Event-based Network Traffic Monitoring In A Wide Area Network

Katsuhisa ABE and Glenn Mansfield Keeni

19 Feb. 2005

Abstract

Network monitoring is necessary to evaluate the performance and to ensure operational stability and efficiency. We, netman WG, have been monitoring traffic statistics for the JGN II network and are studying the results.

In this presentation, we introduce our monitoring and analysis activities. We have focused on two statistics, one is traffic volume, the other is latency. These statistics provide valuable hints about the underlying network's quality of service and throughput.

We also introduce the concept of "event-oriented network management" and discuss some techniques to detect network events using the above statistics.

1 Introduction

Network traffic monitoring is an important aspect of network management and security. For example, observations may reveal the effects of events such as a network failure, an operational failure or a security incident, on network traffic. There are several other usages of network traffic monitoring e.g. in QoS estimation, bandwidth planning etc. But, in routine network monitoring, the interest is on events. If there are no events of interest, the network manager will probably not want to "look" at the traffic. The traffic data in such cases is destined for archiving. From there it will probably be backed-up on off-line media or discarded.

Present monitoring systems do not have a mechanism of detecting events of interest. So it appears that the operator will either look at all the traffic to detect events of interest or will not look at the traffic at all. In our work we attempt to mechanically detect events of interest and draw the operators attention to these events. We use data from a wide area network to examine the utility and effectiveness of the approach.

The process of mechanical event detection heavily depends on the availability and the accuracy of the data. But in a standard monitoring environment there is little guarantee for these two factors. To raise the availability and accuracy of the data we propose the deployment of multiple data collectors at geographically and network topologically separated points. We have carried out experiments on a wide-area network, and have examined how the quality of the data can be raised i.e. how the availability and accuracy of the data can be increased using the collection redundancy.

In Sec. 2 we introduce our monitoring environment. In Sec. 3 we examine the issues involved in raising the data availability and accuracy using data from multiple pollers. In Sec. 4 we discuss the methods of analyzing the data to detect events. In Sec. 5 we describe our ideas of "event–oriented network management".

2 Environment

For our work we set up a monitoring environment over the large-scale very high-speed network the Japan Gigabit Network II (JGN-II) [1].

JGN-II is an open test-bed network environment for research and development and provides nationwide IPv6 network and optical wavelength networks in Japan.

We are executing a project on network traffic monitoring JGN-II network. Our aim is to provide network users with network traffic information. We have deployed passive probes which comprise of some tapping equipment. The probes are placed at various sites in Miyagi, Tokyo, Gifu, Kyoto, Hirosihma and Saga. These probes watch the network traffic and generate statistics. The network statistics are collected by data pollers placed in Sendai and Kyoto using the standard network management protocol SNMP.

Table 1 shows our monitoring topology as of 26 July 2004. The polling agents at Sendai and Kyoto poll the passive probes every 60 seconds using SNMP over IPv6. The traffic data is available for viewing at [2].

We show the monitoring traffic statistics in table 2. Here "other protocols" denotes packets which had an IPv6 packet header but the next header field is not ICMPv6, TCP or UDP. We have also collected elapsed time information obtained by executing traceroute6 from the data collectors to the probes.

Table 1: Monitoring Environment in JGN II

Items	Number
Sites where probe is placed	9
Placed probes	10
Monitoring points	11
Monitoring links	26
(with VLAN)	(19)
Polling Agents	2

Table 2: Measuring statistics

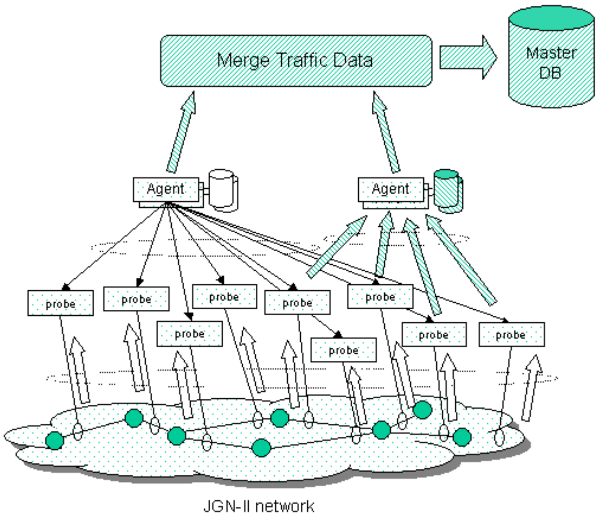
IPv6 packets/traffic volume
ICMPv6 packets/traffic volume
TCP over IPv6 packets/traffic volume
UDP over IPv6 packets/traffic volume
Other protocols packets/traffic volume
SNMP Polling Interval
Elapsed time by Traceroute6

3 Multiple Monitoring

In a standard monitoring environment there is little guarantee about the data availability and accuracy. In the data collection process we use SNMP over UDPover IPv6, to collect traffic statistics from the passive probes. UDP does not guarantee the delivery of packets. So packets may get lost. The applications do several retries in case a response is not received. Yet the case of a response being missed due to packet loss may not be ruled out. There may be also be the case of data loss due to problems at the data collector. The data collector application maybe overloaded, or dead, the data collector host may be overloaded or down. To raise the availability and accuracy of the data we deployed two data collectors at geographically and network topologically separated points.

With data from multiple data collectors we attempt to synthesize a data repository that has data availability and accuracy levels greater than or equal to that of the archives of the individual data collectors. First we select a master archive for the traffic statistics by comparing the data contents of the archives of data collectors. The parameters that are considered in

Fig. 1: Data Merge



selecting the master archive are the number of successful polls, the mean polling interval and the variance of polling interval. The archives that are not a master archive are auxiliary archives. In the next step, we complement the traffic statistics of the master archive with the missing data points, wherever possible, from the auxiliary archives. Finally, wherever there is a fluctuation in the polling interval, the polling interval is normalized by interpolating the traffic data.

In short, our plan to merge traffic statistics comprises of the following steps:

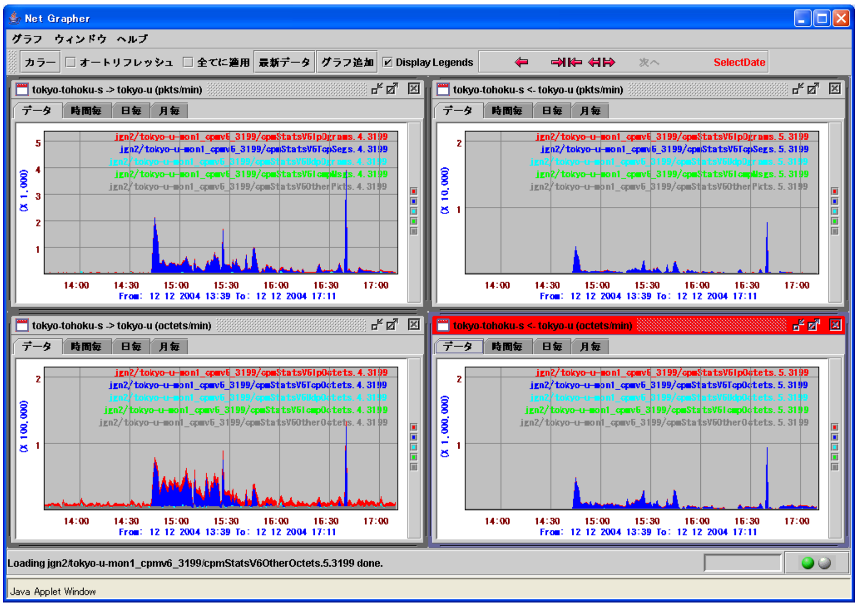
1. Select a master archive
2. Complement the master archive with data from auxiliary archives
3. Normalize the time stamps

4 Network Analysis

To mechanically detect events of interest, we use JGN-II's traffic statistics. We focus on two statistics viz., traffic volume and latency. We discuss the properties of these statistics and describe techniques to analyze them.

4.1 Traffic volume

Traffic volume may be considered to be as one of the indicators of network status. For example, lack of traffic may indicate some network event like a network fault. On the other hand an unusually large traffic may indicate that a DoS attack is underway. The following figure shows the traffic volume between Research Institute of Electric Communication in Tohoku University and the University of Tokyo on Fig. 2.


Net Grapher
グラフ ウィンドウ ヘルプ
カラー ☐ オートリフレッシュ ☐ 全てに適用 最新データ グラフ追加 ☑ Display Legends
次へ SelectDate
tokyo-tohoku-s -> tokyo-u (pkts/min)
tokyo-tohoku-s <- tokyo-u (pkts/min)
tokyo-tohoku-s -> tokyo-u (octets/min)
tokyo-tohoku-s <- tokyo-u (octets/min)
データ 時間毎 日毎 月毎
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6IpDgrams.4.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6TcpSegs.4.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6UdpDgrams.4.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6IcmpMsgs.4.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6OtherPkts.4.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6IpDgrams.5.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6TcpSegs.5.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6UdpDgrams.5.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6IcmpMsgs.5.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6OtherPkts.5.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6IpOctets.4.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6TcpOctets.4.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6UdpOctets.4.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6IcmpOctets.4.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6OtherOctets.4.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6IpOctets.5.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6TcpOctets.5.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6UdpOctets.5.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6IcmpOctets.5.3199
jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6OtherOctets.5.3199
(X 1,000)
(X 10,000)
(X 100,000)
(X 1,000,000)
1 2 3 4 5
14:00 14:30 15:00 15:30 16:00 16:30 17:00
From: 12 12 2004 13:39 To: 12 12 2004 17:11
Java Applet Window

Loading jgn2/tokyo-u-mon1_cpmv6_3199/cpmStatsV6OtherOctets.5.3199 done.

Fig. 2: Traffic Graph between RIEC in Tohoku University and the University of Tokyo

In our project we have provided an easy to use graphical user interface where the user can view the desired traffic by a few mouse-clicks (Fig. 3).

4.2 Latency

Network latency is one of the important indicators of network operational status. It may be used to evaluate quality of service and to estimate throughput for network application. We focus Round Trip Time (RTT) to examine latency.

There are many tools to measure RTT, such as ping, traceroute, skitter, pchar etc. RTT represents different statistics for each of these tools. In the following, we clarify the definition of RTT.

Figure 4 shows the path of a packet from one application to another

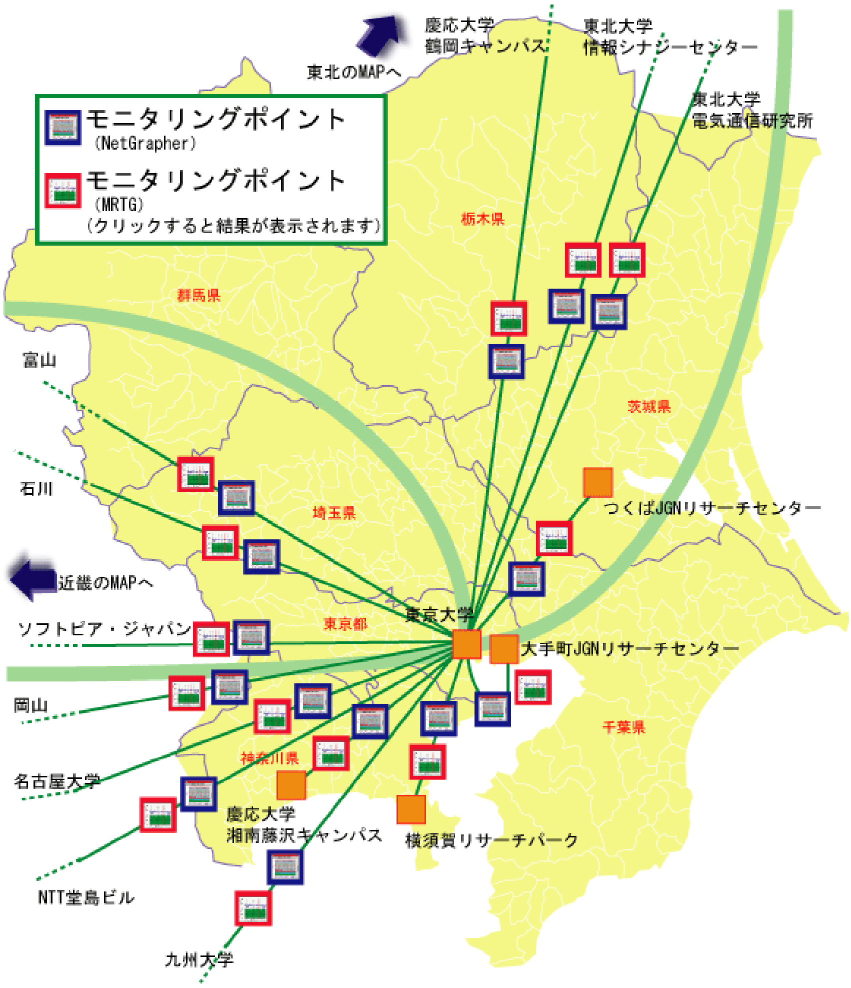


Fig. 3: Clickable Map to show network traffic

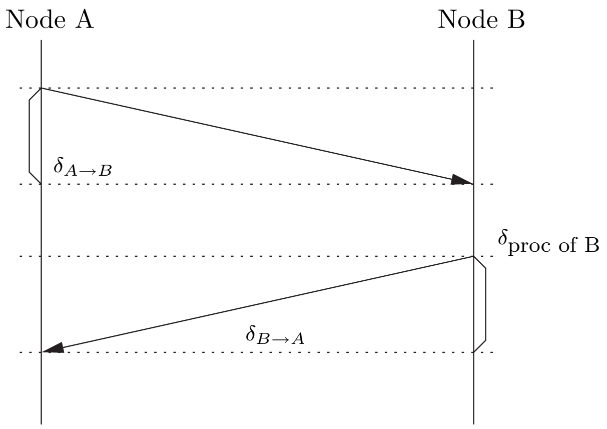


Fig. 4: diagram to measure Round Trip Time

across the network. The RTT from node A to node B along single path may represented by $\mathrm{RTT}_{A\to B}$ as

$$\mathrm{RTT}_{A\to B} = \delta_{A\to B} + \delta_{Proc}(B) + \delta_{B\to A}.$$

The first term ($\delta_{A\to B}$) stands for the time which packet takes from Node A to Node B, and the second term ($\delta_{B\to A}$) vice versa. The last term ($\delta_{Proc}(B)$) denotes the time taken at Node B to process the received packet and return a response.

If the application to measure the RTT is changed, the change will be reflected in latency. It is easy to imagine if we measure the RTT for a ping command and for and HTTP get command, the results will be very different. In our work, we examine two different RTTs. The first is the round trip time measured by traceroute6. Traceroute6 is the IPv6 version of traceroute. It sends UDP packets over IPv6 protocol. The payload length is 20 bytes. The IPv6 header is 40 bytes. It controls the “hop limit” field in the IPv6 header and attempts to elict an ICMP6 TIME_EXCEEDED IN–TRANSIT and finally obtains an ICMP6 PORT UNREACHABLE response. This method measures the time interval from the instant the packet is sent to the instant an ICMP6 PORT UNREACHABLE packet is received.

The second RTT measure is the time interval from the instant the snmp get request is sent to the instant a response is received, We will call this the SNMP-RTT. We have been collecting these values every 60 seconds.

Firstly we examine the RTTs between two nodes on the same link. Fig 5 shows these values measured on 19 Nov. 2004. The left side figure shows the distribution of RTT (traceroute6) and the SNMP-RTT in Sendai. The

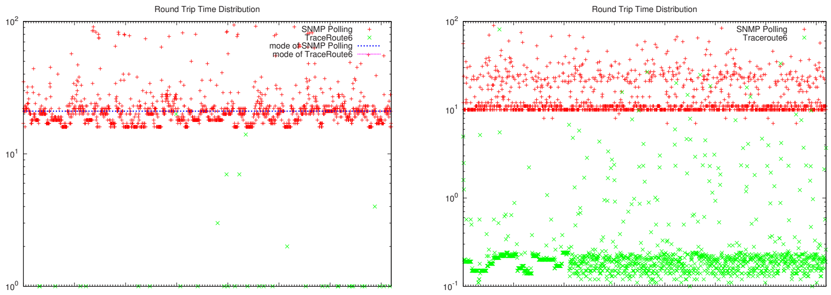


Fig. 5: Distribution of traceroute6 and polling interval for the node on the same LAN

right side figure shows the corresponding distribution in Kyoto. The X–axis shows the sequence number of the trials. The Y–axis scale is logarithmic. The nodes in this experiment connect on the same LAN. These are basically FreeBSD machines.

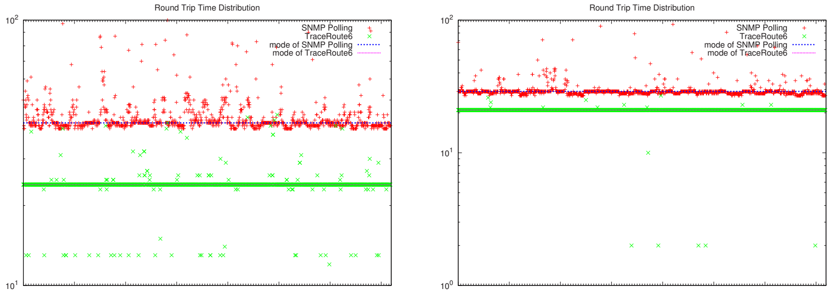


Fig. 6: Distribution of tracertoute6 and SNMP Polling to probe at RIEC

Fig. 6 shows the distribution of RTT measured by traceroute6 and SNMP Polling interval between two different locations on 19 Nov. 2004. Left side figure shows from Sendai to a probe located at RIEC in Tohoku University. Right side figure shows from agents at Kyoto University to the same destination at RIEC.

Finally, we consider the mode and mean value of RTT by traceroute6 and SNMP polling interval. We plot the mode and mean value of traceroute6 and SNMP polling interval on a daily basis for the month of November 2004. Left side of Fig. 7 shows the distribution of RTT (traceroute6) and Polling interval from Sendai to a probe located at Research Institute of Electrical Communication (RIEC), in Tohoku University is shown in the left hand figure. The right hand figure Fig. 7 shows the corresponding values from

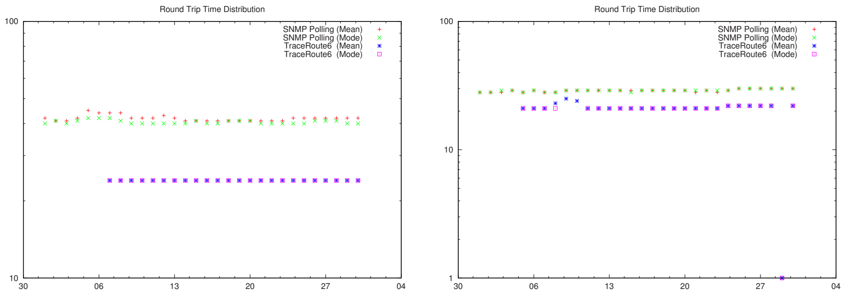


Fig. 7: Distribution of RTT and Polling interval to Tohoku Univ. from two diffrent agents

agents at Kyoto University to the same destination at RIEC. We can see from Fig. 7 that there is no major fluctuation in the RTT of traceroute6 and SNMP polling interval.

5 Event–oriented network analysis

Here we discuss event–oriented network analysis. Event–oriented network analysis involves modeling network traffic statistics. Deviation from the established traffic model may be considered to be an indication of a network event.

For example of in the case of traffic volume, we explain a simple procedure which may be used by an event processor to detect probable indications of events[3]. We assume network traffic follows some statistical distribution e.g. Gaussian, Poisson etc.. We evaluate the delta between traffic value estimated from previous data and the actual traffic value.

We show one of example using the simple method of moving averages. We attempt to estimate the next traffic value from the previous average and the deviation of previous N measured values. We put x_t as the measured traffic value at time t. Then we calculate the average μ_t and deviation σ_t of previous N at time t as

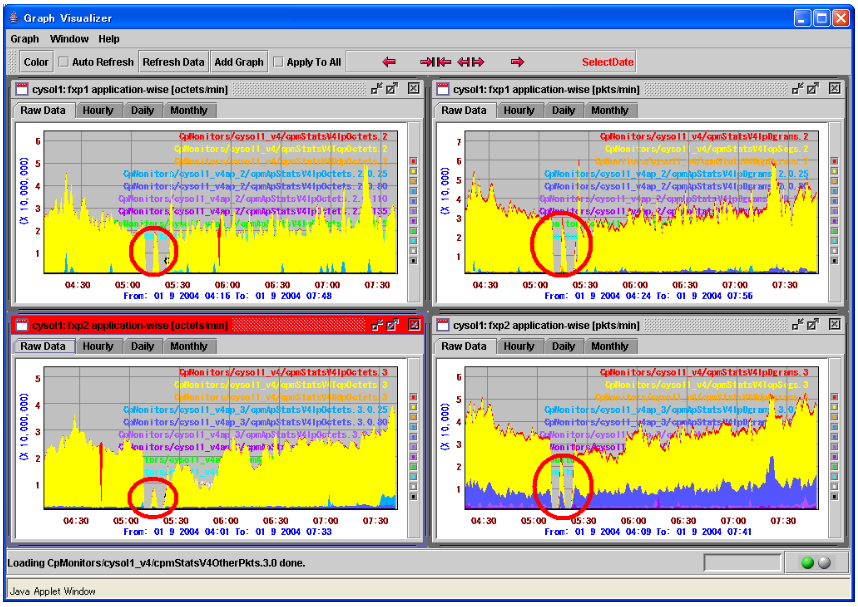
$$\mu_t = \frac{1}{N}\sum_{j=1}^{N} x_{t-j}, \quad \sigma_t^2 = \frac{1}{N}\sum_{j=1}^{N}(\mu_t - x_{t-j})^2. \tag{1}$$

For normalization purposes, we transform the measured value x_t to z_t as follows:

$$z_t = \frac{x_t - \mu_t}{\sigma_t} \tag{2}$$

This normalization transform lets us define the threshold for z_t. We say that an event has occurred at time t if z_t is beyond the threshold value.

Fig. 8 shows traffic graph when network equipments are replaced. Our event detection algorithm using moving average regards it as event.


Graph Visualizer
Graph
Window
Help
Color
□ Auto Refresh
Refresh Data
Add Graph
□ Apply To All
SelectDate
cysol1: fxp1 application-wise [octets/min]
cysol1: fxp1 application-wise [pkts/min]
cysol1: fxp2 application-wise [octets/min]
cysol1: fxp2 application-wise [pkts/min]
Raw Data
Hourly
Daily
Monthly
(X 10,000,000)
(X 10,000)
CpMonitors/cysol1_v4/cpmStatsV4IpOctets.2
CpMonitors/cysol1_v4/cpmStatsV4TcpOctets.2
CpMonitors/cysol1_v4/cpmStatsV4UdpOctets.2
CpMonitors/cysol1_v4ap_2/cpmApStatsV4IpOctets.2.0.25
CpMonitors/cysol1_v4ap_2/cpmApStatsV4IpOctets.2.0.80
CpMonitors/cysol1_v4/cpmStatsV4IpOctets.3
CpMonitors/cysol1_v4/cpmStatsV4TcpOctets.3
CpMonitors/cysol1_v4/cpmStatsV4UdpOctets.3
CpMonitors/cysol1_v4ap_3/cpmApStatsV4IpOctets.3.0.25
CpMonitors/cysol1_v4ap_3/cpmApStatsV4IpOctets.3.0.80
CpMonitors/cysol1_v4/cpmStatsV4IpDgrams.2
CpMonitors/cysol1_v4/cpmStatsV4TcpSegs.2
CpMonitors/cysol1_v4/cpmStatsV4IpDgrams.3
CpMonitors/cysol1_v4/cpmStatsV4TcpSegs.3
04:30
05:00
05:30
06:00
06:30
07:00
07:30
From: 01 9 2004 04:16 To: 01 9 2004 07:48
From: 01 9 2004 04:24 To: 01 9 2004 07:56
From: 01 9 2004 04:01 To: 01 9 2004 07:33
From: 01 9 2004 04:09 To: 01 9 2004 07:41
Java Applet Window

Loading CpMonitors/cysol1_v4/cpmStatsV4OtherPkts.3.0 done.

Fig. 8: Traffic Graph in replacing network equipments

We also show Fig. 9 as an example on the latency analysis, This figure shows the same charts of Fig. 6. But the destination in this case is a probe located at the University of Tokyo.

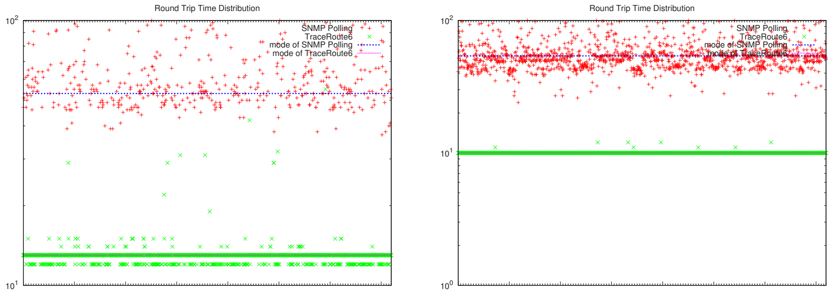


Fig. 9: Distribution of RTT and Polling interval to Univ. of Tokyo from two diffrent monitors

This figure shows the median value and mode value of traceroute6 are stable, but there is a variation in the values of SNMP-RTT when compared with the corresponding values at the RIEC probe. The case of Sendai shows the variation very clearly.

We can say that one of the reason for the fluctuation in SNMP-RTT for the University of Tokyo is that the probe has been monitoring as many as 19 links. The probe probably lacks the ability to deal with monitoring so many links.

6 Conclusion

In this paper, we introduce our monitoring and analysis activities. About monitoring activites, we show our environment in the JGN II network.

About analysis activities, we show our monitoring items, one is traffic volume and the other is latency. We also discuss event detection with these statistics applying for network management.

We plan to study the following as future work: We will estimate the accuracy of detections of indications of events. We will also evaluate the suitability of other traffic models to detect events. We will investigate the area of event classification, for example the relationship between indices.

Acknowledgment

We thank for netwan WG, especially Takeo Saito, Kazuo Doi and Kazuhide Koide to provide JGN II monitoring environment and give us many comments.

Reference

[1] JGN II Advanced Network Testbed for R and D Offical Website. http://www.jgn.nict.go.jp/.

[2] JGN II Monitoring Project. http://www.cysol.co.jp/research/jgn2mon/.

[3] Katsuhisa Abe, Glenn Mansfield Keeni, and Norio Shiratori. Experiments on event detection by traffic monitoring. Technical report, TECHNICAL REPORT OF IEICE NS2004-89, IN2004-48, CS2004-44(2004-09), September 2004.