Net-Net® 4000
Accounting Guide

Release Version S-C6.2.0

Acme Packet, Inc.
71 Third Avenue
Burlington, MA 01803
t 781-328-4400
f 781-425-5077
www.acmepacket.com

Last updated: November 30, 2009
Document Number: 400-0015-62 Rev. 0.00

Notices

Contents

About this Guide

Overview

The *Net-Net 4000 Accounting Guide* describes:

- The Net-Net™ SBC's accounting-based on Remote Authentication Dial-in User Service (RADIUS)
- How to configure RADIUS accounting support, and the features related to it
- Local CDR storage and FTP file push
- Use and maintenance of the Storage Expansion Module
- Diameter-based Rf Accounting

It includes the Acme Packet accounting Vendor-Specific Attributes (VSAs), and the Cisco Systems, Inc.™ VSAs supported by the Net-Net SBC. This reference guide indicates the Cisco Systems' VSAs supported by Acme Packet's Net-Net products.

This guide also includes RADIUS-related statistics and alarm information and associated Acme Packet Command Line Interface (ACLI) configuration element examples. Appendix A of this guide contains a selection of examples of RADIUS logs for purposes of reference.

About Net-Net 4000 Software Releases

Release version S-C6.2.0 is supported on the Net-Net 4000 series platforms. This series contains two systems, the Net-Net 4250 and the Net-Net 4500. S-C6.2.0 also runs on the Net-Net 3000 series of systems.

Who is Acme Packet?

Acme Packet enables service providers to deliver trusted, first class interactive communications—voice, video and multimedia sessions—across IP network borders. Our Net-Net family of session border controllers satisfy critical security, service assurance and regulatory requirements in wireline, cable and wireless networks. Our deployments support multiple applications—from VoIP trunking to hosted enterprise and residential services; multiple protocols—SIP, H.323, MGCP/NCS and H.248; and multiple border points—interconnect, access network and data center.

Established in August 2000 by networking industry veterans, Acme Packet is a public company trading on the NASDAQ and headquartered in Burlington, Massachusetts.

Related Documentation

The following table lists related documents.

Document Name	Document Description
Net-Net 4250 Hardware Installation Guide (400-0003-00)	Contains information about the components and installation of the Net-Net SBC.
Net-Net 4500 Hardware Installation Guide (400-0101-00)	Contains information about the components and installation of the Net-Net 4500 SBC.
Net-Net 4000 Configuration Guide (400-0061-00)	Contains information about the administration and software configuration of the Net-Net SBC.
Net-Net 4000 ACLI Reference Guide (400-0062-00)	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Net-Net 4000 Maintenance and Troubleshooting Guide (400-0063-00)	Contains information about Net-Net SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
Net-Net 4000 MIB Reference Guide (400-0010-00)	Contains information about Management Information Base (MIBs), Acme Packet's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.

Revision History

This section contains a revision history for this document.

Date	Revision Number	Description
November 30, 2009	Revision 0.00	• Initial Release

Technical Assistance

If you need technical assistance with Acme Packet products, you can obtain it on-line by going to https://support.acmepacket.com. With your customer identification number and password, you can access Acme Packet's on-line resources 24 hours a day. If you do not have the information required to access the site, send an email to tac@acmepacket.com requesting a login.

In the event that you are experiencing a critical service outage and require live assistance, you can contact the Acme Packet Technical Assistance Center emergency hotline:

- From the United States, Canada, and Mexico call: 1 866 226 3758

- From all other locations, call: +1 781 756 6920

Please note that a valid support/service contract with Acme Packet is required to obtain technical assistance.

Customer Questions, Comments, or Suggestions

Acme Packet is committed to providing our customers with reliable documentation. If you have any questions, comments, or suggestions regarding our documentation, please contact your Acme Packet customer support representative directly or email support@acmepacket.com.

Contact Us

Acme Packet
71 Third Avenue
Burlington, MA 01803 USA
t 781 328 4400
f 781 425 5077
www.acmepacket.com

1 Using RADIUS with the Net-Net SBC

Introduction

RADIUS is an accounting, authentication, and authorization (AAA) system. In general, RADIUS servers are responsible for receiving user connection requests, authenticating users, and returning all configuration information necessary for the client to deliver service to the user.

You can configure your Net-Net SBC to send call accounting information to one or more RADIUS servers. This information can help you to see usage and QoS metrics, monitor traffic, and even troubleshoot your system. For more information about QoS, refer to the *Admission Control and QoS* chapter of the *Net-Net 4000 ACLI Configuration Guide*.

For information about how to configure the Net-Net SBC for RADIUS accounting use, refer to this guide's Configuring Accounting (39) chapter.

Licensing

In order to use RADIUS with your Net-Net SBC, you must have the accounting license installed and activated on your system. For more information about licensing, see the "Software Licensing" section of the *Net-Net 4000 ACLI Configuration Guide*'s *Getting Started* chapter. This chapter provides details about Acme Packet software licensing, including instructions for how to obtain and install licenses.

Overview

For H.323, SIP, and calls being interworked between H.323 and SIP (IWF), you can obtain sets of records that contain information to help you with accounting and that provide a quantitative and qualitative measurement of the call. For H.323 and SIP calls, the Net-Net SBC generates one set of records; for calls requiring IWF, the Net-Net SBC generates two sets of records.

You can use the RADIUS records generated by your Net-Net SBC to assist you with:

- Usage accounting—See the calling and called parties for a call, the protocol used, the realm the call traversed (as well as local and remote IP address and port information), and the codec used
- Traffic monitoring—You can see information about the setup, connect, and disconnect times, as well as the SIP or H.323 disconnect cause
- SLA monitoring—The Net-Net SBC supports RADIUS attributes that provide information about jitter, latency, and loss for H.323, SIP, and calls that require interworking between H.323 and SIP
- Troubleshooting—Obtain information about calls that can help you to identify and address issues with quality and how calls are setup and torn down.

Standard RADIUS Attributes

This section describes the standard RADIUS attributes that the Net-Net SBC supports. These attributes appear along with VSAs (Vendor-Specific Attributes) in the CDRs that the Net-Net SBC generates.

The Standard RADIUS Attributes Dictionary (12) is a dictionary of the standard RADIUS attributes included in Accounting Request messages sent by the Net-Net SBC to the RADIUS server. The CDR event information determines which messages are generated and which RADIUS attributes are included in the messages. Standard RADIUS messages and attributes are used whenever possible; however, RADIUS does not have attributes to record all important session information.

Possible messages are:

- Start—Marks the start of service delivery and describes the type of service being delivered and the user to whom it is being delivered
- Interim-Update—Indicates to the accounting server that the session parameters have changed
- Stop—
  - Marks the end of service delivery
  - Describes the type of service that was delivered
  - Sometimes describes statistics such as elapsed time, input and output octets, or input and output packets
- On—Marks the start of accounting
- Off—Marks the end of accounting

VSAs are used to record the necessary session information missing from this list of standard RADIUS attributes.

For more information about RADIUS, see to the following Internet Engineering Task Force Request for Comments (IETF RFCs):

- RFC 2865, "Remote Authentication Dial In User Service (RADIUS)," Rigney, et al., June 2000 (http://www.ietf.org/rfc/rfc2865.txt)
- RFC 2866, "RADIUS Accounting," C. Rigney, June 2000 (http://www.ietf.org/rfc/rfc2866.txt)

Standard RADIUS Attributes Dictionary

The table below lists and describes standard RADIUS attributes.

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
NAS-IP-Address	IP address of the SIP proxy or the H.323 stack's call signaling address.	4	IP address	• Start • Interim-Update • Stop • On • Off
NAS-Port	SIP proxy port or the H.323 stack's call signaling RAS port.	5	integer	• Start • Interim-Update • Stop • On • Off

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Called-Station-Id	"To" field value of the SIP INVITE message (a type of message used to initiate a session) or the `calledPartyNumber` of the H.323 message.	30	string	• Start • Interim-Update • Stop
Calling-Station-Id	"From" field value of the SIP INVITE message or the `callingPartyNumber` of the H.323 message.	31	string	• Start • Interim-Update • Stop
NAS-Identifier	Value, if any, set in the optional `NAS-ID` field for the accounting server that you configure as part of the accounting configuration. This identifier sets the value that the remote server (the accounting server) uses to identify the Net-Net SBC so that RADIUS messages can be transmitted. The remote server to which the accounting configuration will send messages uses at least one of two pieces of information for identification: • NAS IP address: always included in the accounting message • NAS identifier: configured in the NAS-ID parameter of the accounting server; if configured, the NAS identifier is sent to the remote server This attribute only appears if a value is configured in the NAS-ID field.	32	string	• Start • Interim-Update • Stop • On • Off
Acct-Status-Type	Whether this Accounting Request marks the beginning of the RADIUS message (Start), the middle (Interim-Update), or the end (Stop), and whether the accounting function is on or off (Accounting-On or Accounting-Off).	40	integer	• Start (1) • Interim-Update • Stop (2) • On • Off
Acct-Session-Id	Either the "Call-ID" field value of the SIP INVITE message, the `callIdentifier` of the H.323 message, or RADIUS client information.	44	string	• Start • Interim-Update • Stop • On • Off
Acct-Session-Time	How much time in seconds the user has received service.	46	integer	• Interim-Update • Stop • Off
Acct-Terminate-Cause	How or why the session ended.	49	integer	• Stop • Off

RADIUS Accounting Termination Causes

The table below describes the possible session termination causes for the Acct-Terminate-Cause RADIUS attribute.

RADIUS Termination Cause	Related Integer Value (per RFC 2059)	Termination Event	Message
User Request	1	A SIP BYE message.	• Stop
User Error	17	Input from user is erroneous; for example, SIP signaling failed to establish the session. Used in combination with the Cisco Systems Disconnect Cause. (This termination cause is not used for H.323.)	• Stop
Lost Service	3	Service cannot be sustained for reasons such as a lost connection.	• Stop
Admin Reset	6	Net-Net SBC hard reset occurred: A hard reset occurs when you use the front panel's orange Reset button; it reboots the Net-Net SBC.	• Off
Admin Reboot	7	Net-Net SBC gracefully rebooted.	• Off
NAS Request	10	RADIUS server is disabled; session terminated for non-error reason.	• Off

VSAs

This section describes the VSAs that the Net-Net SBC supports. These attributes appear along with standard RADIUS attributes in the CDRs that the Net-Net SBC generates.

VSAs are defined by vendors of remote access servers in order to customize how RADIUS works on their servers. This section describes the accounting VSAs for Acme Packet and for Cisco Systems.

Acme Packet RADIUS VSAs

Acme Packet's vendor identification number is 9148. This number refers to the 4-octet VSA Vendor-ID field. The high-order octet is 0 and the low-order 3 octets are the SMI Network Management Private Enterprise Code of the Vendor in network byte order, defined in the Assigned Numbers RFC (http://www.faqs.org/rfcs/rfc1700.html; Reynolds, J. and J. Postel, "Assigned Numbers", STD 2, RFC 1700, October 1994).

The table in this section is a dictionary of Acme Packet's accounting VSAs. You can use this information to translate the Acme Packet VSAs in Net-Net SBC RADIUS messages into human-readable form. Acme Packet maintains VSA dictionary definition files for the most popular RADIUS distributions; ask your Acme Packet account representative for details.

Grouped according to attribute function, this table contains the following sections:

- General Flow Attributes—Overall traits of the media flow, these attributes appear in all CDRs regardless of the session's protocol; these attribute fields are only populated if there are media flows

- Inbound Flow Attributes—Detailed traits of the inbound media flow (including realm, remote IP address and port, and local IP address and port); these attribute fields are only populated if there are media flows
- Outbound Flow Attributes—Detailed traits of the outbound media flow (including realm, remote IP address and port, and local IP address and port); these attribute field are only populated if there are media flows
- Session Attributes—Information about the protocol type, ingress and egress realms used, and an identifier that links the H.323 and SIP legs of a call requiring IWF
- QoS Attributes—RADIUS call records are instantiated by individual signaling applications on the Net-Net SBC. The Net-Net SBC writes the following additional parameters to the call record for QoS (Quality of Service):
  - RTP Lost packets
  - RTP Jitter
  - RTP Maximum Jitter
  - RTCP Lost packets
  - RTCP Jitter
  - RTCP Latency
  - RTCP Maximum Latency
  - RTP Total Packets
  - RTP Total Octets

  Only RADIUS Stop records contain QoS information. For non-QoS calls, the attributes appear in the record, but their values are always be zero (0). When you review the list of QoS VSAs, please note that "calling" in the attribute name means the information is sent by the calling party and "called" in the attribute name means the information is sent by the called party.

Examples of how this information appears in CDRs appears in Appendix A (89) of this guide. Please note that the contents of Interim-Update messages do not depend on what events cause a Start message to be generated.

New in Release S-C6.0.0

The Net-Net SBC reports R-Factor and MOS data for the calling and called segments at the end of a session. This information appears in RADIUS CDRs, and in the Acme Packet VSA dictionary:

- Acme-Calling-R-Factor (151)
- Acme-Calling-MOS (152)
- Acme-Called-R-Factor (153)
- Acme-Called-MOS (154)

Note: These values are reported as * 100 in order to appear as integers.

Notes on Media Flow Attributes

The Net-Net SBC records media flow attributes in RADIUS CDRs, and there can be multiple flows per session. In order to distinguish between the two flows that appear for a basic session (forward and reverse), the Net-Net SBC supports unique media flow attribute names.

The term "flow-set" represents a pair of media flows, where one is the forward flow and one is the reverse. The flow attributes described in the table below have the

designation FS1 or FS2, which identifies it as either the first or the second flow-set. In addition, all non-QoS attributes have a direction indicator: F for forward, and R for reverse.

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
General Attributes				
Acme-CDR-Sequence-Number	Sequence number (that increases by 1) the Net-Net SBC generates; recorded in each CDR.	59	integer	• Start • Interim-Update • Stop
Acme-Intermediate-Time	Time interval at which periodic interim records are generated during a call.	63	string	• Interim-Update
Acme-Local-Time-Zone	Local GMT/UTC time zone that is provisioned on the Net-Net SBC.	57	string	• Start • Interim-Update • Stop
Acme-Firmware-Version	Current software version running on the Net-Net SBC.	56	string	• Start • Interim-Update • Stop
General Flow Attributes				
Acme-FlowID_FS1_F	Unique identifier for every media flow processed by the Net-Net SBC, flow-set 1 forward direction. This VSA always prefaces other flow information.	1	string	• Start • Interim-Update • Stop • On • Off
Acme-FlowID_FS1_R	Unique identifier for every media flow processed by the Net-Net SBC, flow-set 1 reverse direction. This VSA always prefaces other flow information.	78	string	• Start • Interim-Update • Stop • On • Off
Acme-FlowID_FS2_F	Unique identifier for every media flow processed by the Net-Net SBC, flow-set 2 forward direction. This VSA always prefaces other flow information.	90	string	• Start • Interim-Update • Stop • On • Off
Acme-FlowID_FS2_R	Unique identifier for every media flow processed by the Net-Net SBC, flow-set 2 reverse direction. This VSA always prefaces other flow information.	112	string	• Start • Interim-Update • Stop • On • Off
Acme-FlowType_FS1_F	Codec that describes the flow, flow-set 1 forward direction: PCMU, PCMA, G726, G723, G728, G729, H261, H263, T38.	2	string	• Start • Interim-Update • Stop • On • Off

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-FlowType_FS1_R	Codec that describes the flow, flow-set 1 reverse direction: PCMU, PCMA, G726, G723, G728, G729, H261, H263, T38.	79	string	• Start • Interim-Update • Stop • On • Off
Acme-FlowType_FS2_F	Codec that describes the flow, flow-set 2 forward direction: PCMU, PCMA, G726, G723, G728, G729, H261, H263, T38.	91	string	• Start • Interim-Update • Stop • On • Off
Acme-FlowType_FS2_R	Codec that describes the flow, flow-set 2 reverse direction: PCMU, PCMA, G726, G723, G728, G729, H261, H263, T38.	113	string	• Start • Interim-Update • Stop • On • Off
Inbound Flow Attributes				
Acme-Flow-In-Realm_FS1_F	Inbound realm identifier for flow-set 1, forward direction.	10	string	• Start • Interim-Update • Stop
Acme-Flow-In-Realm_FS1_R	Inbound realm identifier for flow-set 1, reverse direction.	80	string	• Start • Interim-Update • Stop
Acme-Flow-In-Realm_FS2_F	Inbound realm identifier for flow-set 2, forward direction.	92	string	• Start • Interim-Update • Stop
Acme-Flow-In-Realm_FS2_R	Inbound realm identifier for flow-set 2, reverse direction.	114	string	• Start • Interim-Update • Stop
Acme-Flow-In-Src-Addr_FS1_F	Inbound source address (remote) information for flow-set 1, forward direction.	11	IP address	• Start • Interim-Update • Stop
Acme-Flow-In-Src-Addr_FS1_R	Inbound source address (remote) information for flow-set 1, reverse direction.	81	IP address	• Start • Interim-Update • Stop
Acme-Flow-In-Src-Addr_FS2_F	Inbound source address (remote) information for flow-set 2, forward direction.	93	IP address	• Start • Interim-Update • Stop
Acme-Flow-In-Src-Addr_FS2_R	Inbound source address (remote) information for flow-set 2, reverse direction.	115	IP address	• Start • Interim-Update • Stop
Acme-Flow-In-Src-Port_FS1_F	Inbound source (remote) port information for flow-set 1, forward direction.	12	integer	• Start • Interim-Update • Stop
Acme-Flow-In-Src-Port_FS1_R	Inbound source (remote) port information for flow-set 1, reverse direction.	82	integer	• Start • Interim-Update • Stop

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Flow-In-Src-Port_FS2_F	Inbound source (remote) port information for flow-set 2, forward direction.	94	integer	• Start • Interim-Update • Stop
Acme-Flow-In-Src-Port_FS2_R	Inbound source (remote) port information for flow-set 2, reverse direction.	116	integer	• Start • Interim-Update • Stop
Acme-Flow-In-Dst-Addr_FS1_F	Inbound destination (local) address information (the IPv4 address field value of the steering pool configuration) for flow-set 1, forward direction.	13	IP address	• Start • Interim-Update • Stop
Acme-Flow-In-Dst-Addr_FS1_R	Inbound destination (local) address information (the IPv4 address field value of the steering pool configuration) for flow-set 1, reverse direction.	83	IP address	• Start • Interim-Update • Stop
Acme-Flow-In-Dst-Addr_FS2_F	Inbound destination (local) address information (the IPv4 address field value of the steering pool configuration) for flow-set 2, forward direction.	95	IP address	• Start • Interim-Update • Stop
Acme-Flow-In-Dst-Addr_FS2_R	Inbound destination (local) address information (the IPv4 address field value of the steering pool configuration) for flow-set 2, reverse direction.	117	IP address	• Start • Interim-Update • Stop
Acme-Flow-In-Dst-Port_FS1_F	Inbound destination (local) port information (a port in the range between the start port and end port field values of the steering pool configuration) for flow-set 1, forward direction.	14	integer	• Start • Interim-Update • Stop
Acme-Flow-In-Dst-Port_FS1_R	Inbound destination (local) port information (a port in the range between the start port and end port field values of the steering pool configuration) for flow-set 1, reverse direction.	84	integer	• Start • Interim-Update • Stop
Acme-Flow-In-Dst-Port_FS2_F	Inbound destination (local) port information (a port in the range between the start port and end port field values of the steering pool configuration) for flow-set 2, forward direction.	96	integer	• Start • Interim-Update • Stop
Acme-Flow-In-Dst-Port_FS2_R	Inbound destination (local) port information (a port in the range between the start port and end port field values of the steering pool configuration) for flow-set 2, reverse direction.	118	integer	• Start • Interim-Update • Stop
Outbound Flow Attributes				
Acme-Flow-Out-Realm_FS1_F	Outbound realm identifier for flow-set 1, forward direction.	20	string	• Start • Interim-Update • Stop
Acme-Flow-Out-Realm_FS1_R	Outbound realm identifier for flow-set 1, reverse direction.	85	string	• Start • Interim-Update • Stop

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Flow-Out-Realm_FS2_F	Outbound realm identifier for flow-set 2, forward direction.	97	string	• Start • Interim-Update • Stop
Acme-Flow-Out-Realm_FS2_R	Outbound realm identifier for flow-set 2, reverse direction.	119	string	• Start • Interim-Update • Stop
Acme-Flow-Out-Src-Addr_FS1_F	Outbound source (local) address information (the IPv4 address field value of the steering port configuration) for flow-set 1, forward direction.	21	IP address	• Start • Interim-Update • Stop
Acme-Flow-Out-Src-Addr_FS1_R	Outbound source (local) address information (the IPv4 address field value of the steering port configuration) for flow-set 1, reverse direction.	86	IP address	• Start • Interim-Update • Stop
Acme-Flow-Out-Src-Addr_FS2_F	Outbound source (local) address information (the IPv4 address field value of the steering port configuration) for flow-set 2, forward direction.	98	IP address	• Start • Interim-Update • Stop
Acme-Flow-Out-Src-Addr_FS2_R	Outbound source (local) address information (the IPv4 address field value of the steering port configuration) for flow-set 2, reverse direction.	120	IP address	• Start • Interim-Update • Stop
Acme-Flow-Out-Src-Port_FS1_F	Outbound source (local) port information for flow-set 1, forward direction (a port in the range between the start port and end port field values of the steering port configuration).	22	integer	• Start • Interim-Update • Stop
Acme-Flow-Out-Src-Port_FS1_R	Outbound source (local) port information for flow-set 1, reverse direction (a port in the range between the start port and end port field values of the steering port configuration).	87	integer	• Start • Interim-Update • Stop
Acme-Flow-Out-Src-Port_FS2_F	Outbound source (local) port information for flow-set 2, forward direction (a port in the range between the start port and end port field values of the steering port configuration).	99	integer	• Start • Interim-Update • Stop
Acme-Flow-Out-Src-Port_FS2_R	Outbound source (local) port information for flow-set 2, reverse direction (a port in the range between the start port and end port field values of the steering port configuration).	121	integer	• Start • Interim-Update • Stop
Acme-Flow-Out-Dst-Addr_FS1_F	Outbound destination (remote) address information for flow-set 1, forward direction.	23	IP address	• Start • Interim-Update • Stop
Acme-Flow-Out-Dst-Addr_FS1_R	Outbound destination (remote) address information for flow-set 1, reverse direction.	88	IP address	• Start • Interim-Update • Stop

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Flow-Out-Dst-Addr_FS2_F	Outbound destination (remote) address information for flow-set 2, forward direction.	100	IP address	• Start • Interim-Update • Stop
Acme-Flow-Out-Dst-Addr_FS2_R	Outbound destination (remote) address information for flow-set 2, reverse direction.	122	IP address	• Start • Interim-Update • Stop
Acme-Flow-Out-Dst-Port_FS1_F	Outbound destination (remote) port information for flow-set 1, forward direction.	24	integer	• Start • Interim-Update • Stop
Acme-Flow-Out-Dst-Port_FS1_R	Outbound destination (remote) port information for flow-set 1, reverse direction.	89	integer	• Start • Interim-Update • Stop
Acme-Flow-Out-Dst-Port_FS2_F	Outbound destination (remote) port information for flow-set 2, forward direction.	101	integer	• Start • Interim-Update • Stop
Acme-Flow-Out-Dst-Port_FS2_R	Outbound destination (remote) port information for flow-set 2, reverse direction.	123	integer	• Start • Interim-Update • Stop
Session Attributes				
Acme-Session-Generic-Id	Common ID shared by H.323 and SIP call legs of a session. This attribute is a combination of a time stamp (measured in seconds) and a monotonically increasing 16-bit integer, followed by an at-sign (@) and the MAC address of the rear interface (wancom). This attribute is only used to correlate the H.323 and SIP legs of an interworking call/session. This VSA is not configurable; all CDRs contain this attribute.	40	string	• Start • Interim-Update • Stop
Acme-Session-Ingress-CallId	Call ID generated by the originating device.	3	string	• Start • Interim-Update • Stop
Acme-Session-Egress-CallId	Call ID generated by the Net-Net SBC to represent a two-way transaction.	4	string	• Start • Interim-Update • Stop
Acme-Session-Ingress-Realm	Explicitly identifies the ingress realm, and contains the name of the ingress realm for the session. All CDRs contain this attribute. This VSA is not configurable; all CDRs contain this attribute.	41	string	• Start • Interim-Update • Stop

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Session-Egress-Realm	Explicitly identifies the egress realm, and contains the name of the egress realm for the session. All CDRs contain this attribute. This VSA is not configurable. All CDRs contain this attribute, but it is only populated if an egress realm is found; a call without a route does not have an egress realm.	42	string	• Start • Interim-Update • Stop
Acme-Session-Protocol-Type	Signaling protocol used for a particular leg of a session (in the case of IWF, there may be two legs). This attribute contains the signaling protocol type; for example, `SIP` or `H323`. This VSA is not configurable; all CDRs contain this attribute.	43	string	• Start • Interim-Update • Stop
Acme-Session-Charging-Vector	Appears when the Net-Net SBC inserts, passes, or deletes the P-Charging-Vector header (SIP). This attribute is only populated for SIP CDRs, and is not populated if the Net-Net SBC does not have P-Charging-Vector information.	54	string	• Start • Interim-Update • Stop
Acme-Session-Charging-Function_Address	Appears when the Net-Net SBC inserts, passes, or deletes the P-Charging-Function-Address. This attribute is only populated for SIP CDRs, and is not populated if the Net-Net SBC does not have P-Charging-Function-Address information.	55	string	• Start • Interim-Update • Stop
Acme-Session-Disposition	Status of the call attempt as it progresses from being initiated (using a SIP INVITE or H.323 Setup message) to being either answered or failing to be answered.	60	integer	• Start • Interim-Update • Stop
Acme-Post-Dial-Delay	Amount of time between session initiation and an alerting event.	58	integer	• Start • Interim-Update • Stop
Acme-P-Asserted-ID	P-Asserted ID as described in RFC 3325.	69	integer	• Start • Interim-Update • Stop
Acme-SIP-Diversion	SIP Diversion header; communicates to the called party from whom and why a call diverted.	70	integer	• Start • Interim-Update • Stop
Acme-Primary-Routing-Number	Primary routing number and phone context (or ingress SIP Request-URI).	64	string	• Start • Interim-Update • Stop

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Egress-Final-Routing-Number	Final routing number and phone context (or egress SIP Request-URI).	134	integer	• Stop
Acme-Disconnect-Initiator	Initiator of a call disconnect.	61	integer	• Stop
Acme-Disconnect-Cause	Q.850 cause code value.	62	integer	• Stop
Acme-SIP-Status	SIP status code for RFC 3326 support.	71	integer	• Stop
Acme-Originating-Trunk-Group	Originating trunk group.	65	string	• Start • Interim-Update • Stop
Acme-Originating-Trunk-Context	Originating trunk group context.	67	string	• Start • Interim-Update • Stop
Acme-Terminating-Trunk-Group	Terminating trunk group.	66	string	• Start • Interim-Update • Stop
Acme-Terminating-Trunk-Context	Terminating trunk group context.	68	string	• Start • Interim-Update • Stop
Acme-Ingress-Local-Addr	Signaling IP address and port of the ingress Net-Net SBC signaling interface.	74	string	• Start • Interim-Update • Stop
Acme-Ingress-Remote-Addr	Signaling IP address and port of the ingress remote signaling element.	75	string	• Start • Interim-Update • Stop
Acme-Egress-Local-Addr	Signaling IP address and port of the egress Net-Net SBC signaling interface.	76	string	• Start • Interim-Update • Stop
Acme-Egress-Remote-Addr	Signaling IP address and port of the destination signaling element.	77	string	• Start • Interim-Update • Stop
Acme-Session-Ingress-RPH	RPH value received in the incoming call (e.g., ets.1). Only populated for NSEP calls.	135	string	• Start • Interim-Update • Stop
Acme-Session-Egress-RPH	RPH value sent in the outgoing call (e.g., ets.3). Only populated for NSEP calls.	136	string	• Start • Interim-Update • Stop
Acme-Ingress-Network-Interface-Id	To differentiate overlapping IP address spaces (with the Acme-Ingress-Vlan-Tag-Value), gives the ID of the ingress network interface.	137	string	• Start • Interim-Update • Stop
Acme-Ingress-Vlan-Tag-Value	To differentiate overlapping IP address spaces (with the Acme-Ingress-Network-Interface-Id), gives the VLAN tag.	138	integer	• Start • Interim-Update • Stop

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Egress-Network-Interface-Id	To differentiate overlapping IP address spaces (with the Acme-Egress-Vlan-Tag-Value), gives the ID of the ingress network interface.	139	string	• Start • Interim-Update • Stop
Acme-Egress-Vlan-Tag-Value	To differentiate overlapping IP address spaces (with the Acme-Egress-Network-Interface-Id), gives the VLAN tag.	140	integer	• Start • Interim-Update • Stop
Acme-Refer-Call-Transfer-Id	For SIP REFER call method transfer, communicates a call has been transferred from the referer to the referree	141	string	• Stop
QoS Attributes				
Acme-Calling-RTCP-Packets-Lost_FS1	Total lost packets reported via Real-time Transport Protocol Control Protocol (RTCP), flow-set 1. Populated only if QoS is enabled.	32	integer	• Stop
Acme-Calling-RTCP-Packets-Lost_FS2	Total lost packets measured on RTP packets in milliseconds, flow-set 2. Populated only if QoS is enabled.	104	integer	• Stop
Acme-Calling-RTCP-Avg-Jitter_FS1	Average jitter reported via RTCP measured in milliseconds, flow-set 1. Populated only if QoS is enabled.	33	integer	• Stop
Acme-Calling-RTCP-Avg-Jitter_FS2	Average jitter reported via RTCP measured in milliseconds, flow-set 2. Populated only if QoS is enabled.	105	integer	• Stop
Acme-Calling-RTCP-Avg Latency_FS1	Average latency reported by comparing the timestamps in RTCP packets for each direction of a call, flow-set 1. Populated only if QoS is enabled.	34	integer	• Stop
Acme-Calling-RTCP-Avg Latency_FS2	Average latency reported by comparing the timestamps in RTCP packets for each direction of a call, flow-set 2. Populated only if QoS is enabled.	106	integer	• Stop
Acme-Calling-RTCP-MaxJitter_FS1	Maximum amount of jitter value reported via RTCP measured in milliseconds, flow-set 1. Populated only if QoS is enabled.	35	integer	• Stop
Acme-Calling-RTCP-MaxJitter_FS2	Maximum amount of jitter value reported via RTCP measured in milliseconds, flow-set 3. Populated only if QoS is enabled.	107	integer	• Stop

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Calling-RTCP-MaxLatency_FS1	Maximum latency value measured in milliseconds as observed through RTCP, flow-set 1. Populated only if QoS is enabled.	36	integer	• Stop
Acme-Calling-RTCP-MaxLatency_FS2	Maximum latency value measured in milliseconds as observed through RTCP, flow-set 2. Populated only if QoS is enabled.	108	integer	• Stop
Acme-Calling-Octets_FS1	Bytes of RTP traffic for this call, flow-set 1. Populated only if QoS is enabled.	28	integer	• Stop
Acme-Calling-Octets_FS2	Bytes of RTP traffic for this call, flow-set 2. Populated only if QoS is enabled.	102	integer	• Stop
Acme-Calling-Packets_FS1	RTP packets for this call, flow-set 1. Populated only if QoS is enabled.	29	integer	• Stop
Acme-Calling-Packets_FS2	RTP packets for this call, flow-set 2. Populated only if QoS is enabled.	103	integer	• Stop
Acme-Calling-RTP-Packets-Lost_FS1	Total lost packets measured on RTP packets in milliseconds, flow-set 1. Populated only if QoS is enabled.	37	integer	• Stop
Acme-Calling-RTP-Packets-Lost_FS2	Total lost packets measured on RTP packets in milliseconds, flow-set 2. Populated only if QoS is enabled.	109	integer	• Stop
Acme-Calling-RTP-Avg-Jitter_FS1	Total jitter measured on RTP packets in milliseconds, flow-set 1. Populated only if QoS is enabled.	38	integer	• Stop
Acme-Calling-RTP-Avg-Jitter_FS2	Total jitter measured on RTP packets in milliseconds, flow-set 2. Populated only if QoS is enabled.	110	integer	• Stop
Acme-Calling-RTP-MaxJitter_FS1	Maximum jitter measured on RTP packets in milliseconds, flow-set 1. Populated only if QoS is enabled.	39	integer	• Stop
Acme-Calling-RTP-Avg-MaxJitter_FS2	Maximum jitter measured on RTP packets in milliseconds, flow-set 2. Populated only if QoS is enabled.	111	integer	• Stop

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Called-Octets_FS1	Bytes of RTP traffic for the ingress side of the call, flow-set 1. Populated only if QoS is enabled.	44	integer	• Stop
Acme-Called-Octets_FS2	Bytes of RTP traffic for the ingress side of the call, flow-set 2. Populated only if QoS is enabled.	124	integer	• Stop
Acme-Called-Packets_FS1	RTP packets for the ingress side of the call, flow-set 1. Populated only if QoS is enabled.	45	integer	• Stop
Acme-Called-Packets_FS2	RTP packets for the ingress side of the call, flow-set 2. Populated only if QoS is enabled.	125	integer	• Stop
Acme-Called-RTCP-Packets-Lost_FS1	Total lost packets measured on RTCP packets in milliseconds for the ingress side of the call, flow-set 1. Populated only if QoS is enabled.	46	integer	• Stop
Acme-Called-RTCP-Packets-Lost_FS2	Total lost packets measured on RTCP packets in milliseconds for the ingress side of the call, flow-set 2. Populated only if QoS is enabled.	126	integer	• Stop
Acme-Called-RTCP-Avg-Jitter_FS1	Average jitter reported via RTCP measured in milliseconds for the ingress side of the call, flow-set 1. Populated only if QoS is enabled.	47	integer	• Stop
Acme-Called-RTCP-Avg-Jitter_FS2	Average jitter reported via RTCP measured in milliseconds for the ingress side of the call, flow-set 2. Populated only if QoS is enabled.	127	integer	• Stop
Acme-Called-Avg-Latency_FS1	Average latency reported via RTCP measured in milliseconds for the ingress side of the call, flow-set 1. Populated only if QoS is enabled.	48	integer	• Stop
Acme-Called-Avg-Latency_FS2	Average latency reported via RTCP measured in milliseconds for the ingress side of the call, flow-set 2. Populated only if QoS is enabled.	128	integer	• Stop
Acme-Called-RTCP-MaxJitter_FS1	Maximum amount of jitter reported via RTCP measured in milliseconds for the ingress side of the call, flow-set 1. Populated only if QoS is enabled.	49	integer	• Stop

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Called-RTCP-MaxJitter_FS2	Maximum amount of jitter reported via RTCP measured in milliseconds for the ingress side of the call, flow-set 2. Populated only if QoS is enabled.	129	integer	• Stop
Acme-Called-RTCP-MaxLatency_FS1	Maximum amount of latency reported via RTCP measured in milliseconds for the ingress side of the call, flow-set 1. Populated only if QoS is enabled.	50	integer	• Stop
Acme-Called-RTCP-MaxLatency_FS2	Maximum amount of latency reported via RTCP measured in milliseconds for the ingress side of the call, flow-set 2. Populated only if QoS is enabled.	130	integer	• Stop
Acme-Called-RTP-Packets-Lost_FS1	Total lost packets measured on RTP packets in milliseconds for the ingress side of the call, flow-set 1. Populated only if QoS is enabled.	51	integer	• Stop
Acme-Called-RTP-Packets-Lost_FS2	Total lost packets measured on RTP packets in milliseconds for the ingress side of the call, flow-set 2. Populated only if QoS is enabled.	131	integer	• Stop
Acme-Called-RTP-Avg-Jitter_FS1	Average jitter reported via RTP measured in milliseconds for the ingress side of the realm, flow-set 1. Populated only if QoS is enabled.	52	integer	• Stop
Acme-Called-RTP-Avg-Jitter_FS2	Average jitter reported via RTP measured in milliseconds for the ingress side of the realm, flow-set 2. Populated only if QoS is enabled.	132	integer	• Stop
Acme-Called-RTP-MaxJitter_FS1	Maximum amount of jitter reported via RTP measured in milliseconds for the ingress side of the call, flow-set1. Populated only if QoS is enabled.	53	integer	• Stop
Acme-Called-RTP-MaxJitter_FS2	Maximum amount of jitter reported via RTP measured in milliseconds for the ingress side of the call, flow-set 2. Populated only if QoS is enabled.	133	integer	• Stop
Acme-Calling-R-Factor New in Release S-C6.1.0	QoS R-Factor calculation for the calling side of a session. Populated only if QoS is enabled. This value is reported as * 100 in order to appear as an integer.	151	integer	Stop

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Calling-MOS New in Release S-C6.1.0	QoS MOS calculation for the calling side of a session. Populated only if QoS is enabled. This value is reported as * 100 in order to appear as an integer.	152	integer	Stop
Acme-Called-R-Factor New in Release S-C6.1.0	QoS R-Factor calculation for the called side of a session. Populated only if QoS is enabled. This value is reported as * 100 in order to appear as an integer.	153	integer	Stop
Acme-Called-MOS New in Release S-C6.1.0	QoS MOS calculation for the called side of a session. Populated only if QoS is enabled. This value is reported as * 100 in order to appear as an integer.	154	integer	Stop
Acme-Session-Forked-Call-Id New in release S-C6.2.0	The VSA is a string value, and appears as the header-value without the header parameters from the P-Multiring-Correlator header for a session identified as part of a forked call.	171	string	Stop

IPv6 Support

The following table lists the media flow attributes for IPv6 flows.

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Flow-In-Src-IPv6_Addr_FS1_F	Inbound source IPv6 address (remote) information for flow-set 1, forward direction.	155	ipv6addr	• Start • Interim-Update • Stop
Acme-Flow-In-Dst-IPv6_Addr_FS1_F	Inbound destination (local) address information (the IPv6 address field value of the steering pool configuration) for flow-set 1, forward direction.	156	ipv6addr	• Start • Interim-Update • Stop
Acme-Flow-Out-Src-IPv6_Addr_FS1_F	Outbound source (local) address information (the IPv6 address field value of the steering port configuration) for flow-set 1, forward direction.	157	ipv6addr	• Start • Interim-Update • Stop
Acme-Flow-Out-Dst-IPv6_Addr_FS1_F	Outbound destination (remote) IPv6 address information for flow-set 1, forward direction.	158	ipv6addr	• Start • Interim-Update • Stop
Acme-Flow-In-Src-IPv6_Addr_FS1_R	Inbound source IPv6 address (remote) information for flow-set 1, reverse direction.	159	ipv6addr	• Start • Interim-Update • Stop

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Flow-In-Dst-IPv6_Addr_FS1_R	Inbound destination (local) address information (the IPv6 address field value of the steering pool configuration) for flow-set 1, reverse direction.	160	ipv6addr	• Start • Interim-Update • Stop
Acme-Flow-Out-Src-IPv6_Addr_FS1_R	Outbound source (local) address information (the IPv6 address field value of the steering port configuration) for flow-set 1, reverse direction.	161	ipv6addr	• Start • Interim-Update • Stop
Acme-Flow-Out-Dst-IPv6_Addr_FS1_R	Outbound destination (remote) IPv6 address information for flow-set 1, reverse direction.	162	ipv6addr	• Start • Interim-Update • Stop
Acme-Flow-In-Src-IPv6_Addr_FS2_F	Inbound source address (remote) IPv6 information for flow-set 2, forward direction.	163	ipv6addr	• Start • Interim-Update • Stop
Acme-Flow-In-Dst-IPv6_Addr_FS2_F	Inbound destination (local) address information (the IPv6 address field value of the steering pool configuration) for flow-set 2, forward direction.	164	ipv6addr	• Start • Interim-Update • Stop
Acme-Flow-Out-Src-IPv6_Addr_FS2_F	Outbound source (local) address information (the IPv6 address field value of the steering port configuration) for flow-set 2, forward direction.	165	ipv6addr	• Start • Interim-Update • Stop
Acme-Flow-Out-Dst-IPv6_Addr_FS2_F	Outbound destination (remote) IPv6 address information for flow-set 2, forward direction.	166	ipv6addr	• Start • Interim-Update • Stop
Acme-Flow-In-Src-IPv6_Addr_FS2_R	Inbound source address (remote) IPv6 address information for flow-set 2, reverse direction.	167	ipv6addr	• Start • Interim-Update • Stop
Acme-Flow-In-Dst-IPv6_Addr_FS2_R	Inbound destination (local) address information (the IPv6 address field value of the steering pool configuration) for flow-set 2, reverse direction.	168	ipv6addr	• Start • Interim-Update • Stop
Acme-Flow-Out-Src-IPv6_Addr_FS2_R	Outbound source (local) address information (the IPv6 address field value of the steering port configuration) for flow-set 2, reverse direction.	169	ipv6addr	• Start • Interim-Update • Stop
Acme-Flow-Out-Dst-IPv6_Addr_FS2_R	Outbound destination (remote) IPv6 address information for flow-set 2, reverse direction.	170	ipv6addr	• Start • Interim-Update • Stop

Acme Packet VSA Values

The table below defines the possible values for several Acme Packet VSAs.

Acme Packet VSA Name	Attribute Value	Possible Values
Acme-PostDial-Delay	58	Unit value in milliseconds
Acme-Session-Disposition	60	• 0=unknown • 1=call_attempt • 2=ringing • 3=answered
Acme-Disconnect-Initiator	61	• 0=UNKNOWN_DISCONNECT_INITIATOR • 1=CALLING_PARTY_DISCONNECT • 2=CALLED_PARTY_DISCONNECT • 3=INTERNAL_DISCONNECT
Acme-Disconnect-Cause	62	• 34=No circuit/channel available • 47=Resource unavailable • 3=No route destination • 31=Normal, unspecified • 88=Incompatible destination • 111=Interworking, unspecified • 38=Network out of order • 42=Switching equip congestion • 28=Invalid number format • 41=Temporary failure • 17=User busy • 16=Normal call clearing • 20=Subscriber absent • 31=Normal call clearing

Acme Packet VSA Name	Attribute Value	Possible Values
Acme-SIP-Diversion	70	SIP Diversion header based on this RFC draft: draft-levy-sip-diversion-05.txt
Acme-SIP-Status	71	This is a complete list of support status codes; only a subset would be reported in a Stop record: • RESP_STATUS_TRYING 100 • RESP_STATUS_RINGING 180 • RESP_STATUS_FORWARD 181 • RESP_STATUS_QUEUED 182 • RESP_STATUS_PROGRESS 183 • RESP_STATUS_OK 200 • RESP_STATUS_CREATED 201 • RESP_STATUS_ACCEPTED 202 • RESP_STATUS_PART 206 • RESP_STATUS_MAX_OK 299 • RESP_STATUS_MULTIPLE 300 • RESP_STATUS_MOVED 301 • RESP_STATUS_MOVED_TMP 302 • RESP_STATUS_USE_PROXY 305 • RESP_STATUS_ALTERNATE 380 • RESP_STATUS_BAD 400 • RESP_STATUS_UNAUTH 401 • RESP_STATUS_PAY_REQ 402 • RESP_STATUS_FORBIDDEN 403 • RESP_STATUS_NOT_FOUND 404 • RESP_STATUS_NOT_ALLOW 405 • RESP_STATUS_NOT_ACCEPT 406 • RESP_STATUS_AUTH_REQ 407 • RESP_STATUS_REQ_TMO 408 • RESP_STATUS_CONFLICT 409 • RESP_STATUS_GONE 410 • RESP_STATUS_LEN_REQ 411 • RESP_STATUS_TOO_BIG 413 • RESP_STATUS_URI_TOO_BIG 414 • RESP_STATUS_MEDIA 415 • RESP_STATUS_URI_SCHEME 416 • RESP_STATUS_BAD_EXT 420 • RESP_STATUS_EXT_REQ 421 • RESP_STATUS_TOO_SMALL 422 • RESP_STATUS_TOO_BRIEF 423 • RESP_STATUS_TMP_UNAVAIL 480 • RESP_STATUS_NO_EXIST 481 • RESP_STATUS_LOOP 482 • RESP_STATUS_TOOMNY_HOPS 483 • RESP_STATUS_ADDR_INCMPL 484 • RESP_STATUS_AMBIGUOUS 485 • RESP_STATUS_BUSY_HERE 486 • RESP_STATUS_CANCELLED 487 • RESP_STATUS_NOT_HERE 488 • RESP_STATUS_BAD_EVENT 489 • RESP_STATUS_PENDING 491 • RESP_STATUS_UNDECIPH 493 • RESP_STATUS_INT_ERR 500 • RESP_STATUS_NOT_IMPL 501 • RESP_STATUS_BAD_GTWY 502 • RESP_STATUS_SVC_UNAVAIL 503 • RESP_STATUS_GTWY_TMO 504 • RESP_STATUS_BAD_VER 505 • RESP_STATUS_MSG_TOO_BIG 513 • RESP_STATUS_PRE_FAIL 580 • RESP_STATUS_BUSY 600 • RESP_STATUS_DECLINE 603 • RESP_STATUS_DONT_EXIST 604 • RESP_STATUS_NOTACCEPT 606

Authentication VSAs

The table below defines Acme Packet VSAs used for RADIUS authentication.

Acme Packet VSA Name	Attribute Value	Attribute Values
Acme-User-Priviledge	Describes at RADIUS login the privileges granted to the administrator (VSA only available with admin security license installed). Values can be: • sftpForAudit (SFTP is allowed for audit logs) • sftpForAll (SFTP is allowed for logging, and audit logs)	253
Acme-User-Class	Identifies the type user on the Net-Net SBC; used for RADIUS authentication only and does not apply to accounting. Values can be user, admin, and SystemAdmin (only with admin security license installed).	254

Cisco Systems RADIUS Decodes

The following table is a dictionary of the Cisco Systems (vendor identification number is 9) accounting VSAs. These attribute names are vendor-specific and subject to change without notice.

You can use the information in this table to translate the Cisco Systems VSAs that sometimes appear in Net-Net SBC RADIUS messages into a more human-readable form.

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Setup Time	Time that a SIP INVITE or H.323 SETUP message was received. The SETUP message is used to request a connection (and therefore corresponds with the SIP INVITE).	25	string	• Start • Stop
Connect Time	Time that a SIP or H.323 session was accepted. This is the time a 200 OK SIP response to the SIP INVITE message was received or the time that a call ANSWERED/CONNECTED response to the H.323 SETUP message was received.	28	string	• Start • Interim-Update • Stop

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Disconnect Time	Time that a SIP BYE or H.323 Release Complete message was received or the session terminated. This is the time a SIP INVITE or H.323 SETUP transaction terminates for any reason.	29	string	• Stop
Disconnect Cause	SIP Reasons for Disconnection (normal, redirection, client error, network error, global error, time-out, or user abandon) or the H.323 Release Complete Reason code (bad format address, unavailable, destination rejection, adaptive busy, etc.). For more information, refer to this guide's Mappings and Disconnect Cause Values (32) section.	30	string	• Stop

Mappings and Disconnect Cause Values

This section provides information about H.323 and SIP disconnect cause values for RADIUS CDRs generated by the Net-Net SBC.

SIP, H.323, and Q.850 Mappings

This section provides tables that show the mappings between SIP Status and: H.323 Disconnect Reason, H.323 Release Complete Reason, and RAS error. It also shows the mapping for Q.850 cause to H.323 Release Complete Reason.

SIP Status to H.323 Disconnect Reason Mapping

SIP Status	H.323 Disconnect Reason
480 Temporarily Unavailable	No Bandwidth
404 Not Found	Gatekeeper Resource
404 Not Found	Unreachable Destination
603 Decline	Destination Rejection
505 Version Not Supported	Invalid Revision
401 Unauthorized	No Permission
503 Service Unavailable	Unreachable Gatekeeper
480 Temporarily Unavailable	Gateway Resource
400 Bad Request	Bad Format Request
486 Busy Here	Adaptive Busy
486 Busy Here	In Conference
500 Internal Server Error	Undefined Reason

SIP Status	H.323 Disconnect Reason
486 Busy Here	Facility Call Deflection
401 Unauthorized	Security Denied

SIP Status to H.323 RAS Error Mapping

SIP Status	H.323 RAS Error
404 Not Found	Gatekeeper Resource
401 Unauthorized	Invalid Permission
503 Service Unavailable	Request Denied
500 Internal Server Error	Undefined
401 Unauthorized	Caller Not Registered
305 User Proxy	Route Call to Gatekeeper
500 Internal Server Error	Invalid Endpoint ID
503 Service Unavailable	Resource Unavailable
401 Unauthorized	Security Denial
501 Not Implemented	QoS Control Not Supported
484 Address Incomplete	Incomplete Address
302 Moved Temporarily	Route Call to SCN
485 Ambiguous	Aliases Inconsistent
401 Unauthorized	Not Currently Registered

SIP Status to H.323 Release Complete Reason Error Mapping

SIP Status	H.323 RAS Error
300 Multiple Choices	Undefined Reason
401 Unauthorized	Security Denied
402 Payment Required	Undefined Reason
403 Forbidden	No Permission
404 Not Found	Unreachable Destination
405 Method Not Allowed	Undefined Reason
606 Not Acceptable	Undefined Reason
407 Proxy Authentication Required	Security Denied
408 Request Timeout	Adaptive Busy

SIP Status	H.323 RAS Error
409 Conflict	Undefined Reason
410 Gone	Unreachable Destination
411 Length Required	Undefined Reason
414 Request-URI Too Large	Bad Format Address
415 Unsupported Media Type	Undefined Reason
420 Bad Extension	Bad Format Address
480 Temporarily Unavailable	Adaptive Busy
481 Call/Transaction Does Not Exist	Undefined Reason
482 Loop Detected	Undefined Reason
483 Too Many Hops	Undefined Reason
484 Address Incomplete	Bad Format Address

Q.850 Cause to H.323 Release Complete Reason Mapping

The table below describes how the Q.850 Causes and the H.323 release complete reasons are mapped internally on the Net-Net SBC.

Q.850 Cause	Numeric Code	H.323 Release Complete Reason
Not Route To Destination	3	Unreachable Destination
Normal Call Clearing	16	Destination Rejection
User Busy	17	In Conference
Subscriber Absent	20	Called Party Not Registered
Invalid Number Format	28	Bad Format Address
Normal Unspecified	16	Undefined Reason
No Circuit/Channel Available	34	No Bandwidth
Network Out of Order	38	Unreachable Gatekeeper
Temporary Failure	41	Adaptive Busy
Switching Equipment Congestion	42	Gateway Resource
Resource Unavailable	47	Gatekeeper Resource
Incompatible Destination	88	Invalid Revision
Interworking Unspecified	111	No Permission

SIP-SIP Calls

The Net-Net SBC maps SIP status codes and events to disconnect cause attribute values used by Cisco Systems Proxy Server (CSPS) accounting services.

SIP Status Category/Event	CDR Disconnect Cause	Description
Undetermined reason	0	Undetermined reason
BYE	1	Normal clearing
3xx: Redirection	2	Redirection
4xx: Client Error	3	Client error
5xx: Server Error	4	Server error
6xx: Global Failure	5	Global error

SIP-H.323 Calls with Interworking

For calls that require SIP-H.323 interworking, the Net-Net SBC generates two sets of RADIUS CDRs: one for the SIP call-leg and one for the H.323 call leg. The values recorded in RADIUS Stop records for the disconnect cause depend on the nature and source of the call disconnect or rejection.

SIP Events and Errors

For calls rejected or disconnected because of SIP events and errors, the Net-Net SBC records Q.850 cause values mapped from the SIP event/status code in the SIP CDR. For the H.323 CDR, the SIP status categories and events are mapped to Q.850 cause codes.

The entries in this table are determined by the SIP Status to H.323 Release Complete Reason Error Mapping (33).

SIP Status Category/Event	SIP CDR Disconnect Cause	H.323 Disconnect Cause Value (Q.850)
BYE	16—Normal call clearing	16—Normal call clearing
3xx	23—Redirection to new destination	16—Normal call clearing
404 Not Found	21—Call rejected	3—No route to destination
410 Gone	21—Call rejected	3—No route to destination
403 Forbidden	21—Call rejected	111—Interworking unspecified
413 Request Entity Too Big	21—Call rejected	28—Invalid number format
414 Request URI Too Large	21—Call rejected	28—Invalid number format
420 Bad Extension	21—Call rejected	28—Invalid number format
484 Address Incomplete	21—Call rejected	28—Invalid number format
408 Request Timeout	21—Call rejected	41—Temporary failure
480 Temporarily unavailable	21—Call rejected	41—Temporary failure
486 Busy Here	21—Call rejected	17—User Busy

SIP Status Category/Event	SIP CDR Disconnect Cause	H.323 Disconnect Cause Value (Q.850)
401 Unauthorized	21—Call rejected	32—Normal unspecified
407 Proxy Authentication Required	21—Call rejected	32—Normal unspecified
All other 4xx	21—Call rejected	16—Normal unspecified
502 Bad Gateway	38—Network out of order	28—Invalid number format
505 Bad Version	38—Network out of order	88—Incompatible destination
All other 5xx	38—Network out of order	16—Normal unspecified
600 Busy Everywhere	31—Normal unspecified	41—Temporary failure
603 Decline	31—Normal unspecified	31—Normal unspecified
604 Does Not Exist Anywhere	31—Normal unspecified	3—No route to destination
All other 6xx	31—Normal unspecified	31—Normal unspecified

H.323 Events and Errors

The Q.850 cause code value is recorded for the disconnect cause in the CDR for the H.323 call leg if the Q.850 cause is received. H.323 recommendations state that either Q.850 Cause of RelCompReason is mandatory for the RELEASE COMPLETE; the Cause information element (IE) is optional everywhere. The Cause IE and the ReleaseCompleteReason (part of the release complete message) are mutually exclusive.

If a Q.850 cause code is not received, the Net-Net SBC records a Q.850 cause value mapped from the received ReleaseCompleteReason as defined in the table below.

The entries in this table are determined by the SIP Status to H.323 Disconnect Reason Mapping (32).

H.323 ReleaseCompleteReason	H.323 CDR Disconnect Cause	SIP Status	SIP CDR Disconnect Cause
No Bandwidth	34—No channel/circuit available	480 Temporarily Unavailable	21—Call rejected
Gatekeeper Resource	47—Resource unavailable	404 Not Found	21—Call rejected
Unreachable Destination	3—No route to destination	404 Not Found	21—Call rejected
Destination Rejected	31—Normal unspecified	603 Decline	31—Normal unspecified
Invalid Revision	88—Incompatible destination	505 Version Not Supported	38—Network out of order

H.323 ReleaseCompleteReason	H.323 CDR Disconnect Cause	SIP Status	SIP CDR Disconnect Cause
No Permission	111—Interworking unspecified	401 Unauthorized	21—Call rejected
Unreachable Gatekeeper	38—Network out of order	503 Service Unavailable	38—Network out of order
Gateway Resource	42—Switching equipment congestion	480 Temporarily unavailable	21—Call rejected
Bad Format Request	28—Invalid number format	400 Bad request	21—Call rejected
Adaptive Busy	41—Temporary failure	486 Busy Here	21—Call rejected
In Conference	17—User busy	486 Busy Here	21—Call rejected
Undefined Reason	16—Normal unspecified	500 Internal Server Error	38—Network out of order
Called Party Not Registered	20—Subscriber absent	404 Not Found	21—Call rejected
Caller Not Registered	31—Normal call clearing		
New Connection Needed	47—Resource Unavailable	401 Unauthorized	21—Call rejected

H.225 RAS Errors

For calls that are rejected because of H.225 RAS, there is no CDR generated for the H.323 call leg as no Setup message is generated. The Net-Net SBC maps RAS errors to SIP Status as specified in the table below.The SIP CDR disconnect cause values are the same as the CSPS disconnect cause values already mentioned and defined.

The entries in this table are determined by the SIP Status to H.323 RAS Error Mapping (33).

H.225 RAS Error	SIP Status	SIP CDR Disconnect Cause
Called Party Not Registered	404 Not Found	21—Call Rejected
Invalid Permission	401 Unauthorized	21—Call Rejected
Request Denied	503 Service Unavailable	38—Network out of order
Undefined	500 Internal Server Error	38—Network out of order
Caller Not Registered	401 Unauthorized	21—Call Rejected
Route Call to Gatekeeper	305 Use Proxy	23—Redirection to new destination
Invalid Endpoint ID	500 Internal Server Error	38—Network out of order
Resource Unavailable	503 Service Unavailable	38—Network out of order
Security Denial	401 Unauthorized	21—Call Rejected
QoS Control Not Supported	501 Not Implemented	38—Network out of order

H.225 RAS Error	SIP Status	SIP CDR Disconnect Cause
Incomplete Address	484 Address Incomplete	21—Call Rejected
Route Call to SCN	302 Moved Temporarily	2—Redirection
Aliases Inconsistent	485 Ambiguous	21—Call Rejected
Not Currently Registered	401 Unauthorized	21—Call Rejected

2 Configuring Accounting

Overview

This chapter provides you with information about configuring RADIUS accounting on your Net-Net SBC.

The Net-Net products support Net-Net SBC RADIUS accounting, including these essential configurations and specialized features:

- Accounting for SIP and H.323
- Local CDR storage on the Net-Net SBC, including CSV file format settings-
- The ability to send CDRs via FTP to a RADIUS sever
- Per-realm accounting control
- Configurable intermediate period
- RADIUS CDR redundancy
- RADIUS CDR content control

Accounting for SIP and H.323

This section explains SIP and H.323 accounting using the RADIUS Accounting System (RAS).

For accounting purposes, the Net-Net SBC uses RADIUS to send accounting messages. These messages are transmitted to one of a predefined list of accounting servers using a predefined forwarding strategy. RAS provides a mechanism for temporarily storing session initiation and completion statistics and for delivering these statistics to accounting servers located elsewhere in the network.

Call Detail Records

The Net-Net SBC supports CDRs through RADIUS reporting with additional VSAs to include information that is not available with the standard RADIUS session information. CDRs provide billing information on sessions traversed through a system, as well as troubleshooting information, fraud detection, fault diagnostics, and service monitoring.

CDRs can contain information about recent system usage such as the identities of sources (points of origin), the identities of destinations (endpoints), the duration of each call, the amount billed for each call, the total usage time in the billing period, the total free time remaining in the billing period, and the running total charged during the billing period.VSAs are defined by vendors of remote access servers in order to customize how RADIUS works on their servers.

RAS Overview

The RAS acts as a RADIUS client. It provides a mechanism for generating accounting information in CDRs. The CDRs are transmitted to a RADIUS server in UDP datagrams, using RADIUS Accounting Request messages.

The RAS receives RADIUS accounting messages when different events occur. The event and CDR event trigger list information determines which RADIUS messages,

if any, are included, as well as which RADIUS attributes are included. The library adds RADIUS messages to the waiting queue only when the message is ready to be sent. The SIP proxy needs to populate the CDR as session information becomes available so, by the time the session ends, it contains the information necessary to generate all of the messages.

The RADIUS accounting client process manages its queue and a list of servers. The servers each have a UDP connection and manage their own pending message queues. Changes in the state of the server connection might cause interaction with the client process waiting queue.

When RADIUS messages are added to the RAS waiting queue, the RAS sends them to a server based on strategy. If the RAS is configured to transmit all the messages when the session ends, all the messages are sent to the same server. Each session continues logging messages according to the event logging scheme in effect when the session began (for example, when the CDR was created).

The RAS notifies the RADIUS server with Accounting-On/Off messages when the RAS's entry for that server is enabled/disabled. The response to the Accounting-On message is the RAS's first determination of RTT, and serves as notification that the server is reachable. Until the Accounting-On response is received, the server cannot send other messages.

RADIUS Accounting Client

The RADIUS accounting client process has a local socket at which it accepts RADIUS messages. RADIUS messages received on the local socket are added to the waiting queue for transmission to a RADIUS server. The waiting queue is a first-in, first-out (FIFO) queue.

The RADIUS accounting client process sends messages to a server queue based on the configuration (servers configured/enable/connected, as well as the strategy). Messages that return from a server (due to server failure/disabling) are first in the FIFO queue.

The RADIUS accounting client process interfaces with the RADIUS accounting servers using the RADIUS protocol with the VSAs outlined above.

The RADIUS server collects a variety of information that can be used for accounting and for reporting on network activity. The RADIUS client sends information to designated RADIUS servers when the user logs on and logs off. The RADIUS client might send additional usage information on a periodic basis while the session is in progress. The requests sent by the client to the server to record logon/logoff and usage information are generally called accounting requests.

RADIUS accounting permits a RADIUS server to track when users commence and terminate their connections. Typical accounting information includes the following:

- Full user name
- RAS identification name or IP address
- RAS port number
- Time connection started

When a client is configured to use RADIUS accounting, it generates an Accounting Start packet describing the type of service being delivered and the user it is being delivered to at the start of service delivery. It sends that packet to the RADIUS Accounting server, which sends back an acknowledgement that the packet has been received. At the end of service delivery, the client generates an Accounting Stop

packet describing the type of service that was delivered and, optionally, statistics such as elapsed time, input and output octets, or input and output packets. It sends that packet to the RADIUS Accounting server, which sends back an acknowledgement that the packet has been received. The Accounting-Request (whether for Start or Stop) is submitted to the RADIUS accounting server through the network.

Transactions between the client and RADIUS accounting server are authenticated through the use of a shared secret, which is never sent over the network.

Session Accounting

The RAS client can record SIP, H.323, and IWF session activity based on configuration and a CDR. The CDR determines which messages are generated and determines the RADIUS attributes included in the messages. The RAS client must be capable of sending CDRs to any number of RADIUS accounting servers, using the defined hunt, failover, round robin, fewest pending, or fastest server strategies.

The establishment, failed establishment, change, or removal of a session can trigger RADIUS Accounting Request messages. The RAS might also send notification of its status (enabled/disabled). RADIUS Accounting Request messages include the following:

- Start—Session has started.
- Interim-Update—Session parameters have changed.
- Stop—Session has ended.
- Accounting-On—Creation of a new RADIUS client.
- Accounting-Off—RADIUS client has shut down.

Each session might generate Start, Interim-Update, and Stop messages based on the local configuration when the session is initiated. Each Start message tells the RADIUS server that a session has started. Each Interim-Update message changes the session parameters, and may report the session characteristics for the session to that point. Each Stop message informs the RADIUS server that a session has ended and reports session characteristics.

The RAS has the ability to transmit all RADIUS messages related to a session at the end of the session, regardless of which messages are generated and when they are generated. Some customers might choose this option to reduce the likelihood of the RADIUS messages being logged to different servers, or in different log files on the same server.

The RAS always generates a RADIUS Stop message when the session ends, regardless of the session termination cause. The termination cause and the session characteristics are reported.

RADIUS Messages

The following table identifies the relationship between the signaling elements and the RADIUS attributes included in Accounting Request messages to the RADIUS server.

RADIUS Attribute	Data Element	Message
NAS IP-Address	IP address of the SIP proxy or the H.323 stack's call signal address.	Start, Interim-Update, Stop, On, Off
NAS Port	SIP proxy port or the H.323 stack's call signaling RAS port.	Start, Interim-Update, Stop, On, Off
NAS Identifier	Value, if any, set in the optional `NAS-ID` field for the accounting server that you configure as part of the accounting configuration. This identifier sets the value that the remote server (the accounting server) uses to identify the Net-Net SBC so that RADIUS messages can be transmitted. The remote server to which the accounting configuration will send messages uses at least one of two pieces of information for identification: • NAS IP address: always included in the accounting message • NAS identifier: configured in the NAS-ID parameter of the accounting server; if configured, the NAS identifier is sent to the remote server This attribute only appears if a value is configured in the NAS-ID field.	Start, Interim-Update, Stop, On, Off
Acct-Session-ID	Either the "Call-ID" field value of the SIP INVITE message, the `callIdentifier` of the H.323 message, or RADIUS client information.	Start, Interim-Update, Stop, On, Off
Called Station ID	"To" field value of the SIP INVITE message (a type of message used to initiate a session) or the `calledPartyNumber` of the H.323 message.	Start, Interim-Update, Stop
Calling Station ID	"From" field value of the SIP INVITE message or the `callingPartyNumber` of the H.323 message.	Start, Interim-Update, Stop
Acct-Terminate-Cause	Reason for session ending (refer to Session Termination session).	Stop, Off
Acct-Session-Time	Length of session (time in seconds).	Interim-Update, Stop, Off

Session Termination

Sessions are terminated for reasons that include normal termination, signaling failure, timeout, or network problems. The following table maps RADIUS accounting termination cause codes to network events.

RADIUS Termination Cause	Event	Message
User request	SIP BYE message or H.323	Stop
User error	SIP signaling failed to establish session (accompanied by disconnect cause)	Stop
NAS request	RADIUS server disabled	Off

ACLI Instructions and Examples

This section tells you how to access and set parameters for RADIUS accounting support. To use the Net-Net SBC with external RADIUS (accounting) servers to generate CDRs and provide billing services requires, you need to configure account configuration and account server list.

Accessing the Accounting and Accounting Servers Configuration

To configure the account configuration and account servers:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter> to access the system-level configuration elements.

   ```
   ACMEPACKET(configure)# session-router
   ```

3. Type **account-config** and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.

   ```
   ACMEPACKET(session-router)# account-config
   ACMEPACKET(account-config)#
   ```

4. To configure account server parameters (a subset of the account configuration parameters, type **account-servers** and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.

   ```
   ACMEPACKET(account-config)# account-servers
   ACMEPACKET(account-server)#
   ```

Setting Up the Account Configuration

You set the account configuration parameters to indicate where you want accounting messages sent, when accounting messages you want them sent, and the strategy you want used to select account servers.

To configure the account configuration:

1. **hostname**—Defaults to and must remain `localhost`.
2. **port**—Retain the default value of 1813 or enter the number of the UDP port associated with the Net-Net SBC from which RADIUS messages are sent.
   - minimum: 1025
   - maximum: 65535

3. **strategy**—Indicate the strategy you want used to select the accounting servers to which the Net-Net SBC will send its accounting messages. The following table lists the available strategies:

Strategy	Description
hunt	Selects accounting servers in the order in which they are listed. If the first accounting server is online, working, and has not exceeded any of the defined constraints, all traffic is sent to it. Otherwise the second accounting server is selected. If the first and second accounting servers are offline or exceed any defined constraints, the third accounting server is selected. And so on through the entire list of configured servers
failover	Uses the first server in the list of predefined accounting servers until a failure is received from that server. Once a failure is received, it moves to the second accounting server in the list until a failure is received. And so on through the entire list of configured servers.
round robin	Selects each accounting server in order, distributing the selection of each accounting server evenly over time.
fastest round trip time	Selects the accounting server that has the fastest round trip time (RTT) observed during transactions with the servers (sending a record and receiving an ACK).
fewest pending	Selects the accounting server that has the fewest number of unacknowledged accounting messages (that are in transit to the Net-Net SBC).

4. **state**—Retain the default value **`enabled`** if you want the account configuration active on the system. Enter **`disabled`** if you do not want the account configuration active on the system.
5. **max-msg-delay**—Retain the default value of **`60`** seconds or indicate the length of time in seconds that you want the Net-Net SBC to continue trying to send each accounting message. During this delay, the Net-Net SBC can hold a generic queue of 4096 messages.
   - Minimum: zero (0)
   - Maximum: 2^{32}-1
6. **max-wait-failover**—Retain the default value of **`100`** messages or indicate the maximum number of accounting messages the Net-Net SBC can store its message waiting queue for a specific accounting server, before it is considered a failover situation.

   Once this value is exceeded, the Net-Net SBC attempts to send it accounting messages, including its pending messages, to the next accounting server in its configured list.
   - Minimum: one (1) message
   - Maximum: 4096 messages
7. **trans-at-close**—Retain the default value of **`disabled`** if you do not want to defer the transmission of message information to the close of a session. Enter **`enabled`** if you want to defer message transmission.
   - **`disabled`**—The Net-Net SBC transmits accounting information at the start of a session (Start), during the session (Interim), and at the close of a session

(Stop). The transmitted accounting information for a single session might span a period of hours and be spread out among different storage files.

- **enabled**—Limits the number of files on the Net-Net SBC used to store the accounting message information for one session. It is easiest to store the accounting information from a single session in a single storage file.

8. **generate-start**—Retain the default value **ok** if you want the RADIUS Start message to be generated once the Net-Net SBC receives an OK message in response to an INVITE. (A RADIUS Start message informs the accounting server that a SIP session has started.)

   Other options include:

   - Start—RADIUS Start message should not be generated.
   - Invite—RADIUS Start message should be generated once the Net-Net SBC receives a SIP session INVITE.

9. **generate-interim**—Retain the default value **reinvite response** to cause the Net-Net SBC to transmit a RADIUS Interim message. (A RADIUS Interim message indicates to the accounting server that the SIP session parameters have changed.)

   You can select none, one, or more than one of the following values:

Option	Description
ok	RADIUS Start message is generated when the Net-Net SBC receives an OK message in response to an INVITE.
reinvite	RADIUS Interim message is generated when the Net-Net SBC receives a SIP session reINVITE message.
reinvite response (default)	RADIUS Interim message is generated when the Net-Net SBC receives a SIP session reINVITE and responds to it (for example, session connection or failure).
reinvite cancel	RADIUS Interim message is generated when the Net-Net SBC receives a SIP session reINVITE, and the Reinvite is cancelled before the Net-Net SBC responds to it.
unsuccessful-attempt	RADIUS Interim message is generated when a SIP session set-up attempt from a preference-ordered list of next-hop destinations is unsuccessful. This can happen when a local policy lookup, LRT lookup, ENUM query response, or SIP redirect returns a preference-ordered list of next-hop destinations. The interim message contains: the destination IP address, the disconnect reason, a timestamp for the failure, and the number that was called.

10. **account-server**—Create the account server list to store accounting server information for the account configuration. Each account server can hold 100 accounting messages. See the next section for step-by-step instructions.

    Account server entries are specific to the account configuration. They cannot be viewed or accessed for editing outside of the account configuration.

    Note: RADIUS will not work if you do not enter one or more servers in a list.

Setting Up Accounting Servers

You must establish the list of servers to which the Net-Net SBC can send accounting messages.

1. **hostname**—Name of the host associated with the account server in hostname format (FQDN) or as an IP address.
2. **port**—Retain the default `1813` or enter the number of the UDP port associated with the account server to which RADIUS messages are sent.
   - minimum: 1025
   - maximum: 65535
3. **state**—Retain the default `enabled` to enable the account servers on the system or enter `disabled` to disable them.
4. **min-round-trip**—Retain the default `250` milliseconds or indicate the minimum round trip time of an accounting message.
   - minimum: 1025 milliseconds
   - maximum: 65535 milliseconds

   A round trip consists of the following:
   – The Net-Net SBC sends an accounting message to the account server.
   – The account server processes this message and responds back to the Net-Net SBC.

   If the fastest RTT is the strategy for the account configuration, the value you enter here can be used to determine an order of preference (if all the configured account servers are responding in less than their minimum RTT).
5. **max-inactivity**—Retain the default `60` seconds or indicate the length of time in seconds that you want the Net-Net SBC with pending accounting messages to wait when it has not received a valid response from the target account server.
   - minimum: 1 second
   - maximum: 300 seconds

   Once this timer value is exceeded, the Net-Net SBC marks the unresponsive account server as disabled in its failover scheme. When a server connection is marked as inactive, the Net-Net SBC attempts to restart the connection and transfers pending messages to another queue for transmission. RADIUS messages might be moved between different account servers as servers become inactive or disabled.
6. **restart-delay**—Retain the default `30` seconds or indicate the length of time in seconds you want the Net-Net SBC to wait before resending messages to a disabled account server.
   - minimum: 1 second
   - maximum: 300 seconds
7. **bundle-vsa**—Retain the default `enabled` if you want the account server to bundle the VSAs within RADIUS accounting messages. Enter `disabled` if you do not want the VSAs to be bundled. (Bundling means including multiple VSAs within the vendor value portion of the message.)

   In a bundled accounting message, the RADIUS message type is vendor-specific, the length is determined for each individual message, and the vendor portion begins with a 4-byte identifier, and includes multiple vendor type, vendor length, and vendor value attributes.
8. **secret**—Enter the secret passed from the account server to the client in text format. Transactions between the client and the RADIUS server are authenticated by the shared secret; which is determined by the source IPv4 address of the received packet.

9. **NAS-ID**—*Optional.* Enter the NAS ID in text format (FQDN allowed). The account server uses this value to identify the Net-Net SBC for the transmittal of accounting messages.

   The remote server to which the account configuration sends messages uses at least one of two potential pieces of information for purposes of identification. The Net-Net SBC accounting messages always includes in the first of these:

   - Network Access Server (NAS) IP address (the IP address of the Net-Net SBC's SIP proxy)
   - NAS ID (the second piece of information) provided by this value. If you enter a value here, the NAS ID is sent to the remote server.

     If you have more than one Net-Net SBC pointing to the same account server, the NAS ID can be used to identify which Net-Net SBC generated the record.

Per Realm Accounting Control

You can enable or disable accounting control for specific realms by setting one parameter. This feature is enabled by default.

The Net-Net SBC's SIP and H.323 tasks check whether this parameter is set to enabled or disabled, and sends record on that basis.

ACLI Instructions and Examples

To configure per realm accounting:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# media-router
   ```

3. Type **realm-config** and press <Enter>.

   ```
   ACMEPACKET(media-router)# realm-config
   ```

4. **accounting-enable**—Either leave this parameter set to `enabled` (default) to generate CDRs for this realm, or change it to `disabled`.
5. Save and activate your configuration.

Configurable Intermediate Period

You can set how often the Net-Net SBC generates periodic interim records for H.323 and for SIP.

- H.323—The periodic timer (set to the value you specify in the accounting configuration) is dynamically created when the Net-Net SBC receives a Connect message and an H.323 call answer method is invoked. The Net-Net SBC deletes the timer when the H.323 session is terminated.
- SIP—The periodic timer (set to the value you specify in the accounting configuration) is dynamically created when the Net-Net SBC receives a a 200 OK response to an INVITE message. The Net-Net SBC deletes the timer when the session is terminated.

To set the timer for periodic interim records:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ```

3. Type **account-config** and press <Enter>.

   ```
   ACMEPACKET(session-router)# account-config
   ```

4. **intermediate-period**—Enter amount of time in seconds between generating periodic interim records during a SIP or H.323 call. This parameter defaults to zero, which is not a valid value.

5. Save and activate your configuration.

RADIUS CDR Content Control

The Net-Net SBC's RADIUS support has been enhanced so that you can limit the size of RADIUS CDRs. The Net-Net SBC's RADIUS accounting provides a detailed set of records that can contain, for example, multiple media flow descriptions for forked calls that can contain multiple sets of media and QoS attributes. While the level of detail might be required for some networks, in others the large CDRs generated to reflect that level of granularity can cause issues for the application receiving the records.

You can use the following enhancements to control the size of the RADIUS CDRs your Net-Net SBC produces:

- Duplicate RADIUS attribute prevention—Using this feature, you can configure the Net-Net SBC to send only one set of RADIUS attributes in CDR for a forked call. (When a forked SIP INVITE contains media information, media and QoS attributes can potentially be duplicated.)
- RADIUS attribute selection—You can set a list of the Acme Packet VSAs you want included in a RADIUS CDR, and the Net-Net SBC will exclude the others from the record; standard attributes are always included. You specify attributes using their unique identifier in a comma-delimited list, and you can list them in any order. However, entering an invalid range disables this feature.

  The Net-Net SBC excludes attributes from the records in which they are already defined. If an attributes only appears in a Stop record, then it will be deleted from Stop records.

  The configuration provides a mechanism to make entries flexible and easy.

ACLI Instructions and Examples

You enable these enhancements using two parameters in the accounting configuration.

Accessing the Accounting Configuration

To access the accounting configuration:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ```

3. Type **account-config** and press <Enter>.

   ```
   ACMEPACKET(session-router)# account-config
   ```

   From this point, you can reach the individual parameters for duplicate RADIUS attribute prevention and for RADIUS attribute selection.

Preventing Duplicate RADIUS Attributes

To enable duplicate RADIUS attribute prevention:

1. **prevent-duplicate-attrs**—Change this parameter from `disabled` (default) to `enabled`.

   ```
   ACMEPACKET(account-config)# prevent-duplicate-attrs enabled
   ```

2. Save and activate your configuration.

RADIUS Attribute Selection

You enter the list of VSAs that you want included as a comma-delimited list. There are special entry types you can use in the comma-delimited list to set ranges and make entries easier:

- `X-` — Where X is a VSA identifier, the Net-Net SBC will include all attributes with an identifier equal to or greater than `X`.
- `-X` — Where X is a VSA identifier, the Net-Net SBC will include all attributes with an identifier equal to or less than `X`.
- `-` — Use the minus sign (-) alone when you want to turn off attribute selection, including all VSAs in the CDR.

To enter a list of RADIUS attributes to include in a CDR:

1. **vsa-id-range**—Enter a comma-delimited list that represents the VSA you want to appear in the RADIUS CDR. There is no default for this parameter.

   Do not use <Spaces> when typing in your comma-delimited list.

   ```
   ACMEPACKET(account-config)# vsa-id-range -5,7,10-
   ```

   This entry specifies that CDRs contain VSA with identifiers equal to and less than 5, VSA 7, and VSAs with identifiers equal to and greater than 10.

2. Save and activate your configuration.

Custom RADIUS CDR VSAs for SIP

This section describes these additions to the Net-Net SBC's RADIUS accounting capabilities for customizing your call detail records (CDRs):

- Generating CDRs with call detail information from a SIP message—The Net-Net SBC reserves a set of vender-specific attributes (VSAs) and then populates them according to your header manipulation (HMR) configuration
- Generating CDRs with trunk group information—You can enable your Net-Net SBC to provide terminating trunk-group and trunk-context data even when the Net-Net SBC is not performing trunk-group routing.

Both support using the CSV file for RADIUS records, which you can either save locally or push to a defined FTP server.

About User-Defined VSAs for SIP Calls

The Net-Net SBC reserves VSAs 200-229 for you to define for use with SIP calls. These VSAs should never be used for other purposes, and their use should never conflict with the need to add new VSAs in the future. Because this leaves a significant number of VSAs unused, there is still ample space for any new VSAs that might be required.

Since RADIUS START records are created on session initiation, their content cannot be updated. However, the content for INTERIM and STOP records can be.

To configure user-defined VSAs for a SIP call, you use HMR. For example, when you set up HMR correctly, the Net-Net SBC reports originating or terminating country

codes in CDRs in whatever format they appear in the SIP username field. The HMR rules you configure uses the SIP header name P-Acme-VSA, adding it to the SIP header from any part of the SIP message. Then the Net-Net SBC searches for the P-Acme-VSA header, generates a VSA for it, and then includes that VSA in the CDR for the call.

You can include multiple custom VSAs per CDR by adding the corresponding number of rules; in essence, you add in the header as many times as required.

HMR Adaptations

The following HMR element rule types support user-defined VSA for SIP calls:

- **uri-user-only**—The **uri-user-only** element rule type represents the URI username without the URI user parameters. You can perform these actions for the **uri-user-only** type: store, replaces, delete, and add. This means, for example, that you can add a username string to SIP or TEL URI without having any impact on other parameters.
- **uri-phone-number-only**—The **uri-phone-number-only** applies when all rules are met. It refers to the user part of the SIP/TEL URI without the user parameters when the user qualifies for the BNF shown here:

```
uri-phone-number-only   =   [+]1*(phone-digit / dtmf-digit / pause-character)
phone-digit             =   DIGIT / visual-separator
DIGIT                   =   "0" / "1" / "2" / "3" / "4" / "5" / "6" / "7" / "8" / "9"
visual-separator        =   "-" / "." / "(" / ")"
dtnf-digit              =   "*" / "#" / "A" / "B" / "C" / "D"
pause-character         =   "p" / "w"
```

  Once the URI user part qualifies as a uri-phone-number-only based on this BNF, the Net-Net SBC ignores the visual separators when comparing it against a match value. Furthermore, the Net-Net SBC performs on or using the uri-phone-number-only after the excluding the visual separators.

  But anew value being added as a uri-phone-number-only or replacing a uri-phone-number-only does not have to match the BNF noted above. That is, you can use the **uri-phone-number-only** type knowing that:

  - The action only occurs if the URI username matches the BNF defined here.
  - Even so, you can also replace the uri-phone-number-only with one that does not match—using the same rule.

HMR String Variable

HMR supports the use of a string variable that you can use to populate headers and elements. You set this value in the **hmr-string** parameter for a realm, SIP session agent, or SIP interface. Then, you reference it as the $HMR_STRING variable.

When a message arrives, the Net-Net SBC matches the string you provision to the closest session agent, realm, or SIP interface. The precedence for matching is in this order: session agent, realm, and then SIP interface. For example, the Net-Net SBC populates messages matching a session agent using the $HMR_STRING variable, but it leaves the value empty for session agents that do not match.

You can use the string variable, for instance, for values specific to realms and session agents such as country code values when the regular expression pattern used to match a country code fails to do so.

ACLI Instructions and Examples: User-Defined VSAs

This section shows you how to configure user-defined VSAs for SIP calls. It also contains subsections with configuration examples so you can see how this feature is put to use.

This section also shows you two configuration examples for this feature.

To create a header manipulation rule that generates user-defined VSAs for SIP calls:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)#
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type **sip-manipulation** and press <Enter>.

   ```
   ACMEPACKET(session-router)# sip-manipulation
   ACMEPACKET(sip-manipulation)#
   ```

4. Type **header-rules** and press <Enter>.

   ```
   ACMEPACKET(session-router)# header-rules
   ACMEPACKET(sip-header-rules)#
   ```

5. **name**—Enter a meaningful name for the header rule you are creating. For example, if you want to add VSA 200 to your CDRs for SIP calls, you might name your rule **generateVSA200**. There is no default for this parameter, and it is required.
6. **header-name**—Set this parameter to P-Acme-VSA so the Net-Net SBC will add this accounting information to CDRs for the call.
7. **action**—Set this parameter to **add**.
8. **new-value**—Enter the regular expression value for the new value you want to add. For example, to add VSA 200 that contains the value from the SIP From header, you would enter **200:+$storeFrom.$0**.
9. Save and activate your configuration.

The first example shows you how to generate custom VSA for the To and From headers in SIP messages.

- VSA 200 contains the header value from the SIP From header.
- VSA 220 contains the header value from the SIP To header.

```
sip-manipulation
        namecustom                          VSA1
        description
        header-rule
                name                        storeFrom
                header-name                 from
                action                      store
                comparison-type             pattern-rule
                match-value                 .*
                msg-type                    request
                new-value
                methods                     INVITE
        header-rule
                name                        storeTo
                header-name                 to
                action                      store
                comparison-type             pattern-rule
```

```
                match-value                     .*
                msg-type                        request
                new-value
                methods                         INVITE
        header-rule
                name                            generateVSA200
                header-name                     P-Acme-VSA
                action                          add
                comparison-type                 case-sensitive
                match-value
msg-type                        any
                new-value                       200:+$storeFrom.$0
                methods                         INVITE
        header-rule
                name                            generateVSA220
                header-name                     P-Acme-VSA
                action                          add
                comparison-type                 case-sensitive
                match-value
                msg-type                        any
                new-value                       220:+$storeTo.$0
                methods                         INVITE
```

The second example shows you how to configure HMR to generate VSA 225, which contains the customer P_From header when it is present. When that header is not present, the rule instructs the Net-Net SBC to include the header value from the SIP From header for VSA 225.

```
sip-manipulation
        name                                    customVSA1
        description
        header-rule
                name                            storePfrom
                header-name                     P_From
                action                          store
                comparison-type                 pattern-rule
                match-value                     .*
                msg-type                        request
                new-value
                methods                         INVITE
        header-rule
                name                            storeFrom
                header-name                     from
                action                          store
                comparison-type                 pattern-rule
                match-value                     .*
                msg-type                        request
                new-value
methods                         INVITE
        header-rule
                name                            generateVSA225_1
                header-name                     P-Acme-VSA
                action                          add
                comparison-type                 case-sensitive
                match-value
```

```
                msg-type                        request
                new-value                       225:+$storeFrom.$0
                methods                         INVITE
        header-rule
                name                            generateVSA225_2
                header-name                     P-Acme-VSA
                action                          manipulate
                comparison-type                 pattern-rule
                match-value                     $storePfrom
                msg-type                        request
                new-value
                methods                         INVITE
element-rule
                        name                            one
                        parameter-name
                        type                            header-value
                        action                          delete-element
                        match-val-type                  any
                        comparison-type                 pattern-rule
                        match-value                     ^225.*
                        new-value
        element-rule
                        name                            two
                        parameter-name
                        type                            header-value
                        action                          add
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                    new-value                       225:+$storePfrom.$0
```

ACLI Instructions and Examples: String Variable

To use the HMR string variable, you set the **hmr-string** value in the SIP session agent, realm, or SIP interface where you want the feature applied. The following sample shows you how to configure the **hmr-string** parameter for SIP session agent.

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)#
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type **session-agent** and press <Enter>.

   ```
   ACMEPACKET(session-router)# session-agent
   ACMEPACKET(session-agent)#
   ```

   If you are adding this feature to an existing configuration, you need to select the configuration (using the ACLI **select** command) before making your changes.

4. **manipulation-string**—Enter a value that references the $HMR_STRING variable that will be used to populate SIP headers and elements using HMR. There is no default value for this parameter.

5. Save and activate your configuration.

Trunk-Group VSA Generation

You can force the Net-Net SBC to generate VSAs related to trunk groups even when you are not using the trunk group feature. With the **force-report-trunk-info** parameter turned on in the session router configuration:

- The Net-Net SBC reports terminating trunk group and trunk-context information even though it has not perform trunk-group routing.

  The appropriate VSAs report the terminating trunk-group (VSA 65) and trunk context (VSA 67) with the information of the matching ingress session agent and realm of the originator.

- The Net-Net SBC reports the terminating trunk-group (VSA 66) and trunk context (VSA 68) as the received trunk group and context from the call's SIP REQUEST message. If the SIP message has none, then the Net-Net SBC uses the information from the matching egress session agent (or egress realm, when available) and next-hop realm.

  Note that information is reported after HMR processing—meaning that header manipulation has been performed on the message information reported.

ACLI Instructions and Examples

You enable trunk-group VSA generation on a system-wide basis in the session-router configuration.

To enable forced trunk-group VSA generation:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)#
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type **session-agent** and press <Enter>.

   ```
   ACMEPACKET(session-router)# session-router
   ACMEPACKET(session-router)#
   ```

4. **forced-report-trunk-info**—Change this parameter to enabled if you want to turn on the Net-Net SBC's ability to generate VSAs for trunk group information even when you are not using trunk-group routing. The Net-Net SBC uses VSAs 65-68 to report originating and terminating trunk group information as described in the Trunk-Group VSA Generation (54) section above. By default, this parameter is **disabled**.

5. Save and activate your configuration.

RADIUS Account Server Prioritization

Especially useful for customers with multiple Net-Net SBCs, the RADIUS account server prioritization feature allows you to assign a priority to each of the account servers you configure. Setting the priority for RADIUS accounting servers allows you to load balance traffic across the servers.

Without this feature, the Net-Net SBC sorts RADIUS accounting servers by their IP addresses and ports. For example, if you have a pre-existing accounting server with the IP address and port combination of 10.1.31.2:1813 and then configure a new server at 10.0.3.12:2145, the new server will take priority over the pre-existing one. Of course, you always have the option of allowing the system to set the priority or your accounting servers in this way.

The prioritization feature works with all of the strategy types you set in the accounting configuration. However, it is most applicable to the **hunt** or **failover** strategies. You can assign a number to each server to mark its priority, or you can leave the priority parameter set to 0 (default) so the Net-Net SBC prioritizes them by IP address and port.

How You Might User Server Prioritization

This example shows you how you can might benefit from using the prioritization feature if you have multiple Net-Net SBCs sending RADIUS CDRs to multiple RADIUS servers. Consider the following Net-Net SBCs and accounting servers.

Net-Net SBC	Account Server1 Priority	Account Server2 Priority	Account Server3 Priority
Net-Net SBC1	10	7	4
Net-Net SBC2	7	4	10
Net-Net SBC3	4	10	7
Net-Net SBC4	10	7	4
Net-Net SBC5	7	4	10
Net-Net SBC6	4	10	7

If the strategy for this example is set to **hunt** or **failover** and assuming no timeouts are pending, you can see that Net-Net SBC1 sends its accounting traffic to Account Server3 over the other two. Net-Net SBC2 sends its traffic to Account Server2 over the others, and likewise for the remainder of Net-Net SBCs and servers. The traffic, then, is load balanced across the servers, less likely to overburden any of them.

ACLI Instructions and Examples

This section shows you how set the priority for an account server.

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)#
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type **account-config** and press <Enter>.

   ```
   ACMEPACKET(session-router)# account-config
   ACMEPACKET(account-config)#
   ```

4. Type **account-server** and press <Enter>.

   ```
   ACMEPACKET(session-router)# account-server
   ACMEPACKET(account-server)#
   ```

5. **priority**—Enter the number corresponding to the priority you want this account server to have in relation to the other account servers to which you send traffic. The default for this parameter is 0, meaning the prioritization feature is turned off—and that the Net-Net SBC will therefore prioritize accounting servers by IP address and port. Otherwise, you can use any numbering scheme that suits your needs and ease of use.

6. Save and activate your configuration.

Accounting Configuration Example

Using the Net-Net SBC with external RADIUS accounting servers to generate CDRs and provide billing services requires you to configure accounting configuration and any associated accounting servers you might need.

The following example shows how you can set accounting configuration and accounting server parameters to support multiple RADIUS accounting servers.

```
ACMEPACKET(account-config)# show
       account-config
              hostname                      localhost
              port                          1813
              strategy                      Hunt
              state                         enabled
              max-msg-delay                 60
              max-wait-failover             100
              trans-at-close                disabled
              file-output                   enabled
              max-file-size                 1000000
              max-files                     5
              file-path                     /ramdrv
              file-rotate-time              60
              ftp-push                      enabled
              ftp-address                   154.0.12.4
              ftp-port                      21
              ftp-user                      Admin
              ftp-password                  A213HG
              ftp-remote-path               /sdRADIUS
              cdr-output-redundancy         enabled
              generate-start                OK
              generate-interim
                                            Reinvite-Response
              intermediate-period           0
              prevent-duplicate-attrs       disabled
              vsa-id-range
              cdr-output-inclusive
       account-server
                     hostname                      10.0.0.189
                     port                          1813
                     state                         enabled
                     min-round-trip                250
                     max-inactivity                60
                     restart-delay                 30
                     bundle-vsa                    enabled
                     secret                        acme
                     NAS-ID
                     priority                      0
        account-server
                     hostname                      192.168.200.70
                     port                          5050
                     state                         enabled
                     min-round-trip                250
                     max-inactivity                60
                     restart-delay                 30
```

```
bundle-vsa                    enabled
secret                        packet
NAS-ID
priority
```

Local CDR Storage and FTP Push

The local CDR storage feature allows you to save RADIUS CDR data to a local CSV text file on the Net-Net SBC. Local CDR file creation and storage can be used in addition to or independently of sending CDRs to RADIUS servers for every call. Once the Net-Net SBC creates and saves local CDR files, you can:

- Send the files to an FTP server by configuring a push receiver
- Develop and implement your own script for retrieving them as necessary from the Net-Net SBC

You configure the Net-Net SBC to:

- Set directory path where you want to save local CDR files
- Set a maximum file size for the CSV file
- Set a maximum number of local CDR files
- Set an interval in which to close the existing local CDR file and begin writing a new file.

Once local CDR file creation is enabled, you can configure push receivers to "push" any non-active and closed CDR files to an FTP server using FTP or SFTP protocols. You configure the Net-Net SBC with the push receiver's:

- server IP address and port information
- login credentials
- path to save the local CDR Files
- The interval at which the Net-Net SBC should send files to a push reciever

For flexibility and security, the Net-Net SBC can log into a push reciever with either FTP or SFTP. If you are creating a secure connection with SFTP, your Net-Net SBC can authenticate to the server with either a public shared key or SSH-encrypted username and password.

Local CDR File Format

The CDRs are written as comma-delimited ASCII records to files on the Net-Net SBC. The types of records are controlled by the same accounting configuration parameters used for RADIUS. The fields of the comma-delimited entries correspond to RADIUS START, INTERIM, and STOP records. Using the accounting configuration, you can configure the Net-Net SBC to record STOP records only.

Because the record types do not have consistent field positioning, any server parsing them would need to read the first field to determine the type and learn how to parse the remaining fields.

Local CDR File Format Consistency

Unpopulated or unused fields in the RADIUS CDR are omitted from the locally-stored CSV file. This means that there is no fixed position for a RADIUS attribute across all CSV files. Instead, the missing values are skipped in the CSV file so that the order and appearance for attribute values can differ from record to record.

You can optionally guarantee the placement of attributes in locally-stored CSV files with the **CDR output inclusive** parameter. With this enhancement enabled,

RADIUS records sent to a RADIUS client contain even empty attributes with an integer, date and time, or IP address format; the default value is zero. In other words, when there is no value to report:

- An IP address attribute will report as `0.0.0.0`
- A date and time attribute will report as `00:00:00.000 UTC JAN 01 1970`
- An integer attribute value will report as `0`

To maintain RFC 2865 and 2866 compliance, the Net-Net SBC will not send empty attributes that are string values to a RADIUS client. And when you enable this feature, the Net-Net SBC adds all attributes to the locally-stored CSV file.

Refer to Appendix B (107) of this document for details about where in locally-generated CSV file VSAs appear for Start, Interim, and Stop records.

Requirements

If you want to guarantee the CSV placement for RADIUS attribute values, you must use the entire RADIUS dictionary. You cannot use the RADIUS CDR abbreviation feature. Using an abbreviated form of the RADIUS dictionary results in adverse effects for the CSV file.

In your configuration, then, you must set the **vsa-id-range** parameter to use the entire range of attributes. Leaving this parameter blank disables abbreviation and all attributes are included. Alternatively, you can specify all of the parameters (by attribute number) that are used in the Net-Net OS release loaded on your system.

See the RADIUS CDR Content Control (48) section for more information.

Local CDR File Naming Convention

Filenames are derived from the date and time that the CDR file is opened for writing. The format is `cdrYYYYMMDDHHMM[a-j]`, where:

- `YYYY`=the year
- `MM`=the month
- `DD`=the day
- `HH`=the hour
- `MM`=the minute
- `[a-j]`=a suffix that provides additional discrimination in case of changing system time, setting the rotation time for this feature to one minute, or in case of another occurrence that might compromise the date and time

Your file name will resemble the following sample: `cdr200511151200`.

Local CDR File Storage Directories

The Net-Net SBC only allows local storage of ASCII CDRs to the `/ramdrv` and `/ramdrv/logs` directories. If you try to save to another directory (such as /code or /boot), you will receive an error message.

If you are using the ACLI and enter an inappropriate directory, the ACLI will issue an error message.

Local CDR File Size and Rotation

You can configure maximum file size, maximum number of local CSV files to store, and the interval at which the files rotate.

The Net-Net SBC saves up to the file size limit (**max file size**) and maintains only number of files that you configure (**max files**). When the maximum file size is reached, the Net-Net SBC closes that file and begins writing VSA attributes and values to a new local CDR file. When it is time for the Net-Net SBC to write the ***max files*** *+ 1* file, the oldest file is deleted so that the newest one can be stored.

More About File Rotation Time

You can use the CDR local storage feature on its own, without enabling the ftp push feature. The Net-Net SBC uses a period of time that you set to periodically rotate the files. The **file rotate time** parameter rotates the local CSV files regardless of whether you use the FTP push feature.

RADIUS CDR Redundancy

When you are using the RADIUS CDR storage and FTP push feature, the Net-Net SBC can create a redundant copy of the comma-delimited CDR files that it stores on the standby system in the HA node.

This enhancement to the CDR storage feature ensures against data loss if, for example, an active Net-Net SBC fails immediately before an FTP push. The standby has a duplicate set of records that it sends. This feature is enabled with the **CDR output redundancy** parameter found in the **account config** configuration element.

Caveats for H.323

H.323 calls proceed without interruption over an HA node in the event of a failover from one Net-Net SBC to another, and RADIUS records are generated and duplicated across the active and standby systems in an HA node. However if a switchover occurs during an H.323 call (that has been initiated, but not completed), the newly active (formerly standby) system will not generate RADIUS Stop records when the call completes.

FTP Push

The FTP push feature is used to copy local CDR files to a remote FTP server on a periodic basis. This feature is configured by defining push receivers which contain standard login and FTP server credentials of the remote machine. At the configured time interval (**file rotate time**), the Net-Net SBC closes the current file, and pushes the files that are complete and have not yet been pushed; including the just-closed-file.

Deprecated ACLI Configuration

The following parameters in the account-config configuration element are deprecated:

- ftp-address
- ftp-port
- ftp-user
- ftp-password
- ftp-remote-path

These parameters will only only be used if no account-config > push-receiver configuration elements have been defined. All new push receivers must be defined in the account-config > push-receiver configuration element.

Multiple Push Receivers

Net-Net SBC now supports up to five CDR push receivers for use with the local file storage and FTP push feature. For each receiver you configure, you can set the file

transfer protocol you want to use—either FTP or SFTP. The system uses the push receivers according to the priorities you set by giving a 0 through 4 priority number to the server when you configure it; 0 is the highest priority, and 4 is the lowest. By default, push receivers always have their priority at the lowest setting (4).

Based on the priority level you set, the Net-Net SBC uses a strategy (which you also set) to select a CDR push receiver. If the highest priority push receiver selected using the strategy becomes unavailable (i.e., times out), the Net-Net SBC uses the strategy (hunt, round robin, etc.) to select another.

This feature is dynamically configurable. When you change the configuration, the Net-Net SBC updates the list of push receivers if it has changed.

Push Recievers

A push receiver configuration includes all the credentials that the Net-Net SBC needs to log into an FTP server and upload any recent local CDR files. Push receiver configurations must include:

- the server's IP address and port
- remote path of where to upload the local CDR files
- protocol used to connect to the server
- account login credentials

Secure FTP Push

The Net-Net SBC can securely log in to a push reciever using one of two methods that create a secure connection.

You can use password-based SSH authentication for logging into an SFTP server by setting the push receiver's **protocol** parameter to sftp, configuring a username and password and leaving the **public-key** parameter blank.

You can use SSH public key authentication for logging into an SFTP server by setting the push receiver's **protocol** parameter to sftp, setting the **public-key** parameter to a configured public key record name (security > public key > name), and including an account **username**.

ACLI Instructions and Examples

This section shows you how to configure Local CDR storage and FTP push on your Net-Net SBC.

Accessing the Accounting Configuration

To configure parameter for these features, you must access the accounting configuration.

To access the accounting configuration:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ```

3. Type **account-config** and press <Enter>.

   ```
   ACMEPACKET(session-router)# account-config
   ACMEPACKET(account-config)#
   ```

   From here, you can enable local CDR storage and FTP push.

Enabling Local CDR Storage

To enable local CDR storage:

4. **file-output**—Enable this paramater for the Net-Net SBC to create comma-delimited CDRs (generated from RADIUS records). By default, this parameter is disabled.
5. **file-path**—You must configure this path or the CDR push feature will not work. Set the path to use on the Net-Net SBC for file storage from these two options:
   - /ramdrv
   - /ramdrv/logs

   To use FTP push, you must configure a usable path.
6. **max-file-size**—Set the maximum file size in bytes permitted for each CDR file. The default and minimum value is 1000000. The maximum value is 10^8.
7. **max-files**—Set the maximum number of files to be stored on the Net-Net SBC at one time. You can configure the Net-Net SBC to store as few as one file or as many as 10. The default is 5.
8. **file-rotate-time**—Set how often in minutes you want to rotate the stored files; the Net-Net SBC will overwrite the oldest file first. The minimum rotation time is 2 minutes; the default is 60 minutes. This parameter defaults to 0, and leaving it set to the default means that the Net-Net SBC will not rotate the files.
9. **cdr-output-redundancy**—Set this paramter to enabled for the Net-Net SBC to store a redundant copy of the local CSV file to the standby HA node.

Configuring a Push Receiver Fallback Method

You set the push receiver strategy and define the maximum timeout in seconds in the main accounting configuration.

Note: You may ignore the following two parameters if only one push receiver is configured.

10. **ftp-strategy**—Set the strategy you want the Net-Net SBC to use when selecting from multiple push receivers. The default is **hunt**.

Strategy	Description
Hunt	The Net-Net SBC selects the push receiver from the available list according the priority level. The system uses this strategy as its default.
Failover	The Net-Net SBC selects the push receiver based on priority level and will continue to use that same push receiver until it fails over.
RoundRobin	The Net-Net SBC selects push receivers systematically one after another, balancing the load among all responsive push receivers.
FastestRTT	The Net-Net SBC selects the push receiver based on best average throughput. For this situation, throughput is the number of bytes transferred divided by the response time. The system uses a running average of the five most recent throughput values to accommodate for network load fluctuations.

11. **ftp-max-wait-failover**—Enter the amount of time in seconds to wait before the Net-Net SBC declares a push receiver to have failed over. This default value for this parameter is **60**.

Setting the CSV File Format

This section shows you how to to guarantee the CSV placement for RADIUS attribute values by using the entire RADIUS dictionary.

To enable fixed value placement in CSV files for RADIUS CDRs:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)#
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ```

3. Type **account-config** and press <Enter>.

   ```
   ACMEPACKET(session-router)# account-config
   ACMEPACKET(account-config)#
   ```

   If you are adding support for this feature to a pre-existing accounting configuration, then you must use the ACLI **select** command so that you can edit it.

4. **vsa-id-range**—Either leave this parameter blank (default), or enter the complete range of VSAs for the Net-Net OS release loaded on your system. The following example shows what you would enter to use all of the VSAs for Net-Net OS Release 4.1.4p4 for a system that is not running QoS.

   ```
   ACMEPACKET(account-config)# vsa-id-range 1-4,10-14,20-24,28,29,32-71,74-136
   ```

5. **cdr-output-inclusive**—Set this parameter to enabled to fill in 0s in otherwise empty fields in local CDR files. It is disabled by default.

Enabling FTP Push

To enable FTP push:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)#
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ```

3. Type **account-config** and press <Enter>.

   ```
   ACMEPACKET(session-router)# account-config
   ```

   If you are adding support for this feature to a pre-existing accounting configuration, then you must use the ACLI **select** command so that you can edit it.

4. **ftp-push**—Set the state of FTP push feature to **enabled**. It is disabled by default.
5. Type push-receiver and press <Enter>.

   ```
   ACMEPACKET(account-config)# push-receiver
   ```

6. **server**—Enter the IP address of this push receiver FTP server.
7. **port**—Enter the port number of this push receiver FTP server.
8. **remote-path**—Enter the remote pathname to which you want CDR files to be sent on the push receiver. There is no default for this parameter.
9. **filename-prefix**—Enter the filename prefix (as a string) to prepend to the to the CDR files the Net-Net SBC sends to the push receiver. The Net-Net SBC does not rename local files. There is no default for this parameter.

10. **protocol**—Enter **SFTP** if you want to change the transport protocol for this push receiver from its default, **FTP**.
11. **username**—Enter the username the Net-Net SBC uses when connecting to this push receiver. There is no default for this parameter. This parameter must be configured whether you are using unencrypted FTP, password or public key authentication.
12. **password**—Enter the password corresponding to the username the Net-Net SBC uses when connecting to this push receiver. There is no default for this parameter.
13. **public-key**—Enter the public key profile to use for authentication to this push receiver if this is the preferred form of authentication. If you define this as an SFTP push receiver but do not set the public-key value, the Net-Net SBC will use password authentication. There is no default for this parameter.
14. Save and activate your configuration.

3 RADIUS Accounting Management

Overview

This chapter provides information about management and monitoring of RADIUS accounting functions on your Net-Net SBC.

- Net-Net SBC alarm generation and monitoring
- Status and statistics monitoring

Alarm Generation and Monitoring

The Net-Net products generate alarms when certain hardware and software events occur. For more information about Net-Net SBC alarms for RADIUS, refer to the *Net-Net Maintenance and Troubleshooting Guide.*

The RADIUS ACCOUNTING CONNECTION DOWN alarm, detailed in the table below, is directly associated with the Net-Net SBC's RADIUS functionality. When enabled connections to RADIUS servers have timed-out without a response from the RADIUS server, the alarm is activated. The RADIUS ACCOUNTING CONNECTION DOWN alarm triggers a Simple Network Management Protocol (SNMP) trap that is sent via the syslog Management Information Base (MIB) (ap-syslog.mib). For a list of all SNMP-related alarms and their associated traps, refer to the table of SNMP trap correlation to Net-Net SBC's alarms in Acme Packet's *MIB Reference Guide*.

This alarm has no impact on a the health score of a Net-Net SBC that is part of an HA Node.

RADIUS Alarms

The table below describes the Net-Net SBC's alarms for RADIUS.

Alarm	Alarm ID	Alarm Severity	Cause	Log Message	Actions
RADIUS ACCOUNTING CONNECTION DOWN	327681	CRITICAL if all enabled and configured RADIUS accounting server connections have timed-out without a response from the RADIUS server. MAJOR if some, but not all configured RADIUS accounting server connections have timed-out without a response from the RADIUS server.	The enabled connections to RADIUS servers have timed-out without a response from the RADIUS server.	CRITICAL: All enabled accounting connections have been lost. Check accounting status for more details. MAJOR: One or more enabled accounting connections have been lost. Check accounting status for more details.	• `apSyslogMessageGenerated` trap generated • critical, major dry contact • syslog

Status and Statistics Monitoring

The ACLI **show radius** command, used with the three arguments described below, displays the status of any established RADIUS accounting connections and authentications. A working RADIUS connection displays `READY`, and a disabled connection displays `DISABLED`.

When an accounting server is disabled, the triggering and clearing of RADIUS ACCOUNTING CONNECTION DOWN alarms is not affected.

For more information about Net-Net SBC about monitoring your Net-Net SBC, refer to the *Net-Net Maintenance and Troubleshooting Guide.*

ACLI Show RADIUS Display

The **show radius** command can take one of the three available arguments:

- authentication—Shows authentication statistics for primary and secondary RADIUS servers, including: server IP address and port; round trip time; information about failed and successful requests/authentications; number of rejections; number of challenges; number of time-outs, number of retransmissions
- accounting—Shows the information described in this table:

Section	Description
Client Display	General accounting setup (as established in the accounting configuration element), including: • Information about the state of the RADIUS client • Accounting strategy used (Hunt, Failover, RoundRobin, FastestRTT, or FewestPending) • IP address and port on which the Net-Net server is listening • Maximum message delay in seconds • Number of configured accounting servers
Waiting Queue	Amount of accounting (RADIUS) messages waiting to be sent. Waiting queue capacity is 4,096 messages.
<IP Address:Port>	Information about each configured accounting server (established in the accounting servers configuration). The heading above each accounting server section is the IPv4 address and port combination of the accounting server described. This section also includes information about the accounting server's state (e.g., `Connect_Attempt, INIT`).

- all—Shows all of the information for both the authentication and accounting displays

The following is an example of the ACLI **show radius authentication** command output.

```
ACMEPACKET# show radius authentication
Active Primary Authentication Servers:
   server ipAddr: 172.30.0.7

Active Secondary Authentication Servers:
   server ipAddr: 172.30.0.8

Authentication Statistics:
        Server:"172.30.0.7:1812"
```

```
                  RoundTripTime          :0
                  MalformedAccessResponse:0
                  AccessRequests         :2
                  BadAuthenticators      :0
                  AccessRetransmissions  :5
                  AccessAccepts          :0
                  Timeouts               :6
                  AccessRejects          :0
                  UnknownPDUTypes        :0
                AccessChallenges       :0

Server:"172.30.0.8:1812"
                  RoundTripTime          :0
                  MalformedAccessResponse:0
                  AccessRequests         :2
                  BadAuthenticators      :0
                  AccessRetransmissions  :9
                  AccessAccepts          :0
                  Timeouts               :10
                  AccessRejects          :0
                  UnknownPDUTypes        :0
                  AccessChallenges       :0
```

The following is an example of the ACLI **show radius accounting** command output.

```
ACMEPACKET# show radius accounting
*********Client Display Start************
Client State = READY, strategy=Hunt
listening on 127.0.0.1:1813
max message delay = 60 s, # of servers = 2
================= Waiting Queue ================
Waiting size = 89
================================================
----------------- 10.0.0.189:1813 ------------------
Remote = 10.0.0.189:1813, Local = 0.0.0.0:1026, sock=45 (BOUND)
conn state=READY, RTT=250 ms
Min Rtt=250 ms, Max inactivity=60 s, expires at Nov 21 13:50:19.582,
Restart delay=30 s
----------------- 192.168.200.70:5050 ------------------
Remote = 192.168.200.70:5050, Local = 0.0.0.0:1027, sock=46 (BOUND)
conn state=DISABLED, RTT=0 ms
Min Rtt=250 ms, Max inactivity=60 s, expires at Nov 21 13:50:19.569,
Restart delay=30 s
*********Client Display End************
```

The following is an example of the ACLI **show radius all** command output.

```
ACMEPACKET# show radius all
*********Client Display Start************
Client State = READY, strategy=Hunt
listening on 127.0.0.1:1813
max message delay = 60 s, # of servers = 2
================= Waiting Queue ================
Waiting size = 89
================================================
```

```
----------------- 10.0.0.189:1813 ------------------
Remote = 10.0.0.189:1813, Local = 0.0.0.0:1026, sock=45 (BOUND)
conn state=READY, RTT=250 ms
Min Rtt=250 ms, Max inactivity=60 s, expires at Nov 21 13:50:19.582,
Restart delay=30 s
----------------- 192.168.200.70:5050 ------------------
Remote = 192.168.200.70:5050, Local = 0.0.0.0:1027, sock=46 (BOUND)
conn state=DISABLED, RTT=0 ms
Min Rtt=250 ms, Max inactivity=60 s, expires at Nov 21 13:50:19.569,
Restart delay=30 s
*********Client Display End************

 Active Primary Authentication Servers:
    server ipAddr: 172.30.0.7

 Active Secondary Authentication Servers:
    server ipAddr: 172.30.0.8

 Authentication Statistics:
         Server:"172.30.0.7:1812"
                 RoundTripTime          :0
                 MalformedAccessResponse:0
                 AccessRequests         :2
                 BadAuthenticators      :0
                 AccessRetransmissions  :5
                 AccessAccepts          :0
                 Timeouts               :6
                 AccessRejects          :0
                 UnknownPDUTypes        :0
                AccessChallenges       :0

         Server:"172.30.0.8:1812"
                 RoundTripTime          :0
                 MalformedAccessResponse:0
                 AccessRequests         :2
                 BadAuthenticators      :0
                 AccessRetransmissions  :9
                 AccessAccepts          :0
                 Timeouts               :10
                 AccessRejects          :0
                 UnknownPDUTypes        :0
                 AccessChallenges       :0
```

Monitoring CDR Push Receivers

You can use the ACLI **show radius cdr** command to view information about CDR push receivers. The existing display for this command has been extended to include information that looks like the following:

```
****************** CDR Push Receiver Display Start******************
strategy = FastestRTT, maxwaitfailover = 10, number of receivers = 1
-------------------- 172.30.0.70:21 --------------------
cdrpush-receiver = 172.30.0.70:21, state = READY, priority = 4
remote path = /home/acme, remote prefix = vik, protocol = ftp
username = acme, password = ********, publickey =
FTP rtt = 0, FTP successes = 0, FTP failures = 0
```

```
FTP timeouts = 0, FTP Delays = 0, FTP Put failures = 0
FTP conn failures = 0, FTP terminates = 0, FTP triggered terminates = 0
```

SNMP Support

The Net-Net SBC sends traps when a single push receiver or all push receivers become unavailable.

- When one CDR push receiver becomes unavailable, the `CDR_PUSH_RECEIVER_FAIL_TRAP` trap is sent and a minor alarm is generated.
- When all of the configured CDR push receivers become unavailable, the `CDR_ALL_PUSH_RECEIVERS_FAIL_TRAP` is sent and a major alarm is generated.

  When one or more of the push receivers comes back, the `CDR_ALL_PUSH_RECEIVERS_FAIL_CLEAR_TRAP` is sent and the alarm is cleared.

CDR File Transfer Failure Alarm

The Net-Net SBC sends out traps and triggers corresponding alarms when it encounters failure when attempting to transfer locally stored CDR files via FTP or SFTP. One set of traps is used for instances when one CDR push receiver fails; another is used when all enabled CDR receivers fail. They are part of the `apSysMgmtCDRPushReceiverNotificationsGroup`.

All of the traps contain information about the type of push receiver, the address of the push receiver, and the failure reason code.

All of the traps contain information about the type of push receiver, the address of the push receiver, and the failure reason code.

The trap and corresponding clearing trap for single push receiver failure are:

- `apSysMgmtCDRPushReceiverFailureTrap`
- `apSysMgmtCDRPushReceiverFailureClearTrap`

The trap and corresponding clearing trap for global push receiver failure are:

- `apSysMgmtCDRAllPushReceiversFailureTrap`
- `apSysMgmtCDRAllPushReceiverFailuresClearTrap`

4 Storage Expansion Module

Storage Expansion Module Use With Local CDRs / FTP Push

The Net-Net 3800 and 4500 can be configured with an optional Storage Expansion Module that extends the system's internal storage beyond the fixed amount of flash RAM. When configuring local CDR creation, you can configure the Net-Net SBC to use the Storage Expansion Module for local CDR files instead of the limited internal flash RAM.

Disk space on the Storage Expansion Module appears as a local volume on the Net-Net SBC. Wherever you specify a volume name for a configuration parameter value, you can enter a volume located on the Storage Expansion Module, (unless the parameter is otherwise specified).

Local CDR Storage Directory

To save local CDR files to the Storage Expansion Module, configure the **file path** parameter in the account config with a volume and directory located on the Storage Expansion Module.

FTP Push Backup

When FTP push is enabled, if all FTP push servers are unreachable, then local CDR files are written to local file system until the FTP push servers return to service. Once an FTP Push server becomes reachable, the Net-Net SBC transfers all local CDR files to the remote server automatically. After all local CDR files have been successfully transferred to the FTP server from the Net-Net SBC, they are deleted from the local volume.

Local CDR File Compression

You can configure the Net-Net SBC to compress local CDRs in zip format to save disk space. The local CDRs will be compressed and appear with a .zip file extension. This feature is enabled with the **cdr compression** parameter.

ACLI Configuration and Examples

The following ACLI configuration procedure describes:

- identifying volumes on the Storage Expansion Module
- configuring Storage Expansion Module volumes as the destination for local CDR files

These procedures are only a portion of local CDR file generation and FTP Push configuration. Please refer to the Net-Net 4000 S-C6.1.0 ACLI Accounting Guide's Local CDR Storage and FTP Push section for a full explanation and all prerequisites before referencing the following procedure.

To identify the volumes on the Storage Expansion Module to use with local CDR storage:

1. Note the volume name on the Storage Expansion Module you wish to use for local CDR output using the **show space hard-drive** command. The following example indicates that there are 4 partitions, which are set in bold:

```
SYSTEM# show space hard-disk

/sys: 19695716352/19695749120 bytes (99%) remaining

/local: 19693335040/19693367808 bytes (99%) remaining

/logs: 19693335040/19693367808 bytes (99%) remaining

/misc: 19693335040/19693367808 bytes (99%) remaining
SYSTEM#
```

   Note: The **check-space-remaining hard-disk** command is identical to the s**how space hard-disk** command.

To configure a Net-Net 3800 or Net-Net 4500 to write local CDRs to the Storage Expansion Module:

1. In Superuser mode, type **configure terminal** and press <Enter>.

```
ACMEPACKET# configure terminal
```

2. Type **session-router** and press <Enter>.

```
ACMEPACKET(configure)# session-router
```

3. Type **account-config** and press <Enter>.

```
ACMEPACKET(session-router)# account-config
ACMEPACKET(account-config)#
```

4. **file-path**—Set this parameter to the volume you identified to use for local CDR file storage in the previous section. Ensure the path begins with a forward slash, "/".
5. Save and activate your configuration.

Storage Expansion Module Management

The Net-Net SBC provides you with a set of tools to manage the Storage Expansion Module.

Identifying Storage Expansion Module Volumes

You can identify volumes that exist on the Storage Expansion Module using the **show space hard-drive** command. In addition, free and used space are reported too. For Example:

```
SYSTEM# show space hard-disk

/sys: 19695716352/19695749120 bytes (99%) remaining

/local: 19693335040/19693367808 bytes (99%) remaining

/logs: 19693335040/19693367808 bytes (99%) remaining

/misc: 19693335040/19693367808 bytes (99%) remaining
SYSTEM#
```

Viewing Directories and Files

You can view files and directories on the Storage Expansion Module using the **show directory <path>** command. Remember to use absolute paths beginning with the forward slash. For example:

```
SYSTEM# show directory /misc

Listing Directory /misc:
-rwxrwxrwx  1 0       0                   0 Aug 24 14:26 tmp.dat
-rwxrwxrwx  1 0       0             1048580 Aug 25 11:50 file_0.txt
SYSTEM#
```

To view all volumes on the Net-Net SBC, type **show directory** without any arguments. For Example:

```
SYSTEM# show directory
Top-level directories:
/ramdrv
/code
/boot
/local
/logs
```

Typing **show directory *** displays all top-level directories and their contents.

Formatting the Storage Expansion Module

You can use the Storage Expansion Module's default partition configuration, or you can create your own scheme creating a maximum of 4 volumes.

Default Format Plan

When formatting the Storage Expansion Module, the ACLI's default partitioning scheme is as follows:

Storage Expansion Module Default Format Plan:

Volume Number	Volume Name	Volume Size
1	/sys	10%
2	/app	90%

Custom Format Plan

Before formatting the Storage Expansion Module, plan the number of volumes, volume names, and relative percentage of Storage Expansion Module disk space. For example:

Storage Expansion Module Format Plan:

Volume Number	Volume Name	Volume Size
1	/archive	20%
2	/misc	35%
3	/localcdrs	45%

The following are invalid Storage Expansion Module volume names:

- ramdrv
- code
- boot

Custom Partition Scheme

To format the Storage Expansion Module using a custom partition scheme:

1. Type **format hard-disk** <Enter>. You will be prompted to confirm this action.

```
SYSTEM# format hard-disk

WARNING: Please ensure device is not currently in use by any
applications before proceeding

Continue [y/n]?:
```

   Type **y** <Enter> to continue

2. Type **n** <Enter> when prompted to use the factory default partitions.

```
Use factory default partitions [y/n]?:
```

3. Enter the number of volumes you wish to create and press <Enter>.

```
Enter the number of partitions to create: 3
```

4. Enter the name of volume 1 and press <Enter>

```
Total unallocated space = 100 %
Enter the name of volume 1 (or 'q' to quit): archive
```

5. Enter the size in percent of volume 1 and press <Enter>

```
Enter the size of the volume (in %): 20
```

6. Repeat steps 4 and 5 for all additional volumes.
7. A summary of how the Storage Expansion Module will be formatted is displayed on the screen. Type **y** <Enter> at the prompt that confirms you wish to commit this.

```
The following partitions will be created:
/archive        16005272371 bytes
/misc   28009226649 bytes
/localcdrs      36011862835 bytes

Format disk and create the partitions as configured above [y/n]?: y
```

8. You will be prompted again to confirm formatting the Storage Expansion Module. All existing data on the Storage Expansion Module will be lost. Type **y** <Enter> to continue.

```
**************************************************
WARNING: All data on the drive will be permanently
erased and unrecoverable.

Are you sure [y/n]?: y
```

9. You will be prompted one last time to confirm formatting the Storage Expansion Module. Type y <Enter> to continue.

```
The format process will take a few minutes. Once
the format process begins, it cannot be stopped.
Please do not power down or reboot the SD until
```

```
the format process is complete.

Continue [y/n]?: y
```

10. The formatting process displays progress on the screen and concludes after several minutes.

```
[progress text removed for brevity]

Format finished successfully
New partitions have been created
SYSTEM#
```

Default Partition Scheme

To format the Storage Expansion Module using the factory default partitions:

1. Type **format hard-disk** <Enter>. You will be prompted to confirm this action.

```
SYSTEM# format hard-disk

WARNING: Please ensure device is not currently in use by any
applications before proceeding

Continue [y/n]?: y
```

Type **y** <Enter> to continue

2. Type y <Enter> when prompted to use the factory default partitions. The factory partition scheme will be displayed on the screen. Type Y <Enter> at the prompt that confirms you wish to commit this.

```
Use factory default partitions [y/n]?: y

The following partitions will be created:
/sys    8002636185 bytes

/app    72023725670 bytes

Format disk and create the partitions as configured above [y/n]?: y
```

3. You will be prompted again to confirm you wish to format the Storage Expansion Module. All existing data will be lost. Type y <Enter> to continue.

```
**************************************************
WARNING: All data on the drive will be permanently
erased and unrecoverable.

Are you sure [y/n]?: y
```

4. You will be prompted one last time to confirm formatting the Storage Expansion Module. Type y <Enter> to continue.

```
The format process will take a few minutes. Once
the format process begins, it cannot be stopped.
Please do not power down or reboot the SD until
the format process is complete.

Continue [y/n]?: y
```

5. The formatting process will display progress on the screen and concludes after several minutes.

```
*** Beginning format process ***
```

```
[progress text removed for brevity]

Format finished successfully
New partitions have been created
SYSTEM#
```

Storage Expansion Module Monitoring

Low Disk Space Warning

The Net-Net SBC can initiate an alarm and an SNMP trap when a volume reaches a configured threshold of remaining free disk space, configured as a percentage of volume. You can configure multiple alarms, each with increasing severity that indicate less free disk space.

Low Disk Space Threshold Alarm

The low disk space threshold alarm is configured in **alarm threshold** configuration element. It is non-health affecting. The threshold alarm appears as follows:

```
SYSTEM# display-alarms
1 alarms to show
ID      Task    Severity        First Occurred          Last Occurred
131142  547896076     4     2009-08-25 13:36:26    2009-08-25 13:36:26
Count   Description
1       Volume /misc space used 81% is over major threshold of 80%.
```

Low Disk Space Threshold SNMP Trap

For any threshold reached, an SNMP trap will be sent to all configured trap-receivers. The apSysMgmtStorageSpaceAvailThresholdTrap trap contains the following information:

- VolumeName—name of the volume where a threshold was exceeded
- CurrentValue—current percentage of disk space value that is exceeding one of the thresholds.
- MinorThreshold—configured minor threshold for this volume, if none then this is 0.
- MajorThreshold—configured major threshold for this volume, if none then this is 0.
- CriticalThreshold—configured critical threshold for this volume, if none then this is 0.

ACLI Configuration and Examples

To configure alarm thresholds for monitoring free disk space:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **system** and press <Enter>.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type **system-config** and press <Enter>.

   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. Type select and press <Enter>.

```
ACMEPACKET(system-config)# select
ACMEPACKET(system-config)#
```

5. Type **alarm-threshold** and press <Enter>.

```
ACMEPACKET(system-config)# alarm-threshold
ACMEPACKET(alarm-threshold)#
```

   The system prompt changes to let you know that you can begin configuring individual parameters.

6. **type**—Set this parameter to **space** to create an alarm based on reduced free disk space.
7. **volume**—Set this parameter to the volume name you wish to monitor. Generally this string should be the same as the **file-path** parameter located in the account-config.
8. **severity**—Enter the severity level of this alarm. Valid severity values are MINOR, MAJOR, and CRITICAL.
9. **value**—Enter the percent of resource (*type*) in use that triggers the configured alarm (*severity*).
10. Save your work.
11. Repeat this procedure to configure multiple alarm thresholds.

The following example reflects what a major and critical alarm would look like:

```
alarm-threshold
        type                    space
        volume                  /misc
        severity                major
        value                   80
alarm-threshold
        type                    space
        volume                  /misc
        severity                critical
        value                   90
```

Local CDR File Delete Warning

You can configure the Net-Net SBC to initiate an alarm and send an SNMP trap when the oldest local CDR file was deleted under fault conditions. This feature is enabled with the **file delete alarm** parameter.

The Net-Net SBC deletes a local CDR file in the following three cases:

1. After the local CDR file has been successfully transferred to a push receiver
2. The number of local CDR files exceed the limit configured in the account-config > **max-files** parameter
3. No free disk space remains on the partition where the local CDR files are written: account-config > **file-path**

If a local CDR file is deleted after it was successfully uploaded to a push receiver, no fault is triggered because this is standard, expected operation. But if a local CDR file is deleted for case 2 or 3 above, it is considered a fault condition initiating an alarm and SNMP trap.

Local CDR File Delete Alarm

The CDR file delete alarm is configured in **account config** configuration element by enabling the **file-delete-alarm** parameter. This is a minor severity alarm and is non-health affecting. This alarm has no clearing condition and must be manually cleared.

Local CDR File Delete SNMP Trap

Under the same circumstances that cause a CDR file delete alarm, an SNMP trap will be sent to all configured trap-receivers. The apSysMgmtCdrFileDeleteTrap trap contains the following information:

- File Name—name of the file that was deleted

Querying Storage Space

You can monitor currently used and remaining storage space on the Storage Expansion Module by ACLI, SNMP MIB, and HDR collection group.

ACLI

To view the total disk space used percentage remaining with the ACLI, use the **show space hard-drive** command. For example:

```
SYSTEM# show space hard-disk

/sys: 19695716352/19695749120 bytes (99%) remaining

/local: 19693335040/19693367808 bytes (99%) remaining

/logs: 19693335040/19693367808 bytes (99%) remaining

/misc: 19693335040/19693367808 bytes (99%) remaining
SYSTEM#
```

Note: The **check-space-remaining hard-disk** command is identical to the s**how space hard-disk** command.

Unmounting The Storage Expansion Module

This section explains the ACLI **unmount hard-disk** command, which—as its name indicates—unmounts the storage expansion module. This command should only be run when you plan to shut down the system. You issue this command to ensure the integrity of the disk when you power off the Net-Net 4500 System or Net-Net 3800 using the power switch. If you do not run the command and use the power switch to power down the system, the Net-Net 4500 System runs a checkdisk on the module the next time the system boots. The checkdisk lasts one to two minutes.

Note that once you run the **unmount hard-disk** command, any application configuration set to use a module partition will no longer work. The only way to regain access is to reboot or power cycle the system.

ACLI Instructions and Examples

To ensure the storage expansion module's integrity when powering down the system (using the power switch), use the **unmount hard-disk** command:

```
ACMEPACKET# unmount hard-disk
```

SNMP MIB

The following MIB Objects are available to query the amount of remaining drive space.

Name	OID	MIB	Description
apSysStorageSpaceTable	1.3.6.1.4.1.9148.3.2.1.1.23	APSYSMGMT-MIB	The total percentage space available on the drive/partitions.

```
apSysStorageSpaceTable         OBJECT-TYPE
        SYNTAX          SEQUENCE OF ApSysStorageSpaceEntry
        MAX-ACCESS      not-accessible
        STATUS          current
        DESCRIPTION
                "A table to hold the total space and available space
                per volume arranged into rows, and indexed by the
                volume name.
                These are all read only."
        ::=  { apSysMgmtMIBGeneralObjects 23 }

apSysStorageSpaceEntry         OBJECT-TYPE
        SYNTAX          ApSysStorageSpaceEntry
        MAX-ACCESS      not-accessible
        STATUS          current
        DESCRIPTION
              "A table entry designed to hold storage space data, on a
                single volume"
        INDEX { apSysVolumeName }
        ::= { apSysStorageSpaceTable 1 }

ApSysStorageSpaceEntry ::= SEQUENCE {
        apSysVolumeName                                 DisplayString,
        apSysVolumeTotalSpace                           Unsigned32,
        apSysVolumeAvailSpace                           Unsigned32,

apSysVolumeName              OBJECT-TYPE
        SYNTAX                  DisplayString (SIZE (0..255))
        MAX-ACCESS              read-only
        STATUS                  obsolete
        DESCRIPTION
                "The name of the volume"
        ::= {apSysStorageSpaceEntry 1}

apSysVolumeTotalSpace           OBJECT-TYPE
        SYNTAX                  Unsigned32
        MAX-ACCESS              read-only
        STATUS                  obsolete
        DESCRIPTION
                "The total size of the volume, in bytes"
        ::= {apSysStorageSpaceEntry 2}

apSysVolumeAvailSpace           OBJECT-TYPE
        SYNTAX                  Unsigned32
        MAX-ACCESS              read-only
```

```
STATUS                  obsolete
DESCRIPTION
        "The total space available on the volume, in bytes"
::= {apSysStorageSpaceEntry 3}
```

HDR

Historical Data Record statistics are available that track the amount of storage space available on each Storage Expansion Module partition. At each collect interval, space consumption statistics are gathered for every partition. The Storage Space collect group, configured as **space,** contains these statistics. The contents of this Storage Space group are:

- TimeStamp
- Partition
- Space used
- Space available

5 Diameter Rf Accounting

Diameter Accounting

The Net-Net SBC supports the Diameter charging interface, Rf. This interface provides similar functionality to the RADIUS interface, but utilizes Diameter as the underlying application layer protocol. As a result, the Net-Net SBC can integrate more thoroughly with IMS standards as well as provide a more dynamic, secure, and robust accounting interface.

Diameter Accounting Messages

The Rf interface can send two types of messages based on the signaling application's actions. These messages are Accounting Charging Request (ACR) Start and ACR Stop messages.

- ACR start messages are sent at the start of service delivery and describes the type of service being delivered and the user to whom it is being delivered.
- Additional ACR Start messages are sent when service changes; this roughly maps to a RADIUS Interim-Update message. See Accounting-Record-Type AVP (480) (82).
- ACR Stop messages are sent at the end of service delivery.

The Net-Net SBC sends a set of a AVPs in each ACR start and stop message that make up the charging data. The following table lists which AVPs are included in ACR Start and ACR Stop messages. Individual AVP descriptions are located in the following section.

AVP	ACR Start	ACR Stop
Session-Id AVP (263)	X	X
Origin-Host AVP (264)	X	X
Origin-Realm AVP (296)	X	X
Destination-Realm AVP (283)	X	X
Destination-Host AVP (293)	X	X
Accounting-Record-Type AVP (480)	X	X
Accounting-Record-Number AVP (485)	X	X
Acct-Application-Id AVP (259)	X	X
User-Name AVP (1)	X	X
Event-Timestamp AVP (55)	X	X
Event-Type AVP (823) • SIP-Method AVP (824) • Content-Type AVP (826) • Content-Length AVP (827)	X	X
Role-of-Node AVP (829)	X	X

AVP	ACR Start	ACR Stop
User-Session-Id AVP (830)	X	X
Calling-Party-Address AVP (831)	X	
Called-Party-Address AVP (832)	X	
Time-Stamps AVP (833) • SIP-Request-Timestamp AVP (834) • SIP-Response-Timestamp AVP (835)	X	X
Inter-Operator-Identifier AVP (838) • Originating-IOI AVP (839) • Terminated-IOI AVP (840)	X	X
SDP-Session-Description AVP (842)	X	
Session-Media-Component AVP (845) • SDP-Media-Name AVP (844) • SDP-Media-Description AVP (845)	X	
Cause AVP (860) • Cause-Code AVP (861) • Node-Functionality AVP (862)		X

ACR AVP Descriptions

Session-Id AVP (263)

Uniquely identify this session. It is a string value and is delimited by semi-colons. hostname of the accounting server the communication is to out on.

The second two parts are values that get generated by the signaling application related to the signaling session that is occurring. It is a number that gets increased every time a new signaling session is created. An example of a Session-Id from the SD is as follows, acmesystem;0;1.

Origin-Host AVP (264)

Contains the account-server configuration element's **hostname** parameter followed by the "@" character, followed by the account-server configuration element's **origin-realm** parameter. For example: acmesystem@wancom.com.

Origin-Realm AVP (296)

Contains the **account server** configuration element's **origin-realm** and **domain-name-suffix** parameters where the server request is sent.

Destination-Realm AVP (283)

Contains the value of the Origin-Realm AVP in the CEA received from the accounting server for this connection.

Destination-Host AVP (293)

Contains the value of the Origin-Host AVP in the CEA received from the accounting server for this connection.

Accounting-Record-Type AVP (480)

Contains the value indicating the type of accounting message being sent.

- start record = 2
- interim record = 3
- stop record = 4

If this is an interim-type message, it's still included in an ACR Start message but with the value of this AVP set to "3".

Accounting-Record-Number AVP (485)

A value that uniquely identifies this message in the session, i.e., a sequence number for this connection. This value is arbitrarily created by the Net-Net SBC with the caveat that it is unique for a session.

Acct-Application-Id AVP (259)

Set to value "3"; This value indicates Diameter-based accounting messages.

User-Name AVP (1)

Contains the account-server configuration element's hostname parameter followed by the "@" character, followed by the account-server configuration element's origin-realm parameter. For example: acmesystem@wancom.com.

Event-Timestamp AVP (55)

Contains the number of seconds since January 1, 1900 when this accounting event took place.

Event-Type AVP (823)

A grouped AVP containing information about the signaling event. It contains the following AVPs:

- SIP-Method AVP (824)—Contains the exact string payload from the SIP request line; i.e., the Method that triggered the accounting event.
- Content-Type AVP (826)—Contains the exact string payload from the "Content-Type" SIP header of the message that triggered the accounting event.
- Content-Length AVP (827)—Contains the exact string payload from the Content-Length" SIP header of the message that triggered the accounting event.

Role-of-Node AVP (829)

Set to the value "2" which indicates that the Net-Net SBC is operating in a PROXY role.

User-Session-Id AVP (830)

Contains VSA 44 as used in the RADIUS interface.

Calling-Party-Address AVP (831)

Contains the calling party address in the SIP message. The Net-Net SBC first checks for a P-Asserted-Id header. If present, its value is used for this AVP. If not present, the Net-Net SBC inserts the "To:" field from the SIP message into this AVP. ONLY IN ACR Start.

Called-Party-Address AVP (832)

Contains the "From:" field of the SIP message. ONLY IN ACR Start.

Time-Stamps AVP (833)

A grouped AVP that contains timestamps for the related SIP signaling. It contains the following AVPs.

- SIP-Request-Timestamp AVP (834)—A UTC formatted timestamp that corresponds to when the SIP INVITE that started the session was received.
- SIP-Response-Timestamp AVP (835)—A UTC formatted timestamp that corresponds to when the SIP 200 OK response to the INVITE that started the session was received.

Inter-Operator-Identifier AVP (838)

A grouped AVP that indicates the ingress and egress networks from the Net-Net SBC's perspective. It contains the following AVPs.

- Originating-IOI AVP (839)—The realm where the Net-Net SBC received the SIP signaling messages.
- Terminated-IOI AVP (840)—The realm where the SIP signaling message exit the Net-Net SBC.

SDP-Session-Description AVP (842)

This AVP may occur multiple times in an ACR message. It is populated with SDP attribute-lines from the SIP messages to which this ACR Stop message refers. Thus, all "i=", "c=", "b=", "k=", "a=", etc.., lines comprise multiple instances of this AVP.

If the Net-Net SBC is configured to generate Start events on the INVITE, the calling SDP will be used; if the Net-Net SBC is configured to generate Start events on the OK, the called SDP will be used. ONLY IN ACR Start.

Session-Media-Component AVP (845)

A grouped AVP that contains information about the media session. It contains the following AVPs. ONLY IN ACR Start.

- SDP-Media-Name AVP (844)—populated with the "m=" line from the SDP being used.
- SDP-Media-Description AVP (845)—this AVP may occur multiple times in this grouped AVP. It is populated with SDP attribute-lines from the media component as specified by the media described in the SDP-Media-Name AVP. Thus, all "i=", "c=", "b=", "k=", "a=", etc..., lines related to the above specified "m=" line comprise multiple instances of this AVP.

Cause AVP (860)

A grouped AVP that contains the reason for the termination event and the role/function of the node where the call was terminated. It contains the following AVPs. ONLY IN ACR Stop.

- Cause-Code AVP (861)—Set to value "0".
- Node-Functionality AVP (862)—Set to value "0".

Configuring Diameter-based Accounting

Diameter-based Rf accounting relies on many of the same configuration elements used for RADIUS based accounting. The following two sections explain how to configure both the **account-config** and **accout-servers** configuration elements. In addition, you must ensure that accounting is enabled for each realm where you want it to occur. The **accounting-enable** parameter in the realm-config is enabled by default.

ACLI Instructions and Examples

To configure the global Diameter-based accounting (Rf) features in the account-config:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ```

3. Type **account-config** and press <Enter>.

   ```
   ACMEPACKET(session-router)# account-config
   ACMEPACKET(account-config)#
   ```

4. **hostname**—Enter a hostname for this system.
5. **port**—Enter 3868 for the RFC-recommended Diameter port number. You may enter a different port number.
   - minimum: 1025
   - maximum: 65535
6. **strategy**—Set the strategy used to select the accounting server which the Net-Net SBC sends accounting messages. The following table lists the available strategies:

Value	Description
hunt	Selects accounting servers in the order in which they are listed. If the first accounting server is online, working, and has not exceeded any of the defined constraints, all traffic is sent to it. Otherwise the second accounting server is selected. If the first and second accounting servers are offline or exceed any defined constraints, the third accounting server is selected. And so on through the entire list of configured servers
failover	Uses the first server in the list of predefined accounting servers until a failure is received from that server. Once a failure is received, it moves to the second accounting server in the list until a failure is received. And so on through the entire list of configured servers.
round robin	Selects each accounting server in order, distributing the selection of each accounting server evenly over time.
fastest round trip time	Selects the accounting server that has the fastest round trip time (RTT) observed during transactions with the servers (sending a record and receiving an ACK).
fewest pending	Selects the accounting server that has the fewest number of unacknowledged accounting messages (that are in transit to the Net-Net SBC).

7. **protocol**—Set this parameter to **diameter** to use the Rf accounting interface with a Diameter-based accounting server.
8. **state**— Enter **enabled** to use accounting on this system.
9. **max-msg-delay**—Retain the default value of **60** seconds or indicate the length of time in seconds that you want the Net-Net SBC to continue trying to send each accounting message. During this delay, the Net-Net SBC can hold a generic queue of 4096 messages.

- Minimum: zero (0)
- Maximum: 2^{32}-1

10. **max-wait-failover**—Retain the default value of **100** messages or indicate the maximum number of accounting messages the Net-Net SBC can store its message waiting queue for a specific accounting server, before it is considered a failover situation.

    Once this value is exceeded, the Net-Net SBC attempts to send it accounting messages, including its pending messages, to the next accounting server in its configured list.

    - Minimum: one (1) message
    - Maximum: 4096 messages

11. **trans-at-close**—Retain the default value of **disabled** if you do not want to defer the transmission of message information to the close of a session. Enter **enabled** if you want to defer message transmission.

    - **disabled**—The Net-Net SBC transmits accounting information at the start of a session (Start), during the session (Interim), and at the close of a session (Stop). The transmitted accounting information for a single session might span a period of hours and be spread out among different storage files.
    - **enabled**—Limits the number of files on the Net-Net SBC used to store the accounting message information for one session. It is easiest to store the accounting information from a single session in a single storage file.

12. **generate-start**—Retain the default value **ok** if you want the ACR Start message to be generated once the Net-Net SBC receives an OK message in response to an INVITE.

    Other options include:

    - none—Accounting Start message should not be generated.
    - invite—Accounting Start message should be generated once the Net-Net SBC receives a SIP INVITE.

13. **generate-interim**—Retain the default value **reinvite-response** to cause the Net-Net SBC to send an Interim charging message to the accounting server.

    You can select none, one, or more than one of the following values:

Value	Description
ok	Start message is generated when the Net-Net SBC receives an OK message in response to an INVITE.
reinvite	Interim message is generated when the Net-Net SBC receives a SIP session reINVITE message.
reinvite-response (default)	Interim message is generated when the Net-Net SBC receives a SIP session reINVITE and responds to it (for example, session connection or failure).

Value	Description
reinvite-cancel	Interim message is generated when the Net-Net SBC receives a SIP session reINVITE, and the Reinvite is cancelled before the Net-Net SBC responds to it.
unsuccessful-attempt	Interim message is generated when a SIP session set-up attempt from a preference-ordered list of next-hop destinations is unsuccessful. This can happen when a local policy lookup, LRT lookup, ENUM query response, or SIP redirect returns a preference-ordered list of next-hop destinations. The interim message contains: the destination IP address, the disconnect reason, a timestamp for the failure, and the number that was called.

14. **intermediate-period**—Enter amount of time in seconds between generating periodic interim ACR messages during a SIP call. This parameter defaults to zero, which disables continuous Interim charging messages.
15. **vsa-id-range**—Ensure that this parameter is left blank when communicating with a Diameter-based Rf accounting server.
16. Save your work.

To configure individual Diameter-based accounting servers:

Configuring Accounting Servers

You must create one or more servers to which the Net-Net SBC can send accounting messages.

1. Continuing from the previous account-config configuration, enter the account server sub-element by typing **account-servers** <Enter>.

   ```
   AZALEA(account-config)# account-servers
   AZALEA(account-server)#
   ```

2. **hostname**—Set this to the IP address or hostname (FQDN)of the Diameter-based Rf accounting server.
3. **port**—Enter 3868 for the RFC-recommended Diameter port number. You may enter a different port number if desired.
   - minimum: 1025
   - maximum: 65535
4. **state**—Retain the default `enabled` to enable this account server or enter `disabled` to disable it.
5. **min-round-trip**—Retain the default `250` milliseconds or indicate the minimum round trip time of an accounting message.
   - minimum: 1025 milliseconds
   - maximum: 65535 milliseconds

   A round trip consists of the following:

   – The Net-Net SBC sends an accounting message to the account server.

   – The account server processes this message and responds back to the Net-Net SBC.

   If the fastest RTT is the strategy for the account configuration, the value you enter here can be used to determine an order of preference (if all the configured account servers are responding in less than their minimum RTT).

6. **max-inactivity**—Retain the default `60` seconds or indicate the length of time in seconds that you want the Net-Net SBC with pending accounting messages to wait when it has not received a valid response from the target account server.

   - minimum: 1 second
   - maximum: 300 seconds

   Once this timer value is exceeded, the Net-Net SBC marks the unresponsive account server as disabled in its failover scheme. When a server connection is marked as inactive, the Net-Net SBC attempts to restart the connection and transfers pending messages to another queue for transmission. Accounting messages might be moved between different account servers as servers become inactive or disabled.

7. **restart-delay**—Retain the default `30` seconds or indicate the length of time in seconds you want the Net-Net SBC to wait before resending messages to a disabled account server.

   - minimum: 1 second
   - maximum: 300 seconds

8. **priority**—Enter the number corresponding to the priorityof this account server, for use with server prioritizaion. The default for this parameter is 0, meaning the prioritization feature is turned off—and that the Net-Net SBC will therefore prioritize accounting servers by IP address and port.

9. **origin-realm**—Enter the realm in which the Net-Net SBC communicates with the Diameter Rf accounting server.

10. **domain-name-suffix**—Enter the suffix to be appeanded to any Diameter FQDN or Diameter Identity used when the Net-Net SBC communicates with the Diameter Rf accounting server. Your value can be any string, to which the Net-Net SBC will prepend with a dot.

11. Save your work.

Appendix A
Net-Net RADIUS Log Examples

Overview

Several examples of RADIUS logs appear in this appendix. These logs were processed and the output generated by a FreeRADIUS server; the labels for each field come from the installed VSA dictionaries, including the Acme Packet RADIUS dictionary.

As you review these examples, please note:

- The `Acct-Unique-Session-Id =` and `Timestamp =` fields shown in the following examples are generated by the RADIUS server and not by the Net-Net SBC.
- For non-QoS calls, the attributes appear in the record, but their values are always zero (0).

RADIUS CDR Samples for SIP

This section provides an example CDRs for SIP calls.

Basic Successful SIP Call

The following sample CDRs are for a successful SIP call.

```
Successfull SIP Call - Peer
=======================================


Acct-Status-Type = Start
NAS-IP-Address = 192.168.12.100
NAS-Port = 5060
Acct-Session-Id = "6edfa77f-f059e59-711c7dce@192.168.11.101"
Acme-Session-Ingress-CallId = "6edfa77f-f059e59-711c7dce@192.168.11.101"
Acme-Session-Egress-CallId = "6edfa77f-f059e59-711c7dce@192.168.11.101"
Acme-Session-Protocol-Type = "SIP"
Calling-Station-Id = ""7812223001"
<sip:7812223001@192.168.11.101>;tag=40335A3-29FEF610"
Called-Station-Id = "<sip:7812223002@192.168.11.101;user=phone>"
h323-setup-time = "16:43:42.452 EST JUL 02 2008"
h323-connect-time = "16:43:53.517 EST JUL 02 2008"
Acme-Egress-Network-Interface-Id = "M10"
Acme-Egress-Vlan-Tag-Value = 0
Acme-Ingress-Network-Interface-Id = "M00"
Acme-Ingress-Vlan-Tag-Value = 0
Acme-Session-Egress-Realm = "Core"
Acme-Session-Ingress-Realm = "Peer"
```

```
Acme-FlowID_FS1_F = "localhost:65594"
Acme-FlowType_FS1_F = "PCMU"
Acme-Flow-In-Realm_FS1_F = "Peer"
Acme-Flow-In-Src-Addr_FS1_F = 0.0.0.0
Acme-Flow-In-Src-Port_FS1_F = 0
Acme-Flow-In-Dst-Addr_FS1_F = 192.168.11.100
Acme-Flow-In-Dst-Port_FS1_F = 49188
Acme-Flow-Out-Realm_FS1_F = "Core"
Acme-Flow-Out-Src-Addr_FS1_F = 192.168.12.100
Acme-Flow-Out-Src-Port_FS1_F = 49152
Acme-Flow-Out-Dst-Addr_FS1_F = 192.168.12.200
Acme-Flow-Out-Dst-Port_FS1_F = 2222
Acme-FlowID_FS1_R = "localhost:65595"
Acme-FlowType_FS1_R = "PCMU"
Acme-Flow-In-Realm_FS1_R = "Core"
Acme-Flow-In-Src-Addr_FS1_R = 0.0.0.0
Acme-Flow-In-Src-Port_FS1_R = 0
Acme-Flow-In-Dst-Addr_FS1_R = 192.168.12.100
Acme-Flow-In-Dst-Port_FS1_R = 49152
Acme-Flow-Out-Realm_FS1_R = "Peer"
Acme-Flow-Out-Src-Addr_FS1_R = 192.168.11.100
Acme-Flow-Out-Src-Port_FS1_R = 49188
Acme-Flow-Out-Dst-Addr_FS1_R = 192.168.11.101
Acme-Flow-Out-Dst-Port_FS1_R = 2224
Acme-FlowID_FS2_F = ""
Acme-FlowType_FS2_F = ""
Acme-Flow-In-Realm_FS2_F = ""
Acme-Flow-In-Src-Addr_FS2_F = 0.0.0.0
Acme-Flow-In-Src-Port_FS2_F = 0
Acme-Flow-In-Dst-Addr_FS2_F = 0.0.0.0
Acme-Flow-In-Dst-Port_FS2_F = 0
Acme-Flow-Out-Realm_FS2_F = ""
Acme-Flow-Out-Src-Addr_FS2_F = 0.0.0.0
Acme-Flow-Out-Src-Port_FS2_F = 0
Acme-Flow-Out-Dst-Addr_FS2_F = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS2_F = 0
Acme-FlowID_FS2_R = ""
Acme-FlowType_FS2_R = ""
Acme-Flow-In-Realm_FS2_R = ""
Acme-Flow-In-Src-Addr_FS2_R = 0.0.0.0
Acme-Flow-In-Src-Port_FS2_R = 0
Acme-Flow-In-Dst-Addr_FS2_R = 0.0.0.0
Acme-Flow-In-Dst-Port_FS2_R = 0
Acme-Flow-Out-Realm_FS2_R = ""
Acme-Flow-Out-Src-Addr_FS2_R = 0.0.0.0
Acme-Flow-Out-Src-Port_FS2_R = 0
```

```
Acme-Flow-Out-Dst-Addr_FS2_R = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS2_R = 0
Acme-Firmware-Version = "C6.0.0 GA (Build 13)"
Acme-Local-Time-Zone = "GMT-05:00"
Acme-Post-Dial-Delay = 223
Acme-Primary-Routing-Number = "sip:7812223002@192.168.11.101;user=phone"
Acme-Ingress-Local-Addr = "192.168.11.100:5060"
Acme-Ingress-Remote-Addr = "192.168.11.101:5060"
Acme-Egress-Local-Addr = "192.168.12.100:5060"
Acme-Egress-Remote-Addr = "192.168.12.200:5060"
Acme-Egress-Final-Routing-Number =
"sip:7812223002@192.168.11.101;user=phone"
Acme-CDR-Sequence-Number = 99
Client-IP-Address = 172.30.21.31
Acct-Unique-Session-Id = "5af95b6a3259b428"
Timestamp = 1215033670

Wed Jul  2 17:21:21 2008
Acct-Status-Type = Stop
NAS-IP-Address = 192.168.12.100
NAS-Port = 5060
Acct-Session-Id = "6edfa77f-f059e59-711c7dce@192.168.11.101"
Acme-Session-Ingress-CallId = "6edfa77f-f059e59-711c7dce@192.168.11.101"
Acme-Session-Egress-CallId = "6edfa77f-f059e59-711c7dce@192.168.11.101"
Acme-Session-Protocol-Type = "SIP"
Calling-Station-Id = ""7812223001"
<sip:7812223001@192.168.11.101>;tag=40335A3-29FEF610"
Called-Station-Id = "<sip:7812223002@192.168.11.101;user=phone>"
Acct-Terminate-Cause = User-Request
Acct-Session-Time = 11
h323-setup-time = "16:43:42.452 EST JUL 02 2008"
h323-connect-time = "16:43:53.517 EST JUL 02 2008"
h323-disconnect-time = "16:44:04.356 EST JUL 02 2008"
h323-disconnect-cause = "1"
Acme-Egress-Network-Interface-Id = "M10"
Acme-Egress-Vlan-Tag-Value = 0
Acme-Ingress-Network-Interface-Id = "M00"
Acme-Ingress-Vlan-Tag-Value = 0
Acme-Session-Egress-Realm = "Core"
Acme-Session-Ingress-Realm = "Peer"
Acme-FlowID_FS1_F = "localhost:65594"
Acme-FlowType_FS1_F = "PCMU"
Acme-Flow-In-Realm_FS1_F = "Peer"
Acme-Flow-In-Src-Addr_FS1_F = 192.168.11.101
Acme-Flow-In-Src-Port_FS1_F = 2224
Acme-Flow-In-Dst-Addr_FS1_F = 192.168.11.100
Acme-Flow-In-Dst-Port_FS1_F = 49188
```

```
Acme-Flow-Out-Realm_FS1_F = "Core"
Acme-Flow-Out-Src-Addr_FS1_F = 192.168.12.100
Acme-Flow-Out-Src-Port_FS1_F = 49152
Acme-Flow-Out-Dst-Addr_FS1_F = 192.168.12.200
Acme-Flow-Out-Dst-Port_FS1_F = 2222
Acme-Calling-RTCP-Packets-Lost_FS1 = 0
Acme-Calling-RTCP-Avg-Jitter_FS1 = 0
Acme-Calling-RTCP-Avg-Latency_FS1 = 0
Acme-Calling-RTCP-MaxJitter_FS1 = 0
Acme-Calling-RTCP-MaxLatency_FS1 = 0
Acme-Calling-RTP-Packets-Lost_FS1 = 0
Acme-Calling-RTP-Avg-Jitter_FS1 = 0
Acme-Calling-RTP-MaxJitter_FS1 = 0
Acme-Calling-Octets_FS1 = 0
Acme-Calling-Packets_FS1 = 0
Acme-FlowID_FS1_R = "localhost:65595"
Acme-FlowType_FS1_R = "PCMU"
Acme-Flow-In-Realm_FS1_R = "Core"
Acme-Flow-In-Src-Addr_FS1_R = 192.168.12.200
Acme-Flow-In-Src-Port_FS1_R = 2222
Acme-Flow-In-Dst-Addr_FS1_R = 192.168.12.100
Acme-Flow-In-Dst-Port_FS1_R = 49152
Acme-Flow-Out-Realm_FS1_R = "Peer"
Acme-Flow-Out-Src-Addr_FS1_R = 192.168.11.100
Acme-Flow-Out-Src-Port_FS1_R = 49188
Acme-Flow-Out-Dst-Addr_FS1_R = 192.168.11.101
Acme-Flow-Out-Dst-Port_FS1_R = 2224
Acme-Called-RTCP-Packets-Lost_FS1 = 0
Acme-Called-RTCP-Avg-Jitter_FS1 = 0
Acme-Called-RTCP-Avg-Latency_FS1 = 0
Acme-Called-RTCP-MaxJitter_FS1 = 0
Acme-Called-RTCP-MaxLatency_FS1 = 0
Acme-Called-RTP-Packets-Lost_FS1 = 0
Acme-Called-RTP-Avg-Jitter_FS1 = 0
Acme-Called-RTP-MaxJitter_FS1 = 0
Acme-Called-Octets_FS1 = 0
Acme-Called-Packets_FS1 = 0
Acme-FlowID_FS2_F = ""
Acme-FlowType_FS2_F = ""
Acme-Flow-In-Realm_FS2_F = ""
Acme-Flow-In-Src-Addr_FS2_F = 0.0.0.0
Acme-Flow-In-Src-Port_FS2_F = 0
Acme-Flow-In-Dst-Addr_FS2_F = 0.0.0.0
Acme-Flow-In-Dst-Port_FS2_F = 0
Acme-Flow-Out-Realm_FS2_F = ""
Acme-Flow-Out-Src-Addr_FS2_F = 0.0.0.0
```

```
Acme-Flow-Out-Src-Port_FS2_F = 0
Acme-Flow-Out-Dst-Addr_FS2_F = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS2_F = 0
Acme-Calling-RTCP-Packets-Lost_FS2 = 0
Acme-Calling-RTCP-Avg-Jitter_FS2 = 0
Acme-Calling-RTCP-Avg-Latency_FS2 = 0
Acme-Calling-RTCP-MaxJitter_FS2 = 0
Acme-Calling-RTCP-MaxLatency_FS2 = 0
Acme-Calling-RTP-Packets-Lost_FS2 = 0
Acme-Calling-RTP-Avg-Jitter_FS2 = 0
Acme-Calling-RTP-MaxJitter_FS2 = 0
Acme-Calling-Octets_FS2 = 0
Acme-Calling-Packets_FS2 = 0
Acme-FlowID_FS2_R = ""
Acme-FlowType_FS2_R = ""
Acme-Flow-In-Realm_FS2_R = ""
Acme-Flow-In-Src-Addr_FS2_R = 0.0.0.0
Acme-Flow-In-Src-Port_FS2_R = 0
Acme-Flow-In-Dst-Addr_FS2_R = 0.0.0.0
Acme-Flow-In-Dst-Port_FS2_R = 0
Acme-Flow-Out-Realm_FS2_R = ""
Acme-Flow-Out-Src-Addr_FS2_R = 0.0.0.0
Acme-Flow-Out-Src-Port_FS2_R = 0
Acme-Flow-Out-Dst-Addr_FS2_R = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS2_R = 0
Acme-Called-RTCP-Packets-Lost_FS2 = 0
Acme-Called-RTCP-Avg-Jitter_FS2 = 0
Acme-Called-RTCP-Avg-Latency_FS2 = 0
Acme-Called-RTCP-MaxJitter_FS2 = 0
Acme-Called-RTCP-MaxLatency_FS2 = 0
Acme-Called-RTP-Packets-Lost_FS2 = 0
Acme-Called-RTP-Avg-Jitter_FS2 = 0
Acme-Called-RTP-MaxJitter_FS2 = 0
Acme-Called-Octets_FS2 = 0
Acme-Called-Packets_FS2 = 0
Acme-Firmware-Version = "C6.0.0 GA (Build 13)"
Acme-Local-Time-Zone = "GMT-05:00"
Acme-Post-Dial-Delay = 223
Acme-Primary-Routing-Number = "sip:7812223002@192.168.11.101;user=phone"
Acme-Ingress-Local-Addr = "192.168.11.100:5060"
Acme-Ingress-Remote-Addr = "192.168.11.101:5060"
Acme-Egress-Local-Addr = "192.168.12.100:5060"
Acme-Egress-Remote-Addr = "192.168.12.200:5060"
Acme-Session-Disposition = 3
Acme-Disconnect-Initiator = 1
Acme-Disconnect-Cause = 0
```

```
Acme-SIP-Status = 0
Acme-Egress-Final-Routing-Number =
"sip:7812223002@192.168.11.101;user=phone"
Acme-CDR-Sequence-Number = 100
Client-IP-Address = 172.30.21.31
Acct-Unique-Session-Id = "5af95b6a3259b428"
Timestamp = 1215033681
```

Unsuccessful SIP Call

The following sample CDRs are for an unsuccessful SIP call.

```
Acct-Status-Type = Stop
NAS-IP-Address = 192.168.12.100
NAS-Port = 5060
Acct-Session-Id = "595e3d3c-e74b9a7e-5924bd1f@192.168.12.200"
Acme-Session-Ingress-CallId = "595e3d3c-e74b9a7e-5924bd1f@192.168.12.200"
Acme-Session-Egress-CallId = "595e3d3c-e74b9a7e-5924bd1f@192.168.12.200"
Acme-Session-Protocol-Type = "SIP"
Calling-Station-Id = ""7812223002"
<sip:7812223002@192.168.12.200>;tag=591ADA30-B9864E09"
Called-Station-Id = "<sip:7812223001@192.168.12.200;user=phone>"
Acct-Terminate-Cause = User-Error
Acct-Session-Time = 0
h323-setup-time = "16:46:09.612 EST JUL 02 2008"
h323-disconnect-time = "16:46:18.762 EST JUL 02 2008"
h323-disconnect-cause = "3"
Acme-Egress-Network-Interface-Id = "M10"
Acme-Egress-Vlan-Tag-Value = 0
Acme-Ingress-Network-Interface-Id = "M10"
Acme-Ingress-Vlan-Tag-Value = 0
Acme-Session-Egress-Realm = "Core"
Acme-Session-Ingress-Realm = "Core"
Acme-FlowID_FS1_F = "localhost:65596"
Acme-FlowType_FS1_F = "PCMU"
Acme-Flow-In-Realm_FS1_F = "Core"
Acme-Flow-In-Src-Addr_FS1_F = 0.0.0.0
Acme-Flow-In-Src-Port_FS1_F = 0
Acme-Flow-In-Dst-Addr_FS1_F = 192.168.12.100
Acme-Flow-In-Dst-Port_FS1_F = 49154
Acme-Flow-Out-Realm_FS1_F = "Core"
Acme-Flow-Out-Src-Addr_FS1_F = 192.168.12.100
Acme-Flow-Out-Src-Port_FS1_F = 49156
Acme-Flow-Out-Dst-Addr_FS1_F = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS1_F = 0
Acme-Calling-RTCP-Packets-Lost_FS1 = 0
Acme-Calling-RTCP-Avg-Jitter_FS1 = 0
Acme-Calling-RTCP-Avg-Latency_FS1 = 0
```

```
Acme-Calling-RTCP-MaxJitter_FS1 = 0
Acme-Calling-RTCP-MaxLatency_FS1 = 0
Acme-Calling-RTP-Packets-Lost_FS1 = 0
Acme-Calling-RTP-Avg-Jitter_FS1 = 0
Acme-Calling-RTP-MaxJitter_FS1 = 0
Acme-Calling-Octets_FS1 = 0
Acme-Calling-Packets_FS1 = 0
Acme-FlowID_FS1_R = "localhost:65597"
Acme-FlowType_FS1_R = "PCMU"
Acme-Flow-In-Realm_FS1_R = "Core"
Acme-Flow-In-Src-Addr_FS1_R = 0.0.0.0
Acme-Flow-In-Src-Port_FS1_R = 0
Acme-Flow-In-Dst-Addr_FS1_R = 192.168.12.100
Acme-Flow-In-Dst-Port_FS1_R = 49156
Acme-Flow-Out-Realm_FS1_R = "Core"
Acme-Flow-Out-Src-Addr_FS1_R = 192.168.12.100
Acme-Flow-Out-Src-Port_FS1_R = 49154
Acme-Flow-Out-Dst-Addr_FS1_R = 192.168.12.200
Acme-Flow-Out-Dst-Port_FS1_R = 2226
Acme-Called-RTCP-Packets-Lost_FS1 = 0
Acme-Called-RTCP-Avg-Jitter_FS1 = 0
Acme-Called-RTCP-Avg-Latency_FS1 = 0
Acme-Called-RTCP-MaxJitter_FS1 = 0
Acme-Called-RTCP-MaxLatency_FS1 = 0
Acme-Called-RTP-Packets-Lost_FS1 = 0
Acme-Called-RTP-Avg-Jitter_FS1 = 0
Acme-Called-RTP-MaxJitter_FS1 = 0
Acme-Called-Octets_FS1 = 0
Acme-Called-Packets_FS1 = 0
Acme-FlowID_FS2_F = ""
Acme-FlowType_FS2_F = ""
Acme-Flow-In-Realm_FS2_F = ""
Acme-Flow-In-Src-Addr_FS2_F = 0.0.0.0
Acme-Flow-In-Src-Port_FS2_F = 0
Acme-Flow-In-Dst-Addr_FS2_F = 0.0.0.0
Acme-Flow-In-Dst-Port_FS2_F = 0
Acme-Flow-Out-Realm_FS2_F = ""
Acme-Flow-Out-Src-Addr_FS2_F = 0.0.0.0
Acme-Flow-Out-Src-Port_FS2_F = 0
Acme-Flow-Out-Dst-Addr_FS2_F = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS2_F = 0
Acme-Calling-RTCP-Packets-Lost_FS2 = 0
Acme-Calling-RTCP-Avg-Jitter_FS2 = 0
Acme-Calling-RTCP-Avg-Latency_FS2 = 0
Acme-Calling-RTCP-MaxJitter_FS2 = 0
Acme-Calling-RTCP-MaxLatency_FS2 = 0
```

```
Acme-Calling-RTP-Packets-Lost_FS2 = 0
Acme-Calling-RTP-Avg-Jitter_FS2 = 0
Acme-Calling-RTP-MaxJitter_FS2 = 0
Acme-Calling-Octets_FS2 = 0
Acme-Calling-Packets_FS2 = 0
Acme-FlowID_FS2_R = ""
Acme-FlowType_FS2_R = ""
Acme-Flow-In-Realm_FS2_R = ""
Acme-Flow-In-Src-Addr_FS2_R = 0.0.0.0
Acme-Flow-In-Src-Port_FS2_R = 0
Acme-Flow-In-Dst-Addr_FS2_R = 0.0.0.0
Acme-Flow-In-Dst-Port_FS2_R = 0
Acme-Flow-Out-Realm_FS2_R = ""
Acme-Flow-Out-Src-Addr_FS2_R = 0.0.0.0
Acme-Flow-Out-Src-Port_FS2_R = 0
Acme-Flow-Out-Dst-Addr_FS2_R = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS2_R = 0
Acme-Called-RTCP-Packets-Lost_FS2 = 0
Acme-Called-RTCP-Avg-Jitter_FS2 = 0
Acme-Called-RTCP-Avg-Latency_FS2 = 0
Acme-Called-RTCP-MaxJitter_FS2 = 0
Acme-Called-RTCP-MaxLatency_FS2 = 0
Acme-Called-RTP-Packets-Lost_FS2 = 0
Acme-Called-RTP-Avg-Jitter_FS2 = 0
Acme-Called-RTP-MaxJitter_FS2 = 0
Acme-Called-Octets_FS2 = 0
Acme-Called-Packets_FS2 = 0
Acme-Firmware-Version = "C6.0.0 GA (Build 13)"
Acme-Local-Time-Zone = "GMT-05:00"
Acme-Post-Dial-Delay = 210
Acme-Primary-Routing-Number = "sip:7812223001@192.168.12.200;user=phone"
Acme-Ingress-Local-Addr = "192.168.12.100:5060"
Acme-Ingress-Remote-Addr = "192.168.12.200:5060"
Acme-Egress-Local-Addr = "192.168.12.100:5060"
Acme-Egress-Remote-Addr = "192.168.12.200:5060"
Acme-Session-Disposition = 2
Acme-Disconnect-Initiator = 1
Acme-Disconnect-Cause = 47
Acme-SIP-Status = 487
Acme-Egress-Final-Routing-Number =
"sip:7812223001@192.168.12.200;user=phone"
Acme-CDR-Sequence-Number = 101
Client-IP-Address = 172.30.21.31
Acct-Unique-Session-Id = "f1c5761c4d973242"
Timestamp = 1215033815
```

SIP Call On Hold

The following sample CDRs are for SIP call on hold.

```
Acct-Status-Type = Start
NAS-IP-Address = 192.168.12.100
NAS-Port = 5060
Acct-Session-Id = "48447425-eb21e8f-d9cc570c@192.168.11.101"
Acme-Session-Ingress-CallId = "48447425-eb21e8f-d9cc570c@192.168.11.101"
Acme-Session-Egress-CallId = "48447425-eb21e8f-d9cc570c@192.168.11.101"
Acme-Session-Protocol-Type = "SIP"
Calling-Station-Id = ""7812223001"
<sip:7812223001@192.168.11.101>;tag=29749EE9-79CDC11E"
Called-Station-Id = "<sip:7812223002@192.168.11.101;user=phone>"
h323-setup-time = "16:47:28.630 EST JUL 02 2008"
h323-connect-time = "16:47:34.016 EST JUL 02 2008"
Acme-Egress-Network-Interface-Id = "M10"
Acme-Egress-Vlan-Tag-Value = 0
Acme-Ingress-Network-Interface-Id = "M00"
Acme-Ingress-Vlan-Tag-Value = 0
Acme-Session-Egress-Realm = "Core"
Acme-Session-Ingress-Realm = "Peer"
Acme-FlowID_FS1_F = "localhost:65598"
Acme-FlowType_FS1_F = "PCMU"
Acme-Flow-In-Realm_FS1_F = "Peer"
Acme-Flow-In-Src-Addr_FS1_F = 0.0.0.0
Acme-Flow-In-Src-Port_FS1_F = 0
Acme-Flow-In-Dst-Addr_FS1_F = 192.168.11.100
Acme-Flow-In-Dst-Port_FS1_F = 49190
Acme-Flow-Out-Realm_FS1_F = "Core"
Acme-Flow-Out-Src-Addr_FS1_F = 192.168.12.100
Acme-Flow-Out-Src-Port_FS1_F = 49158
Acme-Flow-Out-Dst-Addr_FS1_F = 192.168.12.200
Acme-Flow-Out-Dst-Port_FS1_F = 2228
Acme-FlowID_FS1_R = "localhost:65599"
Acme-FlowType_FS1_R = "PCMU"
Acme-Flow-In-Realm_FS1_R = "Core"
Acme-Flow-In-Src-Addr_FS1_R = 0.0.0.0
Acme-Flow-In-Src-Port_FS1_R = 0
Acme-Flow-In-Dst-Addr_FS1_R = 192.168.12.100
Acme-Flow-In-Dst-Port_FS1_R = 49158
Acme-Flow-Out-Realm_FS1_R = "Peer"
Acme-Flow-Out-Src-Addr_FS1_R = 192.168.11.100
Acme-Flow-Out-Src-Port_FS1_R = 49190
Acme-Flow-Out-Dst-Addr_FS1_R = 192.168.11.101
Acme-Flow-Out-Dst-Port_FS1_R = 2226
Acme-FlowID_FS2_F = ""
Acme-FlowType_FS2_F = ""
Acme-Flow-In-Realm_FS2_F = ""
```

```
Acme-Flow-In-Src-Addr_FS2_F = 0.0.0.0
Acme-Flow-In-Src-Port_FS2_F = 0
Acme-Flow-In-Dst-Addr_FS2_F = 0.0.0.0
Acme-Flow-In-Dst-Port_FS2_F = 0
Acme-Flow-Out-Realm_FS2_F = ""
Acme-Flow-Out-Src-Addr_FS2_F = 0.0.0.0
Acme-Flow-Out-Src-Port_FS2_F = 0
Acme-Flow-Out-Dst-Addr_FS2_F = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS2_F = 0
Acme-FlowID_FS2_R = ""
Acme-FlowType_FS2_R = ""
Acme-Flow-In-Realm_FS2_R = ""
Acme-Flow-In-Src-Addr_FS2_R = 0.0.0.0
Acme-Flow-In-Src-Port_FS2_R = 0
Acme-Flow-In-Dst-Addr_FS2_R = 0.0.0.0
Acme-Flow-In-Dst-Port_FS2_R = 0
Acme-Flow-Out-Realm_FS2_R = ""
Acme-Flow-Out-Src-Addr_FS2_R = 0.0.0.0
Acme-Flow-Out-Src-Port_FS2_R = 0
Acme-Flow-Out-Dst-Addr_FS2_R = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS2_R = 0
Acme-Firmware-Version = "C6.0.0 GA (Build 13)"
Acme-Local-Time-Zone = "GMT-05:00"
Acme-Post-Dial-Delay = 217
Acme-Primary-Routing-Number = "sip:7812223002@192.168.11.101;user=phone"
Acme-Ingress-Local-Addr = "192.168.11.100:5060"
Acme-Ingress-Remote-Addr = "192.168.11.101:5060"
Acme-Egress-Local-Addr = "192.168.12.100:5060"
Acme-Egress-Remote-Addr = "192.168.12.200:5060"
Acme-Egress-Final-Routing-Number =
"sip:7812223002@192.168.11.101;user=phone"
Acme-CDR-Sequence-Number = 102
Client-IP-Address = 172.30.21.31
Acct-Unique-Session-Id = "972a994cb16bcdc0"
Timestamp = 1215033890

Wed Jul  2 17:24:59 2008
Acct-Status-Type = Interim-Update
NAS-IP-Address = 192.168.12.100
NAS-Port = 5060
Acct-Session-Id = "48447425-eb21e8f-d9cc570c@192.168.11.101"
Acme-Session-Ingress-CallId = "48447425-eb21e8f-d9cc570c@192.168.11.101"
Acme-Session-Egress-CallId = "48447425-eb21e8f-d9cc570c@192.168.11.101"
Acme-Session-Protocol-Type = "SIP"
Calling-Station-Id = ""7812223001"
<sip:7812223001@192.168.11.101>;tag=29749EE9-79CDC11E"
Called-Station-Id = "<sip:7812223002@192.168.11.101;user=phone>"
```

```
h323-setup-time = "16:47:28.630 EST JUL 02 2008"
h323-connect-time = "16:47:34.016 EST JUL 02 2008"
Acme-Egress-Network-Interface-Id = "M10"
Acme-Egress-Vlan-Tag-Value = 0
Acme-Ingress-Network-Interface-Id = "M00"
Acme-Ingress-Vlan-Tag-Value = 0
Acme-Session-Egress-Realm = "Core"
Acme-Session-Ingress-Realm = "Peer"
Acme-FlowID_FS1_F = "localhost:65598"
Acme-FlowType_FS1_F = "PCMU"
Acme-Flow-In-Realm_FS1_F = "Peer"
Acme-Flow-In-Src-Addr_FS1_F = 0.0.0.0
Acme-Flow-In-Src-Port_FS1_F = 0
Acme-Flow-In-Dst-Addr_FS1_F = 192.168.11.100
Acme-Flow-In-Dst-Port_FS1_F = 49190
Acme-Flow-Out-Realm_FS1_F = "Core"
Acme-Flow-Out-Src-Addr_FS1_F = 192.168.12.100
Acme-Flow-Out-Src-Port_FS1_F = 49158
Acme-Flow-Out-Dst-Addr_FS1_F = 192.168.12.200
Acme-Flow-Out-Dst-Port_FS1_F = 2228
Acme-Calling-RTCP-Packets-Lost_FS1 = 0
Acme-Calling-RTCP-Avg-Jitter_FS1 = 0
Acme-Calling-RTCP-Avg-Latency_FS1 = 0
Acme-Calling-RTCP-MaxJitter_FS1 = 0
Acme-Calling-RTCP-MaxLatency_FS1 = 0
Acme-Calling-RTP-Packets-Lost_FS1 = 0
Acme-Calling-RTP-Avg-Jitter_FS1 = 0
Acme-Calling-RTP-MaxJitter_FS1 = 0
Acme-Calling-Octets_FS1 = 0
Acme-Calling-Packets_FS1 = 0
Acme-FlowID_FS1_R = "localhost:65599"
Acme-FlowType_FS1_R = "PCMU"
Acme-Flow-In-Realm_FS1_R = "Core"
Acme-Flow-In-Src-Addr_FS1_R = 0.0.0.0
Acme-Flow-In-Src-Port_FS1_R = 0
Acme-Flow-In-Dst-Addr_FS1_R = 192.168.12.100
Acme-Flow-In-Dst-Port_FS1_R = 49158
Acme-Flow-Out-Realm_FS1_R = "Peer"
Acme-Flow-Out-Src-Addr_FS1_R = 192.168.11.100
Acme-Flow-Out-Src-Port_FS1_R = 49190
Acme-Flow-Out-Dst-Addr_FS1_R = 192.168.11.101
Acme-Flow-Out-Dst-Port_FS1_R = 2226
Acme-Called-RTCP-Packets-Lost_FS1 = 0
Acme-Called-RTCP-Avg-Jitter_FS1 = 0
Acme-Called-RTCP-Avg-Latency_FS1 = 0
Acme-Called-RTCP-MaxJitter_FS1 = 0
```

```
Acme-Called-RTCP-MaxLatency_FS1 = 0
Acme-Called-RTP-Packets-Lost_FS1 = 0
Acme-Called-RTP-Avg-Jitter_FS1 = 0
Acme-Called-RTP-MaxJitter_FS1 = 0
Acme-Called-Octets_FS1 = 0
Acme-Called-Packets_FS1 = 0
Acme-FlowID_FS2_F = ""
Acme-FlowType_FS2_F = ""
Acme-Flow-In-Realm_FS2_F = ""
Acme-Flow-In-Src-Addr_FS2_F = 0.0.0.0
Acme-Flow-In-Src-Port_FS2_F = 0
Acme-Flow-In-Dst-Addr_FS2_F = 0.0.0.0
Acme-Flow-In-Dst-Port_FS2_F = 0
Acme-Flow-Out-Realm_FS2_F = ""
Acme-Flow-Out-Src-Addr_FS2_F = 0.0.0.0
Acme-Flow-Out-Src-Port_FS2_F = 0
Acme-Flow-Out-Dst-Addr_FS2_F = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS2_F = 0
Acme-Calling-RTCP-Packets-Lost_FS2 = 0
Acme-Calling-RTCP-Avg-Jitter_FS2 = 0
Acme-Calling-RTCP-Avg-Latency_FS2 = 0
Acme-Calling-RTCP-MaxJitter_FS2 = 0
Acme-Calling-RTCP-MaxLatency_FS2 = 0
Acme-Calling-RTP-Packets-Lost_FS2 = 0
Acme-Calling-RTP-Avg-Jitter_FS2 = 0
Acme-Calling-RTP-MaxJitter_FS2 = 0
Acme-Calling-Octets_FS2 = 0
Acme-Calling-Packets_FS2 = 0
Acme-FlowID_FS2_R = ""
Acme-FlowType_FS2_R = ""
Acme-Flow-In-Realm_FS2_R = ""
Acme-Flow-In-Src-Addr_FS2_R = 0.0.0.0
Acme-Flow-In-Src-Port_FS2_R = 0
Acme-Flow-In-Dst-Addr_FS2_R = 0.0.0.0
Acme-Flow-In-Dst-Port_FS2_R = 0
Acme-Flow-Out-Realm_FS2_R = ""
Acme-Flow-Out-Src-Addr_FS2_R = 0.0.0.0
Acme-Flow-Out-Src-Port_FS2_R = 0
Acme-Flow-Out-Dst-Addr_FS2_R = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS2_R = 0
Acme-Called-RTCP-Packets-Lost_FS2 = 0
Acme-Called-RTCP-Avg-Jitter_FS2 = 0
Acme-Called-RTCP-Avg-Latency_FS2 = 0
Acme-Called-RTCP-MaxJitter_FS2 = 0
Acme-Called-RTCP-MaxLatency_FS2 = 0
Acme-Called-RTP-Packets-Lost_FS2 = 0
```

```
Acme-Called-RTP-Avg-Jitter_FS2 = 0
Acme-Called-RTP-MaxJitter_FS2 = 0
Acme-Called-Octets_FS2 = 0
Acme-Called-Packets_FS2 = 0
Acme-Firmware-Version = "C6.0.0 GA (Build 13)"
Acme-Local-Time-Zone = "GMT-05:00"
Acme-Post-Dial-Delay = 217
Acme-Primary-Routing-Number = "sip:7812223002@192.168.11.101;user=phone"
Acme-Ingress-Local-Addr = "192.168.11.100:5060"
Acme-Ingress-Remote-Addr = "192.168.11.101:5060"
Acme-Egress-Local-Addr = "192.168.12.100:5060"
Acme-Egress-Remote-Addr = "192.168.12.200:5060"
Acme-Intermediate_Time = "16:47:42.877 EST JUL 02 2008"
Acme-Egress-Final-Routing-Number =
"sip:7812223002@192.168.11.101;user=phone"
Acme-CDR-Sequence-Number = 103
Client-IP-Address = 172.30.21.31
Acct-Unique-Session-Id = "972a994cb16bcdc0"
Timestamp = 1215033899

Wed Jul  2 17:25:04 2008
Acct-Status-Type = Interim-Update
NAS-IP-Address = 192.168.12.100
NAS-Port = 5060
Acct-Session-Id = "48447425-eb21e8f-d9cc570c@192.168.11.101"
Acme-Session-Ingress-CallId = "48447425-eb21e8f-d9cc570c@192.168.11.101"
Acme-Session-Egress-CallId = "48447425-eb21e8f-d9cc570c@192.168.11.101"
Acme-Session-Protocol-Type = "SIP"
Calling-Station-Id = ""7812223001"
<sip:7812223001@192.168.11.101>;tag=29749EE9-79CDC11E"
Called-Station-Id = "<sip:7812223002@192.168.11.101;user=phone>"
h323-setup-time = "16:47:28.630 EST JUL 02 2008"
h323-connect-time = "16:47:34.016 EST JUL 02 2008"
Acme-Egress-Network-Interface-Id = "M10"
Acme-Egress-Vlan-Tag-Value = 0
Acme-Ingress-Network-Interface-Id = "M00"
Acme-Ingress-Vlan-Tag-Value = 0
Acme-Session-Egress-Realm = "Core"
Acme-Session-Ingress-Realm = "Peer"
Acme-FlowID_FS1_F = "localhost:65598"
Acme-FlowType_FS1_F = "PCMU"
Acme-Flow-In-Realm_FS1_F = "Peer"
Acme-Flow-In-Src-Addr_FS1_F = 0.0.0.0
Acme-Flow-In-Src-Port_FS1_F = 0
Acme-Flow-In-Dst-Addr_FS1_F = 192.168.11.100
Acme-Flow-In-Dst-Port_FS1_F = 49190
Acme-Flow-Out-Realm_FS1_F = "Core"
```

```
Acme-Flow-Out-Src-Addr_FS1_F = 192.168.12.100
Acme-Flow-Out-Src-Port_FS1_F = 49158
Acme-Flow-Out-Dst-Addr_FS1_F = 192.168.12.200
Acme-Flow-Out-Dst-Port_FS1_F = 2228
Acme-Calling-RTCP-Packets-Lost_FS1 = 0
Acme-Calling-RTCP-Avg-Jitter_FS1 = 0
Acme-Calling-RTCP-Avg-Latency_FS1 = 0
Acme-Calling-RTCP-MaxJitter_FS1 = 0
Acme-Calling-RTCP-MaxLatency_FS1 = 0
Acme-Calling-RTP-Packets-Lost_FS1 = 0
Acme-Calling-RTP-Avg-Jitter_FS1 = 0
Acme-Calling-RTP-MaxJitter_FS1 = 0
Acme-Calling-Octets_FS1 = 0
Acme-Calling-Packets_FS1 = 0
Acme-FlowID_FS1_R = "localhost:65599"
Acme-FlowType_FS1_R = "PCMU"
Acme-Flow-In-Realm_FS1_R = "Core"
Acme-Flow-In-Src-Addr_FS1_R = 0.0.0.0
Acme-Flow-In-Src-Port_FS1_R = 0
Acme-Flow-In-Dst-Addr_FS1_R = 192.168.12.100
Acme-Flow-In-Dst-Port_FS1_R = 49158
Acme-Flow-Out-Realm_FS1_R = "Peer"
Acme-Flow-Out-Src-Addr_FS1_R = 192.168.11.100
Acme-Flow-Out-Src-Port_FS1_R = 49190
Acme-Flow-Out-Dst-Addr_FS1_R = 192.168.11.101
Acme-Flow-Out-Dst-Port_FS1_R = 2226
Acme-Called-RTCP-Packets-Lost_FS1 = 0
Acme-Called-RTCP-Avg-Jitter_FS1 = 0
Acme-Called-RTCP-Avg-Latency_FS1 = 0
Acme-Called-RTCP-MaxJitter_FS1 = 0
Acme-Called-RTCP-MaxLatency_FS1 = 0
Acme-Called-RTP-Packets-Lost_FS1 = 0
Acme-Called-RTP-Avg-Jitter_FS1 = 0
Acme-Called-RTP-MaxJitter_FS1 = 0
Acme-Called-Octets_FS1 = 0
Acme-Called-Packets_FS1 = 0
Acme-FlowID_FS2_F = ""
Acme-FlowType_FS2_F = ""
Acme-Flow-In-Realm_FS2_F = ""
Acme-Flow-In-Src-Addr_FS2_F = 0.0.0.0
Acme-Flow-In-Src-Port_FS2_F = 0
Acme-Flow-In-Dst-Addr_FS2_F = 0.0.0.0
Acme-Flow-In-Dst-Port_FS2_F = 0
Acme-Flow-Out-Realm_FS2_F = ""
Acme-Flow-Out-Src-Addr_FS2_F = 0.0.0.0
Acme-Flow-Out-Src-Port_FS2_F = 0
```

```
Acme-Flow-Out-Dst-Addr_FS2_F = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS2_F = 0
Acme-Calling-RTCP-Packets-Lost_FS2 = 0
Acme-Calling-RTCP-Avg-Jitter_FS2 = 0
Acme-Calling-RTCP-Avg-Latency_FS2 = 0
Acme-Calling-RTCP-MaxJitter_FS2 = 0
Acme-Calling-RTCP-MaxLatency_FS2 = 0
Acme-Calling-RTP-Packets-Lost_FS2 = 0
Acme-Calling-RTP-Avg-Jitter_FS2 = 0
Acme-Calling-RTP-MaxJitter_FS2 = 0
Acme-Calling-Octets_FS2 = 0
Acme-Calling-Packets_FS2 = 0
Acme-FlowID_FS2_R = ""
Acme-FlowType_FS2_R = ""
Acme-Flow-In-Realm_FS2_R = ""
Acme-Flow-In-Src-Addr_FS2_R = 0.0.0.0
Acme-Flow-In-Src-Port_FS2_R = 0
Acme-Flow-In-Dst-Addr_FS2_R = 0.0.0.0
Acme-Flow-In-Dst-Port_FS2_R = 0
Acme-Flow-Out-Realm_FS2_R = ""
Acme-Flow-Out-Src-Addr_FS2_R = 0.0.0.0
Acme-Flow-Out-Src-Port_FS2_R = 0
Acme-Flow-Out-Dst-Addr_FS2_R = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS2_R = 0
Acme-Called-RTCP-Packets-Lost_FS2 = 0
Acme-Called-RTCP-Avg-Jitter_FS2 = 0
Acme-Called-RTCP-Avg-Latency_FS2 = 0
Acme-Called-RTCP-MaxJitter_FS2 = 0
Acme-Called-RTCP-MaxLatency_FS2 = 0
Acme-Called-RTP-Packets-Lost_FS2 = 0
Acme-Called-RTP-Avg-Jitter_FS2 = 0
Acme-Called-RTP-MaxJitter_FS2 = 0
Acme-Called-Octets_FS2 = 0
Acme-Called-Packets_FS2 = 0
Acme-Firmware-Version = "C6.0.0 GA (Build 13)"
Acme-Local-Time-Zone = "GMT-05:00"
Acme-Post-Dial-Delay = 217
Acme-Primary-Routing-Number = "sip:7812223002@192.168.11.101;user=phone"
Acme-Ingress-Local-Addr = "192.168.11.100:5060"
Acme-Ingress-Remote-Addr = "192.168.11.101:5060"
Acme-Egress-Local-Addr = "192.168.12.100:5060"
Acme-Egress-Remote-Addr = "192.168.12.200:5060"
Acme-Intermediate_Time = "16:47:47.186 EST JUL 02 2008"
Acme-Egress-Final-Routing-Number =
"sip:7812223002@192.168.11.101;user=phone"
Acme-CDR-Sequence-Number = 104
Client-IP-Address = 172.30.21.31
```

```
Acct-Unique-Session-Id = "972a994cb16bcdc0"
Timestamp = 1215033904

Wed Jul  2 17:25:09 2008
Acct-Status-Type = Stop
NAS-IP-Address = 192.168.12.100
NAS-Port = 5060
Acct-Session-Id = "48447425-eb21e8f-d9cc570c@192.168.11.101"
Acme-Session-Ingress-CallId = "48447425-eb21e8f-d9cc570c@192.168.11.101"
Acme-Session-Egress-CallId = "48447425-eb21e8f-d9cc570c@192.168.11.101"
Acme-Session-Protocol-Type = "SIP"
Calling-Station-Id = ""7812223001"
<sip:7812223001@192.168.11.101>;tag=29749EE9-79CDC11E"
Called-Station-Id = "<sip:7812223002@192.168.11.101;user=phone>"
Acct-Terminate-Cause = User-Request
Acct-Session-Time = 18
h323-setup-time = "16:47:28.630 EST JUL 02 2008"
h323-connect-time = "16:47:34.016 EST JUL 02 2008"
h323-disconnect-time = "16:47:52.721 EST JUL 02 2008"
h323-disconnect-cause = "1"
Acme-Egress-Network-Interface-Id = "M10"
Acme-Egress-Vlan-Tag-Value = 0
Acme-Ingress-Network-Interface-Id = "M00"
Acme-Ingress-Vlan-Tag-Value = 0
Acme-Session-Egress-Realm = "Core"
Acme-Session-Ingress-Realm = "Peer"
Acme-FlowID_FS1_F = "localhost:65598"
Acme-FlowType_FS1_F = "PCMU"
Acme-Flow-In-Realm_FS1_F = "Peer"
Acme-Flow-In-Src-Addr_FS1_F = 192.168.11.101
Acme-Flow-In-Src-Port_FS1_F = 2226
Acme-Flow-In-Dst-Addr_FS1_F = 192.168.11.100
Acme-Flow-In-Dst-Port_FS1_F = 49190
Acme-Flow-Out-Realm_FS1_F = "Core"
Acme-Flow-Out-Src-Addr_FS1_F = 192.168.12.100
Acme-Flow-Out-Src-Port_FS1_F = 49158
Acme-Flow-Out-Dst-Addr_FS1_F = 192.168.12.200
Acme-Flow-Out-Dst-Port_FS1_F = 2228
Acme-Calling-RTCP-Packets-Lost_FS1 = 0
Acme-Calling-RTCP-Avg-Jitter_FS1 = 0
Acme-Calling-RTCP-Avg-Latency_FS1 = 0
Acme-Calling-RTCP-MaxJitter_FS1 = 0
Acme-Calling-RTCP-MaxLatency_FS1 = 0
Acme-Calling-RTP-Packets-Lost_FS1 = 0
Acme-Calling-RTP-Avg-Jitter_FS1 = 0
Acme-Calling-RTP-MaxJitter_FS1 = 0
Acme-Calling-Octets_FS1 = 0
```

```
Acme-Calling-Packets_FS1 = 0
Acme-FlowID_FS1_R = "localhost:65599"
Acme-FlowType_FS1_R = "PCMU"
Acme-Flow-In-Realm_FS1_R = "Core"
Acme-Flow-In-Src-Addr_FS1_R = 192.168.12.200
Acme-Flow-In-Src-Port_FS1_R = 2228
Acme-Flow-In-Dst-Addr_FS1_R = 192.168.12.100
Acme-Flow-In-Dst-Port_FS1_R = 49158
Acme-Flow-Out-Realm_FS1_R = "Peer"
Acme-Flow-Out-Src-Addr_FS1_R = 192.168.11.100
Acme-Flow-Out-Src-Port_FS1_R = 49190
Acme-Flow-Out-Dst-Addr_FS1_R = 192.168.11.101
Acme-Flow-Out-Dst-Port_FS1_R = 2226
Acme-Called-RTCP-Packets-Lost_FS1 = 0
Acme-Called-RTCP-Avg-Jitter_FS1 = 0
Acme-Called-RTCP-Avg-Latency_FS1 = 0
Acme-Called-RTCP-MaxJitter_FS1 = 0
Acme-Called-RTCP-MaxLatency_FS1 = 0
Acme-Called-RTP-Packets-Lost_FS1 = 0
Acme-Called-RTP-Avg-Jitter_FS1 = 0
Acme-Called-RTP-MaxJitter_FS1 = 0
Acme-Called-Octets_FS1 = 0
Acme-Called-Packets_FS1 = 0
Acme-FlowID_FS2_F = ""
Acme-FlowType_FS2_F = ""
Acme-Flow-In-Realm_FS2_F = ""
Acme-Flow-In-Src-Addr_FS2_F = 0.0.0.0
Acme-Flow-In-Src-Port_FS2_F = 0
Acme-Flow-In-Dst-Addr_FS2_F = 0.0.0.0
Acme-Flow-In-Dst-Port_FS2_F = 0
Acme-Flow-Out-Realm_FS2_F = ""
Acme-Flow-Out-Src-Addr_FS2_F = 0.0.0.0
Acme-Flow-Out-Src-Port_FS2_F = 0
Acme-Flow-Out-Dst-Addr_FS2_F = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS2_F = 0
Acme-Calling-RTCP-Packets-Lost_FS2 = 0
Acme-Calling-RTCP-Avg-Jitter_FS2 = 0
Acme-Calling-RTCP-Avg-Latency_FS2 = 0
Acme-Calling-RTCP-MaxJitter_FS2 = 0
Acme-Calling-RTCP-MaxLatency_FS2 = 0
Acme-Calling-RTP-Packets-Lost_FS2 = 0
Acme-Calling-RTP-Avg-Jitter_FS2 = 0
Acme-Calling-RTP-MaxJitter_FS2 = 0
Acme-Calling-Octets_FS2 = 0
Acme-Calling-Packets_FS2 = 0
Acme-FlowID_FS2_R = ""
```

```
Acme-FlowType_FS2_R = ""
Acme-Flow-In-Realm_FS2_R = ""
Acme-Flow-In-Src-Addr_FS2_R = 0.0.0.0
Acme-Flow-In-Src-Port_FS2_R = 0
Acme-Flow-In-Dst-Addr_FS2_R = 0.0.0.0
Acme-Flow-In-Dst-Port_FS2_R = 0
Acme-Flow-Out-Realm_FS2_R = ""
Acme-Flow-Out-Src-Addr_FS2_R = 0.0.0.0
Acme-Flow-Out-Src-Port_FS2_R = 0
Acme-Flow-Out-Dst-Addr_FS2_R = 0.0.0.0
Acme-Flow-Out-Dst-Port_FS2_R = 0
Acme-Called-RTCP-Packets-Lost_FS2 = 0
Acme-Called-RTCP-Avg-Jitter_FS2 = 0
Acme-Called-RTCP-Avg-Latency_FS2 = 0
Acme-Called-RTCP-MaxJitter_FS2 = 0
Acme-Called-RTCP-MaxLatency_FS2 = 0
Acme-Called-RTP-Packets-Lost_FS2 = 0
Acme-Called-RTP-Avg-Jitter_FS2 = 0
Acme-Called-RTP-MaxJitter_FS2 = 0
Acme-Called-Octets_FS2 = 0
Acme-Called-Packets_FS2 = 0
Acme-Firmware-Version = "C6.0.0 GA (Build 13)"
Acme-Local-Time-Zone = "GMT-05:00"
Acme-Post-Dial-Delay = 217
Acme-Primary-Routing-Number = "sip:7812223002@192.168.11.101;user=phone"
Acme-Ingress-Local-Addr = "192.168.11.100:5060"
Acme-Ingress-Remote-Addr = "192.168.11.101:5060"
Acme-Egress-Local-Addr = "192.168.12.100:5060"
Acme-Egress-Remote-Addr = "192.168.12.200:5060"
Acme-Session-Disposition = 3
Acme-Disconnect-Initiator = 1
Acme-Disconnect-Cause = 0
Acme-SIP-Status = 0
Acme-Egress-Final-Routing-Number =
"sip:7812223002@192.168.11.101;user=phone"
Acme-CDR-Sequence-Number = 105
Client-IP-Address = 172.30.21.31
Acct-Unique-Session-Id = "972a994cb16bcdc0"
Timestamp = 1215033909
```

Appendix B
Comma-Delimited Entries for Local Files

Local File Format

Appendix C contains three tables that show where, in locally-generated CSV files, specific VSAs appear. There is one table for each of the following type of record: Start, Stop, Interim.

For more information about this feature and how to enable it, refer to the Local CDR Storage and FTP Push (57) section in this guide's Configuring Accounting (39) chapter.

Start Record CSV Placement

CSV Placement	Attribute Name	VSA ID Number
1	Acct-Status-Type	
2	NAS-IP-Address	
3	NAS-Port	
4	Acct-Session-Id	
5	Acme-Session-Ingress-CallId	3
6	Acme-Session–Egress-CallId	4
7	Acme-Session-Protocol-Type	43
8	Acme-Session–Generic-Id	40
9	Calling-Station-Id	31
10	Called-Station-Id	30
11	h323-setup-time	
12	h323-connect-time	
13	Acme-Egress-Network-Interface-Id	139
14	Acme-Egress-Vlan-Tag-Value	140
15	Acme-Ingress-Network-Interface-Id	137
16	Acme-Ingress-Vlan-Tag-Value	138
17	Acme-Session-Egress-Realm	42
18	Acme-Session-Ingress-Realm	41
19	Acme-FlowId_FS1_F	1
20	Acme-FlowType_FS1_F	2
21	Acme-Flow-In-Realm_FS1_F	10
22	Acme-Flow-In-Src-Addr_FS1_F	11
23	Acme-Flow-In-Src-Port_FS1_F	12
24	Acme-Flow-In-Dst-Addr_FS1_F	13

CSV Placement	Attribute Name	VSA ID Number
25	Acme-Flow-In-Dst-Port_FS1_F	14
26	Acme-Flow-Out-Realm_FS1_F	20
27	Acme-Flow-Out-Src-Addr_FS1_F	21
28	Acme-Flow-Out-Src-Port_FS1_F	22
29	Acme-Flow-Out-Dst-Addr_FS1_F	23
30	Acme-Flow-Out-Dst-Port_FS1_F	24
31	Acme-FlowID_FS1_R	78
32	Acme-FlowType_FS1_R	79
33	Acme-Flow-In-Realm_FS1_R	80
34	Acme-Flow-In-Src-Addr_FS1_R	81
35	Acme-Flow-In-Src-Port_FS1_R	82
36	Acme-Flow-In-Dst-Addr_FS1_R	83
37	Acme-Flow-In-Dst-Port_FS1_R	84
38	Acme-Flow-Out-Realm_FS1_R	85
39	Acme-Flow-Out-Src-Addr_FS1_R	86
40	Acme-Flow-Out-Src-Port_FS1_R	87
41	Acme-Flow-Out-Dst-Addr_FS1_R	88
42	Acme-Flow-Out-Dst-Port_FS1_R	89
43	Acme-FlowID_FS2_F	90
44	Acme-FlowType_FS2_F	91
45	Acme-Flow-In-Realm_FS2_F	92
46	Acme-Flow-In-Src-Addr_FS2_F	93
47	Acme-Flow-In-Src-Port_FS2_F	94
48	Acme-Flow-In-Dst-Addr_FS2_F	95
49	Acme-Flow-In-Dst-Port_FS2_F	96
50	Acme-Flow-Out-Realm_FS2_F	97
51	Acme-Flow-Out-Src-Addr_FS2_F	98
52	Acme-Flow-Out-Src-Port_FS2_F	99
53	Acme-Flow-Out-Dst-Addr_FS2_F	100
54	Acme-Flow-Out-Dst-Port_FS2_F	101
55	Acme-FlowID_FS2_R	112
56	Acme-FlowType_FS2_R	113
57	Acme-Flow-In-Realm_FS2_R	114
58	Acme-Flow-In-Src-Addr_FS2_R	115

CSV Placement	Attribute Name	VSA ID Number
59	Acme-Flow-In-Src-Port_FS2_R	116
60	Acme-Flow-In-Dst-Addr_FS2_R	117
61	Acme-Flow-In-Dst-Port_FS2_R	118
62	Acme-Flow-Out-Realm_FS2_R	119
63	Acme-Flow-Out-Src-Addr_FS2_R	120
64	Acme-Flow-Out-Src-Port_FS2_R	121
65	Acme-Flow-Out-Dst-Addr_FS2_R	122
66	Acme-Flow-Out-Dst-Port_FS2_R	123
67	Acme-Session-Charging-Vector	54
68	Acme-Session-Charging-Function_Address	55
69	Acme-Firmware-Version	56
70	Acme-Local-Time-Zone	57
71	Acme-Post-Dial-Delay	58
72	Acme-Primary-Routing-Number	64
73	Acme-Originating-Trunk-Group	65
74	Acme-Terminating-Trunk-Group	66
75	Acme-Originating-Trunk-Context	67
76	Acme-Terminating-Trunk-Context	68
77	Acme-P-Asserted-ID	69
78	Acme-Ingress-Local-Addr	74
79	Acme-Ingress-Remote-Addr	75
80	Acme-Egress-Local-Addr	76
81	Acme-Egress-Remote-Addr	77
82	Acme-SIP-Diversion	70
83	Acme-Egress-Final-Routing-Number	134
84	Acme-Session-Ingress-RPH	135
85	Acme-Session-Egress-RPH	136
86	Acme-Custom-VSA-200	200
87	Acme-Custom-VSA-201	201
88	Acme-Custom-VSA-202	202
89	Acme-Custom-VSA-203	203
90	Acme-Custom-VSA-204	204
91	Acme-Custom-VSA-205	205
92	Acme-Custom-VSA-206	206

CSV Placement	Attribute Name	VSA ID Number
93	Acme-Custom-VSA-207	207
94	Acme-Custom-VSA-208	208
95	Acme-Custom-VSA-209	209
96	Acme-Custom-VSA-210	210
97	Acme-Custom-VSA-211	211
98	Acme-Custom-VSA-212	212
99	Acme-Custom-VSA-213	213
100	Acme-Custom-VSA-214	214
101	Acme-Custom-VSA-215	215
102	Acme-Custom-VSA-216	216
103	Acme-Custom-VSA-217	217
104	Acme-Custom-VSA-218	218
105	Acme-Custom-VSA-219	219
106	Acme-Custom-VSA-220	220
107	Acme-Custom-VSA-221	221
108	Acme-Custom-VSA-222	222
109	Acme-Custom-VSA-223	223
110	Acme-Custom-VSA-224	224
111	Acme-Custom-VSA-225	225
112	Acme-Custom-VSA-226	226
113	Acme-Custom-VSA-227	227
114	Acme-Custom-VSA-228	228
115	Acme-Custom-VSA-229	229
116	Acme-Custom-VSA-230	230

Interim Record CSV Placement

CSV Placement	Attribute Name	VSA ID Number
1	Acct-Status-Type	
2	NAS-IP-Address	
3	NAS-Port	
4	Acct-Session-Id	
5	Acme-Session-Ingress-CallId	3
6	Acme-Session–Egress-CallId	4

CSV Placement	Attribute Name	VSA ID Number
7	Acme-Session-Protocol-Type	43
8	Acme-Session–Generic-Id	40
9	Calling-Station-Id	31
10	Called-Station-Id	30
11	h323-setup-time	
12	h323-connect-time	
13	Acme-Egress-Network-Interface-Id	139
14	Acme-Egress-Vlan-Tag-Value	140
15	Acme-Ingress-Network-Interface-Id	137
16	Acme-Ingress-Vlan-Tag-Value	138
17	Acme-Session-Egress-Realm	42
18	Acme-Session-Ingress-Realm	41
19	Acme-FlowId_FS1_F	1
20	Acme-FlowType_FS1_F	2
21	Acme-Flow-In-Realm_FS1_F	10
22	Acme-Flow-In-Src-Addr_FS1_F	11
23	Acme-Flow-In-Src-Port_FS1_F	12
24	Acme-Flow-In-Dst-Addr_FS1_F	13
25	Acme-Flow-In-Dst-Port_FS1_F	14
26	Acme-Flow-Out-Realm_FS1_F	20
27	Acme-Flow-Out-Src-Addr_FS1_F	21
28	Acme-Flow-Out-Src-Port_FS1_F	22
29	Acme-Flow-Out-Dst-Addr_FS1_F	23
30	Acme-Flow-Out-Dst-Port_FS1_F	24
31	Acme-Calling-RTCP-Packets-Lost_FS1	32
32	Acme-Calling-RTCP-Avg-Jitter_FS1	33
33	Acme-Calling-RTCP-Avg-Latency_FS1	34
34	Acme-Calling-RTCP-MaxJitter_FS1	35
35	Acme-Calling-RTCP-MaxLatency_FS1	36
36	Acme-Calling-RTP-Packets-Lost_FS1	37
37	Acme-Calling-RTP-Avg-Jitter_FS1	38
38	Acme-Calling-RTP-MaxJitter_FS1	39
39	Acme-Calling-Octets_FS1	28
40	Acme-Calling-Packets_FS1	29

CSV Placement	Attribute Name	VSA ID Number
41	Acme-Calling-R-Factor	151
42	Acme-Calling-MOS	152
43	Acme-FlowID_FS1_R	78
44	Acme-FlowType_FS1_R	79
45	Acme-Flow-In-Realm_FS1_R	80
46	Acme-Flow-In-Src-Addr_FS1_R	81
47	Acme-Flow-In-Src-Port_FS1_R	82
48	Acme-Flow-In-Dst-Addr_FS1_R	83
49	Acme-Flow-In-Dst-Port_FS1_R	84
50	Acme-Flow-Out-Realm_FS1_R	85
51	Acme-Flow-Out-Src-Addr_FS1_R	86
52	Acme-Flow-Out-Src-Port_FS1_R	87
53	Acme-Flow-Out-Dst-Addr_FS1_R	88
54	Acme-Flow-Out-Dst-Port_FS1_R	89
55	Acme-Called-RTCP-Packets-Lost_FS1	46
56	Acme-Called-RTCP-Avg-Jitter_FS1	47
57	Acme-Called-RTCP-Avg-Latency_FS1	48
58	Acme-Called-RTCP-MaxJitter_FS1	49
59	Acme-Called-RTCP-MaxLatency_FS1	50
60	Acme-Called-RTP-Packets-Lost_FS1	51
61	Acme-Called-RTP-Avg-Jitter_FS1	52
62	Acme-Called-RTP-MaxJitter_FS1	53
63	Acme-Called-Octets_FS1	44
64	Acme-Called-R-Factor	153
65	Acme-Called-MOS	154
66	Acme-Called-Packets_FS1	45
67	Acme-FlowID_FS2_F	90
68	Acme-FlowType_FS2_F	91
69	Acme-Flow-In-Realm_FS2_F	92
70	Acme-Flow-In-Src-Addr_FS2_F	93
71	Acme-Flow-In-Src-Port_FS2_F	94
72	Acme-Flow-In-Dst-Addr_FS2_F	95
73	Acme-Flow-In-Dst-Port_FS2_F	96
74	Acme-Flow-Out-Realm_FS2_F	97

CSV Placement	Attribute Name	VSA ID Number
75	Acme-Flow-Out-Src-Addr_FS2_F	98
76	Acme-Flow-Out-Src-Port_FS2_F	99
77	Acme-Flow-Out-Dst-Addr_FS2_F	100
78	Acme-Flow-Out-Dst-Port_FS2_F	101
79	Acme-Calling-RTCP-Packets-Lost_FS2	104
80	Acme-Calling-RTCP-Avg-Jitter_FS2	105
81	Acme-Calling-RTCP-Avg-Latency_FS2	106
82	Acme-Calling-RTCP-MaxJitter_FS2	107
83	Acme-Calling-RTCP-MaxLatency_FS2	108
84	Acme-Calling-RTP-Packets-Lost_FS2	109
85	Acme-Calling-RTP-Avg-Jitter_FS2	110
86	Acme-Calling-RTP-MaxJitter_FS2	111
87	Acme-Calling-Octets_FS2	102
88	Acme-Calling-Packets_FS2	103
89	Acme-FlowID_FS2_R	112
90	Acme-FlowType_FS2_R	113
91	Acme-Flow-In-Realm_FS2_R	114
92	Acme-Flow-In-Src-Addr_FS2_R	115
93	Acme-Flow-In-Src-Port_FS2_R	116
94	Acme-Flow-In-Dst-Addr_FS2_R	117
95	Acme-Flow-In-Dst-Port_FS2_R	118
96	Acme-Flow-Out-Realm_FS2_R	119
97	Acme-Flow-Out-Src-Addr_FS2_R	120
98	Acme-Flow-Out-Src-Port_FS2_R	121
99	Acme-Flow-Out-Dst-Addr_FS2_R	122
100	Acme-Flow-Out-Dst-Port_FS2_R	123
101	Acme-Called-RTCP-Packets-Lost_FS2	126
102	Acme-Called–RTCP-Avg-Jitter_FS2	127
103	Acme-Called–RTCP-Avg-Latency_FS2	128
104	Acme-Called–RTCP-MaxJitter_FS2	129
105	Acme-Called-RTCP-MaxLatency_FS2	130
106	Acme-Called-RTP-Packets-Lost_FS2	131
107	Acme-Called-RTP-Avg-Jitter_FS2	132
108	Acme-Called-RTP-MaxJitter_FS2	133

CSV Placement	Attribute Name	VSA ID Number
109	Acme-Called-Octets_FS2	124
110	Acme-Called-Packets_FS2	125
111	Acme-Session-Charging-Vector	54
112	Acme-Session-Charging-Function_Address	55
113	Acme-Firmware-Version	56
114	Acme-Local-Time-Zone	57
115	Acme-Post-Dial-Delay	58
116	Acme-Primary-Routing-Number	64
117	Acme-Originating-Trunk-Group	65
118	Acme-Terminating-Trunk-Group	66
119	Acme-Originating-Trunk-Context	67
120	Acme-Terminating-Trunk-Context	68
121	Acme-P-Asserted-ID	69
122	Acme-Ingress-Local-Addr	74
123	Acme-Ingress-Remote-Addr	75
124	Acme-Egress-Local-Addr	76
125	Acme-Egress-Remote-Addr	77
126	Acme-SIP-Diversion	70
127	Acme-Intermediate_Time	63
128	Acme-Egress-Final-Routing-Number	134
129	Acme-Session-Ingress-RPH	135
130	Acme-Session-Egress-RPH	136
131	Acme-Custom-VSA-200	200
132	Acme-Custom-VSA-201	201
133	Acme-Custom-VSA-202	202
134	Acme-Custom-VSA-203	203
135	Acme-Custom-VSA-204	204
136	Acme-Custom-VSA-205	205
137	Acme-Custom-VSA-206	206
138	Acme-Custom-VSA-207	207
139	Acme-Custom-VSA-208	208
140	Acme-Custom-VSA-209	209
141	Acme-Custom-VSA-210	210
142	Acme-Custom-VSA-211	211

CSV Placement	Attribute Name	VSA ID Number
143	Acme-Custom-VSA-212	212
144	Acme-Custom-VSA-213	213
145	Acme-Custom-VSA-214	214
146	Acme-Custom-VSA-215	215
147	Acme-Custom-VSA-216	216
148	Acme-Custom-VSA-217	217
149	Acme-Custom-VSA-218	218
150	Acme-Custom-VSA-219	219
151	Acme-Custom-VSA-220	220
152	Acme-Custom-VSA-221	221
153	Acme-Custom-VSA-222	222
154	Acme-Custom-VSA-223	223
155	Acme-Custom-VSA-224	224
156	Acme-Custom-VSA-225	225
157	Acme-Custom-VSA-226	226
158	Acme-Custom-VSA-227	227
159	Acme-Custom-VSA-228	228
160	Acme-Custom-VSA-229	229
161	Acme-Custom-VSA-230	230

Stop Record CSV Placement

CSV Placement	Attribute Name	VSA ID Number
1	Acct-Status-Type	
2	NAS-IP-Address	
3	NAS-Port	
4	Acct-Session-Id	
5	Acme-Session-Ingress-CallId	3
6	Acme-Session–Egress-CallId	4
7	Acme-Session-Protocol-Type	43
8	Acme-Session–Generic-Id	40
9	Calling-Station-Id	31
10	Called-Station-Id	30
11	Acct-Terminate-Cause	

CSV Placement	Attribute Name	VSA ID Number
12	Acct-Session-Time	
13	h323-setup-time	
14	h323-connect-time	
15	h323-disconnect-time	
16	h323-disconnect-cause	
17	Acme-Egress-Network-Interface-Id	139
18	Acme-Egress-Vlan-Tag-Value	140
19	Acme-Ingress-Network-Interface-Id	137
20	Acme-Ingress-Vlan-Tag-Value	138
21	Acme-Session-Egress-Realm	42
22	Acme-Session-Ingress-Realm	41
23	Acme-FlowId_FS1_F	1
24	Acme-FlowType_FS1_F	2
25	Acme-Flow-In-Realm_FS1_F	10
26	Acme-Flow-In-Src-Addr_FS1_F	11
27	Acme-Flow-In-Src-Port_FS1_F	12
28	Acme-Flow-In-Dst-Addr_FS1_F	13
29	Acme-Flow-In-Dst-Port_FS1_F	14
30	Acme-Flow-Out-Realm_FS1_F	20
31	Acme-Flow-Out-Src-Addr_FS1_F	21
32	Acme-Flow-Out-Src-Port_FS1_F	22
33	Acme-Flow-Out-Dst-Addr_FS1_F	23
34	Acme-Flow-Out-Dst-Port_FS1_F	24
35	Acme-Calling-RTCP-Packets-Lost_FS1	32
36	Acme-Calling-RTCP-Avg-Jitter_FS1	33
37	Acme-Calling-RTCP-Avg-Latency_FS1	34
38	Acme-Calling-RTCP-MaxJitter_FS1	35
39	Acme-Calling-RTCP-MaxLatency_FS1	36
40	Acme-Calling-RTP-Packets-Lost_FS1	37
41	Acme-Calling-RTP-Avg-Jitter_FS1	38
42	Acme-Calling-RTP-MaxJitter_FS1	39
43	Acme-Calling-Octets_FS1	28
44	Acme-Calling-Packets_FS1	29
45	Acme-Calling-R-Factor	151

CSV Placement	Attribute Name	VSA ID Number
46	Acme-Calling-MOS	152
47	Acme-FlowID_FS1_R	78
48	Acme-FlowType_FS1_R	79
49	Acme-Flow-In-Realm_FS1_R	80
50	Acme-Flow-In-Src-Addr_FS1_R	81
51	Acme-Flow-In-Src-Port_FS1_R	82
52	Acme-Flow-In-Dst-Addr_FS1_R	83
53	Acme-Flow-In-Dst-Port_FS1_R	84
54	Acme-Flow-Out-Realm_FS1_R	85
55	Acme-Flow-Out-Src-Addr_FS1_R	86
56	Acme-Flow-Out-Src-Port_FS1_R	87
57	Acme-Flow-Out-Dst-Addr_FS1_R	88
58	Acme-Flow-Out-Dst-Port_FS1_R	89
59	Acme-Called-RTCP-Packets-Lost_FS1	46
60	Acme-Called-RTCP-Avg-Jitter_FS1	47
61	Acme-Called-RTCP-Avg-Latency_FS1	48
62	Acme-Called-RTCP-MaxJitter_FS1	49
63	Acme-Called-RTCP-MaxLatency_FS1	50
64	Acme-Called-RTP-Packets-Lost_FS1	51
65	Acme-Called-RTP-Avg-Jitter_FS1	52
66	Acme-Called-RTP-MaxJitter_FS1	53
67	Acme-Called-Octets_FS1	44
68	Acme-Called-Packets_FS1	45
69	Acme-Called-R-Factor	153
70	Acme-Called-MOS	154
71	Acme-FlowID_FS2_F	90
72	Acme-FlowType_FS2_F	91
73	Acme-Flow-In-Realm_FS2_F	92
74	Acme-Flow-In-Src-Addr_FS2_F	93
75	Acme-Flow-In-Src-Port_FS2_F	94
76	Acme-Flow-In-Dst-Addr_FS2_F	95
77	Acme-Flow-In-Dst-Port_FS2_F	96
78	Acme-Flow-Out-Realm_FS2_F	97
79	Acme-Flow-Out-Src-Addr_FS2_F	98

CSV Placement	Attribute Name	VSA ID Number
80	Acme-Flow-Out-Src-Port_FS2_F	99
81	Acme-Flow-Out-Dst-Addr_FS2_F	100
82	Acme-Flow-Out-Dst-Port_FS2_F	101
83	Acme-Calling-RTCP-Packets-Lost_FS2	104
84	Acme-Calling-RTCP-Avg-Jitter_FS2	105
85	Acme-Calling-RTCP-Avg-Latency_FS2	106
86	Acme-Calling-RTCP-MaxJitter_FS2	107
87	Acme-Calling-RTCP-MaxLatency_FS2	108
88	Acme-Calling-RTP-Packets-Lost_FS2	109
89	Acme-Calling-RTP-Avg-Jitter_FS2	110
90	Acme-Calling-RTP-MaxJitter_FS2	111
91	Acme-Calling-Octets_FS2	102
92	Acme-Calling-Packets_FS2	103
93	Acme-FlowID_FS2_R	112
94	Acme-FlowType_FS2_R	113
95	Acme-Flow-In-Realm_FS2_R	114
96	Acme-Flow-In-Src-Addr_FS2_R	115
97	Acme-Flow-In-Src-Port_FS2_R	116
98	Acme-Flow-In-Dst-Addr_FS2_R	117
99	Acme-Flow-In-Dst-Port_FS2_R	118
100	Acme-Flow-Out-Realm_FS2_R	119
101	Acme-Flow-Out-Src-Addr_FS2_R	120
102	Acme-Flow-Out-Src-Port_FS2_R	121
103	Acme-Flow-Out-Dst-Addr_FS2_R	122
104	Acme-Flow-Out-Dst-Port_FS2_R	123
105	Acme-Called-RTCP-Packets-Lost_FS2	126
106	Acme-Called–RTCP-Avg-Jitter_FS2	127
107	Acme-Called–RTCP-Avg-Latency_FS2	128
108	Acme-Called–RTCP-MaxJitter_FS2	129
109	Acme-Called-RTCP-MaxLatency_FS2	130
110	Acme-Called-RTP-Packets-Lost_FS2	131
111	Acme-Called-RTP-Avg-Jitter_FS2	132
112	Acme-Called-RTP-MaxJitter_FS2	133
113	Acme-Called-Octets_FS2	124

CSV Placement	Attribute Name	VSA ID Number
114	Acme-Called-Packets_FS2	125
115	Acme-Session-Charging-Vector	54
116	Acme-Session-Charging-Function-Address	55
117	Acme-Firmware-Version	56
118	Acme-Local-Time-Zone	57
119	Acme-Post-Dial-Delay	58
120	Acme-Primary-Routing-Number	64
121	Acme-Originating-Trunk-Group	65
122	Acme-Terminating-Trunk-Group	66
123	Acme-Originating-Trunk-Context	67
124	Acme-Terminating-Trunk-Context	68
125	Acme-P-Asserted-ID	69
126	Acme-Ingress-Local-Addr	74
127	Acme-Ingress-Remote-Addr	75
128	Acme-Egress-Local-Addr	76
129	Acme-Egress-Remote-Addr	77
130	Acme-SIP-Diversion	70
131	Acme-Session-Disposition	60
132	Acme-Disconnect-Initiator	61
133	Acme-Disconnect-Cause	62
134	Acme-SIP-Status	71
135	Acme-Egress-Final-Routing-Number	134
136	Acme-Session-Ingress-RPH	135
137	Acme-Session-Egress-RPH	136
138	Acme-Refer-Call-Transfer-Id	141
139	Acme-Custom-VSA-200	200
140	Acme-Custom-VSA-201	201
141	Acme-Custom-VSA-202	202
142	Acme-Custom-VSA-203	203
143	Acme-Custom-VSA-204	204
144	Acme-Custom-VSA-205	205
145	Acme-Custom-VSA-206	206
146	Acme-Custom-VSA-207	207
147	Acme-Custom-VSA-208	208

CSV Placement	Attribute Name	VSA ID Number
148	Acme-Custom-VSA-209	209
149	Acme-Custom-VSA-210	210
150	Acme-Custom-VSA-211	211
151	Acme-Custom-VSA-212	212
152	Acme-Custom-VSA-213	213
153	Acme-Custom-VSA-214	214
154	Acme-Custom-VSA-215	215
155	Acme-Custom-VSA-216	216
156	Acme-Custom-VSA-217	217
157	Acme-Custom-VSA-218	218
158	Acme-Custom-VSA-219	219
159	Acme-Custom-VSA-220	220
160	Acme-Custom-VSA-221	221
161	Acme-Custom-VSA-222	222
162	Acme-Custom-VSA-223	223
163	Acme-Custom-VSA-224	224
164	Acme-Custom-VSA-225	225
165	Acme-Custom-VSA-226	226
166	Acme-Custom-VSA-227	227
167	Acme-Custom-VSA-228	228
168	Acme-Custom-VSA-229	229
169	Acme-Custom-VSA-230	230