USER ORIENTED IP ACCOUNTING IN MULTI-USER SYSTEMS

Ge Zhang, Bernd Reuther, Paul Mueller
Department of Computer Science, University of Kaiserslautern
Postfach 3049, 67653 Kaiserslautern, Germany
Tel: ++49 631 2054520, ++49 631 2052161, ++49 631 2052263, Fax: ++49 631 2053056
gezhang@informatik.uni-kl.de, reuther@informatik.uni-kl.de, pmueller@rhrk.uni-kl.de

Abstract: The traditional IP accounting method is IP address oriented, that means one IP address corresponds to one user, but it can not meet the finer granularity accounting requirement in multi-user systems, in which many users share one or more IP address at the same time. In the multi-user systems the user oriented IP accounting can distinguish the producers of the IP traffics, which come from the same IP address. Hence it is a more accurate accounting method than traditional IP address oriented accounting method. In this paper, we present the technology of the user oriented IP accounting, and describe the principle of this method, and the realization considerations.

Keywords: IP Accounting, IP Billing, Multi-user System

1. INTRODUCTION

With the rapid development of the Internet, more and more services are provided by the Internet, more and more users enjoy these Internet services, and consequently more and more traffic are produced. For example, during the last three years the IP data volume of the University of Kaiserslautern doubled every year. In this situation, it is very important to control and measure the Internet usage. IP traffic accounting provides information about the usage of a network and therefore helps to manage it. The accounting data may be used also for billing. Today billing is commonly used by Internet service providers (ISP). But billing systems might be used even within LAN. This enables to allocate the costs, which are produced by the network traffic of a single-user or an institution using a campus network. But billing has also an influence on the behavior of the users. Users will not use the network resource responsible if the usage is free of charge. Because of the rising costs it is reasonable

to present bills to the end users also. This aspect becomes very important when a network offers different Classes of Service (CoS).

It does not depend if billing is used in a LAN to allocate costs or to motivate reasonable network usage. In both cases it makes sense to be able to correlate the network traffic with the users, which are responsible for it. Today several IP accounting and billing solutions exist. But these solutions correlate IP addresses and traffic only. But there are several scenarios where an IP address is not associated with one user. For example in the computer center of University of Kaiserslautern the multi-user computers or PC pools play a very important role. The traditional IP accounting solutions are not able to distinguish different users of those systems.

This paper describes method that enables the distinction of users even on multi-users systems.

2. TRADITIONAL IP ACCOUNTING METHOD

2.1 IP accounting and IP billing system

Accounting is "The collection of resource consumption data for the purposes of capacity and trend analysis, cost allocation, auditing, and billing."[1]. Whereby Billing is the process of utilizing the processed Accounting Records on a per user basis to generate the invoice. The architecture of a general IP billing system is illustrated in Figure 1[2].

An IP Billing system consists of three layers: Traffic Flow Meter Layer, Mediation Layer and Billing / OSS / BSS (Operating / Business Support System) Layer. The Traffic Flow Meter Layer records the network activities in Raw Data Records (RDR) like an electricity meter. The Mediation Layer collects the Raw Data Records from various Network Elements, and processes the Raw Data Records to produce the Usage Records, stores the Usage Records in database, distributes the Usage Records to different applications in layer 3. The applications (e.g. Billing, Fraud Detection, Traffic Analysis etc.) in layer 3 respectively process the Usage Records for different application purposes and generate various reports. IP accounting includes the layer 1 and layer 2 in the IP billing system architecture.

The traditional IP accounting system collects and processes the resource consumption data on the basis of the IP address, that means, in these systems an IP address is considered as one user. But it is not the case in the multi-user systems, e.g. most Unix systems or Windows Terminal Servers, in these systems many users share one or more IP addresses simultaneously. In this case one IP address is not equal to one user. Contrasting with the traditional IP address oriented IP accounting method, we suggest the User oriented IP Accounting method. Our NIPON (Nutzerbasiertes IP accounting) project aims at solving this problem.

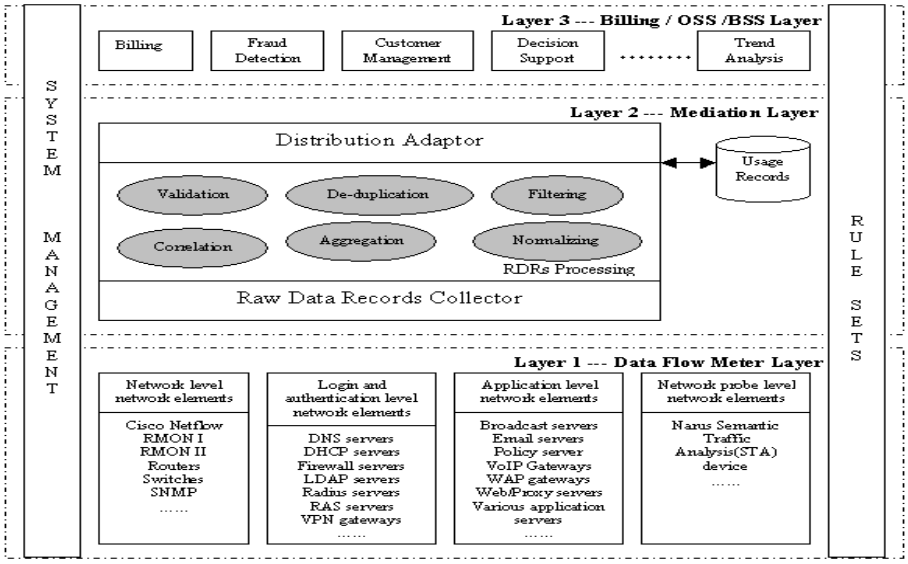


Figure 1. IP Billing System Architecture

2.2 User Information Processing Method in Traditional IP Accounting System

The general IP accounting process can be described in two steps:

1) The Traffic Flow Meter collects IP traffic information from various Network Elements, and stores these information in the form of Raw Data Records;
2) The Mediation layer collects the RDRs, and then processes (Validation, de-duplication, filtering, correlation, aggregation and normalizing) the RDRs to produce the Usage Records.

Figure 2 illustrates the process of IP traffic information processing.

Figure 2. IP Traffic Information Processing

During the process of the IP traffic information processing, the traditional IP accounting method will regard the IP addresses in the RDRs as the user information, and these IP addresses will be mapped to corresponding users by the so called **Correlation** module, which is one of the RDR processing modules in IP mediation layer (see Fig.1). The function of the Correlation module is to merge several RDRs, which have some relationships, to create a single record, this can provide a single, complete view of information about an event [3]. In the traditional IP accounting system the Correlation process is on the basis of IP address. The Correlation module

maintains an IP address & User Map Table, according to this table the Correlation module can map the IP addresses to the corresponding users. Figure 3 illustrates an example of the process of how the Correlation module mapping the IP addresses in RDRs to corresponding Users.

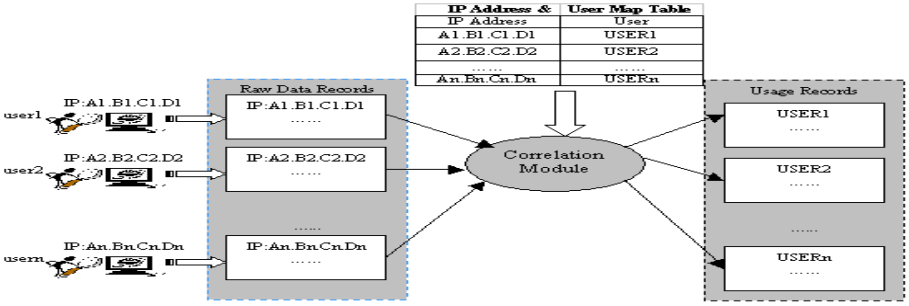


Figure 3. Mapping IP addresses to corresponding Users

The above described user information processing method of traditional IP accounting system has no problem in single-user systems or in the condition that each IP address can be considered as the user who will be responsible for the IP traffic. In these cases an IP address can uniquely represent a person or an institution that will be responsible for the IP traffic generated by this host.

But in multi-user systems, many users can share an IP address at the same time. In this case an IP address cannot uniquely represent a user. The traditional IP accounting method cannot accurately process the user information in this situation.

Figure 4 illustrates an example of the Correlation process of the traditional IP accounting method in multi-user system.

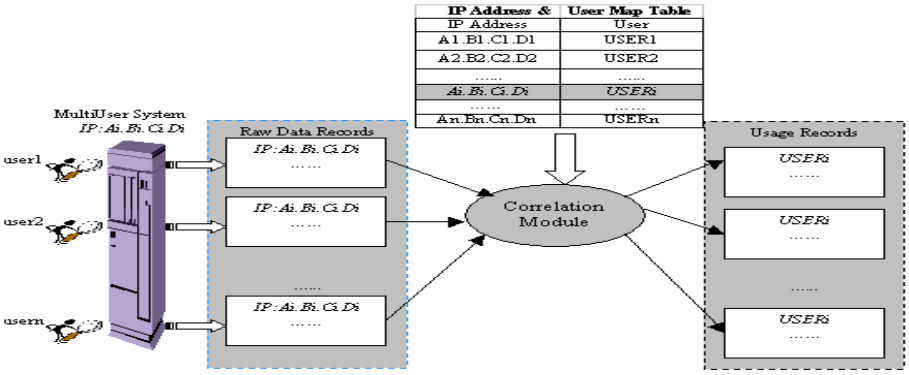


Figure 4. Traditional IP accounting method in mapping IP addresses to corresponding Users in multi-user system

In Figure 4 several users share a multi-user computer, and they share the same IP address Ai.Bi.Ci.Di. According to the traditional user information process method, only the IP address information Ai.Bi.Ci.Di in the Raw Data Records will be used to

represent the user. After the Correlation module processing this IP address is mapped to USERi and the user information is recorded in the generated Usage Records. Through this user information processing method, all the IP traffics, which come from the same multi-user computer with the same IP address Ai.Bi.Ci.Di, but produced by different users (user1, user2, … ,usern), are regarded as produced by the same user (USERi).

From the above introduced traditional IP Address oriented IP accounting method, we know that, this traditional IP accounting method can not meet the fine granularity requirement of the user information processing in multi-user systems.

3. THE PRINCIPLE OF USER ORIENTED IP ACCOUNTING IN MULTI-USER SYSTEMS

User oriented IP accounting collects traffic information and processes the RDRs on the basis of User. Before we discuss about it, we should first answer the question: What is a User? Then we will describe the principle of User oriented IP accounting method and the realization considerations.

3.1 User Model

3.1.1 Terminology

The meaning of the term *user* depends on the context where the term is used. When talking about traditional IP accounting systems a user is a host that is the source or the sink of IP traffic. Within IP billing systems the term user means the person or institution, who is responsible for some IP traffic, i.e. who has to pay for the IP traffic. In a multi-user system a login name or an identifier represents a so-called user. This user may be one real person or a group of real persons. Because of this ambiguous usage of the term user we will present some definitions of terms, which will be used within this paper:

- *Host-Identifier* is a unique identifier for an endsystem of the network layer. In the context of IP networks an IP address can be used as a synonym for a Host-Identifier, since IP addresses are unique numbers for network layer devices, at least within an administrative domain.
- *User-Identifier* or UID is a unique identifier for an account on a multi-user system. This term is commonly used in the context of multi-user systems.
- *Traffic-Originator* ::= <*Host-Identifier*, [*User-Identifier*]>. A Traffic-Originator (TO) is responsible for specific outgoing and incoming traffic flows. A TO may be described only by a Host-Identifier or by a Host-Identifier and a User-Identifier. This means a TO is an exclusively used computer or an account on a multi-user system.
- *User*::= <*Traffic-Originator1* [, … *Traffic-OriginatorN*]> is a unique identifier for real person or a group of persons which are associated with

one or more TOs. Each TO is associated with exactly one User. Usually a User identifies one real person who has access to one or more single-user systems or accounts on multi-user systems. When a group of real persons share an account or a single-user system, this group may be described by one User.

- *Purchaser*::= <*User1* [, …, *UserN*]> is a unique identifier of a person or an institution who will pay for the traffic that is originated by one or more Users.

3.1.2 User oriented IP accounting definition

According to the definitions of the previous subchapter, traditional IP accounting distinguishes traffic from different Host-Identifiers, i.e. IP-Addresses only. Within the mediation or billing layer Host-Identifiers are mapped to purchasers directly. In contrast to this the User oriented IP accounting distinguishes different TOs. Within the mediation or billing layers the TO will be mapped to Users which are mapped to Purchasers. It is important to distinguish between Users and Purchasers, because of their different responsibilities. The User is responsible for the traffic that is produced. If there occur some problems with some traffic flows or the amount of traffic that is produced, then it is important to know who is responsible for the traffic. But in order to send a bill to some person or institution it is only necessary to know who is responsible for paying for the produced traffic.

The User oriented IP accounting extends the concept of traditional IP accounting by considering User-Identifiers in addition to Host-Identifiers. Traditional IP accounting can be regarded as a special case of User oriented IP accounting, since in traditional IP accounting the TOs of the traffic flows have always the same UID. Comparing with traditional IP accounting, User oriented IP accounting should provide information about User-Identifiers, which must be correlated to the accounted IP traffic. Therefore three technical problems must be solved for the User oriented IP accounting:

- Accounting of User-Identifiers. More precisely a relationship between a User-Identifier and a traffic flow must be recorded. This must be done within the multi-user system, since this information is not available outside of the multi-user system.
- Correlation of TOs (which may contain User-Identifiers) with traffic flows.
- Transport of the accounting data that is recorded in the multi-user system to the correlation module.

3.2 User oriented IP Accounting Method

With the above described User model, User oriented IP accounting will identify the producer of each traffic flow or package, and the corresponding TO information will be added into the RDRs to identify who produce them. A flow is defined as a set of packets between two endpoints (as defined by their source and destination attribute values and start and end times) [4]. For example, in the realization of the

traffic meter NeTraMet [5], a flow is identified by a 5-tuple, i.e. <protocol, source address, destination address, source port number, destination port number>.

The TO information is unknown to the outside of the multi-user systems. If we want to obtain the TO information from a multi-user system, a mechanism must be resided in the multi-user system to implement this function. Here we call this mechanism Agent method.

3.2.1 Agent method model of User oriented IP accounting

Figure 5 illustrates the Agent method model of User oriented IP accounting in multi-user systems. The User oriented IP accounting architecture is based on the traditional IP accounting architecture. The differences between the new method and the traditional method are:

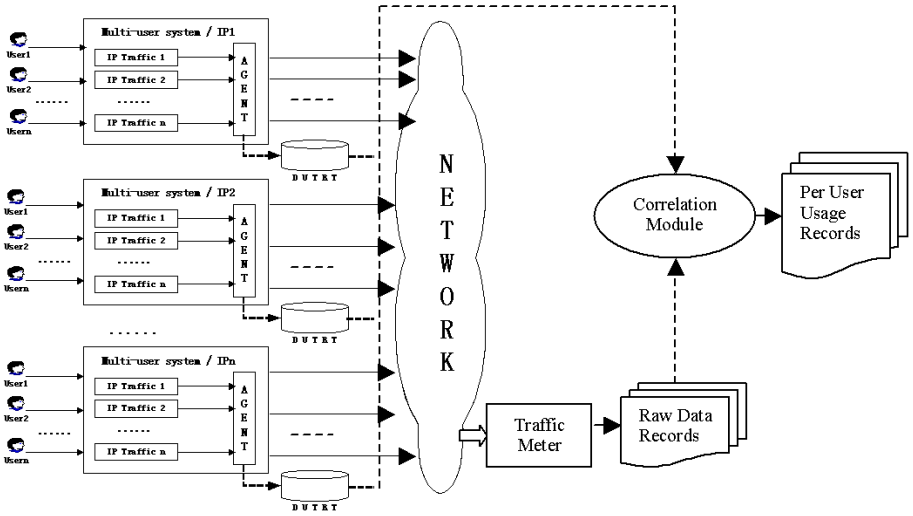


Figure 5. Agent Method Model of User Oriented IP Accounting

- An Agent is introduced into the multi-user system, which is used to collect the User-TrafficFlow relationship information according to the User Model. The collected User-TrafficFlow relationship information will be recorded into a so-called Dynamic User-TrafficFlow Relationship Table (DUTRT). This is used to record the IP traffic flows and their corresponding TO information. The Agent can also act as a standalone IP traffic meter, which measures the IP traffic from the multi-user computer, in which it locates. In this situation the entries in DUTRT can be used as RDRs. This will simplify the correlation processing, but it will contribute more overhead to the multi-user system.
- The Correlation module in the IP mediation layer uses a DUTRT, not a simple IP Address-User Table, to map the RDRs to the corresponding

users. In this case, more attributes in RDRs should be used for the user correlation purpose.

The User oriented IP accounting process with Agent method can be described as below:

1. The Agent checks all traffic flows, and then extracts the corresponding TO and other information to identify each flow. All the generated User-TrafficFlow relationship information will be stored in a DUTRT.
2. Traffic Flow Meter collects the IP traffic information to generate the Raw Data Records.
3. The RDRs and DUTRT records will be sent to or collected by IP mediation layer.
4. The Correlation Module uses the DUTRT to map the RDRs to the corresponding users and adds the user information to the new generated Usage Records.

3.2.2 Dynamic User-TrafficFlow Relationship Table

The Dynamic User-TrafficFlow Relationship Table is generated by the Agent. It is used to record the TO information of each traffic flow or package, and the Correlation Module will use it to identify the users of the traffic flows.

Whenever a new traffic flow is produced, a new entry with this flow's TO and Correlation attributes will be created into the DUTRT. And the start time of the flow will also be recorded. If the Agent is used as a standalone meter, the continuous statistic information of the flow (such as bytes or packages etc.) will be added into the same entry. After the stop of the flow, the end time of the flow will be recorded into this entry.

The records of DUTRT table will be sent to or collected by IP Mediation layer periodically.

According to the User model, several attributes in a traffic flow and corresponding TO information are collected to construct a DUTRT. For example, an entry of the table may include several items as below:

<**UserID, Source IP, Source Port Number, Destination IP, Destination Port Number, Timestamp**>.

A record in the DUTRT includes three kinds of attribute:

1. Traffic-Originator attribute: it is used to uniquely identify a TO, who produces the traffic. As for the above example, TO attribute includes these items: <**UserID, Source IP**>.
2. Correlation attribute: it is used to correlate a traffic flow to a corresponding user. The Correlation attribute includes flow related information that are usually extracted from IP traffic flows or IP packages, and RDRs produced by meters also record all these needed attributes. [6] defines the attributes and format of RDR. As for the above example, Correlation attribute includes these items: <**Source IP, Source Port Number, Destination IP, Destination Port Number, Timestamp**>

3. Statistic attribute: If the Agent is used as a standalone meter, the attributes such as bytes, packages count etc. will be collected for the purpose of measuring the network resource consuming.

The Agent does not generate the RDRs directly, but generates the DUTRT, the reasons are:

- This method can easily be integrated into the now existent IP Billing system.
- Generating all the RDRs and all their attributes will cost more system resource in multi-user systems and will affect the system performance.

3.2.3 Agent

The Agent can be implemented as a standalone software or a part of the multi-user system kernel. It checks all traffic flows to extract user information for the purpose of User oriented IP accounting. Its main functions include:

1. Capturing packages or traffic flows and extracting the Correlation attribute items from them.
2. According to the requirement of the User Model, retrieving the corresponding TO attribute items of the traffic flow from the system.
3. Combining the TO attribute and the Correlation attribute items together to generate a record into the DUTRT.
4. If the Agent works as a standalone meter, it will collect more accounting information of traffic flows and record them into DUTRT. In this case the entries of DUTRT will be used as RDRs.
5. Transferring DUTRT records to IP Mediation layer.

3.2.4 Correlation processing

The Correlation process is the same as it in traditional IP accounting systems, except that an additional Dynamic User-TrafficFlow Relationship Table, combining with a Traffic-Originator & User Map Table, will be used to map the RDRs to the corresponding users. The DUTRT is generated by the Agent, and it is used to identify the TO of each flow. The Traffic-Originator & User Map Table is used to record TO and User's static relationship. Whenever a new user account is created in a multi-user system, a new entry will be added into this table. It is managed by the IP Mediation layer. The Traffic-Originator & User Map Table will not be changed unless the user account is changed in a multi-user system.

Figure 6 illustrates an example of the correlation processing with User oriented IP accounting method.

From the Figure 6 we know, although the users in the multi-user system produce the RDRs all with the same source IP address (Ai.Bi.Ci.Di), the RDRs include other correlation attribute items<**Source IP, Source Port Number, Destination IP, Destination Port Number, Timestamp**>. With the DUTRT and the Traffic-Originator & User Map Table, the Correlation Module can correlate the RDRs to the corresponding USERs and generate the Usage Records with correct user information. Comparing with the IP Address & User Map Table in Figure 4, this

method uses a DUTRT and a Traffic-Originator & User Map Table. The DUTRT includes more detailed TO information to help distinguish all traffic flows' producers in the multi-user systems.

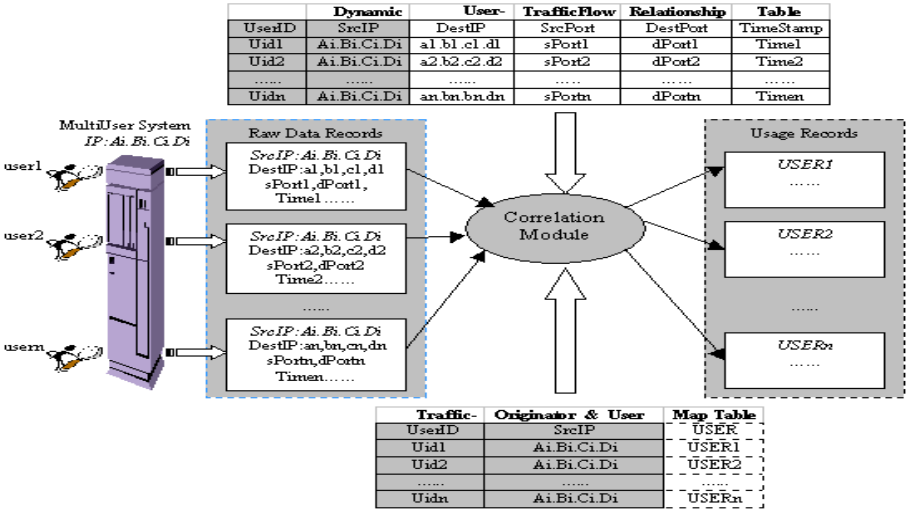


Figure 6. User oriented IP accounting method correlation process in multi-user system

3.2.5 Traffic-Originator information storing and transporting methods

After the collection of the TO information, the next consideration is how to store and transport these TO information.

The legacy accounting protocols [1] such as Radius, Tacacs+ and SNMP etc. can be used to work together with the Agent to implement the User oriented IP accounting. For example, according to the above described User oriented IP accounting principle, the realization of the Agent can be designed as a SNMP agent in the multi-user system. At first the collected TO information will be stored into MIB database, then the SNMP protocol can be used to transport these TO information data in the MIB database to the meters. Using this method, a user oriented IP accounting MIB standard should be defined. The [7], [8] described standards can be modified to meet this requirement.

Another method called protocol header method has been discussed in [9]. The principle of this method is to utilize the option field of the IP protocol header to carry the TO information, which will be inserted by the Agent. By this means, no DUTRT is needed, and the main function of the Agent is only to identify the producer of the IP traffic, and then to add the TO information into IP packages. The TO information will not be stored in the multi-user system. Outside the multi-user systems, the IP traffic meter can collect the IP traffic's TO information directly from the protocol headers of the IP packages.

The advantage of utilizing the legacy accounting protocols is that these accounting protocols are widely accepted, but they will cause more overhead to the multi-user system and the network. The advantage of protocol method is that it will cause less overhead to the multi-user system and network. But the disadvantage is that this method needs the IP protocol to be modified, and security of the user information included in the IP protocol header is also a problem. Therefore the later method is considered to be unpractical.

3.2.6 Realization of Agent Method of User Oriented IP Accounting

According to the principle of Agent method of User oriented IP accounting, the key of the realization of user oriented IP accounting in multi-user systems is the realization of the Agent, which can generate the DUTRT. In order to collect the corresponding TO information of IP traffic flows, the Agent must locate in the multi-user system, outside the multi-user system no mechanism can obtain the TO information of the IP traffic alone.

Because the Agent needs to obtain the TO information of the IP traffic, usually the realization is OS dependent, in other words it is OS kernel dependent. For example, usually the TCP/IP drivers are implemented in kernel mode. Here we consider about two realization methods:

1. Kernel modification.

The principle of this method is, directly modifying the tcpip driver, inserting the Agent function of the user oriented IP accounting into the driver. By this means, the build-in user oriented IP accounting Agent can generate the DUTRT. Because the Agent is located in the tcpip driver, it can check all IP traffics and obtain the corresponding TO information. It can be describe as Figure 7.

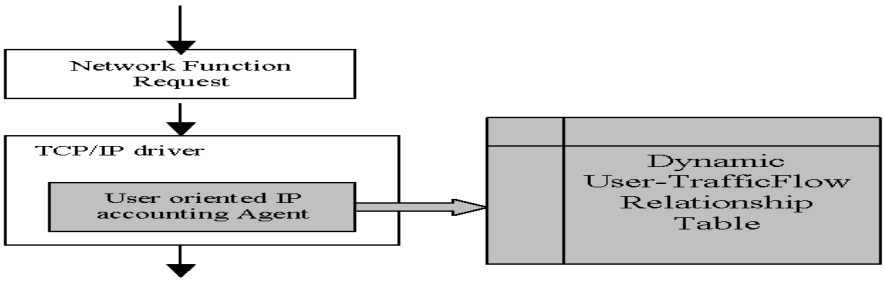


Figure 7. Principle of kernel modification method

This method is based on this precondition: the OS source code can be obtained and modified. It is fit for OS producer to make this modification, or for open source code OS (e.g. Linux).

[10] has implemented UserIPAcct in Linux, which is a User oriented IP accounting realization. In UserIPAcct the tcpip driver is modified and strengthened to record the RDRs with TO information.

2. Kernel patch.

The principle of this method is, making the network requirements to tcpip driver be redirected to the user oriented IP accounting Agent. This method need not modify the system kernel, the Agent will be realized as a kernel patch. Figure 8 illustrates the principle of this method.

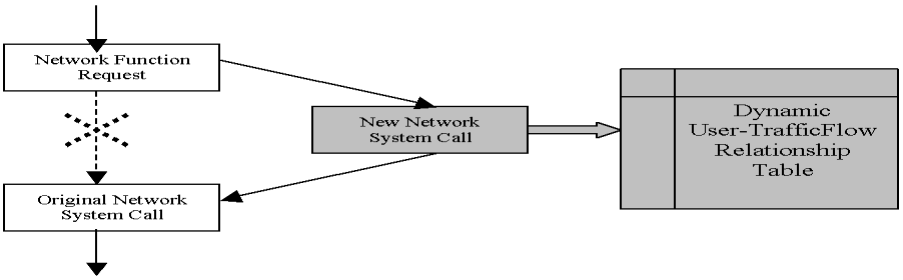


Figure 8. Network system call redirection

In the redirection technique, the request to original network function will be redirected to the new defined network system call, which can capture the network traffic flows and record the traffic and corresponding TO information to generate the DUTRT.

This method is fit for the non-OS producers, who cannot get the OS source code.

In our NIPON project we have implemented the prototype Agent software IPTrafficRecorder (IPTR) respectively in Solaris and Windows 2000 Server operating systems, it can collect IP traffic and corresponding TO information to generate the DUTRT. Figure 9 is a screenshot of the prototype Agent software IPTrafficRecorder's running under the Windows 2000 server. Here we can see that each package is identified by a Traffic-Originator. In the realization of the IPTrafficRecorder in Windows 2000 Server, an Agent, the IPTR driver, works above the tcpip driver, and captures all the network request to the tcpip driver, and then it extracts the traffic information and the corresponding TO information.

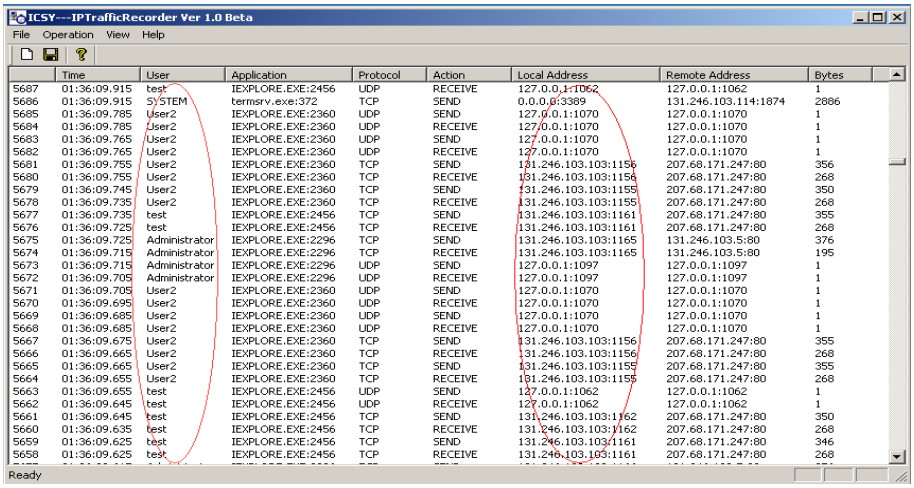
Comparing the two above described user oriented IP accounting realization methods with each other, the kernel modification method is a better solution. Because in this method, the Agent works in the tcpip driver, all the IP traffic related operation can be traced and recorded. But for the kernel patch method, since it works outside the tcpip driver, some in the tcpip driver fulfilled IP traffic related operations cannot be recorded. For example, the three-way handshake of the tcp connection is completed in the tcpip driver, the kernel patch method cannot capture the packages related with this process. For the kernel patch method, it can meter most of the IP traffic, and it is a simple method without modifying the kernel code.

The collection and transferring of the TO information of IP traffic flows will cause overhead to the multi-user system and the network. There are some ways to reduce the performance affection:

1. Agents collect only TO and Correlation attribute information. Other accounting information such as bytes count etc. will be collected by the outside meters. This can relieve the load to the multi-user system, and also

can reduce the transferring data volume from multi-user system to IP mediation system. Agents will not be used as standalone meter.

2. Using kernel modification method to implement the Agent. This will improve the efficiency of the Agent.
3. User oriented IP accounting may be configured as an optional function for the multi-user systems. If this function is not needed, or IP address can be regarded as user, the User oriented IP accounting Agent needs not be started.



	Time	User	Application	Protocol	Action	Local Address	Remote Address	Bytes
5687	01:36:09.915	test	IEXPLORE.EXE:2456	UDP	RECEIVE	127.0.0.1:1062	127.0.0.1:1062	1
5686	01:36:09.915	SYSTEM	termsrv.exe:372	TCP	SEND	0.0.0.0:3389	131.246.103.114:1874	2886
5685	01:36:09.785	User2	IEXPLORE.EXE:2360	UDP	SEND	127.0.0.1:1070	127.0.0.1:1070	1
5684	01:36:09.785	User2	IEXPLORE.EXE:2360	UDP	RECEIVE	127.0.0.1:1070	127.0.0.1:1070	1
5683	01:36:09.765	User2	IEXPLORE.EXE:2360	UDP	SEND	127.0.0.1:1070	127.0.0.1:1070	1
5682	01:36:09.765	User2	IEXPLORE.EXE:2360	UDP	RECEIVE	127.0.0.1:1070	127.0.0.1:1070	1
5681	01:36:09.755	User2	IEXPLORE.EXE:2360	TCP	SEND	131.246.103.103:1156	207.68.171.247:80	356
5680	01:36:09.755	User2	IEXPLORE.EXE:2360	TCP	RECEIVE	131.246.103.103:1156	207.68.171.247:80	268
5679	01:36:09.745	User2	IEXPLORE.EXE:2360	TCP	SEND	131.246.103.103:1155	207.68.171.247:80	350
5678	01:36:09.735	User2	IEXPLORE.EXE:2360	TCP	RECEIVE	131.246.103.103:1155	207.68.171.247:80	268
5677	01:36:09.735	test	IEXPLORE.EXE:2456	TCP	SEND	131.246.103.103:1161	207.68.171.247:80	355
5676	01:36:09.725	test	IEXPLORE.EXE:2456	TCP	RECEIVE	131.246.103.103:1161	207.68.171.247:80	268
5675	01:36:09.725	Administrator	IEXPLORE.EXE:2296	TCP	SEND	131.246.103.103:1165	131.246.103.5:80	376
5674	01:36:09.715	Administrator	IEXPLORE.EXE:2296	TCP	RECEIVE	131.246.103.103:1165	131.246.103.5:80	195
5673	01:36:09.715	Administrator	IEXPLORE.EXE:2296	UDP	SEND	127.0.0.1:1097	127.0.0.1:1097	1
5672	01:36:09.705	Administrator	IEXPLORE.EXE:2296	UDP	RECEIVE	127.0.0.1:1097	127.0.0.1:1097	1
5671	01:36:09.705	User2	IEXPLORE.EXE:2360	UDP	SEND	127.0.0.1:1070	127.0.0.1:1070	1
5670	01:36:09.695	User2	IEXPLORE.EXE:2360	UDP	RECEIVE	127.0.0.1:1070	127.0.0.1:1070	1
5669	01:36:09.685	User2	IEXPLORE.EXE:2360	UDP	SEND	127.0.0.1:1070	127.0.0.1:1070	1
5668	01:36:09.685	User2	IEXPLORE.EXE:2360	UDP	RECEIVE	127.0.0.1:1070	127.0.0.1:1070	1
5667	01:36:09.675	User2	IEXPLORE.EXE:2360	TCP	SEND	131.246.103.103:1156	207.68.171.247:80	355
5666	01:36:09.665	User2	IEXPLORE.EXE:2360	TCP	RECEIVE	131.246.103.103:1156	207.68.171.247:80	268
5665	01:36:09.665	User2	IEXPLORE.EXE:2360	TCP	SEND	131.246.103.103:1155	207.68.171.247:80	355
5664	01:36:09.655	User2	IEXPLORE.EXE:2360	TCP	RECEIVE	131.246.103.103:1155	207.68.171.247:80	268
5663	01:36:09.655	test	IEXPLORE.EXE:2456	UDP	SEND	127.0.0.1:1062	127.0.0.1:1062	1
5662	01:36:09.645	test	IEXPLORE.EXE:2456	UDP	RECEIVE	127.0.0.1:1062	127.0.0.1:1062	1
5661	01:36:09.645	test	IEXPLORE.EXE:2456	TCP	SEND	131.246.103.103:1162	207.68.171.247:80	350
5660	01:36:09.635	test	IEXPLORE.EXE:2456	TCP	RECEIVE	131.246.103.103:1162	207.68.171.247:80	268
5659	01:36:09.625	test	IEXPLORE.EXE:2456	TCP	SEND	131.246.103.103:1161	207.68.171.247:80	346
5658	01:36:09.625	test	IEXPLORE.EXE:2456	TCP	RECEIVE	131.246.103.103:1161	207.68.171.247:80	268

Figure 9. IPTrafficRecorder in Windows 2000 Server

The overhead caused by User oriented IP accounting is unavoidable, because the user information is invisible outside the multi-user system. What we can do is to lessen the performance affection to the multi-user system and the network caused by the Agent.

4. SUMMARY

In this paper we have presented a user oriented IP accounting technology in multi-user systems. It can provide more accurate accounting information than the traditional IP address oriented accounting technology, and it extends the traditional IP accounting technology.

User oriented IP accounting utilizes an Agent to collect TO information of the IP traffic from the multi-user systems, these TO information will then be stored in the Dynamic User-TrafficFlow Table, which can be used to correlate the user with the IP traffic. The extended legacy accounting protocol methods can be used to convey the TO information. In realization of the user oriented IP accounting, two methods, kernel modification method and kernel patch method, have been suggested.

Comparing with the two methods, the kernel modification method is a more precise method, which can collect the required accounting information more completely.

The suggested User oriented IP accounting architecture is based on the traditional IP accounting system. It is an extension of the traditional IP accounting architecture. The traditional IP accounting meters will be used to collect accounting information of single user systems, and the Agent will be used to collect accounting information in multi-user systems. Now existent IP accounting systems can enhance its IP accounting ability in multi-user systems without influencing its ability in single user systems.

In our NIPON project we have implemented a user oriented IP accounting prototype with the kernel patch method in Solaris and Windows 2000 server respectively. In the future we will develop a user oriented IP accounting system in the computer center of University of Kaiserslautern, and this user oriented IP accounting system will mainly run in the Solaris, Linux and Windows 2000 Server. And the kernel patch method will be used to implement this. The kernel modification method maybe a suggestion for the OS producers. To realize the kernel modification method, some standards of the user oriented IP accounting should be defined.

5. REFERENCE

[1] B.Aboda,J.Arkko, D. Harrington: “Introduction to Accounting Management”, RFC2975, October 2000

[2] Ge Zhang, “Comparison and Analysis of IP billing Technologies”, Internal Report, University of Kaiserslautern, November 2001

[3] Lucent Technologies, BILLDATS® Data Manager, http://www.lucent.com/

[4] S.Handelman, S. Stibler, N. Brownlee, G. Ruth: “RTFM: New Attributes for Traffic Flow Measurement”, RFC2724, October 1999

[5] Nevil Brownlee, “Using NeTraMet for Production Traffic Measurement”, Integrated Management Strategies for the New Millennium, December 5, 2001

[6] N.Brownlee,A.Blount: “Accounting Attributes and Record Formats”, RFC2924, September 2000

[7] N. Brownlee, C. Mills, G. Ruth: “Traffic Flow Measurement: Architecture”, RFC2722, October 1999

[8] N. Brownlee: “Traffic Flow Measurement: Meter MIB”, RFC2720, October 1999

[9] Volker Bauer: “Analyse von Netwerk-Abrechnungs-Systemen bezueglich nutzerorientierter Datanerfassung”, Diplomarbeit, Univeritaet Kaiserslautern, September 2000

[10] Lars Fenneberg, et. al., “UserIPAcct - a program to do per user ip accounting”, http://ramses.smeyers.be/homepage/useripacct/