ORACLE
COMMUNICATIONS

ORACLE

Oracle Enterprise Session Border Controller and Interactive Intelligence CIC server

Technical Application Note

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, and end users of the Oracle Enterprise Session Border Controller (E-SBC). It assumes that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller.

Document Overview

Interactive Intelligence offers the ability to connect to Internet telephony service providers (ITSP) using an IP-based SIP trunk. This reduces the cost and complexity of extending an enterprise's telephony system outside its network borders. Oracle Enterprise Session Border Controllers (E-SBCs) play an important role in SIP trunking as they are used by many ITSPs and some enterprises as part of their SIP trunking infrastructure.

This application note has been prepared as a means of ensuring that SIP trunking between ININ, Oracle E-SBCs and IP Trunking services are configured in the optimal manner.

Introduction

Audience

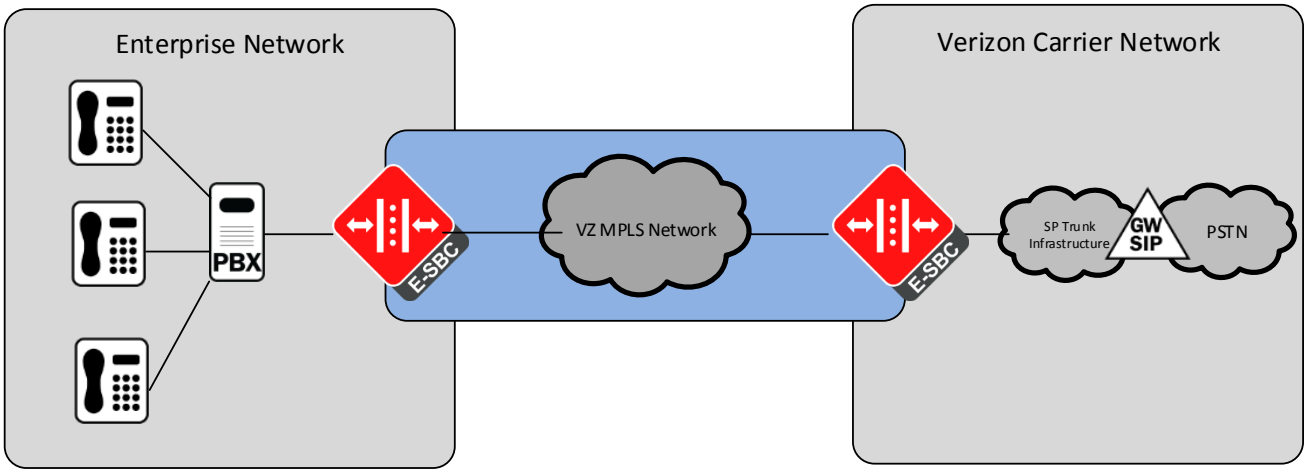
This is a technical document intended for telecommunications engineers with the purpose of configuring the Oracle Enterprise Session Border Controller and ININ CIC. There will be steps that require navigating the Command Line Interface (ACLI). Understanding the basic concepts of TCP/UDP, IP/Routing, SIP/RTP, TLS and SRTP are also necessary to complete the configuration and for troubleshooting, if necessary.

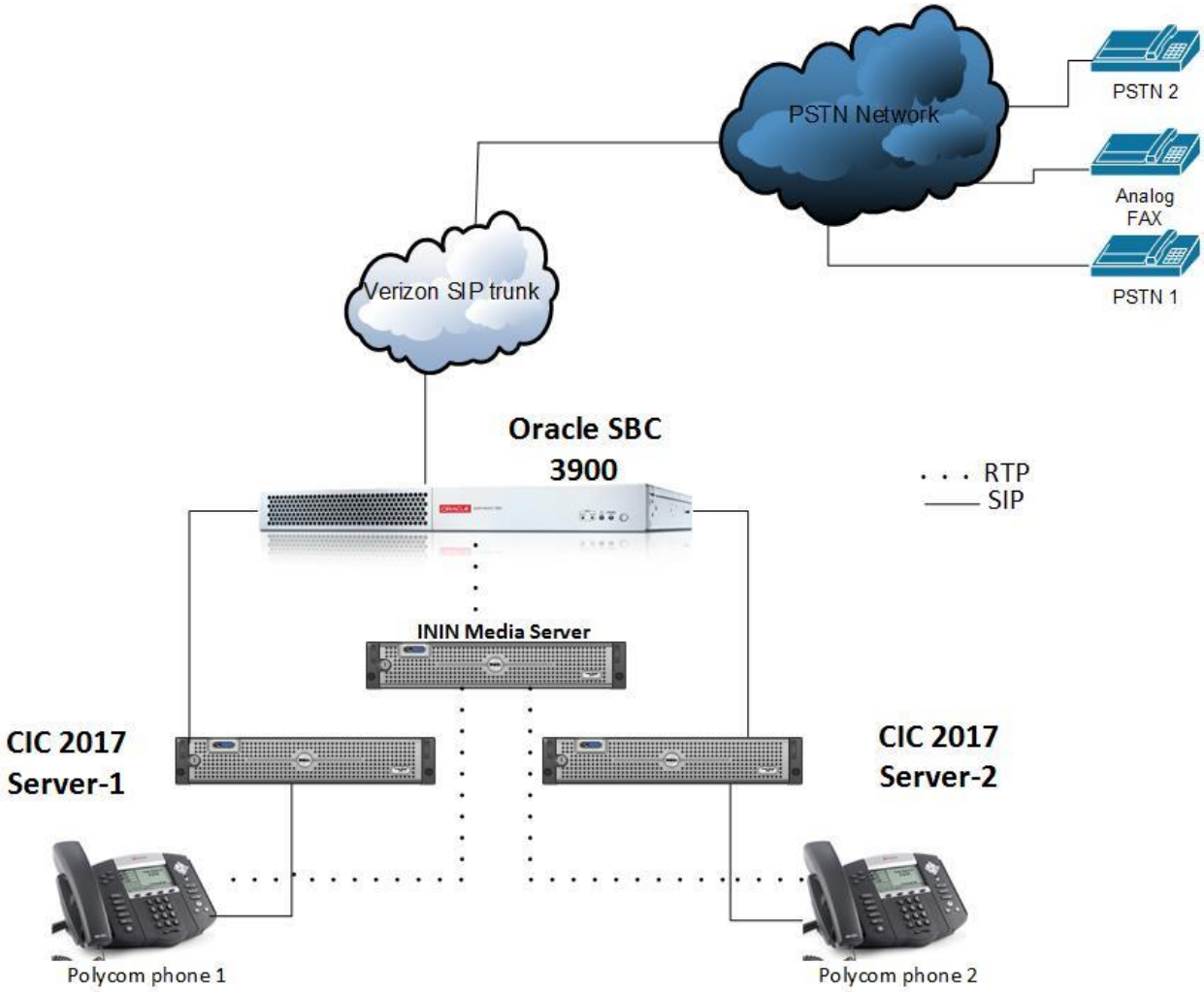
Requirements

- Interactive Intelligence CIC 2017 R2P4 server
- Oracle Enterprise Session Border Controller is running Acme Packet 3900 ECZ7.4 Patch 2
    - Note: the configuration running on the E-SBC is backward/forward compatible with any release in the 7.3.0 & above stream.

Architecture

The following reference architecture shows a logical view of the connectivity




PSTN Network
PSTN 2
Analog FAX
PSTN 1
Verizon SIP trunk
Oracle SBC 3900
RTP
SIP
ININ Media Server
CIC 2017 Server-1
CIC 2017 Server-2
Polycom phone 1
Polycom phone 2

Lab Configuration

Following are the IP addresses used for the Interoperability tests. The IPs below are specific to lab setup at Verizon, the IPs in production will be vastly different from network addresses listed below.

description	network-interface	realm	interface IP	sip-port
SBC interfaces				
management	wancom0		192.168.1.22	
redundancy	wancom1		169.254.1.1	
redundancy	wancom2		169.254.2.1	
media/signaling	s0p0:0	inside	192.65.79.180	5067
media/signaling	s1p0:0	outside	172.16.154.35	5067
Session-Agents				
ININ Server 1		inside	10.64.4.4	5060
ININ Server 2		inside	10.64.4.4	5060
Verizon trunk		outside	10.27.56.7	5060

Configuring the Oracle Enterprise Session Border Controller

In this section we describe the steps for configuring an Oracle Enterprise Session Border Controller, formally known as an Acme Packet Net-Net Enterprise Session Director, for use with CIC Server in a SIP trunking scenario.

In Scope

The following guide configuring the Oracle E-SBC assumes that this is a newly deployed device dedicated to a single customer. If a service provider currently has the E-SBC deployed then please see the ACLI Configuration Guide on http://docs.oracle.com/cd/E56581_01/index.htm for a better understanding of the Command Line Interface (CLI).

Note that Oracle offers several models of E-SBC. This document covers the setup for the E-SBC platform running ECZ7.2.0 or later. If instructions are needed for other Oracle E-SBC models, please contact your Oracle representative.

Out of Scope

- Configuration of Network management including SNMP and RADIUS

What will you need

- Hypervisor with console connectivity through the hypervisor
- Terminal emulation application such as PuTTY or HyperTerm
- Passwords for the User and Super user modes on the Oracle E-SBC
- IP address to be assigned to management interface (Wancom0) of the E-SBC - the Wancom0 management interface must be connected and configured to a management network separate from the service interfaces. Otherwise the E-SBC is subject to ARP overlap issues, loss of system access when the network is down, and compromising DDoS protection. Oracle does not support E-SBC configurations with management and media/service interfaces on the same subnet.
- IP address of CIC external facing NIC
- IP addresses to be used for the E-SBC internal and external facing ports (Service Interfaces)
- IP address of the next hop gateway in the service provider network

Configuring the E-SBC

Enter the following commands to login to the E-SBC and move to the configuration mode. Note that the default E-SBC password is "acme" and the default super user password is "packet".

```
Password: acme
SBC1> enable
Password: packet
SBC1# configure terminal
SBC1 (configure)#
```

You are now in the global configuration mode.

Initial Configuration – Assigning the management Interface an IP address

To assign an IP address, one has to configure the bootparams on the E-SBC by going to

SBC1#**configure terminal --- >bootparams**

- Once you type "bootparam" you have to use "carriage return" key to navigate down
- A reboot is required if changes are made to the existing bootparams

```
SBC1#(configure)bootparam
'.' = clear field;  '-' = go to previous field;          q = quit boot device                : eth0
processor number       : 0
host name        : acmesystem
file name        : /code/images/nnECZ720p2.64.bz --- >location where the software is loaded on the SBC
inet on ethernet (e)     : 192.168.1.22:ffffff80 --- > This is the ip address of the management interface of
                           the SBC, type the IP address and mask in hex
inet on backplane (b)   :
host inet (h)     :
gateway inet (g)         : 192.168.1.1 ->
gateway address here user (u) : vxftp
ftp password (pw) (blank = use rsh)    : vxftp
flags (f)          :
target name (tn)         : SBC1 -> ACLI prompt name & HA peer name
startup script (s)         :
other (o)          :
```

Core ESBC Config

The following section walks you through configuring the Oracle E-SBC. It is outside the scope of this document to include all of the configuration elements as it will differ in every deployment.

Physical Interface:

```
phy-interface
      name                    s0p0
      operation-type              Media
      duplex-mode
      speed
phy-interface
      name                    s0p1
      operation-type              Media
      port                    1
phy-interface
      name                    wancom1
      operation-type              Control
      port                    1
phy-interface
      name                    wancom2
      operation-type              Control
      port                    2
```

High Availability

For additional information on High Availability please see the enterprise SBC documentation for more information (http://www.oracle.com/technetwork/indexes/documentation/oracle-comms-acme-packet-2046907.html)

Interfaces wancom1 and 2 need to be added to facilitate HA communication between the two HA pairs.

```
network-interface
      name                    wancom1
      description               HA_HEARTBEAT1
      pri-utility-addr            169.254.1.1
      sec-utility-addr            169.254.1.2
      netmask                   255.255.255.252
```

```
network-interface
      name                    wancom2
      description             HA_HEARTBEAT2
      pri-utility-addr        169.254.2.1
      sec-utility-addr        169.254.2.2
      netmask                 255.255.255.252
```

```
redundancy-config
      becoming-standby-time         360000
      peer
            name                    SBC1
            type                    Primary
            destination
                  address                 169.254.1.1:9090
                  network-interface           wancom1:0
            destination
                  address                 169.254.2.1:9090
                  network-interface           wancom2:0
      peer
            name                    SBC2
            type                    Secondary
            destination
                  address                 169.254.1.2:9090
                  network-interface           wancom1:0
            destination
                  address                 169.254.2.2:9090
                  network-interface           wancom2:0
```

Additionally primary and secondary interface IPs need to be added to the media/signaling network-interfaces

```
network-interface
      name                    s0p0
      description             WAN
      ip-address              192.65.79.180
      netmask                 255.255.255.128
      gateway                 192.65.79.129
      icmp-address            192.65.79.180
network-interface
      name                    s0p1
      description             LAN
      ip-address              10.64.4.127
```

```
    netmask                 255.255.255.0
    gateway                 10.64.1.1
    hip-ip-list             10.70.65.20
                            10.64.4.127
                            10.64.4.238
    icmp-address            10.70.65.20
                            10.64.4.127
                            10.64.4.238
    telnet-address          10.70.65.20
```

Enable SIP on the SBC and configure default configuration required on the SBC as follows

```
sip-config
    home-realm-id               inside
    registrar-domain             *
    registrar-host              *
    registrar-port              5060
    options                     max-udp-length=0
    extra-method-stats           enabled
```

Routing via Local Policy

For outbound calls the local-policy determines which trunk to forward the call based on the NPA of the request-URI. This is configured in the local policy of the "To". For most configurations there will be only 1 inside and outside realm. For a single inside/outside realm configuration the local policy to and from would be set to "*". Redundant trunk configurations will use a session-agent group.

```
local-policy
    from-address                *
    to-address                  10.64.4.127
    source-realm                *
    policy-attribute
        next-hop                  152.188.29.149
        realm                   outside
local-policy
    from-address                *
    to-address                  *
    source-realm                inside
    policy-attribute
        next-hop                  152.188.29.149
        realm                   outside
local-policy
    from-address                *
```

```
    to-address              *
    source-realm              outside
    policy-attribute
        next-hop                SAG:ININ
        realm                   inside
```

```
session-group
    group-name              ININ
    dest                10.64.4.4
                        10.64.4.5
```

```
session-agent
    hostname                152.188.29.149
    ip-address              152.188.29.149
    port                5072
    realm-id              outside
    ping-method             OPTIONS;hops=0
    ping-interval           30
```

Header manipulation rules required for the Verizon Trunk

The following HMR updates the host portion of the URI to the Verizon trunk IP for Request-URI and To headers. The host portion of the URI is updated with the E-SBC outside sip-interface IP for From, P-Asserted-Identity and Contact so that the E-SBC presents its interface IP to the next hop.

```
sip-manipulation
    name                NAT_IP
    header-rule
        name                From
        header-name             From
        action              manipulate
        msg-type              request
        methods               INVITE
        element-rule
            name                From_er
            type              uri-host
            action             find-replace-all
            new-value             $LOCAL_IP
    header-rule
        name                To
        header-name             To
        action              manipulate
        msg-type              request
        methods               INVITE
        element-rule
```

```
            name                    To_er
            type                   uri-host
            action                  find-replace-all
            new-value                  $REMOTE_IP
    header-rule
        name                    Div
        header-name                 Diversion
        action                  manipulate
        msg-type                  request
        methods                   INVITE
        element-rule
            name                    Div_er
            type                   uri-host
            action                  find-replace-all
            new-value                  $LOCAL_IP
    header-rule
        name                    storeReferredBy
        header-name                 Referred-By
        action                  store
        msg-type                  request
        methods                   INVITE
        match-value                 (.*)(@.*)
    header-rule
        name                    delReferredBy
        header-name                 Referred-By
        action                  delete
        msg-type                  request
        methods                   INVITE
    header-rule
        name                    addPai
        header-name                 P-Asserted-Identity
        action                  add
        comparison-type               boolean
        msg-type                  request
        methods                   INVITE
        match-value                $storeReferredBy
        new-value                  $storeReferredBy.$1+"@"+$LOCAL_IP
    header-rule
        name                    alterReplaces
        header-name                 Refer-To
        msg-type                  request
        methods                   REFER
```

```
        element-rule
            name                    alterReplaces_er
            parameter-name              Replaces
            type                    header-value
            action                  delete-element
    header-rule
        name                    CallAlterRefer
        header-name                 Refer-To
        action                  sip-manip
        new-value                   AlterRefer
sip-manipulation
    name                    AlterRefer
    header-rule
        name                    storeReferTo
        header-name                 Refer-To
        action                  store
        msg-type                  request
        methods                   REFER
        match-value                 (.*)(@.*)
    header-rule
        name                    DelReferTo
        header-name                 Refer-To
        action                  delete
        msg-type                  request
        methods                   REFER
    header-rule
        name                    AddReferTo
        header-name                 Refer-To
        action                  add
        msg-type                  request
        methods                   REFER
        new-value                   $storeReferTo.$1+"@"+$REMOTE_IP+">"
    header-rule
        name                    delxinin
        header-name                 x-inin-crn
        action                  delete
        msg-type                  request
        methods                   REFER
    header-rule
        name                    alterReferredBy
        header-name                 Referred-By
        action                  manipulate
```

```
        msg-type                request
        methods                 REFER
        element-rule
            name                  alterReferredBy_er
            type                 uri-host
            action                find-replace-all
            new-value               $LOCAL_IP
```

SRTP Configuration

SRTP provides encrypted audio streams to/from ININ to the Oracle Enterprise Session Boarder Controller. Verizon Trunking does not support SRTP. For more information regarding SRTP configuration procedures please review the Enterprise Session Border Controller Configuration Guide.

```
sdes-profile
    name                    SRTP
    crypto-list               AES_CM_128_HMAC_SHA1_80
                          AES_CM_128_HMAC_SHA1_32
```

```
media-sec-policy
    name                    noSRTP
```

```
media-sec-policy
    name                    SRTP
    inbound
        profile                SRTP
        mode                    srtp
        protocol                 sdes
    outbound
        profile                SRTP
        mode                    srtp
        protocol                 sdes
```

```
realm-config
    identifier              inside
    network-interfaces          s0p1:0
    mm-in-realm               enabled
    restricted-latching         sdp
    restriction-mask            24
    options                 refer-reinvite
    delay-media-update            enabled
```

```
realm-config
      identifier                  outside
      network-interfaces              s0p0:0
      mm-in-realm                   enabled
      restricted-latching             sdp
      restriction-mask                24
      options                     refer-reinvite
      delay-media-update                enabled`
```

TLS Configuration

TLS provides encrypted SIP signaling between the Oracle Communications E-SBC and ININ 2015. TLS requires the exchange of certificates. The ININ administrator will need to provide the local domain controller root certificate. Likewise the CSR created on the E-SBC will need to be signed by the domain controller certificate authority that the ININ servers are associated with. The signed certificate will then need to be imported back into the SBC. For more information regarding TLS configuration procedures please review the Enterprise Session Border Controller Configuration Guide.

```
certificate-record
      name                      ININ
      state                     TX
      locality                  Plano
      common-name                   ininoracle
```

```
certificate-record
      name                      rootcert
      state                     TX
      locality                  Plano
      common-name                   CICSERVER1_Server Group
```

```
tls-profile
      name                      ININ
      end-entity-certificate          ININ
      trusted-ca-certificates         rootcert
      mutual-authenticate             enabled
      tls-version                tlsv12
```

```
sip-interface
      realm-id                  inside
      sip-port
            address                 10.64.4.127
            allow-anonymous               agents-only
      sip-port
```

```
        address                 10.64.4.127
        port                    5061
        transport-protocol              TCP
        allow-anonymous                 agents-only
    sip-port ---------------------------- set to StaticTLS only when TLS is required
        address                 10.64.4.127
        port                    5061
        transport-protocol              TLS
        allow-anonymous                 agents-only
    registration-caching            enabled
```

```
sip-interface
    realm-id                outside
    sip-port
        address                 192.65.79.180
        allow-anonymous                 agents-only
    sip-port
        address                 192.65.79.180
        port                    8060
        allow-anonymous                 registered
    nat-traversal               always
    registration-caching            enabled
    route-to-registrar          enabled
    out-manipulationid              NAT_IP
    sip-profile                 Replaces
```

```
session-agent
    hostname                10.64.4.4
    ip-address              10.64.4.4
    realm-id                inside
    transport-method        StaticTLS ---------------------------- set to StaticTLS only when TLS is required
    ping-method                 OPTIONS;hops=0
    ping-interval               30
session-agent
    hostname                10.64.4.5
    ip-address              10.64.4.5
    realm-id                inside
    transport-method        StaticTLS ---------------------------- set to StaticTLS only when TLS is required
    ping-method                 OPTIONS;hops=0
    ping-interval               30
```

Configure the following static-flows

The following static flows are required on the SBC to allow phones to download pre-registration files such as config, software, certificates etc.

```
static-flow
      in-realm-id                outside
      in-destination               192.65.79.180:8088
      out-realm-id                inside
      out-source                 10.64.4.127
      out-destination              10.64.4.4:8088
      protocol                  TCP
      alg-type                  NAPT
      start-port                40000
      end-port                  45000
static-flow
      in-realm-id                outside
      in-destination               192.65.79.180:8089
      out-realm-id                inside
      out-source                 10.64.4.127
      out-destination              10.64.4.4:8089
      protocol                  TCP
      alg-type                  NAPT
      start-port                45002
      end-port                  49500
```

Steering pool config:

The following config needs to be enabled on the SBC in order for the media traffic to traverse thru the SBC.

```
steering-pool
      ip-address                10.64.4.127
      start-port                49452
      end-port                  65535
      realm-id                  inside
steering-pool
      ip-address                192.65.79.180
      start-port                49542
      end-port                  65535
      realm-id                  outside
```

System configuration:

Enable System config

```
System-config
      process-log-level             NOTICE
      default-gateway               192.65.79.97
```

Webserver Configuration

A webserver is available on all Enterprise versions of Oracle E-SBCs. The Webserver can be used to provide tracing, configuration and dashboard info. For tracing info, 2 parts must be configured. 1) The webserver must be enabled. 2) Tracing filters must be applied.

```
web-server-config
      state                     enabled
      inactivity-timeout            5
      http-state                enabled
      http-port                 80
      https-state               disabled
      https-port                443
      tls-profile
```

```
sip-monitoring
      match-any-filter              disabled
      state                     enabled
      short-session-duration        0
      monitoring-filters            *
      trigger-window                30
```

Test Plan executed:

Following test plan was executed against the ININ CIC Servers. Please contact your oracle representative for additional information pertaining to test scope and details.

#	Title	Results	
1	Configure SIP Carrier to Route Calls to IC	Pass	
2	Configure SIP Carrier Line	Pass	
3	Configure & Provision Managed IP Phones	Pass	
4	Configure Dial Plan for Outgoing Calls	Pass	
5	Out-of-band DTMF	Pass	
6	G.711 Through Carrier	Pass	
7	Inbound call with ANI	Pass	
8	Inbound Call without ANI	Pass	
9	Outbound Call with ANI	Pass	Call works only if the ANI information is valid DID for ITSP
10	Early Media	Pass	
11	Transfer - Blind (Internal)	Pass	
12	Transfer – Consult (Internal)	Pass	
13	Transfer – Blind (External)	Pass	
14	Transfer – Consult (External)	Pass	
#	Title	Results	
15	Hold Support – Re-Invite to 0.0.0.0	Pass	
16	Forward Incoming Call - from Carrier to Carrier	Pass	
17	3 Party Conference	Pass	
18	Fax - G.711 Pass-through	Pass	10 out of 10 inbound and outbound FAX calls are successful
19	Always In Audio	Pass	
20	Service Unavailable – 503	Pass	ITSP is sending

	response from carrier		announcement saying “The number is no longer is in service".
21	Power Failure	Pass	
22	Switchover Support	Pass	
23	WAN Failure	Pass	
24	Latency SIP Outbound	Pass	Latency is measured as 10ms. Call was loop backed as DUT
25	Outbound Call with RESTRICTED ANI	Pass	
26	Putback (Release Link) Transfer (Blind)	Pass	Completed REFER based test cases using different ITSP as we had issues with Verizon SIP trunk
27	Putback (Release Link) Transfer (Consult)	Pass	Completed REFER based test cases using different ITSP as we had issues with Verizon SIP trunk
28	Fax - T.38 (Inbound)	Pass	10 out of 10 FAX calls are successful
29	Fax - T.38 (Outbound)	Pass	10 out of 10 FAX calls are successful
30	Dynamic Audio	Pass	
#	**Title**	**Results**	
32	QoS tagging of RTP is preserved	Pass	
33	QoS tagging of SIP Signaling is preserved	Pass	
34	Multiple Ports	Pass	
35	SIP to SIP call support	Pass	
36	Support for TCP SIP Messaging	Pass	
37	Support for sRTP	Pass	
38	Support for TLS	Pass	
#	**Title**	**Results**	**Notes**
40	Provision WAN Managed Phone	Pass	
41	WAN Phone Intercom Calls	Pass	
42	WAN Phone External Calls	Pass	

43	WAN Phone Transfer (Blind)	Pass	
44	WAN Phone Transfer (Consult)	Pass	
45	WAN Phone Conference	Pass	
46	WAN Phone Switchover	Pass	Normal switchover scenarios were executed successfully. While trying to execute WAN phone based switchover scenarios, we had an issue with CIC servers not processing any calls (intercoms calls are also failing). Support ticket opened with ININ Incident NO: **927664**

Troubleshooting Tools

Wireshark

Wireshark is also a network protocol analyzer which is freely downloadable from www.wireshark.org.

On the Oracle E-SBC

The Oracle E-SBC provides a rich set of statistical counters available from the ACLI, as well as log file output with configurable detail. The follow sections detail enabling, adjusting and accessing those interfaces. Resetting the statistical counters, enabling logging and restarting the log files.

At the E-SBC Console:

```
SBC1# reset sipd
SBC1# notify sipd debug
SBC1#
enabled SIP Debugging
SBC1# notify all rotate-logs
```

Examining the log files

Note: You will FTP to the management interface of the E-SBC with the username user and user mode password (the default is
“acme”

```
C:\Documents and Settings\user>ftp 192.168.1.22
Connected to 192.168.85.55.
220 SBC1 server (VxWorks 6.4) ready. User (192.168.1.22:(none)): user
331 Password required for user. Password: acme
230 User user logged in.
ftp> cd /opt/logs
250 CWD command successful. ftp> get sipmsg.log
200 PORT command successful.
150 Opening ASCII mode data connection for '/opt/logs/sipmsg.log' (3353 bytes).
226 Transfer complete.
ftp: 3447 bytes received in 0.00Seconds 3447000.00Kbytes/sec. ftp> get log.sipd
200 PORT command successful.
150 Opening ASCII mode data connection for '/opt/logs/log.sipd' (204681 bytes).
226 Transfer complete.
ftp: 206823 bytes received in 0.11Seconds 1897.46Kbytes/sec
```

You may now examine the log files with the text editor of your choice.

Through the Web GUI

You can also check the display results of filtered SIP session data from the Oracle Enterprise Session Border Controller, and provides traces in a common log format for local viewing or for exporting to your PC. Please check the “Monitor and Trace” section (page 145) of the Web GUI User Guide available at http://docs.oracle.com/cd/E56581_01/index.htm

Appendix A

Full E-SBC Configuration

```
certificate-record
      name                    ININ
      state                   TX
      locality                Plano
      common-name                 ininoracle
certificate-record
      name                    rootcert
      state                   TX
      locality                Plano
      common-name                 CICSERVER1_Server Group
local-policy
      from-address                *
      to-address                  10.64.4.127
      source-realm                *
      policy-attribute
            next-hop                  152.188.29.149
            realm                     outside
local-policy
      from-address                *
      to-address                  *
      source-realm                inside
      policy-attribute
            next-hop                  152.188.29.149
            realm                     outside
local-policy
      from-address                *
      to-address                  *
      source-realm                outside
      policy-attribute
            next-hop                  SAG:ININ
            realm                     inside
media-manager
      hnt-rtcp                enabled
      anonymous-sdp               enabled
media-sec-policy
      name                    SRTP
      inbound
            profile                   SRTP
            mode                      srtp
```

```
        protocol                sdes
    outbound
        profile                 SRTP
        mode                    srtp
        protocol                sdes
media-sec-policy
    name                    noSRTP
network-interface
    name                    s0p0
    description               WAN
    ip-address                192.65.79.180
    netmask                   255.255.255.128
    gateway                   192.65.79.129
    icmp-address                192.65.79.180
network-interface
    name                    s0p1
    description               LAN
    ip-address                10.64.4.127
    netmask                   255.255.255.0
    gateway                   10.64.1.1
    hip-ip-list               10.70.65.20
                            10.64.4.127
                            10.64.4.238
    icmp-address                10.70.65.20
                            10.64.4.127
                            10.64.4.238
    telnet-address              10.70.65.20
phy-interface
    name                    s0p0
    operation-type              Media
    duplex-mode
    speed
phy-interface
    name                    s0p1
    operation-type              Media
    port                    1
realm-config
    identifier                inside
    network-interfaces              s0p1:0
    mm-in-realm               enabled
    restricted-latching         sdp
    restriction-mask            24
    options                   refer-reinvite
```

```
        delay-media-update              enabled
realm-config
        identifier                      outside
        network-interfaces              s0p0:0
        mm-in-realm                     enabled
        restricted-latching             sdp
        restriction-mask                24
        options                         refer-reinvite
        delay-media-update              enabled
sdes-profile
        name                            SRTP
        crypto-list                     AES_CM_128_HMAC_SHA1_80
                                        AES_CM_128_HMAC_SHA1_32
session-agent
        hostname                        10.64.4.4
        ip-address                      10.64.4.4
        realm-id                        inside
        ping-method                     OPTIONS;hops=0
        ping-interval                   30
session-agent
        hostname                        10.64.4.5
        ip-address                      10.64.4.5
        realm-id                        inside
        ping-method                     OPTIONS;hops=0
        ping-interval                   30
session-agent
        hostname                        152.188.29.149
        ip-address                      152.188.29.149
        port                            5072
        realm-id                        outside
        ping-method                     OPTIONS;hops=0
        ping-interval                   30
session-group
        group-name                      ININ
        dest                            10.64.4.4
                                        10.64.4.5
sip-config
        home-realm-id                   inside
        registrar-domain                *
        registrar-host                  *
        registrar-port                  5060
        options                         max-udp-length=0
        extra-method-stats              enabled
```

```
sip-interface
    realm-id                    inside
    sip-port
        address                     10.64.4.127
        allow-anonymous                 agents-only
    sip-port
        address                     10.64.4.127
        port                    5061
        transport-protocol              TCP
        allow-anonymous                 agents-only
    registration-caching            enabled
sip-interface
    realm-id                    outside
    sip-port
        address                     192.65.79.180
        allow-anonymous                 agents-only
    sip-port
        address                     192.65.79.180
        port                    8060
        allow-anonymous                 registered
    nat-traversal               always
    registration-caching            enabled
    route-to-registrar              enabled
    out-manipulationid              NAT_IP
    sip-profile                 Replaces
sip-manipulation
    name                        AlterRefer
    header-rule
        name                    storeReferTo
        header-name                 Refer-To
        action                  store
        msg-type                request
        methods                 REFER
        match-value                 (.*)(@.*)
    header-rule
        name                    DelReferTo
        header-name                 Refer-To
        action                  delete
        msg-type                request
        methods                 REFER
    header-rule
        name                    AddReferTo
        header-name                 Refer-To
```

```
        action                  add
        msg-type                request
        methods                 REFER
        new-value               $storeReferTo.$1+"@"+$REMOTE_IP+">"
    header-rule
        name                    delxinin
        header-name             x-inin-crn
        action                  delete
        msg-type                request
        methods                 REFER
    header-rule
        name                    alterReferredBy
        header-name             Referred-By
        action                  manipulate
        msg-type                request
        methods                 REFER
        element-rule
            name                alterReferredBy_er
            type                uri-host
            action              find-replace-all
            new-value           $LOCAL_IP
sip-manipulation
    name                NAT_IP
    header-rule
        name                    From
        header-name             From
        action                  manipulate
        msg-type                request
        methods                 INVITE
        element-rule
            name                From_er
            type                uri-host
            action              find-replace-all
            new-value           $LOCAL_IP
    header-rule
        name                    To
        header-name             To
        action                  manipulate
        msg-type                request
        methods                 INVITE
        element-rule
            name                To_er
            type                uri-host
```

```
            action                  find-replace-all
            new-value                   $REMOTE_IP
    header-rule
        name                    Div
        header-name                 Diversion
        action                  manipulate
        msg-type                request
        methods                 INVITE
        element-rule
            name                    Div_er
            type                    uri-host
            action                  find-replace-all
            new-value                   $LOCAL_IP
    header-rule
        name                    storeReferredBy
        header-name                 Referred-By
        action                  store
        msg-type                request
        methods                 INVITE
        match-value                 (.*)(@.*)
    header-rule
        name                    delReferredBy
        header-name                 Referred-By
        action                  delete
        msg-type                request
        methods                 INVITE
    header-rule
        name                    addPai
        header-name                 P-Asserted-Identity
        action                  add
        comparison-type             boolean
        msg-type                request
        methods                 INVITE
        match-value                 $storeReferredBy
        new-value                   $storeReferredBy.$1+"@"+$LOCAL_IP
    header-rule
        name                    alterReplaces
        header-name                 Refer-To
        msg-type                request
        methods                 REFER
        element-rule
            name                    alterReplaces_er
            parameter-name              Replaces
```

```
                type                    header-value
                action                  delete-element
        header-rule
            name                    CallAlterRefer
            header-name                 Refer-To
            action                  sip-manip
            new-value                   AlterRefer
sip-monitoring
static-flow
        in-realm-id                 outside
        in-destination                192.65.79.180:8088
        out-realm-id                inside
        out-source                  10.64.4.127
        out-destination               10.64.4.4:8088
        protocol                    TCP
        alg-type                    NAPT
        start-port                  40000
        end-port                    45000
static-flow
        in-realm-id                 outside
        in-destination                192.65.79.180:8089
        out-realm-id                inside
        out-source                  10.64.4.127
        out-destination               10.64.4.4:8089
        protocol                    TCP
        alg-type                    NAPT
        start-port                  45002
        end-port                    49500
steering-pool
        ip-address                   10.64.4.127
        start-port                  49452
        end-port                    65535
        realm-id                    inside
steering-pool
        ip-address                   192.65.79.180
        start-port                  49542
        end-port                    65535
        realm-id                    outside
system-config
        process-log-level               DEBUG
        default-gateway                 192.65.79.97
tls-profile
        name                        ININ
```

```
    end-entity-certificate              ININ
    trusted-ca-certificates             rootcert
    mutual-authenticate                 enabled
    tls-version                     tlsv12
web-server-config
```

Appendix B

Accessing the ACLI

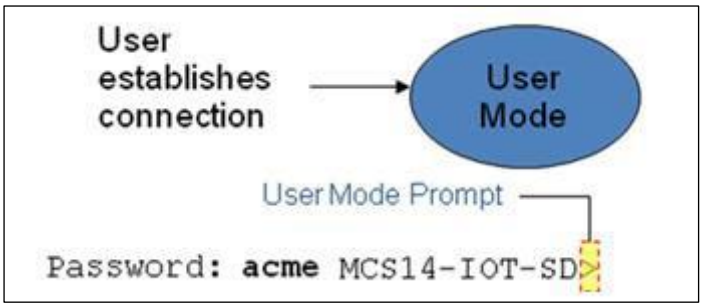
Access to the ACLI is provided by:

- The serial console connection;
- TELNET, which is enabled by default but may be disabled; and
- SSH, this must be explicitly configured.

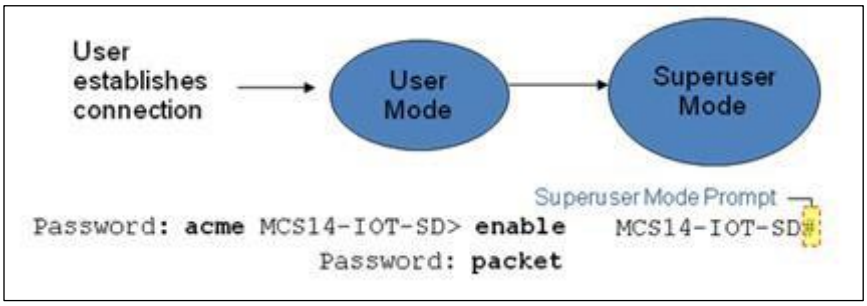
Initial connectivity will be through the serial console port. At a minimum, this is how to configure the management (eth0) i nterface on the E-SBC.

ACLI Basics

There are two password protected modes of operation within the ACLI, User mode and Superuser mode. When you establish a connection to the E-SBC, the prompt for the User mode password appears. The default password is acme. User mode consists of a restricted set of basic monitoring commands and is identified by the greater than sign (>) in the system prompt after the target name. You cannot perform configuration and maintenance from this mode.



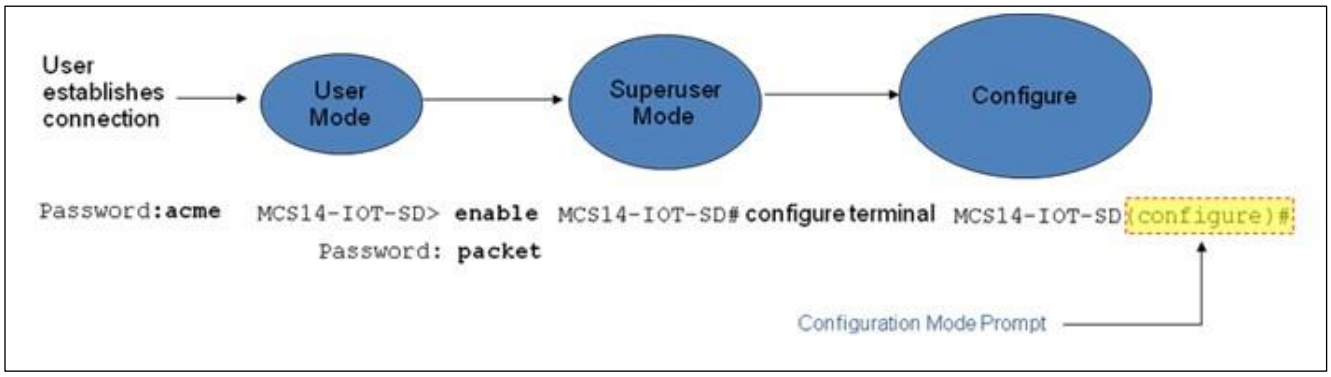
The Superuser mode allows for access to all system commands for operation, maintenance, and administration. This mode is identified by the pound sign (#) in the prompt after the target name. To enter the Superuser mode, issue the enable command i n the User mode.



From the Superuser mode, you can perform monitoring and administrative tasks; however you cannot configure any elements. To return to User mode, issue the exit command.

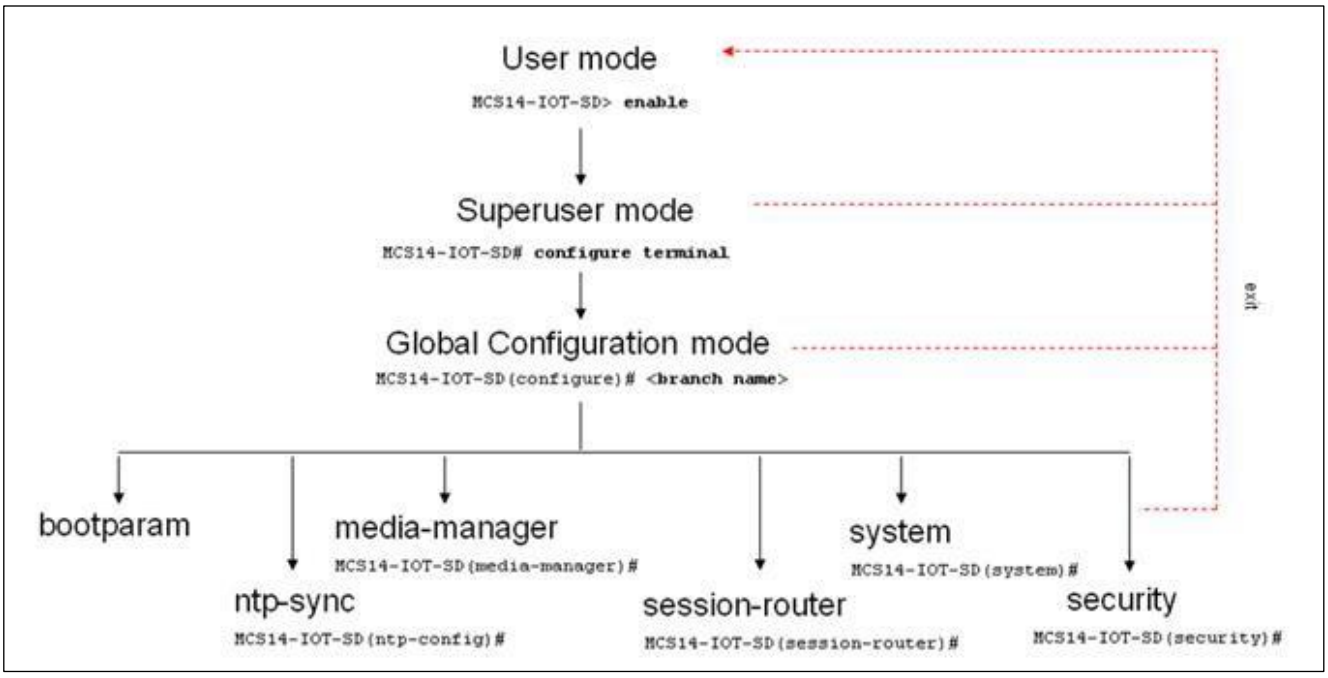
You must enter the Configuration mode to configure elements. For example, you can access the configurati on branches and configuration elements for signaling and media configurations. To enter the Configuration mode, issue the configure terminal command in the Superuser mode.

Configuration mode is identified by the word configure in parenthesis followed by the pound sign (#) in the prompt after the target name, for example, SBC1 (configure)#. To return to the Superuser mode, issue the exit command.



In the configuration mode, there are six configuration branches:

- bootparam;
- ntp-sync;
- media-manager;
- session-router;
- system; and
- security.



The ntp-sync and bootparams branches are flat branches (i.e., they do not have elements inside the branches). The rest of the branches have several elements under each of the branches.

The bootparam branch provides access to E-SBC boot parameters. Key boot parameters include:

- boot device – The global management port, usually eth0
- file name – The boot path and the image file.

- inet on ethernet – The IP address and subnet mask (in hex) of the management port of the SD.
- host inet –The IP address of external server where image file resides.
- user and ftp password – Used to boot from the external FTP server.
- gateway inet – The gateway IP address for reaching the external server, if the server is located in a different network.

```
'.' = clear field;  '-' = go to previous field;  q = quit
boot device             : eth0
processor number        : 0
host name               :
file name               : /tffs0/nnSCX620.gz
inet on ethernet (e)    : 10.0.3.11:ffff0000
inet on backplane (b)   :
host inet (h)           : 10.0.3.100
gateway inet (g)        : 10.0.0.1
user (u)                : anonymous
ftp password (pw) (blank = rsh)      : anonymous
flags (f)               : 0x8
target name (tn)        : MCS14-IOT-SD
startup script (s)      :
other (o)
```

The ntp-sync branch provides access to ntp server configuration commands for synchronizing the E-SBC time and date. The security branch provides access to security configuration.

The system branch provides access to basic configuration elements as system-config, snmp-community, redundancy, physical interfaces, network interfaces, etc.

The session-router branch provides access to signaling and routing related elements, including H323-config, sip-config, iwf-config, local-policy, sip-manipulation, session-agent, etc.

The media-manager branch provides access to media-related elements, including realms, steering pools, dns-config, media- manager, and so forth.

You will use media-manager, session-router, and system branches for most of your working configuration.

Configuration Elements

The configuration branches contain the configuration elements. Each configurable object is referred to as an element. Each element consists of a number of configurable parameters.

Some elements are single-instance elements, meaning that there is only one of that type of the element - for example, the global system configuration and redundancy configuration.

Some elements are multiple-instance elements. There may be one or more of the elements of any given type. For example, physical and network interfaces.

Some elements (both single and multiple instance) have sub-elements. For example:

- SIP-ports - are children of the sip-interface element
- peers – are children of the redundancy element
- destinations – are children of the peer element

Creating an Element

1. To create a single-instance element, you go to the appropriate level in the ACLI path and enter its parameters. There is no need to specify a unique identifier property because a single-instance element is a global element and there is only one instance of this element.
2. When creating a multiple-instance element, you must specify a unique identifier for each instance of the element.
3. It is important to check the parameters of the element you are configuring before committing the changes. You do this by issuing the show command before issuing the done command. The parameters that you did not configure are filled with either default values or left empty.
4. On completion, you must issue the done command. The done command causes the configuration to be echoed to the screen and commits the changes to the volatile memory. It is a good idea to review this output to ensure that your configurations are correct.
5. Issue the exit command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the E-SBC reboots, your configurations will be lost.

Editing an Element

The procedure of editing an element is similar to creating an element, except that you must select the element that you will edit before editing it.

- Enter the element that you will edit at the correct level of the ACLI path.

- Select the element that you will edit, and view it before editing it.
- The select command loads the element to the volatile memory for editing. The show command allows you to view the element to ensure that it is the right one that you want to edit.
- Once you are sure that the element you selected is the right one for editing, edit the parameter one by one. The new value you provide will overwrite the old value.
- It is important to check the properties of the element you are configuring before committing it to the volatile memory. You do this by issuing the show command before issuing the done command.
- On completion, you must issue the done command.
- Issue the exit command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the E-SBC reboots, your configurations will be lost.

Deleting an Element

The no command deletes an element from the configuration in editing. To delete a single-instance element,

- Enter the no command from within the path for that specific element
- Issue the exit command. To delete a multiple-instance element,
- Enter the no command from within the path for that particular element.
- The key field prompt, such as <name>:<sub-port-id>, appears.
- Use the <Enter> key to display a list of the existing configured elements.
- Enter the number corresponding to the element you wish to delete.
- Issue the select command to view the list of elements to confirm that the element was removed.

Note that the configuration changes at this point are not permanently saved yet. If the E-SBC reboots, your configurations will be lost.

Configuration Versions

At any time, three versions of the configuration can exist on the E-SBC: the edited configuration, the saved configuration, and the running configuration.

- The edited configuration – this is the version that you are making changes to. This version of the configuration is stored in the E-SBC's volatile memory and will be lost on a reboot.
- To view the editing configuration, issue the show configuration command
- The saved configuration – on issuing the save-config command, the edited configuration is copied into the non- volatile memory on the E-SBC and becomes the saved configuration. Because the saved configuration has not been activated yet, the changes in the configuration will not take effect. On

reboot, the last activated configuration (i.e., the last running configuration) will be loaded, not the saved configuration.

- The running configuration is the saved then activated configuration. On issuing the activate-config command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration. Although most of the configurations can take effect once being activated without reboot, some configurations require a reboot for the changes to take effect.
- To view the running configuration, issue command show running-config.

Saving the Configuration

The save-config command stores the edited configuration persistently.

Because the saved configuration has not been activated yet, changes in configuration will not take effect. On reboot, the las t activated configuration (i.e., the last running configuration) will be loaded. At this stage, the saved configuration is different from the running configuration.

Because the saved configuration is stored in non-volatile memory, it can be accessed and activated at later time.

Upon issuing the save-config command, the E-SBC displays a reminder on screen stating that you must use the activate- config command if you want the configurations to be updated.

```
SBC1 # save-config
Save-Config received, processing. waiting 1200
for request to finish Request to 'SAVE-CONFIG'
has Finished, Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
SBC1
```

Activating the Configuration

On issuing the activate-config command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration.

Some configuration changes are service affecting when activated. For these configurations, the E-SBC warns that the change could have an impact on service with the configuration elements that will potentially be service affecting. You may decide whether or not to continue with applying these changes immediately or to apply them at a later time.

```
SBC1# activate-config Activate-Config
received, processing. waiting 120000 for
request to finish Request to 'ACTIVATE-
CONFIG' has Finished, Activate Complete
SBC1#
```


Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services