Communications of the IIMA

Volume 6 | Issue 4 Article 2

2006

Utilization of Buffers for Performance Evaluation of Local Area Network Protocols

Sarhan M. Musa
Prairie View A&M University

Emmanuel Uzoma Opara
Prairie View A&M University

Cajetan M. Akujuobi
Prairie View A&M University

Nader F. Mir
Prairie View A&M University

Recommended Citation

Musa, Sarhan M.; Opara, Emmanuel Uzoma; Akujuobi, Cajetan M.; and Mir, Nader F. (2006) "Utilization of Buffers for Performance Evaluation of Local Area Network Protocols," *Communications of the IIMA*: Vol. 6: Iss. 4, Article 2.
Available at: http://scholarworks.lib.csusb.edu/ciima/vol6/iss4/2

Utilization of Buffers for Performance Evaluation of Local Area Network Protocols

Sarhan M. Musa
Center of Excellence for Communication Systems Technology Research (CECSTR)
Prairie View A&M University,
Prairie View, Texas

Emmanuel Uzoma Opara
College of Business
Prairie View A&M University,
Prairie View, Texas

Cajetan M. Akujuobi
Center of Excellence for Communication Systems Technology Research (CECSTR)
Prairie View A&M University,
Prairie View, Texas

Nader F. Mir
Department of Electrical Engineering
San Jose State University,
San Jose, California

ABSTRACT

This paper discusses the performance of traffic flow over Local Area Networks (LAN) utilizing buffers to avoid any irrelevant traffic that clusters the network using sniffer pro. The study applies buffer technology to filter out unnecessary information so the system captures only required information packets. Buffers that capture the protocols are identified. These are: Address Resolution Protocols (ARP), Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP). The study identified to the user/analyzer of an Ethernet technology, how to isolate a cluster network problem, monitor network performance, and offer tips on how to correctly assess and fix network problems. The study provides detailed analysis of threshold gauges, errors, broadcasts, multicasts, packets, and many other facets of dashboard graph configurations thereby ensuring a successful network analysis. The study concludes by providing solutions to poor network performance affecting one user, several users, or an entire network.

INTRODUCTION

The World Wide Web has grown from an early research prototype to a global communication system that has impacted businesses throughout the world. Systematic and exponential growth of online business are among the most interesting and exciting phenomena in networking. System

LAN administrators' management of real-time or on-line data in collaborative environments instigated extensive processing, communication and administrative challenges (Prasad, 1988).

Network communication has successfully remained in existence for a variety of reasons. Most early LANs, were implemented for resource sharing (Touch, 2002). Since then, LAN capabilities have materialized. These include but are not limited to communication, management control, cost effectiveness, downsizing, and new application software design, testing and launching (MeGeehan, 2003).

Today, simulation and analytical models of LAN performance are still important areas to improve within the telecommunication arena. There are many LAN administrators working on the improvement of LAN trafficking. LAN technology is not a static entity (Hoffman, 2004). The reasoning in this analogy is that data stored on LAN changes overtime as new applications are systematically added while old applications are retired. Further, as end users come and go, workstations are added, moved, removed or replaced (Hoffman, 2004). As a result, the LAN administrator must device a mechanism to resolve the clustering of the network. Network platforms must have the technology exchanging large volume of data at local and remote sites that comprise of dedicated systems that are invariably complex and difficult to support (Touch, 2004).

This paper describes the rationale for providing traffic situations for LAN networks by identifying the role of buffer management in controlling the effects of congestion in enterprise network systems. Although large buffers primarily benefit long-term TCP application flows, quality of service (QoS) functionality can be leveraged to allocate appropriate levels of buffering and bandwidth to different classes of traffic thereby protecting delay-sensitive applications from excessive queuing delays associated with large buffers (MeGeehan, 2003). The duty of buffers is to filter out the unwanted traffic. Buffers are identified on the basis of protocols. After being assigned to specific protocol, the buffers in return capture the information packets relating to a specific protocol. In this study, the protocols that will be investigated are ARP, ICP, TCP, and UDP.

Typical simulation and analytical models of Local Area Networks (LAN) performance make assumptions about the packet arrival process, such as fixed packet size, that are exponentially distributed among stations on the network. Early studies have shown that these assumptions are incorrect (Lam, 1980; Kummerle, 1987; Prasad, 1988). Recent studies indicate that accurate Ethernet simulators have been used to eliminate many of the common errors that have been found on common models of the Ethernet (Touch, 2001; Hoffman, 2004; Eggert 2005).

The objective of the experiment described in this paper is to capture data on an Ethernet segment and analyze its performance. In conjunction with that effort, we will discover, analyze, assess, and conclude if the network performance is adequate for an effective LAN communication. In the process of packets, broadcast, and multicast being dispersed at various distinctive rates, we will analyze the potency or their individual affect on the performance on the overall network.

LITERATURE REVIEW

The McGeehan study (2003) indicated that there are three general network subtypes. These are LANs, MANs and WANs. It was documented that within these subtypes, there are a variety of network implementations. Each of these is optimized to fulfill one or more specific networking needs. According to Merchant (2004), LAN technology services a limited geographical area at high speed. These are usually at 10 million bits per second and higher. Peripheries of this technology are usually owned by the enterprise systems that manipulate or use the technology (Kamath, 2004). Touch (2005) noted that LAN technologies have become the most popular form of computer networks. Merchant (2005) concluded by stating this technology now connects more computers than any other type of network. Merchant (2005), Hauer (2003), and Touch (2001) among others conclude that network technology that allows multiple computers to share a communication medium are used for local communication. McGeeham (2005) summarized that Ethernet is a widely used network technology that employs bus topology. This technology was invented by Xerox Corporation's Palo Alto Research Center in the early 1970s. Ethernet is defined as a bus network in which multiple computers share a single transmission medium (Hauer, 2003). This technology is used to coordinate transmission of data and information.

SYSTEM TOPOLOGY

The initial line of defense against congestion is to have adequate buffering available. An appropriate method of buffering is essential so as to minimize packet loss and to maximize the utilization of the end-to-end network (Eggert, 2005). Buffers were implemented to isolate the positive information packets while troubleshooting for congestion causing packets (Hoffman, 2004). This process will ensure that unwanted data will be identified and eliminated

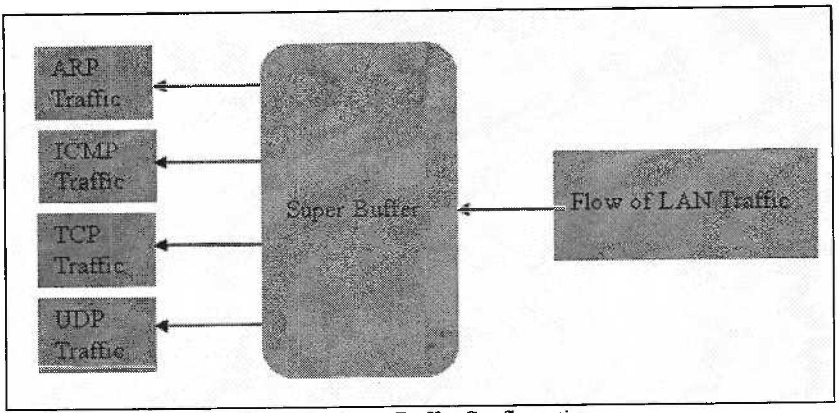


Figure 1: Super Buffer Configurations

Figure 1 shows the different kind of buffers. When LAN traffic flow through a supper buffer which can be one of the protocols ARP, ICMP, TCP, and UDP, the buffers (protocols) filter out unnecessary information so the system captures only the required information packets. The descriptions of each of the traffic protocols are described in the next sections.

NETWORK ANALYSIS AND RESULTS

Address Resolution Protocol

Address Resolution Protocol (ARP) is one of the most important groups of protocols. It allows IP-enabled devices on network to map MAC addresses to IP addresses. We defined ARP and then captured some of the ARP traffic on a network. Below are the results.

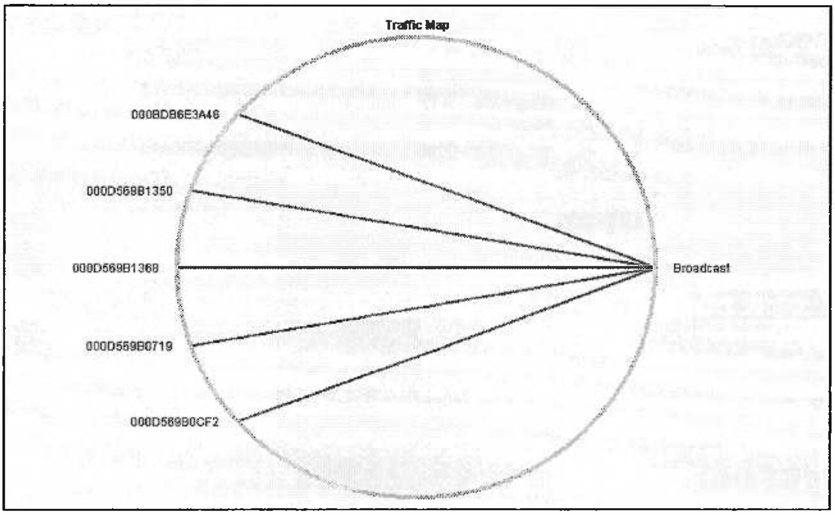


Figure 2: Filtered LAN ARP Traffic

Figure 2 gives the best reason why protocol buffers are used, as it narrows down the vast broadcast. It only captures the source addresses related to ARP which helps in analyzing the problem.

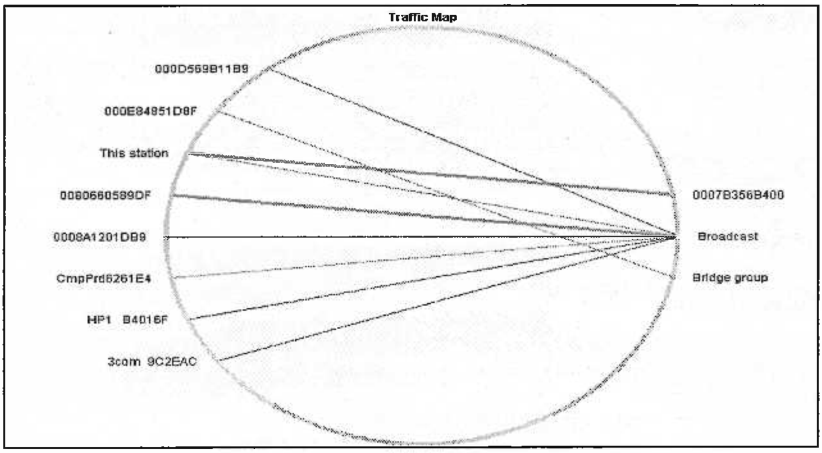


Figure 3: Unfiltered LAN Traffic

Figure 3 shows the traffic map on a network without any specific buffer definition. The difference between Figure 2 and Figure 3 is that Figure 3 shows unnecessarily captured information.

By defining buffers we can specifically know how many bytes we are receiving or sending to hosts using ARP as shown in Figure 4.

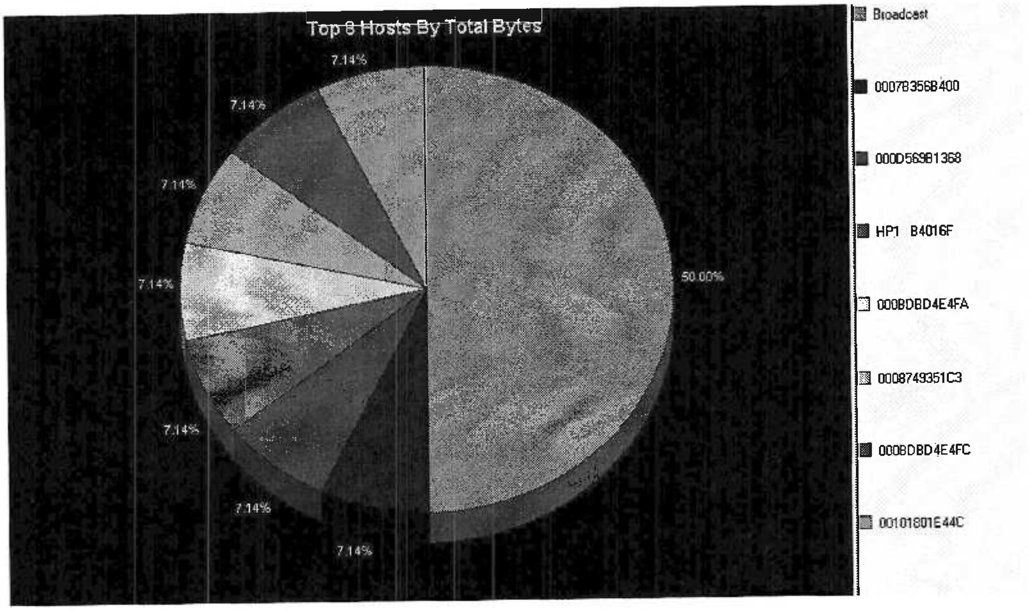
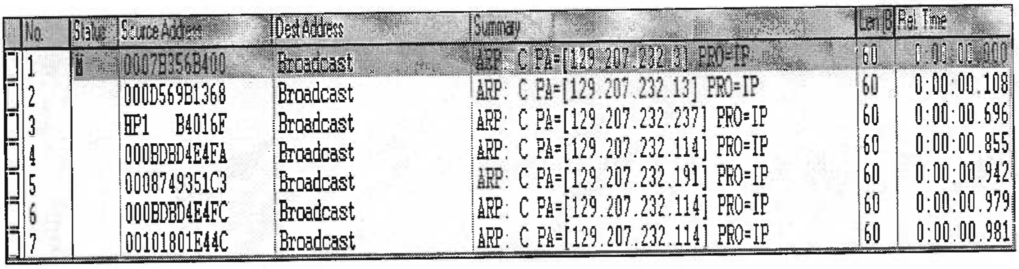


Figure 4: ARP Traffic Flowing Over LAN

Address Resolution Protocol (ARP) also helps in identifying the duplicate IP address problem. Figure 5 shows multiple responses to a single ARP from different devices. This can help as we know the MAC address we fixed by tracking their exact location through MAC.

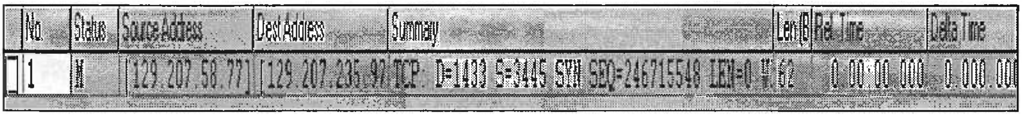


No.	Status	Source Address	Dest Address	Summary	Len (B)	Rel. Time
1	M	0007B356B400	Broadcast	ARP: C PA=[129.207.232.3] PRO=IP	60	0:00:00.000
2		000D569B1368	Broadcast	ARP: C PA=[129.207.232.13] PRO=IP	60	0:00:00.108
3		HP1 B4016F	Broadcast	ARP: C PA=[129.207.232.237] PRO=IP	60	0:00:00.696
4		000BDBD4E4FA	Broadcast	ARP: C PA=[129.207.232.114] PRO=IP	60	0:00:00.855
5		0008749351C3	Broadcast	ARP: C PA=[129.207.232.191] PRO=IP	60	0:00:00.942
6		000BDBD4E4FC	Broadcast	ARP: C PA=[129.207.232.114] PRO=IP	60	0:00:00.979
7		00101801E44C	Broadcast	ARP: C PA=[129.207.232.114] PRO=IP	60	0:00:00.981

Figure 5: Identifying Multiple IP Addresses Using ARP

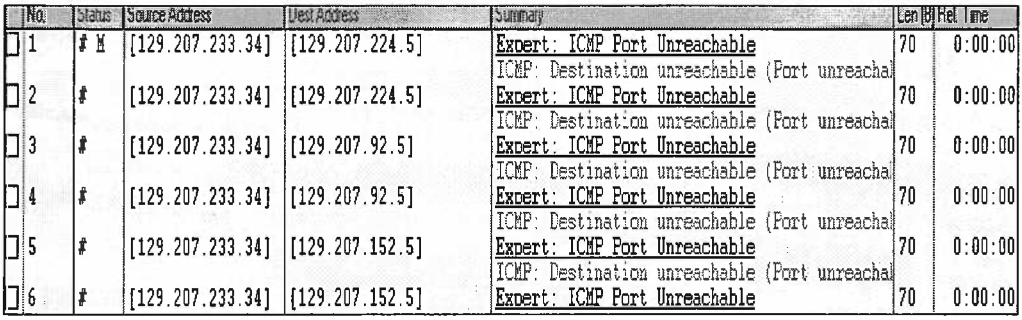
Internet Control Message Protocol

Internet Control Message Protocol (ICMP) supports packets containing error, control and informational messages. An ICMP packet is composed of three different headers: the DLC header, IP header, and ICMP header. We defined ICMP buffers on two different computers and the results were surprisingly interesting.



No.	Status	Source Address	Dest Address	Summary	Len (B	Rel. Time	Delta Time
1	M	[129.207.58.77]	[129.207.235.97	TCP: D=1433 S=3445 SYN SEQ=246715548 LEN=0 W:	62	0:00:00.000	0.000.00

Figure 6: ICMP Traffic Captured on Computer 1



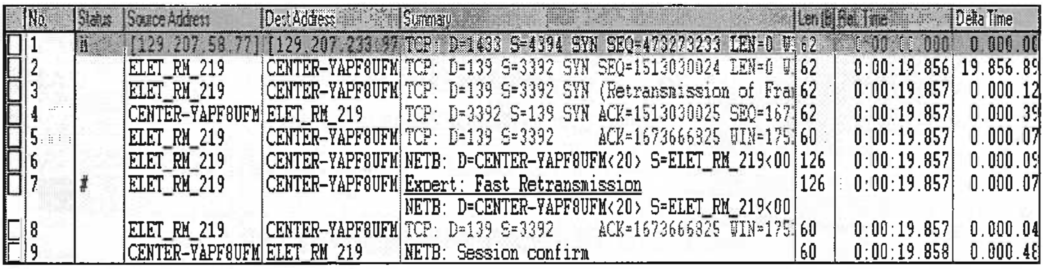
No.	Status	Source Address	Dest Address	Summary	Len (B	Rel. Time
1	# M	[129.207.233.34]	[129.207.224.5]	Expert: ICMP Port Unreachable ICMP: Destination unreachable (Port unreacha	70	0:00:00
2	#	[129.207.233.34]	[129.207.224.5]	Expert: ICMP Port Unreachable ICMP: Destination unreachable (Port unreacha	70	0:00:00
3	#	[129.207.233.34]	[129.207.92.5]	Expert: ICMP Port Unreachable ICMP: Destination unreachable (Port unreacha	70	0:00:00
4	#	[129.207.233.34]	[129.207.92.5]	Expert: ICMP Port Unreachable ICMP: Destination unreachable (Port unreacha	70	0:00:00
5	#	[129.207.233.34]	[129.207.152.5]	Expert: ICMP Port Unreachable ICMP: Destination unreachable (Port unreacha	70	0:00:00
6	#	[129.207.233.34]	[129.207.152.5]	Expert: ICMP Port Unreachable	70	0:00:00

Figure 7: ICMP Traffic Captured on Computer 2

We found that Computer 1 was connected directly to the HUB then to a switch whereas Computer 2 was connected directly to a switch without a HUB.

Transmission Control Protocol

TCP is the most popular protocol on the Internet. With time, more and more legacy protocols such as IPX and AppleTalk are migrating to TCP/IP. IP traffic is dominating on the Internet so the task of capturing and analyzing it is also on the increase and in demand. Traditionally its application is file transferring; TCP can also be used to get passwords. We captured TCP traffic in the same way as we did before we first defined the TCP buffer: we connected it to the LAN and then captured TCP.



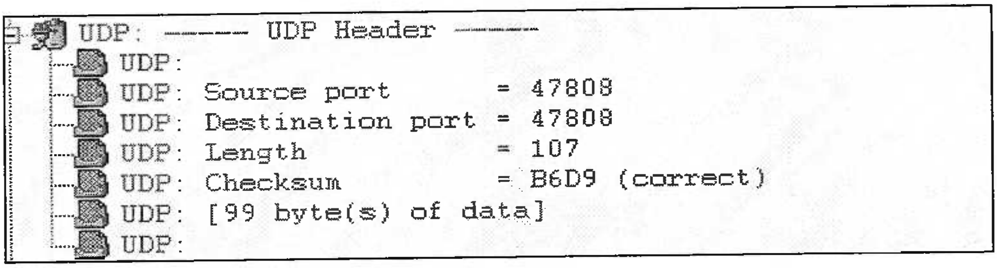
No.	Status	Source Address	Dest Address	Summary	Len (B	Rel. Time	Delta Time
1	M	[129.207.58.77]	[129.207.233.97	TCP: D=1433 S=4394 SYN SEQ=473273233 LEN=0 W	62	0:00:00.000	0.000.00
2		ELET_RM_219	CENTER-YAPF8UFM	TCP: D=139 S=3392 SYN SEQ=1513030024 LEN=0 W	62	0:00:19.856	19.856.89
3		ELET_RM_219	CENTER-YAPF8UFM	TCP: D=139 S=3392 SYN (Retransmission of Fra	62	0:00:19.857	0.000.12
4		CENTER-YAPF8UFM	ELET_RM_219	TCP: D=3392 S=139 SYN ACK=1513030025 SEQ=167	62	0:00:19.857	0.000.39
5		ELET_RM_219	CENTER-YAPF8UFM	TCP: D=139 S=3392 ACK=1673666325 WIN=175	60	0:00:19.857	0.000.07
6		ELET_RM_219	CENTER-YAPF8UFM	NETB: D=CENTER-YAPF8UFM<20> S=ELET_RM_219<00	126	0:00:19.857	0.000.09
7	#	ELET_RM_219	CENTER-YAPF8UFM	Expert: Fast Retransmission NETB: D=CENTER-YAPF8UFM<20> S=ELET_RM_219<00	126	0:00:19.857	0.000.07
8		ELET_RM_219	CENTER-YAPF8UFM	TCP: D=139 S=3392 ACK=1673666325 WIN=175	60	0:00:19.857	0.000.04
9		CENTER-YAPF8UFM	ELET_RM_219	NETB: Session confirm	60	0:00:19.858	0.000.48

Figure 8: Three Stages of TCP Communication

Figure 8 shows that TCP is a three-way handshake. Frame 1 is the beginning of the TCP three-way handshakes. In the first packet NETB client sends a packet to NETB server to destination packet 1433. Then the server acknowledges the frame with number 1513030025. In the last frame of the handshake the workstation confirms the receipt of the frame by sending an acknowledgement packet 1673666825 telling that the connection is established.

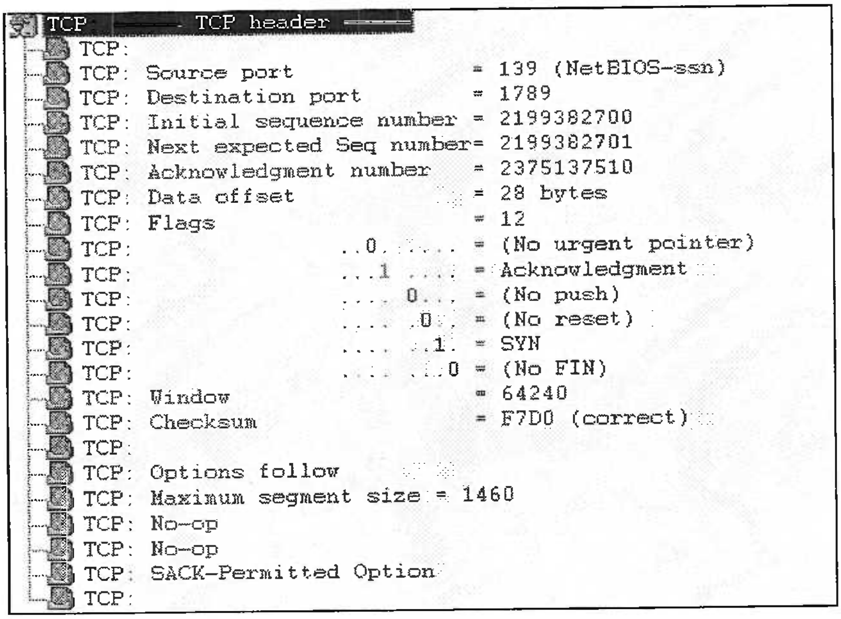
User Datagram Protocol

The major difference between the UDP and TCP protocol is that it is connectionless so there is no need to establish a session between the source and the destination before transmitting the data. Thus we don't have to go through the three-way handshake process. As UDP is a connectionless protocol, it does not have most of the fields in a TCP frame such as sequence numbers, flags, and window size.



```
UDP: ------ UDP Header ------
    UDP:
    UDP: Source port        = 47808
    UDP: Destination port = 47808
    UDP: Length             = 107
    UDP: Checksum           = B6D9 (correct)
    UDP: [99 byte(s) of data]
    UDP:
```

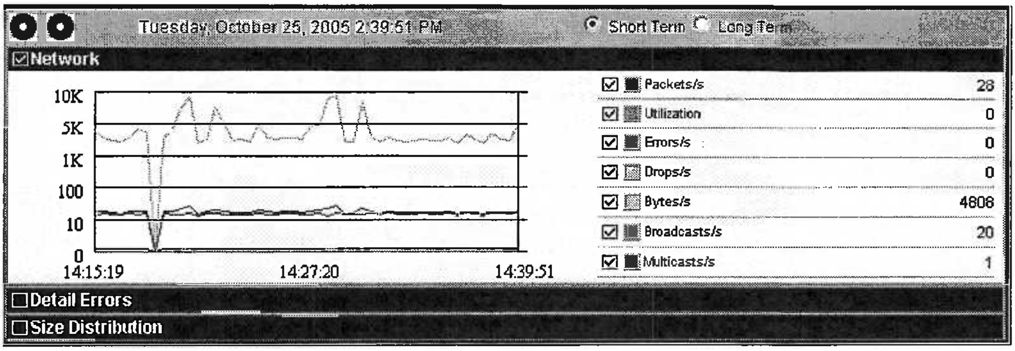
Figure 9: A UDP Header



```
TCP: ----- TCP header -----
    TCP:
    TCP: Source port                  = 139 (NetBIOS-ssn)
    TCP: Destination port             = 1789
    TCP: Initial sequence number      = 2199382700
    TCP: Next expected Seq number= 2199382701
    TCP: Acknowledgment number        = 2375137510
    TCP: Data offset                  = 28 bytes
    TCP: Flags                        = 12
    TCP:                    ..0. .... = (No urgent pointer)
    TCP:                    ...1 .... = Acknowledgment
    TCP:                    .... 0... = (No push)
    TCP:                    .... .0.. = (No reset)
    TCP:                    .... ..1. = SYN
    TCP:                    .... ...0 = (No FIN)
    TCP: Window                       = 64240
    TCP: Checksum                     = F7D0 (correct)
    TCP:
    TCP: Options follow
    TCP: Maximum segment size = 1460
    TCP: No-op
    TCP: No-op
    TCP: SACK-Permitted Option
    TCP:
```

Figure 10: A TCP Header

The advantage of UDP being connectionless over TCP as in Figures 9 and 10 is that UDP is free of sequence numbers, flags and window size.


Tuesday, October 25, 2005 2:39:51 PM ● Short Term ○ Long Term

☑Network

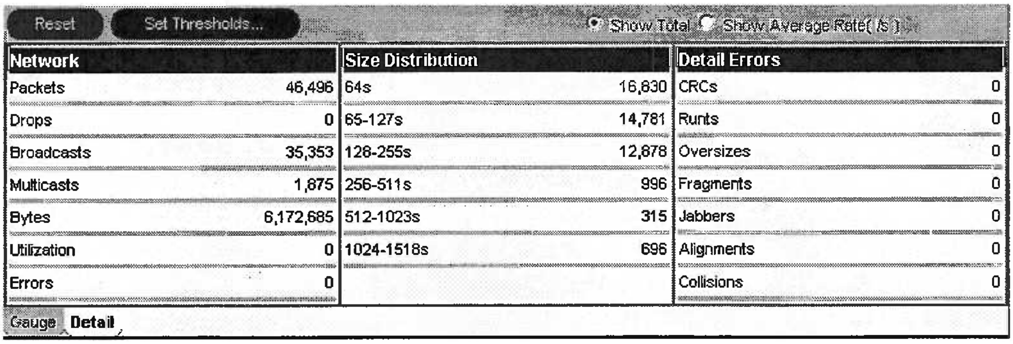
☑ Packets/s	28
☑ Utilization	0
☑ Errors/s	0
☑ Drops/s	0
☑ Bytes/s	4808
☑ Broadcasts/s	20
☑ Multicasts/s	1

□Detail Errors

□Size Distribution

Figure 11: A Network Environment Graph

The graph in Figure 11 is the result of a time period in which the activity of the packets, utilization, errors, drops, bytes, broadcast, and multicast are displayed just to give the user/analyzer a better understanding of the network environment.



● Show Total ○ Show Average Rate(/s)

Network		Size Distribution		Detail Errors	
Packets	46,496	64s	16,830	CRCs	0
Drops	0	65-127s	14,781	Runts	0
Broadcasts	35,353	128-255s	12,878	Oversizes	0
Multicasts	1,875	256-511s	996	Fragments	0
Bytes	6,172,685	512-1023s	315	Jabbers	0
Utilization	0	1024-1518s	696	Alignments	0
Errors	0			Collisions	0

Figure 12: The Distribution Rates and the Network Outputs

These charts in Figure 12 are the products of the distribution rates and the network outputs.

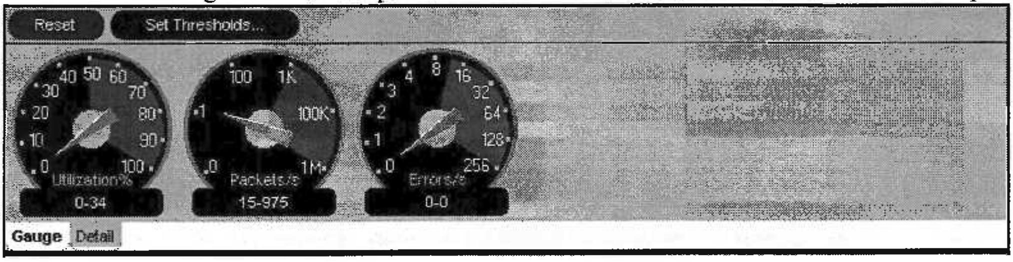
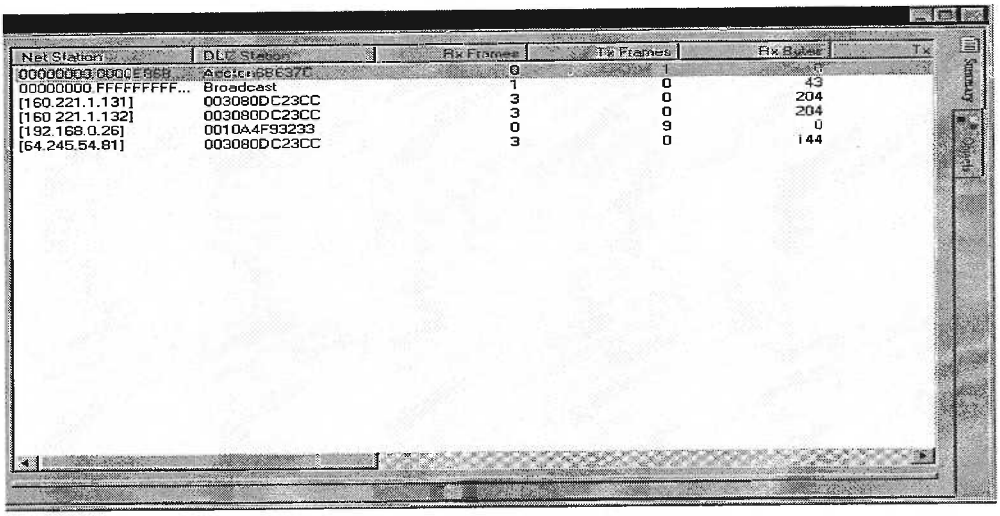


Figure 13: The Dashboard

The dashboard in Figure 13 gives a visual depiction of the number of packets/second, the percentage utilization and the errors/second. In this figure, a gauge tab and a detail tab. The detail of tab gives information on the broadcasts/multicasts, types of errors and packet size distribution. The figures are cumulative. The gauge indicates the default thresholds in red. Using the default values is recommended and the user can see if traffic utilization is hitting over 38% (Ethernet) or 80% (Token Ring), or if error rates are over 10%, or if broadcasts/multicasts are over 10%. The dashboard displays a network segment packet rate, percentage of utilization, and error rate in real time. Also provided are configurable graphs for various network statistics. Various tabs are available to view accumulated detail statistics of average per second statistic for a number of important network parameters. The exact tabs available depend on the currently selected adapter (Kummerle, 1987).



Net Station	DLC Station	Rx Frames	Tx Frames	Rx Bytes	Tx
00000003.0000E96B...	Accton6BE37C	0	1	0	
00000000.FFFFFFFF...	Broadcast	1	0	43	
[160.221.1.131]	003080DC23CC	3	0	204	
[160 221.1.132]	003080DC23CC	3	0	204	
[192.168.0.26]	0010A4F93233	0	9	0	
[64.245.54.81]	003080DC23CC	3	0	144	

Figure 14: The Captured Window

Create a capture by selecting Capture > Start by clicking on the 'Play' icon on the toolbar. Pausing and stopping the capture is carried out the same way. To stop the capture, select Stop and Display. This will immediately view the capture. Select File > Save to save it, giving it a relevant name. To improve monitoring of traffic, all captures are time stamped.

The state of the capture can be monitored by selecting Capture > Capture Panel. This will show how much of the buffer has been used, the number of packets captured/dropped and the buffer size. Figure 14 shows an example of captured window and Figure 15 shows the monitoring tool.

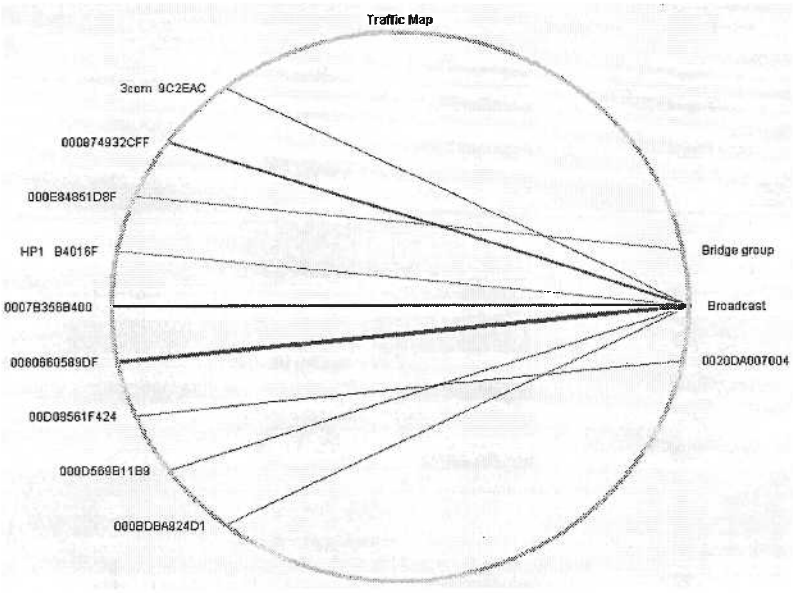


Figure 15: Monitoring Tool

This monitoring tool in Figure 15 gathers statistics on the traffic between stations. It can also be displayed as a table, a bar/pie chart or a traffic map. The Outline view can be used to see the total activity between pairs, or can be separated out into protocols using the Detail View (magnifying glass). The traffic map is good for a quick look at the top talkers (thickest lines) and to find who is talking to whom. Holding the mouse over a line reveals the throughput. Right-clicking allows for zooming in and out. The matrix view is useful for finding devices that are not receiving or transmitting traffic and to see who is talking to whom. The tabs can be used to view the conversations at the MAC layer or at the IP or IPX layer.

Filters can be defined from the matrix view by right-clicking on a device and selecting define filter. Another quick way to filter the display is to create visual filters. This works by clicking on the desired devices in the matrix view, whilst holding down the Ctrl key. Once the visual filter button at the top of the matrix view window is clicked, a new capture is created containing just those devices.

TROUBLESHOOTING

In the act of troubleshooting, there are several methods in which the user can get comfortable and gain familiarization with the network. It is necessary to have a baseline of the network performance to recognize when and where problems have occurred. The following steps are taken in the event of a network problem:

- Take snapshots of graph and gauge outputs over a given time period.
- The snapshots should be for a specified time period, say 5 or 10 minutes.
- Pick the same places each time the snapshots are taken.

- Have a set of commands to measure response times by. These could include ping tests, trace routes, DNS lookups, and finger points.
- Observe the expert system.
- Save the captures and include network diagrams as part of the documentation.
- Note relative times between client requests and server responses, this gives a baseline to test by if network problems occur later on.
- Have a filing system that makes it easy to retrieve the data if required later.

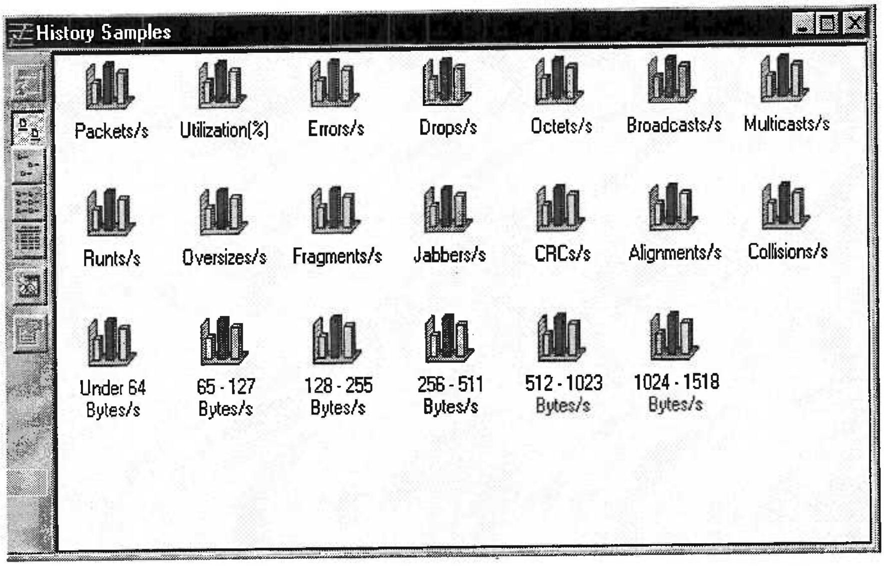


Figure 16: The History Samples

The history samples in Figure 16 allow the user to gather a selection of statistics such as Packets/sec, Utilization, Errors/sec etc. that can be used to gain a profile or baseline of the network when it is functioning correctly. Alarm thresholds can then be set accordingly and future trends can be spotted over time. Up to 10 of these samples can be run at any one time and the user can save them to view later in different formats and mixed in together as multiple histories. The icons on the left hand side of the window give different display options and file export options.

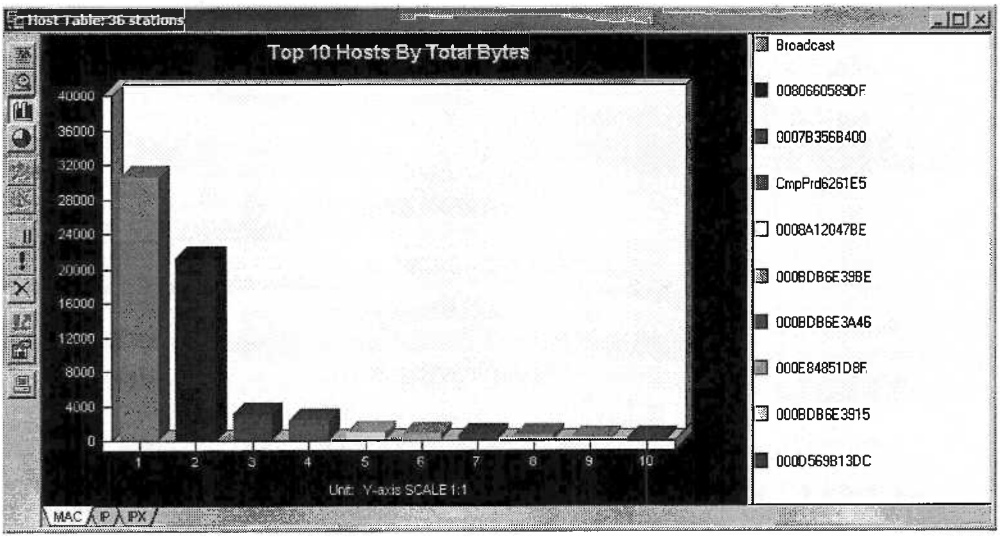


Figure 17: The Host Table in Chart

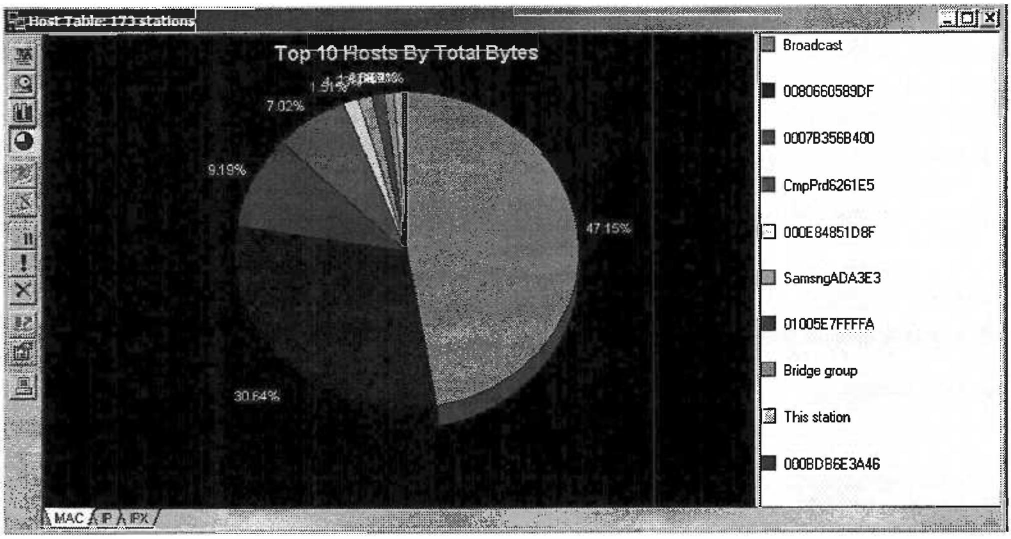


Figure 18: The Host Table in Pie Chart

Chart and Pie graphs in Figures 17 and 18 respectively display various outputs and the use of packets and broadcast are very useful in the research process. The table can be viewed in bar or pie chart format plus the statistics can be exported to a spreadsheet, the format being .csv, .txt or .prn. When viewing in Chart format, the top talkers are listed from the top on the right, and displayed from left to right on the bar chart. Obtaining statistics on a particular station is useful as one can filter a station, determine the highest user, and find incorrectly configured protocol stacks, faulty NICs and export data specific to that station.

MANAGERIAL IMPLICATIONS

Network administrators who are myopic about the opportunities presented by broadband technologies, risk placing their organizations at a competitive disadvantage. As LANs technology progresses to a 10-gigabits-per second range, the need has arisen for LAN interconnection over wide areas and at high speed. Technologies such as switched multimegabit data services ("SMDS" used for data), synchronous optical network ("SONET" used for data and voice), and broadband integrated services digital network ("BISDN" used for data, voice, image, graphics, fax etc) provide high speed LAN interconnection. Network managers should implement these technologies so as to augment communications and the sharing of information among enterprise systems and its suppliers.

To ensure that adequate combinations of services are acquired in the most cost-effective manner, network administrators should closely monitor changes and developments in broadband services and be prepared to make adjustments as needed.

CONCLUSION

Managing the network platform has become essential for enterprise systems to operate effectively and remain a viable and competitive organization. Enterprise systems are therefore required to expand beyond local areas networks to wider geographical networks. The key is mobility, transparency and speed as data move across various platforms.

The study presented technical details on how to isolate clusters of problems in a network. It showed that effective management requires an understanding of the technologies involved with a networking platform. Network administrators will have to deal with definitions and protocols to make good decisions since such decisions will provide the cost advantage and customer support required for a competitive advantage in the information technology platform.

This paper defined the Ethernet buffers and then captured the information packets from LAN traffic. Defining buffers on the basis of specific protocols helped in narrowing down the LAN traffic which was filling up space in the machines. We also came up with the applications of different buffers and ran the traffic tests on them. We identified for the Ethernet user/analyzer, how to isolate a problem by monitoring network performance. The study concludes by providing directions on how to correctly assess and correct a clustered network. Detailed were provided on the threshold gauges, errors calibration, broadcast, multicast, packets, and other facets of the dashboards graph configuration to ensure a successful network analysis.

REFERENCES

Eggert L. & Touch J. (2005). "Idletime Scheduling with Preemption Intervals, 'Proc. SOSP 2005, PP. 249-265.

Hauer M, McGeehan, K. S, Touch, J., Bannister J., Lyons, E., Lin, C., Lau, A., Lee, H., Stardubov & Willner, A. (2003). "Optical-Assisted Internet Routing Using Arrays of Novel

Dynamically Reconfigurable FBG-Based Correlators, *IEEE/OSA Journal of Lightwave Technology,* Special Issue on Optical Networks, V21 N11, Dec., pp. 2765-2778.

Hoffman M., & Kravets, T. (2004). Guest Editors, Special Issue on the *Global Internet, Computer Networks*, V45, pp. 1-3.

Kummerle K, L. & Tobagi, F.A. (1987). *Advances in Local Area Networks,* IEEE Press.

Lam S. S. (1980), A carrier Sense Multiple Access Protocol for Local Networks, *Computer Networks,* 4, 1, Feb. 21-32.

McGeehan J., Kumar, S., Gurkan D., Mttaghian, N., Bannister, J., Touch, J., & Willner. (2003). All Optical Decrementing of a Packet's Time-To-Live (TTL) Field and Subsequent Dropping of a Zero TTL Packet, *IEEE/OSA Journal of Lightwave Technology*, Special Issue of Optical Networks, V21N11, Dec., pp. 2746-2752.

Merchant K., McGeehan, W.A., Ovadia, S., Kamath, P., Touch, J. & Bannister, J. (2005). Analysis of an Optical Burst Switching Router with Tunable Multiwavelength Recirculating Buffers, *IEEE/OSA Journal of Lightwave Technology*, V23, N10, Oct, pp. 3302-3312.

Prasad K. et all. (1988), Performance analysis of Ethernet based on an event driven simulation algorithm. In *Proceedings of the 13th conference on local computer networks,* pages 253-267, Minneapolis, Minn., 10-12 1988. IEEE computer Society.

Touch, J. (2005) Virtual and Overlay Networks, *IEEE Tutorials Now.*

Touch, J. (2001). Dynamic Interest Overlay Deployment and Management Using the X-Bone, *Computer Networks*, July, pp. 117-135.

Touch, J. (2002). Those Pesky NATs, *IEEE Internet Computing,* July/August, pp.96.

Touch, J. (2004). Overlay Networks, Chapter in *Practical Handbook of Internet Computing,* ed. M.P. Singh, CRC Press, Sept., ISBN 1-58488-381-2.