIUS); RFC 1573 (IF-MIB); RFC 894 (IP over Ethernet); RFC 2674 (Q MIB);
30 (Simple NTP); RFC 1213 (MIB-II); RFC 1493 (Bridge MIB); RFC 2863 (Interfaces
MIB); RFC 2665 (Ethernet MIB); RFC 2737 (Entity MIBv2); RFC 2819 (RMON MIB);
57 (RMON); RFC 1271 (RMON); RFC 1157 (SNMP); RFC 2748 (COPS); RFC 2940 (COPS
); RFC 3084 (COPS Provisioning); RFC 2570 (SNMPv3); RFC 2571 (SNMP
works); RFC 2572 (SNMP Message Processing) RFC 2573 (SNMPv3 Applications);
74 (SNMPv3 USM); RFC 2575 (SNMPv3 VACM); RFC 2576 (SNMPv3);

Technical specifications

voltage (AC version) 100-240 VAC @ 47 to 63 Hz
power consumption (AC version) 90 W max.
current (AC version) 1.0 A @ 100 VAC, 0.5 A @ 240VAC

Physical specifications

Weight: 4.8 kg (10.56 lb) for -24T, 5.0 kg (11.0 lb) for -48T
Height: 4.37 cm (1.72 inches)
Width: 43.82 cm (17.25 inches)
Depth: 35.29 cm (13.89 inches)

Environmental specifications

Operating temperature: 0° to 40°C (32° to 104°F)
Storage temperature: -25° to +70°C (-13° to 158°F)
Operating humidity: 85% maximum relative humidity, non-condensing
Storage humidity: 95% maximum relative humidity, non-condensing
Operating altitude: Up to 3,024 m (10,000 ft) above sea level
Storage altitude: Up to 12,096 m (40,000 ft) above sea level

Agency approvals

UL60950
Canada, CAN/CSA-22.2 No.60950
Europe, EN60950/IEC 60950, CB report with all national deviation
Australia/New Zealand, AS/NZS 60950
Japan, NOM-019

Electromagnetic emissions summary

Complies with the following standards USA, FCC CFR47 Part 15, subpart B, Class A
Canada, ICES-003, Class A
Europe, EN55022, CISPR 22, Class A
Australia/New Zealand, AS/NZS 3548, Class A
Japan, VCCI-V-3/02.04, Class A
China, CNS 13438, Class A

Electromagnetic immunity

Complies with EN55024, CISPR 24

ing information

BayStack 470 Switches ordering information

Order Code	Description
34	BayStack 470-48T Switch 48 10/100BASE-TX Ports Plus 2 Built-in GBIC Ports and Built-in Stacking Ports (18 in. Stacking Cable Included)
37	BayStack 470-24T Switch 24 10/100BASE-TX Ports Plus 2 Built-in GBIC Ports and Built-in Stacking Ports (18 in. Stacking Cable Included)
005	-48 V DC-to-DC converter for BayStack 470 for use with BayStack 10 Power Supply System
001	BayStack 400-SRC Cascade Return Cable (1 meter)
002	BayStack 400-SSC Spare Cascade Cable (18 inch)
004	BayStack 400-SRC Cascade Return Cable (3 meter)
013	Console cable for BayStack Switches and Passport 8300 Switch
001	1-port 1000BASE-SX Gigabit Interface Connector (GBIC), SC connector
002	1-port 1000BASE-LX Gigabit Interface Connector (GBIC), SC connector
003	1-port 1000BASE-XD Gigabit Interface Connector (GBIC) -40km SC connector
004	1-port 1000BASE-ZX Gigabit Interface Connector (GBIC) -70km SC connector
042	1-port 1000Base-T Gigabit Interface Converter (GBIC) with 8-pin modular RJ-45 connector
017	1000BaseCWDM Gigabit Interface Connector (GBIC), 1470nm - 70km SC connector
018	1000BaseCWDM Gigabit Interface Connector (GBIC), 1490nm - 70km SC connector
019	1000BaseCWDM Gigabit Interface Connector (GBIC), 1510nm - 70km SC connector
020	1000BaseCWDM Gigabit Interface Connector (GBIC), 1530nm - 70km SC connector
021	1000BaseCWDM Gigabit Interface Connector (GBIC), 1550nm - 70km SC connector
022	1000BaseCWDM Gigabit Interface Connector (GBIC), 1570nm - 70km SC connector
023	1000BaseCWDM Gigabit Interface Connector (GBIC), 1590nm - 70km SC connector
024	1000BaseCWDM Gigabit Interface Connector (GBIC), 1610nm - 70km SC connector

seventh character (?) of the switch order number must be replaced with the proper code to indicate desired product nationalization:

power cord included

ides European "Schuko" power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden

ides power cord commonly used in the United Kingdom and Ireland

ides power cord commonly used in Japan

ides North American power cord

ides Australian power cord, also commonly used in New Zealand and the People's Republic of China

In the United States:
Nortel Networks
35 Davis Drive
Research Triangle Park, NC 27709 USA

In Canada:
Nortel Networks
8200 Dixie Road
Suite 100
Brampton, Ontario L6T 5P6 Canada

In Caribbean and Latin America:
Nortel Networks
1500 Concorde Terrace
Sunrise, FL 33323 USA

In Europe:
Nortel Networks
Maidenhead Office Park
Westacott Way
Maidenhead Berkshire SL6 3QH UK

In Asia:
Nortel Networks Asia
Level 5, 495 Victoria Avenue
Chatswood, NSW, 2067, Australia
Phone: +61 2 8870 5200

Nortel Networks is an industry leader and innovator focused on transforming how the world communicates and exchanges information. The company is supplying its service provider and enterprise customers with communications technology and infrastructure to enable value-added IP data, voice and multimedia services spanning Wireless Networks, Wireline Networks, Enterprise Networks, and Optical Networks. As a global company, Nortel Networks does business in more than 150 countries. More information about Nortel Networks can be found on the Web at:

www.nortelnetworks.com

For more information, contact your Nortel Networks representative, or call 1-800-4 NORTEL or 1-800-466-7835 from anywhere in North America.

*Nortel Networks, the Nortel Networks logo, the globemark design, BayServe, BayStack, and Optivity are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2004 Nortel Networks.

All rights reserved. Information in this document is subject to change without notice.

Nortel Networks assumes no responsibility for any errors that may appear in this document.

NN100100-061704

NORTEL
NETWORKS

BUSINESS WITHOUT BOUNDARIES

APPENDIX E
PRODUCT BRIEF: BUSINESS POLICY SWITCH



This PDF is presented by Super Warehouse. All copyrights and trademarks are the property of their respective holders.

We are here to serve you:

For further information or if you would like to purchase this product, please call us during business hours Monday-Friday from 6am-6pm PST; or you can purchase 24/7 on our site.

Contact Info:

Visit us on the web: <http://www.superwarehouse.com>

Email an expert sales associate: sales@superwarehouse.com

Call Us Toll Free: 1-800-814-5410 Intl: 1-619-216-3465
Press Ext. 1 for Sales

About Super Warehouse:

- Over 50,000 brand name computer hardware and software products
- Discount prices
- Friendly and knowledgeable staff
- Five star customer service
- Free shipping on select orders
- Proudly serve business, education, and government clients
(we ship to APO/AP and AE addresses)
- 16 warehouses throughout the country
- 99% of orders shipped the same day
- Fedex overnight and even same day shipping available
- In business since 1997
- CNET certified merchant
- Clients we have served include virtually all fortune 500 companies, the US military, thousands of schools, colleges and universities, and municipal, state, and federal government organizations



Business Policy Switch

Business Policy Switch

- policy management
- web-based management
- traffic policing and shaping
- up to 8 switches
- with BayStack 450/410
- stacking & resiliency

Single Business Policy Switch.



Business Advantages

QoS is becoming increasingly necessary as more of an organization's critical business runs over the network infrastructure. When you implement the Nortel Networks Business Policy Switch QoS features in your network, you can utilize bandwidth more efficiently, optimizing your existing network resources and capabilities.

The Business Policy Switch makes sound business sense for companies looking to improve productivity to maintain or increase profits. If the network is congested or down, if sales people cannot submit orders, if e-mail and intranet traffic threatens on-line web transactions, and if new applications like voice and video fail, your business could be negatively

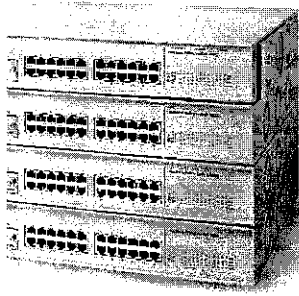
impacted. The Business Policy Switch with QoS gives you the performance, features and tools you need to manage bandwidth and so that your network is always ready and available for the most critical business transactions.

Product Overview

Nortel Networks Business Policy Switch (BPS) is a high-density, stackable 10/100 Mbps Ethernet Layer 2 switch that delivers Layer 2/3/4 packet classification and prioritization to the desktop (see Figure 1 and 2). The Business Policy Switch is a robust and highly reliable LAN solution, with advanced Quality of Service IP capabilities and web-based management

NORTEL
NETWORKS

Business Policy Switch Stack.



With the Business Policy Switch, users and carriers are able to easily and reliably deploy and support critical, resource-intensive or tolerant network communications that can include voice over IP, media and e-Business applications and bandwidth utilization and assured access at the premise.

By classifying, prioritizing, policing and metering (DiffServ Code Point /ToS Byte) traffic, networks can offer reliability and required bandwidth for critical applications like Voice over IP to specific groups and users, and support dual devices.

For all of these applications, advanced features support IETF standard DiffServ QoS architecture, packet scheduling based on the contents of header fields (voice, video, data),

traffic policing, and remote sniffing. As a result, optimal network performance and reliability may be attained while realizing significant cost-savings.

Customized service type and flow-based administrations through traffic-shaping and policing may also be established, providing an opportunity for customer-specific service offerings, which can be implemented to address-specific and unique customer requirements.

High Density Architecture

The Business Policy Switch has twenty-four 10/100 BASE-TX RJ-45 ports, one MDA slot, and a cascade module slot for stacking. Up to eight Business Policy Switches can be stacked to achieve up to 224 10/100 ports (using 4-port 10/100 BASE-TX MDA on each switch). The 2.5 Gigabit cascading bandwidth offers dedicated bandwidth between switches without sacrificing any uplink ports. The uplink ports can be used for connections to backbone switches such as the Passport 8000 routing switches.

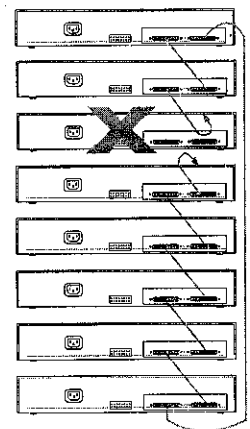
Wire-Speed Performance

2.5 Gigabit per second (Gbps) switching fabric and custom switching ASICs support full 802.1D-compliant MAC Layer frame forwarding and filtering across all ports at the peak rate of 3 million packets per second for the Business Policy Switch.

Stackable with BayStack 450/410 Switches

The Business Policy Switch can also be stacked with the BayStack 450 or 410 Switches providing policy to users or devices that are connected on the Business Policy Switch. With the addition of one Business Policy Switch to an existing BayStack 450 or 410 stack, web-based management can be achieved for the whole stack (see Figure 3). A maximum of eight switches can be stacked together in any combination of Business Policy Switch/BayStack 450/BayStack 410.

Figure 4: In the unlikely event of a switch failure, the stack integrity is maintained: cascade signals loop back at point of failure.

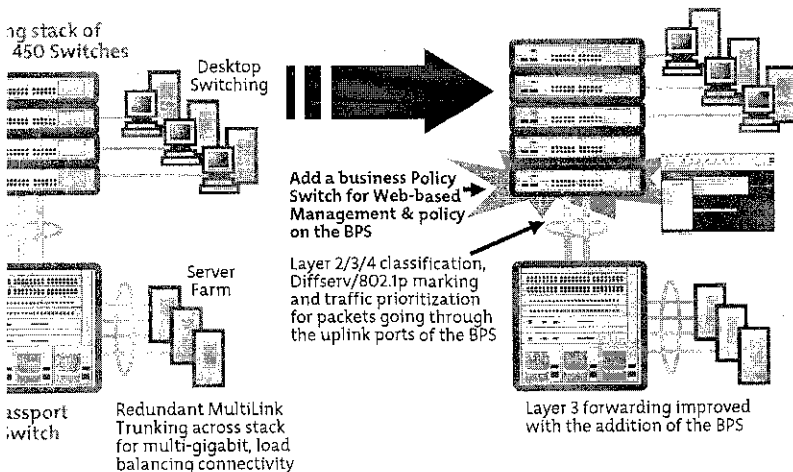


Resiliency

A key differentiation for the Business Policy Switch is its resilient stacking feature. The Business Policy Switch can stack up to 8 units with a cascade stacking design, assuring continuous uptime even if any switch in the stack should fail. A loop-back or cascade cable is used to seamlessly connect the entire stack to provide no single point of failure (see Figure 4).

For redundant power supply support and UPS support for the Business Policy Switch, a -48V DC-to-DC converter module (AL1904001) must be ordered for connectivity to the BayStack 10 Power Supply System.

Web-based management with Business Policy Switch.



DC Versions

Business Policy Switch is available in AC power supply or with a -48V DC power supply suitable for carriers. The AC version has the same features as the DC version except for redundant power supply unit (RPSU) support.

Policy Management

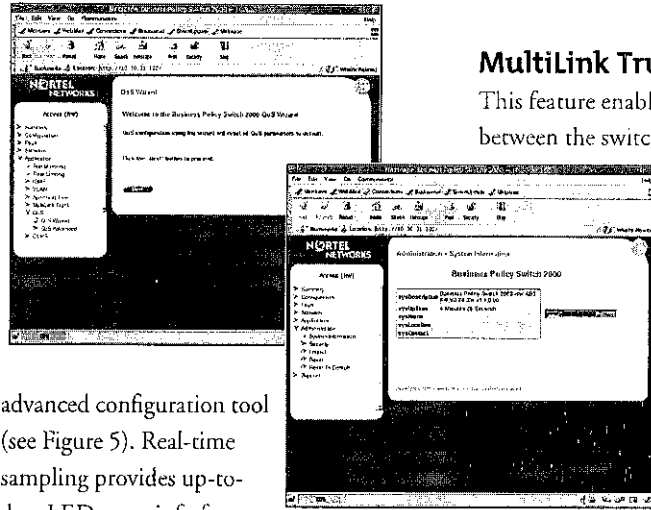
Business Policy Switch provides the ability to read, alter, add, and tag or mark IP traffic based on information imbedded in Type of Service (ToS). Based on the IETF DiffServ's industry standards, the Business Policy Switch provides the ability to prioritize traffic based upon a desired level of service for a given application. This level of service can be defined in the embedded information in each IP packet's Type of Service field. DiffServ is based upon Type of Service (ToS) field. The Business Policy Switch provides application specific integrated ASICs to enable DiffServ Code Points to be mapped to 802.1p.

Business policies can be configured on Business Policy Switch built-in Management tools to facilitate configuration. Alternatively, Optivity* Policy Manager can be utilized for dynamic enterprise-wide policy and QoS management, which is facilitated through common Open Policy Support protocol.

Stacked management

Business Policy Switch supports stacked management. Business Policy Switch only stack or a stack of Business Policy Switches stack 450/410 Switches. This provides summary, configuration, statistics, application, administration report pages for entire stack. Traffic classification and prioritization can be set through Web-based QoS Wizard and

Figure 5: Business Policy Switch features flexible HTML tools.



advanced configuration tool (see Figure 5). Real-time sampling provides up-to-date LED, stats info for stacked units. Web interface also allows for static configuration of numerous parameters of the device.

Queuing Function

The Business Policy Switch provides network availability for mission-critical applications, devices, and users. This is done by classifying, prioritizing, and marking LAN IP traffic using four hardware-based IP service class queues on a per-port basis based on the following parameters:

- ToS / DSCP marking
- IP source address/destination address or subnets
- TCP/UDP source/destination port/port range
- 802.1p priority bits
- Ingress source port
- IP protocol ID (e.g. TCP, UDP, IGMP)
- EtherType (e.g. IP, IPX)
- VLAN ID

It also has the ability to read packets that have been marked from other devices such as the Passport 8000 routing switch. Also, weighted round robin prevents normal priority traffic from being starved by expedited traffic (on a per-packet basis).

MultiLink Trunking

This feature enables grouping of links between the switch and another switch

or a server to provide higher bandwidth of up to 800 Mbps (when used with 10/100 ports or 100BASE-FX ports) or up to 8 Gigabits per second (when used with Gigabit uplink ports on

Business Policy Switches) with active redundant links.

Distributed MultiLink Trunking enables trunked ports to span multiple units of the stack for fail-safe connectivity to mission critical servers and the network center.

Flexible High-Speed Uplink Options

Media Dependant Adapters (MDAs) including Fast Ethernet, Gigabit Ethernet and fiber, connect to Passport routing switches, other high-speed switches, or the network center. Also, the BayStack 450-1GBIC (Gigabit Interface Connector) MDA to supports long-haul connectivity. This GBIC MDA will support one of the following interface connectors: 1000BASE-SX, 1000BASE-LX, 1000BASE-XD (40km), or 1000BASE-ZX (70km). This GBIC MDA also supports CWDM (Coarse Wave Division Multiplexing) GBICs.

With CWDM, a customer can dramatically increase the bandwidth supported over a single fiber. Instead of 1 gigabit per fiber connection with a CWDM GBIC, eight wavelengths can be supported per fiber. In other words, eight gigabits of traffic can be supported across one single mode fiber.

ty

re allows authentication of , not only to the switches for nent and configurations, but the infrastructure through these . This software feature limits ly to network authorized and sers with full tracking of network ons. With BaySecure, network granted or denied network by fAC address (maximum of 448) tion. In addition, with the ed Access List Security feature, access is granted or denied on s. The Business Policy Switch ides Radius authentication for urity management.

rt for EAP

greater security, the Business itch also supports Extensible ation Protocol (EAP). Based EE 802.1x standard, EAP limits the network based on user ls. A user needs to "login" to rk using username/password; atabase is maintained on the ation server (not the switch). ents network connectivity assword authorization for urity and control in physically re areas. It is used where the is not 100% physically secure or ysical security needs enhancement. ple, banks, trading rooms, or 1 training facilities could take e of this feature. EAP supports ess to the network and interop- h Microsoft Windows XP.

Traffic Policing

This feature enables provisioning of different levels of service by limiting traffic throughput at ingress (incoming) port of the Business Policy Switch. For example, if a port is set to certain speed such as 10 Mbps, all traffic under 10 Mbps on that port will pass and traffic that exceeds 10 Mbps on that same port is dropped. Service providers will especially find this useful to control bandwidth to their customers.

MAC Addresses

Business Policy Switches support up to 16,000 MAC addresses per switch or stack for deployment of large-scale enterprise networks with many attached devices and workgroups.

VLAN Support

Up to 256 port-based VLANs can be established for each switch, to extend the broadcast domain and segment network traffic. The 256 VLANs can be spread among port-based, and MAC source address-based VLANs (maximum of 48 MAC source address-based VLANs). The 256 VLANs can be on a standalone switch or across a pure Business Policy Switch stack only. Protocol-based VLANs allow switch ports to be assigned to a broadcast domain, based on the protocol information within the packet. These VLANs can localize broadcast traffic and assure that the specified protocol type packets are sent only to the protocol-based VLAN ports.

Shared VLAN (SVL) and individual VLAN (IVL) learning is supported. SVL is the same as the VLAN implementation on the BayStack 450 Switch, in which all VLANs in the switch share the same forwarding database. IVL is new feature on the Business Policy Switch and lets individual VLANs have separate forwarding databases within the switch. IVL allows the switch to handle duplicate MAC addresses if they are in different VLANs

IGMP Snooping

The Business Policy Switch features IP MultiCast support by examining ('snooping') all IGMP traffic in hardware at line rate, and pruning unwanted data streams from affecting network or endstation performance.

Network Management

The Business Policy Switch supports 4 groups of RMON on all ports. The SNMP agent software resides in the switch and uses the information it collects to provide management for all ports in the stack. In addition, the agent also provides the ability to set up policy-based networks by supporting the Common Open Policy Support, or COPS, protocol. With Optivity Policy Services, policies can be created through a simple intuitive drag and drop workflow. Using Optivity Policy Services, common policies can be implemented across many Business Policy Switches through a single command instead of hours of filter configuration.

Command Line Interface (CLI)

Business Policy Switch offers a Command Line Interface (CLI) management system. CLI commands can be issued through the serial port of the switch or through a Telnet session.

Multiple Spanning Tree Protocol Groups (Up to 8)

Business Policy Switch supports multiple spanning tree groups (STGs). It supports a maximum of 8 STGs, either all in one standalone switch or across a stack consisting of Business Policy Switches only. Multiple STGs provide multiple data paths, which can be used for load-balancing and redundancy.

Configuration File

Business Policy Switch can download a downloadable ASCII configuration file from a TFTP server. The ASCII configuration file can be loaded automatically at boot time or on demand by management systems (console or CLI). Once downloaded, the configuration file automatically configures the switch or stack according to the commands in the file. This feature provides the flexibility of creating command configuration files that can be used on switches or stacks with minor modifications.

Access List

To limit access to the management of the Business Policy Switch by the IP addresses allowed access to the switch.

Version 2.0 Features

Gigabit Ethernet MDAs

Version 2.0 software, the Business Policy Switch will support three new Gigabit Ethernet MDAs. Each of these MDAs will support 3 output queues and support traffic shaping. The three MDAs are:

1000-1GT 1-port 1000BASE-TX

1000-2GT 2-port 1000BASE-TX

1000-2GE 2-port Small Form Factor GBIC MDA

With the dual-port small form factor GBIC MDA, you can plug up to two small form factor pluggable GBICs. There are three types of small form factor pluggable GBICs to choose from:

- 1-port 1000BASE-SX Small Form Factor GBIC (LC connector)
- 1-port 1000BASE-SX Small Form Factor GBIC (MT-RJ connector)
- 1-port 1000BASE-LX Small Form Factor GBIC (LC connector)

Also, new CWDM small form factor pluggable GBICs can also be used with the two-port small form factor GBIC MDA. There will be eight different wavelength GBIC options for 40 km and eight different wavelength GBIC options for 70 km.

Traffic Shaping

Traffic shaping offers the ability to smooth traffic from egress (exiting) ports of the new Gigabit Ethernet MDAs of the Business Policy Switch. While traffic policing is needed to provide different levels of service to data streams on the ingress ports, traffic shaping is needed to smooth the traffic on the uplink connection from BPS to the network core, yielding the most efficient bandwidth utilization. The primary customers for rate shaping are service providers or carrier customers that are selling Ethernet in place of the traditional Frame Relay, ISDN, or ATM WAN access solutions, providing end-to-end Ethernet service for simplicity. Some enterprise customers use traffic shaping as a mechanism to limit bandwidth without having to swap out physical interfaces, leaving them room to grow.

Business Policy Switch

Applications and Solutions

Nortel Networks Business Policy Switch is ideal for enterprise & carrier networks where business applications drive the need to implement and support resource-intensive and delay-intolerant converged voice, video and data applications, devices and users on their network. Businesses implementing applications like voice over IP, video streaming, and e-commerce need more than "best effort" service. Because the Business Policy Switch supports a wide range of applications you can deploy it in your network where you need it most, optimizing your existing network resources.

Summary

With more than 100 years in telecommunications, Nortel Networks is uniquely positioned to help your business reduce cost by combining voice and data into an integrated system. Why take a chance on a vendor that only understands part of the equation? Let us show you how the Business Policy Switch along with other Nortel Networks products, can increase your profitability, streamline your business operations, increase productivity and help you gain the competitive edge.

Technical Specifications

Business Policy Switch Technical Specifications.

Physical Specifications

Weight	4.8 kg (10.60 lb)
Height	7.04 cm (2.77 in.)
Width	43.82 cm (17.25 in.)
Depth	38.35 cm (15.1 in.)

Performance Specifications

Name Forward Rate (64-byte packets)	Up to 3.2 million packets per second (pps) maximum, learned unicast traffic
Port Forwarding/Filtering Performance	For 10 Mb/s: 14,880 pps (64-byte packets) maximum For 100 Mb/s: 148,810 pps maximum
Address Database Size	16,000 entries at line rate (32,000 entries without flooding)
Addressing	48-bit MAC address
Name Length	64 to 1518 bytes (IEEE 802.1Q Untagged) 64 to 1522 bytes (IEEE 802.1Q Tagged)
Bit Rate	10Mb/s Manchester encoded or 100 Mb/s 4B/5B encoded

Interface Options

BASE-T/100BASE-TX	RJ-45 (8-pin modular) connectors for MDI-X interface
100BASE-FX	SC and MT-RJ connectors for switched 100 Mb/s (100BASE-FX) connections over 50/125 and 62.5/125 micron multimode fiber optic cable (2 km/6562 ft. maximum distance)
100BASE-SX (Shortwave Gigabit Fiber) MDA	SC connectors for shortwave 850 nm fiber optic connections over multimode 550 m/1805 ft.) fiber optic cable
100BASE-LX (Longwave Gigabit Fiber) MDA	SC connectors for longwave 1300 nm fiber optic connections over single-mode (3km/9843 ft.) or multimode (550m/1805 ft.) fiber optic cable

BayStack 450-1GBIC MDA supports the following GBICs:

100BASE-SX	Uses shortwave 850 nm fiber optic connectors to connect devices over multimode (550 m or 1,805 ft) fiber optic cable.
100BASE-LX	Uses longwave 1,300 nm fiber optic connectors to connect devices over single mode (5 km or 3.1 mi) or multimode (550 m or 1,805 ft) fiber optic cable.
100BASE-XD	Uses single mode fiber to connect devices over distances up to 40 km (or 31 mi), depending on the quality of the cable.
100BASE-ZX	Uses single mode fiber to connect devices over distances up to 70 km (or 43 mi), depending on the quality of the cable. The ports on this GBIC operate only in full-duplex mode.

Business Policy Switch Technical Specifications (continued).

ork Protocol and Standards Compatibility IEEE 802.3 10BASE-T (ISO/IEC 8802-3, Clause 14)
IEEE 802.3u 100BASE-TX (ISO/IEC 8802-3, Clause 25)
IEEE 802.3u 100BASE-FX (ISO/IEC 8802-3, Clause 26)
IEEE 802.1p (Prioritizing)
IEEE 802.1Q (VLAN Tagging)
IEEE 802.1z (Gigabit)
IETF DiffServ

MIB Support RFC 1493 (Bridge)
RFC 1643 (Ethernet)
RFC 1757 (RMON)
RFC 1213 (MIB II)
RFC 2233 (Interface)
RFC 2271-RFC 2275 (SNMP v3)
RFC 2037 (Entity)

ical Specifications

out voltage (AC Version) 100-240VAC @ 47 to 63 Hz
out voltage (DC Version) -48 Volts DC
out Power consumption (AC Version) 150 W max
out Power consumption (DC Version) 130 W max
out Volt Amperes Rating (AC Version) 200VA max
out current (AC Version) 1.5 A @100 VAC, .6 A @240VAC
out current (DC Version) -48 Volts DC @ 2.75 Amps

onmental Specifications

erating temperature 0 °to 40 °C (32 °to 104 °F)
orage temperature -25 °to +70 °C (-13 °to 158 °F)
erating humidity 85%maximum relative humidity, non-condensing
orage humidity 95%maximum relative humidity, non-condensing
erating altitude Up to 3024 m (10,000 ft.)
orage altitude Up to 3024 m (10,000 ft.)

Agency Approvals

UL Listed (UL 1950)
IEC 950/EN60950
C22.2 No.950 (CUL) with all national deviations
UL-94-V1 flammability requirements for PC board
NOM (NOM-019)

Business Policy Switch Technical Specifications (continued).

Electromagnetic Emissions Summary

Meets the following standards

- US, CFR47, Part 15, Subpart B, Class A
- Canada, ICES-003, Issue 2, Class A
- Australia/New Zealand, AS/NZS 3548:1995, Class A
- Japan, V-3/97.04:1997, Class A
- Taiwan, CNS 13438, Class A
- EN55022:1995, Class A
- EN61000-3-2:1995
- EN61000-3-3:1994

Electromagnetic Immunity

Meets the EN 50082-1:1997 standard

Ordering Information

Business Policy Switch Ordering Information.

No.	Description
31x15*	Business Policy Switch 2000 Autosensing Policy Switch (24 10/100BASE-TX plus 1 MDA Slot and 1 Cascade Module Slot)
31016	Business Policy Switch 2000 DC (-48V DC built-in power supply version)
33011	BPS2000-4TX 4-port 10/100 MDA
33012	BPS2000-4FX 4-port 100BASE-FX MDA w/mini MT-RJ-type connectors
33013	BPS2000-2FX 2-port 100BASE-FX MDA w/SC-type connectors
34001	BPS -48 V DC-to-DC converter for use with BayStack 10 Power Supply System
8001	BayStack 400-SRC Cascade Return Cable (1 meter)
8002	BayStack 400-SSC Spare Cascade Cable (18 inch)
8004	BayStack 400-SRC Cascade Return Cable (3 meter)
33010	BayStack 400-ST1 Cascade Module (includes cascade cable)
33005^	BayStack 450-1SX 1-port 1000BASE-SX Single PHY MDA
33006^	BayStack 450-1SR 1-port 1000BASE-SX Redundant PHY MDA
33007^	BayStack 450-1LX 1-port 1000BASE-LX Single PHY MDA
33008^	BayStack 450-1LR 1-port 1000Base-LX Redundant PHY MDA
33009**	BayStack 450-1GBIC MDA (GBIC not included with MDA)
9001~	1-port 1000BASE-SX Gigabit Interface Connector (GBIC), SC connector
9002~	1-port 1000BASE-LX Gigabit Interface Connector (GBIC), SC connector
9003~	1-port 1000BASE-XD Gigabit Interface Connector (GBIC)-40km, SC connector
9004~	1-port 1000BASE-ZX Gigabit Interface Connector (GBIC)-70km, SC connector
9005~	1-port 1000BASE-WDM Gigabit Interface Connector (GBIC) – 1470nm Wavelength, SC connector
9006~	1-port 1000BASE-WDM Gigabit Interface Connector (GBIC) – 1490nm Wavelength, SC connector
9007~	1-port 1000BASE-WDM Gigabit Interface Connector (GBIC) – 1510nm Wavelength, SC connector

Business Policy Switch Ordering Information (continued).

No.	Description
9008~	1-port 1000BASE-WDM Gigabit Interface Connector (GBIC) – 1530nm Wavelength, SC connector
9009~	1-port 1000BASE-WDM Gigabit Interface Connector (GBIC) – 1550nm Wavelength, SC connector
9010~	1-port 1000BASE-WDM Gigabit Interface Connector (GBIC) – 1570nm Wavelength, SC connector
9011~	1-port 1000BASE-WDM Gigabit Interface Connector (GBIC) – 1590nm Wavelength, SC connector
9012~	1-port 1000BASE-WDM Gigabit Interface Connector (GBIC) – 1610nm Wavelength, SC connector
33014***	BPS2000-1GT 1-port 1000BASE-TX MDA
33015***	BPS2000-2GT 2-port 1000BASE-TX MDA
33016***	BPS2000-2GE 2-port Small Form Factor GBIC MDA (supports up to two Small Form Factor GBICs)
9013	1-port 1000BASE-SX Small Form Factor GBIC (LC connector)
9014	1-port 1000BASE-SX Small Form Factor GBIC (MT-RJ connector)
9015	1-port 1000BASE-LX Small Form Factor GBIC (LC connector)
9025	1-port 1000BASE-CWDM Small Form Factor GBIC – 1470nm Wavelength (40km), LC connector
9026	1-port 1000BASE-CWDM Small Form Factor GBIC – 1490nm Wavelength (40km), LC connector
9027	1-port 1000BASE-CWDM Small Form Factor GBIC – 1510nm Wavelength (40km), LC connector
9028	1-port 1000BASE-CWDM Small Form Factor GBIC – 1530nm Wavelength (40km), LC connector
9029	1-port 1000BASE-CWDM Small Form Factor GBIC – 1550nm Wavelength (40km), LC connector
9030	1-port 1000BASE-CWDM Small Form Factor GBIC – 1570nm Wavelength (40km), LC connector
9031	1-port 1000BASE-CWDM Small Form Factor GBIC – 1590nm Wavelength (40km), LC connector
9032	1-port 1000BASE-CWDM Small Form Factor GBIC – 1610nm Wavelength (40km), LC connector
9033	1-port 1000BASE-CWDM Small Form Factor GBIC – 1470nm Wavelength (70km), LC connector
9034	1-port 1000BASE-CWDM Small Form Factor GBIC – 1490nm Wavelength (70km), LC connector
9035	1-port 1000BASE-CWDM Small Form Factor GBIC – 1510nm Wavelength (70km), LC connector
9036	1-port 1000BASE-CWDM Small Form Factor GBIC – 1530nm Wavelength (70km), LC connector
9037	1-port 1000BASE-CWDM Small Form Factor GBIC – 1550nm Wavelength (70km), LC connector
9038	1-port 1000BASE-CWDM Small Form Factor GBIC – 1570nm Wavelength (70km), LC connector
9039	1-port 1000BASE-CWDM Small Form Factor GBIC – 1590nm Wavelength (70km), LC connector
9040	1-port 1000BASE-CWDM Small Form Factor GBIC – 1610nm Wavelength (70km), LC connector

The character (x) of the switch order number must be replaced with the proper code to indicate desired product nationalization:
 ~ Power cord included; "B" – Includes European "Schuko" power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden;
 S power cord commonly used in the United Kingdom and Ireland; "D" – Includes power cord commonly used in Japan; "E" – Includes North American power cord;
 I Australian power cord, also commonly used in New Zealand and the People's Republic of China.
 50 Gigabit MDAs are fully supported by the Business Policy Switch but they utilize only two hardware based DiffServ queues
 Business Policy Switch version 1.1 software or higher; supports two hardware based DiffServ queues
 ~ GBICs can be installed in the BayStack 450-1GBIC MDA
 Business Policy Switch version 2.0 software or higher; supports eight hardware based DiffServ queues



For more information, contact your Nortel Networks representative or call 1-800-4-NORTEL (1-800-467-8335), or 1-506-674-5470 outside of North America.

www.nortelnetworks.com

United States
Nortel Networks
100 America Parkway
Burlington, MA 01803
Tel: 978-674-2288

Canada
Nortel Networks
1000 University Avenue, Suite 100
Toronto, Ontario
M5G 1R2
Canada
Tel: 416-783-3333

Middle East, and Africa
Nortel Networks EMEA, S.A.
Immeuble Naxos
10 rue Ziller
92000 Paris
France
Tel: 33-1-47-96-6666

Asia Pacific
Nortel Networks
27/F City Plaza One
1111 King's Road
Quarry Bay
Hong Kong
Tel: 852-2100 2888

Caribbean and Latin America
Nortel Networks CALA Inc
1500 Concord Terrace
Sunrise, FL 33323-2815
Tel: 954-851-8000

© 2002 Nortel Networks. All Rights Reserved.
Nortel, the Nortel Networks logo, the Gloemark, and Passport, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for any errors or omissions that may appear in this document.

11019.02/01-02

APPENDIX F

PROTOCOL ANALYZER DECODES ANALYSIS DATA

Record #1308 (From Hub To Node) Captured on 10.13.04 at 16:37:44.800534300 Length
= 64
Runtime Frame# 1308

----- ETHER Header -----

ETHER: Destination: Intrnt-00-00-01 (01-00-5E-00-00-01)
ETHER: Source: 00-04-38-13-41-60
ETHER: Protocol: IP
ETHER: FCS: E2D21F08

----- IP Header -----

IP: Version = 4
IP: Header length = 20
IP: Differentiated Services (DS) Field = 0xC0
IP: 1100 00.. DS Codepoint = Class Selector Codepoint (48)
IP:00 Unused
IP: Packet length = 28
IP: Id = 0
IP: Fragmentation Info = 0x0000
IP: .0.. Don't Fragment Bit = FALSE
IP: ..0. More Fragments Bit = FALSE
IP: ...0 0000 0000 0000 Fragment offset = 0
IP: Time to live = 1
IP: Protocol = IGMP (2)
IP: Header checksum = 471F (Verified 471F)
IP: Source address = 160.0.226.2
IP: Destination address = 239.255.255.254

----- IGMP Header -----

IGMP: Message Type = Membership Query (17)
IGMP: Max Response Time = 5 (in 1/10 seconds)
IGMP: Header checksum = 0xFEFB (Verified 0xFEFB)
IGMP: Group Address = 239.255.255.254

Record #1308 (From Hub To Node) Captured on 10.13.04 at 16:37:44.800534300 Length
= 64

```
01 00 5e 00 00 01 00 04    38 13 41 60 08 00 45 c0    ..^..... 8.A'..E.  
00 1c 00 00 00 01 02    47 1f a0 00 e2 02 ef ff    ..... G.....  
ff fe 11 05 fe fb ef ff    ff fe 00 00 00 00 00    .....  
00 00 00 00 00 00 00    00 00 00 00 e2 d2 1f 08    .....
```

Record #1309 (From Hub To Node) Captured on 10.13.04 at 16:37:44.899709700 Length
= 64
Runtime Frame# 1309

----- ETHER Header -----

ETHER: Destination: Intrnt-00-00-01 (01-00-5E-00-00-01)
ETHER: Source: 00-04-38-13-41-60
ETHER: Protocol: IP
ETHER: FCS: AACD9B7A

----- IP Header -----

IP: Version = 4
IP: Header length = 20
IP: Differentiated Services (DS) Field = 0xC0
IP: 1100 00.. DS Codepoint = Class Selector Codepoint (48)
IP:00 Unused
IP: Packet length = 28
IP: Id = 0
IP: Fragmentation Info = 0x0000
IP: .0.. Don't Fragment Bit = FALSE
IP: ..0. More Fragments Bit = FALSE
IP: ...0 0000 0000 0000 Fragment offset = 0
IP: Time to live = 1
IP: Protocol = IGMP (2)
IP: Header checksum = 5605 (Verified 5605)
IP: Source address = 160.0.226.2

IP: Destination address = 224.0.1.24

----- IGMP Header -----
IGMP: Message Type = Membership Query (17)
IGMP: Max Response Time = 5 (in 1/10 seconds)
IGMP: Header checksum = 0x0DE2 (Verified 0x0DE2)
IGMP: Group Address = 224.0.1.24

Record #1309 (From Hub To Node) Captured on 10.13.04 at 16:37:44.899709700 Length = 64

```
01 00 5e 00 00 01 00 04 38 13 41 60 08 00 45 c0 ..^..... 8.A`..E.  
00 1c 00 00 00 00 01 02 56 05 a0 00 e2 02 e0 00 ..... V.....  
01 18 11 05 0d e2 e0 00 01 18 00 00 00 00 00 00 .....  
00 00 00 00 00 00 00 00 00 00 00 00 aa cd 9b 7a .....z
```

Record #3392 (From Hub To Node) Captured on 10.13.04 at 16:41:56.314742300 Length = 64

Runtime Frame# 3392

----- ETHER Header -----
ETHER: Destination: Intrnt-00-00-01 (01-00-5E-00-00-01)
ETHER: Source: 00-04-38-13-41-60
ETHER: Protocol: IP
ETHER: FCS: E2D21F08

----- IP Header -----
IP: Version = 4
IP: Header length = 20
IP: Differentiated Services (DS) Field = 0xC0
IP: 1100 00.. DS Codepoint = Class Selector Codepoint (48)
IP:00 Unused
IP: Packet length = 28
IP: Id = 0
IP: Fragmentation Info = 0x0000
IP: .0.. Don't Fragment Bit = FALSE
IP: ..0. More Fragments Bit = FALSE
IP: ...0 0000 0000 0000 Fragment offset = 0
IP: Time to live = 1
IP: Protocol = IGMP (2)
IP: Header checksum = 471F (Verified 471F)
IP: Source address = 160.0.226.2
IP: Destination address = 239.255.255.254

----- IGMP Header -----
IGMP: Message Type = Membership Query (17)
IGMP: Max Response Time = 5 (in 1/10 seconds)
IGMP: Header checksum = 0xFEFB (Verified 0xFEFB)
IGMP: Group Address = 239.255.255.254

Record #3392 (From Hub To Node) Captured on 10.13.04 at 16:41:56.314742300 Length = 64

```
01 00 5e 00 00 01 00 04 38 13 41 60 08 00 45 c0 ..^..... 8.A`..E.  
00 1c 00 00 00 00 01 02 47 1f a0 00 e2 02 ef ff ..... G.....  
ff fe 11 05 fe fb ef ff ff fe 00 00 00 00 00 00 .....  
00 00 00 00 00 00 00 00 00 00 00 e2 d2 1f 08 .....z
```

Record #3393 (From Hub To Node) Captured on 10.13.04 at 16:41:56.413956800 Length = 64

Runtime Frame# 3393

----- ETHER Header -----
ETHER: Destination: Intrnt-00-00-01 (01-00-5E-00-00-01)
ETHER: Source: 00-04-38-13-41-60
ETHER: Protocol: IP
ETHER: FCS: AACD9B7A

----- IP Header -----
IP: Version = 4
IP: Header length = 20
IP: Differentiated Services (DS) Field = 0xC0
IP: 1100 00.. DS Codepoint = Class Selector Codepoint (48)
IP:00 Unused
IP: Packet length = 28
IP: Id = 0
IP: Fragmentation Info = 0x0000
IP: .0.. Don't Fragment Bit = FALSE

IP: ..0. More Fragments Bit = FALSE
IP: ...0 0000 0000 0000 Fragment offset = 0
IP: Time to live = 1
IP: Protocol = IGMP (2)
IP: Header checksum = 5605 (Verified 5605)
IP: Source address = 160.0.226.2
IP: Destination address = 224.0.1.24

----- IGMP Header -----
IGMP: Message Type = Membership Query (17)
IGMP: Max Response Time = 5 (in 1/10 seconds)
IGMP: Header checksum = 0x0DE2 (Verified 0x0DE2)
IGMP: Group Address = 224.0.1.24

Record #3393 (From Hub To Node) Captured on 10.13.04 at 16:41:56.413956800 Length
= 64

01 00 5e 00 00 01 00 04	38 13 41 60 08 00 45 c0	..^..... 8.A`...E.
00 1c 00 00 00 00 01 02	56 05 a0 00 e2 02 e0 00 V.....
01 18 11 05 0d e2 e0 00	01 18 00 00 00 00 00 00
00 00 00 00 00 00 00 00	00 00 00 00 aa cd 9b 7az

APPENDIX G

UTP NETWORK SURVEY

Personal Information:

- i. Gender: Male Female
- ii. Standing year: First Year Second Year Third Year Fourth Year Fifth Year
- iii. Residential village: V1 V2 V3 V4 V5

General Information

Do you have a Personal Computer in the residential village?

Do you connect to the network?

How do you rate your understanding of UTP network?

Not At All 2: Basic Understanding 3: Average 4: Quite Good 5: Network Expert

Do you use personal PC Firewall?

If yes, please state the software name: _____

Personal Internet & Intranet

1. How do you rate the reliability of UTP intranet?

1	2	3	4	5

2. How do you rate the accessibility of Internet in UTP?

1	2	3	4	5

3. How do you rate the Internet connection speed during off-peak hour?

1	2	3	4	5

4. How do you rate the Internet connection speed during peak hour?

1	2	3	4	5

1: Very Bad 2: Bad 3: Adequate 4: Good 5: Very Good

Please state your view on the importance of Internet connection in UTP:

How long you stay online in the network in a day?

< 4 hours	< 8 hours	< 12 hours	< 16 hours	24 hours

Please state three applications that you always use in UTP network?
1. _____ 2. _____ 3. _____

Have you ever left your PC on in the network 24 hours a day, even when you are not in UTP?

YES	NO

Have you ever experience major problems with UTP network?

YES	NO

If yes, please state the problem:

How do you rate the security of UTP intranet?

1	2	3	4	5

1: Very Bad 2: Bad 3: Adequate 4: Good 5: Very Good

What is your recommendation to improve the UTP network in the future?
