# Oracle® Communications Session Border Controller

Maintenance Release Guide
Release S-CX6.3.0
*Formerly Net-Net Session Director*

October 2013

## Notices

# Contents

# Preface

## About this guide

The Maintenance Release Guide provides information about the contents of maintenance releases related to release S-CX6.3.0. This information can be related to defect fixes, to adaptations made to the system software, and to adaptations ported to this release from prior releases. When applicable, this guide contains explanations of defect fixes to the software and step-by-step instructions, if any, for how to enables these fixes on your system. This guide contains explanations of adaptations including conceptual information and configuration steps.

### Purpose of this Document

Designed as a supplement to the main documentation set supporting release S-CX6.3.0, this document informs you of changes made to the software in the maintenance releases of S-CX6.3.0. Consult this document for content specific to maintenance releases. For information about general Net-Net OS features, configuration, and maintenance, consult the Related Documentation (iv) listed in the section below and then refer to the applicable document.

### Organization

The Maintenance Release Guide is organized chronologically by maintenance release number, started with the oldest available maintenance release and ending with the most recently available maintenance release.

This document contains a Maintenance Release Availability Matrix, showing when and if given maintenance releases have been issued and the date of issue. Each available maintenance release constitutes one chapter of this guide.

In certain cases, a maintenance release will not have been made generally available. These cases are noted in the Maintenance Release Availability Matrix. When Oracle has not made a maintenance release available, there will be no corresponding chapter for that release. Therefore, you might encounter breaks in the chronological number of maintenance release.

### Maintenance Release Availability Matrix

The table below lists the availability for version S-CX6.3.0 maintenance releases.

| Mainenance release number | Availability Notes |
|---|---|
| S-CX6.3.0M1 | June 15, 2012 |
| S-CX6.3.0M2 | August 7, 2012 |
| S-CX6.3.0M3 | January 28, 2013 |
| S-CX6.3.0M4 | March 25, 2013 |

| Mainenance release number | Availability Notes |
|---|---|
| S-CX6.3.0M5 | June 14, 2013 |

## Related Documentation

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

| Document Name | Document Description |
|---|---|
| Acme Packet 4500 System Hardware Installation Guide (400-0101-00) | Contains information about the components and installation of the Acme Packet 4500 system. |
| Acme Packet 3800 Hardware Installation Guide (400-0118-00) | Contains information about the components and installation of the Acme Packet 3800 system. |
| Release Notes | Contains information about the current documentation set release, including new features and management changes. |
| ACLI Configuration Guide | Contains information about the administration and software configuration of the SBC. |
| ACLI Reference Guide | Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters. |
| Maintenance and Troubleshooting Guide | Contains information about logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives. |
| MIB Reference Guide | Contains information about Management Information Base (MIBs), Acme Packet's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects. |
| Accounting Guide | Contains information about accounting support, including details about RADIUS accounting. |
| HDR Resource Guide | Contains information about the Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information. |
| Administrative Security Essentials | Contains information about support for its Administrative Security license. |

# 1

# S-CX6.3.0M1

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net OS Release S-CX6.3.0 M1.

## Content Map

This section provides a table listing all content in Net-Net OS Release S-CX6.3.0 M1.

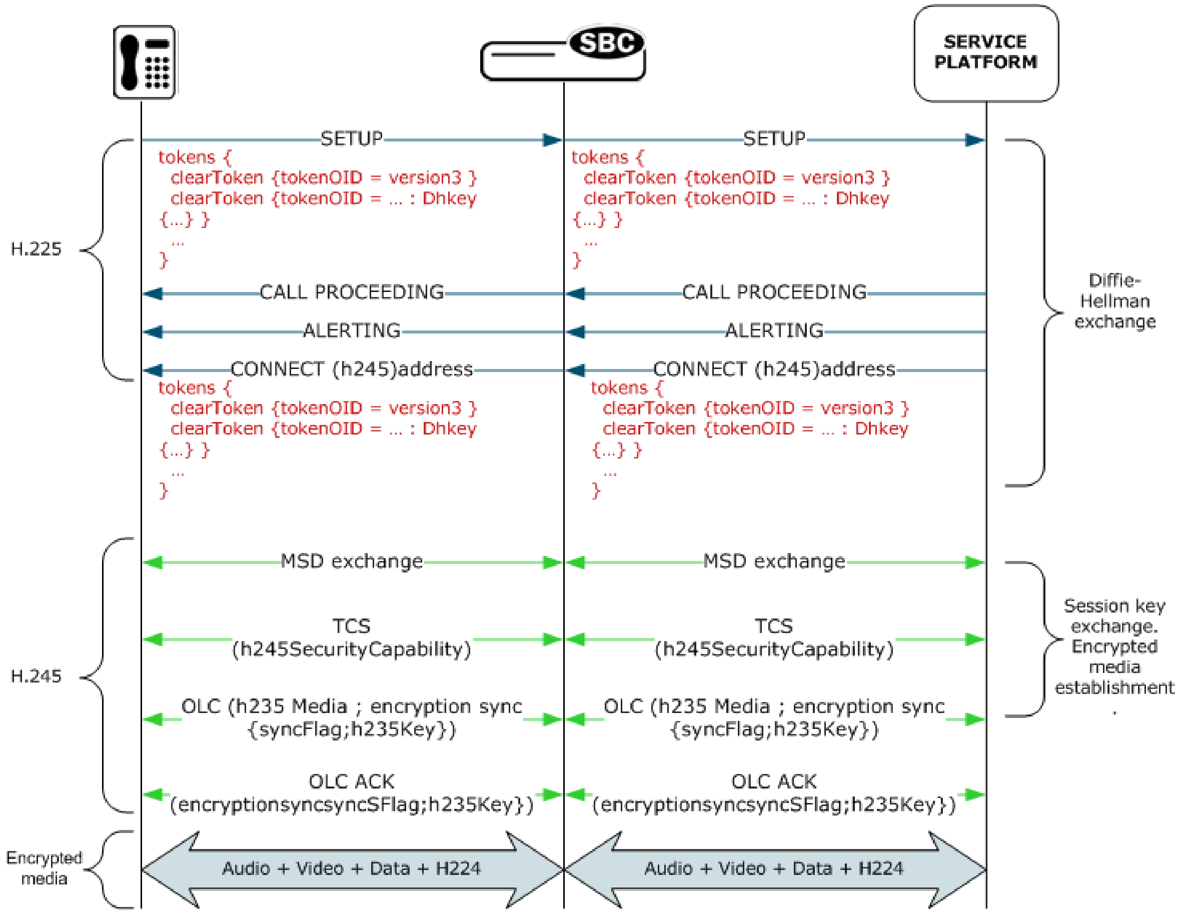
| Content Type | Description |
|---|---|
| Adaptation | H.235 Encryption (REQ 2599, 2693) |

## H.235 Encryption

Following the ITU-T H.235 encryption standard, the Oracle Communications Session Border Controller allows media (audio, video, and data) media that has already been encrypted by endpoints to pass through it, thereby supporting videoconferencing applications where media confidentiality is key. The ITU-T standard provides a profile with key management using Diffie-Hellman keys and the specification of an encryption algorithm.

Specifically, the Oracle Communications Session Border Controller permits the following:

- H.225 Setup and connect—The tokens parameter and its subfields in H.225 Setup and Connect message to pass transparently through the Oracle Communications Session Border Controller
- H.245Teminal CapabilitySet—The H.245 TerminalCapabilitySet messages to pass transparently through the Oracle Communications Session Border Controller, including:
  - Audio, video, and data capabilities
  - The h235SecurityCapability capability
- H.245 OpenLogicalChannel and OpenLogicalChannelAck—OLC messages with dataType h235Media to pass transparently through the Oracle Communications Session Border Controller; to accomplish this, the Oracle Communications Session Border Controller uses the mediaType subfield instead of the dataType field when the dataType is h235Media. The encryptionSync parameter and its subfields found in OLC and OLCAck messages to pass transparently through the Oracle Communications Session Border Controller.


SBC
SERVICE PLATFORM
H.225
SETUP
tokens {
clearToken {tokenOID = version3 }
clearToken {tokenOID = ... : Dhkey
{...} }
...
}
SETUP
tokens {
clearToken {tokenOID = version3 }
clearToken {tokenOID = ... : Dhkey
{...} }
...
}
CALL PROCEEDING
CALL PROCEEDING
ALERTING
ALERTING
CONNECT (h245)address
tokens {
clearToken {tokenOID = version3 }
clearToken {tokenOID = ... : Dhkey
{...} }
...
}
CONNECT (h245)address
tokens {
clearToken {tokenOID = version3 }
clearToken {tokenOID = ... : Dhkey
{...} }
...
}
Diffie-Hellman exchange
H.245
MSD exchange
MSD exchange
TCS (h245SecurityCapability)
TCS (h245SecurityCapability)
OLC (h235 Media ; encryption sync {syncFlag;h235Key})
OLC (h235 Media ; encryption sync {syncFlag;h235Key})
OLC ACK (encryptionsyncsyncSFlag;h235Key})
OLC ACK (encryptionsyncsyncSFlag;h235Key})
Session key exchange. Encrypted media establishment .
Encrypted media
Audio + Video + Data + H224
Audio + Video + Data + H224

You do not need to follow special configuration steps to enable this functionality; it works automatically.

# 2

# S-CX6.3.0M2

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net OS Release Version S-CX6.3.0M2.

## Content Map

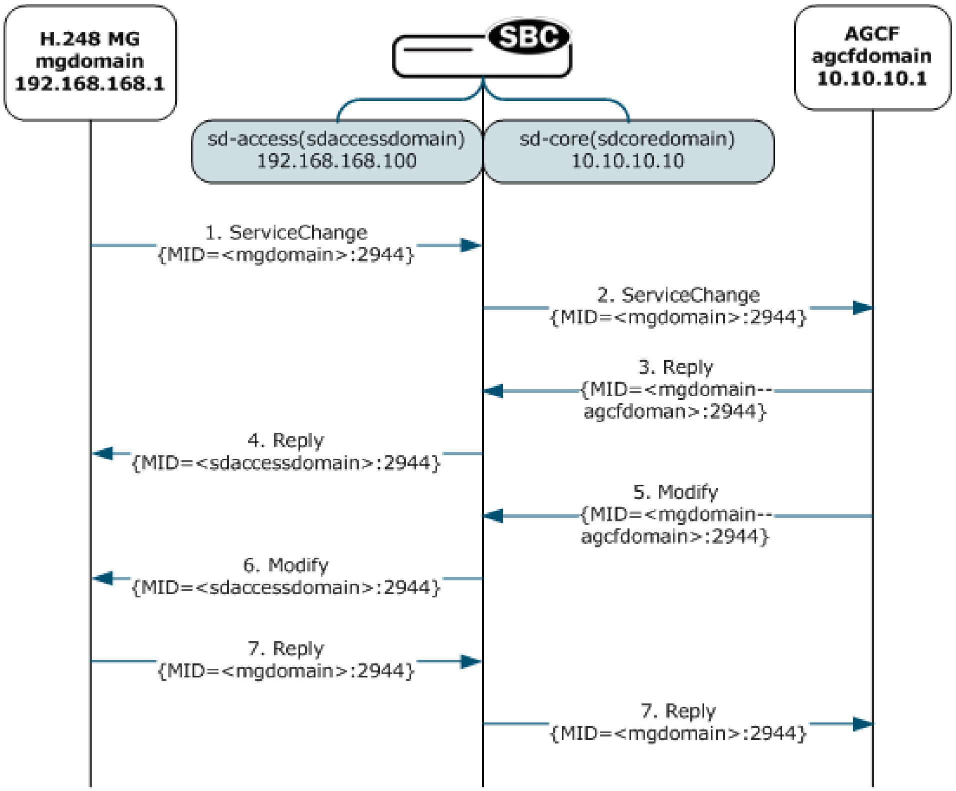
This section provides a table listing all content in Net-Net OS Release Version S-CX6.3.0M2.

| Content Type | Description |
|---|---|
| Adaptation | H.248 MID ALG Mapping (REQ 2648) |
| Adaptation | H.248 Port Mapping ALG (REQ 2651) |
| Adaptation | E2 CLF Timeout (REQ 3172) |

## H.248 ALG MID

When you use message identifier (MID) mapping, you can define the delimiter the Access Gateway Control Function (AGCF) uses to obtain the media gateway's message identifier (MID). This is the MID in the H.248 request from the AGCF. You can define the message identifier (MID) delimiter as either a double asterisk (**) or as a hyphen (-).

You can configure the delimiter for the global H.248 configuration (h248-config) or for an H.248 media gateway configuration (h248-mg-config). The value you set in the H.248 MG configuration's MID delimiter setting always take precedence over the global H.248 configuration's, allowing different H.248 MG configurations to use different delimiter settings.



## H.248 ALG MID Configuration

You set the MID delimiter setting in the options parameter to mid-based-muxing in either the h248-config or the h248-mg-config. These instructions show you how to set the parameter in the h248-mg-config; the steps are the same for the h248-config.

To configure the MID delimiter for the h248-mg-config:

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

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

2. Type session-router and press Enter.

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

3. Type h248-config and press Enter.

```
ACMEPACKET(session-router)# h248-config
ACMEPACKET(h248-config)#
```

4. Type h248-mg-config and press Enter.

```
ACMEPACKET(h248-config)# h248-mg-config
ACMEPACKET(h248-mg-config)#
```

5. options—Enter the option mid-based-muxing name with the value you want to use for the delimiter, either the double asterisk (**) or the hyphen (-). If you are adding this setting to a pre-existing H.248 MG configuration, you need to select the configuration before making additions or changes. If you are adding this option to a list of previously configured options, you must pre-pend the option name with a plus sign (+).

```
ACMEPACKET(h248-mg-config)# options +mid-based-muxing=-
ACMEPACKET(h248-mg-config)#
```

6. Save your work.

# H.248 Port Mapping ALG

The H.248 port mapping ALG is a pool of configured IP addresses and port ranges configured on the core H.248 interface that the Oracle Communications Session Border Controller allocates to registering gateways (GWs). When a GW registers with the Oracle Communications Session Border Controller by sending a ServiceChange message, the Oracle Communications Session Border Controller assigns it a unique IP address and port from it pool of configured port maps. This way, the registered GW has a unique presence—the IP address and port—in the core network that remains for its service life.

## Mapping Scheme Types and Precedence

There are three types of address mapping schemes: address masquerading, mixed-based muxing, and port mapping. All can co-exist on the Oracle Communications Session Border Controller , and are chosen for use on a per-H.248-MG basis in this order of precedence:

1. If an H.248 MG configuration (h248-mg-config) has an address mask other than 32 in its address field (e.g., 192.168.101.13/16), then the Oracle Communications Session Border Controller performs address masquerading.
2. If a port map is configured, then the address mapping scheme will be to use port mapping.
3. If the h248-mg-config has its options parameter set with mid-based-muxing, then that specific h248-mg-config will adopt message identifier (MID) mapping.
4. If the h248-config has its options parameter set with mid-based-muxing, then MID mapping will be adopted globally.

## Creating and Using Port Maps

This section provides information you should know and cover choices you might make as you create port maps.

### ServiceChange Handling

When the Oracle Communications Session Border Controller receives a ServiceChange for which the TerminationId is “root” and the ServiceMethods is anything other than “Forced,” it checks for a pre-existing ALG session with the GW MID. If none exists, theOracle Communications Session Border Controller creates a new ALG session. If port mapping is the chosen mapping procedure for this GW MID, the Oracle Communications Session Border Controller chooses a unique IP port from the pool and assigns that IP port to the GW MID. Then the Oracle Communications Session Border Controller forwards the ServiceChange message to the MGC using the chosen IP address and port. In the event that a unique IP port cannot be allocated, the Oracle Communications Session Border Controller issues this error: <503> “Service Unavailable: failed to get port map”.

### Handling Other Messages

For messages other than ServiceChange, the Oracle Communications Session Border Controller checks for a pre-existing map for the GW sending the message. If a map exists, the Oracle Communications Session Border Controller forwards the message to the core MGC using the IP port leaving the MID unchanged. If there is no map, the Oracle Communications Session Border Controller responds to the message directly with error <503> “Service Unavailable:Session Unavailable”.

When it receives a message from the core MGC, the Oracle Communications Session Border Controller checks for pre-existing mapping from the receiving port to a GW. When such a port mapping exists, the Net-Net SBC forwards the message to the GW leaving the MID unchanged. Without such a port, the Oracle Communications Session Border Controller responds to the message directly with error <503> “Service Unavailable:Session Unavailable”.

### Port Map Allocation

Core-side H.248 interfaces can be associated with multiple IP addresses, each of which can have a range of ports to which mapping can be performed. There is no limit on the number of IP addresses that you can configure on the core-side H.248 ALG.

Each H.248 ALG you configure has:

- A list of available IP ports
- Map of allocated IP ports and the associated GW MID

When the Oracle Communications Session Border Controller needs to allocate a pot map from its pool of available IP ports, it follows this course of actions in order:

1. Returns an error if there are no IP ports available.
2. Obtains the first IP port from the list of available IP ports.
3. Inserts the IP port it obtained into the map of allocated ports in order to create a mapping between the core-side H.248 IP address/port combination and the GW MID.
4. Removes the allocated IP port from the list of available IP ports.
5. Decrements the number of IP ports available on the core side.
6. Increments the number of IP ports allocated on the core side.
7. Generates an alarm and sends out a trap if the number of allocated ports exceeds 90% of the total available IP ports that can be mapped on the core side.

   Returning a Port Map to the Pool

   When the Oracle Communications Session Border Controller needs to return an allocated port map to the pool of available port maps, it follows this course of actions in order:
8. Returns an error if the freed IP port is invalid.
9. Returns an error if the freed IP port is not in the map of allocated IP ports.
10. Clears the alarm raised and clears the corresponding trap if the capacity of used ports exceeded 90%.
11. Removes the IP port being freed from the map of allocated IP ports.
12. Adds the IP port being freed to the end of the list of available IP ports.
13. Decrements the number of allocated IP ports.
14. Increments the number of available IP ports.

## Removing Port Maps

The Oracle Communications Session Border Controller removes port maps when:

- The GW goes out of service—The map is removed when theOracle Communications Session Border Controller received a ServiceChange message for which the Termination is “root” and the ServiceChangeMethod is “Forced.”
- The Oracle Communications Session Border Controller detects a GW fault—The Oracle Communications Session Border Controller fails to receives a the response for the AuditValue it sends to the GW as a heartbeat mechanism.

## H.248 Port Mapping Configuration

To enable H.248 port mapping, you configure port maps with IP address, start port, and end port information. The port map configuration is part of the larger H.248 media gateway (MG) configuration. You can configure multiple port maps.

Note that configuring port mapping supports having any number of MGs registered on the same access media gateway controller (MGC). And when you using the H.248 port mapping ALG, the MID received from the MG is always sent unchanged to the core side MGC.

To configure H.248 port mapping:

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

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)#
   ```
2. Type session-router and press Enter.

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

3. Type h248-config and press Enter.

```
ACMEPACKET(session-router)# h248-config
ACMEPACKET(h248-config)#
```

4. Type h248-mg-config and press Enter.

```
ACMEPACKET(h248-config)# h248-mg-config
ACMEPACKET(h248-mg-config)#
```

5. Type port-map and press Enter.

```
ACMEPACKET(h248-mg-config)# port-map
ACMEPACKET(port-map)#
```

6. address—Enter the IP address for the port map. Note that port maps are indexed based on IP address, meaning that no two port maps can have the same IP address. So you must configure the correct IP address for the port map such that there are no duplicates when flows are created. For example, the SIP interface IP address should not collide with the IP address:Port range you set for a port map. Using the verify-config command catches overlap issues. This parameter is blank by default.
7. start-port—Enter the number of the port that starts the range of ports to be mapped for the IP address you configured for the port map. If you set this parameter to 0, the port map is ignored and will not be used. The default for this parameter is 1025, and the valid range is 1025-65535.
8. end-port—Enter the number of the port that ends the range of ports to be mapped for the IP address you configured for the port map. If you set this parameter to 0, the port map is ignored and will not be used. The default for this parameter is 1025, and the valid range is 1025-65535.

## RTC and HA Considerations

Note the following consideration for real-time configuration (RTC):

- A new port map can be added with a new IP address and port range—There are no issues; data structures and statistics are updated.
- An existing port map might be modified to:
  - Expand the port range—There are no issues; data structures and statistics are updated.
  - Reduce the port range—Whenever a port or IP port is dropped, associated flows on the Oracle Communications Session Border Controller are also dropped. The Oracle Communications Session Border Controller cleans up the relevant ALG and media sessions. The endpoints need to re-register to send subsequent messages. The MGC will also be required to clean up its resources.
- An existing port map might be deleted—Whenever a port or IP port is dropped, associated flows on the Oracle Communications Session Border Controller are also dropped. The Oracle Communications Session Border Controller cleans up the relevant ALG and media sessions. The endpoints need to re-register to send subsequent messages. The MGC will also be required to clean up its resources.
- Another port mapping mechanism might be chosen instead of the H.248 port mapping ALG—A reboot is required whenever the mapping mechanism changes.

For high availability (HA) nodes:

- The core-side IP port must be replicated across systems in order to be highly available.
- Whenever a port map is created or deleted on the Active system, it should also be created or deleted on the Standby.

## Management

This section offers information about management related to IPport resources for the H.248 port mapping ALG.

### Viewing Port Use per MG

Using the ACLI show h248d h248-mg mgc-name command, you can display information about how many IP ports are available, allocated (used), and free.

```
ACMEPACKET# show h248d h248-mg mgc-name <mgc-name>
'Mapping for: <mgc-name>: Port-mapping'
Number of ports available: 64512
Number of ports used: 10
Number of ports free: 64502
```

### Viewing Specific Port Maps

You can see specific port maps between GW MIDs and core-side IPaddress/ports using either the GW MID or the IP port.

```
ACMEPACKET# show h248d gateway by-mid <GWMID>
'Mapping for GWMID: <GWMID>
Local IPPort: 172.16.18.5:2944
Remote IPPort: 192.168.101.111:1025
ACMEPACKET# show h248d gateway ipport <IPPort'>
Mapping for: <mgc-name>: Port-mapping'
Core IPPort: 192.168.101.111:1025
GWMID: mobile1
GW IPPort; 172.16.18.5:2944
```

### Resource Limits and Sample Messages

The Oracle Communications Session Border Controller follows a defined set of actions when port map resources exceed and fall back from 90%:

- When resource use exceeds 90% of the total number of available IP ports, the Oracle Communications Session Border Controller sends information to syslog, generates an alarm, and sends a trap. These actions are taken only once when the 90% threshold is broken. For example, the system does not continue issuing alarms for the entire time the threshold is exceeded—even if the level of use continues to rise (say from 90% to 91%, and then from 91% to 92%).
- When resource use returns to a level less that 90%, the systems clears the trap.

The syslog message looks like this, and is at the WARNING level:

```
<mgc-name> on realm=<realm>: port map usage has exceeded 90%
```

The alarm raised looks like this, and is at the MINOR level. It does not affect the system healthscore.

```
<mgc-name> on realm=<realm>: port map usage has exceeded 90%
```

The MINOR trap sent for usage being exceeded looks like this:

```
apSysMgmtH248PortMapUsageTrap       NOTIFICATION-TYPE
        OBJECTS         { apSysMgmtH248MgcName, apSysMgmtH248Realm,
apSysMgmtH248PortMapUsage }
        STATUS          current
        DESCRIPTION
            " The trap will be generated when the port map usage on H.248
core side
              Exceeds 90%."
        ::= { apSystemManagementMonitors 84 }
```

The trap that clears the MINOR trap for exceeded usage looks like this:

```
apSysMgmtH248PortMapUsageClearTrap       NOTIFICATION-TYPE
        OBJECTS         { apSysMgmtH248MgcName, apSysMgmtH248Realm}
        STATUS          current
        DESCRIPTION
            " The trap will be generated when the port map usage on H.248
core side
              Goes down below 90%."
        ::= { apSystemManagementMonitors 85 }
apSysMgmtH248MgcName OBJECT-TYPE
        SYNTAX          DisplayString
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
                "Number of current cached database-type contacts in the SD."
        ::= { apSysMgmtMIBGeneralObjects 31 }
apSysMgmtH248Realm OBJECT-TYPE
        SYNTAX          DisplayString
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
                "Number of current cached database-type contacts in the SD."
        ::= { apSysMgmtMIBGeneralObjects 32 }
apSysMgmtH248PortMapUsage OBJECT-TYPE
        SYNTAX          Unsigned32
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
                "Number of current cached database-type contacts in the SD."
        ::= { apSysMgmtMIBGeneralObjects 33 }
```

## H.248 ALG Media Timer Expiration

When you enable the H.248 ALG media expiration timer, the Oracle Communications Session Border Controller monitors the media timer for media the Media Gateway Controller (MGC) forwards to it during call set-up. The Oracle Communications Session Border Controller notifies the MGC if the media timer expires.

So the Oracle Communications Session Border Controller can notify the MGC when a media timer expires, the MGC must communicate (using an ADD or MODIFY command) to the Media Gateway (MG) via the Oracle Communications Session Border Controller that the MG must perform network failure detection. The MGC must subscribe to the network package (nt) with netfail event (nt/failure) per termination. When it receives this subscription, the Oracle Communications Session Border Controller tracks subscription on a per-termination basis.

If the Oracle Communications Session Border Controller subscribes to the netfail event and a media timer expiration occurs, it sends a the MGC a NOTIFY message with the netfail event. The NOTIFY message will contain the termination ID and ObservedEvents (with the RequestID obtained from the subscription).

```
MEGACO/1  [168.1.32.52]:2944
Transaction = 31622507{Context = -{Notify = RTP/00000{
ObservedEvents = 2000{20010001T00011400 : nt/netfail{cs="Net Failed"}}}}}
```

Although the Oracle Communications Session Border Controller will absorb the MGC’s response to this NOTIFY message (by not forwarding it to the MG), it will forward all subsequent MGC requests to the MG. The MGC should send a SUBTRACT message to release the call. To prevent hanging resources, the Oracle Communications Session Border Controller sets a ten-second timer on the context; if it fails to receive the MGC’s SUBTRACT message in that time, the Oracle Communications Session Border Controller deletes the context.

If a media timer for which there is no subscription expires, the Oracle Communications Session Border Controller cleans up the context without sending notifications.

### H.248 ALG Media Timer Expiration Configuration

To enable H.248 ALG media timer expiration support:

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

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

2. Type session-router and press Enter.

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

3. Type h248-config and press Enter.

```
ACMEPACKET(session-router)# h248-config
ACMEPACKET(h248-config)#
```

4. Type h248-mg-config and press Enter.

```
ACMEPACKET(h248-config)# h248-mg-config
ACMEPACKET(h248-mg-config)#
```

5. Type port-map and press Enter.

```
ACMEPACKET(h248-mg-config)# port-map
ACMEPACKET(port-map)#
```

6. media-expiration-action—Change this parameter from none (default) to notify-with-netfail if you want the Oracle Communications Session Border Controller to track media timer expiration and notify the MGC should an media expiration occur.
7. Save your work.

# E2 CLF Configurable Timeout

You can configure a transaction timer value for each external policy server based on the round-trip and response times for each specific policy server. Defining this transaction timer value allows you to avoid situations when policy/DIAMETER servers fail to respond to the Oracle Communications Session Border Controller ’s requests, ensuring that transactions proceed in the desired amount of time and avoiding undesirable delays in set-up times.

The time you set for the DIAMETER CLF must be from 1 second to 15 seconds. For purposes of backward compatibility, 15 seconds is the default. It is recommended that you set the timer at 6 seconds or greater in accordance with the smallest DIAMETER Watchdog Request/Answer (DWR/DWA) per RFC 3588.

## Activating a Configuration with the E2 CLF Timeout Defined

When you define a value for the E2 CLF timeout and activate your configuration, the change in time will only affect new client transactions. Previously existing client transactions will use the value in effect prior to your having activated the configuration.

## E2 CLF Timeout Configuration

To define the E2 CLF timeout for an external policy server:

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

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

2. Type media-manager and press Enter.

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

3. Type ext-policy-server and press Enter.

```
ACMEPACKET(media-manager)# ext-policy-server
ACMEPACKET(ext-policy-server)#
```

4. trans-expires—Enter the time (in seconds) for the E2 CLF timeout, a transaction timer value for each external policy server based on the round-trip and response times for each specific policy server. The default for this parameter is 15 seconds; your entry must be between 1 and 15.
5. Save your work.

3

# S-CX6.3.0M3

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net OS Release Version S-CX6.3.0M3.

Current SPL Engine Version: C2.0.1

## Content Map

This section provides a table listing all content in Net-Net OS Release Version S-CX6.3.0M3.

| Content Type | Description |
|---|---|
| Adaptation | Automated Daylight Savings Time (DST) Updates |
| Adaptation | SDP Insertion for (re)INVITEs |
| Adaptation | SBC Communications Monitor - Phase I (Palladion SBC Probe) |
| Adaptation | IPv6 Link Local Address Support |
| Adaptation | Support for 3000 VLANs |
| Adaptation | Alpha Numeric Long Name |
| Defect | Ignoring SDP Version Change on IPSec Card |
| Forward merge | S-CX6.2.0M11 |

## Support for 3000 VLANs

To accomodate 3000 VLANs on the Oracle Communications Session Border Controller , the ARP table is increased to hold 16,000 entries. The complete CAM apportioning scheme is listed below:

| Hardware | Software | Denied | Trusted | Media | Untrusted | Dynamic Trusted | NAT | ARP | VLANs |
|---|---|---|---|---|---|---|---|---|---|
| Net-Net 4500 | S-CX6.3.0M3 | 32000 | 8000 | 64000 | 2000 | 250000 | 114688 | 16384 | 3000 |

| Hardware | Software | Denied | Trusted | Media | Untrusted | Dynamic Trusted | NAT | ARP | VLANs |
|---|---|---|---|---|---|---|---|---|---|
| Net-Net 3800 | S-CX6.3.0M3 | 8000 | 2000 | 32000 | 1000 | 125000 | 49152 | 16384 | 3000 |

# SDP Version Change without SDP Body Change

When an SRTP call is made through the Oracle Communications Session Border Controller and a UE sends a reINVITE, there may be no change in the SDP contents. When the other UE responds, some devices will increment the o= line's session version, despite no SDP change. Normally the change in SDP version indicates that the SDP has changed, which would otherwise require the Oracle Communications Session Border Controller to modify the media flow set-up. In order to leave the media flows unchanged when session version changes but the rest of the SDP does not, an option is configured in the media-manager-config.

If the Oracle Communications Session Border Controller attempts to modify these media flows when unnecessary, calls could be dropped by the system disrupting media packet sequence number synchronization.

The ignore-reinv-session-ver option is set to handle this situation. When configured, the Oracle Communications Session Border Controller compares the current SDP received from a UE against the previously-received SDP from the same UE. If the SDP in the newer and older messages is the same, the Oracle Communications Session Border Controller ignores any changes to the session-version and will not modify the media flow portion of the call.

**Note:** When the SDP change is only a reordering of SDP lines without any other change, the option has no effect.

This option is used only to mitigate compatibility issues when running SRTP calls over any of Acme Packet's IPSec accelerated NIUs for the Net-Net 4500 or 3820. NOT for ETC NIUs.

## SDP Version Change Configuration

To configure media over TCP:

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

   ```
   ACMEPACKET# configure terminal
   ```

2. Type media-manager and press Enter to access the media-level configuration elements.

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

3. Type media-manager and press Enter to begin configuring media over TCP.

   ```
   ACMEPACKET(media-manager)# media-manager
   ACMEPACKET(media-manager-config)#
   ```

4. options — Set the options parameter by typing options, a Space, the option name ignore-reinv-session-ver with a "plus" sign in front of it, and then press Enter.

   ```
   ACMEPACKET(media-manager-config)# options +ignore-reinv-session-ver
   ```

   If you type the option without the "plus" sign, you will overwrite any previously configured options. In order to append the new options to the realm configuration's options list, you must prepend the new option with a "plus" sign as shown in the previous example.

   Save and activate your configuration.

# ACLI Parameter Long String Length

The following parameters may be configured as strings, 128 characters in length. These parameters may also start with a number character.

## media-manager

The following configuration elements and parameters are found under the media-manager path.

| Configuration Element or subelement | Parameter |
|---|---|
| codec-policy | name |
| dns-config | Client-realm |
| dns-config > server-dns-attributes | server-realm |
| ext-policy-server | name<br>realm |
| media-policy | name |
| realm-config | identifier<br>parent-realm<br>dns-realm<br>media-policy<br>Media-sec-policy<br>Class-profile<br>enforcement-profile |
| static-flow | in-realm-id<br>out-realm-id |
| steering-pool | realm-id |
| vbg-config | realm-id |

## security

The following configuration elements and parameters are found under the security path.

| Configuration Element or subelement | Parameter |
|---|---|
| certificate-recorder | name |
| ike> data-flow | name<br>realm-id |
| ike> dpd-params | name |
| ike> ike-interface | Dpd-params-name |
| ike> ike-sainfo | name |
| ike> local-address-pool | name<br>dns-realm- id<br>Data-flow |
| ike> tunnel-orig-params | name |
| ims-aka-profile | name |

| Configuration Element or subelement | Parameter |
|---|---|
| media-media-sec-policy | name |
| media-mikey-policy | name |
| media-sdec-policy | name |
| public-key | name |
| tls-profile | name |

## session-router

The following configuration elements and parameters are found under the session-router path.

| Configuration Element or subelement | Parameter |
|---|---|
| access-control | realm-id |
| call-recording-server | primary-realm<br>secondary-realm |
| class-profile | media-policy |
| class-profile> policy | profile-name |
| enforcement-profile | name |
| enum-config | name<br>realm-id<br>Service-type<br>health-query-number<br>failover-to |
| h248-config> h248-mgc-config | realm-id |
| h248-config> h248-mg-config | realm-id |
| h323> h32h-stack | name<br>realm-id<br>assoc-stack<br>gk-identifier<br>filename |
| local-routing-config | name<br>file-name |
| media-profile | name<br>subname |
| mgcp-config | private-realm<br>public-realm |
| net-management-control | name |

| Configuration Element or subelement | Parameter |
|---|---|
| | next-hop<br>rph-profile |
| qos-constraints | name |
| rph-policy | name |
| rph-profile | name<br>Media-policy |
| session- constraints | name |
| session- router | sr-primary-name<br>sr-secondary-name |
| session-agent | realmid<br>egress-realm-id<br>response-map<br>local-response-map<br>enforcement-profile<br>sip-profile<br>sip-isup-profile |
| session-group | group-name |
| sip-config | Home-realm-id<br>egress-realm-id<br>enforcement-profile |
| sip-interface | realm-id<br>operator-identifier<br>ext-policy-server<br>constraint-name<br>response-map<br>local-response-map<br>enforcement-profile<br>sip-profile<br>sip-isup-profile<br>tunnel-name |
| sip-manipulations | name |
| sip-nat | Realm-id |
| sip-profile | name |
| sip-response-map | name |

| Configuration Element or subelement | Parameter |
|---|---|
| sup-isup-profile | name |
| surrogate-agent | realm-id |

## system

The following configuration elements and parameters are found under the system path.

| Configuration Element or subelement | Parameter |
|---|---|
| network-interface | name |
| phy-interface | name |
| reduncancy> peer | name |
| snmp-user-entry | user-name |

# IPv6 Link Local Addresses

The Oracle Communications Session Border Controller supports IPv6 Link Local addresses configured for a network interface’s gateway.

An IPv6 link local address is signified by its first hextet set to FE80:. Even if a network interface’s first hextet is not FE80, but the gateway is, the Oracle Communications Session Border Controller will still function as expected.

### show neighbor-table

The show neighbor-table command displays the IPv6 neighbor table and validates that there is an entry for the link local address, and the gateway uses that MAC address.

```
System# show neighbor-table
LINK LEVEL NEIGHBOR TABLE
Neighbor                             Linklayer Address  Netif Expire    S
Flags
300::100                             0:8:25:a1:ab:43      sp0 permanent ? R
871962224
400::100                             0:8:25:a1:ab:45      sp1 permanent ? R
871962516
fe80::bc02:a98f:f61e:20%sp0          be:2:ac:1e:0:20      sp0 4s        ? R
871962808
fe80::bc01:a98f:f61e:20%sp1          be:1:ac:1e:0:20      sp1 4s        ? R
871963100
------------------------------------------------------------------------------
ICMPv6 Neighbor Table:
------------------------------------------------------------------------------
------------
  entry: slot port vlan IP                             type       flag
pendBlk Hit MAC
------------------------------------------------------------------------------
------------
  5    : 1    0    0    fe80::bc01:a98f:f61e:20/64     08-DYNAMIC 1
0       1   be:01:ac:1e:00:20
  4    : 1    0    0    0.0.0.0/64                     01-GATEWAY 0
0       1   be:01:ac:1e:00:20
  3    : 1    0    0    400::/64                       02-NETWORK 0
0       1   00:00:00:00:00:00
  2    : 0    0    0    fe80::bc02:a98f:f61e:20/64     08-DYNAMIC 1
0       1   be:02:ac:1e:00:20
  1    : 0    0    0    0.0.0.0/64                     01-GATEWAY 0
```

```
0       1   be:02:ac:1e:00:20
  0    : 0    0    0    300::/64                       02-NETWORK 0
0       1   00:00:00:00:00:00
------------------------------------------------------------------------------
------------
```

# SDP Insertion for (Re)INVITEs

If your network contains some SIP endpoints that do not send SDP in ReINVITEs but also contains others that refuse INVITEs without SDP, this feature can facilitate communication between the two types. The Oracle Communications Session Border Controller can insert SDP into outgoing INVITE messages when the corresponding, incoming INVITE does not contain SDP.

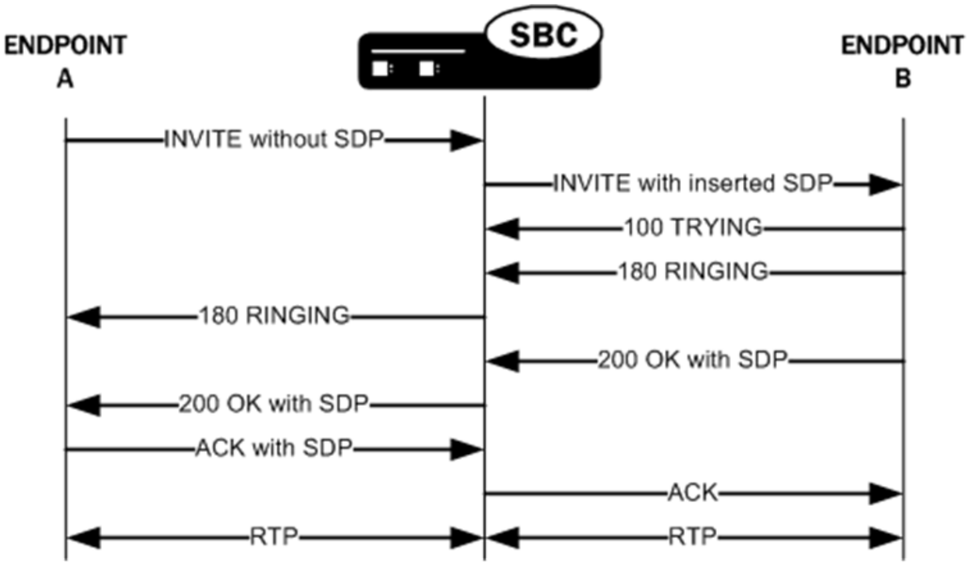
You can also use this feature when the network devices used in H.323-SIP interworking do not include SDP in the INVITEs sent to SIP endpoints. In this case, the Oracle Communications Session Border Controller can insert SDP in the outgoing INVITE messages it forwards to the next hop.

This feature works for either INVITEs, ReINVITEs, or both.

This section explains how the SDP insertion feature works for INVITEs and ReINVITEs. The examples used this section are both pure SIP calls. Even when you want to use this feature for IWF calls, though, you configure it for the SIP side.

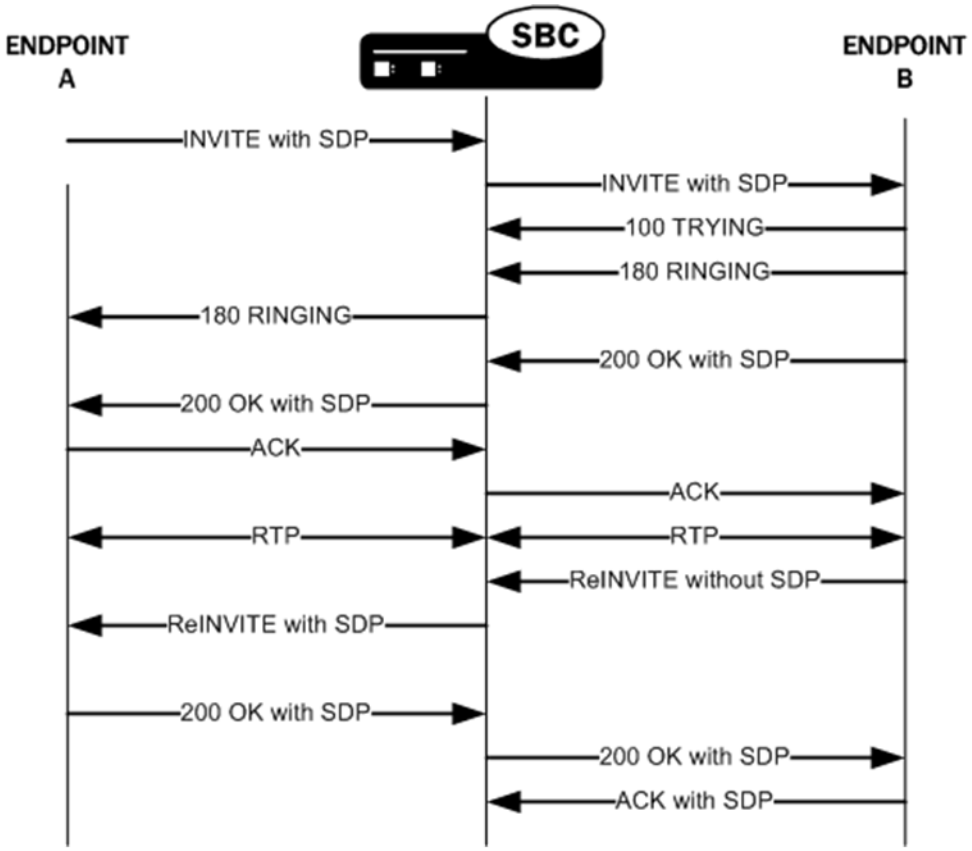
## SDP Insertion for SIP INVITES

The Oracle Communications Session Border Controller inserts SDP into an outgoing INVITE when the corresponding incoming INVITE has none. Because no SDP information is available for the session, the Oracle Communications Session Border Controller uses a media profile from a list of them you configure and then apply for SDP insertion.



## SDP Insertion for SIP ReINVITEs

The section explains SDP insertion for ReINVITEs, using a case where SIP session has been established with an initial INVITE containing SDP. In the diagram below, you can see the initial INVITE results in a negotiated media stream. But after the media stream is established, Endpoint B sends a ReINVITE without SDP to the Oracle Communications Session Border Controller. In this case, theOracle Communications Session Border Controller uses the negotiated media information from the initial INVITE to insert when the ReINVITE has no SDP. It then sends this ReINVITE with inserted SDP to the next hop signaling entity.



## SDP Insertion for SIP INVITEs Configuration

To work properly, SDP insertion for SIP invites requires you to set a valid media profile configuration.

To enable SDP insertion for INVITEs:

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

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

2. Type session-router and press Enter.

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

3. Type sip-interface and press Enter.

```
ACMEPACKET(session-router)# sip-interface
ACMEPACKET(sip-config)#
```

4. add-sdp-invite—Change this parameter from disabled (default), and set it to invite.
5. add-sdp-profile—Enter a list of one or more media profile configurations you want to use when the Net-Net SC inserts SDP into incoming INVITEs that have no SDP. The media profile contains media information the Oracle Communications Session Border Controller inserts in outgoing INVITE.

   This parameter is empty by default.
6. Save and activate your configuration.

## Insertion for SIP ReINVITEs Configuration

In this scenario, theOracle Communications Session Border Controller uses the media information negotiated early in the session to insert after it receives an incoming ReINVITE without SDP. The Oracle Communications Session

Border Controller then sends the ReINVITE with inserted SDP to the next hop signaling entity. You do not need the media profiles setting for ReINVITEs.

To enable SDP insertion for ReINVITEs:

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

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

2. Type session-router and press Enter.

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

3. Type sip-interface and press Enter.

```
ACMEPACKET(session-router)# sip-interface
ACMEPACKET(sip-config)#
```

4. add-sdp-invite—Change this parameter from disabled (default), and set it to reinvite.
5. Save and activate your configuration.

## add-sdp-invite

add-sdp-invite—Enable or disable this SIP interface inserting an SDP into either an INVITE or a REINVITE, or both.

- Default disabled
- Values: disabled—Do not insert an SDP
- invite—Insert an SDP in the invite
- reinvite—Insert an SDP in the reinvite
- both—Insert SDP in both SDP-less invites and reinvites

## Palladion Mediation Engine

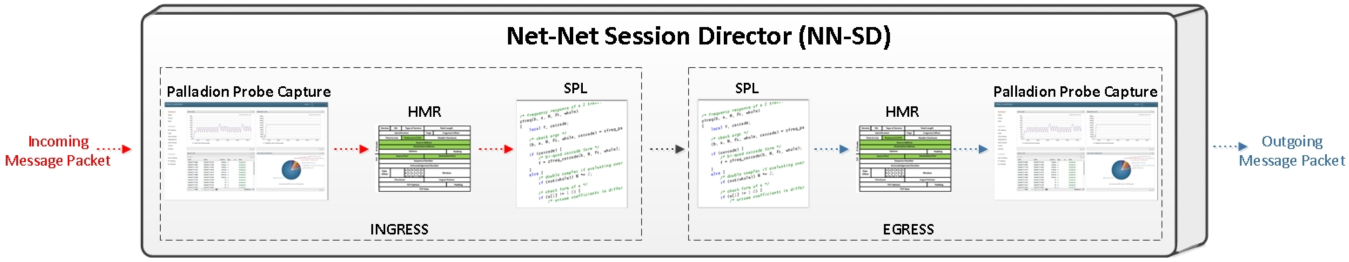
Palladion is Acme Packet’s Communication Experience Manager.

The manager is powered by the Palladion Mediation Engine, a platform that collects SIP, DNS, ENUM, and protocol message traffic received from Palladion Probes. The mediation engine stores the traffic in an internal database, and analyzes aggregated data to provide comprehensive multi-level monitoring, troubleshooting, and interoperability information.

Version E-C[xz]6.4.0 supports an embedded, user-configurable Palladion Communications Monitoring Probe, Version 1. Acting as a Probe, or as an exporter, the Oracle Communications Session Border Controller can:

- Establish an authenticated, persistent, reliable TCP connection between itself and one or more Palladion Mediation Engines.
- Optionally ensure message privacy by encrypting the TCP connection using TLS.
- Use the TCP connection to send a UTC-timestamped, unencrypted copy of a protocol message to the Palladion Engine(s).
- Accompany the copied message with related data to include: the port/vlan on which the message was sent/ received, local and remote IP:port information, and the transport layer protocol.

The following illustration shows how the Palladion Communications Monitor Probe handles incoming and outgoing monitored data on the Net-Net ESD.



# IPFIX

The Net-Net Session Director uses the IPFIX suite of standards to export protocol message traffic and related data to the Palladion Mediation Engine.

- RFC 5101, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*
- RFC 5102, *Information Model for IP Flow Information Export*
- RFC 5470, *Architecture for IP Flow Information Export*
- RFC 5655, *Specification of the IP Flow Information Export (IPFIX) File Format*
- RFC 5815, *Definitions of Managed Objects for IP Flow Information Export*

The IPFIX standards describe the use of templates to format the export of specific types of protocol traffic. The Net-Net Session Director and the Palladion Mediation Engine share ten (10) pre-defined templates that facilitate protocol message exchange, and subsequent processing and analysis by the Palladion Engine.

The pre-defined templates are:

- incoming SIP/DNS over UDP
- incoming SIP over TCP
- incoming SIP over SCTP
- incoming DNS over UDP (entire IP and UDP header not included)
- outgoing SIP/DNS over UDP
- outgoing SIP over TCP
- outgoing SIP over SCTP
- outgoing DNS over UDP (entire IP and UDP header not included)
- media qos and flow record
- IPFIX handshake (used for connection establishment)

# Communications Monitor Configuration

Communications Monitor configuration consists of the following steps.

1. Configuration of one or more Oracle Communications Session Border Controller/Palladion exporter/collector pairs.

   Configuration of the -config object, which defines common operations across all interfaces, is not required. Default values can be retained to enable standard service.
2. Optional assignment of a TLS profile to an exporter/collector pair.

   **Note:** The Palladion Communications Monitor Probe communicates over the media interface for signaling and Quality of Service (QoS) statistics using IPFIX. QoS reporting is done via Call Detail Records (CDR) (accounting).

## Communication Monitor

Use the following procedure to configure communication monitoring:

1. From superuser mode, use the following ACLI sequence to access comm-monitor configuration mode. From comm-monitor mode, you establish a connection between the Oracle Communications Session Border Controller, acting as an exporter of protocol message traffic and related data, and a Palladion Mediation Engine, acting as an information collector.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)# system
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)# comm-monitor
   ACMEPACKET(comm-monitor)#
   ```

2. Use the state parameter to enable or disable communication monitoring.

   Communication monitoring is disabled by default.

   ```
   ACMEPACKET(comm-monitor)# state enabled
   ACMEPACKET(comm-monitor)#
   ```

3. Use the sbc-group-id parameter to assign an integer value to the Oracle Communications Session Border Controller, in its role as an information exporter.

   Retain the default value (0) or assign another integer value.

   ```
   ACMEPACKET(comm-monitor)# sbc-group-id 5
   ACMEPACKET(comm-monitor)#
   ```

4. Use the network-interface parameter to specify the network interface whose traffic will be exported to the Palladion Mediation Engine.

   To specify a media interface (the usual case):

   ```
   ACMEPACKET(comm-monitor)# network-interface m01
   ACMEPACKET(comm-monitor)#
   ```

   To specify the wancom0 management interface (supported, but not generally used):

   ```
   ACMEPACKET(comm-monitor)# network-interface wancom0:0
   ACMEPACKET(comm-monitor)#
   ```

5. If the network interface specified in Step 4 is a media interface, you can optionally use TLS to encrypt the exported traffic and related data.

   To enable TLS encryption, use the tls-profile parameter to identify a TLS profile to be assigned to the network interface. The absence of an assigned TLS profile (the default state) results in unencrypted transmission.

   Refer to *TLS Profile Configuration* for configuration details.

   ```
   ACMEPACKET(comm-monitor)# tls-profile commMonitor
   ACMEPACKET(comm-monitor)#
   ```

6. Use the qos-enable parameter to enable or disable to export of RTP, SRTP, and QOS data flow information.

   ```
   ACMEPACKET(comm-monitor)# qos-enable enabled
   ACMEPACKET(comm-monitor)#
   ```

7. Use the monitor-collector parameter to move to monitor-collector configuration mode.

   While in this mode you identify a Palladion Mediation Engine (a receiver of exported data) by IP address and port number.

   ```
   ACMEPACKET(comm-monitor)# monitor-collector
   ACMEPACKET(monitor-collector)#
   ```

8. Use the address and port parameters to specify the IP address and port number monitored by a Palladion Mediation Engine for incoming IPFIX traffic.

   Enter an IPv4 address and a port number with the range 1025 through 65535, with a default value of 4739.

   ```
   ACMEPACKET(monitor-collector)# address 172.30.101.239
   ACMEPACKET(monitor-collector)# port 4729
   ACMEPACKET(monitor-collector)#
   ```

9. Use done and exit to return to comm-monitor configuration mode.

10. Use done, exit, and verify-config to complete configuration.
11. Repeat Steps 1 through 10 to configure additional as required.

## TSCF Rekey Profile Configuration

Rekeying is a cryptographic technique that enhances security by enforcing the negotiation of existing keys on an ongoing secure connection. Rekeying can be either time-based, in which case new keys are negotiated at the expiration of a timer, or traffic-based, in which case new keys are negotiated when a threshold byte count is exceeded.

Use the following procedure to configure an optional tscf-rekey-profile. Later, you will assign the profile to a specific TSCF interface. If you do not intend to enforce re-keying, this procedure can be safely ignored.

1. From superuser mode, use the following command sequence to access tscf-rekey-profile configuration mode.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# security
ACMEPACKET(security)# tscf
ACMEPACKET(tscf)# tscf-rekey-profile
ACMEPACKET(tscf-rekey-profile)#
```

2. Use the name parameter to provide a unique identifier for this tscf-rekey-profile.

```
ACMEPACKET(tscf-rekey-profile)# name tscfRekey01
ACMEPACKET(tscf-rekey-profile)#
```

3. Use the initiator parameter to identify the rekey initiator.

Supported values are client (default) | server (the Session Director)

```
ACMEPACKET(tscf-rekey-profile)# initiator client
ACMEPACKET(tscf-rekey-profile)#
```

4. Use the max-rekey-time parameter to specify the maximum interval (in minutes) between re-keying operations.

Supported values are 0 (default) | 30 - 1440 (minutes)

The default value, 0, specifies that time-based rekeying is not enforced; other integer values specify that time-based re-keying must be initiated by the tunnel endpoint designated by the initiator parameter.

```
ACMEPACKET(tscf-rekey-profile)# max-rekey-time 30
ACMEPACKET(tscf-rekey-profile)#
```

5. Use the max-rekey-data parameter to specify the maximum traffic exchange (measured in Kb) between rekeying operations.

The default value, 0, specifies that traffic-based rekeying is not enforced; other integer values specify that traffic-based re-keying must be initiated by the tunnel endpoint designated by the initiator parameter.

```
ACMEPACKET(tscf-rekey-profile)# max-rekey-data 0
ACMEPACKET(tscf-rekey-profile)#
```

6. Use done, exit, and verify-config to complete tscf-rekey-profile configuration.
7. Repeat Steps 1 through 6 to configure additional tscf-rekey-profiles as required.

## TLS Profile Configuration

Use the following procedure to configure a tls-profile that identifies the cryptographic resources, specifically certificates and protocols, required for the establishment of a secure/encrypted connection between the Oracle Communications Session Border Controller and the Palladion Mediation Engine.

1. From superuser mode, use the following command sequence to access tls-profile configuration mode.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# security
ACMEPACKET(security)# tls-profile
ACMEPACKET(tls-profile)#
```

2. Use the name parameter to provide a unique identifier for this tls-profile.

```
ACMEPACKET(tls-profile)# name commMonitor
ACMEPACKET(tls-profile)#
```

3. Use the required end-entity-certificate parameter to specify the name of the certificate-record configuration that identifies the credential (specifically, an X509.v3 certificate) offered by the Net-Net Session Director in support of its asserted identity.

   ```
   ACMEPACKET(tls-profile)# end-entity-certificate commMonitor509
   ACMEPACKET(tls-profile)#
   ```

4. Use the required trusted-ca-certificates  parameter to compile a list or one or more certificate-record configuration elements referencing trusted Certification Authority (CA) certificates used to authenticate the offered certificate. These referenced certificates are conveyed to the Palladion Mediation Engine as part of the TLS exchange.

   Provide a comma separated list of existing CA certificate-record configuration elements.

   ```
   ACMEPACKET(tls-profile)# trusted-ca-certificates verisignClass3-
   a,verisignClass3-b,baltimore,thawtePremium,acme-CA
   ACMEPACKET(tls-profile)#
   ```

5. Retain the default value, all, for the cipher-list parameter.

6. Use the verify-depth  parameter to specify the maximum number of chained certificates that will be processed while authenticating end-entity certificate received from the Palladion Mediation Engine.

   Provide an integer within the range 1 through 10 (the default).

   The Oracle Communications Session Border Controller supports the processing of certificate chains (consisting of an end-entity certificate and some number of CA certificates) when X.509v3 certificate-based authentication is used. The following process validates a received TLS certificate chain.

   a) Check the validity dates (Not Before and Not After fields) of the end certificate. If either date is invalid, authentication fails; otherwise, continue chain validation

   b) Check the maximum length of the certificate chain (specified by verify-depth). If the current chain exceeds this value, authentication fails; otherwise, continue chain validation.

   c) Verify that the Issuer field of the current certificate is identical to the Subject field of the next certificate in the chain. If values are not identical, authentication fails; otherwise, continue chain validation.

   d) Check the validity dates (Not Before and Not After fields) of the next certificate. If either date is invalid, authentication fails; otherwise, continue chain validation.

   e) Check the X509v3 Extensions field to verify that the current certificate identifies a CA. If not so, authentication fails; otherwise, continue chain validation.

   f) Extract the Public Key from the current CA certificate. Use it to decode the Signature field of the prior certificate in the chain. The decoded Signature field yields an MD5 hash value for the contents of that certificate (minus the Signature field).

   g) Compute the same MD5 hash. If the results are not identical, authentication fails; otherwise, continue chain validation.

   h) If the hashes are identical, determine if the CA identified by the current certificate is a trust anchor by referring to the trusted-ca-certificates attribute of the associated TLS-profile configuration object. If the CA is trusted, authentication succeeds. If not, return to Step 2.

   ```
   ACMEPACKET(tls-profile)# verify-depth 8
   ACMEPACKET(tls-profile)#
   ```

7. Use the mutual-authenticate parameter to enable or disable (the default) mutual authentication.

   Protocol requirements mandate that the server present its certificate to the client application. Optionally, the server can implement mutual authentication by requesting a certificate from the client application, and authenticating the certificate offered by the client.

   Upon receiving a server certificate request, the client application must respond with a certificate; failure to do so results in authentication failure.

   ```
   ACMEPACKET(tls-profile)# mutual-authenticate disabled
   ACMEPACKET(tls-profile)#
   ```

8. Retain the default value, compatibility, for the tls-version parameter.

9. Retain default values for all other parameters.
10. Use done, exit, and verify-config to complete tls-profile configuration.
11. Repeat Steps 1 through 10 to configure additional tls-profiles as required.

# Automated Daylight Savings Time (DST) Updates

In addition to configuring DST at the command prompt, the Oracle Communications Session Border Controller provides a mechanism to create static or rules-based time updates to reflect your location’s seasonal Daylight Savings Time changes. This configuration offsets the Oracle Communications Session Border Controller ’s internal time, obtained via NTP or from ACLI configuration. When DST is configured as a configuration element, it is persistent across reboots.

When the DST start date/time is reached, 1 hour is added to the system clock. When the DST end date/time is reached, 1 hour is subtracted from the system clock.

## Baseline Configuration

To complete automated DST configuration, you must give a name to the time zone that this system adheres to and the minutes from UTC (offset) from UTC, entered as +/-720.

## Static DST Updates

You can configure the Oracle Communications Session Border Controller to enact and rescind DST offset on a predefined start and stop date. This is set with the following parameters:

dst start/end rule — This parameter is set to static when configuring static DST start and end times.

dst start/end month — The month when DST offset begins or ends, entered as 1-12.

dst start/end day — The day of the month when DST offset begins or ends, entered as 1-31.

dst start/end hour — The hour on the chosen day when DST offset starts or ends, entered as 0-23.

## Rules-based DST Updates

You can configure the Oracle Communications Session Border Controller to enact and rescind DST offset based on rules that correspond to relative dates in a month. That is, start and stop dates can be the Nth (or last) day-name, in a calendar month, as opposed to a day-number of the month.

dst start/end rule — This parameter is set to ordinal number of the start/stop weekday when configuring rules-based DST start and end times. This parameter is entered as: first | second | third | fourth | last.

dst start/end month — The month when DST offset begins or ends, entered as 1-12.

dst start/end weekday — The named day when DST offset begins or ends, entered as: sunday | monday | tuesday | wednesday | thursday | friday | saturday.

dst start/end hour — The hour on the chosen day when DST offset starts or ends, entered as 0-23.

dst start/end day is not configured when entering rules based DST updates.

## DST Update Examples

The current DST rule for North America is that daylight savings starts on the second Sunday in March at 2:00am and ends on the first Sunday in November at 2:00am. Thus the settings for the Eastern Time Zone would be as follows:

```
name                =  EST
minutes-from-utc    =  300
dst-start-month       =  3
dst-start-day         =  1
dst-start-weekday   =  sunday
dst-start-hour       =  2
```

```
dst-start-rule     =  second
dst-end-month       =  11
dst-end-day         =  1
dst-end-weekday       =  sunday
dst-end-hour       =  2
dst-end-rule         =  first
```

**Note:** The dst-start-day and dst-end-day values are ignored.

The European Union directive states that DST starts on the last Sunday in March at 1:00am UTC and ends on the last Sunday in October at 1:00am UTC. Therefore the timezone settings for the UK would be:

```
name                =  GMT
minutes-from-utc    =  0
dst-start-month       =  3
dst-start-day         =  1
dst-start-weekday   =  sunday
dst-start-hour       =  1
dst-start-rule     =  last
dst-end-month       =  10
dst-end-day         =  1
dst-end-weekday       =  sunday
dst-end-hour       =  2
dst-end-rule         =  last
```

Note the dst-end-hour is 2 because this is the local time and 2am BST is 1am UTC.

## Legacy time zone Command Interaction

The existing timezone-set command interacts with the same system structures as explained here. When executing the timezone-set command, the Oracle Communications Session Border Controller prints a warning message to the ACLI and queries you if you wish to overwrite the configuration. For example:

```
ACMEPACKET# timezone
Warning - a timezone configuration element exists and may overwrite this
setting.
This element is now configurable in the system timezone configuration group.
Do you wish to continue ?
```

## timezone Configuration

To configure the timezone-config:

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

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

2. Type system and press Enter.

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

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

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

4. name—Enter the time zone name where this Net-Net SBC resides.
5. minutes-from-utc—Enter the offset from UTC in minutes. Valid values are +/-720 (a “plus” is not required when entering a positive offset.
6. dst-start-rule—Enter static when configuring a static DST start date or the ordinal position of the configured dst-start-weekday parameter when configuring a rules-based DST offset. Valid values are:

   ```
   disabled | static | first | second | third | fourth | last
   ```

7. dst-start-month—Enter the month number that DST starts
8. dst-start-day—Enter the day number of the month when DST starts. This parameter is only configured in static DST rules.
9. dst-start-weekday—Enter the day name when DST starts. This parameter is only configured in non-static DST rules.
10. dst-start-hour—Enter the hour when DST starts.
11. dst-end-rule—Enter static when configuring a static DST end date or the ordinal position of the configured dst-end-weekday parameter when configuring a rules-based DST offset. Valid values are:

    ```
    disabled | static | first | second | third | fourth | last
    ```
12. dst-end-month—Enter the month number when DST ends.
13. dst-end-day—Enter the day number of the month when DST ends. This parameter is only configured in static DST rules.
14. dst-end-weekday—Enter the day name when DST ends. This parameter is only configured in non-static DST rules.
15. dst-end-hour—Enter the hour when DST ends.
16. Type done to save your configuration.

# Maintenance

## show time zone

The show timezone command displays the DST settings. If rules-based DST configuration is used, the Oracle Communications Session Border Controller converts the rule into the absolute DST start or end time for the current year. For example:

```
ACMEPACKET# show timezone
Timezone name: CST
Minutes from UTC(negative if past UTC): -360
Date and hour daylight saving time begins(mmddHH): 031100
Date and hour daylight saving time ends(mmddHH): 110400
```

# timezone-config

The timezone-config element is used to configure the system’s timezone, UTC offset, and DST dates or rules.

## Syntax

```
timezone-config <name | minutes-from-utc | dst-start-rule | dst-start-month |
dst-start-day | dst-start-weekday | dst-start-hour | dst-end-rule | dst-end-
month | dst-end-day | dst-end-weekday | dst-end-hour>
```

## Parameters

name — Name for this configuration element as the timezone for this system.

minutes-from-utc — UTC offset for this timezone in minutes.

- Default 0
- Values: Min: -720 / Max: 720

dst-start-rule — How the DST rule is implemented. If set to static, dst-start-month, dst-start-day, and dst-start-hour are used; the dst-start-weekday parameter is ignored. If set to an ordinal number, the dst-start-weekday is used and the dst-start-day parameter is ignored.

- Default disabled

- Values: first | second | third | fourth | last | static | disabled

dst-start-month — Month when DST goes into affect adding one hour to the system clock.

- Default 1
- Values: Min: 1 / Max: 12

dst-start-day — Day of the month when DST goes into affect adding one hour to the system clock. Only used when dst-start-rule is set to static.

- Default 1
- Values: Min: 1 / Max: 31

dst-start-weekday — Named day of the week when DST goes into affect adding one hour to the system clock. Only used in conjunction with the dst-start-rule parameter set to an ordinal number identifying the precise calendar day.

- Default sunday
- Values: sunday | monday | tuesday | wednesday | thursday | friday | saturday

dst-start-hour — Hour on the day when DST goes into affect adding one hour to the system clock.

- Default 0
- Values: Min: 0 / Max: 23

dst-end-rule — How the DST rule is implemented. If set to static, dst-end-month, dst-end-day, and dst-end-hour are used; the dst-end-weekday parameter is ignored. If set to an ordinal number, the dst-end-weekday is used and the dst-end-day parameter is ignored.

- Default disabled
- Values: first | second | third | fourth | last | static | disabled

dst-end-month — Month when DST ends and subtracts one hour from the system clock.

- Default 1
- Values: Min: 1 / Max: 12

dst-end-day — Named day of the month when DST ends and subtracts one hour from the system clock. Only used in conjunction with dst-start-rule set to an ordinal number identifying the precise calendar day.

- Default sunday
- Values: sunday | monday | tuesday | wednesday | thursday | friday | saturday

dst-end-weekday — Named day of the week when DST ends and subtracts one hour from the system clock. Only used in conjunction with the dst-start-rule parameter set to an ordinal number it identify the precise calendar day.

- Default sunday
- Values: sunday | monday | tuesday | wednesday | thursday | friday | saturday

dst-end-hour — Hour on the day when DST ends and subtracts one hour from the system clock.

- Default 0
- Values: Min: 0 / Max: 23

### Path

timezone-config is an element in the system path. The full path from the topmost ACLI prompt is: configure terminal > system > timezone-config.

### Release

First appearance: S-CX6.3.0M3

### RTC Status

### Notes

This is a single instance configuration element.

# 4

# S-CX6.3.0M4

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net OS Release Version S-CX6.3.0M4.

Current SPL Engine Version: C2.0.1

Current patch baseline: S-CX6.3.0M3p3

## Content Map

This section provides a table listing all content in Net-Net OS Release Version S-CX6.3.0M4.

| Content Type | Description |
|---|---|
| Defect | Latching and stream mode set to inactive |
| Library Update | Update to latest version of OpenSSL library |

## BG RTP Flow Installed When mode=inactive

By default, the Oracle Communications Session Border Controller does not install an RTP flow for H.248 calls that contain SDP mode =inactive. H.248.37 indicates that when call is signaled with sdp mode= inactive, both RTP and RTCP flows should be installed. To explicitly set the system to install both flows, add the install inactive nat flow option in the bgf config configuration element.

### Prerequisites

To ensure individual flows are installed for RTP and RTCP, add the hnt-rtcp =enabled option in the media-manager-config. This ensures that nat-flows are installed as un-collapsed.

### BG RTP Flow Configuration

To configure an RTP flow for H.248 calls with SDP = inactive:

**1.** Navigate to the sip-config configuration element.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# media-manager
ACMEPACKET(media-manager)# bgf-config
ACMEPACKET(bgf-config)#
```

2. Type select to begin configuring this object.

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

3. options—Configure the install-inactive-nat-flow option:

```
ACMEPACKET(bgf-config)# options +install-inactive-nat-flow
ACMEPACKET(bgf-config)#
```

4. Save and activate your configuration.

# 5

# S-CX6.3.0M5

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net OS Release Version S-CX6.3.0.

Current SPL Engine Version: C2.0.2

Current patch baseline: S-CX6.3.0M4p2

## Content Map

This section provides a table listing all content in Net-Net OS Release Version S-CX6.3.0M5.

| Content Type | Description |
|---|---|
| Library Update | Updates SPL engine to version C2.0.2 |