Integrating Network Attached Mass Storage Systems into Educational Networks: Performance and Security Issues

Dennis Guster
Statistics Department/MCS Program
St. Cloud State University
guster@mcs.stcloudstate.edu

Charles Hall
Statistics Department/MCS Program
St. Cloud State University
chall@mcs.stcloudstate.edu

Abstract

In order to access the characteristics of a NAS (network attached storage) device, a case study approach was used to track the installation of one such device at a Midwestern university. Specifically, the NAS will be evaluated in regard to ease of installation, ease of configuration, ease of upgradability, ease of use by end users, security concerns, and performance characteristics under a variety of loads.

Introduction

The growth of computer networks has reached a pinnacle in that almost all devices in the business and educational world have access to some form of connectivity. Although this connectivity opens doors to vast amounts of information, the infrastructure supporting the storage and distribution of this information is often taxed to the limit. One component of this infrastructure is secondary storage. Traditionally, this network-accessible secondary storage is directly attached to some type of file server or host. The problem with this approach is that it labels that pool of storage based on the operating system of that device. In other words, space attached to a Novell server would be organized in Novell format, and a user must be attached to that server to access it. This logic often requires users to have pools of space on several different servers/hosts to support all of the varied applications they might run, and acquiring additional space is often cumbersome or not permitted. However, this diversity of space may have some advantages in regard to performance. By distributing the space across several devices, one can theoretically surmise that the contention on any one device would be lessened.

In an attempt to address some of the limitations of server/host attached storage, vendors have recently begun to offer network-attached storage (NAS) devices. These devices offer a single network entry point (i.e., samba servers) and are modular in nature. This means that a user can begin with a small single device and then upgrade painlessly to many devices offering hundreds of gigabytes of space. In fact, the process may only involve mounting the additional storage units on a rack, plugging them into an Ethernet switch, and spending less than a half-hour redefining the configuration through a web accessible interface. This is in sharp contrast to adding space to a Linux or Novell server. Although the advantages of NAS from an installation, management and scalability perspective are apparent, what about its performance characteristics? On the surface it looks like a centralized system may cause contention problems as the number of users and the amount of potential space available to them increases. Furthermore, does distributing this space results in security concerns beyond what would be expected with dedicated units?

Architecture

Servers, storage and networking have been described as the three pillars of computing [1]. This implies that getting the correct information to the correct place in a timely and secure fashion is paramount. Researching this simplistically stated goal is often easier said than done. In fact, there are often numerous trade-offs regarding network design decision that affect performance.

Currently there appears to be two schools of thought concerning how storage should be integrated into this model [2]. One school advocates server attached storage that is linked via high-speed interfaces, such as fiber channel [3]. The other school feels that storage should be independent of servers and their platforms and be directly attached to the network, hence the acronym, NAS (network attached storage devices). The latter is a

radical departure from the previous model in that it uses the network rather than a dedicated physical channel to transfer data and to perform management functions related to the storage function.

Therefore, the question arises: How well does this new type of traffic integrate into already taxed network environments?

The manner in which these devices attach to the network infrastructure provides some insight. For the sake of flexibility, redundancy and expandability, these storage systems are typically built upon the concept of independent modular units. Each unit contains about 100 gigabytes of raw storage space. A typical configuration would involve 4 units and because redundancy is built in, the yield would be less than the 400 gigabytes expected. Although each unit is an independent module, the logic built into each unit is designed so that all units work together in concert as a single network attached mass storage system. In terms of expandability, it is not unreasonable to configure up to 16 units as a single system.

How is this modularity supported by the physical network? Each unit has its own 100BASETX connection. Not only is this a fairly high performance industry standard, but potential bandwidth increases as additional units are added to the stack.

It is recommended that all units be connected to the hub or switch. This makes sense if one analyzes the packet flow from these devices. A quick analysis reveals that in addition to packets that contain data to be transferred to and from the mass storage system, a number of strictly management packets are transmitted as well. These packets are for synchronizing the individual units into a single mass storage system. By connecting all units to a single hub or switch, the communication path tends to be shorter and quicker. Furthermore, this management traffic remains isolated and does not interfere or cause degradation on other parts of the network.

While this solution appears to be efficient for handling the management overhead, how it affects the flow of data packets to a workstation running an application supported by data stored on the mass storage system merits analysis.

To a certain extent, this would be influenced by topology and architecture. In other words, what is its connective relationship among the hub/switch containing the mass storage system, the placement of the workstation, and the location of server to which the mass storage system is logically attached?

A quick analysis of traffic coming and going from the individual mass storage system units reveals a large number of management packets. In fact, based on one of our packet samples, it appears that one packet arrives on the network approximately every .014 of a second. The purpose of this traffic is to maintain the integrity of the redundant array of mass-storage system units. The traffic pattern involves incoming and outgoing packets in every possible combination among the mass storage units. A second category of traffic that appears a user management/configuration requests via a browser to a Java-applet.

This traffic is of limited intensity and sporadic especially after the original configuration is solidified. The last major category of traffic is applications requesting or writing data to/from the mass storage system. The intensity of this traffic of course is a function of the workload the sum of all applications that will access the mass storage system, its server, and the network itself.

Isolation of Overhead Traffic

Based on the sample of 10,000 packets recorded from a 143.9261 second time interval, one can conclude that the traffic pattern is pretty intense. In other words, about 70 packets per second, on average. In obtaining this traffic, only packets addressed to the samba server, the four mass storage units, and the requesting workstation were recorded. The ratio of data traffic to overhead traffic was quite skewed in favor of the overhead traffic. In fact, only about 200 packets containing data or a request to set up a virtual data circuit were recorded.

This ratio is not all that surprising in that only a single workstation was requesting data. However, this overhead needs to be further examined if intelligent network design decisions are to be made. Therefore, the question needs to be addressed – should the overhead and data traffic be combined in a single switch or separated into two physical channels, thereby requiring two switches.

Comparison of Combined Versus a Two-Channel Configuration

To provide objective data about these two different configurations, a simulation was programmed in Comnet III. In one model all traffic, both data and overhead, was transmitted together in the same physical channel. A second model was devised in which the data traffic and the overhead traffic were separated into two physical channels. As much as possible, values obtained from trapping packets were used to program the simulation. However, two major limitations need to be stated. First, certain values were not readily available such as the delay to be expected in each mass storage unit. In such cases the default values were used which certainly reduced the validity of the simulation. Second, there was a wide variety of the average packet interarrival rates among the samples taken that ranged from .014 to .0001. Therefore, for the sake of simplicity, the case study was run with the worst case scenario logic. In other words, the .0001 value was used, again raising validity questions.

Therefore, this simulation would provide information of limited value if the goal is to understand how a specific mass storage system will perform. However, the goal for this case study was to gain objective data about the relative performance of each topology under the same conditions. In that regard and that regard only, the results obtained are useful. Table 1 provides performance statistics regarding the network link(s) for each model.

Table 1
Link Characteristics

	Combined	two-channel front	two-channel back
utilization	57.67%	40.18%	36.27%
avg/delay (link)	.108 ms	.186 ms	.019 ms
avg frame size	208 bytes	1030 bytes	90 bytes
collided frames	3998	474	5017
avg deferral delay	.03 ms	.06 ms	.001 ms
delivered frames	5246	736	7513

The link utilization of the combined link was reduced from 57.67 percent to about 40 percent on the data link and 36 percent on the overhead link. The 57.67 percent is getting dangerously close to the 80 percent saturation level defined in basic queuing theory. By splitting the channels there certainly would be more tolerance for increased loads. The delay and frame size needs to be analyzed together. Because the data packets tend to be larger by nature, it takes longer to get the whole packet across the link. Also, it is interesting to note that the average frame size for the data channel is fairly well optimized while in the combined channel, it is reduced to about 200 bytes because of the influence of the overhead traffic.

Although it is not realistic to expect the physical channel(s) to be connected to a hub (in fact the makers of the mass-storage system strongly advise against it) in this simulation it was programmed as such to help illustrate potential contention problems. In all cases contention problems occurred at a surprisingly similar ratio. Therefore, the true interarrival rates of both the data and overhead packets need to carefully examined in any design that implements a mass storage system. In terms of deferral when the channel was busy the values again appear to be a function of the average packet size. The number of frames delivered in the 15-second simulation in which identical workload definitions were applied to each model reveals about 3,000 more packets were passed through the two-channel model. Perhaps this indicates more work done in the same time period. This would make sense if information is being delayed along the way and therefore sitting in queues longer in the combined mode simulation. To a certain extent this is supported by the results in Tables 2 and 3.

Table 2
Average Node Delays in Mass Storage System

	Combined Channels		Two-Channel	
Node	Send	Receive	Send	Receive
1	.0001	6.917	.025	.619
2	2.946	3.825	.103	.505
3	1.133	2.369	.027	.386
4	2.236	3.251	.038	.307

Table 3
Average Delays at the Workstation Level

	Combined	Two-Channel
1	.661	.376
2	.743	.215
3	.344	.146
4	.799	.166

Table 2 reports that the results of delay at the mass storage system node level in the mass storage system while Table 3 reports the delay in getting a message from the workstations to the mass storage system nodes. In almost all cases the delay is markedly less in the two-channel system. Again, this would support the contention that the two-channel system is reducing delays and hence queue lengths and therefore resulting in better performance.

Security Concerns

The first concern is related to some of the overhead traffic generated that goes beyond the stations directly involved. For example, the NTP (network time protocol) packets are broadcast to all stations on the home network. There have been documented cases of hackers devising attacks using this protocol mainly to reset the time back to an earlier time and replacing an authentication string [4]. Therefore, filtering this traffic beyond its intended audience may be a good idea. Also, a jini-announcements are multicast to address 224.0.1.84 and although they may perform some valid function (or be a byproduct) in a java-based application, the need to multicast them over the internet needs to be examined.

Within the rest of the packet traffic observed the source and/or destination addresses were to either mass storage system units or servers/workstations requiring access. A good share of the management traffic appears to be proprietary in nature and its payload is not

easily read with a packet sniffer. Some traffic, however, is readable, in particular, ping requests from the primary unit to the secondary units.

Therefore, protection of these units as much as possible would be recommended. The idea of isolating the units on their own switch would reduce the viewing domain if a packet sniffer were involved. Also, some type of packet filtering device should be placed between that switch and the outside to help protect against threats originating primarily from OSI layers 3 and 4.

Conclusions

It appears that a mass storage system has a number of merits to be considered when devising a strategic plan for networked storage. The ease of installment and configuration could be big time savers for network administrators. The same is also true for its ease of expendability and flexibility of access.

In terms of performance, the data samples analyzed did indicate that the packet interarrival times can be quite dense. However, their densities do not appear to be problematic on the 100BASETX architecture. Furthermore, the simulation programmed to test performance of a one versus two channel topology yielded some interesting results. This simulation which was programmed to reflect the worst case scenario in a 200-node domain indicated that even when data and overhead traffic were combined into a single channel that performance was still acceptable. Also, this simulation illustrated that the two-channel approach had advantages over the single-channel approach. This separation of management from data traffic may well have security advantages as well.

There appears to be several security concerns associated with the installation of a mass storage system. However, there are many questions associated with adding a Unix host to the network. Any networked device that supports the prime function of the business needs to be carefully analyzed and integrated into the comprehensive security plan of that business. Therefore, these devices will require firewall protection just like any traditional host.

Acknowledgements

This project was supported by a grant from Tricord Systems, Inc.

References

1. Dahl, Greg. “Server Appliances as Network Devices: Combining the Best of the Three Pillars”. White paper Tricord, Inc., 2000.

2. Farley, Marc. "Three Models for SAN-Based Data Sharing". Infostar, February, 2001.

3. Moore, Fred. "Storage Networks Start to Converge. NAS Gains Momentum and Respect". Computer Technology Review. 20:4, April, 2000.

4. Bishop, Matt. "A Security Analysis of the NTP Protocol". 6th Annual Computer Security Conference, Tucson, AS, 1990