Oracle® Enterprise Session Border Controller

Release Notes

Release E-CX6.4.0

Formerly Net-Net Enterprise Session Director

May 2014

About this Guide

Overview

These *Oracle® Enterprise Session Border Controller Release Notes* support Release E-C[xz]6.4.0*.*

These Release Notes describe the general availability release of software version E-C[xz]6.4.0. The release continues to provide the Enterprise industry, the platform availability of three distinct editions, with each edition targeted toward a specific network environment:

- The **Server Edition**, targeted for distributed small to medium enterprises, runs on a certified server to support a maximum of 1000 concurrent SIP audio calls.
- The **VM Edition**, also targeted for distributed small to medium enterprises, runs on a generic server within a virtualized environment to support a maximum of 250 concurrent SIP audio calls per Virtual Machine (VM).
- The **Oracle Hardware Edition**, targeted for medium to large enterprises, runs on Oracle purpose-built hardware, specifically the Net-Net 3800 SBC and Net-Net 4500 SBC, to support a maximum of 16,000 concurrent SIP audio calls.

This guide provides an overview of features and functions new in Release E-C[xz]6.4.0. It also includes fixed issues since E-C[xz]6.4.0F2, and known issues and limitations in this Release E-C[xz]6.4.0.

For more information about the features/functions in this release, see the *Oracle® Enterprise Session Border Controller Configuration Guide.*

Audience

These release notes are for the Enterprise users to refer to for new features, fixed issues, known issues, and limitations.

Supported Platforms

This guide supports the Acme Packet 3800 and the Acme Packet 4500 C-series platforms, as well as the Enterprise Session Border Controller-Server Edition and Virtual Machine Edition. For more information about these platforms, see the *Oracle® Enterprise Session Border Controller Configuration Guide.*

Related Documentation

The following table lists related documents that are new to E-C[xz]6.4.0.

Document Name	Document Description
Enterprise Session Border Controller Web GUI User Guide	Contains information managing your device using the on-board web GUI.
Enterprise Session Border Controller Configuration Guide	Contains information about the administration, management, and software configuration of the SBC for Enterprises and Service Providers.

The following table lists related S-C[x]6.3.0 documents you can use as reference.

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

Document Name	Document Description
HDR Resource Guide	Contains information about the SBC's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the SBC's support for its Administrative Security license.

Revision History

This section contains a revision history for this document.

Date	Revision Number	Description
April 24, 2013	Revision 1.00	• Release of E-C[xz]6.4.0
August 22, 2013	Revision 1.01	• Active Directory was inadvertently left out of these Release Notes (but was in the Released E-C[xz]6.4.0 Configuration Guide as a new feature in E-C6.4.0). Added Active Directory feature to these Release Notes.
May 1, 2014	Revision 1.02	• Adds item to Features not Supported Section

Contents

Release E-C[xz]6.4.0

Platforms Supported

Release E-C[xz]6.4.0 runs on the following platforms:

- Oracle Hardware: Net-Net 3800 and Net-Net 4500
- Server Edition (SE): HP ProLiant DL120 G7, HP ProLiant DL320e G8, Dell PowerEdge R210 II
- Virtual Machine Edition (VME): VMWare=Preferred, and Hyper-V

Software Images

This section describes software images for this release.

For Oracle Hardware

If you are using Oracle hardware, use the following software image: nnECxz640.tar. The "x" in the file name corresponds to Oracle hardware.

The minimum revision of hardware bootloader is 1/19/2012 or later.

All Other Hardware or Software-only

If you are using hardware other than Oracle's or running this software as a VM, use the file defined in this section for your needs. The "z" in the file name corresponds to non-Oracle hardware or VM.

- Single system image file: nnECxz640.bz
- Boot Media Creator: nnECxz640-img-usb.exe
- Virtual Machine VMWare: nnECxz640-img-bin.ova
- Virtual Machine Hyper-V: nnECxz640-img-bin.vhd

Well-known Enterprise Configurations will be pre-loaded for [z] builds: SWR-0028-00.tar.

New Features

The Release E-C[xz]6.4.0 is a new Enterprise release for the Net-Net Enterprise Session Director SE-VME. All features made available as part of Release S-C(xz)6.3.9M2, E-C[xz]6.4.0 F1, and E-C[xz]6.4.0 F2 are part of Release E-C[xz]6.4.0.

This section lists the new features available since the E-C[xz]6.4.0F2 Release. The features include:

- VMWare ESXi 5.1 Support (2)
- Personal Profile Manager (PPM) Proxy Support (2)
- SIPREC Ping Support (3)
- SIPREC Re-INVITE Collision and Back-off Support (3)
- Active Directory-based Call Routing (5)
- Session Plug-in Language (SPL) Enhancement (13)
- On-Board Web GUI Enhancements (22)
- Secure Real-Time Protocol (SRTP) for Software (SE/VME) (23)
- Relocation of License Information (26)

A brief description about each of these features is presented below. For more information, refer to the applicable documentation specified.

VMWare ESXi 5.1 Support

The Net-Net ESD now supports VMWare ESXi version 5.1 and is the preferred hypervisor. It supports both network booting and Dynamic Host Configuration Protocol (DHCP), while Hyper-V supports neither. Most importantly, the ESXi 5.1 hypervisor supports up to 250 SIP audio sessions per VM; in contrast, Hyper-V supports a maximum of 50 such sessions per VM.

For more information about VMWare ESXi support, see the *Net-Net® Enterprise Session Director Configuration Guide, Release E-C[xz]6.4.0.*

Personal Profile Manager (PPM) Proxy Support

The Net-Net ESD includes a Personal Profile Manager (PPM) proxy feature. PPM is a web service that runs as part of Avaya Aura Session Manager and Aura System Manager. Local and remote SIP clients may download configuration data from the PPM proxy using SOAP messages over HTTP or HTTPS, enabling soft keys to be customized and contact lists to be loaded. Unfortunately, in enterprise networks certain messages may refer to private IP addresses, which are not routable from remote clients. Oracle now incorporates an application proxy in the Net-Net ESD for such messages, replacing the internal IP addresses with the Net-Net ESD's external SIP interface IP address.

The PPM proxy supports incoming messages over HTTP and HTTPS on a configurable IP address / port. If using HTTPS, the PPM proxy uses a selectable server certificate for Transport Layer Security (TLS).

Remote clients accessing the PPM proxy are authenticated by HTTP digest authentication, using their SIP credentials. The PPM proxy forwards such challenges and responses transparently to the PPM web service for which it is configured.

Since the PPM proxy could potentially be a target of a denial-of-service (DoS) attack, the Net-Net ESD allows you to set DoS rules to protect the proxy port as part of standard configurations.

For more information about how the PPM Proxy support works, see the *Net-Net® Enterprise Session Director Configuration Guide, Release E-C[xz]6.4.0.*

SIPREC Ping Support

On the Net-Net ESD, you can now check the connectivity between the Net-Net ESD and the session recording server (SRS) using two new, optional ping commands via the ACLI:

- **ping-method** - SIP message or method for which to ping the SRS.
- **ping-interval** - Amount of time, in seconds, that the Net-Net ESD waits before it pings the SRS in subsequent intervals. For example, if this parameter is set for 60 seconds, the Net-Net ESD pings the SRS every 60 seconds.

This SIPREC ping is a signal that the Net-Net ESD transmits to the connected SRS requesting a response pertaining to the message type that you specify for the ping-method. It uses the ping-interval to determine how long it should wait before sending another ping to the SRS. Once configured (save and activated) the Net-Net ESD uses this feature to perform SIP-based pinging to determine if the SRS is reachable or not.

For more information about configuring SIPREC pinging, see the *Net-Net® Enterprise Session Director Configuration Guide, Release E-C[xz]6.4.0.*

SIPREC Re-INVITE Collision and Back-off Support

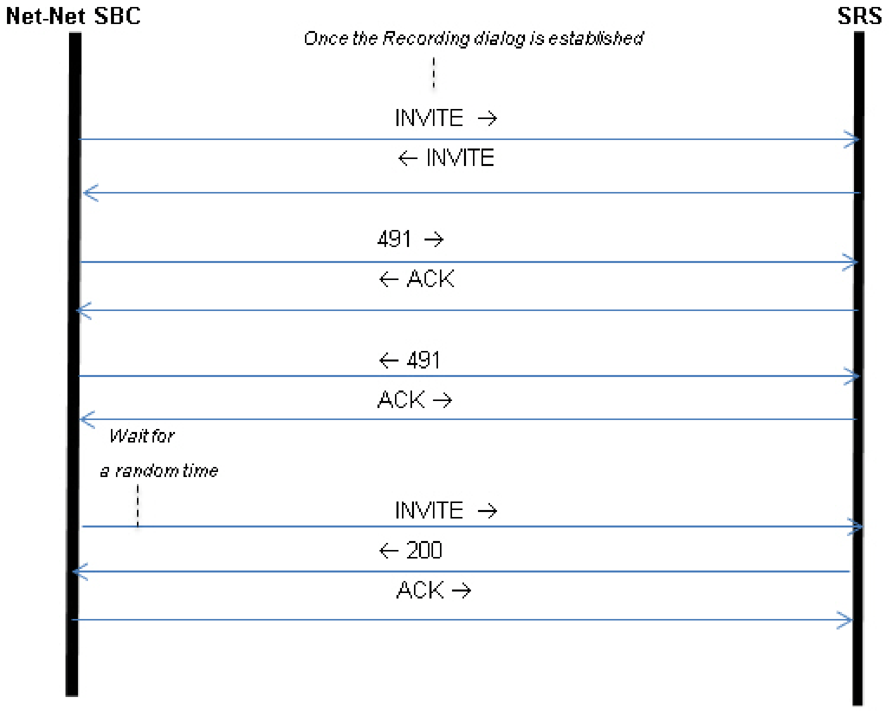
The Net-Net ESD acts a back-to-back User Agent (B2BUA) in all call scenarios. However with SIPREC, the Net-Net ESD acts as a User Agent Client (UAC) when connected with a session recording server (SRS). Therefore, SIP requests can originate from the Net-Net ESD.

During a recording session, when the SRS establishes a recording dialog, the Net-Net ESD and the SRS may send Re-INVITES to each other with updated information. When the Net-Net ESD receives an INVITE while it is still waiting for the response to a previous INVITE it sent out, this produces an INVITE collision.

To avoid an INVITE collision, the Net-Net ESD now sends a “491 Request Pending” response back to the SRS and then waits for a random amount of time before re-trying the INVITE. It also acknowledges (ACK) any 491 response received from the other side. RFC 3261 and RFC 6141 describes the way the User Agent (UA) resolves the INVITE collision. The random wait time is chosen based on the following guidelines from RFC 3261:

- If the UAC is the owner of the Call-ID of the dialog ID (i.e., it generated the value), T (the wait time) is a randomly chosen value between 2.1 and 4 seconds in units of 10 milliseconds.
- If the UAC is not the owner of the Call-ID of the dialog ID (i.e., it did not generate the value), T (the wait time) is a randomly chosen value between 0 and 2 seconds in units of 10 milliseconds.

The following call flow diagram shows the Net-Net ESD’s feature to avoid INVITE collision.



For more information about SIPREC Re-INVITE Collision and Back-off Support, see the *Net-Net® Enterprise Session Director Configuration Guide, Release E-C[xz]6.4.0.*

Active Directory-based Call Routing

A large percentage of Enterprises currently use call servers with Active Directory (Domain Controller) such as Media Servers, Exchange Servers, Lync Servers, etc. For Enterprises that integrate these servers in parallel to their existing communications infrastructure, or transition from their legacy Private Branch Exchange (PBX) to these types of servers, Active Directory becomes a more efficient and cost-effective way of routing the incoming calls within the core Enterprise network.

Clients using Microsoft servers such as a Lync Server deploy their own URI. Therefore, a user in a network with both a desk phone and a Lync client have an IP PBX extension/URI for the desk phone, and a different URI for the Lync client. Currently, all PSTN traffic is sent by default, to a legacy PBX in the core network. If the PBX does not recognize the extension/URI, the PBX forwards it to the Lync client. Sending traffic to the PBX first and then to the Lync Server can be costly in terms of compute resources and/or licensing fees. Routing all incoming sessions from a SIP trunk to the Lync Server first and then to a PBX can be costly.

As a solution, the ESD initiates a query to the Active Directory to initially determine the type of incoming call. The ESD then stores data used to facilitate the routing decision of the call (performed by Lightweight Directory Access Protocol (LDAP)) and then routes the call the first time to the applicable destination (PBX or Lync Server).

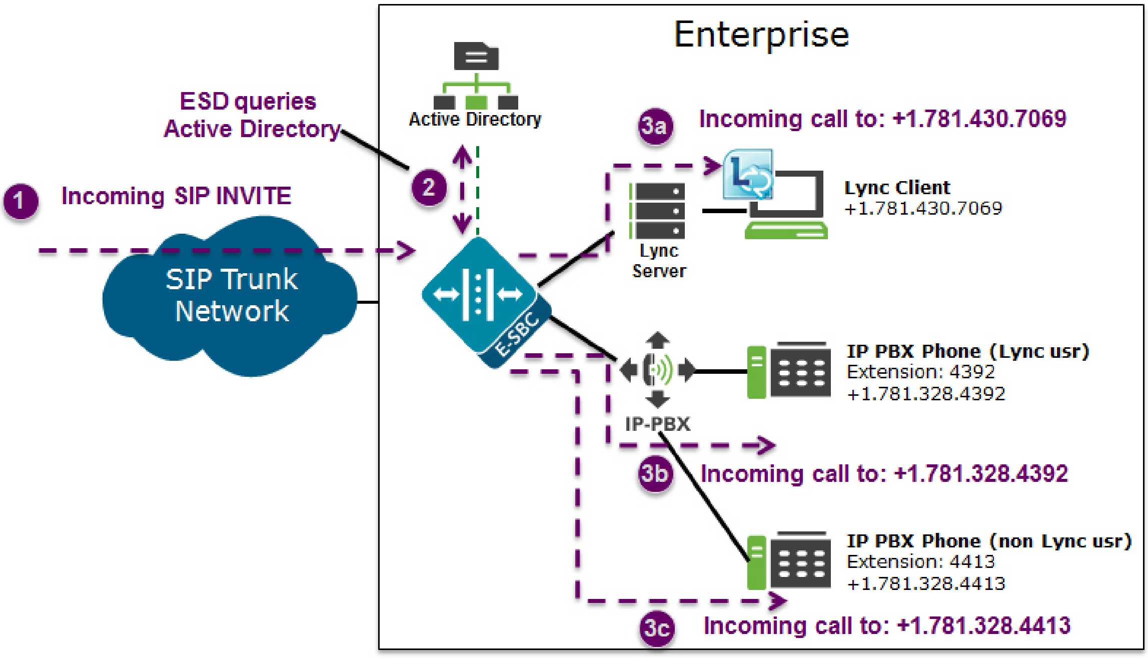
In scenarios where a user has both a Lync phone and a legacy PBX phone, calls destined for the Lync phone number can be routed to the PBX phone number, or calls destined for the PBX phone number can be routed to the Lync phone number. The destination is dependant on the current ESD configuration. The ESD uses the information stored in the Enterprise’s Active Directory, compares it to the ESD configuration and then determines which phone number to utilize for the destined user.

> **Note:** The Active Directory-based call routing feature supports confidential and secure LDAP traffic support by using SSL/TLS (LDAPS).

How it Works

Active Directory-based call routing is a feature of the ESD that facilitates the routing of incoming calls to the appropriate destinations within the Enterprise core network. The ESD's LDAP query to the Active Directory yields whether or not the phone number is associated with a call Server or the PBX.

When the ESD receives an inbound SIP INVITE over a SIP Trunk (1), it checks the current LDAP configuration in the ESD. Depending on this configuration, the ESD then accesses the Enterprise's Active Directory to search for the applicable number being called via an LDAP query (2). When the query has found the number to forward the call, the ESD routes the call directly to the call server client (3a) or to the IP PBX phone (3b) and 3c) as shown in the illustration below.



The Enterprise is responsible for migrating phone numbers from the legacy PBX to the call server by making the necessary updates in their Active Directory in order for the ESD to route the call properly. In the illustration above, the IP PBX extension (4392) is the primary telephone number (+1.781.328.4392); a secondary transition number (+1.781.430.7069) is assigned to Lync.

LDAP in the ESD

Lightweight Directory Access Protocol (LDAP) is the Protocol that the ESD uses to perform queries to the Enterprise's Active Directory to determine where to route incoming calls (to the call server or the IP PBX) in the Enterprise network. Session requests and responses are sent/received based on the ESD's LDAP routing configuration. LDAP determines the destination (call server user or non-call server user) and forwards the call accordingly.

The ESD, using LDAP, performs the following on an inbound call:

- Creates an LDAP search filter based on the dialed number and the configured LDAP attributes.
- Sends an LDAP search query to the configured LDAP Server.
- Creates a route list based on the query response received from the LDAP Server.
- Routes calls to both the call server and the IP PBX. The routing order is dependent on the LDAP attribute configuration and/or whether there was an exact match for the dialed phone number in the Enterprise's Active Directory for the call server or the IP-PBX.

  Note: You configure LDAP Servers, filters, and local policy routing using the ACLI objects and attributes. For more information about configuring LDAP, see Session Plug-in Language (SPL) Enhancement (13).

The ESD keeps a permanent LDAP session open to all configured call servers. It sends an LDAP bind request on all established connections, to those servers. The first call server is considered the primary LDAP Server, and all others are secondary LDAP servers. If a query request sent to the primary server fails, the ESD sends the request to the next configured LDAP Server, until the request is successful in getting a response. If no response is received by the ESD and the ESD cannot find another route successfully, (all ESD configured attributes have been exhausted (local policies, policy attributes, etc.)), it sends a busy to the caller.

LDAP performs call routing based on LDAP attributes configured on the ESD. The **route-mode** attribute setting determines how LDAP handles the called number when accessing the Enterprise's Active Directory. Routing modes can be set to any of the following:

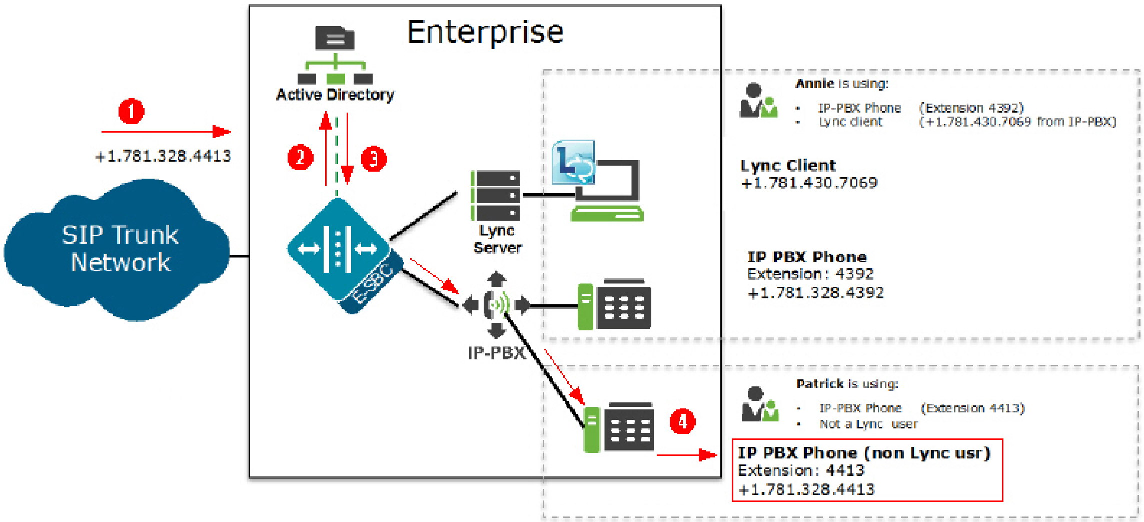
- Exact-match-only (default)
- Attribute-order-only
- Exact-match-first

The following paragraphs describe each of these route-modes.

Exact-match-only

If the LDAP **route-mode** attribute is set to "**exact-match-only**", the ESD performs as follows.

The ESD receives an incoming call to the Enterprise network. If the LDAP route-mode attribute on the ESD is set to "exact-match-only", LDAP queries the Active Directory to find the number that matches exactly to the incoming number. If the number is found, the ESD forwards the call to the client's applicable phone in the Enterprise network.



Number	Description
q	Call comes into the Enterprise network (+1.781.328.4413)
w	Using the configured route-mode of "**exact-match-only**", LDAP queries the exact matching number in the Enterprise's Active Directory.
e	The Active Directory finds the matching number and that number is included in the response to the LDAP query.
r	The ESD forwards the call to the destination phone number (same number as the number that initially called into the Enterprise in Step 1 (+1.781.328.4413)).

Attribute-order-only

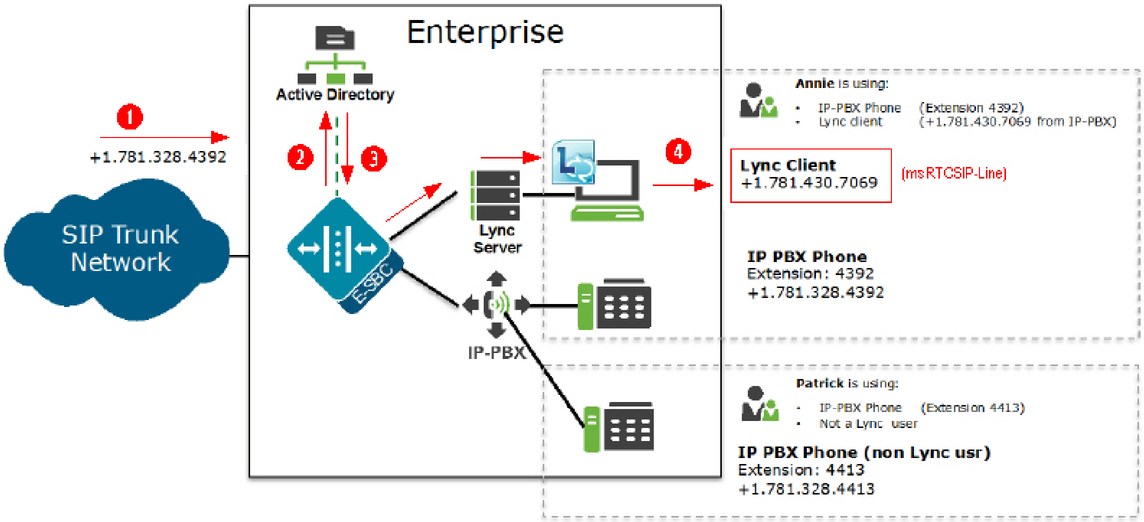
If the LDAP **route-mode** attribute is set to “**attribute-order-only**”, the ESD performs as follows.

The order in which the LDAP attributes are configured on the ESD determines the priority of each route. If an incoming call is destined for the IP-PBX , but the attribute name for a Lync client is configured first, the ESD uses the corresponding next hop (Lync Server) to create the first route in the route list.

> **Note:** An entry in an LDAP search response must have at least one attribute that it matches in the Active Directory.

For example, the incoming phone number could be +1.781.328.4392 (which matches the IP-PBX phone number), and the attribute name “msRTCSIP-Line” (Lync attribute) in the response could be +1.781.430.7069 (Lync phone number). A route is created for the Lync phone number, even though the incoming phone number matches the IP-PBX phone number, since the “msRTCSIP-Line” attribute was configured first. Therefore, the ESD forwards the call to the Lync destination.

Likewise, if an Enterprise uses the same phone number for both Lync and IP-PBX phones, and the attribute-name “msRTCSIP-Line” is configured first (a Lync attribute), the ESD uses the corresponding next hop (Lync Server) to create the first route in the route list.



Number	Description
q	Call comes into the Enterprise network (+1.781.328.4392)
w	Using the configured route-mode of “**attribute-order-only**”, LDAP queries the Active Directory for the matching number.

Number	Description
e	The Active Directory responds with the phone number associated with the first configured LDAP attribute (+1.781.430.7069). In the illustration above, the number was associated with a Lync Client (msRTCSIP-Line) that was configured first in the LDAP configuration.
r	The ESD forwards the call to the applicable destination phone number from the Active Directory response. (+1.781.430.7069).

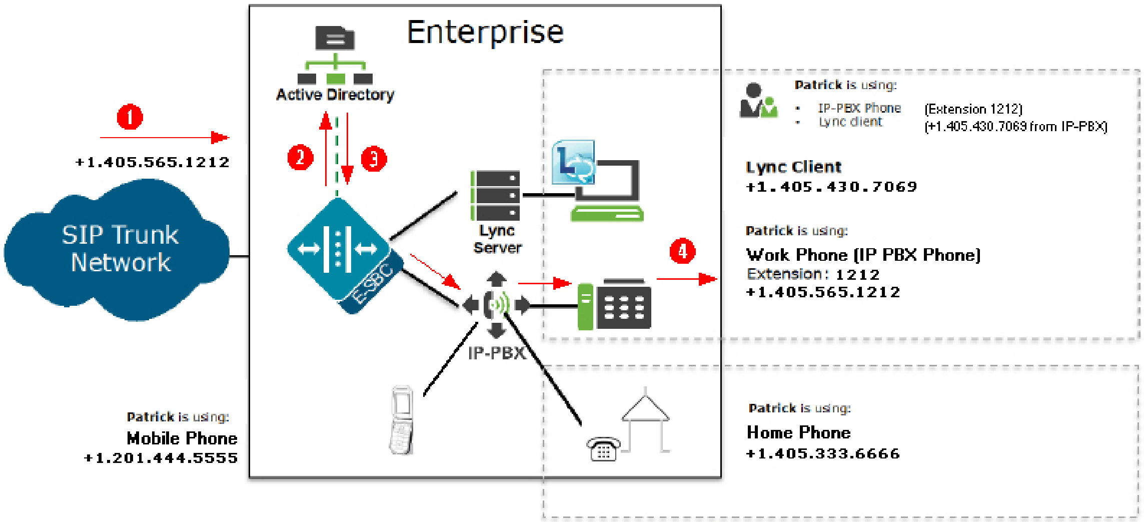
If you configure the attribute name “msRTCSIP-Line” first, the ESD uses the corresponding next hop (Lync Server) to create the second highest priority route in the route list. For example, the dialed telephone number could be +1.781.328.4392 (IP-PBX phone number), and the attribute-name “msRTCSIP-Line” in the response could be +1.781.430.7069 (Lync phone number). A route is created for the Lync phone number, even though the dialed telephone number is the PBX phone number.

Exact-match-first

If the LDAP **route-mode** attribute is set to “**exact-match-first**”, the ESD performs as follows.

When the LDAP query is sent to the Active Directory, the first exact match of the incoming phone number that the LDAP query finds in the Directory, is the number whose corresponding route gets the highest priority in the route list. For all other routes configured on the ESD, the ordering of LDAP attributes in the LDAP configuration determines the priority for each route.

For example, if the incoming number is +1.405.565.1212, and the Active Directory includes a configured mobile number first (+1.201.444.5555), a home number second (+1.405.333.6666) , and a work number third(+1.405.565.1212), the LDAP query searches the mobile number first, then the home number, then finds the exact match on the work phone number. The Active Directory responds with the destination information for the work phone number and the ESD creates a route list with this exact phone number, and then forwards the call accordingly.



Number	Description
q	Call comes into the Enterprise network (+1.405.565.1212)
w	Using the configured route-mode of "**exact-match-first**", LDAP queries the Active Directory for the matching number.
e	The LDAP query searches throughout the Active Directory until it finds the first exact match on the number. Active Directory responds with the exact phone number associated with the incoming number (+1.405.565.1212). In the illustration above, the number was associated with the work phone.
r	The ESD forwards the call to the applicable destination phone number from the Active Directory response. (+1.405.565.1212).

LDAP Messages

If LDAP message logging is enabled in the Active Directory, the ESD sends LDAP messages to a message log called *sipdldap.log*. This log records all received and sent LDAP messages. Messages are in ASCII encoded binary format.

Additionally, when LDAP is invoked for routing, the LDAP messages display in the GUI under the Monitor and Trace tab. For more information about viewing LDAP messages in the GUI, see the *Net-Net Enterprise Session Director Web GUI User Guide.*

> **Note:** The ESD also supports transmitting LDAP messages using the IPFIX Protocol for the Palladion Mediation Engine. For more information about Palladion, see Chapter 19, Communications Monitoring Probe (1169).

LDAP Failure Events

- If an incoming session to a primary phone number routed to Lync fails, the phone number is routed to the IP PBX. If failures occur during LDAP queries for all LDAP Servers, the ESD logs the failure to the *sipdldap.log,* and proceeds with normal configured routing policies, if available.

  Note: The ESD always establishes the TCP/TLS connection towards the configured LDAP server(s). If a TCP connection fails, the ESD continues to attempt to re-establish the connection.

An LDAP connection failure can be due to any one of the following events:

- ESD receives a CANCEL message (LDAP connection termination). The ESD detects this if it receives or issues an 'unbind' operation. The session is then closed down at TCP/TLS.
- ESD receives a call failure message from Lync (TCP/TLS socket termination). If either side receives a “finish” message (FIN) or reset message (RST), the TCP socket closes per standard behavior, which triggers the LDAP layer to detect connection failure. The ESD fails over to a secondary LDAP Server, if configured; otherwise it periodically attempts to reconnect to the Primary LDAP Server.
- ESD is unreachable and SIP session towards Lync times out. User is enabled for Lync but the Lync Server is unreachable by the ESD so a timeout occurs. When consecutive LDAP queries timeout, the ESD concludes that the LDAP session has failed, and then proceeds to terminate the TCP/TLS connection.

  Note: The number of consecutive queries that timeout before a connection is considered failed, and the number of successive query timeouts for each LDAP Server can be set using the ACLI objects and attributes. For more information, see Session Plug-in Language (SPL) Enhancement (13).

ESD Limitations using LDAP

The ESD uses LDAP in the Active Directory when determining the destination of incoming calls. However, the ESD has the following limitations when using LDAP:

- Supports LDAP sessions over the ESD media interfaces only (i.e., not on wancom0).
- Supports LDAPv3 only.
- Establishes a session over the following connections only:
  - LDAP over TCP - default
  - LDAP over TLS (LDAPS)

For information on configuring Active Directory for your network, see the *Net-Net Enterprise Session Director Configuration Guide Release Version E-C[xz]6.4.0*.

Session Plug-in Language (SPL) Enhancement

Your network environment can have unique feature requirements that your Net-Net ESD must accommodate. Your required timeline for the feature must be quick and easy and may not be in line with the next Oracle software delivery schedule. You may have to roll out changes fast with minimal impact to existing users and services because without the new feature, system performance could be affected.

Oracle's solution is the Session Plug-in Language (SPL) tool based on the open scripting language (Lua). An SPL is an executable customized script created to implement a feature on the Net-Net ESD quick and easy. It is an Oracle signed plug-in that integrates with the Net-Net ESD operating system (OS). You can use an SPL to control signaling traffic (including persistent state maintenance). It augments running the software image on the Net-Net ESD, and provides new features when you need them by changing product behavior, but without having to upgrade your software. The SPL is there if you need it. If you don't use the SPL, your Net-Net ESD software performs as normal.

> **Note:** The Net-Net ESD does not load unsigned SPLs or those with invalid signatures.

This enhancement allows the Release E-C[xz]6.4.0 to ship with pre-loaded SPLs.

The following are new SPLs included in this release are:

- Local Media Playback SPL (13)
- Import/Export of Net-Net ESD Configuration SPL (14)
- Lync Emergency Call SPL (15)
- SIPREC Extension Data Enhancements SPL (16)L
- Universal Call Identifier SPL (17)
- Comfort Noise (CN) Generation SPL (19)

Also included are Maintenance and Troubleshooting Commands for SPLs as described in Chapter 23 of the *Net-Net® Enterprise Session Director Configuration Guide, Release E-C[xz]6.4.0.*

The following paragraphs describe each SPL.

Local Media Playback SPL

Commonly, ringback is the media playback of a certain tone informing callers their calls are in progress. In typical deployments, remote endpoints or media servers handle ringback generation, leaving the Net-Net ESD to proxy RTP. When endpoints or media servers do not support ringback generation, the Net-Net ESD becomes responsible for producing it.

> **Note:** The Net-Net ESD supports a maximum of 100 simultaneous playbacks.

You can configure the Net-Net ESD to generate ringback locally, meaning it can produce RTP media on a media flow. The most common use for enabling the system to produce RTP on a media flow is to support locally generated ringback. Since you can also use this capability for music-on-hold, announcements, and interrupting media for notifications, this Net-Net ESD capability is referred to as local playback.

Local playback is controlled through the ACLI using the Local Media Playback SPL configuration.

The Net-Net ESD supports the following playback scenarios:

1. Playback on 183 Session Progress
2. Playback on REFER
3. Playback on header, where the header is P-Acme-Playback

Local media playback is not supported for these Net-Net ESD capabilities:

- SRTP
- Call recording
- SIPREC

Local playback does not work in call flows for which media is released. Concurrent playbacks are limited to 100.

> **Note:** Ringback tones are not recorded with session recording.

For more information about using the Playback SPL in this release, see Chapter 23 in the *Net-Net® Enterprise Session Director Configuration Guide, Release E-C[xz]6.4.0.*

Import/Export of Net-Net ESD Configuration SPL

Release E-C(xz)6.4.0 Final includes an SPL for importing and exporting the NN-ESD configuration from/to a comma-separated value (CSV) file. CSV is a text format file supported by spreadsheet-type applications, such as Microsoft® Excel. You can import a CSV file to the NN-ESD that contains its configuration, or you can export the current configuration on the NN-ESD to the CSV file.

The CSV file format is a text-based format where each "row" is defined on its own line. The items in "columns" are then separated by commas (,). If an entry contains a comma, then it can be enclosed in quotes ("") to prevent it from being treated as a separator. Both the SPL and MS-Excel support enclosing commas in quotes.

> **Note:** The Import/Export SPL is enabled by default in the Release E-C(xz)6.4.0 Final software and no configuration is required.

Import/Export Restrictions

The following table identifies specific restrictions when importing and exporting the NN-ESD configuration.

Import/Export Configuration Restrictions
• Files are read/written to the volatile directory of the file system on the NN-ESD. For 4500, this is the "/ramdrv/" directory. For the NN-ESD, it is the "*/var/*" directory.
• Import and export occurs to/from the editing configuration.
• All error messages are printed to the screen (where the command was issued). Line numbers are provided with the error when possible. • Objects and attributes cannot be set to instances (values) that are not allowed. For instance, you cannot set an IP address to "enabled". Parsing continues as normal after this error. • If an object cannot be written (i.e. key field is missing), then that object is discarded and parsing continues as normal. • The import is additive. Each object that is imported is expected to be new to the configuration. If there is already an object with the same key present, it generates an error 409 and is discarded. Parsing continues as normal after the error.

For more information about using the import/export SPL, see Chapter 23 in the *Net-Net® Enterprise Session Director Configuration Guide, Release E-C[xz]6.4.0.*

Lync Emergency Call SPL

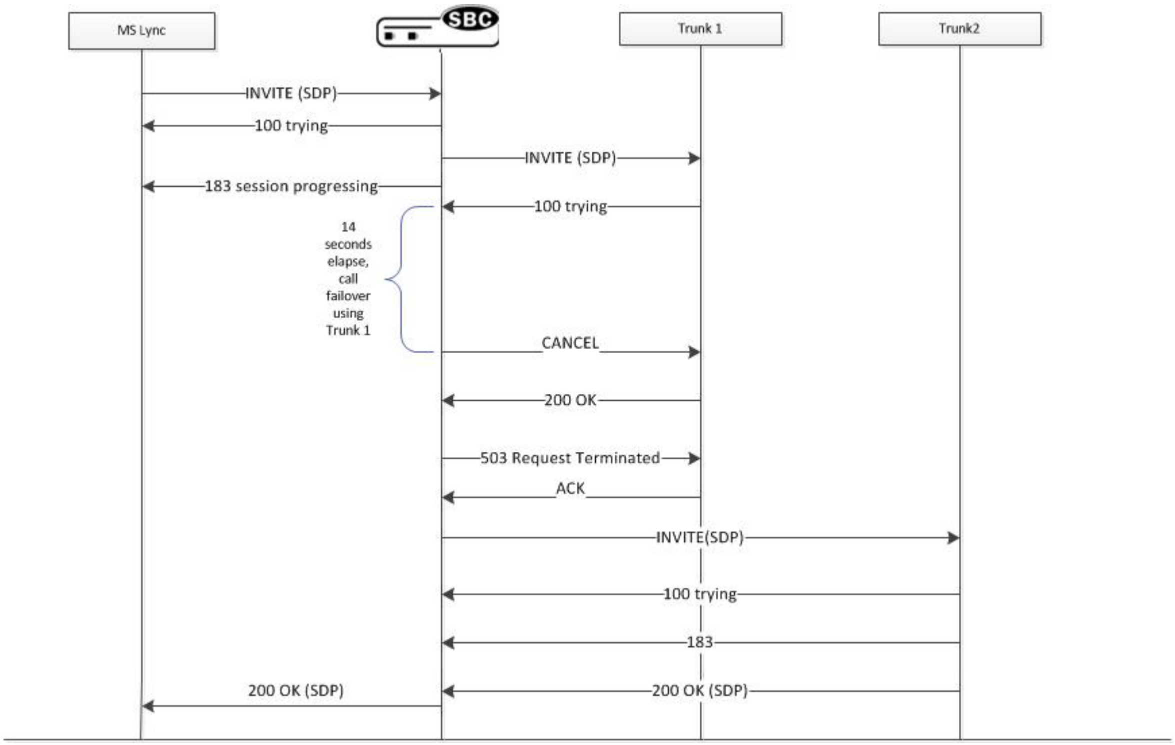
When using the Net-Net ESD as a gateway for E911, service providers may require a Post-dial-delay of at least 6 seconds or greater to receive a 18x message and progress the session. Microsoft Lync emergency calls have an internal timer of 10 seconds to route advance to the alternate gateway in the event no 18x message is received. The Lync Emergency Call SPL responds to initial INVITE with a 183 message, allowing the Net-Net ESD to ensure normal call delivery when there is Post-dial-delay on egress routes that exceed Lync's emergency call timer.

How it Works

When enabled, the **return_183_on_initial_invite** SPL option sends a provisional 183 session progressing message to Lync when the Net-Net ESD receives the initial INVITE request, thus satisfying the 10 second emergency call timer.

The Net-Net ESD monitors the primary and secondary trunks with a SIP OPTIONS ping. If the primary trunk is unavailable, the system will automatically failover to the second destination in session-group and complete the call.

In this example, the Net-Net ESD replies to an emergency call INVITE from Lync with a SIP 183 message. Lync then moves the call and dialog to RFC 3261 Timer C (180 seconds), allowing sufficient time to complete the call and find the nearest PSAP (Public Safety Answering Point) with the primary trunk. In the event that the primary trunk is unavailable (The system monitors the two trunks with a SIP OPTIONS ping), the system will route the emergency call by failing over to a secondary trunk to complete the call.



For more information about using the Lync Emergency Call SPL, see Chapter 23 in the *Net-Net® Enterprise Session Director Configuration Guide, Release E-C[xz]6.4.0.*

SIPREC Extension Data Enhancements SPL

The SIPREC Extension Data Enhancements SPL provides additional header information in the originating SIP messages metadata sent to the Interactive Session Recorder. With this SPL, you can introduce more options for recording policy decisions when using the SIPREC feature of the Net-Net Session Border Controller (SBC). The enhanced metadata also allows for the realm-id to be used as an indicator of the recording account. The SPL also provides configurable values that collect additional header information to store in the metadata.

How it Works

When the SPL is configured, the SIPREC Extension Data Enhancements SPL is only triggered upon INVITE requests, and stores the additional header information in the metadata that is sent to the Net-Net Interactive Session Recorder (NN-ISR). Metadata is a XML MIME attachment that describes recording details to the Net-Net ISR.

By default, the **Extension-Headers** SPL option collects only the Request-URI in a received INVITE. You can store additional header information by configuring the SPL with additional attributes in the **spl-options** under the global **spl-config**.. The values must be in a comma separated list enclosed in double quotation marks. For example:

```
Extension-Headers="P-Asserted-Identity,Diversion"
```

This configuration of the **Extension-Headers** option adds the originating Request-URI along with all P-Asserted-Identity and Diversion-Headers into the participant section of the metadata.

You can configure the **LRE-Identifier** SPL option to add an identifier of the logical remote entity (LRE) that triggered the recording to the <apkt:realm> element of the extension metadata. When configured with a value added, the value appears in place of the identifier. When configured without a value, the identifier of the logical remote entity is used. For example, session-agent will be the hostname, realm-config will be the realm, and sip-interface will be the realm name.

> **Note:** Both options are required for the SPL to function properly.

For more information about using the SIPREC Extension Data SPL, and for an example of the metadata, see Chapter 23 in the *Net-Net® Enterprise Session Director Configuration Guide, Release E-C[xz]6.4.0.*

Universal Call Identifier SPL

The Universal Call Identifier SPL generates or preserves a UCID based on configuration. Once a UCID is generated or preserved, the system adds the value to all subsequent egress SIP requests within the session. You can also set the SPL to remove unwanted UCID headers to avoid duplicity in egress SIP requests.

Using the Universal Call Identifier SPL, you can identify requests within a particular session by manipulating the following vendor specific UCID headers:

- User-to-User
- Cisco-GUID
- Cisco-GUCID

The UCID is added as extension data to the session element of the recording's metadata when using SIPREC.

How it Works

You must configure one of the following SPL options for it to be enabled:

- UCID-App-ID (17)
- GUCID-Node-ID (17)
- GUID-Node-ID (18)

Each SPL option allows you to set an identifying value, as defined by the vendors. The SPL does not validate any input for the SPL options. It is the responsibility of the Administrator to set the correct value.

You may further modify the action of the SPL by adding **replace-ucid** or **convert-to,** to your SPL options.

> **Note:** The replace-ucid and convert-to options have no effect unless you also configure UCID-App-ID, GUID-Node-ID, or GUCID-Node-ID.

UCID-App-ID

The **UCID-App-ID** SPL option allows the Net-Net ESD to examine ingress SIP requests for the "User-to-User" header. When present, the header is transparently passed through the egress SIP message. If set to **replace-ucid** or the header is not present, the system generates a new value for "User-to-User".

You must set the value to a 2-byte hex-ascii value that represents the app ID. All input is truncated to 4 characters. Any characters outside the range of 0-9 and A-F will result in an invalid User-to-User header.

GUCID-Node-ID

The **GUCID-Node-ID** SPL option allows the Net-Net ESD to examine ingress SIP requests for the "Cisco-GUCID" header. When present, the header is transparently passed through the egress SIP message. If set to **replace-ucid** or the header is not present, the system generates a new value for "Cisco-GUCID".

You must set the value to a 48-bit node ID in the version 1 UUID defined by RFC 4122. You can enter the value in decimal or hexadecimal notation. The value must be prefixed with 0x when hexadecimal.

GUID-Node-ID

The **GUID-Node-ID** SPL option allows the Net-Net ESD to examine ingress SIP requests for the Cisco-GUID header. If present, the header is transparently passed through the egress SIP message. The system generates a new value for “Cisco-GUID” if not present or the SPL option is set to **replace-ucid**.

You must set the value to a 48-bit node ID in the version 1 GUID defined by RFC 4122. You can enter the value in decimal or hexadecimal notation. The value must be prefixed with 0x when hexadecimal.

convert-to

The **convert-to** SPL option allows the Net-Net ESD to examine ingress SIP requests for multiple UCID headers. This option has no effect unless appended to another SPL option.

You must set the convert-to SPL option to one of the following values:

- **Avaya**—Removes all Cisco-GUCID and Cisco-GUID headers from egress SIP requests.
- **GUID**—Removes all User-to-User and Cisco-GUCID headers from egress SIP requests.
- **GUCID**—Removes all User-to-User and Cisco-GUID headers from egress SIP requests.

For more information about using the Universal Call Identifier SPL, and for examples of each option, see Chapter 23 in the *Net-Net® Enterprise Session Director Configuration Guide, Release E-C[xz]6.4.0.*

Comfort Noise (CN) Generation SPL

Comfort noise (CN) is the noise in a Real Time Transport Protocol (RTP) message (defined in RFC 3389) that is played to prevent a user from hearing completely dead silence on the connection. The Session Description Protocol (SDP) negotiates this RTP message containing the comfort noise using payload type 13 and an rtpname of "CN".

However, when CN is received, normal RTP ceases. Thus, with no RTP traffic, guard timers may trigger and cause the call to be terminated. To correct this, you can load a Comfort Noise Generation SPL that allows the Net-Net ESD to generate "noise" RTP using the normal audio codec when it receives a CN indication.

The CN Generation SPL must be loaded manually according to the procedures described in “Loading and Enabling the SPL” in Chapter 23 of the *Net-Net® Enterprise Session Director Configuration Guide, Release E-C[xz]6.4.0*. After loading the SPL on the Net-Net ESD, comfort noise is added and removed from the SDP to allow for proper negotiation. If properly negotiated in SDP, CN interworking facility (IWF) is enabled in the media flows allowing the Net-Net ESD to generate noise RTP when CN is received.

> **Note:** CN generation configuration is supported on realms only.

Platforms Supported

CN Generation SPL is supported on the following platforms only:

- Server Edition
- VMWare (preferred hypervisor)
- Hyper-V

Limitations

The following are limitations of the CN Generation SPL:

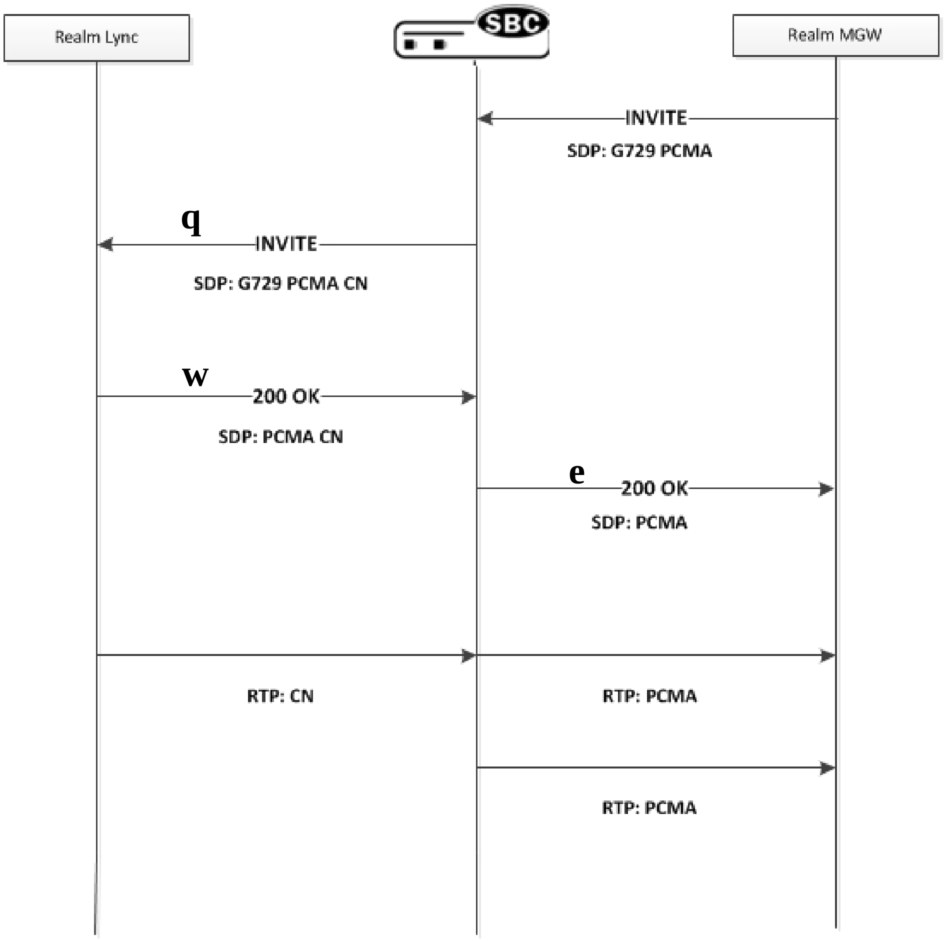
- Supports Pulse Code Modulation u-law (PCMU) and PCM a-law (PCMA) codecs only.
- Supports only 8000Hz.
- Does not support dynamic payload types (i.e. CN must be 13, PCMU = 0 and PCMA = 8).
- Does not support Spiral calls (hairpin).
- Use of codec policies may interfere with the proper negotiation of CN and the enabling of CN generation.
- CN Generation does not handle the following when media is modified (for example, in a re-INVITE):
  - On-hold/call-retrieve: CN does not generate on-hold, and it must be restarted with a new CN message after retrieval.

  - Changing codec/Ptime: CN generation cannot change codec or packetization time while it is generating.

How it Works

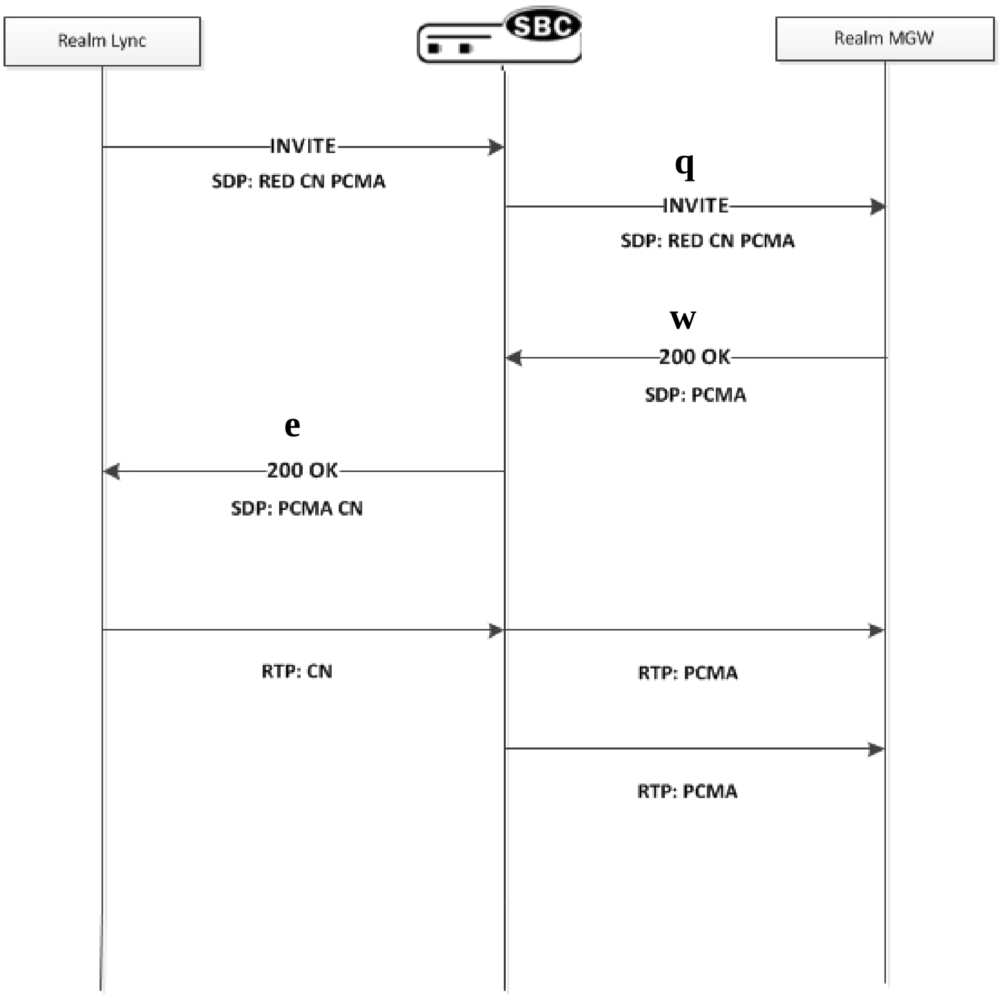
The following describes two different cases of how the Net-Net ESD performs the SDP manipulation using the CN Generation SPL.

Case 1



Process	Description
q	SDP offer received from the realm that has comfort-noise-generate enabled. If the SDP offer contains CN, no IWF is required. If it does not contain CN, and at least one of the offered audio codecs is PCMU or PCMA, CN is added in outgoing SDP offer.
w	If SDP Answer contains the CN codec and topmost audio codec is PCMU or PCMA, Net-Net ESD enables CN IWF.
e	Net-Net ESD strips CN from outgoing SDP Answer.

Case 2



Process	Description
q	SDP offer is sent to a realm that has comfort-noise-generate enabled. If CN was not offered, IWF cannot be performed. If CN is in the offer, the Net-Net ESD forwards the offer to the outbound side.
w	SDP Answer is received from a realm that has comfort-noise-generate enabled. If it contains CN, no IWF is required because both sides support CN. If there is no CN in the Answer, and the topmost audio codec is PCMU or PCMA, the Net-Net ESD enables CN IWF.
e	If CN IWF is enabled, the Net-Net ESD adds CN to the outgoing SDP Answer.

For more information about using the Comfort Noise Generation SPL, see Chapter 23 in the *Net-Net® Enterprise Session Director Configuration Guide, Release E-C[xz]6.4.0.*

On-Board Web GUI Enhancements

The on-board Web GUI is included in this E-C[xz]6.4.0 Release. This Web GUI provides a graphical user interface method for monitoring, managing, and configuring the Net-Net ESD. In addition to the previous SIP Monitor and Trace and System File Managment tabs, the Web GUI now has a Configuration tab that allows you to:

- Configure the Net-Net ESD in Basic Mode which is recommended (drag-and-drop method of configuring the Net-Net ESD)

  or

- For advanced users, configure the Net-Net ESD in Expert Mode (tree configuration method of configuring the Net-Net ESD).

A new Net-Net Session Director Web GUI User Guide has also been added to the Enterprise documentation set.

The Net-Net ESD Web GUI consists of the following components:

- **Configuration** - Allows you to configure specific parameters on the Net-Net ESD in Basic or Expert mode.
- **Monitor and Trace** - Allows you to display SIP session data on one or multiple Net-Net ESDs, and provides traces in a common log format for local viewing or for exporting to your PC.
- **System** - A file management feature that allows you to move specific files (Local Route Table, SPL Plug-In, Playback Media, SIP Trunk Xpress Bootstrap) between the server and your PC. It also allows you to backup your Net-Net ESD configuration and view Log files.

For more information about the on-board Web GUI, see the *Net-Net® Enterprise Session Director Web GUI User Guide.*

Secure Real-Time Protocol (SRTP) for Software (SE/VME)

The Secure Real-Time Transport Protocol, as described in RFC 3711, *The Secure Real-time Transport Protocol (SRTP)*, provides a framework for the encryption and authentication of Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) streams. Both RTP and RTCP are defined by RFC 3550, *RTP: A Transport Protocol for Real-Time Applications*.

Encryption ensures that the call content and associated signalling remains private during transmission. Authentication ensures that (1) received packets are from the purported source, (2) packets are not been tampered with during transmission, and (3) a packet has not been replayed by a malicious server.

Licensing and Hardware Requirements

SRTP/SRTCP support is software-based and requires no special hardware components or licenses

Protocol Overview

While the RFC 3711 framework provides encryption and authentication procedures and defines a set of default cryptographic transforms required for RFC compliance, it does not specify a key management protocol to securely derive and exchange cryptographic keys. RFC 4568, *Session Description Protocol (SDP) Security Description for Media Streams*, defines such a protocol specifically designed to exchange cryptographic material using a newly defined SDP *crypto* attribute. Cryptographic parameters are established with only a single message or in single round-trip exchange using the offer/answer model defined in RFC 3264, *An Offer/Answer Model with the Session Description Protocol*.

> **Note:** The current release provides support for an initial SDP Security Descriptions (SDES) implementation that generates keys used to encrypt SRTP/SRTCP packets. Authentication of packets will be added to a subsequent release.

A sample SDP exchange is shown below:

The SDP *offerer* sends:

```
v=0
o=sam 2890844526 2890842807 IN IP4 10.47.16.5
s=SRTP Discussion
i=A discussion of Secure RTP
u=http://www.example.com/seminars/srtp.pdf
e=marge@example.com (Marge Simpson)
c=IN IP4 168.2.17.12
t=2873397496 2873404696
m=audio 49170 RTP/SAVP 0
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:WVNfX19zZW1jdGwgKCkgewkyMjA7fQp9CnVubGVz|2^20|1:4
```

The SDP *answerer* replies:

```
v=0
o=jill 25690844 8070842634 IN IP4 10.47.16.5
s=SRTP Discussion
i=A discussion of Secure RTP
u=http://www.example.com/seminars/srtp.pdf
e=homer@example.com (Homer Simpson)
c=IN IP4 168.2.17.11
t=2873397526 2873405696

m=audio 32640 RTP/SAVP 0
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4
```

The media-level SDP attribute, *crypto*, describes the cryptographic suite, key parameters, and session parameters for the preceding unicast media line. The crypto attribute takes the form:

```
a=crypto: tag crypto-suite key-parameter [session-parameters]
```

tag

The tag field contains a decimal number that identifies a specific attribute instance. When an offer contains multiple crypto attributes, the answer uses the tag value to identify the accepted offer.

In the sample offer the tag value is 1.

crypto-suite

The crypto-suite field contains the encryption and authentication algorithms, either AES_CM_128_HMAC_SHA1_80 or AES_CM_128_HMAC_SHA1_32.

key-parameter

The key-parameter field contains one or more sets of keying material for the selected crypto-suite and it has following format.

```
"inline:" <key||salt> ["|" lifetime] ["|" MKI ":" length]
```

inline is a method and specifies that the crypto material to be used by the offerer is transmitted via the SDP.

The *key||salt* field contains a base64-encoded concatenated master key and salt.

Assuming the offer is accepted, the key || salt provides the crypto material used by the offerer to encrypt SRTP/SRTCP packets, and used by the answerer to decrypt SRTP/SRTCP packets.

Conversely the key || salt contained in the answer to the offer provides the crypto material used by the answerer to encrypt SRTP/SRTCP packets, and used by the offerer to decrypt SRTP/SRTCP packets.

The *lifetime* field optionally contains the master key lifetime (maximum number of SRTP or SRTCP packets encoded using this master key).

In the sample offer the lifetime value is 1,048, 576 (2^{20}) packets.

The *MKI:length* field optionally contains the Master Key Index (MKI) value and the MKI length.

The MKI is used only when the offer contains multiple keys; it provides a means to differentiate one key from another. The MKI takes the form of an integer, followed by its byte length when included in SRTP/SRTCP packets.

In the sample offer the MKI value is 1 with a length of 4 bytes.

The *session-parameters* field contains a set of optional parameters that may override SRTP session defaults for the SRTP and SRTCP streams.

UNENCRYPTED_SRTP	— SRTP messages are not encrypted
UNENCRYPTED_SRTCP	— SRTCP messages are not encrypted
UNAUTHENTICATED_SRTP	— SRTP messages are not authenticated

When generating an initial offer, the offerer ensures that there is at least one crypto attribute for each media stream for which security is desired. Each crypto attribute for a given media stream must contain a unique tag. The ordering of multiple crypto attributes is significant — the most preferred crypto suite is listed first.

Upon receiving the initial offer, the answerer must either accept one of the offered crypto attributes, or reject the offer in its entirety.

When an offered crypto attribute is accepted, the crypto attribute contained in the answer MUST contain the tag and crypto-suite from the accepted crypto attribute in the offer, and the key(s) the answerer will use to encrypt media sent to the offerer.

The crypto-suite is bidirectional and specifies encryption and authentication algorithms for both ends of the connection. The keys are unidirectional in that one key or key set encrypts and decrypts traffic originated by the offerer, while the other key or key set encrypts and decrypts traffic originated by the answerer.

Key exchange via text-based SDP is unacceptable in that malicious network elements could easily eavesdrop and obtain the plaintext keys, thus compromising the privacy and integrity of the encrypted media stream. Consequently, the SDP exchange must be protected by a security protocol such as TLS.

Operational Modes

SRTP topologies can be reduced to three basic topologies which are described in the following sections.

Single-Ended SRTP Termination

Single-ended SRTP termination is illustrated in the following figure.

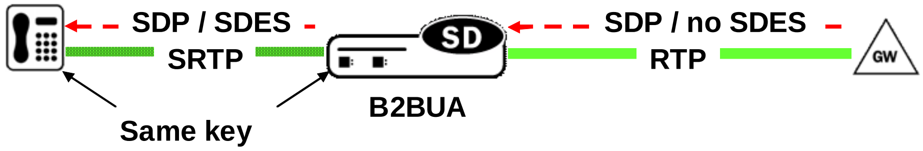


Figure 2 - 1: Single-Ended SRTP Termination

If SRTP is enabled for the inbound realm/interface, the E-SBC handles the incoming call as specified by the Media Security Policy assigned to the inbound realm. If there is crypto attribute contained in the offer, the E-SBC parses the crypto attributes and optional parameters, if any. If the offer contains a crypto attribute or attributes compatible with the requirements specified by the SDES profile assigned to the Media Security policy, it selects the most preferred compatible attribute. Otherwise, the E-SBC rejects the offer. Before the SDP is forwarded to the called party, the E-SBC allocates resources, established SRTP and SRTCP Security Associations and updates the SDP by removing the crypto attribute and inserting possibly NAT'ed media addresses and ports. At the same time, the original crypto attribute is also removed from the SDP.

Once the reply from the called party is received, the E-SBC inserts appropriate crypto attribute(s) to form a new SDP, and forward the response back to the calling party.

Back-to-Back SRTP Termination

Back-to-back SRTP termination is illustrated in the following figure.

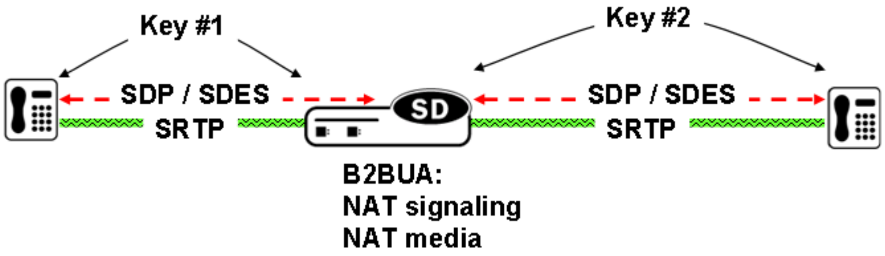


Figure 2 - 2: Back-to-Back SRTP Termination

Initial processing is similar to the single-ended termination described above. Before forwarding the request to the called party, the E-SBC replaces the original crypto attribute with a new one whose crypto attribute conforms to the media security policy for the outbound realm/interface. Upon receiving the answer from the called party, the E-SBC accepts or rejects it, again based upon conformity to the media security policy. If accepted, the E-SBC replaces the original crypto attribute from the called party with its own to form a new SDP, which it forwards back to the calling party. At this point, SRTP media sessions are established on both sides for both calling and called parties.

SRTP Pass-Thru

SRTP pass-thru is illustrated in the following figure.

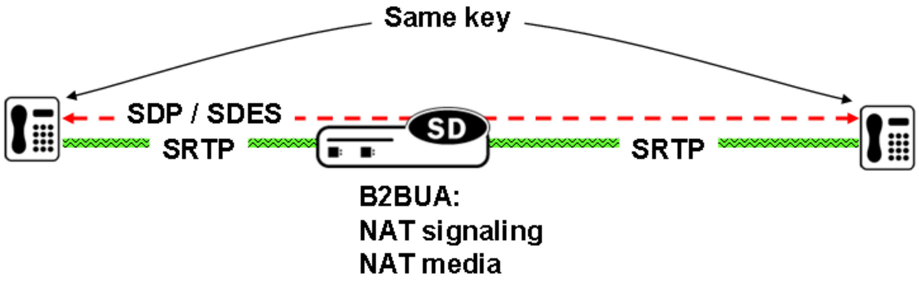


Figure 2 - 3: SRTP Pass-Thru

If the media security policy specifies *pass-through* mode, the E-SBC does not alter the crypto attribute exchange between the calling and the called party; the attribute is transparently passed.

For more information about SRTP in this release, see the *Net-Net® Enterprise Session Director Configuration Guide, Release E-C[xz]6.4.0.*

Relocation of License Information

The Notices and 3rd party licenses information previously documented in an Appendix of the *Net-Net® Enterprise Session Director User Guide,* now display in the "**About**" link in the Web GUI , and by entering the "**show about**" command using the ACLI.

For more information about Notices and 3rd party licenses, see the *Net-Net® Enterprise Session Director Configuration Guide, Release E-C[xz]6.4.0.*

Features Removed or Not Supported

This E-C[xz]6.4.0 Enterprise release contains the information required for an Enterprise to monitor, manage, and configure a Net-Net ESD in their network. There fore, this section lists the features that are not required, and have been removed from the software and the documentation.

Features Not Supported

The following features are not currently supported in Release E-C(xz)6.4.0 Final:

- Session Controller
- Border Gateway (BG)
- Media Gateway Control Protocol (MGCP)
- H.248 (Megaco or Gateway Control Protocol)
- Hide media update
- SNMPv3 (on LINUX)
- Lawful Intercept (LI)
- Packet Trace and Call Recording Server (CRS) may not be run at the same time

Features Not Supported in Software Editions (VME & SE)

In addition to the non-supported features indicated above, the following features are are not supported in the software editions (VME & SE):

- System Access Control Lists (ACLs)
- Physical Layer (PHY) link redundancy
- Session Initiation Protocol (SIP) port mapping
- Source-based routing
- Jumbo packets
- Full-Mode Session Replication for Recording (SRR)
- Online Certificate Status Protocol (OCSP)
- Internet Protocol Security (IPSEC)
- Transcoding
- Fax transcoding
- Internet Protocol version 6 (IPv6)
- Stream Control Transmission Protocol (SCTP)
- Bandwidth policing
- Mid-Reserve bandwidth for session agents

Issues Resolved

The following table lists the problems resolved between Release E-C[xz]6.4.0F2 and Release Version E-C[xz]6.4.0.

Description
Net-Net ESD no longer sends SIPREC INVITE to the next Session Recording Server (SRS) within the Session Recording Group (SRG), regardless of SRS status.
The Net-Net ESD no longer uses mactab interfaces instead of configuration interfaces for packet captures.
After upgrading from 639M1 to 639M2P3, HA nowworks as expected.
Call Processing no longer halts with Palladion Communications Monitoring Probe enabled on NN-3820.
Archive features are now available in E-C[xz]6.4.0.
There are no longer issues when using the Web GUI-based Secure File Transfer Protocol (SFTP) clients.
There are no longer 503 responses (Service Unavailable) observed on the Net-Net ESD.
The Net-Net ESD hardware no longer sends a CANCEL for forwarded INVITES.
The Net-Net ESD hardware no longer sends a CANCEL with a 0.0.0.0 address.
The DID / range-based matching now performs correctly if a Local Route Table (LRT) entry starts with a zero (0).
The "**show lrt route-table**" command now correctly lists all entries.
The Lightweight Directory Access Protocol (LDAP) resultant URI is now correct.
When user reconfigures the *ldap-config -> ldap-servers*, the Real-Time Communication (RTC) - Access Control List (ACL) is now correctly updated.
The correct number of ACLs are now instantiated for ldap-config when multiple ldap-servers are configured.
LDAP ACL's are no longer untrusted even though *realm-config -> access-control-trust-level* is set to “high.”
LDAP responseis no longer rejected by Net-Net ESD.
Dual-tone multifrequency (DTMF) no longer fails when Comfort Noise (CN) interworking facility (IWF) is enabled. RFC2833 Real-Time Protocol (RTP) packets no longer arrive "out-of-order" (seq. no.).
On EC[xz]640F2 and EC[xz]640 GA, you can now configure local-policy next-hop without a routing license.
The Net-Net ESD HTTP server now correctly enforces the Content-Range field.
On the Net-Net ESD, SIP "200 OK" responses now count towards realm thresholds.

Known Issues

The following table lists Release Version E-C[xz]6.4.0 known issues and workaround steps.

Description	Workaround
Net-Net ESD Hardware	
Upon rebooting a DL320 G8 platform, a kernal crash with no restart may occur.	Do not configure VLAN on the media ports or Replace the Network Interface Card (NIC) that uses a Broadcom chip (tg3), with an Intel chip (igb), such as the HP Ethernet 1 Gb 2-port 361T Adapter (Vendor Part # 652497-B21), which is the recommended adapter.
Net-Net ESD hangs if a reboot is performed when the "**show support-info**" command is displaying results.	None
Web GUI/ACLI	
If you are changing the configuration on the Net-Net ESD server or VM via the ACLI, and then open a Web GUI session to that same server or VM, the Web GUI allows you to change the configuration even though you are configuring the server or VM via the ACLI. The Web GUI should display an error message that prevents you from changing the conf iguration. This does not currently happen.	Only open one session at a time to the server or VM to configure it - either use the ACLI or use the Web GUI .
Attributes with textfields are not accepting special character like " " , ' '	Do not use special characters when adding text in the dialog boxes.
Installation wizard: If there is a hung Telnet/SSH session, you cannot perform reboot from the Virtual Machine (VM) VSphere console tab, norcan you open a new telnet session.	Reboot your VM or Net-Net ESD hardware.
When in Basic Mode, and you restore an Expert Mode configuration using the System tab, an error occurs when then switching to the Configuration tab.	None
SIP Monitoring and Trace (SMT) SIP traffic displayed in Session Details is missing the "Via header."	None
LDAP	
LDAP ACL is not dynamically updated for multiple LDAP servers.	None
When configuring the "**ldap-cfg-attributes**" element at the path, *session-router->ldap-config->ldap-transactions->ldap-cfg-attributes*, you MUST specify a value for the "realm" attribute in order for calls to be received correctly.	When configuring the "ldap-cfg-attributes" element, specify a realm to which this configuration applies. For example: ldap-cfg-attributes name msRTCSIP-Line next-hop sag:SA1 **realm net1651** extraction-regex ^\+?1?(\d{2})(\d{3})(\d{4})$ value-format tel:+1$1$2$3

Description	Workaround
SIP KPML Interworking	
Once Key Press Markup Language (KPML)-2833 interworking is negotiated, the Net-Net ESD is not sending out a SUBSCRIBE message.	None

Limitations

The following table lists limitations in Release Version E-C[xz]6.4.0.

Limitation
Web Server
• High-frequency logging into and out of the GUI using an automation script (a rate faster than humanly possible) results in a system crash. It is not expected that manual testing will produce this issue.
• For configurations that contain 2000 or more realms, after logging into the Web GUI and clicking on realm-config in Expert Mode, the configuration may take up to 20 seconds to load.
Hyper-V
• The following are specific limitations when using Hyper-V: - Limited session capacity when using Hper-V hypervisor (50 media sessions). - Network booting is not supported due to Microsoft Firewall Test (MSFT) driver defect. - Dynamic Host Configuration Protocol (DHCP) is not supported due to the MSFT driver defect. - Microsoft does not support USB pass-through via hypervisor. - Virtual LAN (VLAN) tagging is not supported with Hyper-V in Windows 2008 R2. - When using High Availability (HA), the wancom interfaces should be configured as "Legacy Network Adaptors". - Microsoft System Center Virtual Machine Manager (MS-SCVMM) should not be used to deploy Oracle Virtual Machine Edition (VME) products due to a Virtual Hard Disk (VHD) import defect.