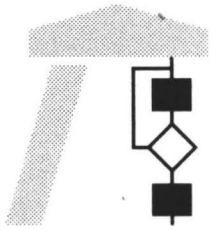
Interner Bericht

Comparison and Analysis of IP Billing Technologies

Ge Zhang

321/02



FACHBEREICH
INFORMATIK

UNIVERSITÄT
KAISERSLAUTERN

Postfach 3049 · D-67653 Kaiserslautern

Comparison and Analysis of IP Billing Technologies

Ge Zhang

November 2001

Integrated Communication Systemes
Computer Science Department,
University of Kaiserslautern,
P.O. Box 3049,
67653 Kaiserslautern
Germany

Contents

1. Introduction

1.1. Purpose

The intent of this paper is to:

1. introduce the IP Billing technology and give some criteria for the evaluation of IP Billing systems;
2. introduce several IP Billing products ;

1.2. Terminology and Glossary

1.2.1. Terminology

1.2.1.1.1. Term	*1.2.1.1.2. Definition*
Accounting	The process of collecting and analyzing network services and resource usage metrics with the purpose of capacity and trend analysis, cost allocation, auditing,a nd billing, etc..Accounting management requires that resource consumption is measured, rated, assigned,a nd interchanged between appropriate business entities.
Billing	The process of consolidating charging records on a per customer basis and delivering a certain aggregate of these records to a customer.
Mediation	The process of collecting information of network services and resource usage, processing the collected data to generate usage records, storing and distributing the usage records.
Network Element	The network devices or application servers that are used to provide communication services
Rating	The process of determining the price of a unit of service according to the price schemes
Resource	A quantifiable asset employed by a service provider,o r on behalf of a service provider by another service provider, to fulfill a request of a service consumer.
Service	Network and/or application operation that provides the service consumer with there quested resource.
Service Consumer	The beneficiary (human or system) of a service.
Service Provider	An enterprise thatp rovides communication-based services.
Usage	Consumption of resources and services by a service consumer.
Usage Attribute	A parameter whose value indicates some aspect of usage of a given service and/or resource.

1.2.2. Glossary

BSS	Business Support System
DNS	Domain Name Service
DHCP	Dynamic Host Configuration Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPDR	Internet Protocol Data Record
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LDAP	Lightweight Directory Access Protocol
MIB	Management Information Base
NE	Network Element
OSS	Operation Support System
QoS	Quality of Service
RADIUS	Remote Access Dial-In Usage Server
RAS	Remote Access Server
RDR	Raw Data Record
RMON	Remote Network Monitoring
RSVP	Resource ReSerVation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
VoIP	Voice over IP
VPN	Virtual Private Network
XML	eXtensible Markup Language

2. IP Billing Technology

2.1. IP Billing Model

The general IP Billing model can be described as seen in Figure 2.1:

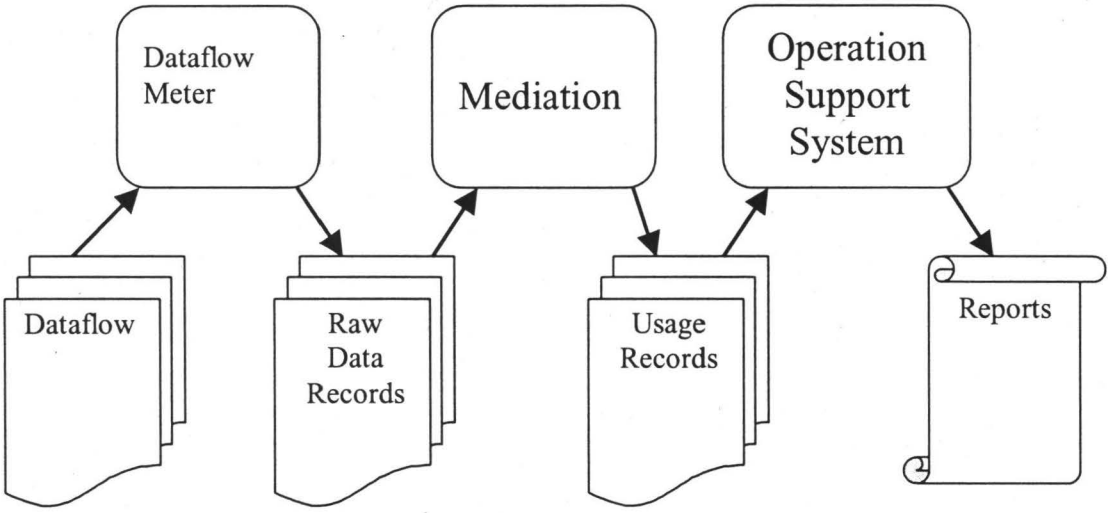


Figure 2-1 IP Billing Model

The IP Billing model consists of three layers: dataflow meter layer, mediation layer and billing / OSS /BSS(Operating/Business Support System) layer. The dataflow meter layer records network activities in Raw Data Records comparable to an electricity meter. The mediation layer collects Raw Data Records from various network elements, and processes these Raw Data Records to produce the usage records,w hich are stored in a database. It also distributes the usage records to different applications in the OSS layer. The OSS layer consists of several applications e.g. Billing, Fraud Detection, Traffic Analyze. Each off them generates reports for different purposes.

A general IP Billing system architecture is described by Figure 2.2:

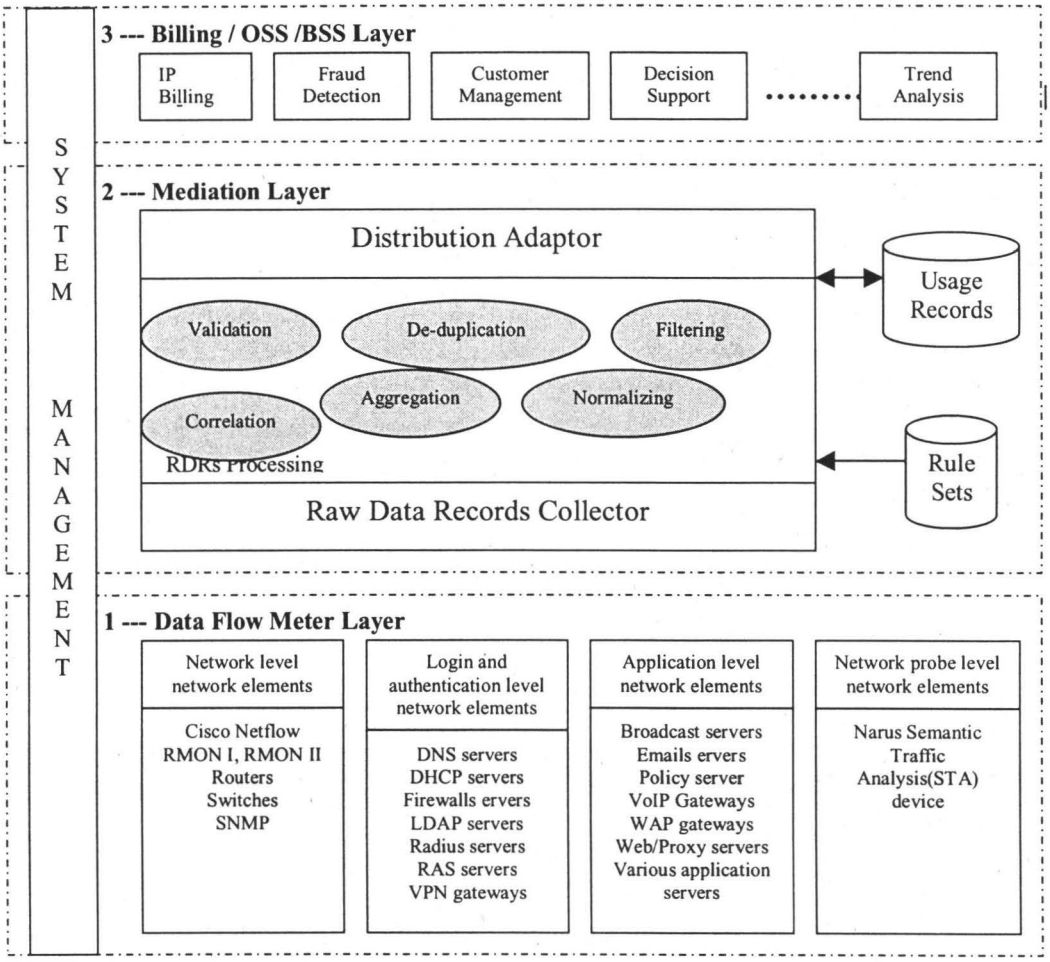


Figure 2-2 IP Billing System Architecture

2.2. Dataflow Meter Layer

The dataflow meter layer is composed of network elements which have the capability to log information about IP traffic passing through them. The Network Elements record network activities in Raw Data Records and store them in certain formats. These Raw Data Records can be sent to or collected by the mediation layer.

The main functions of the dataflow meter layer are:

- Recording information about network activities in Raw Data Records;
- Supporting the analysis of protocol layers 1-7 in order to form Raw Data Records;
- Normalizing the Raw Data Records into a certain format;
- Storing the Raw Data records;
- Providing the mechanism to transport Raw Data Records to the mediation layer.

2.2.1. Types of Dataflow Meter

The dataflow meter layer includes different kinds of network elements. These network elements are provided by differentv endors, and most of them are not only designed for IP Billing. So the approaches of recording dataflow and the formats of the Raw

Data Records are different. There are mainly three approaches of dataflow metering : log file based dataflow meter, flow based dataflow meter and probe based dataflow meter.

2.2.1.1. Log File based Dataflow Meter

A log file is created by a network element, itr ecords the network activities which occur in this network element. These network activities only concern the services which are supported by this network element. For example, when a user dials into an IP network, the network access server collects the user ID and password, and it also records this access event into a log file. Then the network access server sends the login information to an authentication server (e.g. RADIUS, TACCAS). The authentication server may also log the received information.

The main advantage of the log file based dataflow metering is that network elements have the capability of logging the network events when they provide various services. But this approach has several limitations:

- Coverage: Many application sessions can take place from clientt o client. In this situation there is no server to log the network activities. For example, Microsoft Netmeeting can provide the communication between two PCs without using a server. In this case, there is no network element to log the information about the communication between the two PCs.
- Completeness: Log files are not designed for the purpose of IP Billing, so the log files from one network element can not capture and record enough information about the customer activities. Information of a session of a single user may be composed of the attributes, which are extracted from several log files in different network elements.
- Realtime : There is no event driver mechanism in the log file based dataflow meter. The network elements only record the network activities in the log files, they can noti nformother systems about their new log records. So the log files shall be scanned periodically, this can notm eet the requirements of the IP Billing system requirements for realtime capability.
- Different formats of log files: Different type of network elements or even the same type of network elements produced by different vendors have different formats of their log files. A custom interface must be added to process these log files of differentf ormats. The mediation layer has to be flexible to process these formats.
- Data redundancy: Since most of the log files are not designed for the purpose of IP Billing, the log files include many useless data for IP Billing, these redundant data mustb e filtered before or after they are sent to the mediation layer.
- Maintenance: Log files are stored in disks. With increasing size of the log files it may be necessary to backup or delete log files in order to avoid to run out of disk space. These processes must be synchronized with the mediation layer, but there is no mechanism to do this. For example, if an application server wants to delete a log file after backing it up, it must be known if all Raw Data Records in this log file have been collected by the mediation layer, before the mediation layer finally deletes the file.

2.2.1.2. Flow based Dataflow Meter

A network flow is defined as a unidirectional sequence of packets between a given source and destinated endpoints. Flow endpoints are identified both by IP address as

well as by port numbers. Because of their unidirectional nature, flows from a client to a server are different from flows from the server to the client. Flows are also differentiated by the basis of protocol. For example, HTTP packets are different to FTP packets so HTTP and FTP flows can be distinguished even if the source and destination hosts are the same.

The approach of the flow based dataflow meter is: when the first packet of a flow is captured, an entry for this flow is created to record the flow information, the subsequent packets in this flow are recorded and identified within the same flow. When the flow expires, all Raw Data Records of this flow can be exported to the mediation layer. Generation of the Raw Data Records is based on decoding and analyzing the packets in flows. Cisco NetFlow uses this approach.

The approach of the flow based dataflow meter has several advantages:

- It provides fine granularity of the resource utilization information. The Raw Data Records of flow include attributes such as source and destination IP addresses, source and destination port numbers, packets and bytes count, timestamps, type of service etc. These attributes can be used for usage based billing.
- The Raw Data Records are organized on the basis of flows. They can be easily collected and correlated by the mediation layer.
- The flow based dataflow meter can provide sending of eventd riven Raw Data Records. When a flow expires, the dataflow meter device can notify the mediation layer to collect the Raw Data Records. This can improve the realtime capability of IP Billing.

The approach of the flow based dataflow meter also has some disadvantages:

- Flow based approach can not provide complete usage information. Since flow based approach usually records the network and transport layer (OSI reference model layer 3 and 4), it can not provide detailed information about application level usage. NetFlow can provide the Type Of Service(TOS) attribute, but it can not provide more detailed attributes about the service it records.
- The flow based dataflow meter function is usually embedded in network elements such as routers. Since the network elements are in general not designed for dataflow metering purpose, such a function can impact the performance of the network elements. For example, by some estimates, enabling NetFlow on a Cisco router can drain CPU usage as much as 30 percent.[LuCo99]

2.2.1.3. Probe based Dataflow Meter

The probe based dataflow meter uses the network probe, which is usually placed at a key position of a network. The network probe captures all IP packets through the network, extracts the headers and specific data fields, and analyzes the protocols of all seven layer to generate Raw Data Records. The STA device of the Narus uses this approach. The STA device is a typical kind of network probe device, itu ses a session based semantic analysis technique. The STA device can detect, analyze and characterize contextual information transacted by an application during an identifiable period of time. Based on industry standard and proprietary protocol semantics, this device builds a statistical repository of all session per user over time.

The probe based dataflow metering has several advantages:

- This approach can capture all the packets through the network,i t can analyze all seven layer protocols and it can record all the information about the network

activities. This can help the IP Billing system to bill users according to their network resource usage.

- The probe does not rely on network elements to record information. It will not disturb the operation of the network elements.
- The usage information is collected in realtime. So it can meet the realtime requirements of the mediation and OSS layer.
- The Raw Data Records can be recorded on the basis of sessions. It is easy for the mediation layer to generate the usage Records for users.
- The probe can be placed at the key position, where all dataflow passes through, so all dataflow can be captured.

The session based dataflow meter also has disadvantages:

- Probes are additional network elements that must be installed and maintained.
- A large scale network requires more probes to be deployed to record all dataflow. These probes must be synchronized to remove duplicate events. This is a tough problem requiring a well considered solution.

2.2.2. Dataflow Meter Network Elements

A dataflow meter is a network elementw hich is able to record network activities. According to [Schw99], till September 1999 there were about at least 160 types of network elements.

The main types of network elements include:

- sdfsdf

1. Application level network elements:
   - Broadcast servers – support music, video, games or education on demand.
   - Email servers – log information aboute ach email sent or received across the corporate network or via internet.
   - Policy server – implement routing policy on request of subscribers, requiring quality of service through the network. Support for RSVP.
   - VoIP Gateways(MGCP, H.248,H .323) – support video conferencing or VoIP over LANs, intranets and internetl inking H.320 ISDN and H.323 video conferencing systems.
   - WAP gateways – log information about the activity of each WAP session handled by the WAP gateway.
   - Web/Proxy servers – log network traffic.
   - Various application servers.
2. Login and authentication level network elements:
   - DNS servers – associate host names with IP addresses.
   - DHCP servers – used to dynamically assign IP addresses to users while they log on.
   - Firewall servers – used to ensure security of private networks.
   - LDAP servers – directory service to manage user accounts.
   - Radius servers – provide information on individuals logged in via modems or ISDN connections.
   - RAS servers.
   - VPN gateways
3. Network level network elements

- Cisco NetFlow capable devices
- RMON I, RMON II devices
- Routers
- Switches

4. Network probe level network elements
   - Traffic Analysis(STA) devices

2.2.3. Rules and rule sets for a dataflow meter

Rule sets are held within a meter as entries in an array of rule sets. Rule sets define methods for dataflow meters to record the network activities. The rule sets are used by dataflow meters to classify incoming packets and to decide how to generate Raw Data Records.

Different type of network elements have different rule sets. Some network elements have fixed rule sets, which can not be configured. Other network elements have configurable rule sets for dataflow meters, which can be used to change the characteristics of the dataflow meter. The mediation layer is supposed to comprise the interface for configuring the rule sets in the dataflow meter layer in order to provide more flexibility concerning the control of generation of Raw Data Records.

A rule set can abstractly be structured as follows:

Rule Set ::= Rule | {Rule ;}

Rule ::= Test ; Action

Test ::= value=attribute & mask

Action ::= opcode | {parameter ;}

The 'Test' part calculates the condition value, the 'Action' part operates according to the condition value.

2.2.4. Attributes and formats of Raw Data Records

Different types of network elements generate different attributes and formats of Raw Data Records, and these Raw Data Records can be transferred by different transport protocols.

An attribute field consists of an Attribute-Value Pair(AVP). An AVP defines the name of the attribute and the corresponding value. In [RFC2924] the attribute definitions used in many IETF documents are summarized. For example Radius attributes, DIAMETER attributes, ROAMOPS attributes, RTFM attributes, ISDN MIB attributes, AToMMIB attributes, RSVP and DIFFSERV attributes, etc. Except of these standard attributes, different application network elements and different vendors have their own definitions of the AVPs to record their specific application activities.

A Raw Data Record consists of several AVPs, the formato f a Raw Data Record defines the encoding rules, specifying how to encode lists of AVPs into records. There are three main types of record format:

- ASN.1 record format: It uses ASN.1 Basic Encoding Rules(BER) to encode lists of attributes into record. For instance, SNMP MIB, RTFM and AToMMIB use this format. This scheme can fitw ell with SNMP based network management systems and provides a good way to record the network activities. But the

structure of ASN.1 based scheme is very complex, purpose-build tools are needed to deal with these structures.

- Binary record format: It uses octets to encodes the attributes into records. RADIUS and DIAMETER use this type of record format. The structure of this scheme is simple, but it also needs to be processed with purpose-build tools. Furthermore the extensibility is not good.
- Text record format: It uses ASCII text to encode attributes into record. ADIF (Accounting Data Interchange Format) is an example for this kind of record format. It presents a general, text-based format for accounting data files, described in a BNF grammar. The records in this format are easy to be read and understood. The size of files in this format might be bigger, but compression can be used to reduce the file size for storage or transport.

2.2.5. Raw Data Records transfer

Several ways can be used to transfer Raw Data Records:

- File based Raw Data Records: they can be transferred by FTP, SMTP etc. protocols.
- Database based Raw Data Records: they can be retrieved and transferred by SNMP, SQL-like language.
- Cache based Raw Data Records: they can be transferred by TCP, UDP protocols.

2.2.6. Accounting protocols

An accounting protocol, such as RADIUS, DIAMETER,T ACACS+, is a protocol used to record accounting event data and convey data for accounting purpose. Accounting servers use accounting protocols to record the service and resource usage metrics. Note: SNMP could be used to transport accounting information and may provide some functionality of an accounting protocol also.

These protocols define the accounting record attributes, formats, and rules for the transfer of the records. According to the accounting protocol, an accounting server can record network activities and can generate the Raw Data Records, so itc an be used as a dataflow meter.

2.2.7. Criteria for evaluation of products as a dataflow meter

Most of the network elements which are used as dataflow meter are not only designed for the purpose of generating accounting Raw Data Records. So there are no uniform criteria for evaluation of products as a dataflow meter. If a network element meets some basic requirements for a dataflow meter,i t can be used as a dataflow meter.

The basic criteria for a dataflow meter are:

- Capability to record one or more types of network activity.
- Capability to generate Raw Data Records and store them for a period of time in any format.
- Provision of a communication mechanism to support collecting of Raw Data Records by mediation layer devices.

For better recording of the network activities, dataflow meter products have to meet more advanced requirements:

- Realtime capability: recording of network activities in realtime, and reporting Raw Data Records to the mediation layer devices in realtime or supporting of the Raw Data Records being collected by the mediation layer devices in realtime.
- Minimal impact on the performance of the network element: Since most of the network elements are not designed for the purpose of recording network activities, the recording of network activities shouldn't cause too much decline of performance of the network element.
- Fault tolerance: If failures of the network as such or network elements occur, a mechanism, preventing from loss of recording of network activities, has to be provided.
- Reliability: the Raw Data Records have to be stored before they can be collected by mediation layer devices. So the non-volatile storage for undelivered Raw Data Records is a good way to realize the reliability. The mechanisms to transfer reliable Raw Data Records should be applied in order to avoid data loss. During the process of transporting Raw Data Records to the mediation layer, a retransfer mechanism needs to be introduced. The Raw Data Records are not ought to be deleted before a confirmation is received that they have been collected by the mediation layer.
- Configurable rule sets for the generation of Raw Data Records: the configurable rule sets define how to recordn etwork activities, which attributes shall be recorded, and how to generate the Raw Data Records. This can help the dataflow meter to be more flexible in recording network activities.
- The capability of recording usage sensitive information: since usage-based billing will be more popular in the future of IP Billing, the capability of recording usage information will be a requirement for a dataflow meter.

2.3. Mediation Layer

Since many IP Billing systems are first derived from traditional telecommunication billing technology, some of the concepts from telecommunication billing technology are used today for IP Billing technology. The term 'Mediation' in traditional voice technology means taking data off of the switch and capturing it. The data is then passed to a rating system to calculate the actual charges. The IP mediation process is similar to the traditional telecommunication mediation, but the IP mediation is more complex than the one that is used in traditional telecommunication. IP mediation first collects the Raw Data Records from various network elements, and then, according to mediation rules, filters, de-duplicates, merges, correlates, aggregates, and normalizes the collected Raw Data Records to generate the usage Records in any format, stores the usage records, and finally distributes these formatted usage records to different applications in OSS layer for different usage-purpose.

2.3.1. Raw Data Records Collector

The collector is responsible for collecting the Raw Data Records from various types of dataflow meter devices. When using a collector, several factors must be considered:

2.3.1.1. Interface with network elements

Due to the diversity of network elements, the collector should have the capability of interfacing with different types of network elements. A collector device can have one or more interfaces with the network elements. In order to collecta ll Raw Data Records from all network elements more than one collector device is usually used in larger networks.

2.3.1.2. The placement of the collector

Two principles shall be considered, when collectors are deployed:
Enough RDRs can be collected according to the mediation rule sets. This means the collected RDRs can be used effectively to generate usage records to meet the requirements of the applications in the OSS layer. So usually the collector devices are located at the key places, where enough RDRs can be collected, but less redundant or useless RDRs will be collected.

5. Minimal traffic on the network. This means that the RDRs collection shouldn't make an impact on the performance of the network. So the collector devices are usually located close to the information sources.

2.3.1.3. Approaches of Raw Data Records collection

From the point of view of the originator of the Raw Data Records transfer, there are two different kinds of approaches: push and poll communication.

The dataflow meters can be the originator of the RDRs traffic they can start the process of RDRs collection by sending the RDRs to the RDRs collectors. This is called push approach. In this way the collector devices waitf or requests from the network elements for data transport.Then they receive the RDRs sent by the network elements.

The poll approach is the RDR collector devices dragging the RDRs from the network elements. The collector device is the originator of the data collection.

The RDRs collector should have the capability of collecting RDRs in push or poll approaches.

There are four models describing data collection which are used today: Polling model, event- driven model without batching, event-driven model with batching, event-driven polling model. These four models implement the push or poll approaches respectively.

2.3.1.3.1. Polling model

In the polling model, a collector will poll network elements for RDRs at regular intervals. In order to ensure against loss of data, the polling interval will need to be shorter than the maximum time that RDRs can be stored in the polled network elements. For network elements without non-volatile storage, the maximum interval is determined by available memory, for network elements with non-volatile storage the maximum interval is determined by the size of non-volatile storage.

Usually during the interval of the polling, a network element will accumulate data, so data is typically transferred to the collector in batch, data can even be compressed, this can help to improve efficiency of the data transfer.

Since in this model the collector needs to poll all network elements, there are many elements which don't contain any relevantd ata. Another problem of this model is the latency. Because usage of an interval implies an average latency for each network element, which mightb e too high for RDRs that require low processing delay. This model is not suitable for realtime RDRs collection.

2.3.1.3.2. Event-driven model without batching

In the event-driven model without batching, a network element will inform the collector when an event is generated and when it is ready to transfer RDRs. This model offers the lowest latency since events are processed immediately. This model can be used for realtime RDRs collection.

Event-driven without batching usually transfers one event per packet, so this model is inefficient.

2.3.1.3.3. Event-driven model with batching

In the event-driven model with batching, a network element will inform the collector when a batch of a given size of RDRs has been gathered, or when RDRs of a certain type are available or after a minimum time period has elapsed. Such a system can transfer more than one event per packet and is more efficient.

Since the event-driven model with batching usually sends the RDRs to the collector after a batch of RDRs is prepared, latency concerning the events that require low delay might be caused. Through implementation of a scheduling algorithm, event-driven systems with batching are able to deliver urgent events to collector immediately. For example, high-value events can be sent at once, while all other events will be batched. With this approach, this model can be used for the realtime RDRs collection.

2.3.1.3.4. Event-driven polling model

According to the event-driven polling model a collector will poll the network element for RDRs only when it receives an event. The dataflow meter can generate an event

when a batch of given size of RDRs has been gathered, or when RDRs of a certain type are available or after a minimum time period has elapsed.

By transferring the batch of RDRs, the RDRs can be transferred efficiently. Whenever the collector polls the network element, it has to have RDRs to be sent. Compared to the non event driven polling model, the number of network elements needed to be polled is reduced.

Since this model needs at least two round-trips to deliver RDRs: one for the event notification, and one for the resulting poll, the latency in this approach is higher than in the event-driven model with batching.

2.3.1.4. Realtime Collection Consideration

Realtime RDRs collection is the base of realtime IP Billing. DifferentR DRs collection methods have different realtime characters.

- The batch approaches have poor realtime capability. The RDRs will be collected once a certain volume or time limitation is reached. So the RDRs collection is hard to be synchronized with network activities.
- The polling approaches can have close to realtime capability: This approach collects RDRs at regular intervals. If the interval is set short enough, the nearest synchronization can be reached with the network activities.
- The event driven approach can collect RDRs in realtime. An event will be sent to the collector at once when RDRs are generated by the network element,.T hen the collector is able to collect the RDRs. This approach has good realtime capability.

2.3.2. Raw Data Records processing

This stage processes the RDRs to generate usage Records. Rule sets will be used in the course of RDRs processing to control the generation of the usage Records. The main processing functions include:v alidation, de-duplicating, filtering, correlation, aggregation and normalizing.

2.3.2.1. Validation & Correction module

After the RDRs are being collected, some of them may be invalid or may include errors. This module checks, if the RDRs are valid. If a RDR is valid, itc an be processed by other processing modules. If a RDR is not valid, then this module will try to correct the errors according to predefined rule sets. If these errors can be corrected and the RDRs become valid, they will be handed down to other processing modules, otherwise the RDRs with uncorrectable errors will be discarded, and this discarding information will be written down in log files.

2.3.2.2. Filtering module

According to IP mediation rule sets this module discards the RDRs which have no use for generating usage Records. A filtering mechanism can be used in the collectors to reduce the data volume collected from network elements, and this will also lower the network traffic pressure caused by RDRs collection. After the RDRs are being collected, the filtering mechanism can also be used according to the dynamically configurable rule sets in order to reduce the data volume thatn eeds to be processed by other processing modules in the mediation layer.

2.3.2.3. De-duplicating module

This module discards duplicated RDRs collected by different collectors. When a dataflow passes through several network elements, these network elements will record the flow and generate the RDRs. So the same data flow may be measured several times producing redundant RDRs. Discarding these redundantR DRs will also reduce the data volume that needs to be processed to generate the usage Records. This module can be implemented by comparing the key fields of RDRs to decide if these RDRs are redundanto r not. For example, fields like source address, destination address, time-stamp etc. can be used to distinguish the redundant RDRs. If several RDRs of the same type have the same source and destination address, and the time-stamps are also the same, only one of them needs to be kept, others can be discarded.

2.3.2.4. Correlation & enhancement module

This module merges several RDRs, which are related to each other, to create a single record. This can provide a single, complete view of information about an event. For example, during VoIP calls intermediate RDRs are generated before the end of the call is reached. These intermediate RDRs of this VoIP call shall be merged with the Start RDR and the End RDR to generate a single record to represent this VoIP call event. Figure 2.3 below gives an example how NetFlow records , RADIUS records, and LDAP records are correlated to generate a usage record.

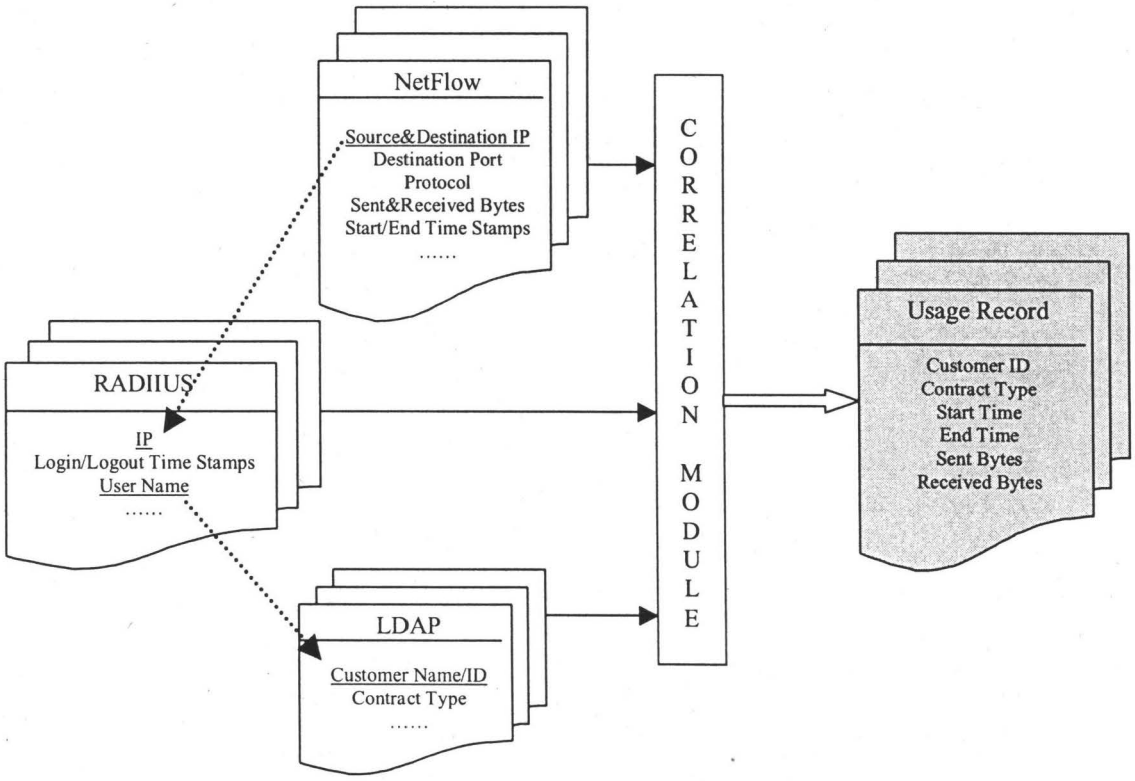


Figure 2-3 Process of Correlation

Enhancement is used when a RDR doesn't include enough information to generate a usage record,o ther RDRs will be referenced to enrich the information of this RDR. For example, usually the RDRs with an IP address only shall be enhanced with the user information. This can be reached by referencing to the collected RDRs from DHCP servers and DNS servers.

2.3.2.5. Aggregation module

According to the rule sets an aggregation module aggregates a set of RDRs to produce a usage record.T he usage record can then be used by the OSS layer applications. In the aggregation module different rule sets will be used to control the aggregation of the RDRs. The rule sets can define which fields are considered a key for the aggregation process, which operation to perform on aggregated fields, and under which circumstances the aggregation should time out.

2.3.2.6. Normalizing module

After processing the RDRs, the usage Records are generated. These usage Records can firstb e stored as a middle format or even as the raw format they are collected as. The normalizing module will then transform the usage Records to different formats according to the rule sets in orderto meet the requirements of different applications in OSS layer. Since different applications in OSS layer may need differentf ormats of usage Records to meet the different requirements, the normalizing module should support generation of specified formats such as IPDR, XML, Text etc. It should also have the extensible capability to support formats which mightb e developed in the future.

2.3.3. Formats of Usage Records

There are many kinds of formats of usage Records that can be used by applications in the OSS layer. For example, AMA, CSV, IPDR, XML etc. Some vendors even define and use their own formats. For the purpose of easy interfacing with OSS layer applications, the mediation layer should have the capability to generate all formats needed for the OSS layer applications .

Using so many formats in the IP Billing area, it is necessary to develop a standard format to make it easy to interchange the usage data between the network elements and the IP Billing applications. It is also a necessary requirement for future IP Billing applications.

IPDR (Internet Protocol Data Record) is a record format which is used as standard. Many IP Billing systems support itn owadays.

The IPDR format is defined by the IPDR working group. The IPDR working group is a non-profit organization that was formed to help facilitate the exchange of IP usage data between network elements, operation support systems, and business support systems. The IPDR standardizes a usage record format and delivery protocol. It represents the usage in encapsulation techniques such as XML. It defines an open, extensible, flexible record that encapsulates the essential parameters for any IP service transaction, including an extension mechanism so that network elements and support systems can exchange optional service metrics for a particular service.

2.3.3.1. IPDR record structure

The IPDR record structure thatm ight be collected from an IP based network or application service is able to characterize any type of usage. There are 5 components common to all IPDR records. These components are the 'who, what, where, when, and why' values that describe a particular usage event.

- Who
  - User ID (in some form, if available)
- When

- Start and Stop Time or Event Time of service usage
- What
  - Service type
  - Usage measures / quantities (e.g. bytes, packets, flows, hits, transactions, time duration)
  - QoS measures
  - State information
  - Eventc ode (logon, logoff, threshold exceeded)
  - Other information about state transition or current state
- Where
  - Traceability / Context
  - Source Identifier
  - Destination Identifier
  - Service ElementI dentifier (originator)
- Why
  - Event trigger type – (i.e., why is the network and service elementr eporting this data)

In addition to the '5Ws' defined, each record may include reference pointers to other IPDR records which either capture related usage information, or contain usage information that was used to create the given record.

In addition to the IPDR record structure, the IPDR specification defines a set of interfaces for exchanging IPDRs between IPDR-enabled devices or systems.

2.3.3.2. Services considered in IPDR

The IPDR considers many service which are structured in a hierarchy. For each service the IPDR specification describes the definition of the service , service requirements, attribute list for service usage and, for some services, the basic flow. The IPDR also defines the formal specification of the records for each service considered.

IPDR is an open standard, it can be extended to support new services in the future. Now the IPDR contain following services:
Application Services(ASP)

- Voice over IP (VoIP)
- E-mail Services
- Authentication and Authorization Services(AA)
- Internet Access
- Content Service
- Push Delivery
- Wholesale Requirements

Future considerations include:

- Video on Demand(VoD)
- Virtual Private Network(VPN)
- Multi-party conferencing(video/voice)
- E-commerce/ M-commerce
- Unified Messaging
- Video Conferencing over IP
- IP Television

2.3.4. Adaptor for distribution of Usage Records

The adaptor for distribution of usage Records interfaces with all applications in the OSS layer. It communicates with the applications of the OSS layer, uses push or poll approaches to send the usage Records to the downstream applications.

2.3.4.1.1. Transfer mechanism

To interface with different OSS layer applications the adaptor for distribution of usage Records should support different kinds of transfer mechanisms such as TCP, UDP, FTP, SMTP, Network File Sharing, CORBA, COM, SQL etc. This allows quick and easy integration of the mediation system with OSS layer applications.

2.3.4.1.2. Reliability

To obtain reliability the re-transmit mechanism should be used to transfer the usage Records again, once the usage Records are not delivered correctly to the applications of the OSS layer due to network failure or other reasons.

2.3.4.1.3. Security

The usage Records include many private information. These records are concerned with money in the billing system, so keeping security during the transfer of usage Records is very important. It is more necessary to add the security mechanism when the usage Records are being transmitted to remote applications.

2.3.5. Rule sets in the mediation layer

During the collection of RDRs, processing of RDRs and the distribution of usage Records , the rule sets of the mediation layer control all these activities.

During the collection of RDRs the rule sets control from which network elements RDRs should be collected, which kind of RDRs should be collected, which should be filtered, and the poll intervals of the collection of RDRs, and which transfer protocols should be used, etc.

During the processing of the RDRs, rule sets can control the validation, correction, filtering, de-duplication, correlation, enhancement, aggregation and normalizing of the RDRs. Rule sets also control the storage of the usage Records.

In the adaptor for distribution of usage records the rule sets also play an important role. They decide which applications the usage records should be sent to, which transfer protocols should be used, which kind of format of usage records should be used to meet the requirement of the downstream application, etc.

The flexibility and scalability of the mediation layer are implemented by configuration of the rule sets.

2.3.6. Management of the mediation layer

The mediation managements ystem implements several functions for management in the mediation layer: Configuration, Providing management interface, status monitoring, operations control.

Configuration

The mediation layer is the bridge between the Dataflow Meter layer and OSS layer. On the one hand, there are many different types of network elements which can be used as dataflow meter, and with the appearance of new network elements in the

future these new network elements may also be used as dataflow meter, the mediation layer should be flexible enough to accept these dynamic changes of network elements. On the other hand,t he mediation layer has to interface with differenta pplications in the OSS layer. The mediation layer should also be flexible enough to meett he requirements of the changes of the OSS layer applications. Furthermore, during the processing of the RDRs, different requirements mightb e desired from the RDRs processing. The rule sets can be defined to control the processing of the RDRs.

The mediation managements ystem can dynamically configure the mediation system through the modification of the rule sets, active adding or deleting its relationship with network elements or downstream applications.

Providing management interface

The mediation managements ystem should provide a user interface to the mediation system administrator. The administrator of the mediation system is able to manage the mediation system through the command line or GUI provided by the mediation management system.

Status monitoring

The mediation managements ystem monitors the status of the mediation system and generates the monitor report, the statistic result can be shown to the mediation system administrator through the management interface. Through monitoring the mediation system, the mediation system administrator can verify the health status of the entire system.

Operations control

The mediation managements ystem monitors can provide the control interface for the administrator of the mediation system to control the mediation system operations.The mediation system administrator can start up, shut down and suspend the operations in mediation layer.

2.3.7. Criteria for evaluation of the mediation layer

The mediation layer acts as a bridge, enabling the RDRs to be collected from different kinds of network elements, and transforming it into high value information, and then distributing the processed information to various downstream applications.

Here some criteria for the evaluation of the functionality of products used in the mediation layer are given:

- Can collect RDRs from multiple types of network elements
- Support push and poll approaches for RDR collection
- Support multiple transport protocols for RDR collection
- Support multiple data formats in input streams
- Support rule based RDR collection
- Support rule based RDR processing, such as filtering, validation, correction, de-duplication, correlation, enhancement, normalizing, etc.
- Can generate differentf ormats of usage records
- Support the storage of usage records
- Support the distribution of usage records to multiple applications
- Support multiple transport protocols for the distribution of usage records
- Provide the management mechanism for the mediation system

Here some criteria for the evaluation of the performance of products used in the mediation layer are given:

2.3.7.1.1. Scalability

The mediation layer can be dynamically extended to easily support adding of new network elements and new OSS layer applications without affecting the operation of the system. The mediation layer should be able to accommodate to the changes of the dataflow meter layer or OSS layer.

2.3.7.1.2. Flexibility

The mediation system can easily support different network infrastructure and application logic with configuration of the rule sets.

2.3.7.1.3. Reliability

The mediation system should be designed fault tolerant. During the collection of RDRs and distribution of usage records the data retransmission mechanism should be used, if faults occured. The validation and correction mechanism should also be used to guarantee the availability of the RDRs. Non-volatile storage should be used to facilitate the disaster recovery and minimize the threat of losing valuable billing data.

2.3.7.1.4. Security

Since data through the mediation system include private information and concern money in IP Billing cases, the importance of keying the security of data is self-evident. During the transport and processing of the data, security mechanisms should be considered.

2.3.7.1.5. Realtime capability

Different application requirements need different realtime capability. In some business cases realtime means better service and more customers, that also means more economic profit. In the mediation layer the realtime capability can be reached in three stages during the RDRs collection, processing and usage records distribution

2.4. IP Billing and OSS/BSS layer

OSS/BSS layer is the highest layer of the IP Billing model. It consists of different types of applications such as IP Billing, decision support, fraud detection, trend analysis, etc.T hese applications use different communication mechanisms to gather the usage records from the mediation systems. These applications are concern of different application areas, here we only discuss the technology of IP Billing.

Billing is the process of consolidating charge records on a per customer basis and delivering a certain aggregate of these records to a customer. So IP Billing means the process of collecting IP usage records from mediation devices, calculating the charge according to the price schemes, reporting their expenditure to the customers or delivering the invoice. This process can be described as shown in Figure 2-4.

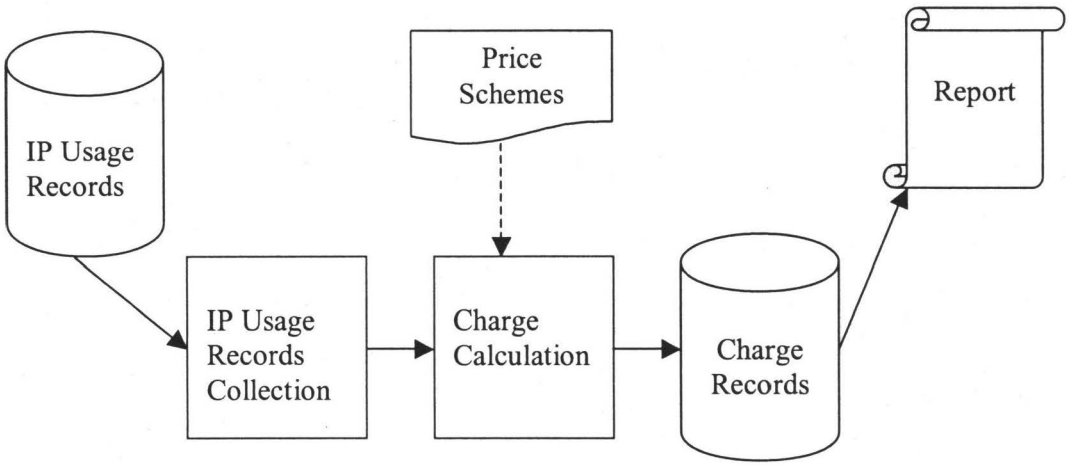


Figure 2-4 IP Billing process

2.4.1. IP Billing process

The IP Billing system consists of several modules.

2.4.1.1.1. Module for collection of IP usage records

This component interfaces with the mediation systems to gather the IP usage records generated by the mediation systems. The push or pull approaches can be used in the collection of the IP usage records. Since the mediation systems are usually flexible enough to transfer the IP usage records of different formats with many different kinds of transport protocols, the IP Billing systems don't need to pay more attention to the format of the IP usage records and the transportp rotocols. During the collection of IP usage records, rule sets can also be used to meet the dynamic change requirements, and this can make the system more flexible. After the IP usage records are collected, they will be sent to the Charge Calculation module at once.

2.4.1.1.2. Charge calculation module

This module accepts the IP usage records collected by the module for collection of IP usage records, and calculates the actual charge of customers according to the price schemes. The results of the calculation will be generated and stored as charge records. The charge records will atl ast be organized to present to the customers.

In the course of charge calculation the price schemes are very important, since all the calculating rules are defined in them. Through the adjustment of the price schemes the IP Billing system can provide flexible billing characters to meet the requirements of complex billing plans.

After the charge calculation the generated charge records are stored in a database, these charge records can then be used to generate the detailed reports or invoices to customers.

2.4.1.1.3. Report module

This module uses the charge records to generate the bills for every customer. The bill may be a printed invoice, additionally the customers can inquire and browse the billing information with a web browser. So the report module provides these functions:

- Bill organizing and generating. The detailed IP usage information should be provided to the customers when they are needed, customers can also design their own style of reports.
- Bill inquiring
- Bill displaying
- Bill printing

2.4.1.1.4. Price Schemes module

The price schemes define how the IP usage records should be calculated, and they also define price per unito f IP usage. The price schemes can be configured dynamically to meett he requirements of a frequently changed price policy. This module should provide the interface for definition and modification of the price rule sets.

2.4.2. Criteria for the evaluation of IP Billing systems

Here criteria for the evaluation of IP Billing systems are listed:

- Can gather IP usage records from mediation system
- Can calculate the charge of the customers' IP usage according to the price schemes
- Can generate the charge records and store them in a database
- Can organize the reports and generate the bills to for customers, and as multiple forms of bills, such as web forms or printed invoices etc., can be provided to the customers
- Can provide flexible mechanisms for price schemes
- Can provide the system management interface
- Can provide realtime billing capability

3. IP Billing products

In this chapter several IP Billing products will be introduced. The architecture of the products will be described, and then the functionality and technical features will be introduced. The product information provided in this chapter is mainly based on information provided by the producers of the products. The intention of this chapter is to provide an overview to the existing products. This is not a detailed or independent analysis of the different products.R eferences to the software producers and their web-sites is found in Appendix 4.

3.1. Product Introduction

Since all information about the products are gathered from internet, all introductions are based on these information. The products below are suggested from the Billing World Magazine. They are the most popular and typical IP billing systems used in the IP billing area. Although an IP Billing system consists of three layers as introduced above, the three layers are self-independent with each other, some of the products only realize one layer of the IP Billing system.These products have the interfaces with products of other layers. Different vendors' products may be used together to construct a complete IP Billing system.

3.1.1. Apogee Network

The NetCountant series products are the main IP Billing products of Apogee Network company.

3.1.1.1. NetCountant Content Collection

This product is a layer 2 product.T he NetCountant Content Collection platform collects descriptions of the IP content of multiple network elements for example Cisco System's NetFlow, Top Layer's TopFlow, network elements from HP, Narus, etc. Its main functions include:

- Aggregation all IP Content data in real-time in tables similar to RMON
- Supporting NetFlow versions 1, 5, and 7
- Provision of filtering and aggregation schemes
- Storage of data and keeping it available for network management applications
- Provision of a robust, flexible and fast way for applications to retrieve and use this information
- Making available of data to client applications via a proprietary and via the files

The NetCountant Content Collection system offers the key features listed below:

- A flexible configuration manager
- Usage-, protocol-, and application-centric
- Collecting NetFlow data from multiple NetFlow-enabled devices in a network
- Reducing the volume of NetFlow data through the use of filters and aggregation schemes
- Storing collected data in the form of multiple aggregations
- Providing mechanisms to retrieve the aggregated data via remote hosts
- Proving persistent storage for NetFlow information
- Notifying third-party applications of the newly generated aggregation files

The NetCountant Content Collection realizes all layer 2 functions of an IP Billing system. But the billing is based on the IP Content, and there are not too many network elements which can be used as RDR sources.

3.1.1.2. NetCountant Billing

NetCountant Billing is a layer 3 product. It provides capabilities for defining pricing plans, collecting usage data from a variety of existing sources and building electronic invoices based on that data. The main functions of NetCountant Billing are:

- Collection of usage data from a variety of existing sources
- Definition of pricing plans
- Content definition
- Pricing
- Workflow creation
- Account management
- Report

The key features are:

- Definition of pricing plans based on:
  - Network usage, network protocol, or application protocol
  - Content delivered, connection time, application usage
  - One-time and recurring charges
  - Time of day, and regional usage
  - Support for multiple fixed and variable cost components
- Settlement & Revenue Sharing
- Global Solutions with multilingual and localization support
- EBPP (Electronic Bill Presentment & Payment)
  - Web Bill Presentment
  - Paper Bill Printing & Feeds to Printing Services
  - Credit Card Processing
- Enterprise & Financial Interfaces
- Order Entry
- Support of typical costumer workflows
- Extensive business reports on financials and on usage

NetCountant Billing consists of the following major components:

- ICDR Databasein which Apogee Networks or third-party collection and mediation components store content and network event information.
- Billing, the main component, including the FlexRater, scalable and flexible rating engines, as well as Plan Management, System Administration, and Accounts Management capabilities.
- Customer Service, a multilingual workflow solution that provides step-by-step activities for both end-user online self-care and customer service representative.
- Bill Presentment Server, which provides the capability for customers to view their real-time billing information online, provides invoice or payment register printing and interfaces to high-volume printing services.
- Report Server, a flexible reportg enerator that displays business reports based on account and billing information as well as usage information.

3.1.2. Belle Systems

IMS(Internet Management System) is the IP Billing product of Belle Systems (or the new name, Digital Quant) company. The IMS is a comprehensive solution with capability to manage and account all aspects of IP services, from initial provisioning and deployment to mediation, rating, self-registration, and Customer Care and Billing.

The IMS provides the layer 2 and layer 3 solutions of IP Billing systems. Figure 3.1 shows the IMS architecture.

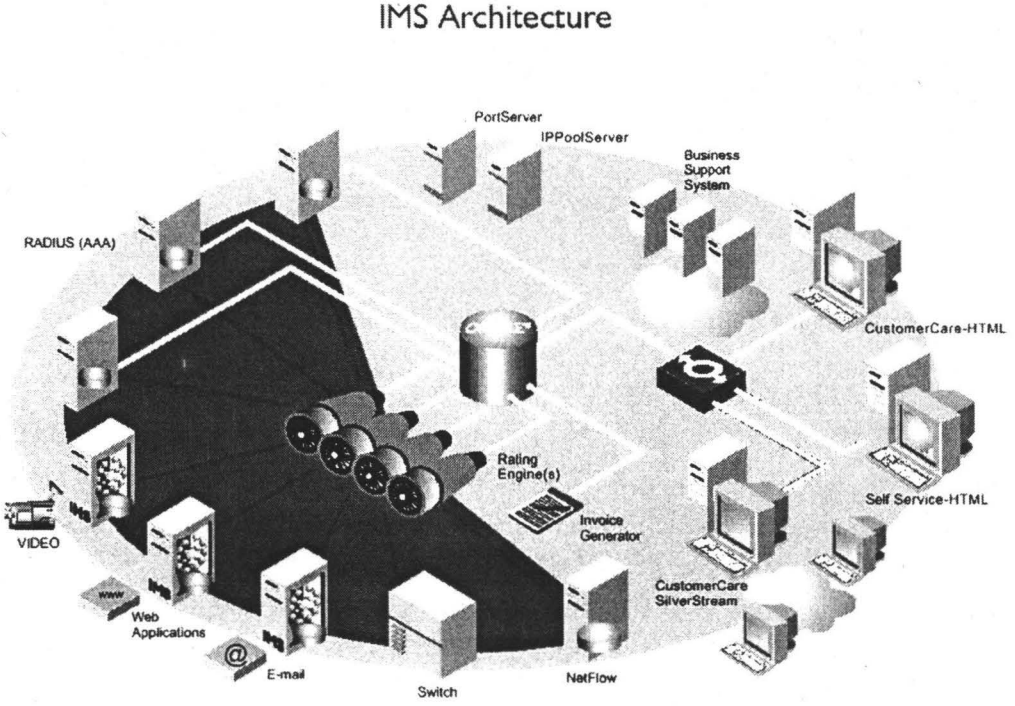


Figure 3-1 IMS Architecture

IMS provided functions include:

- Network element management
  IMS has the capability to manage network elements. It can enable user restrictions on network elements and assign appropriate QoS levels. It can also auto-configure network elements such as routers.
- Authentication and authorization
  IMS offers comprehensive authentication and authorization functions. The RADIUS servers are used to implement the authentication and authorization functions.
- Mediation capability
  The IMS platform has the capability to import and read RDRs from any network elementt hat provides suitable log files. IMS incorporates interfaces with various kinds of network elements to provide flexibility. By structures resembling the architecture above, the RDRs stored in different kinds of network elements, such as NetFlow enabled router, switch, email server, RADIUS server, web applications server, etc., can be collected by IMS. The IMS provides distributed data processing.This can spread the processing without losing performance or efficiency.

- Realtime billing
  IMS realtime billing can support the prepaid and debit card services. When users log on to the network and authenticate themselves, IMS will continuously check their account in realtime. If a user runs out of his funds, the service will be terminated. With the distributed rating architecture IMS is capable of handling thousands of transactions per second. This information will be provided to the relevant network access server to control the users' network usage. IMS also provides plug-in modules for customizing price schemes. IMS billing provides the functions such as online credit checking, and debito r credit card payments.
- Service administration
  The service administration is a management part of the IMS. Iti ncludes the functions listed below:
  - Account creation. IMS can easily create new user accounts within minutes.
  - Activity tracking. With its capability to view all traffic information in minute detail required, IMS is able to provide comprehensive audit trail function.
  - Reporting. IMS can run more than 30 standardized reports.T hese reports incorporate individual customer usage and profile analysis, campaign and revenue patterns or technical reports.I MS also provides the capability to customize reports to meet the flexible requirements.

3.1.3. Cisco

Cisco also provides solutions for IP Billing. Its NetFlow-enabled routers and switches can capture network traffic data to generate RDRs, which can be collected by many mediation systems. The NetFlow- enabled routers and switches are commonly used network elements in IP Billing systems. Its NetFlow FlowCollector can be used as mediation system.

3.1.3.1. NetFlow enabled router and switch

NetFlow is a software application, it is part of the router and switch Internetwork Operating System(IOS) and can capture network traffic data. While the NetFlow-enabled router and switch are capturing the flow, information from the first packet of a flow is used to build an entry in the NetFlow cache. Information about subsequent packets in the flow are recorded in the same entry. The information of flows are temporarily stored in the NetFlow cache, which is managed by NetFlow cache management software. The NetFlow cache management software contains a highly sophisticated set of algorithms for efficient determination whether a packet is part of an existing flow or should generate a new flow cache entry, dynamically updating per-flow accounting measurements residing in the NetFlow cache, and judging the flow expiration. Expired flows are grouped together into 'NetFlow Export' UDP datagrams for exportf rom the NetFlow- enabled device. Flow datagrams are exported from NetFlow- enabled devices atl east once per second, or, as soon as a full UDP datagram of expired flow is available. The NetFlow Export capability can be configured to meet different performance requirements.

The NetFlow Export datagram format can be described as seen in Figure 3.2 below:

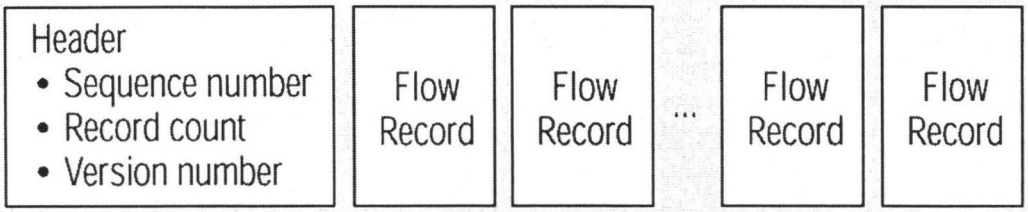


Figure 3.2 NetFlow Export Datagram Format

Nowadays the NetFlow Export Datagram Format version 1, 5, 7, 8 are used for netflow recording.

3.1.3.2. NetFlow FlowCollector

NetFlow FlowCollector is a mediation layer product. It provides scalable data collection from multiple NetFlow capable devices. Figure 3.3 shows how the NetFlow FlowCollector works.

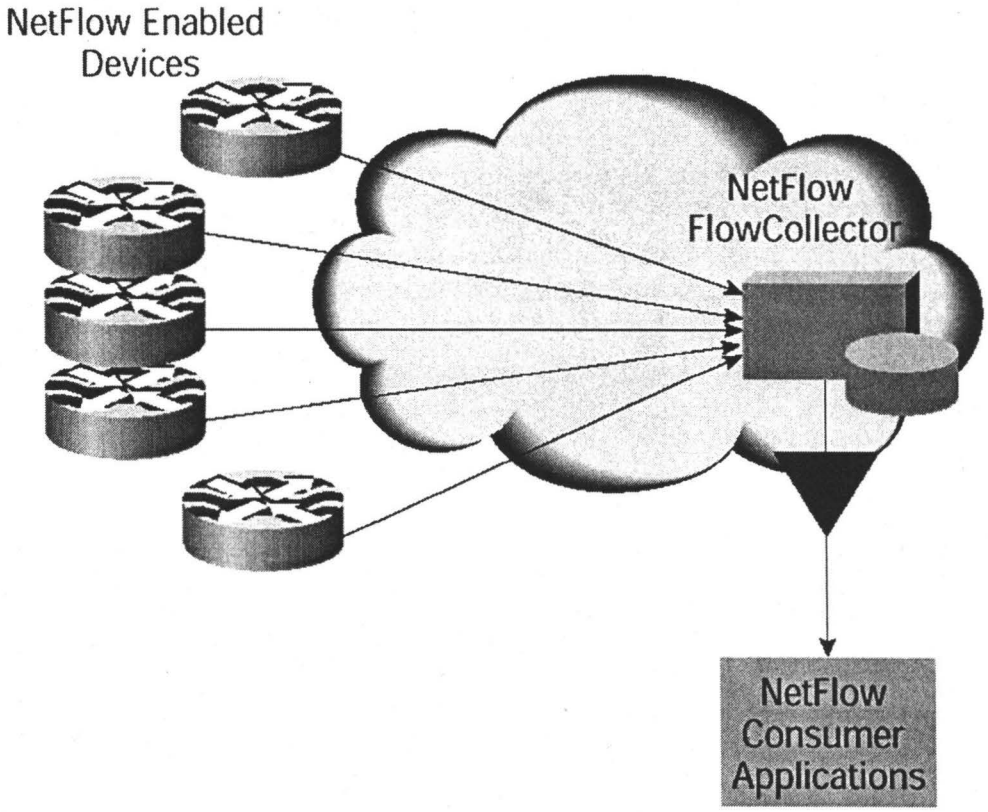


Figure 3-2 NetFlow FlowCollector

The NetFlow FlowCollector provides the following functions :

- Consumption of flow datagrams from multiple NetFlow capable devices.
- Performing of data volume reduction through selective filtering and aggregation. Users can specify the filtering and aggregation rule sets to meet their own requirements.

- Storage of flow information in flat files on disc for post-processing by NetFlow data consumers, including third party billing applications, traffic analysis tools, etc. The NetFlow FlowCollector now is a very important provider of time-based, granular data measurements. It can be used as an integral component of distributed data collection processes. The NetFlow FlowCollector does not provide flow correlation or de-duplication capabilities. These functions must be performed downstream in a post-collection application such as the third-party billing/accounting applications.

3.1.4. Extent

The Extent company mainly provides the OSS solutions for ISPs or ASPs. Its products include Aradial(AAA RADIU server), RBS ISP and Omnispan.

3.1.4.1. Aradial

The Aradial can be used as layer 1 product. The Aradial is a full-featured implementation of the RADIUS protocol for authentication, authorization and accounting (AAA), providing extensive management capabilities for IP Service Providers (ISP). Since Aradial is Web-based, itc an create a single, universal, easy-to-use interface for managing all access management and AAA needs.

3.1.4.2. RBS ISP

Extent RBS ISP is a layer 3 product. It is a full OSS package which combines RADIUS, user management, Web signup, billing, invoicing and other features that can be used by ISP business. The RBS ISP can provide functions such as user management authentication, billing, payment tracking, web interface and other essential elements required to run, sell and manage an ISP business.

RBS ISP can only use RADIUS as dataflow meter. Its architecture is notd istributed, it can support less subscribers than Omnispan. It can only provide flat billing schemes to most of the IP services, and its realtime billing capability is not as good as that by Omnispan.

3.1.4.3. Ominspan

Extent Omnispan is also a layer 3 product. It provides more powerful functions than RBS ISP. Figure 3.4 illustrates how Omnispan helps the service provider to directly serve and provide service to its users.

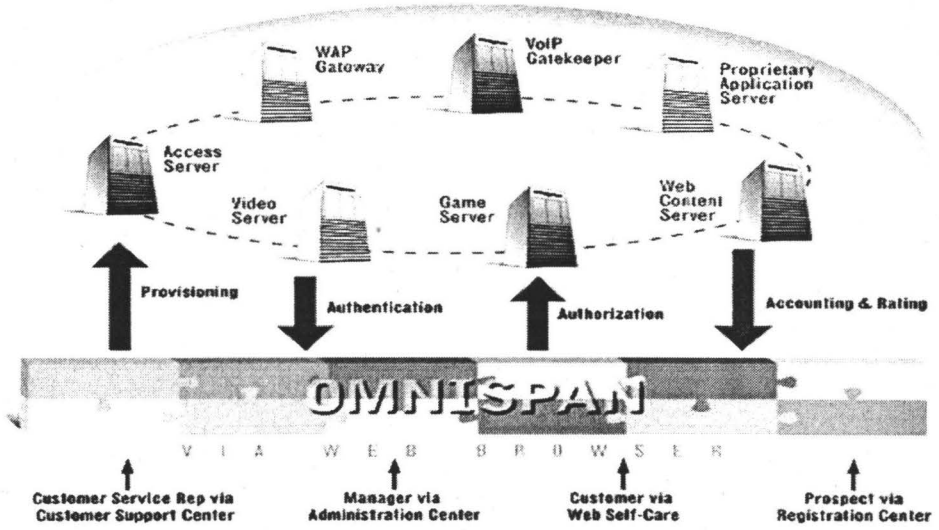


Figure 3-3 Omnispan Architecture

Compared with RBS ISP, Omnispan's distributed architecture can support more subscribers. It is able to provide true realtime billing, which can constantly keep track of user activity and allows to account balance status for instant action and reaction to prevent revenue loss. It also supports usage-billing, and executes flexible price schemes. Its scalability and open architecture can easily be integrated into an existing environment for timely and cost-efficient implementation. Its web-based operation enables easy and fast interaction with users.

3.1.5. Geneva

Geneva provides a layer 3 OSS solution. Ith as been designed to be integrated with other products. Its open modular structure makes rapid implementation possible. Figure 3.5 illustrates the Geneva architecture and how it is integrated with other software components.

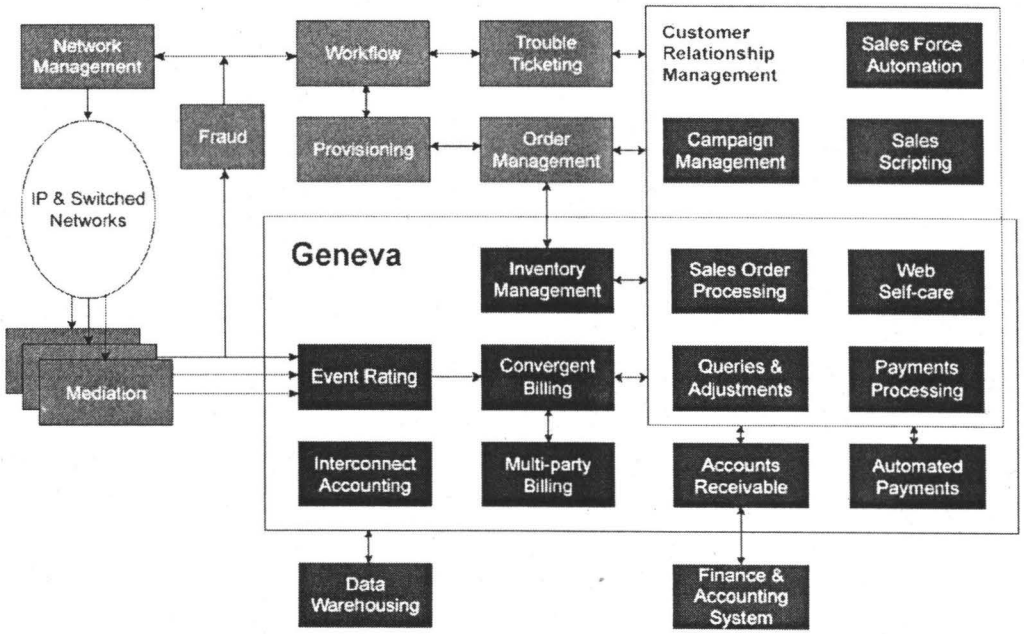


Figure 3-4 Geneva Architecture

Geneva provides following functions:

- Realtime or volume mode billing. In realtime mode, events are priced immediately when they become available from the network.T he relevant account is updated as part of the billing process, so that information about the status of customer accounts is always up-to-date.I n volume mode the billing engine might be run as often as required, at intervals chosen by the operator.
- Support of many business billing models, with flexible allocation of charges and discounts.
- Multinational billing function can support the bill to show information in multi-currency.
- Bills can be formatted and printed directly by Geneva. Geneva users can generate a range of standardized and customized reports.
- Geneva is a centralized system. The Geneva database stores all billing records and provides flexibility for the billing process.
- Customer account maintenance provides all functions needed to create, modify and view data that describes customers, their accounts, the products and packages to which they subscribe, and how they are going to pay.

3.1.6. Intec Telecom Systems

Inter-mediatE is a layer 2 product of the Intec Telecom Systems company. It is a module based collection and mediation platform that collects raw data about network usage and transforms it into rich, billable business information.

Inter-mediatE provides the following functions:

- By using distributed Data Reduction Units (DRUs), close to the network and Remote Gathering Agents(RGAs) running on IP application servers(e.g. Web Hosts, VoD servers, Mail servers, RADIUS, VoIP gatekeepers etc.), Inter-mediatE is able to control and manage the realtime collection of network data. Iti s able to accept multiple record formats.
- Inter-mediatE implements full mediation processing functions:
  - Validation and in-stream record correction
  - Data reduction by filtering and aggregation
  - Transformation or normalization
  - Record creation or usage record cloning
  - Record enrichmentb y using complex reference data
  - Correlation
  - De-duplication
- Support of the distribution of the processed usage records to downstream applications.
- Provision of user level system security and GUI user interfaces.

3.1.7. Lucent (Kenan)

The Interprenet IP Usage Suite is an product of Lucent Technologies. It provides detailed usage information within IP networks to enable usage-based billing, network usage analysis and other user-defined applications. Figure 3.6 illustrates the architecture of InterprenetI P Usage Suite:

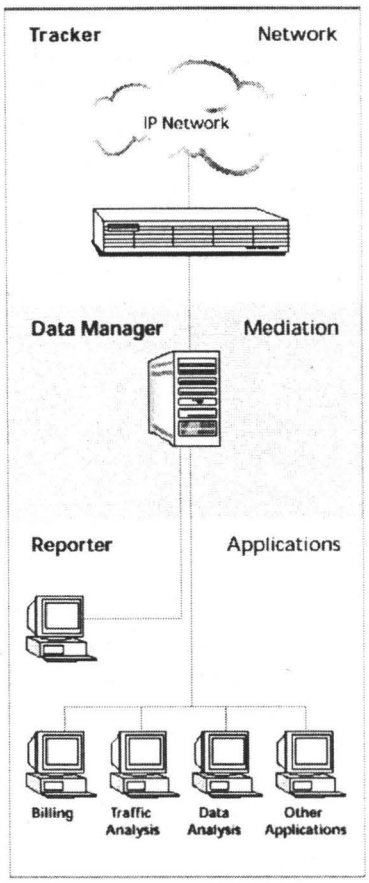


Figure 3-5 Architecture of Interprenet IP Usage Suite

The Interprenet IP Usage Suite consists of two layers. The Interprenet Tracker works as a dataflow meter. The InterprenetD ata Manager implements the mediation functions. The Interprenet Reporter is also part of the mediation layer. The Interprenet IP Usage Suite can be combined with other third party IP Billing and OSS applications.

- Interprenet Tracker is a layer 1 product. It is a network device thatc ollects IP usage events and associates users with usage as it happens. The Tracker processes each packet as it arrives from the network,c ollects usage information and aggregates iti nto a Data Detail Record(DDR).S ome of the functions in the mediation layer are implemented by the Tracker. It can correlate a user with usage in the network in realtime, as soon as the user is authenticated. This allows immediate aggregation of usage records, great reduction of the amount of data sent to the mediation platform and significant cutback of network bandwidth.
- Interprenet Data Manager is the mediation platform within IP Usage Suite. It provides RDRs collection, processing and distribution. The Data Manager supports data collection from multi-service and multi-vendor networks and outputs data to a variety of downstream applications. The Data Manager offers the capability to deliver usage data to multiple applications and in multiple formats.
- The Data Manager provides the following features:
  - Collection of IP network data from Interprenet Trackers, Web Server Logs, Email Server Logs and other data sources.

- Acceptance of usage data from multiple systems and network elements. This allows the Data Manager to provide a single platform to process usage data in a converged (IP, mobile, fixed) network environment.
- User-definable input format that allows the collection of various types of usage data.
- Reformatting of data records before sending them to downstream systems. Different formatm appings can be applied to each application. IPDR, ASCII and Arbor/BP are supported. Support for other downstream systems can also be easily added through a user-definable data layout tool.
- Complete Operations, Administration and Maintenance (OA&M) capabilities through an easy to use GUI.

- Interprenet Reporter is a flexible reporting component of the IP Usage Suite. It is a mediation layer reporter. This Reporter is used to report on usage data that is stored in the Data Manager. It supports reporting on any combination of Data Manager output fields, and supports also pre-load basic IP usage reports. Its web-based reporting can provide the capability to create customizable charts and graphs, and also provides the security and access control to the reporting.

3.1.8. Narus

Narus provides several components for IP Billing solutions. Narus IBI(Internet Business Infrastructure) solutions are based on a highly scalable and distributed open architecture made up of three layers: The Narus IBI platform, the Narus Applications, and the Narus Development Tools that enable third-party applications. Figure 3.7 illustrates Narus architecture :

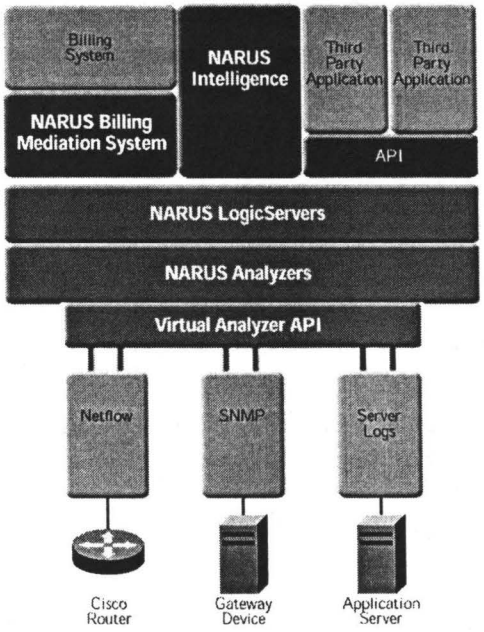


Figure 3-6 Narus IBI Architecture

3.1.8.1. Narus Virtual Analyzers

Narus Virtual Analyzers are lightweight software agents that leverage industry standard protocols, as well as proprietary data formats, to extract information from various network devices and service elements that transmit or terminate traffic. These elements include routers, switches, gateways, firewalls, web servers, proxies,

application servers, session managers, directory services, and more. Narus Virtual Analyzers access these network elements, retrieve session data, and parse various data formats to generate meaningful usage information. Each Virtual Analyzer is designed for a specific type of data source. The Narus IBI platform is packaged with a variety of Virtual Analyzers – some of which include general-purpose, standard-based agents (e.g. SNMP, Radius, DNS, and LDAP), while others are custom and vendor specific (e.g. Cisco NetFlow, Cisco uOne, Lucent Bulkstat, and CacheFlow).

3.1.8.2. Narus Semantic Traffic Analyzers

Narus Semantic Traffic Analyzers are dedicated network appliances that capture and analyze data streams directly from high-speed, carrier-grade IP networks. Connected at key locations in the service provider's network, Semantic Traffic Analyzers perform protocol analysis of captured data streams. These Analyzers use Narus' patented Semantic Traffic Analysis (STA) technology to understand the semantics of a user session across all seven layers of the network stack. This remarkably granular information is collected and processed at line speeds without affecting network performance.

STA technology is an advanced technology in IP dataflow metering. It is a fundamental, new network technology thatc an continuously analyze all user sessions on a heavily trafficked network — remotely and in a noninvasive manner — from a semantic perspective. STA consists of non-intrusive, remote detection, characterization, analysis, and capture of all IP data streams. Not only are all IP data streams detected with STA, but the semantics of the data stream and the quality of service are determined on a session-by-session basis. This includes the protocol (e.g., http, ftp, H.323, and VPN), the application used within the protocol (voice, video, data, real-time data, etc.) and more importantly, the end user's pattern of use within each application or the application context(options selected, service level delivered, duration,t ime of day, data requested, etc.). This process is fundamental to STA, because ite nables the Narus IBI platform to analyze network traffic and extract application-level contenta nd context information. Semantic Traffic Analysis technology is capable of remotely monitoring, analyzing, and capturing the semantics of high-speed data streams with no remarkable degradation in network performance.

3.1.8.3. Narus LogicServer

Narus LogicServers provide an intelligentd ata aggregation and correlation before passing usage information to the Narus applications (or other third-party applications). A LogicServer applies user-defined business rules to transform Analyzer data into aggregated usage records that have meaning in terms of a service provider's offering. With the flexible architecture of the LogicServer, the same stream of events from a set of Analyzers can be processed in different ways to meet the needs of different applications, such as fraud detection, policy monitoring, and archiving. The LogicServer is a high performance software engine — capable of processing and aggregating thousands of network events per second per CPU.

3.1.8.4. Narus Billing Mediation System

The Narus Billing Mediation System(BMS) is an IP Billing mediation system that provides the critical connection to link customer activity on the network to the third party's billing system. The Narus BMS was designed from the bottom up to meet the

current and future requirements of IP Billing systems. It supports a comprehensive field of applications, such as messaging, web browsing, IP telephony, streaming media, hosting, and others. Narus BMS delivers aggregated usage information in typical formats to leading IP Billing applications. It is also designed to support the emerging Internet Protocol Detail Records (IPDR) standard.

3.1.8.5. Narus Application Programming Interface

The Narus Application Programming Interface (API) is an open, well-defined programmatic interface to the Narus IBI platformplatform. The interface is designed to facilitate the rapid development of applications, while maximizing the value of the underlying Narus IBI platformplatform. The application interfaces of the Narus API consist of four primary categories:

- Input and Configuration Interface: the Inputa nd Configuration Interface provides applications with the capability to configure the Narus IBI platform to collect desired session and transaction information for IP services and protocols. Input interfaces also provide applications with the capability to set and query aggregation rules.
- Output Interface: the Output Interface is a robust messaging interface that enables applications to reliably send and receive messages to and from the Narus IBI platformplatform.
- Administration and Control Interface: through this interface, applications such as network administration tools can administer and manage Narus IBI platforms. Administration tools can query, add, or delete applications and services running on the Narus IBI platform, as well as monitor and start,s top, or restart separate components (Analyzer, LogicServer) of the platform.
- Virtual Analyzer Interface: the Narus IBI platform, via the Narus API, provides a mechanism for external sources of information to provide data to the platform for aggregation, analysis, and correlation. These external sources of data appear to the Narus IBI platform as virtual instances of Narus Analyzers, and may include SNMP devices (e.g., gateways), flow devices (RMON-II, NetFlow),o r server logs. The Virtual Analyzer support in the Narus IBI platform enables rapid development and deployment of custom data encapsulation, as well as access to pictorial views for a Narus IBI platform and the Virtual Analyzer.

3.1.8.6. Narus Intelligence

Narus Intelligence (NI) is a decision support application designed to transform detailed customer usage information gathered by the Narus IBI platform into valuable marketing knowledge and operational information. Narus Intelligence is specifically designed to enable service providers to develop an Internet Business Infrastructure that supports the making of business decisions in the areas of customer segmentation, policy monitoring, fraud detection, and churn management.

3.1.9. NetEye

The Hawk Eye NextGen Mediation solution is a product of NetEye corporation. It provides a solution for collection of usage and performance data from various network elements, processing the information and distributing it to downstream systems. Itc an be used as a mediation system for usage-based & content-based billing. Hawk Eye NextGen Mediation provides the following functions:

- Collection of usage and performance data from various network elements such as edge & backbone routers & switches, RADIUS servers, DNS & DHCP servers, firewalls, application servers, voice switches etc.
- Processing of RDRs. It is able to perform intelligent processing of the RDRs.Correlation, aggregation, enhancement, filtering, reformatting mechanisms can be used to process the RDRs. These processing mechanisms can be configured by modification of the rule sets.
- Provision of extensive long-term storage for buffering, backup and history analysis. It supports multiple incoming formats, and provides interfaces with downstream applications.
- Provision of a friendly & flexible GUI environment helping to manage all mediation operations.

3.1.10. OpenCon

The Billing Mediation Platform(BMP) is a mediation product by OpenCon Systems. BMP is a multiple-protocol, multiple-source, and data collection and distribution management solution, enabling service providers to transform raw input data collected from multiple sources and environments to multiple output applications. Figure 3.8 illustrates the architecture of OpenCon Systems BMP.

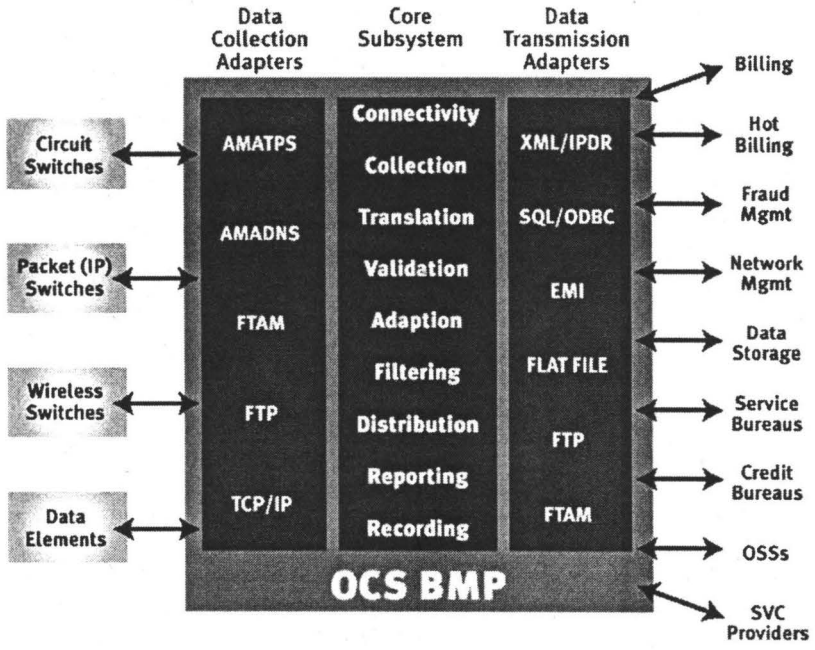


Figure 3-7 Architecture of OpenCon Systems BMP

The OCS BMP consists of three modular components:

- Data Collection Adapters are designed to work with various data sources, including switches, data elements, and tape backup systems. These DCAs support a wide range of formats and standards, including Automatic Messaging Accounting TeleProcessing System (AMATPS), Automatic Messaging Accounting Data Networking System (AMADNS), File Transfer, Access, and Management (FTAM), even XML and IDL encoding.

- The Core Subsystem is optimized to handle the billing mediation requirements common to all or most applications, including mapping and translation rules, data dictionaries, validation services, and OA&M services.
- Data Transmission Adapters are designed to create data for user specific applications and service bureaus, no matter how they receive data: FTP, or X.25. Multiple data sources, can be delivered in a single integrated data stream, this makes it easier for back-end applications to process the data.

3.1.11. Openet

i.Fusion by Openet Telecom has been developed as an intermediary mediation service between internet network elements and individual OSS business applications, such as billing, fraud detection or customer care. Figure 3.9 illustrates the architecture of i.Fusion.

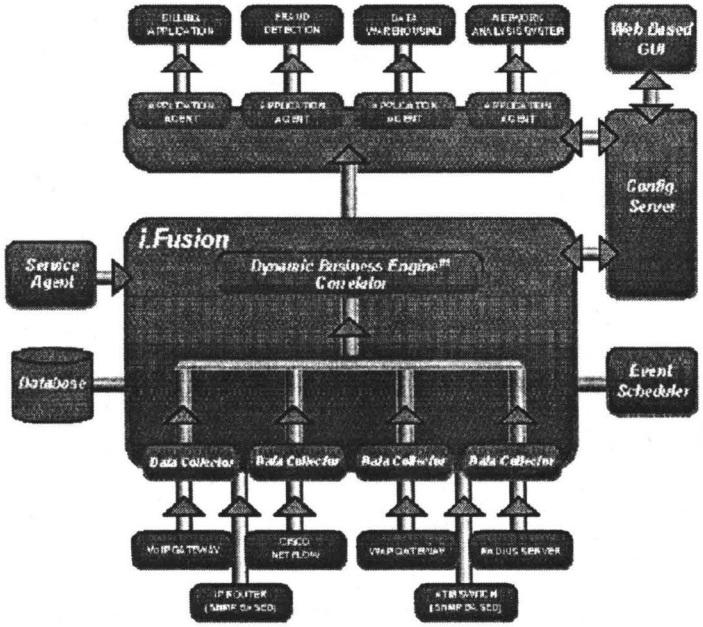


Figure 3-8 i.Fusion Architecture

i.Fusion consists of three key components: Data Collector, Correlator and Dynamic Business Engine(DBE).

3.1.11.1. Data Collector

The Data Collector module is responsible for collecting network information from a particular network element and accumulating appropriate IP session information, producing a new logical IPDR with the relevant data elements included. As the information generated by each network element is different, separate rule sets are defined for filtering the appropriate information. These rule sets are fully configurable through a browser based on Java GUI. The Data Collector is able to collect RDRs from different kinds of network elements.

3.1.11.2. Correlator

The Correlator has the capability to reconstruct each event record from a set of records collected by Data Collectors according to predefined or customized rule sets.

The rule sets can be customized to suit an individual customer's requirements. New business logic can easily be added by simply changing the rule sets of the Correlator.

3.1.11.3. Dynamic Business Engine(DBE)

The Dynamic Business Engine is an intelligent, multi-threaded rule-based inference engine, which interprets business rule sets supporting a customer's specific network or business infrastructure. These rule sets are fully customizable through a browser based Java GUI configurator. The Dynamic Business Engine interprets rule sets for both the Data Collector and Correlator modules, providing complete flexibility with regards to the type of data collected and its interpretation.

3.1.12. Portal

Portal's Infranet provides usage based billing functions. The realtime billing capability is its important character. It can offer multiple billing and customer management functions such as registration, authorization, event tracking, fraud prevention, rating, discounting, balance updated, promotions, financial tracking, etc in realtime. CISCO System and Portal Software have joined the IP Billing area. Infranet can be integrated with Cisco NetFlow this is illustrated in Figure 3.10.

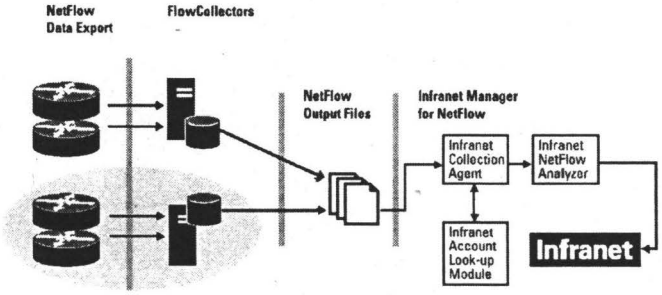


Figure 3-9 NetFlow and Infranet Integration

The Infranet Manager for Cisco NetFlow consists of three modules: Collection Agent, Account Look-Up Module and NetFlow Analyzer.

3.1.13. Primal

Pimal's IP Billing system consists of three main components. Access IM, Outfront CRM and Connect CCB. Figure 3.11 illustrates its architecture.

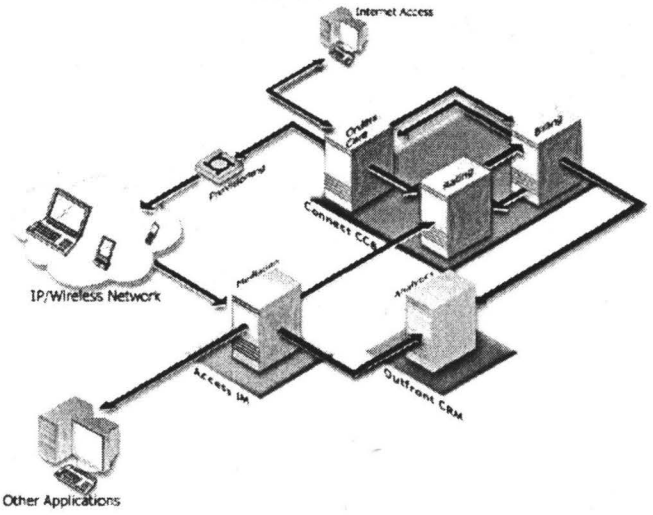


Figure 3-10 Architecture of Primal

3.1.13.1. Access IM

Primal's Access Intelligent Mediation (IM) is a network mediation solution. Access IM collects, formats, and stores Data IP or Radius traffic from any communications network source.T he information can then be routed with guaranteed delivery to multiple applications such as billing systems, fraud detection applications or data marts. Access IM can be deployed in a centralized or distributed configuration. The Access IM application is composed of four primary components:

- Collector Interface
- Message Formatter
- Data Router
- Outfront CRM Usage Analysis application

3.1.13.2. Outfront CRM

Primal's Customer & Business Analytics (Outfront CRM) helps to identify customers this allows to provide customer specific services

3.1.13.3. Connect CCB

Primal's Customer Management & Billing software, Connect CCB, offers convergent billing in a scalable format.I t integrates billing, rating, invoicing, EBP&P, inventory, A/R, customer service, and customer relationship management for multiple IP services including voice, data content etc. Connect CCB claims to be and flexibility. Primal's Connect CCB is easily customized to fit user specific needs. When it's time to enhance, update or change rate plans, discounts or feature sets, Primal's table-driven, rule-based administration lets users quickly and easily make the changes they need. ConnectC CB SDK (*software development kit*) provides all the APIs and tools which help to combine with user's business infrastructure.

3.1.14. XACCT

XACCT Technologies' IP BillingNetwork to Business(N2B) platform provides a bi-directional, realtime link between the physical network infrastructure and Operations and Business SupportS ystems (OSS/BSSs). The core of the XACCT N2B Platform is the XACCT*usage* software, a distributed, centrally managed architecture that ensures

data integrity and system availability. XACCT*usage* provides detailed network information needed for billing, churn, fraud, service level verification, customer relationship management and other OSS/BSS applications. Figure 3.12 illustrates XACCT's architecture.

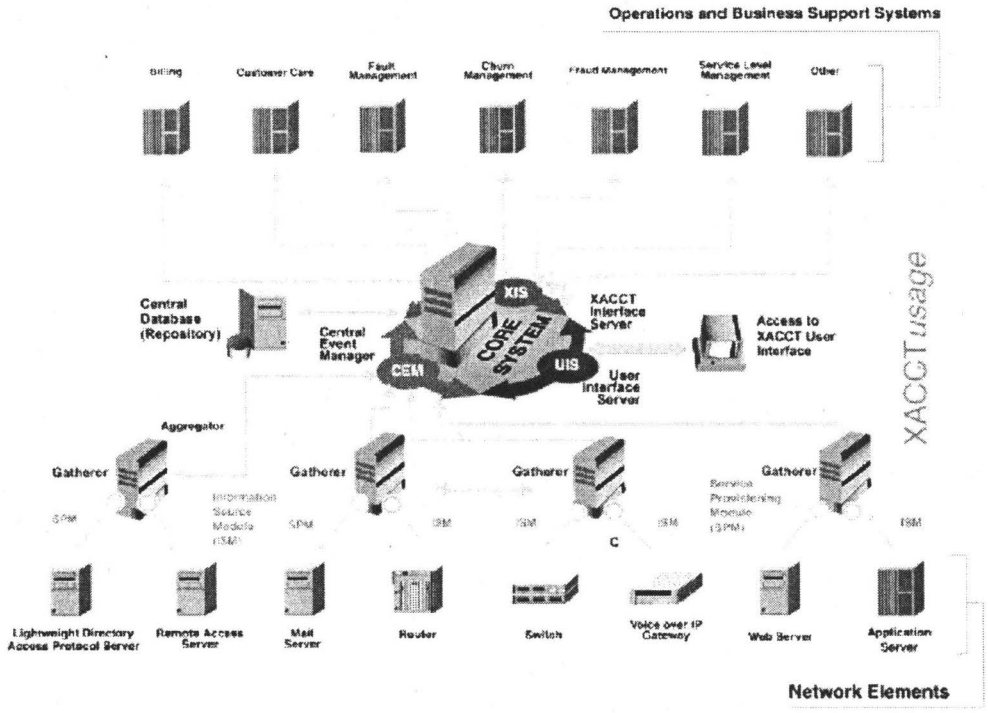


Figure 3-11 XACCT Architecture

The architecture of the XACCT N2B Platform is composed of several functional layers, which together give the product its scalability, flexibility, availability and manageability:

- information source modules (ISMs)
- gatherers
- central event manager (CEM)
- Central Database (CDB)
- user interface server (UIS)
- XACCT interface server (XIS)

3.1.14.1. Information Source Modules

There are four types of information source modules: DCM, DEM, DPM, and SPM: Data Collection Modules (DCMs) DCMs are modules used to extract and collect information from various network and service elements, including transport devices and application servers. DCMs are designed to abstract all complexities involved in data collection. They can be single purpose, vendor-specific modules (e.g. Cisco NetFlow, Netscape Messaging Server 4.x) or general purpose, standard-based modules (e.g. SNMP MIB-II, RMON-II). Every time a DCM is added to a Gatherer, it brings with it a set of input fields which can be selected by the user by simply configuring it, to create their desired XDR. XDR(eXtensible Detail Record) is the output record format of XACCT.

- DEMs (Data Enhancement Modules) are modules used to enrich IP session data acquired from primary sources using data available in other sources. This would

include, for instance, dynamic IP associations derived from remote access servers, DHCP servers and DNS servers as well as LDAP servers and databases. Data provided by a DCM can be enhanced by using the data collected by a DEM. This capability allows data fields to be enhanced with user information and, thus, creates a meaningful XDR.

- DPMs (Data Processing Modules) are modules that process data they receive from other DCMs after enhancements through DEMs. The processing could include flexible, policy-based data filtering and aggregation. Through the DPM, data volumes can be further reduced, improving the scalability and efficiency of the system by reducing volume of data sent across the network.
- SPMs (Service Provisioning Modules) are distributed modules designed to provide IP services by interfacing directly with various network or service elements in order to add, remove, update, enable, or disable user accounts. In much the same way thatD CMs abstract the complexities associated with collecting data from different network elements, SPMs abstract the complexities associated with provisioning users.
- Gatherers are multi-threaded, lightweight, smart agents that run on dedicated or non-dedicated hosts,a s a service or daemon on Windows NT or Solaris, respectively. They can host multiple ISMs and perform flexible, policy-based data filtering and aggregation. Gatherers are typically installed in network proximity to the element from which they collect in order to minimize data traffic impact on the network.

3.1.14.2. Central Event Manager (CEM)

The CEM is the central component of XACCT*usage*. It provides centralized, efficient management and control of all XACCT components. The CEM manages configuration, data collection, licensing, upgrades and security. If a communications link goes down, the Gatherer stores all the UNIRs in persistent queues. Once the link is re-established, the persistent queues are flushed to the data's final destination. A proprietary protocol efficiently controls this data delivery to ensure that no data is lost between the XACCT*usage* components, thus ensuring a highly reliable delivery mechanism.

3.1.14.3. Central Database (CDB)

The XACCT*usage* systems uses a commercial database (Oracle or Microsoft SQL Server) to store the configuration of the system, and optionally, the usage data. Operators can easily modify the data structures and set data retention policies to suit their specific needs. On demand access is enabled through database queries and reports or the scheduler can be programmed for automatic report generation. It can also be used in conjunction with any off-the-shelf ODBC-compliant reporting package to generate customized graphs and charts.

3.1.14.4. User Interface Server (UIS)

The UIS provides a single, secure point of contact for administration and system management. The UIS can be managed through industry leading, Java-enabled web-browsers, including HP Openview. This allows secure access to the system, locally or remotely. The UIS allows easy and efficient system reconfigurations and field upgrades, and includes a customized reporting system with built-in report generation. An open database connectivity or ODBC compliant interface is also available to enable use of third party reporting packages.

3.1.14.5. XACCT Interface Server (XIS)

The XIS extends the functionality of XACCT*usage*, acting as a gateway to the system and enabling direct integration with external systems, such as OSS/BSS and decision support systems. The XIS enables two important functions of the XACCT*usage* system: It is a parallel, multi-channel data delivery system and it creates a programmatic interface for developing client applications that utilize the provisioning functions of the system. The XIS software development kit (SDK) includes sample clients as well as extensive documentation to enable XACCT's customers and partners to develop custom clients to suit their individual needs.

3.2. Considerations about choosing IP Billing products

From the technical point of view some ideas about the consideration concerning the choosing of IP Billing products are given in the textb elow. If we choose an IP Billing product, we have to consider functionality and performance of the product. The factors that should be considered include:

- The interface between collector and network elements. If the collector can support collecting RDRs from different types of network elements,t his scalability can help to add a new type of network elementw ithout affecting the existing system.
- Whether the collectors are distributed or centralized.
- Which kinds of input formats can be supported by the collectors, and which kinds of transport protocols can be supported by the collectors.
- The realtime capability of the collectors, or intervals of the collecting or transfer of RDRs.
- What kinds of processing modules can be used in the processing of the RDRs.
- Whether the processing modules' activities can be controlled by rule sets or not. Rule sets can help to provide the flexibility and scalability of processing the RDRs.
- Which kinds of formats can be supported in generating the output usage records.
- Storage of the usage records, including storage size, supported inquiry mechanism, backup and recovery mechanism, expired usage records handling policy, distributed or centralized storage, etc.
- What kinds of transportp rotocols can be supported in transferring the usage records to the Billing systems or OSS layer applications.
- The management of the mediation system. Through the management of the mediation system, system operators can control and monitor the running of the mediation system. The management system should provide an easyto use operation interface to the system operators.
- Rule sets configuration. Rule sets used to control the activities of the mediation system can provide flexibility and scalability. The rule sets configuration interface should be provided to the operators to customize their own system.
- Whether the provision capability is supported or not. The provision capability can control the network users' accessing of the network. This function is useful, if some users run out of money or exceed some limitations according to the judgment rules of the billing system or OSS applications.
- The supported inputf ormat of the billing system, and the supported transport protocols of the billing system.
- Realtime capability of the billing system. Realtime billing means the billing information can reflect the users' activities in realtime, as a result the reactions to the users' activities can be implemented in a short time.

- User management capability.
- Supported billing activities. For example, registration, authorization, discounting, balance updating, fraud detection, etc.
- Whether usage based billing is supported or not.
- Billing system management capability.
- dynamic configuration capability of the billing system.
- Whether a user friendly interface and flexible report can be provided.
- Maximal amount of users that can be supported by the system.

4. Appendix

4.1. References

[AbLi00] B. Aboba, D. Lidyard: "The Accounting Data Interchange Format(ADIF)", draft-ietf-roamops-actng-07.txt, April 2000

[ACPZ00] J. Arkko, P. R. Calhoun, P. Patel, G. Zorn: "DIAMETER Accounting Extension", draft-calhoun-diameter-07.txt, July 2000

[Apogee] Apogee Networks Documentation
www.apogeenetworks.com

[Baue00] Volker Bauer : 'Analyse von Netwerk-Abrechnungs-Systemen bezüglich nutzerorientierter Datanerfassung'; Diplomarbeit, Univerität Kaiserslautern, September 2000

[BelleSys] Belle Systems Documentation
www.bellesystems.com

[Cisco] Cisco Documentation
www.cisco.com

[CRAG00] P. R. Calhoun, A. C. Rubens, H. Akhtar,E . Guttman:" DIAMETER Base Protocol", draft-calhoun-diameter-16.txt, July 2000

[Extent] Extent Technologies Documentation
www.extent.com

[FSPl97] G. Fankhauser, B. Stiller, B. Plattner: "Arrow:A Flexible Architecture for an Accounting and Charging Infrastructure in the NextG eneration Internet", TIK, ETH Zürich, October 1997

[GenevaTech] Geneva Technology Documentation
www.genevatechnology.com

[IntecTelSys] Intec Telecom Systems Documentation
www.intec-telecom-systems.com

[IPDR00] ipdr.org: "Network Data Management – Usage(NDM-U) for IP-Based Services", version 2.0, October 2000

[Karv00] A. Karve: "Cisco Systems' Billing Strategy", Billing World, Febuary 2000

[Lucent] Lucent Documentation
www.lucent.com

[LuCo99] M. Lucas, O. Cohen:" Usage Collection and Analysis in an IP OSS", Billing World, March 1999

[LuLu98] M. Lucas, D. Lubuda: "Batch Systems for Internet Billing", Billing World, January 1999

[LuSc98] M. Lucas, L. Schweitzer: "Mediation in a Multi-Service IP Network", Billing World, October 1998

[Narus] Narus Documentation
www.narus.com

[Neteye] NetEye Documentation
www.neteyecorp.com

[OpenconSys] Opencon Systems Documentation
www.opencon.com

[OpenetTel] Openet Telecom Documentation
www.openet-telecom.com

[Portal] Portal Documentation
www.portal.com
[Primal] Primal Documentation
www.primal.com
[RFC1272] C. Mill, D. Hirsh, G. Ruth: "Internet Accounting: Background", RFC1272, November 1991
[RFC2063] N. Brownlee, C. Mills, G. Ruth: "Traffic Flow Measurement: Architecture ", RFC 2063, January 1997
[RFC2138] C. Rigney, S. Willens, A. Rubens, W. Simpson: "Remote Authentication Dial In User Service(RADIUS)", RFC2138, June 2000
[RFC2139] C. Rigney: "RADIUS Accounting", RFC 2139, Apil 1997
[RFC2251] M. Wahl, T. Howes, S. Kille: "Lightweight Directory Access Protocol(v3)", RFC2251, December 1997
[RFC2460] S. Deering, R. Hinden: "Internet Protocol, Version 6(Ipv6) Specification", RFC2460, December,1998
[RFC2819] S. Waldbusser: "Remote Network Monitoring Management Information Base", RFC2819, may 2000
[RFC2924] N. Brownlee, A. Blount: "Accounting Attributes and Record Formats", RFC 2924, September 2000
[RFC2975] B. Aboda, J. Arkko, D. Harrington: "Introduction to Accounting Management", RFC2975, October 2000
[Schw99] S. Schwartz : "Mediation Systems: Pressure's On for Usage-Based IP", Billing World, September 1999
[SFPW98] B. Stiller, G. Fankhauser, B. Plattner, N. Weiler:" Pre-study on Customer Care, Accounting, Charging, Billing, and Pricing", TIK, ETH Zürich, Febraury 1998
[Stev97] W. R. Stevens: "TCP/IP Illustrated, Volume I – The Protocols", Addison Wesley, 1997
[Xacct] XACCT Documentation
www.xacct.com