

A Model for User Based Traffic Accounting

Ge Zhang, Bernd Reuther

Department of Computer Science, University of Kaiserslautern

P. O. Box 3049, 67653 Kaiserslautern, Germany

Tel: ++49 631 2054520, ++49 631 2052161, Fax: ++49 631 2053056

gezhang@informatik.uni-kl.de, reuther@informatik.uni-kl.de

Abstract

Today's traffic accounting systems are based on the assumption that one IP address is associated with one user. But this assumption cannot be applied to multi-user systems, where an IP address can be shared by multiple users at the same time. In this case an IP address can not be uniquely mapped to a single user. In order to provide finer granularity traffic accounting information we suggest a user based traffic accounting concept which can collect and analyze network resource usage metrics on the basis of users. This is an extension to current traffic accounting methods. With this not only IP address attribute but also user attribute are used as aggregating index in collecting the network resource usage information. This paper introduces user based traffic accounting technology and discusses several different mechanisms for user based traffic accounting. The implementation of a user based traffic accounting prototype system with Agent mechanism is introduced. Performance test results indicate that, if carefully designed the user based traffic accounting system affects performance of the system in which it resides only slightly.

1. Introduction

The Internet has become a part of the daily life. It offers a large scale of services from simple news services to complex bandwidth consuming multimedia services, and consequently more people are using the Internet for many different purposes at different places. But the usage of these services in Internet produces costs. In order to control the traffic volume to guarantee the QoS of multimedia services, to facilitate network resource usage reasonably and to allocate the cost fairly, not only ISPs but also enterprises and organizations such as universities and institutes will use accounting mechanisms on a per user basis to solve this problem.

Accounting is the process of collecting resource consumption data for the purposes of capacity and trend analysis, cost allocation, auditing, and billing [9]. Although many researches have been made concerning traffic accounting and many IP accounting products have been developed for network accounting purposes, almost all of them utilize IP address based accounting technology. With IP address based accounting technology, IP addresses are used to identify the corresponding consumers of the network resources. This is based on the assumption that each IP address is owned by one person or one institute, who or which will be responsible for this IP address. This is correct for IP accounting in single user systems. But if we think about the multi-user systems such as typical Unix sever, Windows Terminal Server etc., where an IP address can be shared by several users at the same time, an IP address cannot be uniquely mapped to one user. Therefore network resource consumption in these systems can only be ascribed to the owners of these systems instead of corresponding users who have made use of the network resources. Consequently the problem of how to allocate the network resource usage costs to different users in these multi-user systems will be left to the owners of the systems. This is a problem with which institutes, organizations and especially the computer centers of universities are confronted.

In order to amend the above described insufficiency of the traditional traffic accounting technology, NIPON project [15] was suggested to research for user based traffic accounting technology which can provide a finer granularity traffic accounting mechanism to distinguish the network resource usages among the users. Through user based traffic accounting technology IP addresses with user ID will be utilized to identify the network resource consumer.

The rest of this paper is organized as follows: section 2 describes related works, section 3 explains the user based traffic accounting mechanism and analyzes several user based traffic accounting schemes,

section 4 and 5 concentrate on the user based traffic accounting prototype implementation in NIPON project and the related performance test analysis, and section 6 gives summary.

2. Related works

Several standards have been suggested by IETF concerning Internet Accounting. [4] introduced the basic information about Internet accounting architecture whereas [6] suggested the traffic flow measurement architecture. A flow based accounting system "NeTraMet" [3] has been implemented based on the [6] suggested Internet accounting architecture. Although the user information has been defined as attributes "flowDataSourceSubscriberID" and "flowDataDestSubscriberID" in the MIB [7], these two attributes are neglected by "NeTraMet". In this implementation user information is obtained simply by mapping the IP address to its owner. No user information collection mechanism was described in the standards. Many commercial accounting systems such as XACCT [10], NARUS [2] etc. have also implemented their accounting systems with the similar Internet accounting architecture. But they all provide IP address based accounting. [1] proposed a user based accounting method only for TCP traffic. The principle of this method is to intercept the TCP connection request to verify user's TCP connection establishment authorization and to measure the user's TCP traffic after a connection has been established. But this method can not meter the non-connection protocol traffic such as UDP, and extra verification server is needed. [5] suggested also a user information retrieving protocol about the users of an established TCP connection. This protocol may encounter error in querying user information for short live TCP connection, and it is also impossible in metering the UDP traffics.

3. User based traffic accounting mechanism

3.1. IP accounting infrastructure

In this paper traffic accounting refers mainly to the IP layer traffic accounting, therefore the term IP accounting and traffic accounting are interchanged in this paper. Before we explain the user based IP accounting mechanism, let's take a brief look at the IP accounting system infrastructure. [4] has defined a simple Internet accounting model which consists of three basic elements: meter, collector and application. [6] adds a Manager element on the basis of this

accounting model and further illustrates the relationship between these elements. Accounting products such as XACCT, NARUS etc. introduce more components to process data collected from meters before sending them to different applications. The IP accounting system infrastructure can be summarized as Figure 1.

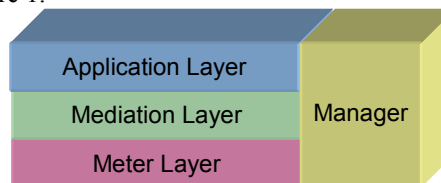


Figure 1. IP accounting infrastructure

The Meter Layer measures network traffic as well as aggregates measurement results. The Mediation Layer collects measurement data from the Meter Layer, and processes (aggregate, de-duplicate, validate, correlate etc.) collected data and stores them. The Application Layer consists of applications for different purposes such as billing, audit, trend analysis etc. using data from mediation layer. The Manager configures and controls the whole IP accounting system. Rules are used by the Manager to control the activities of elements in three layers.

When a Meter measures the network traffic, it generates the accounting records which consist of several accounting attributes. Usually the accounting attributes can be divided into two categories: identification attribute and usage attribute. These two types of attributes describe which entity is measured and how much resources are used respectively. The identification attribute is used to uniquely identify the measured entity, and it is the aggregating index of the accounting records. IP address is usually used as identification attribute in traditional IP accounting system to identify user. The usage attribute is used to record the quantitative results of the measured traffic.

3.2 User based IP accounting concept

User based IP accounting can be defined as the process of collecting network resource consumption data with corresponding (on the basis of) user information.

In the definition the "user information" is indispensable for the accounting process.

The term User has different meaning in different layers of the IP accounting infrastructure:

In the Meter Layer User is defined as a person who generates the network traffic from an end-system. In this Layer User can be uniquely identified by the 2-tuple <UserID, HostIP>. A person who has more than

one UserID in an end-system should be regarded as different Users.

In the Mediation Layer the term User can denote a person or a group of persons who generate network traffic from the whole accounting administration domain. For example, if a person has several accounts in different end-systems, all his/her meter records from different end-systems can be aggregated together as one User in the Mediation Layer.

In the Application Layer or Billing Layer, the term User denotes a person or a group of persons who should be responsible for the consumption of the network traffic resources. Specifically for the IP Billing, a User is a person or a group of persons who should pay for his/their consumption of resources.

From the definition we can see that the user based IP accounting process depends mainly on the Meter Layer to collect the user information to identify the consumers of the network resource usages. Therefore the User meaning in Meter Layer is adopted by user based IP accounting technology.

The User information refers to the 2-tuple <UserID, HostIP> which can be used to uniquely identify the consumer of corresponding network resource usage. HostIP can be extracted from IP header as in the traditional IP accounting technology. UserID is used to distinguish the users in the same host. The goal of user based IP accounting is to identify the network traffic with both HostIP and UserID. In other words every IP packet or every traffic flow must be marked with corresponding user information.

There are two reasons why the traditional IP accounting systems can not provide user based IP accounting information. One is based on the assumption that one IP address is equal to one user. This assumption usually comes from the simplification of the accounting information collection, or only single user end-systems need to be measured, or the accounting systems are serviced for the organizations or institutes which need only coarser granularity accounting information. Another reason relates to the location of meters of traditional IP accounting system. Meters are usually placed in the location where not only all needed IP traffic can be monitored but also cost and overhead can be minimized [4]. For example, typically routers in the network boundaries are chosen as a place to integrate the meter function. Although this location principle for the meters is a reasonable choice for efficiency and cost, on the other hand the placement of the Meter limits its ability to IP address based accounting, since only IP address rather than user information can be extracted from the IP traffic.

3.3 User based IP accounting schemes

In this section two user based IP accounting schemes are discussed.

3.3.1 Multi-IP scheme. The principle of this scheme is, assigning a block of IP addresses to a multi-user host, and then these IP addresses will be allocated to every user statically or dynamically. Through this, an IP address is bound to a single user during a period of time and therefore an IP address can be used to identify every user uniquely in the multi-user host.

IP address allocation to the users can be either statically or dynamically. With static allocation method every registered user in the host can have a unique fix IP address when her/his account is first created. All her/his future network usages are all with this IP address. Obviously the size of the IP address pool of the multi-user host corresponds to the number of registered users in it. Usually this static method requires more IP addresses than the following described dynamic method. The dynamic method allocates IP addresses to users only when a user login. And the allocated IP address will be released and recycled after the user logout. In order to record the IP address allocation history, corresponding log file must be created to provide information for future user - IP address mapping. This requires corresponding modification in OS to be made to support this scheme. And the multi-user system must also be configured to support multi-IP.

Since IPv4 address is a scarce resource, private IP addresses can be assigned to the multi-user host and consequently a NAT server is required to translate the private IP addresses to the IP address which is used by the multi-user host before. In IPv6 [16] environment IP address will be not so scarce and allocating a block of global unicast IP address may be not a big issue. Therefore NAT [17] server will not be needed in IPv6 environment.

When a multi-user host is equipped with the ability of supporting different users with different IP addresses, the multi-user host can be regarded as a group of single user hosts. Therefore a meter can be located between the multi-user host and the NAT server to collect information or when no NAT existing, e.g. in IPv6 environment, traditional IP accounting mechanisms can be applied without any change to achieve the goal of user based IP accounting. Figure 2 illustrates multi-IP scheme with NAT server support:

In Figure 2 a traditional IP accounting meter is located between the multi-user system and the NAT server checks the IP headers of all IP traffics. Since each IP address can be uniquely mapped to corresponding user, extracting IP address from an IP header can identify the user who is responsible for this IP packet.

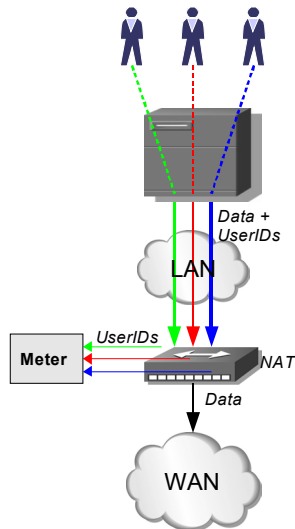


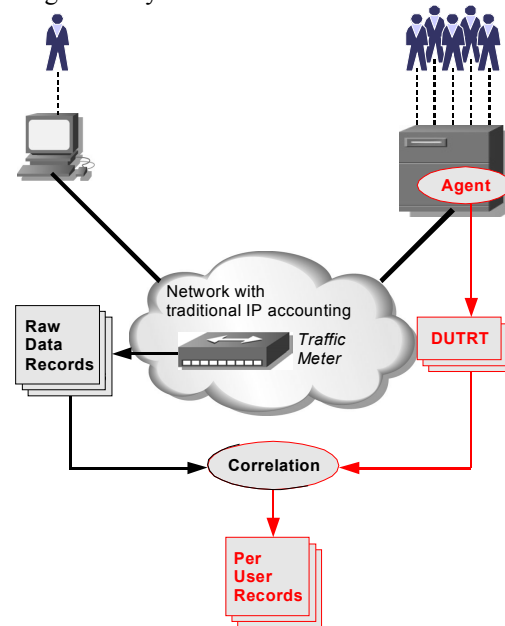
Figure 2. Multi-IP scheme with NAT server

The key of this scheme is the mechanism to assign different IP addresses to different users. In order to integrate this mechanism OS should be modified.

The advantage of this method is that no modification is needed for traditional IP accounting systems to perform user based IP accounting operations. But disadvantages of the method are: additional hardware is needed for NAT server in IPv4 environment, some software may encounter problems when they work behind NAT server, and OS needs to be modified to facilitate different users performing network operations with their own IP addresses.

3.3.2 Agent scheme. The Agent scheme is an extension to the traditional IP accounting infrastructure [11] [18]. Figure 3 depicts the user based IP accounting architecture with Agent mechanism. This user based IP accounting architecture is composed of several components. An Agent resides in each multi-user host is responsible for identifying traffic with corresponding users and generating a Dynamic User Traffic Relationship Table (DUTRT). It is a key entity added to the traditional IP accounting architecture. The traffic meters are the same as in the traditional IP accounting architecture, which locate in the key position to collect information of traffic both come from single user hosts and multi-user hosts. The metered information will be stored in Raw Data Records (RDR). The correlation module in Mediation Layer will use the user traffic relationship information in DUTRT to identify the users of the RDRs which relate to the multi-user hosts. Since in the single user system an IP address can be uniquely mapped to one user, the RDRs of the single user hosts can be identified with corresponding users simply by the IP addresses. This architecture does not

make any change to the traditional accounting on single user systems.



DUTRT = Dynamic User Traffic flow Relation Table
 — new to user based IP accounting

Figure 3. User based IP accounting architecture with Agent mechanism

The Agent identifies the corresponding users of IP traffic as follows:

- Capturing IP packet
- Identifying user of this packet
- Extracting traffic information such as source IP and port, destination IP and port from IP header
- Storing both user and traffic information into the DUTRT

In this architecture, the Agent can be implemented either as a standalone meter which provides all required accounting information of the monitored host, or as a supplementary accounting information resource of the Meter Layer to provide complementary user information to the traditional IP accounting system.

If the Agent is applied as a standalone meter, the records of the DUTRT should include all required identification attributes (such as UserID, IP address etc) and usage attributes (such as sent bytes, received bytes etc.). In this case the DUTRT can be regarded as accounting records table other than a simple user traffic relationship table. Otherwise the Agent only needs to collect the user information and traffic identification attributes. For example with the [8] suggested traffic flow measurement method an Agent needs only to collect user information to identify every flow whose normal accounting attributes are collected by the traffic flow meters. The user traffic flow relationship information will be used by the correlation

module in the Mediation Layer to identify the accounting records. With this method the efficiency of the Agent can be improved and the generated accounting information volume can be reduced.

3.4.4 Comparison. Figure 4 below summarizes the comparison results between above described user based IP accounting schemes.

Both schemes make any change to the existing Internet protocols. OS should be modified to integrate multi-IP scheme, whereas the Agent mechanism can be implemented as a kernel patch without OS modification. With multi-IP scheme, traditional IP accounting system can be simply applied for the purpose of user based IP accounting for multi-user systems without problem, and no performance affection will be resulted to the routers or local

systems. But additional hardware may be demanded as NAT servers. In IPv6 environment the NAT servers may be not necessary. With Agent scheme, the Agents will cause performance affection to the hosts they reside and correlation module in traditional accounting system should be adjusted to accommodate the DUTRT for user traffic relationship mapping. The Agent scheme will not affect the performance of routers and require no additional hardware. From the implementation prospect of view, multi-IP is more difficult to be realized due to modification on OS. The Agent scheme can be implemented either by modifying OS or as patches without OS modification. The patch method is suitable for realizing user based IP accounting on legacy systems whose OS cannot be modified.

	Protocol change	OS change	Change old Accounting System	Affection to local system	Affection to router	Additional Hardware	Realization Difficulty
Multi-IP	-	+	-	-	-	+/-	+
Agent	-	+/-	+	+	-	-	-

Figure 4. User based IP accounting schemes comparison

4. Prototype Implementation

In our user based IP accounting project “NIPON” [15] a user based IP accounting prototype system was implemented according to the above described Agent mechanism. The reason of choosing Agent scheme is that it can be implemented as patches for systems such as Solaris, Windows Terminal Server 2000 etc. whose source code cannot be obtained for modification.

The NIPON prototype system is implemented on the basis of open source “NeTraMet” IP accounting software suite. The “NeTraMet” distribution includes following programs:

- NeTraMet: it implements the traffic flow Meter. The package capture driver [13] or [14] is used to collect the traffic flows’ information in UNIX/LINUX or Windows environment respectively. The collected traffic flow information is stored into MIB database which can be accessed by the Meter Reader NeMaC with the SNMP protocol. It provides IP address based traditional IP accounting capabilities.
- NeMaC: it implements both Meter Reader and Manager functions as described in [6]. It can collect measured traffic flow data from meters, which provides the Mediation layer functions. It can also manage an arbitrary number of meters with specific rules for each meter.
- Other support programs such as fd_filter,

fd_extract, nm_rc, and nifty etc. “Nifty” is an X-Windows Network Traffic Flow Analyser. “fd_filter” and “fd_extract” are NeTraMet flow data file Utility Programs.

Meter “NeTraMet” and Meter Reader “NeMaC” are modified to be extended to provide user based IP accounting capability. Other applications in the “NeTraMet” suite are not chosen.

Figure 5 illustrates the NIPON prototype system architecture. It extends the [6] suggested traffic flow measurement architecture by integrating a user based IP traffic measurement Agent into meter, and supplements the Application Layer functions. The Agent instead of the libpcap or winpcap is responsible for capturing IP packets with hook mechanism. Agent records each packet’s accounting information with its corresponding user information and then sends them to NeTraMet. In NIPON project Agents are implemented in Solaris and Windows Terminal Server 2000. The NeTraMet is modified to process the information recorded by Agent to generate flow based meter records with user information. In order to avoid producing extra traffic on the network between the Agent and the NaTraMet, the Agent is integrated into the “NeTraMet” and they run in the same measured multi-user host. The generated meter records are stored in SNMP MIB. Meter Reader “NeMaC” collects meter records from NeTraMet meters with SNMP [12] protocol and stores them in an accounting information database.

And an accounting information web server is developed to provide user based traffic accounting information, which can be retrieved with Internet browsers.

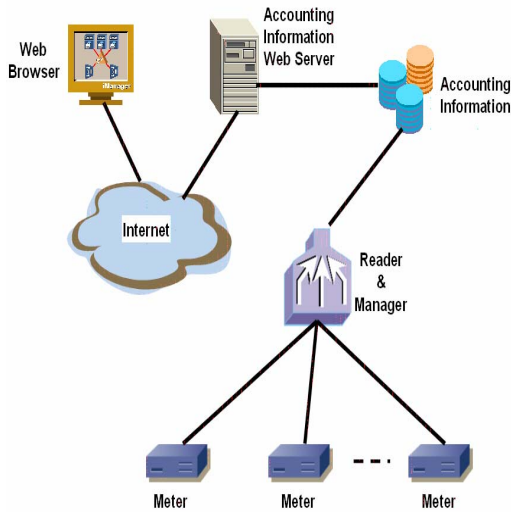


Figure 5. NIPON prototype system architecture

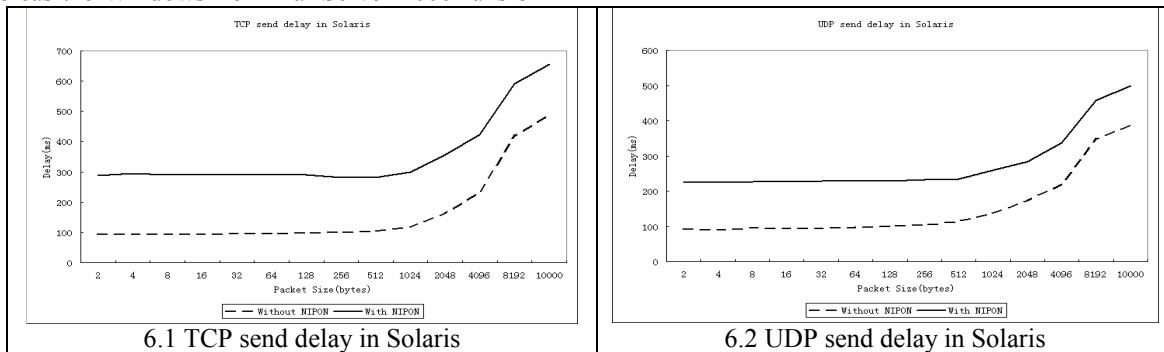
5. Performance test of prototype system

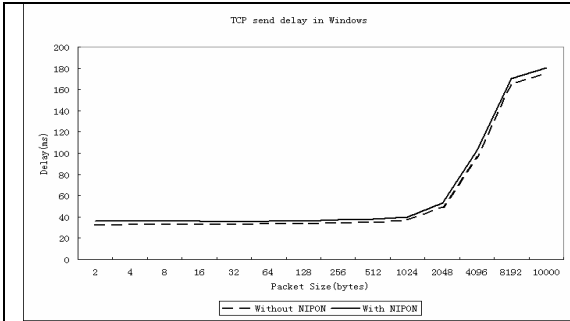
In the NIPON prototype system the user based IP accounting Agent is a key component which can influence the performance of measured systems. Because the Agent is located in the measured host to intercepts all network operation requests and it is implemented running in the kernel of the monitored multi-user host, it will certainly affect the performance of the measured host. In order to analyze the performance affection to the monitored host caused by the Agent, performance tests emphasizing on the network throughput and the delay of network operations have been made with the prototype system in the condition with or without NIPON Agent. This test was made in Solaris and Windows 2000 Terminal Server respectively. The Solaris runs on a SUN UltraSparc 143MHz CPU, whereas the Windows Terminal Server 2000 runs on

a Pentium III 500MHz CPU. The network performance test utility “netperf” [19] is used to simulate an application generating network traffic and to record performance statistic data. Figure 6.1 to Figure 6.8 below illustrate the test results.

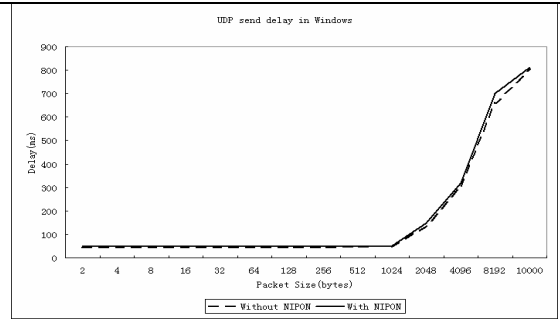
The Figure 6.1 and 6.2 show that in Solaris with NIPON Agent TCP/UDP send delay are about 200ms and 120 ms respectively higher than without Agent, whereas Figure 6.3 and 6.4 show that in Windows the TCP/UDP send delays difference between with and without NIPON Agent are all less than 10ms. The reason for the different performance affection caused by Agents in different systems is that the Solaris runs with a lower power CPU, whereas the Windows runs with a more powerful CPU. It is obvious that the Agent affects the delay performance mainly on the hosts with lower CPU capabilities. The Figure 6.5 and 6.6 show that in Solaris with NIPON Agent TCP/UDP send throughputs have obvious decline than without Agent when datagram size less than 300 bytes, but Figure 6.7 and 6.8 show that in Windows with NIPON Agent there is no obvious TCP/UDP send throughputs decline. The reason is that, given a fix length data to be sent, the smaller size packets cause more processing requests than the bigger size packets, which will in turn cause more processing by NIPON Agent with the smaller size packets. Therefore the NIPON Agent results more throughput decline in sending small size packets. And the test results show that when the packet size increases to more than 300 bytes the NIPON Agent’s affection to the throughput in Solaris decreases to almost zero. This indicates that the NIPON Agent affects the throughput performance mainly on the operations on small size packets.

From the test result we can conclude that the NIPON IP accounting system will not produce too much overhead to the measured system. Its performance affection is mainly on the processing of great number of small size packets in the system with lower performance CPU.





6.3 TCP send delay in Windows



6.4 UDP send delay in Windows

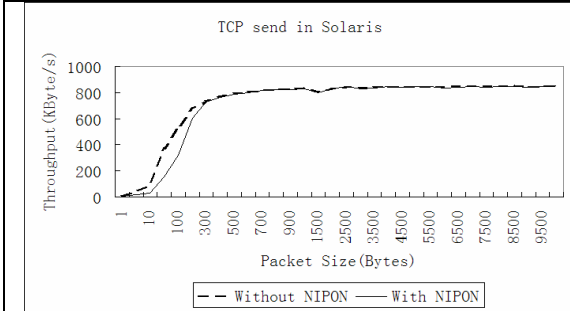


Figure 6.5 TCP send throughput in Solaris

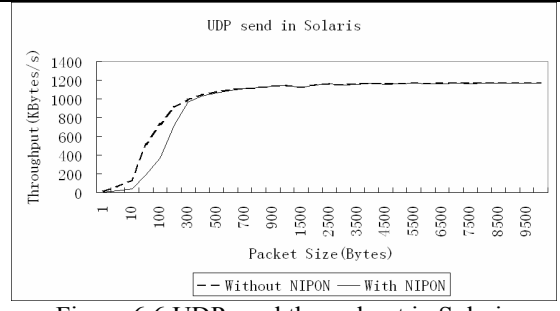


Figure 6.6 UDP send throughput in Solaris

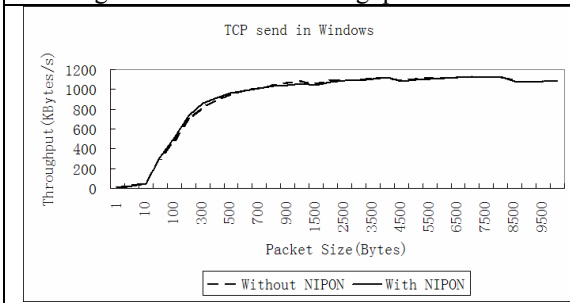


Figure 6.7 TCP send throughput in Windows

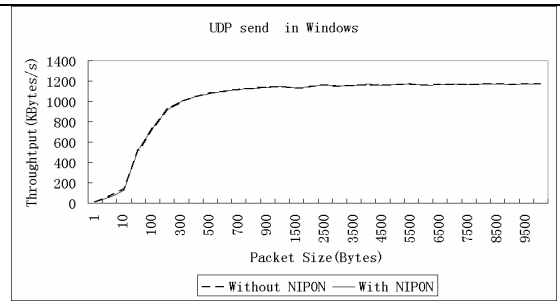


Figure 6.8 UDP send throughput in Windows

6. Summary

User based traffic accounting systems collect the traffic information on the basis of users. Thus it can provide more accurate accounting information than the traditional traffic address based accounting system. This paper discussed two different user based IP accounting mechanisms, and their characters are compared. Multi-IP scheme is an elegant solution, since it can simply utilize traditional IP accounting technology to realize user based IP accounting. But this method requires OS to be modified, which is difficult for some systems, especially for legacy systems. If NAT server is used to support this scheme, problems like some software cannot work correctly behind NAT will be raised. Agent mechanism can be easily integrated into traditional IP accounting system to provide user based IP accounting, and no protocol change is required. But this method will affect performance of the measured

systems. In the NIPON project a user based IP accounting system with Agent mechanism was implemented. In this system an Agent is developed in Solaris and Windows Terminal Server 2000 platforms respectively to collect the user information to identify corresponding traffic flow. The performance test results show that the performance decline caused by NIPON prototype system is mainly on the processing of great number of small size packets in the system with lower performance CPU.

Security is not addressed in this paper, although it is very important. The security issues concern the areas of software and data. The user based IP accounting system should be designed carefully against the probably attacks. Authentication mechanism can be used to reject unauthorized accessing. The meter records should be stored safely to prevent from unauthorized access. During the transmission of the meter records, accounting protocols with corresponding security mechanisms should be applied for collecting data.

7. References

- [1] R. J. Edell, N. McKeown, P. P. Varaiya: "Billing Users and Pricing for TCP", IEEE Journal on selected areas in communications, Vol. 13. No. 7. September 1995
- [2] Narus Documentation, <http://www.narus.com>
- [3] NeTraMet, <http://www2.auckland.ac.nz/net/NeTraMet/>
- [4] C. Mill, D. Hirsh, G. Ruth: "Internet Accounting: Background", RFC1272, November 1991
- [5] M. St. Johns, "Identification Protocol", RFC1413, February 1993
- [6] N. Brownlee, C. Mills, G. Ruth: "Traffic Flow Measurement: Architecture", RFC 2063, January 1997
- [7] N. Brownlee: "Traffic Flow Measurement: Meter MIB", RFC2720, October 1999
- [8] N. Brownlee, C. Mills, G. Ruth: "Traffic Flow Measurement: Architecture", RFC2722, October 1999
- [9] B. Aboda, J. Arkko, D. Harrington: "Introduction to Accounting Management", RFC2975, October 2000
- [10] XACCT Documentation, <http://www.xacct.com>
- [11] G. Zhang, B. Reuther, P. Mueller, "User Oriented IP Accounting in Multi-user Systems", The 8th IFIP/IEEE International Symposium on Integrated Network Management, 24-28 March 2003
- [12] J. D. Case, M. Fedor, M. L. Schoffstall, J. Davin, "Simple Network Management Protocol (SNMP)", RFC1157, May 1990
- [13] Libpcap: packet capture library
<http://www.tcpdump.org/>
- [14] Winpcap: the packet capture library for Windows
<http://winpcap.polito.it/default.htm>
- [15] NIPON: Nutzerbasiertes IP accounting,
<http://www.icsy.de/forschung/nipon/>
- [16] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC2460, December 1998
- [17] P. Srisuresh, K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC3022, January 2001
- [18] G. Zhang, B. Reuther, P. Mueller, "Distributed Agent Method for User Based IP Accounting", 7th. CaberNet Radicals Workshop, 13-16 October 2002
- [19] Netperf HomePage
<http://www.netperf.org/netperf/NetperfPage.html>