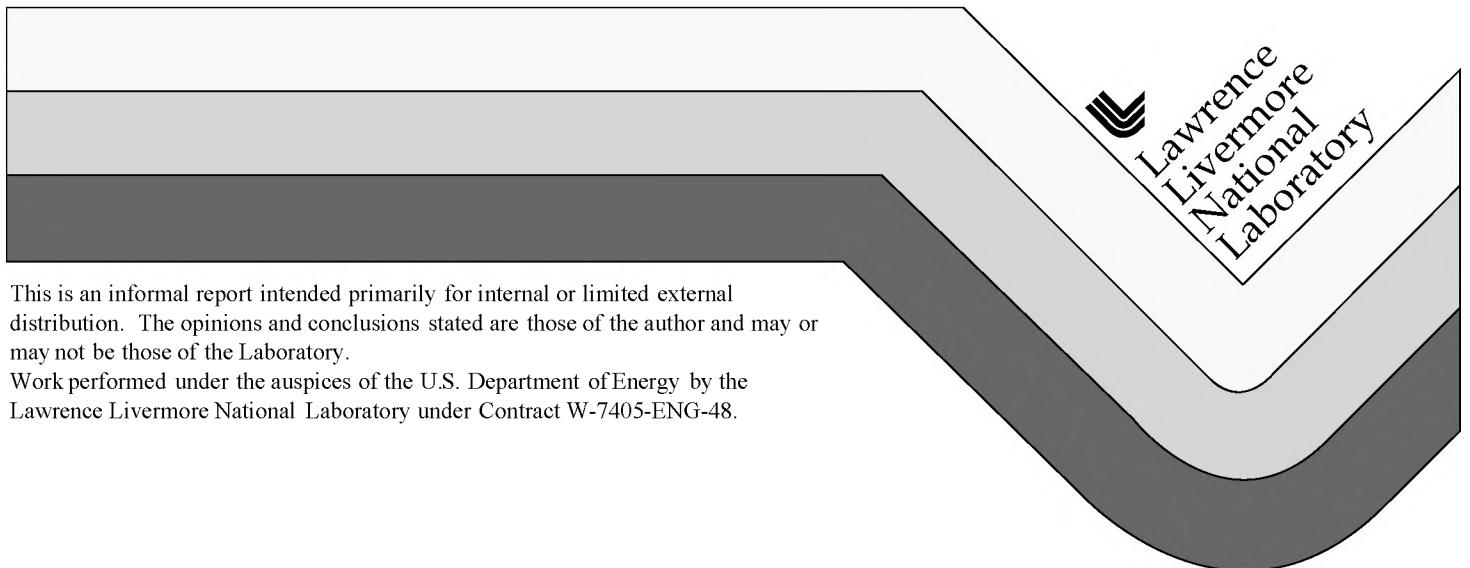


**ICCS Network Simulation
LDRD Project Final Report Summary**

R. W. Bryant

January 9, 1999



DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This report has been reproduced
directly from the best available copy.

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information
P.O. Box 62, Oak Ridge, TN 37831
Prices available from (423) 576-8401

Available to the public from the
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd.,
Springfield, VA 22161

ICCS Network Simulation LDRD Project Final Report Summary

Robert W. Bryant, 1/9/99

Abstract

A critical component of the NIF Integrated Computer Controls System (ICCS) is the local area network (LAN) that enables timely and reliable communication between control applications running on the 600+ computer systems distributed throughout the NIF facility. This project analyzed critical portions of the NIF ICCS network (referred to as “the network” in this report) applying the OPNET Modeler discrete event simulation package to model and simulate network operation and the Network Associates Distributed Sniffer network analyzer to collect actual network performance data in the ICCS Testbed. These tools were selected and procured for use on this project.

Simulations and initial network analysis indicate that the network is capable of meeting system requirements. ICCS application software is currently in development, so test software was used to collect performance data. As application software is tested in the Testbed environment, more accurate timing information can be collected which will allow for more accurate large-scale simulations.

Introduction

This report describes the work that was done and results that were obtained on this LDRD project. It refers to earlier documents and presentations that provide details on specific topics. The complete list of documents is provided in the reference section at the end of this report.

The NIF network design utilizes both Ethernet (10 and 100 Mbit/s) and Asynchronous Transfer Mode (ATM) technologies, taking advantage of the best features of each. ATM is utilized on systems having time sensitive video requirements. All ATM links are 155 Mbit/s OC-3c running over multi-mode fiber. A core ATM switching system directly interconnects all end-systems with ATM network interface cards. Ethernet provides connectivity to all end-systems in the network, including the ones that also have ATM connections. A core Ethernet switch provides 100 Mbit/s connectivity and distributed Ethernet switches provide a mix of 10 Mbit/s and 10/100 Mbit/s ports depending on subsystem needs. Both fiber and twisted pair cabling are used for Ethernet connections, depending on distance and other system requirements (e.g. optical isolation needs, EMI issues).

This report is broken into sections which cover: the process for selecting the commercial simulation package; simulation analysis of network triggers running across the Ethernet and ATM switching systems; models developed for simulation of the baseline network; simulation analysis of the communication among systems involved in laser alignment; network analysis systems and their configuration; and streaming video data that was captured using the network analyzer.

Simulation Tool Selection

The initial task on this project was to select the appropriate commercial network modeling and simulation tool to be used. The goal was to assist in the validation of the network design with respect to various performance requirements.

To reduce the number of candidates for the simulation tool to be used, input was collected from several people involved in network modeling at LLNL and at other sites, including LANL and SNL. Also, an extensive report by TASC evaluating various communication simulation tools was reviewed. As a result, the selection process was narrowed to the CACI COMNET III and the OPNET Modeler packages. They are both widely used packages within the network simulation communities. These two tools were evaluated by building a representative NIF network model on each and comparing their ability to accurately model and simulate real traffic. A copy of OPNET was in use already onsite and there was expertise in its use. A 3-day training course on COMNET III was attended and an evaluation copy was obtained and used for its evaluation.

As a result of our evaluation, the MIL3 OPNET Modeler software package (Version 3.5) was selected. The OPNET software was procured and installed on a Sun Ultra II 200 Mhz workstation. The advantages that OPNET has over COMNET that lead to its selection are:

- 1) OPNET allows models to be modified or new models can be created from scratch, whereas COMNET models cannot be changed (i.e. one can only build new models based on the ones provided). During the evaluation of COMNET, it was found that certain needed modeling features to accurately represent the NIF network design were not provided and thus the simulations we would create may not accurately reflect real network performance. Examples of lacking modeling features were 1) a model of full duplex Ethernet, and 2) modeling of the ARP protocol.
- 2) The code that implements the COMNET models cannot be viewed, so it is not possible to see how the models are implemented without running test examples or calling for technical support. There is documentation but it does not provide all the details of the model implementation. This would make it difficult to verify that the models accurately reflect the network equipment to be used.
- 3) LLNL already had some expertise in OPNET and there were other projects onsite that were planning to use OPNET. Also, OPNET was the tool of choice at LANL and SNL for their network modeling.
- 4) OPNET was less expensive than COMNET, \$18K vs. \$40K.

Network Trigger Simulations

The first problems studied with OPNET were to evaluate the latency of “trigger” signals sent over the Ethernet and ATM switches. If the latency of the Ethernet and ATM networks were low enough, then separate networks, with associated computer interface cards, to support trigger distribution would not be needed. This would save a significant amount of money for design, hardware, and maintenance.

There were two different triggers that were evaluated: the “T-1 trigger” and the “Video Capture Trigger.”

T-1 Trigger

The T-1 trigger must be delivered from the Master Timing (MT) system to a set of Alignment Control (AC) FEPs at 1 second before the shot time. The requirement was that T-1 trigger must arrive at the AC FEPs no later than 10 milliseconds after it is sent by the MT application. The approach uses an IP multicast or broadcast packet, which is sent by the MT system and broadcast to all AC FEPs “simultaneously.” This trigger should be sent multiple times to protect against the potential loss of a packet due to a link bit error or loss within a switch. There are two layers of Ethernet switches in the network between the MT system and the AC FEPs. We modeled the use of 10 and 100

Mbit/s full-duplex switches to see the differences. We also generated a simulated load on the network and FEPs to evaluate the effect of this load on the trigger latency.

The simulations indicate that the 10 millisecond network latency can easily be met, even with a background load (which is not expected). 100 Mbit/s Ethernet provides the lowest latency, well under 1 millisecond, and is the choice for this application.

Video Capture Trigger

The requirement was that the video capture trigger must be delivered from the MT system to the video FEPs within 5 milliseconds. Since the MT system and video FEPs have ATM ports directly connected to the core ATM switching system, ATM will be used to distribute this trigger. As with the T-1 trigger, this trigger should be sent multiple times to protect against the potential loss of a packet due to a link bit error or loss within a switch. A multicast PVC will be established in the ATM switch to support the simultaneous multicast of this trigger to all video FEPs. We also added a simulated load to determine its effect on trigger latency, even though no load is expected. In fact, there will be essentially no other traffic into the video FEPs when this trigger is sent.

The simulations indicate that the latency will be much less than 1 millisecond, even under the simulated load that was provided. The latency through the ATM switch itself is typically 15 microseconds. The majority of the simulated latency was from the trigger packet processing in the MT system and the video FEPs.

Baseline Network Models

Following the 100% design review of the network, we began developing the specific node models in OPNET for the key systems in the network. This included the ATM and Ethernet switches, the Supervisory workstations, the Automatic Alignment systems, the Video FEPs, and the Alignment Control FEPs. With these models we were able to simulate the network during the alignment phase, which is when the network is most heavily loaded. Note that since the network is fully switched (i.e. every end-system has its own non-shared network link), traffic is isolated within the switches to only the ports that are communicating. This allows various independent subsystems to be modeled separately, which simplifies the simulation and allows the simulation to run within a reasonable timeframe. This also makes the network displays in the GUI more manageable and reduces the likelihood of introducing errors.

The node models provided with OPNET Version 3.5 (which was the latest version at the time these models were developed) did not support some features needed to accurately represent nodes in the network design. Therefore, we developed the following new node models:

- 1) A 50-port Ethernet switch model with full-duplex 100 Mbit/s ports was created which is used as the Core Ethernet switch or distributed Ethernet switches. 50 ports was adequate to model the portion of the network of interest.
- 2) A 32-port ATM switch model with 155 Mbit/s OC-3c ports was created as the Core ATM switch. A larger switch could easily have been created, but 32 was preferred for the simulations that were run.
- 3) A workstation model of an Alignment Supervisor workstation was created. This model had several new features that were not provided in the standard OPNET models.

- a) It has dual network ports, one Ethernet (100 Mbit/s) and one ATM. Note that because of the way OPNET simulates communication between Clients and Servers, dual ported workstations only work correctly on Client nodes, not Server nodes. For this reason, the Alignment Supervisor was implemented as a Client node.
- b) It was provided with two options for Client communication over the ATM link.
 - I. Through the standard TCP/IP protocol stack (including UDP), or
 - II. Bypassing TCP/IP, and communicating directly to the ATM AAL layer. This more accurately models the direct ATM API communication that takes place for transport of streaming video from the video FEPs.
- c) The OPNET-provided Client code which implements FTP was modified to accurately model the streaming video transfer from the Video FEPs.
- d) Multiple Client modules (four) were implemented within a workstation (note: the standard OPNET models only provide a single Client module). Three Client modules are used to initiate three independently controlled streams of 10 frame/sec video from the video FEPs (over ATM), and the fourth is for communication with the Alignment Control FEPs (over Ethernet).

4) A workstation model of an Automatic Alignment system was created. This is nearly identical to the Alignment Supervisor workstation, except it only has two Client modules, one to communicate with the video FEPs and the other to communicate with the Alignment Control FEPs. It uses TCP/IP for all communication, since it needs error free delivery of all data, including images from the video FEPs.

5) A workstation model of a video FEP was created. This model has a Server module which responds to client requests and provides both a TCP/IP stack (for communication with the Automatic Alignment systems) and direct ATM AAL communication (for streaming video transfers to the Alignment control workstations).

6) A workstation model of an Alignment Control FEP was created. This is based on the OPNET provided server model and provides a 100 Mbit/s Ethernet connection and TCP/IP connectivity.

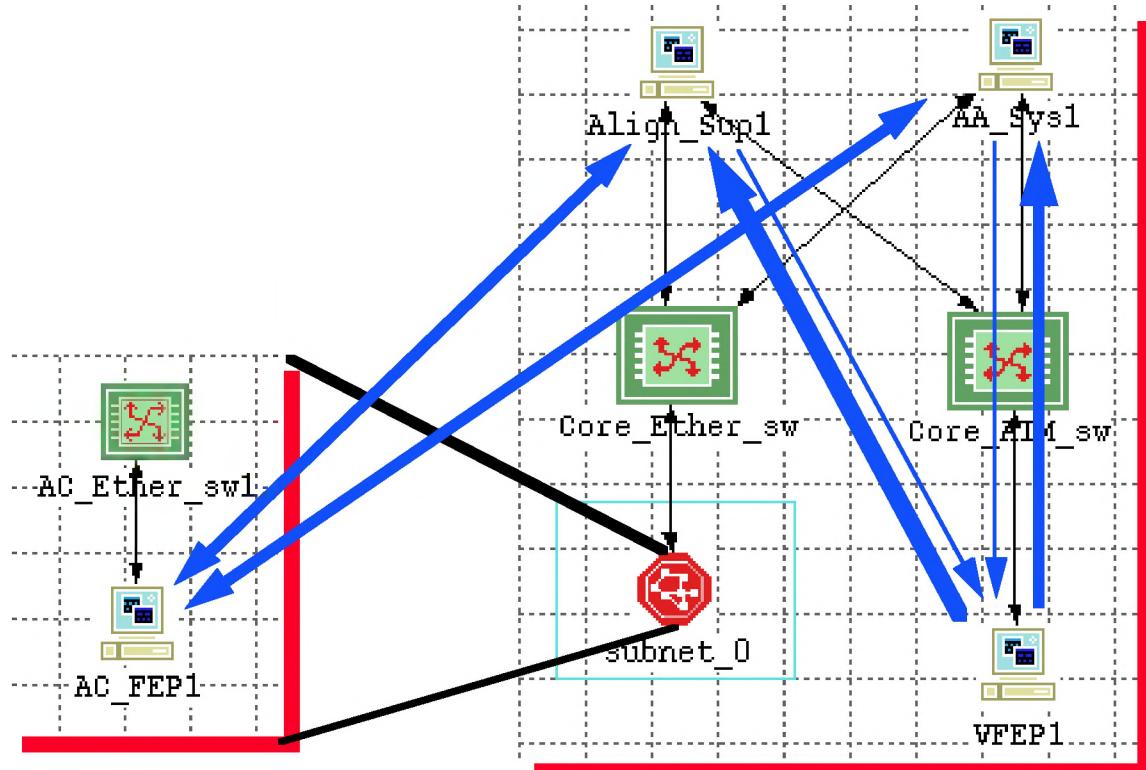
These node models are interconnected as planned in the baseline network design. OPNET model attribute values are set to model the expected performance of the equipment to be used.

Alignment Simulation

After creating the node models mentioned above, a network model was created and traffic levels were defined between the Client and Server nodes. A large number of traffic statistics were collected during the simulation runs. This allowed verification that the models and the simulation were set up correctly, and to evaluate the throughputs, latencies, packet loss, and link utilization at various points in the network. Special “filters” were created which allowed us to view statistics in more meaningful ways. For example, a filter was created to generate windowed link utilization averages over a user-selectable window.

The simulation results confirm the prior design analysis conclusions that the network design will meet the system requirements. The simulation and results are summarized here.

The network model that was simulated is shown below. One each of an Alignment Supervisor workstation (Align_Sup1), Automatic Alignment system (AA_Sys1), video FEP (VFEP1), and Alignment Control FEP (AC_FEP1) were included. Worst case expected traffic was applied. The simplified network allowed realistic simulation results to be obtained within a reasonable amount of time.



The heavy traffic load applied in the simulation is given in the following table. These traffic levels were obtained from worst case ICD traffic and discussions with the responsible engineers. The load of 5 requests/sec from the AA_Sys to the VFEP created a heavy traffic load between these systems. The load of 108 requests/sec from both the Align_Sup and the AA_Sys to the AC_FEP greatly exceeds what any Alignment Control FEP can expect. This traffic is more indicative of a high load on the Alignment Supervisors and Automatic Alignment systems communicating with the 108 Alignment Control FEPs.

Client Nodes	Ser ver Nodes	Networ k	Protocol	Requests[3] / sec	Req. size Bytes	Resp. si ze Bytes[4]	Req. size dist.	Resp. si ze dist.	Ser ver time, msec
Align_Sup	VFEP[1]	ATM	AAL5	10	Const.	3 07 ,200	Const.	2 0.48	
	VFEP[1]	ATM	AAL5	10	Const.	3 07 ,200	Const.	2 0.48	
	VFEP[1]	ATM	AAL5	10	Const.	3 07 ,200	Const.	2 0.48	
	AC_FEP[2]	Ethernet	TCP/ IP	108	Normal	200	Const.	64	0.0625
AA_Sys	VFEP[2]	ATM	TCP/ IP	5	Normal	200	Const.	3 07 ,200	2 0.00
	AC_FEP[2]	Ethernet	TCP/ IP	108	Normal	200	Const.	64	0.0625

[1] An Align_Sup requests 3 video streams from one VFEP (worst case)

[2] Clients randomly select a server

[3] Requests made per each Client node (i.e. Align_Sup or AA_Sys)

[4] 307,200 Bytes = single camera image (640 x 480 x 1 Byte)

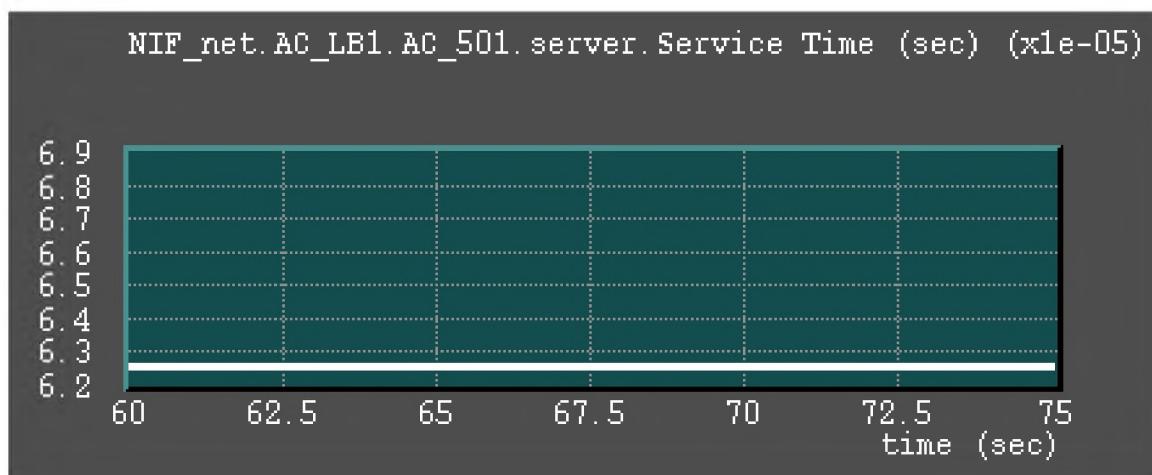
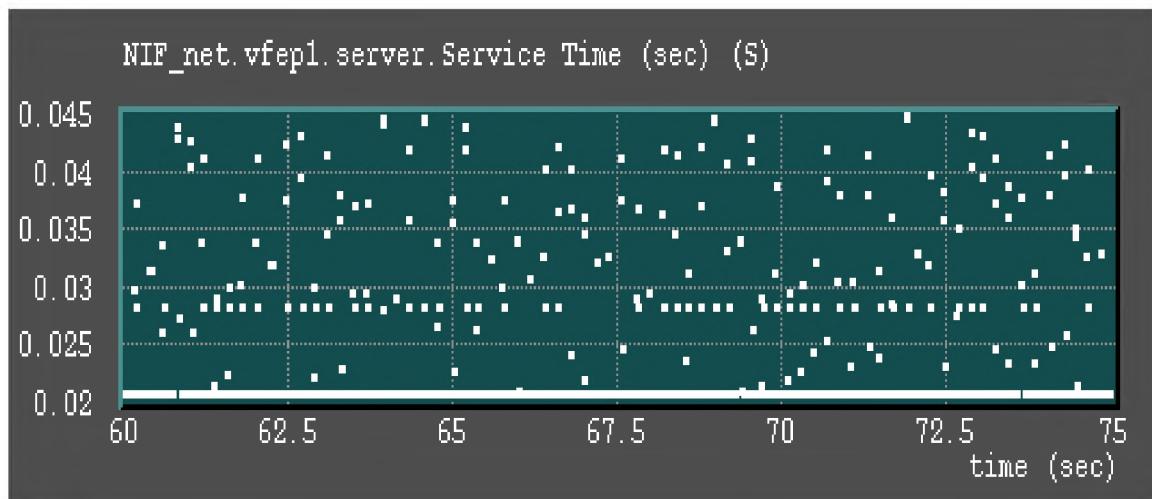
The “dist” columns represent the distributions for the traffic. “Const” means a constant distribution is applied (i.e. all are the same). “Normal” means that a normal distribution is applied providing some randomness in the traffic around the listed mean.

Three streams of video between the VFEP and the Alignment Supervisor are flowing simultaneously and each one is allocated 30 Mbit/s of the 155 Mbit/s ATM bandwidth. Therefore the video flows are spread out in time rather than being burst at the full ATM rate. This allows the VFEP to respond without large delays to video frame requests from the Automatic Alignment system while video is streaming to the Alignment system. Note that in the actual ICCS implementation, there will only be a single request for an entire video stream, rather than a request for each video frame, as is done in the simulation. It was simulated this way to match the client/server models provided in OPNET. As shown in the table above, the requests are implemented as 1 Byte transfers which have essentially no impact on the simulation results.

Because of the heavy traffic load on the ATM portion of the network, the simulation runs quite slow relative to real time. This is due to the fact that all data transfers are segmented into 53 Byte ATM cells, which are each handled as independent simulation events. For this reason, the simulation was only run for 15 seconds of simulated time. Given the heavy traffic load and relatively consistent traffic patterns in this simulation, 15 seconds is sufficient to obtain the results of interest.

To allow for a delay within the video FEP in getting a video image ready to transfer, a processing load was implemented in the VFEP. For this simulation, the processing/service time per image was set at approximately 20 msec (note: this parameter can easily be varied). This was selected based on measurements that the VFEP could handle approximately 50 video frames per second. When multiple video frames are being serviced by the VFEP simultaneously, the Server model divides the processing time between them, thus delaying the Server responses for all video frames.

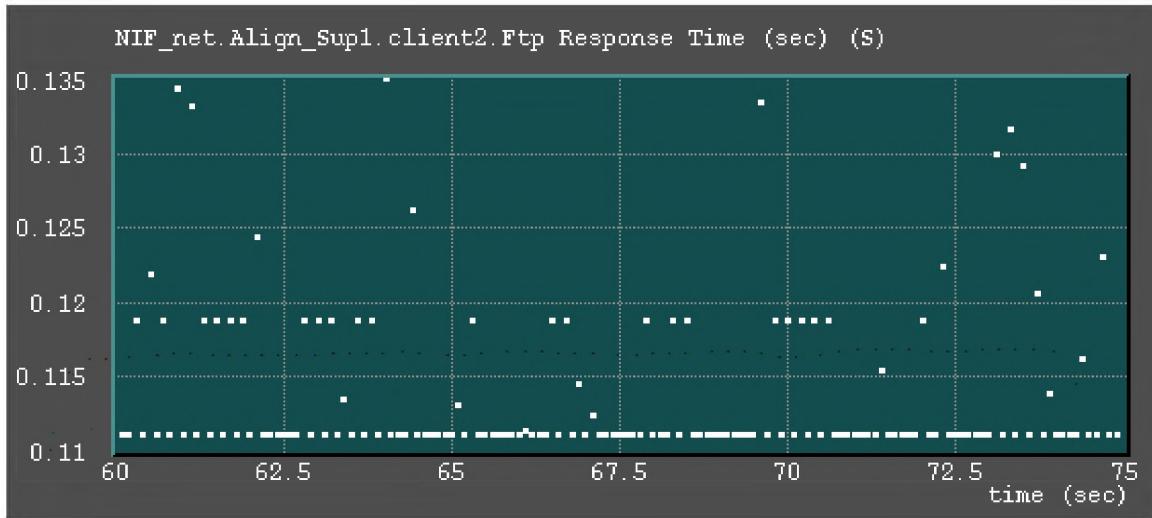
The following graphs show the service times for the two servers, the VFEP and the AC_FEP.



The VFEP server times varies from the minimum of 20.48 msec, to a maximum of about 45 msec which occurs when image frame requests from the Automatic Alignment system overlap with the streaming video requests. The Alignment Control FEP service times are constant at 62.5 microseconds, which is the service time that was set in the simulation. The service time is much faster than the request rate, so there is never an overlap in requests that would lead to service delays.

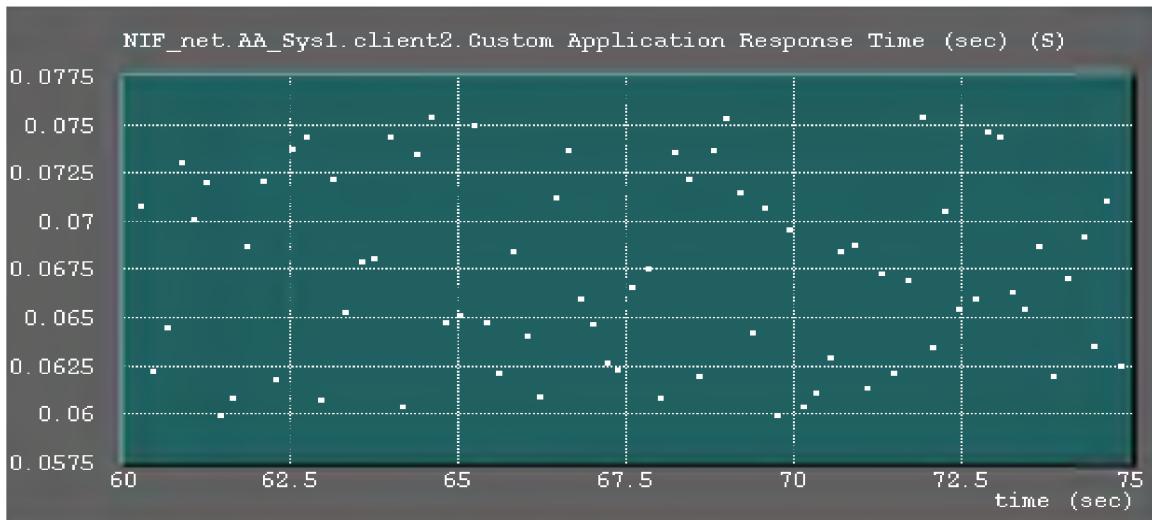
Round trip response time statistics were also collected, which includes all time between the time the Client process issues the request frame until it has fully received the response frame. This includes the server service times discussed above as well as the protocol stack processing times on both ends and the link transmission times.

The following graph shows the round trip response times for streaming video frames from the VFEP to the Alignment Control Supervisor. Note that the graph title indicates FTP. This is because the standard FTP traffic model in OPNET was modified to generate the desired traffic load.



The graph shows that the minimum response time is about 111 msecs. and the maximum is about 135 msecs. This latency is the sum of the service time and the transmission time of the image (about 2.46 Mbits), which at 30 Mbit/s takes about 90 msecs. This 100+ msec latency should be sufficiently low to allow manual alignment by a person at the supervisory console. The most critical factor is that the video data is received without large losses and that the jitter/variation between images does not become very large (e.g. >100 msecs) such that the video display would become jittery.

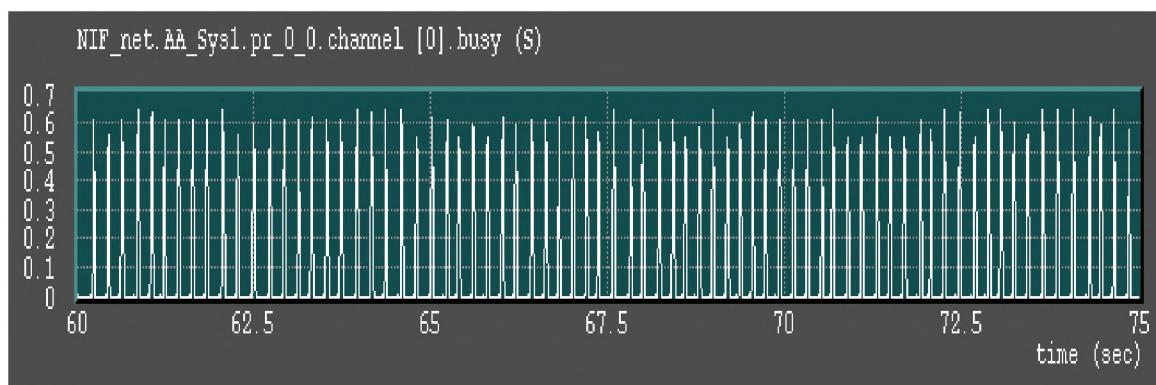
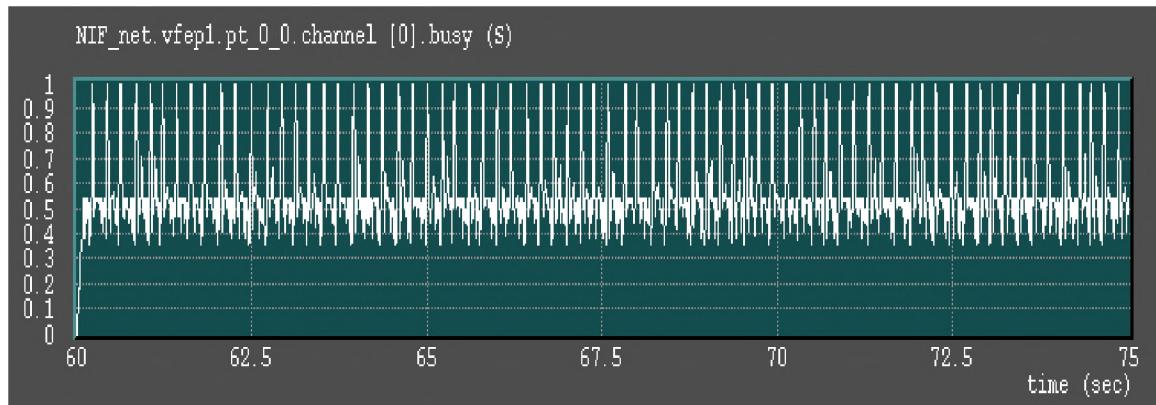
The next graph shows the response time of image frames from the VFEP to the Automatic Alignment system. In this simulation, since 90 Mbit/s is allocated to the three video streams to the Alignment Supervisor, the rest of the ATM bandwidth (65 Mbit/s) is allocated for image transfers to the Automatic Alignment system.



This graph shows a response time between approximately 60 and 75 msecs. A minimum of about 20 msecs is the VFEP service time and a minimum of about 40 msecs is the image transmission time, including TCP/IP protocol stack processing. The Automatic Alignment system will be simultaneously getting images from multiple VFEPs so this latency will not delay the automatic alignment process. Note that if the streaming video were turned off, so that all ATM bandwidth is available to the Automatic Alignment system, then these

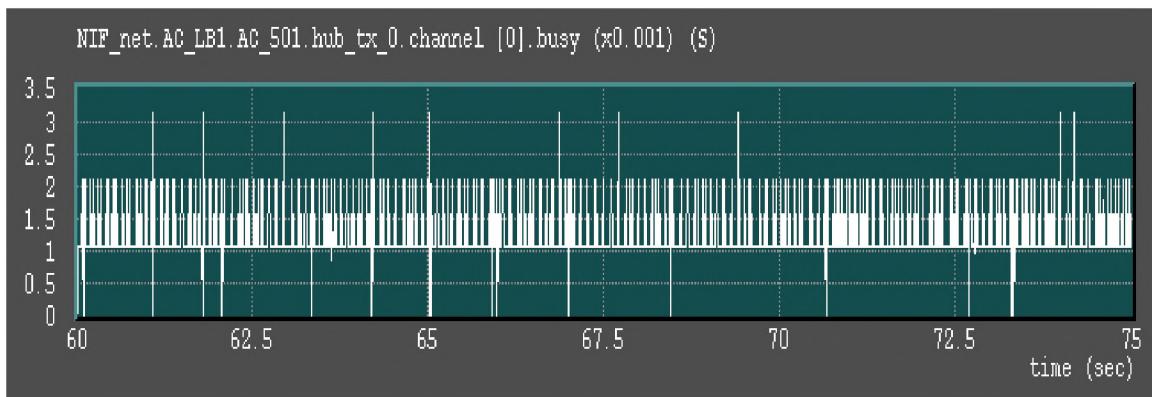
response times could be reduced to less than 40 msec., of which 20 msec. is assumed for VFEP service time.

Link utilization statistics were collected for the three ATM links and two graphs are shown below. The first graph is for the ATM transmitter on the VFEP and the second graph is for the ATM receiver on the Automatic Alignment system. Note that the utilization of the ATM link on the Alignment Supervisor is the difference between the first and second graphs. These % utilization statistics were moving window averages over intervals of 100 msec.

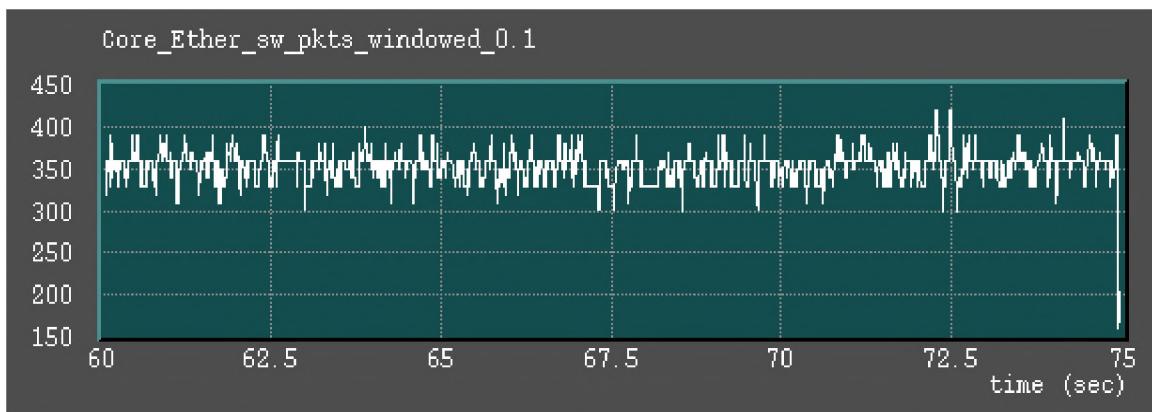


The VFEP ATM transmitter utilization is typically at about 50% due to the 3 streams of video (82 Mb/s). It bursts to 100% utilization when the Automatic Alignment system requests a video image. The Automatic Alignment system ATM receiver utilization jumps to about 60% each time a video frame arrives from the VFEP.

Ethernet traffic statistics were also collected. The utilization on the Alignment Control FEP is shown next and indicates that the 100 Mbit/s link is very lightly loaded, always being less than .3% utilization over the 100 msec. moving window.



The packet forwarding rate on the Core Ethernet switch is shown in the next graph, running between 300 and 400 per second, which is very light for Fast Ethernet switches. Ignore the dip at the end of the graph, which is an artifact of the moving window calculation.



Packet/cell loss statistics were also collected to ensure that data is not lost. This simulation assumed that the Bit Error Rate (BER) is zero (i.e. no bit errors occur). This was done so that any lost cells could be attributed to buffer overflow issues. In reality, bit error rates will occur very seldom in our switched Ethernet and ATM networks, so modeling them is not very meaningful. The BER specs are better than 10E-10. On a worst case link, one error will occur on average about every minute. In practice, links generally run with much lower bit error rates, particularly fiber optic links.

Network Analysis System

In order to be able to monitor and measure traffic on specific links in the network, a network analyzer system was procured. Such a tool is needed to capture and decode network traffic of interest, with timestamps on individual frames/cells. One can measure specific latencies on applications and network devices, link utilization, and distributions of traffic on the network. The ability to capture individual frames with time-stamps and decode them is not available on network management systems that access performance information with SNMP/RMON. Network management systems can collect global statistics, but do not have the detailed capture, filter, decode, and time-stamping features of network analyzers.

A review of commercially available network analyzers was performed which support 10 and 100 Mbit/s Ethernet and 155 Mbit/s ATM. As a result of this evaluation, the Network

Associates Distributed Sniffer System (DSS) was selected. Network Associates is the leading vendor for local area network analyzers, supports both ATM and Ethernet interfaces, has the best protocol decoding capabilities available, and has many features not available in other analyzers. For more information on the capabilities of the DSS, see [1] - [3].

There are two types of Sniffer systems available from Network Associates, a standalone portable unit and the DSS. The portable unit has both network interface types, but only one can be used at a time. The analysis data is only accessible from the portable unit itself. We selected the DSS solution because separate ATM and Ethernet units allow different network data to be captured simultaneously in different locations on the network, while being controlled and viewed from any location in the network. A DSS Console provides access to the Sniffer Analyzers (referred to as Sniffer Servers). The DSS Console windows can be displayed on any workstation supporting X-windows. This allows the analyzer to be controlled and monitored by any software developers, engineers, and technicians that want to analyze network traffic under test conditions.

There are three DSS Servers, two 10/100 Ethernet and one ATM. The Ethernet Analyzer analysis ports were attached to the Fore ES-3810 switch on 10/100 ports. The ES-3810 supports traffic sniffing by allowing traffic into any port to be output on other ports. This allows the selection of systems to be monitored through the switch's management system, which is also accessible from the network. Note that the traffic from all selected switch ports is multiplexed to the port attached to the Sniffer analyzer. The ATM DSS must be physically connected to the ATM link of interest. A pod (provided with the analyzer) optically taps (50/50) into both fibers and provides both signals to the ATM ports on the DSS. There are two ATM ports in the DSS for receiving traffic from both link directions. For testing, the ATM DSS was connected between "vfepp" and the Fore LE155 ATM switch. This allowed streaming video traffic to be captured.

All three analyzers are on-line, configured, and available for use in the ICCS Testbed. Experience in the use of these analyzers has been gained relating to configuration of capture filters and display filters, displaying captured data in different way (e.g. summary, decoded, Hex, ASCII), and saving configuration and data files.

Some bugs in the ATM DSS which have been referred to Network Associates. The most serious bugs are: 1) the timer used to time-stamp captured network frames runs about 10% too fast, and 2) the expert decode capability erroneously tries to decode the raw streaming video ATM AAL5 traffic as LANE 802.5 (Token Ring) data, leading to meaningless error-filled decodes. There is a partial workaround for (2), but not for (1). The timing problem does not exist in the Ethernet Analyzers. These bugs affected the data collected during our video capture test.

Streaming Video Data Capture

The ATM DSS was used to capture streaming video transfers in the Testbed between "vfepp" and "merced." The streaming video application sends video at a full 30 frames/sec, each frame being 640 x 480 bytes (307,200 bytes). This utilizes approximately 82 Mbit/s of the 155 Mbit/s ATM link bandwidth. The DSS is able to capture all data in this stream.

A summary view of a single video frame captured from a video stream is shown below. Note that due to the timing bug mentioned above, the Delta Times are low by approximately 10%. Also, the DSS erroneously decodes some of the AAL5 frames as LANE, although the actual data is captured correctly and can be viewed in detail.

The captured data shows that each video image is subdivided and sent over the network as 35 ATM AAL5 frames. The first AAL5 frame consists of 11 ATM cells (53 bytes each) which contain ASCII text and other data about the video image to follow. Next, there are 33 AAL5 frames, each containing 192 ATM cells. Each of these frames contain 9,184 bytes of data, which is the MTU size for this ATM interface. The last AAL5 frame contains the remaining 87 ATM cells of video data, completing the 307,200 byte image transfer.

Frame	Delta Time	Destination	Source	Protocol	Summary
22	0.0159771	DCE	DTE.video	Cell	Count=1 1
23	0.0005839	DCE	DTE.video	Cell	Count=1 92
24	0.0004968	DCE	DTE.video	Cell	Count=1 92
25	0.0004973	DCE	DTE.video	Cell	Count=1 92
26	0.0004993	DCE	DTE.video	Cell	Count=1 92
27	0.0004965	DCE	DTE.video	Cell	Count=1 92
28	0.0004973	DCE	DTE.video	Cell	Count=1 92
29	0.0004995	DCE	DTE.video	Cell	Count=1 92
30	0.0013423	DCE	DTE.video	Cell	Count=1 92
30	0.0013423	DCE	DTE.video	LANE	CTRL invalid X
31	0.0011498	DCE	DTE.video	Cell	Count=1 92
32	0.0014113	DCE	DTE.video	Cell	Count=1 92
33	0.0011495	DCE	DTE.video	Cell	Count=1 92
34	0.0009353	DCE	DTE.video	Cell	Count=1 92
35	0.0005071	DCE	DTE.video	Cell	Count=1 92
36	0.0004965	DCE	DTE.video	Cell	Count=1 92
37	0.0004994	DCE	DTE.video	Cell	Count=1 92
37	0.0004994	DCE	DTE.video	LANE	CTRL invalid X
38	0.0004971	DCE	DTE.video	Cell	Count=1 92
39	0.000497	DCE	DTE.video	Cell	Count=1 92
40	0.000497	DCE	DTE.video	Cell	Count=1 92
41	0.0004997	DCE	DTE.video	Cell	Count=1 92
42	0.0004964	DCE	DTE.video	Cell	Count=1 92
43	0.0004971	DCE	DTE.video	Cell	Count=1 92
44	0.0004992	DCE	DTE.video	Cell	Count=1 92
45	0.0006906	DCE	DTE.video	Cell	Count=1 92
46	0.0015598	DCE	DTE.video	Cell	Count=1 92
47	0.0008279	DCE	DTE.video	Cell	Count=1 92
48	0.0013073	DCE	DTE.video	Cell	Count=1 92
49	0.0011135	DCE	DTE.video	Cell	Count=1 92
50	0.0011136	DCE	DTE.video	Cell	Count=1 92
51	0.0004995	DCE	DTE.video	Cell	Count=1 92
52	0.0004969	DCE	DTE.video	Cell	Count=1 92
53	0.0004967	DCE	DTE.video	Cell	Count=1 92
54	0.0004994	DCE	DTE.video	Cell	Count=1 92
55	0.0004971	DCE	DTE.video	Cell	Count=1 92
56	0.0002246	DCE	DTE.video	Cell	Count=8 7
57	0.0027112	DCE	DTE.video	Cell	Count=1 1

The sequence of video image frames is repeated at the nominal rate of 30 frames/sec. The following table shows the Delta Times between the start of successive captured image frames. The nominal rate would be about 33 msec between image frames. As can be seen, there is some variation in the actual time.

Frame	Delta Time	Destination	Source	Protocol
93	0.0269858	DCE	DTE.video	Cell
128	0.0362176	DCE	DTE.video	Cell
164	0.0270949	DCE	DTE.video	Cell
200	0.0379714	DCE	DTE.video	Cell
235	0.0247965	DCE	DTE.video	Cell
270	0.0269317	DCE	DTE.video	Cell

References

- [1] "Expert Sniffer Network Analyzer Operations, Release 5.5," Network Associates documentation, PDF document.
- [2] "ATM Sniffer Network Analyzer Operations, Release 5.25," Network Associates documentation, PDF document.
- [3] "Distributed Sniffer System: Using the ATM Sniffer Server, Release 4.4," Network Associates documentation, PDF document.