Oracle® Communications Session Border Controller

HDR Resource Guide
Release 7.1.2

2014

ORACLE

Notices

Contents

About this Guide

The Oracle Communications Session Border Controller HDR Resource Guide provides information about Historical Data Recording (HDR) for S-C Series products. This document includes the following information:

- Description of HDR and how it works
- Enabling/disabling HDR
- Starting, stopping, restarting, purging, and requesting HDR status using the Acme Command Line Interface (ACLI)
- Using a Push Receiver to push the data to a server
- HDR Groups and Group Statistics
- "Show" commands associated with the HDR Groups and Group Statistics

Release S-CZ7.1.2 is supported on the Acme Packet 4500 and Acme Packet 6300 series platforms.

Related Documentation

The following table describes related documentation for the Oracle Communications Session Border Controller.

Document Name	Document Description
Acme Packet 4500 Hardware Installation Guide	Contains information about the components and installation of the AP4500.
Acme Packet 3820 Hardware Installation Guide	Contains information about the components and installation of the AP 3800.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the AP 6300.
Acme Packet 6100 Hardware Installation Guide	Contains information about the components and installation of the AP 6100.
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 of the Oracle Communications Session Border Controller.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about Oracle Communications Session Border Controller 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), Acme Packet's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the Oracle Communications Session Border Controller's accounting support, including details about RADIUS accounting.

Document Name	Document Description
HDR Resource Guide	Contains information about the Oracle Communications Session Border Controller's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the Oracle Communications Session Border Controller's support for its Administrative Security license.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the Oracle Communications Session Border Controller family of products.

Revision History

The following table describes updates to this guide.

Date	Description
July 2013	• Initial Release
Sept 2013	• Added outputs of "Local Contacts," "HNT Entries," and "Non-HN Entries" in the **show sipd realms** command.
May 2014	• Adds public key configuration procedure. • Removes MIB OID Numbers for Group: Space per request from ENG. • Improves description for Average one way signlaing latency and Maximum one way signaling latency objects. • Fixes capitalization error presented in the I2C Bus State variable description. • Adds caveats on data within CSVs. • Added missing Current Deny Entries Allocated data field to system group. • Added missing Total Subscriptions data field to session-realm group. • Added missing Call Rejects data field to sip-errors group. • Corrects data type and range for sip-status' session rate variable. • Corrects data type and range for sip-status' load rate variable. • Adds note indicating that transaction timeout statistics are not valid for server operations. • Adds note indicating that locally throttled statistics are not valid for server operations. • Corrects typo mislabeling sip-rate-per-agent.
Sept 2014	• Compressed chapter 3 statistics into a single table according to group. • Changed Range values of "Application Load Rate" in system group from "0 to 4294967295" to "0% to 100%".

1

Overview

This section provides an overview of Historical Data Recording (HDR) and how it works on the C-Series products. It also provides information about enabling and disabling HDR on the SBC.

What is HDR

Historical data recording (HDR) refers to a group of management features that allow you to configure the SBC to collect statistics about system operation and function, and then send those records to designated servers. System statistics, defined in detail below, are saved to a comma-separated value (CSV) file, which are then sent to the designated server(s).

Information types are grouped so that you can refer to a set of statistics by simply invoking their group name (For example, the system statistics are in a group called **System**; interface statistics are in a group called **Interface**; etc.). Within each group, there are several metrics available.

The following table describes the type of HDR statistics that the SBC can collect and forward to a designated server.

HDR Statistics	Description
Group Name	The name of the group that contains the HDR statistics. This name is similar to the current SBC ACLI parameters. For example, system, interface, session-agent, session-realm, etc. The SBC uses the group name when generating the .CSV file (for example, system.csv, interface.csv, etc.).
Group Statistics	Various statistical parameters within a group. These statistical parameters appear in the first record of the header in each .CSV file (for example, in the system.csv file, the header would include the statistic headings of CPU Utilization, Memory Utilization, Health Score, etc.).
Type	Type of statistical parameter. This document makes use of the following data types: **counter** - A counter is an integer with a minimum possible value of 0 and a maximum value of 4294967295. A counter is always increasing in value or remaining unchanged. It decreases only in response to reaching its maximum possible value, at which point it's next value (when the next counted entity or event occurs) will be 0. **gauge** - A gauge is an integer with the same bounds as a counter. However, it does not always have an increasing value. Its value may go up or down.

HDR Statistics	Description
	period - A period type represents a value determined as the sum of a number of events which occurred during a specified window of time, or stated alternatively, a time period. There are three windows defined, the "current window", the "previous window", and the "sliding window". For more information about these windows, see **Windows of Time** . **config** - For the config type, the value for this field comes from a configuration record. **timeticks** - For the timeticks type, each tick is 1/100th of a second. **string** - A statistic type pertains to statistics that display as an alpha-numeric character string.
Timer Value (seconds)	For period statistics (statistics that use a period timer), this is the default value, in seconds, of the timer. This value is usually not configurable. However, this value may fall within a range of values if applicable.
Range	The range of values that a group statistic may use when the SBC collects statistics.

For descriptions of specific HDR Statistics and values, see **HDR Groups and Group Statistics**.

Enabling/Disabling HDR

In the system configuration, you can enable HDR by first turning on the system's collection function, then choosing the records you want to capture, and finally setting up server(s) to which you want records sent.

The main collect configuration (found within the main system configuration) allows you to create global settings that:

- Enable or disable HDR at boot time
- Set the sample rate in seconds, or the time between sample individual collections
- Set the time, in seconds, between individual pushes to designated servers (configured in the push receiver configuration accessed via the collect configuration)
- Set the time you want the collect to start and stop; time is entered in year, month, day, hours, minutes, and seconds

You also configure settings for each group of data you want to collect, and the push receiver (server) to which you want data sent.

For more information about configuring HDR on the SBC, see the Configuring HDR section.

Protocol Use

You can configure HDR to send files using File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP) for added security. FTP is the default.

Note: Public key authentication is not available when you choose SFTP. Instead, the SBC uses password authentication. However, for SFTP to work, it is still required that you load the SFTP's host public key on the SBC.

About the CSV File

When HDR is enabled, statistical records are forwarded from the SBC to push servers that send the data (in standard format) to a receiving server for viewing in a comma-separated value (CSV) file on the server. Before pushing a file, the collector creates the directory by group name for which the statistic belongs (for example, fan, sip-client, system, etc.), if the directory does not exist from a previous push.

The collector can push multiple CSV files per directory. Each file is formatted as <Unix timestamp>.csv (for example, 1302041977.csv). The first record of each file is a header containing the attribute name. For example, in the

System directory, a file name of 13020441977.csv can contain the header names of CPU Utilization, Memory Utilization, Health Score, Redundancy State, etc. The collector appends a Timestamp heading attribute to the beginning of every record as well. You can open the CSV file for viewing with any application that reads a CSV file format. For more information about the CSV file, see **HDR Data**.

Note: The records in a CSV file may display differently, depending on the record data included in the file, and the method used to open the file. For more information about the display of record data in a CSV file, see Appendix A, **CSV File Data Formats**.

Collection Interval and Push

In your HDR configuration, you can set parameters that allow you to:

- Select the groups for record collection
- Set the frequency of record collection
- Set the frequency of off-box record collection

After configuring and enabling HDR, the SBC forwards group records to push servers that send the data to a receiving server. The number of records in a push equals the push interval divided by the sample interval time multiplied by the number of groups, plus one:

push interval ÷ sample interval time x number of groups +1 header record per group = number of records in a push

For example, if you set a push interval time of 60 minutes and a sample interval time of 5 minutes, with 10 groups, the SBC would send 120 group records plus 10 header records (for a total of 130 records) for each push:

[(60 ÷ 5) x 10] +10 = 130

You can configure an option parameter (disabled by default) that instructs the SBC to send a trap when data has been successfully pushed. This trap is defined in the ap-smgmt.mib. It contains the name of the node that successfully pushed the HDR file to an HDR server, a unique file name for the HDR file that was pushed, and the IP address of the push receiver (configured in the global collection configuration). For more information about the HDR SNMP traps, see the product-specific SBC MIB Reference Guide.

Note: After each push, the SBC clears (deletes) all records. The SBCSD also clears files on system reboot, and after three consecutive push failures.

2

Configuring HDR

This section provides information and procedures for configuring HDR on the C-Series products. It also includes procedures for starting and stopping the collection of data at the Acme Packet Command Line Interface (ACLI).

Configuring HDR via the ACLI

This section provides procedures for configuring HDR. HDR configuration includes:

- setting parameters to govern sample and push intervals, and start/end times for collection
- setting parameters to support HDR across a high availability (HA) node
- setting group parameters to inform the Oracle Communications Session Border Controller (SBC), which groups of records to collect, when to start and stop collecting, and how often to sample for a specific group.
- setting push receivers that transport the records forwarded by the SBC

Note: If you modify the HDR configuration parameters using the ACLI, the changed parameters DO NOT take affect until you reboot the SBC

Enabling HDR Collection

You access the parameters that enable and support HDR using the ACLI **system-config** path.

To enable HDR collection:

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

```
ACMEPACKET# configure terminal
```

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

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

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

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

4. Enter **collect** and press Enter. From here, you can type a question mark (?) to see individual parameters for the configuration.

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

Setting Global Collection

You access the collection configuration through the ACLI system-configuration menu. Once in the collection configuration, you can establish the global settings for HDR collection.

To set HDR global collection:

1. In Superuser mode, navigate to the collect parameter level in the ACLI.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# system
ACMEPACKET(system)# system-config
ACMEPACKET(system-config)# collect
ACMEPACKET(collect)#
```

2. **Set global collection parameters as applicable. Parameters include:**

   - **sample-interval**—Enter the time in minutes for how often you want the SBC to sample data records. The default is **5**. The valid range is:
     - Minimum—1
     - Maximum—120
   - **push-interval**—Enter the time in minutes for how often you want the SBC to send collected records to push receiver(s). The default is **15**. The valid range is:
     - Minimum—1
     - Maximum—120
   - **boot-state**—Set this parameter to **enabled** to start group collection, or to **disabled** to prevent the SBC from collecting HDR statistics. This parameter does not go into effect until the system is rebooted. You can also use the ACLI request collect start command to start collection; using this command, you can start collection for all groups, or for one specified group. The default is **disabled**. Valid values are:
     - enabled | disabled
   - **start-time**—Enter the exact date and time (for your local timezone) when you want the SBC to start HDR collection. You can enter **now** to set the start-time to the current time, or you can specify a time in the future. If you specify a time, it must be in the format yyyy-mm-dd-hh:mm:ss, where: yyyy is the year, mm is the month, dd is the day, hh in the hour, mm is the minutes, and ss is the second (24-hour clock). The default is **now**.
   - **end-time**—Enter the exact date and time (for your local timezone) when you want the SBC to finish HDR collection. You can enter **never** to set the time to never end, or you can specify an end time in the future. If you specify a time, it must be in the format yyyy-mm-dd-hh:mm:ss, where: yyyy is the year, mm is the month, dd is the day, hh in the hour, mm is the minutes, and ss is the second (24-hour clock). The default is **never**.
   - **push-success-trap-state**—Set this parameter to **enabled** if you want the SBC to send a trap confirming successful data pushes to HDR servers. Default is **disabled**. Valid values are:
     - enabled | disabled

Setting HDR for an HA Node

If you are using the HDR feature on a High Availability (HA) node (or redundant pair of SBCs), several parameters in the collection configuration must be set for HDR to perform properly.

Oracle recommends strongly that you do not change these parameters from their defaults for a normal HA node configuration. Therefore, if you need to change them to support HDR, you should do so with caution.

To set HDR support across an HA node:

1. In Superuser mode, navigate to the **collect** parameter level in the ACLI.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# system
ACMEPACKET(system)# system-config
ACMEPACKET(system-config)# collect
ACMEPACKET(collect)#
```

2. **Set HDR collection parameters for an HA node as applicable. Parameters include:**

   - **red-collect-state**—Set the state of HA support for the collector function. The default is **disabled**. Valid values are:

     - enabled | disabled
   - **red-max-trans**—Enter the maximum number of HA synchronized transactions to maintain on the active system in the HA node. The default is **1000**. The valid range is:

     - Minimum—0
     - Maximum—999999999
   - **red-sync-start-time**—Enter the amount of time, in milliseconds, that the active SBC checks to confirm that it is still the active system in the HA node. If the active system is still adequately healthy, this timer resets itself. If for any reason the active has become the standby, it starts to checkpoint with the newly active system when this timer expires. The default is **5000**. The valid range is:

     - Minimum—0
     - Maximum—999999999
   - **red-sync-comp-time**—Enter amount of time, in milliseconds, that determines how frequently after synchronization the standby SBC checkpoints with the active SBC. The first interval occurs after initial synchronizations of the systems; this is the timeout for subsequent synchronization requests. The default is **1000**. The valid range is:

     - Minimum—0
     - Maximum—999999999

Setting Multiple Collection Groups

You can configure the SBC to collect multiple groups of statistics. Collection group settings are accessible through the collection configuration. For specific group names, group statistics, and values, see **HDR Groups and Group Statistics**.

The sample-interval, start-time, and end-time parameters that you set for multiple collection groups override the same parameters set for global collection.

Note: For multiple collection groups, the sample-interval value must always be smaller than the global collection parameter value for push-interval.

To set multiple collection groups:

1. Access the **group-settings** configuration element.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# system
ACMEPACKET(system)# system-config
ACMEPACKET(system-config)# collect
ACMEPACKET(collect)#group-settings
ACMEPACKET(group-settings)#
```

2. **group-name**—Enter the group name corresponding to the records that you want to collect; there are 25 possible groups for which the SBC can collect data. The **system** group name is the default for this parameter. For additional group names, see **HDR Groups and Group Statistics**.
3. **sample-interval**—Enter the time in minutes for how often you want the SBC to sample data records for the specified group. The default is **5**. The valid range is:

   - Minimum—1
   - Maximum—120
4. **boot-state**—Set this parameter to **enabled** to start group collection, or to **disabled** to prevent the SBC from collecting HDR statistics for this group. This parameter does not go into effect until the system is rebooted. You can also use the ACLI request collect start command to start collection; using this command, you can start collection for all groups, or for one specified group. The default is **disabled**. Valid values are:

- enabled | disabled

5. **start-time**—Enter the exact date and time (for your local timezone) when you want the SBC to start collecting records for this group. You can enter **now** to set the start-time to the current time, or you can specify a time in the future. If you specify a time, it must be in the format yyyy-mm-dd-hh:mm:ss, where: yyyy is the year, mm is the month, dd is the day, hh in the hour, mm is the minutes, and ss is the second (24-hour clock). The default is **now**.
6. **end-time**—Enter the exact date and time (for your local timezone) when you want the SBC to stop collecting records for this group. You can enter **never** to set the time to never end, or you can specify an end time in the future. If you specify a time, it must be in the format yyyy-mm-dd-hh:mm:ss, where: yyyy is the year, mm is the month, dd is the day, hh in the hour, mm is the minutes, and ss is the second (24-hour clock). The default is **never**.
7. Type **done** to save your configuration.

Setting Servers as Push Receivers

You can configure multiple push receivers that represent FTP or SFTP destination servers for which the SBC pushes records. Push receiver settings are accessible through the collection configuration.

If you configure more than one server, the SBC sends data to all of the servers. If one server fails, the SBC generates an SNMP trap. The SBC makes 3 attempts to send data to the failed server. If the server cannot receive the data, the SBC clears the data for that server. For example, if there are four servers configured, and the SBC successfully pushes data to three of them, the SBC generates a trap indicating the fourth server is down and after 3 attempts to send the data, the data is cleared.

To set servers as push receivers:

1. In Superuser mode, navigate to the collect parameter level in the ACLI.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# system
ACMEPACKET(system)# system-config
ACMEPACKET(system-config)# collect
ACMEPACKET(collect)#
```

2. Access the push receiver (**push-receiver**) parameters.

```
ACMEPACKET(collect)# push-receiver
ACMEPACKET(push-receiver)#
```

- **address**—Enter the IP address of the push receiver (server) to which you want records sent. The default for this parameter is **0.0.0.0**.
- **username**—Enter the username that the SBC uses when it tries to send records to this push server using FTP. There is no default for this parameter.
- **password**—Enter the password (corresponding to the username) that the SBC uses when it sends records to this push server using FTP. There is no default for this parameter. Enter this password parameter using the following procedure:
  - Type the parameter name password, and then press Enter.

    ```
    ACMEPACKET(push-receiver)# password
    ```
  - Enter the password that the SBC uses to send records to the push server. The display does not echo the password you enter.

    ```
    Enter password: [enter the password]
    ```
  - Enter the password again to confirm that you entered the password correctly. If the passwords match, the user prompt displays to continue the push server configuration.

    ```
    Enter password again: [enter the password again]
    ACMEPACKET(push-receiver)#
    ```

    If the passwords do not match, an error message displays. Repeat Steps a through c to set the password.

    ```
    Error:  Password mismatch - aborted.
    ACMEPACKET(push-receiver)#
    ```

- **data-store**—Enter the directory on the push receiver where you want collected data placed. There is no default for this parameter.
- **protocol**—Set this parameter to the protocol with which to send HDR collection record files. Default is **FTP**. Valid values are:
  - FTP | SFTP

Note: Public key authentication is not available when you choose SFTP. Instead, the SBC uses password authentication. However, for SFTP to work, it is still required that you load the SFTP's host public key on the SBC.

Creating a Public Key Profile

The Secure Shell (SSH) and related Secure Shell File Transfer (SFTP) protocols provide for the secure transfer of audit files and for the secure transfer of management traffic across the wancom0 interface. When using password or public key authentication with push receiver configurations, use the procedures described below to create your profiles.

Create your profile by configuring:

- SSH Properties
- Import an SSH Host Key
- Create the public key profile

The following two tasks are required for public key authentication mode only.

- Generate an SSH Key Pair
- Copy the SBC public key to the SFTP server

After the above, you can use this profile within the context of your FTP push configuration.

SSH Operations

SSH Version 2.0, the only version supported on the Oracle SBC, is defined by a series of five RFCs.

- RFC 4250, *The Secure Shell (SSH) Protocol Assigned Numbers*
- RFC 4251, *The Secure Shell (SSH) Protocol Architecture*
- RFC 4252, *The Secure Shell (SSH) Authentication Protocol*
- RFC 4253, *The Secure Shell (SSH) Transport Layer Protocol*
- RFC 4254, *The Secure Shell (SSH) Connection Protocol*

RFCs 4252 and 4253 are most relevant to SBC operations.

The transport layer protocol (RFC 4253) provides algorithm negotiation and key exchange. The key exchange includes server authentication and results in a cryptographically secured connection that provides integrity, confidentiality and optional compression. Forward security is provided through a Diffie-Hellman key agreement. This key agreement results in a shared session key. The rest of the session is encrypted using a symmetric cipher, currently 128-bitAES, Blowfish, 3DES, CAST128, Arcfour, 192-bit AES, or 256-bit AES. The client selects the encryption algorithm to use from those offered by the server. Additionally, session integrity is provided through a crypto-graphic message authentication code (hmac-md5, hmac-sha1, umac-64 or hmac-ripemd160).

The authentication protocol (RFC 4252) uses this secure connection provided and supported by the transport layer. It provides several mechanisms for user authentication. Two modes are supported by the SBC: traditional password authentication and public-key authentication.

ACLI Instructions and Examples

This section provides ACLI procedures for SFTP push configurations, including SSH property configuration, certificate import, and public key profile configuration on your SBC.

Configuring SSH Properties

The single instance **ssh-config** configuration element specifies SSH re-keying thresholds.

1. From admin mode, use the following command path to access the ssh configuration element:

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# security
ACMEPACKET(security)# admin-security
ACMEPACKET(admin-security)# ssh-config
ACMEPACKET(ssh-config)#
```

ssh configuration element properties are shown below with their default values

```
rekey-interval        60
rekey-byte-count      31
```

2. **rekey-interval**—specifies the maximum allowed interval, in minutes, between SSH key negotiations

   Allowable values are integers within the range 60 through 600, with a default of 60 (minutes). Shorter lifetimes provide more secure connections.

   Works in conjunction with **rekey-byte-count**, which sets a packet-based threshold, to trigger an SSH renegotiation. If either trigger is activated, an SSH renegotiation is begun.

   Retain the default value, or specify a new value.

```
ACMEPACKET(ssh-config)# rekey-interval 20
ACMEPACKET(ssh-config)
```

3. **rekey-byte-count**—specifies the maximum allowed send and receive packet count, in powers of 2, between SSH key negotiations

   Allowable values are integers within the range 20 (1,048,576 packets) through 31 (2,147,483,648 packets), with a default of 31 (2^31). Smaller packet counts provide more secure connections.

   Works in conjunction with **rekey-interval**, which sets a time-based threshold, to trigger an SSH renegotiation. If either trigger is activated, an SSH renegotiation is begun.

   Retain the default value, or specify a new value.

```
ACMEPACKET(ssh-config)# rekey-packet-count 24
ACMEPACKET(ssh-config)
```

   A sample SSH configuration appears below:

```
ACMEPACKET(ssh-config)# rekey-interval 20
ACMEPACKET(ssh-config)# done
ACMEPACKET(ssh-config)# exit
ACMEPACKET(admin-security)#
```

   Specifies a key renegotiation every 20 minutes, or at the reception/transmission of 2,147,483,648 packets, whichever comes first.

Import an SSH host Key

Importing a host key requires access to the SFTP server or servers which receive audit log transfers. Access is generally most easily accomplished with a terminal emulation program such as PuTTY, SecureCRT, or TeraTerm.

1. Use a terminal emulation program to access the SSH file system on a configured SFTP server.
2. Copy the server's base64 encoded public file making sure in include the Begin and End markers as specified by RFC 4716, *The Secure Shell (SSH) Public Key File Format*.

   For OpenSSH implementations host files are generally found at /etc/ssh/ssh_host_dsa_key.pub, or /etc/ssh/sss_host_rsa.pub. Other SSH implementations can differ.
3. From admin mode use the ssh-pub-key command to import the host key to the SBC.

   For importing a host key, this command takes the format:

```
ssh-pub-key import known-host <name>
```

where name is an alias or handle assigned to the imported host key, generally the server name or a description of the server function.

```
ACMEPACKET# ssh-pub-key import known-host fedallah

IMPORTANT:
Please paste ssh public key in the format defined in rfc4716.
Terminate the key with ";" to exit.......
```

4. Paste the public key with the bracketing Begin and End markers at the cursor point.
5. Enter a semi-colon (;) to signal the end of the imported host key.
6. Follow directions to save and activate the configuration.

The entire import sequence is shown below.

```
ACMEPACKET# ssh-pub-key import known-host fedallah

IMPORTANT:
    Please paste ssh public key in the format defined in rfc4716.
    Terminate the key with ";" to exit.......

---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, converted from OpenSSH by klee@acme54"
AAAAB3NzaC1yc2EAAAABIwAAAQEA7OBf08jJe7MSMgerjDTgZpbPblrX4n17LQJgPC7clL
cDGEtKSiVt5MjcSav3v6AEN2pYZihOxd2Zzismpoo019kkJ56s/IjGstEzqXMKHKUr9mBV
qvqIEOTqbowEi5sz2AP31GUjQTCKZRF1XOQx8A44vHZCum93/jfNRsnWQ1mhHmaZMmT2LS
hOr4J/Nlp+vpsvpdrolV6Ftz5eiVfgocxrDrjNcVtsAMyLBpDdL6e9XebQzGSS92TPuKP/
yqzLJ2G5NVFhxdw5i+FvdHz1vBdvB505y2QPj/iz1u3TA/3O7tyntBOb7beDyIrg64Azc8
G7E3AGiH49LnBtlQf/aw==
---- END SSH2 PUBLIC KEY ----
;
SSH public key imported successfully....
WARNING: Configuration changed, run "save-config" command to save it
and run "activate-config" to activate the changes
ACMEPACKET# save-config
checking configuration
------------------------------------------------------------------------
...
...
...
------------------------------------------------------------------------
Save-Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
ACMEPACKET# activate-config
Activate-Config received, processing.
waiting for request to finish
SD is not QOS-capable
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
ACMEPACKET#
```

It is important to note that it is often difficult to determine whether the server is using RSA or DSA keys for your application. Unless you can definitively determine this, bear in mind that you need to try importing both.

Create the Public Key Record

The initial step in generating an SSH key pair is to configure a public key record which will serve as a container for the generated key pair.

1. Navigate to the public-key configuration element.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# security
ACMEPACKET(security)# public-key
ACMEPACKET(public-key)#
```

2. Use the name command to provide the object name, and the show command to verify object creation.

```
ACMEPACKET(public-key)# name KeyTest
ACMEPACKET(public-key)# show
public-key
        name                                    KeyTest
        type                                    rsa
        size                                    1024
        last-modified-by
        last-modified-date
```

This command creates a public key record named tashtego.

3. Use the done command to complete object creation.

```
ACMEPACKET(public-key)# done
public-key
        name                                    KeyTest
        type                                    rsa
        size                                    1024
        last-modified-by                        admin@console
        last-modified-date                      2014-05-14 14:40:55

ACMEPACKET(public-key)#
```

4. Make a note of the last-modified-date time value.
5. Move back to admin mode, and save and activate the configuration.

```
ACMEPACKET(public-key)# exit
ACMEPACKET(security)# exit
ACMEPACKET(configure)# exit
ACMEPACKET#

ACMEPACKET# save-config
...
...
...
ACMEPACKET# activate-config
...
...
...
ACMEPACKET#
```

Generate an SSH key pair

1. Now use the ssh-pub-key generate command, in conjunction with the name of the public key record created in Step 3, to generate an SSH key pair.

   For importing an SSH key pair, this command takes the format:

   ```
   ssh-pub-key generate <name>
   ```

   where name is an alias or handle assigned to the generated key pair, generally the client name or a description of the client function.

   ```
   ACMEPACKET# ssh-pub-key generate tashtego
   Please wait...
   public-key 'tashtego' (RFC 4716/SECSH format):
   ---- BEGIN SSH2 PUBLIC KEY ----
   Comment: "1024-bit rsa"
   AAAAB3NzaC1yc2EAAAABIwAAAIEArZEP1/WiYsdGd/Pi8V6pnSwV4cVG4U+jVOwiSwNJCC9Nk82/
   FKYleLZevy9D3lrZ8ytvu+sCYy0fNk4nwvz20c2N
   +r86kDru88JkUqpelJDx1AR718Icpr7ZaAx2L
   ```

```
+e7cpyRSXCgbQR7rXu2H3bp9Jc0VhR2fmkclmrGAIr7Gnc=
---- END SSH2 PUBLIC KEY ----

SSH public-key pair generated successfully....
WARNING: Configuration changed, run "save-config" command to save it and
run "activate-config" to activate the changes
ACMEPACKET#
```

2. Copy the base64-encoded public key. Copy only the actual public key — do not copy the bracketing Begin and End markers nor any comments. Shortly you will paste the public key to one or more SFTP servers.
3. Save and activate the configuration.

```
ACMEPACKET# save-config
...
...
...
ACMEPACKET# activate-config
...
...
...
```

4. Return to the public-key configuration object, and select the target public key record instance.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# security
ACMEPACKET(security)# public-key
ACMEPACKET(public-key)# sel
<name>:
1: acme01
2: acme02
3: tashtego

selection: 3
ACMEPACKET(public-key)# show
public-key
        name                tashtego
        type                rsa
        size                1024
        last-modified-by    admin@console
        last-modified-date  2009-03-06 11:24:32
ACMEPACKET(public-key)#
```

5. Verify that the record has been updated to reflect key generation by examining the value of the last-modified-date field.

Copy a client public key to an SFTP server.

Copying the client public key to an SFTP server requires server access generally using a terminal emulation program such as PuTTY, SecureCRT, or TeraTerm.

1. Use a terminal emulation program to access the SSH file system on a configured SFTP server.
2. Copy the client key to the SFTP server.

   On OpenSSH implementations, public keys are usually stored in the ~/.ssh/authorized_keys file. Each line this file (1) is empty, (2) starts with a pound (#) character (indicating a comment), or (3) contains a single public key.

   Refer to the sshd man pages for additional information regarding file format.

   Use a text editor such as vi or emacs to open the file and paste the public key to the tail of the authorized_keys file.

   For SSH implementations other than OpenSSH, consult the system administrator for file structure details.

View a Public key on the SBC

You can use the show security ssh-pub-key command to display information about SSH keys imported to the SBC with the ssh-pub-key command; you cannot display information about keys generated by the ssh-pub-key command.

```
ACMEPACKET# show security ssh-pub-key brief
login-name:
    acme74
finger-print:
    51:2f:f1:dd:79:9e:64:85:6f:22:3d:fe:99:1f:c8:21
finger-print-raw:
    0a:ba:d8:ef:bb:b4:41:d0:dd:42:b0:6f:6b:50:97:31

login-name:
    fedallah
finger-print:
    c4:a0:eb:79:5b:19:01:f1:9c:50:b3:6a:6a:7c:63:d5
finger-print-raw:
    ac:27:58:14:a9:7e:83:fd:61:c0:5c:c8:ef:78:e0:9c
ACMEPACKET#
```

This command displays summary information for all SSH imported keys.

- login-name: contains the name assigned to the RSA or DSA public key when it was first imported.
- finger-print: contains the output of an MD5 hash computed across the base64-encoded public key.
- finger-print-raw: contains the output of an MD5 hash computed across the binary form of the public key

```
ACMEPACKET# show security ssh-pub-key brief fedallah
login-name:
    fedallah
finger-print:
    c4:a0:eb:79:5b:19:01:f1:9c:50:b3:6a:6a:7c:63:d5
finger-print-raw:
    ac:27:58:14:a9:7e:83:fd:61:c0:5c:c8:ef:78:e0:9c
ACMEPACKET#
```

This command displays summary information for a specific SSH public key (in this case fedallah).

```
ACMEPACKET# show security ssh-pub-key detail fedallah
host-name:
    fedallah
comment:
    "2048-bit RSA, converted from OpenSSH by klee@acme54"
finger-print:
    c4:a0:eb:79:5b:19:01:f1:9c:50:b3:6a:6a:7c:63:d5
finger-print-raw:
    ac:27:58:14:a9:7e:83:fd:61:c0:5c:c8:ef:78:e0:9c
pub-key:

AAAAB3NzaC1yc2EAAAABIwAAAQEA7OBf08jJe7MSMgerjDTgZpbPblrX4n17LQJgPC7clLcDGEtKSi
Vt5MjcSav3v6AEN2pYZihOxd2Zzismpoo019kkJ56s/
IjGstEzqXMKHKUr9mBVqvqIEOTqbowEi5sz2AP31GUjQTCKZRF1XOQx8A44vHZCum93/
jfNRsnWQ1mhHmaZMmT2LShOr4J/Nlp
+vpsvpdrolV6Ftz5eiVfgocxrDrjNcVtsAMyLBpDdL6e9XebQzGSS92TPuKP/yqzLJ2G5NVFhxdw5i
+FvdHz1vBdvB505y2QPj/iz1u3TA/3O7tyntBOb7beDyIrg64Azc8G7E3AGiH49LnBtlQf/aw==

modulus: (256)
ECE05FD3C8C97BB3123207AB8C34E06696CF6E5AD7E27D7B2D02603C2EDC94B703184B4A4A256D
E4C8DC49ABF7BFA004376A5866284EC5DD99CE2B26A68A34D7D924279EACFC88C6B2D133A9730A
1CA52BF66055AAFA8810E4EA6E8C048B9B33D803F7D4652341308A6511755CE431F00E38BC7642
BA6F77FE37CD46C9D64359A11E66993264F62D284EAF827F365A7EBE9B2FA5DAE8955E85B73E5E
8957E0A1CC6B0EB8CD715B6C00CC8B0690DD2FA7BD5DE6D0CC6492F764CFB8A3FFCAACCB2761B9
355161C5DC398BE16F747CF5BC176F079D39CB640F8FF8B3D6EDD303FDCEEEDCA7B4139BEDB783
C88AE0EB803373C1BB137006887E3D2E706D9507FF6B
exponent: (1)
```

```
23
ACMEPACKET#
```

This command displays detailed information for specific SSH public key (in this case fedallah, an RSA key).

- host-name: contains the name assigned to the RSA key when it was first imported
- finger-print: contains the output of an MD5 hash computed across the base64-encoded RSA public key
- finger-print-raw: contains the output of an MD5 hash computed across the binary form of the RSA public key
- public key: contains the base64-encoded RSA key
- modulus: contains the hexadecimal modulus (256) of the RSA key
- exponent: (also known as public exponent or encryption exponent) contains an integer value that is used during the RSA key generation algorithm. Commonly used values are 17 and 65537. A prime exponent greater than 2 is generally used for more efficient key generation.

```
ACMEPACKET# show security ssh-pub-key detail acme74
host-name:
    acme74
comment:
    DSA Public Key
finger-print:
    51:2f:f1:dd:79:9e:64:85:6f:22:3d:fe:99:1f:c8:21
finger-print-raw:
    0a:ba:d8:ef:bb:b4:41:d0:dd:42:b0:6f:6b:50:97:31
pub-key:

AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbETW6ToHv8D1U
J/z+zHo9Fiko5XybZnDIaBDHtblQ
+Yp7StxyltHnXF1YLfKD1G4T6JYrdHYI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yi
sk/gF
+1VAAAAFQDb8D5cvwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdt
W9vGfJ0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/
FAAvioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACBAN7CY
+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO
+JsvphVMBJc9HSn24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7
dLM5sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV

p: (128)
F63C64E1D8DB2152240E97602F47470347C5A7A1BF1E70389D2BCD9773A12397C5B1135BA4E81E
FF03D5427FCFECC7A3D162928E57C9B6670C86810C7B5B950F98A7B4ADC7296D1E75C5D582DF28
3D46E13E8962B747608D783A6D5E83D7B836709195E6AAA193C5DD419F6626BA6D7AC64D07F780
9AB67BB622B24FE017ED55

q: (20)
DBF03E5CBF01D64D90CF7D7D03DACF5177B341BD

g: (128)
94DF76F816FB0F828B624DC8C116D76E5C177643E0800E297DDB56F6F19F274FD11DDF8D8C1E1E
A350FED1D8B1EAD5F060637B3CA4B947F1573CDC311CF6A9723F6E2F5267D80590D9DB249DFFA2
FC5000BE2A143E499D31CD33B96A12384B12361543B57DD676F55C19C06AF5C7ADCEBB4E2963A8
709989F34A9A7714D11ED5

pub_key: (128)
DEC263E28ABF5807A51CC5C1D426EC72BD6DBD4B028D8AC1AA179DA74581EA6D34141E4971B5BC
EF89B2FA6154C04973D1D29F6E1562D62DB0CBBBE2A5EF8988F3895B9C58A8E32846F5D63BAA9C
5D060E50775559B11CB9B19C0CFAE3758AE3667B74B339B18DBDA2E7B3BF85F3D8FB8C721E5518
F3FE083AB308CE25A16815
ACMEPACKET#
```

This command displays detailed information for specific SSH public key (in this case acme74, a DSA key).

- host name: contains the name assigned to the DSA public key when it was first imported
- comment: contains any comments associated with the DSA key
- finger-print: contains the output of an MD5 hash computed across the base64-encoded DSA public key

- finger-print-raw: contains the output of an MD5 hash computed across the binary form of the DSA public key
- public key: contains the base64 encoded DSA key
- p: contains the first of two prime numbers used for key generation
- q: contains the second of two prime numbers used for key generation
- g: contains an integer that together with p and q are the inputs to the DSA key generation algorithm

```
ACMEPACKET# show security ssh-pub-key detail
...
...
...
ACMEPACKET#
```

This command displays detailed information for all SSH imported keys.

Starting and Stopping HDR using the ACLI

For ease-of-use, you can start and stop record collection from Acme Packet's command line interface (ACLI) in Superuser Mode. You can start and stop record collection for the entire HDR process, or you can specify a group name for which you want to start and stop collection.

Starting HDR

To start record collections:

- In Superuser mode, at the root prompt, enter **request collect start all** and press **Enter**. The SBC starts all record collection.

  ```
  ACMEPACKET# request collect start all
  ```

To start a group-name record collection:

- In Superuser mode, at the root prompt, enter **request collect start <group-name>**, and press **Enter**. The SBC starts collection for that group name only. In the following example, voltage record collection is started.

  ```
  ACMEPACKET# request collect start voltage
  ```

Stopping HDR

To stop all record collections:

- In Superuser mode, at the root prompt, enter **request collect stop all** and press **Enter**. The SBC stops all record collection.

  ```
  ACMEPACKET# request collect stop all
  ```

To stop a group-name record collection:

- In Superuser mode, at the root prompt, enter **request collect stop <group-name>**, and press **Enter**. The SBC stops collection for that group name only. In the following example, voltage record collection is stopped.

  ```
  ACMEPACKET# request collect stop voltage
  ```

Purging HDR Data using the ACLI

Using the ACLI, you can delete all HDR record collections resident on the SBC.

To purge all record collections:

- In Superuser mode, at the root prompt, enter **request collect purge** and press **Enter**. The SBC deletes all record collections.

  ```
  ACMEPACKET# request collect purge
  ```

Restarting HDR using the ACLI

You can restart the collector using the boot configuration.

To restart the collector using the boot configuration:

- In Superuser mode, at the root prompt, enter **request collect restart** and press **Enter**. The SBC restarts all record collections using the boot configuration.

```
ACMEPACKET# request collect restart
```

Requesting HDR Collection Status

You can display the status of collection groups and push servers on the SBC, when required, using the ACLI.

To display the status of collection groups and push servers:

- In Superuser mode, at the root prompt, enter **request collect status** and press **Enter**. The SBC displays the current status of all record collections and push receivers. In the following example, the group, fan is disabled at boot time, the start time is immediately when the system comes up, and there is no end time. The Push Receiver configured for this SBC is 172.30.11.16 and it is currently reachable. The date and time of the next scheduled push is also indicated as well as the interval of time between each push.

```
ACMEPACKET# request collect status
Collector is currently collecting on:
Group    Boot-State    Start Time    End Time
fan     disabled    now    never
Next Push Scheduled for: 2008-01-11-11:12:06
Subsequent Push Interval: 15 minutes
Registered push receivers are:
IP Address    Status
172.30.11.16    reachable
```

3

HDR Groups and Group Statistics

This section provides information about the Historical Data Recording (HDR) Groups and Group Statistics that make up the HDR records on the C-Series products. It also includes information about the source of the HDR data.

HDR Data

HDR data consists of a "Group" with associated Group Statistics that apply to each group. HDR data comes from two sources:

- Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) (MIB-Associated Groups and Group Statistics)
- Acme Packet's Command Line Interface (ACLI) (ACLI-Associated Groups and Group Statistics)

When you configure HDR on the SBC, the Groups and associated Group Statistics are included in the collection of data. You can configure the SBC to collect all group statistics or specific group statistics. For information on configuring global collection, see Setting Global Collection. For information on specific group collections, see Setting Multiple Collection Groups.

When HDR is enabled, the SBC forwards statistical records to push servers which send the data (in standard format) to a receiving server for viewing in a comma-separated value (CSV) file. Before pushing a file, the collector creates the directory by group name for which the statistic belongs (for example, fan, sip-client, system, etc.), if the directory does not exist from a previous push.

The collector can push multiple CSV files per directory. Each file is formatted as <Unix timestamp>.csv (for example, 1302041977.csv). Within the file, each record also has an associated record timestamp. The **filename timestamp** is the time that the CSV file was create. The **record timestamp** is the window of time that the HDR collector used to collect the data. For more information on windows of time, see Windows of Time.

The first record of each file is a header containing the attribute name. For example, in the "System" directory, a file name of 13020441977.csv can contain the header attribute names of CPU Utilization, Memory Utilization, Health Score, Redundancy State, etc. The collector appends a Timestamp heading attribute to the beginning of every record as well.

Note: The records in a CSV file may display differently, depending on the record data included in the file, and the method used to open the file. For more information about the display of record data in a CSV file, see Appendix A, CSV File Data Formats.

The following example shows the output from a "System" HDR collection. The output format reflects that the file was opened using the Unix command cat <timestamp>.csv.

```
[AcmePacket]$ cd system
[AcmePacket]$ ls -l

-rw-r--r-- 1 moles src 453 Apr 15 05:38 1302041737.csv
-rw-r--r-- 1 moles src 453 Apr 15 05:40 1302041857.csv
-rw-r--r-- 1 moles src 455 Apr 15 05:42 1302041977.csv

[AcmePacket]$ cat 1302041977.csv
TimeStamp,CPU Utilization,Memory Utilization,Health
Score,Redundancy State,Signaling Sessions,
Signaling Rate (CPS),CAM Utilization (NAT),
Cam Utilization (ARP),I2C Bus State,License Capacity,
Current Cached SIP Local Contact Registrations,
Current MGCP Public Endpoint Gateway Registrations,
Current H323 Number of Registrations,
Application Load Rate

1302041977,39,22,50,active,0,0,0,0,online,0,0,0,0,39
1302042037,100,22,50,active,0,0,0,0,online,0,0,0,0,100
```

Windows of Time

Each table in this chapter identifies a data type for a Group Statistic: counter, gauge, config, timeticks, and period.

Note: For more information about Group Statistic data types, see What is HDR?.

A period type represents a value determined as the sum of a number of events which occurred during a specified window of time (or a time period). There are three possible windows in which events can occur:

- current window
- previous window
- sliding window

The **current window** is the window during which events are currently being accumulated. The current window ends D seconds after the start of the current window, where D is the duration of the window. The current window is always of size Dc < D. Once the current window becomes of size D, it becomes the previous window, and a new current window is started.

The **previous window** is the time period of duration D which ended at the start of the current window.

The **sliding window** marks the period of time for the previous window, D, plus the time passed in the current window. For example: For the "session-agent" and "session-realm" HDR groups, the default timer value is 30 seconds. The "current window" is between 0 and 30 seconds. When the current window reaches 30 seconds it becomes the previous window and a new current window is initialized. The "sliding window" is the sum of the current window and previous window. Therefore the initial sliding window is between 0 and 30 seconds and after that the sliding window is between 30 and 60 seconds.

For the session-agent statistics and the session-realm statistics groups, the default period timer is 30 seconds. In the SBC configuration, if the sustained-rate-window parameter is not configured, the default window size is 30 seconds. If the sustained-rate-window parameter is configured, the default period is set to the configured value of the sustained-rate-window.

MIB-Associated Groups and Group Statistics

The Groups and Group Statistics in this section are a subset of MIB variables on the SBC. Each table specifies the MIB that pertains to the Group or Group Statistics. Groups in this section include:

- Group: system
- Group: interface

- Group: session-agent *
- Group: session-realm
- Group: voltage
- Group: fan
- Group: temperature
- Group: space
- Group: network-util

*In addition to being a subset of a MIB variable, the session-agent Group maps to the **show sipd agents** command, the registration-realm Group maps to the **show sipd realms**, and some statistics in the session-realm Group map to the **show sipd realms** command. For more information, see **show sipd agents** and **show sipd realms** in Chapter 4.

system

Group name that consists of general system statistics.

SNMP MIB
ap-smgmt.mib
apSysMgmtGeneralObjects
1.3.6.1.4.1.9148.3.2.1.1

Position	Statistic	Type	Timer Value	Range	OID	Description
1	CPU Utilization	gauge	N/A	0% to 100%	1.3.6.1.4.1.9148.3.2.1.1.1	Percentage of total usage of SBC's central processing unit (CPU).
2	Memory Utilization	gauge	N/A	0% to 100%	1.3.6.1.4.1.9148.3.2.1.1.2	Percentage of total memory usage on SBC
3	Health Score	gauge	N/A	0% to 100%	1.3.6.1.4.1.9148.3.2.1.1.3	Percentage of system health with a value of 100% being the healthiest.
4	Redundancy State	integer	N/A	active (1) System is in active mode. standby (2) System is in standby mode. unassigned (3) System has not been assigned as active or standby. recovery (4) System is in recovery mode. outOfService (5) System is currently out of service.	1.3.6.1.4.1.9148.3.2.1.1.4	For high availability (HA), specifies whether this SBC is active or standby. A standalone system has an active state.

Position	Statistic	Type	Timer Value	Range	OID	Description
				Contact your Technical Support representative.		
5	Signaling Sessions	gauge	N/A	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.1.5	Total number of global, concurrent, active sessions in real time.
6	Signaling Rate (CPS)	gauge	N/A	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.1.6	Total number of calls per second (CPS). This is a real-time value which is the sum of SIP H.323 and Media Gateway Control Protocol (MGCP) calls.
7	CAM Utilization (NAT)	gauge	N/A	0% to 100%	1.3.6.1.4.1.9148.3.2.1.1.7	Percentage of Content Addressable Memory (CAM) usage for Network Address Translation (NAT).
8	CAM Utilization (ARP)	gauge	N/A	0% to 100%	1.3.6.1.4.1.9148.3.2.1.1.8	Percentage of Content Addressable Memory (CAM) usage for Address Resolution Protocol (ARP).
9	I2C Bus State	integer	N/A	online (0) SBC is online and processing calls. becomingoffline (1) SBC is in the process of going offline. offline (2) SBC is offline and not processing calls. However, other administrative functions are available.	1.3.6.1.4.1.9148.3.2.1.1.9	Current SBC state.
10	License Capacity	gauge	N/A	0% to 100%	1.3.6.1.4.1.9148.3.2.1.1.10	Percentage of licensed SBC

Position	Statistic	Type	Timer Value	Range	OID	Description
						sessions currently in progress.
11	Current Cached SIP Local Contact Registrations	gauge	N/A	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.1.11	Total number of currently cached registered contacts in the SBC.
12	Current MGCP Public Endpoint Gateway Registrations	gauge	N/A	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.1.12	Total number of registered Media Gateway Control Protocol (MGCP) gateway endpoints in the SBC.
13	Current H323 Number of Registrations	gauge	N/A	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.1.13	Total number of H323 registrations in the SBC.
14	Application Load Rate	period	30 seconds	0% to 100%	1.3.6.1.4.1.9148.3.2.1.1.16	Average Central Processing Unit (CPU) utilization of the SBC during the current window. The average is computed every 10 seconds unless load-limit is configured in the SipConfig record, in which case it is 5 seconds.
15	Current Deny Entries Allocated	integer	N/A	0 to 4294967295	.1.3.6.1.4.1.9148.3.2.1.1.26	The total number of endpoints currently denied.

interface

Consists of statistics pertaining to the physical interface(s) on the SBC.

Position	Statistic	Type	Timer Value	Range	OID	Description
1	Index	config	N/A	N/A	1.3.6.1.2.1.2.2.1.1	Unique value that identifies the interface.
2	Description	config	N/A	N/A	1.3.6.1.2.1.2.2.1.2	String that provides a description of the interface.

Position	Statistic	Type	Timer Value	Range	OID	Description
3	Type	config	N/A	N/A	1.3.6.1.2.1.2.2.1.3	Type of interface distinguished according to the Physical/Link Protocol(s).
4	MTU	config	N/A	N/A	1.3.6.1.2.1.2.2.1.4	Maximum Transmission Unit (MTU) - largest datagram size, in octets (eight-bit bytes), that can be sent/received on the interface specified in octets.
5	Speed	config	N/A	N/A	1.3.6.1.2.1.2.2.1.5	Estimate of the current bandwidth, in bits per second, on the interface.
6	Physical Address	config	N/A	N/A	1.3.6.1.2.1.2.2.1.6	IP Address of the interface at the protocol layer immediately below the network layer in the protocol stack.
7	Admin Status	config	N/A	N/A	1.3.6.1.2.1.2.2.1.7	Current administrative state of the interface.
8	Operational State	integer	N/A	up(1) Interface is operational and in the UP state. down(2) Interface is not operational and in the DOWN state. testing(3) Interface is in TESTING state. unknown(4) Interface state is UNKNOWN. dormant(5) Interface is inactive and in DORMANT state. notPresent(6) No interface is present. lowerLayerDown(7) Lower layer protocol	1.3.6.1.2.1.2.2.1.8	Current operational state of the interface.

Position	Statistic	Type	Timer Value	Range	OID	Description
				on the interface is down.		
9	IfLastChange	timeticks	N/A	0 to 4294967295	1.3.6.1.2.1.2.2.1.9	Specifies the sysUpTime (system up time) value with the time the interface entered its current operational state
10	InOctets	counter	N/A	0 to 4294967295	1.3.6.1.2.1.2.2.1.10	Total number of octets received on the interface.
11	InUnicastPackets	counter	N/A	0 to 4294967295	1.3.6.1.2.1.2.2.1.11	Number of subnetwork-unicast packets delivered to a higher layer protocol. A unicast packet is a regular IP packet that has a destination IP address.
12	InNon-UnicastPackets	counter	N/A	0 to 4294967295	1.3.6.1.2.1.2.2.1.12	Number of non-unicast packets (i.e., subnetwork-broadcast or subnetwork-multicast packets) delivered to a higher layer protocol.
13	InDiscards	counter	N/A	0 to 4294967295	1.3.6.1.2.1.2.2.1.13	Number of inbound packets that were discarded even though no errors had been detected. This prevented the packets from being delivered to a higher-layer protocol.
14	InErrors	counter	N/A	0 to 4294967295	1.3.6.1.2.1.2.2.1.14	Number of inbound packets that contained errors, preventing them from being delivered to a

Position	Statistic	Type	Timer Value	Range	OID	Description
						higher-layer protocol.
15	OutOctets	counter	N/A	0 to 4294967295	1.3.6.1.2.1.2.2.1.16	Total number of octets sent out the interface.
16	OutUnicastPackets	counter	N/A	0 to 4294967295	1.3.6.1.2.1.2.2.1.17	Total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including packets that were discarded or not sent.
17	OutNon-UnicastPackets	counter	N/A	0 to 4294967295	1.3.6.1.2.1.2.2.1.18	Total number of packets that higher-level protocols requested be transmitted to a non-unicast address (i.e., subnetwork-broadcast or subnetwork-multicast addresses), including packets that were discarded or not sent.
18	OutDiscards	counter	N/A	0 to 4294967295	1.3.6.1.2.1.2.2.1.19	Number of outbound packets discarded even though no errors were detected, to prevent the packets from being transmitted.
19	OutErrors	counter	N/A	0 to 4294967295	1.3.6.1.2.1.2.2.1.20	Number of outbound packets that were not transmitted because of errors.

session-agent

A signaling endpoint that applies traffic-shaping attributes and information regarding next hops or previous hops.

SNMP MIB
ap-smgmt.mib
apCombinedSessionAgentStatsEntry
1.3.6.1.4.1.9148.3.2.1.2.1.1

Position	Statistic	Type	Timer Value	Range	OID	Description
1	Hostname	config	N/A	N/A	1.3.6.1.4.1.9148.3.2.1.2.1.1.2	Hostname of the session agent, in Fully Qualified Domain Name (FQDN) or IP Address format, for which the group statistics are being calculated.
2	System Type	config	N/A	N/A	1.3.6.1.4.1.9148.3.2.1.2.1.1.3	Type of the specified session agent – either SIP or H323.
3	Status	integer	N/A	disabled Session agent is disabled. outofService Session agent is out of service. standby Session agent in standby mode. inService Session agent is in service. constraintsViolation Session agent has a signaling & bandwidth constraints violation. inServiceTimedOut Session agent that is currently in Service has timed out because of inactivity.	1.3.6.1.4.1.9148.3.2.1.2.1.1.22	Current state of the specified session agent.
4	Inbound Active Sessions	gauge	N/A	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.4	Total number of current, active, inbound sessions.
5	Inbound Session Rate	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.5	Current inbound session rate in calls per second (CPS) during the

Position	Statistic	Type	Timer Value	Range	OID	Description
						sliding window period.
6	Outbound Active Sessions	gauge	N/A	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.6	Total number of current, active, outbound sessions.
7	Outbound Session Rate	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.7	Current outbound session rate in calls per second (CPS) during the sliding window period.
8	Inbound Sessions Admitted	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.8	Total number of inbound sessions admitted during the sliding window period.
9	Inbound Sessions Not Admitted	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.9	Total number of inbound sessions rejected because of insufficient bandwidth during the sliding window period.
10	Inbound Concurrent Sessions High	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.10	Highest number of concurrent inbound sessions during the sliding window period.
11	Inbound Average Session Rate	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.11	Average rate of inbound sessions during the sliding window period in calls per second (CPS).
12	Outbound Sessions Admitted	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.12	Total number of outbound sessions admitted during the sliding window period.
13	Outbound Sessions Not Admitted	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.13	Total number of outbound sessions rejected due to insufficient bandwidth during the sliding window period.
14	Outbound Concurrent	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.14	Highest number of concurrent

Position	Statistic	Type	Timer Value	Range	OID	Description
	Sessions High					outbound sessions during the sliding window period.
15	Outbound Average Sessions Rate	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.15	Average rate of outbound sessions during the sliding window period in calls per second (CPS).
16	Max Burst Rate	period	10	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.16	Burst rate of traffic (both inbound and outbound) measured during the current window period. The time period is equal to the value of the configuration parameter burst-rate-window in the session constraint or session-agent configuration record. It is equal to 1 if not configured. Its value is the number of active calls plus 1 divided by the time period. This is different from the Max Burst Rate value in the ACLI command "show sipd agent. In the ACLI it is the high-water mark during the window period.
17	Total Seizures	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.17	Total number of seizures during the sliding window period.
18	Total Answered Sessions	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.18	Total number of answered sessions during the sliding window period.

Position	Statistic	Type	Timer Value	Range	OID	Description
19	Answer/ Seizure Ratio	period	30	0% to 100%	1.3.6.1.4.1.9148.3.2.1.2.1.1.19	Answer-to-seizure ratio expressed as a percentage during the sliding window period. For example, a value of 90 would represent 90% or . 90.
20	Average One-Way Signaling Latency	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.20	Average observed one-way signaling latency during the current window period. This is the average amount of time the signaling travels in one direction. Each latency measurement used to calculate this average begins with a request and ends with its first response. Subsequent responses do not affect this measurement. For example, if a 100 Trying arrives as the first response to an INVITE, the system uses that latency for this purpose. Requests that trigger these measurements include every request that receives a response.
21	Maximum One-Way Signaling Latency	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.1.1.21	Maximum observed one-way signaling latency during the sliding window period. This is the maximum amount of time the signaling travels in one direction.

Position	Statistic	Type	Timer Value	Range	OID	Description
						Each latency measurement used to calculate this average begins with a request and ends with its first response. Subsequent responses do not affect this measurement. For example, if a 100 Trying arrives as the first response to an INVITE, the system uses that latency for this purpose. Requests that trigger these measurements include every request that receives a response.

session-realm

A collection of Web security servers in a single Domain Name System (DNS) that are configured to share sessions. The statistic tables in this section identify the statistics that display in the “show sipd realms” output. Not all statistics are applicable to this show command.

SNMP MIB
ap-smgmt.mib
apSigRealmStatsEntry
1.3.6.1.4.1.9148.3.2.1.2.4.1

Position	Statistic	Type	Timer Value	Range	OID	Description
1	Realm Name	config	N/A	N/A	1.3.6.1.4.1.9148.3.2.1.2.4.1.2	Name of the realm for which the group statistics are being calculated.
2	Inbound Active Sessions	gauge	N/A	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.3	Total number of current, active, inbound sessions.
3	Inbound Session Rate	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.4	Current inbound session rate in calls per second (CPS)

Position	Statistic	Type	Timer Value	Range	OID	Description
						during the sliding window period.
4	Outbound Active Sessions	gauge	N/A	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.5	Total number of current, active, outbound sessions.
5	Outbound Session Rate	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.6	Current outbound session rate in calls per second (CPS) during the sliding window period.
6	Inbound Sessions Admitted	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.7	Total number of inbound sessions during the sliding window period.
7	Inbound Sessions Not Admitted	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.8	Total number of inbound sessions rejected because of insufficient bandwidth during the sliding window period.
8	Inbound Concurrent Sessions High	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.9	Highest number of concurrent inbound sessions during the sliding window period.
9	Inbound Average Session Rate	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.10	Average rate of inbound sessions during the sliding window period in calls per second (CPS).
10	Outbound Sessions Admitted	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.11	Total number of outbound sessions admitted during the sliding window period.
11	Outbound Sessions Not Admitted	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.12	Total number of outbound sessions rejected due to insufficient bandwidth during the sliding window period.
12	Outbound Concurrent Sessions High	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.13	Highest number of concurrent outbound sessions during the

Position	Statistic	Type	Timer Value	Range	OID	Description
						sliding window period.
13	Outbound Average Sessions Rate	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.14	Average rate of outbound sessions during the sliding window period in calls per second (CPS).
14	Max Burst Rate	period	Equal to the burst-rate - window parameter in the Session Agent configuration record. If this value is less than 10, the timer value is set to 10.	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.15	Burst rate of traffic (both inbound and outbound) measured during the current window period. The time period is equal to the value of the configuration parameter burst-rate-window in the session constraint or session-agent configuration record. It is equal to 1 if not configured. Its value is the number of active calls plus 1 divided by the time period. This is different from the Max Burst Rate value in the ACLI command "show sipd agent. In the ACLI it is the high-water mark during the window period.
15	Total Seizures	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.16	Total number of seizures during the sliding window period.
16	Total Answered Sessions	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.17	Total number of answered sessions during the sliding window period.
17	Answer/Seizure Ratio	period	30	0% to 100%	1.3.6.1.4.1.9148.3.2.1.2.4.1.18	Answer-to-seizure ratio expressed as a percentage during the sliding window period. For example, a value of 90 would

Position	Statistic	Type	Timer Value	Range	OID	Description
						represent 90% or . 90.
18	Average One-Way Signaling Latency	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.19	Average observed one-way signaling latency during the current window period. This is the average amount of time the signaling travels in one direction.
19	Maximum One-Way Signaling Latency	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.20	Maximum observed one-way signaling latency during the sliding window period. This is the maximum amount of time the signaling travels in one direction.
20	Average QoS RFactor	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.24	Average Quality of Service (QoS) factor observed during the current window period. Quality of service shapes traffic to provide different priority and level of performance to different data flows. R-factors are metrics in VoIP, that use a formula to take into account both user perceptions and the cumulative effect of equipment impairments to arrive at a numeric expression of voice quality. This statistic defines the call or transmission quality expressed as an R factor.
21	Maximum QoS RFactor	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.25	Maximum Quality of Service (QoS) factor observed during the sliding window period. Quality of service

Position	Statistic	Type	Timer Value	Range	OID	Description
						shapes traffic to provide different priority and level of performance to different data flows. R-factors are metrics in VoIP that use a formula to determine a numeric expression of voice quality. This statistic defines the call or transmission quality expressed as an R factor.
22	Current QoS Major Exceeded	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.26	Peg counts of the number of times the major Rfactor threshold was exceeded during the sliding window period. The peg count provides counts of calls with different service classes that occur during intervals of frequency which reliability indicate the traffic load. R-factors are metrics in VoIP that use a formula to determine a numeric expression of voice quality.
23	Total QoS Major Exceeded	counter	N/A	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.27	Count of the number of times the major Rfactor threshold was exceeded. Provides counts of calls with different service classes that occur during intervals of frequency which reliability indicate the traffic load. R-factors are metrics in VoIP that use a formula to determine a numeric

Position	Statistic	Type	Timer Value	Range	OID	Description
						expression of voice quality.
24	Current QoS Critical Exceeded	period	30	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.28	Count of the number of times the critical Rfactor threshold was exceeded during the sliding window period. Provides counts of calls with different service classes that occur during intervals of frequency which reliability indicate the traffic load. R-factors are metrics in VoIP that use a formula to determine a numeric expression of voice quality.
25	Total QoS Critical Exceeded	counter	N/A	0 to 4294967295	1.3.6.1.4.1.9148.3.2.1.2.4.1.29	Count of the number of times the critical Rfactor threshold was exceeded. Provides counts of calls with different service classes that occur during intervals of frequency which reliability indicate the traffic load. R-factors are metrics in VoIP that use a formula to determine a numeric expression of voice quality.
26	Early Sessions	counter	N/A	0 to 4294967295	N/A	Indicates the number of early sessions for each realm. Each time the SBC receives an INVITE on the ingress realm or the egress realm sends an INVITE request, a counter increments if the session is established with a

Position	Statistic	Type	Timer Value	Range	OID	Description
						200 OK response. This counter also increments in sessions when there are no 18x responses (Ringing (180), Call is Being Forwarded (181), Queued (182), Session in Progress (183)), but a 200 OK is established. This counter represents the number of sessions that have reached the early dialog state or later.
27	Successful Sessions	counter	N/A	0 to 4294967295	N/A	Indicates the number of successful sessions for each realm. Successful sessions are when the SBC receives a successful 200 OK response from an initial INVITE request. **Note:** This counter is NOT incremented for re-INVITES.
28	Active Subscriptions	counter	N/A	0 to 4294967295	N/A	Current domain count of active SIP subscriptions.
29	SubscriptionsPerMax	counter	N/A	0 to 4294967295	N/A	Maximum domain count of SIP subscriptions initiated during any 100 second period since the last SBC re-boot.
30	Subscriptions High	counter	N/A	0 to 4294967295	N/A	Maximum domain count of active SIP subscriptions since the last SBC re-boot.
31	Total Subscriptions	counter	N/A	N/A	1.3.6.1.4.1.9148.3.2.1.2.4.1.35	Count of lifetime total subscriptions for the SBC.

Position	Statistic	Type	Timer Value	Range	OID	Description
32	Active Local Contacts	counter	N/A	N/A	1.3.6.1.4.1.9148.3.2.1.2.4.1.31	Current Domain count of active SIP registrations

voltage

Current operating voltages for components in the SBC.

SNMP MIB
ap-env-monitor.mib
apEnvMonVoltageStatusEntry
1.2.6.1.4.1.9148.3.3.1.2.1.1

Position	Statistic	Type	Timer Value	Range	OID	Description
1	Type	string	N/A	v2p5 Uses a 2.5V power supply v3p3 Uses a 3.3V power supply v5 Uses a 5V power supply vdd Uses a positive supply of voltage cpu Uses the computer processing unit (CPU) power supply	N/A	Type of power supply currently used on the SBC hardware.
2	Description	string	N/A	2.5V voltage 2.5V power supply 3.3V voltage 3.3V power supply 5V voltage 5V power supply VDD voltage Positive voltage power supply CPU voltage Computer processing unit (CPU) power supply	N/A	Textual description of the voltage currently used on the power supply in the SBC.
3	Voltage (millivolts)	gauge	N/A	0 to 4294967295	1.2.6.1.4.1.9148.3.3.1.2.1.1.4	Current measurement of voltage, in millivolts (if available).

fan

Environmental fan statistics

SNMP MIB
ap-env-monitor.mib
apEnvMonFanStatusEntry
1.3.6.1.4.1.9148.3.3.1.4.1.1

Position	Statistic	Type	Timer Value	Range	OID	Description
1	Location	string	N/A	left Located on the left of the circuit board. middle Located in the middle of the circuit board. right Located on the right of the circuit board.	N/A	Physical location of the cooling fan on the circuit board in the SBC.
2	Description	string	N/A	Fan 1 speed Slow speed fan Fan 2 speed Medium speed fan Fan 3 speed Fast speed fan	N/A	Textual description that specifies the speed of the cooling fan currently installed in the SBC.
3	Speed	gauge	N/A	0% to 100%	1.3.6.1.4.1.9148.3.3.1.4.1.1.4	Current measurement of the fan speed expressed as a percentage.

temperature

Environmental temperature statistics

SNMP MIB
ap-env-monitor.mib
apEnvMonTemperatureStatusEntry
1.3.6.1.4.1.9148.3.3.1.3.1.1

Position	Statistic	Type	Timer Value	Range	OID	Description
1	Type	string	N/A	ds 1624s Main Main board on the SBC ds 1624s CPU Central processing unit (CPU)	N/A	Indicates the entity being monitored for temperature.

Position	Statistic	Type	Timer Value	Range	OID	Description
				ds 1624s Phy0 Physical Interface 0 ds 1624s Phy1 Physical Interface 1 NE1775s SDRAM Synchronous dynamic random access memory (SDRAM) NE1775s PMC Polymer matrix composites (PMC)		
2	Description	string	N/A	Main board PROM Temperature Monitoring temperature on the programmable read-only memory (PROM) on the main board. Host processor PROM Temperature Monitoring temperature on the host processor PROM. PHY0 PROM Temperature Monitoring temperature on the Physical Interface 0 PROM. PHY1 PROM Temperature Monitoring temperature on the Physical Interface 1 PROM. SDRAM Temperature Monitoring temperature on the synchronous dynamic random access memory (SDRAM) PMC Temperature Monitoring temperature on the polymer matrix composites (PMC)	N/A	Textual description of the entity being monitored for temperature.
3	Temperature (Celsius)	gauge	N/A	0° to 100°	1.3.6.1.4.1.9148.3.3.1.3.1.1.4	Current temperature on the main board's programmable read-only

Position	Statistic	Type	Timer Value	Range	OID	Description
						memory (PROM), in Celsius.

space

Statistics that display storage space information on the SBC

Position	Statistic	Type	Timer Value	Range	Description
1	Volume Name	string	N/A	hard-disk0 Hard disk volume 0 hard-disk1 Hard disk volume 1 hard-disk2 Hard disk volume 2 hard-disk3 Hard disk volume 4 /ramdrv Random Access Memory (RAM) drive /boot/code Boot code volume /boot Boot volume	Name of the volume used for storage space.
2	Space Used	gauge	N/A	0 to 4294967295	Total space used on the volume in Megabytes (Mb)
3	Space Available	gauge	N/A	0 to 4294967295	Total space available on the volume in Megabytes (Mb)

network-util

Statistics that display network utilization information

SNMP MIB
ap-env-monitor.mib
apSysMgmtPhyUtilTableEntry
1.3.6.1.4.1.9148.3.2.1.8.1.1

Position	Statistic	Type	Timer Value	Range	OID	Description
1	Index	counter	N/A	0 to 4294967295	N/A	An integer that contains the ifIndex of a media port
2	Rx Utilization	gauge	N/A	0% to 100%	1.3.6.1.4.1.9148.3.2.1.8.1.1.1	Receive (Rx) network utilization of the physical port measured over a one second period

Position	Statistic	Type	Timer Value	Range	OID	Description
3	Tx Utilization	gauge	N/A	0% to 100%	1.3.6.1.4.1.9148.3.2.1.8.1.1.2	Transmit (Tx) network utilization of the physical port measured over a one second period

ACLI-Associated Groups and Group Statistics

The Groups and Group Statistics in this section correspond to the data that displays as output from some of the current ACLI commands. For example, the output for the **show sipd sessions** command, when run from the ACLI, is shown in the figure below:

Example of Show Command Output

```
ACMEPACKET> show sipd sessions
12:50:45-131
SIP Session Status          -- Period -- -------- Lifetime --------
                  Active     High   Total       Total  PerMax     High
Sessions               0        0       0           0       0        0
  Initial              0        0       0           0       0        0
  Early                0        0       0           0       0        0
  Established          0        0       0           0       0        0
  Terminated           0        0       0           0       0        0
Dialogs                0        0       0           0       0        0
  Early                0        0       0           0       0        0
  Confirmed            0        0       0           0       0        0
  Terminated           0        0       0           0       0        0
```

For the **sip-session group**, the HDR Collector stores the same data that would display in the Lifetime/Total column if you ran the ACLI command at the same time the Collector sampled the statistics. In the ACLI output, the data is grouped by Sessions and Dialogs. When mapped into the HDR data for the sip-session group header, the ACLI names are further clarified, as shown in the table below:

ACLI Name	Group Header Name
Sessions	Sessions
Initial	Sessions Initial
Early	Sessions Early
Established	Sessions Established
Terminated	Sessions Terminated
Dialogs	Dialogs
Early	Dialogs Early
Confirmed	Dialogs Confirmed
Terminated	Dialogs Terminated

The following is an example of a CSV file containing the HDR statistics for the sip-session Group generated by the HDR Collector. The output format reflects that the file was opened using an application compatible with a CSV file.

Example of a CSV File for the sip-session Group

```
Timestamp     Sessions    Sessions Initial   Sessions Early ...
1301702288    45          45                 28             ...
1301702456    35          35                 35             ...
```

Note: The records in a CSV file may display differently, depending on the record data included in the file, and the method used to open the file. For more information about the display of record data in a CSV file, see Appendix A, CSV File Data Formats.

This section provides a description of each Group and Group Statistic associated with the ACLI. Each Group table identifies the ACLI Show command for which it is associated, and provides a link to the applicable command in Chapter 4.

Groups in this section include:

- sip-sessions
- sip-acl-oper
- sip-acl-status
- sip-client
- sip-server
- sip-policy
- sip-errors
- sip-status
- sip-invites
- registration-realm
- enum-stats
- mgcp-state
- mgcp-trans
- mgcp-media-events
- mgcp-oper
- mgcp-acl
- h323-stats

sip-sessions

Consists of statistics pertaining to the Session Initiation Protocol (SIP) sessions. Use "show sipd sessions" to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	Sessions	counter	N/A	0 to 4294967295	Total number of sessions established by INVITE and SUBSCRIBE messages
2	Sessions Initial	counter	N/A	0 to 4294967295	Total number of sessions for which an INVITE or SUBSCRIBE is being forwarded
3	Sessions Early	counter	N/A	0 to 4294967295	Total number of sessions for which the first provisional response (1xx other than 100) is received.
4	Sessions Established	counter	N/A	0 to 4294967295	Total number of sessions for which a success (2xx) response is received.
5	Sessions Terminated	counter	N/A	0 to 4294967295	Total number of sessions that have ended by receiving or sending a BYE for an Established session or forwarding an error response for an Initial or Early session. The session remains in the terminated state until all the resources for the session are freed up.

Position	Statistic	Type	Timer Value	Range	Description
6	Dialogs	counter	N/A	0 to 4294967295	Total number of end-to-end SIP signaling connections.
7	Dialogs Early	counter	N/A	0 to 4294967295	Total number of dialogs that were created by a provisional response.
8	Dialogs Confirmed	counter	N/A	0 to 4294967295	Total number of dialogs that were created by a success response. An Early dialog transitions to Confirmed when a success response is received.
9	Dialogs Terminated	counter	N/A	0 to 4294967295	Total number of dialogs that were ended by a receiving/sending of a BYE for an Established session, or a receiving/sending error response Early dialog. The dialog remains in the Terminated state until all the resources for the session are freed up.

sip-acl-oper

Consists of statistics pertaining to the Session Initiation Protocol (SIP) access control list (ACL) operations. Use "show sipd acls" to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	ACL Requests	counter	N/A	0 to 4294967295	Total number of ACL requests
2	Bad Messages	counter	N/A	0 to 4294967295	Total number of bad messages
3	Promotions	counter	N/A	0 to 4294967295	Total number of ACL entry promotions. These are the ACL entries that have been promoted from untrusted to trusted status.
4	Demotions	counter	N/A	0 to 4294967295	Total number of ACL entry demotions.
5	Demote Trust-Untrust	counter	N/A	0 to 4294967295	Total number of ACL entries demoted from trusted to untrusted.
6	Demote Untrust-Deny	counter	N/A	0 to 4294967295	Total number of ACL entries demoted from untrusted to deny.

sip-acl-status

Consists of statistics pertaining to the Session Initiation Protocol (SIP) access control list (ACL) state. Use "show sipd acls" to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	Total Entries	counter	N/A	0 to 4294967295	Total number of ACL entries, both trusted and blocked.
2	Trusted	counter	N/A	0 to 4294967295	Total number of trusted ACL entries
3	Blocked	counter	N/A	0 to 4294967295	Total number of blocked ACL entries

sip-client

Consists of statistics pertaining to the Session Initiation Protocol (SIP) client state. Use "show sipd client" to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	AllStates	counter	N/A	0 to 4294967295	Total number of all client session transactions
2	Initial	counter	N/A	0 to 4294967295	Total number of times the Initial state was entered due to the receipt of a request.
3	Trying	counter	N/A	0 to 4294967295	Total number of times the Trying state was entered due to the receipt of a request
4	Calling	counter	N/A	0 to 4294967295	Total number of times the Calling state was entered due to the receipt of an INVITE request
5	Proceeding	counter	N/A	0 to 4294967295	Total number of times the Proceeding state was entered due to the receipt of a provisional response while in the Calling state
6	Cancelled	counter	N/A	0 to 4294967295	Total number of INVITE transactions that received a CANCEL
7	EarlyMedia	counter	N/A	0 to 4294967295	Total number of times the Proceeding state was entered due to the receipt of a provisional response that contained a Session Description Protocol (SDP) while in the Calling state
8	Completed	counter	N/A	0 to 4294967295	Total number of times that the Completed state was entered due to the receipt of a status code in the range of 300-699 when either in the Calling or Proceeding state
9	Setmedia	counter	N/A	0 to 4294967295	Total number of transactions in which the SBC was setting up NAT and steering ports
10	Established	counter	N/A	0 to 4294967295	Total number of times the client received a 2xx response to an INVITE, but could not forward it because the NAT and steering port information was missing
11	Terminated	counter	N/A	0 to 4294967295	Total number of times the Terminated state was entered after a 2xx message

sip-server

Consists of statistics pertaining to the Session Initiation Protocol (SIP) server state. Use "show sipd server" to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	AllStates	counter	N/A	0 to 4294967295	Total number of all server session transactions
2	Initial	counter	N/A	0 to 4294967295	Total number of times the Initial state was entered due to the receipt of a request
3	Trying	counter	N/A	0 to 4294967295	Total number of times the Trying state was entered due to the receipt of a request

Position	Statistic	Type	Timer Value	Range	Description
4	Proceeding	counter	N/A	0 to 4294967295	Total number of times the Proceeding state was entered due to the receipt of a provisional response while in the Calling state
5	Cancelled	counter	N/A	0 to 4294967295	Total number of INVITE transactions that received a CANCEL
6	Established	counter	N/A	0 to 4294967295	Total number of times the server received a 2xx response to an INVITE, but could not forward it because the NAT and steering port information was missing
7	Completed	counter	N/A	0 to 4294967295	Total number of times that the Completed state was entered due to the receipt of a status code in the range of 300-699 when either in the Calling or Proceeding state
8	Confirmed	counter	N/A	0 to 4294967295	Total number of times that an ACK was received while the server was in the Completed state and then transitioned to Confirmed state
9	Terminated	counter	N/A	0 to 4294967295	Total number of times the Terminated state was entered after a 2xx message, or never received an ACK in the Completed state, and then transitioned to the Terminated state.

sip-policy

Consists of statistics pertaining to the Session Initiation Protocol (SIP) local policy / routing statistics. Use "show sipd policy" to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	Local Lookup	counter	N/A	0 to 4294967295	Total number of local policy lookups
2	Local Hits	counter	N/A	0 to 4294967295	Total number of successful local policy lookups
3	Local Misses	counter	N/A	0 to 4294967295	Total number of local policy lookup failures
4	Local Drops	counter	N/A	0 to 4294967295	Total number of local policy lookups where the next hop session agent group is H323
5	Agent Group Hits	counter	N/A	0 to 4294967295	Total number of successful local policy lookups for session agent groups
6	Agent Group Misses	counter	N/A	0 to 4294967295	Total number of successful local policy lookups where no session agent was available for the session agent group
7	No Routes Found	counter	N/A	0 to 4294967295	Total number of successful local policy lookups, but temporarily unable to route (for example, session agent out of service)
8	Missing Dialog	counter	N/A	0 to 4294967295	Total number of local policy lookups where the dialog was not found for a

Position	Statistic	Type	Timer Value	Range	Description
					request addressed to the SBC with a To tag or for a NOTIFY-SUBSCRIBE SIP request
9	Inb SA Constraints	counter	N/A	0 to 4294967295	Total number of successful local policy lookups where the inbound session agent (SA) exceeded constraints
10	Outb SA Constraints	counter	N/A	0 to 4294967295	Total number of successful local policy lookups where the outbound SA exceeded constraints
11	Inb REG SA Constraints	counter	N/A	0 to 4294967295	Total number of successful inbound local policy lookups where the registrar (REG) SA exceeded constraints
12	Outb REG SA Constraints	counter	N/A	0 to 4294967295	Total number of successful outbound local policy lookups where the registrar (REG) SA exceeded constraints
13	Requests Challenged	counter	N/A	0 to 4294967295	Total number of requests that were challenged.
14	Challenges Found	counter	N/A	0 to 4294967295	Total number of challenges found.
15	Challenges Not Found	counter	N/A	0 to 4294967295	Total number of challenges not found.
16	Challenge Drops	counter	N/A	0 to 4294967295	Total number of challenges dropped.

sip-errors

Consists of statistics pertaining to errors that occur in SIP media events. Use "show sipd errors" to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	SDP Offer Errors	counter	N/A	0 to 4294967295	Total number of errors encountered in setting up the media session for a session description in a SIP request or response which is a Session Description Protocol (SDP) Offer in the Offer/ Answer model (RFC 3264)
2	SDP Answer Errors	counter	N/A	0 to 4294967295	Total number of errors encountered in setting up the media session for a session description in a SIP request or response which is a Session Description Protocol (SDP) Answer in the Offer/Answer model (RFC 3264)
3	Drop Media Errors	counter	N/A	0 to 4294967295	Total number of errors encountered in tearing down the media for a dialog or session that is being terminated due to: a) non-successful response to an INVITE transaction, or b) a BYE transaction received from one of the participants in a dialog/session, or

Position	Statistic	Type	Timer Value	Range	Description
					c) a BYE initiated by the SBC due to a timeout notification from the Middlebox Control Daemon (MBCD).
4	Transaction Errors	counter	N/A	0 to 4294967295	Total number of errors in continuing the processing of the SIP client transaction associated with setting up or tearing down of the media session.
5	Application Errors	counter	N/A	0 to 4294967295	Total number of miscellaneous errors in the SIP application that are otherwise uncategorized
6	Media Exp Events	counter	N/A	0 to 4294967295	Total number of flow timer expiration notifications received from the Middlebox Control Daemon (MBCD).
7	Early Media Exps	counter	N/A	0 to 4294967295	Total number of flow timer expiration notifications received for media sessions that were not completely set up due to an incomplete or pending INVITE transaction
8	Exp Media Drops	counter	N/A	0 to 4294967295	Total number of flow timer expiration notifications from the Middlebox Control Daemon (MBCD) that resulted in the termination of the dialog/session by the SIP application.
9	Expired Sessions	counter	N/A	0 to 4294967295	Total number of sessions terminated due to the session timer expiring
10	Multiple OK Drops	counter	N/A	0 to 4294967295	Total number of dialogs terminated upon reception of a 200 OK response from multiple User Agent Servers (UASs) for a given INVITE transaction that was forked by a downstream proxy
11	Multiple OK Terms	counter	N/A	0 to 4294967295	Total number of dialogs terminated upon reception of a 200 OK response that conflicts with an existing established dialog on the SBC
12	Media Failure Drops	counter	N/A	0 to 4294967295	Total number of dialogs terminated due to a failure in establishing the media session.
13	Non-ACK 2xx Drops	counter	N/A	0 to 4294967295	Total number of sessions terminated because an ACK was not received for a 2xx response
14	Invalid Requests	counter	N/A	0 to 4294967295	Total number of invalid requests (for example, an unsupported header was received).
15	Invalid Responses	counter	N/A	0 to 4294967295	Total number of invalid responses (for example, no Via header in response)
16	Invalid Messages	counter	N/A	0 to 4294967295	Total number of messages dropped due to parse failure
17	CAC Session Drop	counter	N/A	0 to 4294967295	Total number of call admission control (CAC) session setup failures

Position	Statistic	Type	Timer Value	Range	Description
18	CAC BW Drop	counter	N/A	0 to 4294967295	Total number of call admission control (CAC) session setup failures due to insufficient bandwidth (BW)
19	Call Rejects	counter	N/A	0 to 4294967295	Total number of calls rejected during the window.

sip-status

Consists of statistics pertaining to Session Initiation Protocol (SIP) transactions. Use "show sipd status" to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	Sessions	counter	N/A	0 to 4294967295	Total number of sessions established by INVITE and SUBSCRIBE messages
2	Subscriptions	counter	N/A	0 to 4294967295	Total number of sessions established by SUBSCRIPTION
3	Dialogs	counter	N/A	0 to 4294967295	Total number of end-to-end SIP signaling connections
4	CallID Maps	counter	N/A	0 to 4294967295	Total number of successful session header Call ID mappings
5	Rejections	counter	N/A	0 to 4294967295	Total number of rejected INVITEs
6	ReINVITEs	counter	N/A	0 to 4294967295	Total number of ReINVITEs
7	Media Sessions	counter	N/A	0 to 4294967295	Total number of successful media sessions
8	Media Pending	counter	N/A	0 to 4294967295	Total number of media sessions waiting to be established
9	Client Trans	counter	N/A	0 to 4294967295	Total number of client transactions
10	Server Trans	counter	N/A	0 to 4294967295	Total number of server transactions that have taken place on the SBC
11	Resp Contexts	counter	N/A	0 to 4294967295	Total number of response contexts
12	Saved Contexts	counter	N/A	0 to 4294967295	Total number of saved contexts
13	Sockets	counter	N/A	0 to 4294967295	Total number of SIP sockets
14	Req Drops	counter	N/A	0 to 4294967295	Total number of dropped requests
15	DNS Trans	counter	N/A	0 to 4294967295	Total number of Domain Name System (DNS) transactions
16	DNS Sockets	counter	N/A	0 to 4294967295	Total number of Domain Name System (DNS) sockets
17	DNS Results	counter	N/A	0 to 4294967295	Total number of Domain Name System (DNS) results

Position	Statistic	Type	Timer Value	Range	Description
18	Session Rate	fixed decimal	30	0 to 4294967295	The rate, per second, of SIP invites allowed to or from the SBC during the sliding window period. The rate is computed every 10 seconds .
19	Load Rate	guage	30	0% to 100%	Average Central Processing Unit (CPU) utilization of the SBC during the current window. The average is computed every 10 seconds unless the load-limit is configured in the SIPConfig record, in which case it is 5 seconds.
20	Active Subscriptions	counter	N/A	0 to 4294967295	specifies the current global count of active SIP subscriptions.
21	SubscriptionsPerMax	counter	N/A	0 to 4294967295	specifies the maximum global count of SIP subscriptions initiated during any 100 second period since the last SBC re-boot.
22	Subscriptions High	counter	N/A	0 to 4294967295	specifies the maximum global count of active SIP subscriptions since the last SBC re-boot.

sip-invites

Consists of statistics pertaining to Session Initiation Protocol (SIP) INVITEs. Use "show sipd invite" to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	INVITE Requests	counter	N/A	0 to 4294967295	Total number of INVITE requests
2	Retransmissions	counter	N/A	0 to 4294967295	Total number of retransmissions of INVITEs
3	Response Retrans	counter	N/A	0 to 4294967295	Total number of response retransmissions
4	Transaction Timeouts	counter	N/A	0 to 4294967295 for client. Server values are always “—”; transaction timeout statistics are not valid for server operations.	Total number of INVITE request transaction timeouts
5	Locally Throttled	counter	N/A	0 to 4294967295 for client. Server values are always “—”; locally throttled statistics are not valid for server operations.	Total number of INVITE requests locally throttled

registration-realm

Statistics that display registration information (counters) for the total registrations received, number of successful registrations, and number of unsuccessful registrations for each of the following categories: initial registrations, refresh registrations, and de-registrations. Use "show sipd realms" to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	Realm Name	config	N/A	N/A	Name of the realm for which the group statistics are being calculated.
2	Total Initial Registrations	counter	N/A	0 to 4294967295	Total number of initial registrations. This counter is incremented once for each initial REGISTER message even when the REGISTER is challenged. This counter is based on ingress (received) messages only. Note: This counter is not incremented when registrations are challenged by the following response messages: 401 (Unauthorized - user authentication required) 407 (Proxy authentication required) 423 (Interval too brief - expiration time of the resource is too short)
3	Successful Initial Registrations	counter	N/A	0 to 4294967295	Number of successful initial registrations. This counter is incremented once for each successful initial registration with a 200 OK response. This counter is based on ingress (received) messages only.
4	Unsuccessful Initial Registrations	counter	N/A	0 to 4294967295	Number of unsuccessful initial registrations. This counter is incremented once for each unsuccessful initial registration when the response to the initial REGISTER has a non-success status code. This counter is based on ingress (received) messages only. Note: This counter is not incremented when registrations are challenged by the following response messages: 401 (Unauthorized - user authentication required) 407 (Proxy authentication required) 423 (Interval too brief - expiration time of the resource is too short)
5	Total Refresh Registrations	counter	N/A	0 to 4294967295	Total number of registrations that were refreshed. This counter is incremented once for every refresh registration. This counter is based on ingress (received) messages only.
6	Successful Refresh Registrations	counter	N/A	0 to 4294967295	Total number of registrations that were successfully refreshed. This counter is incremented once for each successful refresh registration. This

Position	Statistic	Type	Timer Value	Range	Description
					counter is based on ingress (received) messages only.
7	Unsuccessful Refresh Registrations	counter	N/A	0 to 4294967295	Total number of registrations that were unsuccessfully refreshed. This counter is incremented once for each unsuccessful refresh registration. This counter is based on ingress (received) messages only.
8	Total De-Registrations	counter	N/A	0 to 4294967295	Total number of registrations that de-registered. This counter is incremented once for every de-registration. This counter is based on ingress (received) messages only. In the event a de-registration message is received on a realm that is different than that of the initial registration message, the de-registration counter for the ingress realm of that de-registration message is incremented.
9	Successful De-Registrations	counter	N/A	0 to 4294967295	Total number of registrations that successfully de-registered. This counter is incremented once for each successful de-registration. This counter is based on ingress (received) messages only. In the event a successful de-registration message is received on a realm that is different than that of the initial registration message, the de-registration counter for the ingress realm of that successful de-registration message is incremented.
10	Unsuccessful De-Registrations	counter	N/A	0 to 4294967295	Total number of registrations that unsuccessfully de-registered. This counter is incremented once for each unsuccessful de-registration. This counter is based on ingress (received) messages only. In the event an unsuccessful de-registration message is received on a realm that is different than that of the initial registration message, the de-registration counter for the ingress realm of that unsuccessful de-registration message is incremented.

enum-stats

Consists of statistics pertaining to the Telephone Number Mapping (ENUM) Agent on the SBC. Use **show enum** to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	Enum Agent	config	N/A	N/A	Name of the ENUM Agent
2	Queries Total	counter	N/A	0 to 4294967295	Total number of ENUM queries
3	Successful Total	counter	N/A	0 to 4294967295	Total number of successful ENUM queries
4	Not found Total	counter	N/A	0 to 4294967295	Total number of ENUM queries returning a not found
5	Timeout Total	counter	N/A	0 to 4294967295	Total number of ENUM query timeouts

mgcp-state

Consists of statistics pertaining to the Media Gateway Control Protocol (MGCP) state on the Oracle Communications Session Border Controller. This group captures many of the counters from the **show mgcp** command.

Position	Statistic	Type	Timer Value	Range	Description
1	MGCP Sessions	counter	N/A	0 to 4294967295	Total number of MGCP sessions
2	CA Endpoints	counter	N/A	0 to 4294967295	Total number of call agent (CA) endpoints
3	GW Endpoints	counter	N/A	0 to 4294967295	Total number of gateway (GW) endpoints
4	Media Sessions	counter	N/A	0 to 4294967295	Total number of media sessions
5	Client Trans	counter	N/A	0 to 4294967295	Total number of client transactions
6	Server Trans	counter	N/A	0 to 4294967295	Total number of server transactions
7	Pending MBCD	counter	N/A	0 to 4294967295	Total number of pending media requests to the Middlebox Control Daemon (MBCD)
8	MGCP ALGs	counter	N/A	0 to 4294967295	Total number of MGCP Application Layer Gateways (ALGs)
9	Port Maps Available	counter	N/A	0 to 64511	Total number of port maps (i.e., IP ports) available
10	Port Maps Allocated	counter	N/A	0 to 64511	Total number of port maps (i.e., IP ports) allocated

mgcp-trans

Consists of statistics pertaining to the Media Gateway Control Protocol (MGCP) transactions on the SBC. Use **show mgcp** to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	Requests Received	counter	N/A	0 to 4294967295	Total number of requests received
2	Responses Sent	counter	N/A	0 to 4294967295	Total number of responses sent
3	Duplicates Received	counter	N/A	0 to 4294967295	Total number of duplicates received
4	Requests Sent	counter	N/A	0 to 4294967295	Total number of requests sent
5	Responses Received	counter	N/A	0 to 4294967295	Total number of responses received
6	Retransmissions Sent	counter	N/A	0 to 4294967295	Total number of retransmissions sent

mgcp-media-events

Consists of statistics pertaining to the Media Gateway Control Protocol (MGCP) media event errors on the SBC. Use **show mgcp errors** to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	Calling SDP Errors	counter	N/A	0 to 4294967295	Total number of errors encountered in setting up the media session for a session description in a Request or Response, which is a Session

Position	Statistic	Type	Timer Value	Range	Description
					Description Protocol (SDP) Offer in the Offer/ Answer model (RFC 3264)
2	SDP Answer Errors	counter	N/A	0 to 4294967295	Total number of errors encountered in setting up the media session for a session description in a Request or Response, which is a Session Description Protocol (SDP) Answer in the Offer/Answer model (RFC 3264)
3	Drop Media Errors	counter	N/A	0 to 4294967295	Total number errors encountered in tearing down the media for a session that is being terminated
4	Transaction Errors	counter	N/A	0 to 4294967295	Total number errors in continuing the processing of the client transaction associated with setting up or tearing down of the media session
5	Application Errors	counter	N/A	0 to 4294967295	Total number of miscellaneous errors that are otherwise uncategorized
6	Media Exp Events	counter	N/A	0 to 4294967295	Total number of flow timer expiration notifications received from Middlebox Control Daemon (MBCD)
7	Early Media Exps	counter	N/A	0 to 4294967295	Total number of flow timer expiration notifications received for media sessions that have not been completely set up
8	Exp Media Drops	counter	N/A	0 to 4294967295	Total number of flow timer expiration notifications from the Middlebox Control Daemon (MBCD) that resulted in the termination of the session

mgcp-oper

Consists of statistics pertaining to the Media Gateway Control Protocol (MGCP) operations on the SBC. Use **show mgcp acls** to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	ACL Requests	counter	N/A	0 to 4294967295	Total number of access control list (ACL) requests
2	Bad Messages	counter	N/A	0 to 4294967295	Total number of bad messages
3	Promotions	counter	N/A	0 to 4294967295	Total number of ACL entry promotions. These are the ACL entries that have been promoted from untrusted to trusted status.
4	Demotions	counter	N/A	0 to 4294967295	Total number of ACL entry demotions

mgcp-acl

Consists of statistics pertaining to the Media Gateway Control Protocol (MGCP) access control list (ACL) events on the SBC. Use **show mgcp acls** to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	Total Entries	counter	N/A	0 to 4294967295	Total number of ACL entries, including both trusted and blocked
2	Trusted	counter	N/A	0 to 4294967295	Total number of trusted ACL entries
3	Blocked	counter	N/A	0 to 4294967295	Total number of blocked ACL entries

h323-stats

Consists of statistics pertaining to H323 events on the SBC. Use **show h323** to view statistics.

Position	Statistic	Type	Timer Value	Range	Description
1	Incoming Calls	counter	N/A	0 to 4294967295	Total number of incoming H.323 calls
2	Outgoing Calls	counter	N/A	0 to 4294967295	Total number of outgoing H.323 calls
3	Connected Calls	counter	N/A	0 to 4294967295	Total number of connected H.323 calls
4	Incoming Channels	counter	N/A	0 to 4294967295	Total number of established incoming calls
5	Outgoing Channels	counter	N/A	0 to 4294967295	Total number of established outgoing calls
6	Contexts	counter	N/A	0 to 4294967295	Total number of established H.323 contexts (or call terminations)
7	Queued Messages	counter	N/A	0 to 4294967295	Total number of messages queued
8	TPKT Channels	counter	N/A	0 to 4294967295	Total number of ThroughPacket (TPKT) channels open(ed)
9	UDP Channels	counter	N/A	0 to 4294967295	Total number of User Datagram Protocol (UDP) channels open(ed)

sip-rate

Records SIP processing level in terms of messages per method (i.e. both request and response) per second on system-wide basis.

Position	Statistic	Type	Timer Value	Range	Description
1	Method Name	string	N/A	N/A	SIP method name for which the group statistics are being calculated
2	Messages Received Rate	counter	N/A	0 to 4294967295	Messages per second for messages received for a SIP method on all SIP interfaces
3	Messages Sent Rate	counter	N/A	0 to 4294967295	Messages per second for messages sent for a SIP method on all SIP interfaces
4	Requests Received Rate	counter	N/A	0 to 4294967295	Messages per second for requests received for a SIP method on all SIP interfaces
5	Requests Sent Rate	counter	N/A	0 to 4294967295	Messages per second for requests sent for a SIP method on all SIP interfaces

Position	Statistic	Type	Timer Value	Range	Description
6	Responses Received Rate	counter	N/A	0 to 4294967295	Messages per second for responses received for a SIP method on all SIP interfaces
7	Responses sent Rate	counter	N/A	0 to 4294967295	Messages per second for responses sent for a SIP method on all SIP interfaces

sip-rate-per-interface

Records SIP message rates l in terms of messages per method (i.e. both request and response) per second per SIP interface.

Position	Statistic	Type	Timer Value	Range	Description
1	Interface Name	string	N/A	N/A	SIP interface where these statistics are being calculated
2	Method Name	string	N/A	N/A	SIP method name for which the group statistics are being calculated
3	Messages Received Rate	counter	N/A	0 to 4294967295	Messages per second for messages received for a SIP method on all SIP interfaces
4	Messages Sent Rate	counter	N/A	0 to 4294967295	Messages per second for messages sent for a SIP method on all SIP interfaces
5	Requests Received Rate	counter	N/A	0 to 4294967295	Messages per second for requests received for a SIP method on all SIP interfaces
6	Requests Sent Rate	counter	N/A	0 to 4294967295	Messages per second for requests sent for a SIP method on all SIP interfaces
7	Responses Received Rate	counter	N/A	0 to 4294967295	Messages per second for responses received for a SIP method on all SIP interfaces
8	Responses sent Rate	counter	N/A	0 to 4294967295	Messages per second for responses sent for a SIP method on all SIP interfaces

sip-rate-per-agent

Records SIP message rates in terms of messages per method (i.e. both request and response) per second per SIP session agent.

Position	Statistic	Type	Timer Value	Range	Description
1	Agent Name	string	N/A	N/A	SIP Agent where these statistics are being calculated
2	Method Name	string	N/A	N/A	SIP method name for which the group statistics are being calculated
3	Messages Received Rate	counter	N/A	0 to 4294967295	Messages per second for messages received for a SIP method on all SIP interfaces

Position	Statistic	Type	Timer Value	Range	Description
4	Messages Sent Rate	counter	N/A	0 to 4294967295	Messages per second for messages sent for a SIP method on all SIP interfaces
5	Requests Received Rate	counter	N/A	0 to 4294967295	Messages per second for requests received for a SIP method on all SIP interfaces
6	Requests Sent Rate	counter	N/A	0 to 4294967295	Messages per second for requests sent for a SIP method on all SIP interfaces
7	Responses Received Rate	counter	N/A	0 to 4294967295	Messages per second for responses received for a SIP method on all SIP interfaces
8	Responses sent Rate	counter	N/A	0 to 4294967295	Messages per second for responses sent for a SIP method on all SIP interfaces

dnsalg-rate

Records DNS Message rate (i.e. both request and response) per second on system-wide basis.

Position	Statistic	Type	Timer Value	Range	Description
1	Messages Received Rate	counter	N/A	0 to 4294967295	Messages per second for all DNS messages received by the system
2	Messages Sent Rate	counter	N/A	0 to 4294967295	Messages per second for all DNS messages sent on the system
3	Requests Received Rate	counter	N/A	0 to 4294967295	Messages per second for DNS requests received on the system.
4	Requests Sent Rate	counter	N/A	0 to 4294967295	Messages per second for DNS requests sent by the system.
5	Responses Received Rate	counter	N/A	0 to 4294967295	Messages per second for DNS responses received on the system.
6	Responses sent Rate	counter	N/A	0 to 4294967295	Messages per second for DNS responses sent by the system.

dnsalg-rate-per-realm

Records DNS Message rate (i.e. both request and response) per second on per-realm basis.

Position	Statistic	Type	Timer Value	Range	Description
1	Client Realm ID	string	N/A	N/A	Client realm name for which the group statistics are being calculated
2	Messages Received Rate	counter	N/A	0 to 4294967295	Messages per second for all DNS messages received by the system
3	Messages Sent Rate	counter	N/A	0 to 4294967295	Messages per second for all DNS messages sent on the system
4	Requests Received Rate	counter	N/A	0 to 4294967295	Messages per second for DNS requests received on the system.
5	Requests Sent Rate	counter	N/A	0 to 4294967295	Messages per second for DNS requests sent by the system.

Position	Statistic	Type	Timer Value	Range	Description
6	Responses Received Rate	counter	N/A	0 to 4294967295	Messages per second for DNS responses received on the system.
7	Responses sent Rate	counter	N/A	0 to 4294967295	Messages per second for DNS responses sent by the system.

dnsalg-rate-per-addr

Records DNS Message rate (i.e. both request and response) per second on system-wide basis.

Position	Statistic	Type	Timer Value	Range	Description
1	Server IP Address	string	N/A	N/A	DNS Server Address for which the group statistics are being calculated
2	Messages Received Rate	counter	N/A	0 to 4294967295	Messages per second for all DNS messages received by the system
3	Messages Sent Rate	counter	N/A	0 to 4294967295	Messages per second for all DNS messages sent on the system
4	Requests Received Rate	counter	N/A	0 to 4294967295	Messages per second for DNS requests received on the system.
5	Requests Sent Rate	counter	N/A	0 to 4294967295	Messages per second for DNS requests sent by the system.
6	Responses Received Rate	counter	N/A	0 to 4294967295	Messages per second for DNS responses received on the system.
7	Responses sent Rate	counter	N/A	0 to 4294967295	Messages per second for DNS responses sent by the system.

enum-rate

Records ENUM Message rate (i.e. both request and response) per second on system-wide basis.

Position	Statistic	Type	Timer Value	Range	Description
1	Messages Received Rate	counter	N/A	0 to 4294967295	Messages per second for all ENUM messages received by the system
2	Messages Sent Rate	counter	N/A	0 to 4294967295	Messages per second for all ENUM messages sent on the system
3	Requests Received Rate	counter	N/A	0 to 4294967295	Messages per second for ENUM requests received on the system.
4	Requests Sent Rate	counter	N/A	0 to 4294967295	Messages per second for ENUM requests sent by the system.
5	Responses Received Rate	counter	N/A	0 to 4294967295	Messages per second for ENUM responses received on the system.
6	Responses sent Rate	counter	N/A	0 to 4294967295	Messages per second for ENUM responses sent by the system.

enum-rate-per-name

Records ENUM Message rate (i.e. both request and response) per second on per-interface (i.e. the network interface on which the ENUM config's realm exists) basis.

Position	Statistic	Type	Timer Value	Range	Description
1	ENUM Config Name	string	N/A	N/A	Enum config name for which the group statistics are being calculated
2	Messages Received Rate	counter	N/A	0 to 4294967295	Messages per second for all ENUM messages received by this configuration object.
3	Messages Sent Rate	counter	N/A	0 to 4294967295	Messages per second for all ENUM messages by this configuration object.
4	Requests Received Rate	counter	N/A	0 to 4294967295	Messages per second for ENUM requests received by this configuration object.
5	Requests Sent Rate	counter	N/A	0 to 4294967295	Messages per second for ENUM requests sent by this configuration object.
6	Responses Received Rate	counter	N/A	0 to 4294967295	Messages per second for ENUM responses received by this configuration object.
7	Responses sent Rate	counter	N/A	0 to 4294967295	Messages per second for ENUM responses sent by this configuration object.

enum-rate-per-addr

Records ENUM Message rate (i.e. both request and response) per second on system-wide basis. Records ENUM Message rate (i.e. both request and response) per second on a per-address basis (i.e. ENUM server provisioned in the ENUM Config).

Position	Statistic	Type	Timer Value	Range	Description
1	Server IP Address	string	N/A	N/A	ENUM Server Address for which the group statistics are being calculated
2	Messages Received Rate	counter	N/A	0 to 4294967295	Messages per second for all ENUM messages received by this server.
3	Messages Sent Rate	counter	N/A	0 to 4294967295	Messages per second for all ENUM messages sent by this server.
4	Requests Received Rate	counter	N/A	0 to 4294967295	Messages per second for ENUM requests received by this server.
5	Requests Sent Rate	counter	N/A	0 to 4294967295	Messages per second for ENUM requests sent by this server.
6	Responses Received Rate	counter	N/A	0 to 4294967295	Messages per second for ENUM responses received by this server.
7	Responses sent Rate	counter	N/A	0 to 4294967295	Messages per second for ENUM responses sent by this server.

4

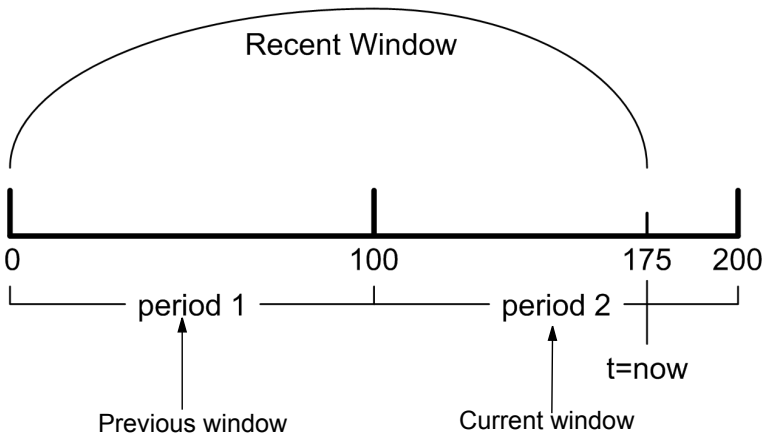
HDR Show Commands

This section provides information about the Oracle Communications Session Border Controller (SBC) Show commands you can enter at the root level of the Acme Packet Command Line Interface (ACLI). The parameters in these tables map to the Historical Data Recording (HDR) data used by the HDR Collector when generating comma-separated value (CSV) reports.

For more information about the HDR Collection data, see *HDR Groups and Group Statistics*.

Statistic Counts

For each Show command table output, statistical counts are based on the SBC defining a period as 100 seconds. The recent window represents the previous complete period (period 1 shown below) PLUS the time incurred into the current period (period 2 shown below). Period 1 = 100 seconds and period 2 = 75 seconds. The complete window period = 175 seconds. After period 3 is entered (not pictured below), the Recent window will begin at the 100 second mark.



When you execute a **show** command, a timestamp and period count display.

```
ACMEPACKET> show sipd sessions
10:37:25-141
```

In the period count, the number after the dash, indicates the number of seconds into the recent period. In the above example, the number of seconds into the recent period is 158 seconds. Therefore, the recent window ranges from 100 to 199 seconds.

Table Column Descriptions

For each Show command table, the columns are defined as follows:

Column	Description
Period Active	Represents the current number of active counts
Period High	Represents the highest number during the recent window
Period Total	Represents the total accumulated count during the recent window
The Lifetime statistics begin accumulating from the last reboot.	
Lifetime Total	Represents the total accumulated count
Lifetime PerMax	Represents the maximum recorded in one period
Lifetime High	Represents the highest momentary count

Show Commands Associated with HDR Groups

This section provides ACLI show command output tables and descriptions. These show commands are associated with the HDR Groups described in the section, **ACLI-Associated Groups and Group Statistics**.

Show commands in this section include:

- show sipd sessions
- show sipd agents *
- show sipd acls
- show sipd client
- show sipd server
- show sipd policy
- show sipd errors
- show sipd status
- show sipd invite
- show sipd realms *
- show enum
- show mgcp
- show mgcp errors
- show mgcp acls
- show h323
- show sipd rate
- show sipd rate agent
- show sipd rate interface
- show dnsalg rate
- show dnsalg rate realm-id
- show dnsalg rate server-ip-addr
- show enum rate
- show enum rate config-name
- show enum rate server-ip-addr

*The **show sipd agents** command is associated with the **session-agent** HDR Group, and the **show sipd realms** command is associated with the **session-realm** HDR Group (in the section **MIB-Associated Groups and Group Statistics**). The **show sipd realm** command is also associated with the registration-realm HDR Group in the section, **ACLI-Associated Groups and Group Statistics**.

show sipd sessions

The **show sipd sessions** command displays information about SIP session transactions on the SBC. These statistics include session information over Period and Lifetime monitoring spans, as well as information on active sessions. For associated HDR Group and Group Statistics, see **sip-sessions**.

```
ACMEPACKET> show sipd sessions
09:40:09-105
SIP Session Status         -- Period -- -------- Lifetime --------
                 Active    High   Total       Total  PerMax    High
Sessions             10      10      10          65      10      55
  Initial            10      30      40          65      50       5
  Early              20      10      30          65      45      10
  Established        15      10      25          60      30      35
  Terminated          3       0       3           5      10      10
Dialogs              10       3      13          45      20      30
  Early               7       8      15          47      25      25
  Confirmed          15       0      15          60      40      10
  Terminated          4       0       4          45      25      20
```

Parameter	Description
Sessions	Number of sessions established by INVITE and SUBSCRIBE messages
Initial	Number of sessions for which an INVITE or SUBSCRIBE is being forwarded.
Early	Number of sessions for which the first provisional response (1xx other than 100) is received.
Established	Number of sessions for which a success (2xx) response is received.
Terminated	Number of sessions for which the session is ended by receiving or sending a BYE for an “Established” session or forwarding an error response for an “Initial” or “Early” session. The session remains in the Terminated state until all the resources for the session are freed.
Dialogs	Number of end-to-end SIP signaling connections.
Early	Number of dialogs created by a provisional response.
Confirmed	Number of dialogs created by a success response. An “Early” dialog transitions to Confirmed when a success response is received.
Terminated	Number of dialogs that ended by receiving/sending a BYE for an “Established” session or receiving/sending error response “Early” dialog. The dialog remains in the Terminated state until all the resources for the session are freed.

show sipd agents

The **show sipd agents** command displays statistics related to defined SIP session agents. SIP session agents can be softswitches, SIP proxies, application servers, SIP gateways, or SIP endpoints.

In addition to functioning as a single logical next hop for a signaling message (for example, where a SIP INVITE is forwarded), session agents can provide information about next or previous hops for packets in a SIP agent, including providing a list of equivalent next hops.

Entering this show command without arguments, list all SIP session agents. By adding the IP address or hostname of a session agent as well as a specified method at the end of the command, you can display statistics for that specific session agent and method. For associated HDR Group and Group Statistics, see **Group: session-agent**.

Show sipd agents Command

```
ACMEPACKET> show sipd agents
11:44:S1-49 (recent)
```

```
                 ------Inbound------ ---- Outbound ---- -- Latency --   Max
Session Agent    Active  Rate  Confix Active  Rate Confix   Avg   Max   Burst
session—agent1   I    0   0.0      0      0   0.0     0 0.000 0.000       0
session—agent2   I    0   0.0      0      0   0.0     0 0.000 0.000       0
```

Parameter	Description
Session Agent	Host name of the session agent in Fully Qualified Domain Name (FQDN) or IP Address format (softswitch, SIP proxy, application server, SIP gateway or SIP endpoint).
Inbound	
Active	Total number of current, active inbound sessions sent to the session agent.
Rate	Average rate of inbound session invitations (per second) sent to the session agent.
ConEx	Number of times that signaling & bandwidth constraints for inbound packets sent to the session agent were exceeded on the session agent. This helps determine resource availability.
Outbound	
Active	Total number of current, active outbound sessions sent to the session agent.
Rate	Average rate of outbound session invitations (per second) sent to the session agent.
ConEx	Number of times that signaling & bandwidth constraints for outbound packets were exceeded on the session agent. This helps determine resource availability.
Latency	
Avg	Average amount of time between the moment the session-agent transmits a SIP packet and the moment it reaches its destination.
Max	Maximum amount of time between the moment the session-agent transmits a SIP packet and the moment it reaches its destination.
Max Burst	Maximum burst rate for each session agent as total number of session invitations sent to or received from the session agent within the amount of time configured for the burst-rate window.

Show sipd agents <IP address or hostname> Command

```
AcmePacket> show sipd agents session—agent1
12:11:17-51
Session Agent session-agent1(public) [In Service]
                         ------ Period -----  ----- Lifetime -----
                         Active  High  Total   Total  PerMax  High
Inbound Sessions              0     0      0       0       0     0
Rate Exceeded                 -     -      0       0       0     -
Num Exceeded                  -     -      0       0       0     -
Burst Rate                    0     0      0       0       0     0
Reg Rate Exceeded             -     -      0       0       0     -
Outbound Sessions             0     1     11      11      11     1
Rate Exceeded                 -     0      0       0       0     -
Num Exceeded                  -     -      0       0       0     -
Burst Rate                    0    11      0       0       0    11
Reg Rate Exceeded             -     -      0       0       0     -
Out of Service                -     -      0       0       0     -
Trans Timeout                 0     0      0       0       0     0
Requests Sent                 -     -      0       0       0     -
Requests Complete             -     -      0       0       0     -
Seizure                       -     -      0       0       0     -
```

```
Answer                          -      -       0        0        0      -
ASR Exceeded                    -      -       0        0        0      -
Messages Received               -      -      30       30       30      -
Latency=0.000: max=0.000
```

Parameter	Description
Inbound Sessions	Number of inbound SIP sessions for this session agent.
Rate Exceeded	Number of times session rate was exceeded for inbound SIP sessions on this session agent.
Num Exceeded	Number of times that signaling & bandwidth constraints for inbound SIP sessions were exceeded on this session agent. This helps determine resource availability.
Burst Rate	Number of times burst rate was exceeded for this session agent on inbound SIP sessions.
Reg Rate Exceeded	Number of times the registration rate was exceeded for this session agent on inbound SIP sessions.
Outbound Sessions	Number of outbound SIP sessions for this session agent.
Rate Exceeded	Number of times session rate was exceeded for outbound SIP sessions.
Num Exceeded	Number of times time constraints were exceeded for outbound SIP sessions.
Burst Rate	Maximum burst rate of traffic (both inbound and outbound).
Reg Rate Exceeded	Number of times the registration rate was exceeded for this session agent on outbound SIP sessions.
Out of Service	Number of times this session agent went out of service.
Trans Timeout	Number of SIP transactions that timed out for this session agent.
Requests Sent	Number of SIP requests sent via this session agent.
Requests Complete	Number of SIP requests completed for this session agent.
Seizure	Number of seizures that occurred on this session agent.
Answer	Number of answered SIP sessions on this session agent.
ASR Exceeded	Number of times that Access Service Requests (ASRs) were exceeded on this session agent.
Messages Received	Number of SIP messages received by this session agent.
Latency	Average and maximum amount of time between the moment the session-agent transmits a SIP packet and the moment it reaches its destination.

show sipd acls

An access control list (ACL) allows/denies specific sources (IP or IP:port) to access the SBC.

The **show sipd acls** command displays information about SIP ACL activity on the SBC. These statistics include ACL information over Period and Lifetime monitoring spans, as well as information on active ACL status. For associated HDR Group and Group Statistics, see **sip-acl-oper** and **sip-acl-status**.

```
ACMEPACKET> show sipd acls
09:12:04-120
SIP ACL Status              -- Period -- -------- Lifetime --------
                  Active    High   Total      Total  PerMax    High
Total Entries          0       0       0          0       0       0
Trusted                0       0       0          0       0       0
```

```
Blocked                0        0        0           0        0        0
Blocked NATs           0        0        0           0        0        0

ACL Operations                    ---- Lifetime ----
                         Recent       Total  PerMax
ACL Requests                  0           0       0
Bad Messages                  0           0       0
Promotions                    0           0       0
Demotions                     0           0       0
Trust->Untrust                0           0       0
Untrust->Deny                 0           0       0
```

Parameter	Description
SIP ACL Status	
Total Entries	Total number of ACL entries, both trusted and blocked.
Trusted	Number of trusted ACL entries
Blocked	Number of blocked ACL entries
ACL Operations	
ACL Requests	Number of ACL requests
Bad Messages	Number of bad messages
Promotions	Total number of ACL entry promotions. These are the ACL entries that have been promoted from untrusted to trusted status.
Demotions	Number of ACL entry demotions.
Trust->Untrust	Number of ACL entries demoted from trusted to untrusted
Untrust->Deny	Number of ACL entries demoted from untrusted to deny

show sipd client

A SIP client can initiate and terminate SIP sessions. The **show sipd client** command displays statistics for SIP client events when the SBC is acting as a SIP client in its back-to-back User Agent (B2BUA) role. These statistics include SIP client information over Period and Lifetime monitoring spans, as well as information on active SIP client status. For associated HDR Group and Group Statistics, see **sip-client**.

```
ACMEPACKET> show sipd client
09:28:15-191
SIP Client Trans           -- Period -- -------- Lifetime --------
                  Active    High   Total      Total  PerMax    High
All States             0       0       0          0       0       0
<Initial>              0       0       0          0       0       0
<Trying>               0       0       0          0       0       0
<Calling>              0       0       0          0       0       0
<Proceeding>           0       0       0          0       0       0
<Cancelled>            0       0       0          0       0       0
<EarlyMedia>           0       0       0          0       0       0
<Completed>            0       0       0          0       0       0
<SetMedia>             0       0       0          0       0       0
<Established>          0       0       0          0       0       0
<Terminated>           0       0       0          0       0       0
```

Parameter	Description
All States	Number of all client session transactions
Initial	Number of times the Initial state was entered due to the receipt of a request

Parameter	Description
Trying	Number of times the Trying state was entered due to the receipt of a request
Calling	Number of times the Calling state was entered due to the receipt of an INVITE request
Proceeding	Number of times the “Proceeding” state was entered due to the receipt of a provisional response while in the Calling state
Cancelled	Number of INVITE transactions that received a CANCEL
EarlyMedia	Number of times the “Proceeding” state was entered due to the receipt of a provisional response that contained a Session Description Protocol (SDP) while in the Calling state
Completed	Number of times that the “Completed” state was entered due to the receipt of a status code in the range of 300-699 when either in the “Calling” or Proceeding state
SetMedia	Number of transactions in which the SBC was setting up NAT and steering ports
Established	Number of times the client received a 2xx response to an INVITE, but could not forward it because the NAT and steering port information was missing
Terminated	Number of times the Terminated state was entered after a 2xx message

show sipd server

A SIP server can receive and terminate SIP sessions. The **show sipd server** command displays statistics for SIP server events when the SBC is acting as a SIP server in its back-to-back User Agent (B2BUA) role. These statistics include SIP server information over Period and Lifetime monitoring spans, as well as information on active SIP server status. For associated HDR Group and Group Statistics, see **sip-server**.

```
ACMEPACKET> show sipd server
09:39:22-158
SIP Server Trans            -- Period -- -------- Lifetime --------
                  Active    High   Total       Total  PerMax    High
All States             0       0       0           0       0       0
<Initial>              0       0       0           0       0       0
<Queued>               0       0       0           0       0       0
<Trying>               0       0       0           0       0       0
<Proceeding>           0       0       0           0       0       0
<Cancelled>            0       0       0           0       0       0
<Established>          0       0       0           0       0       0
<Completed>            0       0       0           0       0       0
<Confirmed>            0       0       0           0       0       0
<Terminated>           0       0       0           0       0       0
```

Parameter	Description
All States	Number of all server session transactions
Initial	Number of times the Initial state was entered due to the receipt of a request
Queued	Number of times the Queued state was entered due to the receipt of a request
Trying	Number of times the Trying state was entered due to the receipt of a request
Proceeding	Number of times the “Proceeding” state was entered due to the receipt of a provisional response while in the Calling state
Cancelled	Number of INVITE transactions that received a CANCEL

Parameter	Description
Established	Number of times the server received a 2xx response to an INVITE, but could not forward it because the NAT and steering port information was missing
Completed	Number of times that the “Completed” state was entered due to the receipt of a status code in the range of 300-699 when either in the “Calling” or Proceeding state
Confirmed	Number of times that an ACK was received while the server was in “Completed” state, and then transitioned to the Confirmed state
Terminated	Number of times the Terminated state was entered after a 2xx message, or never received an ACK in the “Completed” state, and then transitioned to the Terminated state.

show sipd policy

Multistage local policy routing enables the SBC to perform multiple stages of route lookups where the result from one stage is used as the lookup key for the next routing stage.

The **show sipd policy** command displays single and multistage local policy lookups. All counters are reported for the recent, lifetime total, and lifetime maximum periods. For associated HDR Group and Group Statistics, see **sip-policy**.

```
ACMEPACKET> show sipd policy
09:38:43-118
SIP Policy/Routing            ---- Lifetime ----
                        Recent      Total  PerMax
Local Policy Lookups         0          0       0
Local Policy Hits            0          0       0
Local Policy Misses          0          0       0
Local Policy Drops           0          0       0
Agent Group Hits             0          0       0
Agent Group Misses           0          0       0
No Routes Found              0          0       0
Missing Dialog               0          0       0
Inb SA Constraints           0          0       0
Outb SA Constraints          0          0       0
Inb REG SA Constraint        0          0       0
Out REG SA Constraint        0          0       0
Requests Challenged          0          0       0
Challenge Found              0          0       0
Challenge Not Found          0          0       0
Challenge Dropped            0          0       0
Local Policy Inits           0          0       0
Local Policy Results         0          0       0
Local Policy Exceeded        0          0       0
Local Policy Loops           0          0       0
```

Parameter	Description
Local Policy Lookups	Number of local policy lookups
Local Policy Hits	Number of successful local policy lookups
Local Policy Misses	Number of local policy lookup failures
Local Policy Drops	Number of local policy lookups where the next hop session agent group is H.323
Agent Group Hits	Number of successful local policy lookups for session agent groups
Agent Group Misses	Number of successful local policy lookups where no session agent was available for the session agent group

Parameter	Description
No Routes Found	Number of successful local policy lookups, but temporarily unable to route (for example, session agent out of service)
Missing Dialog	Number of local policy lookups where the dialog was not found for a request addressed to the SBC with a To tag or for a NOTIFY-SUBSCRIBE SIP request
Inb SA Constraints	Number of successful local policy lookups where the inbound session agent (SA) exceeded constraints
Outb SA Constraints	Number of successful local policy lookups where the outbound SA exceeded constraints
Inb REG SA Constraint	Number of successful inbound local policy lookups where the registrar (REG) SA exceeded constraints
Outb REG SA Constraint	Number of successful outbound local policy lookups where the registrar (REG) SA exceeded constraints
Request Challenged	Number of requests that were challenged.
Challenge Found	Number of challenges found.
Challenge Not Found	Number of challenges not found.
Challenge Dropped	Number of challenges dropped.
Local Policy Inits	Number of times the SBC made an initial local policy lookup
Local Policy Results	Number of times the SBC truncated the number of routes returned for a local policy lookup because the maximum number of routes per local policy lookup (max local policy lookups routes per lookup) threshold was reached.
Local Policy Exceeded	Number of times the SBC truncated the number of routes returned for a local policy lookup because the maximum number of routes per message request (total local policy routes) threshold was reached.
Local Policy Loops	Number of times the SBC detected a loop while performing a multistage local policy lookup

show sipd errors

The **show sipd errors** command displays statistics for SIP media event errors. These statistics are errors encountered by the SIP application in processing SIP media sessions, dialogs, and session descriptions (SDP). Error statistics display for the lifetime monitoring span only. For associated HDR Group and Group Statistics, see **sip-errors**.

```
ACMEPACKET> show sipd errors
09:31:49-105
SIP Errors/Events             ---- Lifetime ----
                       Recent      Total  PerMax
SDP Offer Errors            0          0       0
SDP Answer Errors           0          0       0
Drop Media Errors           0          0       0
Transaction Errors          0          0       0
Application Errors          0          0       0
Media Exp Events            0          0       0
Early Media Exps            0          0       0
Exp Media Drops             0          0       0
Expired Sessions            0          0       0
Multiple OK Drops           0          0       0
Multiple OK Terms           0          0       0
Media Failure Drops         0          0       0
Non-ACK 2xx Drops           0          0       0
```

```
Invalid Requests            0          0       0
Invalid Responses           0          0       0
Invalid Messages            0          0       0
CAC Session Drop            0          0       0
Nsep User Exceeded          0          0       0
Nsep SA Exceeded            0          0       0
CAC BW Drop                 0          0       0
```

Parameter	Description
SDP Offer Errors	Number of errors encountered in setting up the media session for a session description in a SIP request or response which is a Session Description Protocol (SDP) Offer in the Offer/Answer model (RFC 3264)
SDP Answer Errors	Number of errors encountered in setting up the media session for a session description in a SIP request or response which is a Session Description Protocol (SDP) Answer in the Offer/Answer model (RFC 3264)
Drop Media Errors	Number of errors encountered in tearing down the media for a dialog or session that is being terminated due to: a) non-successful response to an INVITE transaction, or b) a BYE transaction received from one of the participants in a dialog/session, or c) a BYE initiated by the SBC due to a timeout notification from the Middlebox Control Daemon (MBCD).
Transaction Errors	Number of errors in continuing the processing of the SIP client transaction associated with setting up or tearing down of the media session.
Application Errors	Number of miscellaneous errors in the SIP application that are otherwise uncategorized
Media Exp Events	Number of flow timer expiration notifications received from the Middlebox Control Daemon (MBCD).
Early Media Exps	Number of flow timer expiration notifications received for media sessions that were not completely set up due to an incomplete or pending INVITE transaction
Exp Media Drops	Number of flow timer expiration notifications from the Middlebox Control Daemon (MBCD) that resulted in the termination of the dialog/session by the SIP application.
Expired Sessions	Number of sessions terminated due to the session timer expiring
Multiple OK Drops	Number of dialogs terminated upon reception of a 200 OK response from multiple User Agent Servers (UASs) for a given INVITE transaction that was forked by a downstream proxy
Multiple OK Terms	Number of dialogs terminated upon reception of a 200 OK response that conflicts with an existing established dialog on the SBC
Media Failure Drops	Number of dialogs terminated due to a failure in establishing the media session.
Non-Ack 2xx Drops	Number of sessions terminated because an ACK was not received for a 2xx response
Invalid Requests	Number of invalid requests (for example, an unsupported header was received).
Invalid Responses	Number of invalid responses (for example, no Via header in response)
Invalid Messages	Number of messages dropped due to parse failure
CAC Session Drop	Number of call admission control (CAC) session setup failures

Parameter	Description
CAC BW Drop	Number of call admission control (CAC) session setup failures due to insufficient bandwidth (BW)
Nsep User Exceeded	Number of Emergency Telecommunications Service (ETS), user call sessions that exceeded the calls-per-second rate configured on the SBC for National Security and Emergency Preparedness (NSEP).
Nsep SA Exceeded	Number of Emergency Telecommunications Service (ETS), Session Agent (SA) call sessions that exceeded the calls-per-second rate configured on the SBC for National Security and Emergency Preparedness (NSEP).

show sipd status

The **show sipd status** command displays information about Session Initiation Protocol (SIP) transactions. These statistics are given for the Period and Lifetime monitoring spans. This display also provides statistics related to SIP media events. These statistics include SIP status information over Period and Lifetime monitoring spans, as well as information on active SIP status. For associated HDR Group and Group Statistics, see **sip-status**.

```
ACMEPACKET> show sipd status
09:41:00-156
SIP Status                 -- Period -- -------- Lifetime --------
                  Active     High   Total       Total  PerMax     High
Sessions               0        0       0           0       0        0
Subscriptions          0        0       0           0       0        0
Dialogs                0        0       0           0       0        0
CallID Map             0        0       0           0       0        0
Rejections             -        -       0           0       0
ReINVITEs              -        -       0           0       0
ReINV Suppress         -        -       0           0       0
Media Sessions         0        0       0           0       0        0
Media Pending          0        0       0           0       0        0
Client Trans           0        0       0           0       0        0
Server Trans           0        0       0           0       0        0
Resp Contexts          0        0       0           0       0        0
Saved Contexts         0        0       0           0       0        0
Sockets                0        0       0           0       0        0
Req Dropped            -        -       0           0       0
DNS Trans              0        0       0           0       0        0
DNS Sockets            0        0       0           0       0        0
DNS Results            0        0       0           0       0        0
Rejected Msgs          0        0       0           0       0        0

Session Rate = 0.0
Load Rate = 0.0
Remaining Connections = 200000 (max 200000)
```

Parameter	Description
Sessions	Number of sessions established by INVITE and SUBSCRIBE messages
Subscriptions	Number of sessions established by SUBSCRIPTION
Dialogs	Number of end-to-end SIP signaling connections
CallID Map	Number of successful session header Call ID mappings
Rejections	Number of rejected INVITEs
ReINVITEs	Number of ReINVITEs
ReINV Suppress	Number of ReINVITEs that were suppressed

Parameter	Description
Media Sessions	Number of successful media sessions
Media Pending	Number of media sessions waiting to be established
Client Trans	Number of client transactions
Server Trans	Number of server transactions that have taken place on the SBC
Resp Contexts	Number of response contexts
Saved Contexts	Number of saved contexts
Sockets	Number of SIP sockets
Req Dropped	Number of dropped requests
DNS Trans	Number of Domain Name System (DNS) transactions
DNS Sockets	Number of Domain Name System (DNS) sockets
DNS Results	Number of Domain Name System (DNS) results
Rejected Msgs	Number of rejected messages
Session Rate	The rate, per second, of SIP invites allowed to or from the SBC during the sliding window period. The rate is computed every 10 seconds .
Load Rate	Average Central Processing Unit (CPU) utilization of the SBC during the current window. The average is computed every 10 seconds unless the load-limit is configured in the SIPConfig record, in which case it is 5 seconds.
Remaining Connections	Number of SIP connections currently available

show sipd invite

The **show sipd invite** command displays information about Session Initiation Protocol (SIP) INVITE requests. These statistics are given for both Server and Client and display recent, per maximum, and total for each. For associated HDR Group and Group Statistics, see **sip-invites**.

```
ACMEPACKET> show sipd invite
09:05:20-106
INVTTE (20:O2:28-127)
                      ------ Server -------  ------ Client -------
Message/Event        Recent  Total  PerMax  Recent  Total  PerMax
                     ------  -----  ------  ------  -----  ------
INVITE Requests           0      0       0       0      0       0
Retransmissions           0      0       0       0      0       0
Response Retrans          0      0       0       0      0       0
Transaction Timeouts      -      -       -       0      0       0
Locally Throttled         -      -       -       0      0       0

Avg Latency=0.000 for 0
Max Latency=0.000
```

Parameter	Description
INVITE Requests	Number of INVITE requests
Retransmissions	Number of retransmissions of INVITEs
Response Retrans	Number of response retransmissions
Transaction Timeouts	Number of INVITE request transaction timeouts

Parameter	Description
Locally Throttled	Number of INVITE requests locally throttled
Avg Latency	Average latency of traffic flow for inbound and outbound packets
Max Latency	Maximum latency of traffic flow for inbound and outbound packets.

show sipd realms

Realms are a logical distinction representing routes (or groups of routes) reachable by the SBC and what kinds of resources and special functions apply to those routes. Realms are used as a basis for determining ingress and egress associations to network interfaces, which can reside in different VPNs. The ingress realm is determined by the signaling interface on which traffic arrives. The egress realm is determined by the following:

- Routing policy - Where the egress realm is determined in the session agent configuration or external address of a SIP-NAT
- Realm-bridging - As applied in the SIP-NAT configuration and H.323 stack configurations
- Third-party routing/redirect (i.e., SIP redirect or H.323 LCF) 170

Realms can also be nested in order to form nested realm groups. Nested realms consist of separate realms that are arranged within a hierarchy to support network architectures that have separate backbone networks and VPNs for signaling and media.

The **show sipd realms** command displays information about sessions (both inbound and outbound), out of service sessions, early and successful sessions, and session registration information for realms. This information displays for Period and Lifetime monitoring spans, as well as for active sessions. For associated HDR Group and Group Statistics, see the **session-realm**, and **registration-realm**.

Note: The following example shows the statistics for the realm name of public.

```
ACMEPACKET> show sipd realms public
15:23:54-47
Realm access() [In Service]
                          -- Period --  ------ Lifetime -----
                    Active  High   Total  Total    PerMax  High

Inbound Sessions         0     0       0      0         0     0
  Rate Exceeded          -     -       0      0         0     0
  Num Exceeded           -     -       0      0         0     0
  Burst Rate             0     0       0      0         0     0
  Reg Rate Exceeded      0     0       0      0         0     0
  Reg Burst Rate         0     0       0      0         0     0
Outbound Sessions        0     0       0      0         0     0
  Rate Exceeded          -     -       0      0         0     0
  Num Exceeded           -     -       0      0         0     0
  Burst Rate             0     0       0      0         0     0
  Reg Rate Exceeded      0     0       0      0         0     0
Local Contacts           2     2       0      0         2     2
HNT Entries              0     0       0      0         0     0
Non—HNT Entries          2     2       0      0         2     2
Subscriptions            0    42      23    112        48    48
Out of Service           0     0       0      0         0     0
Trans Timeout            0     0       0      0         0     0
Requests Sent            -     -      46    222        96     -
Requests Complete        -     -       0      0         0     -
Seizure                  -     -       0      0         0     -
Answer                   -     -       0      0         0     -
  ASR Exceeded           -     -       0      0         0     -
Requests Received        -     -      46    226        96     -
QoS Major Exceeded       -     -       0      0         0     -
QoS Critical Exceeded    -     -       0      0         0     -
```

Parameter	Description
Inbound Sessions	Total number of active inbound sessions during an Active and Lifetime period.
Rate Exceeded	Number of times session rate was exceeded for inbound SIP sessions on this realm.
Num Exceeded	Number of times time constraints were exceeded for inbound sessions.
Burst Rate	Number of times burst rate was exceeded for this realm on inbound SIP sessions.
Reg Rate Exceeded	Number of times the registration rate was exceeded for this realm on inbound SIP sessions.
Reg Burst Rate	Number of times the registration burst rate was exceeded for this realm on inbound SIP sessions.
Outbound Sessions	Total number of active outbound sessions during an Active and Lifetime period.
Rate Exceeded	Number of times session rate was exceeded for outbound SIP sessions on this realm.
Num Exceeded	Number of times time constraints were exceeded for outbound sessions.
Burst Rate	Number of times burst rate was exceeded for this realm on outbound SIP sessions.
Reg Rate Exceeded	Number of times the registration rate was exceeded for this realm on outbound SIP sessions.
Local Contacts	Number of contact entries in the registration cache.
HNT Entries	Number of hosted NAT traversal (HNT) contact entries that are behind a NAT device.
Non-HNT Entries	Number of contact entries that are not hosted NAT traversal that are behind a NAT device.
Subscriptions	Specifies the following: Active Subscriptions: The current global count of active SIP subscriptions during Survivability. Subscriptions PreMax: The maximum global count of SIP subscriptions initiated during any 100 second period since the last SBC re-boot, and during Survivability. Subscriptions High: The maximum global count of active SIP subscriptions since the last SBC re-boot, and during Survivability.
Out of Service	Number of times this realm went out of service.
Trans Timeout	Number of transactions timed out for this realm.
Requests Sent	Number of requests sent via this realm.
Requests Complete	Number of requests that have been completed for this realm.
Seizure	Number of seizures that occurred on this realm.
Answer	Number of answered SIP sessions on this session agent.
ASR Exceeded	Number of times that Access Service Requests (ASRs) were exceeded on this realm.
Requests Received	Number of requests received on this realm.

Parameter	Description
QoS Major Exceeded	Number of times the major Rfactor threshold was exceeded during the sliding window period. The peg count provides counts of calls with different service classes that occur during intervals of frequency which reliability indicate the traffic load. R-factors are metrics in VoIP that use a formula to determine a numeric expression of voice quality.
QoS Critical Exceeded	Number of times the critical Rfactor threshold was exceeded during the sliding window period. Provides counts of calls with different service classes that occur during intervals of frequency which reliability indicate the traffic load. R-factors are metrics in VoIP that use a formula to determine a numeric expression of voice quality.
Latency	
Avg	Average amount of time between the moment the realm transmits a SIP packet and the moment it reaches its destination.
Max	Maximum amount of time between the moment the realm transmits a SIP packet and the moment it reaches its destination.
QoS R-Factor	
Avg	Average Quality of Service (QoS) factor observed during the current window period. Quality of service shapes traffic to provide different priority and level of performance to different data flows. R-factors are metrics in VoIP, that use a formula to take into account both user perceptions and the cumulative effect of equipment impairments to arrive at a numeric expression of voice quality. This statistic defines the call or transmission quality expressed as an R factor.
Max	Maximum Quality of Service (QoS) factor observed during the sliding window period. Quality of service shapes traffic to provide different priority and level of performance to different data flows. R-factors are metrics in VoIP that use a formula to determine a numeric expression of voice quality. This statistic defines the call or transmission quality expressed as an R factor.
Early Sessions	Indicates the number of early sessions for each realm. Each time the SBC receives an INVITE on the ingress realm or the egress realm sends an INVITE request, a counter increments if the session is established with a 200 OK response. This counter also increments in sessions when there are no 18x responses (Ringing (180), Call is Being Forwarded (181), Queued (182), Session in Progress (183)), but a 200 OK is established. This counter represents the number of sessions that have reached the early dialog state or later.
Successful Sessions	Indicates the number of successful sessions for each realm. Successful sessions are when the SBC receives a successful 200 OK response from an initial INVITE request. Note: This counter is NOT incremented for re-INVITES.
Initial Registrations	
Total	Total number of initial registrations. This counter is incremented once for each initial REGISTER message even when the REGISTER is challenged. This counter is based on ingress (received) messages only. Note: This counter is not incremented when registrations are challenged by the following response messages: 401 (Unauthorized - user authentication required)

Parameter	Description
	407 (Proxy authentication required) 423 (Interval too brief - expiration time of the resource is too short)
Successful	Number of successful initial registrations. This counter is incremented once for each successful initial registration with a 200 OK response. This counter is based on ingress (received) messages only.
Unsuccessful	Number of unsuccessful initial registrations. This counter is incremented once for each unsuccessful initial registration when the response to the initial REGISTER has a non-success status code. This counter is based on ingress (received) messages only. Note: This counter is not incremented when registrations are challenged by the following response messages: 401 (Unauthorized - user authentication required) 407 (Proxy authentication required) 423 (Interval too brief - expiration time of the resource is too short)
Refresh Registrations	
Total	Total number of registrations that were refreshed. This counter is incremented once for every refresh registration. This counter is based on ingress (received) messages only.
Successful	Total number of registrations that were successfully refreshed. This counter is incremented once for each successful refresh registration. This counter is based on ingress (received) messages only.
Unsuccessful	Total number of registrations that were unsuccessfully refreshed. This counter is incremented once for each unsuccessful refresh registration. This counter is based on ingress (received) messages only.
De-Registrations	
Total	Total number of registrations that de-registered. This counter is incremented once for every de-registration. This counter is based on ingress (received) messages only. In the event a de-registration message is received on a realm that is different than that of the initial registration message, the de-registration counter for the ingress realm of that de-registration message is incremented.
Successful	Total number of registrations that successfully de-registered. This counter is incremented once for each successful de-registration. This counter is based on ingress (received) messages only. In the event a successful de-registration message is received on a realm that is different than that of the initial registration message, the de-registration counter for the ingress realm of that successful de-registration message is incremented.
Unsuccessful	Total number of registrations that unsuccessfully de-registered. This counter is incremented once for each unsuccessful de-registration. This counter is based on ingress (received) messages only. In the event an unsuccessful de-registration message is received on a realm that is different than that of the initial registration message, the de-registration counter for the ingress realm of that unsuccessful de-registration message is incremented.

show enum

Telephone Number Mapping (ENUM) is an IETF standard (RFC 2916) for mapping the public telephone number address space into the Domain Name System (DNS). It links a phone number to an Internet address that is published in the DNS system. This allows a number to be reachable anywhere via the best and cheapest route.

The **show enum** command displays information about the ENUM Agent. These statistics provide current information only. For associated HDR Group and Group Statistics, see **enum-stats**.

```
ACMEPACKET> show enum
09:05:20-106

            ---Queries--- --Successful-- --NotFound--- --Timed Out--
ENUM Agent  Current Total Current  Total Current Total Current Total
```

Parameter	Description
Enum Agent	Name of the ENUM Agent on the SBC.
Queries Total	Number of ENUM queries
Successful Total	Number of successful ENUM queries
Not Found Total	Number of ENUM queries returning a not found
Times Out Total	Number of ENUM query timeouts

show mgcp

The Media Gateway Control Protocol (MGCP) is an implementation of the MGCP architecture for controlling media gateways on Internet Protocol (IP) networks and the Public Switched Telephone Network (PSTN). It is used to establish, maintain, and terminate calls between two or more endpoints. The SBC provides MGCP/Network Call Signaling (NCS) Application Layer Gateway (ALG) functionality for MGCP/NCS messages between media gateways and media gateway controllers.

The **show mgcp** command displays information about MGCP. These statistics include MGCP information over Period and Lifetime monitoring spans, as well as information on active MGCP status. For associated HDR Group and Group Statistics, see **mgcp-state** and **mgcp-trans**.

Note: MGCP Transaction displays recent Lifetime monitoring information ONLY.

```
ACMEPACKET> show mgcp
08:59:19-155
State                    -- Period -- -------- Lifetime --------
                 Active    High   Total       Total  PerMax    High
MGCP Sessions         0       0       0           0       0       0
CA Endpoints          0       0       0           0       0       0
GW Endpoints          0       0       0           0       0       0
Media Sessions        0       0       0           0       0       0
Client Trans          0       0       0           0       0       0
Server Trans          0       0       0           0       0       0
Pending MBCD          0       0       0           0       0       0
MGCP ALGs             0       0       0           0       0       0
Free Map Ports        0       0       0           0       0       0
Used Map Ports        0       0       0           0       0       0
                    --------- Gateway --------- ------- Call Agent --------
MGCP Transactions           ---- Lifetime ----          ---- Lifetime ----
                     Recent      Total  PerMax   Recent      Total  PerMax
Requests received         0          0       0       0          0       0
Responses sent            0          0       0       0          0       0
Duplicates received       0          0       0       0          0       0
Requests sent             0          0       0       0          0       0
```

```
Responses received          0          0       0       0          0       0
Retransmissions sent        0          0       0       0          0       0
```

Parameter	Description
State	
MGCP Sessions	Number of MGCP sessions
CA Endpoints	Number of call agent (CA) endpoints
GW Endpoints	Number of gateway (GW) endpoints
Media Sessions	Number of media sessions
Client Trans	Number of client transactions
Server Trans	Number of server transactions
Pending MBCD	Number of pending media requests to the Middlebox Control Daemon (MBCD)
MGCP ALGs	Number of MGCP Application Layer Gateway (ALG) connections
Free Map Ports	Number of port maps (i.e., IP Ports) available
Used Map Ports	Number of port maps (i.e., IP Ports) allocated
MGCP Transactions	
Requests received	Number of requests received
Responses sent	Number of responses sent
Duplicates received	Number of duplicate requests received
Requests sent	Number of requests sent
Responses received	Number of responses received
Retransmissions sent	Number of retransmissions sent

show mgcp errors

The Media Gateway Control Protocol (MGCP) is an implementation of the MGCP architecture for controlling media gateways on Internet Protocol (IP) networks and the Public Switched Telephone Network (PSTN). It is used to establish, maintain, and terminate calls between two or more endpoints. The SBC provides MGCP/Network Call Signaling (NCS) Application Layer Gateway (ALG) functionality for MGCP/NCS messages between media gateways and media gateway controllers.

The **show mgcp errors** command displays information about MGCP media event errors. These statistics include MGCP error information over Lifetime monitoring spans only. For associated HDR Group and Group Statistics, see **mgcp-media-events**.

```
ACMEPACKET> show mgcp errors
09:04:02-138
MGCP Media Events              ---- Lifetime ----
                        Recent      Total  PerMax
Calling SDP Errors           0          0       0
Called SDP Errors            0          0       0
Drop Media Errors            0          0       0
Transaction Errors           0          0       0
Application Errors           0          0       0
Media Exp Events             0          0       0
Early Media Exps             0          0       0
Exp Media Drops              0          0       0
```

Parameter	Description
Calling SDP Errors	Number of errors encountered in setting up the media session for a session description in a Request or Response which is a Session Description Protocol (SDP) Offer in the Offer/Answer model (RFC 3264)
Called SDP Errors	Number of errors encountered in setting up the media session for a session description in a Request or Response which is a Session Description Protocol (SDP) Answer in the Offer/Answer model (RFC 3264)
Drop Media Errors	Number of errors encountered in tearing down the media for a session that is being terminated
Transaction Errors	Number of errors in continuing the processing of the client transaction associated with the setting up or tearing down of the media session
Application Errors	Number of miscellaneous errors that are otherwise uncategorized
Media Exp Events	Number of flow timer expiration notifications received from Middlebox Control Daemon (MBCD).
Early Media Exps	Number of flow timer expiration notifications received for media sessions that have not been completely set up
Exp Media Drops	Number of flow timer expiration notifications from the Middlebox Control Daemon (MBCD) that resulted in the termination of the session

show mgcp acls

The Media Gateway Control Protocol (MGCP) is an implementation of the MGCP architecture for controlling media gateways on Internet Protocol (IP) networks and the Public Switched Telephone Network (PSTN). It is used to establish, maintain, and terminate calls between two or more endpoints. The SBC provides MGCP/Network Call Signaling (NCS) Application Layer Gateway (ALG) functionality for MGCP/NCS messages between media gateways and media gateway controllers.

The **show mgcp acls** command displays information about MGCP access control lists (ACLs). These statistics include MGCP ACL information over Period and Lifetime monitoring spans, as well as information on active MGCP ACL status. For associated HDR Group and Group Statistics, see **mgcp-acl**.

Note: ACL Operations displays recent Lifetime monitoring information ONLY.

```
ACMEPACKET> show mgcp acls
09:02:01-117
MGCP ACL Status           -- Period -- -------- Lifetime --------
                Active    High   Total      Total  PerMax    High
Total Entries        0       0       0          0       0       0
Trusted              0       0       0          0       0       0
Blocked              0       0       0          0       0       0

ACL Operations         ---- Lifetime ----
                Recent      Total  PerMax
ACL Requests         0          0       0
Bad Messages         0          0       0
Promotions           0          0       0
Demotions            0          0       0
Trust->Untrust       0          0       0
Untrust->Deny        0          0       0
```

Parameter	Description
MGCP ACL Status	

Parameter	Description
Total Entries	Total number of Access Control List (ACL) entries, both trusted and blocked
Trusted	Number of trusted ACL entries
Blocked	Number of blocked ACL entries
ACL Operations	
ACL Requests	Number of ACL requests
Bad Messages	Number of bad messages
Promotions	Number of ACL entry promotions. These are the ACL entries that have been promoted from untrusted to trusted status
Demotions	Number of ACL entry demotions. These are the ACL entries that have been demoted from trusted to untrusted.
Trust->Untrust	Number of ACL entries demoted from trusted to untrusted
Untrust->Deny	Number of ACL entries demoted from untrusted to deny

show h323

H.323 is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network. H.323 addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point calls. The SBC responds to and forwards H.323 signaling messages and sets up H.323 sessions based on the system configuration.

The **show h323** command displays information about H323 operations. These statistics include H323 information over Period and Lifetime monitoring spans, as well as information on active H323 status. For associated HDR Group and Group Statistics, see **h323-stats**.

Note: H323D Status displays recent Lifetime monitoring information ONLY.

```
ACMEPACKET> show h323

10:36:07—94
Session Stats         -- Period --    -------- Lifetime -------
                      Active  High    Total    Total PerMax High
Incoming Calls             0     0        0        0      0    0
Outgoing calls             0     0        0        0      0    0
Connected Calls            0     0        0        0      0    0
Incoming Channels          0     0        0        0      0    0
Outgoing Channels          0     0        0        0      0    0
Contexts                   0     0        0        0      0    0

H3230 status          Current   Lifetime
Queued Messages             0          0
TPKT Channels               0          0
UDP Channels                0          0

Load Rate = 0.2
```

Parameter	Description
Session Stats	
Incoming Calls	Number of incoming H.323 calls
Outgoing Calls	Number of outgoing H.323 calls

Parameter	Description
Connected Calls	Number of connected calls
Incoming Channels	Number of established incoming calls
Outgoing Channels	Number of established outgoing channels
Contexts	Number of established H.323 contexts (or call terminations)
H323D Status	
Queued Messages	Number of messages queued
TPKT Channels	Number of ThroughPacket (TPKT) channels open(ed)
UDP Channels	Number of User Datagram Protocol (UDP) channels open(ed)
Load Rate	Total H323 current load rate, in seconds, on the SBC

show sipd rate

The show sipd rate command displays request and response rates for messages (per method) on a system-wide basis. The rates are calculated based on the time in the current monitoring window (100+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ACMEPACKET# show sipd rate
17:24:28-103
Method Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                Rate      Rate      Rate      Rate       Rate       Rate
INVITE           0.0       0.0       0.0       0.0        0.0        0.0
ACK              0.0       0.0       0.0       0.0        0.0        0.0
BYE              0.0       0.0       0.0       0.0        0.0        0.0
REGISTER         0.0       0.0       0.0       0.0        0.0        0.0
CANCEL           0.0       0.0       0.0       0.0        0.0        0.0
PRACK            0.0       0.0       0.0       0.0        0.0        0.0
OPTIONS          0.0       0.0       0.0       0.0        0.0        0.0
INFO             0.0       0.0       0.0       0.0        0.0        0.0
SUBSCRIBE        0.0       0.0       0.0       0.0        0.0        0.0
NOTIFY           0.0       0.0       0.0       0.0        0.0        0.0
REFER            0.0       0.0       0.0       0.0        0.0        0.0
UPDATE           0.0       0.0       0.0       0.0        0.0        0.0
MESSAGE          0.0       0.0       0.0       0.0        0.0        0.0
PUBLISH          0.0       0.0       0.0       0.0        0.0        0.0
OTHER            0.0       0.0       0.0       0.0        0.0        0.0
ALL              0.0       0.0       0.0       0.0        0.0        0.0
clank#
```

show sipd rate agent

The show sipd rate agent command displays request and response rates for messages (per method) for all session agents. By adding a session agent name in the form show sipd rate agent <session-agent-name>, you can view statistics for the identified agent only. The rates are calculated based on the time in the current monitoring window (30+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ACMEPACKET# show sipd rate agent 192.168.202.100
17:26:47-42
Session Agent 192.168.202.100
Method Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                Rate      Rate      Rate      Rate       Rate       Rate
INVITE           0.0       0.0       0.0       0.0        0.0        0.0
ACK              0.0       0.0       0.0       0.0        0.0        0.0
```

```
BYE                0.0        0.0        0.0        0.0        0.0        0.0
REGISTER           0.0        0.0        0.0        0.0        0.0        0.0
CANCEL             0.0        0.0        0.0        0.0        0.0        0.0
PRACK              0.0        0.0        0.0        0.0        0.0        0.0
OPTIONS            0.0        0.0        0.0        0.0        0.0        0.0
INFO               0.0        0.0        0.0        0.0        0.0        0.0
SUBSCRIBE          0.0        0.0        0.0        0.0        0.0        0.0
NOTIFY             0.0        0.0        0.0        0.0        0.0        0.0
REFER              0.0        0.0        0.0        0.0        0.0        0.0
UPDATE             0.0        0.0        0.0        0.0        0.0        0.0
MESSAGE            0.0        0.0        0.0        0.0        0.0        0.0
PUBLISH            0.0        0.0        0.0        0.0        0.0        0.0
OTHER              0.0        0.0        0.0        0.0        0.0        0.0
```

show sipd rate interface

The show sipd rate interface command displays request and response rates for messages (per method) for all configured sip-interfaces. The rates are calculated based on the time in the current monitoring window (30+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ACMEPACKET# show sipd rate interface
17:24:33-58
Sip Interface core
Method Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                Rate      Rate      Rate      Rate       Rate       Rate
INVITE           0.0       0.0       0.0       0.0        0.0        0.0
ACK              0.0       0.0       0.0       0.0        0.0        0.0
BYE              0.0       0.0       0.0       0.0        0.0        0.0
REGISTER         0.0       0.0       0.0       0.0        0.0        0.0
CANCEL           0.0       0.0       0.0       0.0        0.0        0.0
PRACK            0.0       0.0       0.0       0.0        0.0        0.0
OPTIONS          0.0       0.0       0.0       0.0        0.0        0.0
INFO             0.0       0.0       0.0       0.0        0.0        0.0
SUBSCRIBE        0.0       0.0       0.0       0.0        0.0        0.0
NOTIFY           0.0       0.0       0.0       0.0        0.0        0.0
REFER            0.0       0.0       0.0       0.0        0.0        0.0
UPDATE           0.0       0.0       0.0       0.0        0.0        0.0
MESSAGE          0.0       0.0       0.0       0.0        0.0        0.0
PUBLISH          0.0       0.0       0.0       0.0        0.0        0.0
OTHER            0.0       0.0       0.0       0.0        0.0        0.0
17:24:33-58
Sip Interface peer
Method Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                Rate      Rate      Rate      Rate       Rate       Rate
INVITE           0.0       0.0       0.0       0.0        0.0        0.0
ACK              0.0       0.0       0.0       0.0        0.0        0.0
BYE              0.0       0.0       0.0       0.0        0.0        0.0
REGISTER         0.0       0.0       0.0       0.0        0.0        0.0
CANCEL           0.0       0.0       0.0       0.0        0.0        0.0
PRACK            0.0       0.0       0.0       0.0        0.0        0.0
OPTIONS          0.0       0.0       0.0       0.0        0.0        0.0
INFO             0.0       0.0       0.0       0.0        0.0        0.0
SUBSCRIBE        0.0       0.0       0.0       0.0        0.0        0.0
NOTIFY           0.0       0.0       0.0       0.0        0.0        0.0
REFER            0.0       0.0       0.0       0.0        0.0        0.0
UPDATE           0.0       0.0       0.0       0.0        0.0        0.0
MESSAGE          0.0       0.0       0.0       0.0        0.0        0.0
PUBLISH          0.0       0.0       0.0       0.0        0.0        0.0
OTHER            0.0       0.0       0.0       0.0        0.0        0.0
```

By entering a configured interface, the ACLI displays aggregate statistics for that interface and then displays all Session Agents' counts configured on that SIP interface. Displays have been truncated below. For example:

```
ACMEPACKET# show sipd rate interface peer
17:24:40-34
Sip Interface peer
Method Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                Rate      Rate      Rate      Rate       Rate       Rate
INVITE           0.0       0.0       0.0       0.0        0.0        0.0
[...]
OTHER            0.0       0.0       0.0       0.0        0.0        0.0
clank#
```

```
____
Session Agent 172.16.202.102
Method Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                Rate      Rate      Rate      Rate       Rate       Rate
INVITE           0.0       0.0       0.0       0.0        0.0        0.0
ACK              0.0       0.0       0.0       0.0        0.0        0.0
BYE              0.0       0.0       0.0       0.0        0.0        0.0
REGISTER         0.0       0.0       0.0       0.0        0.0        0.0
CANCEL           0.0       0.0       0.0       0.0        0.0        0.0
PRACK            0.0       0.0       0.0       0.0        0.0        0.0
OPTIONS          0.0       0.0       0.0       0.0        0.0        0.0
INFO             0.0       0.0       0.0       0.0        0.0        0.0
SUBSCRIBE        0.0       0.0       0.0       0.0        0.0        0.0
NOTIFY           0.0       0.0       0.0       0.0        0.0        0.0
REFER            0.0       0.0       0.0       0.0        0.0        0.0
UPDATE           0.0       0.0       0.0       0.0        0.0        0.0
MESSAGE          0.0       0.0       0.0       0.0        0.0        0.0
PUBLISH          0.0       0.0       0.0       0.0        0.0        0.0
OTHER            0.0       0.0       0.0       0.0        0.0        0.0
17:26:21-46
Session Agent 192.168.202.100
Method Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                Rate      Rate      Rate      Rate       Rate       Rate
INVITE           0.0       0.0       0.0       0.0        0.0        0.0
[...]
OTHER            0.0       0.0       0.0       0.0        0.0        0.0
ACMEPACKET#
```

show dnsalg rate

The show dnsalg rate command displays request and response rates for DNS messages on a system-wide basis. The rates are calculated based on the time in the current monitoring window (100+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ACMEPACKET# show dnsalg rate
17:31:21-15
Realm-id  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
             Rate      Rate      Rate      Rate       Rate       Rate
ALL           0.0       0.0       0.0       0.0        0.0        0.0
```

show dnsalg rate realm-id

The show dnsalg rate realm-id command displays request and response rates for DNS messages on a per-realm basis. If you add a realm-name to the query, that specific realm's data will be returned. Entered without a realm name, all configured realms will be displayed. The rates are calculated based on the time in the current monitoring window (30+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ACMEPACKET# show dnsalg rate realm-id peer
17:31:31-26
Realm-id  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
             Rate      Rate      Rate      Rate       Rate       Rate
peer          0.0       0.0       0.0       0.0        0.0        0.0
```

show dnsalg rate server-ip-addr

The show dnsalg rate server-ip-addr command displays request and response rates for DNS messages on a per-DNS server basis. If you add a DNS Server IP address to the query, that specific server's data will be returned. Entered without a server IP address, all configured servers will be displayed. The rates are calculated based on the time in the current monitoring window (30+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ACMEPACKET# show dnsalg rate server-ip-addr 172.16.10.5
17:32:19-44
DNS ALG Realm peer
Ip Address             Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv
Resp Sent
                           Rate      Rate      Rate      Rate
Rate       Rate
172.16.10.5                 0.0       0.0       0.0       0.0
0.0        0.0
```

show enum rate

The show enum rate command displays request and response rates for ENUM messages on a system-wide basis. The rates are calculated based on the time in the current monitoring window (100+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ACMEPACKET# # show enum rate
17:22:28-23
Config Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                 Rate      Rate      Rate      Rate       Rate       Rate
ALL               0.0       0.0       0.0       0.0        0.0        0.0
```

show enum rate config-name

The show enum rate config-name command displays request and response rates for ENUM messages per ENUM configuration. If you add a an enum-config-name to the query, that specific configuration's data will be returned. Entered without a name, all configured enum-configs will be displayed. The rates are calculated based on the time in the current monitoring window (30+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ACMEPACKET# show enum rate config-name test1
17:22:53-48
Config Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                 Rate      Rate      Rate      Rate       Rate       Rate
test1             0.0       0.0       0.0       0.0        0.0        0.0
```

show enum rate server-ip-addr

The enum rate server-ip-addr command displays request and response rates for individual enum-servers. If you add an IP address to the query, that specific server's data will be returned. Entered without a server IP address, all configured servers will be displayed. If an IP address is present in more than one ENUM configuration then the message processing level is displayed separately for each configuration object. The rates are calculated based on the time in the current monitoring window (30+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ACMEPACKET# show enum rate server-ip-addr 192.168.201.5
17:24:00-55
ENUM Config Name enum
Ip Address       Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                     Rate      Rate      Rate      Rate       Rate       Rate
192.168.201.5         0.0       0.0       0.0       0.0        0.0        0.0
17:24:00-55
ENUM Config Name test1
Ip Address       Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
```

	Rate	Rate	Rate	Rate	Rate	Rate
192.168.201.5	0.0	0.0	0.0	0.0	0.0	0.0

A

CSV File Data Formats

When enabled, the HDR collector transmits data to a Comma-Separated-Value (CSV) file. The format of the HDR data in the CSV file is dependant on the type of Group Statistics in the file and the method used to open the file. This appendix describes the data formats of the HDR data in the CSV file.

Methods for Display and Format of CSV File Contents

The HDR collector transmits data to a CSV file in standard format. Each file is formatted as <Unix timestamp>.csv (for example, 1302041977.csv). Within the file, each record also has an associated record timestamp. The **filename timestamp** is the time that the CSV file was create. The **record timestamp** is the window of time that the HDR collector used to collect the data. For more information on windows of time, see **Windows of Time**.

When the HDR collector has created a CSV file, you can open the file in any of the following ways:

- using the UNIX command **cat <timestamp>.csv** at the UNIX root prompt (displays raw data)
- using the Microsoft command **type <timestamp>.csv** at a Microsoft® Windows DOS command prompt (displays raw data)
- using a rendering agent application (such as a Microsoft® application)

The following examples show each of these methods.

Example 1 - Using the UNIX Command

The following shows the use of the **cat <timestamp>.csv** UNIX command to display the contents of a system group CSV file in raw data format.

```
[AcmePacket]$ cat 1302041977.csv
TimeStamp,CPU Utilization,Memory Utilization,Health
Score,Redundancy State,Signaling Sessions,
Signaling Rate (CPS),CAM Utilization (NAT),
CAM Utilization (ARP),I2C Bus State,License Capacity,
Current Cached SIP Local Contact Registrations,
Current MGCP Public Endpoint Gateway Registrations,
Current H323 Number of Registrations,
Application Load Rate

1302041977,39,22,50,active,0,0,0,0,online,0,0,0,0,39
1302042037,100,22,50,active,0,0,0,0,online,0,0,0,0,100
```

Example 2 - Using the DOS Command

The following shows the use of the **type <timestamp>.csv** Microsoft® Windows DOS command to display the contents of a sip-sessions group CSV file in raw data format.

```
C:\AcmePacket> type 1301702284.csv
Timestamp,Sessions,Sessions Initial,
Sessions Early,Sessions    Established,Sessions
Terminated,Dialogs,Dialogs Early,
Dialogs Confirmed,Dialogs Terminated

1301702288,45,45,28,35,10,35,35,35,0
1301702456,35,35,21,35,0,0,0,0,0
```

Example 3 - Using a Rendering Agent

The following shows the use of a rendering agent (a Microsoft application) to display the contents of a sip-sessions group CSV file in table format.

```
Timestamp   Sessions  Sessions Initial  Sessions Early ...
130170228   45        45                28             ...
1301702456  35        35                35             ...
```

The formats in the examples above pertain to all of the HDR groups specified in **HDR Groups and Group Statistics**, except the **sip-invite** Group. For information on the sip-invite HDR data format in the CSV file, see the next section.

Sip-invite Format of HDR Data in CSV File

The HDR data for the sip-invite group displays on multiple lines in the CSV file. The first HDR record displays the list of statistics in column format. The second HDR record also displays statistics in column format, and so on. Both client and server totals are included in the data.

The following shows an example of the sip-invite group CSV file for a client and a server displayed in a Microsoft DOS window format.

```
C:\AcmePacket> type 130204198.csv
Timestamp,Message/Event,Server Totals,Client Totals
1301702288,INVITE Requests ,0,0
1301702288,Retransmission,0,0
1301702288,100 Trying,0,0
1301702288,180 Ringing,0,0
1301702288,181 Forwarded,0,0
1301702288,183 Progress,0,0
1301702288,1xx Provisional,0,0
1301702288,200 OK,0,0
1301702288,202 Accepted,0,0
1301702288,2xx Success,0,0
1301702288,30x Moved,0,0
.,,,
.,,,
.,,,
1301702288,Transaction Timeouts,,0
1301702288,Locally Throttled,,0
1301702348,INVITE Requests ,0,0
1301702348,Retransmission,0,0
1301702348,100 Trying,0,0
1301702348,180 Ringing,0,0
1301702348,181 Forwarded,0,0
1301702348,183 Progress,0,0
1301702348,1xx Provisonal,0,0
1301702348,200 OK,0,0
1301702348,202 Accepted,0,0
1301702348,2xx Success,0,0
```

```
1301702348,30x Moved,0,0
.,,,
.,,,
.,,,
1301702348,Response Retrans,0,0
1301702348,Transaction Timeouts,,0
1301702348,Locally Throttled,,0
```

The following shows an example of the sip-invite group CSV file for a client and a server displayed in a Microsoft rendering application format.

```
Timestamp       Message/Event     Server Totals     Client Totals
1301702288      INVITE Requests   0                 0
1301702288      Retransmission    0                 0
1301702288      100 Trying        0                 0
1301702288      180 Ringing       0                 0
1301702288      181 Forwarded     0                 0
1301702288      183 Progress      0                 0
1301702288      1xx Provisional   0                 0
1301702288      200 OK            0                 0
1301702288      202 Accepted      0                 0
1301702288      2xx Success       0                 0
1301702288      30x Moved         0                 0
```

Data Caveats

For those who wish to extract data from HDR CSVs, please note the following:

- Although SNMP presents enumerated fields as integers, HDR translates this data presenting the applicable string in the CSV.
- In some cases, no data is available for a given record. An example of this is a record for an agent that is out of service during the collection window. For these cases, HDR presents only the timestamp and a single field indicating that no data is available, as shown below.

  ```
  enum-stats:
  TimeStamp,ENUM Agent,Queries Total,Successful Total,Not Found Total,Timeout
  Total
  1314110727,no data available
  ```

Glossary