Hardware and Software
Engineered to Work Together

Oracle Communications Core Session Manager SCZ 7.1.5m1p1 and Oracle Communications Session Border Controller SCZ 7.2.0 with Broadworks Platform R19SP1

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, end users of the Oracle Communications Core Sessions Manager (CSM) and Session Border Controller (SBC). It assumes that the reader is familiar with basic operations of the Oracle Communications Core Sessions Manager and Session Border Controller.

Document Overview

This document is intended for use as a guide for a successful integration of Broadworks Platform, Oracle Communications Core Sessions Manager and Session Border Controller. It outlines the architecture design, CSM and SBC configuration including troubleshooting tools, as well as test cases executed as part of the integration process.

Introduction

Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Oracle Communications Core Session Manager and Oracle Communications Session Border Controller as an SBC IMS function. There will be steps that require navigating throught the Acme Packet Command Line Interface (ACLI). Understanding the basic concepts of TCP/UDP, IP/Routing, and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

Requirements

- Oracle Core Sessions Manager Virtual Machine series running SCZ 7.1.5m1p1.
- Oracle Session Border Controller 3820 or 4500 series running SCZ 7.2.0 GA.
- Broadworks Platform R19SP1.
- Home Subscriber Server.
- Various SIP endpoints.
- Network DNS services.
- 100MB Ethernet Switch.

Architecture

The following reference architecture shows a logical view of the connectivity.

HSS IP Mgmt:
172.18.255.18
HSS IP Cx:
10.0.200.18

BSFT NS IP (ISC):
10.0.200.11
BSFT AS IP (ISC):
10.0.200.10

Cx

sip:6175551001@as.lab
tel:+16175551001

sip:6175551002@as.lab
tel:+16175551002

Access network

sip:6175551003@as.lab
tel:+16175551003

sip:6175551011@as.lab
tel:+16175551011

Gm

Mw

ISC

Mj

ASBC IP Mgmt:
172.18.255.100
ASBC IP Access:
10.0.210.150
ASBC IP Core (Mw):
10.0.200.150

CSM IP Mgmt:
172.18.255.53
CSM IP Access (Mw):
10.0.200.110
CSM IP Core (ISC):
10.0.200.100

broadsoft

Xsp   APPLICATION
PROFILE   NETWORK
ELEMENT MGMT   MEDIA RESOURCE
CALL DETAIL   WEB

PSTN

tel:+16175551007

P-CSCF/SBC, CSM and Broadworks represent the Service provider domain infrastructure which provides PSTN service as well.
Access network represent the different access technologies (DSL, UMTS, WLAN, etc) of subscribers and enterprises.

Configuring the Oracle Communications SBC and CSM

In this section we describe the steps for configuring an Oracle Communications SBC, formally known as an Acme Packet Net-Net Session Director ("SBC") in an IMS scenario, as well as Oracle Communications CSM formally known as an Acme Packet Net-Net Core Sessions Manager ("CSM").

In Scope

The following step-by-step guide shows the configuration of Oracle Communications SBC as an IMS function to work with Oracle Communications CSM and Broadworks platform.

Note that Oracle offers several models of SBC. This document covers the setup for the 3820 and 4500 platform series running SCZ 7.2.0 GA or later. If instructions are needed for other Oracle SBC models, please contact your Oracle representative.

Oracle CSM is only offered as a virtualized solution. This document cover the setup running SCZ 7.1.5m1p1 or later.

First step of provisioning of HSS FHoSS (The FOKUS Home Subscriber Server) and Broadworks platform is also shown.

Out of Scope

- Configuration of Network management.

What will you need

- Serial Console cross-over cable with RJ-45 connector.
- Terminal emulation application such as PuTTY or HyperTerm.
- Passwords for the User and Superuser modes on the SBC and CSM.
- IP addresses to be assigned to management interfaces (Wancom0) of both SBC and CSM - the Wancom0 management interface must be connected and configured to a management network separate from the service interfaces. Otherwise the SBC and CSM are subject to ARP overlap issues, loss of system access when the network is down, and compromising DDoS protection. Oracle does not support SBC and/or CSM configurations with management and media/service interfaces on the same subnet.
- IP address of Core Sessions Manager internal and external facing ports (Service interfaces).
- IP address to be used for the SBC internal and external facing ports (Service Interfaces).
- IP address of HSS and Broadworks Platform servers.
- IP address of the next hop gateway in every network.

Configuring the SBC

Once the SBC is racked and the power cable connected, you are ready to set up physical network connectivity.
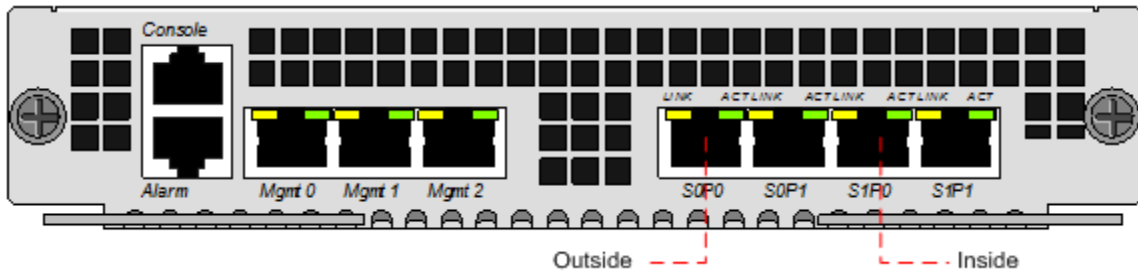
Plug the slot 0 port 0 (s0p0) interface into your outside (subscribers facing) network and the slot 0 port 1 (s1p0) interface into your inside IMS network. Once connected, you are ready to power on and perform the following steps.
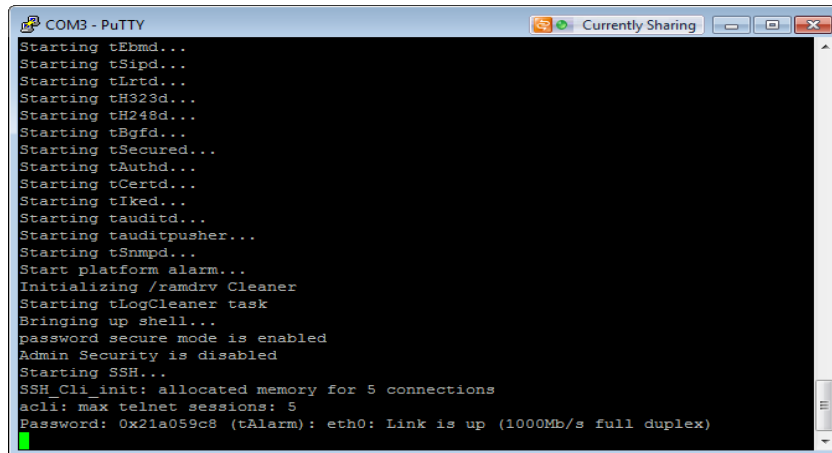
All commands are in bold, such as `configure terminal`; parameters in bold red such as ASBC-IOT are parameters which are specific to an individual deployment. **Note:** The ACLI is case sensitive.

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 front console port (which is active by default) on the SBC and the other end to console adapter that ships with the SBC, connect the console adapter (a DB-9 adapter) to the DB-9 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
ASBC-IOT> enable
Password: packet
ASBC-IOT# configure terminal
ASBC-IOT(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

ASBC-IOT#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

```
ASBC-IOT#(configure)bootparam
'.' = clear field;  '-' = go to previous field;  q = quit
boot device          : eth0
processor number     : 0
host name            : acmesystem
file name            : /boot/nnSCZ720.64.bz --- >location where the
software is loaded on the SBC
inet on ethernet (e)  : 172.18.255.100:ffff0000 --- > This is the ip
address of the management interface of the A-SBC, type the IP address and
mask in hex
inet on backplane (b)  :
host inet (h)          :
gateway inet (g)       : 172.18.0.1 --- > gateway address here
user (u)               : vxftp
ftp password (pw) (blank = use rsh)     : vxftp
flags (f)              :
target name (tn)       : ASBC-IOT
startup script (s)     :
other (o)              :
```

Configure system element values

To configure system element values, use the `system-config` command under the system branch. Then enter values appropriate to your environment, including your default gateway IP address for your management Ethernet interface.

```
ASBC-IOT(configure)# system
ASBC-IOT(system)# system-config
ASBC-IOT(system-config)# hostname ASBC-IOT
ASBC-IOT(system-config)# description "ASBC"
ASBC-IOT(system-config)# location "Bedford, MA"
ASBC-IOT(system-config)# default-gateway 172.18.0.1
ASBC-IOT(system-config)# done
```

Once the **system-config** settings have completed and you enter **done**, the SBC will output a complete listing of all current settings. This will apply throughout the rest of the configuration and is a function of the **done** command. Confirm the output reflects the values you just entered as well as any configuration defaults.

```
system-config
        hostname                            ASBC-IOT
        description                         ASBC
        location                            Bedford, MA
        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                   WARNING
        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
        restart                             enabled
        exceptions
        telnet-timeout                      0
```

```
         console-timeout                        0
         remote-control                         enabled
         cli-audit-trail                        enabled
         link-redundancy-state                  disabled
         source-routing                         disabled
         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
```

Configure Physical Interface values

To configure physical Interface values, use the **phy-interface** command under the system branch. To enter the system branch from system-config, you issue the **exit** command then the **phy-interface** command.

You will first configure the slot 0, port 0 interface designated with the name M00. This will be the port plugged into your outside subscribers-facing interface.

```
ASBC-IOT(system-config)# exit
ASBC-IOT(system)# phy-interface
ASBC-IOT(phy-interface)# name M00
ASBC-IOT(phy-interface)# operation-type media
ASBC-IOT(phy-interface)# slot 0
ASBC-IOT(phy-interface)# port 0
ASBC-IOT(phy-interface)# done
```

Once the **phy-interface** settings have completed for slot 0 port 0 and you enter **done**, the SBC will output a complete listing of all current settings. Confirm the output reflects the values you just entered.

```
phy-interface
      name                      M00
      operation-type            Media
      port                      0
      slot                      0
      virtual-mac
      admin-state               enabled
      auto-negotiation          enabled
      duplex-mode               FULL
      speed                     100
      overload-protection       disabled
```

You will now configure the slot 1 port 0 phy-interface, specifying the appropriate values. This will be the port plugged into your inside CSM-facing IMS interface.

```
ASBC-IOT(phy-interface)# name M10
ASBC-IOT(phy-interface)# operation-type media
ASBC-IOT(phy-interface)# slot 1
ASBC-IOT(phy-interface)# port 0
ASBC-IOT(phy-interface)# done
phy-interface
      name                      M10
      operation-type            Media
      port                      0
      slot                      1
      virtual-mac
      admin-state               enabled
      auto-negotiation          enabled
      duplex-mode               FULL
      speed                     100
      overload-protection       disabled
```

Configure Network Interface values

To configure Network Interface values, use the `network-interface` command under the system branch. To enter the system branch from phy-interface, you issue the `exit` command, then the `network-interface` command.

You will first configure the IP characteristics for the M10 interface defined above

```
ASBC-IOT(phy-interface)# exit
ASBC-IOT(system)# network-interface
ASBC-IOT(network-interface)# name M10
ASBC-IOT(network-interface)# description "CSM-facing interface"
ASBC-IOT(network-interface)# ip-address 10.0.200.150
ASBC-IOT(network-interface)# netmask 255.255.255.0
ASBC-IOT(network-interface)# gateway 10.0.200.1
ASBC-IOT(network-interface)# add-hip-ip 10.0.200.150
ASBC-IOT(network-interface)# add-icmp-ip 10.0.200.150
ASBC-IOT(network-interface)# done

network-interface
        name                        M10
        sub-port-id                 0
        description                 CSM-facing interface
        hostname
        ip-address                  10.0.200.150
        pri-utility-addr
        sec-utility-addr
        netmask                     255.255.255.0
        gateway                     10.0.200.1
        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
        hip-ip-list                 10.0.200.150
        ftp-address
        icmp-address                10.0.200.150
        snmp-address
        telnet-address
        ssh-address
```

You will now configure the slot 0 port 0 sub port 0 network-interface, specifying the appropriate values.

```
ASBC-IOT(network-interface)# name M00
ASBC-IOT(network-interface)# description "Subscribers-facing interface"
ASBC-IOT(network-interface)# ip-address 10.0.210.150
ASBC-IOT(network-interface)# netmask 255.255.255.0
ASBC-IOT(network-interface)# gateway 10.0.210.1
ASBC-IOT(network-interface)# add-hip-ip 10.0.210.150
ASBC-IOT(network-interface)# add-icmp-ip 10.0.210.150
ASBC-IOT(network-interface)# done

network-interface
        name                        M00
        sub-port-id                 0
        description                 Subscribers-facing interface
        hostname
        ip-address                  10.0.210.150
        pri-utility-addr
        sec-utility-addr
        netmask                     255.255.255.0
        gateway                     10.0.210.1
        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
        hip-ip-list                 10.0.210.150
        ftp-address
        icmp-address                10.0.210.150
        snmp-address
        telnet-address
        ssh-address
```

Configure Global SIP configuration

To configure the Global SIP values, use the `sip-config` command under the session-router branch. To enter the session-router branch from network-interface, you issue the `exit` command twice, followed by the `sip-config` command.

```
ASBC-IOT(network-interface)# exit
ASBC-IOT(system)# exit
ASBC-IOT(configure)# session-router
ASBC-IOT(session-router)# sip-config
ASBC-IOT(sip-config)# operation-mode dialog
ASBC-IOT(sip-config)# home-realm-id core
ASBC-IOT(sip-config)# egress-realm-id core
ASBC-IOT(sip-config)# registrar-domain *
ASBC-IOT(sip-config)# registrar-host *
ASBC-IOT(sip-config)# registrar-port 5060
ASBC-IOT(sip-config)# options +max-udp-length=0
ASBC-IOT(sip-config)# done

sip-config
        state                           enabled
        operation-mode                  dialog
        dialog-transparency             enabled
        home-realm-id                   core
        egress-realm-id                 core
        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                             max-udp-length=0
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
```

Configure Global Media configuration

To configure the Media values, use the **media-manager** command under the media-manager branch. To enter the media-manager branch from sip-config, you issue the **exit** command twice, followed by the **media-manager** command twice.

By issuing the **select** then **done** commands at this level, you will be creating the media-manager element, enabling the media management functions in the SBC with the default values.

```
ASBC-IOT(sip-config)# exit
ASBC-IOT(session-router)# exit
ASBC-IOT(configure)# media-manager
ASBC-IOT(media-manager)# media-manager
ASBC-IOT(media-manager)# select
ASBC-IOT(media-manager-config)# done

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
        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                      disabled
        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
```

Configure Realms

To configure the realm values, use the `realm-config` command under the media-manager branch. To enter the media-manager branch from media-manager-config, you issue the `exit` command, followed by the `realm-config` command.

You will create two realms:

- The core, which represents the CSM-facing (inside) IMS network; and

- The access, which represents the Subscribers-facing (outside) network.

```
ASBC-IOT(media-manager-config)# exit
ASBC-IOT(media-manager)# realm-config
ASBC-IOT(realm-config)# identifier core
ASBC-IOT(realm-config)# description "CSM-facing interface"
ASBC-IOT(realm-config)# network-interfaces M10:0
ASBC-IOT(realm-config)# done

realm-config
        identifier                         core
        description                        CSM-facing interface
        addr-prefix                        0.0.0.0
        network-interfaces                 M10:0
```

```
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
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
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
accounting-enable                 enabled
net-management-control            disabled
delay-media-update                disabled
refer-call-transfer               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
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
```

You will now configure the realm for Subscribers-facing side of the SBC, specifying the appropriate values.

```
ASBC-IOT(realm-config)# identifier access
ASBC-IOT(realm-config)# description "Subscribers-facing interface"
ASBC-IOT(realm-config)# network-interfaces M00:0
ASBC-IOT(realm-config)# done

realm-config
        identifier                            access
        description                           Subscribers-facing
interface
        addr-prefix                           0.0.0.0
        network-interfaces                    M00:0
        mm-in-realm                           enabled
        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
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
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
accounting-enable                   enabled
net-management-control              disabled
delay-media-update                  disabled
refer-call-transfer                 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
        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
```

Configure SIP signaling configuration

To configure the SIP signaling values, use the `sip-interface` command under the session-router branch. To enter the session-router branch from realm-config, you issue the `exit` command twice, followed by the `sip-interface` command.

Here you will be configuring the IP addresses and UDP/TCP ports on which the SBC will listen for and transmit SIP messages. These will be the same IP addresses as configured on the associated network-interface elements. Additionaly for strict 3GPP compliance regarding caching and handling of display-names in PAU and PAI headers add option strict-3gpp-pai-compliance. Lastly to instruct the Session Director disregard and strip all route headers for requests received on subscriber facing interface add option strip-route-headers.

```
ASBC-IOT(configure)# session-router
ASBC-IOT(session-router)# sip-interface
ASBC-IOT(sip-interface)# realm access
ASBC-IOT(sip-interface)# description "Subscribers-facing interface"
ASBC-IOT(sip-interface)# sip-ports
ASBC-IOT(sip-port)# address 10.0.210.150
ASBC-IOT(sip-port)# done

sip-port
address                    10.0.210.150
port                       5060
transport-protocol         UDP
tls-profile
allow-anonymous            all
ims-aka-profile

ASBC-IOT(sip-port)# address 10.0.210.150
ASBC-IOT(sip-port)# transport-protocol TCP
ASBC-IOT(sip-port)# done

sip-port
address                    10.0.210.150
port                       5060
transport-protocol         TCP
tls-profile
allow-anonymous            all
ims-aka-profile

ASBC-IOT(sip-port)# exit
ASBC-IOT(sip-interface)# registration-caching enabled
ASBC-IOT(sip-interface)# route-to-registrar enabled
ASBC-IOT(sip-interface)# options +strict-3gpp-pai-compliance
BSFT-IOT(sip-interface)# options +strip-route-headers
BSFT-IOT(sip-interface)# nat-traversal always
BSFT-IOT(sip-interface)# sip-ims-feature enabled
BSFT-IOT(sip-interface)# network-id as.lab

ASBC-IOT(sip-interface)# done

sip-interface
       state                              enabled
```

```
realm-id                            access
description                         Subscribers-facing
interface
sip-port
        address                             10.0.210.150
        port                                5060
        transport-protocol                  UDP
        tls-profile
        allow-anonymous                     all
        multi-home-addrs
        ims-aka-profile
sip-port
        address                             10.0.210.150
        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                       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                             strict-3gpp-pai-compliance
                                    strip-route-headers
trust-mode                          none
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                    enabled
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                         as.lab
ext-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
        reg-cache-route                        disabled
```

You will now configure the CSM-facing SIP interface.

```
ASBC-IOT(configure)# session-router
ASBC-IOT(session-router)# sip-interface
ASBC-IOT(sip-interface)# realm core
ASBC-IOT(sip-interface)# description "CSM-facing interface"
ASBC-IOT(sip-interface)# sip-ports
ASBC-IOT(sip-port)# address 10.0.200.150
ASBC-IOT(sip-port)# done

sip-port
address                     10.0.200.150
port                        5060
transport-protocol          UDP
tls-profile
allow-anonymous             all
ims-aka-profile

ASBC-IOT(sip-port)# exit
ASBC-IOT(sip-interface)# done

sip-interface
        state                                   enabled
        realm-id                                core
```

```
description                          CSM-facing interface
sip-port
        address                              10.0.200.150
        port                                 5060
        transport-protocol                   UDP
        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
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                      enabled
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
default-location-string
term-tgrp-mode                         none
charging-vector-mode                   delete-and-respond
charging-function-address-mode         delete-and-respond
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
        reg-cache-route                          disabled
```

Configure next-hop signaling configuration

To configure the next-hop signaling elements (i.e., Oracle Communications Core Sessions Manager) you define session-agents. Use the **session-agent** command under the session-router branch. To enter the session-router branch from sip-interface, you issue the **exit** command, followed by the **session-agent** command.

Here you will be configuring the IP addresses and UDP ports to which the SBC will send and from which it will expect to receive SIP messages for your next-hop signaling elements.

We configure a session-agent that will represent CSM.

```
ASBC-IOT(sip-interface)# exit
ASBC-IOT(session-router)# hostname 10.0.200.110
ASBC-IOT(session-router)# ip-address 10.0.200.110
ASBC-IOT(session-router)# port 5060
ASBC-IOT(session-router)# realm-id core
ASBC-IOT(session-router)# done

session-agent
        hostname                                10.0.200.110
        ip-address                              10.0.200.110
        port                                    5060
        state                                   enabled
        app-protocol                            SIP
        app-type
        transport-method                        UDP
        realm-id                                core
        egress-realm-id
        description
        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
cac-trap-threshold                         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
ping-interval                              0
ping-send-mode                             keep-alive
ping-all-addresses                         disabled
ping-in-service-response-codes
out-service-response-codes
load-balance-dns-query                     hunt
options
media-profiles
in-translationid
out-translationid
trust-me                                   enabled
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
```

Configure SIP routing

To configure the SIP routing, use the `local-policy` command under the session-router branch. To enter the session-router branch from session-agent, you issue the `exit` command, followed by the `local-policy` command.

We configure the route from the Subscribers to IMS network.

```
ASBC-IOT(session-agent)# exit
ASBC-IOT(session-router)# local-policy
ASBC-IOT(local-policy)# from-address *
ASBC-IOT(local-policy)# to-address *
ASBC-IOT(local-policy)# source-realm access
ASBC-IOT(local-policy)# policy-attributes
ASBC-IOT(local-policy-attributes)#next-hop 10.0.200.110
ASBC-IOT(local-policy-attributes)# realm core
ASBC-IOT(local-policy-attributes)# app-protocol sip
ASBC-IOT(local-policy-attributes)# done

policy-attribute
```

```
            next-hop                      10.0.200.110
            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                  SIP
            methods
            media-profiles
            lookup                        single
            next-key
            eloc-str-lkup                 disabled
            eloc-str-match

ASBC-IOT(local-policy-attributes)# exit
ASBC-IOT(local-policy)# done
```

Configure media handling

To configure the media handling, use the **steering-pool** command under the media-manager branch. To enter the steering-pool branch from local-policy, you issue the **exit** command twice, followed by the **media-manager** then the **steering-pool** command.

You will use the same IP addresses for the steering pool as the one used for the SIP interfaces. Note that the port ranges provide a means of limiting the number of concurrent media sessions within a given realm. For example, assigning 100 ports to a realm would limit it to 50 concurrent bidirectional calls, where two ports are assigned (one per unidirectional media stream).

Configure the media handling for the core realm (CSM-facing side).

```
ASBC-IOT(local-policy)# exit
ASBC-IOT(session-router)# exit
ASBC-IOT(configure)# media-manager
ASBC-IOT(media-manager)# steering-pool
ASBC-IOT(steering-pool)# ip-address 10.0.200.150
ASBC-IOT(steering-pool)# start-port 10000
ASBC-IOT(steering-pool)# end-port 19999
ASBC-IOT(steering-pool)# realm-id core
```

```
ASBC-IOT(steering-pool)# done
steering-pool
        ip-address                    10.0.200.150
        start-port                    10000
        end-port                      19999
        realm-id                      core
        network-interface
```

You will now configure the media handling for the access realm (Subscribers-facing side).

```
ASBC-IOT(steering-pool)# ip-address 10.0.210.150
ASBC-IOT(steering-pool)# start-port 10000
ASBC-IOT(steering-pool)# end-port 19999
ASBC-IOT(steering-pool)# realm-id access
ASBC-IOT(steering-pool)# done
steering-pool
        ip-address                    10.0.210.150
        start-port                    10000
        end-port                      19999
        realm-id                      access
        network-interface
```

Configure sip-manipulations and translation rules

The sip-manipulation element can be found under the session-router element. We now configure the manipulations required on the realm facing the Subscribers (access realm). To enter the sip-manipulation element from steering-pool, you issue the `exit` command twice, followed by the `session-route` then the `sip-manipulation` command.

- First we configure a manipulation called NATting for topology hiding. Then we apply it as an outbound manipulation on the Subscribers-facing SIP interface. Please configure the NATting sip-manipulation as in the output next:

```
sip-manipulation
        name                          NATting
        description
        split-headers
        join-headers
        header-rule
                name                          From
```

```
                header-name                    From
                action                         manipulate
                comparison-type                case-sensitive
                msg-type                       any
                methods
                match-value
                new-value
                element-rule
                        name                           From_header
                        parameter-name
                        type                           uri-host
                        action                         replace
                        match-val-type                 any
                        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                           To
                        parameter-name
                        type                           uri-host
                        action                         replace
                        match-val-type                 any
                        comparison-type                case-sensitive
                        match-value
                        new-value                      $REMOTE_IP

//Once the NATting sip-manipulation is created apply it to access realm as
follows:

ASBC-IOT(session-router)# sip-interface
ASBC-IOT(sip-interface)# select
<realm-id>:
```

```
1: core   10.0.200.150:5060
2: access 10.0.210.150:5060

selection: 2
ASBC-IOT(sip-interface)# out-manipulationid NATting
ASBC-IOT(sip-interface)# done

sip-interface
        state                               enabled
        realm-id                            access
        description                         Subscribers-facing
interface
        sip-port
                address                             10.0.210.150
                port                                5060
                transport-protocol          UDP
                tls-profile
                allow-anonymous             all
                multi-home-addrs
                ims-aka-profile
        sip-port
                address                             10.0.210.150
                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                       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                          strict-3gpp-pai-compliance
                                 strip-route-headers
trust-mode                       none
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               NATting
sip-ims-feature                  enabled
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                       as.lab
ext-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
        reg-cache-route                           disabled
```

Verify configuration integrity

You will verify your configuration referential integrity before saving and activating it with the verify-**config** command. This command is available from Superuser Mode. To enter the Superuser Mode from sip-manipulation, you issue the **exit** command three times.

```
ASBC-IOT(sip-interface)# exit
ASBC-IOT(session-router)# exit
ASBC-IOT(configure)# exit
ASBC-IOT# verify-config
--------------------------------------------------------------------

Verification successful! No errors nor warnings in the configuration
```

Save and activate your configuration

You will now save your configuration with the `save-config` command. This will make it persistent through reboots, but it will not take effect until after you issue the `activate-config` command. Before issuing commands `activate-config` make sure verify-config output is successful.

```
ASBC-IOT# save-config
checking configuration
Save-Config received, processing.
waiting 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'.

ASBC-IOT# activate-config
Activate-Config received, processing.
waiting for request to finish
Setting phy0 on Slot=0, Port=0, MAC=00:08:25:03:FC:43,
VMAC=00:08:25:03:FC:43
Setting phy1 on Slot=1, Port=0, MAC=00:08:25:03:FC:45,
VMAC=00:08:25:03:FC:45
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete

ASBC-IOT# reboot
```

SBC configuration is now complete. Reboot the system issuing `reboot` command.

Configuring the CSM

Configure the virtual slot 0 port 1 (s1p0) interface into your inside IMS network, facing BSFT as well as SBC. Once connected, 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 CSM-IOT are parameters which are specific to an individual deployment. **Note:** The ACLI is case sensitive.

Establish the serial connection and logging in the CSM

Console access is available through the GUI/tool your hypervisor has available. Power on the CSM and confirm that you see the following output from the bootup sequence.

```
Starting tEbmd...
Starting tSipd...
Starting tLrtd...
Starting tH323d...
Starting tH248d...
Starting tBgfd...
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tIked...
Starting tauditd...
Starting tauditpusher...
Starting tSnmpd...
Start platform alarm...
Initializing /ramdrv Cleaner
Starting tLogCleaner task
Bringing up shell...
password secure mode is enabled
Admin Security is disabled
Starting SSH...
SSH_Cli_init: allocated memory for 5 connections
acli: max telnet sessions: 5
Password: 0x21a059c8 (tAlarm): eth0: Link is up (1000Mb/s full duplex)
```

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

```
Password: acme
CSM-IOT> enable
Password: packet
CSM-IOT# configure terminal
CSM-IOT(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 CSM by going to

CSM-IOT#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

```
CSM-IOT (configure)# bootparam

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

Boot File              : /boot/nnSCZ715.64.bz --- >location where the
software is loaded on the SBC
IP Address             : 172.18.255.53 --- > This is the ip address of
the management interface of the A-SBC
VLAN                   :
Netmask                : 255.255.0.0 – This is the mask of the management
interface of the A-SBC
Gateway                : 172.18.0.1 --- > gateway address here
Host IP                :
FTP username           :
FTP password           :
Flags                  :
Target Name            : CSM-IOT
Console Device         : VGA
Console Baudrate       : 115200
Other                  :
```

Configure system element values

To configure system element values, use the `system-config` command under the system branch. Then enter values appropriate to your environment, including your default gateway IP address for your management Ethernet interface.

```
CSM-IOT(configure)# system
CSM-IOT(system)# system-config
CSM-IOT(system-config)# hostname CSM-IOT
CSM-IOT(system-config)# description "CSM"
CSM-IOT(system-config)# location "Bedford, MA"
```

```
CSM-IOT(system-config)# default-gateway 172.18.0.1
CSM-IOT(system-config)# done
```

Once the **system-config** settings have completed and you enter `done`, the CSM will output a complete listing of all current settings. This will apply throughout the rest of the configuration and is a function of the `done` command. Confirm the output reflects the values you just entered as well as any configuration defaults.

```
system-config
        hostname                          CSM-IOT
        description                       CSM
        location                          Bedford, MA
        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
      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
      service-cluster-id
```

Configure Physical Interface values

To configure physical Interface values, use the `phy-interface` command under the system branch. To enter the system branch from system-config, you issue the `exit` command then the `phy-interface` command.

You will now configure the slot 1 port 0 phy-interface, specifying the appropriate values. This will be the port plugged into your inside IMS network (BSFT-facing interface as well as ASBC-facing interface).

```
CSM-IOT(system-config)# exit
CSM-IOT(system)# phy-interface
CSM-IOT(phy-interface)# name M10
CSM-IOT(phy-interface)# operation-type media
CSM-IOT(phy-interface)# slot 1
```

```
CSM-IOT(phy-interface)# port 0
CSM-IOT(phy-interface)# done
```

Once the **phy-interface** settings have completed for slot 1 port 0 and you enter **done**, the CSM will output a complete listing of all current settings. Confirm the output reflects the values you just entered.

```
CSM-IOT(phy-interface)# name M10
CSM-IOT(phy-interface)# operation-type media
CSM-IOT(phy-interface)# slot 1
CSM-IOT(phy-interface)# port 0
CSM-IOT(phy-interface)# done
phy-interface
        name                            M10
        operation-type                  Media
        port                            0
        slot                            1
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        wancom-health-score             50
        overload-protection             disabled
```

Configure Network Interface values

To configure Network Interface values, use the **network-interface** command under the system branch. To enter the system branch from phy-interface, you issue the **exit** command, then the **network-interface** command.

You will first configure the IP characteristics for the M10 interface defined above

```
CSM-IOT(phy-interface)# exit
CSM-IOT(system)# network-interface
CSM-IOT(network-interface)# name M10
CSM-IOT(network-interface)# ip-address 10.0.200.100
CSM-IOT(network-interface)# netmask 255.255.255.0
CSM-IOT(network-interface)# gateway 10.0.200.1
CSM-IOT(network-interface)# add-hip-ip 10.0.200.100
```

```
CSM-IOT(network-interface)# add-icmp-ip 10.0.200.100
CSM-IOT(network-interface)# done

network-interface
        name                            M10
        sub-port-id                     0
        description
        hostname
        ip-address                      10.0.200.100
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.0
        gateway                         10.0.200.1
        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                     10.0.200.100
        ftp-address
        icmp-address                    10.0.200.100
        snmp-address
        telnet-address
        ssh-address
```

Configure Global SIP configuration

To configure the Global SIP values, use the `sip-config` command under the session-router branch. To enter the session-router branch from network-interface, you issue the `exit` command twice, followed by the `sip-config` command.

```
CSM-IOT(network-interface)# exit
CSM-IOT(system)# exit
```

```
CSM-IOT(configure)# session-router
CSM-IOT(session-router)# sip-config
CSM-IOT(sip-config)# operation-mode dialog
CSM-IOT(sip-config)# home-realm-id coreAS
CSM-IOT(sip-config)# egress-realm-id coreAS
CSM-IOT(sip-config)# registrar-domain *
CSM-IOT(sip-config)# registrar-host *
CSM-IOT(sip-config)# registrar-port 5060
CSM-IOT(sip-config)# options +max-udp-length=0
CSM-IOT(sip-config)# options +force-unregistration

CSM-IOT(sip-config)# done

sip-config
        state                           enabled
        operation-mode                  dialog
        dialog-transparency             enabled
        home-realm-id                   coreAS
        egress-realm-id                 coreAS
        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                          force-unregistration
                                 max-udp-length=0
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
```

Configure Realms

To configure the realm values, use the **`realm-config`** command under the media-manager branch. To enter the media-manager branch from media-manager-config, you issue the **`exit`** command, followed by the **`realm-config`** command.

You will create two realms:

- The core, called coreAS which represents the BSFT-facing side; and

- The access, called accessAS which represents the ASBC-facing side.

```
CSM-IOT(media-manager-config)# exit
CSM-IOT(media-manager)# realm-config
CSM-IOT(realm-config)# identifier coreAS
CSM-IOT(realm-config)# description "BSFT-facing interface"
CSM-IOT(realm-config)# network-interfaces M10:0
CSM-IOT(realm-config)# done


realm-config
        identifier                      coreAS
        description                     BSFT-facing interface
        addr-prefix                     0.0.0.0
        network-interfaces              M10:0
        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
        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
        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
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
accounting-enable                       enabled
net-management-control                  disabled
delay-media-update                      disabled
refer-call-transfer                     disabled
refer-notify-provisional                none
dyn-refer-term                          disabled
codec-policy
codec-manip-in-realm                    disabled
codec-manip-in-network                  disabled
constraint-name
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
```

You will now configure the realm for ASBC-facing side of the CSM, specifying the appropriate values.

```
CSM-IOT(realm-config)# identifier accessAS
CSM-IOT(realm-config)# description "ASBC-facing interface"
CSM-IOT(realm-config)# network-interfaces M10:0
CSM-IOT(realm-config)# done

realm-config
        identifier                              accessAS
        description                             ASBC-facing interface
        addr-prefix                             0.0.0.0
        network-interfaces                      M10:0
        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
        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
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
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
accounting-enable                   enabled
net-management-control              disabled
delay-media-update                  disabled
refer-call-transfer                 disabled
refer-notify-provisional            none
dyn-refer-term                      disabled
codec-policy
codec-manip-in-realm                disabled
codec-manip-in-network              disabled
constraint-name
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
```

Configure SIP signaling configuration

To configure the SIP signaling values, use the `sip-interface` command under the session-router branch. To enter the session-router branch from realm-config, you issue the `exit` command twice, followed by the `sip-interface` command.

Here you will be configuring the IP addresses and UDP ports on which the CSM will listen for and transmit SIP messages. These will be the same IP addresses as configured on the associated network-interface elements.

```
CSM-IOT(configure)# session-router
CSM-IOT(session-router)# sip-interface
CSM-IOT(sip-interface)# realm accessAS
CSM-IOT(sip-interface)# description "ASBC-facing interface"
CSM-IOT(sip-interface)# sip-ports
CSM-IOT(sip-port)# address 10.0.200.110
CSM-IOT(sip-port)# done

sip-port
address                         10.0.200.110
port                            5060
transport-protocol              UDP
tls-profile
allow-anonymous                 all
ims-aka-profile

CSM-IOT(sip-port)# exit
CSM-IOT(sip-interface)# registration-caching enabled
CSM-IOT(sip-interface)# route-to-registrar enabled
CSM-IOT(sip-interface)# sip-authentication-profile AuthSIPASMode
CSM-IOT(sip-interface)# done

sip-interface
        state                           enabled
        realm-id                        accessAS
        description                     ASBC-facing interface
        sip-port
                address                         10.0.200.110
                port                            5060
                transport-protocol              UDP
                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                   enabled
min-reg-expire                         300
registration-interval                  3600
route-to-registrar                     enabled
secured-network                        disabled
teluri-scheme                          disabled
uri-fqdn-domain
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
ims-access                             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
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
        ims-aka-feature                     disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                       none
        add-sdp-invite                      disabled
        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
        unregister-on-connection-loss       disabled
        sip-authentication-profile          AuthSIPASMode
        ping-response                       disabled
        session-recording-server
        session-recording-required          disabled
```

You will now configure the BSFT-facing SIP interface.

```
CSM-IOT(configure)# session-router
CSM-IOT(session-router)# sip-interface
CSM-IOT(sip-interface)# realm coreAS
CSM-IOT(sip-interface)# description "BSFT-facing interface"
CSM-IOT(sip-interface)# sip-ports
```

```
CSM-IOT(sip-port)# address 10.0.200.100
CSM-IOT(sip-port)# done

sip-port
address                      10.0.200.100
port                         5060
transport-protocol           UDP
tls-profile
allow-anonymous              all
ims-aka-profile

CSM-IOT(sip-port)# exit
CSM-IOT(sip-interface)# done

sip-interface
        state                           enabled
        realm-id                        coreAS
        description                     BSFT-facing interface
        sip-port
                address                         10.0.200.100
                port                            5060
                transport-protocol              UDP
                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
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
ims-access                          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
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
ims-aka-feature                     disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive                       none
```

```
        add-sdp-invite                          disabled
        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
        unregister-on-connection-loss           disabled
        sip-authentication-profile
        ping-response                           disabled
        session-recording-server
        session-recording-required              disabled
```

Configure next-hop signaling configuration

To configure the next-hop signaling elements (i.e., Oracle Communications SBC, Broadworks Network Server, PSTN-GW) you define session-agents. Use the `session-agent` command under the session-router branch. To enter the session-router branch from sip-interface, you issue the `exit` command, followed by the `session-agent` command.

Here you will be configuring the IP addresses and UDP ports to which the CSM will send and from which it will expect to receive SIP messages for your next-hop signaling elements.

We configure a session-agent that will represent SBC.

```
CSM-IOT(sip-interface)# exit
CSM-IOT(session-router)# hostname 10.0.200.150
CSM-IOT(session-router)# ip-address 10.0.200.150
CSM-IOT(session-router)# port 5060
CSM-IOT(session-router)# realm-id accessAS
CSM-IOT(session-router)# done

session-agent
        hostname                                10.0.200.150
        ip-address                              10.0.200.150
```

```
port                              5060
state                             enabled
app-protocol                      SIP
app-type
transport-method                  UDP
realm-id                          accessAS
egress-realm-id
description
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
cac-trap-threshold                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
ping-interval                     0
ping-send-mode                    keep-alive
ping-all-addresses                disabled
ping-in-service-response-codes
out-service-response-codes
load-balance-dns-query            hunt
```

```
options
media-profiles
in-translationid
out-translationid
trust-me                              enabled
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
```

We configure a session-agent that will represent Broadworks Network Server.

```
CSM-IOT(sip-interface)# exit
CSM-IOT(session-router)# hostname ns-sig.pe.lab
CSM-IOT(session-router)# ip-address 10.0.200.11
CSM-IOT(session-router)# port 5060
CSM-IOT(session-router)# realm-id coreAS
CSM-IOT(session-router)# done

session-agent
        hostname                        ns-sig.pe.lab
        ip-address                      10.0.200.11
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        coreAS
        egress-realm-id
        description
        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
ping-interval                         0
ping-send-mode                        keep-alive
ping-all-addresses                    disabled
ping-in-service-response-codes
out-service-response-codes
load-balance-dns-query                hunt
options
media-profiles
in-translationid
out-translationid
trust-me                              enabled
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
```

We configure a session-agent that will represent Broadworks Application Server.

```
CSM-IOT(sip-interface)# exit
CSM-IOT(session-router)# hostname 10.0.200.10
CSM-IOT(session-router)# ip-address 10.0.200.10
CSM-IOT(session-router)# port 5060
CSM-IOT(session-router)# realm-id coreAS
CSM-IOT(session-router)# done

session-agent
        hostname                                10.0.200.10
        ip-address                              10.0.200.10
        port                                    5060
        state                                   enabled
        app-protocol                            SIP
        app-type
        transport-method                        UDP
        realm-id                                coreAS
        egress-realm-id
        description
        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
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
media-profiles
in-translationid
out-translationid
trust-me                          enabled
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
```

We configure a session-agent that will represent PSTN-GW.

```
CSM-IOT(sip-interface)# exit
CSM-IOT(session-router)# hostname 10.0.200.98
CSM-IOT(session-router)# ip-address 10.0.200.98
CSM-IOT(session-router)# port 5060
CSM-IOT(session-router)# realm-id coreAS
CSM-IOT(session-router)# done

session-agent
        hostname                           10.0.200.98
        ip-address                         10.0.200.98
        port                               5060
        state                              enabled
        app-protocol                       SIP
        app-type
        transport-method                   UDP
        realm-id                           coreAS
        egress-realm-id
        description
        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
ping-interval                            0
ping-send-mode                           keep-alive
ping-all-addresses                       disabled
ping-in-service-response-codes
out-service-response-codes
load-balance-dns-query                   hunt
options
media-profiles
in-translationid
out-translationid
trust-me                                 enabled
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
```

Configure SIP routing

To configure the SIP routing, use the `local-policy` command under the session-router branch. To enter the session-router branch from session-agent, you issue the `exit` command, followed by the `local-policy` command.

We configure the route from the Subscribers to PSTN network.

```
CSM-IOT(session-agent)# exit
CSM-IOT(session-router)# local-policy
CSM-IOT(local-policy)# from-address *
CSM-IOT(local-policy)# to-address *
CSM-IOT(local-policy)# source-realm coreAS
CSM-IOT(local-policy)# policy-attributes
CSM-IOT(local-policy-attributes)#next-hop 10.0.200.98
CSM-IOT(local-policy-attributes)# realm coreAS
CSM-IOT(local-policy-attributes)# app-protocol sip
CSM-IOT(local-policy-attributes)# done
```

```
policy-attribute
            next-hop                    10.0.200.97
            realm                       coreAS
            action                      none
            terminate-recursion         disabled
            carrier
            start-time                  0000
            end-time                    2400
            days-of-week                U-S
            cost                        0
            app-protocol                SIP
            state                       enabled
            methods
            media-profiles
            lookup                      single
            next-key
            eloc-str-lkup               disabled
            eloc-str-match

CSM-IOT(local-policy-attributes)# exit
CSM-IOT(local-policy)# done
```

Configure SIP Authentication

To configure the SIP authentication, use the `sip-authentication-profile` command under the session-router branch. To enter the session-router branch from session-agent, you issue the `exit` command, followed by the `sip-authentication-profile` command.

We configure CSM to challenge SIP REGISTER methods and Diameter reference point towards HSS to retrieve the SIP Authentications vectors.

```
CSM-IOT(session-router)# sip-authentication-profile
CSM-IOT(sip-authentication-profile)# name AuthSIPASMode
CSM-IOT(sip-authentication-profile)# methods (REGISTER)
CSM-IOT(sip-authentication-profile)# credential-retrieval-method cx
CSM-IOT(sip-authentication-profile)# credential-retrieval-config
FHoSSASMode
CSM-IOT(sip-authentication-profile)# done

sip-authentication-profile
```

```
name                            AuthSIPASMode
methods                         REGISTER
anonymous-methods
digest-realm
credential-retrieval-method     cx
credential-retrieval-config     FHoSSASMode
```

Configure SIP registrar

To configure the SIP registrar, use the `sip-registrar` command under the session-router branch. To enter the session-router branch from sip-authentication-profile, you issue the `exit` command, followed by the `sip-registrar` command.

We configure CSM to handle/own a particular domain, Diameter reference point and HSS associated to that domain, realm to be used for Cx traffic, as well as the CSM SIP URI to register in Cx SAR/MAR messages as Server-Name AVP. It is worth to mention that not all objects referenced here have been created yet, but they will be in next sections for a complete and successful CSM configuration.

```
CSM-IOT(session-router)# sip-authentication-profile
CSM-IOT(sip-registrar)# name as.lab
CSM-IOT(sip-registrar)# domains (as.lab)
CSM-IOT(sip-registrar)# subscriber-database-method cx
CSM-IOT(sip-registrar)# subscriber-database-config FHoSSASMode
CSM-IOT(sip-registrar)# authentication-profile AuthSIPASMode
CSM-IOT(sip-registrar)# home-server-route sip:10.0.200.100:5060
CSM-IOT(sip-registrar)# egress-realm-id coreAS
CSM-IOT(sip-registrar)# ifc-profile ASMode
CSM-IOT(sip-registrar)# done

sip-registrar
        name                            as.lab
        state                           enabled
        domains                         as.lab
        subscriber-database-method      CX
        subscriber-database-config      FHoSSASMode
        authentication-profile          AuthSIPASMode
        home-server-route               sip:10.0.200.100:5060
        third-party-registrars
        routing-precedence              REGISTRAR
        options
        egress-realm-id                 coreAS
```

```
      location-update-interval          1440
      ifc-profile                       ASMode
      max-contacts-per-aor              0
      regevent-notification-profile
      ims-core
      lb-list
```

Configure Home Subscriber Server

To configure the HSS server use the `home-subscriber-server` command under the session-router branch. To enter the session-router branch from sip-registrar, you issue the `exit` command, followed by the `home-subscriber-server` command.

We configure the HSS referenced in CSM sip-registrar object previously, the realm CSM should use to reach it, as well as some specific Cx AVP values.

```
CSM-IOT(session-router)# home-subscriber-server
CSM-IOT(home-subscriber-server)# name FHoSSASMode
CSM-IOT(home-subscriber-server)# address 10.0.200.18
CSM-IOT(home-subscriber-server)# realm coreAS
CSM-IOT(home-subscriber-server)# origin-realm as.pe.lab
CSM-IOT(home-subscriber-server)# origin-host-identifier CSM01
CSM-IOT(home-subscriber-server)# done

home-subscriber-server
      name                              FHoSSASMode
      state                             enabled
      transport-protocol                TCP
      address                           10.0.200.18
      port                              3868
      realm                             coreAS
      multi-home-addrs
      origin-realm                      as.pe.lab
      origin-host-identifier            CSM01
      watchdog-ka-timer                 0
      destination-host-identifier
      num-auth-vectors                  3
```

Configure ifc-profile

To enable the store and processing of Initial Filter Criteria, use the `ifc-profile` command under the session-router branch. To enter the session-router branch from home-subscriber-server, you issue the `exit` command, followed by the `ifc-profile` command.

```
CSM-IOT(session-router)# ifc-profile
CSM-IOT(ifc-profile)# name ASMode
CSM-IOT(ifc-profile)# options +add-sescase-to-route
CSM-IOT(ifc-profile)# done

ifc-profile
        name                            ASMode
        state                           enabled
        default-ifc-filename
        shared-ifc-filename
        options                         add-sescase-to-route
```

Verify configuration integrity

You will verify your configuration referential integrity before saving and activating it with the `verify-config` command. This command is available from Superuser Mode. To enter the Superuser Mode from session-agent, you issue the `exit` command three times.

```
CSM-IOT(ifc-profile)# exit
CSM-IOT(session-router)# exit
CSM-IOT(configure)# exit
CSM-IOT# verify-config
---------------------------------------------------------------------

Verification successful! No errors nor warnings in the configuration
```

Save and activate your configuration

You will now save your configuration with the `save-config` command. This will make it persistent through reboots, but it will not take effect until after you issue the `activate-config` command. Before issuing commands `activate-config` make sure verify-config output is successful.

```
CSM-IOT# save-config
checking configuration
Save-Config received, processing.
waiting 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'.

CSM-IOT# activate-config
Activate-Config received, processing.
waiting for request to finish
Setting phy0 on Slot=0, Port=0, MAC=00:08:25:03:FC:43,
VMAC=00:08:25:03:FC:43
Setting phy1 on Slot=1, Port=0, MAC=00:08:25:03:FC:45,
VMAC=00:08:25:03:FC:45
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
```

CSM configuration is now complete. Reboot the system issuing `reboot` command.

Provisioning the Home Subscriber Server FHoSS

Connect the network interface of the HSS server into your inside IMS network so that CSM can reach it. Once connected, you are ready to power on and perform the following steps.

Edit following file /opt/OpenIMSCore/FHoSS/deploy/hss.properties and set the IP address and port where the web application should start listening:

```
host=172.18.255.18
port=8080
```

Then edit next file /opt/OpenIMSCore/FHoSS/deploy/DiameterPeerHSS.xml and specify the Diameter reference point parameters such as Diameter realm, S-CSCF IP address and port.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- HSS Server config -->
<DiameterPeer
        FQDN="FHoSS.pe.lab"
        Realm="pe.lab"
        Vendor_Id="10415"
        Product_Name="JavaDiameterPeer"
        AcceptUnknownPeers="1"
        DropUnknownOnDisconnect="0"
        Tc="30"
        Workers="4"
        QueueLength="32"
>
        <Acceptor port="3868" bind="10.0.200.18" />

        <Auth id="16777216" vendor="10415"/><!-- 3GPP Cx -->
        <Auth id="16777216" vendor="4491"/><!-- CableLabs Cx -->
        <Auth id="16777216" vendor="13019"/><!-- ETSI/TISPAN Cx -->
```

```
        <Auth id="16777216" vendor="0"/><!-- ETSI/TISPAN Cx -->

        <Auth id="16777217" vendor="10415"/><!-- 3GPP Sh -->

        <Auth id="16777221" vendor="10415"/>
```
```
</DiameterPeer>
```

Login into the Web interface by the IP address and port specified previously. Next the provision of a user is shown through several screenshots:

User Identities. IMS Subscription:

User Identities. Private User Identity:

FHoSS - The FOKUS Home Subscriber Server (Rel. 7)

User Identities

- **IMS Subscription**
  Search
  Create

- **Private Identity**
  Search
  Create

- **Public User Identity**
  Search
  Create

Private User Identity -IMPI-

ID	5
Identity*	6175551001@as.lab
Secret Key*	6175551001

Authentication Schemes*	
Digest-AKAv1 (3GPP)	☐
Digest-AKAv2 (3GPP)	☐
Digest-MD5 (FOKUS)	☐
Digest (CableLabs)	☐
SIP Digest (3GPP)	☐
HTTP Digest (ETSI)	☐
Early-IMS (3GPP)	☐
NASS Bundled (ETSI)	☐
All	☑
Default	Digest-AKAv1-MD5 ▼

AMF*	0000
OP*	00000000000000000000000000000000
SQN*	000000000507

Early IMS IP	
DSL Line Identifier	
GUSS	**Configure**

Mandatory fields were marked with "*".
The Secret Key in this form is considered in hex representation if its value is 16 bytes long or else in ASCII representation.

[Save] [Refresh] [Delete]

Associate an IMSU

IMSU Identity		Add/Change

Associated IMSU

ID	IMSU Identity	Delete
3	6175551001	☐

Create & Bind new IMPU ✚

Associate IMPU(s)

IMPU Identity		Add

Warning: The current IMPI will be associated with all the corresponding IMPUs (within the same implicit-set)!

List of associated IMPUs

ID:	IMPU Identity:	Delete:
3	sip:6175551001@as.lab	☐
25	tel:+16175551001	☐

Push Cx Operation

Apply for	User-Data ▼
Execute	PPR

RTR Operation

Apply for	IMPU(s) of crt IMPI ▼
Select Identities	
Reason	Select Reason... ▼
Reason Info	
Execute	RTR-All RTR-Selected

User identities. Public User Identity:

FHoSS - The FOKUS Home Subscriber Server (Rel. 7)

HOME   USER IDENTITIES   SERVICES   NETWORK CONFIGURATION   STATISTICS

User Identities

- **IMS Subscription**
  Search
  Create

- **Private Identity**
  Search
  Create

- **Public User Identity**
  Search
  Create

Public User Identity -IMPU-

ID	3
Identity*	sip:6175551001@as.lab
Barring	☐
Service Profile*	ASMode ▼
Implicit Set	3
Charging-Info Set	default_charging_set ▼
Can Register	☑
IMPU Type*	Public_User_Identity ▼
Wildcard PSI	
PSI Activation	☐
Display Name	
User-Status	NOT-REGISTERED

Mandatory fields were marked with "*"

[Save] [Refresh] [Delete]

Add IMPU(s) to Implicit-Set

IMPU Identity		[Add]

List IMPUs from Implicit-Set

ID	IMPU Identity	Delete
3	sip:6175551001@as.lab	
25	tel:+16175551001	☐

Add Visited-Networks

Select Visited-Network... ▼	[Add]

List of Visited Networks

ID	Identity	Delete
2	as.lab	☐

Associate IMPI(s) to IMPU

IMPI Identity		[Add]

Warning: This IMPI will be associated with all the corresponding IMPUs (within the same implicit-set)!

List of associated IMPIs

ID	IMPI Identity	Delete
5	6175551001@as.lab	☐

Push Cx Operation

Apply for	User-Data ▼
Execute	[PPR]

Services. Service Profiles:

Services. Application Servers:

FHoSS - The FOKUS Home Subscriber Server (Rel. 7)

HOME USER IDENTITIES SERVICES NETWORK CONFIGURATION STATISTICS

Services

- **Service Profiles**
  Search
  Create

- **Application Servers**
  Search
  Create

- **Trigger Points**
  Search
  Create

- **Initial Filter Criteria**
  Search
  Create

- **Shared iFC Sets**
  Search
  Create

- **DSAI**
  Search
  Create

Application Server -AS-

ID	2
Name*	NS
Server Name*	sip:ns-sig.pe.lab:5060
Diameter FQDN*	ns-sig.pe.lab
Default Handling*	Session - Continued ▾
Service Info	
Rep-Data Limit	1024

Sh Interface - Permissions

Permission for	UDR	PUR	SNR
Allowed Request	☑	☑	☑
Repository-Data	☐	☐	☐
IMPU	☐		☐
IMS User State	☐		☐
S-CSCF Name	☐		☐
iFC	☐		☐
Location	☐		
User-State	☐		
Charging-Info	☐		
MS-ISDN	☐		
PSI Activation	☐	☐	☐
DSAI	☐	☐	☐
Aliases Rep Data	☐	☐	☐

Mandatory fields were marked with "*"

Save Refresh Delete

Services. Trigger Point:

FHoSS - The FOKUS Home Subscriber Server (Rel. 7)

HOME   USER IDENTITIES   SERVICES   NETWORK CONFIGURATION   STATISTICS

Services

- **Service Profiles**
  Search
  Create

- **Application Servers**
  Search
  Create

- **Trigger Points**
  Search
  Create

- **Initial Filter Criteria**
  Search
  Create

- **Shared iFC Sets**
  Search
  Create

- **DSAI**
  Search
  Create

Trigger Point -TP-

ID	2
Name*	ASMode
Condition Type CNF*	Disjunctive Normal Form ▼

Mandatory fields were marked with "*"

[Save] [Refresh] [Delete]

Attach IFC

| Select IFC... ▼ | [Attach] |

List of attached IFCs

ID	IFC Name	Detach
2	ASMode	☐

Add SPTs to Trigger Point

Not	☐	SIP Method	INVITE ▼		[Delete]
			AND		
Not	☐	Session Case	Origin - Session ▼		[Delete]
			AND		
			Request-URI ▼ ✚		
			OR		
Not	☐	SIP Method	REGISTER ▼	Reg ☐ ReReg ☐ DeReg ☐	[Delete]
			AND		
			Request-URI ▼ ✚		
			OR		
Not	☐	SIP Method	INVITE ▼		[Delete]
			AND		
Not	☐	Session Case	Term - Reg ▼		[Delete]
			AND		
			Request-URI ▼ ✚		
			OR		
Not	☐	Session Case	Term - UnReg ▼		[Delete]
			AND		
Not	☐	SIP Method	INVITE ▼		[Delete]
			AND		
			Request-URI ▼ ✚		
			OR		
			Request-URI ▼ ✚		

Services. Initial Filter Criteria:

Provisioning of one user in FOKUS HSS is now completed.

Provisioning the Broadworks Application Server

Connect the Broadwork Platforms interfaces into your inside IMS network so that CSM can reach it. Once connected, you are ready to login into the Broadworks Application Server web interface by the corresponding IP address and port. Next the provision of a user is shown through several screenshots:

Create a new enterprise. Click on Enterprises and then Add button.

Once the enterprise is created, create a Group inside the enterprise clicking on Groups and then Add button.

BROADSOFT
Innovation calling.

Help - Home

Welcome Default Administrator [Logout]

Options:
- ▶ Profile
- Resources
- Services
- Call Center
- Communication Barring
- Meet-Me Conferencing
- Utilities

Profile

Basic

Groups
Add, modify, or remove groups.

Users
Display all users in the enterprise.

Service Instances
Display all service instances in the enterprise.

Profile
Display or modify profile information.

Administrators
Add, modify, or remove administrators.

Departments
Add, modify, or remove departments.

Schedules
Add, modify, or remove schedules.

Advanced

Call Processing Policies
Configure service provider/enterprise level Call Processing Policies

Dial Plan Policy
Configure service provider/enterprise level Dial Plan Policy

Routing Profile
View or modify the routing profile for the service provider/enterprise.

Voice VPN
Manage the enterprise virtual private network.

Virtual On-Net Enterprise Extensions
Manage Virtual On-Net Users.

Dialable Caller ID
Automatically prepend digits to the incoming caller ID of public calls so the caller ID is presented in dialable format.

Once the group is created, create a User inside the group clicking on Users and then Add button.

BROADSOFT
Innovation calling.

Help - Home

Welcome Default Administrator [Logout]

Options:
- ▶ Profile
- Resources
- Services
- Call Center
- Calling Plan
- Communication Barring
- Meet-Me Conferencing
- Utilities

Profile

Basic

Users
Add, modify, or remove users.

Profile
View or modify your group profile information.

Administrators
Add, modify, or remove group administrators and department administrators.

Departments
Add, modify, or remove departments in your group.

Schedules
Add, modify, or remove schedules.

Advanced

Call Processing Policies
Configure group-level Call Processing Policies

Communication Barring Auth Codes
Configure group-level Communication Barring Authorization codes.

Dial Plan Policy
Configure group-level Dial Plan Policy

Group Web Policies
Configure group-level web policies.

Routing Profile
View or modify the routing profile for the group.

Virtual On-Net Enterprise Extensions
Create and manage Virtual On-Net Users.

Dialable Caller ID
Automatically prepend digits to the incoming caller ID of public calls so the caller ID is presented in dialable format.

Welcome Default Administrator [Logout]

System >ASModeEnterprise1 >ASModeGrp1 >Users : asmodeuser1

Profile

Profile allows you to view and maintain your profile information. The information filled in specifies your primary phone number, extension, and device that are used for handling calls. Filling in the additional information section allows your mobile phone, pager, and other information to be visible to other group members in the group phone list. Some of this information can only be modified by your administrator.

| OK | Apply | Delete | Cancel |

Enterprise ID: ASModeEnterprise1   Group: ASModeGrp1
User ID: asmodeuser1   Change User ID (Also saves current screen data)
* Last Name: ASModeE1G1   * First Name: ASModeE1G1
* Calling Line ID Last Name: ASModeE1G1   * Calling Line ID First Name: ASModeE1G1
Department: None ▼   Language: English ▼
Time Zone: (GMT-05:00) (US) Eastern Time ▼   Network Class of Service: None ▼

Additional Information
Title:
Pager: Mobile:
E-mail: YahooID:
Location:
Address:

City: State/Province: -- Select -- ▼
Zip/Postal Code: Country:

| OK | Apply | Delete | Cancel |

Once the user is created assing it a phone number clicking on Addresses.

Help - Home

Welcome Default Administrator [Logout]

System >ASModeEnterprise1 >ASModeGrp1 >Users : asmodeuser1

Profile

Basic   **Advanced**

Profile   **Assign Services**
Display and configure profile information such as your name, department and address.   Assign or unassign services and service packs.

Addresses   **Call Application Policies**
Addresses allows you to view and maintain your phone numbers and other identities that are used to make and receive calls.   Select Call Control Applications enabled for a user.

                                                             Call Policies
Passwords   Configure user Call Policies
Set web access and portal passwords.
                                                             Call Processing Policies
Schedules   Configure user-level Call Processing Policies
Add, modify, or remove schedules.
                                                             Communication Barring Auth Codes
                                                             Configure Communication Barring Authorization codes for a user.

                                                             Device Policies
                                                             Configure user Device Policies.

BROADSOFT
Innovation calling.

Welcome Default Administrator [Logout]

Options:
- ▶ Profile
  - Incoming Calls
  - Outgoing Calls
  - Call Control
  - Calling Plans
  - Client Applications
  - Messaging
  - Utilities

Addresses

Addresses allows you to view and maintain your phone number and other identities that are used to make and receive calls.

| OK | Apply | Cancel |

Phone Number: 6175551001 ▼ Activated

Extension: 1001

◉ Identity/Device Profile ○ Trunking ○ None

Identity/Device Profile

Identity/Device Profile Name: 6175551001 (Group) ▼   Configure Identity/Device Profile

* Public Identity: 6175551001   @ as.lab ▼ AdvancedSettings

Contact: sip:

Aliases: sip: asmodeuser1@as.lab

sip: [   ] @ as.lab ▼

sip: [   ] @ as.lab ▼

sip: [   ] @ as.lab ▼

| OK | Apply | Cancel |

Provisioning of one user in Broadworks AS is now completed.

Test Plan Executed

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

	IMS Interoperability Test Plan		
ID	**IMS Test Cases (AS Mode)**	**Result**	**Comments**
	Network Call Origination		
1	Network Call Origination: Network User to BroadWorks User, Network User Disconnects After Answer	🟩	
2	Network Call Origination: Network User to BroadWorks User, Network User Disconnects Before Answer	🟩	
3	Network Call Origination: Network User to BroadWorks User, BroadWorks User Disconnects After Answer	🟩	
	Network Call Termination		
4	Network Call Termination: BroadWorks User to Network User, BroadWorks User Disconnects After Answer	🟩	
5	Network Call Termination: BroadWorks User to Network User, BroadWorks User Disconnects Before Answer	🟩	
6	Network Call Termination: BroadWorks User to Network User, Network User Disconnects After Answer	🟩	
	Intra-group Calls		
7	Intra-group Calls: BroadWorks User to BroadWorks User, Originator Disconnects After Answer	🟩	
8	Intra-group Calls: BroadWorks User to BroadWorks User, Originator Disconnects Before Answer	🟩	
9	Intra-group Calls: BroadWorks User to BroadWorks User, Terminator Disconnects After Answer	🟩	
	Privacy		
10	Privacy: BroadWorks User A Anonymous Call to BroadWorks User C	🟩	
11	Privacy: BroadWorks User A Anonymous Call to Network User	🟩	
12	Privacy: Network User Anonymous Call to BroadWorks User D	🟩	
13	Privacy: BroadWorks User A Anonymous Call to BroadWorks User D, Call Rejected	🟩	
14	Privacy: Network User Anonymous Call to BroadWorks User D, Call Rejected	🟩	
	Phone-Controlled Services		
15	Phone-Controlled Services: BroadWorks User C to BroadWorks User A, Call Waiting	🟩	
16	Phone-Controlled Services: Network User to BroadWorks User A, Call Waiting	🟩	
17	Phone-Controlled Services: BroadWorks User A to BroadWorks User B, BroadWorks User A Hold/Retrieve	🟩	
18	Phone-Controlled Services: Network User to BroadWorks User A, BroadWorks User A Hold/Retrieve	🟩	
19	Phone-Controlled Services: BroadWorks User B to BroadWorks User A, Blind Transfer	🟧	None of the softphones support required functionality.

#	Test	Status	Notes
20	Phone-Controlled Services: BroadWorks User B to BroadWorks User A, Attended Transfer	🟧	None of the softphones support required functionality.
21	Phone-Controlled Services: BroadWorks User A to BroadWorks User B, Three-Way Call	🟩	
22	Phone-Controlled Services: BroadWorks User A to BroadWorks User B, Network-Based Conference	🟧	None of the softphones support required functionality.
23	Phone-Controlled Services: BroadWorks User B to BroadWorks User A, Call Forwarding Always	🟩	
	Call Forwarding Always		
24	Call Forwarding Always: BroadWorks User A to BroadWorks User B, CFA to BroadWorks User C	🟩	
25	Call Forwarding Always: BroadWorks User A to BroadWorks User B, CFA to Network User	🟩	
26	Call Forwarding Always: Network User to BroadWorks User B, CFA to BroadWorks User C	🟩	
27	Call Forwarding Always: Network User 1 to BroadWorks User B, CFA to Network User 2	🟩	
	Call Forwarding Always with 181		
28	Call Forwarding Always: BroadWorks User A to BroadWorks User B, CFA to BroadWorks User C	🟩	
29	Call Forwarding Always: Network User to BroadWorks User B, CFA to BroadWorks User C	🟩	
	Call Forwarding No Answer		
30	Call Forwarding No Answer: BroadWorks User A to BroadWorks User B, CFNA to BroadWorks User C	🟩	
31	Call Forwarding No Answer: BroadWorks User A to BroadWorks User B, CFNA to Network User	🟩	
32	Call Forwarding No Answer: Network User to BroadWorks User B, CFNA to BroadWorks User C	🟩	
33	Call Forwarding No Answer: Network User 1 to BroadWorks User B, CFNA to Network User 2	🟩	
	Call Forwarding Busy		
34	Call Forwarding Busy: BroadWorks User A to BroadWorks User B, CFB to BroadWorks User C	🟩	
35	Call Forwarding Busy: BroadWorks User A to BroadWorks User B, CFB to Network User	🟩	
36	Call Forwarding Busy: Network User to BroadWorks User B, CFB to BroadWorks User C	🟩	
37	Call Forwarding Busy: Network User 1 to BroadWorks User B, CFB to Network User 2	🟩	
	Call Forwarding Not Reachable		
38	Call Forwarding Not Reachable: B Not Registered; BroadWorks User A to BroadWorks User B, CFNRc to BroadWorks User C	🟩	
39	Call Forwarding Not Reachable: B Not Registered; BroadWorks User A to BroadWorks User B, CFNRc to Network User	🟩	
40	Call Forwarding Not Reachable: B Not Registered; Network User to BroadWorks User B, CFNRc to BroadWorks User C	🟩	
41	Call Forwarding Not Reachable: B Not Reachable; BroadWorks User A to BroadWorks User B, CFNRc to BroadWorks User C	🟩	
42	Call Forwarding Not Reachable: B Not Reachable; BroadWorks User A to BroadWorks User B, CFNRc to Network User	🟩	

43	Call Forwarding Not Reachable: B Not Reachable; Network User 1 to BroadWorks User B, CFNRc to Network User 2		
	Selective Call Forwarding		
44	Selective Call Forwarding: BroadWorks User A to BroadWorks User B, Selective Call Forwarding to Network User 1		
45	Selective Call Forwarding: Network User 1 to BroadWorks User B, Selective Call Forwarding to BroadWorks User C		
	Do Not Disturb		
46	Do Not Disturb: BroadWorks User A to BroadWorks User B, Do Not Disturb		
47	Do Not Disturb: Network User to BroadWorks User B, Do Not Disturb		
	Voice Messaging		
48	Voice Messaging: BroadWorks User A to BroadWorks User B, Voice Message Deposit		SMTP server required for BSFT voicemail functionality. *Will ask BSFT for traces.
49	Voice Messaging: Network User to BroadWorks User B, Voice Message Deposit		SMTP server required for BSFT voicemail functionality. *Will ask BSFT for traces.
50	Voice Messaging: BroadWorks User B to Voice Portal, Voice Message Retrieval		SMTP server required for BSFT voicemail functionality. *Will ask BSFT for traces.
51	Voice Messaging: Network User to Voice Portal, Voice Message Retrieval		SMTP server required for BSFT voicemail functionality. *Will ask BSFT for traces.
52	Voice Messaging: Message Waiting Indicator; Unsolicited		SMTP server required for BSFT voicemail functionality. *Will ask BSFT for traces.
53	Voice Messaging: Message Waiting Indicator; Solicited, MWI Subscription		SMTP server required for BSFT voicemail functionality. *Will ask BSFT for traces.
54	Voice Messaging: Message Waiting Indicator; Solicited		SMTP server required for BSFT voicemail functionality. *Will ask BSFT for traces.
	Voice Portal Calling		
55	Voice Portal Calling: BroadWorks User A to Voice Portal, Outcall to Network User		SMTP server required for BSFT voicemail functionality. *Will ask BSFT for traces.
56	Voice Portal Calling: Network User 1 to Voice Portal, Outcall to Network User 2		SMTP server required for BSFT voicemail functionality. *Will ask BSFT for traces.
	Auto Attendant		
57	Auto Attendant: BroadWorks User A to Auto Attendant, Transfer to BroadWorks User B		
58	Auto Attendant: Network User to Auto Attendant, Transfer to BroadWorks User B		
	DTMF Relay		

59	DTMF Relay: BroadWorks User A to Auto Attendant, DTMF-Relay		
	Call Pickup		
60	Call Pickup: BroadWorks User A to BroadWorks User B, Call Pickup by BroadWorks User C		
61	Call Pickup: Network User to BroadWorks User B, Call Pickup by BroadWorks User C		
	Directed Call Pickup with Barge-In		
62	Directed Call Pickup with Barge-In: BroadWorks User A to BroadWorks User B, Barge-In by BroadWorks User C		
63	Directed Call Pickup with Barge-In: Network User to BroadWorks User B, Barge-In by BroadWorks User C		
	Call Park		
64	Call Park: BroadWorks User A to BroadWorks User B, BroadWorks User A Call Park		
65	Call Park: BroadWorks User C Call Park Retrieve		
	Call Return		
66	Call Return: BroadWorks User A to BroadWorks User B, B Invokes Call Return		
67	Call Return: Network User to BroadWorks User B, B Invokes Call Return		
	Distinctive Ring		
68	Distinctive Ring: BroadWorks User A to BroadWorks User B, Ring Splash		
69	Distinctive Ring: Network User to BroadWorks User, Priority Alert		
70	Distinctive Ring: BroadWorks User A to BroadWorks User B, Alternate Number		NS rejects the alternate number with 404 Not found. BSFT could not figure out why NS rejects request.
	Intercept User		
71	Intercept User: BroadWorks User A to BroadWorks User B, Intercept B		
72	Intercept User: Network User to BroadWorks User B, Intercept B		
73	Intercept User: BroadWorks User B to BroadWorks User A, Intercept B		
	Music On Hold		
74	Music On Hold: BroadWorks User A to BroadWorks User B, BroadWorks User B Holds, MOH		
75	Music On Hold: Network User to BroadWorks User B, BroadWorks User B Holds, MOH		
	Speed Dial		
76	Speed Dial: BroadWorks User A Speed Dials BroadWorks User B		
77	Speed Dial: BroadWorks User A Speed Dials a Network User		
	Simultaneous Ring		
78	Simultaneous Ring: BroadWorks User A to BroadWorks User B, Simultaneous Ring to BroadWorks User C		
79	Simultaneous Ring: BroadWorks User A to BroadWorks User B, Simultaneous Ring to Network User		

#	Description		Notes
80	Simultaneous Ring: Network User to BroadWorks User B, Simultaneous Ring to BroadWorks User C	🟩	
81	Simultaneous Ring: Network User 1 to BroadWorks User B, Simultaneous Ring to Network User 2	🟩	
	Simultaneous Ring with Answer Confirmation		
82	Simultaneous Ring with Answer Confirmation: BroadWorks User A to BroadWorks User B, Simultaneous Ring to BroadWorks User C, Answer Confirmation	🟩	
83	Simultaneous Ring with Answer Confirmation: BroadWorks User A to BroadWorks User B, Simultaneous Ring to Network User, Answer Confirmation	🟩	
	Sequential Ring		
84	Sequential Ring: BroadWorks User A to BroadWorks User B, Sequential Ring, Answer by Network User 2	🟩	
85	Sequential Ring: Network User 3 to BroadWorks User B, Sequential Ring, Answer by Network User 2	🟩	
	Call Center		
86	Call Center: BroadWorks User A to Call Center, Call Center Agent Answers	🟩	
87	Call Center: Network User to Call Center, Call Center Agent Answers	🟩	
	Hoteling		
88	Hoteling: Call from Hoteling Guest to BroadWorks User C	🟧	AS rejects with 480 Temporarily Unavailable.
89	Hoteling: Call from Hoteling Guest to Network User	🟧	AS rejects with 480 Temporarily Unavailable.
90	Hoteling: Call to Hoteling Guest from BroadWorks User C	🟧	AS rejects with 480 Temporarily Unavailable.
91	Hoteling: Call to Hoteling Guest from Network User	🟧	AS rejects with 480 Temporarily Unavailable.
	Third Party Call Control		
92	Third Party Call Control: Click-to-Dial	🟩	
93	Third Party Call Control: Click-to-Answer	🟧	CommPilot answer option is grayed out. None of the softphones support required functionality.
94	Third Party Call Control: Click-to-Hold	🟩	
95	Third Party Call Control: Click-to-Transfer	🟩	
96	Third Party Call Control: Click-to-Conference	🟧	CommPilot answer option is grayed out. None of the softphones support required functionality.
	Remote Office		
97	Remote Office: Click-to-Dial	🟩	
98	Remote Office: Click-to-Hold	🟩	
99	Remote Office: Click-to-Transfer	🟩	

100	Remote Office: Click-to-Conference		CommPilot answer option is grayed out. None of the softphones support required functionality.
	Session Audit		
101	Session Audit: BroadWorks User A to BroadWorks User B, Wait for Session Audit		
102	Session Audit: BroadWorks User A to BroadWorks User B, BroadWorks User B Holds, Wait for Session Audit		
103	Session Audit: Network User to BroadWorks User B, Wait for Session Audit		
104	Session Audit: Network User to BroadWorks User B, BroadWorks User B Holds, Wait for Session Audit		
	Session Timer		
105	Session Timer: BroadWorks User A to BroadWorks User B, Wait for Session Timer		
106	Session Timer: BroadWorks User A to BroadWorks User B, BroadWorks User B Holds, Wait for Session Timer		
107	Session Timer: Network User to BroadWorks User B, Wait for Session Timer		
108	Session Timer: Network User to BroadWorks User B, BroadWorks User B Holds, Wait for Session Timer		
	Shared Call Appearance		
109	Shared Call Appearance: Subscribe for Call-Info		Open source phones at our disposal doesn't support this functionality
110	Shared Call Appearance: Seize Shared Line, Cancel Seize		Open source phones at our disposal doesn't support this functionality
111	Shared Call Appearance: Seize Shared Line, Call to BroadWorks User C		Open source phones at our disposal doesn't support this functionality
112	Shared Call Appearance: Seize Shared Line, Call to Network User		Open source phones at our disposal doesn't support this functionality
113	Shared Call Appearance: BroadWorks User C to Shared Line		Open source phones at our disposal doesn't support this functionality
114	Shared Call Appearance: Network User to Shared Line		Open source phones at our disposal doesn't support this functionality
115	Shared Call Appearance: BroadWorks User C to Shared Line, Hold/Retrieve		Open source phones at our disposal doesn't support this functionality
116	Shared Call Appearance: BroadWorks User C to Shared Line, Hold/Remote Retrieve		Open source phones at our disposal doesn't support this functionality
117	Shared Call Appearance: Multiple Call Arrangement, Call to Network User		Open source phones at our disposal doesn't support this functionality
118	Shared Call Appearance: Bridging		Open source phones at our disposal doesn't support this functionality
	Feature Key Synchronization		
119	Feature Key Synchronization: Subscribe for Feature Key Synchronization		Open source phones at our disposal doesn't support this functionality
120	Feature Key Synchronization: Activate Do Not Disturb from Phone		Open source phones at our disposal doesn't support this functionality
121	Feature Key Synchronization: De-Activate Do Not Disturb from BroadWorks Web Portal		Open source phones at our disposal doesn't support this functionality

	Busy Lamp Field		
122	Busy Lamp Field: Subscribe to Monitored User List		Open source phones at our disposal doesn't support this functionality
123	Busy Lamp Field: Modify Monitored User List		Open source phones at our disposal doesn't support this functionality
124	Busy Lamp Field: BLF Notify User Busy		Open source phones at our disposal doesn't support this functionality
	TCP		
125	TCP: BroadWorks User A to BroadWorks User B, Disconnect Before Answer		
126	TCP: BroadWorks User A to BroadWorks User B, Disconnect After Answer		
127	TCP: BroadWorks User A to BroadWorks User B, Hold/Retrieve		
128	TCP: Click-to-Dial		
	Video		
129	Video: BroadWorks User A Video Call to BroadWorks User B		Open source phones at our disposal doesn't support this functionality
130	Video: Network User Video Call to BroadWorks User B		Open source phones at our disposal doesn't support this functionality
131	Video: BroadWorks User A Video Call to BroadWorks User B, Hold/Retrieve		Open source phones at our disposal doesn't support this functionality
132	Video: BroadWorks User A to BroadWorks User B, Video Voice Message Deposit		Open source phones at our disposal doesn't support this functionality
133	Video: BroadWorks User B to Voice Portal, Video Voice Message Retrieval		Open source phones at our disposal doesn't support this functionality
	Business Trunking		
134	Business Trunking: BroadWorks Trunk Group User E to BroadWorks User A		Not applicable. IP-PBX with support of Pilot Number Trunking feature is required.
135	Business Trunking: BroadWorks Trunk Group User E to Network User		Not applicable. IP-PBX with support of Pilot Number Trunking feature is required.
136	Business Trunking: BroadWorks User A to BroadWorks Trunk Group User E		Not applicable. IP-PBX with support of Pilot Number Trunking feature is required.
137	Business Trunking: Network User to BroadWorks Trunk Group User E		Not applicable. IP-PBX with support of Pilot Number Trunking feature is required.
138	Business Trunking: Network User 1 to BroadWorks Trunk Group User E, Call Forward to Network User 2		Not applicable. IP-PBX with support of Pilot Number Trunking feature is required.
	Third-Party Registration		
139	Third-Party Registration: REGISTER		
140	Third-Party Registration: REGISTER With Authentication		Not applicable.

141	Third-Party Registration: Click-to-Dial		
142	Third-Party Registration: Message Waiting Indicator; Unsolicited		SMTP server required for BSFT voicemail functionality.
	Failover		
143	Failover: REGISTER Failover		Not applicable. No AS redundant available.
144	Failover: INVITE Failover		Not applicable. No AS redundant available.
145	Failover: BYE Failover		Not applicable. No AS redundant available.

During each phase of testing all the test cases defined in this document will be run and results will be reported as per definition given below. Defects will be reported in the defect-tracking database for the failed tests.

Result	Definition
Passed	When the expected results of a test are observed, the test is considered to have passed.
Not passed	When the expected results of a test are not observed, the test is considered to have failed.
Not tested	When a test has not been executed.

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 Oracle Communications CSM and 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.

Since we are concerned with communication between the Broadworks Platform, CSM and SBC we will focus on the troubleshooting tools to use between those devices if calls are not working or tests are not passing.

Wireshark

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

On the Oracle Communications CSM and SBC

The CSM and SBC provide 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 CSM or SBC Console:

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

Examining the log files.

Note: You will SFTP or FTP to the management interface of the CSM or 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 BSFT-IOT FTP 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 /ramdrv/logs
250 CWD command successful.
ftp> get sipmsg.log
200 PORT command successful.
150 Opening ASCII mode data connection for '/ramdrv/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 '/ramdrv/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.

Appendix A

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) interface on the SBC.
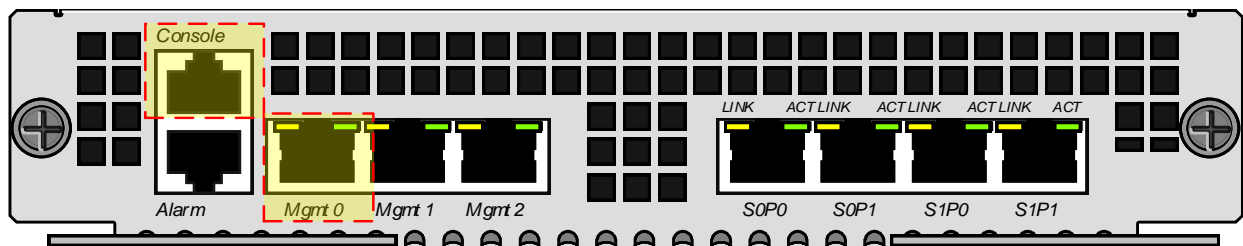
ACLI Basics

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

When you establish a connection to the CSM or 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.
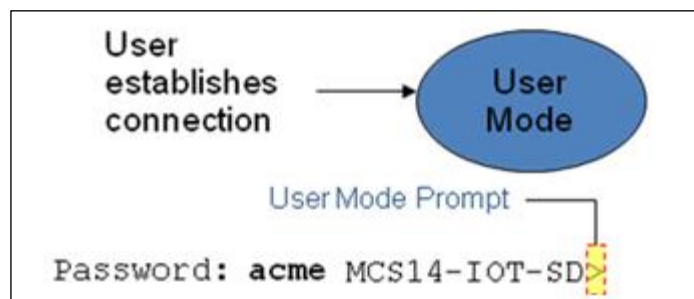
The Superuser mode allows for access to all system commands for operation, maintenance, and administration. This mode is identified by the pound sign (#) in the prompt after the target name. To enter the Superuser mode, issue the enable command in the User mode.
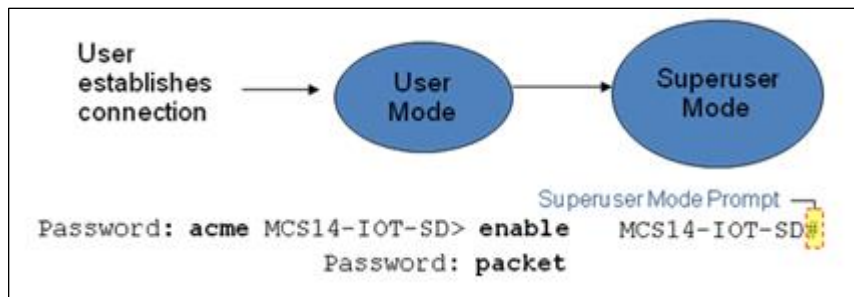
From the Superuser mode, you can perform monitoring and administrative tasks; however you cannot configure any elements. To return to User mode, issue the exit command.

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, **BSFT-IOT(configure)#**. To return to the Superuser mode, issue the `exit` command.
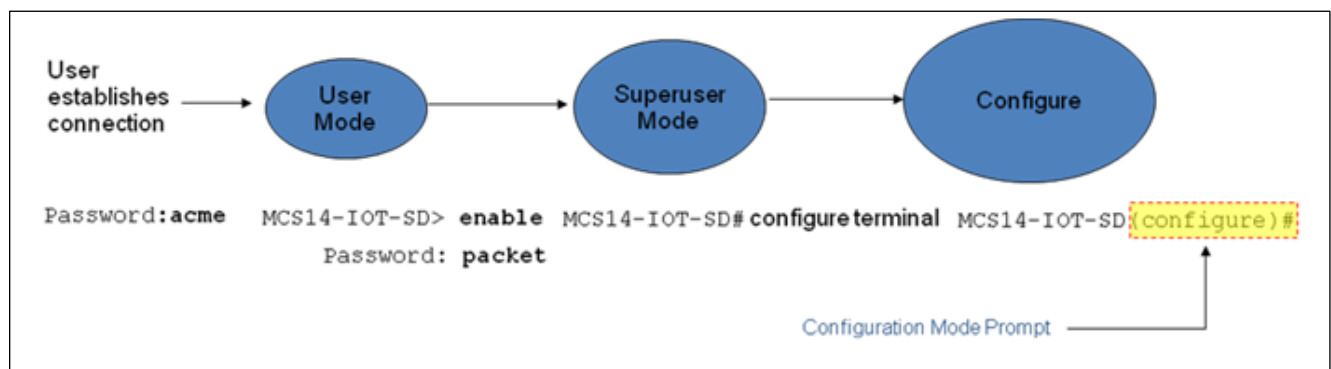
In the configuration mode, there are six configuration branches:

- bootparam;
- ntp-sync;
- media-manager;
- session-router;
- system; and
- security.
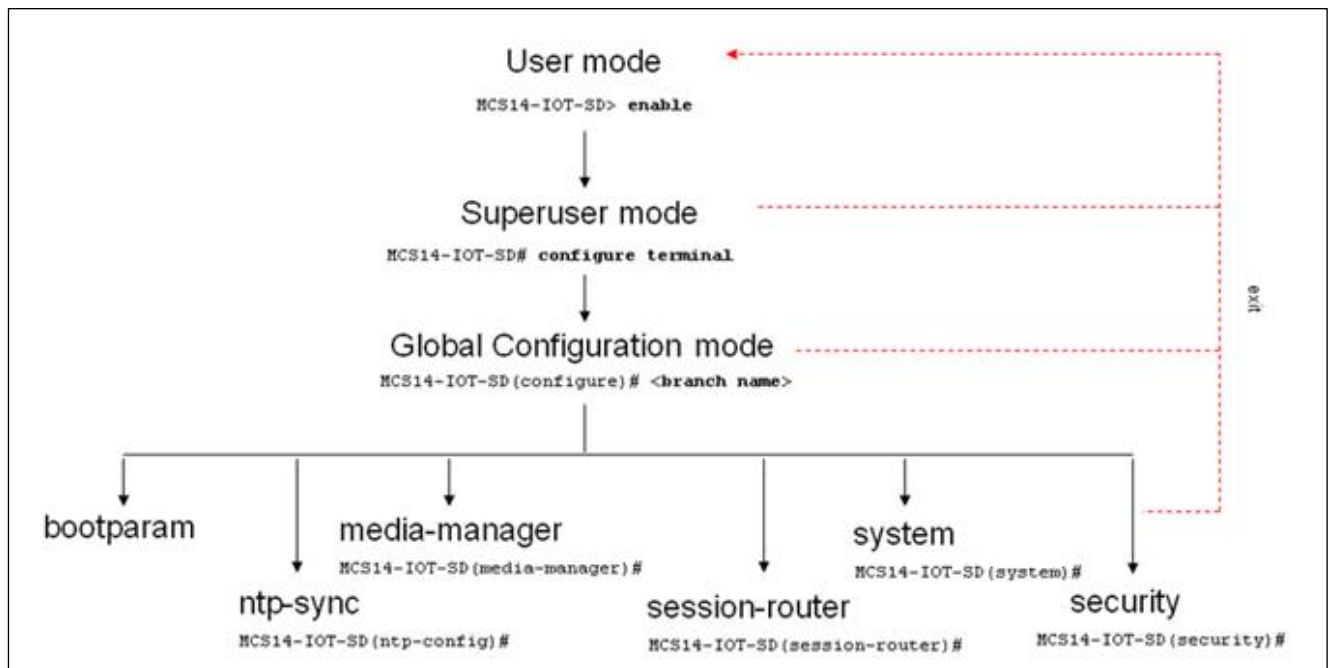
The ntp-sync and bootparams branches are flat branches (i.e., they do not have elements inside the branches). The rest of the branches have several elements under each of the branches.

The bootparam branch provides access to CSM and 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 device.

- 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 CSM and 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
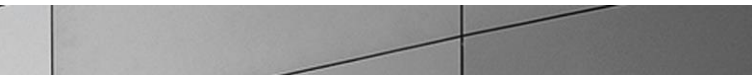
1. To create a single-instance element, you go to the appropriate level in the ACLI path and enter its parameters. There is no need to specify a unique identifier property because a single-instance element is a global element and there is only one instance of this element.

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 CSM or SBC reboots, your configuration 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 ACLI 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 CSM or 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 CSM or SBC reboots, your configurations will be lost.

Configuration Versions

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

```
BSFT-IOT# 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'.
```

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 CSM and SBC warn 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.

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

ORACLE®

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together