Oracle® Communications Session Border Controller

Release Notes

Release S-CX6.1.0

Formerly Net-Net Session Director

October 2013

ORACLE®

Contents

Contents iii

S-C6.1.0 Release Notes

Introduction

The *S-C6.1.0 Release Notes* provide the following information about Net-Net OS Release C6.1.0:

- 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

Introduction of the Net-Net 3800

Net-Net OS Release S-C6.1.0m1 supports the introduction of the Acme Packet 3800, a new platform that takes its lineage from the Acme Packet family of SBC products. This new platforms supports the same features and functions as its Net-Net 4000 counterparts, with a focus on the 150-500 session range.

The front of the Acme Packet 3800 looks like this:

For hardware details about this system and information about how to install it, refer to the *Net-Net 3800 Hardware Installation Guide*.

Other than the licensing changes described in this section and minor additions to SNMP support, the Net-Net 3800 has the same software as both the Net-Net 4250 and the Net-Nt 4500.

Licensing Information for the Net-Net 3800

Although all features currently available on the Net-Net 4000 series of products are available on the Net-Net 3800, you will see some minor changes in licensing when using this newest addition to the Net-Net family of products. These changes involve:

- Session capacity limits
- Finer session capacity granularity
- Denial of Service
- Software TLS

For more information about Net-Net system licensing, including examples of how to install licenses, refer to the *Getting Started* chapter of the *Net-Net 4000 ACLI Configuration Guide*.

Session Capacity and Your Net-Net 3800

The Net-Net 3800 supports lower session capacity than the Net-Net 4250 or 4500, with a maximum limit of 500 concurrent sessions. The following values are the session capacity values you can license for the Net-Net 3800:

- 150
- 250
- 350
- 500

Additional session capacities may be added at a later date through purchase of sessions in increments of 25, 50 or 100. Session capacity is additive in the Net-Net 3800, meaning the total number of sessions for the system is the sum of all session capacities licensed. The sum total of the licenses cannot exceed 500 sessions.The Net-Net 3800 strictly enforces this limit.

Granularity and Oversubscription Limits

Only on the Net-Net 3800, the Net-Net SBC uses a 10-to-1 oversubscription limit, meaning that the system allows ten registrations for a single licensed session. The system enforces the limits across all signalling protocols.

An SNMP OID, `apSysRegistrationCapacity`, supports querying the percentage of used registration capacity. When the percentage approaches the registration capacity limit, an alarm triggers and the Net-Net 3800 sends an SNMP trap.

- SIP—For SIP, the 10-to-1 ratio limits has possible implications for the SIP registrations cache limiting feature. When you enable that feature, the Net-Net SBC rejects new registrations when they exceed the configurable registration cache limit. Likewise, the system can rejects registrations when they exceed the global oversubscription limit. It uses whichever is the lower of the two.

  The Net-Net 3800 first checks the configurable registrations cache limits. If you have configured this value to be higher than the global oversubscription limits, the Net-Net 3800 leaves the registration cache limit value intact. However, if registrations go over the global oversubscription limit, the Net-Net 3800 will reject them, regardless of the cache limit, and the corresponding traps and alarms might not be triggered.
- H.323—The Net-Net 3800 tracks the number of CallSignalingAddress records as a means of counting registrations. This methods relies on each endpoint having a unique CallSignalingAddress.
- MGCP—Since there can be an unknown number of endpoints registered at once with MGCP, the Net-Net 3800 uses the count called `MGCP Sessions` shown in the MGCP statistics display s a way to count the number of registrations. Note that this value is different from the one listed for MGCP media sessions.

SNMP Support for Global Registration Capacity

For the Net-Net 3800 only, you can use the `apSysRegistrationCapacity` object to query the percentage of used global registration capacity on your system. This object and corresponding group are now part of the apSystemManagement MIB, `ap-smgmt.mib`. The OID and its value are also sent as parameters in the apSysMgmtGroupTrap when an alarm condition occurs. The alarm for this condition is `SYS_REG_OVER_THRESHOLD` with these values: 0x0002003A (hexidecimal) and 131130 (decimal).

The alarm condition depends on whether or not you have set any alarm thresholds for the session type in the system configuration.

- If you have configured them, the thresholds apply to registration capacity. The registration capacity alarm uses the same percentage values and severities for the alarm as those set for the session alarm thresholds.
- If you have not configured them, then the registration capacity alarm triggers at 90%.

The alarm clears when two successive checks, performed once every five seconds, report a value under the threshold.

Denial of Service Feature Group

For the Net-Net 3800 only, a denial of service (DoS) license now exists. When the DoS license not percent, certain whole configurations and specific parameters within unrestricted configurations related to DoS functionality are not available. You can neither configure them, nor can you see them when you use the ACLI `show configuration` command.

The table below details the restrictions.

Restricted Configuration Element	Restricted Parameters
access-control	realm-id source-address destination-address application-protocol transport-protocol access average-rate-limit trust-level invalid-signal-threshold maximum-signal-threshold untrusted-signal-threshold deny-period
media-manager	max-signaling-bandwidth max-untrusted-signaling min-untrusted-signaling fragment-msg-bandwidth tolerance-window arp-msg-bandwidth rtcp-rate-limit
media-profile	average-rate-limit
realm-config	average-rate-limit access-control-trust-level invalid-signal-threshold maximum-signal-threshold untrusted-signal-threshold nat-trust-threshold deny-period
static-flow	average-rate-limit

Software TLS Feature Group

Software TLS is a feature group for the Net-Net 3800 only. It allows for the use of TLS functionality without the presence of an SSM card. If you want to achieve higher capacity for TLS on your Net-Net 3800, you can use the SSM card.

Net-Net 4500 Additions

This section describes the additions made to the Net-Net 4500 that are supported in Net-Net OS Release S-C6.1.0.

IPSec NIU

This section discusses IPSec manual keying for the Net-Net 4500 in the ways that it differs form the Net-Net 4250. In essence, there is very little difference between the two so that explanations and examples of configurations, statistics display commands, and utility command remain applicable.

Link Redundancy

The Net-Net 4500 NIU supports link redundancy such that there is one active port and one standby port. Link redundancy is supported for the entire system, and you must not configure the second physical interface. Any attempt to configure both ports and then use link redundancy will result in error.

The configuration parameter link-redundancy state applies here as it does to the Net-Net 4250, as does the ACLI **show redundancy link** command.

Overview of New Features for Release S-C6.1.0

This section describes new features and capabilities introduced in Acme Packet's Net-Net OS Release S-C6.1.0.

Security

This section describes additions to security.

TLS Key Usage and Other Enhancements

This section describes a body of enhancements to the Net-Net SBC's TLS support. In Release S-C6.1.0, you can:

- Control the role of the certificate based on the usage model
- Set the TLS version, including the deprecation of the **cipher-list** parameter values TLSv1 and SSLv3

A parameter called options has been reserved for future enhancements both in the TLS profile and the certificate record configurations.

External Diameter Interfaces

This section describes the addition to external Diameter interfaces.

DIAMETER AAR Query Post SDP Exchange

For DIAMETER, the Net-Net SBC supports sending the Authentication-Authorize-Request (AAR) query upon SDP answer instead of the SDP offer. This change can useful in WiMax environments where mobile phones go idle and become semi-detached from their base stations and from the WiMax access controller (WAC). In such a case, the WAC receives an AAR from the idle user but, because it cannot determine that user's base station, rejects the request.

The Net-Net SBC's external policy server support now offers three ways for you to handle the reservation of bandwidth for incomplete flows. You set these **reserve-incomplete** parameter.

- Enabled—This mode supports the usual behavior when the AAR is sent upon SDP offer as well as SDP answer. This mode ensures backwards compatibility.

- Orig-realm-only—This mode allows calls originating from a realm with a policy server associated with it to send the AAR upon SDP offer. However, calls terminating at a realm with a policy server associated with it send the AAR post SDP exchange.
- Disabled—This mode allows no bandwidth reservation for incomplete flows.

PCMM COPS Interface

The Net-Net SBC now supports a packet cable multimedia (PCMM) common open policy service (COPS) interface to support bandwidth reservation on an external policy server. This interface allows the Net-Net SBC to perform bandwidth call admission control (CAC) by making bandwidth requests to an external, centralized policy server. This feature allows more flexibility than the Net-Net SBC's internal CAC policies. The PCMM COPS interface allows the Net-Net SBC and policy server to communicate using admissions requests and responses in a standardized and fault tolerant way.

Resource and Admission Control

This section describes the additions to resource and admission control.

Aggregate Session Constraints: Nested Realms

In addition to setting session constraints per realm for SIP and H.323 sessions, you can also enable the Net-Net SBC to apply session constraints across nested realms. For example, if a call enters on a realm that has no constraints but its parent does, then the constraints for the parent are applied. This parameter is global and so applies to all realms on the system. For the specific realm the call uses and for all of its parents, the Net-Net SNC increments the counters upon successful completion of an inbound or outbound call.

Bandwidth CAC Fallback Based on ICMP Failure

For networks where backup links (operating in active-standby mode) from CE-routers to the MPLS backbone are provisioned with less bandwidth than the primary links, the Net-Net SBC can use an ICMP ping to:

- Detect remote link failures
- Trigger bandwidth updates at the realm level when using backup links
- Detect remote link failback to primary

Bandwidth CAC for Aggregate Emergency Sessions

You can configure the maximum amount of bandwidth on your Net-Net SBC you want used specifically for priority (emergency) calls in the realm configuration's **max-priority-bandwidth** parameter. You set this limit on a per-realm basis, and the limit is enforced for nested realms. Setting a bandwidth limit specifically for priority calls allows the Net-Net SBC to reject calls exceeding the threshold, and also to accept calls that exceed the bandwidth limit for non-priority calls (set in the **max-bandwidth** parameter).

Dynamic Demotion for NAT Devices

Net-Net OS Release S-C6.1.0 adds to the various ways the Net-Net SBC promotes and demotes devices to protect against DoS attacks: It can now block off an entire NAT device. The Net-Net SBC can detect when a configurable number of devices behind a NAT have been blocked off, and then shut off the entire NAT's access.

This dynamic demotion of NAT devices can be enabled for an access control (ACL) configuration or for a realm configuration. When you enable the feature, the Net-

Net SBC tracks the number of endpoints behind a single NAT that have been labeled untrusted. It shuts off the NAT's access when the number reaches the limit you set. The demoted NAT device remains on the untrusted list for the length of the time you set in the **deny-period** parameter.

Media Profiles Per Realm

For different codecs and media types, you can set up customized media profiles that serve the following purposes:

- Police media values
- Define media bandwidth policies
- Support H.323 slow-start to fast-start interworking

You can use media policies globally for the Net-Net SBC, or—starting with Release C6.1.0—you can configure them for application on a per-realm basis. For a realm, you can configure a list of media profiles you want applied. The Net-Net SBC matches the media profiles values you configure for a realm, and then it applies those media profiles to the realm itself and to all of its child realms (but not to its parent realms).

NSEP Enhancements

This group of NSEP enhancements covers:

- The ability to configure and monitor NSEP call admission control (CAC) as applied to session agents
- Call treatment when the Net-Net SBC receives a SIP INVITE with and RPH matching the network management controls (NMC) with an ETS DN, but whose r-values do not match the NMC's rph-profile
- Log level changes for instances when users or session agents exceed constraints

QoS Based Routing

In addition to configuring your system for routing based on certain session constraints, you can also set up routing based on QoS. QoS based routing uses the R-Factor on a per-realm basis to either cut back on the traffic allowed by a specific realm, or to shut that traffic off altogether.

- To use this feature, you set up QoS constraints configurations and apply one per realm. The QoS constraints configuration allows you to set up two thresholds:
- Major—The major threshold sets the R-Factor limit beyond which the Net-Net SBC rejects a certain percentage (that you configure) of calls. That is to say, it rejects inbound calls at the rate you set with a `503 Service Unavailable` status code, and rejects outbound calls if there are no alternative routes.
- Critical—The critical threshold, when exceeded, causes the Net-Net SBC to behave the same way it does when any of the session constraints (set in the session-constraints configuration) are exceeded. All inbound calls to the realm are rejected with a `503 Service Unavailable` status code, and (if there is no alternate route) outbound calls are rejected, too. Until the R-Factor falls within acceptable means and the session constraint's time-to-resume value has elapsed, the realm remains in this state.

This feature has SNMP, HDR, and ACLI **show** command support.

IMS Features

This section describes the addition to IMS support.

IMS-AKA

The Net-Net SBC supports IP Media Subsystem-Authentication and Key Agreement (IMS-AKA).

Defined in 3GPPr7 (specifications in TS 33.203 and call flows in TS 24.228), IMS-AKA can be used as a framework for authentication and for securing the signaling path between a UE and the Net-Net SBC (when the Net-Net SBC is acting as a P-CSCF or as a B2BUA) across the Gm interface.

In addition, the Net-Net SBC's serving as an IMS-AKA termination point is valuable because it allows IMS-AKA use behind by multiple endpoints sitting behind a NAT device. IMS-AKA support also works when there are no NAT devices between endpoints and the Net-Net SBC acting as a P-CSCF, and when the Net-Net SBC sits behind a third-party P-CSCF. In addition, you can use IMS-AKA when the endpoint uses SIP UDP.

SIP, IMS, P-CSCF: P-Asserted Identity in Responses

In releases earlier than Release S-C6.1.0, the Net-Net SBC—operating as a P-CSCF—removes the P-Preferred-Identity header (if present) on receipt of a 1xx or 2xx response. It also inserts a P-Asserted-Identity header with the value received in the P-Preferred-Identity header.

Release S-C6.1.0 changes this behavior. Now the Net-Net SBC:

- Caches a copy of the P-Called-Party-ID header when it receives one of the following destined for a UE prior to forwarding the request:
  - An initial request for dialog
  - A request for a standalone transaction
  - A request for an unknown method that does not related to an existing dialog

  The SIP interface receiving the request should have the SIP IMS feature enabled.

Removes the P-Preferred-Identity header (if present) and inserts a P-Asserted-Identity header with the value saved from the P-Called-Party-ID header on receipt of a 1xx or 2xx response.

IMS Charging Vector Mode Adaptation

This adaptation to the Net-Net SBC's IMS functionality provides the ability to remove the P-Charging-Vector from incoming requests for a session and store it. Then the Net-Net SBC inserts it into outbound responses related to that session om a P-Charging-Vector header.

IMS: P-CSCF Endpoint Identification Using Address and Port

You can configure the Net-Net SBC, acting as a P-CSCF, to match a Request it receives to a registration cache entry based only on the IP address and port from which the Request came. When you enable this behavior, the Net-Net SBC will perform this kind of endpoint identification even when there nothing in the message matches the cache entry.

SIP Features

This section describes additions to SIP signaling features.

Globally Unique Call ID for Call Replication

During IP call session replication recording (SRR), the Net-Net SBC records both media and signaling information and then sends them to a configured call recording server (CRS). It is the CRS's responsibility to correlate signaling messages for specific calls, which can be difficult given that call information can traverse other network

elements before reaching the CRS. The task or correlating the call information is simplified by the addition of a globally unique call ID.

For each SIP session, the Net-Net SBC can generate a unique call ID (UCID) that it inserts in SIP Request and Response messages for a call.

Increased CRS Capacity

For IP call session replication recording (SRR), the Net-Net SBC can now support up to 256 call recording servers. No special configuration is required to use this increased number of CRSs.

SIP Method Matching and To Header Use for Local Policies

This feature allows the Net-Net SBC to include SIP methods in routing decisions, granting you greater flexibility when using local policies and has two aspects:

- Basing local policy routing decisions on one or more SIP methods you configure
- Enabling the Net-Net SBC to use the TO header in REGISTER messages for routing REGISTER requests

If you want to use this feature, you set a list of one or more SIP methods in the local policy attributes. These are the SIP methods you can enter in the list: INVITE, REGISTER, PRACK, OPTIONS, INFO, SUBSCRIBE, NOTIFY, REFER, UPDATE, MESSAGE, and PUBLISH.

SIP Per User Subscribe Dialog Limit

On a per-user basis, you can limit the number of SIP SUBSCRIBE dialogs by configuring the number allowed for a given realm. Without setting these limits, the Net-Net SBC permits an unlimited number of SUBCRIBE dialogs. Leaving the number of these dialogs uncontrolled might have potentially damaging consequences:

- Endpoints might create multiple dialogs per event package, causing undesirable Net-Net SBC resource consumption.
- If many endpoints create multiple dialogs, the problem can reach the point of creating a SUBSCRIBE DoS attack on the Net-Net SBC.

You set the restrictions this feature uses in the enforcement profile, where you set the subscription event type and the limitations you want applied to it. You can enter more than one set of subscribe event limitations per enforcement profile.

STUN Server

The Net-Net SBC supports RFC 3489, which defines Simple Traversal User Datagram Protocol (UDP) through Network Address Translators (NATs). Known as STUN, this lightweight protocol that allows applications to:

- Discover the presence and types of both NATs and firewalls between themselves and the public Internet
- Determine the public IP addresses allocated to them by the NAT

SIP endpoints use the STUN protocol to find out the public IP addresses and ports for SIP signaling and RTP media transport. Then they can use the address and port information to create multimedia sessions with other endpoints on the public network.

You can define STUN servers functionality on a per-realm basis, allowing you set up multiple STUN servers.

Synchronize A-HNT Successful Timer to Standby

The Net-Net SBC's Adaptive Hosted NAT Traversal (A-HNT) feature assists SIP endpoints communicating with the Net-Net SBC behind a NAT. The feature enables the Net-Net SBC to determine, through testing, an optimum SIP REGISTER expires time interval that keeps the NAT pinhole open.

For an HA node, this successful time value is determined through testing by the active system and then replicated to the standby. If there is a switchover during the active system's testing process, then it will restart for that endpoint.

Routing and Load Balancing Enhancements

This section describes additions to routing and load balancing.

Custom ENUM Service Type Support

You can configure the ENUM service type that you want to use for an ENUM group. The Net-Net SBC has always supported `E2U+sip` and `sip+E2U` by default, and still does. With Release S-C6.1.0, however, you are also able to configure the service type to those supported in RFCs 2916 and 3721. For example, you can now set the service type in the ENUM configuration to support `E2U+sip` and `E2U+voicemsg:sip`.

Local Policy: DTMF-Style URI Routing

The Net-Net OS Release S-C6.1.0 supports the alphanumeric characters a-d, A-D, the asterisk (*), and the ampersand (#) for local policy matching purposes. The Net-Net SBC handles these characters as standards DN (POTS) or FQDN when found in the **to-addr** (req-uri username) or **from-addr** (from-uri username for SIP, SIPS, and TEL URIs. In addition, before performing the lookup match, the Net-Net SBC strips characters that provide ease-of-reading separation. For example, if the Net-Net SBC were to receive a req-uri containing `tel:a-#1-781-328-5555`, it would treat it as `tel:a#17813285555`.

Local Route Table Support for H.323 and IWF

Local Route Table (LRT) support for H.323 and IWF is compatible with that currently offered for SIP. LRT and ENUM provide the Net-Net SBC with the ability to perform routing based on ENUM queries to a DNS server or local to an onboard database.

For the LRT feature, this means that entries in the local routing table now include those prefixed with the `h323:` URI scheme, indicating that H.323 is the next hop protocol.

DNS Transaction Timeout

To provide resiliency during DNS server failover, you can now enable a transaction timeout for DNS servers. If you have endpoints that are only capable of being configured with a single DNS server, this can allow DNS queries to be sent to the next configured server—even when contacting the Net-Net SBC's DNS ALG on a single IP address. So when the first server in the list times out, the request is sent to the next server in the list.

The Net-Net SBC uses the transaction timeout value set in the **dns-server-attributes** configuration (part of the **dns-config**).

Media Treatment Enhancements

This section describes additions to media treatment.

Multiple Media Profiles

You can use the media profiles configuration to set up:

- One media profile for a particular SIP SDP encoding (such as G729), where the name of the profile identifies it uniquely. This behavior is your only option in Net-Net OS release prior to Release C6.1.0.
- Multiple media profiles for the same SIP SDP encoding. Available in Release C6.1.0 and forward, you can create multiple media profiles for the same encoding. To do so, you add a subname to the configuration, thereby identifying it uniquely using two pieces of information rather than one.

Transport Protocol Additions

This section describes additions to transport protocol support.

SIP over SCTP

In releases prior to Release S-C6.1.0, the Net-Net SBC supports UDP and TCP as transport protocols for SIP signaling. Release S-C6.1.0 introduces support for Stream Control Transport Protocol (SCTP). Young in relation to UDP and TCP, SCTP seeks to address some of the shortcomings of the other two transport protocols—most notably by supporting

- Multi-homing—When multiple IP addresses are assigned to a host on the network. Typically, this arrangement entails a host that has multiple network interface cards. (To be supported in future Net-Net OS releases.)
- Multi-streaming—Ability to partition data within an association into multiple logical communication channels. Each logical channel—or stream—has the property of independent sequenced delivery. This means that data loss on one stream has no impact on delivery on other streams. (Net-Net OS Release S-C6.1.0 supports two incoming and two outgoing streams.)

For a full description of SCTP, refer to RFC 2960 Stream Control Transmission Protocol.

Management Enhancements

This section describes the management enhancements that have been added in Net-Net OS Release S-C6.1.0.

Realm-Specific Delete Command

The ACLI provides a way to delete a specific realm and the configurations (objects) associated with that realm. You use the **delete realm-specifics** command with the name of the realm you want to delete. Not only does the Net-Net SBC delete that realm, it also deletes the configurations where that realm is also used as a primary or foreign key—such as steering pools, session agents, and SIP interfaces. A complete list of configurations and parameters subject to deletion appears in the *Net-Net S-C6.1.0 ACLI Maintenance and Troubleshooting Guide*.

Clearing ENUM and DNS Statistics

To clear statistics for ENUM and DNS, you can use additions to the ACLI **reset** command. Before you reset the counters, however, you might want to confirm the current statistics on the system are not zero. You can do so using the show command—by typing, for example, **show enum stats**.

The **reset** command takes the ENUM and DNS arguments to clear those sets of statistics. When you use the command, the system notifies you whether it has successfully cleared the statistics (even if the counter are zero) or if it has run into an error causing the command to fail.

You can **reset all** system statistics using the reset all command.

Wancom Port Speed and Duplex Mode Display

You can display the negotiated duplex mode and speed for all Net-Net system control ports by using the ACLI **show wancom** command. Available in Releases S-C6.1.0 and later, this command allows you to diagnose network issues more efficiently. When you use this command, the systems shows information for all three control ports with the numbers starting at 0. It will then tell you the negotiated duplex mode and speed, or that the link is down.

Displaying the System Timezone

You can display the timezone configured for your Net-Net SBC using the ACLI show timezone command. The new **timezone-set** command displays: the name of the timezone, its minutes from UTC, and the start and stop date and hours for daylight saving time.

ACLI Verify-Config Enhancements

This section summarizes the enhancements made to the ACLI **verify-config** command. For detailed information about IP address and port checks, refer to the *Net-Net S-C6.1.0 ACLI Maintenance and Troubleshooting Guide*.

Verifying Configurations

The **verify-config** command checks the consistency of configuration elements that make up the current configuration and should be carried out prior to activating a configuration on the Net-Net SBC.

When the **verify-config** command is run, anything configured that is inconsistent produces either an error or a warning message. An error message lets the user know that there is something wrong in the configuration that will affect the way Net-Net SBC runs. A warning message lets the user know that there is something wrong in the configuration, but it will not affect the way the Net-Net SBC runs.

Verifying Address Duplication

The **verify-config** command, entered either directly or via the **save-config** command, checks for address duplication for a given network-interface within a configuration. Addresses are checked for duplication based on the following criteria:

- Every address entered is checked against the Primary and Secondary Utility addresses
- All UDP, TCP, and TFTP addresses are checked against other UDP, TCP, and TFTP addresses respectively within the same port range

RADIUS Accounting Enhancements

This section describes the enhancements to RADIUS accounting.

QoS: R-Factor and MOS Generation for End of Call Statistics

The Net-Net SBC now 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:

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Calling-R-Factor	QoS R-Factor calculation for the calling side of a session.	151	integer	• Stop
Acme-Calling-MOS	QoS MOS calculation for the calling side of a session.	152	integer	• Stop
Acme-Called-R-Factor	QoS R-Factor calculation for the called side of a session.	153	integer	• Stop
Acme-Called-MOS	QoS MOS calculation for the called side of a session.	154	integer	• Stop

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.

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.

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.

SIP Accounting: Interim RADIUS Records for Recursive Attempts

When the Net-Net SBC routes calls, it performs local policy look-ups that can return several next hops, ordered by preference. This can also happen as a results of and LRT lookup, an ENUM query response, or SIP redirect. To set up sessions, the Net-Net SBC uses—in ordered preference—and recurses through the list if it encounters failures.

You can configure SIP accounting to send RADIUS Interim records when the Net-Net SBC encounters these failures. The interim message contains: the destination IP address, the disconnect reason, a timestamp for the failure, and the number that was called.

MIB, Trap, and Alarm Changes

This section lists the changes to MIBs, traps, and alarms made as part of Net-Net OS Release S-C6.1.0. This document's SNMP Changes (23) section provides more information about these additions, and you can find full details in the *Net-Net 4000 MIB Reference Guide* for this release.

Alarm Synchronization

Two trap tables in the `ap-smgmt.mib` record trap information for any condition on the Net-Net SBC that triggers an alarm condition (when you enable your system to do so). You can poll these two tables from network management systems, OSS applications, and the Net-Net EMS to view the fault status on one or more Net-Net SBCs.

The two trap tables that support alarm synchronization, and by polling them you can obtain information about the current fault condition on the Net-Net SBC. These tables are:

- apSysMgmtTrapTable
- apSysMgmtTrapInformationTable

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.

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`

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. The following is defined in the apSysMgmtGeneralObjects:

```
apSysApplicationCPULoadRate    OBJECT-TYPE
        SYNTAX          Unsigned32
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
             " The average load rate of the service applications taken
over a period, up to 10 seconds."
    ::= { apSysMgmtMIBGeneralObjects 16 }
```

SNMP Support for Bandwidth CAC Fallback Based on ICMP Failure

Net-Net OS Release S-C6.1.0 provides the following SNMP support for Bandwidth CAC Fallback Based on ICMP Failure (9).

When it determines a target is unreachable, the Net-Net SBC issues the `apSysMgmtRealmICMPReachableTrap` indicating ICMP heartbeat failure and sends the corresponding alarm. Because it can be sent for different realms, the trap might go out multiple times. However, the alarm appears only once in the alarm display. It will be cleared with the `apSysMgmtRealmICMPReachableClearTrap` only when all instances are cleared.

SNMP Support for QoS Based Routing

Net-Net OS Release S-C6.1.0 provides the following SNMP support for QoS Based Routing (10).

The MIBs in the following table are defined in the `apSigRealmStatsTable` for the `apSigRealmStatsEntry`.

SNMP GET Query Name	Object Identifier	Description
apSigRealmStatsAverageQosRFactor	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.24	Average QoS RFactor
apSigRealmStatsMaximumQosRFactor	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.25	Maximum QoS RFactor
apSigRealmStatsCurrentMajorRFactorExceeded	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.26	Number of times Major RFactor exceeded in current window
apSigRealmStatsTotaltMajorRFactorExceeded	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.27	Number of times Major RFactor exceeded over the lifetime
apSigRealmStatsCurrentCriticalRFactorExceeded	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.28	Number of times Critical RFactor exceeded in current window
apSigRealmStatsTotaltCriticalRFactorExceeded	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.29	Number of times Critical RFactor exceeded over the lifetime
apSigRealmStatsRealmStatus	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.30	Current status of the realm (INS, ConstraintsViolation, callLoadReduction)

The trap defined in the following table also support QoS based routing.

Trap Name	Object Identifier	Description
apSysMgmtRealm StatusChangeTrap	1.3.6.1.4.1.9148.3.2.6.0.45	Generated when a realm changes status. • apSysMgmRealmName—The realmId • apSysMgmtRealmStatusReason—The status reasons Possible status reasons are: • administrative(0) • oosbyproxyerror(1) • standby(2) • inservice(3) • constraintsexceeded(4) • unresponsive(5) • oosprovisionedresponse(6) • callloadreduction(7)

Management Changes Summary

This section summarizes the projected ACLI, SNMP, and RADIUS accounting management changes for Net-Net OS Release S-C6.1.0. Changes appearing in this document have been added since the availability of Net-Net OS C6.0.0.

ACLI Changes

This section summarizes the ACLI command and configuration changes that appear in Net-Net OS Release S-C6.1.0.

Availability	Change	Description
nnC600m1	session-router>account-config>generate-interim>unsuccessful-attempt	Adding parameter value to support sending RADIUS Interim records for recursive attempts associated with a call
nnC600m1	media-manager>media-manager-config>dnsalg-server-timeout	Adding parameter to support DNS transaction timeout
nnC600m1	session-router>sip-interface>options>reg-via-match	Adding parameter value to support IMS P-CSCF identification using address and port
nnC600m1	session-router>sip-interface>charging-vector-mode>delete-and-respond	Adding parameter value to support the ability to remove the P-Charging-Vector from incoming requests for a session, store it, and inserts it into outbound responses related to that session in a P-Charging-Vector header
nnSC610	security>ipsec>security-associaton>manual> • in-local-ip-mask • in-remote-ip-mask • in-vlan-id-mask • full-policy-match	Removing parameters no longer needed for IPSec manual security association configurations

Availability	Change	Description
nnSC610	session-router>session-router-config>nested-realm-stats	Adding parameter to support using session constraints for nested realms across the entire system
nnSC610	system>system-config>trap-event-lifetime	Adding parameter to support alarm synchronization
nnSC610	media-manager>realm-config> • icmp-detect-multiplier • icmp-advertisement-interval • icmp-target-ip • fallback-bandwidth	Adding parameters to support bandwidth CAC based on ICMP failure
nnSC610	media-manager>realm-config>max-priority-bandwidth	Adding parameter to support bandwidth CAC for aggregate emergency sessions
nnSC610	media-manager>ext-policy-server>reserve-incomplete	Changing parameter to support Diameter AAR query post SDP exchange; new value is **orig-realm-only**
nnSC610	session-router>access-control>nat-trust-threshold media-manager>realm-config>nat-trust-threshold	Adding parameters to support dynamic demotion of NAT devices
nnSC610	session-router>enum-config>service-type	Adding parameter to support custom ENUM service type
nnSC610	session-router>sip-config>add-ucid-header	Adding parameter to support globally unique call ID for IP call session replication recording
nnSC610	security>ims-aka-profile> • name • protected-server-port • protected-client-port • encr-alg-list • auth-alg-list security>ipsec>ipsec-global-config> • red-ipsec-port • red-max-trans • red-sync-start-time • red-sync-comp-time session-router>sip-interface>ims-aka-feature session-router>sip-interface>sip-port>ims-aka-profile	Adding element and parameters to support IMS-AKA
	show sa stats	Changing command output to display information for IMS-AKA
nnSC610	session-router>local-policy>from-address	Changing parameter to accept values prefixed with **DS:** (dialed string) for supporting DTMF-style URI routing
nnSC610	session-router>h323>enum-sag-match	Adding parameter to support Local Route Table (LRT) support for H.323 and IWF calls

Availability	Change	Description
nnSC610	media-manager>realm-config>match-media-profiles	Adding parameter to support media profiles per realm
nnSC610	session-router>media-profile>subname	Adding parameter to support using multiple media profiles for the same codec
nnSC610	session-router>sip-config>nsep-sa-sessions-rate	Adding parameter to support NSEP limits for SIP session agents
nnSC610	session-router>qos-constraints> • name • state • major-rfactor • critical-factor • call-load-reduction	Adding element and parameters to support QoS-based routing
nnSC610	show sipd sa-nsep-burst	Adding command to display the NSEP burst rate for all session agents
	media-manager>realm-config>qos-constraints	
nnSC610	show realm> • external • internal	Changing command and subcommands to display QoS-based routing data, and these statistics: • QoS Major Factor Exceeded • QoS Critical Exceeded • QoS R-Factor Average
nnSC610	session-router>account-config>account-server>priority	Adding parameter to support RADIUS account sever prioritization
nnSC610	delete realm-specifics <realm ID>	Adding command to delete a specific realm
nnSC610	show timezone	Adding to support display the configured timezone
nnSC610	session-router>local-policy>policy-attributes>methods	Adding parameters to support SIP method local policies
nnSC610	session-router>sip-config>register-use-to-for-lp	Adding and changing parameters to support using the To header for routing; **next-hop** now accepts ENUM as a value
	session-router>local-policy>policy-attributes>next-hop	
nnSC610	system>network-parameters>sctp-send-mode	Adding parameters to support SIP over SCTP
nnSC610	session-router>sip-interface>sip-port>transport-protocol	Changing parameters to support SIP over SCTP; SCTP is now a valid value for these parameters
	session-router>session-agent>transport-method	
	session-router>session-agent>reuse-connections	

Availability	Change	Description
nnSC610	session-router>enforcement-profile>subscribe-event> • event-type • max-subscriptions	Adding subelement and parameters to support SIP per user subscribe dialog limit
nnSC610	show registrations sipd subscriptions-by-user	Adding to command to support displaying data related to SIP per user subscribe dialog limit
nnSC610	media-manager>realm-config> • stun-enable • stun-server-ip • stun-server-port • stun-changed-ip • stun-changed-port	Adding subelement and parameters to support the STUN server
nnSC610	show mbcd stun	Changing command to add STUN server data
nnSC610	security>certificate-record> • key-usage-list • extended-key-usage-list	Adding parameters to support TLS key usage and extended key usage extensions
nnSC610	security>tls-profile>tls-version	Adding parameter to support setting the TLS version
nnSC610	security>tls-profile>cipher-list • tlsv1 • sslv3	Removing these values from the parameter because; they have been made redundant by the **tls-version** parameter
nnSC610	reset enum	Adding command to reset ENUM statistics
nnSC610	session-router>session-agent>manipulation-string session-router>session-router>forced-report-trunk-info session-router>sip-manipulation>header-rules>element-rules>type • uri-user-only • uri-phone-number-only	Adding to support custom RADIUS VSAs for SIP calls
nnSC610	media-manager>ext-policy-server>watchdog-ka-timer media-manager>ext-policy-server>application-mode • pkt-mm-3	Adding to support the COPS PCMM interface
nnSC610	reset dns	Adding command to reset DNS statistics
nnSC610	show wancom	Adding command to show the duplex mode and speed for control interfaces
nnSC610	verify-config	Changing command to broaden the scope of configuration verification; checks consistency of configuration elements

Availability	Change	Description
nnSC610	batch	Removing command from the ACLI
nnSC610m1	mgcp-config>ca-ping-retries	Adding parameter to support graceful MGCP switchover

SNMP Changes

This section summarizes the SNMP/MIB changes that appear in Net-Net OS Release S-C6.1.0.

Availability	Changes	MIB Details	Description
nnSC610		**Default gateway synchronization in ARP table**	
	Capability group in MIBS README.txt	apSystemManagementGatewaySynchronizedMonitorCap	Acme Packet agent capability
	Object group in ap-smgmt.mib	apSysMgmtMonitorNetworkGatewaySynchronizedNotifcationsGroup Notifications: • apSysMgmtGatewaySynchronizedTrap (apSystemManagementNotificationsGroups 20)	Objects to monitor synchronized gateway trap
	Trap in ap-smgmt.mib	apSysMgmtGatewaySynchronizedTrap (apSystemManagementMonitors 49)	Generated when the default gateway is synchronized in the ARP table
nnSC610		**CDR push receivers**	
	Capability group in ap-agentcapability.mib	apSmgmtCDRPushReceiverFailureCap, including: • apSysMgmtCDRPushReceiverNotificationsGroup (apSmgmtMibCapabilities 33)	Acme Packet agent capability
	Object group in ap-smgmt.mib	apSysMgmtCDRPushReceiverNotificationsGroup Notifications: • apSysMgmtCDRPushReceiverFailureTrap • apSysMgmtCDRPushReceiverFailureClearTrap • apSysMgmtCDRPushAllReceiversFailureTrap • apSysMgmtCDRPushAllReceiversFailureClearTrap (apSystemManagementNotificationsGroups 24)	Objects to monitor CDR push receiver failures
	CDR push receiver trap in ap-smgmt.mib	apSysMgmtCDRPushReceiverFailureTrap Objects: • apSysCDRPushReceiverAddressType • apSysCDRPushReceiverAddress • apSysCDRPushReceiverFailureReasonCode (apSystemManagementMonitors 53)	Generated when an enabled CDR push receiver fails
	CDR push receiver trap in ap-smgmt.mib	apSysMgmtCDRPushReceiverFailureClearTrap Objects: • apSysCDRPushReceiverAddressType • apSysCDRPushReceiverAddress (apSystemManagementMonitors 54)	Generated when an enabled CDR push receiver resumes normal operation after a failure
	CDR push receiver trap in ap-smgmt.mib	apSysMgmtCDRPushAllReceiversFailureTrap (apSystemManagementMonitors 55)	Generated when all enabled CDR push receivers fail

Availability	Changes	MIB Details	Description
	CDR push receiver trap in ap-smgmt.mib	apSysMgmtCDRPushAllReceiversFailureClearTrap (apSystemManagementMonitors 56)	Generated when one or more enabled CDR push receivers return to normal operation after failures occured on all receivers
nnSC610		**Session controller trap table**	
	Capability group in ap-agentcapability.mib	apSmgmtTrapTableObjectCap, including: • apSysMgmtTrapTableObjectGroup (apSmgmtMibCapabilities 32)	Acme Packet agent capability
	Object group in ap-smgmt.mib	apSysMgmtTrapTableObjectGroup Objects: • apTrapTableNumVariables • apTrapTableSysUptime • apTrapInformationTableDataType • apTrapInformationTableDataLength • apTrapInformationTableDataOctets (apSystemManagementGroups 14)	Attributes of the trap table in the Session Border Controller
nnSC610		**Realm ICMP Failure**	
	Capability group in ap-agentcapability.mib	apSmgmtRealmIcmpFailureCap, including: • apSysMgmtIcmpFailureNotificationsGroup (apSmgmtMibCapabilities 31)	Acme Packet agent capability
	Object group in ap-smgmt.mib	apSysMgmtIcmpFailureNotificationsGroup Notifications: • apSysMgmtRealmIcmpFailureTrap • apSysMgmtRealmIcmpFailureClearTrap (apSystemManagementNotificationsGroups 23)	Objects to monitor ICMP failure
	Realm ICMP trap in ap-smgmt.mib	apSysMgmtRealmIcmpFailureTrap Objects: • apSysMgmtRealmID (apSystemManagementMonitors 51)	Generated when ICMP heartbeat failure occurs
	Realm ICMP trap in ap-smgmt.mib	apSysMgmtRealmIcmpFailureClearTrap Objects: • apSysMgmtRealmID (apSystemManagementMonitors 52)	Generated when ICMP heartbeat failure clears
nnSC610		**Application CPU usage**	
	Capability group in ap-agentcapability.mib	apSmgmtApplicationCPUUsageCap, including: • apSysMgmtApplication CPUUsageGroup (apSmgmtMibCapabilities 36)	Acme Packet agent capability
	Object group in ap-smgmt.mib	apSysMgmtApplicationCPUUsageGroup Objects: • apSysApplicationCPULoadRate (apSystemManagementGroups 16)	Objects to monitor appliation CPU usage
	Object in ap-smgmt.mib	apSysApplicationCPULoadRate (apSysMgmtMIBGeneralObjects 16)	Average load rate of the service applications taken over a period of up to 10 seconds

Known Issues

This section provides a summary of known issues for Net-Net OS Release S-C6.1.0.

Issue Area	Description	Workaround
apSysMgmtTrapTable, Net-Net 4500	On the Net-Net 4500 only, there is an issue when running the TRAP_TABLE.	Do NOT run the apSysMgmtTrapTable on the Net-Net 4500.
IPSec and Session replication for recording	Session replication for recording (SRR) feature should not be enabled on Net-Net 4500s equipped with IPSec cards.	N/A

Documentation Updates

Since the ACLI **batch** command is no longer supported and has been removed from the ACLI, all mention of it has likewise been removed from the Net-Net ACLI documentation set. This change has the most impact on the *Net-Net 4000 ACLI Reference Guide*.

Revision History

This section contains a revision history for this document.

Date	Revision Number	Description
March 27, 2009	Revision 1.10	• Adds Net-Net 3800 introduction and licensing information • Adds new parameter for MCGP switchover support • Documentation set supports the following adaptations introduced in Release S-C6.1.0m1: DIAMETER STR timeouts, International Peering with IWF and H.323 Calls, MGCP Switchover Adaptation • Adds known issues about call recording and IPSec