Net-Net OS-E

Release 3.6.0M4

Release Notes

780-0004-00
Revision 1.41
September 30, 2011

Notices

© 2011 Acme Packet, Inc., Bedford, Massachusetts. All rights reserved. Acme Packet, Session Aware Networking, Net-Net, and related marks are trademarks of Acme Packet, Inc. All other brand names are trademarks, registered trademarks, or service marks of their respective companies or organizations.

Patents Pending, Acme Packet, Inc.

The Acme Packet Documentation Set and the Net-Net systems described therein are the property of Acme Packet, Inc. This documentation is provided for informational use only, and the information contained within the documentation is subject to change without notice.

Acme Packet, Inc. shall not be liable for any loss of profits, loss of use, loss of data, interruption of business, nor for indirect, special, incidental, consequential, or exemplary damages of any kind, arising in any way in connection with the Acme Packet software or hardware, third party software or hardware, or the documentation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusions may not apply. These limitations are independent from all other provisions and shall apply notwithstanding the failure of any remedy provided herein.

Copying or reproducing the information contained within this documentation without the express written permission of Acme Packet, Inc., 100 Crosby Drive, Bedford, MA 01730, USA is prohibited. No part may be reproduced or retransmitted.

Contents

NNOS-E
Release Notes, Version 3.6.0

NNOS-E Release Notes, Version 3.6.0

This notice describes the current release of the Acme Packet OS-E® software. OS-E systems and third-party hardware running the OS-E software provide application level security, control, monitoring and interoperability services for real-time communication and collaboration applications and VoIP services based on the Session Initiation Protocol (SIP).

Note: For existing customers who are upgrading from a prior release, the Covergence software components have been renamed under Acme Packet, Inc., as follows:

- Covergence — Now **Acme Packet**
- Session Manager — Now **Net-Net OS-E (OS-E)**
- CMS Web — Now **OS-E Management System**
- CXC-354 — Now **OS-E**
- CXC-554 — Now **OS-E**
- CVA — Now **Net-Net OS-E Virtual Machine (or OS-E-VM)**
- CLI prompt — Now **NNOS-E** (default)

You should review this notice for details about Release 3.6.0, information about operational considerations and known issues from prior releases, and for instructions on installing and upgrading to this release.

Contacting Acme Packet

Acme Packet, Inc.
100 Crosby Drive
Bedford, MA 01730 USA
t: 781-328-4400
f: 781-275-8800

www.acmepacket.com

Evaluation Site Information

Product evaluation sites are provided with a customer-specific Web site URL that connects to the Acme Packet Support Web page. This page provides current software downloads, documentation, MIBs, and troubleshooting information.

For problem reporting and technical support, e-mail Acme Packet at support@acmepacket.com

Technical Documentation

The Net-Net OS-E references in this documentation apply to the Net-Net OS-E operating system software that is used for the following Acme Packet and third-party SBC products:

- Net-Net Application Session Controller (ASC)
- Net-Net OS-E Session Director (SD) Session Border Controller (SBC)
- Net-Net 2600 Session Director (SD) Session Border Controller (SBC)
- Third-party SBC products that license and use Net-Net OS-E software on an OEM basis

Unless otherwise stated, references to Net-Net OS-E in this document apply to all of the Acme Packet and third-party vendor products that use Net-Net OS-E software.

Acme Packet provides the following documentation set in PDF format, viewable using Adobe Reader 5.0 or later. These PDF files are available when you download OS-E software from Acme Packet, as well from your customer Web portal.

- *Net-Net OS-E – Net-Net 2610/2620 Quick Installation*

- *Net-Net OS-E – Network Interface Card Installation*
- *Net-Net OS-E – USB Creation and Commissioning Instructions*
- *Net-Net OS-E – Slide Rail Kit Installation Instruction*
- *Net-Net OS-E – Virtual Machine Information Guide*
- *Net-Net OS-E – System Installation and Commissioning Guide*
- *Net-Net OS-E – Management Tools*
- *Net-Net OS-E – System Administration Guide*
- *Net-Net OS-E – Session Services Configuration Guide*
- *Net-Net OS-E – Objects and Properties Reference*
- *Net-Net OS-E — Objects and Properties Reference*
- *Net-Net OS-E — System Operations and Troubleshooting*

Note: Acme Packet provides updates to the manuals on a regular basis. Go to your Acme Packet Web portal for the latest files in PDF format.

Release Note Revision History

This section contains a revision history for this document.

Date	Revision Number	Description
December 14, 2009	Revision 1.01	• Initial Release of 3.6.0 software.
March 9, 2010	Revision 1.10	• Updates document to include 3.6.0m1 adaptations.
June 18, 2010	Revision 1.20	• Updates document to include 3.6.0m2 adaptations.
December 3, 2010	Revision 1.30	• Updates document to include 3.6.0m3 adaptations. • Updates Acme Packet contact information.

Date	Revision Number	Description
June 24, 2011	Revision 1.40	• Updates document to include 3.6.0m4 adaptations. • Changes references to the software from Net-Net 2600 and NN2600 to Net-Net OS-E and OS-E.
September 30, 2011	Revision 1.41	• Changes references to document names to reflect the switch from Net-Net 2600 to Net-Net OS-E. • Corrects inaccurate file name in the Upgrading to Release 3.6.0 from Release 3.5.x section. • Changes references from Least Cost Routing (LCR) functionality to Route-Server.

Third-Party Platforms and Blades

The OS-E software is supported on third-party platforms and blades as part of integrated solutions that can only be obtained through authorized OEM partners.

For additional details, contact your Acme Packet representative.

OS-E Virtual Machine

The OS-E, available as a VMware® or Xen virtual machine (VM), runs on x86-based PCs and servers.

The VM is intended for SIP customers who are interconnecting branch offices and small businesses to SIP service providers.

For complete information on downloading and running the VM on compatible x86-based PCs and servers, refer to the *Net-Net OS-E — Virtual Machine Information Guide*.

Software Download and Commissioning Process

The software download mechanism allows new and existing customers to acquire OS-E software directly from Acme Packet. Using secure URLs that can be accessed over the internet, Acme Packet provides all necessary software downloads for USB creation, product licensing, and commissioning of your selected hardware.

As part of each download, and depending on your actual requirements, Acme Packet provides the following:

- Acme Packet Boot Media Creator with the OS-E Release 3.6 software.
- Feature licenses.
- Documentation on how to create a OS-E USB stick for commissioning the software on your selected hardware.
- Standard set of OS-E technical publications.

If not included in the shipment, you will need to provide a USB stick with between 1-4GB storage to handle OS-E software downloads. Acme Packet has tested a variety of USB sticks available from current suppliers and manufacturers. Most USB sticks manufactured today will work.

For complete information on accessing the Acme Packet download server, creating an installation USB, and commissioning a OS-E device, refer to the *Net-Net OS-E — USB Creation and Commissioning Instructions*.

Upgrading to Release 3.6.0

This section explains now to upgrade to Release 3.6.0 from previous releases of the OS-E.

Upgrading To Release 3.6.0m4 From Release 3.6.0m3

From Release 3.6.0m3, perform the upgrade to Release 3.6.0m4 using the following procedure.

Note: Acme Packet recommends you run the procedure from a local console so you do not lose connectivity during the procedure itself. If you choose to run the upgrade remotely over SSH, or from the CMS Web **Tools** option, you will not be able to observe when the OS-E has completed the upgrade process.

Perform the following steps:

1. From the current configuration, save the standard configuration using a unique file name of your choice wiht the .cfg extesion. Preserve this file as a backup copy of your configuration if you need to revert to the earlier release.

For example:

```
NNOS-E>> config save standard cxcbackup.cfg
Success
```

2. Save the configuration as an XML file.

   For example:

   ```
   NNOS-E>> config save xml /cxc_common/cfg360m3.xml
   Success
   ```

3. Copy or run SCP to copy the following file to the /cxc directory on the OS-E.

   - nnSE360m4.tar.gz

     If you are currently logged on using the CMS Web, you can use the **Tools/ Upload File** option to browse for the file on your local PC or network location to obtain the file to upload to the OS-E.

4. At the NNOS-E prompt, run the **install** action, as follows:

```
NNOS-E> install file nnSE360m4.tar.gz
Are you sure (y or n)? y
Installing: nnSE360m4.tar.gz
Success! Rebooting Session Manager
```

5. Convert the Release 3.6m3 configuration using the following style sheet:

   - 3.6.0m3--to-3.6.0m4.xsl

```
NNOS-E>> xml transform 3.6.0m3-to-3.6.0m4.xsl /cxc_common/
cxc360m3.xml cxc360m4.xml
Success!
```

6. Replace the configuration file with the new file named cxc360m4.xml.

   ```
   NNOS-E>> config replace cxc360m4.xml
   ```

7. Save the configuration in standard format using the default configuration file name (cxc.cfg).

   ```
   NNOS-E>> config save standard cxc.cfg
   ```

8. Perform a restart warm to boot wtih the new configuration.

   ```
   NNOS-E>> restart warm
   ```

If you are using the CMS Web to perform the upgrade remotely, use the CMS **Tools/ Update Software** option with the “Install the Update” selection checked off to run the upgrade.

Upgrading To Release 3.6.0m4 From Release 3.6.0, 3.6.0m1, and 3.6.0m2

From an earlier 3.6 release, perform the upgrade to Release 3.6.0m4 using the following procedure.

Note: Acme Packet recommends you run the procedure from a local console so you do not lose connectivity during the procedure itself. If you choose to run the upgrade remotely over SSH, or from the CMS Web **Tools** option, you will not be able to observe when the OS-E has completed the upgrade process.

Perform the following steps:

1. From the current configuration, save the standard configuration using a unique file name of your choice wiht the .cfg extesion. Preserve this file as a backup copy of your configuration if you need to revert to the earlier release.

   For example:

   ```
   NNOS-E>> config save standard cxcbackup.cfg
   Success
   ```

2. Save the configuration as an XML file.

   For example:

   ```
   NNOS-E>> config save xml /cxc_common/cfg360.xml
   Success
   ```

3. Copy or run SCP to copy the following file to the /cxc directory on the OS-E.

   - nnSE360m4.tar.gz

     If you are currently logged on using the CMS Web, you can use the **Tools/ Upload File** option to browse for the file on your local PC or network location to obtain the file to upload to the OS-E.

4. At the NNOS-E prompt, run the **install** action, as follows:

```
NNOS-E> install file nnSE360m4.tar.gz
Are you sure (y or n)? y
Installing: nnSE360m4.tar.gz
Success! Rebooting Session Manager
```

5. Convert the Release 3.6 configuration using the following style sheets:

   - 3.6.0-to-3.6.0m3.xsl
   - 3.6.0m3-to-3.6.0m4.xsl

```
   NNOS-E>> xml transform 3.6.0-to-3.6.0m3.xsl /cxc_common/cxc360.xml
/cxc_common/cxc360m3.xml
   Success!
   NNOS-E>> xml transform 3.6.0m3-to-3.6.0m4.xsl /cxc_common/
cxc360m3.xml /cxc_common/cxc360m4.xml
   Success!
```

6. Replace the configuration file with the new file named cxc360m4.xml.

   ```
   NNOS-E>> config replace cxc360m4.xml
   ```

7. Save the configuration in standard format using the default configuration file name (cxc.cfg).

   ```
   NNOS-E>> config save standard cxc.cfg
   ```

8. Perform a restart warm to boot wtih the new configuration.

   ```
   NNOS-E>> restart warm
   ```

If you are using the CMS Web to perform the upgrade remotely, use the CMS **Tools/ Update Software** option with the “Install the Update” selection checked off to run the upgrade.

Upgrading To Release 3.6.0 From Release 3.5.x

The accounting functionality has changed from release 3.5.x to release 3.6.0. When purging is enabled, your OS-E accounting service deletes all 3.5.x unpersisted CDRs it finds during the upgrade process.

In order to not lose any raw CDRs, you must find accounting targets which have not received all applicable CDR data using the **scan utility** to view an accounting store to see if there are any unpersisted CDRs in the 3.5.x version that need to be persisted before the upgrade to 3.6.0 can be done. The execution of the scan utility action is performed in the shell.

1. Copy or run SCP to copy the following file to the /cxc directory on OS-E.

   - accounting35store

   If you are currently logged on using the OS-E Management System, you can use the **Tools/Upload File** option to browse for the file on your local PC or network location to get the file uploaded to OS-E.

2. Stop running traffic. This allows any lagging accounting service time to catch up.
3. At the NNOS-E> prompt, enter the **shell** action as follows:

```
NNOS-E> shell
localhost app_slot_1 #
```

4. Enter the scan utility command using the following syntax:

```
localhost app_slot_1 # accounting35store -s [3.5x store location]
-m [target]
```

where:

- -s—Specifies the accounting store folder. The location of this folder is specified in the configuration under the **accounting-root-directory**.
- -m—Specifies the mode for results which can be **target** (results per target), **file** (results per file), or **incomplete** (list incomplete files only; default behavior)

For example:

```
localhost app_slot_1 # accounting35store -s /acme_common/
accounting35/test1/ -m target
```

The following are more arguments you can use with the **scan utility** to narrow down your accounting target search:

- -f—Specifies an individual file to check
- -csv—Output the results in CSV format
- -w—The results are printed into this file.
- -force—Scan every file
- -d—Specifies the debug mode which can be **error** (only errors are printed; default), **info** (information level messages are printed), or **debug** (debug level messages are printed)
- -h—Displays the help for the scan utility.

5. If any bad accounting targets are found, fix them. The following is an example of the message you receive when a bad target is found:

```
localhost app_slot_1 # accounting35store -s /acme_common/
accounting35/test1/ -m target
-------------------------------------------------------------------
***  Failed Targets ***
-------------------------------------------------------------------
  1. vsp\accounting\database\group mssqlDB
         server-name:
                type: database
```

```
                failed: 24
-------------------------------------------------------------------
```

6. Allow accounting service to run until processing is complete. To ensure the process is complete you can execute the **scan utility** again.

   After all of this has been completed, you can begin the upgrade process.

If you are currently running Release 3.5.x, perform the upgrade to Release 3.6.0 using the procedure covered in the section using the Release 3.6.0 tar file, available from your Acme Packet Web portal.

Caution: Acme Packet recommends that you run the upgrade procedure from a local console so that connectivity is not lost during the procedure itself. If you choose to run the upgrade remotely over SSH, or from the OS-E Management System **Tools** options, you will not see when the OS-E device has completed the upgrade process.

To upgrade the OS-E, perform the following steps:

1. From the current configuration, save the standard configuration using a unique file name of your choice with the .cfg extension. Preserve this file as a backup copy of your configuration if you need to revert to the earlier release.

   For example:

   ```
   NNOS-E>> config save standard cxcbackup.cfg
   Success
   ```

2. Save the configuration as an XML file.

   For example:

   ```
   NNOS-E>> config save xml /cxc_common/cxc35.xml
   Success
   ```

3. Copy or run SCP to copy the following files to the /cxc directory on OS-E.

   - nnSE360m4.tar.gz

   If you are currently logged on using the OS-E Management System, you can use the **Tools/Upload File** option to browse for the file on your local PC or network location to get the file uploaded to OS-E.

4. At the NNOS-E> prompt, run the **install** program, as follows:

   ```
   NNOS-E>> install file nnSE360m4.tar.gz
   Are you sure (y or n)? y
   ```

```
Installing: nnSE360m4.tar.gz
Success! Rebooting Net-Net OS-E
```

5. Convert the Release 3.5 configuration using the following style sheets:
   - 3.5-to-3.6.xsl
   - 3.6.0-to-3.6.0m3.xsl
   - 3.6.0m3-to-3.6.0m4.xsl

```
NNOS-E>> xml transform 3.5-to-3.6.xsl /cxc_common/cxc35.xml /
cxc_common/cxc360.xml
Success!
NNOS-E>> xml transform 3.6.0-to-3.6.0m3.xsl /cxc_common/cxc360.xml
/cxc_common/cxc360m3.xml
Success!
NNOS-E>> xml transform 3.6.0m3-to-3.6.0m4.xsl /cxc_common/
cxc360m3.xml /cxc_common/cxc360m4.xml
Success!
```

6. Replace the configuration file with the new file named cxc36m4.xml

```
NNOS-E>> config replace cxc36m4.xml
```

7. Save the configuration in standard format using the default configuration file name (cxc.cfg).

```
NNOS-E>> config save standard cxc.cfg
```

8. Perform a restart warm to boot with the new configuration.

```
NNOS-E>> restart warm
```

If you are using the OS-E Management System to perform the upgrade remotely, use the **Tools/Update Software** option with the “Install the Update” selection checked off to run the upgrade.

Upgrading To Release 3.6.0 From Release 3.4.x or later

If you are currently running Release 3.4.2, 3.4.3 or 3.4.4, you should perform the upgrade to Release 3.6.0 from a USB stick. Refer to the *Net-Net OS-E — USB Creation and Commissioning Instructions* for information on creating the USB stick and commissioning the OS-E device. Contact Acme Packet for assistance when performing these upgrades.

Note: When upgrading from release 3.4 to releases 3.5 or 3.6 on third party hardware, a manual procedure must be performed to ensure that the interfaces remain on the current ethernet ports. For more information about this, contact Acme Packet technical support.

Special Considerations After Running the Upgrade

OS-E creates an alternate, inactive directory that captures the files associated with the release from which you are upgrading. This inactive directory holds customer-created configuration files and phone configurations. You may need to access this directory to copy these custom files to the new active release directory. Otherwise, for example, SIP phones may not work properly.

The release files associated with the older release are moved to a directory of the form:

/cxc_rel/app-<slot 1-3>

where "app" is a literal text string, followed by the version and release numbers that are explicit to the release software.

Acme Packet recommends that you place a copy of any uploaded configuration or phone files into a common directory for easy access when upgrades are completed. For example, copy the files into the /cxc_common/ directory so that the files remain there after any upgrade.

Release 3.6.0m4

This section describes all of the new adaptations added to the OS-E in release 3.6m4, including new features, configuration objects and properties, and MIBs.

New Features

The following section describes all of the new adaptations added to the 3.6m4 software.

The new features for 3.6m4 are:

- Named Variable Support
- CDR Custom Data Fields and Reserved Keywords
- Custom Data Fields in AA-SBC Events
- Embedded Route-Server Import Tool Support
- HTTPS Support for Call Rates Files Downloading
- AA-SBC DID Range Enhancements
- DTMF Translation Framework
- Threaded Session Mixing Action
- ARP Heartbeat Configuration on VM Clusters
- Dual HA Heartbeat Configuration Enhancements
- TCP/TLS Ephemeral Port Range Configuration
- Event Log Translation into SNMP Traps
- ToS Marking for H.323 Packets
- 302 Redirect Messages for Cross-Cluster Load Balancing
- Archiving Enhancements
- Server State Detection via OPTIONS PING Response
- RTCP QoS Accounting
- Called Party Name Interworking
- Expanded File System Support

- Manually Issuing an LRQ Action
- H.323 Settings Supported Under Session Config
- Virtual Dial Plans Support
- User Roles and Access Enhancements
- File Security Enhancements

Named Variable Support

The OS-E now supports a generic database used to hold named variables. A named variable is a variable paired with a value through the reg-exp header code. This allows you to modify SIP message fields and CDR fields more generically.

You can configure named variable support in several ways. The **header-settings > named-variable-collector** object allows you to alter SIP header messages.

The **named-variables** object, configured on a per-session basis, allows you to create a static list of named variables that can be used in several features throughout the OS-E configuration. You create named variables under the **session-config** object and you can create a named variable list for each configured session.

In addition, you can create a named variable condition list via the **named-variable-condition** for both the **session-policies** and **dial-plan** objects. This allows you to configure the OS-E to match a particular policy or dial plan route, depending on the named variables contained in the session.

When a session is created, a named variable list is automatically created. If any named variables are configured in the **default-session-config**, they populate this list. All variable names in the named variable list must be unique.

The OS-E updates the named variable list when any of the following happens.

- When the session configuration **merge-object** is set to **merge**, the named variables configured in the new session config are appended to the existing named variable list.
- When the session configuration **merge-named-variables** is set to **replace**, the existing session configuration named variables are replaced by the newly configured named variables.
- When the **header-settings > named-variable-collector** collects new named variables via the reg-exp code.

- When you specify or create a named variable list and a named variable of the same name already exists, the OS-E overwrites the value of the existing variable name.

  Note: Variable names cannot start with a “$” and you should not use special characters such as “\”, “%”, “#”, “!”, “?”, “[“, “]”, :&”, “{“, “}”, “@” when naming variables.

Configure the **named-variable-collector** under **header-settings.** This object allows you to configure the OS-E to look at any SIP message header, and by applying regular expressions, extract any part of the header and store the value in the specified named variable table. You can apply these settings to both requests and responses.

Under this object you assign the named variable collector a number and a name. This is also where you create the variable. To create a variable, first select the header type you want to serve as the source of the data. This can be either any valid SIP message header. Then specify a regular expression to run against the value of the source header. Finally, specify the replacement expression to apply when there is a match. If you want to append a string to the existing named-variable value, appending is done the same way as creating.

Other things you can configure under the **named-variable-collector** object include the SIP methods to apply variables, whether the OS-E applies variables to responses, which type of dialog variables should be applied, if a CSEQ field needs to be matched, and what actions to take on the expression if there is not a complete match.

To configure the named variable functionality under **header-settings**, access the **named-variable-collector** object.

```
NNOS-E>config vsp
config vsp>config default-session-config header-settings
config header-settings>config named-variable-collector 1
config named-variable-collector 1>set admin enabled
config named-variable-collector 1>set named-variable var1
config named-variable-collector 1>set create To (.*) \1
config named-variable-collector 1>set append To (.*) ;2
config named-variable-collector 1>set apply-to-methods invite
config named-variable-collector 1>set apply-to-responses no
config named-variable-collector 1>set apply-to-dialog both
config named-variable-collector 1>set create-on-failed-match false
config named-variable-collector 1>set append-on-failed-match false
config named-variable-collector 1>return
config header-settings>return
```

For more information about **named-variable-collector** properties, see the Configuration Changes in 3.6.0m4 section of this guide.

Under the **named-variables** object, you can configure static variables to be applied on a per-session basis, You can also name the variable, set a value for that variable, and decide if you want to append the existing set of session configuration named variables, or use this value to replace the existing set of session configuration named variables.

To configure the named variable functionality on a per-session basis, access the **named-variables** object.

```
config>config vsp
config vsp>config default-session-config
config default-session-config>config named-variables
config named-variables>set merge-object replace
config named-variables>config named-variable var1
config named-variable var1>set value (*)
config named-variable var1>return
config named-variables>return
```

For more information about **named-variables** properties, see the Configuration Changes in 3.6.0m4 section of this guide.

To configure the **session-policy** condition list, access the **session-policies condition-list** object. This object matches a particular policy depending on the named variables contained in the session.

Specify whether you want to compare the **named-variable-value**, which compares specified named variable values, or if you want to compare the **compare-named-values**, which compares the values of two different named variables.

If you compare the **named-variable-value**, you must provide the name of the variable, the type of match, and the value.

```
NNOS-E>config vsp
config vsp>config policies session-policies
config session-policies>config policy policy1
Creating 'policy policy1'
config policy policy1>config rule rule1
Creating 'rule rule1'
config rule rule1>config condition-list
config condition-list>set named-variable-condition
   named-variable-value variable1 match (*)
config condition-list>return
```

If you compare the **compared-named-variables**, you must provide the name of the first variable, the type of match, and the name of the second variable.

```
config>config vsp
config vsp>config policies session-policies
config session-policies>config policy policy2
Creating 'policy policy2'
config policy policy2>config rule rule2
Creating 'rule rule2'
config rule rule2>config condition-list
config condition-list>set named-variable-condition
   compare-named-variables var1 match var2
config condition-list>return
```

To configure the dial plan route condition list, access the **dial-plan condition-list**. This object matches a particular dial plan route depending on the named variables contained in the session.

Specify whether you want to compare the **named-variable-value**, which compared specified named variable values, or if you want to compare the **compare-named-values**, which compares the values of two different named variables.

If you compare the **named-variable-value**, you must provide the name of the variable, the type of match, and the value.

```
NNOS-E>config vsp
config vsp>config dial-plan
config dial-plan>config route route1
Creating 'route route1'
config route route1>config condition-list
config condition-list>set named-variable-condition
   named-variable-value variable1 match (*)
config condition-list>return
```

If you compare the **compared-named-variables**, you must provide the name of the first variable, the type of match, and the name of the second variable.

```
NNOS-E>config vsp
config vsp>config dial-plan
config dial-plan>config route route1
Creating 'route route1'
config route route1>config condition-list
config condition-list>set named-variable-condition
   compare-named-variables policy1 match policy2
config condition-list>return
```

For more information about **named-variable-condition** properties, see the Configuration Changes in 3.6.0m4 section of this guide.

A new status provider, **show named-variables-by-session**, has been created to display the named-variables per active session.

```
NNOS-E>show named-variables-by-session

------------------------------------------------
Named Variables for session 0x04c3e0841669a1b7
------------------------------------------------
variable1 = value1
variable2 = value1
variable3 = value3
variable4 = value4
variable5 = value3
------------------------------------------------
```

When you add a **-v** to the end of this action, the OS-E displays a verbose output which also shows the association ID of the session, the session type, creation time, and the value and source for each variable.

CDR Custom Data Fields and Reserved Keywords

Using the named variable table, the OS-E is able to write out any information in the customData field of CDRs.

Leverage the existing **accounting-data** configuration object to write out any information you want in the CDR customData field. Use the **entry > value** property to reference the named variables table collected earlier via the **session-config** or **reg-exp** code. Or use it to reference a reserved keyword (reserved keywords are described later in this section).

Via Radius Access message, VSA can also be stored and referenced in the named variable table. In the **accounting-data > entry** property, reference this information in the CDR customData field.

The OS-E now has a list of reserved keywords you can use in CDRs or reg-exp code to access information you want. This avoids any confusion with named variables.

Reserved keywords must be referenced using the **\!<*reserved-keyword*>!** syntax.

The following table shows a list of keywords that extract information from either a SIP message or a session.

Current Abbreviation	New Custom Keyword	Information Source
\r	$MSG_REMOTE_IP	SIP Message - Remote IP
\R	$MSG_REMOTE_PORT	SIP Message - Remote Port
\p	$MSG_PRIVATE_REMOTE_IP	SIP Message - Private Remote IP
\P	$MSG_PRIVATE_REMOTE_PORT	SIP Message - Private Remote Port
\l	$MSG_LOCAL_IP	SIP Message - Local IP
\L	$MSG_LOCAL_PORT	SIP Message - Local Port
\n	$SESS_LOCAL_IN_IP	SIP Session - IP Address of the Interface For the In-Leg
\N	$SESS_LOCAL_IN_PORT	SIP Session - IP Port of the Interface For the In-Leg
\a	$SESS_LOCAL_OUT_IP	SIP Session - IP Address of the Interface for the Out-Leg
\A	$SESS_LOCAL_OUT_PORT	SIP Session - IP Port of the Interface For the Out-Leg
\g	$SESS_REMOTE_IN_IP	SIP Session - IP Address of the Remote End of the In-Leg
\G	$SESS_REMOTE_IN_PORT	SIP Session - IP Port of the Remote End of the In-Leg
\d	$SESS_DEST_OUT_IP	SIP Session - Out-Leg Destination IP Address
\D	$SESS_DEST_OUT_PORT	SIP Session - Out-Leg Destination Port
\e	$SESS_PEER_IP	SIP Session - OS-E Peer IP Address
\E	$SESS_PEER_PORT	SIP Session - OS-E Peer Port
\z	$SESS_LOCAL_PEER_IP	SIP Session - OS-E Local Peer IP Address
\Z	$SESS_LOCAL_PEER_PORT	SIP Session - OS-E Local Peer Port
\t	$SESS_IN_CONTACT_HDR	SIP Session - OS-E's In-Leg Contact HDR
\o	$SESS_OUT_CONTACT_HDR	SIP Session - OS-E's Out-Leg Contact HDR
\h	$SESS_ORIG_IN_REQUEST_URI	SIP Session - Origin In Request URI

Current Abbreviation	New Custom Keyword	Information Source
\i	$SESS_ORIG_IN_TO_URI	SIP Session - Origin In To URI
\j	$SESS_ORIG_IN_FROM_URI	SIP Session - Origin In From URI

The following table shows a list of keywords used in CDRs.

Current Abbreviation	New Custom Keyword	Information Source
\b	$BOX_ID	Box Identifier
\d	$CDR_DIGEST_REALM	SIP Session - Digest Realm
\s	$CDR_SRC_LNP	SIP Session - Source LNP
\e	$CDR_DEST_LNP	SIP Session - Destination LNP
\v	$CDR_DIV_HDR	SIP Session - Diversion Header
\c	$CLUSTER_NAME	SIP Meta - Cluster Name
\r	$CDR_RADIUS_CALLER_ID	SIP Session - RADIUS Caller ID
\o	$CDR_REQUEST_ID	SIP Session - Request ID
\z	$CDR_CONNECTED	Call Data - Connected Bool
\y	$CDR_SCAN_TIME	Call Data - Scan Time
\x	$CDR_FILE_TIME	Call Data - File Time
\w	$CDR_PLAY_TIME	Call Data - Play Time
\u	$CDR_DISCONNECT_REASON	Call Data - Disconnect Reason
\t	$CDR_FINAL_REASON_CODE	SIP Session - Last Response Code
\q	$CDR_POST_DIAL_DIGITS	Call Data - Post Dial Digits
\j	$CDR_SRCLEG_CURR_JITTER	Normalized Source Leg Current Jitter
\m	$CDR_SRCLEG_MAX_JITTER	Normalized Source Leg Max Jitter
\i	$CDR_DESTLEG_CURR_JITTER	Normalized Destination Leg Current Jitter
\k	$CDR_DESTLEG_MAX_JITTER	Normalize Destination Leg Max Jitter

Custom Data Fields in OS-E Events

You now have the ability to add custom fields into OS-E-generated events. By using the named variables table, you can extract information from any SIP message header and reference it in the events to add the custom information. Three new events have been added which allow you to include this information: callCreatedEventCustom, callConnectedEventCustom, and callTerminatedEventCustom.

An object, **custom-event-fields**, has been added to the **third-party-call-control** object. This object allows you to add a custom data field to the callCreated, callConnected, and callTerminated events. Within this object, define the content of that field via the **named-variable-entry** object.

Two advanced properties have been added under the **custom-event-fields** object, **custom-events-grouping-string** and **custom-event-delimiter**. These properties allow you to change the characters used to associate an event's variable with its value (default is **=**) as well as the character used to separate a group's custom event entries (default is **;**).

The following is a sample **custom-event-fields** configuration.

```
NNOS-E>config vsp
config vsp>config default-session-config
config default-session-config>config third-party-call-control
config third-party-call-control>config custom-event-fields
config custom-event-fields>set named-variable-entry variable=\s
config custom-event-fields>return
config third-party-call-control>return
```

Embedded Route-Server Import Tool Support

You can now download the Route-Server Import tool as an embedded application on the OS-E software. As opposed to using the stand-alone Route-Server Import tool, which runs on a Windows PC or workstation.

The embedded route-server import tool must be run on an OS-E system dedicated just for this purpose. You cannot use this OS-E for anything else.

To view and use the embedded route-server import tool, the user must have lcr-import permissions granted. Users can be granted one of the following route-server permissions:

- **enabled—**Allows the user to perform all route-server import functions.

- **view—**Allows the user to perform read-only tasks.
- **disabled—**Bars the user from all access to the route-server import tool.

For more information on configuring user permissions, see Management System Access in this guide.

Before installing the embedded route-server import tool, you must have the OS-E software installed and running properly. Also, you must configure the following:

- Enable the **master-services > database** object.
- Add a certificate via the **vsp > tls** object.
- Enable the **web-service** object and select the certificate to use.

Enable the master-services database:

To use the embedded route-server import tool properly, the **master-services > database** object must be **enabled**. If you attempt to use the route-server import without the database enabled, you get the following error message.

```
"Cannot fetch the LCR import records. [internal error: No suitable
   driver found for jdbc:postgresql://127.0.0.1.5432/lcrimport]"
```

1. Log in to the OS-E.

2. Under the **Configuration** tab, enable the **master-services** > **database** object.

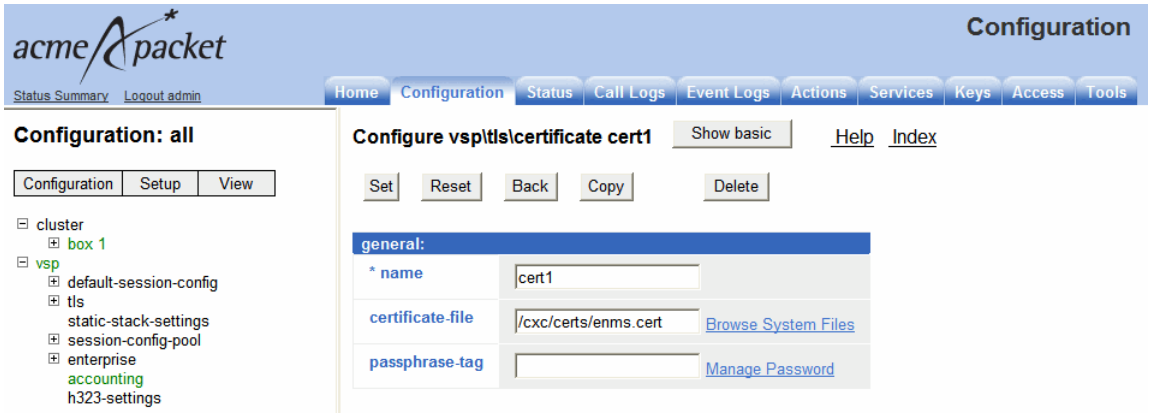
3. Update and save the configuration.

Adding a certificate to the TLS object:

You must configure a TLS entry to add the appropriate certificate.

1. Under the **Configuration** tab select **tls**, then click **Add certificate**.
2. Enter the name you are using for the certificate and click **Create**.

3. Browse to the certificate file in the **certificate-file** property.

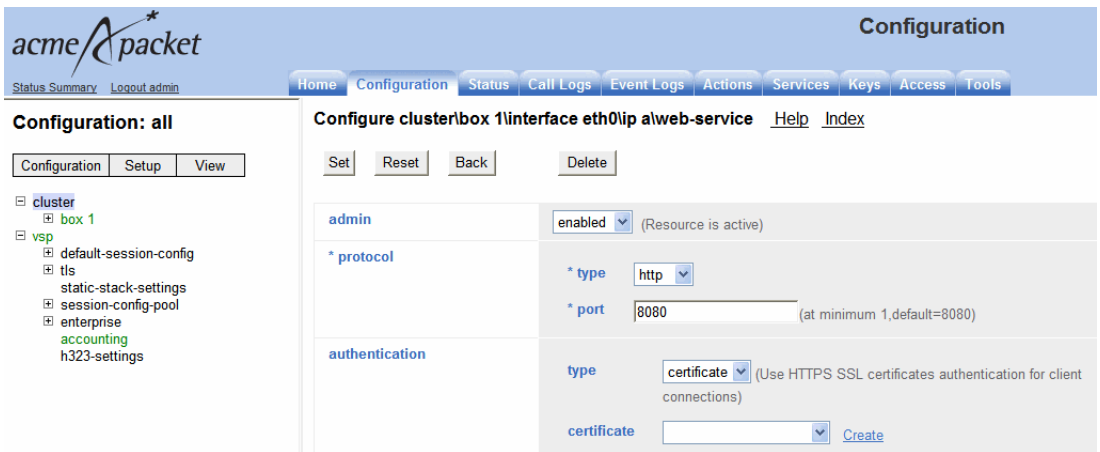


4. Update and save the configuration.

Enabling and updating web-service:

You must also enable and update **web-service** to use the certificate you add under **tls**.

1. Under the **Configuration** tab, use the following path to get to the web-service object: **cluster > box > interface > ip > web-service**.
2. Ensure the object is **enabled**.
3. Select **certificate** for **authentication type**. Select the certificate you added under **tls**.



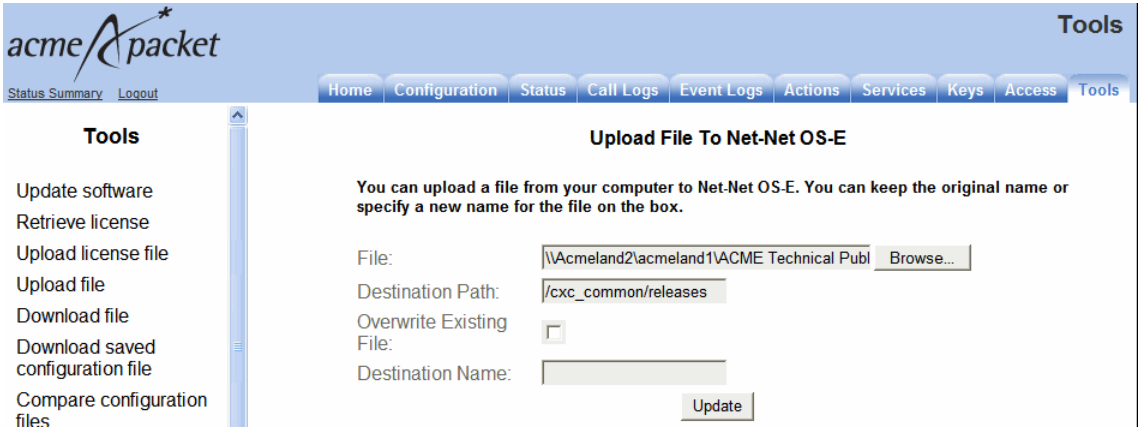
4. Update and save your configuration.

Installing the Embedded Route-Server Import Tool

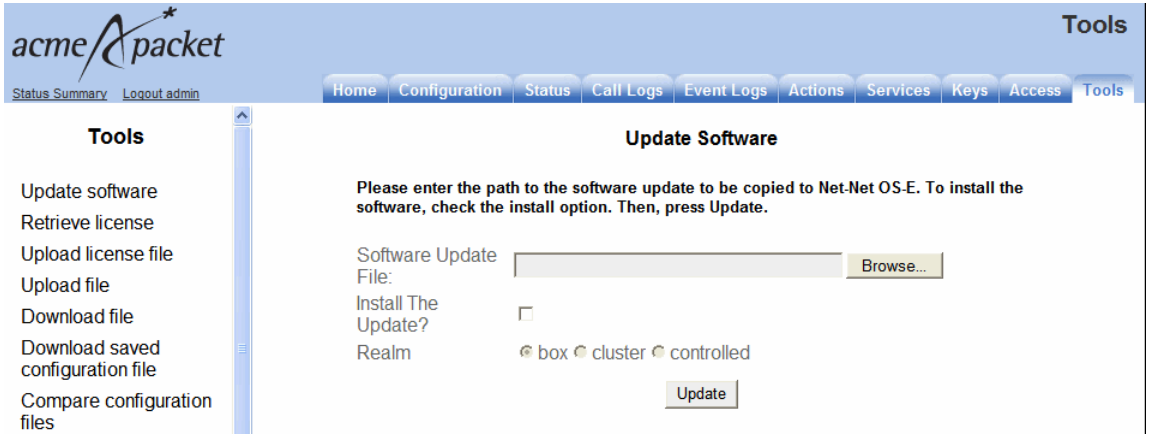
This section explains how to install the embedded route-server import tool.

Note: To run the embedded route-server tool, the DOS process must be running at level 7. To ensure you have this version running, execute the **show processes** action under **System** on the left hand list below the **Status** tab.

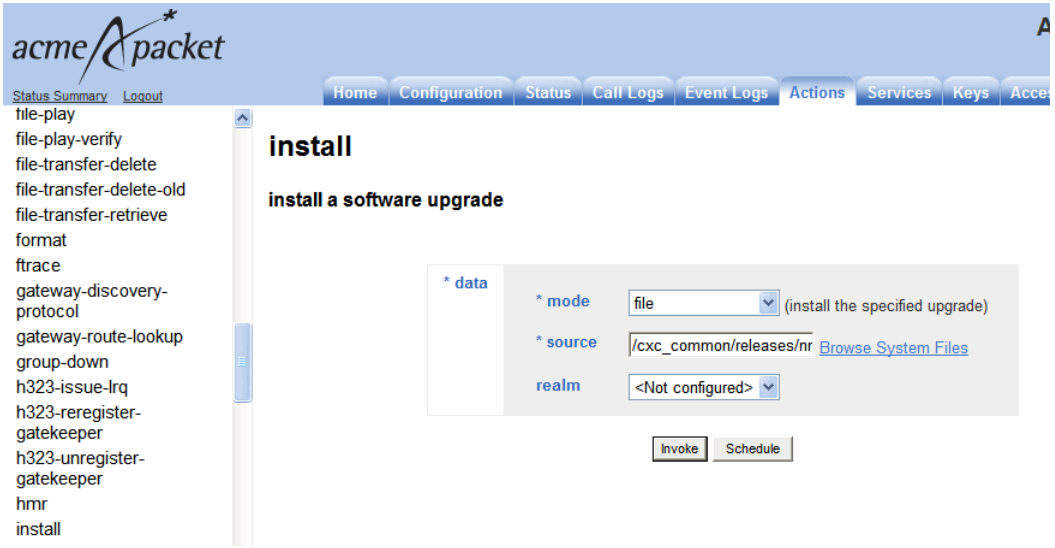
5. Upload the ***lcrimport.tar.gz*** file to the "/releases" directory on your OS-E using either the **Upload file** action under the **Tools** tab.



Or the **Update software** action under the **Tools** tab.



6. Under the **Actions** tab, execute the **install file releases *lcrimport.tar.gz*** action to install the embedded route-server import tool to the OS-E.



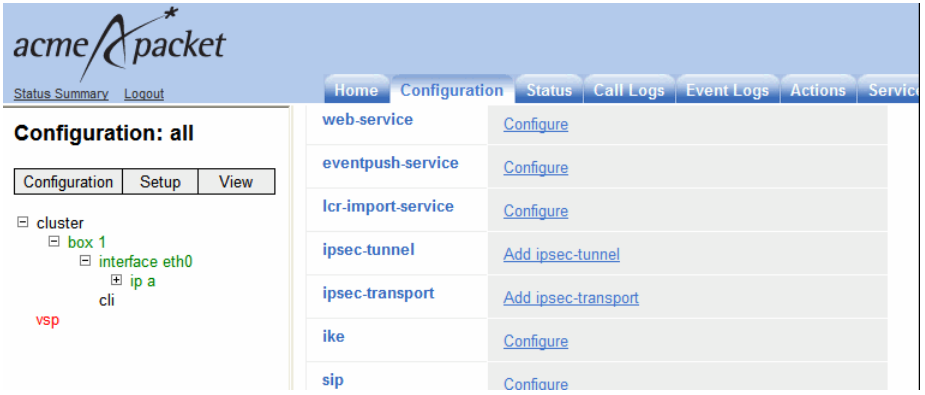
7. The OS-E restarts.

Configuring the embedded Route-Server Import Tool

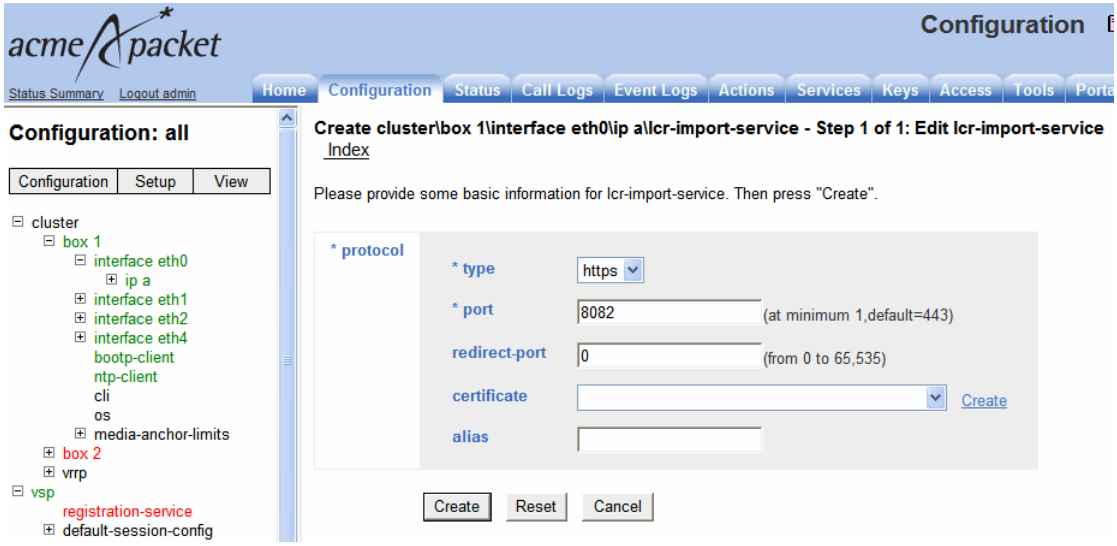
This section explains how to configure the embedded route-server import tool.

8. Under the **Configuration** tab, select the **ip** object under the **cluster** > **box** > **interface** object.

9. Click **Configure** next to **lcr-import-service**.

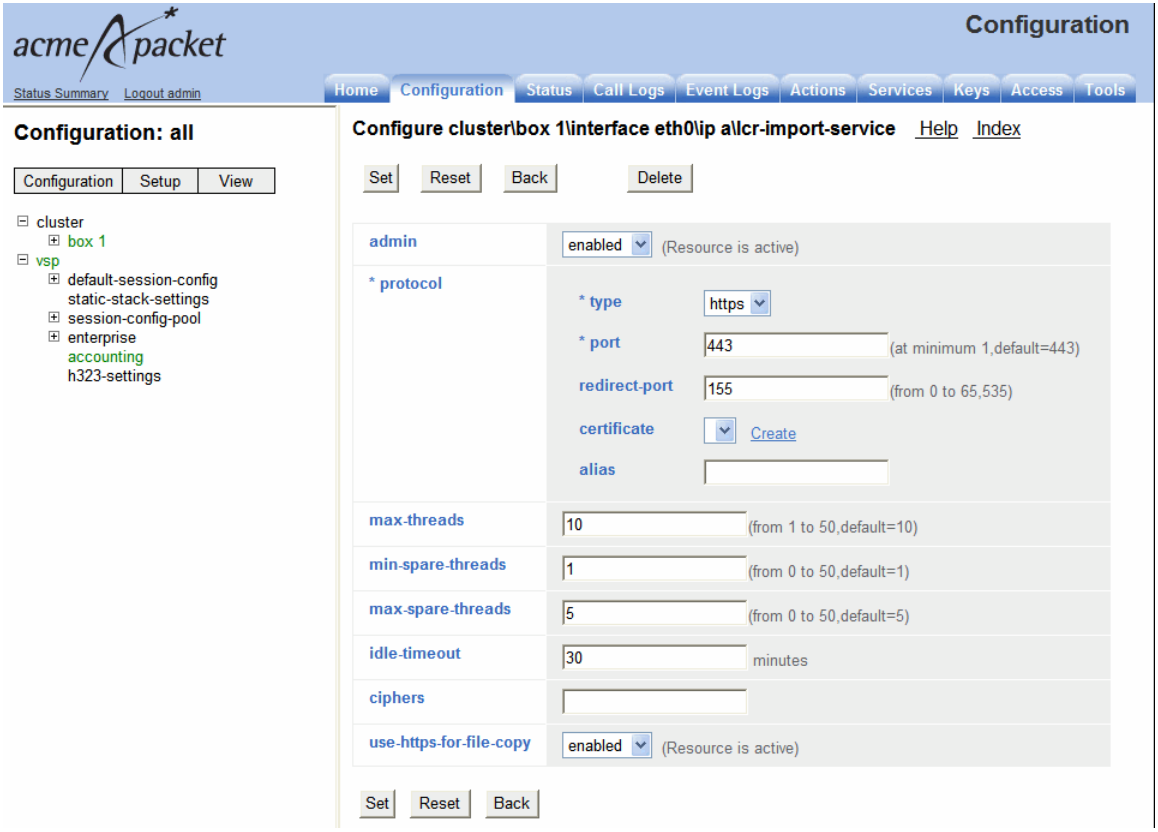


10. Select the protocol **type**, **http** or **https**, and specify the target **port**. The default is **8082**.



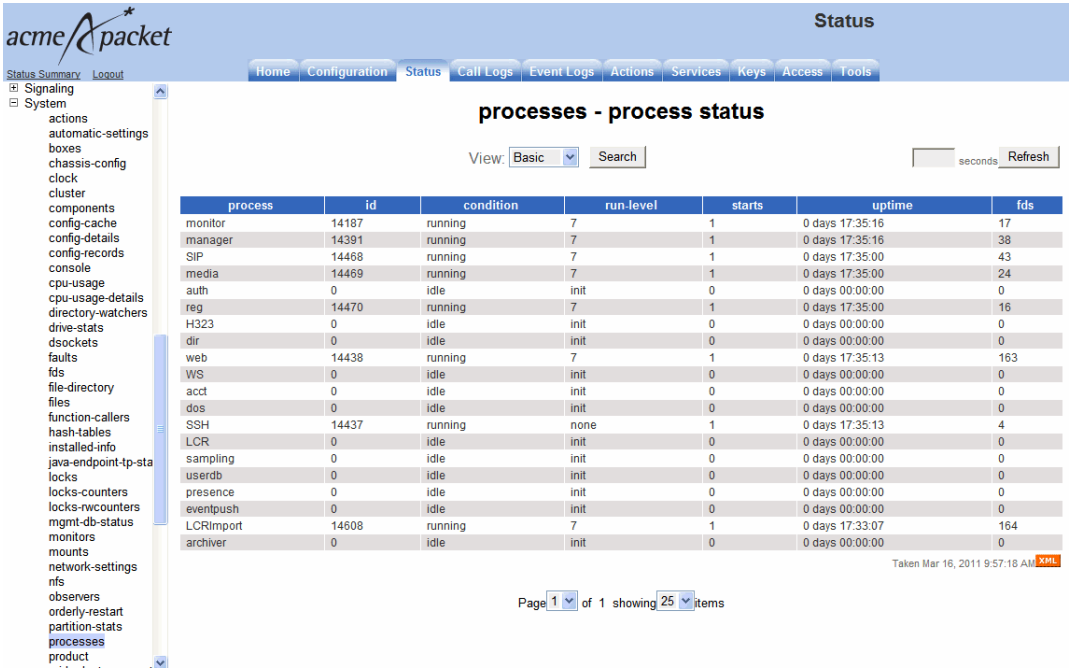
11. Click **Create**.

12. Configure the route-server import values the way you want to implement the functionality. For more information on the **lcr-import-service** properties and what they mean, see the New Objects in Release 3.6.0m4 section of this guide.



13. Click **Set**. Update and save your configuration.

14. The route-server import process must be running at Level 7. To view the route-server import process status, select the **Status** tab, expand **System** on the list at the left hand of the screen, and select **processes**.



15. You must now create a file event log for embedded route-server import functionality. Select the **Services** tab.

16. Select **event-log** and click **Add file**. Name the file and click **Create**.

17. Configure the event log properties for the route-server import functionality. For more information on the **services** > **event-log** > **file** properties, see the *Net-Net OS-E Objects and Properties Reference Guide*.

18. Click **Set**. Update and save your configuration.

To launch the embedded route-server import tool:

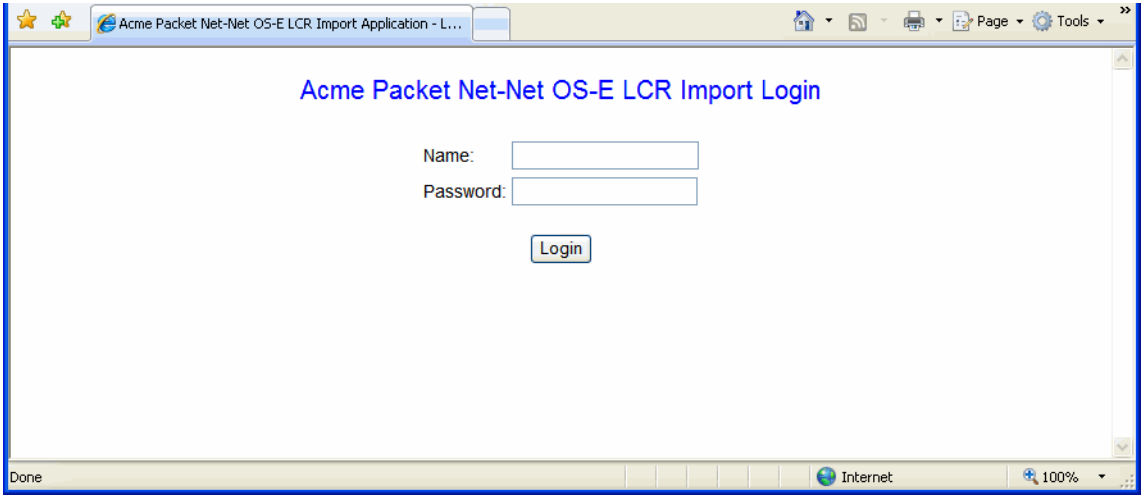
1. Launch the embedded route-server import tool by opening a browser window and entering either:

   - http://<*ipNumber*>:<*port*>/lcrimport
   - https://<*ipNumber*>:<*port*>/lcrimport

   Where <*ipNumber*> is the OS-E's management IP address and <*port*> is the port value specified in Step 8 of the installation process.

   Use either HTTP or HTTPS depending on the configured **lcr-import-service** protocol type.

2. You can now log into the route-server import login page.



HTTPS Support for Call Rate Files Transferring

By default, HTTPS is used to transfer call rate files between the embedded route-server import and the route server. HTTPS is a combination of HTTP and SSL/TLS protocols which provides encryption and secure identification of the server.

You have the ability to use a custom certificate for authentication. To add a custom key store, under the **vsp > tls** config object, click **Add certificate**. The route-server import tool only supports custom key stores created with the “PKCS12” format. If you do not specify a certificate and certificate alias, the OS-E uses the default certificate.

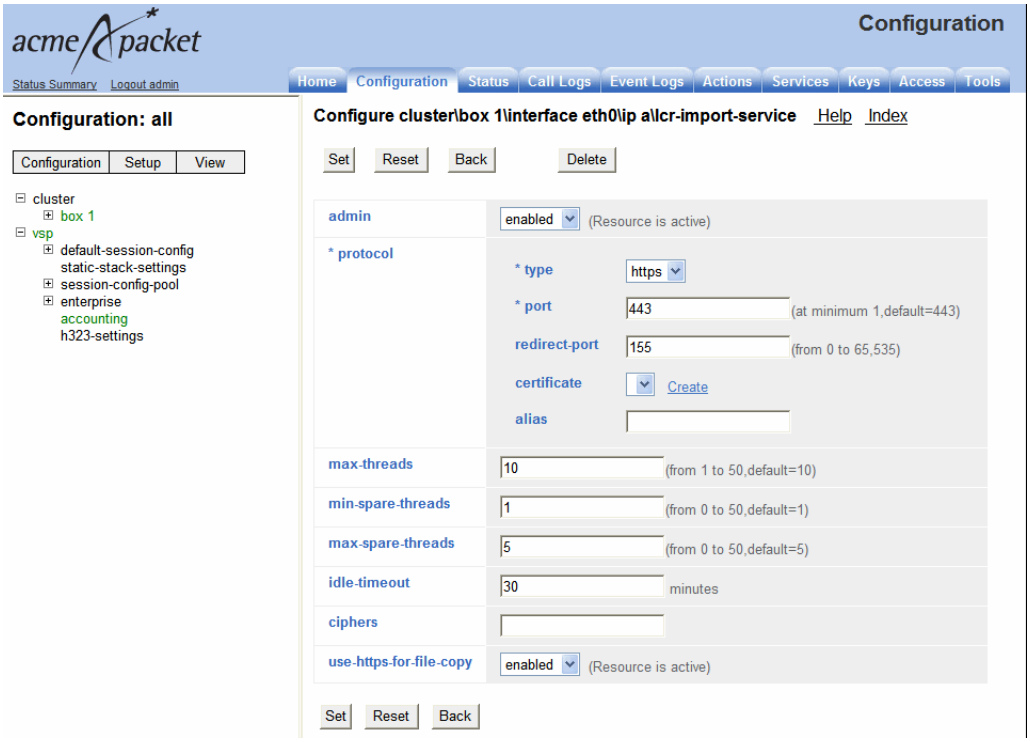
A new property has been added to the **lcr-import-service** object, use-**https-for-file-copy**. This new property takes effect when you select not to use SCP for file copy. This property allows you to select whether to use HTTP or HTTPS to copy call rate files between the route-server import tools server and the route server. By default this property is enabled and HTTPS is used. When disabled, HTTP is used.

When you configure a 3.6m4 OS-E with a pre-3.6m4 route server, HTTPS is not supported. To copy files to the route server, you must use either HTTP or SCP.

Note: HTTPS for file copying is supported on the embedded route-server import tool only. For the stand-alone route-server import tool, you can only use SCP or HTTP.

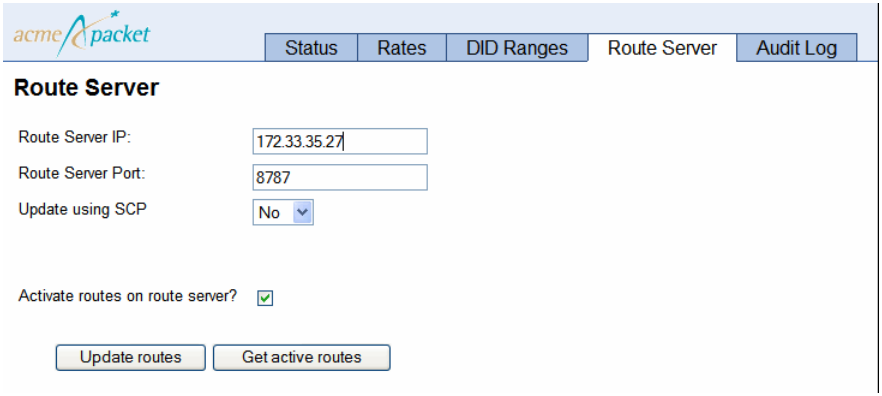
To use HTTPS to transfer call rates files to the route server:

1. Under the **lcr-import-service** configuration object, set **protocol** to **https**.
2. Set the **port** number to use to access the route-server import tool web interface.
3. Select the **certificate** you are using.
4. Set **use-https-for-copy-file** to **enabled**. This configures the OS-E to use HTTPS to transfer call rates files.



5. Save and update your configuration.
6. Log into the route-server import tool.
7. Under the **Route Server** tab set **LCR Server IP** to the address of the OS-E interface.
8. Set the route-server server **Port** to the port of the OS-E interface.

9. Set **Update using SCP** to **No**. When this property is set to **No**, the route-server import tool uses the value configured in the **use-https-for-file-copy**.



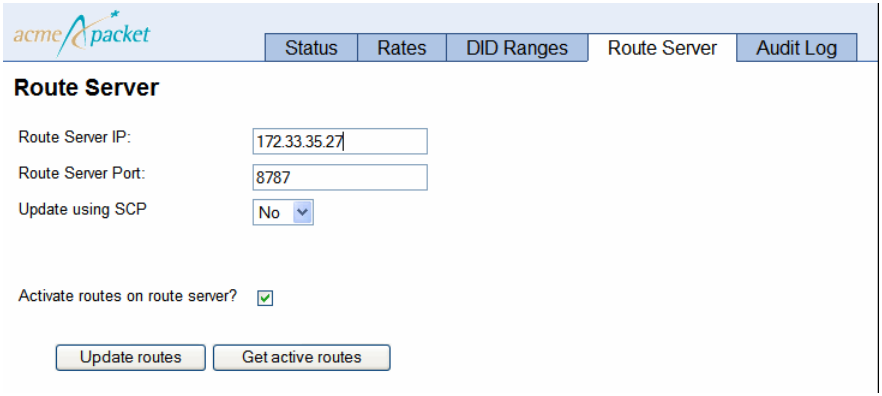
To use HTTP to download call rates files to the route server:

1. Under the **lcr-import-service** configuration object, set **protocol** to **https**.
2. Set the **port** number you are using to access the route-server import tool web interface.

3. Set **use-https-for-file-copy** to **disabled**. This configures the OS-E to use HTTP to download call rates files.

4. Update and save your configuration.
5. Log into the route-server import tool.
6. Under the **Route Server** tab set the **LCR Server IP** to the address of the OS-E interface.
7. Set the route-server **Port** to the port of the OS-E interface.

8. Set **Update using SCP** to **No**. When this property is set to **No**, the route-server import tool uses the value configured in the **use-https-for-file-copy**



For information on configuring SCP to download call rates files to the route server, see the *Net-Net OS-E Session Services Guide*.

OS-E DID Range Enhancements

In previous releases, the route-server import tool only managed individual DID numbers and imported Direct Inward Dial (DID) ranges by using prefixes. This consumed large amounts of memory and slowed down the route activation process. The route-server import tool can now import and manage DID ranges. This results in a significant reduction in memory consumption.

Existing rate routes in the route-server import database are preserved, but any previous DID route entries are deleted from the database. You must update your CSV files to the new format and reissue the DID range import to get your information into the new format.

Because of these changes, much of the route-server import tool has been affected. This section covers the changes caused by DID range support.

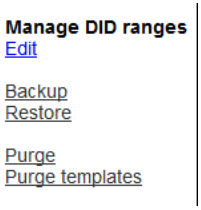
The route-server import tool validates all DID ranges during import, add, edit, slit, and replace functions. The following are the validation rules.

- Remove any trailing minus “-” and plus “+” signs in DID ranges.
- Required fields are **did-range-start**, **did-range-end**, and **carrier**. These values cannot be null or left empty.
- The DID range start value cannot be greater than the DID range end value.

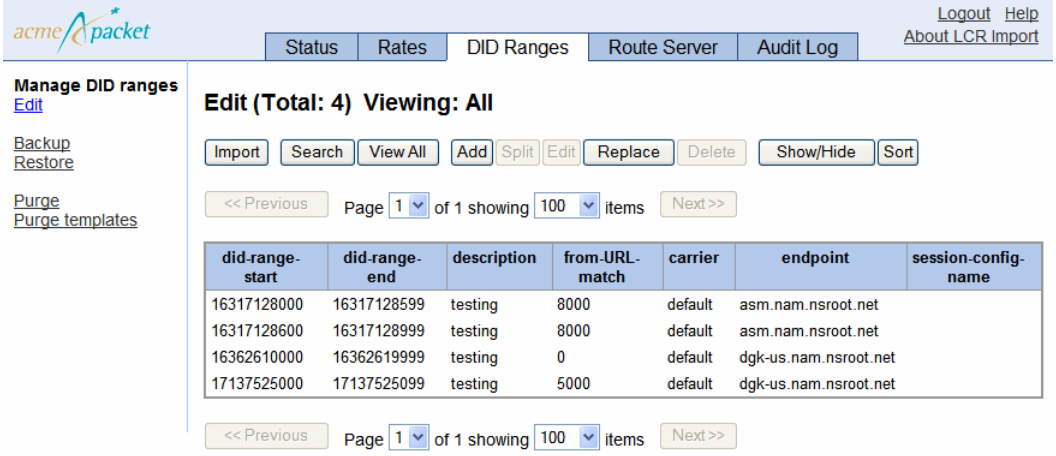
- Any alpha prefix for DID range start and end must be the same.
- The only situation where you can import or add DID rages which match existing DID routes, is a range that contains only one number, meaning the did-start-range equals the did-end-range.

Viewing and Editing DID Ranges

The **DID Mapping** tab has been renamed to **DID Ranges**. When you click on the **DID Ranges** tab, the following is displayed in the left pane. For users with read-only access, the **Backup**, **Restore**, **Purge**, and **Purge templates** links are disabled.



When you click on the **DID Ranges** tab, the default display in the right panel is the **Edit** display for viewing and editing DID ranges. Once you select a DID entry, the **Split**, **Edit**, and **Delete** buttons also become available.



Users who have read-only access may read the existing records, however, they will not be able to perform any modifications and the **Import**, **Add**, **Split**, **Edit**, **Replace**, and **Delete** buttons are inactive.

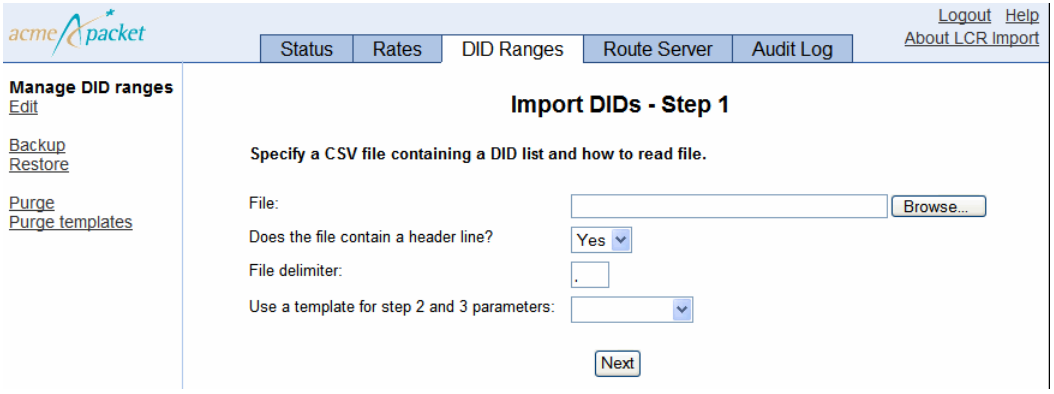
Importing DID ranges

The **DID Ranges** tab allows you to import DID ranges in a CSV file, backup DID configurations, restore a previous backup into the local database, view, edit, delete, create, and split DID mappings, and purge DID mappings and templates.

Importing DID Ranges — Step 1

There are five steps associated with importing DIDs. Step 1 requires that you locate and specify the name of the CSV file, as well as configure other settings.

- **File**—Browse to the directory containing the CSV DID file you are importing, provided by your carrier.
- **Does the file contain a header line?**—Specify **yes** or **no**. **Yes** means the DID file has a header line. **No** means there is no header line and in Step 2 you assign the columns by number.
- **File delimiter**—Enter the delimiter for the file. The default setting is the comma (,).
- **Use a template for step 2 and 3 parameters**—Specify a previously-created CSV columns mapping template if you have one configured and want to use it. Leave this field blank if you are not using a template.



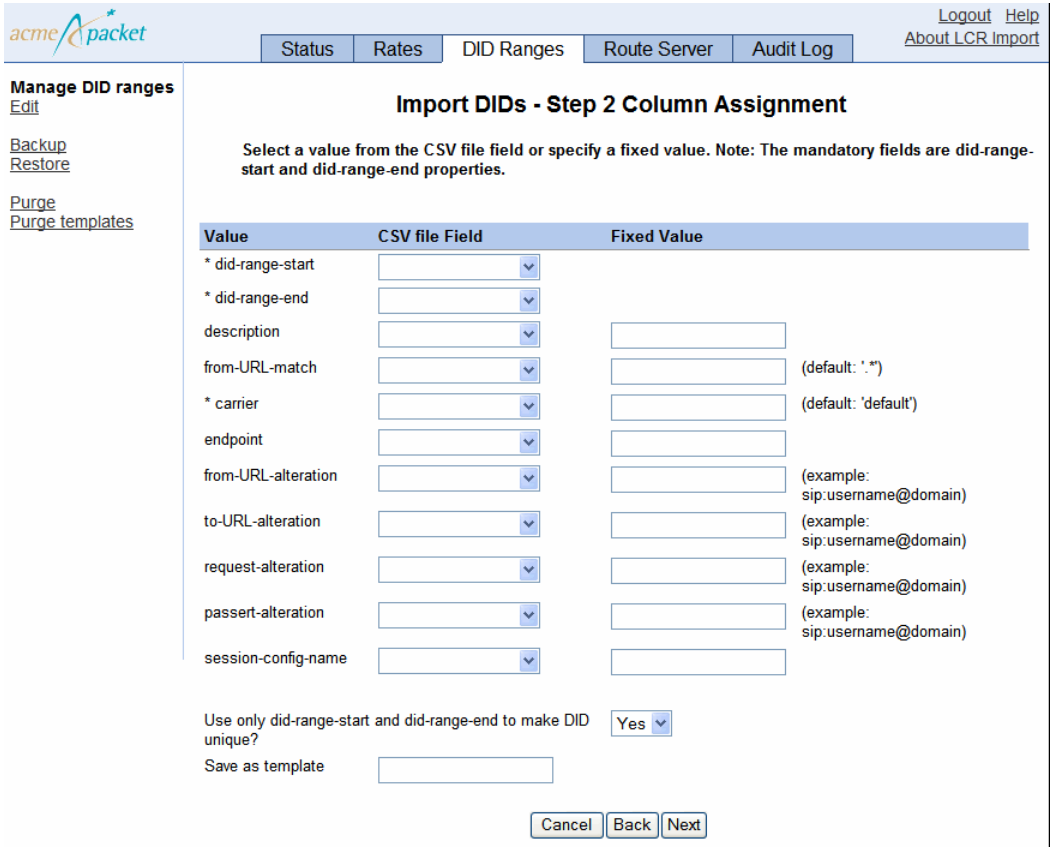
Click **Next** to proceed to Step 2.

Importing DID Ranges — Step 2

In Step 2 map the columns in your CSV file to the route-server import properties. If a header is present in the CSV file, the column headings can be used in the mapping. Otherwise, column numbers starting with 0 are used for mapping.

- **did-range-start**—Select the column from the CSV file that represents the start value of the DID range. This is a required field.
- **did-range-end**—Select the column from the CSV file that represents the end value of the DID range. This is a required field.
- **description**—Enter a description of this DID range.
- **from-URL-match**—Select the column from the CSV file that represents the From: URL field.
- **carrier**—Select the column from the CSV file that represents the carrier name. This is a required field.
- **endpoint**—Select the column from the CSV file that represents the endpoint name. This name needs to be in your configuration already.
- **from-URL-alteration**—Select the column from the CSV file that represents the alterations of the from-uri-specification.
- **to-URL-alteration**—Select the column from the CSV file that represents alterations of the to-url-specification.
- **request-alteration**—Select the column from the CSV file that represents the Request URI header.
- **passert-alteration**—Select the column from the CSV file that represents the number in the P-Asserted-Identity field.
- **session-config-name**—Select the column from the CSV file that represents a **session-config-pool** entry from the OS-E configuration.
- **Use only did-range-start and did-range-end to make DID unique?**—Select **Yes** if you want to only use the **did-range-start** and **did-range-end** values for matching.

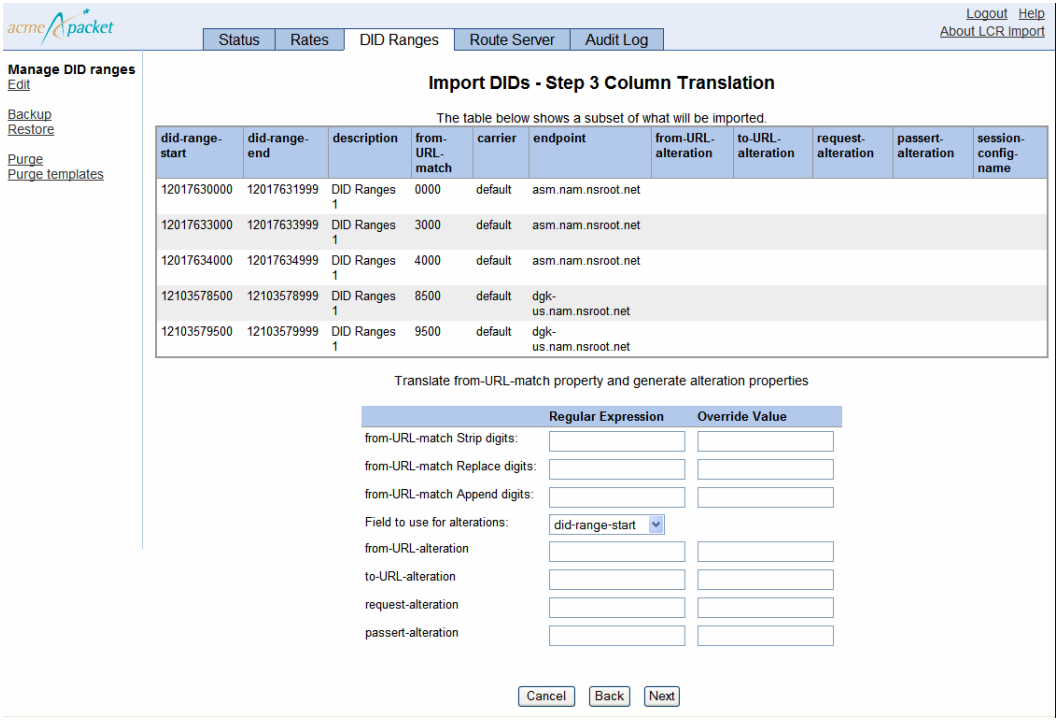
- **Save as template**—Saves the current column mappings to a name you specify. Once created, you can specify the named template in the Importing DID Ranges — Step 1.



Click **Next** to proceed to Step 3.

Importing DID Ranges — Step 3

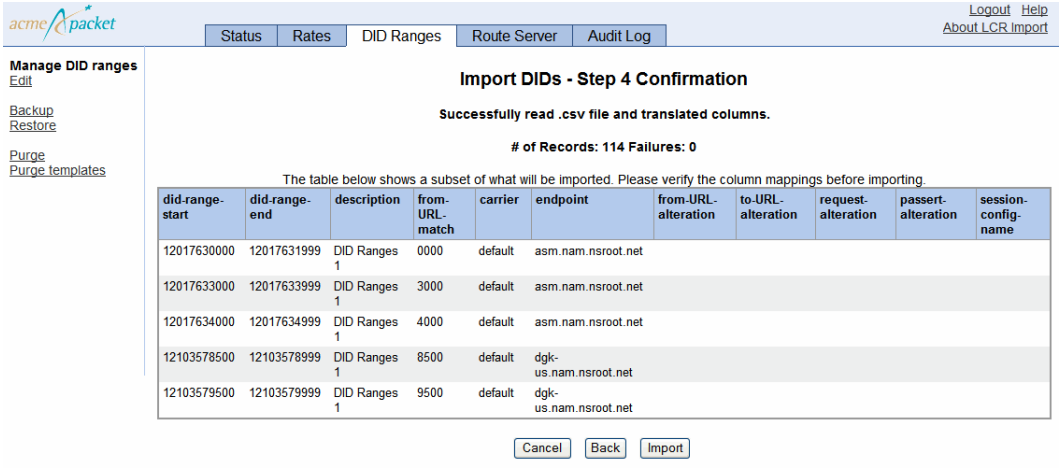
In Step 3 the route-server import reads the CSV file, reports any issues, and displays sample records for verifying that the CSV column to DID route record column assignment is correct. On this page you can also make any necessary translations using regular expressions.



Click **Next** to proceed to Step 4.

Importing DID Ranges — Step 4

In Step 4, the route-server import tool displays a preview of what is going to be imported after you have made any translations.



Click **Import**. The route-server import stores DID records constructed from the CSV file into the database

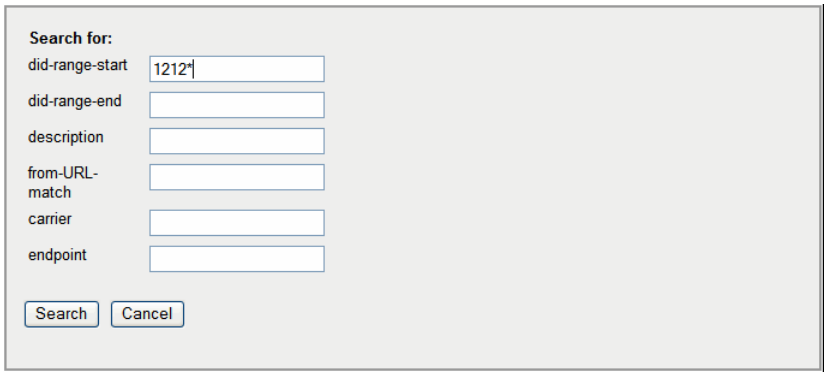
Importing DID Ranges — Step 5

In Step 5, you have the option to **Finish** the import, or to continue importing files.

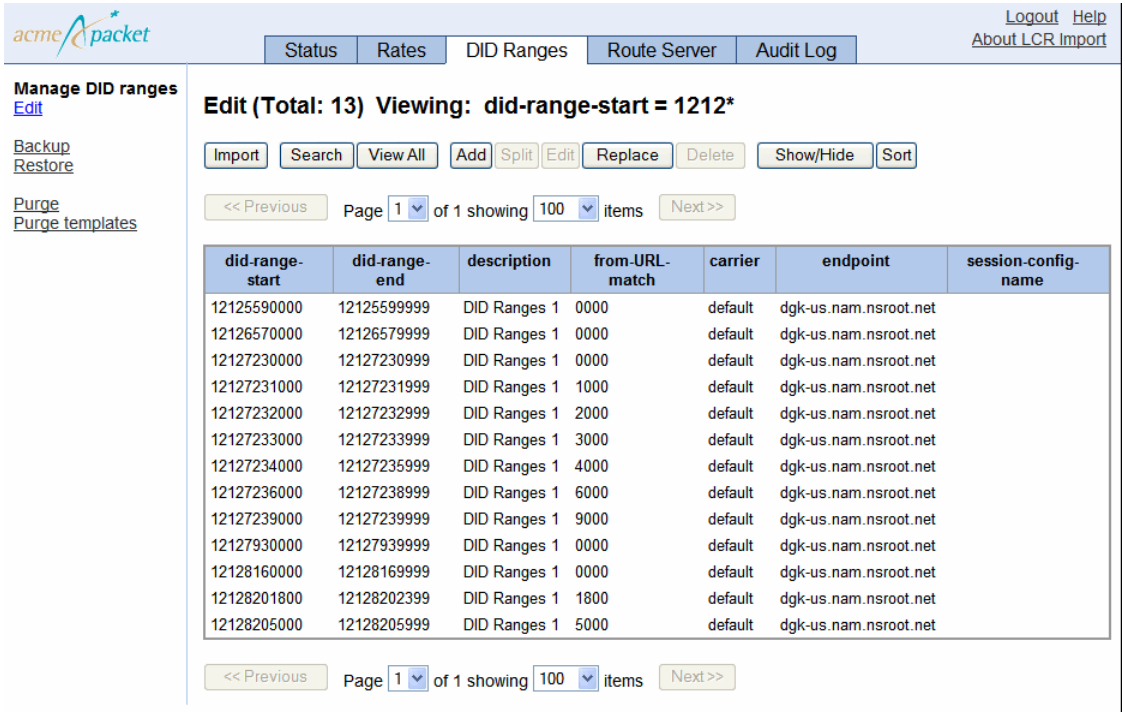
Once all imports are complete, you can then update the route-server by going to the **Route Server** tab. If you choose not to update the route server, clicking **Finish** returns you to the **DID Ranges** Edit/View display.

Searching DID Ranges

To narrow the view of what is displayed in the DID Ranges tab, click the **Search** button.



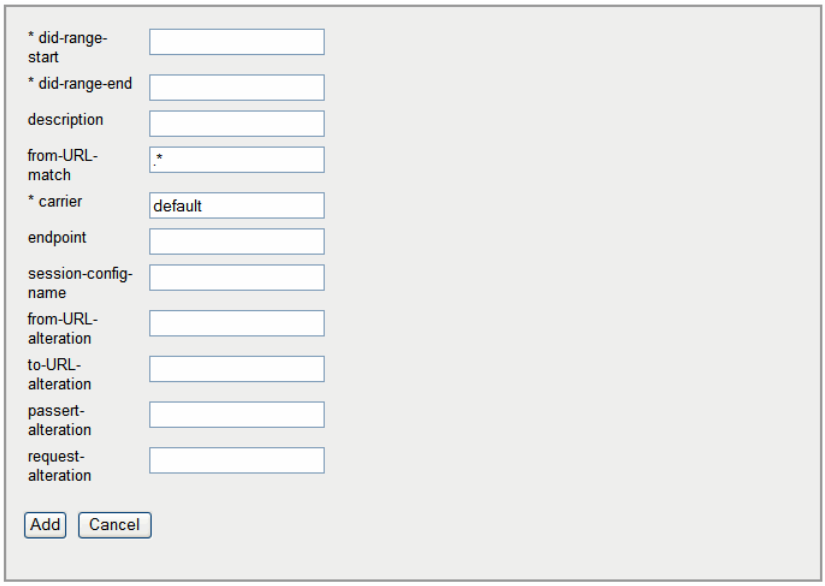
You can specify "*" as a wildcard in any position in the search string. This wildcard can match 0 or more characters. Below is the resulting filtered view from the above search.



Click the **View All** button to restore the DID Ranges tab to displaying all of the DID ranges present in the route-server import database.

Adding DID Ranges

To add a DID range, click the **Add** button.

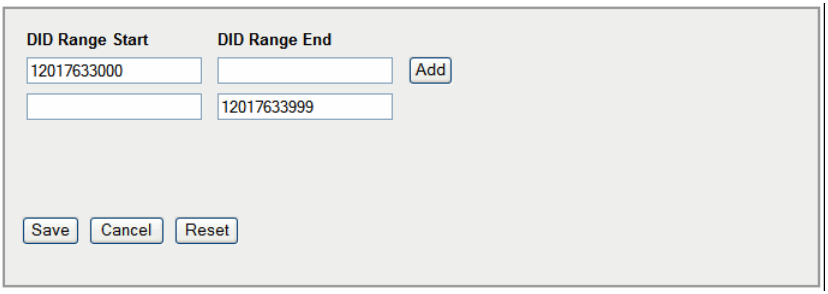


The **carrier** and **from-URL-match** properties are populated with default values. The only required fields to add a DID range are **did-range-start**, **did-range-end**, and **carrier**.

If you attempt to add a duplicate or overlapping DID range with a record already stored in the database, you receive an error message from the route-server import and the range is not added to the database.

Splitting DID Ranges

The route-server allows you to split a single existing DID range into two or more individual ranges. To split a DID range, select the DID route record you want to divide and click the **Split** button.



Only one split row can be added at a time, however, multiple split ranges within the same DID range are supported.

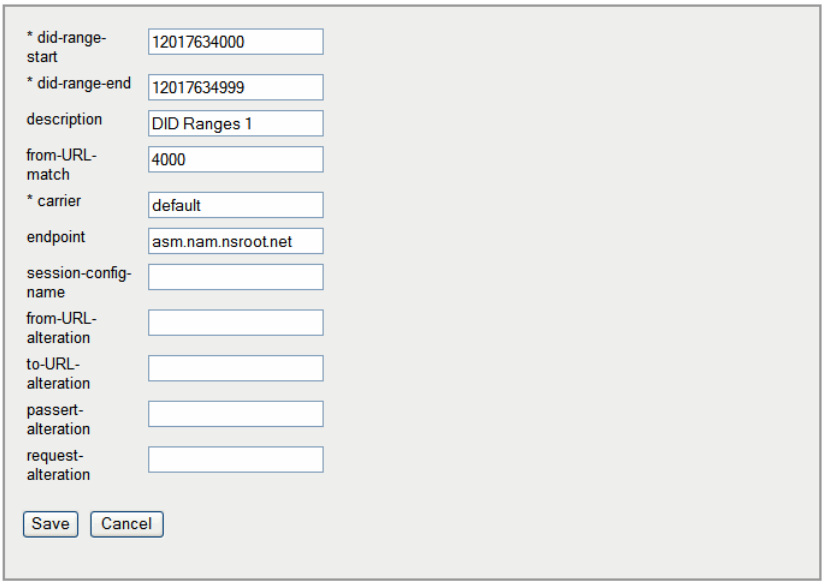
If you enter all **DID Range Start** values, the route-server import tool calculates the **DID Range End** automatically, or vice versa. You cannot, however, enter consecutive blank **DID Range Start** and **DID Range End** values.

If the selected DID range has an alphabetical prefix, the new ranges contain the same prefix.

Click **Add** to complete the splitting process.

Editing DID Ranges

To edit a DID range, select the DID route record and click **Edit**.

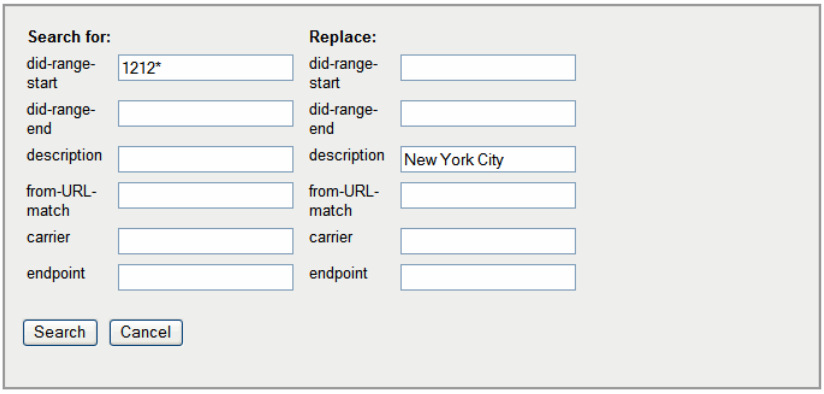


After you've made the changes you want to make, click **Save** to complete the editing process.

Replacing DID Ranges

Clicking the Replace button allows you to select DID ranges using a search criteria, and then replacing values in that selection with new values.

First specify search criteria and replacement values for each DID range in the selection.

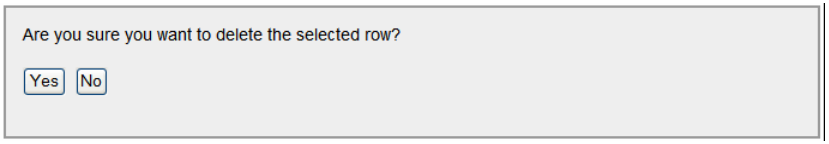


Click **Search.** The route-server import displays the number of records found and asks for confirmation.

Click **Replace** and the route-server import replaces values with the new values you specified.

Deleting a Range Route Record

To delete a DID route record, select the record in the display and click the **Delete** button. You see the following confirmation.

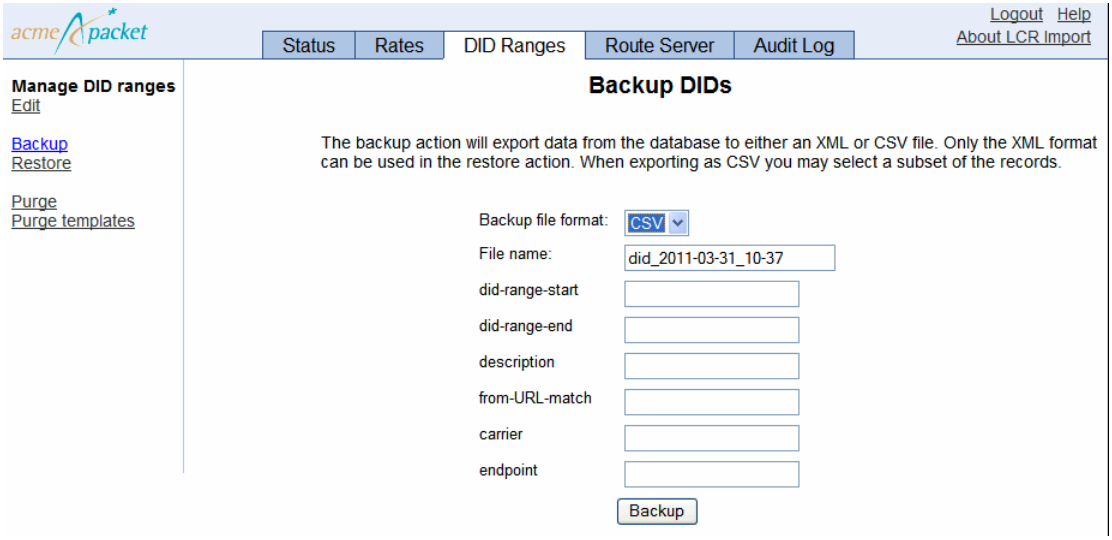


Click **Yes** to complete the deletion process.

Backing Up and Restoring DID Ranges

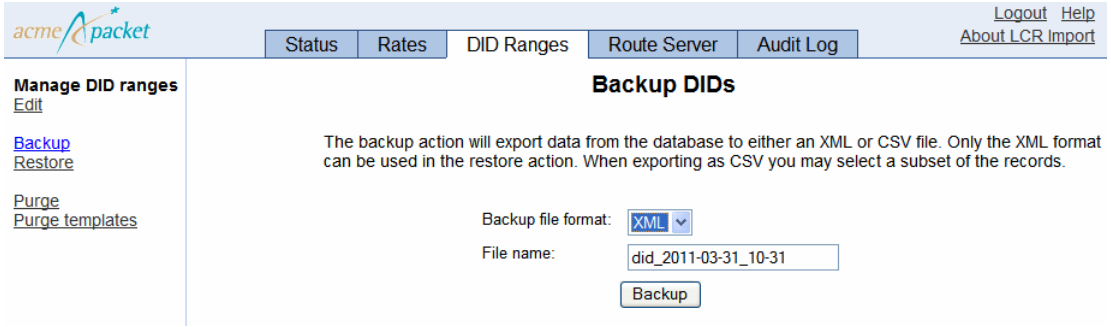
You can backup DID ranges using either an XML or CSV file. By default, the route-server import tool names the XML file with the date and time. If you want to name your file differently you can change this.

You can backup a subset of DID ranges based on specified criteria to a CSV file. If both **did-range-start** and **did-range-end** are specified, all DID ranges that match the DID range criteria will be included in the CSV file.



Click **Backup** to complete the backup process.. When the backup completes the route-server import tool displays a confirmation on the screen.

You can backup all of the DID ranges to an XML file. Click **Backup** in the left pane.



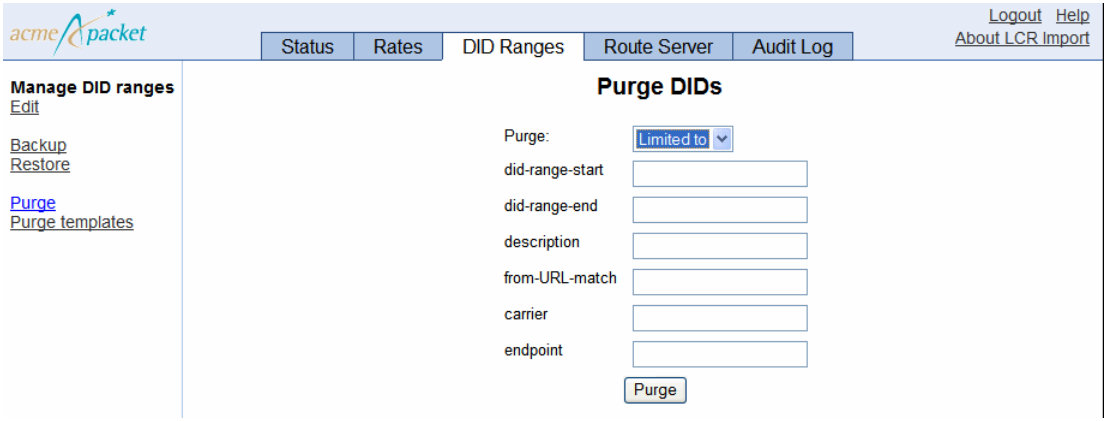
Click **Backup** to complete the backup process. When the backup completes the route-server import tool displays a confirmation on the screen.

Depending on how the file has been saved, there are two ways to restore a file onto the route-server import tool.

- Restore an XML file using the **Restore** link in the left pane. Browse to the XML file and click **Restore**.
- Restore a CSV file by reimporting it via the **Import** button.

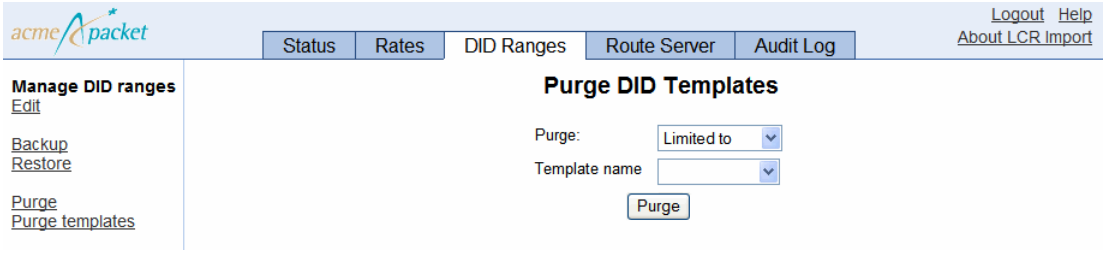
Purging DID Ranges and Templates from the Route-Server Import Tool

Use the **Purge** and **Purge DID Templates** functions from the left pane to remove DIDs and templates from the route-server import tool database. When purging DIDs, you have the option to purge **All DIDs**, or DIDs **Limited to** by specifying DID start and end range, description, from-URL-match, carrier, and endpoint.



Click **Purge** to complete the purging process.

When purging DID templates, you have the option to purge **All templates**, or templates **Limited to** a specific template name.



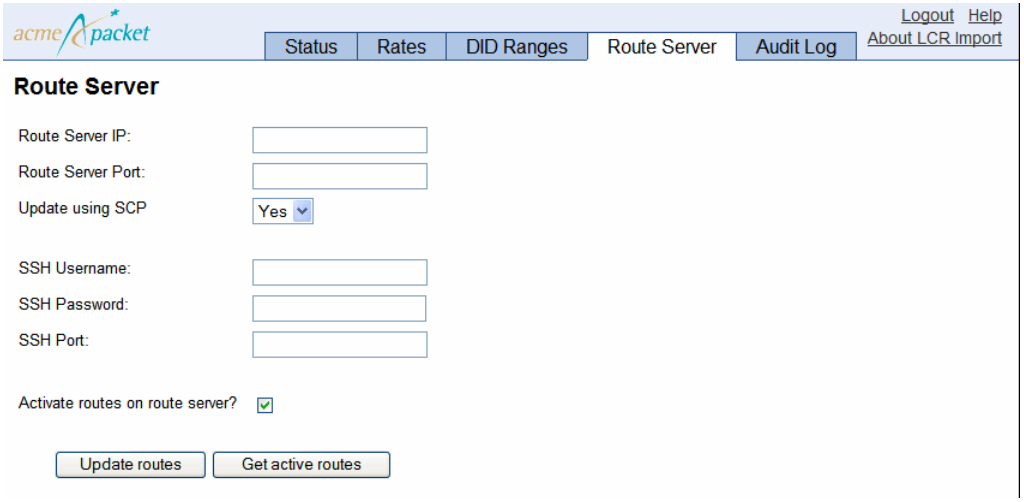
Click **Purge** to complete the purging process.

Updating the Route Server

Once you have imported DID ranges you must update the route server for your changes to take effect.

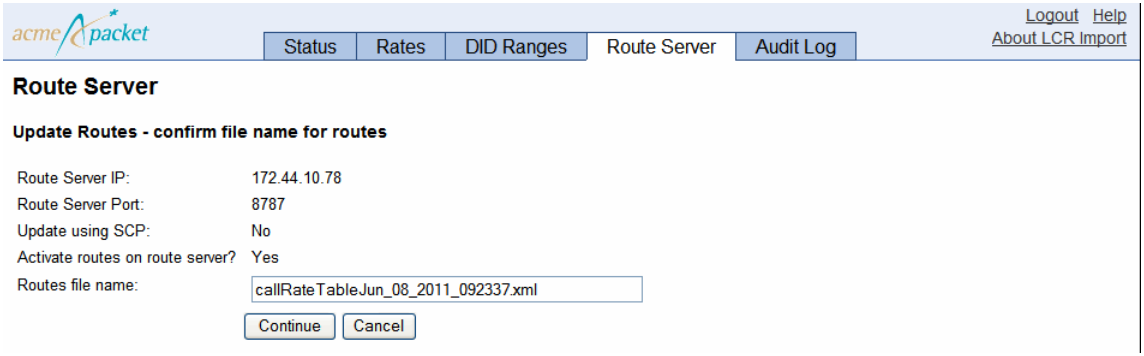
Click on the **Route Server** tab. Fill in route server IP and port information. This must be the IP and port that has the **web-service** configuration enabled on the route server. Then select the protocol you want to use to transfer files. If you are using SCP, you must specify a user name, password, and SSH port. For more information on supported protocols for file transfer, see HTTPS Support for Call Rates Downloading.

You can copy the routes over to the route server without making those routes active. To do that, uncheck the **Activate routes** checkbox. This allows you to test routes via the CLI route-server-test without them being the active route set.



Click **Update routes** to complete the update process. The display changes to show a progress bar, a description of the current stage of the route server update operation and a **Cancel** button.

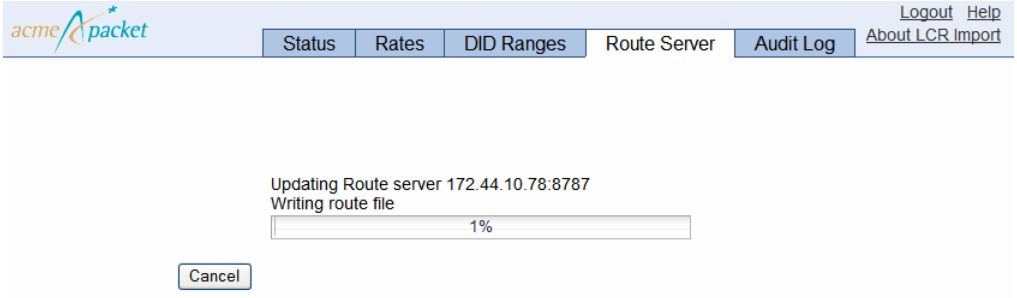
Before the update can complete you must confirm a file name for the routes. The route-server import displays a default file name, which is the name of the last file retrieved from the route server. You can either leave the default name or overwrite it to something else.



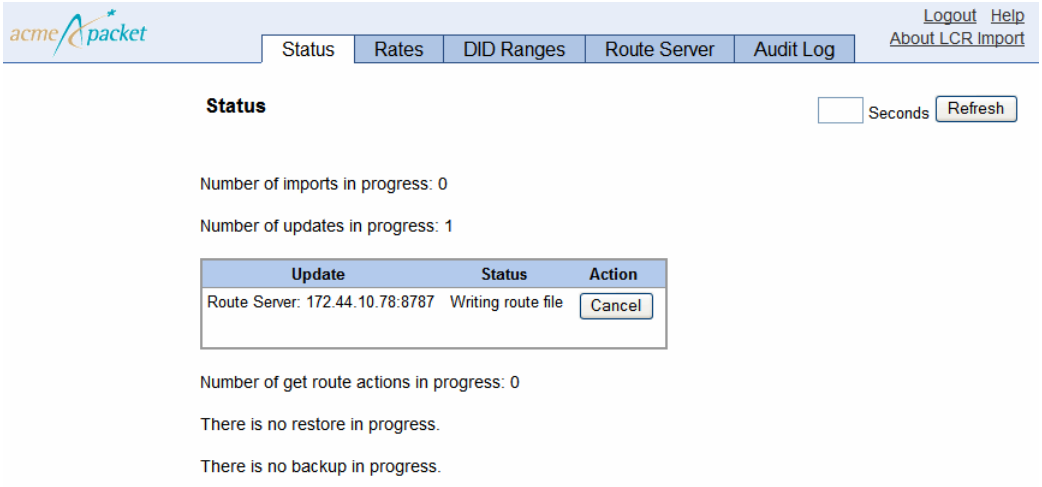
Click **Continue** to complete the route server update.

Cancelling a Route Server Update

There are two ways to cancel a route server update in progress. You can click the Cancel button on the **Route Server** tab.



Or you can click the **Cancel** button under the **Status** tab.

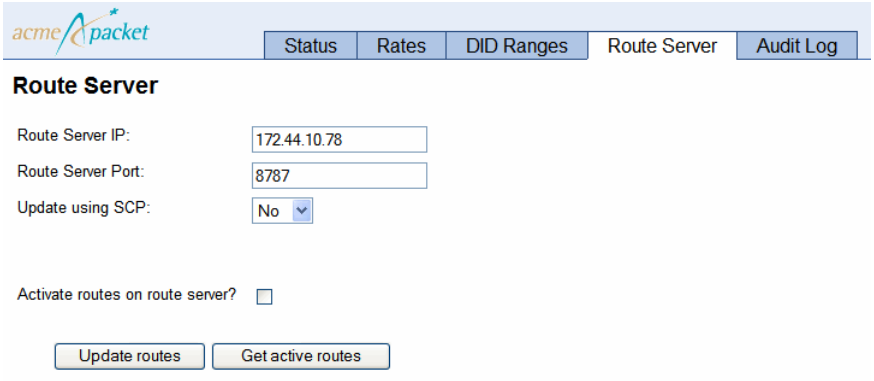


Retrieving Routes from the Route Server

Via the route-server import tool, you can retrieve the list of active route server files from the route server. The route server copies all of the active route set files, deletes all rates and DID ranges from the database, and reads the rate file into the database. These files are transferred via either HTTP, HTTPS, or SCP (depending on what you have configured).

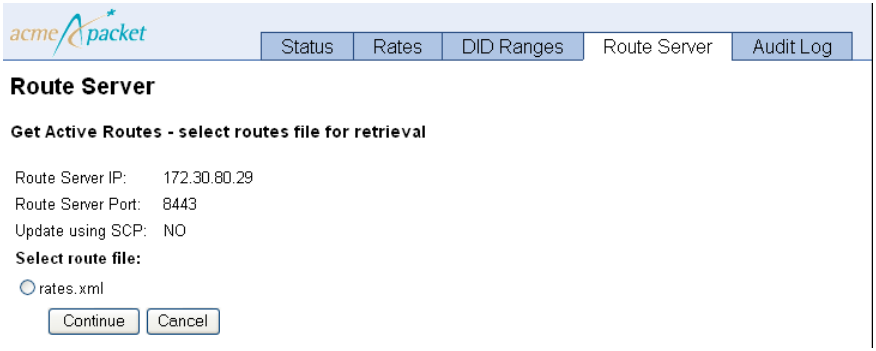
The route-server import tool loads the records to the database accordingly, based on whether the route set retrieved from the route server contains all DID ranges, all rates, or a mixture of DID ranges and rates.

To retrieve active routes from the route server, click on the **Route Server** tab. Fill in route server IP and port information. This must be the IP address and port configured in the **web-service** object on the route server. Select the protocol you are using to transfer files. If you are using SCP, specify a user name, password, and SSH port. For more information on supported protocols for file transfer, see the section, "HTTPS Support for Call Rates Downloading," in this guide.



Click **Get active routes**. A pop-up box appears reminding you that retrieving routes deletes existing rates and DID entries in the database. Click **OK** to complete the retrieval process. Once you confirm the operation, the route-server import tool displays a progress bar, description of the current stage of the operation and a **Cancel** button.

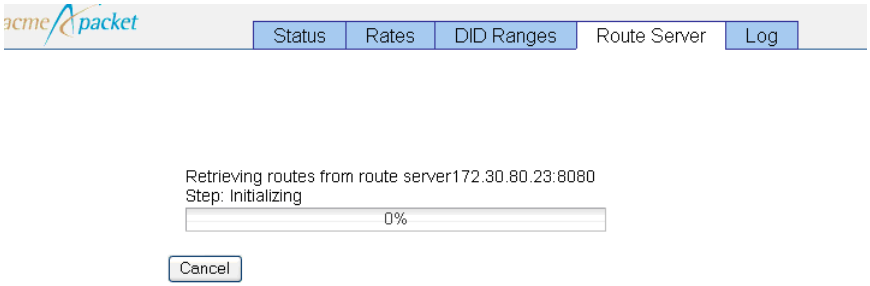
When retrieving routes, the route-server import tool reminds you that the current routes will be lost and you must confirm you want to finish the operation. A list of files is presented. Select the file you want to retrieve.



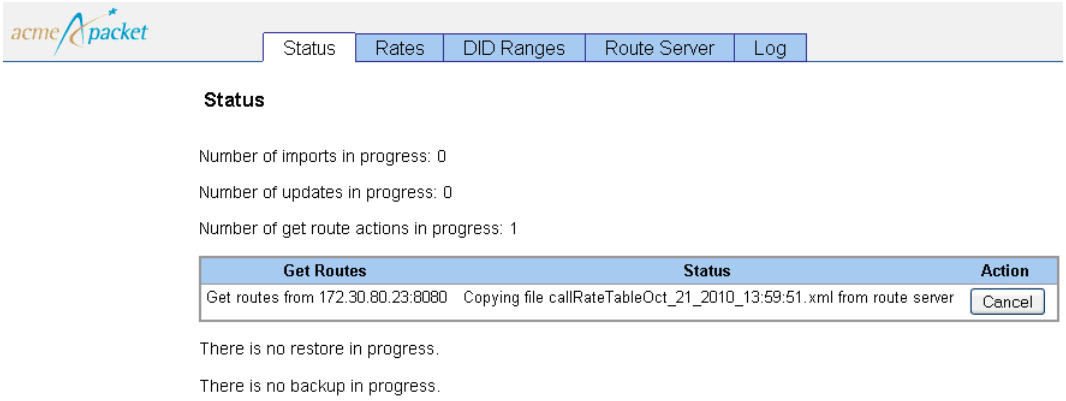
Click **Continue** to finish the retrieval process.

Cancelling Active Routes Retrieval

When you cancel a **Get Routes** operation, the route-server import tool restores the rates and/or DID entries for the backup that was created prior to when the **Get Routes** was initiated. There are two ways to cancel an active route retrieval in progress. You can click the Cancel button on the **Route Server** tab.

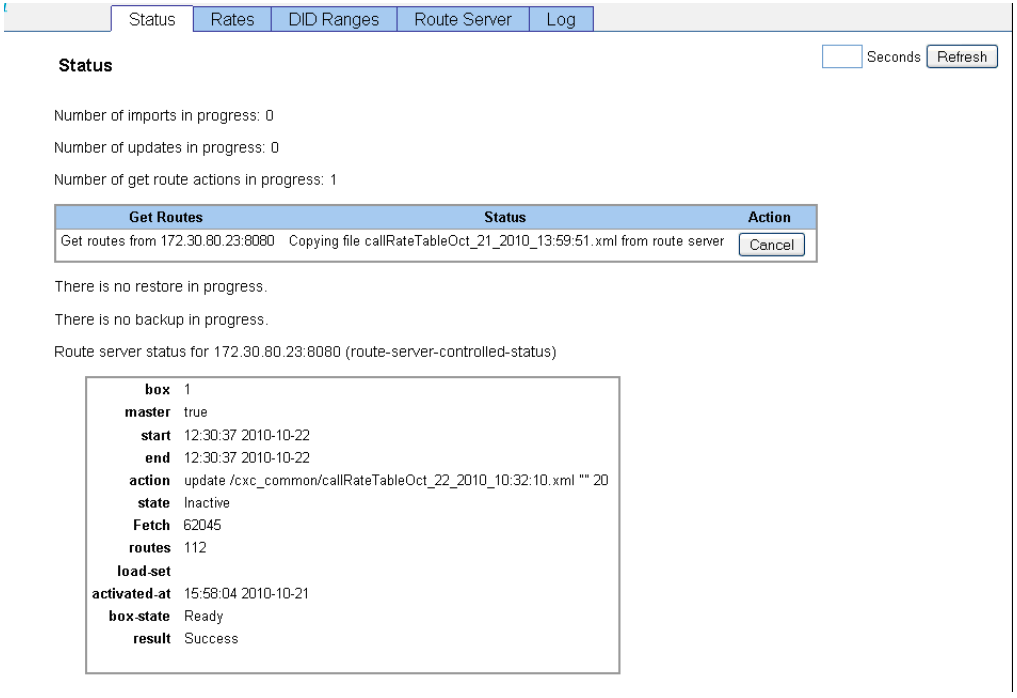


Or you can click the **Cancel** button under the **Status** tab.



Viewing the Status of Route-Server Import Operations

The route-server import tool status page displays import and route update operations in progress, **Get Route** operations in progress, and current **route-server-controlled-status** status report from the route server.



Testing DID Ranges and Prefix Changes

You can test imported DID ranges and prefix changes you have made in the route-server import tool before you activate them in a live environment. A new action has been created, **route-server-test**, that allows you to test routes, CDRs, and queries, and analyze, compare, and validate results of the routes.

```
NNOS-E>route-server-test ?

 Route server test action

 syntax: route-server-test config [file] [test-vector-file]
         route-server-test cdr file [test-vector-file]
        route-server-test lookup test-vector-file [test-results-file]
   [table]
         route-server-test analyze test-results-file
   [analysis-results-file]
```

```
      route-server-test compare test-results-file1
   test-results-file2 [diff-results-file]
      route-server-test validate test-results-file
   [validation-results-file] [table]
```

The **route-server-test config [*routes.xml*] [*test.xml*]** action generates a series of test vectors derived from the routes.xml file and outputs them to a specified test.xml file. If you do not specify a test.xml file, the OS-E writes the resulting output to the screen. The test.xml file has the following format.

```
<config xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="mgmt_data.xsd">
<RouteServerTestSuite suite="1">
 <description>DID 1000-1002</description>
 <tests>
  <RouteServerTestCase>
   <query>1000-1002</query>
   <from/>
   <time></time>
  </RouteServerTestCase>
 </tests>
</RouteServerTestSuite>
</config>
```

The **route-server-test cdr [*cdr.csv*] [*text.xml*]** action generates a series of test vectors derived from accounting records in the CSV format and outputs them to a specified test.xml file. If you do not specify a test.xml file, the OS-E writes the resulting output to the screen. The test.xml file has the following format.

```
<config xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="mgmt_data.xsd">
<RouteServerTestSuite suite="1">
 <description>DID 1000-1002</description>
 <tests>
  <RouteServerTestCase>
   <query>1000-1002</query>
   <from/>
   <time></time>
  </RouteServerTestCase>
 </tests>
</RouteServerTestSuite>
</config>
```

The CSV file has the following format.

```
"SessionID","Recorded","CallID","To","From","Method","IncomingRequestU
   RI","PreviousHopIp","PreviousHopVia","OutgoingRequestURI","NextHop
   Ip","NextHopDn","Header","Origin","SetupTime","ConnectTime","Disco
   nnectTime","DisconnectCause","Duration","scpName","CallID2","OrigG
   W","TermGW","PacketsReceivedOnSrcLeg","PacketsLostOnSrcLeg","Packe
   tsDiscardedOnSrcLeg","PdvOnSrcLeg","MaxJitterOnSrcLeg","CodecOnSrc
Leg","MimeTypeOnSrcLeg","LatencyOnSrcLeg","MaxLatencyOnSrcLeg","RFacto
   rOnSrcLeg","PacketsReceivedOnDestLeg","PacketsLostOnDestLeg","Pack
   etsDiscardedOnDestLeg","PdvOnDestLeg","MaxJitterOnDestLeg","CodecO
   nDestLeg","MimeTypeOnDestLeg","LatencyOnDestLeg","MaxLatencyOnDest
   Leg","RFactorOnDestLeg","Rx1000FactorOnDestLeg","Rx1000FactorOnSrc
   Leg","MOSFmtOnDestLeg","MOSFmtOnSrcLeg","callType","disconnectErro
   rType","ani","callSourceRegid","callDestRegid","newAni","cdrType",
   "huntingAttempts","callPDD","callSourceRealmName","callDestRealmNa
   me","callDestCRName","in_peer_dst","in_anchor_src","in_anchor_dst"
   ,"in_peer_src","out_peer_dst","out_anchor_src","out_anchor_dst","o
   ut_peer_src","calledPartyAfterSrcCallingPlan","lastStatusMessage",
   "LastMediaPktTimestampOnDestLeg","LastMediaPktTimestampOnSrcLeg","
   SetupTimeInt","IncomingURIStripped","dnis","newDnis","customData",
   "CreationTimestamp"
```

The **route-server-test lookup [*test.xml*] [*result.xml*] [*table*]** action uses the test vectors generated from the **route-server-test config** and **route-server-test cdr** actions and queries the route-server. The results of the queries are outputted to a specified results.xml file. If you do not specify a result.xml file, the OS-E writes the resulting output to the screen. The result.xml file has the following format.

```
<config xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="mgmt_data.xsd">
<RouteServerTestSuiteResults suite="1">
 <description>DID 1000-1002</description>
 <results>
  <RouteServerTestResult>
   <query>1000</query>
   <from/>
   <time></time>
   <routes>
    <RouteServerTestRouteResult>
     <match>route-plan:2</match>
     <carrier>default</carrier>
     <endpoint>example.net</endpoint>
    </RouteServerTestRouteResult>
   </routes>
  </RouteServerTestResult>
 </results>
 <results>
  <RouteServerTestResult>
   <query>1001</query>
   <from/>
   <time></time>
```

```
   <routes>
    <RouteServerTestRouteResult>
     <match>route-plan:2</match>
     <carrier>default</carrier>
     <endpoint>example.net</endpoint>
    </RouteServerTestRouteResult>
   </routes>
  </RouteServerTestResult>
 </results>
 <results>
  <RouteServerTestResult>
   <query>1002</query>
   <from/>
   <time></time>
   <routes>
    <RouteServerTestRouteResult>
     <match>route-plan:2</match>
     <carrier>default</carrier>
     <endpoint>example.net</endpoint>
    </RouteServerTestRouteResult>
   </routes>
  </RouteServerTestResult>
 </results>
</RouteServerTestSuiteResults>
</config>
```

You can also execute this action with the optional ***table*** parameter. This allows you to execute the lookup in a different routing table other than the currently active one.

The **route-server-test analyze [*results.xml*] [*analysis.xml*]** action analyzes the results file generated by the **route-server-test lookup** action and summarizes the results. The results of the analysis are outputted to a specified analysis.xml file. If you do not specify an analysis.xml file, the OS-E writes the resulting output to the screen. This action allows you to view how various resources are utilized with the current routing configuration being tested. The output of the analysis has the following format.

```
Analysis of results file : /tmp/results.xml
           Analysis created on : 13:09:56.729762 Mon 2010-11-01
             Total test suites : 1
              Total test cases : 3
     Total results with routes : 3
  Total results without routes : 0
          Smallest hunt result : 1
           Largest hunt result : 1

 Route position : 1
         Total : 3
--------------------------------------------------------------------------
        Carrier "default" referenced 3 times
```

```
            |--- Endpoint "example.net" referenced 3 times


        Route "route-plan:2" referenced 3 times

Queries with no route results:
--------------------------------------------------------------------------
None
```

The **route-server-test compare [*test-results-file1*] [*test-results-file2*] [*diff-results*]** action compares two results files and outputs the differences to a specified diff-results.xml file. If you do not specify a diff-results.xml file, the OS-E writes the output to the screen. The output of the comparison has the following format.

```
Comparing results from file /tmp/results.xml with /tmp/results2.xml
--------------------------------------------------------------------------
Test suite 1 "DID 1000-1002"
   |--- Query "1001"
          |--- Route 0
                 |--- name "route-plan:2" not equal "route-plan:3"
```

The **route-server-test validate [*results.xml*] [*output.xml*] [*table*]** action compares the results file with the active routes and outputs the differences to a specified validation-results.xml file. If you do not specify a validation-results.xml file, the OS-E writes the output to the screen. Any differences between the results.xml file and the active routing tables has the following format.

```
Comparing results from file /tmp/results.xml with /tmp/results2.xml
--------------------------------------------------------------------------
Test suite 1 "DID 1000-1002"
   |--- Query "1001"
          |--- Route 0
                 |--- name "route-plan:2" not equal "route-plan:3"
```

You can also execute this action with the optional ***table*** parameter. This allows you to execute the validation in a different routing table other than the currently active one.

Loading Route-Server Tables Without Activating Them

The **route-server** action has been enhanced to support loading route-server tables into memory without activating them.

The **route-server load** action allows you to load a route.xml file into a temporary non-active routing-table that can be referenced with the *table* name.

```
route-server load <file> <table>
```

The **route-server drop** action allows you to remove a previously loaded routing table from memory.

```
route-server drop <table>
```

The existing **route-server lookup** action has been enhanced to support two new parameters. You can now specify the table loaded into memory, as well as a time parameter to specify a query in the future in order to test time of day routing.

```
route-server lookup <to-url> [from-url] [table] [time] [display-mode]
```

Viewing Route-Server Statistics

The **show route-server-did** status provider allows you to display DID routes in a DID start to DID end range. This is helpful since, internally, DID routes are converted into prefix routes, making it harder for you to get a summary of active DID routes.

```
table range-start   range-end     carrier    endpoint       description
------  ----------   ------------   --------   ---------    ------------
active    78153000   78153999     default   example.net    Peru
active    97896000   97896999     default    example.net    Brazil
```

The existing **show route-server-table** status provider has been enhanced to show the table tag and route description. You can view the temporary routing-tables loaded into memory by specifying the table name. Also, a new user-defined description field and a did-entry-index has been added. When the did-entry-index is not “-1”, it can be used in conjunction with the **route-server-did** action to get more information on the DID entry.

```
tag       to-match      carrier     endpoint        description
------   ----------     --------    --------        -------------
active    612864*        default    example.net     Peru
active    8621289*       default    example.net     Brazil
```

DTMF Translation Framework

The OS-E now supports a new configuration model for DTMF translation, which simplifies the different ways to translate DTMF from one flavor to another. This model provides a centralized configuration for translating DTMF.

Among other things, the following improvements have been made:

- DTMF duration has improved to provide consistent and accurate reports of an event’s duration.

- The OS-E provides translation of the received DTMF volume from one method to another.
- The OS-E allows you to control how a DTMF event plays out by providing defaults for DTMF events, particularly when a DTMF method does not support these values.
- There are now minimum and maximum values for digit duration applied during translation.

In previous releases, DTMF translation was configured under the **vsp** > **session-config > in-dtmf-translation** and **out-dtmf-translation** objects. For the purpose of backwards compatibility, these objects are still supported, however, they are considered Advanced properties.

Two configuration objects have been created which now allow you to configure these preferences of one or more DTMF methods per call leg. These are configured under the **session-config** object; **in-dtmf-preferences** object applies to in-leg and **out-dtmf-preferences** applies to out-leg.

DTMF methods are configured based on their assigned preference. Preference values are ordered in the range of 1-100 with a 1 being the highest preference, 100 being the lowest preference.

The OS-E sends the DTMF to an endpoint based on the most preferred method that an endpoint is capable of supporting. If more than one DTMF method is specified with the same preference, and the endpoint negotiates the ability to support each of the DTMF methods, then the DTMF method sent is the first DTMF found in the list of supported methods.

The OS-E supports the following DTMF types:

- Audio
- RFC-2833
- SIP INFO-DTMF-Relay
- SIP-INFO-DTMF
- SIP NOTIFY
- H.245 alphanumeric
- H.245 Signal

- Q.931

To configure DTMF method preference, access the **in-dtmf-preferences** and **out-dtmf-preferences** objects under **session-config**.

```
NNOS-E>config vsp
config vsp>config default-session-config
config default-session-config>config in-dtmf-preferences
config in-dtmf-preferences>set preference audio 1
config in-dtmf-preferences>set preference sip-notify 2
config in-dtmf-preferences>return
config default-session-config>config out-dtmf-preferences
config out-dtmf-preferences>set admin enabled
config out-dtmf-preferences>set preference audio 1
config out-dtmf-preferences>set preference sip-notify 2
config out-dtmf-preferences>return
config default-session-config>return
```

For more information on these configuration properties, see the Configuration Changes in Release 3.6.0m4 section in this guide.

You also have the ability to control how the OS-E forwards DTMF tones in inbound and outbound calls via the **in-dtmf-settings** and **out-dtmf-settings**. These are configured under **session-config**.

To configure DTMF translation properties, access the **in-dtmf-settings** and **out-dtmf-settings** objects.

```
NNOS-E>config vsp
config vsp>config default-session-config
config default-session-config>config in-dtmf-settings
config in-dtmf-settings>set digit-volume -15
config in-dtmf-settings>set digit-duration 1000
config in-dtmf-settings>set min-digit-duration 50
config in-dtmf-settings>set max-digit-duration 5000
config in-dtmf-settings>set digit-duration-update 750
config in-dtmf-settings>set inter-digit-duration 300
config in-dtmf-settings>set pause-duration 4000
config in-dtmf-settings>set as-audio false
config in-dtmf-settings>return
config default-session-config>config out-dtmf-settings
config out-dtmf-settings>set digit-volume -15
config out-dtmf-settings>set digit-duration 1000
config out-dtmf-settings>set min-digit-duration 50
config out-dtmf-settings>set max-digit-duration 5000
config out-dtmf-settings>set digit-duration-update 750
config out-dtmf-settings>set inter-digit-duration 300
config out-dtmf-settings>set pause-duration 4000
config out-dtmf-settings>set as-audio false
```

```
config out-dtmf-settings>return
config default-session-config>return
```

For more information on these configuration properties, see the Configuration Changes in Release 3.6.0m4 section in this guide.

Threaded Session Mixing Action

A new session mixing action, **mix-session-threaded**, has been added to the OS-E. This action does the same thing as the **mix-session** action, but with improved performance from multi-threading:

The following is the **mix-session-threaded** syntax:

```
mix-session-threaded <session-id> <file> [output-channels]
    [wav-format] [recorded-path]
```

Valid wave formats are PCMU, PCMA, and PCM16.

In addition, an advanced property, **cluster > box > rtp-mixing-action-threads**, has been added to the configuration that allows you to select the number of threads that can be used for **mix-session-threaded** actions. The default setting is **automatic,** meaning the OS-E uses the platform-specific factory default value.

ARP Heartbeat Configuration on VM Clusters

In previous releases, in a VRRP implementation on either a VM system or within a complicated network, the OS-E would not always receive a link down event when the OS-E lost connectivity to the network.

A configuration object, **arp-heartbeat**, has been created that allows each VX to be associated with another OS-E on the network. In addition to sending periodic VRRP advertisements across the messaging interface, the OS-E sends ARP requests across the VX interface to the associated system.

If the ARP probe times out, the master OS-E knows that its connection to the network is broken. It then transitions into a “link-down” state and notifies the backup OS-E to take over. While in the link-down state, the OS-E periodically sends an ARP probe to continue checking the link. The OS-E stays in this state until it gets an ARP response. The OS-E is then able to take over the VX again if required.

The following is an example of an ARP heartbeat configuration:

```
config box
```

```
config interface eth0
 config ip a
  config arp-heartbeat
   set admin enabled
   set heartbeat-system 100.10.10.100
```

Dual HA Heartbeat Configuration Enhancements

In previous releases, when you configured a dual HA heartbeat, you had to configure an unused interface, assign it to the IP associated with the VRRP interface, and attach the messaging service.

Now the OS-E searches through the VX interfaces looking for one that is hosted on a single system and has messaging enabled. If the OS-E is unable to find a messaging interface while scanning the configuration, the OS-E falls back to the VX-only interface.

To configure this feature, configure dual HA the same way as before, leaving out the fake interface.

TCP/TLS Ephemeral Port Range Configuration

When using TCP/TLS as the transport method, the OS-E uses ephemeral ports for sending data. You can now configure the ephemeral port ranges. Well-known ports or ports configured for use with SIP and H.323 should not be allocated in the local port pool range.

Two advanced configuration elements, **tcp-ephemeral-port-start** and **tcp-ephemeral-port-end** have been created under the **services > network** object. You can configure each of these values between 1024 and 65535.

To view the TCP ephemeral port range, execute the **show network-settings** action.

Event Log Translation into SNMP Traps

The OS-E now has the ability to translate event logs into SNMP traps. When a log event is generated, the log system checks if the class and severity levels fall under any filters specified in the **event-log** config. If it is determined that this log event should be translated into an SNMP trap, the log system fills in the SNMP trap fields. Any interfaces that have SNMP targets configured transmit the trap.

The SNMP trap contains the following fields:

- Box ID
- Severity Level
- Process
- Log Class
- Log Message

The filter that the OS-E uses for the event-to-SNMP feature is a list of regular expression filters which you configure as a regular expression that runs on the generated log string. The OS-E first checks the “allowed-trap” list, then the “blocked-trap” list. When a log string does not match either list, it is allowed through. If it matches the “allowed” list, the log message is let through and the severity is modified. If it matches the “blocked” list, the log event is not generated.

In addition, a filter for each category type has been created. This filter contains each trap that falls under the filter. The following are the eight trap categories:

- CSTA
- DOS
- H.323
- LB
- SIP
- System
- TLS
- generic

This filtering mechanism is now available under each event log type.

Existing SNMP traps are not affected. These traps are transmitted regardless of the **event-log > snmp-trap** settings. When you use this in conjunction with legacy trap filters, the OS-E checks original filters first, then new filters.

The configuration to send and filter SNMP traps is configured in the **snmp** config object.

Two new configuration objects, **snmp-trap** and **advanced-filter**, have been created to support this feature. The following are examples:

```
config>config services
config services>config event-log
config event-log>config snmp-trap
Creating 'snmp-trap'
config snmp-trap>set admin enabled
config snmp-trap>set filter sipRouting debug
config snmp-trap>set filter sipSvr notice
config snmp-trap>set filter all error
config snmp-trap>return
config event-log>return
config services>return

config>config services
config services>config event-log
config event-log>config snmp-trap
Creating 'snmp-trap'
config snmp-trap>config advanced-filter
config advanced-filter>set allowed-event "SIP server peer (.+) server
   (.+) changed" info
config advanced-filter>set blocked-event (.*)
config advanced-filter>return
config snmp-trap>return
config event-log>return
config services>return
```

ToS Marking for H.323 Packets

The OS-E now supports Type of Service (ToS) marking for H.323 packets. The ToS value determines the quality of service that a call receives. The ToS byte in the IP header is used to mark packets for special consideration during routing. When the OS-E forwards a packet marked with a ToS value, this information is used by downstream routers to prioritize packet forwarding or perform other quality of service mechanisms.

When the OS-E receives an in-leg H.323 session with a ToS value set, you have the option to either forward this value to the out-leg session or override the in-leg ToS.

Additionally, when the OS-E receives an in-leg SIP session, you can either preserve the initial ToS value or override it in the out-leg during IW translation to H.323.

You configure in-leg and out-leg ToS settings for H.323 packets under the **session-config > h323-tos-settings**. The **h323-tos-settings > in-leg-tos > value** property determines the ToS value setting for the in-leg of the session. This ToS value determines the quality of service that the call receives. The OS-E marks the ToS field of all packets it sends out on the in-leg with the value you specify. Enter a number that represents the 8-bit Differentiated Services (DS) field of the IP packet in decimal format, such as 26 for 00011010 or 104 for 01101000. This value can be of use to upstream devices.

The **h323-tos-settings > out-leg-tos > value** property determines the ToS value setting for the out-leg of the session. This ToS value determines the quality of service that the call receives. If set to **preserve**, the OS-E uses the ToS value in the first received message of the session. If set to **overwrite**, the OS-E marks the ToS field of all packets it sends out on the in-leg with the value you specify. Enter a number that represents the 8-bit Differentiated Services (DS) field of the IP packet in decimal format, such as 26 for 00011010 or 104 for 01101000. This value can be of use to upstream devices.

```
config vsp>config policies
config policies>config session-policies
config session-policies>config policy 1
Creating 'policy 1'
config policy 1>config rule 1
Creating 'rule 1'
config rule 1>config session-config
config session-config>config h323-tos-settings
config h323-tos-settings>config in-leg-tos
config in-leg-tos>set value 4
config in-leg-tos>return
config h323-tos-settings>config out-leg-tos
config out-leg-tos>set value overwrite 4
config out-leg-tos>return
config h323-tos-settings>return
```

For messages that are sent without a session, you can configure ToS for the H.323 gateway.

```
config>config vsp
config vsp>config enterprise
config enterprise>config servers
config servers>config h323-server server1
config h323-server server1>set domain 10.33.80.58
config h323-server server1>config server-pool
config server-pool>config server server2
Creating 'server server2'
config server server2>set host 10.33.80.58
config server server2>set transport tcp
```

```
config server server2>set port 1720
config server server2>set connection-role responder
config server server2>return
config server-pool>return
config h323-server server1>config h323-ras-settings
config h323-ras-settings>set tos 4
config h323-ras-settings>return
```

For messages sent via TCP, the ECN field (the least significant two bits of the ToS) can neither be preserved nor overwritten by the OS-E. For these sessions, the ECN field in outgoing packets is always marked as zero, regardless of the incoming or overwritten value.

Additionally, if TLS over TCP is supported via H.235, the ToS value cannot be preserved, but it can be overwritten to the same ECN limitation as TCP.

302 Redirect Messages for Cross-Cluster Load Balancing

The 302 redirect feature is a cross-cluster load balancing solution. In previous releases, when a carrier trunk was statically connected to an OS-E cluster and that cluster reached its session limit, the trunk was unable to hunt to another cluster.

The OS-E can now be configured to generate a 302 Redirect message when a configurable session threshold has been reached. The contact address of the 302 is the SIP contact address of another OS-E cluster.

Each cluster that participates in the redirect pool is configured with contact information for all other clusters (including itself). It also contains cross-cluster 302 redirect call statistics. These redirect call statistics are used to select the redirect target cluster by calculating weights based on current, max, and total call capacities.

Under the **forking-settings** object, in addition to **sequential** and **parallel**, there is a new **forking-type** called **redirect**. This must be enabled in order for 302 redirect to work.

Also, a new outbound arbiter rule type, **weighted-round-robin,** is now available under the **forking-settings** config object. When configured for **sequential** and **parallel** hunting, the legacy call admission control counters are used as inputs into the weighted round robin algorithm. For **redirect** hunting, the redirect call statistics are used as inputs into the algorithm.

```
config>config vsp
config vsp>config session-config-pool
config session-config-pool>config entry redirection
```

```
Creating 'entry redirection'
config entry redirection>config forking-settings
config forking-settings>set forking-type redirect
config forking-settings>set outbound-arbiter-rule weighted-round-robin
config forking-settings>return
```

There is a new set of call counters used for 302 redirects via the **show sip-server-redirect** action.

```
NNOS-E>show sip-server-redirect

gateway             peer                current    maximum    total
-------             ----                -------    -------    -----
RedirectClusters      cluster-Moog/Neely    0         1000      0
RedirectClusters     cluster-Butler/Thacker 0         50        0
SIPp-A                 SIPp1                    0          50    ` 0
```

Properties

Field	Description
gateway	The name of each configured gateway.
peer	The name of each gateway's configured peer.
current	Indicates the current weight relative to the maximum. This value resets by either all gateways reaching their maximum weights or the cross cluster stats being reported.
maximum	The maximum session threshold for each gateway.
total	A count of the number of redirects sent to a server.

A new **session-config** object, **overflow-route**, allows the OS-E to override the dial plan route once a configurable threshold has been reached. This object allows you to configure the session **limit** and the **peer** to use once the threshold has been reached.

```
config>config vsp
config vsp>config session-config-pool
config session-config-pool>config entry 1
Creating 'entry 1'
config entry 1>config overflow-route
config overflow-route>set limit 100
config overflow-route>set peer server
   "vsp\enterprise\servers\sip-gateway RedirectClusters"
config overflow-route>return
```

Additionally, two advanced configuration properties have been created under the **server-pool** config object that allow you to configure cross-cluster statistics collection. The **remote-web-services** property configures the HTTP address of the cluster web services' remote web service address. When this property is configured, the OS-E makes a web service request to that address and stores the session information returned as the redirect statistics. The **remote-web-services-fetch-timer** property configures the interval used to collect these statistics.

```
config>config vsp
config vsp>config enterprise
config enterprise>config servers
config servers>config sip-gateway gw1
Creating 'sip-gateway gw1'
config sip-gateway gw1>config server-pool
config server-pool>set remote-web-services-fetch-timer 5000
config server-pool>config server server1
Creating 'server server1'
config server server1>set remote-web-services http://170.30.0.11:8080
config server server1>return
```

Two pieces of information are returned in response to the **remote-web-services** query:

- The active session count
- The maximum redirect session count

By default, the redirect session limit is the enforced session limit on that OS-E, however this setting can be overridden with the **static-stack-settings > max-redirect-sessions** advanced property.

```
config vsp>config static-stack-settings
config static-stack-settings>set max-redirect-sessions 100
config static-stack-settings>return
```

Unlike other **static-stack-settings**, this does not require a VSP reset to take effect. When cluster statistics are reported, it is considered a "refresh event" for the weighted round robin algorithm. The reported statistics overwrite any locally calculated redirect statistics.

You can prohibit a redirect for certain previously redirected sessions by setting the **sip-settings > allow-redirect** parameter to **disabled**. In this situation, the OS-E responds with a 503.

```
config vsp>config default-session-config
config default-session-config>config sip-settings
config sip-settings>set allow-redirect disabled
config sip-settings>return
```

Archiving Enhancements

The OS-E now supports archiving as an accounting target, configured under the **accounting** object. Archiving targets can be configured as either **archive-local** or **archive-external**.

The existing (pre-3.6m4) configuration is still available as an Advanced property under the **accounting > archiving** object. However, Acme Packet recomments using the new per-session archiving. Also, only one target, either external or local, should be configured at a time.

Also, this new archiving uses the **mix-session-threaded** action to mix sessions. This allows the archiving to handle a higher call load. The existing (pre-3.6m4) archiving continues to use the **mix-session** action.

The following are enhancements to archiving functionality:

- Archiving is configurable on a per-session basis as opposed to per-OS-E system.
- Additional protocols, SFTP and SCP, are supported for sending archives to remote locations.
- Archiving is always continuous; as a call ends it is archived immediately.

Once the archiving functionality is enabled and configured on the OS-E, the archiver listens for requests from the accounting server. A request from the server tells the archiver that there are calls that needs to be archived. The archiver creates a task for each CDR. This task gathers data to put in the archive by executing actions and status requests and querying databases.

The archiving target cycles through two states:

- Clear—The target is ready to handle requests.
- Blocked—The target has reached the maximum number of files it can save. You must remove saved archives to enable the target to start processing again.

When the OS-E sends an archive to a remote location and the send fails, the OS-E retries sending the archive as many times as it is configured to do so. If all retries fail, the OS-E saves the archive in the archive-save-folder and logs a message similar to the following.

```
Warning: "Target archive-test, saved 1234.zip containing records 1000
   to 1000 as /ɔxc_common/archive/saved/1234.zip (failure was: Connect
   timed out)"
```

You can configure the number of archives that can be saved in the archive-save-folder via the **max-saved-on-send-failure** property under the archive-external and archive-local objects. Once the OS-E hits this threshold, the target enters the "Blocked" state and stops processing any more CDRs until the saved archives are removed from the folder. When this condition is reached, the OS-E logs a message similar to the following:

```
Critical: "Target archive-test cannot process any more CDRs because
    the maximum of 200 archives that can be saved locally on failure is
    met or exceeded. Delete saved archives to enable further
    processing.
```

Note that the number of saved archives may be slightly higher than the configured number. This is because archives are not created in order and it is possible that some newer CDRs finished processing earlier than the archive that finally blocked the target.

Due to accounting server purges, there may be missing CDRs. The OS-E handles missing records by skipping over them and continuing the process. Missing records are logged and can be viewed in the status provider.

During an HA failover, the target on the new master OS-E picks up from where the previous master OS-E left off.

You configure the archiving targets under the **vsp > accounting** object.

```
vsp
 accounting
  admin enabled
  duration-type default
  retention-period 0 days 00:01:00
  subdirectory-size 100 records
  purge-criteria purge-always
  radius
  database
  syslog
  file-system
  external-file-system
  archiving
  purge-check-interval 0 days 01:00:00
  purge-disk-utilization-percent 90 %
  archive-local
  archive-external
  archive-worker-threads automatic
  archive-max-inprogress 120
  archive-tries 2
  archive-name-format[1] recordID
```

```
  compatible-archives false
  server-idle-timeout 300
```

For more information on the new archiving configuration properties, see the Configuration Changes in Release 3.6.0m4 section in this guide.

The target can then be applied to a session-config via the **session-config** > **accounting** object.

```
config vsp>config default-session-config
config default-session-config>config accounting
config accounting>set target archive-external-file-system
   "vsp\accounting\archive-external\url""archivetest""
```

You can view information regarding archive targets using the following status providers.

The **show accounting-targets** action is a previously existing status provider that displays summary data from all accounting targets. This status action now includes archiving targets.

```
NNOS-E>show accounting-targets

                    type: archive-external
                    name: url archive-day1
                received: 641 CDRs
               processed: 641 CDRs
                failures: 0
          missing-records: 0
        last-acked-record: 1495276
     acked-pending-record: 1495276
average-processing-time: 2278 milliseconds/CDR
```

Field	Description
type	The type of file system target this command is displaying.
name	The name of the accounting target whose status is displayed.
received	The number of raw CDRs received.
processed	The number of CDRs processed by this target.
failures	The number of failures.
missing-records	The number of raw CDRs the target found missing and could not write to the output. These messages may be missing, corrupt, or could have been caused by a purge. Check logs for details.

Field	Description
last-acked-record	The last CDR processed completely by the target when requested by the accounting master.
acked-pending-record	The last CDR started by the target, but that has not yet completed processing.
average-processing-time	The average processing time per CDR of this accounting target.

The **show accounting-targets-archive** action displays detailed information regarding archive targets.

```
NNOS-E>show accounting-targets-archive

               name: archive-day1
                url: http://172.40.100.1/cgi-bin/
  archive_http_upload_example_null.pl/dev/null
 tasks-in-progress: 0
          received: 641 CDRs
       in-progress: 0
              sent: 0 archives
             saved: 0
     archive-fails: 0
     create-errors: 0
   transmit-errors: 0
             state: clear
     current-saved: 0
last-commit-success: 16:12:35 Tue 2011-03-22
 average-time-taken: 228 msec/archive
```

Field	Description
name	The name of the displayed archiving target.
url	The URL of this external archiving target.
tasks-in-progress	The number of archiving tasks currently in progress.
received	The number of raw CDRs received.
processed	The number of raw CDRs processed.
sent	The number of archive files sent to the archiving target.
archive-fails	The number of failures that occurred during the archiving process.

Field	Description
create-errors	The number of errors that occurred during the creation of the archive file.
transmit-errors	The number of errors that occurred during the transmission of the archive file.
saved	The number of saved CDRs.
state	The state of the archiving target.
last-commit-success	The last time the OS-E successfully sent a file to the archiving target.
average-time-taken	The average processing time per CDR of this archiving target.

Adding a **-v** to this command displays a verbose status.

The **show accounting-targets-archive-tasks** action displays information about currently running archiving tasks on the OS-E.

```
NNOS-E>show accounting-targets-archive-tasks

name record              errors     in-progress
------                 ------     -----------
nnose-backup                1170995            2          (send)
nnose-backup               1171000             2          (send)
nnose-backup                1171001            2          (send)
```

Field	Description
name	The name of the archiving target.
record	The CDR ID that the archive target is processing.
errors	The number of errors encountered while this CDR is being processed. These are errors that do not stop processing. For example if a send has failed but there are retries left.
in-progress	A task is the processing for a CDR. A task has several operations it performs. This property shows the operations within the task currently in progress.

Adding a **-v** to this command displays a verbose status.

Server State Detection via OPTIONS PING Response

Functionality has been created that allows you to modify how the OS-E decides when to mark a server up or down. In previous releases, when the **server > failover-detection** property was set to **ping**, the OS-E sent an OPTIONS ping to the server. If the OS-E received no response back, the server was considered down. If any SIP response was received, the server was considered to be in service. However, it was possible for a remote server to send a SIP error in response to the OS-E ping, indicating it was in a down state, and the OS-E would still think it was up.

A new configuration property, **ping-mode,** has been created under the **sip-gateway> server** and the **dns-group > server**.

```
config vsp>config enterprise
config enterprise>config servers
config servers>config sip-gateway gw1
config sip-gateway gw1>config server-pool
config server-pool>config server server1
config server server1>set ping-mode restricted
config server server1>return

Maxwell>config vsp
config vsp>config enterprise
config enterprise>config servers
config servers>config dns-group dns1
config dns-group dns1>set ping-mode restricted
config dns-group dns1>return
```

This property can either be set to Promiscuous Mode or Restricted Mode.

- Promiscuous Mode—When an OPTIONS ping is sent to the server, if any response is received, the server is considered up. The server is only considered down if it times out. This is the default behavior.
- Restricted Mode—When an OPTIONS ping is sent to the server, it is only considered up if the OS-E receives a 200OK response from the server.

RTCP QoS Accounting

In previous releases, when the OS-E received RTCP packets from an endpoint, the packets were sent directly to the database.

The OS-E is now able to analyze this RTCP data and report it in accounting records. This gives better visibility into the fate of RTP packets as they travel from the OS-E to their destination.

The OS-E accumulates the RTP statistics data received from the endpoint in the RTCP logging session for the duration of the call. The statistics collected from the RTCP packets are:

- Packets lost—The total number of RTP data packets lost since the beginning of the reception. This number is defined as the number of packets expected minus the number of packets actually received. This number received includes late or duplicate packets. Therefore the loss could be negative.
- Interarrival jitter—An estimate of the statistical variance of the RTP data packet interarrival time, measured in timestamp units. This value is expressed as an insigned integer.
- R-factor—Calculated based on the codec used.
- MOS—Collected using jitter, packet delay, r-factor, total packets, and packets lost.

When the call is terminated and the accounting data is collected, the final RTCP statistics are calculated and made available for inclusion in the accounting records.

Latency is not currently supported and is assumed to be 0 for any calculations.

To enable this feature, the **session-config > media > rtp-stats** property must be set to **enabled** and the **rtcp log** must be set to **true**.

```
config>config vsp
config vsp>config default-session-config
config default-session-config>config media
config media>set rtp-stats enabled
config media>set rtcp drop true
config media>return
config default-session-config>return
```

Called Party Name Interworking

Both SIP UAs and H.323 terminals are capable of providing information about their local communicating parties. If this communicating party information is supplied in the call-initiating message (ie., in an INVITE or SETUP message), the information identifies the calling party. If the information is supplied in a subsequent message, the information identifies the called party.

H.323 uses the Q.931 Display Information Element (IE) to communicate this information. SIP communicates this information via either an Asserted-Identity header or a To or From header display name.

When the H.323 stack receives a Q.931 message containing a Display IE, the stack moves the identifying information to the ooCall object (the internal object that stores call state and other call-related information), storing the information as either the caller or the called.When the H.323 stack communicates this event to the SIP process, H.323 stores this identifying information in the H.323 -> SIP interprocess (IPC) message.

To configure this feature, the **q931-settings** object's **use-display-ie** and **use-pai-for-iw-call** properties must be configured. Based on the message type and configuration settings, the following table shows where this calling party information is stored in the IPC message.

	Configuration Settings		**H.323->SIP IPC Message**		
Msg Type	**use-display-ie**	**use-pai-for-iw-calls**	**fromDisplay**	**toDisplay**	**pAssertedIdentity**
Setup	True	True	Empty	Empty	Display IE
	True	False	Display IE	Empty	Empty
	False	True or False	Empty	Empty	Empty
Proceeding	True	True	Empty	Empty	Display IE
	True	False	Empty	Display IE	Empty
	False	True or False	Empty	Empty	Empty
Alerting	True	True	Empty	Empty	Display IE
	True	False	Empty	Display IE	Empty
	False	True or False	Empty	Empty	Empty
Connect	True	True	Empty	Empty	Display IE

	Configuration Settings		H.323->SIP IPC Message		
Msg Type	**use-display-ie**	**use-pai-for-iw-calls**	**fromDisplay**	**toDisplay**	**pAssertedIdentity**
	True	False	Empty	Display IE	Empty
	False	True or False	Empty	Empty	Empty

When the SIP stack receives a SIP message as part of an IW call, it extracts relevant header display-name information and asserted-identity information and passes these to the H.323 process. When a SIP stack receives an INVITE message, it extracts the From: header display-name and asserted-identity header information. When a SIP stack receives provisional and final responses, it extracts To: header display-name and asserted-identity information.

When the SIP stack communicates the event to the H.323 process, SIP stores this identifying information in the SIP->H.323 IPC message. The H.323 process consults the **use-display-ie** and **use-pai-for-iw-call** properties to determine if a Display IE should be added to the outgoing Q.931 message, and if so, if the asserted-identity information is used.

Based on the message type and configuration settings, the following table shows whether this calling party information is added to the outgoing Q.931 message.

	Configuration Settings		H.323->SIP IPC Message		
Msg Type	**use-display-ie**	**use-pai-for-iw-calls**	**fromDisplay**	**toDisplay**	**pAssertedIdentity**
INVITE	True	True	Use From: header	Ignore	Use SETUP PAI header
	True	False	Use SETUP PAI header	Ignore	Ignore
	False	True or False	Ignore	Ignore	Ignore
Provisional response	True	True	Ignore	Use From: header	Use SETUP PAI header
	True	False	Ignore	Use SETUP PAI header	Ignore
	False	True or False	Ignore	Ignore	Ignore
Final response	True	True	Ignore	Use From: header	Use SETUP PAI header

	Configuration Settings		H.323->SIP IPC Message		
Msg Type	**use-display-ie**	**use-pai-for-iw-calls**	**fromDisplay**	**toDisplay**	**pAssertedIdentity**
	True	False	Ignore	Use SETUP PAI header	Ignore
	False	True or False	Ignore	Ignore	Ignore

Expanded File System Support

The OS-E supports two new file systems, ext3 and ext4. Ext3 is an enhancement to ext2. This version adds journaling and is considered the stable standard Linux filesystem. Ext4 is largely a fork of ext3, but has developed such that it is not compatible. It is considered stable, faster and more reliable in its journaling, and is fast becoming the standard Linux file system.

These file systems can be configured using either the **format device** or **add-device device** actions. The **format device** syntax is as follows:

```
NNOS-E>format device ?

syntax: format device [fileSystemType]

 reiser-3 Reiser 3 journaling file system
 xfs      XFS journaling file system
 ext4     Extended file system 4
 ext3     Extended file system 3
 vfat     VFAT (Virtual File Allocation Table)
```

The **add-device device** syntax is as follows:

```
NNOS-E>add-device device ?

 syntax: add-device device fileSystemType

 reiser-3 Reiser 3 journaling file system
 xfs      XFS journaling file system
 ext4     Extended file system 4
 ext3     Extended file system 3
```

Manually Issuing an LRQ Action

The OS-E now supports an action that allows you to manually issue an H.225 RAS Location Request (LRQ) to a configured peer gatekeeper (GK). If a peer GK with this remote IP address is configured, the LRQ reports the results. The result can be either a route-server with an address, an LRJ with a reason, or a timeout.

```
NNOS-E>h323-issue-lrq ?
 Issue LRQ to Peer Gatekeeper
 syntax: h323-issue-lrq addr destinfo destinfotype [srcinfo]
   [srcinfotype]
NNOS-E>
```

You must enter the configured GK address, a string representing the destination to locate, and the type of destination to locate. Optionally, you can enter a string representing the source and the type of source.

The following is an example of this action executed with an IP address of 172.44.200.35:1719, the destination information is 8675309, type of destination dialedDigits, source information is CXC-h323-1, and source type is h323ID:

```
NNOS-E>h323-issue-lrq 172.44.200.35:1719 8675309 dialedDigits CXC-h323-1 h323ID
LRQ sent to peerGK at 172.44.200.35:1719
LRQ for '8675309' was Confirmed, Call Address 10.1.20.126:1720

H.225.0  RAS: locationRequest

H.225.0 RAS
    0... .... Extension Bit: False
    Range = 25 Bitfield length 5, Choice Index: .100 10..
    Choice Index: 18
    RasMessage: locationRequest (18)
        locationRequest
            .... ..1. Extension Bit: True
            .... ...1 Optional Field Bit: True (endpointIdentifier is present)
            0... .... Optional Field Bit: False (nonStandardData is NOT present)
            requestSeqNum: 3
            Range = 128 Bitfield length 7, Octet String Length: 0001 001.
            Octet String Length: 10
            endpointIdentifier: CXC-H323-1
            Sequence-Of Length: 1
            destinationInfo: 1 item
                Item 0
```

```
                    0... .... Extension Bit: False
                    Range = 2 Bitfield length 1, Choice Index: .0.. ....
                    Choice Index: 0
                    DestinationInfo item: dialedDigits (0)
                       Range = 128 Bitfield length 7, Octet String Length: ..00
0011  0... ....
                        Octet String Length: 7
                        dialedDigits: 8675309
             .... 0... Extension Bit: False
             Range = 7 Bitfield length 3, Choice Index: .... .000
             Choice Index: 0
             replyAddress: ipAddress (0)
                 ipAddress
                     ip: 172.44.10.67 (172.44.10.67)
                     port: 1719
             0... .... Small Number Bit: False
             Number of Sequence Extensions: 15
             .... ...1 Extension Present Bit: True (sourceInfo is present)
             0... .... Extension Present Bit: False (canMapAlias is NOT present)
             .0.. .... Extension Present Bit: False (gatekeeperIdentifier is NOT
present)
             ..0. .... Extension Present Bit: False (tokens is NOT present)
             ...0 .... Extension Present Bit: False (cryptoTokens is NOT present)
             .... 0... Extension Present Bit: False (integrityCheckValue is NOT
present)
             .... .0.. Extension Present Bit: False (desiredProtocols is NOT
present)
             .... ..0. Extension Present Bit: False (desiredTunnelledProtocol is
NOT present)
             .... ...0 Extension Present Bit: False (featureSet is NOT present)
             0... .... Extension Present Bit: False (genericData is NOT present)
             .0.. .... Extension Present Bit: False (hopCount is NOT present)
             ..0. .... Extension Present Bit: False (circuitInfo is NOT present)
            ...0 .... Extension Present Bit: False (callIdentifier is NOT present)
             .... 0... Extension Present Bit: False (bandWidth is NOT present)
             .... .0.. Extension Present Bit: False (sourceEndpointInfo is NOT
present)
            .... ..0. Extension Present Bit: False (canMapSrcAlias is NOT present)
             Open Type Length: 23
             Sequence-Of Length: 1
             sourceInfo: 1 item
```

```
    Item 0
        0... .... Extension Bit: False
        Range = 2 Bitfield length 1, Choice Index: .1.. ....
        Choice Index: 1
        AliasAddress: h323-ID (1)
            Octet String Length: 10
            h323-ID: CXC-h323-1
```

There is no new configuration associated with the LRQ action, however, a peer GK and LRQ timeout must be configured.

The following example shows a configured peer GK with an LRQ timeout set to 5 seconds.

```
config vsp
 config enterprise
  config servers
   config h323-server GnuGK-FC4
    set domain WTFDomain
    set server-type h323-gatekeeper
    config server-pool
     config server GnuGK-FC4
      set host 172.44.200.35
      set port 1719
      set local-port 1748
      set connection-role responder
     return
    return
    set local-server-type h323-gatekeeper
    config h323-ras-settings
     set wait-for-location-response 5
    return
   return
```

H.323 Settings Supported under Session Config

A new H.323 model has been created which allows you to configure H.323 on a per-session basis. In previous releases, all H.323 functionality was configured on the H.323 server. The **vsp > session-config-pool > entry** path leads to the following configuration objects.

- **q931-settings**
- **h225-settings**
- **h245-settings**

- **h323-to-sip-fromheader-spec**
- **h323-to-sip-toheader-spec**
- **q931-cause-sip-response-map**
- **sip-response-q931-cause-map**

An H.323 session is created for all H.225 RAS operations including:

- Remote gatekeeper discovery
- Remote gatekeeper registration
- Inbound LRQ processing
- Outbound LRQ
- Outbound ARQ, URQ, and DRQ

H.323 sessions are created for each inbound and outbound H.323 call.

For RAS operations initiated by the OS-E, the requestSeqNum serves as the session identifier for the lifetime of the operation. This allows RAS response traffic to be matched to the correct session. For RAS operations initiated outside of the OS-E, the session identifier is a combination of the IP address transmitting the RAS PDU, the local port receiving the RAS PDU, and the RAS requestSeqNum. The OS-E does not allow more than 65536 outstanding RAS operations.

For H.323 calls to associate a received PDU with a session, the OS-E uses a combination of the H.225.0 CS TCP connection, the Q.931 CRV, and the Q.931 Reference Flag. If H.245 traffic is not tunneled over H.225.0, the TCP connection itself is sufficient to associate the received H.245 message with the existing session. The OS-E allows a maximum of 65536 inbound and 65536 outbound calls on a single TCP connection.

By moving the H.323 configuration from the servers object to the **session-config-pool** object, it is possible to handle SIP-H.323 IW traffic without having to configure remote H.323 gatekeepers and gateways.

The way H.323 handles DTMF has changed and can be configured on a per-session basis, as well. The **sip-h323-dtmf-translate** property is now configured under **vsp > session-config-pool > entry > h245-settings**.

DTMF translation has been enhanced to allow a call to advertise and accept more than one DTMF format. The configuration you set is used only as, “advice.” In cases where the actual supported DTMF formats of the endpoint are unknown, the OS-E uses these configured values. However, when endpoint DTMF formats are known, they are used and the configured values are ignored. The OS-E configuration is never used as a way to reject certain DTMF event formats.

Via the **sip-h323-dtmf-translate** property, specify the **sip-dtmf-type** and the **h323-dtmf-type**.

Valid sip-dtmf-types are:

- INBAND
- RFC2833
- INFO

Valid h323-dtmf-types are:

- INBAND
- RFC2833
- Q931
- H245ALPHA
- H245SIGNAL

Virtual Dial Plans Support

Users can now move from an existing PBX infrastructure onto the OS-E, while still preserving the legacy PBX dial-plan and extension number configuration.

By configuring a Virtual Dial Plan (VDP), you can virtualize the PBX onto the OS-E. Users that are part of the same VDP are able to reach each other via extension dialing. Any dial plan routes and digit manipulations that existed on the legacy system are applied on the OS-E as they would have been on the PBX.

Via the **vsp > virtual-dial-plan-pool** object, configure **virtual-dial-plans** along with the **dial-prefix**, **normalization**, **source-normalization**, **arbiter**, **route**, and **source-route** elements for each. These objects are configured the same as **vsp > dial-plan** objects. For more information on configuring VDPs, see the Chapter 21, Dial Plan Objects in the *Net-Net OS-E — Objects and Properties Reference Guide*.

To determine a user's VDP assignment, configure the **virtual-dialplan-settings**. Specify the assigned VDP in the **entry** property**.** You can also specify a **match-limit** in case you configure the entry points and dial plans incorrectly and a VDP loop occurs.

```
config vsp>config default-session-config
config default-session-config>config virtual-dialplan-settings
config virtual-dialplan-settings>set match-limit 150
config virtual-dialplan-settings>set entry vsp\tls\certificate test
config virtual-dialplan-settings>return
```

User Roles and Access Enhancements

The OS-E now supports new filtering mechanisms which allow you to control which users have access to specific actions and configuration objects and properties. This functionality has been added to the existing **access > permissions** configuration.

Two new permission filters have been added:

- **Action-filter**
- **Config-filter**

There are three steps to assigning users' action and configuration filters. First create the filters in the **access > permission-filters** object. Then assign filters to an access permissions set. Finally, assign each user with a permission set.

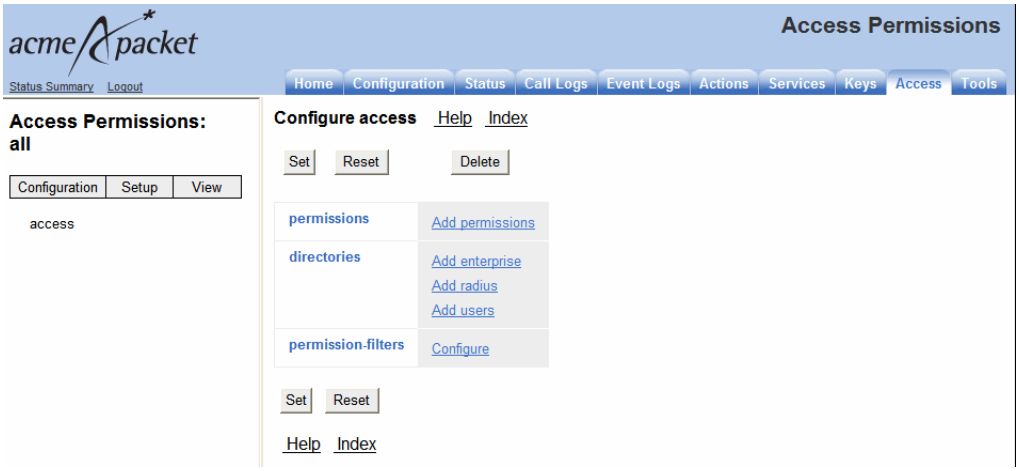
Via the **action-filter**, you can specify a list of disabled actions. When you attempt to execute a disabled action, you get the following error message:

```
Insufficient permissions for user
```

Actions are filtered by action name only, without any parameters or arguments. When anything more than an action name is specified, the OS-E ignores the filter.

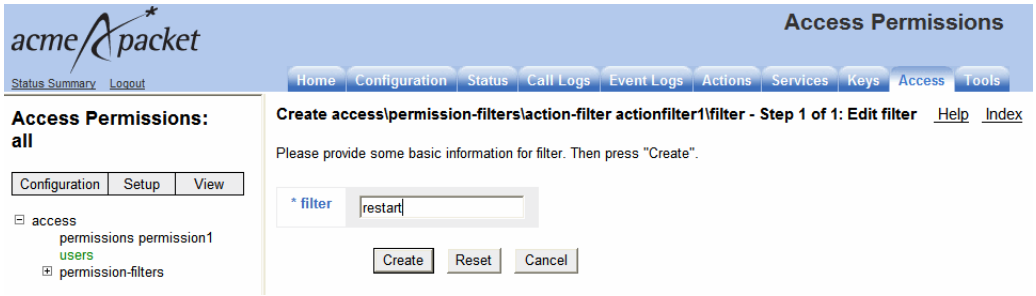
To configure action filter functionality following these steps.

1. Click on the **Access** tab and select **Access**. Click **permission-filters**.



2. Click **Add action-filter**. Enter a name for the filter and click **Create**. Ensure that the filter is **enabled** and click **Add filter**.

3. Specify the filter you are creating. To enter a filter, type the action name only. The following example shows the filter **restart**.



4. Click **Create**. Update and save the configuration.

Once you have added all of the **action-filters**, assign an **action-filter** to your **access** > **permissions**.

5. Under the **Access** tab, click **access.** Either create a new set of permissions by clicking **Add permissions** or click **Edit** on an existing permission. Assign the **action-filter** you are adding to this permission set.

6. Now create a user. Under the **Access** tab click **Add users**.

7. Enter the name you want to give the user, the user password, and select the permission set to assign this user.

8. Click **Create**.

The filters are applied.

Config-filters have three permission levels.

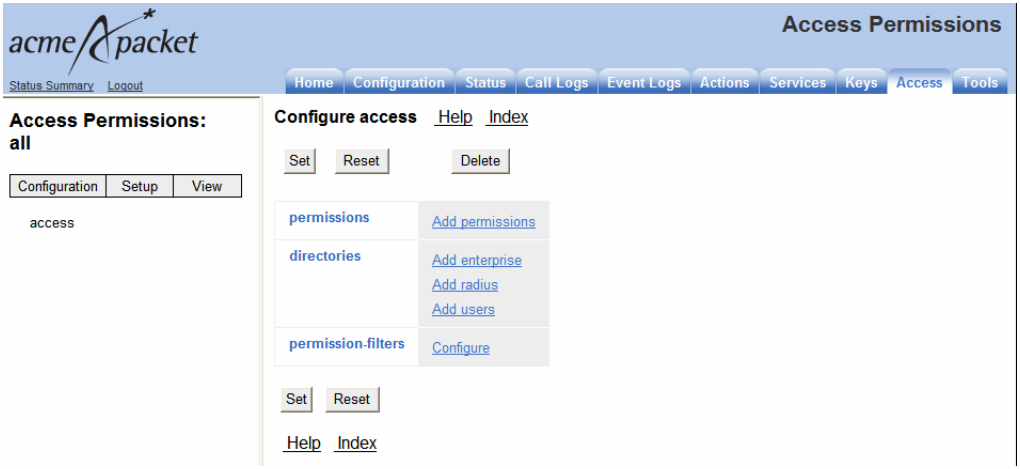
- read-write—Users can modify the configuration
- read-only—Users can view the configuration but cannot modify it
- none—Users cannot view or modify the configuration

By default, child objects and properties inherit permissions from their parent classes, however, a user may apply a lesser permission to a child object or property. The following table lists the inheritance of permissions for the configuration.

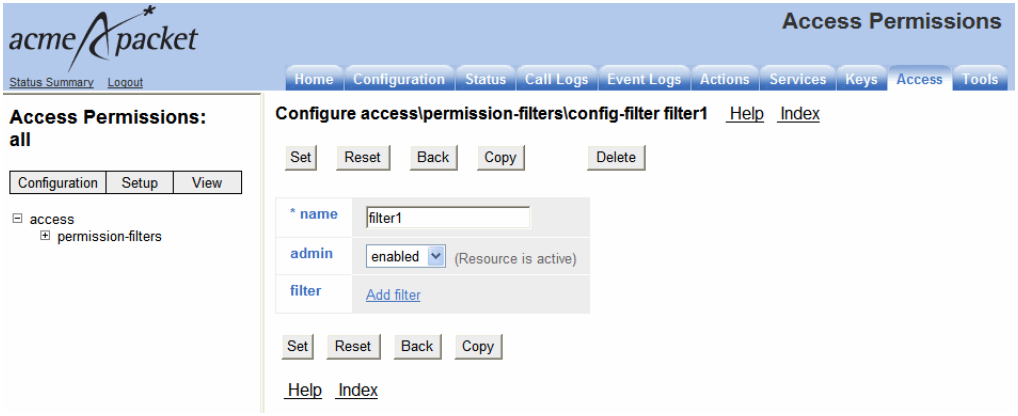
Inherited Permission	Child Object/Property Permission	Effective Permission of Child Object/ Property Permission
read-write	read-write	read-write
read-write	read-only	read-only
read-write	none	none
read-only	read-only	read-only
read-only	none	none
none	none	none

To configure configuration filter functionality following these steps.

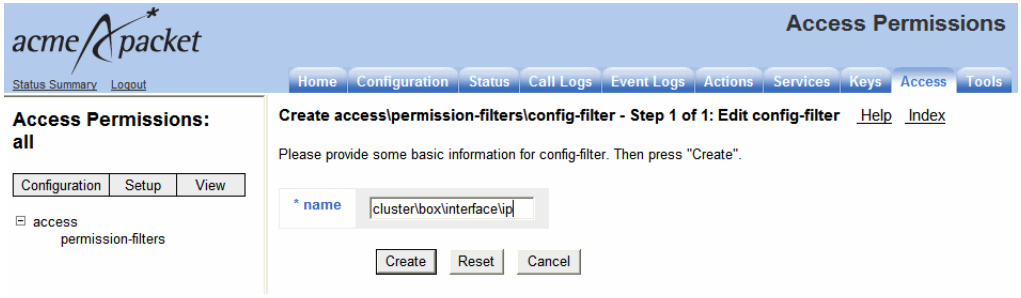
1. Click on the **Access** tab and select **Access**. Click **permission-filters**.



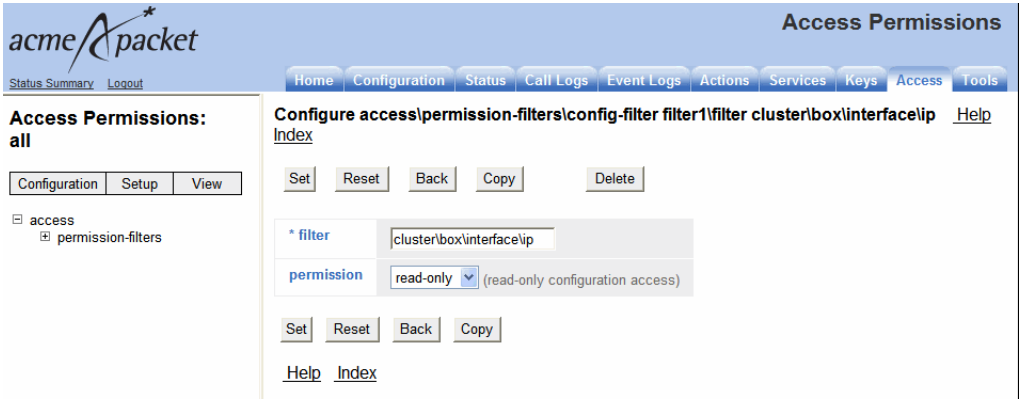
2. Click **Add config-filter**. Enter a name for the filter and click **Create**. Ensure that the filter is **enabled** and click **Add filter**.



3. Specify a filter. To enter a filter, type the class, object, and property in free form, separating each with a back slash "\". The following example shows the filter **cluster\box\interface\ip**. Click **Create**.



4. Apply a filter permission. This example assigns **read-only** permissions to the filter.



5. Update and save the configuration.

Once you have added all of the **config-filters** and assigned them permissions, assign a **config-filter** to your **access > permissions**.

6. Under the **Access** tab click **access.** Either create a new set of permissions by clicking **Add permissions** or click **Edit** on an existing permission. Assign the **config-filter** you want to add to this permission set.

7. Now create a user. Under the **Access** tab click **Add users**.

8. Enter the name you want to give the user, the user password, and select the permission set to assign this user.

9. Click **Create**.

The filters are applied.

File Security Enhancements

The OS-E now provides more granular control of who can access the file system and by what means they do so due to the fact that it is possible for a user to inadvertently delete or replace key files in the file system directory.

Three basic changes have been made:

- SSH users can only use the /tmp folder when configuring properties or executing actions where an output is placed on the file system.
- User permissions have been enhanced, limiting a list of actions and configuration objects and properties users are allowed to modify and view. For more information on configuring permissions, see the User Roles and Access Enhancements Section of this guide.
- Three permissions have been added under the **Access** tab, allowing you to control what users can modify and view under the **Tools** tab. These are accessed via the **access > permissions** path.
    - **gui-tools-update-software**—When **enabled**, this privilege allows the user to use the **Update software** action under the **Tools** tab. This permission is **enabled** by default.

- **gui-tools-upload-file**—When **enabled**, this privilege allows the user to use the **Upload license** file and **Upload file** actions under the **Tools** tab. This permission is **enabled** by default.
- **gui-tools-download-file**—When **enabled**, this privilege allows the user to use the **Retrieve license**, **Download file,** and **Download saved configuration file** actions under the **Tools** tab. This permission is **enabled** by default.

Configuration Changes in Release 3.6.0m4

The section provides a summary of the additions, changes, and deletions to the OS-E configuration when upgrading to Release 3.6.0m4. It covers new objects and properties, configuration objects and properties that have been renamed, and those objects that have been deleted and are no longer available.

New Objects in Release 3.6.0m4

Object name	Associated properties	Description
lcr-import-service		Configures route-server import services settings.
	admin	Enable or disable the use of route-server import service over the selected interface. If enabled, the OS-E functions as a route-server import services server. enabled | disabled The default setting is **enabled**. **Example: set admin enabled**
	protocol	Sets the protocol to use for route-server import operations. After setting a protocol, you can select the route-server import server's listening port (or accept the default). This is the port the server listens on for HTTP(S) requests. Enter the **protocol** and **port**. • HTTP—Use for unencrypted transmission • HTTPS—Use for secure transmission of web pages by using HTTP over SSL The default setting is **http 8082** **Example: set protocol https 8085**
	max-threads	Specifies the maximum number of total worker threads, both active and spare (idle), allocated to the route-server import service server. Min: 1 / Max: 50 The default setting is **10**. **Example: set max-threads 20**

Object name	Associated properties	Description
	min-spare-threads	Specifies the minimum number of inactive threads that the OS-E must leave allocated to the route-server import service server. When the OS-E removes idle threads, it must leave this number available. Min: 0 / Max: 50 The default setting is **1**. **Example: set min-spare-threads 5**
	max-spare-threads	Specifies the maximum number of inactive threads the OS-E can leave allocated to the route-server import service server. When the OS-E detects idle threads, it will not use more than this number for the route-server. Min: 0 / Max: 50 The default setting is **5**. **Example: set max-spare-threads 10**
	idle-timeout	Specifies an inactivity timeout, in minutes, for the OS-E GUI. When a session has been inactive for this amount of time, the OS-E logs the user off the system. Min: 0 / Max: 4294967296 The default setting is **30**. **Example: set idle-timeout 50**
	ciphers	Specifies SSL cipher suite names separated by commas. There is no default setting. **Example: set ciphers SSL_RSA_WITH_RC4_128_SHA_TLS_RSA_WTH_AES**

Object name	Associated properties	Description
	use-https-for-file-copy	When enabled, the route-server import service sends the route-server request to the Web server and specifies using HTTPS to download call rates file. When disabled, HTTP is used for downloading. enabled | disabled The default setting is **enabled**. **Example: set use-https-for-file-copy disabled**
codec-parameters		Specifies the CODEC and the parameter to apply to it in the a=fmtp line of the SDP.
	param	Specifies the maximum number of frames per second (FPP) for audio CODECs that the OS-E advertises. Enter the type of **codec** followed by the **max-fpp**. The following are supported codecs: • any • g722 • g7221 • g723 • g729 • g729a • gsm • pcma • pcmu • *string* The **max-fpp** can be a value between **0** and **255**. There is no default **codec**. The default **max-fpp** value is **24**. **Example: set param audio g729 35**
virtual-dial-plan-pool		This object allows you to move an existing PBX infrastructure onto an OS-E, creating a virtual dial plan. This preserves the legacy PBX dial-plan and extension number configuration.
	virtual-dial-plan	Configures individual virtual dial plans on the OS-E.

Object name	Associated properties	Description
virtual-dial-plan		Configures individual virtual dial plans on the OS-E.
	name	Enter the name you want to use for this virtual dial plan. There is no default setting. **Example: set name vdp1**
	dial-prefix	Applies a custom session configuration based on a dial prefix found either in the To or request URI of the SIP header. Enter the prefix name and the prefix. For more information on configuring dial-prefixes, see Chapter 21, Dial Plan Objects in the *Net-Net OS-E — Objects and Properties Reference Guide*. **Example: set dial-prefix dialprefix1 555**
	normalization	Facilitates routing lookup by normalizing the SIP message. For more information on configuring dial-prefixes, see Chapter 21, Dial Plan Objects in the *Net-Net OS-E — Objects and Properties Reference Guide*. **Example: set normalization norm1**
	source-normalization	Facilitates routing lookup by normalizing the HOST portion of the SIP message. Enter the source-normalization **name**, **type**, and **source-ipnet**. For more information on configuring dial-prefixes, see Chapter 21, Dial Plan Objects in the *Net-Net OS-E — Objects and Properties Reference Guide*. **Example: set source-normalization snorm1 ipnet 10.10.10.10/16**

Object name	Associated properties	Description
	arbiter	Configures an ordered set of rules to influence the routing arbitration decision. It functions as a, “master plan,” determining which metrics to use in selecting a destination server. For more information on configuring dial-prefixes, see Chapter 21, Dial Plan Objects in the *Net-Net OS-E — Objects and Properties Reference Guide*. **Example: set arbiter arb1**
	route	Creates an entry based on the prefix and determines which part of the header to consider. For more information on configuring dial-prefixes, see Chapter 21, Dial Plan Objects in the *Net-Net OS-E — Objects and Properties Reference Guide*. **Example: set route route1**
	source-route	Configures the OS-E to make call routing and forwarding decisions based on the source IP address rather than the Request URI. Enter the source-route **name**, **type**, and **source-ipnet**. For more information on configuring dial-prefixes, see Chapter 21, Dial Plan Objects in the *Net-Net OS-E — Objects and Properties Reference Guide*. **Example: set source-route sroute1 ipnet 15.15.15.15/16**
virtual-dialplan-settings		Configures the VDP settings on the OS-E.
	entry	Specify the assigned VDP for this session-config. There is no default setting. **Example: set entry vsp\tls\certificate\vdp1**

Object name	Associated properties	Description
	match-limit	You can also specify a **match-limit** in case you configure the entry points and dial plans incorrectly and a virtual dial plan loop occurs. Min: 0 / Max: 65536 The default setting is 100. **Example: set match-limit 150**
h323-ras-settings		Sets the configuration for scenarios when the OS-E is communicating with an external H.323 GK. (This property is only applicable if the **server-type** property is set to **h323-gatekeeper**.) When the OS-E registers on behalf of a client, these settings allow the systems to exchange RAS messages.
	registration-ttl	Sets the time to live (TTL), in seconds, for registration to the external GK. Min: 0 / Max: 4294967296 The default setting is **3600**. **Example: set registration-ttl 5000**
	registration-retries	Sets the number of RRQs or GRQs the OS-E resends to an external GK before abandoning the request. A value of **0** allows unlimited retries. If multiple external GKs exist, this property is not used to control RRQ and GRQ retransmission. Min: 0 / Max: 4294967296 The default setting is **5**. **Example: set registration-retries 100**
	admission-retries	Sets the number of times the OS-E resends an ARQ to an external GK before refusing to admit the call. Min: 0 / Max: 4294967296 The default setting is **3**. **Example: set admission-retries 5**

Object name	Associated properties	Description
	endpoint-alias	Assigns a string to the GRQ and RRQ to allow the external GK to identify the OS-E. The default setting is **EPAlias**. **Example: set endpoint-alias alias1**
	supported-prefix	Sets the value for GKs that need digits prepended to a number. The default setting is **+1**. **Example: set supported-prefix +4**
	prefix-type	Adds a voice capability supported prefix to the supported protocols identified in the OS-E-transmitted GRQ and RRQ. • none • dialedDigits • h323ID • urlID • emailID The default setting is **h323ID**. **Example: set prefix-type none**
	reregister-on-urq	Specifies whether the OS-E tries to reregister a client after having received an UNREGISTER from the GK. When enabled, the OS-E tries to reregister the client up to the number of times specified in the **registration-retries** property. enabled | disabled The default setting is **disabled**. **Example: set reregister-on-urq enabled**

Object name	Associated properties	Description
	calls-gk-routed	When true, T_H225CallModel_gatekeeperRouted is the call model in an OS-E-transmitted ARQ. When false, T_H225CallMode_direct is the call mode the OS-E uses. true | false The default setting is **false**. **Example: set calls-gk-routed true**
	use-alternate-gks	When true, supportsAltGKPresent is present in an OS-E-transmitted RRQ. true | false The default setting is **false**. **Example: set use-alternate-gks false**
	retries-before-alt-gk	Specifies how many times the OS-E resents an RRQ or GRQ to an external GK when multiple external GKs exist. Min: 0 / Max: 4294967296 The default setting is **10**. **Example: set retries-before-alt-gk 55**
	use-lightweight-rrq	When true, the OS-E reregisters with an external GK using a lightweight RRQ. true | false The default setting is **false**. **Example: set use-lightweight-rrq true**
	gk-round-robin	Specifies how the OS-E handles external GKs that have previously rejected the OS-E. • IgnoreRejected—The OS-E ignores rejected GKs. • PollRejected—The OS-E contacts external GKs that have previously sent GRJ or RRJ to the OS-E. The default setting is **PollRejected**. **Example: set gk-round-robin IgnoreRejected**

Object name	Associated properties	Description
	wait-for-gk-response	Determines the length of time, in seconds, the OS-E waits for a response to a GRQ or RRQ. Min: 1 / Max: 4294967296 The default setting is **15**. **Example: set wait-for-gk-response 44**
	wait-for-admit-response	Determines the length of time, in seconds, the OS-E waits for a response to an ARQ. Min: 1 / Max: 4294967296 The default setting is **5**. **Example: set wait-for-admit-response 10**
	wait-for-location-response	Determines the length of time, in seconds, that the OS-E has to process a received LRQ before timing out. **Example: set wait-for-location-response 15**
	delay-all-gks-rejected	Specifies the length of time, in seconds, the OS-E waits before attempting external GK discovery and registration when all external GKs have rejected all GRQs and RRQs from the OS-E. Min: 1 / Max: 4294967296 The default setting is **15**. **Example: set delay-all-gks-rejected 25**
	use-lrqsrc-endpoint-info	Determines if the H.323 process extracts sourceEndpointInfo from a received LRQ to pass to SIP for use in destination route lookup. true | false The default setting is **false**. **Example: set use-lrqsrc-endpoint-info true**

Object name	Associated properties	Description
	create-gk-sessions	When true, the OS-E creates sessions for all RAS discovery and registration traffic sent by the OS-E to external GKs. true | false The default setting is **false**. **Example: set create-gk-session true**
	tos	Enables or disables packet marking. Marking (tagging) a packet provides a QoS indicator, which routers along the path may act on. The OS-E writes this value to the ToS field of the IP header. Enter this value in hesadecimal or decimal format. disabled | tos *value* Min: 0 / Max: 255 **Example: set tos 128**
overflow-route		Allows the OS-E to override the dial plan route once a configurable threshold has been reached. Under this config object you can configure the session limit and the peer to use once the limit has been reached.
	admin	Enables or disables the overflow route feature. When enabled, the OS-E overrides the dial plan route once a configurable threshold has been reached. enabled | disabled The default setting is **enabled**. **Example: set admin enabled**
	limit	Enter the session limit threshold to be reached before the overflow route overrides the dial plan route. Min: 0 / Max: 20000 The default setting is **0**. **Example: set limit 150**

Object name	Associated properties	Description
	peer <*type*> <*address*>	Specify the peer to which you want traffic forwarded once the session limit threshold has been reached. Enter the peer **type** and **address**. The following are valid peer types: • none • server • carrier • exchange • switch • trunk • hunt-group • calling-group • virtual-dial-plan The default setting is **none**. **Example: set peer server “vsp\enterprise\servers\sip-gateway RedirectClusters”**
archive-local		Configures archiving locally on the OS-E.
	path	Configures a name and path for archiving locally on the OS-E.
path		Configures a path for archiving locally on the OS-E.
	admin	Enable or disable the local archiving target. enabled | disabled The default setting is **enabled**. **Example: set admin enabled**
	include-sip-messages	Indicates whether individual SIP messages are to be included in the archive. true | false The default setting is **true**. **Example: set include-sip-messages true**

Object name	Associated properties	Description
	mixed-media	Specifies whether to include resulting WAV files in the archive record. true | false The default setting is **false.** **Example: set mixed-media true**
	include-raw-media	Indicates whether the raw media streams are to be included in the archive file. true | false The default setting is **false**. **Example: set include-raw-media true**
	include-audit-events	Indicates whether audit events are to be included in the archive. true | false The default setting is **false**. **Example: set include-audit-events true**
	use-compression	Specify whether or not to compress the archived zip files. true | false The default setting is **true**. **Example: set use-compression true**
	purge-archives [true | false]	Specify whether the OS-E removes local archives created earlier than the retention period. true | false The default setting is **true**. **Example: set purge-archives false**
	retention-period	Specify how many days archives should be retained on the local file system. The default setting is **P7D**. **Example: set retention-period P6D**

Object name	Associated properties	Description
	file-path	Sets the target OS-E file-system path for logging accounting and SIP CDRs. A file-path consists of a valid OS-E directory path and file name. There is no default setting. **Example: set file-path "vsp\accounting\file-system\path "cdr backup""**
archive-external		Configures archiving to an external file system.
	url	Configures the URL of the external archiving target. **Example: set url externalarchive1**
url		Configures the URL of the external archiving target.
	admin	Enables or disables the archiving target. enabled | disabled The default setting is **enabled**. **Example: set admin enabled**
	include-sip-messages	Indicates whether individual SIP messages are to be included in the archive. true | false The default setting is **true**. **Example: set include-sip-messages true**
	mixed-media	Specifies whether to include result WAV files in the archive record. true | false The default setting is **false**. **Example: set mixed-media true**

Object name	Associated properties	Description
	include-raw-media	Indicates whether the raw media streams are to be included in the archive. true | false The default setting is **false.** **Example: set include-raw-media true**
	include-audit-events	Indicates whether audit events are to be included in the archive. true | false The default setting is **false**. **Example: set include-audit-events true**
	use-compression	Specifies whether the OS-E should compress archived zip files. true | false The default setting is **true**. **Example: set use-compression false**
	purge-archives [true | false]	Specifies whether the OS-E should remove local archives created earlier than the retention period. true | false The default setting is **true**. **Example: set purge-archives false**
	retention-period	Specifies how many days archives should be retained on the local file system. The default setting is **P7D.** **Example: set retention period P6D**
	destination	The external remote server to which the archives are to be sent. The URL can be entered two ways, detailed or concise. There is no default setting. **Example: set destination scp:// user@10.33.5.10:/acct/test/**

Object name	Associated properties	Description
	max-saved-on-send-fail	Enter the maximum number of archives that are saved locally if a send fails. Min: 0 / Max: 1000 The default setting is **100**. **Example: set max-saved-on-send-fail 200**
	save-dir-on-sender-file	Enter the remote folder to save archives that failed to be sent. The default setting is **/cxc_common/archive/saved**. **Example: set save-dir-on-sender-file /cxc_common/archive/saved**
accounting		Configures the OS-E RADIUS accounting services, system logging (syslog), the accounting database, accounting file-system, and archiving. You can configure one or more of these accounting methods for capturing SIP CDRs.
	archive-worker-threads	*Secondary property.* Specifies the number of worker threads to allocate to archiving. Enter either automatic or an integer. The default setting is **automatic** which means the OS-E uses the platform-specific factory default. **Example: set archive-worker-threads 100**
	archive-max-inprogress	*Secondary property.* Enter the maximum number of CDRs that can be concurrently processed for archiving by a target. Min: 1 / Max: 500 The default setting is **150**. **Example: set archive-max-inprogress 250**

Object name	Associated properties	Description
	archive-tries	*Secondary property.* Enter the number of tries made for operations within the archiving process. Min: 1 / Max: 10 The default setting is **3**. **Example: set archive-tries 5**
	archive-name-format	*Secondary property.* Fields to form the archive name. The name length is restricted to 250 characters. The default setting is **SetupTime**, **From**, and **callID**. **Example: set archive-name-format To**
	compatible-archives	*Secondary property.* Specify whether the archives sent are compatible archives generated with a box-wide archiving. Setting this as **true** adds call.txt to the archives and sends an XML file in addition to the zip file to the destination. true | false The default setting is **false**. **Example: set compatible-archives true**
	server-idle-timeout	*Secondary property.* Specifies the time, in seconds, that the OS-E connection to the server can remain open without a response before the OS-E closes the connection. Min: 0 / Max: 4294967296 The default setting is **300**. **Example: set server-idle-timeout 500**

Object name	Associated properties	Description
	delete-raw-media-on-archive-complete	When **true**, the OS-E deletes raw media files for a call once all archive targets successfully archive that session. If any one target configured to include media fails to archive, the raw media files are not deleted. true | false The default setting is **false**. **Example: set delete-raw-media-on-archive-complete**
named-variable-collector		Provides granular modification capabilities to create or modify a named variable.
	admin [enabled | disabled]	Enables or disables named variable collection on the OS-E. The default setting is **enabled**. **Example: set admin enabled**
	number	Specifies an indexed number for this entry. Min: 0 / Max: 4294967296 There is no default setting. **Example: set number 10**
	named-variable	Specifies the named-variable you are creating or modifying. The value of this variable will be the replacement string. There is no default setting **Example: set named-variable var1**

Object name	Associated properties	Description
	create	Identifies the header containing the data to be modified and the value assigned to the named-variable. First, select the header that serves as the source of the data. This can be **To**, **From**, or **Request**. Then specify a regular expression to run against the value of the source header. Finally, supply the replacement expression to apply if there is a match. There is no default setting. **Example: set create To (.*) \1;\1>**
	append	Identifies the header containing the data to be added to the named-variable value. First, select the header that serves as the source of the data. This can be To, From, or Request. Then specify a regular expression to run against the value of the source header. Finally, supply the replacement expression to apply if there is a match. The OS-E appends this string to the existing named-variable value. To add spaces or commas, include them using quotation marks. There is no default setting. **Example: set append From (.*) \2;\2>**
	apply-to-methods	Specifies the message type from which the OS-E extracts the specified named-variable value. The default setting is **INVITE**. **Example: set apply-to-methods REGISTER**

Object name	Associated properties	Description
	apply-to-responses	Specifies whether to apply header value changes to SIP requests or both requests and responses. When set to **no**, changes are only applied to requests. When set to **yes**, changes are applied to both requests and responses. • no • yes [*response-code*] • both [*response-code*] The default setting is **no**. **Example: set apply-to-responses both 500**
	apply-to-dialog	Specifies whether to apply header value changes to a specific dialog or not. • inbound—Apply to the inbound dialog only • outbound—Apply to the outbound dialog only • both—Apply to both inbound and outbound dialogs. The default setting is **both**. **Example: set apply-to-dialog inbound**
	cseq	*Secondary property.* Sets a mechanism to further filter which SIP messages have the header expression modifications applied. If this property is set to **0** (the default), the OS-E applies the changes to all SIP messages. If set to any other value, the OS-E only applies the changes to SIP messages having a CSEQ field that matches that value. Min: 0 / Max: 4294967296 The default setting is **0**. **Example: set cseq 100**

Object name	Associated properties	Description
	create-on-failed-match	*Secondary property.* Construct a create header even when the expression is not a complete match. true | false The default setting is **true**. **Example: set create-on-failed-match false**
	append-on-failed-match	*Secondary property.* Execute the append action event even when the create expression fails to match. true | false The default setting is **true**. **Example: set append-on-failed-match false.**
named-variables		This object allows you to configure named variables and their values per session.
	named-variable	Enter the name of the named variable for this session. There is no default setting **Example: set named-variable var1**
	value	Enter the value of the named variable for this session. There is no default setting **Example: set value 100**

Object name	Associated properties	Description
	merge-object	Specifies whether this new set of session configuration named variables overwrites the previous set of session configuration named variables, or if it is appended to the previous set. • merge—Append to the existing set of session configuration named variables. • replace—Overwrite the existing set of session configuration named variables with the new one. The default setting is **merge**. **Example: set merge-object replace**
arp-heartbeat		Allows each VX to be associated with another system on the network. In addition to sending periodic VRRP advertisements across the messaging interface, this object allows the OS-E to send ARP requests across the VX interface to the associated timeout.
	admin	Enables or disables the ARP heartbeat on a redundant VM system or in a complicated network. enabled | disabled **Example: set admin enabled** The default setting is **enabled**.
	heartbeat-system	Enter the IP address of the system on the subnet to query with ARPs. **Example: set heartbeat-system 10.10.10.10** There is no default setting.
h323-tos-settings		Configures ToS settings for H.323 support on the OS-E.
	in-leg-tos	Configures the in-leg settings for H.323 support on the OS-E.
	out-leg-tos	Configures the out-leg settings for H.323 support on the OS-E.

Object name	Associated properties	Description
in-leg-tos		Configures the in-leg settings for H.323 support on the OS-E.
	value	Determines the ToS value setting for the in-leg of the session. The TOS value determines the quality of service that the call receives. The OS-E marks the ToS field of all packets it sends out on the inleg with the value you specify. Enter a number that represents the 8-bit Differentiated Services (DS) field of the IP packet in decimal format, such as 26 for 00011010 or 104 for 01101000. This value can be of use to upstream devices. Min: 0 / Max: 255 The default setting is **0**. **Example: set value 22**
out-leg-tos		Configures the out-leg settings for H.323 support on the OS-E.
	value	Determines the ToS value setting for the out-leg of the session. The TOS value determines the quality of service that the call receives. If set to **preserve**, the OS-E uses the ToS value in the first received message of the session. If set to **overwrite**, the OS-E marks the ToS field of all packets it sends out on the inleg with the value you specify. Enter a number that represents the 8-bit Differentiated Services (DS) field of the IP packet in decimal format, such as 26 for 00011010 or 104 for 01101000. This value can be of use to upstream devices. preserve | overwrite <*value*> The default setting is **preserve**. If you select overwrite, the default value is **0**. **Example: set value overwrite 22**
permission-filters		This object allows you to apply action and configuration filtering on a per-user basis.

Object name	Associated properties	Description
config-filter		This object applies configuration filtering on a per-user basis. Enter a name for the filter. There is no default setting. **Example: set config-filter filter1**
	admin	Enable or disable this configuration filter. enabled | disabled The default setting is **enabled**. **Example: set admin enabled**
	filter	Specify the filter. Enter this value in free form, separating the class, object, and properties with a backslash "\". There is no default setting. **Example: set filter filter1 enabled cluster\box\interface\ip**
action-filter		This object applies action filtering on a per-user basis. Enter a name for the filter. There is no default setting. **Example: set action-filter actionfilter1**
	admin	Enable or disable this action filter. enabled | disabled The default setting is **enabled**. **Example: set admin enabled**
	filter	Specify the filter. Enter the action without any arguments. If you enter the action with arguments, the filter is ignored. There is no default setting **Example: set filter restart**
table-config		This object allows you to configure route-server tables.

Object name	Associated properties	Description
	table	Enter the name of the table you are creating. There is no default setting. **Example: set table table5**
	description	Give a brief description of the table you are creating. There is no default setting. **Example: set description 1000-1050**
	filename	Enter the name of the file containing the routes for this table. There is no default setting **Example: set filename /routes**
advanced-filter		*Secondary object*. This object allows you to configure more granular snmp-trap events. Specify allowed and blocked events (for example the server state change).
	allowed-event	*Secondary object*. Enter specific events you want allowed by the SNMP trap feature. There is no default setting. **Example: set allowed-event "SIP server peer (.+) server (.+) changed" info**
	blocked-event	*Secondary object*. Enter specific events you want blocked by the SNMP trap feature. There is no default setting **Example: set blocked-event (.*)**
snmp-trap		The snmp-trap object allows you to enable the translation of event logs into SNMP traps.
	admin	Enables or disables the OS-E's ability to translate event logs into SNMP traps. enabled | disabled The default setting is **enabled**. **Example: set admin enabled**

Object name	Associated properties	Description
	filter	Specifies the event message filter log class and severity level for transferring event-logs to SNMP traps. Repeat the command to specify multiple event filters. The default setting is **all**. **Example: set filter sipRouting debug**
in-dtmf-preferences		Configures the OS-E's in-leg DTMF method preferences.
	admin	Specifies whether or not this DTMF preference list is applied to calls matching this session configuration. enabled | disabled The default setting is **disabled**. **Example: set admin enabled**
	preferences	Allows you to configure supported dtmf-types and assign them with a priority to determine the OS-E's preferences. First select a DTMF method. The available DTMF methods are: • audio • rfc-2833 • sip-info-dtmf • sip-info-dtmf-relay • sip-notify • h245-alphanumeric • h245-signal • q931 Then assign it a priority. This can be from 0-100. A value of **0** means the method is not supported. The lower the priority, the more preferred the DTMF method. The default setting is **audio 1**. **Example: set preferences rfc-2833 2**
out-dtmf-preferences		Configures the OS-E's out-leg DTMF method preferences.

Object name	Associated properties	Description
	admin	Specifies whether or not this DTMF preference list is applied to calls matching this session configuration. enabled | disabled The default setting is **disabled**. **Example: set admin enabled**
	preferences	Allows you to configure supported dtmf-types and assign them with a priority to determine the OS-E's preferences. First select a DTMF method. The available DTMF methods are: • audio • rfc-2833 • sip-info-dtmf • sip-info-dtmf-relay • sip-notify • h245-alphanumeric • h245-signal • q931 Then assign it a priority. This can be from 0-100. A value of **0** means the method is not supported. The lower the priority, the more preferred the DTMF method. The default setting is **audio 1**. **Example: set preferences rfc-2833 2**
in-dtmf-settings		The OS-E can be configured to translate one DTMF method to another. Through this object, you can control the length of play and pause time and volume for the digits that the OS-E plays on the in-leg.

Object name	Associated properties	Description
	digit-volume	Specifies the volume setting for the DTMF tones. The digit volume is measured in decibel (dB) of the measured power referenced to one milliwatt, measured at a zero transmission level point. The smaller the dBm0, the louder the volume. Min: -36 / Max: 0 The default setting is **-20**. **Example: set digit-volume -15**
	digit-duration	Specifies the length of time, in milliseconds, that the OS-E plays each DTMF digit. Min: 100 / Max: 10000 The default setting is **750**. **Example: set digit-duration 1000**
	min-digit-duration	Specifies the minimum length of time, in milliseconds, that the OS-E plays each DTMF digit. If a DTMF event has a duration less than this value, the **digit-duration** property overrides the duration and is used to play the DTMF event. Min: 5 / Max: 100 The default setting is **60**. **Example: set min-digit-duration 75**
	max-digit-duration	Specifies the maximum length of time, in milliseconds, that the OS-E plays each DTMF digit. If a DTMF event has a duration greater than this value, the **digit-duration** property overrides the duration and is used to play the DTMF event. Min: 100 / Max: 10000 The default setting is **2000**. **Example: set max-digit-duration 3000**

Object name	Associated properties	Description
	inter-digit-duration	Specifies the length of time, in milliseconds, that the OS-E pauses between playing each digit. Min: 0 / Max: 1000 The default setting is **250**. **Example: set inter-digit-duration 500**
	pause-duration	Specifies the length of time, in milliseconds that the OS-E pauses when it encounters a comma character in the conference code. The comma is a special character in the conference code that indicates a specified time the OS-E must wait before playing the next tone. Min: 500 / Max: 10000 The default setting is **3000**. **Example: set pause-duration 4000**
	minimum-duration	Specifies the minimum time, in milliseconds, between detecting RFC-2833 events. Min: 0 / Max: 1000 The default setting is **60**. **Example: set minimum-duration 100**
	as-audio	Specifies whether the OS-E sends audio or DTMF packets to the conference server when representing conference code tones. When true, the OS-E encodes the sound in the current CODEC. When false, the OS-E sends DTMF packets. true | false The default setting is **true**. **Example: set as-audio false**
out-dtmf-settings		The OS-E can be configured to translate one DTMF method to another. Through this object, you can control the length of play and pause time and volume for the digits that the OS-E plays on the out-leg.

Object name	Associated properties	Description
	digit-volume	Specifies the volume setting for the DTMF tones. The digit volume is measured in decibel (dB) of the measured power referenced to one milliwatt, measured at a zero transmission level point. The smaller the dBm0, the louder the volume. Min: -36 / Max: 0 The default setting is **-20**. **Example: set digit-volume -15**
	digit-duration	Specifies the length of time, in milliseconds, that the OS-E plays each DTMF digit. Min: 100 / Max: 10000 The default setting is **750**. **Example: set digit-duration 1000**
	min-digit-duration	Specifies the minimum length of time, in milliseconds, that the OS-E plays each DTMF digit. If a DTMF event has a duration less than this value, the **digit-duration** property overrides the duration and is used to play the DTMF event. Min: 5 / Max: 100 The default setting is **60**. **Example: set min-digit-duration 75**
	max-digit-duration	Specifies the maximum length of time, in milliseconds, that the OS-E plays each DTMF digit. If a DTMF event has a duration greater than this value, the **digit-duration** property overrides the duration and is used to play the DTMF event. Min: 100 / Max: 10000 The default setting is **2000**. **Example: set max-digit-duration 3000**

Object name	Associated properties	Description
	inter-digit-duration	Specifies the length of time, in milliseconds, that the OS-E pauses between playing each digit. Min: 0 / Max: 1000 The default setting is **250**. **Example: set inter-digit-duration 500**
	pause-duration	Specifies the length of time, in milliseconds that the OS-E pauses when it encounters a comma character in the conference code. The comma is a special character in the conference code that indicates a specified time the OS-E must wait before playing the next tone. Min: 500 / Max: 10000 The default setting is **3000**. **Example: set pause-duration 4000**
	minimum-duration	Specifies the minimum time, in milliseconds, between detecting RFC-2833 events. Min: 0 / Max: 1000 The default setting is **60**. **Example: set minimum-duration 100**
	as-audio	Specifies whether the OS-E sends audio or DTMF packets to the conference server when representing conference code tones. When true, the OS-E encodes the sound in the current CODEC. When false, the OS-E sends DTMF packets. true | false The default setting is **true**. **Example: set as-audio false**
custom-event-fields		Adds a custom data field to the callCreated, callConnected, and callTerminated events. This object defines the content of the field.

Object name	Associated properties	Description
	named-variable-entry	Specifies the content of the custom data field added to the accounting record. This is in the form variable=value. There is no default setting. **Example: set named-variable-entry variable=\s**
	custom-events-grouping-string	*Secondary property.* The characters used to associate an event's variable and values. The default setting is **=**. **Example: set custom-events-grouping-string :**
	custom-event-delimiter	*Secondary property.* The characters used to separate group custom event entries. The default setting is **;**. **Example: set custom-event-delimiter **
route-server-config		Reserved for future use.
	route-server-sequence	Reserved for future use.
route-server-sequence		Reserved for future use.
	description	Reserved for future use.
	query	Reserved for future use.
query		Reserved for future use.
	description	Reserved for future use.
	query	Reserved for future use.
	table	Reserved for future use.
	lookup-type	Reserved for future use.
	appent	Reserved for future use.
	variable-load	Reserved for future use.
	variable-mappings	Reserved for future use.
	variable-ignore-additional	Reserved for future use.
	condition-list	Reserved for future use.
condition-list		Reserved for future use.

Object name	Associated properties	Description
	abort-on-failure	Reserved for future use.
	stop-on-success	Reserved for future use.

New properties in Release 3.6.0m4

Object name	Associated properties	Description
third-party-call-control	inhibit-provisional-response-after-prack	*Secondary property*. When enabled, the OS-E does not send 18x messages after receiving a Prack. This prevents problems when invalid codecs are presented in the 18x's SDP after valid codecs have already been sent. enabled | disabled The default setting is **disabled**. **Example: set inhibit-provisional-response-after-prack enabled**
	call-control-events-version	When custom-event-fields object on the OS-E is configured, when this property is set to **custom**, it enables the OS-E to add custom information in call control events (for example, callCreated, callConnected, and callTerminated). • legacy—The events generated follow the legacy format. • custom—The events generated have new custom fields. The default setting is **legacy**. **Example: set call-control-events-version custom**
inbound-header-settings | header-settings	sip-manipulation	Specify the configured sip-manipulation you want to associate with this header-setting. Configure the sip-manipulation in the **sip-manipulation-pool > sip-manipulation** object. There is no default setting. **Example: set sip-manipulation sipmanip1**

Object name	Associated properties	Description
static-stack-settings	max-redirect-sessions [automatic | *integer*]	*Secondary property.* When configured, this property overrides the redirect session limit enforced on the OS-E. The default setting is **automatic** which means the OS-E uses the platform-specific factory default value. **Example: set max-redirect-sessions 100**
server | switch	remote-web-services	Configures the HTTP address of the remote web service address of the cluster web services. When this property is configured, the OS-E makes a web service request to that address and stores the session information returned as the redirect statistics. There is no default setting. **Example: set remote-web-services http://170.30.10.10:8080**
server-pool	remote-web-services-fetch-timer	Configures the allowed interval to collect redirect statistics before the OS-E times out. Min: 0 / Max: 4294967296 The default setting is **5000**. **Example: set remote-services-fetch-timer 7000**
box	rtp-mixing-threads	*Secondary property.* Configures the number of threads that the worker pool will contain when the mix-session-threaded action is executed. The default setting is **automatic**. This means the OS-E uses the platform-specific factory default value. automatic | <*integer*> **Example: set rtp-mixing-threads automatic**

Object name	Associated properties	Description
condition-list	named-variable-condition	Specifies the named variable to match to this policy rule and how you want to compare them. • named-variable-value<*variable-name*><*match-type*><*regexp-value*>—Compare the specified variable value. Named match values for this argument are: • match—Allow values which match the specified expression. • exclude—Exclude values which match the specified expression. • contains—Allow values which contain the specified expression. • compare-named-variables<*variable-name-1*><*match-type*><*variable-name-2*>—Compare the values of two different named variables. The default **match-type** and only option is **match**, which means the OS-E compares if the named variable values match. **Example: set named-variable-condition named-variable-value var1 exclude \s**
sametime | server | lcs | mcs | avaya | sip-gateway | h323-server | sip-host | dns-group | sip-connection	ping-mode	Allows you to modify how the OS-E decides when to mark a server up or down when it receives a response from a remote server to an OPTIONS ping. The following are valid options: • promiscuous-mode—When an OPTIONS ping is sent to the server, if any response is received, the server is considered up. The only case where the server is marked down is a timeout from no response. • restricted-mode—When an OPTIONS ping is sent to the server, the server must respond with a 200OK or it will be considered down. The default setting is **promiscuous-mode**. **Example: set ping-mode restricted-mode**

Object name	Associated properties	Description
accounting-data	named-variable-entry	Specifies the content of the field added to the accounting record in the format, tag=value. There is no default setting. **Example: set named-variable-entry \s**
server	use3dot4-schema	When enabled, accounting CDRs sent to an external database use the OS-E 3.4 schema instead of the 3.6.0m3 CDR database schema. enabled | disabled The default setting is **disabled**. **Example: set use3dot4-schema**
permissions	config-filter	Select the existing config-filter you want to use for this permission set. There is no default setting. **Example: set config-filter filter1**
	action-filter	Select the existing action-filter you want to use for this permission set. There is no default setting. **Example: set action-filter actionfilter1**
	gui-tools-update-software	When **enabled**, this privilege allows users to use the **Update software** action under the **Tools** tab. enabled | disabled The default setting is **enabled**. **Example: set gui-tools-update-software disabled**

Object name	Associated properties	Description
	gui-tools-upload-files	When **enabled**, this privilege allows users to use the **Upload license file** and **Upload file** actions under the **Tools** tab. enabled | disabled The default setting is **enabled**. **Example: set gui-tools-upload-files disabled**
	gui-tools-download-files	When **enabled**, this privilege allows users to use the **Retrieve license**, **Download file**, and **Download saved configuration file** actions under the **Tools** tab. enabled | disabled The default setting is **enabled**. **Example: set gui-tools-download-files disabled**
task	action	Specify the action that the task performs. There is no default setting. **Example: set action database-maintenance**
	arguments	Specifies additional information for the action you have specified. There is no default setting. **Example: set arguments force**
tasks	config-update-task	Specifies the action to be performed when the configuration is modified. There is no default setting. **Example: set config-update-task restart**

Object name	Associated properties	Description
network	tcp-ephemeral-port-start	*Secondary property.* Configures the local TCP ephemeral port range start. Well-known ports or ports configured for use with SIP or H.323 should not be allocated in the local port pool range. Min: 1024 / Max: 65535 The default setting is **1024** **Example: set tcp-ephemeral-port-start 2025**
	tcp-ephemeral-port-end	*Secondary property.* Configures the local TCP ephemeral port range end. Well-known ports or ports configured for use with SIP or H.323 should not be allocated in the local port pool range. Min: 1024 / Max: 65535 The default setting is **4999** **Example: set tcp-ephemeral-port-end 3025**
authorization	sequence	Select an existing sequence to use for querying the route server. This is a sequence you must have configured in the **vsp > route-server-config > route-server-sequence object**. **Example: set sequence query1**
dtmf-generation	min-digit-duration	Specifies the minimum length of time, in milliseconds, that the OS-E plays each DTMF digit. If a DTMF event has a duration less than this value, the **digit-duration** property overrides this value and is used to play the DTMF event. Min: 5 / Max: 100 The default setting is **60**. **Example: set min-digit-duration 75**

Object name	Associated properties	Description
	max-digit-duration	Specifies the maximum length of time, in milliseconds, that the OS-E plays each DTMF digit. If a DTMF event has a duration greater than this value, the **digit-duration** property overrides this value and is used to play the DTMF event. Min: 100 / Max: 10000 The default setting is 2000. **Example: set max-digit-duration 3000**
	digit-duration-update	When the actual duration of a DTMF event is not known, the OS-E sends this value in the Call-Info header when Notify-based out-of-band DTMF is supported, or as the initial duration sent in a DTMF H.245 Signal message. Min: 60 / Max: 10000 The default setting is **2000**. **Example: set digit-duration 1500**
event-service	content-type-char-set	Specify the charset the OS-E uses on the ContentType field of outgoing Web Service requests sent to this endpoint. • iso-8859-1—The OS-E uses the ISO-8859-1 character encoding. • utf-8—The OS-E uses the UTF-8 character encoding. The default setting is **iso-8859-1** **Example: set content-type-char-set utf-8**
settings	strict-sip-parsing	*Secondary property*. When **true**, The OS-E performs stricter validation of parsed SIP data. Nothing is accepted that has any quirks or violates the specification in anyway. The default setting is **false**. true | false **Example: set strict-sip-parsing true**

Object name	Associated properties	Description
	strict-sdp-parsing	*Secondary property.* When **true**, The OS-E performs stricter validation of parsed SDP data. Nothing is accepted that has any quirks or violates the specification in anyway. The default setting is **false**. true | false **Example: set strict-sdp-parsing true**
h225-settings	enum-returnednaptr-replace	*Secondary property.* Enter a regexp and a replacement value. When configured, if the OS-E performs an ENUM dip for an inbound H.323 call, the regexp and replacement string are applied to the result of the ENUM lookup. That then becomes the called party identifier. There is no default setting. **Example: set enum-returnednaptr-replace (*) \?**
	session-duration-max	Sets the maximum duration of an H.323 call, in seconds. A value of **0** (the default) indicates there is no maximum lifetime. Min: 0 / Max: 1000000 The default setting is **0**. **Example: set session-duration-max 1000**
media	pass-candidate-attributes	Specifies whether or not ICE candidate SDP attributes received by the OS-E are forwarded to an endpoint. enabled | disabled The default setting is **disabled**. **Example: set pass-candidate-attributes enabled**

Object name	Associated properties	Description
	propagate-reinvite-from-header	When enabled, when the OS-E receives an Invite request, the OS-E switches to the new From: header when it is different in a reinvite. When disabled, the OS-E uses the From: header received in the initial Invite. enabled | disabled The default setting is **disabled**. **Example: set propagate-reinvite-from-header enabled**
	dtmf-detected-events	Specifies whether received DTMF events are reported to web services. • disabled—Provides the normal DTMF handling based on the **session-config > dtmf-preferences** settings or the older legacy **dtmf-translation** settings. • report-and-forward—DTMF events are reported to web services and translated and forwarded based on the **session-config > dtmf-preference** settings or the older legacy **dtmf-translation** settings. • report-and-discard—DTMF events are reported to web services and then discarded without being translated. The default setting is **disabled**. **Example: set dtmf-detected-events report-and-forward**

Deleted Objects in Release 3.6.0m4

Object name
surveillance

Changed Properties in Release 3.6.0m4

Property name	Path change
use-incoming-display-ie	Renamed to **use-display-ie**.

Moved Objects in Release 3.6.0m4

Object name	Path change
q931-settings	From: **vsp > enterprise > servers** To: **vsp > session-config-pool > entry**
h225-settings	From: **vsp > enterprise > servers** To: **vsp > session-config-pool > entry**
h245-settings	From: **vsp > enterprise > servers** To: **vsp > session-config-pool > entry**
h323-to-sip-fromheader-spec	From: **vsp > enterprise > servers** To: **vsp > session-config-pool > entry**
h323-to-sip-toheader-spec	From: **vsp > enterprise > servers** To: **vsp > session-config-pool > entry**
q931-cause-sip-response-map	From: **vsp > enterprise > servers** To: **vsp > session-config-pool > entry**
sip-response-q931-cause-map	From: **vsp > enterprise > servers** To: **vsp > session-config-pool > entry**

Moved Properties in Release 3.6.0m4

Property name	Path change
sip-h323-dtmf-translate	From: **vsp > enterprise > servers > h245-settings** To: **vsp > session-config-pool > entry > h245-settings**

MIB Changes in Release 3.6.0m4

This section covers changes that have been applied to Management Information Base (MIB) object definitions.

New MIB Tables in Release 3.6.0m4

MIB table name	Description
accountingTargetsArchiveTable	accounting-targets-archive: archive targets
routeServerDidTable	route-server-did: Route Server DID Range Entries

MIB table name	Description
sipManipTable	sip-manip: Sip Manipulation Rules
sipManipElementRulesTable	sip-manip-element-rules: Sip Manipulation Element Rules
sipManipHeaderRulesTable	sip-manip-header-rules: Sip Manipulation Header Rules
named VariablesBySessionTable	named-variables-by-session: Named variables per session (indexed by session ID)
clusterConnectionsTable	cluster-connections: Cluster connections
dtmfTable	dtmf: DTMF statistics
dtmfTranslationTable	dtmf-translation: DTMF translation statistics
routeServerQueriesTable	route-server-queries: Route Server Queries
accountingTargetsArchiveTasksTable	accounting-targets-archive-tasks: archive tasks
proxyTransactionDataTable	proxy-transaction-data: Information about active and deleted proxy transactions
routeServerSequencesTable	route-server-sequences: Route Server Sequences
routeServerTableConfigTable	route-server-table-config: Route Server Configuration

New MIB Objects in Release 3.6.0m4

MIB object/table name
networkSettingsTcpEphemeralPortStart
networkSettingsTcpEphemeralPortEnd

Changed Tables in Release 3.6.0m4

MIB table name	Description
callingGroupPoolTable	ADDED: callingGroupPoolRemoteWebServices, callingGroupPoolPingMode
carrierRoutingTable	NAME CHANGED: carrierRoutingMinPrefixDigits is now carrierRoutingMinDigits
routeServerTableTable	NAME CHANGED: routeServerTableMinPrefix digits is now routeServerTableMinDigits ADDED: routeServerTableMaxDigits, routeServerTableDescription, routeServerTableDidEntryIndex, routeServerTableTable, routeServerTableVariables

MIB table name	Description
switchPoolTable	ADDED: switchPoolRemoteWebServices
sipServerPoolTable	ADDED: sipServerPoolRemoteWebServices
h323ExternalGatewaysTable	DELETED: h323ExternalGatewaysConnIdleTimeout
callingGroupsTable	ADDED: callingGroupsPingMode
switchPoolTable	ADDED: switchPoolPingMode
huntGroupsTable	ADDED: huntGroupsPingMode
signalingSessionsTable	ADDED: signalingSessionsSessionNamedVariablesSource, signalingSessionsSessionNamedVariablesVariable, signalingSessionsSessionNamedVariablesValue
sipPeersTable	ADDED: sipPeersPingMode
sipServerAvailabilityTable	ADDED: sipServerAvailabilityPingMode
sipServerPoolTable	ADDED: sipServerPoolPingMode
carrierExchangesTable	ADDED: carrierExchangesPingMode
mediaSessionRecordTable	ADDED: mediaSessionRecordDtmfPrefIn, mediaSessionRecordDtmfPrefOut
routeServerBoxTable	ADDED: routeServerBoxTable
routeServerControlledActionStatusTable	ADDED: routeServerControlledActionStatusTable
routeServerDidTable	REMOVED: routeServerDidTag ADDED: routeServerDidTable, routeServerDidVariables
registrationPlanTable	ADDED: registrationPlanAlterUserParam
registrationRoutingTable	ADDED: registrationRoutingAlterUserParam

New Traps in Release 3.6.0m4

Trap name
callConnectedEventCustom
callCreatedEventCustom
callEventsCustomBase
callTerminatedEventCustom
eventLogTrap
h323SessCfgResponse
incomingDtmfDigitStart

Trap name
incomingDtmfDigitUpdate
outgoingDtmfDigitStart
outgoingDtmfDigitUpdate
processCoreDump
processDead
processFault

Changed Traps in Release 3.6.0m4

MIB table name	Description
h323CallAlerting	Objects included in trap have changed.
h323CallConnected	Objects included in trap have changed.
h323CallCreated	Objects included in trap have changed.
h323CallProceeding	Objects included in trap have changed.
callCreated	Added varbind for DTMF capability.
h323CallMediaChannelsUp	Added varbind for DTMF capability.

Removed MIB Objects in Release 3.6.0m4

MIB object/table name
h323ExternalGatewaysTable - h323ExternalGatewaysConnIdleTimeout

Known Problems, Restrictions, and Operational Considerations in 3.6.0m4

Virtual Dial Plan's Known Problems

- When the OS-E is routing to a hunt group via a VDP, the forward counters are incremented for each hunt attempt. The OS-E should not be doing this. (PD20410)
- When performing pre-dial plan normalization, the OS-E matches normalization routes owned by different VDPs. For example, if you have multiple VDPs configured as A, B, and C, when you route to A and check A's pre-routing normalization routes, the OS-E checks B and C as well. (PD20126)
- CAC only works on the last VDP selected in the chain. (PD19972)
- When using VDPs, the actions call-lookup and call-lookup-detail do not work. These commands only work with legacy dial plans. (PD19943)
- When the OS-E receives a 3xx with the legacy dial plans, you can configure the OS-E to lookup the contacts in the Contact header. This lookup does not occur when VDP is configured for these routes. (PD20111)

Deleting Primary IP Causes Secondary IP to Go Down

When deleting the primary IP, the secondary IP interface goes down. In order for the secondary IP to take over, the OS-E must be restarted. (PD19795)

Media Sessions Counter Between Active and Standby OS-E Not Synchronized

In a distributed-clustering configuration, the media-sessions counter is not synchronized between the active and standby OS-E. In the "active" OS-E, the media-sessions counter shows the number of media sessions correctly, however, the "standby" OS-E media-sessions counter is always zero. (PD17468)

Call Logs Archiving Link Does Not Work with New Archiving System

The management GUI Call Logs Archive link continues to work with the new archiving system configured and enabled. However, the Call Logs Archive link and the "Archive Specific" action do not work unless an accounting local database is configured for capturing call details records. (PD19631)

DTMF Translation From 2833 To SIP INFO Fails After Media Failover

DTMF translation from 2833 to SIP INFO fails after media failover. This situation occurs in a two-box HA setup where the caller supports SIP INFO and the called endpoint supports RFC-2833. When the call comes up, both signaling and media are running on Box 1, and DTMF is successfully translated. When a failover occurs, both signaling and media run on the backup box. However, the 2833 events received from the called endpoint are incorrectly being sent to the old master box. Instead, the 2833 events should be handled locally. (PD20156)

Call Logs Displaying Incorrect Numbers

In the Call Logs -> Sessions -> Call Record display in the Gui, the call-soure-regid and call-dest-regid are incorrectly reversed (i.e., the call-source-regid incorrect shows the destination info and vice-versa). (PD21359)

OS-E in Route-Server Clusters Not Booting Latest Route File

When running the Route Server engine on a multi-box cluster, Acme Packet recommends using a new name for the route set file each time it is updated. There is a known issue when an updated route set has the same file name as a route set that had been previously loaded on a restarting OS-E. In this case, the previous version of the route set file is incorrectly used. (PD12750)

Problems Using Management GUI on IE9

The management GUI does not support running on Internet Explorer 9 systems. The Call Logs Details display and tool tip pop-up information is rendered incorrectly. (PD22201)

Call Log Timestamps Do Not Match Clock and Timezone

Changing the timezone setting while the OS-E system is initializing can lead to some parts of the system using the old timezone value and some parts using the new value. To prevent this, perform a system restart after changing the timezone setting. (PD12406)

Default Policy Session-Config Is Not Applied to Inbound H.323 Calls

The **default-policy > session-config** isn't correctly applied to inbound H.323 calls. The default-policy is not being applied to the inbound leg, but instead applied to the outbound leg. Acme Packet recommends you create a **session-config-pool** entry and reference it from the appropriate configured **h323-server**. (PD19597)

Disabled Interface Still Active on OS-E

If you disable an ethernet interface on the OS-E and then restart it, the IP interfaces remain active. To keep the interfaces in a down state, use the **admin** state setting on the IP interfaces to disable them. (PD21542)

Unregistered Sender Directive Not Applied to Calls From Unregistered Parties

Pre-session-config > unregistered-sender-directive is not correctly applied to calls from unregistered parties. Even when this is set to **refuse**, making a call from an unregistered party results in a successful call.(PD22209)

Eventpush Process Not Sending Events Consistently

At times, when changing the ip > eventpush-service configuration, the OS-E stops sending events from the eventpush process. If that happens, do a warm restart. (PD18982)

Source Route Lookup Using Phone-Exact and Phone-Prefix Does Not Work

Source route lookup using phone-exact and/or phone-prefix does not work. When the OS-E is configured to use source route lookup, even though an incoming INV matches a source route using source-match as phone-exact, the OS-E rejects the call with a 404 Not Found. The same issue occurs with phone-prefix as well. (PD21370)

DNS-Group Server Pool Entries Remain after TTL Expires and Cache Entries are Removed

DNS-group server pool entries still remain, even after TTL expires and cache entries are removed. The dns-group initiates a DNS lookup after it receives an INVITE. The record from the DNS SRV/A query shows up as servers in sip-server-pool. The received response from the DNS server is stored in cache until the TTL of the corresponding entry expires. As soon as teh cache TTL expires, cache entries are removed. The OS-E fails to remove teh server from the server pool for the dns-group.(PD22179)

Calls Rejected Due to NAPTR Query Errors

In the case of a configured DNS-group, when the NAPTR query returns a response without any record, the OS-E starts the SRV query by appending_sip._UDP in front of the domain. If the SRV query also returns the response, “No Such Name,” the OS-E should then initiate an A query. It fails to do that and the call gets rejected with a 503. (PD22208)

Accounting Data to a Syslog Target Requires Configured Call Field Filters

If Accounting data is sent to a Syslog Target but no specific call field filters are configured, the different file types (proprietary, CSV, tab, and SML) output different fields. (PD22189)

Sip-Server-Availability Reason Does Not Change if REG Received Before Server Goes Down

The sip-server-availability status display may not display the correct “reason” parameter. In some cases, the “reason” status does not change to “response-received”.(PD22012)

OS-E Sends UDP Instead of TCP After NAPTR Query

If a NAPTR query on an FQDN returns a response indicating the TCP protocol field should be used, and after the SRV and A query lookups are done, the INV goes out using UDP instead of TCP. The OS-E fails to use the protocol field from NAPTR record for SIP messaging. (PD22210)

The NAPTR Records Order Field Not Working Properly

The OS-E is not correctly handling the “order” field in NAPTR records. When there are multiple NAPTR records, the order field has no effect on the next step. An SRV query goes out for all of the records. (PD22180)

VX Vlan Interface Being Incorrectly Marked Down

A VX vlan interface is incorrectly marked down if the primary VX IP interface is deleted without saving the config.

To work around this issue, delete the IP interface, save the config, create a new VLAN interface, and save the config. (PD19794)

Incorrect Route Numbers After Performing Multiple DID Range Imports

The **show route-server-controlled-action-status** action show how many DID/Prefix entries that were processed. Since DID routes are then expanded into multiple prefixes, the **show route-server-box** and **show route-server-table** actions may show something different. (PD20274)

The OS-E is Sending Accounting Records When It Should Not

If **vsp > accounting > admin** property is disabled, accounting records are still sent to configured file systems. (PD22005)

Release 3.6.0m3

New Features

The following sections describe the new features that have been added to Release 3.6.0m3.

Collecting Diagnostic Data From a Running OS-E

The OS-E has the ability to collect support data and store it in a single compressed file to be downloaded and forwarded to the Acme Packet support team for analysis. A **collect** action has been created which allows you to collect the information necessary to troubleshoot problems occurring on the OS-E.

By default, the OS-E collects the following data when the **collect** action is executed.

- Configuration data, including the following:
  - Current running configuration (even if it has not been saved yet)
  - Current /cxc/cxc.cfg configuration file
  - Backup configuration files in /cxc/backup
  - Schema files (*.xsd in /cxc/web)
- Certificate files found in the /cxc/certs directory
- Status data which is collected in two forms:
  - Text files that contain output equivalent to the status show commands
  - XML files that contain the same data, but in a structured format that is machine-readable and is used for automated analysis

  Status data can be collected in two different ways:
  - Default collection, in which a standard, pre-configured list of status classes is collected
  - Custom collection, in which status classes not included in the default list can be specified
- Crash files found in the /cxc_common/crash directory
- Log files found in the /cxc_common/log directory

- Directory contents

Enabling and Disabling Default Collection Parameters

Using the **services > collect > default-collect-settings** parameter, you can enable or disable these default parameters. When one of these properties is set to **disabled**, the corresponding data is not collected.

Note: Do not change the default-collect-settings object unless told to do so by technical support personnel.

```
config default-collect-settings>show -v

services
 collect
  default-collect-settings
   config enabled
   certificates enabled
   status enabled
   crash-files enabled
   log-files enabled
```

Under this object you can also edit the list of status classes, databases, and directories from which data is collected.

The **status-class** property specifies additional status classes to be collected. This property is a vector, so you can specify multiple entries. In addition, wildcards can be specified as well as the **-v** property to specify a verbose display in the status text file. For example:

```
config default-collect-settings>set status-class location-bindings-rejected -v
config default-collect-settings>set status-class system-*
config default-collect-settings>set status-class arena
```

The **database** property specifies the databases you want to collect. The valid databases are:

- log
- spotlite
- status
- dos
- directory
- accounting

This property is a vector, so you can specify multiple entries. For example:

```
config default-collect-settings>set database directory
config default-collect-settings>set database accounting
```

Note: Use the **directory** property with caution as it is possible to specify the collection of enormous amounts of data.

The **directory** property specifies any additional directories to be collected. For example:

```
config default-collect-settings>set directory /cxc_common/data1/dir1
config default-collect-settings>set directory /cxc_common/data1/dir2
```

Note: Use the **directory** property with caution as it is possible to specify the collection of enormous amounts of data.

Customizing Collection Parameters

In addition to the default parameters, you can configure custom collection parameters using the **services > collect > collect-group** parameter. Once you create a collect-group, you have the ability to disable the default collection parameters, certificates, status, crash-files, and log-files for that collect-group.

The following example shows the OS-E configured to collect only data related to accounting, while disabling collection of the other default collection parameters:

```
config collect>config collect-group accounting
Creating 'collect-group accounting'
config collect-group accounting>set description "Just accounting data"
config collect-group accounting>set certificates disabled
config collect-group accounting>set status disabled
config collect-group accounting>set status-class accounting*
config collect-group accounting>set crash-files disabled
config collect-group accounting>set database accounting
```

To collect this customized data, specify the group name when executing the **collect** action.

```
NNOS-E>collect accounting
```

Managing Collection Output Files

You can specify where the output files will be stored via the **services > collect > directory** property. The default (/cxc_common/collect) is sufficient in most cases. However, if you are collecting the contents of large databases, this property allows you to specify a mount with more available disk space.

When a new collect file is created, the old files are saved as backups. Older backup files are deleted when the number of backups exceeds the **services > collect > max-old-files** property.

```
config collect>set directory /cxc_common/collect_1
config collect>set max-old-files 5
```

Collecting Data from a Cluster

By default, the collect action collects data only from the box on which it is executed. Cluster-wide data collection can be specified by adding the cluster parameter to the action.

To collect the default data throughout the cluster, you must specify the **default** parameter.

```
NNOS-E>collect default cluster
```

To collect custom data from a configured collect-group, specify the collect-group (in this example accounting is used).

```
NNOS-E>collect accounting cluster
```

When cluster-wide data collection is specified, each OS-E collects the appropriate data independently and simultaneously. The OS-E on which the **collect** action is executed then combines the resulting data into a single file.

Viewing Status Classes Being Collected

The **show collect-status-classes** action displays which status classes are being collected. When entered with the **default** parameter, the OS-E default status classes are listed.

```
NNOS-E>show collect-status-classes default
```

You can also use the **show collect-status-classes** status provider to display status classes defined in custom configurations. The following shows accounting as an example.

```
NNOS-E>show collect-status-classes accounting

Status classes to be collected for 'Accounting':
--------------------------------------------------------------------------------
Source   Status class               Description
--------------------------------------------------------------------------------
```

```
config   accounting-recent           calls recently accounted
config   accounting-database        request information for accounting database
connections
config   accounting-files            accounting file information
config   accounting-store            accounting disk storage information
config   accounting-cdr-summary      accounting CDR summary
config   accounting-targets-file-system accounting file-system and
external-file-system targets
config   accounting-targets          accounting targets
```

Properties

Field	Description
Source	The source of the status classes being collected.
Status class	The status classes the OS-E is configured to be collecting.
Description	A description of the status classes being collected.

Collect Log Messages

The log class ‘collect’ has been added. The following messages are logged:

- collect[warning]: Collect action invoked with the following arguments:
- collect[info]: <various progress messages>
- collect[warning]: Collect action succeeded after X seconds; file ‘/cxc_common/collect/collect.tar.gz’ is X bytes
- collect[error]: <various error messages>
- collect[error]: Collect action failed; <error message>

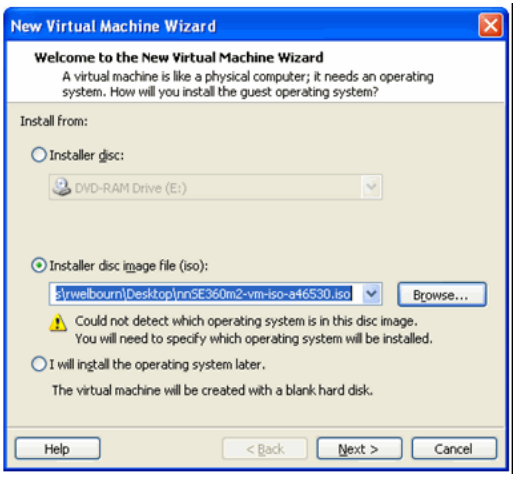
The recommended setting for the ‘collect’ log class is ‘warning’. The ‘info’ setting produces many log messages, all of which will appear in the log file (e.g., /box1/box1.txt).

Consolidating the VMPlayer Image

The OS-E no longer supports a VMPlayer-specific image. Instead, VMPlayer v3.1 allows installation via an ISO disk image, similar to the ESXi installer. For more information on the ESXi installer, see the *Net-Net OS-E Virtual Machine Information Guide*.

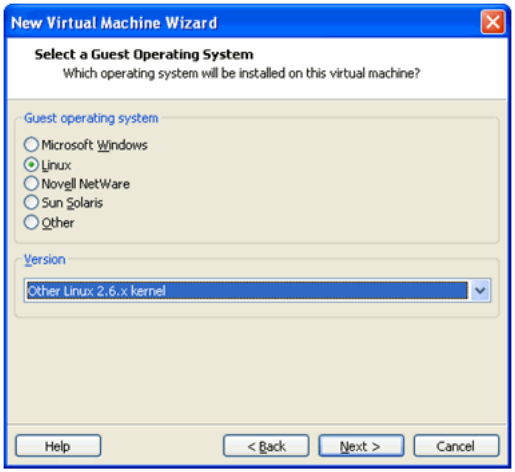
To install the VMPLayer 3.6.0m3 on your PC:

1. Download the OS-E ISO file to your PC.
2. Run the VMware Player and select **Create a New Virtual Machine**.
3. Browse in the Installer disc image file selection to the ISO image you have previously downloaded. Click **Next**.

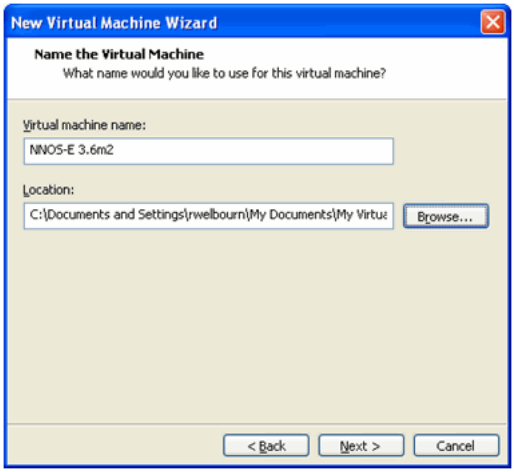


4. Specify **Linux** for the Guest operating system.

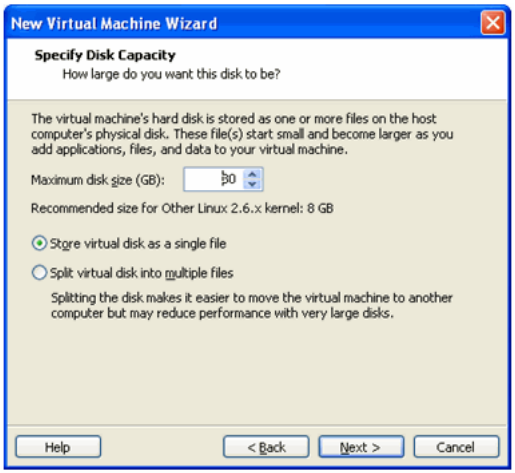
5. Specify **Other Linux 2.6.x kernel** in the Version drop-down box. Click **Next**.



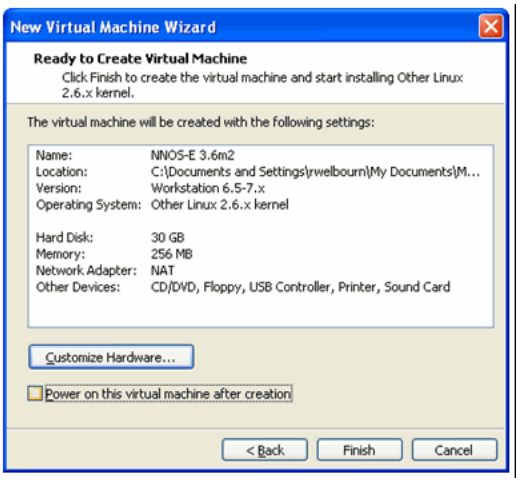
6. Enter the name you want to use for the virtual machine. Click **Next**.



7. Specify Maximum disk size in GB. You must specify a minimum of 30 GB, however Acme Packet suggests you run with a minimum of 80 GB. Click **Next**.



8. Click Customize Hardware...



9. Set the Memory to one of the following values:
   - 1024 MB
   - 2048 MB
   - 4096 MB
10. Change the number of Processors to a value greater than one if you have a multi-core system.

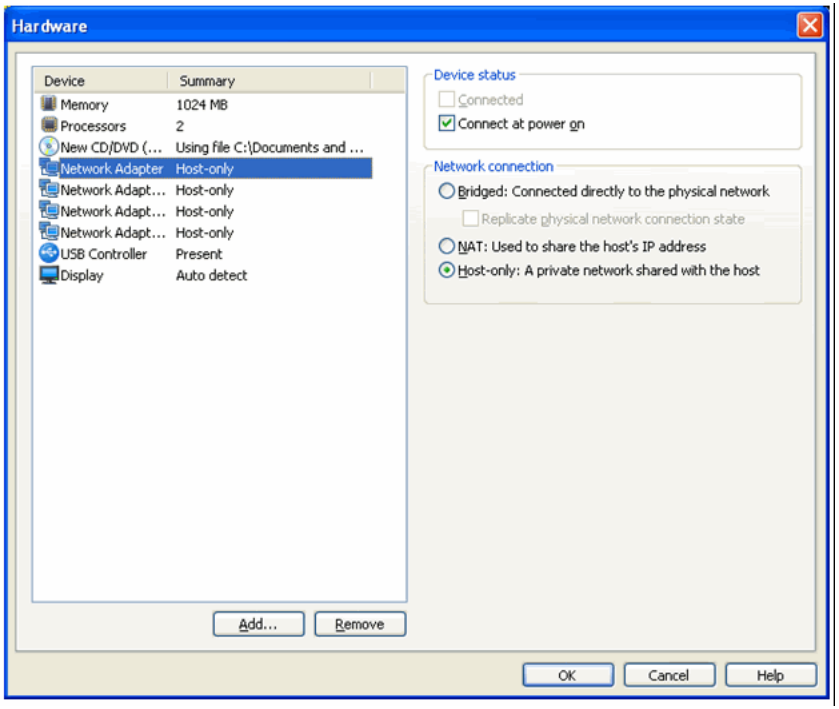
11. Remove support for the following devices by selecting them in the left-column and clicking **Remove**:

    - Floppy
    - Sound Card
    - Printer

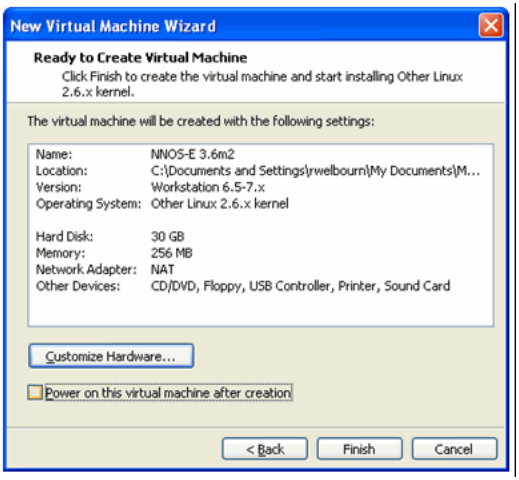
12. Change the existing Network Adapter to the to the Network Connection type you want to use. Ensure that **Connect at power on** is checked.

    Create as many additional network interfaces as you need by clicking **Add...** and selecting **Network Adapter**. Click **Next**. Set the Network Connection type you want to use and ensure that Connect at power is on is checked. Click **Finish**.

13. Click **OK** when you are finished.



14. Uncheck the **Power on this virtual machine after creation** box. Click Finish.



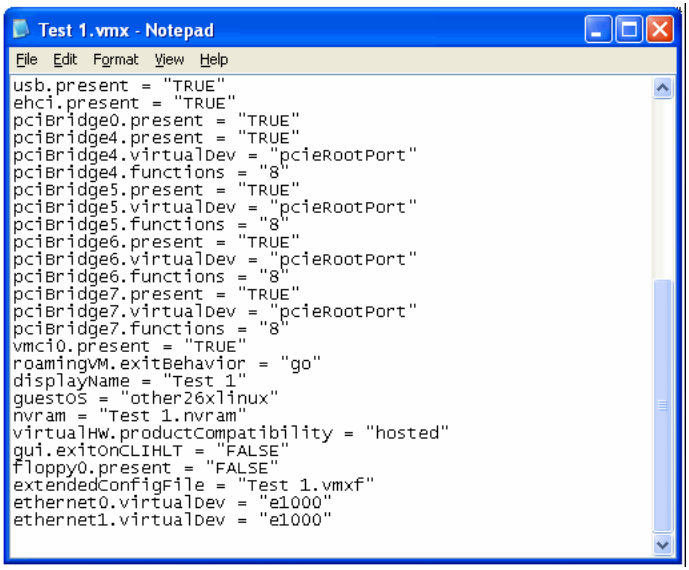
To ensure full support for the OS-E networking options, Acme Packet recommends setting the VM network adapters to e1000 as follows:

1. Find the directory where the VM was created. On a Windows system this defaults to **My Documents/My Virtual Machines/<name-given-to-VM>**. Open the file **<name-given-to-VM>.vmx** with a text editor.
2. Add a line for each Ethernet network adaptor at the end of the file as follows.

   ```
   ethernet<n>.virtualDev = "e1000"
   ```

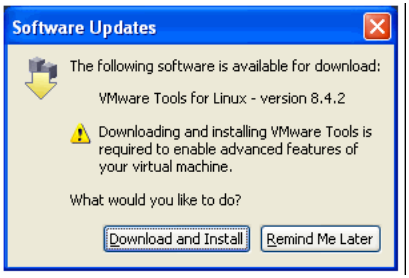
   Where <n> is 0, 1, 2, etc.

3. Save the file and exit the editor.



To complete the installation of the VMPlayer v3.1 onto your PC:

1. On the VMPlayer, select **Play virtual machine**. The VM starts and installation commences.
2. Choose **Remind Me Later** when prompted for Software Updates.



The installer will pause to confirm the installation.

3. Press **y** and **<enter>**. Installation will continue.

Limiting Licensing for Session Replication Recording

The OS-E allows you to enable the forwarding of audio to a Call Recording Server (CRS). With this functionality, you can limit the number of concurrent CRS sessions.

When the OS-E receives a request to establish a CRS session, it attempts to obtain a license for the call. If no license can be obtained for the call, the request is automatically rejected.

If a license is obtained by the OS-E, the recording session is allowed, and the call state gets updated in the signaling session information. Once the call is completed, the license is released.

The **features** > **media-forwarding-sessions** property specifies the number of concurrent media forwarding sessions the OS-E is licensed to handle.

Configuration Changes in Release 3.6.0m3

The section provides a summary of the additions, changes, and deletions to the OS-E configuration when upgrading to Release 3.6.0m3. It covers new objects and properties, configuration objects and properties that have been renamed, and those objects that have been deleted and are no longer available.

New Objects in Release 3.6.0m3

Object name	Associated properties	Description
collect		Configures the handling of data collection output files.
	directory	Specifies where the data collection output files will be stored. While the default directory is sufficient in most cases, if you are collecting the contents of a large database, this property allows you to specify a mount with more available disk space. **Example: set directory /cxc_common/collect_directory** The default setting is **/cxc_common/collect**.
	max-old-files	Specify the maximum number of old files the AA-SBC saves before backups are deleted. The minimum valid value is 1 and the maximum valid value is 50. **Example: set max-old-files 25** The default setting is **5**.
default-collect-settings		Enables or disables the default collection parameters. When one of these properties is set to disabled, the corresponding data is not collected.
	config [enabled | disabled]	Enable or disable the collection of configuration data. **Example: set config disabled** The default setting is **enabled**.
	certificates [enabled | disabled]	Enable or disable the collection of certificate data. **Example: set certificates disabled** The default setting is **enabled**.

Object name	Associated properties	Description
	status [enabled | disabled]	Enable or disable the collection of status data. **Example: set status disabled** The default setting is **enabled**.
	crash-files [enabled | disabled]	Enable or disable the collection of crash-file data. **Example: set crash-files disabled** The default setting is **enabled**.
	log-files [enabled | disabled]	Enable or disable the collection of log-files data. **Example: set log-files disabled** The default setting is **enabled**.
	status-class	Specifies additional status classes to be collected. This property is a vector, so you can specify multiple entries. In addition, wildcards can be specified as well as the -v property to specify a verbose display in the status output file. **Example: set status-class location-bindings-rejected -v**
	database	Specifies the databases you want to collect. This property is a vector, so you can specify multiple entries. The following are valid databases you can collect: • log • spotlite • status • dos • directory • accounting Note: Use this property with caution as it is possible to specify the collection of enormous amounts of data. **Example: set database accounting**

Object name	Associated properties	Description
	directory	Specifies any additional directories you want collected. This property is a vector, so you can specify multiple entries. Note: Use this property with caution as it is possible to specify the collection of enormous amounts of data. **Example: set directory /cxc_common/ data1/dir1**
collect-group		Configures custom collection parameters as well as the default parameters.
	config [enabled | disabled]	Enable or disable the collection of config data for this collect-group. **Example: set config disabled** The default setting is **enabled**.
	certificates [enabled | disabled]	Enable or disable the collection of certificate data for this collect-group. **Example: set certificates disabled** The default setting is **enabled**.
	status [enabled | disabled]	Enable or disable the collection of status data for this collect-group. **Example: set status disabled** The default setting is **enabled**.
	crash-files [enabled | disabled]	Enable or disable the collection of crash-file data for this collect-group. **Example: set crash-files disabled** The default setting is **enabled**.
	log-files [enabled | disabled]	Enable or disable the collection of log-file data for this collect-group. **Example: set log-files disabled** The default setting is **enabled**.

Object name	Associated properties	Description
	status-class	Specifies additional status classes to be collected for this collect-group. This property is a vector, so you can specify multiple entries. In addition, wildcards can be specified as well as the -v property to specify a verbose display in the status output file. **Example: set status-class location-bindings-rejected -v**
	database	Specifies the databases you want to collect for this collect-group. This property is a vector, so you can specify multiple entries. The following are valid databases you can collect: • log • spotlite • status • dos • directory • accounting Note: Use this property with caution as it is possible to specify the collection of enormous amounts of data. **Example: set database accounting**
	directory	Specifies any additional directories you want collected for this collect-group. This property is a vector, so you can specify multiple entries. Note: Use this property with caution as it is possible to specify the collection of enormous amounts of data. **Example: set directory /cxc_common/ data1/dir1**
lcr-import-service		Reserved for future use.
	admin	Reserved for future use.
	protocol	Reserved for future use.
	max-threads	Reserved for future use.

Object name	Associated properties	Description
	min-spare-threads	Reserved for future use.
	max-spare-threads	Reserved for future use.
	idle-timeout	Reserved for future use.
	ciphers	Reserved for future use.
	https-call-rates-download	Reserved for future use.

New properties in Release 3.6.0m3

Object name	Associated properties	Description
session-config\sip-settings; <server-type>\default-sip-settings	preserve-session-config-on-3xx [enabled | disabled]	Apply the same session configuration that was used for the initial INVITE when sending the INVITE for a 302. When disabled, the AA-SBC removes the dial plan and server session configurations from the merged configuration. **Example: set preserve-session-config-on-3xx enabled** The default setting is **disabled**.
static-stack-settings	max-proxy-transactions-per-vsp	*Secondary property.* Sets the maximum number of concurrent proxy transactions for the entire VSP. You can specify an integer or use the default, **automatic**, to use the platform specific factory value. **Example: set max-proxy-transactions-per-vsp** The default setting is **automatic**.
settings	max-proxy-transactions-per-session	*Secondary property.* Sets the maximum number of concurrent proxy transactions that a session can have. The minimum valid value is 1 and the maximum valid value is 65535. **Example: set max-proxy-transactions-per-session 30** The default setting is **20**.
permissions	lcr-import	Reserved for future use.
os	ip-frag-queue-control	Specify the number of milliseconds the AA-SBC holds onto an IP fragment when the first fragment has not been received. The minimum valid value is 1 and the maximum valid value is 20. **Example: set ip-frag-queue-control 15** The default value is **5**.

Object name	Associated properties	Description
media	discard-media-on-hold [enabled | disabled	*Secondary property*. Specifies whether to discard media from an endpoint when that endpoint is placed on hold. **Example: set discard-media-on-hold enabled** The default setting is **disabled**.
reg-ex-header	create-on-failed-match [true | false]	*Secondary property*. When **true**, construct a create header even when the expression is not a complete match. **Example: set create-on-failed-match false** The default setting is **true**.
reg-ex-header	append-on-failed-match [true | false	*Secondary property*. When **true**, execute the append action event when the create expression fails to match. **Example: set append-on-failed-match false** The default setting is **true**.
same time | lcs | mcs | avaya | sip-gateway | h323-server | sip-host | dns-group | sip-connection | trunk-group	add-user-to-connect [enabled | disabled]	*Secondary property*. When enabled, the OS-E puts the “user” (defined in the same server configuration) into the contact during register fail-over detection. For example the contact looks like this: “Contact: sip:user@1.2.3.4:5060; transport=udp;expires=3600” By default this parameter is disabled and the contact looks like this: “Contact: sip:user@1.2.3.4:5060; transport=udp;expires=3600” **Example: set add-user-to-connect enabled** The default setting is **disabled**.

Object name	Associated properties	Description
settings	unescape-header-params [true | false]	*Secondary property.* When set to the default value **true**, the OS-E changes the To-tag parameter and messages can be ignored. To ensure the OS-E does not alter any of the tag parameters, set this parameter to **false**. **Example: set unescape-header-params false** The default setting is **true**.
third-party-call-control	notify-dtmf-when-complete [enabled | disabled]	*Secondary property.* Specifies whether the OS-E forwards the DTMF notification via the Notify request sent at the beginning of the DTMF tone or the Notify request sent after the DTMF tone. **Example: set notify-dtmf-when-complete enabled** The default setting is **enabled**.

MIB Changes in Release 3.6.0m3

This section covers changes that have been applied to Management Information Base (MIB) object definitions.

New MIB Tables in Release 3.6.0m3

MIB table name	Description
There are no new MIB tables in Release 3.6.0m3.	

New MIB Objects in Release 3.6.0m3

MIB object/table name
licenseInfoOemBoxId
uid32InitialSeed
uid32CurrentSeed
uid32SeedWraps

MIB object/table name
uid32InitialSerial
uid32CurrentSerial
uid32FirstID
uid32LastID
uid32Created
uid32BoxBits
uid32BoxShift
uid32BoxMask
uid32SeedBits
uid32SeedShift
uid32SeedMask
uid32SerialBits
uid32SerialShift
uid32SerialMask

Changed Tables in Release 3.6.0m3

MIB table name	Description
auditTrailTable	REMOVED: auditTrailConfigRecId, auditTrailReferrerRecId
registrationPlanTable	ADDED: registrationPlanAlterUseUniquePortPerBinding
registrationProxyTable	ADDED: registrationProxyAlterUseUniquePortPerBinding
registrationProxyRoutingTable	ADDED: registrationProxyRoutingAlterUseUniquePortPerBinding
registrationRoutingTable	ADDED: registrationRoutingAlterUseUniquePortPerBinding
callingGroupsTable	ADDED: callingGroupsAddUserToContact
hungGroupsTable	ADDED: huntGroupsAddUserToContact
signalingSessionsTable	ADDED: signalingSessionsOrigInRequestURI
sipPeersTable	ADDED: sipPeersAddUserToContact
carrierExchangeTable	ADDED: carrierExchangeAddUserToContact

Known Problems, Restrictions, and Operational Considerations in 3.6.0m3

Master OS-E returns route-set results inaccurately

In a cluster configuration, the master OS-E consistently returns “result: not found” when the route-set is applied corrently.

To verify that routes have correctly loaded execute the **show route-server-table** command. (PD17429)

OS-E not creating a kernel rule after making changes to H.323 port

The OS-E does not create a kernel rule after making changes to the H.323 listener port.

To work around this issue, you must use different port ranges for peer and KG listeners. (PD12210)

Back-up/restore plug-in does not restore eth1 outside IP address on HP Procurve

The IP address of eth1 was changed after initial installation of a new template. When installing the template, eth1 was given a new IP during the installation process. Eth1’s IP address reverted back to the original IP address of when the template was upgraded to a new version. The outside IP is the only config that failed to be restored as the rest of the configuration restored properly.

To work around this issue, do not change addresses on the OS-E directly. (PD16576)

Note: This is specific to Avaya Aura installations.

CPU usage not being accurately displayed in the GUI or CLI

The CPU usage of the NNOS-E VM is not being correctly displayed in either the “Home” screen of the NNOS-E GUI or through the “show cpu-usage” command in the NNOS-E CLI. It appears that the actual CPU usage is being displayed at certain points but not others. (PD16521)

No call failover if media/signaling eth link is lost (if op-state marked down on DOM0 only)

When running a test using two OS-Es configured as a two-SBC cluster, create a call with anchored media. Media-stream-stats shows RTP moving end-end in both directions. Pull eth3 cable and note that DOM0 recognizes loss of link:

e1000e: eth3 NIC Link is Down

sbcPublic: port1(eth3) entering disabled state

There is currently no notification from DOM0 back to OS-E when operational state transitions from up to down. (PD16525)

Note: This is specific to Avaya Aura installations.

SIP process crashed in openSSL during lab “fuzzing” test

IW call fuzzing tests were being run. A fault was seen on the OS-E while investigating IW call failures-details of what traffic was running through the SBC at the time of the crash unknown.

This only occurs in H.323 — SIP interworking. (PD16581)

GUI tabs disappearing

GUI tabs may disappear and/or unreadable characters appear at the top of left frame when clicking on an object on the left frame. This is an intermittent problem. (PD16637)

Release 3.6.0m2

New Features

The following sections describe the new features that have been added to Release 3.6.0m2.

Route Server Tandem Routing Enhancement

The OS-E now supports tandem hop route server functionality when a call must traverse regions. In previous OS-E releases, only specific gateways configured locally were routed.

When the OS-E receives a response from the route server, it looks for a specific match configured on the sip-gateways. Both the carrier and endpoint tags must match for the OS-E to route the server.

The **settings > named-lookup-match** property allows you to configure a secondary lookup system. When an endpoint does not match, this property allows you to either match all endpoints under the carrier, or use DNS to resolve the endpoint as an FQDN. For more information on the **named-lookup-match** property, see "Configuration Changes in Release 3.6.0m2.".

Improved ANI Configurations For H.323-SIP Calls

In releases prior to 3.6.0m2, the OS-E required specification of the ANI source for use in creating the SIP From: header URI. The OS-E is now flexible while creating the SIP From: header used for inbound H.323 calls that are interworked to SIP and ensures the From: header always contains a complete URI.

A property, **useanon**, under the **h323-to-sip-fromheader-spec** object, has been created to enable this functionality. For more information on the useanon property, see "Configuration Changes in Release 3.6.0m2." When this property is enabled, the From: header is assembled in the following manner:

- The configured scheme (default value sip:) is always used.
- The configured user is then appended. This value can be taken from the Q931 Calling Party Number, the sourceAddress alias in the Setup-UUIE (h323-id, url-id, or email-id), or a configured string. If this portion is omitted, the user is automatically set to "anonymous."
- The configured host is then appended. This value can be taken from the configured h323-server domain, the sourceAddress alias in the Setup-UUIE (h323-id, url-id, or email-id), or a configured string. If this portion is omitted, the host is automatically set to the IP address of the H.323 gateway which transmitted the Setup.
- The configured suffix is then appended. This value defaults to an empty string unless otherwise configured by the OS-E Administrator.

Linking H.323 Servers to Services Routing Mechanics

The OS-E now uses standard services routing to dynamically identify the most appropriate local interface and listening port to use and advertise for each remote H.323 gateway and gatekeeper. When the H.323 process starts, services routing is consulted to determine the most appropriate local listening ports to use when contacting the server for each configured H.323 server.

The following lists the types of remote H.323 servers that can be configured on a OS-E and the way the OS-E binds listening ports to servers for each type:

- A remote H.323 Gateway (GW). This configuration is often referred to as "GW-GW." No specific listeners are bound to the configured remote H.323 GW. When the OS-E makes an outbound H.323 call, services routing is used to select the appropriate local interface for reaching the remote H.323 GW and establishing H.225.0 and H.245 TCP connections.
- A remote H.323 Gatekeeper (GK) where the OS-E contacts the remote GK as an H.323 GW. This configuration is often referred to as "GW-GK." An H.225.0 RAS listener and H.225.0 call signal listener are bound to each remote GK (both active and standby). When the OS-E registers, these listeners are sent to the remote GK. If the GK supplies any alternate GKs, the OS-E binds RAS and H.225.0 call signal listeners to each alternate GK.
- A remote H.323 GK where the OS-E contacts the remote GK as a peer GK. This configuration is often referred to as "GK-GK." An H.225.0 RAS listener and an H.225.0 call signal listener are bound to the remote peer GK. If the OS-E confirms a location request from that GK, these listeners are transmitted to the peer GK.

Thus, there are 3 types of H.323 listening ports that can be configured on the OS-E. All H.323 listening ports are configured under a particular interface and IP address. The following table displays the port types that can be configured:

Configuration	Port	Transport	Use
h323 > port	H.225.0 Call Signaling	TCP	All
h323 > gatekeeper-port > port-type=peer	H.225.0 RAS	UDP	GK-GK
h323 > gatekeeper-port > port-type=client	H.225.0 RAS	UDP	GW-GK

Peer Gatekeeper Support on the OS-E

The OS-E allows for the configuration of external peer gatekeepers. A peer gatekeeper (peer-GK) is an H.323 gatekeeper that communicates with the OS-E via Location Request (LRQ) messages for call routing information.

The following configurations must be applied for the peer-GK to function properly on the OS-E:

- A peer-GK must have a unique IP address.
- A peer-GK's IP address and UDP RAS port must be configured in the first server-pool entry.
- The server-pool for a configured peer-GK must have only one entry.
- At least one peer GKPort must be configured. The OS-E creates a UDP listener for each GKPort specified.

Note: Clustered GK support exists only for non-peer GKs.

A peer-GK is configured in the **vsp > enterprise > servers** object. The following example shows a configuration for a peer-GK:

```
   config h323-server GnuGK-Peer-FC4
    set server-type h323-gatekeeper
    config server-pool
     config server GnuGK-Peer-FC4
      set host 172.44.200.35
      set port 1719
      set local-ip 172.44.10.67
      set connection-role responder
     return
    return
    set local-server-type h323-gatekeeper
    set ras-settings 3600 5 3 X +1 h323ID disabled false false 10 false
PollRejected 15 5 5 15
    config h225-settings
     set h323-user-alias dialedDigits
    return
   return
```

It is possible to specify the RAS listening port for peer-GK communication. This is configured in the box > interface > ip > h323 > gkport. The following example shows a configuration for two listening TCP ports accepting inbound H.323 call requests (ports 1720 and 1721) and two listening UDP ports for accepting peer-GK RAS traffic (1719 and 1725):

```
config interface eth0
   config ip federate-a
    set ip-address static 172.44.10.67/16
    config h323
     set port 1720
     set port 5021
     set port 5022
     set port 5023
     set gatekeeper-port 1717 client
     set gatekeeper-port 1719 peer
     set gatekeeper-port 1748 client
     set gatekeeper-port 7000 peer
```

If destination route lookup for the LRQ succeeds, an LCF message is sent by the OS-E to the peer-GK. The location confirmation message contains the IP address and port indicated by the destination route lookup engine. The location confirmation rasAddress is set to the OS-E local IP and port used for RAS messaging to this peer.

The following table lists conditions when LRQ will not be confirmed. In some cases the LRQ will be silently discarded and in others an LRJ will be generated by the OS-E:

Errors encountered during processing LRQ	Action
Remote GK not found in config	Discard LRQ
Remote GK not peer	Discard LRQ
Internal errors (ie., memory allocation)	Discard LRQ
LRQ already being processed	Discard LRQ
LRQ destinationInfo aliases missing	LRJ sent, aliasesInconsistent
LRQ destinationInfo aliases unsupported	LRJ sent, neededFeatureNotSupported
LRQ replyAddress not ipAddress	LRJ sent, neededFeatureNotSupported
LRQ processing timeout	LRJ sent, resourceUnavailable
SIP LCR returns not-found	LRJ sent, notRegistered

Using Peer-GK for H.323 Outbound Call Routing

With the peer-GK support on the OS-E, the OS-E is now capable of issuing H.225.0 RAS Location Requests to configured peer-GKs when making outbound H.323 calls, regardless of whether the inbound call-leg is SIP or H.323. The LRQ response furnished by the peer-GK is used to decide if the call should be admitted or rejected and determine to where the outbound SETUP message should be delivered.

Zone-Directory Gatekeeper Support

The OS-E now handles receiving RAS admission and location responses from any configured external gatekeeper. The OS-E can issue an admission or location RAS request to one gatekeeper and receive the corresponding RAS response from a different gatekeeper.

One example of this is to have a Zone Gatekeeper (ZGK) configured to receive admission and location requests from the OS-E. The ZGK then goes onto forward those requests to a Directory Gatekeeper (DGK).

If the external gatekeeper transmitting the RAS response is not configured on the OS-E and there is no default gatekeeper configured, the RAS response is discarded. There can be no more than 65535 outstanding admission and location requests with zone-directory gatekeeper support.

Clustered Gatekeeper Support

The OS-E allows you to configure multiple external gatekeepers with identical **server-pool** > **host** and **port** values. When configured this way, the OS-E supplies each remote gatekeeper with unique RAS information in order to differentiate.

When a remote gatekeeper sends RAS traffic to the OS-E, the combination of the gatekeeper remote IP address and the local RAS port receiving the RAS traffic is used as a lookup key to identify the remote gatekeeper. Once identified, the OS-E validates the traffic. If no default gatekeeper exists, any RAS traffic not matching a configured external gatekeeper is discarded.

However, when an external gatekeeper is configured with **server-pool > local-port** set to zero, the user must ensure each remote gatekeeper has a unique IP address.

Paravirtualization Support for Xen

The OS-E now supports paravirtualization (PV) for Xen support. Because of this, the Xen installation has changed.

Installing software on the Xen server

This section explains how to install a OS-E disk image on a generic 3.4.2 Xen server running on a Centos 5.4 system.

NOTE: These instructions should be considered a guide and may need to be modified appropriately for a particular environment.

1. Place the disk image on the Centos server with an applicable method such as SCP or FTP.
2. Uncompress the image:

   ```
   gunzip nnSE360m3-xen.img.gz
   ```

3. Ensure there are at least two virtual bridges for connecting to the OS-E. A standard Xen installation should create a bridge based on the primary interface. The example used here is eth0. In the following example, two additional virtual bridges are created and physical interfaces eth1 and eth2 are attached to them:

   ```
   brctl addbr virbr0
   brctl addif virbr0 eth1
   brctl addbr virbr1
   brctl addif virbr1 eth2
   ```

4. Create a Xen configuration file in /etc/xen. Further steps assume the name **NNOSE**. The following example sets the memory to 1GB with 4 CPUs. Change the mac addresses to be unique in your network, and ensure that the file in the **disk** line properly references your disk image.

   ```
   name="NNOSE"
   memory=1024
   vcpus=4
   on_poweroff="destroy"
   on_reboot="restart"
   on_crash="restart"
   disk=['file:/vms/nnSE360m4.tar.gz,xvda,w']
   vif=["mac=00:16:4e:00:00:00,bridge=eth0","mac=00:16:4e:00:00:01,
   bridge=virbr0",
   "mac=00:16:4e:00:00:02,bridge=virbr1"]
   kernel="/usr/lib/xen/boot/pv-grub-x86_32.gz"
   extra="(hd0,1)/grub/menu.lst"
   ```

5. Launch the VM with the serial console to complete installation. The following is a small sample of the expected output from this step:

```
xm create -c NNOSE
[root@xen-centos vms]# xm create -c NNOSE
Using config file "/etc/xen/NNOSE".
Started domain NNOSE (id=1)

                            Xen Minimal OS!
  start_info: 0xa67000(VA)
    nr_pages: 0x40000
  shared_inf: 0xcfe50000(MA)
     pt_base: 0xa6a000(VA)
nr_pt_frames: 0x9
    mfn_list: 0x967000(VA)
   mod_start: 0x0(VA)
     mod_len: 0
       flags: 0x0
    cmd_line: (hd0,1)/grub/menu.lst
  stack:      0x946780-0x966780
MM: Init
      _text: 0x0(VA)
     _etext: 0x61af5(VA)
   _erodata: 0x76000(VA)
     _edata: 0x7b6d4(VA)
stack start: 0x946780(VA)
       _end: 0x966d34(VA)
  start_pfn: a76
    max_pfn: 3fffd
Mapping memory range 0xc00000 - 0x3fffd000
setting 0x0-0x76000 readonly
skipped 0x1000
MM: Initialise page allocator for c70000(c70000)-0(3fffd000)
MM: done
Demand map pfns at 3fffe000-bfffe000.
Heap resides at bfffff000-fffff000.
Initialising timer interface
Initialising console ... done.
gnttab_table mapped at 0x3fffe000.
Initialising scheduler
Thread "Idle": pointer: 0xbfffff008, stack: 0xc90000
Initialising xenbus
Thread "xenstore": pointer: 0xbfffff478, stack: 0xca0000
Dummy main: start_info=0x966880
Thread "main": pointer: 0xbfffff8e8, stack: 0xcb0000
"main" "(hd0,1)/grub/menu.lst"
vbd 51712 is hd0
```

```
   ******************** BLKFRONT for device/vbd/51712 **********


   backend at /local/domain/0/backend/vbd/1/51712
   Failed to read /local/domain/0/backend/vbd/1/51712/feature-barrier.
   Failed to read /local/domain/0/backend/vbd/1/51712/
feature-flush-cache.
   83886080 sectors of 0 bytes
   **************************
   Press `ESC' to enter the menu... 0
     Booting 'Covergence Session Manager on 1st partition'

   root (hd0,2)
    Filesystem type is reiserfs, partition type 0x83
   kernel /boot/vmlinuz-covergence root=/dev/xvda3 rootdelay=10
ramdisk_size=4096
   crashkernel=64M@16M clocksource=acpi_pm

   ...

   Net-Net OS-E
   Copyright (c) 2004-2010  Acme Packet Inc.

   username:
   Net-Net OS-E
   Copyright (c) 2004-2010  Acme Packet Inc.

   username:
```

Locally Generated Ringback During Unattended Call Transfers

The OS-E provides support to specify an audio file to be played to the user while waiting for an unattended call transfer to be completed. Upon successful connection to the transferee, the audio file is terminated and the transferred party is re-invited with audio information from the transferee.

If the connection attempt fails after all possible configured routes have been attempted, the audio file is terminated and, if possible, audio is restored between the transferred and transferrer. If the transferrer is no longer available, the transferred party is disconnected.

The configuration parameter **transfer-file**, under the **third-party-call-control** object, has been created to allow the user to specify the audio file to be played during transfer. For more information about this parameter see "Configuration Changes in Release 3.6.0m2."

TCP Kernel Buffer Congestion Control Status Display

The **show tcp-skb-congestion-control** command displays the status of the TCP kernel buffer congestion control feature, including the admin state, current threshold, as well as some kernel buffer usage counters.

```
NNOS-E> show tcp-skb-congestion-control
  admin:  enabled
  threshold:  5000
  skbs-in-use:  2096
  max-skbs-in-use: 2506
  tcp-dropped-pkts: 378
```

Field	Description
admin	**Displays whether or not TCP kernel buffer congestion control is enabled.**
threshold	**Displays the configured threshold of the TCP kernel buffer congestion control.**
skbs-in-use	**Displays the current number of system-wide kernel buffers currently in use.**
max-skbs-in-use	**Displays the maximum number of kernel buffers that the OS-E has had in use at any given time.**
tcp-dropped-pkts	**Displays the number of TCP packets that have been dropped because the kernel buffer usage has exceeded the configured threshold.**

Fixes

The following table summarizes the fixes that have been applied in Release 3.6.0m2:

Component	Description	Problem ID	Found in Release
Routing	Some trace events, associated with weighted round robin load balancing in services-routing are at error level when they are not really error conditions.	pd11171	3.6m1
SIP	Pointer incorrectly deleted, causing faults.	pd11008	3.6m1
Dial Plans	Joined-matches does not work when one route is a hunt group.	pd11256	3.6m1
H.323	The OS-E is transmitting a 404 Not Found when there is a default gatekeeper configured.	pd11217	3.6m1
LCR	Move memory allocation so that the allocated resource persists for the life of the call.	pd11288	3.6m1
Cluster	Errors in the SIP process after a vsp-reset is executed in a multibox cluster.	pd11029	3.6m1
SIP	Handle null pre-session configuration settings.	pd11083	3.6m1
SIP	Faults occurring during parallel forking.	pd10571, 10572, 10573	3.5.4
Database	Database problems after load test.	pd10774	3.5.8
Accounting	File-system accounting not working properly.	pd10952	3.6.0
H.323	LRJ takes 5 seconds to respond to GK.	pd11559, 11565	3.6m2
H.323	H.323 to SIP calls need a Local IP option when creating To: address.	pd11610	3.6m2
H.323	H.323 calls that are routed back to GK get an LCF.	pd11623	3.6m2
H.323	LRQ gets LCF even with LCR lookup failure.	pd11603	3.6m2
LCR	LCR diameter traffic being routed improperly.	pd11498	3.6m2
H.323	The capability preference table is being overrun.	pd10951	3.5.2
LCR	Route-server missing alteration settings after a replace-file.	pd11665	3.6m1
Media	Auto anchoring not releasing the media.	pd11056	3.5.5

Component	Description	Problem ID	Found in Release
Media	In cases where endpoints are behind a NAT for which the OS-E will release media, crypto information is negotiated between both parties and the call comes up fine. However, after the call is put on hold, the crypto information is not included when the OS-E sends an Invite.	pd9954	3.5.5
Media	Post-Dial Digits for file-play-broadcast are not being recognized by distant end systems.	pd11629	3.6m1
LCR	Cannot call-hunt in conjunction with LCR hookups.	pd11763	3.6m2
SIP	When the UAC performs parallel forking where the only difference in the invites is the Via branch, both calls share the same session.	pd11818	3.6m1
Diameter	Diameter connection does not detect a down server and failover to another member of the diameter group.	pd11936	3.6m2
Interworking	If media ports are unavailable during a SIP-H.323 call, the H.323 side of the call fails but does not clear out the SIP side of the call.	pd11934	3.6m2
DNS	When a DNS endpoint is returned via the route server, the OS-E only routes the first result.	pd11975	3.6m2
H.323	LRQ and LCF handling uses the GK server profile for the outbound setup rather than the default or explicit server profile.	pd11695	3.6m2
Route Server	When resolving routes via DNS, the route server does not route to addresses not already configured on the OS-E.	pd11930	3.6m2
SSH	Intermittent SSH connectivity problems occurring.	pd11898	3.6m2
Dial Plans	Subscribe messages using dial plan routed incorrectly after a 401 Unauthorized message.	pd10833	3.6.0
Route Server	Route-set configuration does not have the ability to trim duplicates.	pd11935	3.6m2

Component	Description	Problem ID	Found in Release
Diameter	Diameter request not honoring the **diameter-group** > **request-timeout** configuration.	pd12076, 12148	3.6m2
Interworking	Information for policy matching not being sent over to SIP for H.323-SIP calls.	pd12157	3.6m2
Interworking	Session-config policy authorization not merged into H.323-SIP calls	pd12161	3.6m2
Loopback Calls	Loopback call support not functioning properly.	pd11199, 11200	3.6.0
LCR	LCR to DNS must be able to resolve to a sip-gateway.	pd11947	3.6m2
Interworking	H.323 to SIP calls are ignoring sip-directive policy.	pd12187	3.6m2
Status	After issuing **show sip-summary-rates-by-box** sampling services experiences faults.	pd12188	3.6m2
SIP	The OS-E refuses a NOTIFY after the initial SUBSCRIBE and NOTIFY messages succeed.	pd12183	3.6m1p1
SIP	The 3PCC pre-call announcement is not being played.	pd11885	3.6m2
Kernel	The **tcp-skb-congestion-control** property incorrectly defaults to enabled with a 40,000 kernel buffer threshold if the **box > os** configuration object is not configured.	pd12099	3.6m1
SIP	After receiving a REFER message, the OS-E disconnects the call.	pd11855	3.6m1
DNS	The OS-E needs the ability to configure CNAME DNS records locally.	pd12238	3.6m2
Config	The master-service server-load is no longer present after an upgrade from 3.4 to 3.6.	pd12237	3.6m1p1
Base Services	Fix initializing timing issue with memory pools.	pd12329	3.6m2
LCR	Route-server databases become out of sync after upgrade.	pd11950	3.6m2

Component	Description	Problem ID	Found in Release
SIP	The virtual dial plan is selectable in the dial plan peer type compound, however the virtual dial plan pool is hidden.	pd12469	3.6.0m1
DNS	Need the ability to configure CNAME and wildcard CNAME DNS records locally.	pd12238	3.6.0m2

Configuration Changes in Release 3.6.0m2

The section provides a summary of the additions, changes, and deletions to the OS-E configuration when upgrading to Release 3.6.0m2. It covers new objects and properties, configuration objects and properties that have been renamed, and those objects that have been deleted and are no longer available.

New Objects in Release 3.6.0m2

Object name	Associated properties	Description
cluster-server-load		Configures sampling for the SIP server load status.
	admin [enabled | disabled]	Specifies whether the status sampling configuration is active and in effect. **Example: set admin disabled** The default setting is **enabled**.
	interval	Defines how often the OS-E polls the status provider for data. The minimum polling time is 30 seconds. **Example: set interval 1:45:00** The default setting is **1:00:00**.
active-calls		Configures the sampling for currently active calls.
	admin [enabled | disabled]	Specifies whether the status sampling configuration is active and in effect. **Example: set admin disabled** The default setting is **enabled**.

Object name	Associated properties	Description
	interval	Defines how often the OS-E polls the status provider for data. The minimum polling time is 30 seconds. **Example: set interval 1:30:00** The default setting is **1:00:00**.
cname		A CNAME record maps a configured alias to a known name. This value can be exact or wildcarded. **Example: config cname abc.com**
	match	Select whether the OS-E matches the CNAME exactly or if it is a wildcarded match. The following are valid options: • exact — The OS-E only matches if the FQDN is exact (in this example abc.com). • wildcard — The OS-E matches if the FQDN is a wildcard (in this example www.abc.com, but not if it's exactly abc.com). **Example: set match wildcard** The default setting is **exact**.
	alias	Enter the alias you want associated with the CNAME records. **Example: set alias internal.abc.com**

New Properties in Release 3.6.0m2

Object name	Associated properties	Description
settings	named-lookup-match	When the OS-E receives a response from the route server, it looks for a specific match configured on the sip-gateways. Both the carrier and endpoint tags must match for the OS-E to route the server. This parameter allows you to configure a secondary lookup. The following are valid values: • specific—The OS-E does not make a second effort. The carrier and endpoint tags must both match. • grouped—If the endpoint does not match, match all endpoints under the carrier. • dns—If the endpoint does not match, use DNS to resolve the endpoint as an FQDN. **Example: set named-lookup-match dns** The default setting is **grouped**.
h323-to-sip-fromheader-spec	use-anon [true | false]	When enabled, as the H.323 process builds the SIP From: header for a received H.323 SETUP message it will do the following: • use anonymous as the user portion of the URI if after applying h323-to-sip-fromheader-spec config the user portion is empty • use the IP address of the H.323 gateway which transmitted the SETUP as the host portion of the URI if, after applying h323-to-sip-fromheader-spec config, the host portion is empty This guarantees a valid From: header URI will exist when sent to the SIP process. When set to false there is some chance an incomplete URI could be passed to SIP. **Example: set use-anon true** The default setting is **false**.

Object name	Associated properties	Description
route-server	client-request-sender	Describes who sends requests to the route-server. The following are valid values: • only-master—The request goes from the route-server master in the client cluster. • local-host-box—The host must be listed as a host-box for route-server master-service. **Example: set client-request-sender local-host-box** The default setting is **only-master**.
session-config>sip-settings\ session-config-pool>sip-settings	last-resort-request-uri [enabled | disabled]	If both the dial plan and location cache look ups fail, when this parameter is enabled, the OS-E attempts to route the call using the Request-URI of the incoming INVITE. If you want to limit routing to dial plans and the location cache, set this parameter to disabled. **Example: set last-resort-request-uri disabled** The default setting is **enabled**.
authentication	initial-challenge-stale	Specifies whether the stale parameter is included in authentication challenges, per RFCs 2069 and 3261. The following are valid values: • true—Includes stale=”true” in the challenge. • false—Includes stale=”false” in the challenge. • none—The stale parameter is not included in the challenge. **Example: set initial-challenge-stale none** The default setting is **true**.

Object name	Associated properties	Description
altered-header\header-normalization\altered-body\reg-ex-header\reg-ex-collector	apply-to-dialog	Allows you to configure where to apply these options for a session. The following are valid values: • inbound—Apply to inbound dialog only. • outbound—Apply to outbound dialog only. • both—Apply to both inbound and outbound dialogs. **Example: set apply-to-dialog inbound** The default setting is **both**.
inbound-header-settings\header-settings	apply-to-allow-block-to-dialog	Specifies whether the allow and block properties of this object apply to a specific dialog or not. The following are valid values: • inbound—Apply to the inbound dialog only. • outbound—Apply to the outbound dialog only. • both—Apply to both inbound and outbound dialogs. **Example: set apply-to-allow-block-to-dialog inbound** The default setting is **both**.
third-party-call-control	allow-lcr-for-refer [enabled | disabled]	When running the route server under third-party-call-control, information may need to be obtained off of the OS-E, causing a delay. When this parameter is enabled, the OS-E can avoid potential problems caused by this delay. **Example: set allow-lcr-for-refer enabled** The default setting is **disabled**.
third-party-call-control	transfer-file	Select the file of the media to be played while a blind transfer is taking place. **Example: set transfer-file data1** There is no default setting.

Object name	Associated properties	Description
settings	track-sip-messages [enabled | disabled]	Specifies whether the OS-E tracks the response to SIP REGISTER and INVITE messages. When enabled, the show sip-register-responses and show sip-invite-responses status providers include data indicating the type and number of responses sent and received (e.g., the number of 200 OKs, 503s, etc.) **Example: set track-sip-messages enabled** The default setting is **disabled**.
settings	database-connection-memory-limit	Specifies the maximum memory, in kilobytes, allowed per database connection. The connection ends if this memory limit is exceeded. Minimum: 100000 Maximum: 3000000 **Example: set database-connection-memory-limit 200000** The default setting is **automatic**.
settings	unclean-shutdown-recover	Specifies how the local database is handled during startup after an unclean shutdown. An unclean shutdown may cause corruption in the database and is usually caused by a crash. The following are valid values: • always-archive—Always archive data if unclean shutdown is detected. You must also enter the number of times for the OS-E to archive (from 1 to 20). • attempt-repair—Attempt corruption detection and repair and archive only if repair fails. **Example: set unclean-shutdown-recover attempt-repair** The default setting is **always-archive 3**.

Object name	Associated properties	Description
settings	allow-route-set-duplicates [enabled | disabled]	*This is a secondary property.* By default, the OS-E allows duplicate destination routes. When this property is disabled, duplicate entries are removed and the OS-E has only one entry in the route-set. **Example: set allow-route-set-duplicates disabled** The default setting is **enabled**.
os	tcp-skb-congestion-control [enabled | disabled] <threshold>	Sets a threshold of system-wide kernel buffer usage before the OS-E will proactively prevent the depletion of the remaining system resources by dropping all received TCP packets. When enabled, TCP packets will be dropped until the kernel buffer usage falls below the configured threshold. **Example: set tcp-skb-congestion-control enabled 300000** The default settings are **disabled** and **automatic**.
route-server	simple-updates	This parameter allows users to run controlled updates only without the possibility of running a simple update accidentally. When disabled and a simple update is executed, the user receives the error, “Only controlled updates are permitted by config.” **Example: set simple-updates disabled** The default setting is **enabled**.

Deleted Properties in Release 3.6.0m2

Object name
vinterface > preempt-delay

Default and Other changes in Release 3.6.0m2

Property name	Change
h323 > gkport	**Default for port-type is now peer.**
virtual-threads > urgent-congestion-threshold	**Default changed from 128 to 32.**
virtual-threads > priority-congestion-threshold	**Default changed from 256 to 64.**
virtual-threads > regular-congestion-threshold	**Default changed from 32 to 128.**

MIB Changes in Release 3.6.0m2

This section covers changes that have been applied to Management Information Base (MIB) object definitions.

New MIB Tables in Release 3.6.0m2

MIB table name	Description
clusterServerLoadTable	Previously marked obsolete.
clusterServerLoadDetailTable	Previously marked obsolete.
gatewayLoadMirrorTable	Previously marked obsolete.
trunkLoadMirrorTable	Previously marked obsolete.
callsTable	Displays a list of active calls for the specified time period.
sessionsTable	Active sessions, indexed by session ID.
sipRequestsTable	Statistics for SIP request messages.
sipRequestsByTagTable	Statistics for SIP request messages associated with tags.
routeServerBackupsTable	Statistics for LCR backup.

New MIB Objects in Release 3.6.0m2

MIB object/table name
routeServerActionStatusAction
tcpSkbCongestionControlAdmin
tcpSkbCongestionControlThreshold

MIB object/table name
tcpSkbCongestionControlSkbsInUse
tcpSkbCongestionControlMaxSkbsInUse
tcpSkbCongestionControlTcpDroppedPkts

New SNMP Trap Entries in MIB for Release 3.6.0m2

Trap name	Description
h323CallRejected	An H.323 call leg has been terminated.
skbUsageTrap	An increase in the kernel buffer usage indicates a possible depletion of OS-E resources.
tcpSkbCongestionDroppedPktsTrap	TCP packets dropped due to kernel buffer congestion indicates a possible depletion of OS-E resources.

Obsolete MIB Objects/Tables in Release 3.6.0m2

MIB object/table name
There are no obsolete MIB objects or tables in Release 3.6.0m2.

Changed Tables in Release 3.6.0m2

MIB table name	Description
activeSessionTable	ADDED: activeSessionInitialMethod
arenaAllocatorTable	arenaAllocatorTotalMemory changed from an Integer to Counter64
h323ExternalGatekeepersTable	ADDED: h323ExternalGatekeepersConfigType, h323ExternalGatekeepersGatekeeperType, h323ExternalGatekeepersRaslisten, h323ExternalGatekeepersCallsiglisten
activeH323CallsTable	ADDED: activeH323CallsH225Port, activeH323CallsH245Port
sipAuthorizationDetailsTable	ADDED: sipAuthorizationDetailsOtherErrorCount

Known Problems, Restrictions, and Operational Considerations in 3.6.0m2

Changing a Configured H.323 IP Address

When an IP address has H.323 configured and enabled, if the user changes the ip-address property, then the user must disable and then reenable H.323 in order for the OS-E to recognize the IP address change.

Configuring Gatekeeper Ports on a Single Interface

When configuring an H.323 server, you cannot configure a **gatekeeper-port** of type **client** and a second port of type **peer** using the same port number. The OS-E does not currently enforce this rule. This applies to a single interface only.

Performing Controlled Updates and Activations on Route Servers

Previously, when upgrading, activating, or deleting a backup route server file on the OS-Es within a cluster, there was nothing to ensure route server databases on each OS-E were properly synced.

An action has been created that allows you to manually verify that route servers on each OS-E in a cluster are synced up properly during a route-set update, activating a new route-set, deleting a backup, or cancelling a controlled update or activation.

When this action, **route-server-controlled**, is executed, the master OS-E controls and checks the success of each operation on each of the OS-E slaves. The following are the operations you can execute with this action.

- **route-server-controlled update <file> [activate-time] [peer-wait-seconds]**—Allows you to replace the route-set used by the cluster while ensuring the route server databases on each OS-E are properly synced. You can optionally configure the specific time for this action to be executed, as well as how many seconds the master will wait for a peer to finish each step in the action. The master allows each peer three attempts at a step. The first attempt, the master waits the configured number of seconds. The second try, the master waits twice the configured number of seconds, and the third time three times the number of seconds before the master will halt the entire action.

- **route-server-controlled activation [activate-time] [peer-wait-seconds]**—Activate a new route-set used by the cluster while ensuring the route server databases on each OS-E are properly synced. You can optionally configure the specific time for this action to be executed, as well as how many seconds the master will wait for a peer to finish each step in the action. The master allows each peer three attempts at a step. The first attempt, the master waits the configured number of seconds. The second try, the master waits twice the configured number of seconds, and the third time three times the number of seconds before the master will halt the entire action.
- **route-server-controlled delete-backup <backup-name>**—Delete a backup route-set that the cluster does not use anymore while ensuring the route server databases on each OS-E are properly synced.
- **route-server-controlled cancel [peer-wait-seconds]**—Cancel a controlled update or activation that is currently in progress. You can optionally configure the number of seconds the master will wait for a peer to finish each step in the action. The master allows each peer three attempts at a step. The first attempt, the master waits the configured number of seconds. The second try, the master waits twice the configured number of seconds, and the third time three times the number of seconds before the master will halt the entire action.

When this action, **route-server-controlled**, is executed, the master OS-E controls the update, activation, or deletion, and checks the success of each operation on each of the OS-E slaves. Any error that occurs during the upgrade and activation processes, either on the master or any slave, results in the master initiating a rollback. The entire operation is retried and all failures that occur are logged and traced.

Before executing the **route-server-controlled** action, both NTP and logging must be configured on all OS-Es. This action must always be executed by the master. Any attempt to execute this action on a slave results in the error, “Execute action on master.”

To execute a controlled update, activation, or deletion:

1. Generate and save (in XML format) a route-set file using the LCR import tool and DID mapping. For more information on using the LCR import tool, see the *Net-Net OS-E Session Services Guide*.
2. Using a method such as FTP, upload the route-set file to the master route-server box.
3. Unzip the .xml.gz file on the OS-E.

4. Run the **route-server-controlled** command.

Both the master and slave OS-Es cycle through a set of states during a controlled update. The following table shows the states a master OS-E goes through.

State	Description
Ready	The master is ready to receive a new action request.
Loading	The master is loading.
Peers_Fetching	Waiting for all slaves to get the file from the master.
Peers_Loading	Waiting for all slaves to load.
Peers_Activating	Waiting for all slaves to activate before the master activates itself.
Peers_Cancelling	Cancel the current operation.
Initializing	The master OS-E is initializing its state.
Activate_Scheduled	A controlled activation is scheduled.

The following table shows the states a slave OS-E goes through.

State	Description
Ready	The slave is ready to receive a new action request.
Fetching file	Received route-set .xml file from master.
Loading	Slave is loading.
Activating	Slave is activating.
Cancelling	Master requested a cancel.

To view the progress of a currently executing update, activation, or deletion, use the **show route-server-controlled-action-status** action.

```
Cluster1> show route-server-controlled-action-status

box        master state                    routes     load-set
---        ------ -----                    ------     --------
2          true   Peer_Fetch_InProgress    80993      rsdid_201004131550.xml
3          false  Fetch_Success            0          rsdid_201004131550.xml
4          false  Active                     3
5          false  Fetch_Success            0          rsdid_201004131550.xml
6          false  Fetch_Success            0          rsdid_201004131550.xml
```

Field	Description
box	The OS-E ID.
master	Whether the OS-E is the master.
state	The state of the OS-E. This field captures the information in both the box-state and result.
routes	The number of routes currently loaded.
load-set	The cluster is updating to this route-set.

To view the state of the route-server in the cluster use the **show route-server-box** action:

```
Cluster1> show route-server-box

box         master activated-at              routes     active-set
---         ------ ------------              ------     ----------
2           true   19:13:22 Wed 2010-05-26   3          five.xml
3           false  19:13:31 Wed 2010-05-26   3          five.xml
4           false  19:13:22 Wed 2010-05-26   3          five.xml
5           false  19:13:22 Wed 2010-05-26   3          five.xml
6           false  19:13:21 Wed 2010-05-26   3          five.xml
```

Field	Description
box	The OS-E ID.
master	Whether the OS-E is the master
activated-at	The currently active route-set was activated at this time.
routes	The number of routes in the currently active route-set.
active-set	The route-set file that is currently active.

Syncing a New OS-E With an Existing Cluster

When adding a new OS-E to an existing cluster, you may find that the new OS-E does not update to the active route-set. To ensure all OS-Es in a cluster are in sync perform the following steps.

1. Check the following status providers.

   ```
   show route-server-box
   show route-server-controlled-update
   ```

2. If you find the OS-Es are not all in sync, execute the **route-server-controlled-cancel** command. This works as a reset and syncs the OS-Es in a cluster.

3. Or you can also execute the **route-server-controlled update** command with the route-set you want to activate. Even if that route-set is already active on some OS-Es, it will ensure all of the OS-Es in the cluster are running the same route-set.

Using IWF In a Redundant Cluster

When running IWF traffic in a redundant cluster, the backup OS-E logs irrelevant BYE messages to the call-logs following the termination of a call. These erroneous BYE messages appear only in the call-logs and do not affect functionality.

Release 3.6.0m1

New Features

The following sections describe the new features that have been added to Release 3.6.0m1.

Server Pool Call Admission Control

The OS-E now supports server pool call admission control (CAC). A **server-pool-call-admission-control** object can be configured on any enterprise server that contains a server pool. A CAC object can be configured for each member of a server pool.

This server-level CAC can be enforced as either admission or emission control and you can configure the following statistics:

- Calls in setup
- Concurrent calls
- Used bandwidth

- Call rate

The server pool CAC configuration settings and call stats can be seen via the new status provider **show sip-gateway-cac**. The server pool call statistics are an aggregate of all server pool members below it. If the server pool CAC limits are exceeded, then all pool members are removed from active routes.

```
NNOS-E> show sip-gateway-cac

gateway current-local current-cluster current-max   bw-local    bw-cluster bw-max
-------    ------------- --------------- -----------   --------    ---------- 
SIPpServer 0             0               0             0           0          0
SIPpClient 0             0               0             0           0          0
```

Field	Description
gateway	**The gateway whose statistics you are viewing.**
current-local	**Number of calls connected locally to this gateway, but not mirrored around the cluster.**
current-cluster	**Number of calls connected to this gateway, mirrored around the cluster.**
current-max	**Maximum number of concurrent calls configured on the OS-E.**
bw-local	**Amount of bandwidth in use locally by calls that are not mirrored around the cluster.**
bw-cluster	**Amount of bandwidth in use by calls mirrored around the cluster.**
bw-max	**Maximum bandwidth configured on the OS-E.**

Forked Media Flow Direction Control with NICE systems

In OS-E releases previous to 3.6.0, via the “Forwarding-Based Recording Using SIP” protocol, the NICE equipment identified sessions and which RTP traffic should be replicated, providing the destination for replication for each stream direction (Rx and Tx). The Session Director always used the originator of the call as a reference for deciding which stream is the Rx and which is the Tx.

A configuration property has been created which allows you to indicate which leg is the call center PBX, and thereby control how the Rx and Tx streams of a call are determined so that they match the NICE equipment’s Rx and Tx streams. The property under the **third-party-call-control** object is the **media-forward-direction-reference** and allows you to specify **in-leg** or **out-leg**.

Configuration Backup Enhancement

In releases prior to 3.6.0, the OS-E retained 4 backup configurations in the backup directory. It now retains up to 100.

File-Play-Broadcast Post-Dial Digits

The file-play and file-play-broadcast actions provide unattended outbound dialing services. This feature enhances the file-play and file-play-broadcast actions to allow for post-dialing digits to be sent as DTMF after the initial call is established. Each called party specified in these actions have the option of including a post-dial digit sequence as part of the user information section of the SIP To URL.

The post-dial digit sequence is an optional string that can be included in the user portion of the SIP To URL. When present, the post-dial digit sequence is played after the initial call is established. The post-dial digit string is case insensitive and is represented by the following string:

;postd=xxxx

where xxxx can be one of the following:

- phone digit— 0-9
- DTMF digit— * | # | A | B | C | D
- Pause character— ‘p’ to pause one second
- Visual separator characters (These are used for visual purposes only and are ignored during the playing of the sequence):
  - Period ‘.’
  - Hyphen ‘-’
  - Open parenthesis ‘(‘
  - Closed parenthesis ‘)’

file-play

Purpose

Places a call to the specified SIP URL, plays the .WAV file, and then disconnects the call. This could be a .WAV file you recorded and moved to OS-E, for instance with the **file fetch** action.

Compare this to the **playback** action. The **playback** action plays recorded sessions only (OS-E takes care of mixing the media for playing). This action plays any audio file. For example, if you made a file using the **mix-session** action, you can play it using **file-play**.

Enter the following information:

- filename—The location of the .WAV file you want played.
- to—The SIP URL that specifies where to place the call. Enter the optional post-dial value here (**;postd=xxxx**).
- from—A SIP URL that appears as the caller ID.
- transport—The transport protocol to use, either **any**, **UDP**, **TCP**, or **TLS**.
- requestID—The optional string that represents this call's request Identifier. This is returned in all events from this action.
- actionIdentifier—The optional action ID string that is returned in the accounting record associated with this call.

file-play-broadcast

Purpose

Places a call to multiple specified SIP URIs, plays the .WAV file, and then disconnects the call. This could be a .WAV file you recorded and moved to OS-E, for instance with the **file fetch** action.

Compare this to the **playback** action. The **playback** action plays recorded sessions only (OS-E takes care of mixing the media for playing). This action plays any audio file. For example, if you made a file using the **mix-session** action, you can play it using **file-play-broadcast**.

Enter the following information:

- filename—The location of the .WAV file you want played.
- from—A SIP URI that appears as the caller ID.

- to—The SIP URIs that specify where to place the calls. Enter the optional post-dial value here (**;postd=xxxx**).
- config—(Optional) The **session-config** to use when calling the To SIP URL. For example: "**vsp\session-config-pool\entry <name>"**.

2175 - RADIUS Authorization and Routing

The OS-E now supports RADIUS authorization and routing. When configured, the OS-E sends a request to the RADIUS server, including the to-URL and from-URL. The RADIUS server responds with information the OS-E uses to create session-configs applied to the session.

To configure RADIUS authorization and routing:

1. Enter the **route-server** configuration object.

```
NNOS-E> config master-services route-server
config route-server>
```

2. Enable the **route-server** object and configure the **host-box** and **group**.

```
config route-server> set admin enabled
config route-server> set host-box cluster\box 5
config route-server> set group 0
```

3. Enter the **radius-group** configuration object.

```
NNOS-E> config vsp radius-group rgroup1
config radius-group>
```

4. Enable the **radius-group** object and set the **application** parameter to **routing**.

```
config radius-group> set admin enabled
config radius-group> set application routing
```

5. Enter the **authorization** configuration object.

```
NNOS-E> config vsp default-session-config authorization
config authorization>
```

6. Set the **mode** parameter to **radius <group-name>**.

```
config authorization> set mode radius rgroup1
config authorization>
```

7. Configure the RADIUS server per the server's documentation to accept the request from the OS-E.
8. Save and activate your configuration.

show radius-routing

Purpose

Displays configuration information, status, count, and speed statistics for each RADIUS server configured for routing.

Sample output

```
NNOS-E> show radius-routing

Status for RADIUS group 'Boston' (fail-over):
-------------------------------------------------------------------------------
Server Name      State    Pr | Out  Pending  Requests  Accepts  Rejects Errors
-------------------------------------------------------------------------------
boston           Idle      1 |   0        0         0        0        0       0
127.0.0.1        Idle      1 |   0        0         0        0        0       0
-------------------------------------------------------------------------------
    -
Totals:                      |   0        0         0        0        0       0
```

Properties

Field	Description
Status for RADIUS group...	The name of the group reported on as well as the RADIUS group authentication operational algorithm.
Server Name	The name of IP address that identifies the server that is part of this RADIUS group.

Field	Description
State	The state of the RADIUS server. The following are valid options: • **Idle**—The server is enabled, but has not received traffic. • **Disabled**—The server is disabled in the configuration. • **Healthy**—The server is responding normally to system requests. • **Failing**—The server has not responded to some system requests, but not enough to trigger a fail-over (if configured). • **Failed**—The server has failed to respond to too many requests and the OS-E has determined that it is down. If the RADIUS group is configured with fail-over mode, and a backup server is configured, the OS-E stops sending requests to this server and begins forwarding requests to the next. • **Secret**—There is an error with the shared secret configured for this server.
Pr	The priority of the RADIUS group ranging from 1 (highest priority) to 99 (lowest property).
Out	The number of outstanding requests that the OS-E has sent to the RADIUS server without a response.
Pending	The number of requests that have been generated but have not yet been sent to the server. The server's **window** setting defines the number of allowed requests. Requests generated once that threshold has been reached are considered pending.
Requests	The total number of authentication requests generated.
Accepts	The number of times the RADIUS server has accepted a request, indicating that the user has the correct password.
Rejects	The number of times the RADIUS server has rejected a request, indicating that either the user has an incorrect password or the shared secret isn't right.
Errors	The number of request errors.

radius-authorize

Purpose

Enables, disables, or tests a previously configured server that is part of a RADIUS group configured for authorization. Enter a reference to the configured server (configured with the RADIUS group server object.) Enclose the reference path in quotation marks. The server name is case-sensitive.

When using the test action, you can validate user credentials on the server via the OS-E. When invoked, the OS-E sends a test message to the server to ensure the RADIUS server is configured properly. This action verifies the server and to-url, and optionally the from-url and display-mode. Enter the following:

- **server**—a reference to the configured server and group. Enter this in quotations marks in the format "groupNamePath\server ipAddress."
- **to-url**—the to-url IP address.
- **from-url**—optional; the from-url IP address
- **display-mode**—optional; select either **standard** or **verbose**.

Syntax

```
radius-authorize deactivate <server>
radius-authorize reactivate <server>
radius-authorize test <server> <to-url> [from-url] [display-mode]
```

Example

```
NNOS-E> radius-authorize deactivate "vsp\radius-group boston\server
boston"
NNOS-E> radius-authorize reactivate "vsp\radius-group boston\server
boston"
NNOS-E> radius-authorize test "vsp\radius-group boston\server
boston" sip: 2125551212@voiop.acmepacket.com standard
```

Management System Access

The OS-E has three new permissions regarding what a user can view and edit. The View menu under the Configuration tab lists the permitted views. The following are the permitted views:

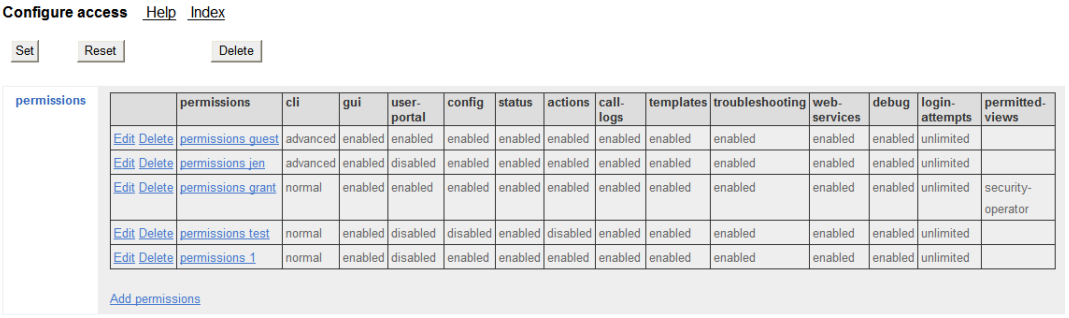
- Security-admin—Users with this permitted view are able to add, modify, and delete the following configuration objects that are security related:

- **interface/op** (all objects)
- **vsp/policies/dos-policy**
- **vsp/tls**
- **filter-intf** can be changed

- Security-operator—Users with this permitted view are able to add, modify, and delete objects under Access/Users. Users are blocked from viewing anything under the Configuration tab.
- Sip-admin—Users with this permitted view are able to add, modify, and delete configuration objects that are not security related. Users with this view are blocked from viewing the Access configuration.

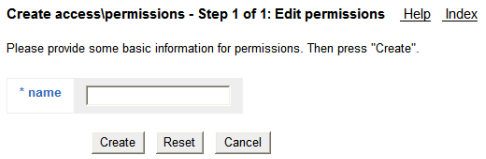
To assign a permission set:

1. Create a new access permission under the Access tab by clicking **Add permissions**.



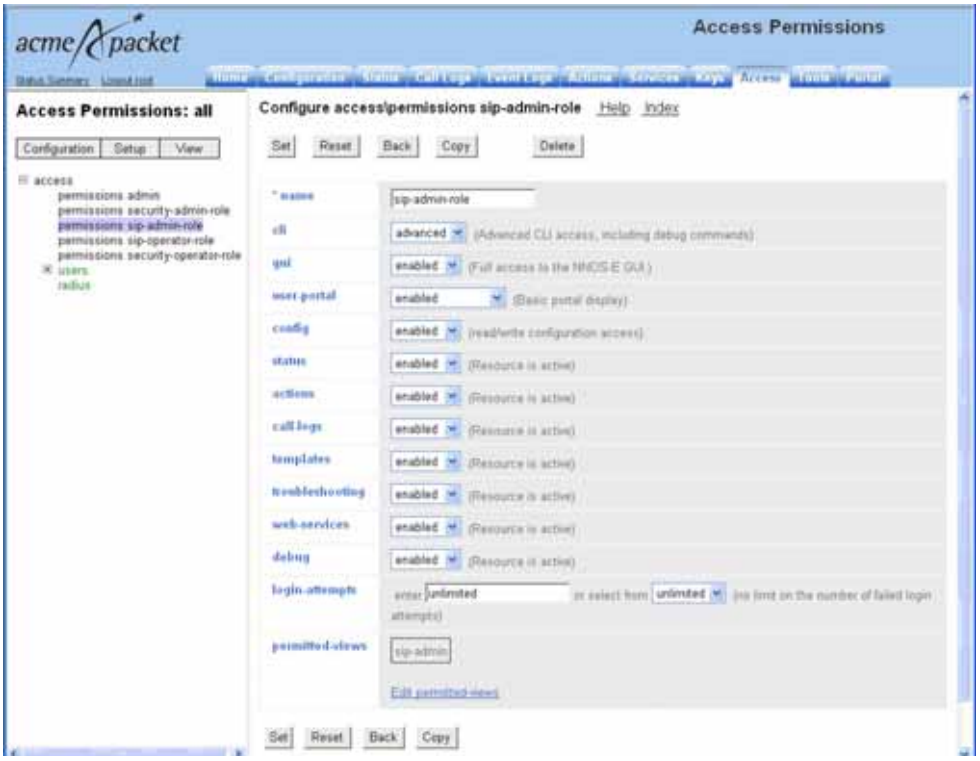
	permissions	cli	gui	user-portal	config	status	actions	call-logs	templates	troubleshooting	web-services	debug	login-attempts	permitted-views
Edit Delete	permissions guest	advanced	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	unlimited	
Edit Delete	permissions jen	advanced	enabled	disabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	unlimited	
Edit Delete	permissions grant	normal	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	unlimited	security-operator
Edit Delete	permissions test	normal	enabled	disabled	disabled	enabled	disabled	enabled	enabled	enabled	enabled	enabled	unlimited	
Edit Delete	permissions 1	normal	enabled	disabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	unlimited	

2. Enter the name you want to use for this access permission and select **Create**.

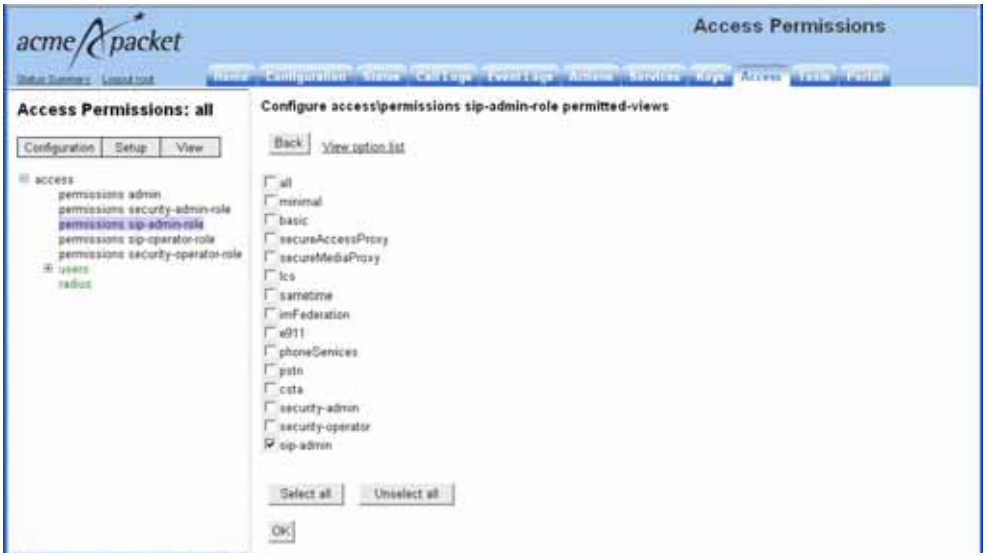


The page listing all permissions appears.

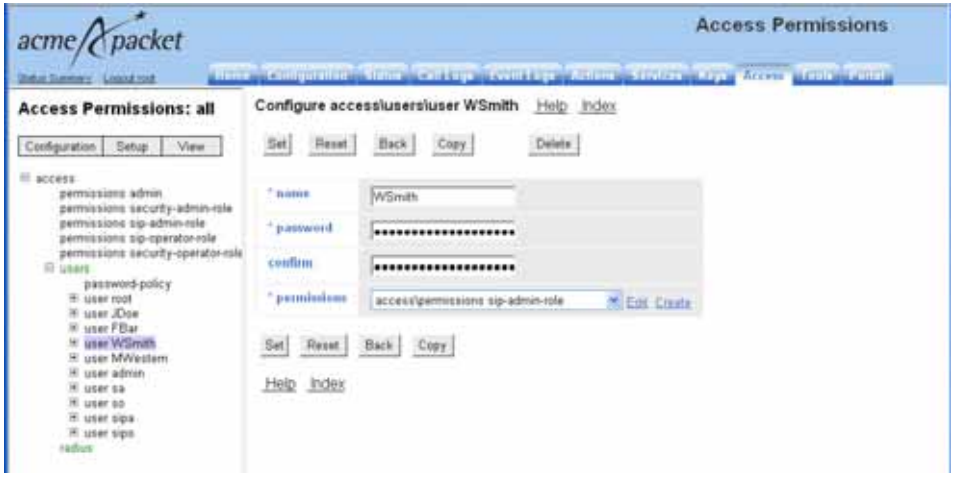
3. The following image shows access permission **sip-admin-role** created with permitted view **security-admin** assigned.



The following image shows available permitted views.



4. Create a new user and assign the access permissions to the user. The following image shows user **WSmith** created with access permission **sip-admin-role** assigned.



5. Save and activate your configuration.

Fixes

The following table summarizes the fixes that have been applied in Release 3.6.0m1:

Component	Description	Problem ID	Found in Release
Transcoding	Codec renegotiation, using **terminate-reinvite-locally** sending wrong codec.	pd7956	3.5.5
DTMF Translation	**dtmf-notify** header incorrect.	pd8310	3.5.4
Pushlet	Incorporate p_xxx properties from original pushlet into eventpush service.	pd8266	3.6.0
NICE	Only one direction of call replicated to NICE.	pd8297	3.5.2
OS	Adjusting hardware clock could change the time significantly.	pd8091	3.5.5
SIP	SIP Crash on OS-E after upgrade to 3.6.0.	pd8418	3.6.0
Kernel	Modify kernel TCP buffer handling under congestion	pd8181	3.5.5
Route Server	“Up to outbound peer,” logic is removed from RS routing.	pd8568	3.6.0
Registration	Calling-Group REGISTERs fail.	pd8452	3.5.5
SIP	No ringback when A calls B (g711) and B refers to C (g729) and C answers with a different codec.	pd10000	3.6.0
3PCC	Fault attempting **call-control** park.	pd8573	3.5.x
Media	200 OK to delayed offer INVITE does not offer all codecs.	pd8502	3.6.0
H.323	RIP to sender of LRQ should use replyAddress.	pd10038	3.6.0m1
SIP	Server unregistered-sender-directive does not work.	pd4717	3.3.8
SIP	Action **call-control** call is timing out.	pd10110	3.6.0m1
Location Services	Best-match location-match-preferred using session from peer sip-gw when routing to registered endpoints.	pd8476	3.5.3
DNS	DNS fails processing for tel URLs.	pd10219	3.6.0m1
SIP	No way to remove SDP from OS-E SIP messages.	pd10097	3.5.5

Component	Description	Problem ID	Found in Release
H.323	The OS-E SIP functionality does not differentiate between g729 and g729A	pd10241	3.6.0m1
SIP	DTMF Notify Content-Length 0; bw-local and bw-cluster counter leaking with server pool CAC.	pd10240/10259	3.6.0m1
H.323	SIP fault while running an H.323/SIP test with logs of DTMF <--> SIP INFO translations	pd10273	3.5.2
Kernel	Kernel fault causing failover.	pd10202	3.5.2
H.323	H.323-H.323 calls using internal tunnel-msg to forward Progress pass incorrect ports to H.323	pd10217	3.6.0m1
GUI	Can't load XML file into web interface configuration	pd10297	3.6.0m1
Accounting	Post-Digit Dialed Numbers provided in file-play-broadcast are missing from CDR.	pd10306	3.6.0m1
SIP	Post-Dial Digit Functionality not working with TEL URL	pd10242	3.6.0m1
SIP	SIP fault when loopback test is run.	pd10469	3.6.0
SIP	Segmentation Fault with Reg-Ex Rule for REFER.	pd10390	3.5.7
ENUM	Third party call control must be enabled for TEL/SIPS translation to work on ENUM.	pd10392	3.6.0
H.323	CUCM SIP to Avaya ACM H.323 one-way voice race condition.	pd10398	3.6.0m1
Dial Plans	Route dial plan matching on From-URI of directory CSV.	pd8349	3.5.3
LCR	Fix for poisoned-buffer access on LCR lookup timeout.	pd10490	3.6.0m1
SIP	600 error when 487 Request Terminated is ACKed.	pd8340	3.6.0
H.323	When H.323 side shuffle is complete, the SDP is copied to the SIP side outbound message.	pd8367	3.6.0
Kernel	Lock references to the kernel rule refcnt causing faults.	pd10596	3.6.0m1

Component	Description	Problem ID	Found in Release
Kernel	Kernel page counts error in the media-drop shared memory.	pd10632	3.6.0m1
SIP	SIP process faults during upgrade.	p-d10474	3.6.0m1
SIP	Unable to modify Request Header before routing.	pd10622	3.6.0m1
Util	Faults after load test during NSN testing.	pd10595	3.5.8
Kernel	Ensure all rule-handles are converted to rules using Krnl_RuleLock().	pd10634	3.6.0m1
Media	Fault during load test.	pd10635	3.6.0m1
H.323	Crash during H.323-H.323 calls	pd10731	3.6.0m1
Cfg Transform	The active-call incorrectly handled during upgrade.	pd10732	3.5.7
DNS	DNS faults during synchronous requests.	pd10039	3.6.0
SIP	Parallel forking faults.	pd10571 pd10572 pd10573	3.5.4
3PCC	The OS-E isn't sending 100 Trying for re-INVITEs when 3PCC is enabled.	pd10845	3.6.0m1
SIP	The OS-E sends ACK for 200 OK responses from port 5060 after sending all subsequent messages from source port 5060.	pd10879	3.6.0
SIP	Multiple entries on outgoing Call-Info header	pd10912	3.6.0m1
Accounting	File-system accounting errors.	pd10952	3.6.0

Configuration Changes in Release 3.6.0m1

The section provides a summary of the additions, changes, and deletions to the OS-E configuration when upgrading to Release 3.6.0m1. It covers new objects and properties, configuration objects and properties that have been renamed, and those objects that have been deleted and are no longer available.

New Objects in Release 3.6.0m1

Object name	Associated properties	Description
vsp/enterprise/servers/ sip-gateway | h323-server | avaya | lcs | mcs | sametime / server-pool/ server-pool-admission-control		Allows you to configure a server-pool CAC on any enterprise server that contains a pool.
	max-bandwidth	Enter the maximum amount of bandwidth, in kbits per second, the OS-E allocates to the AOR. When the system reaches the maximum bandwidth limit for a server, it rejects calls until bandwidth use drops below the maximum. **Example**: set max-bandwidth 10000 Min: 0 / Max: unlimited The default setting is **unlimited**.
	max-number-of-concurrent-calls	Specify the maximum number of active calls allowed for this AOR at one time. When this value is reached, the connection does not accept calls until the value drops below the threshold. **Example**: **set max-number-of-concurrent-calls 5000** Min: 0 / Max: 1000000 The default setting is **1000**.
	max-calls-in-setup	Sets the maximum number of simultaneous call legs in setup stage that are allowed for this AOR. A call leg in setup is much more compute-intensive than established call legs, so this value is more restrictive than the concurrent call leg value. A value of 0 causes the system to decline all calls and registrations. **Example**: **set max-calls-in-setup 5000** Min: 0 / Max: 10000 The default setting is **30**.

Object name	Associated properties	Description
	call-rate-limiting	Limits the number of calls sent to an AOR within a certain interval in seconds. Once this interval is reached, the system rejects any calls to or from this AOR until the rate decreases, returning a response code and message. This feature sets the acceptable arrival rate for incoming calls when used with admission-control and the acceptable set-up rate when used with emission-control. When this feature is enabled, set the number of calls and the measurement interval. You can also enter a result code from 400 to 699 and a text string to accompany call rejection if no available server is found. **Example**: **set call-rate-limiting enabled** The default setting is **disabled**
	admission-control {enabled | disabled}	Specifies whether the system considers AOR limitations when forwarding a call from the AOR. The system tracks the number of concurrent (both incoming and outgoing) active calls for this AOR. **Example**: **set admission-control enabled** The default setting is **disabled**.
	emission-control	Specifies whether the system considers AOR limitations when forwarding a call to this AOR. The system tracks the number of concurrent (both incoming and outgoing) active calls for this AOR. **Example**: **set emission-control enabled** The default setting is **disabled**.
	call-admission-control-error-code	Enter the call admission error code. **Example**: **set call-admission-control-error-code 700** Min: 400 / Max: 999 The default setting is **503**.

Object name	Associated properties	Description
	call-admission-control-error-string	Enter the text string the users sees when a call admission control error occurs. **Example**: **set call-admission-control-string cac error**
	call-emission-control-error-code	Enter the call emission error code. **Example**: **set call-emission-control-error-code 800** Min: 400 / Max: 999 The default setting is **503**.
	call-emission-control-error-string	Enter the text string the user sees when a call emission control error occurs. **Example**: **set call-emission-control-error-string cec error**

Object name	Associated properties	Description
default-session-config > dialog-control-settings		Allows you to configure the OS-E to reject a message sent within a dialog that contains specified release code and text.
	refused-methods	Select the type of message you want the OS-E to reject. The following are valid values: • INVITE • ACK • BYE • REGISTER • REFER • NOTIFY • OTHER • PRACK • CANCEL • SUBSCRIBE • OPTIONS • MESSAGE • INFO • PUBLISH • UPDATE • SERVICE • PING • NONE Specify the release code you want the OS-E to reject. The minimum value is 400 and the maximum value is 499. The default value is 405. Specify the text you want the OS-E to reject. The default setting is Method Not Allowed. **Example**: **set refused-methods invite 450 Method Rejected**

New Properties in Release 3.6.0m1

Object name	Associated properties	Description
permissions	permitted-view	Assign a permitted view you want a user to have. If no permitted-view is specified, the default permitted view is set to **all**. The following are valid permitted views: • all • minimal • basic • secureAccessProxy • secureMediaProxy • lcs • sametime • imFederation • phoneServices • pstn • csta • security-admin • security-operator • sip-admin **Example**: **set permissions security-admin** The default setting is **all**.
server | server-pool {static | dynamic}	server-gatekeeper-id	*Secondary property.* Specifies the way the OS-E reaches an H.323 Gatekeeper. • dynamic—The OS-E learns the Gatekeeper ID via RAS messaging. • static—The GKId string must be configured. The OS-E uses this configured string to contact a remote H.323 Gatekeeper. **Example**: **set server-gatekeeper-id dynamic** The default value is **dynamic**.

Object name	Associated properties	Description
third-party-call-control	media-forward-reference-direction	Identifies which leg of a call is to the call-center PBX, mapping the Rx and Tx streamsx to match the NICE equipment Rx and Tx streams. The following are valid options: • in-leg • out-leg **Example**: **set media-forward-reference-direction in-leg** The default setting is **out-leg**.
	inhibit-100-trying-for-reinvite	When enabled, the OS-E does not send out a 100 Trying when it receives a re-INVITE. When disabled, the OS-E does send out a 100 Trying in response to a re-INVITE. Example: **set inhibit-100-trying-for-reinvite disabled** The default setting is **enabled**.
radius-group	application	Enter the RADIUS application ID for the servers in this group. The following are valid options: • authentication—use SIP authentication • routing—use Acme Packet SIP routing Note that Java accounting ignores this setting and considers all RADIUS servers as candidates for RADIUS accounting. **Example: set application routing** The default setting is **authentication**.
contact-uri-settings-3xx-response	add-maddr [enabled | disabled]	When enabled, the OS-E adds a maddr URI parameter if the original host is a fully qualified domain name (FQDN). **Example: set add maddr enabled** The default setting is **disabled**.

Object name	Associated properties	Description
session-policies	outbound-policy	Apply a session configuration policy to a session as it egresses the OS-E. **Example: set outbound-policy vsp\tls\certificate test**
altered-body	remove-body {true | false}	*Secondary property.* When this property is set to true, the OS-E removes the SIP message body from the matching of SIP messages. This includes the “Content-Type” and other related headers. **Example: set remove-body true** The default setting is **false**.
q931-cause-sip-response map		Allows the configuration of q931-cause and/or h225 reason code for calls cleared by an external SIP UA. When an IW call is cleared on the SIP side, the SIP response code is used to consult an internal table for q931/h225 information needed when generating the ReleaseComplete, Admission Reject, or Location Reject message. By adding a q931-cause-sip-response-map entry, you can override the internal table defaults.
	q931-cause	Select a q931-cause to use when clearing the H.323 side of the call. If this map entry will not generate a q931-cause, or you want to use the default, select **Any**. **Example: set q931-cause userbusy**

Object name	Associated properties	Description
	h2250-reason	Select a h225-reason to use when clearing the H.323 side of the call. The following are valid values: • none—use the default h225-reason. • lrj—select lrj if you are generating LRJ messages and enter a relevant reason. • arj—select arj if you are generating ARJ messages and enter a relevant reason. • any—specifying only the q931-cause in this entry. **Example: set h225-reason arj** The default setting is **none**.
	sip-response	Select the sip-response match criteria for this entry. If this entry will not generate a q931-cause or you want to use the default, select **Any**. **Example: set sip-response 500** Min: 300 / Max: 699 The default setting is **0**.
sip-response-q931-cause-map		Allows the configuration of sip-response code for calls cleared by an external H.323 GW. When a ReleaseComplete, Admission Reject, or Location Reject message is received by the OS-E, the OS-E consults an internal table to determine the appropriate SIP response code to generate when clearing the SIP side of the call. By adding a sip-response-q931-cause-map entry, you can override the internal table defaults.
	sip-response	Define the sip-response that will be used when clearing the SIP side of the call. **Example: set sip-response 350** Min: 300 / Max: 699 The default setting is **0**.

Object name	Associated properties	Description
	q931-cause	Select a q931-cause that helps to qualify the H.323 call-clear. If this map entry does not depend on the q931-cause value, either because there is no Q.931 present or because any Q.931 cause qualifies, choose **Any**. Example: **set q931-cause noresponse**
	h2250-reason	Select a h2250-reason type. The following are valid values: • LRJ—match an incoming LRJ message. • ARJ—match an incoming ARJ message. • H.225—match all other relevant traffic • none—H.225 reason should not be used as match criteria for this entry. **Example: set h225-reason lrj** The default setting is **none**.
third-party-call-control	transfer-file	Enter the media file you want played while an unattended call transfer is taking place. **Example: set transfer-file ring1** There is no default setting.

Deleted Objects in Release 3.6.0m1

Object name	Property name
vsp > enterprise > servers	**call-hunting-type**

Deleted Properties in Release 3.6.0m1

Object name
vsp > surveillance

Moved Properties in Release 3.6.0m1

Property name	Former location	New location
ras-settings	cluster/box/number/interface/ip/h323	**session-config\ dns-client-settings\ routing-last-resort-dn**s

Changed Properties in Release 3.6.0m1

Property	Change
sip-settings > persistent-destination-address	Default is now **true**.

Renamed Objects in Release 3.6.0m1

Old name	New name
private-ip-gateway\group	**private-group**
vrrp	**vrrp-advertisements**
cluster-server-load	**server-load-db**
least-cost-routing	**route-server**
3pcc	**jtapi**

Renamed Properties in Release 3.6.0m1

Old name	New name
private-ip-gateway\selfConnected	**self-connected**
term-transc-on-bye	**terminate-transaction-on-bye**
cxc-call-policy	**nnos-call-policy**
apply-policy-to-cxc-calls	**apply-policy-to-nnos-calls**
add-cxc-domain	**add-nnos-domain**
use-cxc-domain-in-search	**use-nnos-domain-in-search**
cxc-tunnel-creation	**nnos-tunnel-creation**
lcr-lookup-timeout	**route-server-lookup-timeout**

Old name	New name
lcr-lookup-max-pending	**route-server-lookup-max-pending**
cms-preferences	**gui-preferences**
cms	**gui**

MIB Changes in Release 3.6.0m1

This section covers changes that have been applied to Management Information Base (MIB) object definitions.

New MIB Tables in Release 3.6.0m1

MIB table name	Description
sipGatewayCacTable	SIP Gateway Calling Group Call Admission Control Statistics
callingGroupCacRejectsTable	SIP Calling Group Call Admission Control Reject Statistics”
locationCacheCacRejectsTable	Net-Net OS-E Location Call Admission Control Reject Statistics”
locationCacheCacRejectsInboundTable	Net-Net OS-E Location Call Admission Control Inbound Reject Statistics”
locationCacheCacRejectsOutboundTable	Net-Net OS-E Location Call Admission Control Outbound Reject Statistics”
radiusRoutingTable	RADIUS status for Routing peers”
sipServerCacRejectsTable	SIP Server Call Admission Control Reject Statistics
switchCacRejectsTable	SIP Voice Gateway Call Admission Control Reject Statistics”
trunkCacRejectsTable	SIP TrunkGroup Call Admission Control Reject Statistics”

New MIB Objects in Release 3.6.0m1

MIB object/table name
arenaCacheOutstandingCurrentActive
arenaCacheOutstandingMostActive
arenaCacheOutstandingTotalFailures
arenaCacheOutstandingMaxFailures

Obsolete MIB Objects/Tables in Release 3.6.0m1

MIB object/table name
installInfoTable
InstallInfoProvidesTable
installingInfoRequirementsTable
arenaCacheUsageByAllocatorOtherCount

Changed Tables in Release 3.6.0m1

MIB table name	Description
callAdmissionControlTable	ADDED: callAdmissionControlRejectsInSetup, callAdmissionControlRejectsMaxCalls
servicesRouteDatabaseTable	Index changed
sipServerAvailabilityTable	ADDED: sipServerAvailabilityReason
activeCallsTable	ADDED: activeCallsPostDialDigits
sipGatewayCacTable	ADDED: sipGatewayCacCallRateLimitingState, sipGatewayCacCallRateLimitingRate, sipGatewayCacCallRateLimitingInterval
arenaCacheByAllocatorTable	ADDED: arenaCacheByAllocatorCurrentActive, arenaCacheByAllocatorMostActive, arenaCacheByAllocatorTotalFailures, arenaCacheByAllocatorMaxFailures
arenaCacheUsageOutstandingTable	OBSOLETED: arenaCacheUsageOutstandingOtherCount

Known Problems, Restrictions, and Operational Considerations in 3.6.0m1

Configuring Forking-Settings

When configuring **forking-settings** under **session-configs**, you must enter a value for the **outbound-arbiter-rule** parameter or the **forking-type** parameter is not applied to the session.

Release 3.6

New Features and Major Product Changes

This section provides a description of the major features and changes applied with Release 3.6. Refer to the section, “Configuration Changes in Release 3.6,” for detailed information on new configuration objects and properties.

H.323 Gateway Registration

The OS-E uses primary, backup, and alternate gatekeepers to route H.323 traffic. When the primary gatekeeper becomes inaccessible, you can configure the OS-E to automatically switch to either a backup gatekeeper or an alternate gatekeeper. The primary difference is that backup gatekeepers are configured statically, while alternate gatekeepers are configured dynamically.

The OS-E also provides support for an administrator to configure multiple remote H.323 gateways co-located on the same external IP address. The differentiating characteristic is their TCP port number. Each configured co-located gateway must be provisioned to initiate connections to a unique OS-E TCP port.

The OS-E provides the capability for the administrator to map Q.931 cause codes and/or H225 reasons to and from specific SIP response codes.

Configuring Secondary Properties

In order to simplify the presentation of configuration objects to those that are the most commonly used, the following properties listed below are now secondary properties. In order to set these properties via the GUI, you must click on the **Show advanced** button at the top of the screen. To set them in the CLI you need to explicitly set or configure them. They do not show up in the help or command completion.

Object name	Advanced property
servers	• federations • avaya • sip-host • lcs • mcs • sip-connection • sametime • dns-group
enterprise	• user-group-policy • unknown-server-policy
server	• local-ip • local-port • connection-retry-interval
network	• tcp-keepalive-time • tcp-keepalive-probes • tcp-keepalive-interval
carriers	• carrier • qos • currency • country • timeplan • hunt-group

Object name	Advanced property
settings	• accounting-anonymous-match • clear-binding-on-connection-broken • connection-timeout • database-write • filter-mcs-authint-to-auth • filter-mcs-force-IM-decrypt • filter-mcs-independent-header-schemes • filter-mcs-rewrite-ping-contact-hdr • filter-mcs-site-failover-threshold • filter-mcs-suppress-100rel • filter-lcs-input-remove-user-params • filter-lcs-input-remove-record-route-hdrs • ignore-contact-on-ack • location-cache-write-thru • resolve-routing-through-server-domain • max-udp-outbound-log • prune-associations • pruning-interval • read-header-max • read-line-max • read-message-max • cxc-tunnel-creation • socket-receive-buffer-size • sockets-idle-max • sockets-idle-min • sockets-initial-message-timeout • sockets-per-box-max • sockets-per-peer-max • stack-message-queue-max • stack-message-queue-min • stack-message-queue-reg-clip-threshold • supported-extensions • tunnel-policy • udp-tunnel-reclaim • udp-tunnel-reclaim-scan-interval • backup-server • register-retransmit-detection • remote-party-id-accounting • apply-to-methods

Object name	Advanced property
vsp	• local-identity • local-normalization • server-normalization • de-normalization • external-inbound-normalization • displayname-character-set-info • registration-proxy • pstn-gateway • pre-session-config • sip-timers • virtual-threads • virtual-dial-plan-pool • monitor-group • im-filtering • from-interface-group • to-interface-group • phones • presence-database • detect • oci-settings • external-policy-group • external-location-group • external-event-group • surveillance • gateway-routing • dtmf-generation • sip-manipulation-pool

The following properties listed below have been changed from secondary properties to basic.

Object name	Required property
settings	• local-directory-based-user-services

DID Support

In release 3.6, direct inward dial (DID) mapping is supported via the OS-E Route Server Application, also known as the Route-Server client-server application. Under the route-server DID tab, you have the ability to import, generate, restore, backup, view, edit, delete, and purge DID mappings.

For complete information regarding DID support, refer to chapter 12 of the *Session Session Services Configuration Guide*.

Speaker Detection

Speaker detection functionality was introduced in release 3.6. When this feature is enabled and a call connects, the OS-E monitors the audio to determine whether an answering machine or person are on the other end, or if the answering party is a modem or a fax machine. If the OS-E detects the constant power training tone of a modem or fax machine, the call is disconnected.

Accounting Enhancements

Several accounting enhancements have been added to release 3.6:

- The **accounting flush** action has been modified. One of two things can happen when this action is executed. A target whose send has previously failed and is waiting for a retry interval to try again, will send again immediately. Also if there is a target writing to an output file, the OS-E performs a rollover on the file, regardless of whether or not the condition to rollover has been reached yet. The results of this operation are logged and you can view the logs to obtain more information about files that have been flushed.
- You can create an **external-file-system** configuration which allows you to write accounting records to an outside server.
- The **file-system** configuration object, which allows you to write accounting records locally, has been enhanced. You can now format the output to **postgresql**.
- The **file-play** action has been enhanced so that you can configure the accounting CDRs to report more specific information pertinent to call control applications including: whether or not a call was connected successfully, disconnect reasons for specified calls, final response codes for specified calls, and scan times, play times, and file times for specified file-play actions.

IP Discard Packet Logging

You can now configure the OS-E to account for all discarded packets that do not hit an existing pinhole. You can also generate log messages when such packets are discarded and record more complete information about a selection of these packets. This feature is configured via a new **packet-discard** object.

Re-Invite Handling Modification

As of release 3.6, you have the option to change the way the OS-E handles re-INVITEs via a new parameter, **terminate-hold-retrieve-locally**, under the **third-party-call-control** object. When this property is enabled and a re-INVITE is received with an SDP that indicates it is either a hold or retrieve request, the OS-E accepts the re-INVITE locally with the SDP acknowledging the hold or retrieve and the message is not forwarded.

Codec Handling Enhancements

The OS-E now supports a preferred codec feature. This allows you to define the preferred codec as deduced from SDP offers and answers, adapt to match received codecs, and rewrite rfc-2833 headers when encoding audio. A new configuration object, **transcoding-policy**, has been created to configure this feature.

Media Auto-Anchoring

In releases prior to 3.6, you could enable the OS-E to auto-anchor media. When the OS-E has auto-anchoring enabled, it uses certain algorithms to determine anchoring necessity based on a variety of criteria, including whether you have configured smart anchoring via the **autonomous-ip** object and whether the calling devices are behind a firewall.

A new configuration property, **attributeless-auto-anchor**, under the **media** object, has been created. When this property is enabled, the OS-E attempts to auto-anchor streams without additional OS-E attributes in the SDP.

Xen Support

The OS-E can now be downloaded as a Xen virtual machine. For detailed information on how to install the OS-E software on a Xen server, see chapter one of the *Virtual Machine Information Guide*.

USB Support

As of release 3.6, the OS-E supports USB sticks with up to 4 GB of storage to handle the OS-E commissioning.

Acme Packet Naming Conventions

For existing customers who are upgrading from a prior release, the Covergence file names have been renamed under Acme Packet, Inc., as follows:

- Supertar upgrade file: now nnSE360.tar.gz
- USB file: now nnSE360-usb.img.gz
- ISO: now nnSE360.iso
- Archive Viewer: now nnSE360-av.zip
- Troubleshooter: now nnSE360-tshoot.zip
- SDK: now nnSE360-sdk.zip
- .NET SDK: now nnSE360-sdk-dotnet.zip
- JBOSS SDK: now nnSE360-jboss-sdk.zip
- Route Server Import: nnSE360-rsimport.zip
- WSDL tools: nnSE360-wstools.zip

Eventpush-Service Configuration

The **ip > eventpush-service** allows you to configure and redirect logged events to external computer Web browsers. The eventpush-service requires the **external-services > event-group** to declare the destination service URL of the external device.

Perform the following steps to enable and configure the eventpush-service:

1. Configure the **ip > eventpush-service**.

```
NNOS-E> config box
config box> config interface eth3
config interface eth3> config eventpush-service
config eventpush-service> set admin enabled
config eventpush-service> set protocol http 8081
config eventpush-service> set page-domain acmepacket.com
```

2. Edit the target Web application to include an IFrame. The IFrame is comprised of the name of the OS-E device running the eventpush-service application, the web services port, and the string /cometapp/acmepacket.html.

For example, if the name of the OS-E device running the eventpush-service is xyz.com with the service running on port 8081, and if the system is running over HTTP, then the reference is `http://xyz.com:8081/cometapp/acmepacket.html`.

3. Configure the external-service > event-group > event-service service-url property so that events are passed to the destination eventpush service. Enter the destination domain IP, the eventpush-service port, and the string /cometapp/ callouts. For example, `http://127.0.0.1:8081/cometapp/callouts`.

```
NNOS-E> config external-services
config external-services> config event-group a
config event-group a> config event-service cometd
Creating 'event-service cometd'
config event-service cometd> set service-url http://172.0.0.1:8081/
    cometapp/callouts
```

4. Configure vsp to forward events to event-group.

```
NNOS-E> config vsp
config vsp> set external-event-group external-services\event-group a
```

5. Save the configuration.

To change the reporting mechanism from the pushlet-app configuration to the eventpush-service configuration:

1. Configure the eventpush-service object as described in Step 1.
2. Remove the pushlet-app setting from the **box > interface > ip > web-service** application property.
3. Change the service-url property of the external-service > event-group > event-service object, removing the pushlet event service and replacing it with the eventpushservice.

   To do so, enter the eventpush port, and change the context portion of the URL from “pushletapp” to cometapp.”

Fixes

The following table summarizes the fixes that have been applied in Release 3.6.

Component	Description	Problem ID	Found in Release
Policy	SIP faults observed during an OCS/ATT transfer test case.	14421	3.4.4
SIP	OS-E sends 100 trying to the port specified in the VIA header rather than the source port.	14470	3.3.7
Policy	Enhance regex header functionality to be able to specify where the expression is applied.	14511	3.5.1
Management	Problems with sampling active calls.	14219	3.4.4
Media	Calls were improperly terminated after a 180 Ringing message is received.	14567	3.4.4
Location Services	NN260 not sending SIP-directive “refuse” messages.	14340	3.4.4
ENUM	INVITE not generated after ENUM query; ENUM lookup transforming SIP URI incorrectly.	14726, 14684	3.5.1
Manager	Fix fault related to a scheduled action.	14546	3.4.2
OS (upgrade)	After upgrading from 3.3.6 to 3.5.1, eth0 and eth2 interchanged on IBM 3250.	14758	3.5.1
LCR Import	Add to-URL-match and from-URL-match properties to purge a particular LCR route table entry.	14931	3.4.4
Kernel	In-leg and out-leg TOS does not work with TCP.	14072	3.5.0
Servers	Add support for multiple servers with the same IP address but different ports to be configured as h323-server objects.	14767	3.5.1
Pushlet	Web-service leaving connections in a close-wait state.	9346	3.3.0
TCP	OS-E not opening TCP connection to Tomcat server.	14940	3.4.3
H.323	Control IE element in H.225 setup message.	15014	3.5.1
Transcoding	Preferred codec not always being enforced.	15032	3.5.1

Component	Description	Problem ID	Found in Release
OS	OS drive suddenly went to read-only.	15125	3.5.0
Media Auto Anchor	Auto anchor functionality not working appropriately.	14060	3.5.1
Call Control	Wrong reason code display in session call logs.	13067	3.5.0
Media	Sequence number reset in the same SSRC causes mixer to wait until one leg of the call completed before continuing to play out.	15147	3.4.4
Media	OS-E anchors call after on-hold.	11989	3.2.8
SIP	Issues with the way the OS-E is handling NAT on the sametime interface.	14069	3.3.8
Transcoding	Fax failing when transcoding is invoked.	14850	3.5.1
Kernel	Kernel issue processing packets that arrive out of order.	15310	3.5.0
Dial Plans	When first server of the hunt-group is disabled, the OS-E does not try the entire group.	14887	3.5.1
SIP	Add support for a new parameter from WSDL file-play/file-play-broadcast actions to be added to CDR records.	15352	3.5.1
Servers	Enhance the ability to handle duplicate IPs for servers.	11613, 11922	3.4.4
Kernel	Fix kernel memory leak.	15304	3.5.1
Media	Enhanced support for proprietary secure call indication procedures.	14599	3.5.0
LCR Import	A blank “from” field in an imported CSV file causes an error in the LCRimport application.	15430	3.5.1
Registration	Support forwarding a request to another OS-E when the binding was registered on another box of the cluster.	15559	3.5.1
GUI	GUI doesn’t properly handle the “monitor” configuration property and causes a fault.	15588	3.6.0
OS	The USB Installer fails on a RAID system without 6 drives.	15607	3.5.1
Location Services	Memory corruption issue in the location services code.	15593	3.5.0

Component	Description	Problem ID	Found in Release
Config Audit	Enhance logging to indicate configuration property changes.	15620	3.5.1
Location Services	Location-summary, total-bindings, and total-aged not being incremented properly.	15348	3.5.0
Kernel	OS-E not relaying RTP packets in hairpin scenario.	15641	3.5.2
Servers	SIP deadlock causing fault.	15672	3.4.4
Accounting	Enhance the disconnect cause field in the CDR to provide more information on the reason for the disconnect.	15725	3.6.0
SIP	New accounting features added.	15756	
SIP	Add source and destination information labels in the GUI ladder diagrams.	14572	3.5.1
H.323	OS-E sending an incorrect Call Reference Value in Setup message.	15701	
SNMP	OS-E not handling getnext properly.	15761	3.4.4
MX	Archiving to FTP server fails after a few calls.	15734	3.5.2
Accounting	Response code should be in CDR.	15812	3.6.0
Location Services	Contact header in the 200 OK to a SUBSCRIBE isn't modified by the OS-E.	15661	3.4.4
Dial Plans	When all servers in the hunt-group are down, the **show call-routing** status displays them as "up."	15558	3.5.1
Location Services	There is no cap on the amount of bindings the OS-E can register.	15550	
SIP	Added configuration property to control addition of "received=" parameters.	15647	3.5.1
Database	Database failure causing system to be unresponsive.	7455, 15412	3.2.1 / 3.5.1
Registration	When **unregister-aged-bindings**=**client-side**, too many sessions created.	15904	3.5.0
Accounting	The accounting-data entry fields no longer require the tag field to be specified.	15815	3.6.0

Component	Description	Problem ID	Found in Release
SIP	Unable to alter the Allow header with the reg-ex-header settings object.	13844	3.5.0
GUI	Call Logs tab in the GUI faulted if a configuration property was missing.	15941	
Transcoding	Fix transcoding issue where most-preferred codec was not honored.	15032	3.6.0
Media	INVITE wrongly rejected when it is excluding the most-preferred codec.	15970	3.6.0
SIP	OS-E incorrectly resetting the remote address of the INVITE transaction.	15974	3.6.0
Configuration	**Session-config > sip-settings > persistent-destination-address** needs to default to false.	16042	3.5.2
Accounting	CDR archive push support for one minute intervals.	16083	3.5.4
H.323	If H.323 call has no calling party, SIP-IWF functioning fails.	16126	3.5.2
CAC	Call admission not allowing configured number of calls.	16139	3.5.5
Manager	Unable to mount NFS drive on release 3.5.3.	16188	3.5.3
SIP	OS-E can't forward received INVITE due to internal parser errors.	16178	
Call Logs	The "Result" value in the call logs is inaccurate.	15793	3.6.0
SIP	In 3PCC, OS-E unable to apply Inbound or Outbound session configurations.	16183	3.5.5
Media	Incorrect jitter statistics displayed.	16021	3.5.2
Media	OS-E terminates call due to inactivity timer even after it has released itself from media path.	16112	3.5.2
Kernel	Ensure that auto-anchored calls that are released are not terminated due to the inactivity timer.	15828	3.5.2
Media	After a failover a hold is not detected.	16292, 16234	3.6.0

Component	Description	Problem ID	Found in Release
SNMP	SNMP standard MIB-2 returns nonexisting interface indexes for VRRP IPs.	16202	3.5.5
SIP	Delayed to Early Offer doesn't respond to a 491.	16322, 16374	3.5.1

Configuration Changes in Release 3.6

The section provides a summary of the additions, changes, and deletions to the OS-E configuration when upgrading to Release 3.6. It covers new objects and properties, configuration objects and properties that have been renamed, and those objects that have been deleted and are no longer available.

New Objects in Release 3.6.0

Object name	Associated properties	Description
altered-body		This configuration object allows you to alter the body of any SIP message for a matching session. You should only change the SIP message body under specific, required circumstances.
	admin [enabled | disabled]	When enabled, you can alter the body of any SIP message for a matching session. The default setting is enabled.
	altered-body	Alters the body of any SIP message for a matching session.
	apply-to-methods	Specifies the message type to which the system applies message body changes. The system then changes the specified URI according to the settings of the header and destination properties of this object. When you modify this value, the system overwrites the current setting with only the message types you specify. To enter multiple types, enter them separated by a plus sign (+) with no spaces. The default setting is INVITE.

Object name	Associated properties	Description
	apply-to-responses	Specifies whether to apply message body changes to just SIP requests, or to both requests and responses. If you enter a value of yes, you must include the response-code. The default setting is yes.
altered-header		This configuration object allows you to modify or create header values in calls matching this session configuration. You can create multiple header-altering configurations.
	admin [enabled | disabled]	When enabled, you can alter header values in calls matching this session configuration. The default setting is enabled.
	source-header	Specifies the URI from which the OS-E initially derives the data that is to be written to the destination header.
	source-field	Specifies the portion of the URI that the system writes to the destination. Possible values are: user, host, selection, and value.
	destination	Specifies the header to be created or modified by the properties set in this object. The URI specified in this property is modified with the data from the source-field property. If the header doesn't exist in the message, the OS-E creates it. The following are valid values: to, from, request. The default setting is from.
	destination-field	Specifies the field in the destination URI to overwrite. The following are valid values: user, host, display, full. There is no default setting.
available-memory		This object allows you to enable a sampling interval for the OS-E to check the available memory.
	admin [enabled | disabled]	Enable or disable the OS-E checking the available memory. The default setting is enabled.
	interval	Defines how often the OS-E pools the status provider for data. The minimum value is 30 and the maximum value is 1036800. The default setting is 1:00:00 (1 hour).

Object name	Associated properties	Description
codec-payload-type-bindings		The codec-payload-type-bindings configures a binding between a codec name and a payload type. Without any codec-payload-type-bindings configured, the OS-E uses a default DTMF payload type of 101. This configuration element is set when you want to change the default DTMF payload type offered by the OS-E. This property takes precedence over the default of 101. Codec-payload-type-bindings is used when the OS-E generates its own SDP for outgoing calls. The OS-E generates its own SDP for features like file-play or when the OS-E is in a Delayed-Offer/Early-Offer network.
	binding	Bind a codec name to a particular payload type. The syntax for this parameter is: codec-payload-type-bindings <codec> <payload-type>. Payload type can range from 0-127.
external-file-system		Configures the external file system, allowing you to write accounting records to an outside server.
	admin [enabled | disabled]	When enabled, the OS-E forwards accounting and SIP call detail records to the target file path. The default setting is enabled.
	format	The output format of the file you are creating. The available file formats are: csv, proprietary, tab, and postgresql. The default setting is csv.
	url	Enter the URL of the external target to which you are sending CDRs.
	cdr-processing	Specify how the CDRs are collected. The following are available processes: batch (Min: 0 / Max: 4294967295; default 20000), roll-over (never, hourly, daily, per-minute; default hourly), and interval (Min: 60 seconds, Max: 1036800 seconds; default 0).

Object name	Associated properties	Description
h225-settings		This configuration object allows you to configure H.225 support on the OS-E.
	fast-start [enabled | disabled]	When enabled, the OS-E accepts inbound H.323 fast start calls and includes fast start in SETUP messages for outbound H.323 calls. The calls fall back to slow if fast start is unsuccessful. The default setting is enabled.
	manual-ringback [enabled | disabled]	If enabled, the OS-E prohibits remote ringback. When this property is disabled, SIP to H.323 calls attempt to open an audio channel for remote ringback. The default setting is enabled.
	use-inbound-call-settings [enabled | disabled]	When enabled for an H.323 to H.323 call, the OS-E uses inbound H.323 call settings for H.323 outbound calls. The default setting is disabled.
	fwd-progress-as-alerting [enabled | disabled]	When enabled, the OS-E sends an Alerting message instead of a Progress message. The default setting is disabled.
	default-terminal-type	Identifies the OS-E terminal type. This is used for MSD. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 60.
	multiple-calls [enabled | disabled]	When enabled, the OS-E allows calls to share an H.225 connection. The default setting is disabled.
	maintain-connection [enabled | disabled]	When enabled, the OS-E keeps an H.225 connection open after calls are cleared. The default setting is disabled.
	conn-idle-timeout	Specifies the maximum lifetime in seconds of an idle H.225 connection. A value of 0 indicates an idle connection should never timeout. The minimum configuration value is 300 and the maximum is 65535. The default setting is 3600.

Object name	Associated properties	Description
	h323-user-alias	Specifies the source and destination address type in Setup, Alerting, Connect, ARQ, and LRQ messages. The following are valid h323-user-alias values: none, dialedDigits, h323ID, urlID, emailID. The default setting is none.
	call-alerting-timeout	The maximum number in seconds the OS-E waits for Alerting message after sending a SETUP. The call clears if this timeout is reached. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 4.
	call-establishment-timeout	The maximum number in seconds the OS-E waits for an H.323 call to be established. The call clears if this timeout is reached. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 60.
	end-session-timeout	The maximum number of seconds the OS-E waits after sending a ReleaseComplete before call resources are reclaimed. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 15.
	h245-establish-timeout	The maximum time, in seconds, the OS-E waits for an H245 connection to be established. The call clears if this timeout is reached. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 1.
	reinvite-type	*Secondary property.* Indicates if the OS-E should use Terminal Capability Set or Extended Fast Connect messages to reconfigure media channels. The default setting is emptyTermCapSet.
	use-progress-inband [enabled | disabled]	When enabled, inband ring information from the inbound H.323 call-leg is propagated to the outbound call-leg. The default setting is enabled.

Object name	Associated properties	Description
	fwd-retrieve-no-tx [true | false]	When true, the OS-E does not pause remotetransmitted if media information is 0.0.0.0. The default setting is true.
	use-server-connection [true | false]	*Secondary property.* specifies whether the OS-E creates a new, or uses an existing, TCP connection. If true, the OS-E uses a TCP connection created by the remote gateway instead of creating a new outbound TCP connection. Use this property for a remote H.323 gateway using connection sharing for its H.225 traffic. (It uses a single TCP connection for multiple calls.) The default setting is true.
	enum-lookup-called-party [enabled | disabled]	When enabled, the OS-E performs an ENUM lookup of the called number before making an outbound H.323 call. The default setting is disabled.
	enum-domain	The domain used for ENUM lookups. The default setting is e164.arpa.
h245-settings		The H.245 settings configuration object allows you to configure H.245 on the OS-E.
	h245-tunnel [enabled | disabled]	When enabled, the OS-E attempts to use an H.225.0 connection for H.245 traffic. The use of H.245 tunneling depends on indication from both H.323 terminals and gateways. The default setting is enabled.
	early-h245	The OS-E does not support early H.245. Set this property to indicate how to handle a request for early H.245. The following are valid early-h245 values: • notunnel—The OS-E ignores the early H.245 and completes the call setup using slowstart. • reject—The OS-E rejects the call. The default setting is notunnel.

Object name	Associated properties	Description
	wait-for-remote-tcs [true | false]	When true, the OS-E waits to receive a Terminal Capability Set message before advertising its capabilities. When false, the OS-E issues a TCS message after a slowstart call is connected. The default setting is true.
	clc-when-pausing-remote [true | false]	*Secondary property.* When true, the OS-E closes its TX channels when pausing the remote H.323 terminal. The default setting is false.
	send-msd-when-unpausing-remote [true | false]	*Secondary property.* Specifies whether the OS-E will conduct master-slave determination (MSD) when using TCS to unpause a remote H.323 gateway. The default setting is false.
	use-h450-hold-retrieve [enabled | disabled]	When enabled, the OS-E uses H.450 supplemental service PDUs for holds and retrieves. The default setting is enabled.
	sip-h323-dtmf-translate	Sets preferences for H.323-SIP DTMF interworking for a particular H.323 trunk. The default setting is inband.
	codec-selection	*Secondary property.* Indicates how the OS-E chooses converged codecs. The following are valid values: • none—No codec is being used. • local—Use the highest preference common codec seen in SIP SDP. • remote—Use the highest preference common codec in remote TCS. • followMSD—Use the result of master-slave determination to decide. The default setting is remote.
	map-ptime-to-fpp [true | false]	*Secondary property.* When set to **true**, the OS-E uses SDP ptime parameter to set max-frames-per-packet codec value in Terminal Capability Set. Ptime and FPP are not equivalent, however, this allows compatibility in some interworking scenarios. The default setting is false.

Object name	Associated properties	Description
	map-fpp-to-ptime [true | false]	*Secondary property.* When true, the OS-E uses max-frames-per-packet codec value in Terminal Capability Set to set SDP ptime parameter. Ptime and FPP are not equivalent, however, this allows compatibility in some interworking scenarios. The default setting is false.
	add-equivalent-codecs [true | false]	*Secondary property.* When true, the OS-E adds equivalent codecs to Terminal Capability Set. The currently supported case is G729 present in SDP which would add both G729 and G729A in TCS. The default setting is false.
h323-service-routing		Configures the H.323 service routing metrics.
	metric1	Sets the metric1 load type. The following are valid values: • none • user-metric • intf-thruput The default setting is user-metric.
	metric2	Sets the metric2 load type. The following are valid values: • none • user-metric • intf-thruput The default setting is none.
	metric3	Sets the metric3 load type. The following are valid values: • none • user-metric • intf-thruput The default setting is none.
	metric4	Sets the metric4 load type. The following are valid values: • none • user-metric • intf-thruput The default setting is none.

Object name	Associated properties	Description
	metric5	Sets the metric5 load type. The following are valid values: • none • user-metric • intf-thruput The default setting is none.
header-normalization		This object alters the user portion of the specified header.
	admin [enabled | disabled	Enable or disable header normalization on the OS-E. The default setting is enabled.
	destination	Specifies the header to be created or modified by the properties in this object. That is, the OS-E modifies this URI with the data from the source.
	value	Specifies the field in the specified destination URI to overwrite. The following are valid values: • none—No normalization applied • prepend—Prepend string • prepend-to—Prepend string to certain length • strip-off—Strip off N characters • strip-off-to—Strip off prefix to certain length • replace-prefix—Replace prefix with a different prefix • replace-with—Replace with a different name • append—Append extension number The default setting is none.
	apply-to-methods	Specifies the message type to which the system applies header value changes. The OS-E then changes the specified URI according to the settings of the header and destination properties of this object. When you modify this value, the OS-E overwrites the current settings with only the message types you specify. Enter multiple types separated by a plus sign (+) with no spaces. The default setting is INVITE.

Object name	Associated properties	Description
	apply-to-responses	Specifies whether to apply header value changes to SIP requests or requests and responses. If you enter a value of **yes**, you must include the response-code. The following are valid values: • no—Do not apply to responses (requests only) • yes—Apply to responses of this type The default setting is no.
	session-persistent [enabled | disabled]	Specifies to which messages in a session the OS-E should apply changes made with this object. When enabled, the OS-E applies any TO, FROM, or REQUEST URI changes to the first and all subsequent messages in a session. When disabled, the system applies the changes only to the first message in the session. The default setting is disabled.
inbound-header-settings		This configuration object allows you to set fields to remove and/or replace header settings in the SIP headers for inbound traffic.
	pAssert-mode [enabled | disabled]	*Secondary property.* Sets whether or not to strip the number in the P-Asserted-Identity field from the SIP header. When enabled, the OS-E replaces the value in the From field with the value from the P-Asserted-Identity field for the outbound call leg. (Note that the OS-E maintains the original From field value in the Contact field.) The default setting is disabled.
	header-to-strip	*Secondary property.* Configures the OS-E to strip the value of the specified field. Enter a SIP header field name.
	allowed-header	Sets the SIP headers that should be explicitly allowed to remain in the SIP message. You can enter any number of header names by re-executing the command.
	blocked-header	Sets the SIP headers that should be explicitly removed from the SIP message. You can enter any number of header names by re-executing the command.

Object name	Associated properties	Description
	apply-allow-block-to	Sets whether the allow and block properties of this object apply to request messages, response messages, or both. The following are valid apply-allow-block-to values: • requests—Apply to requests only • responses—Apply to responses only • requests-and-responses—Apply to requests and responses The default setting is requests-and-responses.
media-scanner-settings		This object allows you to configure media scanner settings. When media scanner settings are enabled, the media-scanner is started after the outgoing call connects and the pre-scan-time has elapsed. The media-scanner monitors the signal strength and duration of the received audio to divide into intervals.
	admin [enabled | disabled]	Enable or disable the media scanner settings for play-file-broadcast. The default setting is disabled.
	pre-scan-time	The number of milliseconds to delay before invoking the media scanner for speaker detection. The minimum configuration value is 0 and the maximum is 4294967295. The default value is 20 msecs.
	max-scan-time	The maximum number of milliseconds before canceling media scanning due to timeout. The minimum configuration value is 0 and the maximum is 4294967295. The default value is 30000 msecs.
	low-threshold	Enter the quiet signal power threshold in dbM. The minimum configuration value is -63 and the maximum is 3. The default setting is -36.
	high-threshold	Enter the talk or tone signal power threshold in dbM. The minimum configuration value is -63 and the maximum is 3. The default setting is -36.

Object name	Associated properties	Description
	low-long-duration	The number of milliseconds of detected quiet before declaring a long-pause. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 2000.
	high-long-duration	The number of milliseconds of detected talk or tone before declaring a long-talk or stable-tone.The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 900.
	averaging-window	*Secondary property* The window of time used when calculating signal strength. The minimum configuration value is 10 and the maximum is 1000. The default setting is 100.
	nominal-rounding-factor	*Secondary property.* The signal strength is rounded to the nearest multiple of the value you enter for this property. The minimum configuration value is 1 and the maximum is 25. The default setting is 2.
packet-discard		This configuration element allows you to configure the IP discard packet logging feature. If an IP interface has media-ports configured, you must first disable the media-ports > idle-monitor property, before the packet-discard object can be enabled.
	admin [enabled | disabled]	Enable or disable the packet discard feature. The default setting is enabled.
	track-port [enabled | disabled]	When enabled, this will log an additional type of message with the list of ports that were hit within the logging interval. The default setting is disabled.
	scan-interval	The interval in seconds between reading and logging the latest discarded packet information. The minimum configuration value is 10 and the maximum is 86400. The default setting is 60.
provisional-response		This object allows you to add any additional provisional responses you want sent along after the “100 Trying” response at the start of a normal INVITE dialog.

Object name	Associated properties	Description
	additional-response	Enter additional provisional responses you want sent with the INVITE dialog.
q931-cause-sip-response-map		This configuration object allows you to map Q.931 cause codes to SIP response codes.
	translation	Translates Q.931 cause/H.225 reason to SIP response codes.
q931-settings		This configuration object is used to configure Q.931 settings on the OS-E.
	numbering-play	The Q.931 numbering plan set in Calling and Called Party number information elements. The following is a list of valid numbering-plan values: • unknown • ISDN • data • telex • national-standard • private • reserved The default setting is ISDN.
	numbering-type	The Q.931 numbering type set in Calling and Called Party number information elements. The following is a list of valid numbering-type values: • unknown • international • national • network-specific • subscriber • abbreviated • reserved The default setting is allowed.

Object name	Associated properties	Description
	presentation-indicator	Enter the static presentation value to use. The following is a list of valid presentation-indicator values: • allowed • restricted • numberNotAvailable • reserved The default setting is allowed.
	screening-indicator	Enter the static screening value to use. The following is a list of valid screening-indicator values: • notScreened • verifiedPassed • verifiedFailed • networkProvided The default setting is notScreened.
	privacy-dynamic [true | false]	When true, the screening and presentation are dynamic. The default setting is true.
	use-incoming-display-ie [true | false]	When true, the OS-E attempts to use Display IE from the SETUP message when building SIP From: header display-name. The default setting is true.
	add-outgoing-displaytext-ie [true | false]	When true, the OS-E attempts to use SIP From: header display-name when building Display IE in the outgoing SETUP message. The default setting is false.
	q931-bearer-capability-ie	Set the Q931. Bearer Capability values used in outgoing H.323 messages.
sip-manipulation		Configure a specific SIP manipulation. This lets you add, modify, and delete SIP headers and parts of the SIP headers called SIP header elements. SIP header elements are the different subparts of the header, such as the header value, header parameter, and URI parameter.
	description	Enter a description of this SIP manipulation object.
	header-rule	Enter a list of header rules for this SIP manipulation.

Object name	Associated properties	Description
sip-manipulation-pool		Secondary object. Allows you to configure the pool of named SIP manipulation objects for the OS-E. These contain lists of SIP header manipulation rules and elements.
	sip-manipulation	Enter the SIP manipulation you want to configure.
sip-response-q931-cause-map		Allows you to translate SIP response codes to q931-cause and h225-reason. This is used when clearing H.323 calls.
	translation	Translate SIP response codes to q931-cause/h225-reason.
transcoding-policy		This transcoding policy object allows you to configure the transcoding policy for the OS-E. This includes defining the preferred codec as deduced from SDP offers and answers, adapting to match received codecs, and rewriting rfc-2833 headers when encoding audio.
	media-types	The types of codecs that may be transcoded. These values are added to the SDP. The following is a list of codecs that may be transcoded: • pcma • pcmu • g7221 • g723 • g728 • g729 • g726-16 • g726-24 • g726-32 • g726-30 • gsm • gsm-amr • iLBC
	most-preferred [true | false]	When true, the OS-E forces audio to only use the most preferred codec. The default setting is false.

Object name	Associated properties	Description
	symmetric-codec [true | false]	When true, the OS-E adapts and matches the correct codec when the endpoint has switched the “primary” codec. The default setting is false.
	balance-ptime [true | false]	When true, the OS-E attempts to balance RTP packet times with the SDP. The default setting is true.
	auto-release [true | false]	When true, the OS-E attempts to release transcode resources when auto-anchoring is enabled. The default setting is true.
	block-unknown [true | false]	When true the OS-E blocks unnegotiated packet types. The default setting is false.
	decode-telephone-events [true | false]	When true, the OS-E decodes telephone-events into audio during transcoding when both sides do not support telephone-events. The default setting is false.

New Properties in Release 3.6.0

Existing object name(s)	New property name	Description
accounting-data	**custom-data-grouping-string**	The characters used to associate custom data tags and values. The default setting is =.
	custom-data-delimiter	The characters used to separate group data entries. The default setting is ;.
call-failover	**server-load [enabled | disabled]**	When enabled, the OS-E calculates the server load and distributes traffic counters around the cluster. Based on these distributed counts, each OS-E in a cluster knows the fail-over status. The default setting is disabled.
cluster	**share-h323-port [true | false]**	Controls whether the H.323 service routes are pushed around a OS-E cluster. This property is not currently supported. The default setting is false.
database-group	**batch-insert-size**	The number of CDRs in one database insert request. The minimum configuration value is 1 and the maximum is 50. The default setting is 25.

Existing object name(s)	New property name	Description
eventpush-service	**page-domain**	Specifies the common domain name of the OS-E and the system running the web application.
file-client	**http-max-redirects**	The number of redirects in an HTTP URL before the OS-E issues a warning. The minimum configuration value is 1 and the maximum is 100. The default setting is 10.
file-system	**format**	The output format of the file you are creating. The following are available file formats: • csv • proprietary • tab • postgresql The default setting is csv.
	call-field-filter	Filter out what fields are sent with accounting records. If this is left blank, all fields are sent in the accounting records. The following are valid fields: • SessionID • Recorded • CallID • To • From • Method • IncomingRequestURI • PreviousHopIp • PreviousHopVia • OutgoingRequestURI • NextHopIp • NextHopDn • Header • Origin
	file-path	Enter the path and name of the file to write the records.

Existing object name(s)	New property name	Description
	roll-over	Set the schedule for creating new log files. The following values are valid: • never—never renew the file • minute—renew the file once a minute • hourly—renew the file once an hour • daily—renew the file once a day The default setting is daily.
	purge-old-logs [true | false]	Allows you to remove files modified earlier than the retention period, excluding the current file. You can identify the current file using the status provider. The default setting is false.
	retention-period	Set the number of days logs should be retained in the system. The minimum configuration value is 0 and the maximum is 5184000. The default setting is 3 days.
forking-settings	**max-arbitration-options**	*Secondary property.* Specifies the number of potential destinations to consider when applying a rule. The smaller of this and **max-hunt** takes effect when the final destinations are determined. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is unlimited.
h323-server	**session-duration-max**	Sets the maximum duration, in seconds, of an H.323 call. A value of **0** indicates there is no maximum lifetime. The minimum configuration value is 0 and the maximum is 1000000. The default setting is 0.
	admission-control [enabled | disabled]	Enable or disable admission control for SIP as all calls (H.323-SIP and H.323-H.323) pass through the SIP process. The default setting is disabled.
	max-concurrent-h323-calls	The maximum concurrent H.323 calls on this server. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 1500.
h323-settings	**stack-worker-threads-max**	Enter the number of H.323 stack worker threads. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 4.

Existing object name(s)	New property name	Description
	connection-threads-max	Enter the number of threads processing H.255 TCP traffic. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 4.
	process-auto-restart [enabled | disabled]	When enabled, causes the H.323 stack to restart when deadlocks are detected. The default setting is enabled.
icmp	**limit**	Limits the number of ICMP packets that can be received per second on this IP interface. The minimum configuration value is 1 and the maximum is 1000. The default setting is 10.
media	**attributeless-auto-anchor [enabled | disabled]**	*Secondary property.* When enabled in conjunction with the **anchor-mode=auto**, the OS-E attempts to auto-anchor streams without additional OS-E attributes in the SDP. The default setting is disabled.
	release-provisionally-anchored-media [true | false]	*Secondary property.* Release media resources that have been provisionally anchored. The default setting is false.
	report-last-timestamp [enabled | disabled]	When enabled the OS-E reports the timestamp of the last received media packet. The default setting is disabled.
	monitor-rfc-2833 [enabled | disabled]	Specifies whether to have the OS-E change SSRC when it detects RTP sequence number discontinuity on active SSRC. The default setting is disabled.
registration	**ignore-from-tag [enabled | disabled]**	When enabled, the OS-E uses the call ID only to associate the registration with a session. When disabled, the OS-E uses both the call ID and the From tag to associate the registration to a session. The default setting is enabled.
sip-settings	**allow-redirect [enabled | disabled]**	When enabled, the OS-E is able to redirect incoming calls to other servers. The default setting is enabled.
syslog	**port**	Specifies the port number over which the OS-E should communicate with this syslog server. The minimum configuration value is 1 and the maximum is 65535. The default setting is 514.

Existing object name(s)	New property name	Description
third-party-call-control	**terminate-hold-retrieve-locally [enabled | disabled]**	When this property is enabled, if a re-INVITE is received with an SDP that indicates it is either a hold or retrieve request, The OS-E accepts the re-INVITE locally with the SDP acknowledging the hold or retrieve and the message is not forwarded. When this property is disabled, re-INVITE messages with an SDP that indicate hold or retrieve receive no special treatment. The default setting is disabled.
	reinvite-originator [enabled | disabled]	When enabled, the OS-E reinvites the original UAC after the call is initially set up. The default setting is disabled.
	skip-shuffle-complete-if-anchored [enabled | disabled]	When enabled, no reinvite is sent forwarding the SDP contained in the ACK for calls with anchored media. The default setting is disabled.
	forward-302-diversion-header	*Secondary property.* When enabled, if a 302 Redirected response with a Diversion: header is received by the OS-E, the Diversion: header is forwarded in the response. The default setting is enabled.
web-service	**max-message-process-threads**	The maximum number of messaging processing threads. The minimum configuration value is 10 and the maximum is 200. The default setting is 10.
	max-http-connections	The maximum number of outbound http connections. The minimum configuration value is 100 and the maximum is 300. The default setting is 100.
	max-http-client-connections	The maximum number of outbound HTTP connections per host. The minimum configuration value is 5 and the maximum is 100. The default setting is 10.

Renamed Objects and Properties in Release 3.6.0

Old object or property name (in bold text)	New name
There are no new renamed objects or properties in release 3.6.	

Moved Objects and Properties in Release 3.6.0

Property name	Former location	New location
settings > local-directory-based-user-services	Secondary property.	Basic property.
hunt-group	vsp > carriers > hunt-group	vsp > hunt-group

Deleted Objects and Properties in Release 3.6.0

Configuration path	Deleted object or property
vsp > accounting	• accounting-file-check-interval • num-of-threads • queue-directory-allowed-when-busy • directories-to-be-queued
vsp > accounting > archiving	• archive-in-progress-sessions
vsp > default-session-config > file-transfer	• virus-scan
vsp > autonomous-ip location-pattern	• admin • description • match • priority • location • validate-bindings
vsp > default-session-config > media	• rtp-source-lock • hold-translation • hold-remove-telephone-events
preferences > pushlet-app	• page-domain
vsp > default-session-config > sip-settings	• session-match-callid-only
services > virus-scan	
vsp	• de-normalization
box > mx	• network
box > mx > card	• admin • file

Deleted Actions in Release 3.6.0

Action or status provider
mx

New and Revised Actions in Release 3.6.0

Action or status provider	Description
accounting-flush	The **accounting flush** action purges an accounting file you specify. The results of this operation are logged and you can view the logs to obtain more information on files that have been flushed. You can specify a **file-system** or an **external-file-system**.
show accounting-targets	Displays information from all accounting targets configured on the OS-E. The settings are configured using the **file-system** object.
show accounting-targets-file-system	Displays information for each accounting target configured on the OS-E. This shows information for both file-system and external-file-system targets.
show kernel-rule-stats	To display the cumulative packet discard statistics, enter the command with **show kernel-rule-stats instance= packet-discard.**
show media-scanner-summery	Displays media scanner settings. The media-scanner monitors the signal strength and duration of the received audio to divide it into intervals.
show media-scanner-interval	Displays media scanner intervals. The media-scanner monitors the signal strength and duration of the received audio to divide it into intervals.

MIB Changes in Release 3.6

This section covers changes that have been applied to Management Information Base (MIB) object definitions since Release 3.5.5.

New MIB Objects in Release 3.6.0

MIB Object name
arenaCacheOutstandingInstrumentation
arenaCacheOutstandingMaxCount
arenaCacheOutstandingInitialSize
arenaCacheOutstandingMaxSize

MIB Object name
arenaCacheOutstandingAllocatedFromCache
arenaCacheOutstandingFreedToCache
arenaCacheOutstandingCreated
arenaCacheOutstandingCreateFailed
arenaCacheOutstandingDestroyed
arenaCacheOutstandingCurrentFree
arenaCacheOutstandingFewestFree
arenaCacheOutstandingCurrentSmall
arenaCacheOutstandingCurrentCorrect
arenaCacheOutstandingcurrentLarge
arenaCacheOutstandingSampleCount
arenaCacheOutstandingTotalAllocs
arenaCacheOutstandingMinAllocs
arenaCacheOutstandingMaxAllocs
arenaCacheOutstandingTotalBytes
arenaCacheOutstandingMinBytes
arenaCacheOutstandingMaxBytes
arenaCacheOutstandingArea1
arenaCacheOutstandingArea2
arenaCacheOutstandingArea3
arenaCacheOutstandingArea4
arenaCacheOutstandingArea5
arenaCacheOutstandingArea6
arenaCacheOutstandingArea7
arenaCacheOutstandingArea8
arenaCacheOutstandingArea9
arenaCacheOutstandingArea10
arenaCacheOutstandingArea11
arenaCacheOutstandingArea12
arenaCacheOutstandingArea13

MIB Object name
arenaCacheOutstandingArea14
arenaCacheOutstandingArea15
arenaCacheOutstandingArea16
accountingFilesMirrors
accountingFilesTargets
kernelSummaryNumberRulesInGarbage
accountingStoreDirectory
accountingStoreDiskUsage
accountingStoreState
accountingStorePurgeOperations
accountingStoreRecordsPurged
accounting StoreLastPurgeStart
accountingStoreLastPureFinish
interceptSummaryWhatever

Removed MIB Objects for Release 3.6.0

MIB name
httpConnectionTable
kernelSummaryNumCmdPending
kernelSummaryNumberRulesInGarbage

Renamed MIB Objects in Release 3.6.0

Old object name	New name
lcrActionStatus group	**routeServerActionStatus group**
lcrCarriersTable	**routeServerCarriersTable**
sipLcrLookupTable	**sipRouteServerLookupTable**

Obsolete Objects for Release 3.6.0

Object name
locationPatternTable
servicesRoutingMetricsTable
gatewayLoadMirrorTable
trunkLoadMirrorTable
accountingFilesSubdirectoryCount
accountingStatusTable
clusterServerLoadTable
clusterServerLoadDetailTable
virusScanTable
cnxInterfacesTable

New MIB Tables in Release 3.6.0

MIB table name	Description
accountingTargetsTable	Destination targets for accounting CDRs.
accountingTargetsFileSystemTable	Information on file system accounting targets for CDRs.
httpClientsTable	HTTP connection status.
arenaCacheByAllocatorTable	Arena cache statistics by allocator address.
arenaCacheUsageByAllocatorTable	Arena cache usage distribution by allocator address.
arenaCacheUsageOutstandingTable	Arena cache usage distribution for outstanding arenas.
autonomousTableSummaryTable	Autonomous IP route table summary info by tag.
availableMemoryTable	Basic measure of available memory.
callingGroupQosTable	SIP Calling Group Quality of Service Statistics.
callingGroupRedirectTable	SIP Calling Group 302 Redirect Call Statistics.
functionCallersTable	Function callers.
gatewayAdjacencyTable	Gateway adjacency status.

MIB table name	Description
gatewayRoutingTable	Gateway routing status.
interceptSentinelsTable	Current intercept sentinel status.
interceptSessionsTable	Information about RTP data on intercepted sessions.
mediaPortsSessionsTable	Addresses used by media stream sessions.
mediaScannerIntervalTable	Media Scanner Interval.
mediaScannerSummaryTable	Media Scanner Summary.
mediaStreamHairpinTable	Addresses in use by hairpinned media stream.
messagingReferencesTable	Messaging session reference status.
serverLoadDbTable	SIP Server Load Status.
servicesRoutingConfigTable	Services routing config status.
servicesRoutingLoadShareTable	Services routing table load share status.
sipServerQosTable	SIP Server Quality of Service Statistics.
sipServerRacTable	SIP Server Registration Admission Control Statistics.
switchQosTable	SIP Voice Gateway Quality of Service Statistics.
switchRacTable	SIP Voice Gateway Registration Admission Control Statistics.
trunkQosTable	SIP Trunk Group Quality of Service Statistics.
trunkRacTable	SIP Trunk Group Registration Admission Control Statistics.
serverLoadExternalStatsTable	SIP server statistics used in calculating server load.
sipServerRedirectTable	SIP Server 302 Redirect Calls Statistics.
switchRedirectTable	SIP Voice Gateway 302 Redirect Calls Statistics.
trunkRedirectTable	SIP Trunk Group 302 Redirect Calls Statistics.

Revised MIB Tables in Release 3.6.0

MIB table name	Description of change
autonomousIpGatewayTable	ADDED: autonomousIpGatewayRoutingTag, autonomousIpGatewaySubnetAddress, autonomousIpGatewaySubnetMask, autonomousIpGatewayGroupCount REMOVED: autonomousIpGatewayAddressPool, autonomousIpGatewayClassId, autonomousIpGatewayObjectId
autonomousIpGroupTable	ADDED: autonomousIpGroupRoutingTag, autonomousIpGroupSubnetAddress, autonomousIpGroupSubnetMask, autonomousIpGroupHits REMOVED: autonomousIpGroupGateway, autonomousIpGroupClassId, autonomousIpGroupObjectId, autonomousIpGroupGrpIndex
autonomousIpRouteTable	Fields added and removed.
autonomousPrivateGroupTable	Fields added and removed.
autonomousPrivateRouteTable	Fields added and removed.

MIB table name	Description of change
callingGroupCacTable	Added: callingGroupCacCurrentLocal, callingGroupCacCurrentCluster, callingGroupCacCurrentMax, callingGroupCacCurrentMax, callingGroupCacSetupCluster, callingGroupCacSetupMax OBSOLETE: callingGroupCacMaxBandwidth, callingGroupCacMaxBandwidth, callingGroupCacMaxNumberOfConcurrentCalls, callingGroupCacConnectedCalls, callingGroupCacMaxCallsInSetup, callingGroupCacCallsInSetup, callingGroupCacCallRateLimitingState, callingGroupCacCallRateLimitingRate, callingGroupCacCallRateLimitingInterval, callingGroup CacMaxNumberOfRegistrations, callingGroupCacRegisteredAors, callingGroupMaxRegistrationInProgress, callingGroupCacRegistrationsInProgress, callingGroupCacClusterUsedBandwidth, callingGroupCacClusterConnectedCalls, callingGroupCacClusterCallsInSetup, callingGroupCacClusterWcaNextPercentage, callingGroupCacClusterWcaNextPercentageCalls, callingGroupCacClusterRegisteredAors, callingGroupoCacClusterRegistrationsInProgress, callingGroupCacCLusterRegistrationPercentage, callingGroupCacClusterNextPercentageRegistrations
switchCacTable	Objects added and removed
kernelInstanceTable	ADDED: kernelInstanceAcceleratorRulesDeleteFailed
mediaStreamAddressesTable	Added: mediaStreamAddressesAnchorState OBSOLETE: mediaStreamAddressesAnchored
mediaStreamRtpStatsTable	ADDED: mediaStreamRtpStatsAnchorState OBSOLETE: mediaStreamRtpStatsAvgLatency, mediaStreamRtpStatsMinLatency, mediaStreamRtpStatsMaxLatency, mediaStreamRtpStatsMinTTL, mediaStreamRtpStatsMaxTTL
mediaStreamSrtpTable	ADDED: mediaStreamSRTPAnchorState
mediaStreamStatsTable	ADDED: mediaStreamStatsAnchorState
sipServerCacTable	Objects added and removed
trunkCacTable	Objects added and removed

MIB table name	Description of change
sipSummaryByBoxTable	ADDED: sipSummaryRatesByBoxCallIDurationMax
sipSummaryRatesByBoxTable	ADDED: sipSummaryRatesByBoxCallDurationMax, sipSummaryRatesByBoxCallDuration replaced by sipSummaryRatesByBoxCallDurationAVG
kernelRuleDetailTable	ADDED: kernelRuleDetailId, kernelRuleDetailSessionID
mediaStreamDtmfTable	ADDED: mediaStreamDtmfAnchorState
rtcpGenerateSessionsTable	rtcpGenerateSessionsReportsSent replaced with rtcpGenerateSessionsGenerated OBSOLETE: rtcpGenerateSessionsType
rtcpGenerateStatsTable	rtcpGenerateStatsReportsSent replaced by rtcpGenerateStatsGenerated OBSOLETE: rtcpGenerateStatsType
callNormalizationTable	ADDED: callNormalizationIsExternal, callNormalizationVirtualDialPlan
callRoutingTable	ADDED: callRoutingIsExternal, callRoutingVirtualDialPlan
mediaPortsHeldTable	ADDED: mediaPortsHeldInterface
mediaPortsProcessUnitsTable	ADDED: mediaPortsProcessUnitsPresent
mediaPortsSummaryTable	ADDED: mediaPortsSummaryInterface
rtcpGenerateReceiverTable	ADDED: rtcpGenerateReceiverTime
rtcpGenerateSenderTable	ADDED: rtcpGenerateSenderTime
serverConnLookupTable	ADDED: serverConnLookupLocalIp, serverConnLookupRoutingTag
serverHostLookupTable	ADDED: serverHostLookupLocalIp, serverHostLookupRoutingTag
serverNameLookupTable	ADDED: serverNameLookupLocalIp, serverNameLookupRoutingTag
servicesBoxDatabaseTable	ADDED: servicesBoxDatabaseMediaMetricMax, servicesBoxDatabaseMediaMetricCurrent
accountingDatabaseTable	ADDED: accountingDatabaseState, accountingDatabaseMissingRecords
activeCallsTable	Added: actyiveCallsConnectyed, activeCallsScanTime, activeCallsFileTime, activeCallsPlayTime, activeCallsDisconnectReason

MIB table name	Description of change
carrierRoutingTable	RENAMED: carrierRoutingMatch to CarrierRoutingToMatch; carrierRoutingMin to carrierRoutingMinPrefixDigits OBSOLETE: carrierRoutingRoutingTag, carrierRoutingtype, carrierRoutingPrefixPattern, carrierRoutingTime, carrierRoutingTimeRecordId, carrierRoutingAction, carrierRoutingFwd, carrierRoutingSetting
dialPlanTable	ADDED: dialPlanIsExternal, dialPlanVirtualDialPlan
lcrRoutingTable	ADDED: lcrRoutingTableToMatch, lcrRoutingTableMinPrefixDigits OBSOLETE: lcrRoutingTableRoutingTag, lcrRoutingTableType, lcrRoutingTablePrefixPattern, lcrRoutingTableTime, lcrRoutingTableTimeRecordId, lcrRoutingTableAction, lcrRoutingTableFwd, lcrRoutingTableSetting
fileTransferSummaryTable	OBSOLETE: fileTransferSummaryVirusChecked
kernelRuleTable	ADDED: kernelRuleSessionID
kernelRuleAnchorTable	ADDED: kernelRuleAnchorSessionID
kernelRuleRouteTable	ADDED: kernelRuleRouteSessionID
kernelRuleStatsTable	ADDED: kernelRuleStatsSessionID
registrationArbitrationTable	ADDED: registrationArbitrationIsExternal, registrationArbitrationVirtualDialPlan
registrationNormalizationTable	ADDED: registrationNormalizationIsExternal, registrationNormalizationVirtualDialPlan
registrationPlanEntry	ADDED: registrationPlanIsExternal, registrationPlanVirtualDialPlan
registrationProxyTable	ADDED: registrationProxyIsExternal, registrationProxyVirtualDialPlan
registrationProxyRoutingTable	ADDED: registrationProxyRoutingIsExternal, registrationProxyRoutingVirtualDialPlan
registrationRoutingTable	ADDED: registrationRoutingIsExternal, registrationRoutingVirtualDialPlan
routingArbitrationTable	ADDED: routingArbitrationIsExternal, routingArbitrationVirtualDialPlan
servicesInterfaceDatabaseTable	ADDED: servicesInterfaceDatabaseH323
servicesRouteDatabaseTable	ADDED: servicesRouteDatabaseH323
signalingSessionsTable	Objects added and removed

MIB table name	Description of change
h323ExternalGatekeepersTable	ADDED: h323ExternalGatekeepersObjectID‘
mediaStreamServerSessionsTable	ADDED: mediaStreamServerSessionsAnchorState
productModel	Changed from integer to OCTET STRING
systemInfoModel	Changed from integer to OCTET STRING

New SNMP Trap Entries in MIB for Release 3.6.0

Trap name	Description
h323CallPortRelease	An H.323 port has been released.
playFailed	Media has failed to be played out onto a leg.
playInitiated	Media has begun to be played out onto a leg.

Revised SNMP Trap Entries in MIB for Release 3.6.0

Trap name	Description
playComplete	New fields added to trap.
h323CallQ931TunneledMsg	New fields added to trap.

Obsolete SNMP Trap Entries for Release 3.6.0

Trap name
fileTransferAntiVirusFail

Known Problems, Restrictions, and Operational Considerations in 3.6

The following section describes the known problems, restrictions, and operational considerations in Release 3.6.

- Issuing the **vsp-reset** command now requires a user confirmation to execute the command successfully.
- In releases previous to 3.5.5, setting the **sticky-via** configuration property modified the VIAs of all messages sent to the next-hop server. Now the OS-E does not modify response messages going back to the server.

- In releases previous to 3.5.5, the Master Service Up event log message was not given the same severity as the Master Service Down event. Now these are both set to the “alert” severity.
- When using media-shuffle, media anchoring must be enabled to work properly. (ID 14490)

RADIUS Attributes, CDRs and RADIUS Servers

The following table lists the vendor-specific attributes (VSAs) that Acme Packet writes to RADIUS packets, type Cisco, in Release 3.6..

VSA number (vendor)	Attribute Name	Description
1 (Cisco)	SESSION_PROTOCOL	
1 (Cisco)	CALL_ID	
1 (Cisco)	INCOMING_REQ_URI	
1 (Cisco)	OUTGOING_REQ_URI	
1 (Cisco)	NEXT_HOP_DN	
1 (Cisco)	NEXT_HOP_IP	
1 (Cisco)	PREV_HOP_IP	
1 (Cisco)	DISCONNECT_CAUSE	
1 (Cisco)	PREV_HOP_VIA	
1 (OS-E)	**CXC-Permissions**	The full name of the configuration permissions object for OS-E users. **Format:** "access permissions admin"
2 (OS-E)	**CXC-SIP-Address**	The SIP address of the user. **Format:** name@companyABC.com
3 (OS-E)	**CXC-Object**	Used when RADIUS is a policy server to return policies and configuration information.
4 (OS-E)	**CXC-Sess-Attr**	Used when RADIUS is a policy server to return policies and configuration information.
5 (OS-E)	**CXC-Version**	The build number associated with the software release.

VSA number (vendor)	Attribute Name	Description
25 (Cisco)	H323_SETUP_TIME	
26 (Cisco)	H323_CALL_ORIGIN	
28 (Cisco)	H323_CONNECT_TIME	
28 (Cisco)	H323_DISCONNECT_TIME	
30 (RADIUS)	CALLING_STATION_ID	
31 (RADIUS)	CALLED_STATION_ID	
200 (OS-E)	**SESSION_ID**	The session identifier assigned by OS-E on a call session when authenticating a SIP INVITE message.
201 (OS-E)	**RECORDED**	For RADIUS accounting record: TRUE or FALSE.
21798 (Vendor)	**Acme Packet**	The OS-E globally-assigned RADIUS vendor attribute.

When sending CDRs to an external RADIUS server, ensure that you have configured the **radius-group/call-field-filter** so that the essential records are forwarded to that server. Additionally, the external RADIUS server must have attributes to extract critical records from the CDR, such as the calling party number information for billing purposes. These configured attributes are generally set up in a “dictionary” for that server, but dictionaries are specific to RADIUS vendors.

OS-E RADIUS VSAs are defined in the directory **/cxc/web/dictionary.covergence**.

Problems, Restrictions, and Considerations from Prior Releases

Upgrading to Release 3.6.0

- Currently, cluster and controlled upgrades from any release prior to Release 3.6.0 are not supported. Perform the upgrade procedure on each individual box in the cluster. (ID 15131)

- If you are currently running a release prior to 3.3.8, 3.4.2, or 3.5.1, you will need to perform the upgrade to Release 3.6.0 from a USB stick. Refer to the *Net-Net OS-E — USB Creation and Commissioning Instructions* for information on creating the USB stick and commissioning the OS-E device.
- If you are currently running Release 3.3.8, 3.4.2, 3.5.1, or later you can perform the upgrade to Release 3.6.0 using the procedure covered in the section, "RADIUS Attributes, CDRs, and RADIUS Servers," using the Release 3.6 tar file, or you can perform the upgrade from a USB stick. This means that you can choose either procedure, however, Acme Packet recommends that you apply the upgrade from the USB stick for better compatibility with future upgrades.
- If the OS-E device had data drives mounted on the original version of software, these data drives will no longer be mounted after the upgrade to Release 3.6. Run the **add-device** action to restore the data drives to operate with the new software by specifying the *data-1* or *data-2* drive position and the relevant file system.
- When upgrading a OS-E from a USB stick, the configuration, license, certificates and other components are preserved. However, any data on the RAID-10 data-1 drive is not preserved during this operation as the RAID array is always re-configured, with its data erased. If you require the contents of the RAID-10 data-1 drive, perform the upgrade to 3.6.0 using the procedure, "RADIUS Attributes, CDRs, and RADIUS Servers."

  This does not affect any other platform, including 3rd-party platforms with RAID configured. (ID 14736)

USB Stick Restrictions

If you are upgrading an existing OS-E device from a USB stick, check the /cxc directory for .cfg and .xml files that are larger than 2 MB. Files that are larger than 2 MB will not be backed up to the USB stick and restored during the upgrade process.

All *.cfg and *.xml files in the current working directory (/cxc) less than 2 MB in size are backed up to the stick and restored during the upgrade. (ID 13207)

It is important to remember to remove the USB stick once an upgrade is completed in order to maintain the correct modified configuration. (ID 15640)

Virtual Interfaces per Physical Ethernet

Each physical Ethernet interface supports up to 14 virtual (VX) interfaces.

IP Interfaces per Physical OS-E Device

Release 3.6 supports a maximum of 4096 named IP interfaces per OS-E device.

CDR Values on External Databases

When sending accounting CDRs to external databases, values that are unsigned 32-bit integers are stored as signed 32 bit integers in the database record. If the value of the field is larger than 2147483647 and retrieved as an integer, the value is stored as a negative number.

To decode the negative number, add 2^{32} or 4294967296 to the value.

The following columns are affected:

- Duration
- PacketsReceivedOnSrcLeg
- PacketsLostOnSrcLeg
- PacketsDiscardedOnSrcLeg
- PdvOnSrcLeg
- MaxJitterOnSrcLeg
- LatencyOnSrcLeg
- MaxLatencyOnSrcLeg
- PacketsReceivedOnDestLeg
- PacketsLostOnDestLeg
- PacketsDiscardedOnDestLeg
- PdvOnDestLeg
- MaxJitterOnDestLeg
- LatencyOnDestLeg

- MaxLatencyOnDestLeg
- Rx1000FactorOnDestLeg
- Rx1000FactorOnSrcLeg
- huntingAttempts
- callPDD

(ID 15898)

Modifying the Timezone

When the timezone property is modified in the Box configuration several Java processes must be manually restarted on that OS-E to pickup the modification. The java processes that need to be restarted are:

- Web
- DIR
- WS
- Acct
- Presence
- Eventpush
- DOS

(ID 15640)

Using the Configuration Import Utility

The import and conversion utility that allows you to move the configuration file (*cxc.cfg* by default) to other OS-E devices. This solves problems associated with managing MAC addresses from one system to another anytime the configuration file is transferred. The import utility uses the XML transform program to run the conversion.

Perform the following steps:

1. Save the current configuration to XML format to a USB stick. The new file is named *template.xml*.

```
NNOS-E>> config save xml /mnt/usb/template.xml
```

2. Insert the USB stick into the USB port on the OS-E master system to which the template.xml file is imported.
3. Run the XML transform program to import the **template.xml** file.

```
NNOS-E>> xml transform cfg-import.xsl /mnt/usb/template.xml new.xml
“box1=11:11:11:11:11:11 box2=22:22:22:22:22:22
box3=33:33:33:33:33:33 box4=44:44:44:44:44:44”
Success
```

   where *cfg-import.xsl* is the name of the style sheet included with OS-E, *template.xml* is the name of the original *cxc.cfg* file (saved as XML), and *new.xml* is the resulting name of the new configuration file that you just imported to OS-E. Included in quotation marks (“) is the list of MAC addresses to which the new configuration file is imported.

4. At the master OS-E device receiving the new configuration file, replace the running the configuration file with the *new.xml* file. If the new configuration is operating as expected, execute **config save**. The four devices in cluster will automatically receive the new configuration file.

```
NNOS-E>> config replace new.xml
NNOS-E>> config save
```

Installing the Cisco JTAPI Jar File

This is needed only for customers who are using the external presence JTAPI communication feature on a OS-E device interoperating with the Cisco CallManager.

Perform the following steps to install the Cisco JTAPI software.

1. Log in to the computer where you want to install the Cisco JTAPI client software.
2. Close all Windows programs.
3. Open a Web browser.
4. Go to the Cisco CallManager administration windows at:

   http://*name*/CCMAdmin/main.asp

   where:

   name specifies the name or IP address of the Cisco CallManager.

Note: If the above web address does not access the Cisco CallManager administration window properly, try using the following:

http://<call manager>/plugins/jtapi.jar

5. Choose **Application->Install Plugins**.
6. Choose the **Cisco JTAPI** link.
7. Save the file on your desktop and follow the instructions in the pop-up windows.

Note: Install Cisco JTAPI software on the default drive as directed by the installation software. When Windows NT is installed in C:\WINNT, the default directory, for example, is C:\WINNT\Java\lib.

At the platform or blade running OS-E, perform the following steps:

8. Copy the *jtapi.jar* from the **Windows\Java\lib** directory to **/cxc_common/jtapi** and rename the files to the following:
   - Cisco 4 CallManager **jtapi jar** to **jtapi-cisco-2.1.jar**
   - Cisco 5 Call Manager **jtapi.jar** to **jtapi-cisco-3.0.jar**
   - Cisco 6 Call Manager **jtapi.jar** to **jtapi-cisco-4.0.jar**
9. Restart the presence process by performing a **restart warm**.

Routing to Location Cache When Destination Server is “Down”

In Release 3.6, calls are no longer routed to the location-cache if the destination server is detected as “down” during failover-detection. If there is a matching dial-plan, OS-E will now return a SIP 503 (Service Unavailable) message rather than route the call through the location-cache and returning a SIP 404 message.

Previously, when all the servers on a route were down, the route was removed from the active routing table, causing failure of the dial-plan match and returning a SIP 404.

Virus Scanning

All virus scanning functionality (to include McAfee and icap-server) has been removed and is no longer supported in OS-E.

OS-E Virtual Machine Limitations

- Transcoding is not supported on the VM.
- Feature options that require fine-grained timing such as music-on-hold and announcements may not work properly in the virtual environment. This is due to virtual OS timing issues that are beyond the control of the Acme Packet software. If you plan on using these features as part of your application, please contact your Acme Packet sales representative for further information.

Accounting Reset

When directing accounting records to an external database target, you will need to execute the **accounting reset** action if you edit the database secret password after OS-E has started forwarding records to this database. Otherwise, OS-E will not be able to contact the external database.

The external database password is configured under the **vsp accounting database group server** object using the **password-tag** property. (ID 15403)

Combination of Ringback-File and Call Introduction

Currently, if a ringback file and a call introduction are configured simultaneously, the call introduction is played immediately, followed by the ringback file. As a result, the call recipient never hears the introduction, and the call originator hears the introduction before the ringback file is played.

When operating correctly, the call introduction is played after the call is connected so that both the caller and the call recipient hear it. (ID 13282)

Web Service Pushlets Over HTTPS

Currently, Web service pushlets and external event service applications with a self-signed certificate will not operate over HTTPS connections. (ID 13421, 14394)

Cisco CallManager Interoperability — Automatic Call Forwarding

When Cisco CallManager (CCM) over H.323 is handling an automatic call forward with **inbound faststart** on the CCM disabled, OS-E sends a CCM non-responding **termCap** when handling remote ringback.

For automatic call forwarding to work properly, ensure that CCM **inbound faststart** is enabled. (ID 13748)

Inleg and Outleg TOS Values

When editing the session configuration **sip-settings\inleg-tos** and **outleg-tos** overwrite value settings, specify a number that represents the 8-bit Differentiated Services (DS) field of the IP packet in decimal format, such as 26 for 00011010, and 104 for 01101000. The default setting for both of these properties is 0. (ID 14110)

Google Gadgets and OS-E Management System Browser Windows

When running the OS-E Management System and iGoogle (with Gadgets) simultaneously, make sure that you are run the OS-E Management System and iGoogle in separate browser windows. (ID 14450, 14451)

Accounting

- Currently, when directing CDRs to a RADIUS target, call field filtering (as configured with the vsp\radius-group**call-field-filter** object) does not work. By default, all fields are sent to the RADIUS target. (ID 14893)
- With the vsp\accounting\file-system\path **roll-over** property set to *daily*, the OS-E software currently creates a new accounting file each time the system is restarted, resulting in multiple accounting targets per day. All files are sent to the target, so the target receives all CDRs meant for it. (ID 14568)
- If you disable an accounting target that is referenced by an accounting policy in any session configuration and then re-enable the target, accounting will not send the records that accumulated while the accounting target was disabled. (ID 15044)
- For CDRs to be properly sent to an external MS SQL database server, the **box\hostname** property must be specified using an IP address or fully qualified domain name (FQDN). If a partial hostname is specified, then the domain name must be qualified using the **vsp\static-stack-settings**. (ID 13292)

- Currently, the **accounting purge** action is operating slowly, causing call records to consume large amounts of disk space. Acme Packet recommends that you set up a second disk for accounting records and set the **accounting-root-directory** (under services\data-locations) to that new drive and directory location. Additionally, set the vsp\accounting **retention-period** to 1 (one day) to ensure frequent purging.

  To enable a second drive, perform the following steps:

  1. Unmount, format, and mount the new target drive, such as *data-1*.

```
NNOS-E>> umount data-1
Success !
NNOS-E>> format data-1 reiser-3
Are you sure (y or n)? y
Success!
NNOS-E>> mount data-1
Device is mounted.

NNOS-E>> show mounts (to display the data-1 drive in the list)
```

  2. Under services\data-locations, set the **accounting-root-directory** property to the new target drive and directory.

```
config data-locations> set accounting-root-directory /cxc_common
  data-1/accounting
```

  3. Set the vsp\accounting **retention-period property** to 1 (one day) to ensure frequent purging of accounting records and free disk space.

  (ID 14905)

Generic JDBC Driver

If you are sending CDRs to an external MySQL database server group, (where type is generic), you will need to download and copy the MySQL driver to the OS-E **/cxc/lib/jdbc** directory to properly connect to the MySQL database.

The MySQL 5.1 download is available from the following link.

http://dev.mysql.com/downloads/mysql/5.1.html

- mysql-connector-java-5.1.7-bin.jar

After copying the driver over to the OS-E device, restart the accounting process by issuing a **restart warm**.

At the MySQL database server (Windows XP, NT, Linux), you will need to open port 3306 to allow client access, as follows:

1. **Start->Control Panel->Windows Firewall**.
2. Select **Exceptions** and **Add Port**
3. Add the port name *mysql_port* and port number *3306.*

Note: Follow this procedure for any JDBC driver used with accounting generic database target type.

Removing and Adding Network Interface (NIC) Cards

Whenever an Ethernet network interface is removed and reinstalled on an OS-E you need to perform either the **install nic** or the **install nic-reinitialize** action to reassign Ethernet port numbering. Not doing so could result in a system deadlock.

- **install-nic** — Adds a NIC card to a system that was previously running. Interfaces on the new card are assigned "next" available Ethernet interface numbers.
- **nic-reinitialize** — Removes all the existing NIC interface assignments and rebuilds the interfaces in order. For hardware, the order is based on how the PCI buses are scanned.

  When upgrading or replacing a NIC card with the same number of ports, either **install-nic** or **nic-reinitialize** action may be used. (ID 14333)

H.323 Call Details in the Call Logs

To view H.323 call details from the OS-E Management System Call Logs, select **Sessions,** then select **View->Other** at the right side of the page. Currently, the **H323 Messages** function does not work. (ID 14852)

H.323 Operational Issues

Currently, unanchored calls over H.323 networks (most deployments) will result in remote ringback, call hold and release, call transfer, and music-on-hold (MOH) failures. (ID 14490, 14519, 14523, 14927, 14977)

CUCM-SIP and ACM-SIP Interoperability — Calls on Hold

With interoperating SIP environments involving Cisco Unified Communications Manager (CUCM) and Avaya Call Manager (ACM), set the session configuration third-party-call-control **reinvite-delayed-offer-wait-on-ack** setting to *enabled* and the session configuration **in-hold-translation** and **out-hold-translation** offer and answer attributes to *sendrecv*. Otherwise, inconsistent re-INVITE behaviors will result when calls are placed on hold in these environments. (ID 15091)

Multiple VLANs on VRRP Networks

If you configure multiple VLANs on a VRRP network, and if you have a VLAN configured on that physical interface, you will need to create corresponding (“phantom”) VRRP VLANs on the Ethernet physical interface to enable traffic to reach the VRRP network. However, if the Ethernet interface does not have a VLAN configured, then there is no need to configure the corresponding “phantom” VRRP VLANs. (ID 12378)

OS-E Management System — Configuration Change Indication

When exiting the OS-E Management System, the software does not currently post a configuration change indication if additions and edits were applied with a **Set** or **OK** selection during the active session. Proceed to save or cancel the configuration, as desired. (ID 3920)

Proxy Re-Registration of SNOM Phones

In a proxy registration configuration involving Broadworks and SNOM phones, the first re-register of the phone allows the unregister/register requests to be handled in the correct order. On a second re-register of the phone, the register requests are handled out of order, forcing the phone into the "in-service" state. A third re-register of the phone returns it to the registered state.

DNS and ENUM

The following notes summarize operational issues with the DNS and ENUM functionality.

- The **vsp/enum/resolver** and **vsp/enum/mapping** objects have been removed from the configuration. Both DNS and ENUM servers are now configured using the **vsp/dns/resolver/server** object using the server IP address and the **type** property (dns-only, enum-only, or both).
- The **vsp/dns/resolver/server** entries no longer have the **sip-location** setting. This setting is now a per-session setting that applies to **routing-last-resort-dns** and is configured in **session-config/dns-client-settings**.
- The new **vsp/dns/enum-mapping** requires a domain-name to be specified, replacing the previous **vsp/enum/mapping** object. An upgrade puts e164.arpa as the domain-name.
- An **enum-domain** can not be referenced per server in **vsp/dns/resolver/server**. Use the **vsp/dial-plan/normalization/condition-list/enum-server** configuration. (ID 12881)

Archiving

In Release 3.6, an accounting target of the local database must be configured in order for archiving to work. (ID 12883)

Directory and Master Services

If the directory Service is configured and enabled in a cluster environment, the directory service and master database must be configured on the same system before upgrade installation.

Directory service and master system database must be configured and co-exist in the same box. In 3.6, the directory service communicates with the master system database and instructs master system database to load users data from the local file system where the directory service is running. If the Directory service and the master system database do not co-exist on the same device, the master system database will no be able to load files generated by the directory service.

Additionally, directory services database tables are not populated to the backup device. In a cluster, OS-E does not support directory services failing over to the backup box. This is because user ID numbers get regenerated and may not match IDs stored in the database for past traffic. (ID 13203)

Monitor-Groups

Currently, the **vsp/monitor-group** and the **media/monitor** *monitor-group* reference are not currently operational. In the OS-E Management System, this affects the **Call-out** function found under Call Logs/Sessions, User Sessions, and Accounting, and when selecting the **Set up playback** template from Call Logs/User Sessions. (ID 13425)

Siemens Fujitsu RX100 and RX300 Servers

When running OS-E on Siemens Fujitsu RX100 and RX300 servers, the onboard Ethernet ports (two) on these servers not currently supported in Release 3.6. (ID 13294)

Media Verification Issue

When using media-verification, if call endpoints do not agree upon a packet interval (ptime), the media-verification may end up dropping RTP packets as outside the range for that CODEC/packet interval. (ID 12381)

Inleg and Outleg TOS Values

When editing the session configuration **sip-settings\inleg-tos** and **outleg-tos** overwrite value settings, specify a number that represents the 8-bit Differentiated Services (DS) field of the IP packet in decimal format, such as 26 for 011010, and 104 for 01101000. The default setting for both of these properties is 0. (ID 14110)

Call Monitoring and Transcoding — No Audio

Currently, there is no audio heard between call endpoints if both transcoding and attendant call monitoring are configured in combination. This problem will be addressed in a later release. (ID 12387)

Policy Manager Running Over WebSphere

When running Policy Manager over WebSphere, note the following:

- An HTTP 500-Internal Server error will occur when retrieving any status using Call Manager and the Status application. This problem only occurs if there are no users and permissions configured under the **access** object. Be sure to configure OS-E user names and passwords for the required Web services authentication as described in the manual, *Net-Net OS-E — Using the OS-E Management Tools*. (ID 11114)
- Ensure that the proper web-service credentials are provided when making web service requests to the OS-E domain. Otherwise, OS-E will return an HTTP 401 (Unauthorized) response, causing the WebSphere Policy Manager application to hang. (ID 11619)

Third Party Call Control (3PCC) Call Transfers

During third party call control (3PCC) sessions involving a Cisco Call Manager server, a call transfer involving multiple recipients will result in a new call control window at first call transfer recipient. Normally, the original call control window should remain active without a refresh. (ID 11298)

SIP Server Pools

Currently, the **show sip-server-pool** command does not display the number of out packets; a 0 count is reported. (ID 11504)

Virtual Machine Uptime Reporting

Currently, if you shut down and then restart the OS-E Virtual Machine on the same device, executing the **show system-info** command will report the new VM with an incorrect uptime. The command shows the uptime starting with the statistic associated with previous VM instead of beginning at zero uptime. (ID 11396)

Attendant Call Monitoring

- With anchoring, recording, and call monitoring enabled, OS-E records the call for the call participants (caller A to caller B), but does not record the call session with the third-party attendant (C). Although the call log shows a separate entry for the INVITE from A to C, the Play field is greyed out, indicating no recording. (ID 9542)

- Currently, an intermittent SIP trace error has been observed with locally-registered phones when the call attendant endpoint picks up while the dialed phone is still ringing. (ID 10989)

QoS Call Duration Statistics

Currently, QoS average call duration and post dial delay statistics for endpoints are not being reported (displaying 0 with the **show switch-pool -v** command). (ID 11549)

H.323 — SIP Directive

The session configuration **sip-directive/directive refuse** setting is not currently applied in H.323 to SIP sessions. (ID 11925)

Unmatched Sessions Returned When Searching by Date/To/From

When searching the OS-E Management System **Call Logs->Sessions** using the Date/To/From criteria, a partial fromURI field is shown in the display, causing the matched sessions to appear “unmatched” in the search results. (ID 11868)

Call Field Filtering on Jitter and Media CDR Fields

To properly display jitter and media CDR fields that are added with the **vsp\accounting\database\group\call-field-filter** object, select PDV on the call-field-filter to display the jitter fields, and select RFACTOR under media fields to display the rfactor fields. (ID 11866)

No Audio Available to Call Monitors

Currently, audio is not being sent to SIP phone third-party endpoints configured in the VSP **monitor-group**. (ID 11951)

Microsoft LCS to IBM Sametime

OS-E users federating IBM Sametime and Microsoft LCS may experience issues with federated presence when moving to 3.4.1 and using their previous configuration. Specifically, **sip-settings** can no longer be used to configure the transport for federated traffic. The **request-uri-specification** should be used instead. (ID 11950)

Admission Control Behavior Changes

To address call admission control behaviors, the following admission control settings are now *disabled* by default:

- **registration-admission-control** — If enabled, the controls set with the pending registration high- and low-watermarks are applicable. This admission control suppresses new registrations to allow resolving registrations in progress, preventing “rate of registration” attacks.
- **call-admission-control** — If enabled, allows call admission control (CAC) on OS-E. The following settings are only applicable if **call-admission-control** is enabled:
  - **cac-max-calls**
  - **cac-max-calls-in-setup**
  - **cac-min-calls-in-setup**
  - **cac-max-number-of-tls**
  - **cac-max-tls-in-setup**
  - **calls-cpu-limit**
  - **call-response-code-at-threshold**
  - **call-response-string-at-threshold**

  When disabled, only the **static-stack-settings max-number-of-sessions** property controls setup and connection limits.

The following threshold settings have also been modified:

- **registrations-high-cpu-threshold** — Default is 90%. Sets an upper threshold, as a percentage, for registration processing average CPU usage. The registration dynamic threshold is calculated based on the admission-control/ **pending-registrations-high-watermark** property. When the average CPU usage exceeds this high threshold, OS-E decrements the dynamic threshold by 10% until it reaches the value set with the **pending-registrations-low-watermark** property.
- **registrations-low-cpu-threshold** — Default is 70%. Sets the low-end threshold, as a percentage, for registration processing average CPU usage based on the registration dynamic threshold. When the SIP process CPU falls to the low threshold, OS-E increments the threshold by 16% if the average CPU is less than the low threshold and by 4% if less than the high watermark.

Audio Viewer — Audio Loss During Playback

The Archive Viewer may loose audio or video during playback if the RTP stream switches to a CODEC not supported by the Archive Viewer. (ID 9256)

Location-Cache Changes Not Taking Effect

If you edit the **location-call-admission-control** settings in the session configuration, the changes do not take effect after updating and saving the configuration. Any **location-call-admission-control** changes in the session configuration will require a **location-database flush** action for the new settings to take effect. (ID 10801)

Apply-To-Methods Settings

For REGISTER-based sessions and existing registered endpoints, if you edit the **apply-to-method** setting in the session configuration, the change does not take effect after updating and saving the configuration. Any **apply-to-method** change in the session configuration will require a **location-database flush** action for the new setting to take effect. (ID 11149)

H.323 Protocol

High availability support (call failover) is not supported. (ID 10966)

Identical SSH Host Keys

In order to secure access through SSH, Acme Packet recommends that you periodically run the new **ssh-regenerate** action to create unique SSH host keys on each platform running OS-E software. The action will initiate a cold restart of the system.

New software installations from USB sticks will automatically generate new and unique SSH host keys at installation time.

After running the **ssh-regenerate** action, some SSH clients may experience a problem when making a secure connection to the system.

Over Putty:

The SSH client will display a pop-up window with the message "WARNING - POTENTIAL SECURITY BREACH!" and explain that the server's host key does not match. Since the host key was changed, the correct action is to click **Yes** to begin the Putty session.

Over Linux-Based SSH:

The SSH client will display the following banner followed by a series of messages:

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

To correct this problem, review the series of messages and edit the file specified in the "Offending key in" line at the line number indicated. You can delete this line and then save the file. When the SSH client is run again, the new host key will be added to the known hosts file. (ID 10909)

Large Configurations with 4K VLANs or More

When running large configurations containing 4000 VLANs or more, OS-E may take several minutes to load at a system **restart,** or from other operations involving the configuration file, such as a **config replace.** Use the **cpu-monitor** action to observe CPU usage during configuration loading or any time while OS-E is running. When the CPU usages falls below 10%, the configuration has successfully loaded. (ID 10050)

Call Recording and File Mirroring Limits

When performing call recording and file mirroring, the system now caps the number of files at 50,000 to prevent an excessive number of stored records and overconsumption of system and memory resources. You should configure periodic maintenance (**services/tasks**) to remove old records at regular and scheduled intervals. Optionally, Acme Packet provides a software license that will allow you to increase the call recording and file mirroring capacity to 200,000 files. (ID 10036)

TFTP Servers

Configuring a TFTP server on a OS-E interface over UDP/TFTP port 69 may result in TFTP not working. For information on properly configuring a TFTP server, Acme Packet recommends that you run the WinAgents download from the following Web location.

http://www.winagents.com/en/solutions/tftp-over-firewall.php

(ID 10293)

Calling Group Address Limitation

In vsp/calling-groups/group, the **max-number-of-addresses** property sets the maximum number of AORs that can be associated with a calling group. However, currently only one AOR can be associated with a calling-group.

Licensed Features Display

When displaying features from the OS-E Managment System **Services->Features** page, fields that appear in the greyed-out state showing the default values currently being enforced cannot be edited from this page. This includes the “no royalty” CODECs and other licensed features.

The fields that appear greyed-out require the Acme Packet license update that includes the field(s) to be configurable. (ID 10496)

SIP Tracing During System Load

The OS-E tracing functions are designed to be used in short duration, isolated troubleshooting conditions. These tools should not be used when the system is under heavy SIP traffic load, and doing so may cause system deadlocks and crashes. This is a tool intended for use only with the assistance of Acme Packet. (ID 9875)

Outbound Local Port Setting

The session configuration **sip-settings/outboundLocalPort** property is not supported with the new tag routing feature in Release 3.3. (ID 8746)

Multiple Unique Media Streams

With some SIP phones, OS-E (with media anchoring enabled) may return two unique media streams, one disabled, and one accepted. This happens in cases where the SIP phones offer multiple media descriptions for alternate SRTP/clear RTP.
(ID 8899)

Alter-Contact Setting Overriding Sip-Settings/OutboundLocalPort

The **registration-plan/route alter-contact** property setting is currently overriding the session configuration **sip-settings/outbound-local-port** setting used for communicating with the peer. The **alter-contact** setting should only select a port if it is set to trunk-port-per-aor or trunk-port-per-binding. (ID 8749)

Local Enterprise Directory User Files

Local user files for XML and CSV directories, as well as introduction and periodic announcement files, should be stored in a folder under the OS-E-recognized directory named **/cxc_common**. If you place local user files in an unknown or unique directory, OS-E will not be able to locate users after you upgrade the device to the current release. (ID 5578)

SIP Sessions

- The SIP transport is currently missing a time-out setting for TLS and TCP connections. A connection is dropped only if the connection is terminated by the remote SIP client or SIP server.
- During the SIP call session, **disconnect-call** and **terminate-call** actions only operate in back-to-back mode and not in proxy mode.
- The condition-list associated with a policy rule is applied to the first SIP call session only.
- Session termination due to a media verification failure will not work when OS-E is operating in proxy mode. This includes voice and video calls created using Windows Messenger. Calls using Sametime or regular SIP phones are not affected. The **terminate-session** setting in the media verification object (vsp/media-verify-config <name>) contains the configuration setting.

EyeBeam Softphone with Rport Option Turned On

The EyeBeam softphone puts a contact address in the INVITE with a port that is different from where the INVITE is sent. Any requests within the dialog originating from the far end are sent to this contact address. This behavior is correct but the EyeBeam phone is ignoring the request in this case. (ID 8286)

Preventing Call Routing Loops

Forwarding loops can occur when a user agent (UA) registered over OS-E, in delegate or local mode, sends an INVITE to a delegate server, and then that delegate server sends the INVITE back to OS-E for further routing. In some cases, the INVITE from the delegate server might be destined for a UA that is also registered over OS-E. Administrators should ensure that if an INVITE is destined for the UA, that the INVITE matches an existing dial-plan, with the dial-plan **location-match-preferred** property set appropriately. Depending on your network routing, this tells OS-E about the order in which it should attempt a match with the **location-cache** rather than with the **dial-plan**.

A routing loop can also occur if OS-E forwards an INVITE to a delegate server, and that delegate server returns the INVITE to OS-E. In some cases, the inbound INVITE may match the same dial-plan, causing a routing loop where both OS-E and the delegate server continue to send INVITE sessions to each other for the same destination until the **max-forwards** property setting has expired to 0. This causes OS-E to allocate several hundred media ports (where OS-E is anchoring the call), quickly exhausting resources if several UAs are participating in the loop.

OS-E administrators can reduce the possibility of routing loops by performing the following tasks:

- Enable the **vsp/location-service/admission-control** to prevent an address-of-record (AOR) from placing more than **vsp/location-service/ max-concurrent-calls-per-AOR** setting for simultaneous calls.
- Enable the **vsp/location-service/emission-control** to prevent an AOR from receiving more than **vsp/location-service/max-concurrent-calls-per-AOR** setting for simultaneous calls.

These settings are only active when the **unregistered-sender-directive** is not set to *allow* for the AOR in question. The **unregistered-sender-directive** property must be set to *refuse* in the **vsp/enterprise/servers/sip-gateway** configuration. Setting the **unregistered-sender-directive** in the **pre-session-config** has no effect.

OS-E returns a “503 Server Unavailable “message to an INVITE if the AOR attempts to place more than the supported number of concurrent calls when these settings are enabled.

Additionally, if OS-E acts as a back-to-back user agent (B2BUA) between several user agents, routing loops may occur. In this configuration, OS-E forwards an INVITE to a server, and then that server sends it back to the OS-E device where OS-E again forwards the INVITE on to another server. In some cases, this may not be a routing loop but a valid routing configuration. OS-E administrators can prevent invalid routing loops by editing the **vsp/enterprise/servers/sip-gateway *name*/ loop-detection** property.

RADIUS Authentication and Server Priorities

If you set the **vsp/radius-group/authentication-mode** to *prioritized*, be sure to change the **vsp/radius-group/server** *priority* setting on any configured RADIUS group servers. All previously configured servers inherit the default value of 1. Without setting different priority values, OS-E randomly selects from these servers and ignores the prioritized mode. The system will generate an event indicating that multiple servers have the same priority.

Media Transcoding

- When performing transcoding, OS-E drops RTCP (regardless of the setting of the media **rtcp** property). OS-E records RTCP according to the session-config/ media/ **rtcp log** setting, but does not forward it since the transcoding may change the synchronization source (SSRC) of RTP along the way. If RTCP were forwarded, it may cause problems for endpoints because the stream described with RTCP may not match the RTP packets sent and received.
- When OS-E is transcoding, it changes the SSRC from the original RTP stream. Some phones do not respond well to an SSRC change in the middle of a call. This may occur when a phone changes from a CODEC that is passed through to a CODEC that is transcoded. (ID 7802)

Eyebeam Phones

Eyebeam softphones (Version 1.5.10.2 build 33793) do not play music-on hold generated by OS-E. (ID 7799)

Registration Plans and Registered States

In an LCS environment, a **registration-plan** must be configured to enable the location-cache to report an AOR in a registered state. Without a registration-plan, the AOR state will be declared as unregistered. The registration-plan must have a configured **route** with the **peer**, **action**, and **registration-throttling** settings configured. (For example, peer=LCS-server, action=tunnel, registration-throttling=no). (ID 8162)

CODEC Licensing

- If transcoding is configured with CODECs that require licenses and if a call is placed on hold without the available licenses, the call will be terminated. (ID 8206)
- In the OS-E Management System, some CODECs display a message saying they are "Available with upgrade." In fact, these CODECs are available, but the number of license seats, set at 200,000, is not configurable. This applies to the following CODECs: g728, g726-16, g726

SSH Session Limit Clarification

The SSH object **max-sessions** property sets the maximum number of concurrent SSH sessions allowed, enforced at the box level. The enforced value is an aggregate of the SSH session limits set on each IP interface that has SSH enabled. For example, to enforce a limit of five total SSH sessions per box, you could set IP "A" to an SSH session limit of two and IP "B" to an SSH session limit of three, for a total of five.

Call Failover

If you configure the fault-group so that a SIP process crash results in a VRRP failover, if the call-failover group is not set, and if the failed OS-E device is the call-failover master, the failover master-service is not transferred and the resulting call is lost. All active calls are deleted across all OS-E devices. (ID 7110)

Encryption of Fragmented RTP Packet

Currently, OS-E does not perform reassembly of fragmented RTP packets that require encryption. Because encryption requires the entire non-fragmented RTP packet, fragmented RTP packets are dropped. (ID 6462)

Eyebeam 1.5 Phone Disconnect

Performing Broadsoft session auditing on both legs of a SIP call will cause Eyebeam 1.5 phones running TLS/SRTP to disconnect. (ID 4700)

Rapid UDP Registrations and Maximum Sessions

When the **vsp\settings\max-number-of-sessions** property setting is reached, and with **vsp\call-admission-control** set to *disabled*, repeated error messages will occur if there are rapid UDP registrations consuming OS-E memory resources.

Use the **vsp\sip-timers\max-udp-session-linger** property to set the number of milliseconds that OS-E maintains a SIP session after its useful life is over. Enter a value from 0 to 60,000 milliseconds; the default setting is 30,000 ms (30 seconds). A value of 5 sets OS-E to remove the session 5 milliseconds after receipt/transmission of the first final response. (ID 5483)

NOTIFY Message From BroadSoft Server

If the **vsp\enterprise\servers\dns-group** is set with the **domain-port** property configured, or if the **local-port** is configured for an enterprise server, configure that port on all interfaces so that a SIP NOTIFY uses that port on the inbound call leg to the call destinations. Otherwise, the SIP NOTIFY will attempt to use a nonexisting local port and generate a “400 Bad Request” message back to the server on the trunk side of the network. (ID 5893)

OS-E Management System

- There will be a conflict the first time two users simultaneously open a OS-E configuration in the OS-E Management System (using the Configuration, Services or Access tab), and if one of the users does not make any changes or configuration updates before the other user. This problem will resolve itself after the first update without any actual configurations changes applied. However, there will be ongoing conflicts if the configuration contains a phantom directory. (ID 6182)
- The OS-E Management System is not supported over the Firefox Web browser. (ID 3506)
- In order for online help to display properly using Internet Explorer, you must be logged in to the OS-E Management System with an active session. The OS-E Management System is only supported over Internet Explorer, even though the default browser on your system may be different.
- After making any changes to the OS-E Web server configuration, such as changes made to the idle timeout and the connection protocol, and enabling and disabling the trap target, there may be a delay of three minutes while the Web server resets and allows the OS-E Management System to reconnect. Since there is a significant delay while the new settings are applied, the OS-E Management System user interface may be unresponsive if you attempt to perform other operations immediately after making changes to the Web server configuration. (ID 4052)

OS-E Actions Available at the NNOS-E> Prompt

The **set-call-forwarding** and **set-do-not-disturb** actions each show an optional cookie argument in the command line. The optional cookie argument is not supported for customer use. (ID 4180)

DHCP

DHCP is not currently implemented, even though you can configure DHCP using the OS-E Management System. (ID 4367)

Call Recording and Playback

- Recording of a video call will only record the audio portion of the call.

- After changing from an audio-only to audio & video call (and vice-versa), only the audio will be recorded.
- The call monitor-group "snoop" method does not function in this release. (ID 1100)
- Recorded calls cannot be played back using Windows Media Player V10.0 when the Web port is Port 443 (HTTPS). Windows Media Player only plays back recorded calls over Web port 80 (HTTP). As a workaround, use QuickTime instead of Windows Media Player, as QuickTime supports HTTPS. (ID 1732)

IM Management Policies

Message-to-sender and **message-to-recipient** text configured as part of an IM policy is not delivered as a separate IM message. The **message-to-recipient** text is prepended to the current message. The **message-to-sender** text is pre-pended to the next message going back to the sender. (ID 696)

Presence Database

In the **vsp/presence-database** object, the **repair-st-tags** and **force-un-subscribe** properties are available for debugging purposes only and are not intended for customer use. (ID 4618)

SMTP Archiving with Authentication

The password-tag and authentication functionality associated with SMTP archiving (**vsp\accounting\archiving\smtp-server**) is not currently supported. (ID 4521)

Policies

If you are using the header or content **sip-message-condition** properties, you must use the '(?s).' option at the beginning of the regular expression. For example, if you want to search for a user-agent RTC, use **`header match "(?s).*\bRTC/*\b".`** If you want to search for the media type in SDP, use **`content match "(?s).*\bm=video\b"`**

User and Group Filters

If you create a user or group filter under vsp/enterprise/directories, the filter will only take effect after a **directory-reset** action. (ID 2458)

LDAP and LDAP Authentication

- When you login to OS-E using SSH, it first asks you for a username and a password. This is the username/password combination of *root/sips* and not the LDAP username/password that you may have configured.
- Due to problems in the Java library, if an LDAP retrieval (import) of users fails, subsequent imports from other directories are not completed. This is a Java problem that will be fixed in a later JDK release. (ID 3300)

SNOM Phone Interoperability

- Certain random SRTP key values cause SNOM to play static or cause audio silence to the user. (ID 1587)
- SRTP with SNOM versions before v5.2 always produce static.

SRTP

Most RTCP implementations are still under development. If doing SRTP with an Eyebeam v1.5.6.1 or earlier, all RTCP packets requiring encryption (Sender and Receiver Reports) will be dropped. Since SNOM phones do not include authentication in RTCP packets, all SNOM RTCP Sender and Receiver Report packets are dropped. (ID 5206).

Linksys SRTP

In the **vsp/default-session-config/media** object, if you set the **rtcp** property to *pass*, OS-E will not send RTCP packets to endpoints in a Linksys SRTP configuration. (ID 6878)

Registration-Plan

The **location-service settings** object and the **registration-plan route** object both allow you to set the **max-bindings-per-AOR** property. Currently this value is set to 1 in settings and 0 (as-is) in route, and should not be changed.

Archiving

- If OS-E is configured for registration delegation (instead of handling registrations directly), and if archiving is enabled, SIP calls will be archived twice, with both archives containing the same information. (ID 2658)
- When configuring archiving based on the new **record-count** property in Release 3.1, calls made through a server (such as Asterisk) originate two records per call so that the number of records is twice the real number of calls. For example, if you configure the archive **record-count** to 100, archiving occurs at the 50th call because of the two records per call. (ID 5335)
- If using the **record-count** property to set the threshold that determines the number of accounting records to be written before the whole group is then archived, setting a value to 0 (the default), disables this feature. When set to any number greater than 0, the accounting software checks every 30 seconds to calculate whether the requisite number of records are waiting.

  Archiving only occurs when you invoke it specifically, as an action or as a scheduled text. Note that setting this property to any value other than 0 causes both the archive action and/or task to fail. Use this property with care, as the archiving function consumes system resources. (ID 5387, 5404)

Assigning a Management IP Address

Before you can configure the OS-E device remotely over the Internet using the OS-E Management System, or over a Telnet connection, you need to locally assign an IP address to one of the Ethernet interfaces, **eth0**, **eth1, eth2,** or **eth3.** If you are setting up the device remotely, you will also need to configure an IP route, a route to a destination host or network, and a gateway IP address.

If you are using the OS-E Management System, you will also need to know the assigned IP address on one of the Ethernet ports to manage the configuration. You access the OS-E Management System application running on the OS-E device over the Internet using the Internet Explorer Web browser.

The following CLI session creates and enables an IP interface named *mgmt-int***,** sets the static IP address and network mask, configures an IP route (if connecting remotely), and enables Web access on this IP interface. You will need to enable ICMP on the IP interface before you can use the **ping** command from your console to test the device as a responding node on the network. Use the **show -v** command to display the configuration.

CLI session

```
NNOS-E> config box
config box> set hostname localCXC
config box> config interface eth0
config interface eth0> config ip mgmt-int
Creating 'mgmt-int'
config mgmt-int> set admin enabled
config mgmt-int> set ip-address static 192.168.124.5/24
config mgmt-int> config routing
config routing> config route internetGateway
Creating 'route internetGateway'
config route internetGateway> set destination default
config route internetGateway> set gateway 192.168.124.3
config route internetGateway> return
config routing> return
config ip mgmt-int> config web
config web> set admin enabled
config web> set port 80
config web> return
config mgmt-int> config icmp
config icmp> set admin enabled
config icmp> top
config> save
config> show -v
```

Using the Setup Script

An optional configuration setup script called *cxc.setup* is included with OS-E software. After installing a new system, you can run the script directly from the NNOS-E> prompt, as shown in the example session below.

The script presents a set of questions to help you with the initial system configuration. The information in the script includes the following:

- Local hostname
- IP interface names and addresses
- SSH and Web access
- Default route and any additional static routes per interface for remote management
- User-defined CLI prompt

Every OS-E Series system has a minimum of two Ethernet interfaces. Any Ethernet interface can be used for management traffic, however, Acme Packet recommends the use of eth1, as eth0 is reserved for fault-tolerant clustering with other OS-E devices . Management traffic is also supported on any interface that is carrying private or public network traffic. This means that it would be possible to use eth1 to carry SIP traffic and management traffic.

CLI session

```
NNOS-E> config setup
set box\hostname: <name>
config box\interface: eth1
set box\interface eth1\ip a\ip-address: <ipAddress/mask>
config box\interface eth1\ip a\ssh (y or n)? y
config box\interface eth1\ip a\web (y or n)? y
config box\interface eth1\ip a\routing\route: <routeName>
set box\interface eth1\ip a\routing\route localGateway\gateway:
<ipAddress>
set box\cli\prompt: <newPrompt>
Do you want to commit this setup script (y or n) y
Do you want to update the startup configuration (y or n)? y
```

Note: The /cxc directory on the OS-E device may include vendor-specific scripts that address unique startup configuration requirements. Specify the name of the script on the command line following the **config setup** command. For example:

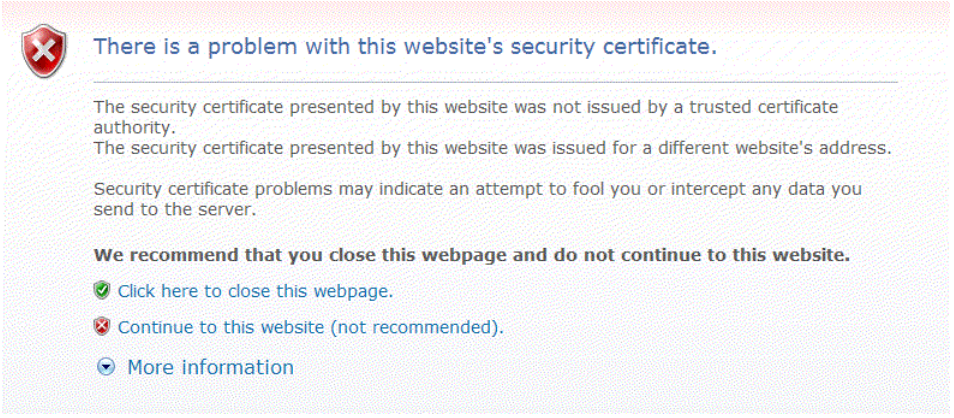
```
NNOS-E> config setup vendor.setup
```

Check the /cxc directory for any vendor-specific setup files included with your system.

Logging on Using the OS-E Management System

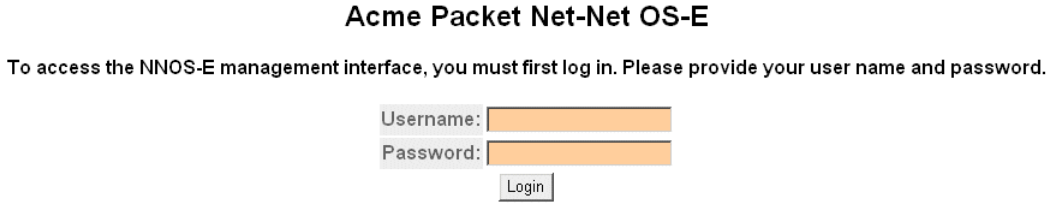
If you are using HTTPS (Port 443) to connect to the OS-E device (HTTPS://<ipaddress> from your Web browser), you will need to configure the Web service so that a valid SSL certificate is referenced at login time. Otherwise, your Web browser will display a screen similar to the following image, warning you of the security issues with the absence of an SSL certificate.

Security Certificate Warning



To proceed immediately to the OS-E Management System login page, select **Continue to this website**, as illustrated in the following image. Then, click **Login** to bypass the Username and Password prompts. Once you are logged in, you can configure usernames and passwords for access to this OS-E device using the **access\users\user** configuration path.

OS-E Log In Screen.



Acquiring and Configuring the Certificate

OS-E requires a signed SSL certificate from a valid Certificate Authority (CA), or you can use OS-E to create a self-signed certificate. The supported format for the certificate is PKCS#12, (Public Key Cryptography, standard #12 format).

For complete information on managing certificates, refer to the *Net-Net OS-E — System Installation and Commissioning Guide*.

Configuring the Web Service for HTTPS

Once you have installed a valid certificate, you will need to edit the OS-E **web-service** object to reference the certificate at OS-E Management System login time. This will remove the security certificate warning shown above. The following CLI session references the certificate over Port 443 using the **protocol** property under the **web-service** object.

CLI session

```
NNOS-E> config box
config box> config interface eth1
config interface eth1> config ip 172.26.2.14
Creating 'ip 172.26.2.14'
config ip 172.26.2.14> config web-service
config web-service> set protocol https 443 “vsp tls certificate
   company.pfx”
```

Building the Configuration File

The OS-E configuration file (*cxc.cfg*) is made up of configuration objects and property settings that control how the system processes and manages SIP traffic. As you open these objects and set properties using the CLI or the OS-E Management System, OS-E builds a configuration hierarchy of objects that are applied to SIP sessions. You can display this configuration hierarchy using the **show** and **show -v** commands.

For new users, as well as for users who are adding functionality to their configuration, you will need to open configuration objects using the **config** command to enable the default settings for those objects, even if you choose not to edit any of their associated properties. For example, if you need to enable the **ICMP** protocol and its default settings, you simply open the object and execute **return**, as shown in the session below. Notice that the ICMP object has been added to the configuration hierarchy at the end of the session on the eth4 interface.

```
config> config box interface eth4
config interface eth4> config ip 172.26.2.14
config ip 172.26.2.14> config icmp
config ip 172.26.2.14> return
config interface eth4> return
config box> return
config> show -v
    interface eth4
      admin enabled
      mtu 1500
      arp enabled
      speed 1Gb
      duplex full
      autoneg enabled
      ip 172.26.2.14
       admin enabled
       ip-address dhcp
       geolocation 0
       metric 1
       classification-tag
       security-domain
       address-scope
       filter-intf disabled
       icmp
        admin enabled
        limit 10 5
```

To remove an object from the configuration hierarchy, use the CLI or OS-E Management System **delete** command.

Creating Cluster Networks

If you are installing multiple OS-E devices in a high-availability cluster, refer to the *Net-Net OS-E — System Installation and Commissioning Guide* for information.

Installing OS-E Software Updates

Periodic OS-E software updates and patches are available to Acme Packet customers whenever software improvements and functionality changes enhance OS-E operation. System software updates are available from the Acme Packet Support Web site.

Getting Software from the Product Support Web Site

Using your Web browser, open your Acme Packet customer URL to access the Product Support Web site. Follow the instructions on your screen to download the software update to your PC or to a network location, then follow one of the procedures below to install the new OS-E software.

- Installation procedure using the CLI.
- Installation procedure using the OS-E Management System.

Installation Procedure Using the CLI

Once you have downloaded the OS-E release software, you can use the CLI to install the file on each OS-E device in the network. Use the **file fetch** command to get the file from its current location to the OS-E device.

The **file fetch** command accepts a large number of URL schemes that you can you use to fetch the release file. Use the **file fetch ?** command to display the file fetch command options. The CLI session below shows only those URL schemes that would be the most useful for file transfers.

CLI session

```
NNOS-E> file fetch ?

manage Net-Net OS-E files

 syntax: file erase file
```

```
          file fetch source-url [destination-file]
          file send source-file destination-url

ftp://             File Transfer Protocol (RFC 1738)
http://            Hypertext Transfer Protocol (RFC 2616)
https://           Hypertext Transfer Protocol Secure (RFC 2818)
gopher://          The Gopher Protocol (RFC 1738)
file://            Host-specific file names (RFC 1738)
ftps://            File Transfer Protocol Secure
                     (RFC-draft-murray-auth-ftp-ssl-16.txt)
tftp://            Trivial File Transfer Protocol (RFC 3617)
```

Refer to the RFC that applies to the URL scheme you are using for the exact formatting of the command line.

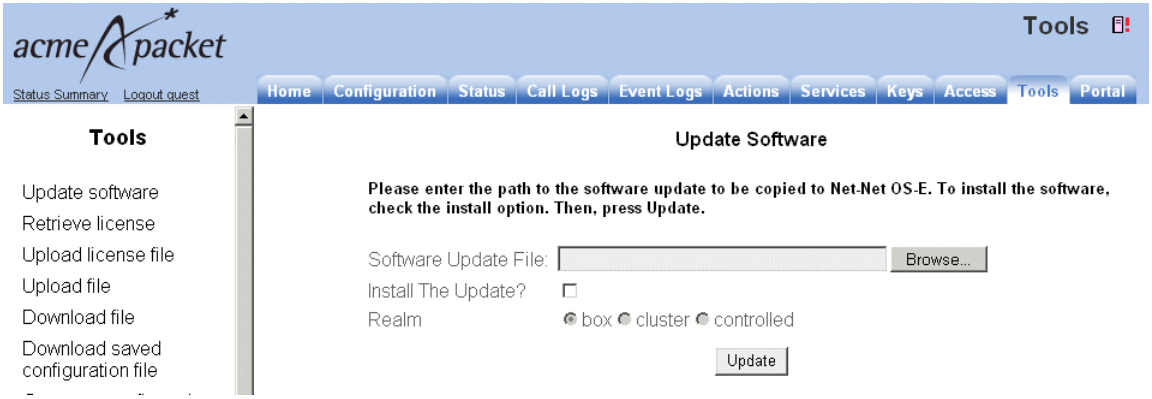
Installation Procedure Using the OS-E Management System

Once you have downloaded the OS-E software update from the Product Support Web site, use the OS-E Management System to install the software on the OS-E device. Perform the following steps:

1. Launch the OS-E Management System.
2. Click on the **Tools** tab, as shown in Figure 5.
3. Click **Update Software**.
4. At the “Software Update File” field, click **Browse** to locate the software release file on your PC, or enter the path and file name in the box.
5. At the “Install the Update?” field, check the box to install the software.
6. At the “Realm” field, check one of the option: **box**, **cluster**, or **controlled**. This instructs the upgrade software to operate on the local OS-E device (box), across the OS-E cluster, or in a controlled manner.

   Selecting **controlled** in a two system (active/standby) cluster configuration performs the cluster upgrade so that the currently active OS-E device continues to handle SIP traffic. Once the backup device has completed the software upgrade, it informs the active device that it is available to process calls. New SIP traffic then migrates to the backup device. When the active OS-E device is no longer processing calls, it becomes the backup device where the software update is applied.
7. Click **Update** to install the software and to restart the OS-E device.

8. Refresh your Internet Explorer Web browser by selecting **View->Refresh.**Update Software page



Information on OS-E Licensing

You are no longer required to run the **license fetch** command with newly-installed third-party hardware platforms to activate the features that you purchased. Your licensed features are included with your initial OS-E download. Refer to the *Net-Net OS-E — USB Creation and Commissioning Instructions* for complete information.

However, you will need to run **license fetch** under certain conditions, such as renewing an expired license, and when installing licensed features that you did not originally purchase with the system.

Adding Licensed Features

If you find that you do not have one or more of the features that you purchased, or if you want to add features that you did not originally purchase, contact your Acme Packet Sales Representative or Acme Packet Product Support. Acme Packet will correct the problem and supply you with a new key that operates with the **license fetch** command.

As OS-E software becomes available with newly-added features, your Acme Packet Sales Representative will assist you with ordering the software. Acme Packet will then provide you with a new licensing key.

License Expirations and Renewals

If your customer-specific license comes with an expiration date, OS-E will generate an event when the license nears that expiration date. You can renew your license by re-executing the **license fetch** command. The Acme Packet license server verifies that there is a valid license renewal associated with your system ID, and then resets the license expiration to a new date.

Evaluation Systems

For evaluation systems in lab environments without Internet connectivity, Acme Packet will provide you with an alternate method for acquiring the appropriate license to operate and configure OS-E. Contact your Acme Packet Sales Representative or Acme Packet Support for details.

License Fetch Procedure

Before you execute the **license fetch** command, ensure that

1. You have a connection to the public Internet, and
2. Port 616 is available and not blocked by any firewalls. This allows connectivity to the Acme Packet license server.

Note: If you do not run the **license fetch** command to successfully unlock your customer-specific features, you will not be able to configure OS-E with any of the licensed options provided by Acme Packet.

Fetching the Signed License from the CLI

From the CLI prompt, run the following command:

```
NNOS-E> license fetch <license-key-text>
Success!
```

Where **<license-key-text>** is the private key provided to you by Acme Packet. This command will contact the Acme Packet licensing server, authenticate your unique key, and then install a license on your system. Make sure that OS-E reports "Success!"

Note: If you are unable to fetch an encrypted license using the Acme Packet key, cannot access the licensing server, or if you receive a message other than "Success!,"contact Acme Packet Product Support immediately for assistance.

Fetching the Signed License from the OS-E Management System

If you are using the OS-E Management System, go the **Actions** tab and select **license->fetch** and paste the Acme Packet key into the key field, as illustrated in the following image. Click **Invoke** to install the signed license.

License Fetch Page

You can also manage licenses from the **Tools** tab using the **Retrieve License** and the **Upload License** functions. **Retrieve License** operates the same as the **license fetch** command, contacting the Acme Packet license server over the Internet.

If for some reason you are unable to access the Acme Packet license server, and if Acme Packet e-mails the license file to you, place the license on your local PC, use the OS-E Management System **Tools->Upload License file** to browse for the file, select **Apply License**, then click **Upload.**

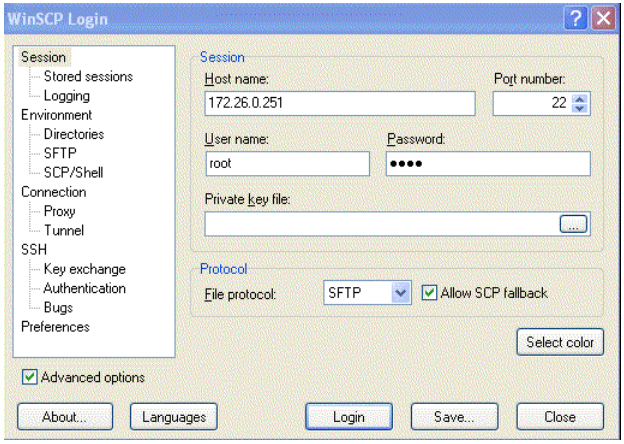
Using WinSCP to Transfer the License

If you do not have access to the OS-E Management System, Acme Packet recommends that you use WinSCP to transfer the license file to the OS-E device. WinSCP is an open source free SFTP client and FTP client for Windows and is available as a free download from the following URL:

http://winscp.net/eng/index.php

The following image illustrates the WinSCP login window.

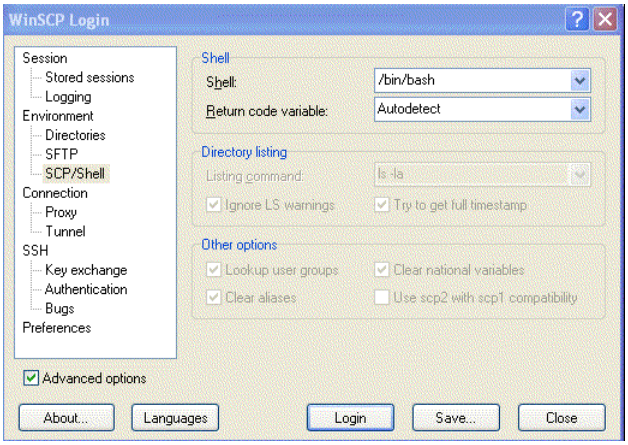
WinSCP Login



Perform the following steps:

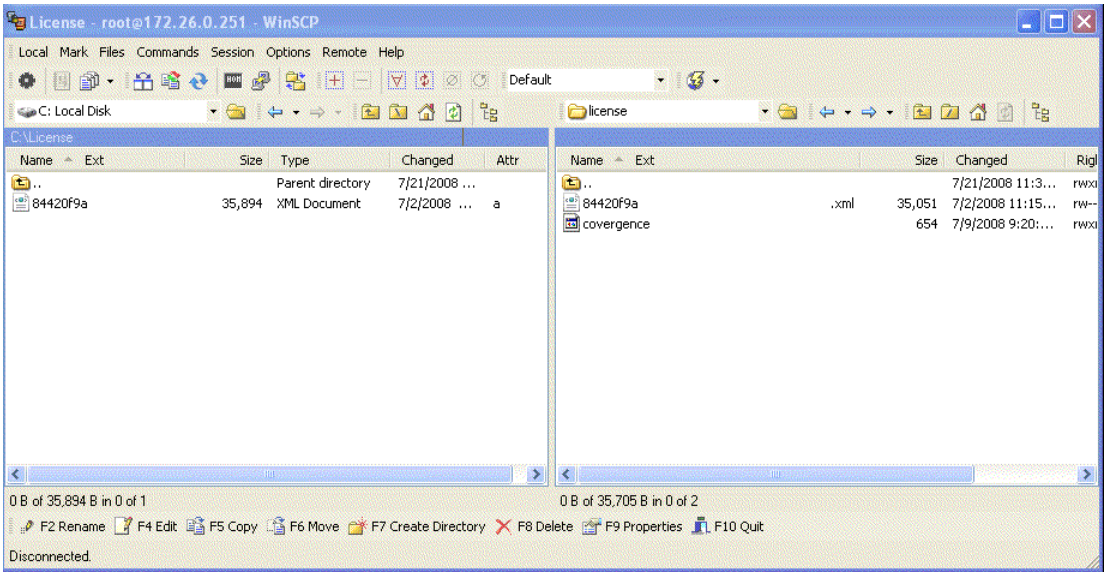
1. At the **Hostname** field, enter the IP address that you assigned to the management interface at OS-E device. Port **22** is the default port number for SSH sessions.
2. At the **Username** and **Password** fields, type *root* for the username and *sips* for the password.
3. At the Environment menu, select **SCP/Shell** and select **/bin/bash** from the pull-down menu, as illustrated in the following image. Leave all other fields at their default settings.

WinSCP Login SCP/Shell Window



4. Click **Login**. A series of progress message will appear as the connection is established.
5. From the left pane, browse and locate the license file, then drag the license to the *cxc/license* directory, as illustrated in the following image. In this example, the file is copied from the **c:\license** directory to the **cxc\license** directory on OS-E.

Using WinSCP to Copy the License to OS-E



6. Once the license file is present in the /cxc/license folder, you will need to do one of the follow tasks for the OS-E license to take effect:

   - Perform a physical restart of the OS-E device, or
   - From a CLI session to the OS-E device, execute the **license apply** action, as follows:

```
NNOS-E> license apply /cxc/license/
84420g9a-da13-3007-8853-z00a7a4d771d.xml
Success!

NNOS-E> show licenses

name: License for customer.com
description: License for customer.com
        key: 84420g9a-da13-3007-8853-z00a7a4d771d
    expires:
       file: 84420g9a-da13-3007-8853-z00a7a4d771d.xml
```

Interoperating with SIP Vendors

OS-E devices are designed to interoperate with SIP servers, hosted SIP applications, and SIP PBX equipment for VoIP applications.

Contact your Acme Packet sales representative for a complete list of SIP vendors who interoperate with OS-E software.

Downloading Optional Management Files

If you are using an SNMP management application, use the OS-E Management System to download the CXC.MIB (Acme Packet OS-E Enterprise MIB) file from the OS-E software release:

Perform the following steps:

1. Launch the OS-E Management System.
2. Click on the **Tools** tab.
3. At the Management Information section, click **MIB** to download the file to your Web browser.
4. Use the **Save** command from your browser to save a copy of the file. Import the CXC-MIB file into the SNMP management application.

CDR Field Descriptions and Data Types

The following table lists and describes the fields and data types that make up a call detail record in this release.

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
session-id	type="uint64" format="hex" key="index"	type=”int8”	**NUMBER**	The unique session identifier in hexadecimal format, unassigned 64-bit integer.
recorded	type="Boolean"	type=”int4”	**NUMBER**	The true or false indication as to whether the SIP call was recorded.

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
call-id	type="String"	type-”name”	**VARCHAR2 (256) (256)**	The unique call identifier of the inbound call leg.
to	type="String"	type=”name”	**VARCHAR2 (256) (256)**	The string in the To URI: field of the SIP header.
from	type="String"	type=”name”	**VARCHAR2 (256)**	The string in the From URI:field of SIP header.
method	type="String”	type=”name”	**VARCHAR2 (256)**	The SIP method, such as INVITE or REGISTER, that initiated the call session.
incoming-request-uri	type="String”	type=”name”	**VARCHAR2 (256)**	The Request URI on the inbound call leg.
previous-hop-ip	type="IPHost"	type=”int4”	**NUMBER**	The IP address of the previous hop; the last network node handling the call before received at the OS-E device.
previous-hop-via	type="String"	type=”name”	**VARCHAR2 (256)**	The VIA header from the previous hop.
outgoing-request-uri	type="String"	type=”name”	**VARCHAR2 (256)**	The Request URI on the outbound leg.
next-hop-ip	type="IPHost”	type=”int4”	**NUMBER**	The IP address of the next hop; the next network node handling the call forwarded by the OS-E device.
next-hop-dn	type="String"	type=”name”	**VARCHAR2 (256)**	The fully qualified domain name (FQDN) or IP address of the next network node handling the call forwarded by the OS-E.
header	type="String"	type=”name”	**VARCHAR2 (256)**	An arbitrary header associated with the SIP call.
origin	type="String"	type=”name”	**VARCHAR2 (256)**	The ORIGIN header associated with the SIP call.
setup-time	type="Time" key="index"	type= ”timestamp”	**TIMESTAMP**	The time at which the SIP was set up at the OS-E in the format *hour:minutes:seconds.milliseconds: weekday year-month-day.*

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
connect-time	type="Time"	type= ”timestamp”	**TIMESTAMP**	The time at which the SIP was connected to the SIP call destination in the format *hour:minutes:seconds.milliseconds: weekday year-month-day.*
disconnect-time	type="Time"	type= ”timestamp”	**TIMESTAMP**	The time at which the SIP was disconnected from the SIP call destination in the format *hour:minutes:seconds.milliseconds: weekday year-month-day.*
disconnect-cause	type=“DisconnectType"	type=”int4”	**NUMBER**	The reason for the call disconnection, such as BYE.
duration	type=”uint32”	type=”int4”	**NUMBER**	Duration of the call in seconds.
scp-name	type="String"	type=”name”	**VARCHAR2 (256)**	The OS-E virtual system partition (VSP) that handled the call.
call-id-2	type="String"	type=”name”	**VARCHAR2 (256)**	The secondary call identifier for the outgoing leg.
origGW	type=”String”	type=”name”	**VARCHAR2 (256)**	The name of the originating gateway associated with the call.
termGW	type-”String”	type=”name”	**VARCHAR2 (256)**	The name of the gateway where the call was terminated.
packets-received-on src-leg	type="uint32"	type=”int4”	**NUMBER**	The total number of packets received on the inbound call leg.
packets-lost-on-src-leg	type="uint32"	type=”int4”	**NUMBER**	The total number of packets lost on the inbound call leg.
packets-discarded-on-src-leg	type="uint32"	type=”int4”	**NUMBER**	The total number of packets discarded on the inbound call leg.
pvd-on-src -leg	type="uint32"	type=”int4”	**NUMBER**	The packet delay variation (jitter) associated with the call on the inbound call leg.
max-jitter-on-src-leg	type="uint32"	type=”int4”	**NUMBER**	The maximum jitter on the source leg.
codec-on-src-leg	type="String"	type=”name”	**VARCHAR2 (256)**	The CODEC associated with the inbound call leg.

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
mimetype-on-src-leg	type="String"	type=”name”	**VARCHAR2 (256)**	The MIME type associated with the inbound call leg, such as audio/pcmu.
latency-on-src-leg	type="uint32"	type=”int4”	**NUMBER**	The total processing time of the inbound call leg.
max-latency-on-src-leg	type="uint32"	type=”int4”	**NUMBER**	The maximum latency on the inbound call leg.
rfactor-on-src-leg	type="uint16” or type=”uint32”	type=”int4”	**NUMBER**	The R-factor integer used in the MOS score compilation on the inbound call leg.
packets-received-on-dest-leg	type="uint32"	type=”int4”	**NUMBER**	The total number of packets received on the outbound call leg.
packets-lost-on-dest-leg	type="uint32"	type=”int4”	**NUMBER**	The total number of packets lost on the outbound call leg.
packets-discarded-on-dest-leg	type="uint32"	type=”int4”	**NUMBER**	The total number of packets discarded on the outbound call leg.
pvd-on-dest-leg	type="uint32"	type=”int4”	**NUMBER**	The packet delay variation (jitter) associated with the call on the outbound call leg.
max-jitter-on-dst-leg	type="uint32"	type=”int4”	**NUMBER**	The maximum jitter on the destination leg.
codec-on-dest-leg	type="String"	type=”name”	**VARCHAR2 (256)**	The CODEC associated with the outbound call leg.
mimetype-on-dest-leg	type="String"	type=”name”	**VARCHAR2 (256)**	The MIME type associated with the outbound call leg, such as audio/pcmu.
latency-on-dest-leg	type="uint32"	type=”int4”	**NUMBER**	The total processing time of the outbound call leg.
max-latency-on-dst-leg	type="uint32"	type=”int4”	**NUMBER**	The maximum latency on the destination leg.
rfactor-on-dest-leg	type="uint16”	type=”int4”	**NUMBER**	The R-factor integer used in the MOS score compilation on the destination call leg.

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
rfactor-on-dest-leg-times-1000	type-”uint32”	type=”int4”	**NUMBER**	The R-factor integer * 1000 this is used in the MOS score compilation on the destination call leg.
rfactor-on-src-leg-times-1000	type-”uint32”	type=”int4”	**NUMBER**	The R-factor integer * 1000 this is used in the MOS score compilation on the inbound call leg.
mos-fmt-dest-leg	type="String"	type=”name”	**VARCHAR2 (256)**	The formatted MOS calculation on the oubound call leg. See the *Net-Net OS-E — Session Services Configuration Guide* for more information.
mos-fmt-on-src-leg	type="String"	type=”name”	**VARCHAR2 (256)**	The formatted MOS calculation on the inbound call leg. See the *Net-Net OS-E — Session Services Configuration Guide* for more information.
mos-on-dest-leg	type="uint32"	type=”int4	**NUMBER**	The MOS calculation * 1000 on the oubound call leg. See the *Net-Net OS-E — Session Services Configuration Guide* for more information.
mos-on-src-leg	type="uint32"	type=”int4	**NUMBER**	The MOS calculation * 1000 on the inbound call leg. See the *Net-Net OS-E — Session Services Configuration Guide* for more information.
call-type	type="String"	type=”name”	**VARCHAR2 (256)**	The type of call, such as IV for Inbound Voice.
disconnect-error-type	type="String"	type=”name”	**VARCHAR2 (256)**	The type of error that caused the disconnection.
ani	type="String"	type=”name”	**VARCHAR2 (256)**	The caller ID for the ANI after any manipulation is done by the OS-E.
call-source-regid	type="String"	type=”name”	**VARCHAR2 (256)**	The server name if available, or user portion of the From: URI.
call-dest-regid	type="String"	type=”name”	**VARCHAR2 (256)**	The server name if available, or user portion of the To: URI.

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
new-ani	type="String"	type=”name”	**VARCHAR2 (256)**	The caller ID for the ANI after any manipulation is done by the OS-E.
cdr-type	type="String"	type=”name”	**VARCHAR2 (256)**	The call record type, either START or STOP.
hunting-attempts	type="uint32"	type=”int4”	**NUMBER**	The number of times the OS-E used the arbiter to select a dial-plan and a failure occurred (including subsequent attempts).
call-pdd	type="uint32"	type=”int4”	**NUMBER**	The post dial delay between the initial INVITE and the 180/183 RINGING.; calculated in msec.
call-source-realm-name	type="String"	type=”name”	**VARCHAR2 (256)**	The source domain name from which the call was received.
call-dest-realm-name	type="String"	type=”name”	**VARCHAR2 (256)**	The destination domain name to which the call was forwarded.
call-dest-cr-name	type="String"	type=”name”	**VARCHAR2 (256)**	The name of the dial plan that forwarded the call.
in_peer_dst	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port of the destination phone to which the OS-E forwarded the inbound call leg. (See the *Net-Net OS-E — Session Services Configuration Guide*, Appendix B, for more information.)
in_anchor_ src	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port at the OS-E where the inbound call leg was forwarded to the destination peer. (See the *Net-Net OS-E — Session Services Configuration Guide*, Appendix B, for more information.)
in_anchor_ dst	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port at the OS-E where the inbound call leg was received from the source peer. (See the *Net-Net OS-E — Session Services Configuration Guide*, Appendix B, for more information.)

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
in_peer_src	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port of the source phone that contacted the OS-E over an inbound call leg. (See the *Net-Net OS-E — Session Services Configuration Guide*, Appendix B, for more information.)
out_peer_dst	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port of the destination phone to which the OS-E forwarded the outbound (return) call leg. (See the *Net-Net OS-E — Session Services Configuration Guide*, Appendix B, for more information.)
out_anchor_ src	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port at the OS-E where the outbound call leg was forwarded back to the source peer. (See the *Net-Net OS-E — Session Services Configuration Guide*, Appendix B, for more information.)
out_anchor_ dst	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port at the OS-E where the outbound (responding) call leg was received from the destination peer. (See the *Net-Net OS-E — Session Services Configuration Guide*, Appendix B, for more information.)
out_peer_src	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port of the responding destination phone from which an outbound call leg was returned to the OS-E. (See the *Net-Net OS-E — Session Services Configuration Guide*, Appendix B, for more information.)
called-party-after-src-calling-plan	type="String"	type=”name”	**VARCHAR2 (256)**	The called party number after any manipulation on leg 1, but before any manipulation on leg 2.
last-status-message	type="uint16”	type=”int4”	**NUMBER**	An integer indicating SIP message type last status message (omitting “200 OK”) and therefore call progress.

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
last-pkt-timestamp-on-dest-leg	type=”Time”	type= ”timestamp”	**TIMESTAMP**	The time of the last media packet on the destination leg.
last-pkt-timestamp-on-src-leg	type= “Time”	type= ”timestamp”	**TIMESTAMP**	The time of the last media packet on the source leg.
setup-time-integer	type=”uint64”	type=”int8”	**NUMBER**	The call setup time indicated as an integer.
incoming-uri-stripped	type=”String”	type=”name”	**VARCHAR2 (256)**	The stripped down version of the incoming request URI.
dnis	type=”String”	type=”name”	**VARCHAR2 (256)**	Dialed Number Identification Service
newDnis	type=”String”	type=”name”	**VARCHAR2 (256)**	New Dialed Number Identification Service
custom-data	type=”String”	type=”name”	**VARCHAR2 (256)**	Custom data field as defined by the **accounting-data** object.
creation-timestamp	type= “Time”	type= ”timestamp”	**TIMESTAMP**	The time the accounting record was written to the accounting target.

New Event Log Messages

This section lists the new events under each category for Release 3.6 versions. For a complete listing of event messages, refer to *Net-Net OS-E — Using the OS-E Management Tools*.

Accounting Events

Event Name	Severity	Displayed Text
process_accounting_request	debug	Processing accounting request for %s: CDR file range %s/%s - %s/%s
accounting_response	debug	Sending accounting response '%s' for '%s': Last CDR: %s/%s
badfield	error	Illegal field for report %s: %s
badmatch	error	Illegal match expression for report %s
secret_failure	error	Failed to get secret for server %s, %s Target '%s' failed to send file %s to %s
file_send_failed	error	Target '%s' failed to send file %s to %s (try %d, records %llu to %llu), error is '%s', retrying in %u:%02u minutes
target_register_failed	error	Target '%s' failed to register with accounting server (%s)
target_unregister_failed	error	Target '%s' failed to unregister with accounting server (%s)
file_send_failed_final	error	Target '%s' failed to send file %s to %s (try %d, records %llu to %llu), error is '%s'
save_failed	error	Target '%s' failed to process CDR %s, error is '%s'
flush_failed	error	Flush action for target '%s' failed, error is %s.
reapply_failure	error	Target '%s' failed to process reapply action, reason: %s, CDR file range: %s/%s - %s/%s
unreachable	error	Target '%s' is not reachable
missing_records	error	Target '%s': Records %s to %s are missing, maybe due to a purge
duration_negative	error	Call duration calculated to be %d seconds
disconnect_time_invalid	error	Disconnect time %s prior to Connect Time %s
target_register_success	info	Target '%s' registered with accounting server
target_unregister_success	info	Target '%s' unregistered with accounting server
rollover_filesystem	info	Rolling over. Target '%s' wrote %llu record(s) in file %s (records %llu to %llu)

Event Name	Severity	Displayed Text
rollover_filesystem_zero	info	Rolling over. Target '%s' did not receive any records. File %s is not created
file_sending	info	Target '%s' sending file %s to %s (try %d, records %llu to %llu). File has %llu records
purgestart	notice	Performing a purge on %s, for records prior to '%s'
purgecomplete	notice	Completed a purge on %s, %u record(s) deleted
purgeerror	notice	Error during purge on %s: %s
file_send_success	notice	Target '%s' successfully sent file %s to %s (try %d, records %llu to %llu). File has %llu record(s)
purge_output_file	notice	Purged %s, last modified at %s
purgestart_filesystem	notice	Performing a purge for target '%s' on %s, for files prior to '%s'
purgecomplete_filesystem	notice	Completed a purge for target '%s' on %s, %llu file(s) deleted
purgeerror_filesystem	notice	Error during purge on %s: %s, target '%s'
flush_not_handled	notice	Target '%s' does not handle flush action
flush_handled	notice	Target '%s' is handling flush action
flush_externalfs_nothing_to do	notice	Target '%s' has nothing to do for flush. Target has nothing to rollover and is not waiting to resend
reapply_handled	notice	Target '%s' is handling reapply action
reapply_success	notice	Target '%s' successfully processed reapply action, CDR file range: %s/%s - %s/%s
reachable	notice	Target '%s' is reachable.
reconfig	notice	Handling reconfiguration with respect to '%s' changes
flush_fs_config_nothing_to do	notice	Target '%s' is processing a config change and will not handle flush. Retry later
reapply_fs_config_nothing_ todo	notice	Target '%s' is processing a config change and will not handle reapply. Retry later
flow_on	notice	Handling flow ON request, current state is %s time: %s.

Event Name	Severity	Displayed Text
flow_off	notice	Handling flow OFF request, current state is %s time: %s
cli_flow_on	notice	Handling CLI flow ON request, current state is %s
cli_flow_off	notice	Handling CLI flow OFF request, current state is %s
processed_flow_on	notice	Processed flow ON. Latest state is %s
processed_flow_off	notice	Processed flow OFF. Latest state is %s
sync_flow_control	notice	Re-synchronizing internal flow control at startup to %s, current state is %s
diskfull	warning	Device for %s is %u%% full...performing a purge
files_left	warning	Target '%s' is deleted. Files more recent than %d day(s) need to be purged manually from %s

Archive Events

Event Name	Severity	Displayed Text
mix_problem	error	Problem mixing session %s: %s
archive_create_error	error	Create archive error. Thread=%d, %s, start/ end free memory=%s. %s

Cluster Events

Event Name	Severity	Displayed Text
missing_intf	error	No cluster interface found - mark box %d as disabled

Collection Events

Event Name	Severity	Displayed Text
error	error	%s
failure	error	Collect action failed: %s
progress	info	%s
invoked	warning	Collect action invoked with the following arguments: \n%.*s\n
success	warning	Collect action succeeded after %d.%03d seconds; file ‘%s’ is %u bytes

DIAMETER Events

Event Name	Severity	Displayed Text
watchdog	error	group %s peer %s has not responded to %u consecutive watchdog messages; disconnecting

H.323 Failed Call Events

Event Name	Severity	Displayed Text
callcrit	crit	Desc: %s, Error: %s
callerror	error	Desc: %s, Error: %s
failedcallhistory	error	[call %p %s] %s
callinfo	info	Desc: %s

H.323 Process Events

Event Name	Severity	Displayed Text
heartbeat	crit	%s, last known healthy time %u, current time %u
invalidip	error	%s ip: %s, intf: %s, transport: %s, port: %u

H.323 RAS Events

Event Name	Severity	Displayed Text
raserror	error	GK: %p Error: %s - %s
rasinfo	info	GK: %p - %s - %p
listeninfo	info	GK: %p Listener: %p - %s
raswarning	warning	GK: %p Warning: %s - %s
gkstartstop	warning	GK: %p State: %s - % - Caller %p

Install Events

Event Name	Severity	Displayed Text
debug	debug	%s
entry	info	%s

Kernel Events

Event Name	Severity	Displayed Text
adding	debug	%u: adding: %s
added	debug	%u: added
addFailed	debug	%u: add-failed
MXadded	debug	%u: MX-added %s/%s
MXaddFailed	debug	%u: MX-add-Failed %s/%s
changing	debug	%u: changing
changed	debug	%u: changed
changeFailed	debug	%u: change-failed
MXchanged	debug	%u: MX-changed %s/%s
MXchangeFailed	debug	%u: MX-change-failed %s/%s
deleting	debug	%u: deleting
deleted	debug	%u: deleted
deleteFailed	debug	%u: delete-failed
MXdeleted	debug	%u: MX-deleted %s/%s
MXdeleteFailed	debug	%u: MX-delete-failed %s/%s

Load-Balancing Events

Event Name	Severity	Displayed Text
if_self	error	Interface %s (%s) is configured to be its own backing interface; interface will be ignored
if_disabled	info	Interface %s (%s) is configured as a backing interface to %s (%s), but is disabled, and thus will not be used
backing_removed	notice	Interface %s has been removed as a backing interface to head-end interface %s

LCR Events

Event Name	Severity	Displayed Text
all_done	debug	All done. No file to load
operation_started	debug	*** Operation started, caller %p
operation_ended	debug	*** Operation ended, caller %p
routeset_load_failed	error	Failed to load route-set from %s: %s
action_failed	error	Action \'%s\' failed with error: %s.
routeset_read_failed	error	Failed to read %s: %s
file_get_failed	error	Failed to get %s from route-server master: %s
backup_delete_failed	error	Failed to delete route set %s on box %u: %s
invalid_entry	error	Invalid entry found in file %s while importing: %s
propagate_failed	error	Failed to update %s: %s
cancel_peer_unresponsive	error	Rolling back operation because peer %s did not respond in %u tries
action_success	info	Action \'%s\' succeeded.
scheduled_activate_execute	info	Activate scheduled for %s is executing
slave_report	info	%s gets peer report %s
wait_status	info	Notify from box %u; waiting for %u more
wait_start	info	Wait for %s for 20 secs, try %u (%s!)
save_state	info	Save state: box %s -> (%s, %s)
master_request	info	%s gets Master request %s %s %s
report_to_master	info	Report to master: box %s -> (%s, %s)
master_request_nothing_to_do	info	Master request %s: Nothing to do
routeset_load_success	notice	Loaded %u routes from %s
master_stop	notice	Switching to route-server slave mode
master_start	notice	Switching to route-server master mode
activate_scheduled	notice	Activate for new route set %s is scheduled for %s
routeset_read_success	notice	Read %u entries from %s. Time taken is %s

Event Name	Severity	Displayed Text
file_get_success	notice	Fetched %s of size %u. Time taken is %s
backup_delete_success	notice	Deleted backup route set %s
activated	notice	Activated new route set %s with %u routes
wait_start_summary	notice	Waiting for %u peers
loading	notice	Loading %s
pulling_file	notice	Pulling file %s from master
file_overwrite	notice	File %s activated at %s of size %u bytes is being overwritten by file of same name with size %u bytes
file_exists	notice	Processing %s available locally since name and size of file in new request matches. Size is %u bytes
ignore_peer_response	notice	Ignoring response from peer %u since we were not waiting for a response
member	notice	Box is a route-server host. Sending notification
not_member	notice	Box is no longer a route-server host. Sending notification
wait_for_peer_success	notice	Wait for %s (box %u) for %u secs, try %u
wait_for_peer_failed	notice	Wait for %s (box %u) for %u secs, try %u failed. (%s)
file_backed_up	notice	File %s (%u routes, %u bytes, activated at %s) is replaced by active file %s. Old file %s is backed up in %s
peer_unresponsive	warning	Peer %s did not respond in try %u

LCR Import Events

	Severity	Displayed Text
did_import_db_failure	error	Failed to commit DIDs to database (initiated by %s): %s
did_import_error	error	Perform import DIDs error: %s
did_purge_failure	error	Failed to purge DIDs (initiated by %s): %s
did_purge_template_error	error	Failed to purge DID templates (initiated by %s): %s
did_restore_failure	error	Failed to restore DIDs from file %s (initiated by %s), too many errors
did_restore_error	error	Restore DIDs from file %s (initiated by %s) error: %s
did_backup_failure	error	Failed to back up DIDs (initiated by %s). 0 records were backed up
did_backup_error	error	Failed to back up DIDs (initiated by %s) due to error: %s
did_edit_error	error	Failed to edit DID from (%s) to (%s), initiated by %s: %s
did_delete_error	error	Failed to delete DID (%s), initiated by %s
update_server_error	error	Failed to update server %s (initiated by %s): %s
update_revert_server_error	error	Failed to update (revert) server %s (initiated by %s): %s
rates_import_db_failure	error	Failed to commit Rates to database initiated by %s): %s
rates_import_error	error	Perform import rates error: %s
rates_purge_failure	error	Failed to purge Rates (initiated by %s): %s
rates_purge_templates_failure	error	Failed to purge Rate Templates (initiated by %s): %s
rates_restore_failure	error	Failed to restore Rates (initiated by %s), too many errors. filename=%s
rates_backup_failure	error	Restore Rates (initiated by %s) from file (%s) error: %s
rates_backup_error	error	Filed to backup Rates (initiated by %s) due to error: %s

	Severity	Displayed Text
intralate_rates_import_failure	error	Failed to import Intra LATA Rates. Action initiated by %s
lata_rates_import_failure	error	Failed to import LATA Rates to NPA.NXX. Action initiated by %s
regioncode_import_failure	error	Failed to import Region Code to Dial Code. Action initiated by %s
db_failed_create	error	Failed to create internal database: %s
data_loading_error	error	%s
region_import_failure	error	Failed to import region code from file %s (initiated by %s). %s
lata_import_failure	error	Failed to import LATA from file %s (initiated by %s). %s
no_crypto	error	No crypto store is provided for authentication
no_crypto_password	error	No crypto store password is provided for authentication
start	info	The LCR Import service started
stop	info	The LCR Import service stopped
web_start	info	Web server started
web_start_failed	info	Web server failed to start
web_stop	info	Web server stopped
did_import_db_start	info	Import DIDs to database started (initiated by %s)
did_import_db_success	info	Successfully imported DIDs to database (initiated by %s). %s
did_purge_start	info	Purge DIDs started (initiated by %s).
did_purge_success	info	Successfully purged DIDs (initiated by %s); purged %d records
did_purge_template_start	info	Purge DID templates started (initiated by %s).
did_purge_template_success	info	Successfully purged DID templates (initiated by %s); purged %d records
did_restore_start	info	Restoring DIDs started (initiated by %s).
did_restore_success	info	Successfully restored DIDs from file %s (initiated by %s). %s
did_backup_start	info	Backup DIDs started (initiated by %s).

	Severity	Displayed Text
did_backup_success	info	Successfully backed up DIDs (initiated by %s). %s
did_edit_success	info	Successfully updated DID (initiated by %s) from (%s) to (%s).
did_delete_success	info	Successfully deleted DID (%s), initiated by %s
did_generate_success	info	Successfully generated DIDs (initiated by %s). %s
update_server_success	info	Successfully updated server %s (initiated by %s), %d records inserted; used SSH for copying (%s)
update_revert_server_success	info	Successfully updated (revert) server %s (initiated by %s), %d records inserted; used SSH for copying (%s)
rates_import_db_start	info	Import Rates to database started (initiated by %s).
rates_import_db_success	info	Successfully imported Rates to database (initiated by %s). %s
rates_purge_start	info	Purge Rates started (initiated by %s).
rates_purge_success	info	Successfully purged Rates (initiated by %s); purged %d records
rates_purge_templates_start	info	Purge Rate templates started (initiated by %s).
rates_purge_templates_success	info	Successfully purged Rate Templates (initiated by %s); purged %d records
rates_restore_start	info	Resting Rates started (initiated by %s).
rates_restore_success	info	Successfully restored Rates (initiated by %s) from file (%s). %s
rates_backup_start	info	Backup Rates started (initiated by %s).
rates_backup_success	info	Successfully backed up Rates (initiated by %s). %s
intralata_rates_import_success	info	Successfully imported Intra LATA Rates. Action initiated by %s
lata_rates_import_success	info	Successfully imported LATA Rates to NPA.NXX. Purged existing records (%s). Action initiated by %s

	Severity	Displayed Text
regioncode_import_success	info	Successfully imported Region Code to Dial Code. Purged existing records (%s). Action initiated by %
db_ready	info	Internal database: %s is ready for use
data_loading_status	info	%s
login	info	%s login
logout	info	%s logout
region_import_success	info	Successfully imported region code from file %s (initiated by %s). %s
lata_import_success	info	Successfully imported LATA from file %s (initiated by %s). %s
did_import_cancel	warning	%s canceled Import DIDs
did_import_stop	warning	Stopped import DIDs, too many failures
rates_import_cancel	warning	%s canceled Import Rates
rates_import_stop	warning	Stopped import Rates, too many failures
login_failure	warning	%s login failure. %s

Management Events

Event Name	Severity	Displayed Text
actionexecinternal	debug	‘%s’ action executed internally: %s
changeproperty	info	‘%s\\%s’ changed by %s via %s: %s
changepropertyanon	info	‘%s\\%s’ changed: %s
changeconfig	notice	‘%s’ configuration changed by %s via %s
changeconfiganon	notice	‘%s’ configuration changed
actionexec	notice	‘%s’ action executed by %s via %s: %s
actionexecanon	notice	‘%s’ action executed: %s

Media Events

Event Name	Severity	Displayed Text
ignored_dtmf	error	Session %llx, leg %u dropped DTMF event-id=%u: last event only started %u msecs ago (%u msec minimum)

Messaging System Events

Event Name	Severity	Displayed Text
session_attach_socket	error	session %s already has socket handle %p attached - caller %p
session_create	info	Session %s (%s) (handle %p) created by %p, %p
session_destroy	info	Session %s (%s) (handle %p) destroyed by %p, %p
cluster_notice	notice	Box %s notice: %s (%u successes, %u errors)
box_created	warning	Box %s (handle %p) has been created by %p: %s
box_destroyed	warning	Box %s (handle %p) has been destroyed by %p: %s

Event Name	Severity	Displayed Text
socket_attach	warning	Session %s (handle %p) gets socket %d (handle %p) from %p
socket_detach	warning	Session %s (handle %p) loses socket %d (handle %p) from %p
socket_error	warning	Session %s (handle %p) has socket %d (handle %p); ignoring socket %d (handle %p) from %p

MX Events

Event Name	Severity	Displayed Text
alert	alert	%s
crit	crit	%s
debug	debug	%s
emerg	emerg	%s
error	error	%s
info	info	%s
notice	notice	%s
warning	warning	%s

PktLog Events

Event Name	Severity	Displayed Text
stats	error	%s@%s: Discarded %llu %s pkts within previous %u seconds
blacklist	error	%s@%s: Blacklist %s:%u Discarded %llu %s pkts within previous %u seconds
packet	notice	%s@%s: Discarded pkt: %s:%u -> %s:%u, Proto: %s
track_port	notice	%s@%s: %u %s ports hit within previous %u seconds. %s

RADIUS Events

Event Name	Severity	Displayed Text
no_ref	error	request on session %016llx (%s -> %s) has no RADIUS group reference; configuration is likely incorrect
bad_ref	error	request on session %016llx (%s -> %s) has bad RADIUS group reference (ID %d, string '%s'); configuration is likely incorrect

RTP Events

Event Name	Severity	Displayed Text
unmixable	error	Session %llx not mixed due to an internal error

Sensor Events

Event Name	Severity	Displayed Text
physical_security_0	alert	general chassis intrusion
physical_security_1	alert	drive bay intrusion
physical_security_2	alert	I/O card area intrusion
physical_security_3	alert	processor area intrusion
physical_security_5	alert	unauthorized dock/undock
physical_security_6	alert	fan area intrusion
event_logging_disabled_4	alert	log full
management_subsystem_health_0	alert	sensor access degraded or unavailable
management_subsystem_health_1	alert	controller access degraded or unavailable
management_subsystem_health_2	alert	management controller off-line
management_subsystem_health_3	alert	management controller unavailable
management_subsystem_health_4	alert	sensor failure
management_subsystem_health_5	alert	FRU failure
event_threshold_4	alert	lower non-recoverable going low
event_threshold_5	alert	lower non-recoverable going high
event_threshold_10	alert	upper non-recoverable going low
event_threshold_11	alert	upper non-recoverable going high
badprocessor	crit	%s: %s
processor_7	debug	presence detected

Event Name	Severity	Displayed Text
processor_8	debug	disabled
processor_9	debug	terminator presence detected
processor_10	debug	throttled
power_supply_0	debug	presence detected
power_supply_1	debug	failure detected
power_supply_2	debug	predictive failure
power_supply_6_0	debug	config error: vendor mismatch
power_supply_6_1	debug	config error: revision mismatch
power_supply_6_2	debug	config error: processor missing
power_supply_6	debug	config error
power_unit_0	debug	power off/down
power_unit_1	debug	power cycle
power_unit_2	debug	240VA power down
power_unit_3	debug	interlock power down
power_unit_5	debug	soft-power control failure
power_unit_6	debug	failure detected
power_unit_7	debug	predictive failure
memory_0	debug	correctable ECC
memory_1	debug	uncorrectable ECC
memory_2	debug	parity
memory_3	debug	memory scrub failed
memory_4	debug	memory device disabled
memory_5	debug	correctable ECC logging limit reached
memory_6	debug	presence detected
memory_7	debug	configuration error
memory_8	debug	spare
memory_9	debug	throttled
drive_slot_0	debug	drive present
drive_slot_1	debug	drive fault
drive_slot_2	debug	predictive failure
drive_slot_3	debug	hotspare

Event Name	Severity	Displayed Text
drive_slot_4	debug	parity check in progress
drive_slot_5	debug	in critical array
drive_slot_6	debug	in failed array
drive_slot_7	debug	rebuild in progress
drive_slot_8	debug	rebuild aborted
system_firmware_progress _2_0	debug	unspecified
system_firmware_progress _2_1	debug	memory initialization
system_firmware_progress _2_2	debug	hard-disk initialization
system_firmware_progress _2_3	debug	secondary CPU Initialization
system_firmware_progress _2_4	debug	user authentication
system_firmware_progress _2_5	debug	user-initiated system setup
system_firmware_progress _2_6	debug	USB resource configuration
system_firmware_progress _2_7	debug	PCI resource configuration
system_firmware_progress _2_8	debug	option ROM initialization
system_firmware_progress _2_9	debug	video initialization
system_firmware_progress _2_10	debug	cache initialization
system_firmware_progress _2_11	debug	SMBus initialization
system_firmware_progress _2_12	debug	keyboard controller initialization
system_firmware_progress _2_13	debug	management controller initialization
system_firmware_progress _2_14	debug	docing station attachment

Event Name	Severity	Displayed Text
system_firmware_progress_2_15	debug	enabling docking station
system_firmware_progress_2_16	debug	docking station ejection
system_firmware_progress_2_17	debug	disabling docking station
system_firmware_progress_2_18	debug	calling operating system wake-up vector
system_firmware_progress_2_19	debug	system boot initiated
system_firmware_progress_2_20	debug	motherboard initialization
system_firmware_progress_2_21	debug	reserved
system_firmware_progress_2_22	debug	floppy initialization
system_firmware_progress_2_23	debug	keyboard test
system_firmware_progress_2_24	debug	pointing device test
system_firmware_progress_2_25	debug	primary CPU initialization
system_firmware_progress_2	debug	unknown progress
event_logging_disabled_0	debug	correctable memory error logging disabled
event_logging_disabled_1	debug	event logging disabled
event_logging_disabled_3	debug	all event logging disabled
watchdog_1_0	debug	BIOS reset
watchdog_1_1	debug	OS reset
watchdog_1_2	debug	OS shut down
watchdog_1_3	debug	OS power down
watchdog_1_4	debug	OW power cycle
watchdog_1_5	debug	OS NMMI/diag interrupt
watchdog_1_6	debug	OS expired

Event Name	Severity	Displayed Text
watchdog_1_7	debug	OS pre-timeout interrupt
system_event_0	debug	system reconfigured
system_event_1	debug	OEM system boot event
system_event_2	debug	undetermined system hardware failure
system_event_3	debug	entry added to auxiliary log
system_event_4	debug	PEF action
ctitical_interrupt_0	debug	front panel NMI
ctitical_interrupt_1	debug	bus timeout
ctitical_interrupt_2	debug	I/O channel check NMI
ctitical_interrupt_3	debug	software NMI
ctitical_interrupt_4	debug	PCI PERR
ctitical_interrupt_5	debug	PCI SERR
ctitical_interrupt_6	debug	EISA failsafe timeout
ctitical_interrupt_7	debug	bus correctable error
ctitical_interrupt_8	debug	bus uncorrectable error
ctitical_interrupt_9	debug	fatal NMI
cable_interconnect_0	debug	connected
cable_interconnect_1	debug	config error
boot_error_0	debug	no bootable media
boot_error_1	debug	non-bootable disk in drive
boot_error_2	debug	PXE server not found
boot_error_3	debug	invalid boot sector
boot_error_4	debug	timeout waiting for selection
os_boot_0	debug	A: boot completed
os_boot_1	debug	C: boot completed
os_boot_2	debug	PXE boot completed
os_boot_3	debug	diagnostic boot completed
os_boot_4	debug	CD-ROM boot completed
os_boot_5	debug	ROM boot completed
os_boot_6	debug	boot completed - device not specified
os_critical_stop_0	debug	error during system startup

Event Name	Severity	Displayed Text
os_critical_stop_1	debug	run-time critical stop
os_critical_stop_2	debug	OS graceful stop
os_critical_stop_3	debug	OS graceful shutdown
os_critical_stop_4	debug	PEF initiated soft shutdown
os_critical_stop_5	debug	agent not responding
slot_connector_0	debug	fault status asserted
slot_connector_1	debug	identify status asserted
slot_connector_2	debug	slot/connector device installed/attached
slot_connector_3	debug	slot/connector ready for device installation
slot_connector_4	debug	slot/connector ready for device removal
slot_connector_5	debug	slot power is off
slot_connector_6	debug	slot/connector device removal request
slot_connector_7	debug	interlock asserted
slot_connector_8	debug	slot is disabled
slot_connector_9	debug	spare device
system_acpi_power_state_0	debug	S0/G0: working
system_acpi_power_state_1	debug	S1: sleeping with system hw & processor context maintained
system_acpi_power_state_2	debug	S2: sleeping, processor context lost
system_acpi_power_state_3	debug	S3: sleeping, processor & hw context lost, memory retained
system_acpi_power_state_4	debug	S4: non-volatile sleep/suspend-to-disk
system_acpi_power_state_5	debug	S5/G2: soft-off
system_acpi_power_state_6	debug	S4/S5: soft-off
system_acpi_power_state_7	debug	G3: mechanical off
system_acpi_power_state_8	debug	Sleeping in S1/S2/S3 state

Event Name	Severity	Displayed Text
system_acpi_power_state_9	debug	G1: sleeping
system_acpi_power_state_10	debug	S5: entered by override
system_acpi_power_state_11	debug	legacy ON state
system_acpi_power_state_12	debug	legacy OFF state
system_acpi_power_state_14	debug	unknown
watchdog_2_0	debug	timer expired
watchdog_2_1	debug	hard reset
watchdog_2_2	debug	power down
watchdog_2_3	debug	power cycle
watchdog_2_4	debug	reserved
watchdog_2_5	debug	reserved
watchdog_2_6	debug	reserved
watchdog_2_7	debug	reserved
watchdog_2_8	debug	timer interrupt
platform_alert_0	debug	platform generated page
platform_alert_1	debug	platform generated LAN alert
platform_alert_2	debug	platform event trap generated
platform_alert_3	debug	platform generated SNMP trap, OEM format
entity_presence_0	debug	present
entity_presence_1	debug	absent
entity_presence_2	debug	disabled
lan_0	debug	heartbeat lost
lan_1	debug	heartbeat
battery_0	debug	low
battery_1	debug	failed
battery_2	debug	presence detected
version_change_0	debug	hardware change detected

Event Name	Severity	Displayed Text
version_change_1	debug	firmware or software change detected
version_change_2	debug	hardware incompatibility detected
version_change_3	debug	firmware or software incompatibility detected
version_change_4	debug	invalid or unsupported hardware version
version_change_5	debug	invalid or unsupported firmware or software version
version_change_6	debug	hardware change success
version_change_7	debug	firmware or software change success
fru_state_0	debug	not installed
fru_state_1	debug	inactive
fru_state_2	debug	activation requested
fru_state_3	debug	activation in progress
fru_state_4	debug	active
fru_state_5	debug	deactivation requested
fru_state_6	debug	deactivation in progress
fru_state_7	debug	communication lost
fru_hot_swap_0	debug	transition to M0
fru_hot_swap_1	debug	transition to M1
fru_hot_swap_2	debug	transition to M2
fru_hot_swap_3	debug	transition to M3
fru_hot_swap_4	debug	transition to M4
fru_hot_swap_5	debug	transition to M5
fru_hot_swap_6	debug	transition to M6
fru_hot_swap_7	debug	transition to M7
ipmb_status_0	debug	IPMB-A disabled, IPMB-B disabled
ipmb_status_1	debug	IPMB-A enabled, IPMB-B disabled
ipmb_status_2	debug	IPMB-A disabled, IPMB-B enabled
ipmb_status_3	debug	IPMB-A enabled, IPMB-B enabled
module_hot_swap_0	debug	module handle closed
module_hot_swap_1	debug	module handle opened
module_hot_swap_2	debug	quiesced

Event Name	Severity	Displayed Text
oem_0	debug	OEM specific
event_threshold_0	debug	lower non-critical going low
event_threshold_1	debug	lower non-critical going high
event_threshold_6	debug	upper non-critical going low
event_threshold_7	debug	upper non-critical going high
event_discrete_usage_0	debug	transition to idle
event_discrete_usage_1	debug	transition to active
event_discrete_usage_2	debug	transition to busy
event_discrete_state_0	debug	state deasserted
event_discrete_state_1	debug	state asserted
event_discrete_predictive_failure_0	debug	predictive failure deasserted
event_discrete_predictive_failure_1	debug	predictive failure asserted
event_discrete_limit_exceeded_0	debug	limit not exceeded
event_discrete_limit_exceeded_1	debug	limit exceeded
event_discrete_performance_met_0	debug	performance met
event_discrete_performance_met_1	debug	performance lags
event_discrete_serverity_0	debug	transition to OK
event_discrete_serverity_1	debug	transition to non-critical from OK
event_discrete_serverity_2	debug	transition to critical from less severe
event_discrete_serverity_3	debug	transition to non-recoverable from less severe
event_discrete_serverity_4	debug	transition to non-critical from more severe
event_discrete_serverity_5	debug	transition to critical from non-recoverable
event_discrete_serverity_6	debug	transition to non-recoverable
event_discrete_serverity_7	debug	monitor
event_discrete_serverity_8	debug	informational
event_discrete_device_presence_0	debug	device absent

Event Name	Severity	Displayed Text
event_discrete_device_presence_1	debug	device present
event_discrete_device_enable_0	debug	device disabled
event_discrete_device_enabled_1‘	debug	device enabled
event_discrete_availability_0	debug	transition to running
event_discrete_availability_1	debug	transition to in test
event_discrete_availability_2	debug	transition to power off
event_discrete_availability_3	debug	transition to on line
event_discrete_availability_4	debug	transition to off line
event_discrete_availability_5	debug	transition to off duty
event_discrete_availability_6	debug	transition to degraded
event_discrete_availability_7	debug	transition to power save
event_discrete_availability_7	debug	install error
event_discrete_redundancy_0	debug	fully redundant
event_discrete_redundancy_2	debug	redundancy degraded
event_discrete_redundancy_4	debug	non-redundant: sufficient from insufficient
event_discrete_redundancy_6	debug	redundancy degraded from fully redundant
event_discrete_redundancy_7	debug	redundancy degraded from non-redundant
event_discrete_acpi_power_0	debug	D0 power state

Event Name	Severity	Displayed Text
event_discrete_acpi_power_1	debug	D1 power state
event_discrete_acpi_power_2	debug	D2 power state
event_discrete_acpi_power_3	debug	D3 powerstate
platform_security_0	error	front panel lockout violation attempted
platform_security_1	error	pre-boot password violation - user password
platform_security_2	error	pre-boot password violation - setup password
platform_security_3	error	pre-boot password violation - network boot password
platform_security_4	error	other pre-boot password violation
platform_security_5	error	out-of-band access password violation
processor_0	error	IERR
processor_1	error	thermal trip
processor_2	error	FRB1/BIST failure
processor_3	error	FRB2/hang in POST failure
processor_4	error	FRB3/processor startup/init failure
processor_5	error	configuration error
processor_6	error	SM BIOS uncorrectable CPU-complex error
system_firmware_progress_0_0	error	unspecified
system_firmware_progress_0_1	error	no system memory installed
system_firmware_progress_0_2	error	no usable system memory
system_firmware_progress_0_3	error	unrecoverable IDE device failure
system_firmware_progress_0_4	error	unrecoverable system-board failure
system_firmware_progress_0_5	error	unrecoverable diskette failure
system_firmware_progress_0_6	error	unrecoverable hard-disk controller failure

Event Name	Severity	Displayed Text
system_firmware_progress_0_7	error	unrecoverable PS/2 or USB keyboard failure
system_firmware_progress_0_8	error	removable boot media not found
system_firmware_progress_0_9	error	unrecoverable video controller failure
system_firmware_progress_0_10	error	no video device selected
system_firmware_progress_0_11	error	BIOS corruption detected
system_firmware_progress_0_12	error	CPU voltage mismatch
system_firmware_progress_0_13	error	CPU speed mismatch failure
system_firmware_progress_0	error	unknown error
system_firmware_progress_1_0	error	unspecified
system_firmware_progress_1_1	error	memory initialization
system_firmware_progress_1_2	error	hard-disk initialization
system_firmware_progress_1_3	error	secondary CPU Initialization
system_firmware_progress_1_4	error	user authentication
system_firmware_progress_1_5	error	user-initiated system setup
system_firmware_progress_1_6	error	USB resource configuration
system_firmware_progress_1_7	error	PCI resource configuration
system_firmware_progress_1_8	error	option ROM initialization
system_firmware_progress_1_9	error	video initialization

Event Name	Severity	Displayed Text
system_firmware_progress _1_10	error	cache initialization
system_firmware_progress _1_11	error	SMBus initialization
system_firmware_progress _1_12	error	keyboard controller initialization
system_firmware_progress _1_13	error	management controller initialization
system_firmware_progress _1_14	error	docking station attachment
system_firmware_progress _1_15	error	enabling docking station
system_firmware_progress _1_16	error	docking station ejection
system_firmware_progress _1_17	error	disabling docking station
system_firmware_progress _1_18	error	calling operating system wake-up vector
system_firmware_progress _1_19	error	system boot initiated
system_firmware_progress _1_20	error	motherboard initialization
system_firmware_progress _1_21	error	reserved
system_firmware_progress _1_22	error	floppy initialization
system_firmware_progress _1_23	error	keyboard test
system_firmware_progress _1_24	error	pointing device test
system_firmware_progress _1_25	error	primary CPU initialization
system_firmware_progress _1	error	unknown hang
critical_interrupt_10	error	bus fatal error
event_threshold_2	error	lower critical going low

Event Name	Severity	Displayed Text
event_threshold_3	error	lower critical going high
event_threshold_8	error	upper critical going low
event_threshold_9	error	upper critical going high
event_discrete_redundancy_3	info	non-redundant: sufficient from redundant
physical_security_4	notice	system unplugged from LAN
event_logging_disabled_2	notice	log area reset/cleared
system_event_5	notice	timestamp clock sync
button_0	notice	power button pressed
button_1	notice	sleep button pressed
button_2	notice	reset button pressed
button_3	notice	FRU latch
button_4	notice	FRU service
system_boot_initiated_0	notice	initiated by power up
system_boot_initiated_1	notice	initiated by hard reset
system_boot_initiated_2	notice	initiated by warm reset
system_boot_initiated_3	notice	user requested PXE boot
system_boot_initiated_4	notice	automatic boot to diagnostic
system_boot_initiated_5	notice	OS initiated hard reset
system_boot_initiated_6	notice	OS initiated warm reset
system_boot_initiated_7	notice	system restart
power_supply_3	warning	power supply AC lost
power_supply_4	warning	AC lost or out-of-range
power_supply_5	warning	AC out-of-range, but present
power_unit_4	warning	AC lost
event_logging_disabled_5	warning	log almost full
event_discrete_redundancy_1	warning	redundancy lost
event_discrete_redundancy_5	warning	non-redundant insufficient resources

Setup Information

Event Name	Severity	Displayed Text
system	info	system name: %s, description: %s, contact: %s, location: %s
software	info	software version: %s, build: %s
chassis	info	chassis model: %s, build: %s
license	info	license name: %s, key: %s, expiration: %s
interface	info	interface device: %s, name: %s, address: %s

SIP Events

Event Name	Severity	Displayed Text
transportVThread	error	SIP worker threads are overloaded, current time %s, number of pending events %u, high-water %u, low-water mark %u

SIP Registration Logs

Event Name	Severity	Displayed Text
unregister_failed	error	Failed to send unregister for AOR %s contact %s call-ID %s : %s
unregister_timeout	info	We encountered a problem while trying to unregister AOR %s contact %s : %s

SIP Routing Logs

Event Name	Severity	Displayed Text
vdp_match_limit	alert	Hit virtual-dial-plan match limit of %d
route_set_leak	error	Route destroyed during deferred cleanup. Session 0x%0X (sessID: %08llX), initial method %s, from-uri: %s, to-uri: %s
vdp_not_supported	warning	Virtual dial plan functionality is not supported

System Events

Event Name	Severity	Displayed Text
monitoralertskbusage	alert	Monitor alert %u SKB usage exceeds threshold %u in the last %u minute%s
monitoralerttcpskbdrops	alert	Monitor alert %u TCP dropped packets due to SKB congestion exceeds threshold %u in the last %u minute%s
process_crash	crit	External process %s PID %d has crashed; will restart
actionexecinternal	debug	'%s' action executed internally: %s
db_corrupt_block	error	Database corruption detected: file %s, block %d
postbadinstall	error	%s: Install failed: %s
savebeforeupgrade_error	error	Errors while backing up current configuration : %s
action_args	info	'%s' action arguments: %.*s
action_info	info	'%s' action information returned: %s
restartsend	info	Controlled restart sending %s to %s
restartexec	info	Controlled restart restarting %s
restartsave	info	Controlled restart saving %s
restartload	info	Controlled restart loading %s
restorestickcomplete	notice	restore-stick-create operation complete
db_record_count	notice	database %s, table %s has %u records exceeding limit of %u
postinstalling	notice	%s: Started installing at %s
postinstall	notice	%s: Completed installation at %s
postinstallinfo	notice	%s: %s
savebeforeupgrade	notice	Current configuration is backed up as %s (%s format)

Tracing Information

Event Name	Severity	Displayed Text
debug	debug	%s
enabled	notice	Trace target %s enabled.
disabled	notice	Trace target %s disabled.
disable_all	notice	Tracing to %s disabled.
enable_all	notice	Tracing to %s enabled.
update	notice	Tracing %s at %s level.
command	notice	Trace command %s executed by %s.
start_command	notice	Tracing to %s STARTED by %s.
stop_command	notice	Tracing to %s STOPPED by %s.

UID32 Events

Event Name	Severity	Displayed Text
generated	debug	Value %08x was generated (box %02x, seed %02x, serial %08x)
read_seed	warning	Seed value %02x was read from file
wrote_seed	warning	Seed value %02x was written to file
gen_seed	warning	Seed value %02x was generated randomly
wrap_seed	warning	Seed value %02x was arrived at via wrap
serial_init	warning	Serial value %08x was generated randomly
init	warning	Initialized with seed %02x, serial %08x

Result Codes

For information on the possible result codes that can appear within event messages, refer to the *Net-Net OS-E — Using the OS-E Management Tools*.