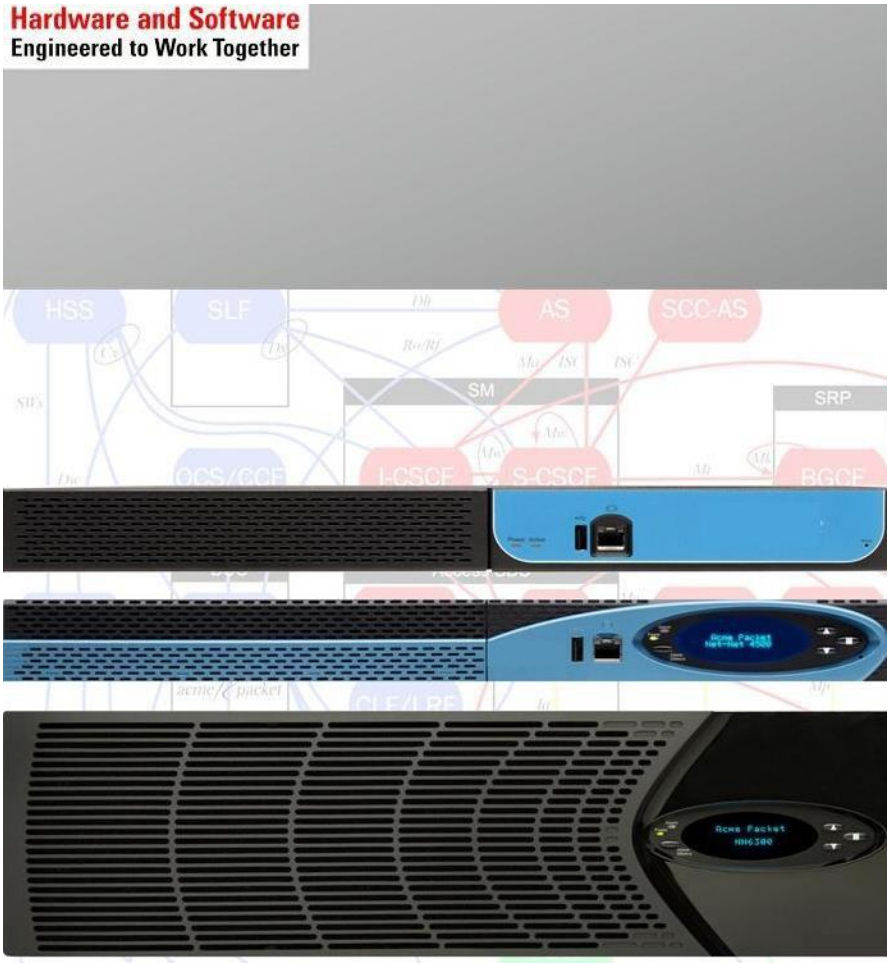


Oracle Enterprise Session Border Controller and Cisco Jabber and Phones with Cisco Call Manager (SIP/TCP and voice-only)

Technical Application Note

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

1. 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.

1.1. Document Overview

Cisco Jabber clients, phones and Cisco Call Manager (CUCM) offer the ability to utilize Unified Communications (UC) and Voice over IP (VoIP) over the enterprise network. This reduces the cost and complexity of offering voice services within the enterprise. Oracle Enterprise Session Border Controllers (E-SBCs) play an important role in SIP access environments to protect the core call controller (CUCM) from rogue endpoints and denial of service attacks.

This application note has been prepared as a means of ensuring that SIP access between Cisco Call Manager, Oracle E-SBCs, Cisco Jabber clients, and Cisco phones are configured in the optimal manner.

It should be noted that the E-SBC configuration provided in this guide focuses strictly on the Cisco Jabber, phone, and CUCM associated parameters. Many E-SBC users may have additional configuration requirements that are specific to other applications. These configuration items are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

The

For additional information on Cisco Jabber and CUCM, please visit http://www.cisco.com/web/products/voice/jabber.html and http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-callmanager/index.html.

2. Introduction

2.1. Audience

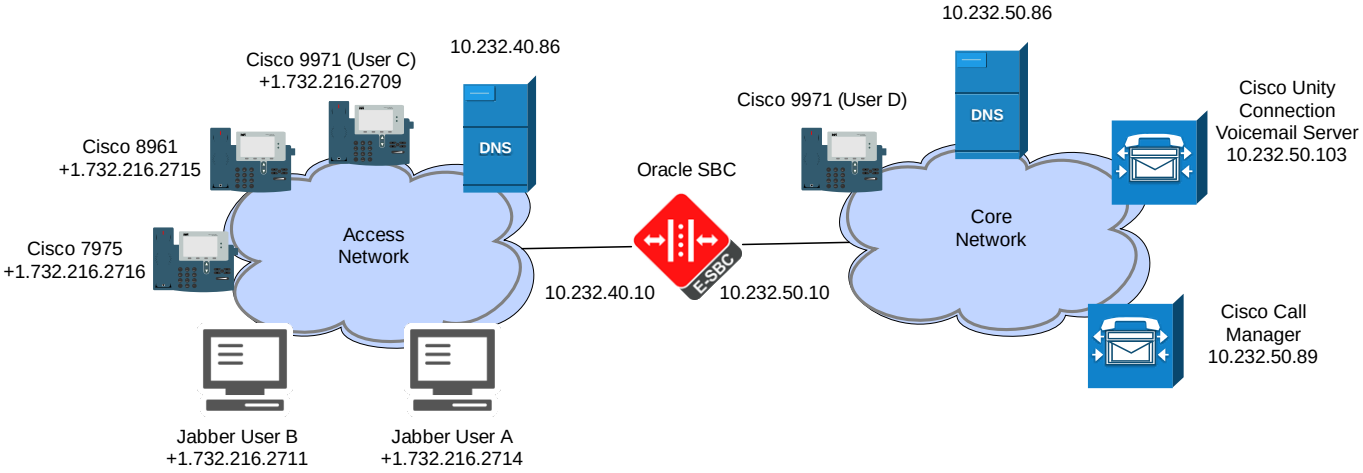
This is a technical document intended for telecommunications engineers with the purpose of configuring the Oracle Enterprise Session Border Controller, the Cisco Jabber client, Cisco phones, and Cisco Call Manager (CUCM). There will be steps that require navigating CUCM as well as the Oracle E-SBC Command Line Interface (CLI). Understanding the basic concepts of TCP/UDP, IP/Routing, and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

2.2. Requirements

- Fully functioning CUCM deployment, including DNS on the outside (access side) and inside (core side) of the SBC
- CUCM version 10.5.2.10000-5
- Cisco Jabber client version 10.6.0 and/or Cisco Phones (Cisco 7975, 8961, and 9971 were tested)
- Oracle Enterprise Session Border Controller running nnECZ730p2.

2.3. Lab Configuration

The following diagram illustrates the lab environment created to facilitate testing.



3. Configuring the Cisco Call Manager (CUCM)

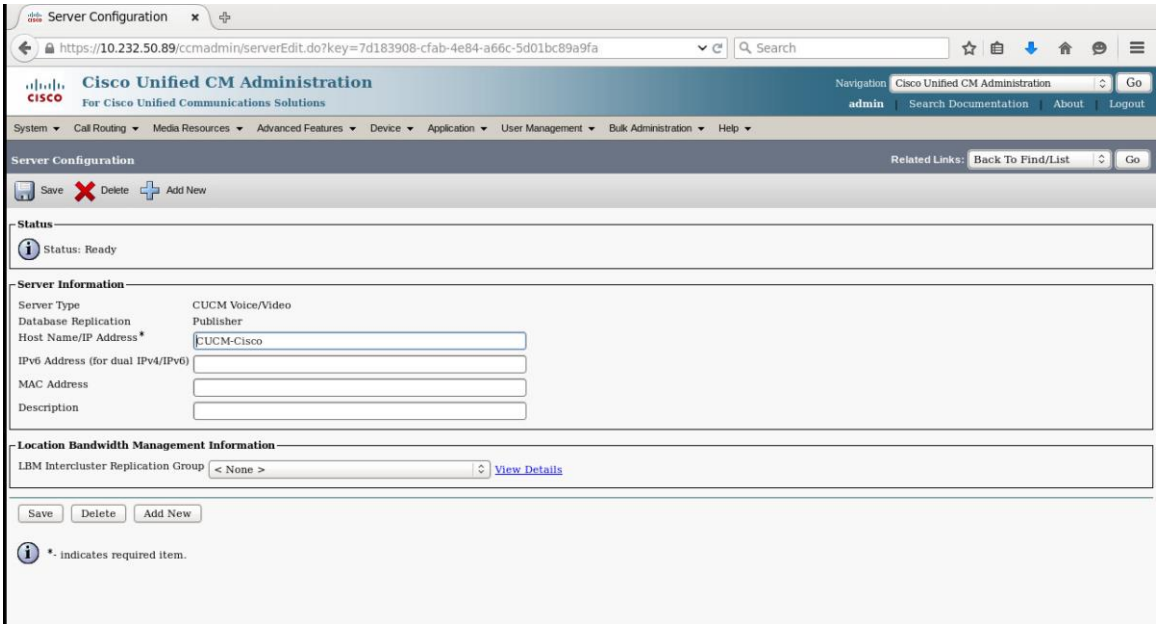
The only special configuration required on CUCM to interoperate with the Oracle SBC is ensuring a hostname is used in the configuration instead of an IP address.

The hostname sent to the Jabber clients and phones in their config files is set in the Cisco Unified CM Administration page under System > Server. This needs to be a hostname, not an IP address. The Jabber client will do a DNS SRV query on
"_cisco-uds._tcp.customer.com", where "customer.com" is the domain-suffix defined on the Jabber PC, which will return an A-record, such as
"CUCM-Cisco.customer.com". The Jabber client will then do a DNS query on
"CUCM-Cisco.customer.com", which should resolve to the SBC's access-side IP address, or 10.232.40.10 in this document. The client will then download its config file from CUCM via the SBC, and the config file will have "CUCM-Cisco" as the Call Manager name. Here is an excerpt from the Jabber and phone config files:

```
<member  priority="0">
<callManager>
<name>CUCM-Cisco</name>
<description>CUCM-Cisco</description>
```

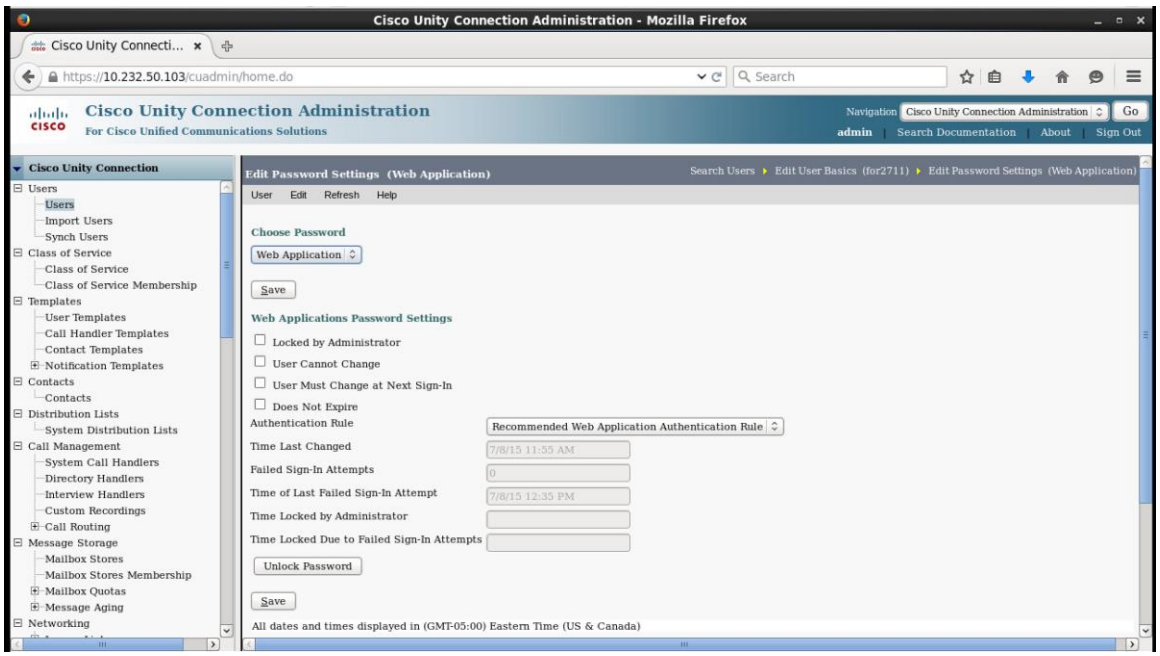
The phones use DHCP to determine where to download their config files from, with DHCP option 150 specifying the SBC's access side IP address. The phones will then do a DNS query on "CUCM-Cisco.customer.com" which will also resolve to the SBC's access-side IP.

WARNING: changing this hostname value may impact CUCM and should be done with caution and in strict accordance with Cisco documentation.



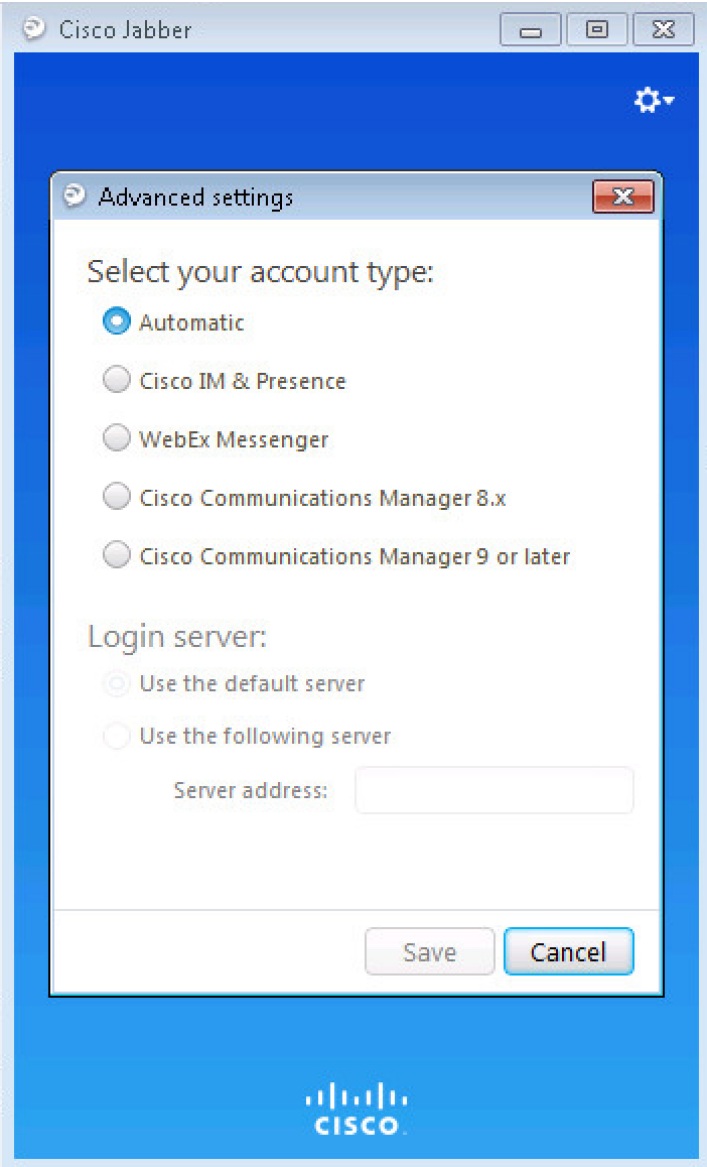
4. Configuring the Cisco Unity Connection (CUC) Server for Jabber

There is an issue with the default Cisco Unity Connection (CUC) voicemail server settings as they are not compatible with Jabber. To correct this, login to CUC, select Users, then click on the individual Jabber user, then select Edit > Password Settings, then select Web Application from the drop-down box, and uncheck “User Must Change at Next Sign-In”.

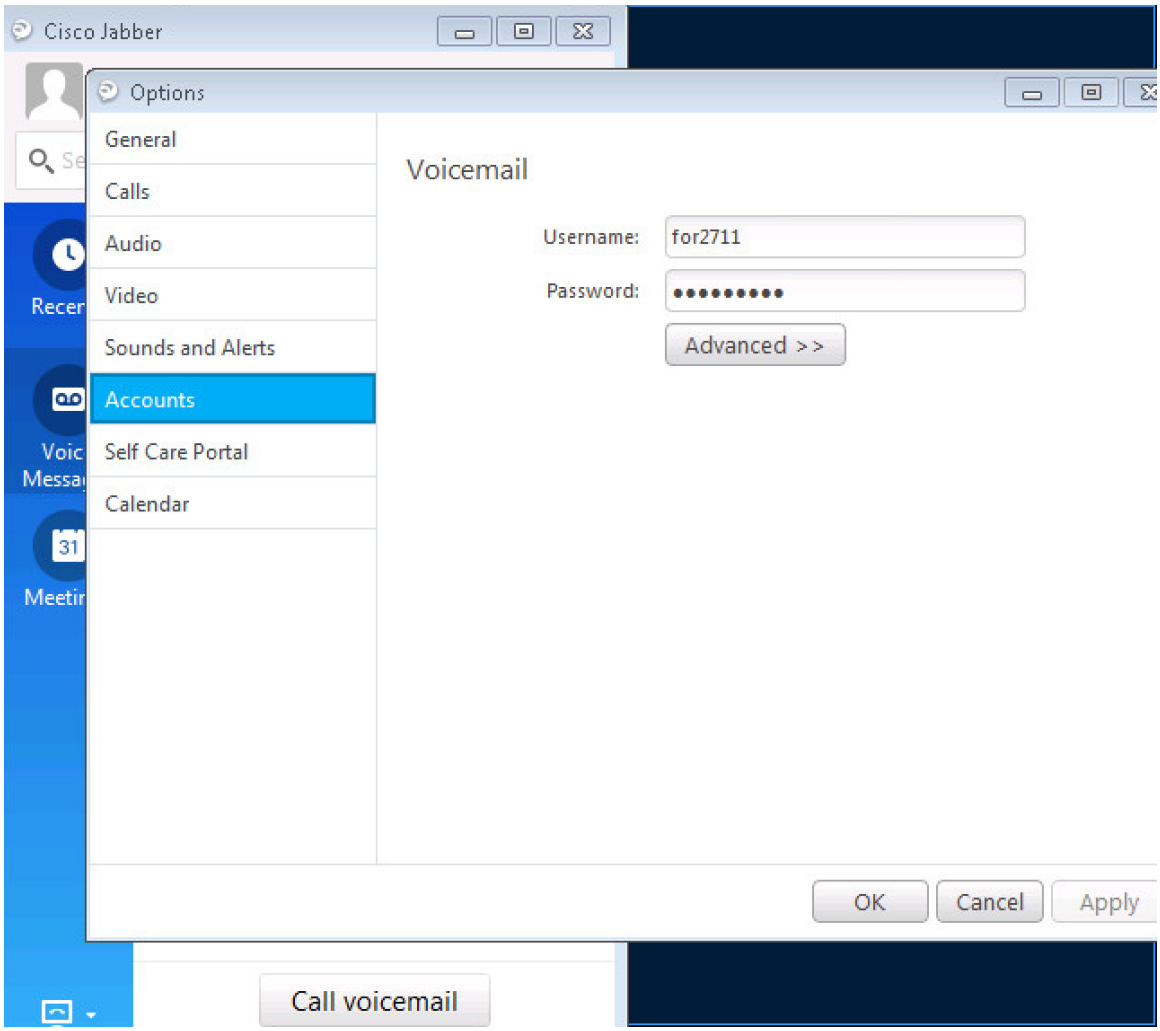


5. Configuring the Jabber Clients

There is no special configuration required on the Jabber clients. The Advanced Settings should be their defaults:



To configure the user's voicemail username and password, select File, then Options, then Accounts:



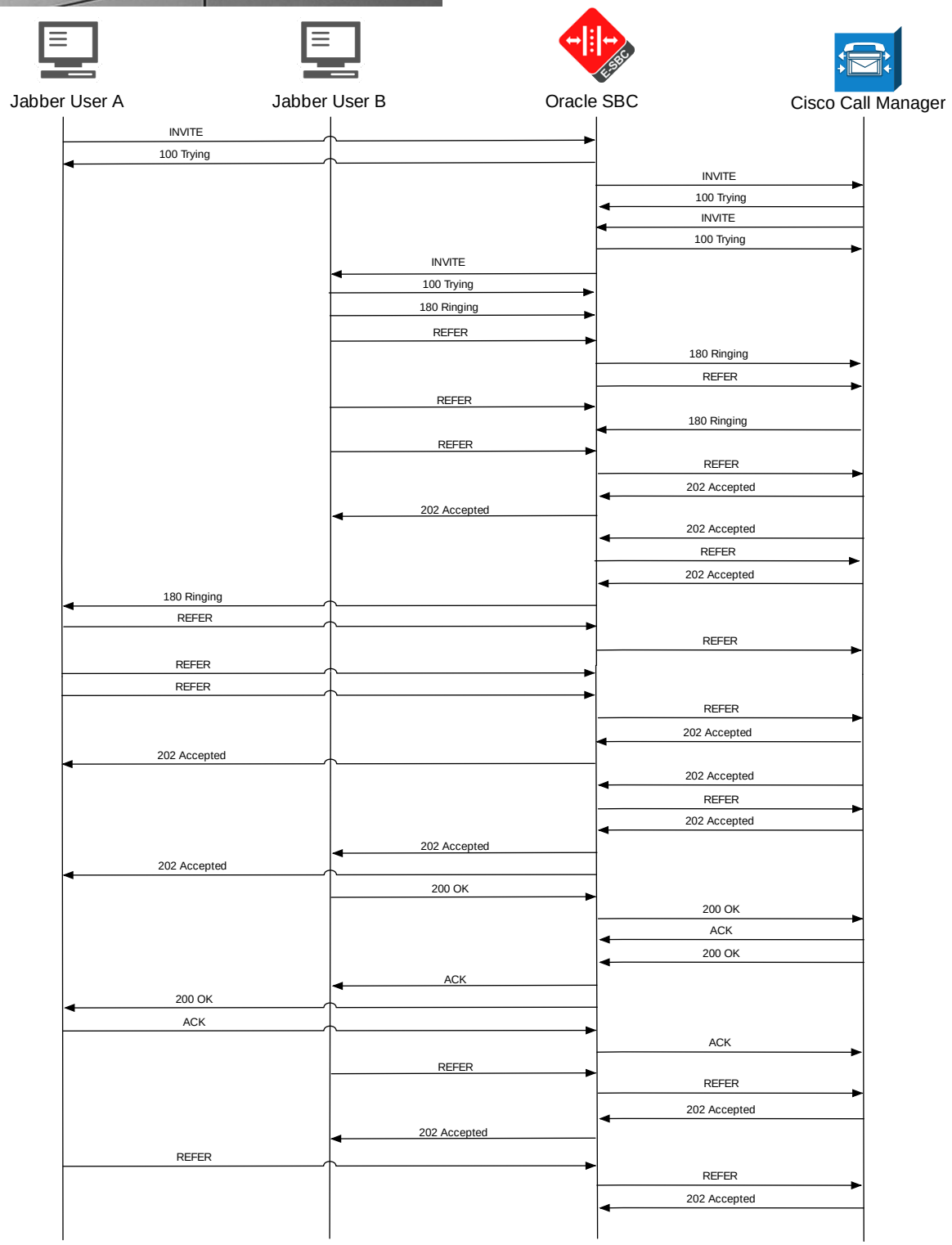
6. Configuring the Cisco Phones

There is no special configuration required on the Cisco phones. They should be configured to use DHCP.

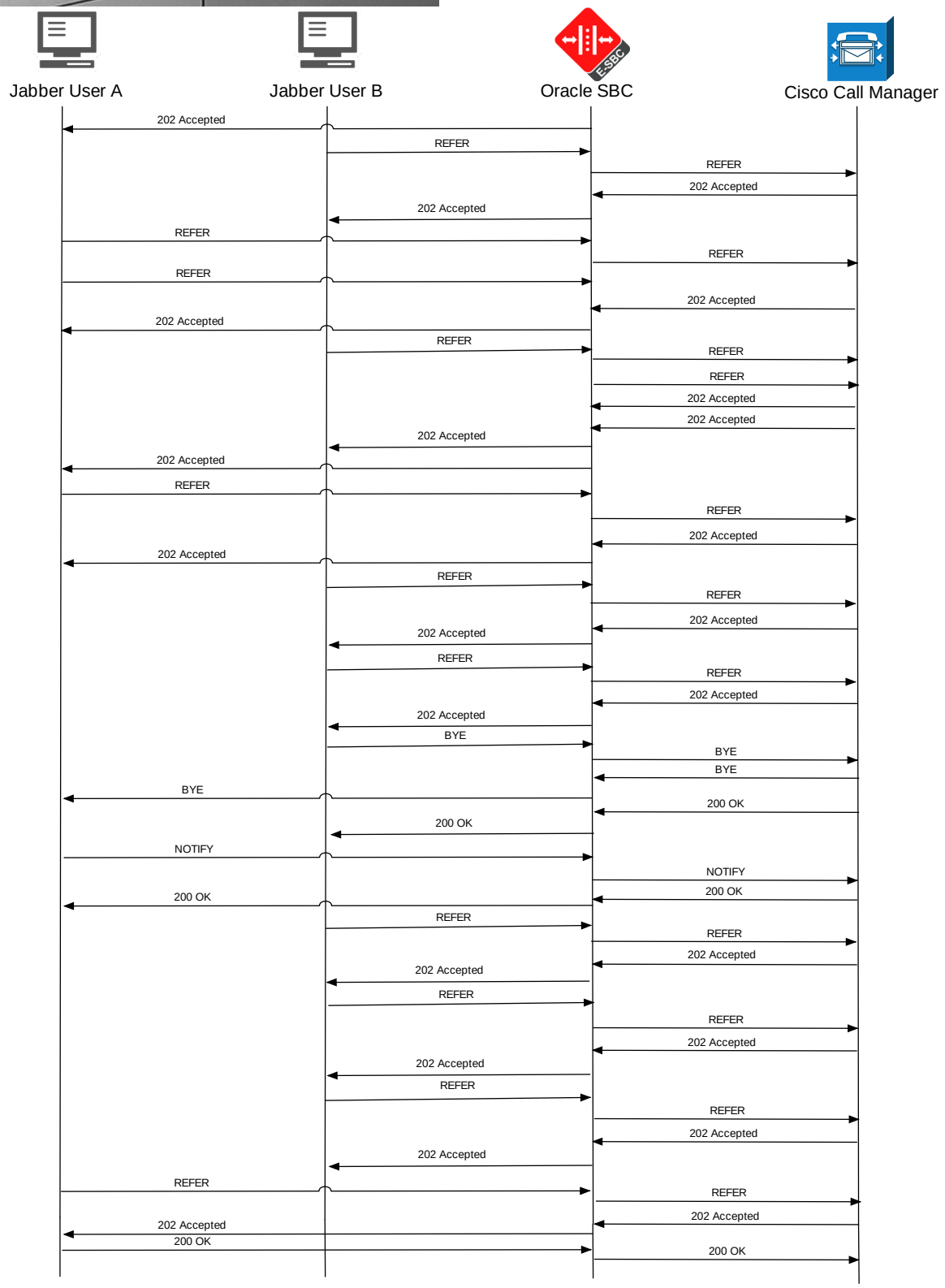
7. SIP Messaging Capacity Considerations with Jabber

The following diagram (two pages) depicts a typical call with video enabled on both endpoints. Even though user B did not have a camera on their laptop, it still resulted in a large number of REFER and 202 Accepted messages related to video. Disabling video on CUCM for these users cut down from 38 REFERs/202s to 16, significantly reducing the number of SIP messages per call between Jabber users, with the total number of messages decreasing from 52 messages down to 34, or 17 messages per user per call. This is still 10 more messages than a typical VoIP call (INVITE, 100 Trying, 180 Ringing, 200 OK, ACK, BYE, 200 OK).

To disable video for each user in CUCM, go to Device > Phone, then click on the Device Name (Line). Under the Product Specific Configuration Layout section, set Video Calling to Disabled. **Note that this also disables screen sharing capabilities.**



Continued on next page…


Jabber User A
Jabber User B
Oracle SBC
Cisco Call Manager
202 Accepted
REFER
REFER
202 Accepted
202 Accepted
REFER
REFER
REFER
REFER
202 Accepted
202 Accepted
REFER
REFER
REFER
202 Accepted
202 Accepted
202 Accepted
202 Accepted
202 Accepted
REFER
REFER
202 Accepted
202 Accepted
REFER
REFER
202 Accepted
202 Accepted
REFER
REFER
202 Accepted
202 Accepted
BYE
BYE
BYE
BYE
200 OK
200 OK
NOTIFY
NOTIFY
200 OK
200 OK
REFER
REFER
202 Accepted
202 Accepted
REFER
REFER
202 Accepted
202 Accepted
REFER
REFER
202 Accepted
202 Accepted
REFER
REFER
202 Accepted
202 Accepted
200 OK
200 OK

8. Configuring Outside (Access Side) DNS

The following entries are required in the outside (access side) DNS server, accessible to the Jabber clients and phones.

SRV record 1 (required only for Jabber)
- Domain: customer.com (change this to be your customer's domain)
- Service: _cisco-uds
- Protocol: _tcp
- Priority: 0
- Weight: 0
- Port Number: 8443
- Host offering service: CUCM-Cisco (change this to be CUCM's hostname)

A record 1 (required for Jabber and phones)
- FQDN: CUCM-Cisco.customer.com (change this to be your customer's FQDN)
- IP address: 10.232.40.10 (the SBC's outside/access side IP)

DNS records in the Oracle lab DNS zone file (Linux DNS server):

```
CUCM-Cisco          IN    A     10.232.40.10
_cisco-uds._tcp     IN    SRV   0     0     8443   CUCM-Cisco
```

9. Configuring the Oracle Enterprise SBC

In this section we describe the steps for configuring an Oracle Enterprise SBC, formally known as an Acme Packet Net-Net Session Director ("SBC"), for use with the Cisco Jabber client, Cisco phones, and Call Manager (CUCM) server.

9.1. In Scope

The following guide configuring the Oracle SBC assumes that this is a newly deployed device dedicated to a single customer. Please see the ACLI Configuration Guide on http://docs.oracle.com/cd/E61547_01/index.htm for a better understanding of the Command Line Interface (CLI).

Note that Oracle offers several models of the SBC. This document covers the setup for the 1100, 3820, 4500, 4600, and 6300 platforms running OS E-CZ730p2. If instructions are needed for other Oracle SBC models, please contact your Oracle representative.

9.2. Out of Scope

- Configuration of Network management including SNMP and RADIUS.
- Configuration of Distributed Denial of Service (DDoS) protection parameters as these are based on individual customer requirements.
- Configuration of High Availability (HA).
- SIP/TLS and SRTP are not currently supported by the Oracle SBC with Cisco Jabber, phones, and CUCM.

9.3. What will you need

- RJ45/DB9 serial adapter provided with the SBC, along with a straight-through Ethernet cable to go from the adapter to the SBC's console port on the front of the SBC.
- Terminal emulation application such as PuTTY or HyperTerm
- Passwords for the User and Superuser modes on the Oracle SBC
- IP address to be assigned to management interface (eth0, labeled Mgmt0 on the SBC chassis) of the SBC - the eth0 management interface must be connected and configured to a management network separate from the service interfaces. Otherwise the SBC is subject to ARP overlap issues, loss of system access when the network is down, and compromising DDoS protection. Oracle does not support SBC configurations with management and media/service interfaces on the same subnet.
- IP addresses of the Cisco Call Manager (CUCM) and Cisco Unity Connection (CUC) servers
- IP addresses to be used for the SBC internal and external facing ports (Service Interfaces)

9.4. Configuring the SBC

Once the Oracle SBC is racked and the power cable connected, you are ready to set up physical network connectivity. **Note: use the console port on the front of the SBC, not the one on the back, on platforms such as the 3820 and 4500 that have two console ports.**

Plug the slot 0 port 0 (s0p0) interface into your outside (Jabber client-facing) network and the slot 0 port 1 (s0p1) interface into your inside (CUCM-facing) network. Once connected, perform you are ready to power on and perform the following steps.

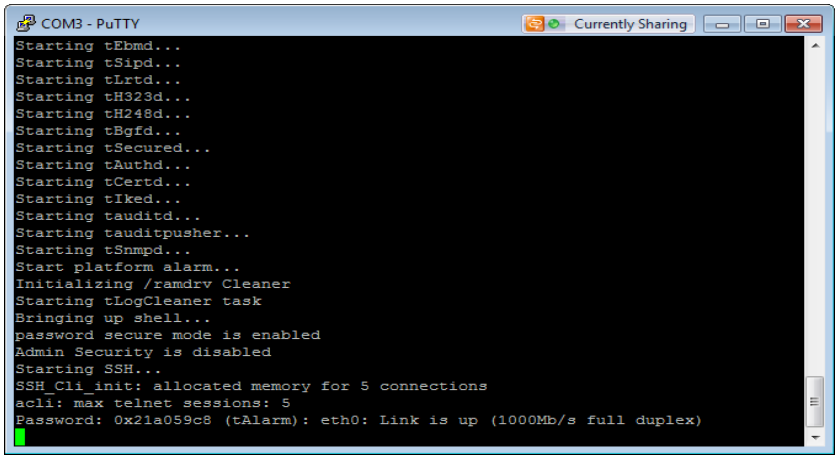
All commands are in bold, such as **`configure terminal`**; parameters in bold red such as **oraclesbc1** are parameters which are specific to an individual deployment. **Note:** The CLI is case sensitive.

Establish the serial connection and logging in the SBC

Confirm the SBC is powered off and connect one end of a straight-through Ethernet cable to the console port on the SBC and the other end to console adapter that ships with the SBC, connect the console adapter (a DB9 adapter) to the DB9 port on a workstation, running a terminal emulator application such as PuTTY. Start the terminal emulation application using the following settings:

- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None

Power on the SBC and confirm that you see the following output from the bootup sequence.



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

```
Password: acme
acmesystem> enable
Password: packet
acmesystem# configure terminal
acmesystem(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 SBC by going to

oraclesbc1#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. **Note these example boot parameters are specific to the 3820 platform. Other platforms will have different boot parameters. Use nnECZ730p2.64.bz for the 1100, 4500, 4600, and the 6300. Use nnECZ730p2.32.bz for the 3820.**

```
oraclesbc1#(configure)bootparam
'.' = clear field;  '-' = go to previous field;  q = quit
boot device             : eth0
processor number        : 0
host name               :
file name               : /boot/nnECZ730p2.32.bz --- >location where
the software is loaded on the SBC.
inet on ethernet (e)    : 172.18.255.52:ffffff00 --- > This is the ip
address of the management interface of the SBC, type the IP address and
mask in hex (e.g., 255.255.255.0 is ffffff00)
```

```
inet on backplane (b)   :
host inet (h)           :
gateway inet (g)        : 172.18.0.1 --- > management
gateway address here
user (u)                : vxftp
ftp password (pw) (blank = use rsh)     : vxftp flags (f)       :
target name (tn)        : oraclesbc1 --- > hostname of the SBC.  In a Highly
Available (HA) pair, each SBC will have its own hostname.  These target
names will match those configured in the redundancy-config in an HA pair.
startup script (s)      :
other (o)               :
```

9.5. SIP/TCP and RTP Configuration

```
local-policy

        from-address                            *
        to-address                              *
        source-realm                            access
        description
        activate-time
        deactivate-time
        state                                   enabled
        policy-priority                         none
        policy-attribute
                next-hop                                10.232.50.89
                realm                                   core
                action                                  none
                terminate-recursion                     disabled
                carrier
                start-time                              0000
                end-time                                2400
                days-of-week                            U-S
                cost                                    0
                state                                   enabled
                app-protocol
                methods
                media-profiles
                lookup                                  single
                next-key
                eloc-str-lkup                           disabled
                eloc-str-match
```

```
media-manager
        state                                   enabled
        latching                                enabled
        flow-time-limit                         86400
        initial-guard-timer                     300
        subsq-guard-timer                       300
        tcp-flow-time-limit                     86400
        tcp-initial-guard-timer                 300
        tcp-subsq-guard-timer                   300
        tcp-number-of-ports-per-flow            2
        hnt-rtcp                                disabled
        algd-log-level                          NOTICE
        mbcd-log-level                          NOTICE
        options                                 unique-sdp-id
        red-flow-port                           1985
        red-mgcp-port                           1986
        red-max-trans                           10000
        red-sync-start-time                     5000
        red-sync-comp-time                      1000
        media-policing                          enabled
        max-signaling-bandwidth                 10000000
        max-untrusted-signaling                 100
        min-untrusted-signaling                 30
        app-signaling-bandwidth                 0
        tolerance-window                        30
        trap-on-demote-to-deny                  disabled
        trap-on-demote-to-untrusted             disabled
        syslog-on-demote-to-deny                disabled
        syslog-on-demote-to-untrusted           disabled
        rtcp-rate-limit                         0
        anonymous-sdp                           enabled
        arp-msg-bandwidth                       32000
        fragment-msg-bandwidth                  0
        rfc2833-timestamp                       disabled
        default-2833-duration                   100
        rfc2833-end-pkts-only-for-non-sig       enabled
        translate-non-rfc2833-event             disabled
        media-supervision-traps                 disabled
        dnsalg-server-failover                  disabled
        syslog-on-call-reject                   disabled
```

```
network-interface
        name                                    s0p0
        sub-port-id                             0
        description
        hostname
        ip-address                              10.232.40.10
        pri-utility-addr
        sec-utility-addr
        netmask                                 255.255.255.0
        gateway                                 10.232.40.1
        sec-gateway
        gw-heartbeat
                state                                   disabled
                heartbeat                               0
                retry-count                             0
                retry-timeout                           1
                health-score                            0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                             11
        signaling-mtu                           0
        hip-ip-list                             10.232.40.10
        ftp-address
        icmp-address                            10.232.40.10
        snmp-address
        telnet-address
        ssh-address
network-interface
        name                                    s0p1
        sub-port-id                             0
        description
        hostname
        ip-address                              10.232.50.10
        pri-utility-addr
        sec-utility-addr
        netmask                                 255.255.255.0
        gateway                                 10.232.50.1
        sec-gateway
        gw-heartbeat
                state                                   disabled
                heartbeat                               0
                retry-count                             0
                retry-timeout                           1
                health-score                            0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                             11
        signaling-mtu                           0
        hip-ip-list                             10.232.50.10
        ftp-address
        icmp-address                            10.232.50.10
        snmp-address
        telnet-address
        ssh-address
```

```
phy-interface
        name                                    s0p0
        operation-type                          Media
        port                                    0
        slot                                    0
        virtual-mac
        admin-state                             enabled
        auto-negotiation                        enabled
        duplex-mode                             FULL
        speed                                   100
        wancom-health-score                     50
        overload-protection                     disabled
        mac-filtering                           disabled
phy-interface
        name                                    s0p1
        operation-type                          Media
        port                                    1
        slot                                    0
        virtual-mac
        admin-state                             enabled
        auto-negotiation                        enabled
        duplex-mode                             FULL
        speed                                   100
        wancom-health-score                     50
        overload-protection                     disabled
        mac-filtering                           disabled
realm-config
        identifier                              access
        description
        addr-prefix                             0.0.0.0
        network-interfaces                      s0p0:0
        mm-in-realm                             disabled
        mm-in-network                           enabled
        mm-same-ip                              enabled
        mm-in-system                            enabled
        bw-cac-non-mm                           disabled
        msm-release                             disabled
        qos-enable                              disabled
        generate-UDP-checksum                   disabled
        max-bandwidth                           0
        fallback-bandwidth                      0
        max-priority-bandwidth                  0
        max-latency                             0
        max-jitter                              0
        max-packet-loss                         0
        observ-window-size                      0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        srtp-msm-passthrough                    disabled
        class-profile
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid                      NAT_IP
        average-rate-limit                      0
        access-control-trust-level              none
        invalid-signal-threshold                0
        maximum-signal-threshold                0
        untrusted-signal-threshold              0
        nat-trust-threshold                     0
        max-endpoints-per-nat                   0
```

```
        nat-invalid-message-threshold           0
        wait-time-for-invalid-register          0
        deny-period                             30
        cac-failure-threshold                   0
        untrust-cac-failure-threshold           0
        ext-policy-svr
        diam-e2-address-realm
        subscription-id-type                    END_USER_NONE
        symmetric-latching                      disabled
        pai-strip                               disabled
        trunk-context
        device-id
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching                     none
        restriction-mask                        32
        user-cac-mode                           none
        user-cac-bandwidth                      0
        user-cac-sessions                       0
        icmp-detect-multiplier                  0
        icmp-advertisement-interval             0
        icmp-target-ip
        monthly-minutes                         0
        options
        spl-options
        accounting-enable                       enabled
        net-management-control                  disabled
        delay-media-update                      disabled
        refer-call-transfer                     disabled
        hold-refer-reinvite                     disabled
        refer-notify-provisional                none
        dyn-refer-term                          disabled
        codec-policy
        codec-manip-in-realm                    disabled
        codec-manip-in-network                  enabled
        rtcp-policy
        constraint-name
        call-recording-server-id
        session-recording-server
        session-recording-required              disabled
        manipulation-string
        manipulation-pattern
        stun-enable                             disabled
        stun-server-ip                          0.0.0.0
        stun-server-port                        3478
        stun-changed-ip                         0.0.0.0
        stun-changed-port                       3479
        sip-profile
        sip-isup-profile
        match-media-profiles
        qos-constraint
        block-rtcp                              disabled
        hide-egress-media-update                disabled
        tcp-media-profile
        monitoring-filters
        node-functionality
        default-location-string
        alt-family-realm
        pref-addr-type                          none
```

```
realm-config
        identifier                              core
        description
        addr-prefix                             0.0.0.0
        network-interfaces                      s0p1:0
        mm-in-realm                             disabled
        mm-in-network                           enabled
        mm-same-ip                              enabled
        mm-in-system                            enabled
        bw-cac-non-mm                           disabled
        msm-release                             disabled
        qos-enable                              disabled
        generate-UDP-checksum                   disabled
        max-bandwidth                           0
        fallback-bandwidth                      0
        max-priority-bandwidth                  0
        max-latency                             0
        max-jitter                              0
        max-packet-loss                         0
        observ-window-size                      0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        srtp-msm-passthrough                    disabled
        class-profile
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid                      NAT_IP
        average-rate-limit                      0
        access-control-trust-level              none
        invalid-signal-threshold                0
        maximum-signal-threshold                0
        untrusted-signal-threshold              0
        nat-trust-threshold                     0
        max-endpoints-per-nat                   0
        nat-invalid-message-threshold           0
        wait-time-for-invalid-register          0
        deny-period                             30
        cac-failure-threshold                   0
        untrust-cac-failure-threshold           0
        ext-policy-svr
        diam-e2-address-realm
        subscription-id-type                    END_USER_NONE
        symmetric-latching                      disabled
        pai-strip                               disabled
        trunk-context
        device-id
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching                     none
        restriction-mask                        32
        user-cac-mode                           none
        user-cac-bandwidth                      0
        user-cac-sessions                       0
        icmp-detect-multiplier                  0
        icmp-advertisement-interval             0
        icmp-target-ip
        monthly-minutes                         0
        options
        spl-options
```

```
        accounting-enable                       enabled
        net-management-control                  disabled
        delay-media-update                      disabled
        refer-call-transfer                     disabled
        hold-refer-reinvite                     disabled
        refer-notify-provisional                none
        dyn-refer-term                          disabled
        codec-policy
        codec-manip-in-realm                    disabled
        codec-manip-in-network                  enabled
        rtcp-policy
        constraint-name
        call-recording-server-id
        session-recording-server
        session-recording-required              disabled
        manipulation-string
        manipulation-pattern
        stun-enable                             disabled
        stun-server-ip                          0.0.0.0
        stun-server-port                        3478
        stun-changed-ip                         0.0.0.0
        stun-changed-port                       3479
        sip-profile
        sip-isup-profile
        match-media-profiles
        qos-constraint
        block-rtcp                              disabled
        hide-egress-media-update                disabled
        tcp-media-profile
        monitoring-filters
        node-functionality
        default-location-string
        alt-family-realm
        pref-addr-type                          none
session-agent
        hostname                                10.232.50.89
        ip-address
        port                                    5060
        state                                   enabled
        app-protocol                            SIP
        app-type
        transport-method                        StaticTCP
        realm-id                                core
        egress-realm-id
        description                             Cisco CUCM
        carriers
        allow-next-hop-lp                       enabled
        constraints                             disabled
        max-sessions                            0
        max-inbound-sessions                    0
        max-outbound-sessions                   0
        max-burst-rate                          0
        max-inbound-burst-rate                  0
        max-outbound-burst-rate                 0
        max-sustain-rate                        0
        max-inbound-sustain-rate                0
        max-outbound-sustain-rate               0
        min-seizures                            5
        min-asr                                 0
        time-to-resume                          0
        ttr-no-response                         0
        in-service-period                       0
        burst-rate-window                       0
        sustain-rate-window                     0
        req-uri-carrier-mode                    None
        proxy-mode
```

```
        redirect-action
        loose-routing                           enabled
        send-media-session                      enabled
        response-map
        ping-method                             OPTIONS;hops=0
        ping-interval                           30
        ping-send-mode                          keep-alive
        ping-all-addresses                      disabled
        ping-in-service-response-codes
        out-service-response-codes
        load-balance-dns-query                  hunt
        options
        spl-options
        media-profiles
        in-translationid
        out-translationid
        trust-me                                disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate               0
        early-media-allow
        invalidate-registrations                disabled
        rfc2833-mode                            none
        rfc2833-payload                         0
        codec-policy
        enforcement-profile
        refer-call-transfer                     disabled
        refer-notify-provisional                none
        reuse-connections                       NONE
        tcp-keepalive                           none
        tcp-reconn-interval                     0
        max-register-burst-rate                 0
        register-burst-window                   0
        sip-profile
        sip-isup-profile
        kpml-interworking                       inherit
        monitoring-filters
        session-recording-server
        session-recording-required              disabled
        hold-refer-reinvite                     disabled
        send-tcp-fin                            disabled
```

```
sip-config
        state                                   enabled
        operation-mode                          dialog
        dialog-transparency                     enabled
        home-realm-id                           core
        egress-realm-id
        auto-realm-id
        nat-mode                                None
        registrar-domain                        *
        registrar-host                          *
        registrar-port                          5060
        register-service-route                  always
        init-timer                              500
        max-timer                               4000
        trans-expire                            32
        initial-inv-trans-expire                0
        invite-expire                           180
        inactive-dynamic-conn                   32
        enforcement-profile
        pac-method
        pac-interval                            10
        pac-strategy                            PropDist
        pac-load-weight                         1
        pac-session-weight                      1
        pac-route-weight                        1
        pac-callid-lifetime                     600
        pac-user-lifetime                       3600
        red-sip-port                            1988
        red-max-trans                           10000
        red-sync-start-time                     5000
        red-sync-comp-time                      1000
        options                                 reg-cache-mode=from
        add-reason-header                       disabled
        sip-message-len                         4096
        enum-sag-match                          disabled
        extra-method-stats                      disabled
        extra-enum-stats                        disabled
        rph-feature                             disabled
        nsep-user-sessions-rate                 0
        nsep-sa-sessions-rate                   0
        registration-cache-limit                0
        register-use-to-for-lp                  disabled
        refer-src-routing                       disabled
        add-ucid-header                         disabled
        proxy-sub-events
        allow-pani-for-trusted-only             disabled
        atcf-stn-sr
        atcf-psi-dn
        atcf-route-to-sccas                     disabled
        eatf-stn-sr
        pass-gruu-contact                       disabled
        sag-lookup-on-redirect                  disabled
        set-disconnect-time-on-bye              disabled
        msrp-delayed-bye-timer                  15
        transcoding-realm
        transcoding-agents
        create-dynamic-sa                       disabled
        node-functionality                      P-CSCF
        match-sip-instance                      disabled
        sa-routes-stats                         disabled
        sa-routes-traps                         disabled
        rx-sip-reason-mapping                   disabled
        add-ue-location-in-pani                 disabled
        hold-emergency-calls-for-loc-info       0
```

```
sip-feature
        name                                    norefersub
        realm
        support-mode-inbound                    Pass
        require-mode-inbound                    Pass
        proxy-require-mode-inbound              Pass
        support-mode-outbound                   Pass
        require-mode-outbound                   Pass
        proxy-require-mode-outbound             Pass
sip-interface
        state                                   enabled
        realm-id                                access
        description
        sip-port
                address                                 10.232.40.10
                port                                    5060
                transport-protocol                      TCP
                tls-profile
                allow-anonymous                         registered
                multi-home-addrs
                ims-aka-profile
        carriers
        trans-expire                            0
        initial-inv-trans-expire                0
        invite-expire                           0
        max-redirect-contacts                   0
        proxy-mode
        redirect-action
        contact-mode                            none
        nat-traversal                           always
        nat-interval                            30
        tcp-nat-interval                        90
        registration-caching                    enabled
        min-reg-expire                          300
        registration-interval                   3600
        route-to-registrar                      enabled
        secured-network                         disabled
        teluri-scheme                           disabled
        uri-fqdn-domain
        options                                 reg-via-key
                                                reg-via-match

        spl-options
        trust-mode                              all
        max-nat-interval                        3600
        nat-int-increment                       10
        nat-test-increment                      30
        sip-dynamic-hnt                         disabled
        stop-recurse                            401,407
        port-map-start                          0
        port-map-end                            0
        in-manipulationid
        out-manipulationid
        sip-ims-feature                         disabled
        sip-atcf-feature                        disabled
        subscribe-reg-event                     disabled
        operator-identifier
        anonymous-priority                      none
        max-incoming-conns                      0
        per-src-ip-max-incoming-conns           0
        inactive-conn-timeout                   0
        untrusted-conn-timeout                  0
        network-id
        ext-policy-server
        ldap-policy-server
        default-location-string
        term-tgrp-mode                          none
```

```
        charging-vector-mode                    pass
        charging-function-address-mode          pass
        ccf-address
        ecf-address
        implicit-service-route                  disabled
        rfc2833-payload                         101
        rfc2833-mode                            transparent
        constraint-name
        response-map
        local-response-map
        sec-agree-feature                       disabled
        sec-agree-pref                          ipsec3gpp
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                           none
        add-sdp-invite                          disabled
        p-early-media-header                    disabled
        p-early-media-direction
        add-sdp-profiles
        manipulation-string
        manipulation-pattern
        sip-profile
        sip-isup-profile
        tcp-conn-dereg                          0
        tunnel-name
        register-keep-alive                     none
        kpml-interworking                       disabled
        msrp-delay-egress-bye                   disabled
        send-380-response
        pcscf-restoration
        session-timer-profile
        session-recording-server
        session-recording-required              disabled
        service-tag
        reg-cache-route                         disabled
sip-interface
        state                                   enabled
        realm-id                                core
        description
        sip-port
                address                                 10.232.50.10
                port                                    5060
                transport-protocol                      TCP
                tls-profile
                allow-anonymous                         all
                multi-home-addrs
                ims-aka-profile
        carriers
        trans-expire                            0
        initial-inv-trans-expire                0
        invite-expire                           0
        max-redirect-contacts                   0
        proxy-mode
        redirect-action
        contact-mode                            none
        nat-traversal                           none
        nat-interval                            30
        tcp-nat-interval                        90
        registration-caching                    disabled
        min-reg-expire                          300
        registration-interval                   3600
        route-to-registrar                      disabled
```

```
        secured-network                          disabled
        teluri-scheme                            disabled
        uri-fqdn-domain
        options
        spl-options
        trust-mode                               all
        max-nat-interval                         3600
        nat-int-increment                        10
        nat-test-increment                       30
        sip-dynamic-hnt                          disabled
        stop-recurse                             401,407
        port-map-start                           0
        port-map-end                             0
        in-manipulationid
        out-manipulationid
        sip-ims-feature                          disabled
        sip-atcf-feature                         disabled
        subscribe-reg-event                      disabled
        operator-identifier
        anonymous-priority                       none
        max-incoming-conns                       0
        per-src-ip-max-incoming-conns            0
        inactive-conn-timeout                    0
        untrusted-conn-timeout                   0
        network-id
        ext-policy-server
        ldap-policy-server
        default-location-string
        term-tgrp-mode                           none
        charging-vector-mode                     pass
        charging-function-address-mode           pass
        ccf-address
        ecf-address
        implicit-service-route                   disabled
        rfc2833-payload                          101
        rfc2833-mode                             transparent
        constraint-name
        response-map
        local-response-map
        sec-agree-feature                        disabled
        sec-agree-pref                           ipsec3gpp
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                            none
        add-sdp-invite                           disabled
        p-early-media-header                     disabled
        p-early-media-direction
        add-sdp-profiles
        manipulation-string
        manipulation-pattern
        sip-profile
        sip-isup-profile
        tcp-conn-dereg                           0
        tunnel-name
        register-keep-alive                      none
        kpml-interworking                        disabled
        msrp-delay-egress-bye                    disabled
        send-380-response
        pcscf-restoration
        session-timer-profile
        session-recording-server
        session-recording-required               disabled
        service-tag
        reg-cache-route                          disabled
```

```
sip-manipulation
        name                                    NAT_IP
        description
        split-headers
        join-headers
        header-rule
                name                                    From
                header-name                             From
                action                                  manipulate
                comparison-type                         case-sensitive
                msg-type                                request
                methods
                match-value
                new-value
                element-rule
                        name                                    modFromUri
                        parameter-name
                        type                                    uri-host
                        action                                  replace
                        match-val-type                          ip
                        comparison-type                         case-sensitive
                        match-value
                        new-value                               $LOCAL_IP
        header-rule
                name                                    To
                header-name                             To
                action                                  manipulate
                comparison-type                         case-sensitive
                msg-type                                request
                methods
                match-value
                new-value
                element-rule
                        name                                    modToUri
                        parameter-name
                        type                                    uri-host
                        action                                  replace
                        match-val-type                          ip
                        comparison-type                         case-sensitive
                        match-value
                        new-value                               $REMOTE_IP
        header-rule
                name                                    Ruri
                header-name                             request-uri
                action                                  manipulate
                comparison-type                         case-sensitive
                msg-type                                request
                methods
                match-value
                new-value
                element-rule
                        name                                    modRuri
                        parameter-name
                        type                                    uri-host
                        action                                  replace
                        match-val-type                          ip
                        comparison-type                         case-sensitive
                        match-value
                        new-value                               $REMOTE_IP
```

```
header-rule
        name                                    Rpid
        header-name                             Remote-Party-ID
        action                                  manipulate
        comparison-type                         case-sensitive
        msg-type                                any
        methods
        match-value
        new-value
        element-rule
                name                                    modRpidHost
                parameter-name
                type                                    uri-host
                action                                  replace
                match-val-type                          ip
                comparison-type                         case-sensitive
                match-value
                new-value                               $LOCAL_IP
header-rule
        name                                    ReferredBy
        header-name                             Referred-By
        action                                  manipulate
        comparison-type                         case-sensitive
        msg-type                                request
        methods
        match-value
        new-value
        element-rule
                name                                    modReferredByUri
                parameter-name
                type                                    uri-host
                action                                  replace
                match-val-type                          ip
                comparison-type                         case-sensitive
                match-value
                new-value                               $LOCAL_IP
header-rule
        name                                    StoreReferTo
        header-name                             Refer-To
        action                                  store
        comparison-type                         pattern-rule
        msg-type                                request
        methods
        match-value                             (.+@)([0-9.]+)(.*)
        new-value
header-rule
        name                                    modReferToUri
        header-name                             Refer-To
        action                                  manipulate
        comparison-type                         boolean
        msg-type                                request
        methods
        match-value                             $StoreReferTo
        new-value            $StoreReferTo.$1+$LOCAL_IP+$StoreReferTo.$3
header-rule
        name                                    StoreContentId
        header-name                             Content-Id
        action                                  store
        comparison-type                         pattern-rule
        msg-type                                request
        methods
        match-value                             (.+@)([0-9.]+)>
        new-value
```

```
        header-rule
                name                                    modContentIdUri
                header-name                             Content-Id
                action                                  manipulate
                comparison-type                         boolean
                msg-type                                request
                methods
                match-value                             $StoreContentId
                new-value                       $StoreContentId.$1+$LOCAL_IP+>
        header-rule
                name                                    modXml
                header-name                             Content-Type
                action                                  manipulate
                comparison-type                         case-sensitive
                msg-type                                request
                methods                                 NOTIFY
                match-value
                new-value
                element-rule
                        name                                    natXml
                        parameter-name             application/dialog-info+xml
                        type                                    mime
                        action                                find-replace-all
                        match-val-type                          ip
                        comparison-type                         pattern-rule
                        match-value
entity=(.*)(\b(?:\d{1,3}\.){3}\d{1,3}\b)[[:2:]]
                        new-value                               $LOCAL_IP

NOTE:  the match-value in the natXml element-rule needs to have the question
mark escaped with a backslash before it when entering it in the CLI.  Here is
the command to issue:

match-value entity=(.*)(\b(\?:\d{1,3}\.){3}\d{1,3}\b)[[:2:]]
```

```
static-flow
        in-realm-id                                 access
        description                                 For Voicemail Access to Cisco
Unity Connection (CUC) for Jabber only
        in-source                                   0.0.0.0
        in-destination                              10.232.40.10:443
        out-realm-id                                core
        out-source                                  10.232.50.10
        out-destination                             10.232.50.103:443
        protocol                                    TCP
        alg-type                                    NAPT
        start-port                                  30001
        end-port                                    40000
        flow-time-limit                             0
        initial-guard-timer                         60
        subsq-guard-timer                           60
        average-rate-limit                          0
static-flow
        in-realm-id                                 access
        description
        in-source                                   0.0.0.0
        in-destination                              10.232.40.10:6970
        out-realm-id                                core
        out-source                                  10.232.50.10
        out-destination                             10.232.50.89:6970
        protocol                                    TCP
        alg-type                                    NAPT
        start-port                                  20001
        end-port                                    30000
        flow-time-limit                             0
        initial-guard-timer                         60
        subsq-guard-timer                           60
        average-rate-limit                          0
static-flow
        in-realm-id                                 access
        description                                 For Voicemail Access to Cisco
Unity Connection (CUC) for Jabber only
        in-source                                   0.0.0.0
        in-destination                              10.232.40.10:7080
        out-realm-id                                core
        out-source                                  10.232.50.10
        out-destination                             10.232.50.103:7080
        protocol                                    TCP
        alg-type                                    NAPT
        start-port                                  40001
        end-port                                    50000
        flow-time-limit                             0
        initial-guard-timer                         60
        subsq-guard-timer                           60
        average-rate-limit                          0
static-flow
        in-realm-id                                 access
        description
        in-source                                   0.0.0.0
        in-destination                              10.232.40.10:8443
        out-realm-id                                core
        out-source                                  10.232.50.10
        out-destination                             10.232.50.89:8443
        protocol                                    TCP
        alg-type                                    NAPT
        start-port                                  10000
        end-port                                    20000
        flow-time-limit                             0
        initial-guard-timer                         60
        subsq-guard-timer                           60
        average-rate-limit                          0
```

```
steering-pool
        ip-address                                      10.232.40.10
        start-port                                      49152
        end-port                                        65535
        realm-id                                        access
        network-interface
steering-pool
        ip-address                                      10.232.50.10
        start-port                                      49152
        end-port                                        65535
        realm-id                                        core
        network-interface
system-config
        hostname
        description
        location
        mib-system-contact
        mib-system-name
        mib-system-location
        snmp-enabled                                    enabled
        enable-snmp-auth-traps                          disabled
        enable-snmp-syslog-notify                       disabled
        enable-snmp-monitor-traps                       disabled
        enable-env-monitor-traps                        disabled
        snmp-syslog-his-table-length                    1
        snmp-syslog-level                               WARNING
        system-log-level                                WARNING
        process-log-level                               NOTICE
        process-log-ip-address                          0.0.0.0
        process-log-port                                0
        collect
                sample-interval                                 5
                push-interval                                   15
                boot-state                                      disabled
                start-time                                      now
                end-time                                        never
                red-collect-state                               disabled
                red-max-trans                                   1000
                red-sync-start-time                             5000
                red-sync-comp-time                              1000
                push-success-trap-state                         disabled
        comm-monitor
                state                                           disabled
                sbc-grp-id                                      0
                tls-profile
                qos-enable                                      enabled
        call-trace                                      disabled
        internal-trace                                  disabled
        log-filter                                      all
        default-gateway                                 172.18.0.1 ← eth0 gateway
        restart                                         enabled
        exceptions
        telnet-timeout                                  0
        console-timeout                                 0
        remote-control                                  enabled
        cli-audit-trail                                 enabled
```

```
link-redundancy-state                    disabled
source-routing                           enabled
cli-more                                 disabled
terminal-height                          24
debug-timeout                            0
trap-event-lifetime                      0
ids-syslog-facility                      -1
options
default-v6-gateway                       ::
ipv6-signaling-mtu                       1500
ipv4-signaling-mtu                       1500
cleanup-time-of-day                      00:00
snmp-engine-id-suffix
snmp-agent-mode                          v1v2
```

A basic configuration on the SBC to route calls to and from the Cisco Call Manager environment with the Cisco Jabber client and phones is now complete. The following sections highlight some of the useful tips to configure the SBC in order to successfully resolve and overcome interoperability challenges in a SIP access environment between CUCM, Cisco Jabber, and phones. It is outside the scope of this document to include all the interoperability working information as it will differ in every deployment.

10. Test Plan Executed – Jabber

The following is the test plan executed against this setup and results have been documented below.

Test Case	Result
Basic call. User A calls User B	Pass
Basic call. User B calls User A	Pass
Basic call. A calls B, A cancels.	Pass
Basic call. A calls C, C answers, C hangs up.	Pass
Basic call. A calls C, C answers, A hangs up.	Pass
Basic call. C calls B, B answers, B hangs up.	Pass
Basic call. C calls B, B answers, C hangs up.	Pass
Long duration call. A calls B, call up for 20 minutes. Media directly between A & B	Pass
Long duration call. A calls D, call up for 20 minutes. Media through SBC.	Pass
Call Hold. A calls B, B holds, B resumes	Pass
Call Hold. A calls B, B holds, B resumes, B holds, B resumes	Pass
Attended transfer. A calls B, B answers, transfers to C, B hangs up after C answers.	Pass
Blind transfer. A calls B, B answers, transfers to C, B hangs up before C answers.	Pass
Voicemail. A calls B, B declines, A sent to VM.	Pass
Voicemail. A calls B, B forwarded to VM, A sent to VM.	Pass
Voicemail. A calls B, B doesn't answer, A sent to VM.	Pass
Voicemail. C calls B, B doesn't answer, A leaves VM. B displays MWI.	Pass
Call Forwarding. A calls B, B forwarded to C, C answers.	Pass
Conferencing. A calls B, B conferences C, C hangs up. A and B still on call.	Pass
Conferencing. A calls B, B conferences C, B hangs up. A and C still on call.	Pass
Conferencing. B calls C, A calls B, B merges calls. B hangs up. A and C still on call.	Pass
Conferencing. B calls C, A calls B, B merges calls. A hangs up. B and C still on call.	Pass
Conferencing. B calls C, A calls B, B merges calls. C hangs up. A and B still on call.	Pass
Conferencing. B calls C, A calls B, B answers. C hears MoH.	Pass

11. Test Plan Executed – Cisco Phones

The following is the test plan executed against this setup and results have been documented below.

Test Case	Result
Basic Call	Pass
Conference calling	Pass
Incoming and outgoing call logging (including missed calls)	Pass
Call Progress Tones	Pass
Call Waiting	Pass
Direct Outward Dialing	Pass
Do Not Disturb (DND)	Pass
Dual Tone Multi-Frequency signaling (DTMF) pass-through	Pass
Hunt Group	Pass
Message Waiting Indicator	Pass
Music on Hold	Pass
Single-Line Extension	Pass
Speed Dialing	Pass
Direct Inward Dialing	Pass
Call Back Activation (ring again)	Pass
Call Hold	Pass
Consultation on Hold	Pass
Call Park	Pass
Call Transfer (supervised and blind)	Pass
Call Pickup	Pass
Caller name identification display	Pass
Caller number identification display	Pass
Call Forward on Busy	Pass
Call Forward on No Answer, with the option to select variable ring count	Pass
Mute (hard or soft keys/buttons)	Pass
Last Number Redial	Pass

12. Troubleshooting Tools

If you find that you are not able to complete calls or have problems with the test cases, there are a few tools available for CUCM and the Oracle SBC like logging and tracing which may be of assistance. In this section we will provide a list of tools which you can use to aid in troubleshooting any issues you may encounter.

Cisco Real-Time Monitoring Tool (RTMT)

The Cisco Real-Time Monitoring Tool (RTMT) is a tool that can be downloaded from CUCM to a Windows or Linux computer. See https://supportforums.cisco.com/document/93281/using-rtmt-monitor-cisco-unity-connection-and-cucm for details.

Wireshark

Wireshark is also a network protocol analyzer which is freely downloadable from www.wireshark.org. Wireshark could be installed on a laptop running Jabber, and it can also be used to decode packet traces from the SBC – see the "Through a packet capture on the Oracle SBC" section below.

On the Oracle SBC

The Oracle SBC provides a rich set of statistical counters available from the CLI, 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 SBC Console:

```
oraclesbc1# reset sipd
oraclesbc1# notify sipd debug
oraclesbc1#
enabled SIP Debugging
oraclesbc1# notify all rotate-logs
```

Examining the log files

Note: You will FTP to the management interface of the SBC with the username user and user mode password (the default is "**acme**").

```
C:\Documents and Settings\user>ftp 192.168.5.24
Connected to 192.168.85.55.
220 oraclesbc1FTP server (VxWorks 6.4) ready.
User (192.168.85.55:(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.
ftp> bye
221 Goodbye.
```

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 165) of the Web GUI User Guide available at http://docs.oracle.com/cd/E61547_01/index.htm

Through a packet capture on the Oracle SBC

You can enable a packet capture on the Oracle SBC that can be decoded in Wireshark. To enable a packet capture on a network-interface:

packet-trace local <network-interface>

So for example, to start a packet capture on network-interface s0p0:0, use the following command:

packet-trace local s0p0:0

To stop the packet capture, type Control-C.

You can then FTP or Secure FTP (SFTP) the file from /opt/traces through the SBC's management interface.

13. Appendix A

Accessing the SBC's CLI

Access to the CLI is provided by:

- The serial console connection;
- TELNET, which is enabled by default but may be disabled; and
- SSH

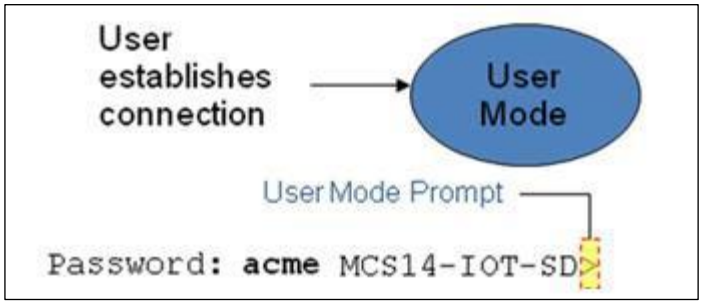
Initial connectivity will be through the serial console port. At a minimum, this is how to configure the management (eth0) interface on the SBC.

CLI Basics

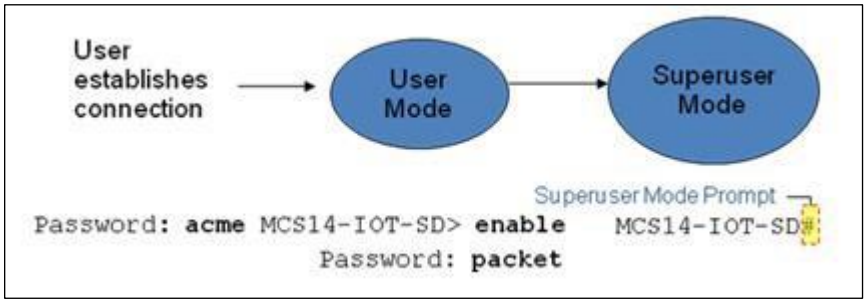
There are two password protected modes of operation within the ACLI, User mode and Superuser mode.

When you establish a connection to the 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.



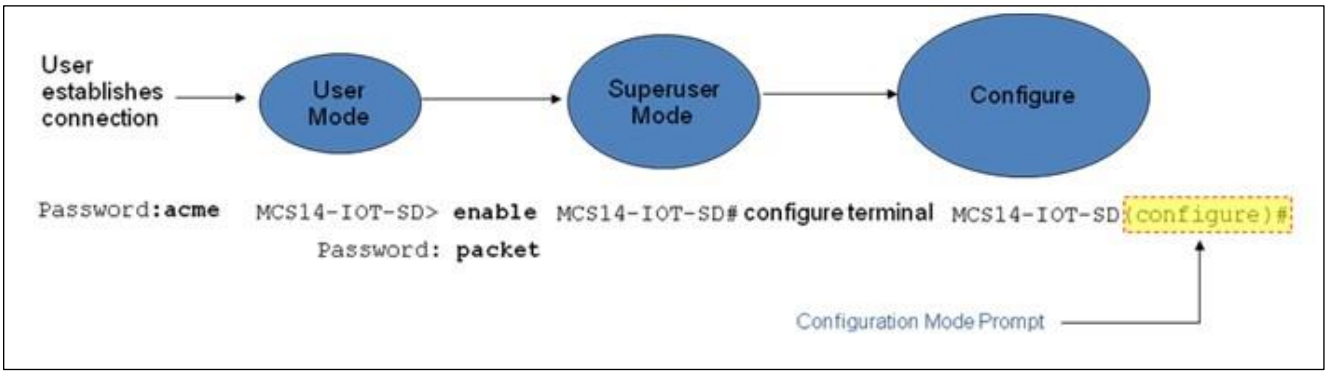
The Superuser mode allows for access to all system commands for operation, maintenance, and administration. This mode is identified by the pound sign (#) in the prompt after the target name. To enter the Superuser mode, issue the enable command in the User mode.



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.

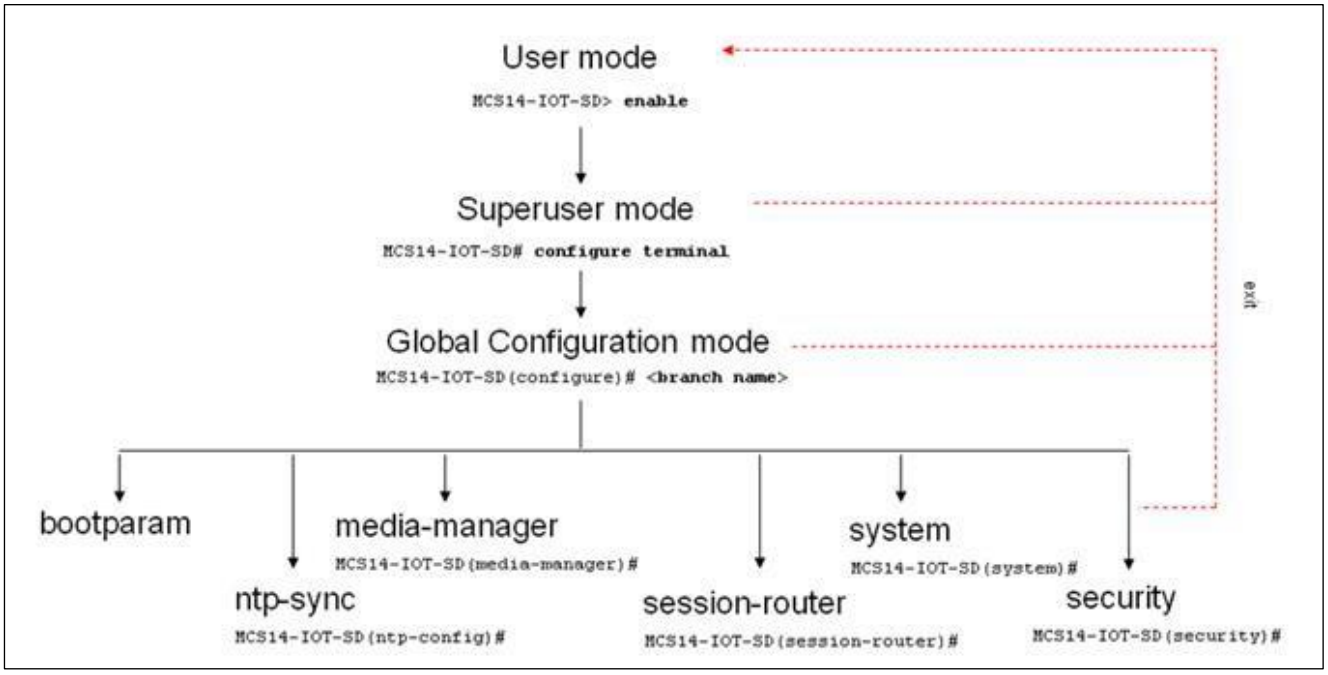
You must enter the Configuration mode to configure elements. For example, you can access the configuration branches and configuration elements for signaling and media configurations. To enter the Configuration mode, issue the **`configure terminal`** command in the Superuser mode.

Configuration mode is identified by the word configure in parenthesis followed by the pound sign (#) in the prompt after the target name, for example, **oraclesbc1(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 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.

NOTE: These are the boot parameters for the 3820 platform. Other platforms may differ.

```
oraclesbc1# configure terminal
oraclesbc1(configure)# bootparam

'.' = clear field;  '-' = go to previous field;  q = quit

boot device             : eth0
processor number  : 0
host name         :
file name         : /boot/nnECZ730p2.32.bz
inet on ethernet (e)     : 10.18.255.169:ffff0000
inet on backplane (b)    :
host inet (h)            :
gateway inet (g)  : 10.18.0.1
user (u)          : vxftp
ftp password (pw) (blank = use rsh)    : vxftp
flags (f)         : 0x3b
target name (tn)  : oraclesbc1
startup script (s)       :
other (o)         :

NOTE: These changed parameters will not go into effect until reboot.  Also, be aware that
some boot parameters may also be changed through PHY and Network Interface Configurations.

oraclesbc1(configure)#
```

The ntp-sync branch provides access to NTP server configuration commands for synchronizing the 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 CLI 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 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.

1. Enter the element that you will edit at the correct level of the CLI path.

2. 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.
3. 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.
4. 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.
5. On completion, you must issue the **`done`** command.
6. Issue the **`exit`** command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the 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,

1. Enter the **`no`** command from within the path for that specific element
2. Issue the **`exit`** command.

To delete a multiple-instance element,

1. Enter the **`no`** command from within the path for that particular element.
   The key field prompt, such as <name>:<sub-port-id>, appears.
2. Use the <Enter> key to display a list of the existing configured elements.
3. Enter the number corresponding to the element you wish to delete.
4. 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 SBC reboots, your configurations will be lost.

Configuration Versions

At any time, three versions of the configuration can exist on the 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 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 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 the 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 last 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 SBC displays a reminder on screen stating that you must use the **`activate-config`** command if you want the configurations to be updated.

```
oraclesbc1 # 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'.
oraclesbc1 #
```

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 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.

```
oraclesbc1# activate-config Activate-
Config received, processing. waiting
120000 for request to finish Request to
'ACTIVATE-CONFIG' has Finished, Activate
Complete
oraclesbc1#
```

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com