Network Working Group
INTERNET-DRAFT
Category: Standards Track
<draft-arkko-acctreqlis-00.txt>
6 August 1998

Jari Arkko
Ericsson

Requirements for Internet-Scale Accounting Management

1. Status of this Memo

The document is an Internet-Draft and is in full conformance with all of the provisions of Section 10 of RFC 2026.

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html.

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the Internet-Drafts Shadow Directories on ftp.ietf.org (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

The distribution of this memo is unlimited. It is filed as <draft-arkko-acctreq-00.txt>, and expires February 1, 1999. Please send comments to the authors.

2. Abstract

Over the years, as Internet services have evolved, sophisticated inter-domain applications such as roaming, voice over IP, Internet fax, and QoS provisioning have arisen. This document discusses whether accounting for these services services can be reliably and securely accomplished using established techniques, and explores the requirements for Internet-scale Accounting Management.

3. Table of Contents

1. Status of this Memo
2. Abstract
3. Table of Contents
4. Introduction
   4.1 Terminology
   4.2 Requirements language
5. Flexibility properties of accounting systems
6. Requirements
   6.1. Flexibility
   6.2. Scalability
   6.3. Security
   6.4. Accounting record transfer
   6.5. Accounting record information
7. Analysis of current protocols
8. Conclusions
9. Acknowledgements
10. References
11. Authors' Addresses

4. Introduction

Over the years, as Internet services have evolved, sophisticated inter-domain applications such as roaming, voice over IP, Internet fax, and QoS provisioning have arisen. This document discusses whether accounting for these services services can be reliably and securely accomplished using established techniques, and explores the requirements for Internet-scale Accounting Management.

4.1. Terminology

This document frequently uses the following terms:

Accounting
: The act of collecting information on resource usage for the purpose of trend analysis, auditing, billing, or cost allocation.

Rating
: The act of determining the price to be charged for use of a resource.

Billing
: The act of preparing an invoice.

Auditing
: The act of verifying the correctness of a procedure.

Cost Allocation
: The act of allocating costs between entities. Note that cost allocation and rating are fundamentally different processes.

Interim accounting
: An interim accounting packet provides a snapshot of usage during a user's session. It is typically implemented in order to provide for partial accounting of a user's session in the event of a device reboot or other network problem that prevents the reception of a session summary packet or session record.

Session record
: A session record represents a summary of the resource consumption of a user over the entire session. Accounting gateways creating the session record may do so by processing interim accounting events.

Accounting Protocol
: A protocol used to convey data for accounting purposes.

Intra-domain accounting
: Intra-domain accounting involves the collection of informa-

tion on resource within an administrative domain, for use within that domain. In intra-domain accounting, accounting packets and session records typically do not cross administrative boundaries.

Inter-domain accounting
: Inter-domain accounting involves the collection of information on resource usage of an entity with an administrative domain, for use within another administrative domain. In inter-domain accounting, accounting packets and session records will typically cross administrative boundaries.

Real-time accounting
: Real-time accounting involves the processing of information on resource usage within a defined time window. Time constraints are typically imposed in order to limit financial risk.

4.2. Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [24].

5. Flexibility properties of accounting systems

This document is concerned with understanding how a general mechanism can be used for the accounting management of a number of different applications. It is therefore appropriate that we examine the potentially differing requirements:

Information
: While there are some generally applicable information elements in accounting (such as service name and time information), different services typically have widely different needs to convey information. It must be possible to extend the basic accounting mechanisms to new application areas in a well-defined manner.

Security
: An intra-domain trend analysis application has very low or non-existent security requirements; hop-by-hop integrity support is almost certainly sufficient. In contrast, an inter-domain billing application has very high security requirements including data-object integrity through proxies, confidentiality, and so on.

Data amount
: Many applications produce relatively small amounts of data from each event, such as the few dozen variables needed to describe a dial-in session with a NAS. In contrast, some other applications may require the

inclusion of lengthy public key material and signatures, or detailed descriptions of the provided service.

Delay Many applications don't require immediate delivery of accounting information, and are unwilling to pay the price of such fast service. Other applications do require immediate delivery. Yet other applications insist also on fast acknowledgement of the delivery in order to minimize the time the user has to wait before service can be provided.

Applications differ also much depending on the amount of resources they can dedicate for the accounting tasks:

CPU resources An application such as the accounting of dial-in sessions of a NAS produces relatively infrequent accounting events. Other applications, such as accounting the browsing of a web page produce substantially higher amounts of events.

Storage resources
Many existing systems have no non-volatile memory or use memory types that don't allow constant modifications. In contrast, future systems are likely to employ large and cheap non-volatile memories.

Code size and complexity
For a workstation size computer the support of a number of encryption algorithms, IPSec, MIME encoding, SMTP, TCP, and so on is relatively easy. For a smaller device such as an embedded processor in a fax or copy machine, phone, set top box, and so on there are much tighter requirements on how much protocol support can be included.

If possible, these differing requirements and constraints should still be supported within one accounting management mechanism.

6. Requirements

6.1. Flexibility

The following flexibility requirements suggest themselves:

Extensibility	The protocol MUST be extensible to new services. It MUST be possible to define service-specific extensions to the accounting protocol. There MUST be a possibility to define new standard and vendor-specific attributes.

There MUST be a possibility to define new messages. There MUST be a possibility to detect version differences between protocol peers, and to revert to least common denominator behaviour.

Security
It MUST be possible to use the accounting protocol both in situations which need and tolerate only hop-by-hop integrity protection, as well as in situations which need full integrity and confidentiality protection for data objects and hop-by-hop.

Data amount
It MUST be possible to use the accounting protocol both in situations in which the amount of transferred information fits the MTU and in which it doesn't.

Delay
It MUST be possible to use the accounting protocol both when real-time transfer of information is needed and when it is not tolerated.

Fast UDP Delivery
It MUST be possible to use the accounting protocol both with TCP and UDP. UDP is needed when real-time requirements dictate that retransmission policies are specified in a different manner than what TCP allows. For instance, when a critical service requests to send an accounting record and expects an acknowledgement, it may be necessary to switch to an alternate server if the primary server does not respond to a retransmitted packet within a second.

Storage
It MUST be possible to use the accounting protocol both in devices which have a large non-volatile memory and which don't.

Code size
It MUST be possible to have conforming accounting protocol implementations from a stripped down version which includes nothing more than basic protocol, UDP, IP, and MD5 to a version which includes all security and transport protocol support.

Proxy support
It MUST be possible to forward accounting protocol messages through proxies with all supported transfer mod-

els.

6.2. Scalability

The following scalability requirements are set:

Per-device state
: It MUST be possible to implement the accounting systems with a per-device state when real-time requirements don't call for event-driven information transfer.

Amortize overhead
: It MUST be possible to amortize the packet header and security overhead over several accounting records when real-time requirements don't call for event-driven information transfer.

6.3. Security

The following security related requirements are set:

Data object integrity
: Data object integrity MUST be supported even through proxies.

Data object confidentiality
: Data object confidentiality MUST be supported even through proxies.

Hop-by-hop integrity
: Hop-by-hop integrity MUST be supported.

Hop-by-hop confidentiality
: Hop-by-hop confidentiality MUST be supported.

IPSec/TLS
: Standard Internet security mechanisms such as IPSec or TLS MUST be supportd for hop-by-hop security protection.

Data-based access control
: Access control MUST be based also on the data in the accounting records (such as for whose customers the data is).

6.4. Accounting record transfer

The following requirements are set on how the accounting protocol allows records to be transferred.

Polling
: It MUST be possible to use the polling model.

Event-driven
: It MUST be possible to use the event-driven model.

Event-driven polling
: It MUST be possible to use the event-driven polling model.

Interim-accounting
: It MUST be possible to use the interim accounting model.

Transfer negotiation
: It MUST be possible for the service device and the accounting server to negotiate the desired transfer model and interim accounting parameters.

6.5. Accounting record information

The following requirements are related to the information in the accounting records transferred by the protocol:

Finite sessions
: The accounting protocol MUST support the accounting of service usage in which a session begins at a certain time and ends at a later time.

Infinite sessions
: The accounting protocol MUST support sessions of indefinite length. [Discussion: This requirement is set by services which are turned on at one time such as when you order for some web space from a server, continue for possibly a very long time, and might but need not be terminated later.]

Indivisible events

The accounting protocol MUST support the accounting of service usage which consists of an indivisible event. [Discussion: In theory, this could be simulated with a start followed immediately by stop, perhaps even in the

same packet. However, this is clumsy for a number of services such as ordering a pizza.]

Service naming The protocol MUST have a standard attribute which identifies the name of the provided service. [Discussion: Should there be something to manage these names, e.g. object identifiers?]

Service amount specification
The protocol MUST have a standard attribute which gives the "amount" of service provided. Amount is interpreted in an service-specific manner, but it could be the amount of calls made, amount of pizzas delivered, and so on. The interpretation of the amount attribute is defined in service-specific extensions to the accounting protocol. It MUST be possible to represent also real numbers and not just integers.

Service length specification
The protocol MUST have a standard attribute which gives the "length" of the service provided. Length is interpreted in the same way for all services, and MUST have at least a one second granularity.

Service parameter specification
The protocol MUST have a standard attribute which gives parameter information about the provided service. The interpretation of this parameter is service-specific, and defined in service-specific extensions to the accounting protocol. [Discussion: Introduction of this attribute may remove many of unnecessary RFCs about video movie name attributes, pizza name attributes, and so on.]

Note that the amount of money used for the service is NOT required to be within the standard attributes.

7. Analysis of current protocols

In the following table we analyze how RADIUS Accounting as defined in [4], TACACS+ as defined in [32], SNMP v3 as defined in [12]-[16], SMTP and EDI functionality described in [17]-[23], and DIAMETER as defined in [33] - [35] compare. We have used the following notation in the table:

NO The protocol does not and can not support the feature.

YES The protocol supports the feature.

CAN The basic protocol could support the feature, given a simple appropriate extension such as a new attribute is defined.

FEATURE	RADIUS	TACACS+	SNMPv3	SMTP	DIAMETER
Flexibility					
Extensibility	NO	NO(?)	YES	YES	YES
Security	NO	NO	NO	YES	YES
Data amount	NO	YES	NO	YES	YES
Delay	NO	NO	YES	YES	YES
Fast UDP delivery	YES	YES	YES	NO	YES
Storage	YES	YES	YES	NO	YES
Code size	NO	NO	YES	NO	YES
Proxy support	YES	YES	YES	YES	YES
Scalability					
Per-device state	NO	NO	NO(?)	YES	CAN
Amortize overhead	NO	NO	NO(?)	YES	CAN
Security					
Data object integrity	NO	NO	NO	YES	YES
Data object confidentiality	NO	NO	NO	YES	YES
Hop-by-hop integrity	YES	YES	YES	YES	YES
Hop-by-hop confidentiality	NO	YES	YES		

YES	YES	IPSec/TLS	CAN	CAN	CAN
YES	YES	Data-based access control	YES	YES	NO
YES	YES	**Accounting record transfer**			
		Polling	NO	NO	YES
YES	CAN	Event-driven	YES	YES	YES
YES	YES	Event-driven polling	NO	NO	YES
YES	CAN	Interim accounting	YES	YES	CAN
YES	CAN	Transfer negotiation	YES	NO(?)	NO
CAN	CAN	**Accounting record information**			
		Finite sessions	YES	YES	CAN
CAN	YES	Infinite sessions	CAN	CAN	CAN
CAN	CAN	Indivisible events	CAN	CAN	CAN
CAN	CAN	Service naming	CAN	CAN	CAN
CAN	CAN	Service amount specificatio	CAN	CAN	CAN
CAN	CAN	Service length specificatio	CAN	CAN	CAN
CAN	CAN	Service parametrization	CAN	CAN	CAN

8. Conclusions

As noted above, RADIUS, TACACS+, and DIAMETER accounting are suitable for use in low-delay applications, SMTP is well suited for applications requiring high security and efficient transfer, and implementing non-volatile storage, and SNMP v3 is suitable for use in intra-domain

accounting applications without need for data object security. However, since no single protocol satisfies all the requirements, we believe that the need for a special-purpose accounting protocol arises in the situations that involve more than one of the following requirements:

- Accounting applications which require low processing delay in order to detect security or appropriate use violations in progress, manage credit risk or prevent fraud. In such applications, it is often required that accounting-data be handled in an event-driven manner, and sent in small batches.

- Accounting applications which must incorporate information from many devices or transfer very large volumes of data. In such applications, efficiency is very important.

- Light-weight accounting applications running on small devices.

While RADIUS and TACACS+ are in principle capable of handling the above two requirements, the lack of data object security, extensibility, and support for large record sizes makes it hard use these protocols.

The following decisions now await resolving:

- The first decision is whether to handle credit risk management, fraud detection, and so as a part of an accounting protocol, or whether to handle it as a part of yet to be defined resource management protocol. Support for these tasks could be included in products that use the DIAMETER resource management extensions [34], for instance. If the resource management protocol is used for this purpose then many of the requirements set in this document will apply to it. If not, a separate protocol needs to be constructed for the accounting part. [Discussion: The line between a resource management and accounting tasks is blurred in my mind - what IS the actual difference?]

- The second decision is to decide whether the support for large-voleme or light-weight applications is important enough to warrant the definition of a new protocol.

- The third decision is to decide whether the accounting work may assume the universal existence of large non-volatile memories or not.

9. Acknowledgements

The authors would like to thank Pat Calhoun (Sun Microsystems), Jan Melen (Ericsson), Jarmo Savolainen (Ericsson), and Glen Zorn (Microsoft) for many useful discussions of this problem space.

10. References

[1] B. Aboba, J. Lu, J. Alsop, J. Ding, W. Wang. "Review of Roaming Implementations." RFC 2194, Microsoft, Aimnet, i-Pass Alliance,

Asiainfo, Merit, September 1997.

[2] B. Aboba, G. Zorn. "Roaming Requirements." Internet draft (work in progress), draft-ietf-roamops-roamreq-07.txt, Microsoft, March 1998.

[3] C. Rigney, A. Rubens, W. Simpson, S. Willens. "Remote Authentication Dial In User Service (RADIUS)." RFC 2138, Livingston, Merit, Daydreamer, April, 1997.

[4] C. Rigney. "RADIUS Accounting." RFC 2139, Livingston, April, 1997.

[5] J. Gray, A. Reuter. Transaction Processing: Concepts and Techniques, Morgan Kaufmann Publishers, San Francisco, California, 1993.

[6] S. Bradner. "Key words for use in RFCs to Indicate Requirement Levels." RFC 2119, Harvard University, March, 1997.

[7] D. Crocker, P. Overrell. "Augmented BNF for Syntax Specifications: ABNF." RFC 2234, Internet Mail Consortium, Demon Internet Ltd., November 1997.

[8] G. Good. "The LDAP Data Interchange Format (LDIF) - Technical Specification." Internet draft (work in progress), draft-ietf-asid-ldif-02.txt, Netscape, July 1997.

[9] K. McCloghrie, J. Heinanen, W. Greene, A. Prasad. "Accounting Information for ATM Networks." Internet draft (work in progress), draft-ietf-atommib-atmacct-04.txt, Cisco Systems, Telecom Finland, MCI, November 1996.

[10] K. McCloghrie, J. Heinanen, W. Greene, A. Prasad. "Managed Objects for Controlling the Collection and Storage of Accounting Information for Connection-Oriented Networks." Internet draft (work in progress), draft-ietf-atommib-acct-04.txt, Cisco Systems, Telecom Finland, MCI, November 1996.

[11] B. Aboba, D. Lidyard. "Accounting Data Interchange Format (ADIF)." Internet draft (work in progress), draft-ietf-roamops-actng-04.txt, Microsoft, Telco Research, March 1998.

[12] D. Harrington, R. Presuhn, B. Wijnen, "An Architecture for Describing SNMP Management Frameworks", RFC 2271, Cabletron, BMC Software, IBM, January 1998.

[13] J. Case, D. Harrington, R. Presuhn, B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", RFC 2272, SNMP Research, Cabletron Systems, BMC Software,

IBM, January 1998.

[14] D. Levi, P. Meyer, B. Stewart, "SNMPv3 Applications", RFC 2273, SNMP Research, Secure Computing Corporation, Cisco Systems, January 1998.

[15] U. Blumenthal, B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", RFC 2274, IBM, January 1998.

[16] B. Wijnen, R. Presuhn, K. McCloghrie, "View-based Access Control Modem (VACM) for the Simple Network Management Protocol (SNMP)", RFC 2275, IBM, BMC Software, Cisco Systems, January 1998.

[17] R. Fajman. "An Extensible Message Format for Message Disposition Notifications." Internet draft (work in progress), draft-ietf- receipt-mdn-08.txt, National Institute of Health, August 1998.

[18] M. Elkins. "MIME Security with Pretty Good Privacy (PGP)." RFC 2015, The Aerospace Corporation, October, 1996.

[19] G. Vaudreuil. "The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages." RFC 1892, Octel Network Services, January, 1996.

[20] J. Galvin., et al. "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted." RFC 1847, Trusted Information Systems, October, 1995.

[21] D. Crocker. "MIME Encapsulation of EDI Objects." RFC 1767, Brandenburg Consulting, March, 1995.

[22] C. Shih, M. Jansson, R. Drummond. MIME-based Secure EDI." Internet draft (work in progress), draft-ietf-ediint-as1-05.txt, Actra, LiNK, Drummond Group, July 1997.

[23] C. Shih, M. Jansson, R. Drummond, L. Yarbrough. "Requirements for Inter-operable Internet EDI." Internet draft (work in progress), draft-ietf-ediint-req-04.txt, Actra, LiNK, Drummond Group, July 1997.

[24] S. Bradner. "Key words for use in RFCs to Indicate Requirement Levels." RFC 2119, Harvard University, March, 1997.

[25] Borenstein, N., Freed, N. "MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies", RFC 1521, Bellcore, Innosoft, December 1993.

[26] N. Joffe, D. Wing, L. Masinter. "SMTP Service Extension for Immediate Delivery", Internet draft (work in progress), draft-ietf-fax-smtp-session-02.txt, Cisco Systems, Xerox, February 1997.

[27] H. T. Johnson, R. S. Kaplan. Relevance Lost: The Rise and Fall of Management Accounting, Harvard Business School Press, Boston, Massachusetts, 1987.

[28] C. T. Horngren, G. Foster. Cost Accounting: A Managerial Emphasis. Prentice Hall, Englewood Cliffs, New Jersey, 1991.

[29] R. S. Kaplan, Anthony A. Atkinson. Advanced Management

Accounting. Prentice Hall, Englewood Cliffs, New Jersey, 1989.

[30] R. Cooper, R. S. Kaplan. The Design of Cost Management Systems. Prentice Hall, Englewood Cliffs, New Jersey, 1991.

[31] P. R. Calhoun, M. A. Beadles, A. Ratcliffe. "RADIUS Accounting Interim Accounting Record Extension", Internet draft (work in progress), draft-ietf-radius-acct-interim-00.txt, July 1997.

[32] D. Carrel, L. Grant. "The TACACS+ Protocool Version 1.78", Internet draft (work in progress), draft-grant-tacacs-02.txt, Cisco Systems, January, 1997.

[33] P. R. Calhoun, A. Rubens. "DIAMETER Base Protocol", Internet draft (work in progress), draft-calhoun-diameter-01.txt, Sun Microsystems, Merit Networks, March, 1998.

[34] P. R. Calhoun. "DIAMETER Resource Management Extensions", Internet draft (work in progress), draft-calhoun-diameter-res-mgmt-00.txt, Sun Microsystems, March, 1998.

[35] P. R. Calhoun. "DIAMETER User Authentication Extensions", Internet draft (work in progress), draft-calhoun-diameter-authent-01.txt, Sun Microsystems, March, 1998.

11. Authors' Addresses

Jari Arkko
Oy LM Ericsson Ab
02420 Jorvas
Finland

Phone: +358 40 5079256
EMail: Jari.Arkko@ericsson.com