Oracle® Communications Session Border Controller

Release Notes

Release S-CX6.2.0

Formerly Net-Net Session Director

October 2013

ORACLE®

About this Guide

Overview

The *Oracle Communications Session Border Controller Release Notes* provides the following information when applicable:

- An overview of the new features available
- An overview of the management enhancements
- An overview of the accounting enhancements
- A summary of changes to the Acme Packet Command Line Interface (ACLI)
- A summary of known issues and fixed defects
- Documentation updates

If any of these sections does not appear in the document, then there were no changes to summarize in that category for that specific release.

Supported Platforms

Release Version S-C6.2.0 is supported on the Acme Packet 4500 and Acme Packet 3800 series platforms.

Related Documentation

The following table lists the members that comprise the documentation set for this release:

Document Name	Document Description
Acme Packet 4500 System Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4500 system.
Acme Packet 3800 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3800 system.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration SBC.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.

Document Name	Document Description
Maintenance and Troubleshooting Guide	Contains information about Net-Net SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), 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.
Accounting Guide	Contains information about the SBC's accounting support, including details about RADIUS accounting.

Revision History

This section contains a revision history for this document.

Date	Revision Number	Description
January 19, 2012	Revision 1.01	• Adds informationabout Open Source Software notices.

Contents

Net-Net OS S-C6.2.0 Release Notes

Introduction

The *Net-Net OS S-C6.2.0 Release Notes* provide the following information about Net-Net OS Release C6.2.0:

- An overview of the new features available
- A summary of changes to the Acme Packet Command Line Interface (ACLI)
- A summary of known issues
- An overview of changes to the Acme Packet Technical Publications documentation set that supports the Net-Net 3000 and 4000 series products using the ACLI

Platform Divergence for Feature Support

In Net-Net OS Release S-C6.2.0, there is a difference in the features available on the Net-Net 4250 in comparison to those available on the Net-Net 3800 and Net-Net 4500.

The following is a list of features that are only supported on the Net-Net 3800 and Net-Net 4500:

- IPv6 support
- IPv4-IPv6 interworking
- Multimedia Internet KEYing Configuration (MIKEY)
- Secure Real-Time Transport Protocol (SRTP) and Source Description RTCP (Real-Time Control Protocol) Packet (SDES)
- Serial port control for Administrative Security
- Storage Expansion Module Use With Local CDRs/FTP Push
- H.248 ALG
- IPsec IKEv2 for the wancom
- Net-Net Border Gateway

New Features

This section describes the new features available in Net-Net OS Release S-C6.2.0.

SIP Features

This section provides an overview of the new SIP signaling features available in Net-Net OS Release S-C6.2.0.

SIP GRUU

SIP Globally Routable User Agent (UA) URIs (GRUU) are designed to route a SIP message reliably to a specific device or end user. This contrasts with a SIP AoR, which can refer to multiple UAs for a single user, thus contributing to routing confusion. The Net-Net SBC can perform different behaviors when it finds SIP GRUUs in Contact headers.

User agents supporting GRUU include a GRUU-identifying parameter in the Contact header of a dialog forming and target refresh requests. The Net-Net SBC scans for the GRUU parameter in the Contact header only when the endpoint it receives a request from is registered or when the **pass-gruu-contact** parameter is enabled.

SIP maddr Resolution

Net-Net OS Release S-C6.2.0 provides enhanced resolution of addresses found in SIP contact headers, or in the *maddr* (multicast address) parameter of SIP 3xx REDIRECT messages. Previous releases resolved these addresses as either a host address or as a session agent name. With Release S-C6.2.0, these addresses can also be resolved as session agent group (SAG) names.

REFER-Initiated Call Transfer

In prior releases, the Net-Net SBC supports REFER-initiated call transfer either by proxying the REFER to the other User Agent in the dialog, or by terminating the received REFER and issuing a new INVITE to the referred party. These static alternate operational modes could be configured for specific SIP interfaces, realms, or session agents.

Release S-C6.2.0 enhances support with an additional operational mode that determines on a call-by-call basis whether to proxy the REFER to the next hop, or to terminate the REFER and issue an INVITE in its stead.

With the Release S-C6.2.0, support for REFER-initiated call transfer is no longer available for SIP interfaces; support must be configured for realms and/or session agents.

SIP REFER: Re-Invite for Call Leg SDP Renegotiation

Enhancing the original implementation of SIP REFER termination introduced in Release S-C6.0.0, this change to Net-Net SBC behavior allows for SDP renegotiation between both parties of a transferred call.

SIP Diversion to SIP-ISUP Interworking

For networks in which there are devices that do not support SIP-T or SIP-I (and support native SIP alone), the Net-SBC now supports SIP Diversion interworking. This feature enables such devices to function properly in instances that require SIP-T/SIP-I style ISUP IAM message encapsulation in ISUP requests, and to receive any call forwarding information in the IAM according to ISUP standards.

The Net-Net SBC interworks a native SIP INVITE request to SIP-T one by inserting an ISUP IAM body based on the INVITE; this includes redirection information based on the Diversion header. This feature can also perform the reverse translation. That is, it can interwork a SIP INVITE that does have the ISUP IAM body to a non-ISUP INVITE. In this case, the Net-Net SBC generates the necessary Diversion headers based on the IAM's Redirection information.

SIP-ISUP Format Version Interworking

An ISUP message can be carried in SIP messages through either a standard body or through a multipart MIME encoded body. While ANSI and ITU are the two major groups, but each contains many specific variants. To facilitate instances where two sides of a call use different versions, the Net-Net SBC supports interworking between the following SIP ISUP formats: ANSI, ITU, ETSI-356 (an ITU variant), and GR-317 (an ANSI variant). To do so, the Net-Net SBC can move, delete, and add parameters to various sections of the message.

Unique HMR Regex Patterns and Other Changes

In addition to the HMR support it offers in earlier releases, the Net-Net SBC can now be provisioned with unique regex patterns for each logical remote entity. This supplement to pre-existing HMR functionality saves you provisioning time and saves Net-Net SBC resources in instances when it was previously necessary to define a unique SIP manipulation per PBX for a small number of customer-specific rules.

In addition, Release S-C6.2.0 also introduces these changes:

- Manipulation per remote entity—You can configure logical remote entities (session agents, realms, and SIP interfaces) with a manipulation pattern string that the system uses as a regular expression.
- Addition of the **reject** action—You can configure rules that instruct the Net-Net SBC to reject requests (while not dropping responses) and to increment a counter tracking rejections.
- Changes to storing pattern rule values (i.e., changing how the **store** action works)—You no longer need to specify the **store** action. The simple fact of referencing another rule tells the system it must store a value. When SIP manipulation is used, the system first checks to see if any values require storing. The **add** action is an exception to this process; storing happens after a header is added.
- Removal of restrictions—The following restrictions related to HMR are removed from Release S-C6.2.0:
  - The action **find-replace-all** now executes all element rules. Previously, no child rules were executed.
  - The action **sip-manip** now executes existing all element rules. Previously, no child rules were executed.
  - The action **store** now executes existing all element rules. Previously, only child rules with the **store** action were executed.
  - The action **add** now executes existing all element rules. Previously, only child rules with the **add** action were executed.
- Name restrictions for manipulation rules—Historically, you have been allowed to configure any value for the name parameter within a manipulation rule. This method of naming caused confusion when referencing rules, so now manipulation rules name must follow a specific syntax. They must match the expression `"^[[alpha:]][[:alnum:]_]+$"` and contain at least one lower case letter.

  In other words, the name must:
  - Start with a letter, and then it can contain any number of letters, numbers, or underscores
  - Contain at least one lower case letter

  All pre-existing configurations will continue to function normally.

Dialog-Matching Header Manipulation

The most common headers to manipulate using HMR are the To-URI and From-URI. Along with the to-tag, from-tag, and Call-ID values, these are also all headers that represent dialog-specific information that must match the UAC and UAS to be considered part of the same dialog. If these parameters are modified through HMR, the results can be that the UAC or UAS rejects messages.

While it is possible to ensure that dialog parameters match correctly using regular HMR, this feature offers a simpler and less error-prone method of doing so.

Built-in SIP Manipulations

In the course of HMR use, certain rules have become commonly used. Although lengthy and complex, these rules do not include any customer-specific information and so they can be used widely. To make using them easier, they have been turned into built-in rules that you can reference in the **in-manipulationid** and **out-manipulationid** parameters that are part of the realm, session agent, and SIP interface configurations.

Built-in rules start with the prefix `ACME_`, so Acme Packet recommends you name your own rules in a different manner to avoid conflict.

HMR for SIP-ISUP

The Net-Net SBC's HMR functionality can operate on ISDN user party (ISUP) binary bodies. Using the same logic and mechanisms that are applied to SIP header elements, HMR for SIP-ISUP manipulates ISUP parameter fields and ISUP message parts. You can create MIME rules that function in much the same way the SIP header rules do; but whereas SIP header rules can change the specific headers of a SIP message, MIME rules can manipulate targeted body parts of a SIP message.

In addition, this feature also introduces:

- Changes and additions to equality operators—These changes are detailed in the *SIP Signaling Services* chapter of the *Net-Net 4000 ACLI Configuration Guide*.
- Reserved words—To improve system performance and simplify configuration, the Net-Net SBC now supports pre-defined reserved words for commonly-used URI parameters for HMR. Reserved words retrieve values directly from the SIP message, without your needing to create rules to store them.

HMR Import-Export

Due to the complexity of SIP manipulations rules and the deep understanding of system syntax they require, it is often difficult to configure reliable rules. This feature provides support for importing and exporting pieces of SIP manipulation configuration in a reliable way so that they can be reused.

IMS Features

This section provides an overview of the new IMS features available in Net-Net OS Release S-C6.2.0.

E-CSCF Support

An Emergency Call Session Control Function (E-CSCF) is an IMS core element that aids in routing emergency calls to an appropriate destination, such as a public safety answering point (PSAP). E-CSCF functionality can be performed by the Net-Net SBC with appropriate local policy and network management control configuration.

The E-CSCF feature lets the Net-Net SBC internally prioritize and route emergency calls to the corresponding Emergency Service Center, based on:

- The calling party's request URI
- The location information retrieved from a CLF (Connectivity Location Function) for wireline/TISPAN networks

By integrating E-CSCF functionality into the Net-Net SBC's P-CSCF, your network can satisfy the common local requirement that certain telephony elements be deployed locally, rather than using single, centralized elements.

H.323 Features

This section provides an overview of the new H.323 signaling features available in Net-Net OS Release S-C6.2.0.

H.323 Stack Monitoring

In releases prior to S-C6.2.0, the Net-Net SBC provides SNMP monitoring of H.323 session agents but not of the H.323 interfaces (stacks) themselves. The H.323 stack/interface configuration now provides a way for you to set alarm thresholds on a per-stack basis. When enabled, this alarm system ties into the **max-calls** value to send critical, major, or minor alarms when the number of calls approaches the threshold.

H.323: H.239 Support for Video+Content

The Net-Net SBC supports multiple media streams for the same payload, generic capabilities, and H.239 generic messages. As a result, these additions broaden the Net-Net SBC's support for videoconferencing, and free you from having to configure media profiles for H.323 support.

> **Note:** These additions are supported for H.323-H.323 traffic only. These additions do not support SIP-H.323 interworking (IWF), so you still need to configure media profiles for that application.

Session Routing and Load Balancing Features

This section provides an overview of the new routing and load balancing features available in Net-Net OS Release S-C6.2.0.

Multi-Stage Local Policy Routing for SIP

In releases prior to S-C6.2.0, the Net-Net SBC provides a single-stage local policy routing mechanism, meaning that it performs a single local policy look-up when routing SIP traffic. This look-up can result in multiple matching routes. Then the Net-Net SBC tries the matching routes in order of preference, either hitting a terminate-recursion or trying until none is left. With ENUM or local routing table (LRT) entries defined as the next hop, the Net-Net SBC queries the ENUM server or consults the local routing table. Then it uses the results to perform routing based on the hostname in the NAPTR or LRT next hop entries. If all of those fail, the system then tries the next matching local policy results.

By contrast, multi-stage local policy routing provides a mechanism whereby you can configure the Net-Net SBC to use multiple stages of route look-ups, where the result from one stage can be used as the look-up key for the next.

ENUM Failover and Query Distribution

- ENUM query distribution—The Net-Net SBC can intelligently distribute ENUM queries among all configured ENUM servers. By setting the enum-config's **query-method** parameter to **round-robin**, the Net-Net SBC will cycle ENUM queries, sequentially, among all configured ENUM servers. For example, query 1 will be directed to server 1, query 2 will be directed to server 2, query 3 will be directed to server 3, and so on.

  The default query method, **hunt**, directs all ENUM queries toward the first configured ENUM server. If the first server is unreachable, the Net-Net SBC directs all ENUM queries toward the next configured ENUM server, and so on.
- Failover to new enum-config—When an enum-config's configured servers are unreachable via the network (i.e., no response is received on a query), the Net-Net SBC can failover to a defined ENUM config that contains different ENUM servers to query. This failover behavior works when all servers in an ENUM config are unreachable, rather than when the Net-Net SBC receives not-found type responses.

CNAM Subtype Support for ENUM Queries

CNAM, calling name, data is a string up to 15 ASCII characters of information associated with a specific calling party name. The Internet-draft, draft-ietf-enum-cnam-08.txt, registers the ENUM service 'pstndata' and subtype 'cnam' using the URI scheme 'pstndata:' to specify the return of CNAM data in ENUM responses. The Net-Net SBC recognizes CNAM data returned via this mechanism. CNAM data is then inserted into the display name of the From: header in the original Request. If a P-Asserted-ID header is present in the original request, the CNAM data is inserted there as well.

The Net-Net SBC can preform CNAM queries on the signaling message's ingress or egress from the system by setting the cnam lookup direction parameter to either ingress or egress. If the CNAM lookup direction parameters are configured on both the ingress and egress sides of a call, the Net-Net SBC will only preform the lookup on the ingress side of the call.

Caching ENUM Responses

As DNS responses often lead to further DNS queries, a DNS server can send multiple records in a response to attempt to anticipate the need for additional queries. The Net-Net SBC can locally cache additional NAPRT, SRV, and A records returned from an ENUM query to eliminate the need for unnecessary external DNS requests. The Net-Net SBC can then refer to these cached records.

Source URI Information in ENUM Requests

ENUM queries can include the source URI that caused the ENUM request. The Net-Net SBC can add the P-Asserted-ID URI (only if not in an INVITE) or the From URI into an OPT-RR Additional Record to be sent to the ENUM server. It can be useful to specify the originating SIP or TEL URI from a SIP request that triggered the ENUM query, so the ENUM server can provide a customized response based on the caller.

This feature implements the functionality described in the Internet Draft, *DNS Extension for ENUM Source-URI*, draft-kaplan-enum-source-uri-00.

SIP Session Agent DNS-SRV Load Balancing

Prior to Release S-C6.2.0 the Net-Net SBC provided the ability to specify a fully qualified domain name (FQDN) for a destination session-agent. During DNS lookup the FQDN could resolve to multiple resource record for servers (SRV) records. Each SRV could resolve to a single IP address via A-Record query in IMS or DNS.

With Release 6.2.0 the Net-Net SBC supports load balancing behavior as described in RFC 3263, *Session Initiation Protocol (SIP): Locating SIP Servers*. It supports internal load balancing, and monitors the availability of dynamically resolved IP addresses obtained from a DNS server. Then the Net-Net SBC can recurse through the list of in-service IP addresses. It also support the selection of routing destinations based on SRV weights.

Security Features

This section provides an overview of the new security features available in Net-Net OS Release S-C6.2.0.

IDS Reporting

The Net-Net SBC supports intrusion protection capabilities, and the IDS reporting feature enables more detailed reporting of intrusions the system detects. IDS reporting feature is useful for enterprise customers requirement to report on intrusions and suspicious behavior that it currently monitors.

IPsec IKEv1 Support

To create IPsec tunnels dynamically, Release S-C6.2.0 provides support for Version 1 of the Internet Key Exchange (IKE) Protocol as defined in RFC 2409, *Internet Key Exchange*, and for the Dead Peer Detection (DPD) protocol as defined in RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*.

The following IKEv1 functionality is supported:

- IKE pre-shared secret support
- IKE/ISAKMP Main Mode support
- IKE/ISAKMP Aggressive Mode support
- Phase 2 Quick Mode support

In addition, with IKEv1 enabled, the Net-Net SBC can support IPsec between itself and an endpoint behind a NAT device.

IKEv2 for Wancom

Net-Net OS Release S-C6.2.0 provides encryption of management traffic by enabling the creation of up to 10 IKEv2-keyed IPsec tunnels across the wancom0 interface.

SRTP MIKEY

Certain customers require the ability to encrypt the content and signalling of their real time communications sessions. The Net-Net SBC meets this need by supporting SRTP MIKEY.

For the Net-Net 3800 and 4500 only, Release S-C6.2.0 supports signaling of SRTP keys with MIKEY through an implementation of a subset of RFC 3830. This implementation of MIKEY offers encryption of both RTP media and RTCP statistical information. The Net-Net SBC's SRTP MIKEY implementation requires signaling plane encryption using SIP-TLS.

OCSP

The Net-Net SBC now supports Online Certificate Status Protocol (OCSP).

OSCP is used for dynamic validation of certificates from TLS endpoints connected to the Net-Net SBC. Acting as an OSCP client, the Net-Net SBC forwards the endpoint's offered certificate to an OSCP responder. The endpoint is allowed to establish a connection with the Net-Net SBC only if the OSCP responder replies that the certificate is valid for the endpoint in question.

SRTP/SDES

SRTP/SDES is supported on the Net-Net 3800 and 4500 only.

The Secure Real-Time Transport Protocol (SRTP) provides encryption and authentication for the call content and call signalling streams. Authentication provides assurance that packets are from the purported source, and that they (the packets) have not been tampered with during transmission. Encryption provides assurance that the call content and associated signalling has remained private during transmission.

RTP and RTCP traffic are encrypted as described in RFC3711, *The Secure Real-time Transport Protocol (SRTP)*. The negotiation and establishment of keys and other cryptographic materials that support SRTP is described in RFC4568, *Session Description Protocol (SDP) Security Description for Media Streams*. Cryptographic parameters are established with only a single message or in single round-trip

exchange using the offer/answer model defined in RFC 3264, *An Offer/Answer Model with the Session Description Protocol*.

Administrative Security Features

Net-Net OS S-C6.2.0 offers a new set of features for administrative security, which are enabled in the presence of a valid administrative security license. This feature set includes support for: multiple administrative users, enhanced password strength, password usage policies, user roles, management of administrative users, and serial console port control on Net-Net 3800s and 4500s.

Under this type of security, users cannot access the Net-Net SBC via Telnet or FTP, nor can they access the system using ACP. The set of administrative security features also offers these capabilities.

- Console-only access to Net-Net 3800s and 4500s
- When a local or RADIUS users logs into the system via console or SSH connection, a banner appears. No banner appears for SFTP connections.
- Password strength is imposed only on local users.
- Password history is maintained only for local users. RADIUS user passwords are not tracked on the Net-Net 3800 and 4500.
- There are new SFTP file access privileges and user roles for RADIUS users.
- Two-factor authentication is available for the Net-Net 3800 and 4500; this is not applicable to RADIUS and SFTP access to the system.

Accounting Features

This section provides an overview of the new accounting features available in Net-Net OS Release S-C6.2.0.

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.

> **Note:** VSAs 172-177 (for Diameter) never appear in RADIUS messages, and you cannot query RADIUS for them. They are only used for Diameter accounting and are hidden when RADIUS is enabled. These VSAs are converted to Diameter accounting AVPs, and so they show up as AVPs.

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).

Support for Multiple CDR Push Receivers

Your 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).

Management Features

This section provides an overview of the new management features available in Net-Net OS Release S-C6.2.0.

Interface Utilization: Graceful Call Control, Monitoring, and Fault Management

When you enable this feature, the Net-Net SBC monitors network utilization of its media interfaces and sends alarms when configured thresholds are exceeded. You can also enable overload protection on a per-media interface basis, where the Net-Net SBC will prevent call initializations during high traffic but still allow established calls to continue if traffic passes the critical threshold you define.

HDR Support for ENUM and SIP

Historical data recording (HDR) support has been expanded to include data for ENUM and for SIP INVITE messages and methods. These groups are the **enum** group and the **sip-invite** group.

CPU Load Rate SNMP OID

The Net-Net SBC now supports an OID that provides the CPU load rate over a five-to-ten second widow; it is defined in the apSysMgmtGeneralObjects.

Admission Control

This section provides an overview of the new call admission control (CAC) features available in Net-Net OS Release S-C6.2.0.

Shared CAC for SIP Forked Calls

A forked call is one which has multiple INVITEs for the same call. For example, if an Application Server in the provider core network forks a call attempt, the application server sends several INVITEs for the same call toward the Net-Net SBC. Each INVITE is destined for a unique device that belongs to the same user. Ideally, that user will only answer one device. The Net-Net SBC treats each INVITE as a unique call request.

Conditional Bandwidth CAC for Media Release

The Net-Net SBC supports conditional call admission control (CAC) using the SIP profile configuration. With this feature enabled, you can allow the conditional admission of SIP calls that could potentially have their media released instead of risking the possible rejection of those calls due to internal bandwidth limits.

External Policy Servers

This section provides an overview of the new external policy server features available in Net-Net OS Release S-C6.2.0.

Diameter Heartbeat

Device-Watchdog-Request (DWR) and Device-Watchdog-Answer (DWA) messages are used to detect transport failures at the application layer between the Net-Net SBC communicating with a policy server via Diameter. The request/answer message pair forms a heartbeat mechanism that can alert the requesting side if the answering side is not reachable.

The Net-Net SBC always responds to a DWR by replying with a DWA message. In addition, the Net-Net SBC can be configured to initiate DWR messages toward a policy server or other Diameter-based network device.

You configure the **watchdog ka timer** with a timeout value that determines the number of seconds a DWA is expected in response to the Net-Net SBC sending a DWR.

Diameter Destination Realm AVP

As of S-C6.2.0, the Destination Realm AVP's value does not contain the realm of the incoming SIP message. Now, it contains the realm where the Policy Server resides as learned from the Origin-Realm AVP received in a CEA message from the Policy Server. The Net-Net SBC can be configured with an option to retain the previous behavior of sending an incoming SIP message's realm to a policy server.

Net-Net BG

The Net-Net 3800 and 4500 can be configured as a BGF logical device as used in the ETSI/TISPAN IMS architecture. This fills a single logical role (in a decomposed model with a session controller), whereas the integrated SBC model spans several logical roles. When the Net-Net 4000 is configured to act in the BGF role, it is responsible for controlling media streams as they enter and exit the network. A session controller controls a BG's media operations using H.248 v.2 ETSI/TISPAN Ia profile with long text over a UDP interface.

The BG performs the following tasks on media traffic (RTP and RTCP):

- VLAN tagging
- DSCP Marking
- Resource allocation and reservation
- Media supervision
- QoS Statistics Collection & Reporting
- DoS protection
- Fault management
- Bandwidth Policing
- Media Latching for HNT

Additional Features

This section provides an overview of the additional new features available in Net-Net OS Release S-C6.2.0.

IPv6

IPv6 support has been added to the Net-Net 3800 and Net-Net 4500. Ideally, IPv6 support would be a simple matter of configuring IP addresses of the version type you want in the configurations where you want them. While this is the case for some configuration areas, in others you will need to take care with—for example—the format of your IPv6 address entries or where parameters must be configured with IP addresses of the same version type.

You do not need a specific license to use IPv6 on your Net-Net 3800 or 4500; it works out of the box. However, you do need a valid, activated license to perform interworking between IPv4 and IPv6.

IPv4-IPv6 Interworking

In addition to supporting IPv6 on the Net-Net 3800 and Net-Net 4500, both of these systems can be enabled to perform interworking between IPv4 and IPv6. In order to use this feature, you need to have the appropriate license activated on your system.

Peer-to-Peer MSRP TCP Stitching

The Net-Net SBC supports peer-to-peer TCP connections for peers behind NATs, enabling Message Session Relay Protocol (MSRP) client to communicate with one another. More specifically, the Net-Net SBC can:

- Establish incoming TCP connections with each endpoint participating in the MSRP session using a 3-way handshake. The Net-Net SBC receives incoming SYNs on the local address and port provided in the SDP offer and answer to each endpoint.
- Stitch together the two TCP connections internally after successful establishment of both connections. This capability is used when the caller and the callee initiate TCP SYNs towards one another via the Net-Net SBC; the "stitching" makes both clients think they are talking to a server. To achieve this end, the Net-Net SBC caches SYNs from both sides so it can modify the SYN packets to SYN-Acks with the correct sequence and Ack numbers.

  Note, though this case is rare, that if a user is behind a NAT offers a=passive, then this feature cannot function properly.
- Relay MSRP stream between the endpoints.
- Police bandwidth for MSRP streams based on a defined media profile for MSRP.

Management Changes Summary

This section summarizes the projected ACLI, SNMP, and RADIUS accounting management changes for Net-Net OS Release S-C6.2.0. Changes appearing in this document have been added since the availability of Net-Net OS C6.1.0.

ACLI Command Changes

This section summarizes the ACLI command changes that appear in Net-Net OS Release S-C6.2.0.

Availability	Change	Description
nnSC620	delete-import	Adding command to support importing SIP-manipulation rules as files in a directory; delete-import will delete the selected file from the "code/import" directory
nnSC620	format	Adding command to support storage expansion on SBC; format device specified
nnSC620	ipv6	Adding command to enable testing of IPv6
nnSC620	show • accounting • built-in-sip-manipulations • imports	Expanding command to show: • Accounting statistics • Built-in SIP-manipulation rules • List of imported files on "code/import" directory

Availability	Change	Description
nnSC620	show directory	Adding command to display files in directories that are supported by storage expansion in SBC
nnSC620	show enum • status	Expanding command to display ENUM statistics supported by new ENUM configuration parameters
nnSC620	show h323d stack alarms	Expanding command to support monitoring and alerting max-calls within H.323 stack via SNMP
nnSC620	show ip	Expanding command to display SCTP statistics
nnSC620	show mbcd • forked-session	Expanding command to support checking bandwidth constraints once for forked sessions
nnSC620	show media • utilization	Expanding command to show network utilization of each port
nnSC620	show radius • CDR	Expanding command to display CDR statistics
nnSC620	show redundancy • iked redundancy statistics • manuald redundancy statistics	Expanding command to include: • IKE redundancy statistics • manual redundancy statistics
nnSC620	show security • ike • srtp	Expanding command to include arguments for identifying: • IKE information • SRTP information
nnSC620	show space	Adding command to show remaining space on device specified
nnSC620	show sipd forked	Expanding command to display the total number of forked sessions received and the total number rejected

Availability	Change	Description
nnSC620	show configuration • auth-params • ike-config • ike-sainfo • local-address-pool • data-flow • dpd-params • • ike-interface • ike-certificate-profile • public-key • cert-status-profile • ims-aka-profile • ipsec-global-config • qos-constraints • sip-profile • sip-isup-profile • ssh-config • login-config • audit-logging	Adding arguments to: • Show the authentication template configured • Show the global Internet Key Exchange (IKE) configuration object • Show the IKE Security Authentication configurations • Show the IP address enabled from the local address pool • Show the data-trafficking configurations • Show the dead peer detection configurations • Show the IKE interface configurations • Show the IKE certificate profiles • Show the public key configurations • Show certificate status profile • Show the IMS-aka profiles • Show the IPsec global configurations • Show the QoS constraint configurations • Show the SIP-profile configurations • Show the SIP-ISUP-profile configurations • Show the SSH configurations • Show the login configurations • Show the audit-logging configurations

Availability	Change	Description
nnSC6200	show running-config • audit-logging • auth-params • cert-status-profile • ike-config • ike-sainfo • local-address-pool • data-flow • dpd-params • • ike-interface • ike-certificate-profile • network-parameters • public-key • cert-status-profile • ims-aka-profile • ipsec-global-config • login-config • qos-constraints • ssh-config • sip-profile • sip-isup-profile • sip-response-map • tunnel-orig-params	Adding arguments to: • Show audit logging configuration • Show the auth-params configurations • Show certificate status profiles • Show the IKE configurations • Show the IKE-sainfo configurations • Show the local-address-pool configurations • Show the data-flow configurations • Show the dpd parameters configurations • Show the IKE interface configurations • Show the IKE certificate profiles • Show all network parameters • Show the public key configurations • Show certificate status profile • Show the IMS-aka profiles • Show the IPsec global configurations • Show login configuration objects • Show the QoS constraint configurations • Show SSH configuration object • Show the SIP-profile configurations • Show the SIP-ISUP-profile configurations • Show all SIP-response-map objects • Show tunnel origination parameters
nnSC620	ssh-pub-key	Adding command to generate and export SSH public keys
nnSC620	test-audit-log	Adding command to test audit log functionality
nnSC620	test-sip-manipulation	Adding command to test a SIP-manipulation

ACLI Configuration Changes

This section summarizes the ACLI command changes that appear in Net-Net OS Release S-C6.2.0.

Availability	Change	Description
nnSC620	media-manager>ext-policy-server>service-class-options	Adding configuration to support specification of service class classification for video, audio, application, data, control, image, text, and message; an integer value sets the classification

nnSC620	media-manager>media-manager-config>syslog-on-demote-to-deny	Adding parameter to enable the Net-Net SBC to send a message to the syslog in the event of an endpoint demotion
nnSC620	media-manager>media-manager-config>trap-on-demote-to-deny	Adding parameter to enable the Net-Net SBC to send traps in the event of an endpoint demotion
nnSC620	media-manager>mgcp-config>ca-ping-retries	Adding parameter to configure number of times session retries pinging the call agent
nnSC620	media-manager>realm-config>dyn-refer-term	Adding configuration to enhance REFER-initiated call transfers; when enabled, the Net-Net SBC will terminate the REFER and issue a new INVITE to complete REFER processing. Support for REFER-initiated call transfer is no longer available for SIP-interfaces; must be configured for realms and/or session agents
nnSC620	media-manager>realm-config> • manipulation-pattern • manipulation-string	Adding configurations to apply, on a per-realm basis, SIP-manipulation in HMR through logical remote entities
nnSC620	media-manager>realm-config>sip-isup-profile	Adding configurations to support, on a per-realm basis, SIP-ISUP format version interworking
nnSC620	session-router>session-agent>sip-profile	Adding configurations to apply, on a per-realm basis, SIP-profile configurations
nnSC620	security>auth-params	Adding configuration to provide a list of RADIUS servers used for authentication, along with protocol and operation details that define RADIUS access
nnSC620	security>authentication>ike-radius-params-name	Adding configuration to identify the auth-params instance to be assigned to this element
nnSC620	security>authentication>management-servers	Adding configuration to identify a list of RADIUS servers
nnSC620	security>authentication>management-strategy	Adding configuration to identify the management strategy configured: • Hunt uses a linear method, and always contacts the first server in the server list; only if that server is unavailable will another server be contacted • Round-robin uses a circular method and contacts each server in the list sequentially; e.g. Server 1 is contacted for the first request, Server 2 for the next, and so on

nnSC620	security>cert-status-profile • name • ip-address • port • type • trans-proto • requestor-cert • responder-cert • realm-id • batch	Adding sub-element and parameters to support Online Certificate Status Protocol (OSCP) for end-certificate verification. SIP-TLS connection is made after request is verified and deemed safe
nnSC620	security>ike	Adding IKE protocol to perform mutual authentication between two parties. Adding parameters to:
	• data-flow	• Configure data flows for passthrough data-traffic processing
	• dpd-params	• Configure dead peer detection parameters to set number of attempts to establish connection with peer
	• ike-certificate-profile	• Authenticate a specific IKE identity using a CA certificate to validate a remote certificate
	• ike-config	• Configure global IKE parameters
	• ike-interface	• Enable multiple IKE-enabled interfaces
	• ike-sainfo	• Configure IKE Security Association templates, which identify cryptographic material available for IPsec tunnel establishment
	• local-address-pool	• Configure local address pools; when enabled, they provide a local internal address in response to remote requests for IP addresses
	• tunnel-orig-params	• Configure tunnel origination parameters to define a single remote IKEv2 peer
nnSC620	security>public-key	Adding sub-element to support viewing, importing, and deleting public keys used for authentication of SSHv2 sessions from administrative remote users
nnSC260	security>tls-profile • cert-status-check • cert-status-profile-list	Adding configurations to identify certificate profiles for running SIP over TLS
nnSC620	session-router>access-control> • cac-failure-threshold • untrust-cac-failure-threshold	Adding configurations to set the number of CAC failures for any single endpoint that will demote it from the trusted queue to the untrusted queue (cac-failure-threshold), or from the untrusted queue to the denied trusted queue (untrust-cac-failure-threshold)
nnSC620	session-router>account-config> • file-compression • file-delete-alarm	Adding parameters to support storage expansion for CDR files

nnSC620	session-router>account-config> • ftp-strategy • ftp-max-wait-failover	Adding configurations to support CDR push-receivers; • strategy displays algorithm configured for push-receivers • max-wait displays the maximum wait-time for CDR push-receivers before failover
nnSC620	session-router>account-config>interim-stats-id-types	Adding configuration to set up a correlation ID between calling and called session types for interim statistics
nnSC620	session-router>account-config>protocol	Adding configuration to set the protocol type for CDRS, either RADIUS or DIAMETER
nnSC620	session-router>account-config>push-receiver> • server • port • admin-state • remote-path • filename-prefix • priority • protocol • username • password • public-key	Adding sub-element and parameters to support up to five CDR push receivers; configurable to FTP or SFTP protocols
nnSC620	session-router>enum-config> • query method • failover-to	Adding configurations to support ENUM queries, either Hunt or Round-robin: • Hunt uses a linear method, and always contacts the first server in the server list; only if that server is unavailable will another server be contacted • Round-robin uses a circular method and contacts each server in the list sequentially; e.g. Server 1 is contacted for the first request, Server 2 for the next, and so on When an enum-config's servers are unreachable, the Net-Net SBC can failover to a defined ENUM config that contains different enum servers
nnSC620	session-router>enum-config> • health-query-number • health-query-interval	Adding configurations to support a health query of ENUM servers by sending a standard ENUM NAPTR query
nnSC620	session-router>enum-config>include-source-info	Adding configuration to enable the Net-Net SBC to send source URI information to the ENUM server with any ENUM queries
nnSC620	session-router>enum-config>cache-addl-records	Adding configuration for adding additional records received in an ENUM query to the local cache

nnSC620	session-router>h323>alarm-threshold	Adding configuration to support monitoring and alerting max-calls within H.323 stack via SNMP
nnSC620	session-router>local-policy>policy-attributes> • lookup • next-key	Adding parameters to support multiple stage local policy routing
nnSC620	session-router>local-policy>policy-attributes>ping-all-addresses	Adding parameter to enable pinging each IP address dynamically resolved via DNS; supports session-agent DNS-SRV load balancing
nnSC620	session-router>session-agent>manipulation-pattern	Adding configuration to apply, on a per-session agent basis, sip-manipulation in HMR through logical remote entities
nnSC620	session-router>session-agent>sip-isup-profile	Adding configurations to support, on a per-session basis, SIP-ISUP format version interworking
nnSC620	session-router>session-agent>sip-profile	Adding configurations to apply, on a per SIP-interface basis, SIP-profile configurations
nnSC620	session-router>session-router> • reject-message-threshold • reject-message-window	Adding configuration to apply, on a per-session router basis, sip-manipulation in HMR through logical remote entities
nnSC620	session-router>session-router> • additional-lp-lookups • max-routes-per-lookup • total-lp-routes	Adding configuration to support multiple stage local policy routing
nnSC620	session-router>sip-config>pass-gruu-contact	Adding configuration to support using GRUUs in SIP call flows
nnSC620	session-router>sip-config>refer-src-routing	Adding configuration to trigger a local policy look-up on the source-realm's call originator or REFER originator (for new INVITEs generated from a REFER)
nnSC620	session-router>sip-config>sag-lookup-on-redirect	Adding configuration to look up SAG name when a Redirect is received
nnSC620	session-router>sip-interface>sip-isup-profile	Adding configurations to support, on a per-SIP-interface basis, SIP-ISUP format version interworking
nnSC620	session-router>sip-interface>sip-profile	Adding configurations to apply, on a per SIP-interface basis, SIP-profile configurations
nnSC620	session-router>sip-interface> • manipulation-pattern • manipulation-string	Adding configurations to apply, on a per SIP-interface basis, SIP-manipulation in HMR through logical remote entities
nnSC620	session-router>sip-isup-profile • isup-version • convert-isup-format	Adding sub-element and parameters to configure SIP-ISUP format version interworking

nnSC620	session-router>sip-profile>forked-cac-bw	Adding command to configure CAC bandwidth for forked sessions and enable bandwidth sharing
nnSC620	session-router>sip-profile • ingress-conditional-cac-admit • egress-conditional-cac-admit	Adding sub-element to configure SIP profiles: • ingress-conditional-cac-admit parameter allows Net-Net SBC to process an INVITE with a Require tag as received on an ingress interface • egress-conditional-cac-admit allows Net-Net SBC use conditional bandwidth CAC for media release for calls that are first received by this system SIP-profile configurations can be applied to session agents, realms, and SIP-interfaces via the sip-profile configuration element
nnSC620	session-router>sip-profile • cnam-lookup-server • cnam-lookup-dir • cnam-unavailable-ptype • cnam-unavailable-utype	Adding configuration to support CNAM subtype ENUM queries; can be applied to session agents, realms, and SIP interfaces via the sip-profile configuration element
nnSC620	session-router>sip-manipulation> • export • import	Adding configurations to support importing SIP-manipulation rules as files in a directory that can be exported at a later time
nnSC620	session-router>sip-manipulation>mime-rules> • name • content-type • action • match-value • comparison-type • msg-type • methods • new-value • mime-header-rules session-router>sip-manipulation>mime-isup-rules> • name • content-type • isup-spec • isup-msg-types • action • match-value • comparison-type • msg-type • methods • new-value • mime-header-rules • isup-param-rules	Adding sub-elements and parameters to support SIP-ISUP functionality, which allows for manipulation of ISUP parameters and message parts

nnSC620	session-router>test-sip-manipulation> • sip-manipulation • load-sip-message • refresh-manipulations • display-sip-message • debugging • direction • manipulation-string • manipulation-pattern • tgrp-context • local-ip • remote-ip • execute	Adding configuration to test SIP manipulations
nnSC620	system>network-interface> • add-ssh-ip • remove-ssh-ip	Adding configuration for adding and removing IP addresses for SSH use
nnSC620	system>phy-interface>network-alarm-threshold> • severity • value	Adding sub-element and parameters to set the threshold on a per-port basis; which when exceeded, the system rejects new traffic and allows media only for already-established calls
nnSC620	system>phy-interface>overload-protection	Adding configuration to set the threshold on a per-port basis; when enabled, this feature will reject new SIP-INVITE messages
nnSC620	system>system-access-list>protocol	Adding configuration to specify by protocol the type of management traffic allowed to access the system

SNMP Changes

This section summarizes the SNMP/MIB changes that appear in Net-Net OS Release S-C6.20.

Availability	Changes	MIB Details	Description
nnC620		**Counting global endpoint demotions**	
	Capability group in ap-agentcapability.mib	apSmgmtEndPtDemotionCap Includes: • apSysMgmtEndPtDemotionObjectGroup • apSysMgmtInetAddrWithReasonDOSNotificationGroup (apSmgmtMibCapabilities 39)	Acme Packet agent capability
	Object group in ap-smgmt.mib	apSysMgmtEndPtDemotionObjectGroup Objects: • apSysSipEndptDemTrustToUntrust • apSysSipEndptDemUntrustToDeny • apSysMgcpEndptDemTrustToUntrust • apSysMgcpEndptDemUntrustToDeny (apSystemManagementGroups 19)	Group of attributes for counting global endpoint demotions
	Object in ap-smgmt.mib	apSysSipEndptDemTrustToUntrust (apSysMgmtMIBGeneralObjects 19)	Global counter for SIP endpoint demotion from trusted to untrusted

Availability	Changes	MIB Details	Description
	Object in ap-smgmt.mib	apSysSipEndptDemUntrustToDeny (apSysMgmtMIBGeneralObjects 20)	Global counter for SIP endpoint demotion from untrusted to deny
	Object in ap-smgmt.mib	apSysMgcpEndptDemTrustToUntrust (apSysMgmtMIBGeneralObjects 21)	Global counter for MGCP endpoint demotion from trusted to untrusted
	Object in ap-smgmt.mib	apSysMgcpEndptDemUntrustToDeny (apSysMgmtMIBGeneralObjects 22)	Global counter for MGCP endpoint demotion from untrusted to deny
	Object group in ap-smgmt.mib	apSysMgmtInetAddrWithReasonDOSNotificationsGroup (apSystemManagementGroups 27)	Collection of traps to extend reporting capabilities, which incluses the capability to report both IPv4 and IPv6 addresses
	Endpoint demotion trap in ap-smgmt	apSysMgmtInetAddrWithReasonDOSTrap (apSysMgmtDOSNotifications 4)	Trap generated when an IP address is placed on a deny list because of denial-of-service attempts. It provides the: • IP address that has been demoted • realm ID of that IP address (if available) • URI portion of the SIP From header of the message that caused the demotion • reason for the demotion
nnC620		**H.323 stack information**	
	Capablilty group in ap-agentcapability.mib	apH323StackCap Includes: • apH323StackObjectsGroup • apH323StackNotificationsGroup (apH323MibCapabilities 1)	Acme Packet agent capability
	Object group in ap-h323.mib	apH323StackObjectsGroup Objects: • apH323StackName • apH323StackCurrentCalls (apH323Groups 1)	Object group for providing H.323 stack information
	Object to monitor in ap-h323.mib	apH323StackName (apH323StackEntry 1)	Configured H.323 stack name
	Object to monitor in ap-h323.mib	apH323StackCurrentCalls (apH323StackEntry 2)	Number of current calls
	Notification group in ap-h323.mib	apH323StackNotificationsGroup Notifications: • apH323StackMaxCallThresholdTrap • apH323StackMaxCallThresholdClearTrap (apH323NotificationsGroups 1)	Group listing the traps generated while monitoring H.323 stack

Availability	Changes	MIB Details	Description
	Traps in ap-h323.mib	apH323StackMaxCallThresholdTrap Objects: • apH323StackName • apH323StackMaxCalls • apH323StackMaxCallsThreshold • apH323StackCurrentCalls (apH323Notifications 1) pH323StackMaxCallThresholdClearTrap (apH323Notifications 2)	Trap generated when the number of H.323 calls increases percentage of the max-calls threshold Trap generated when the number of H.323 calls decreases to below the lowest max-calls theshold
nnC620		**Admin security events**	
	Capability group in ap-agentcapability.mib	apSmgmtAdminCap, including: • apSysMgmtAdminGroup (apSmgmtMibCapabilities 40)	Acme Packet agent capability
	Object group in ap-smgmt.mib	apSysMgmtAdminGroup Notifications: • apSysMgmtAuthLockoutTrap • apSysMgmtAuditLogFullTrap • apSysMgmtAuditLogFullClearTrap • apSysMgmtAuditPushFailTrap • apSysMgmtAuditPushFailClearTrap • apSysMgmtWriteFailTrap • apSysMgmtWriteFailClearTrap (apSystemManagementNotificationsGroups 28)	Objects to monitor admin security events
	Admin security trap in ap-smgmt.mib	apSysMgmtAuthLockoutTrap (apSystemManagementMonitors 64)	Generated upon system lockout after multiple authentication failures
	Admin security trap in ap-smgmt.mib	apSysMgmtAuditLogFullTrap Objects: • apSysAdminAuditLogFullReason • apSysCAdminFileName (apSystemManagementMonitors 58)	Generated when one of the audit logs full threshold is met: • time interval • file size • percentage full
	Admin security trap in ap-smgmt.mib	apSysMgmtAuditLogFullClearTrap (apSystemManagementMonitors 59)	Generated when free audit log storage space becomes available
	Admin security trap in ap-smgmt.mib	apSysMgmtAuditPushFailTrap (apSystemManagementMonitors 60)	Generated when the audit file transfer fails
	Admin security trap in ap-smgmt.mib	apSysMgmtAuditPushFailClearTrap (apSystemManagementMonitors 61)	Generated when the audit file is successfully transferred
	Admin security trap in ap-smgmt.mib	apSysMgmtWriteFailTrap (apSystemManagementMonitors 61)	Generated when a write to file fails
	Admin security trap in ap-smgmt.mib	apSysMgmtWriteFailClearTrap (apSystemManagementMonitors 61)	Generated when a write to file succeeds
nnC620		**Phy utilization**	

Availability	Changes	MIB Details	Description
	Capability group in ap-agentcapability.mib	apSmgmtPhyUtilCap, including: • apSysMgmtPhyUtilGroup • apSysMgmtPhyUtilNotificationsGroup (apSmgmtMibCapabilities 42)	Acme Packet agent capability
	Object group in ap-smgmt.mib	apSysMgmtPhyUtilGroup Objects: • apPhyUtilTableRXUtil • apPhyUtilTableTXUtil (apSystemManagementGroups 21)	Objects to monitor PHY utilization
	Object in ap-smgmt.mib	apPhyUtilTableRXUtil (apSysMgmtPhyUtilTableEntry 1)	Generated when the RX network utilization of the physical port is measured over a 1 second period
	Object in ap-smgmt.mib	apPhyUtilTableTXUtil (apSysMgmtPhyUtilTableEntry 2)	Generated when the TX network utilization of the physical port is measured over a 1 second period
	Notification group in ap-smgmt.mib	apSmgmtPhyUtilNotificationsGroup Notifications: • apSysMgmtPhyUtilThresholdTrap • apSysMgmtPhyUtilThresholdClearTrap (apSystemManagementNotificationsGroups 30)	Traps to monitor PHY utilization
	Phy utilization trap in ap-smgmt.mib	apSysMgmtPhyUtilThresholdTrap Objects: • apSysMgmtPhyUtilCurrent • apSysMgmtPhyUtilMinorThreshold • apSysMgmtPhyUtilMajorThreshold • apSysMgmtUtilCriticalThreshold • apSysMgmtPhyRejectOverUtil (apSystemManagementMonitors 66)	Generated when the media port's utilization crosses a configured threshold. Indicates whether the OverloadProtection feature is active.
	Phy utilization trap in ap-smgmt.mib	apSysMgmtPhyUtilThresholdClearTrap (apSystemManagementMonitors 67)	Generated when a media port's utilization falls below the lowest configured threshold
nnC620		**Storage space**	
	Capability group in ap-agentcapability.mib	apSmgmtStorageSpaceCap, Including: • apSysMgmtStorageSpaceGroup • apSysMgmtStorageSpaceNotificationsGroup (apSmgmtMibCapabilities 43)	Acme Packet agent capability
	Object group in ap-smgmt.mib	apSysMgmtStorageSpaceGroup Objects: • apSysVolumeIndex • apSysVolumeName • apSysVolumeTotalSpace • apSysVolumeAvailSpace (apSystemManagementGroups 22)	Objects to monitor storage space
	Object in ap-smgmt.mib	apSysVolumeIndex (apSysStorageSpaceEntry 1)	Monotonically increasing integer for the purpose of indexing volumes
	Object in ap-smgmt.mib	apSysVolumeName (apSysStorageSpaceEntry 2)	Name of the volume

Availability	Changes	MIB Details	Description
	Object in ap-smgmt.mib	apSysVolumeTotalSpace (apSysStorageSpaceEntry 3)	Total size of the volume in MB
	Object in ap-smgmt.mib	apSysVolumeAvailSpace (apSysStorageSpaceEntry 4)	Total space available on the volume in MB
	Notification group in ap-smgmt.mib	apSmgmtStorageSpaceNotificationsGroup Notifications: • apSysMgmtSpaceAvailThresholdTrap • apSysMgmtpaceAvailThresholdClearTrap (apSystemManagementNotificationsGroups 31)	Monitor available storage space
	Storage space trap in ap-smgmt.mib	apSysMgmtSpaceAvailThresholdTrap • apSysMgmtSpaceAvailCurrent • apSysMgmtSpaceAvailMinorThreshold • apSysMgmtSpaceAvailMajorThreshold • apSysMgmtSpaceAvailCriticalThreshold • apSysMgmtPartitionPath (apSystemManagementMonitors 68)	Generated when the space available on a partition crosses a configured space threshold
	Storage space trap in ap-smgmt.mib	apSysMgmtSpaceAvailThresholdClearTrap (apSystemManagementMonitors 69)	Generated when the space available on a partition falls below the lowest configured threshold
nnC620		CDR file deletion	
	Trap added to apSysMgmtNotificationsGroup in ap-smgmt.mib	apSysMgmtCdrFileDeleteTrap • apSysAdminFileName (apSystemManagementMonitors 70)	Generated when a CDR file is deleted because of lack of space on the partition or the drive exceeds the number of files specified

Accounting VSA Changes

This section summarizes the changes to the Net-Net SBC's VSA support for Net-Net OS Release S-C6.2.0.

RADIUS Additions

This section describes the changes to RADIUS accounting. The VSA in the table below have been added to the Acme Packet RADIUS dictionary.

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

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
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
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

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
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-Session-Forked-Call-Id	Header-value without the header parameters from the P-Multiring-Correlator header for a session identified as part of a forked call.	171	string	• Interim-Update • Stop
Acme-User-Privilege	• USED FOR AUTHENTICATION PURPOSES ONLY	253	string	N/A

Diameter Additions

The table below lists RADIUS VSAs that have been created to enable Diameter-based accounting. Refer to this document's Diameter Accounting (14) section for more information about the VSAs listed below.

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Diam-Sess-Id	N/A	172		
Acme-Sip-Method	N/A	173		
Acme-Content-Type	N/A	174		
Acme-Content-Length	N/A	175		
Acme-Event-Time	N/A	176		
Acme-Sdp-Media	N/A	177		

Known Issues

This section lists the known issues associated with Net-Net OS S-C6.2.0.

Defect Area	Description
Access control lists (ACLs) (1852)	When the Net-Net SBC is configured to deny or allow access based on IP address and port, the port number is ignored. Access is denied based ingress realm.
HA nodes using an IPsec interface (1973)	HA nodes do not synchronize properly if they are using an IPsec interface. When the standby system boots, the active advertises that it is synching with its peer. However, the standby remains in the Becoming Active state for an extended time before then going OOS.

Defect Area	Description
TLS with OSCP (2083)	When configured to use TLS only on the peer SIP interface through mutual authentication and UDP on the core-side SIP interface, you might see the ubsec_CipherCommand: Timeout error.
IPsec *Net-Net 3800 and 4500 only* (2159)	With the IPsec physical interface card, jumbo packet support (with fragmentation/reassembly) mgith not work while running over Vlan.
Management Interface	Encrypted fragments are not supported on WANCOM.

Documentation Updates and Changes

There have been the following changes to the Acme Packet documentation set supporting Net-Net OS Release S-C6.2.0.

New Guides

Two new guides appear in the Acme Packet documentation set supporting Net-Net OS Release S-C6.2.0.

- *Net-Net 4000 Administration Security Essentials*—This guide provides information related to the complete set of functionality associated with the Net-Net SBC's Administration Security License. Before you install that license or start to use any of the feature associated with it, you should read the information and fully heed the warning and limitations presented in this guide.
- *Net-Net 4000 Storage Module Installation Guide*—This guide provides information about the storage module that you can use for local CDR storage, and gives instructions for installing the module in your Net-Net 3800 or 4500.
- *Net-Net 4000 Border Gateway Essentials*—This guides provides information related to the complete set of functionality for the Net-Net BG. Previously versions of this document have appeared on their own to support software releases that were specific only to the Net-Net BG, it now appears as part of the main Acme Packet documentation set.