STATISTICAL MONITORS FOR LOCAL AREA NETWORKS

David C. Feldmeier

Massachusetts Institute of Technology

Laboratory for Computer Science

Cambridge, Ma. 02139

Abstract

As local area networks become more common, there is an increasing demand for network management tools for these networks. These management tools need to make network measurements, and measurement devices for local area networks have been built for network research. This paper describes network measurements of interest and the types of network monitors that can obtain these measurements. The token ring network monitor at the MIT Laboratory for Computer Science is described. Other existing monitors and the monitoring functions included in the Texas Instruments token-ring chipset are mentioned briefly.

1. Introduction

Network management requires real-time surveillance and control of a network, including:

- 1. Real-time measurement of network parameters
- 2. Real-time analysis and summarization of network measurements
- 3. Interpretation of summarized measurements
- 4. Action based on interpretation of these measurements

A network monitor performs the first two of these functions - it collects network data and presents it in a usable form. For an interconnected system of networks, a single network monitor is desirable for maintenance of the entire system. The main monitor must receive information about each individual network, so each network needs its own network monitor. This paper discusses only network monitors for a single network, although some of the ideas are applicable to more general monitoring systems. Also, the network monitor as described in this paper is purely a measurement device - it is unnecessary for the normal operation of the monitored network.

The purpose of network monitoring falls into three categories: performance analysis, performance verification and network management. Monitors have been built by network researchers for performance analysis and comparison of actual network performance with that predicted by analytical or simulation studies^{1, 2, 3, 4}. Performance verification is similar; this type of monitoring ensures that a network meets its design specifications. Network management monitoring is to determine whether a network is operating properly and to watch for performance changes caused by degradation of some network element.

Statistical monitors collect statistics about network traffic rather than keep a complete record of network transactions. Because the traffic on larger networks easily may exceed one million packets per day, the storage requirements for a complete record of network traffic is excessive, especially for long-term monitoring over weeks or months.

Packets therefore must be reduced to statistics soon after arrival. Because the original data cannot be recovered from the statistical data, the data reduction process must be carefully developed so that all necessary information is retained, while unnecessary data is discarded to ease storage requirements. Before a monitor is developed, the measurements of interest must be determined.

A change in the network error rate can predict the failure of some network element. The number of packet errors should be measured to determine the network error rate. A properly operating network has a low error rate; an increased error rate could be caused by a network component that is about to fail. Correlating the network error rate with the network configuration and active hosts could isolate potential failures.

Network utilization is an obvious way of determining whether a network is operating properly. Network utilization includes both the packet rate and the network load for various time intervals. One set of measurements should be the network utilization over one minute intervals for a week. This measurement allows the

network usage for various times during the day and various days during the week to be compared. Network performance should be evaluated during periods of high utilization. If performance is inadequate, then the network should be split and the pieces connected by gateways. Two networks with low utilization may be combined to eliminate a gateway and improve overall network performance. Bulk data transfers and network maintenance should be performed when network utilization is low.

Another measurement is of network utilization for one second intervals over a short (5 minute) period at various times during the day. This shows how the network utilization varies over short periods of time, something that cannot be determined by the long-term measurements.

Not only should network utilization be measured for the entire network, but it should also be measured for each host on the network. This measurement can be simpler than the one for the entire network, perhaps just a packet and byte count for each host. This allows the hosts with the heaviest loads to be detected. The optimization of hosts that transmit a large amount of traffic provides the largest overall improvement in network performance. A list of currently active hosts may be useful for determining if a host is at fault when the network utilization of each source-destination pair of hosts. Heavily utilized source-destination pairs should be on the same network, rather than communicate through a gateway, for the best performance.

Interpacket arrival time measurements are useful for determining network interface and network server performance. If many packets arrive too closely spaced, a network interface is unable to receive all the packets. Good performance is particularly important for a network server that may be serving several stations simultaneously and receiving packet from all of them.

Packet length distribution shows the types of applications running on the network; for example, remote login produces short packets and data transfer produces long packets. Also, some network software has a maximum packet size that it will accept, and any packets exceeding this size can be detected by the monitor.

The number of packets transmitted for each network protocol shows the types of protocols used and the popularity of each. This allows the detection of widely used protocols, and these protocols should operate efficiently for good network performance.

Channel acquisition delay is the amount of time that a packet must wait at the source before it is transmitted on the network. The distribution of delay time determines whether the network can support real-time applications, such as voice transmission. If the delay time varies widely, the network may be too loaded for

real-time applications.

2. Types of Network Monitors

Several different types of network monitors may be built, each with its advantages and disadvantages. Three basic types of monitors are the probe monitor, the host monitor and the spy monitor. These monitor types were first discussed in an MIT Laboratory for Computer Science internal working paper by Liba Svobodova.

2.1. The Probe Monitor

The probe monitor is the simplest of the three monitors. Unlike the other monitors, which collect information on existing network traffic, the probe monitor is an active monitor that measures only its own traffic.

A probe monitor injects packets into the network at intervals, an approach that corresponds to random sampling of the network state. The probe monitor observes the channel acquisition delay, transmission delay, and transmission errors for each injected packet. On a token ring, the acquisition delay is the waiting time until a token arrives and is thus a measure of the traffic load on the network. The transmission delay is the ring round-trip propagation delay, a measure that approximately determines the number of active nodes on the system.

A disadvantage of the probe monitor is that it adds traffic to the network, and thus introduces a monitoring artifact. Also, the probe monitor measures the frequency of network events, but its measurement resolution for event durations is determined by the time between probe packets. A short interprobe time increases the duration measurement resolution, but it also increases the monitoring artifact. If the monitoring artifact is reduced, then the resolution decreases. Although the probe monitor is simple, the information that it collects is limited.

2.2. The Host Monitor

Another approach to network monitoring is to have each host maintain a record of its transactions on the network. If all hosts are monitored, then complete information is obtained, although most likely each host will do some data reduction to reduce the storage requirements. The monitoring may be done with either hardware or software.

A hardware monitoring system includes network monitoring equipment on each network interface, and thus requires no modifications to the hosts. It is difficult to modify existing network interfaces, so this approach mainly applies to future network interface design. A hardware monitoring system, even if initially included in the network interface design, increases the cost of the

network interface. Users who have no interest in network monitoring may not wish to purchase network interfaces with network monitoring equipment, because of the higher cost. On the other hand, a low-cost hardware monitoring system may be unable to collect enough information.

A software monitoring system requires no hardware modifications, and can be used with existing equipment. The software approach is more flexible than the hardware approach because monitoring software is easily modified. A problem is that the monitoring software will increase the processing load on the host, which may affect the host's network behavior. Some machines, such as personal computers, may be unable to accommodate the additional load. Also, different versions of the monitoring software are needed for each type of host on the network, making the software more expensive and difficult to maintain than a single monitoring program. As a practical matter, it may be difficult to obtain permission to install and maintain monitoring software on some hosts, particularly on a network that crosses administrative boundaries.

Regardless of how each host is monitored, somehow the collected data must be correlated at a central location. If network monitoring need not be done in real time, then each host simply stores the recorded data and transmits the data to a central location at a later time. For network management, however, real-time monitoring of the network is essential. If the monitoring is done in real time, then the data could be communicated to the correlator by some secondary channel, the most obvious being another network. This is likely to be expensive and impractical. The alternative is to transmit the data via the network that is being monitored, which introduces a monitoring artifact and distorts the network measurements. This method also introduces positive feedback onto the network; if the network becomes loaded, the monitoring data transmitted via the network increases the network load even more.

Also, if the network itself is involved with the monitoring process, if the network malfunctions, then the monitor loses some if not all of its capabilities. Clearly, this is unacceptable because when the network fails is when a working monitor is the most heeded.

Another problem is that the correlation of the data recorded at the hosts requires that the timing of all network transactions be accurately recorded. All hosts therefore need accurate, synchronized clocks. Also, as the number of hosts increases, the processing time at the correlator may become large. Because host monitoring collects complete information, the correlator requires a large amount of storage. The monitoring of all hosts is impractical and expensive and is only justified if the desired data cannot be collected in some other manner.

A variation on the monitoring of all hosts is to monitor some subset of the hosts on the network. The problems

are the same as those of monitoring all hosts, but the magnitude of the problem is reduced. Selected monitoring biases the collected data, but the bias can be corrected for if the differences between the monitored host and a typical host is accounted for. Unfortunately, the statistics of a typical host are difficult to determine unless all hosts are monitored. a discontificación o

" Lead to the contract of the second state of

deposit Translate agency (Albert 1994) of L 2.3. Spy Monitor

The spy monitor provides more information than the probe monitor and is simpler than host monitoring. The spy monitor is a special dedicated network host that passively receives all packets on the network.

The spy monitor is a passive system that receives and analyzes all traffic passing by its network interface. A spy monitor perturbs the network by adding a network interface, but no other modifications to the network or its hosts are necessary. Because the system is passive, it produces no monitoring artifact and collects statistics over a long period with little inconvenience. A spy monitor must be fast, have a large amount of storage, and be able to assimilate data at the maximum speed of the network for at least a short time. On a network that has more than a million packets a day as does the MIT token ring, the storage requirements are in the tens of megabytes per day. If the data is not stored, then it must be analyzed as it is collected. The analyzer must also be able to analyze data at the maximum packet arrival rate. del figuradità e delle le compre el

The spy monitor appears to be the best approach to network monitoring of the options considered. It obtains the most information with the least amount of modification to network and its hosts.

2.4. Hybrid Monitors No matter what network information must be collected. a spy monitor is probably the best approach. However, some data of interest may not be collectible with a spy monitor, in which case a hybrid monitor is needed. A hybrid monitor is simply a combination of the above monitors as necessary to collect the data of interest. For example, a type of data that a spy monitor cannot collect is the transmission time of a packet. This requires that either a probe monitor or a host monitor be used in conjunction with a spy monitor if this information is required. collecte vites stand-alone softw in

Although not a monitor itself, a traffic generator is sometimes used with a monitor for testing the network under high-load conditions. A traffic generator generates artificial traffic, usually much more traffic than the hosts on the network. Edutes the real-time display data, and further

compromes the data for transmission to the data

ek sama - 👀 en gung filmenan da Arkitikasan sebali

lo salve Jage amiliane broom textone deall

3. Existing Statistical Monitors

Statistical monitors have been built at MIT and at other institutions for network research purposes. This section describes the MIT system in detail and briefly mentions work done by others:

3.1. The MIT Token Ring Statistical Monitor

The MIT token ring statistical monitor is a spy monitor, a design chosen for simplicity and effectiveness. The monitor is designed to collect information about a ProNET ten megabit token ring local area network. Monitors derived from the MIT monitor are running at Bell Communications Research and Proteon, Inc. The complete monitor consists of two parts: a tlata collector and a data analyzer. The data collector receives all packet on the network and extracts the relevant information from each packet. This data, along with each packet's arrival time is formatted for transmission to the data analyzer. The data collector also does some simple real-time data analysis. The data analyzer analyzes and stores the data from the data collector.

The data collector is a PDP 11/20 minicomputer with two specially configured network interfaces and an auxiliary monitor board. The monitor needs two network interfaces to provide accurate measurements because each interface has only a single receive packet buffer. Whenever a network interface receives a packet, there is a time while the interface is being readied to receive the next packet during which the interface cannot receive a packet. Although this time is minimized in the monitor by using fast assembly language interrupt routines for the network interfaces, packets can still be missed. The second network interface on the monitor is modified so that it only receives a packet if the first interface does not, and thus minimizes the number of packets missed by the system while assuring that no packet is received more than once.

The auxiliary monitor board provides a 32 bit, 25 microsecond resolution clock for timestamping packet arrivals. The auxiliary monitor board also interrupts the processor each time the token on the ring is lost or reestablished, so that the number of token losses and the total ring operational time can be measured. An external frequency counter observes either the frequency of the monitor's phase-locked loop modem (and thus the ring's operational frequency) or the inter-token arrival time.

The data collector runs stand-alone software written in the C programming language for ease of programming and good system performance. The network interfaces are serviced by interrupt routines that extract relevant packet data and place this data in a large circular buffer. The main program extracts this data from the circular buffer, updates the real-time display data, and further compresses the data for transmission to the data analyzer. Each packet record contains eight bytes of data:

- 1 byte of ring source address
- 1 byte of ring destination address
- 1 byte of higher level (Internet Protocol).
 protocol field
- 2 bytes of packet length
- 3. bytes of packet arrival time data (25 μs resolution)

the tollware approach is deal at the little

Although the data collector does mostly collection and compression of data, it also provides some real-time data analysis. The data collector displays the current, previous, and peak number of packets and network load for the time periods of a day, hour, minute, and second. Also displayed are the number of packet errors, the time since the last token recovery, and the cumulative ring down time.

The data analyzer is a VAX 1147750 timesharing system running the Berkeley Unix operating system. The data analyzer runs a program that receives compressed data from the data collector and either stores the information for every packet or uses the data to update various histograms on the data analyzer. Complete storage is usually impractical because the network carries over one million packets daily, producing over 8 megabytes of data-daily.

In addition to the suggested measurements described in section; one, the MIT monitor salso measures the cumulative ring up time. The measurement results may be found in an MIT Laboratory for Computer Science technical memorandum. The data for each packet is processed and stored as histograms on the data analyzer. Other programs on the data analyzer read these histograms and present the data in a usable form.

The data collector and the data analyzer should be connected by a communication link other than the network that is being monitored to avoid introducing a monitoring artifact. Unfortunately, due to cost, the data collector sends packets of compressed data to the data analyzer via the monitored network. The data collector transmits less than one percent of the packets on the ring, so the measurement distortion is minor. To further reduce the monitoring artifact, the data collector does not count its own packets.

3.2. Other Statistical Monitors

Shoch and Hupp built a monitor for the three megabit experimental Ethernet at Xerox Palo Alto Research Center⁴. The Ethernet there spans 1800 feet and connects over 120 machines. Their monitor is a spy monitor that runs a series of specialized monitoring programs to collect network data.

the standard of Spokia antiference. Our protecting thing is they

In addition to the spy monitor, which makes the measurements described in section one except for channel acquisition delay, the Xerox monitor also uses a probe monitor to measure the acquisition delay and the number of collisions on the Ethernet. An artificial traffic generator is also used to study network performance under high load.

A monitor was built by Amer for the National Bureau of Standards for measurements of the NBSNET¹. The NBSNET is a one megabit CSMA/CD network similar to the Ethernet. The NBS monitor is a hybrid monitor which consists of a spy monitor for most measurements, but also includes some host monitoring.

In addition to the measurements described in section one, the NBS monitor also measures total packet transmission delay, the number of collisions, and the number of tries that each packet requires for successful transmission. An artificial traffic generator is used to determine network performance under high load.

Another statistical monitor was also built by Amer, but this time at the University of Delaware for a ten megabit Ethernet². This monitor is similar to the MIT monitor because it is a spy monitor that sends compressed versions of the collected data for storage and analysis to another machine on the network via the network being monitored.

The monitor makes the measurements in section one except for channel acquisition delay and the interpacket arrival time measurement. Instead, the monitor measures the number of packets to arrive during a one second interval. Although this measurement provides some information similar to that provided by interpacket arrival time, it is probably not as useful a measurement in general.

5.1

FA. 179 500 A

4. Network Monitoring in the TI Token Ring Chipset

Texas Instruments produces a chipset which not only supports the IEEE 802.5 token ring standard but also provides some network management functions. The chipset contains several counters, one for each type of network error that is measured. The error information is periodically transmitted to a Ring Error Monitor (REM) with special type of packets called a Medium Access Control (MAC) frame. MAC frames are for network monitoring and control functions on the ring. The system is a form of host monitoring if the REM only accumulates host error data and makes no independent network measurements. Because each individual station reports observed errors, the REM monitor has powerful diagnostic capabilities for network maintenance.

A problem with this approach is the same as that of any host monitor; any disruption of the network also disrupts the network monitor. Also, although this

system is fine for maintenance of a single local area network, it is unsuitable for determining which hosts should share a network, how various networks should be inter-connected, whether a network is over- or under-utilized and similar questions of importance in a multinetwork environment. The REM must measure the network state directly, and thus become a hybrid monitor, for the most effective network management.

allegate agreement a property

5. Conclusion beausing a strict end

Network management requires that network measurements be made in some manner. This paper suggests measurements of interest, describes different types of network monitors, and specifically describes the monitor, implementation at MIT. Other existing monitors make measurements similar to those made by the MIT monitor. The Texas Instruments token-ring chipset supports some monitoring functions in each network interface that are useful for maintaining a single network but may be inadequate for a multi-network environment.

Network monitoring is a vital part of any network management system. Although some types of measurements have been suggested, more experience is needed to determine the best network parameters to measure and how to interpret them.

akanan ji jerope na trada persek ina imirene Miratiar. Kabupat kareti ki ji pala a kabupatan ketak ka a ina a

References and all the ware of the and by an

- 1. Paul D. Amer, "A Measurement Center for the NBS Local Area Computer Center", IEEE Transactions on Computers, Vol. C-31, No. 8, August 1982, pp. 723-729
- 2. P. D. Amer, et. al., "Local Area Broadcast
 Network Measurement Traffic Characterization",
 Tech. report 86-12, Department of Computer and
 Information Sciences, University of Delaware,
 January 1986
- 3. D. C. Feldmeier, "Empirical Analysis of a Token
 Ring Network", Technical Memorandum TM-254,
 MIT Laboratory for Computer Science, January
 1984
- 4. John F. Shoch and Jon A. Hupp, "Measured Performance of an Ethernet Local Network", Comm. ACM, Vol. 23, No. 12, December 1980, pp. 7f1-721.
- State of Texas Instruments, Inc., TMS380 Adapter

in' and about radered and deer the autabar in the

con resees the man for an inversion on a contract the Europe rule of the contract to the contract of the contr

In addition to the upy mapper, which calm the removement of charge in action one sample for charged for second sec

A monitor was built by Amer for the Caledari Servand of Standards for consequences of the NESSELT. The NESSELT is a one margable Calefa Conservate consistent to the Science of the NESS are noted to a soluted monitor but also make manufacturing.

In within a the memorana described is audient out, the 1945 member was memoral falls parted the compact of collections and the reported of collections and the reported of the reported for reported to reported the reported the reported to reported the reported to reported the reported to reported the reported the reported to reported the reporte

the many of the contract of th

The mornior makes the presentational of the integralists overpt, for objected samplement withy and the integralists street that the makes of property to same the mornior of property to same ourne a second integral which the nonnewement provides come integral provides in the nonnewement provides come in the makes and the intermediate contribution in the property and a suppression of potential

4. Network Monitoring in the TI Tolem Ring Chippet

Texas Instruments produces a characteristic code only supports the 1000 and a token ring standard but also provides gone notated management (uncotons). The object contacts revisal counters, and for each type of management of the outer information is periodically transmitted or a stress firm of the outer information is periodically transmitted or a stress factor observe (SEM) with appeared type of puriodic collect a birthma Alense monitoring and country branch based or the first management of the first monitoring is form of bost monitoring if the first monitoring is a love of the first monitoring in the first monitoring and management is a love of the first monitoring the powerful network magnification countries for attracts and monitoring has powerful diagrams in a powerful diagrams in a powerful diagrams in a powerful

A problem with the approach is the name of third of the bost soonier, any distingtion of the network the disrupts the network monitor. Also, although this

release the transported for descriptions which produced a second areas are a second by the control of the various and and a control of the various and the control of the various and the various and various an

medical made 2

Principle Self response to the company of the representation of th

Detecti morganica is a cital past on our meaning transportation of transportation of the transportation of the court of the transportation of the transpor

Red merpilodi

Hard D. James "A Measurement Course 18th the NESS from Seesa Computer Control." IEEE Thursdeliver on Computers Vol. Cot. No. 8, August 1982, pp. 723-758.

- T. D. Anger, et. 23. "Local titre Evaduals Network Mars uniques Tradic Computer and Tach cuport No.12, Department of Computer and Information Sciences, University of Decision, Indianally rolls."
- D. G. Neidmann, "Simplemed Analysis of W. Token String Verwerk," Technical Memorandrum Till 254, MIT Linkerstone for Computer Schools Pentucy 1984.
- John F. Smern and Von A. Ellippi, "Manufed Performance of an Ethernal Local Network" Comes MCM Vol 23 No. 12 December 1930, pp. 741-721
- Owigaet Citie V Guada, 1980
 - Control of the Contro