Best Current Practise

OCSBC – user authentication using RADIUS

Category: Informational

February 2024, Version 1.00

Revision History

Version	Author	Description of Changes	Date Revision Completed
1.00	Devon Thomas	Initial version	

Abstract

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

The configurations provided in this document SHOULD NOT be treated as RECOMMENDED. The information is intended to provide guidance as to the OCSBC behaviour when configurations listed in this document are applied.

This document is intended to provide, the reader, with information regarding configuration of an OCSBC (when configured as a Network Access Server (NAS)) to provide user authentication server via several RADIUS servers.

Applicability

The details provided are relevant to physical & virtual Oracle Communications Session Border Controller (OCSBC) instances.

Contents

Figures

Tables

1. Network Functions

An AP1100 SBC (product setup: Oracle Enterprise SBC) was used to provide the CLI/GUI information, in this document.

2. Software

OCSBC s/w release nnSCZ920p3.bz

FreeRADIUS Version 3.0.20

3. Introduction

By default, OCSBCs perform local authentication on two default accounts. i.e., “user” & “admin”. This document will show the configuration necessary for:

1. RADIUS authentication of non-default accounts. The RADIUS servers will be configured with Cisco Vendor Specific Attributes (VSAs) & Acme VSAs.
2. Load sharing (using Round Robin) of user authentications across several RADIUS servers.
3. User authentication via OCSBC’s management & media/signalling interfaces (see Figure 1).

3.1. Test environment Overview

Figure 1 & Table 1 show:

1. The IP addresses used in the test environment.
2. The Linux servers represent 4 RADIUS server instances.
3. RADIUS authentication is available via OCSBC management & media/signaling interfaces.

Figure 1 - Test setup

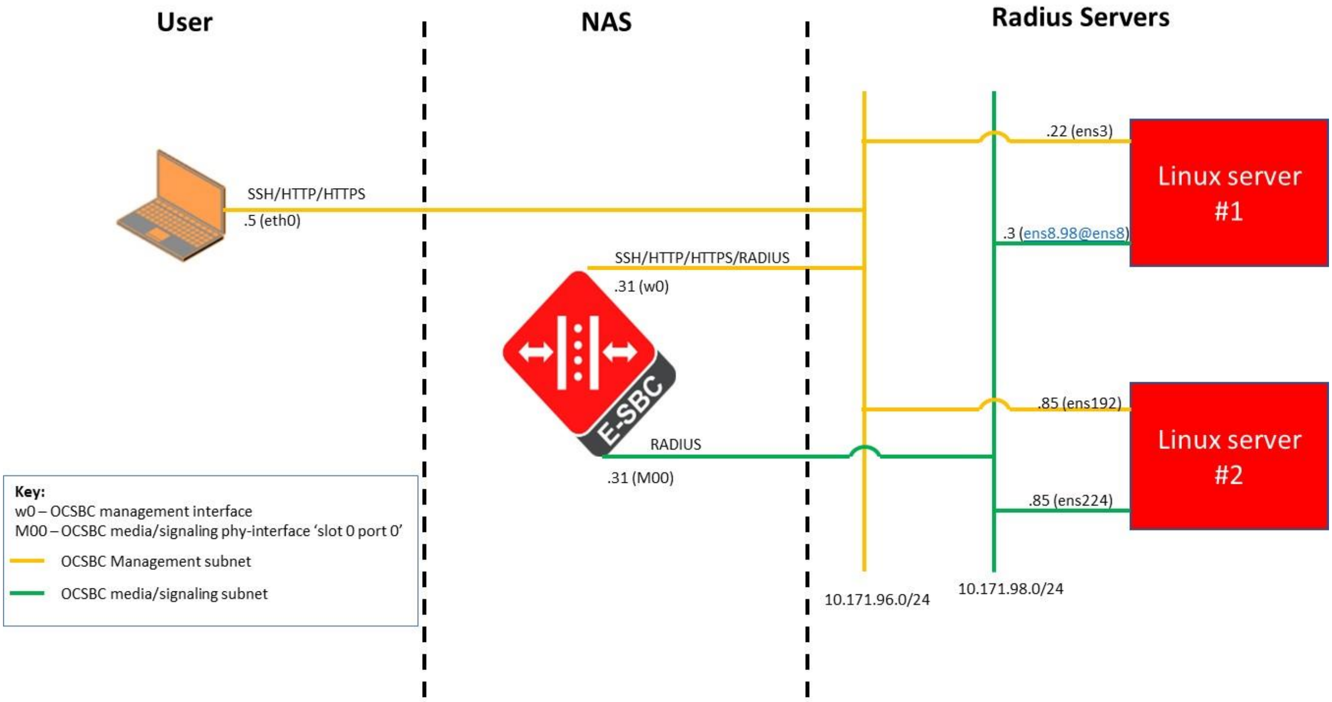


Table 1 - RADIUS server instances

Linux Server number	Linux server IP address	OCSBC ingress/egress phy-interface for RADIUS
1	10.171.96.22	wancom0
1	10.171.98.3	M00
2	10.171.96.85	wancom0
2	10.171.98.85	M00

4. OCSBC configuration summary

This section provides details of the configuration elements related to user authentication using RADIUS. Appendix A contains the OCSBC configuration.

4.1. authentication

For brevity, parameters that are not relevant or have default values which were thought to have minor impact on the required OCSBC behaviour, with respect to RADIUS authentication, have been removed from the CLI output of ‘show run authentication’, shown in section 4.1.1. See Ref 1 for more details.

4.1.1. Configuration element – CLI View

```
authentication
        source-port                             1812
        type                                    radius
        protocol                                pap
       : (for brevity some parameters have been removed)
        allow-local-authorization               disabled
        login-as-admin                          disabled
        management-strategy                     round-robin
        ike-radius-params-name
        management-servers                      10.171.96.22
                                                10.171.96.85
                                                10.171.98.3
                                                10.171.98.85
        radius-server
                address                                 10.171.96.22
                port                                    1812
                state                                   enabled
                secret                                  ********
                nas-id                                  10.171.96.31
                realm-id
              : (for brevity some parameters have been removed)
                class                                   primary
                dead-time                               10
                authentication-methods                  all
        radius-server
                address                                 10.171.98.3
                port                                    1812
                state                                   enabled
                secret                                  ********
                nas-id                                  10.171.98.31
                realm-id                                access-radius
              : (for brevity some parameters have been removed)
```

```
                class                                   primary
                dead-time                               10
                authentication-methods                  all
        radius-server
                address                                 10.171.96.85
                port                                    1812
                state                                   enabled
                secret                                  ********
                nas-id                                  10.171.96.31
                realm-id
              : (for brevity some parameters have been removed)
                class                                   primary
                dead-time                               10
                authentication-methods                  all
        radius-server
                address                                 10.171.98.85
                port                                    1812
                state                                   enabled
                secret                                  ********
                nas-id                                  10.171.98.31
                realm-id                                access-radius
              : (for brevity some parameters have been removed)
                class                                   primary
                dead-time                               10
                authentication-methods                  all
```

Table 2, provides some information concerning the configured parameters.

Table 2 – authentication element & radius-server sub-element parameters

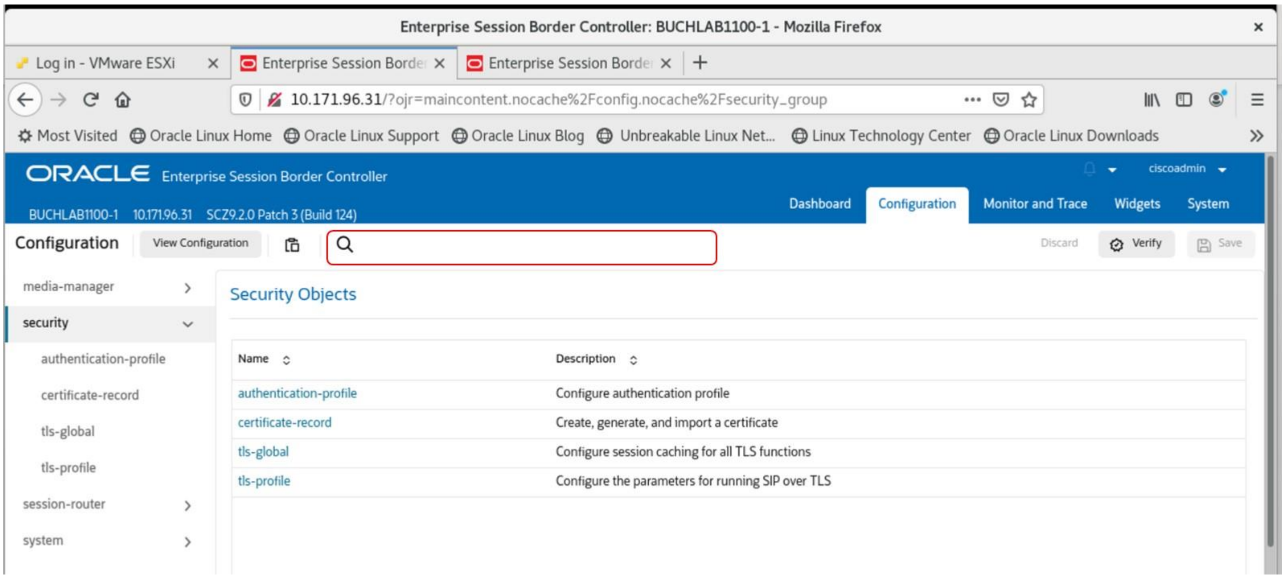
Parameter Name	Parameter Setting	Notes
authentication>type	radius	Possible values are “local, radius, tacacs”
authentication>protocol	pap	Possible values are “pap, chap, mschapv2, ascii”. Ensure value here, matches each radius server instance’s authentication-methods value OR authentication-methods is set to “all”
authentication> allow-local-authorization	disabled	Leave as “disabled”. Reason being radius server instances will return either ACME_USER_CLASS or Cisco-AVPair.
authentication> login-as-admin	disabled	Leave as “disabled”. To allow for “user” & “Superuser” access to the OCSBC.
authentication> management-strategy	round-robin	Set to “round-robin” to allow load sharing across radius server instances.
authentication>management-servers	10.171.96.22 10.171.96.85 10.171.98.3 10.171.98.85	List of radius server instances for load sharing.
authentication> radius-server>address	<value-per-radius-server-element>	IP address of radius server
authentication> radius-server>secret	<value-per-radius-server-element>	Shared secret between NAS & RADIUS server.

authentication> radius-server>nas-id	<value-per-radius-server-element>	Configured IP address of ingress/egress OCSBC network-interface as the NAS-ID
authentication> radius-server>realm-id	<value-per-radius-server-element>	Leave empty if ingress/egress interface is OCSBC's management interface. Otherwise use name of the realm from/to which RADIUS exchanges will occur.
authentication>radius-server>authentication-methods	all	Ensure value is set to "all" or it matches the value of authentication>protocol.

4.1.2. Configuration element – GUI view

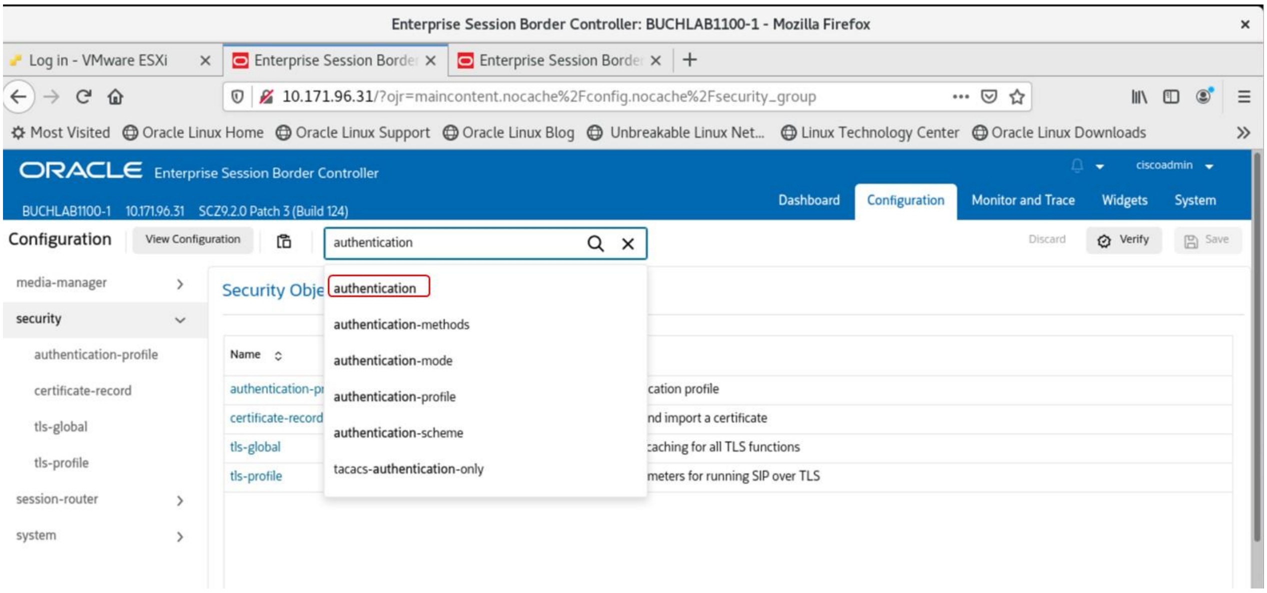
As indicated in Figure 2, the authentication object may not be visible in the GUI. Use the ‘search’ feature (highlighted in red) in Figure 2 and Figure 3, to find it.

Figure 2 - authentication element not immediately visible from GUI



Name	Description
authentication-profile	Configure authentication profile
certificate-record	Create, generate, and import a certificate
tls-global	Configure session caching for all TLS functions
tls-profile	Configure the parameters for running SIP over TLS

Figure 3 - Search for authentication object - select it from list when ready

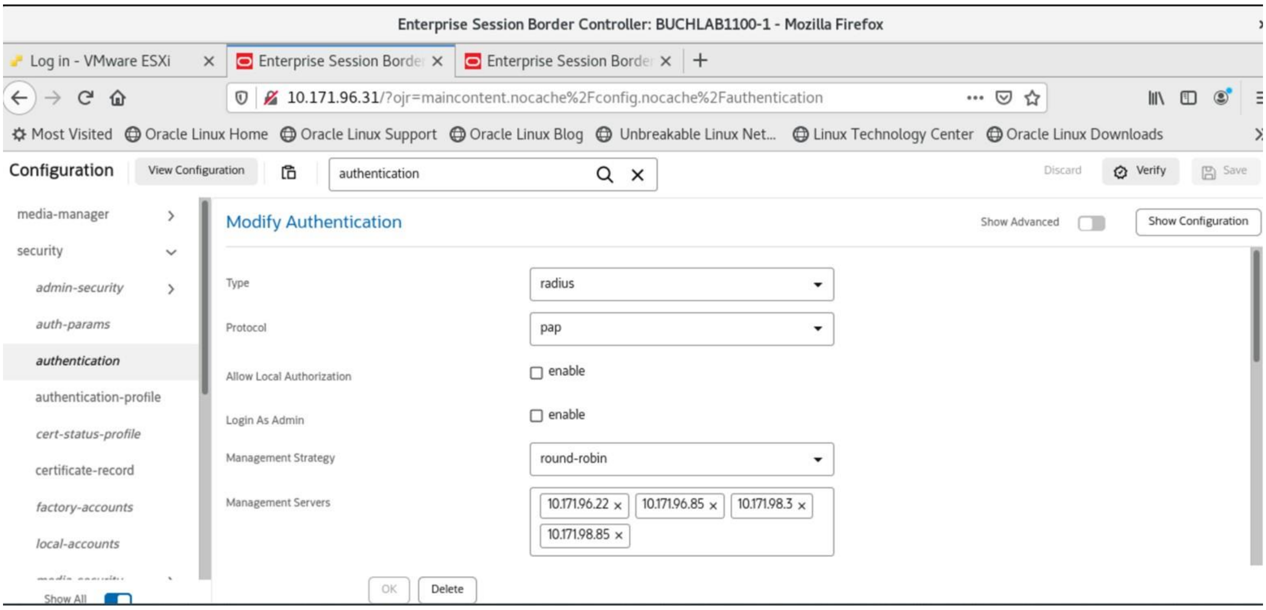


authentication

- authentication
- authentication-methods
- authentication-mode
- authentication-profile
- authentication-scheme
- tacacs-authentication-only

Figure 4 & Figure 5 shows the two halves of the authentication element.

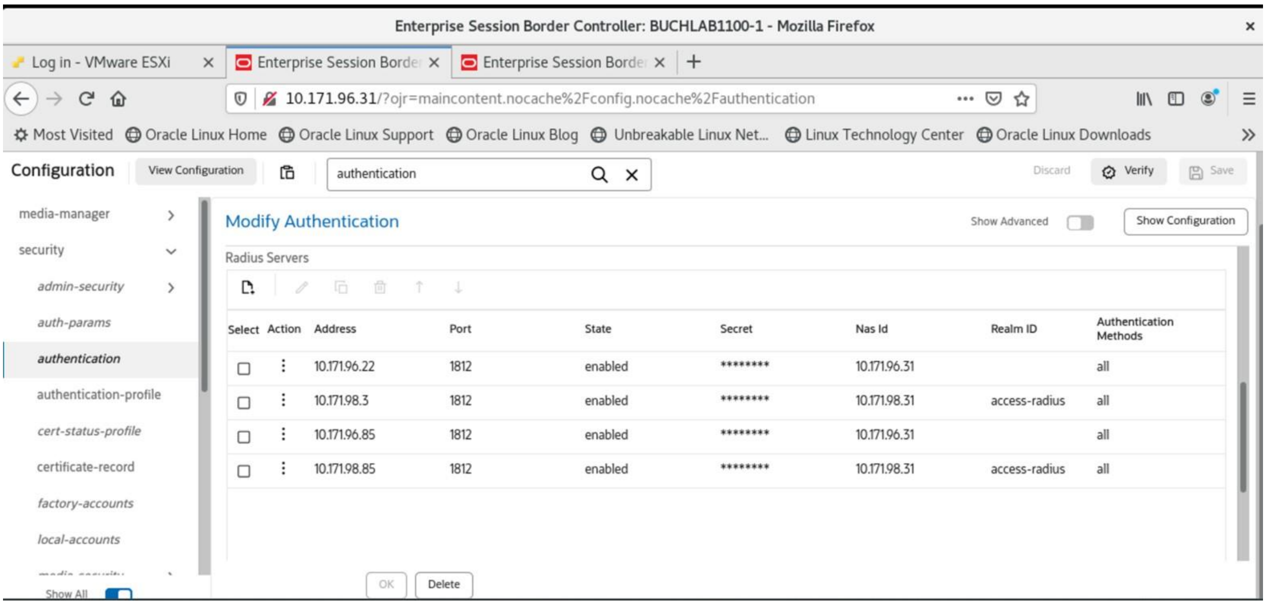
Figure 4 - authentication object - GUI view pt1



Modify Authentication

Type	radius
Protocol	pap
Allow Local Authorization	□ enable
Login As Admin	□ enable
Management Strategy	round-robin
Management Servers	10.171.96.22 × 10.171.96.85 × 10.171.98.3 × 10.171.98.85 ×

Figure 5 - authentication object - GUI view pt2 (scroll down to see)



Modify Authentication

Radius Servers

Select	Action	Address	Port	State	Secret	Nas Id	Realm ID	Authentication Methods
□	⋮	10.171.96.22	1812	enabled	********	10.171.96.31		all
□	⋮	10.171.98.3	1812	enabled	********	10.171.98.31	access-radius	all
□	⋮	10.171.96.85	1812	enabled	********	10.171.96.31		all
□	⋮	10.171.98.85	1812	enabled	********	10.171.98.31	access-radius	all

4.2. realm-config

Instances of this object are required when the RADIUS server should be reachable via a OCSBC media/signaling interface. See also authentication>radius-server>realm-id in Table 2.

4.2.1. Configuration element – CLI view

For brevity, only non-default parameter settings are shown below.

```
realm-config
        identifier                            access-radius
        network-interfaces                    M00:0
        access-control-trust-level            high
```

Table 3, provides some information regarding the parameters that have been set to non-default values. The ‘access-control’ parameter setting of ‘high’ assumes that all devices that can reach the OCSBC with packet destination tuple “network-interface>ip-address: UDP:1812” are highly trusted.

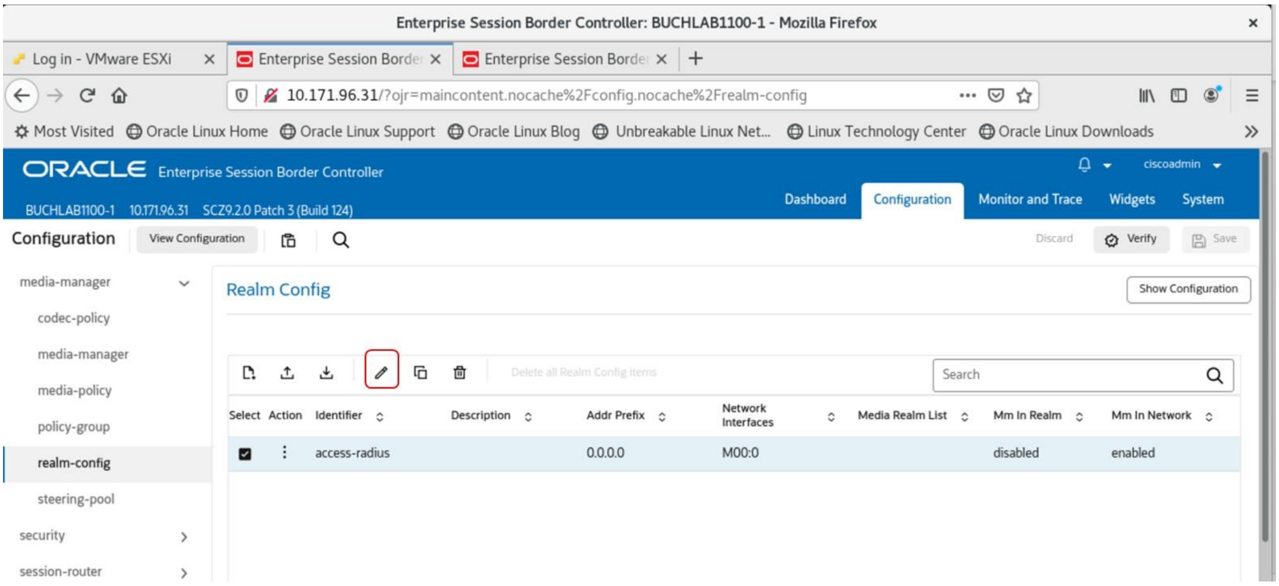
Table 3 - realm-config parameters

Parameter Name	Parameter Setting	Notes
realm-config>identifier	access-radius	Name of realm associated with a media/signaling network-interface instance. OCSBC will exchange RADIUS messages via this realm.
realm-config>network-interface	M00:0	Network-interface associated with this realm.
realm-config>access-control-trust-level	high	OCSBC will trust pkts from any device that matches destination tuple “network-interface>ip-address: UDP:1812”. access-control elements may be configured to further limit which source device(s) the OCSBC will accept pkts from. Details of this is outside the scope of this document.

4.2.2. Configuration element – GUI view

Figure 6 shows the location of realm-config instances. Select an instance and click on the ‘edit’ button (highlighted in red, in Figure 6) to view/edit the parameter settings.

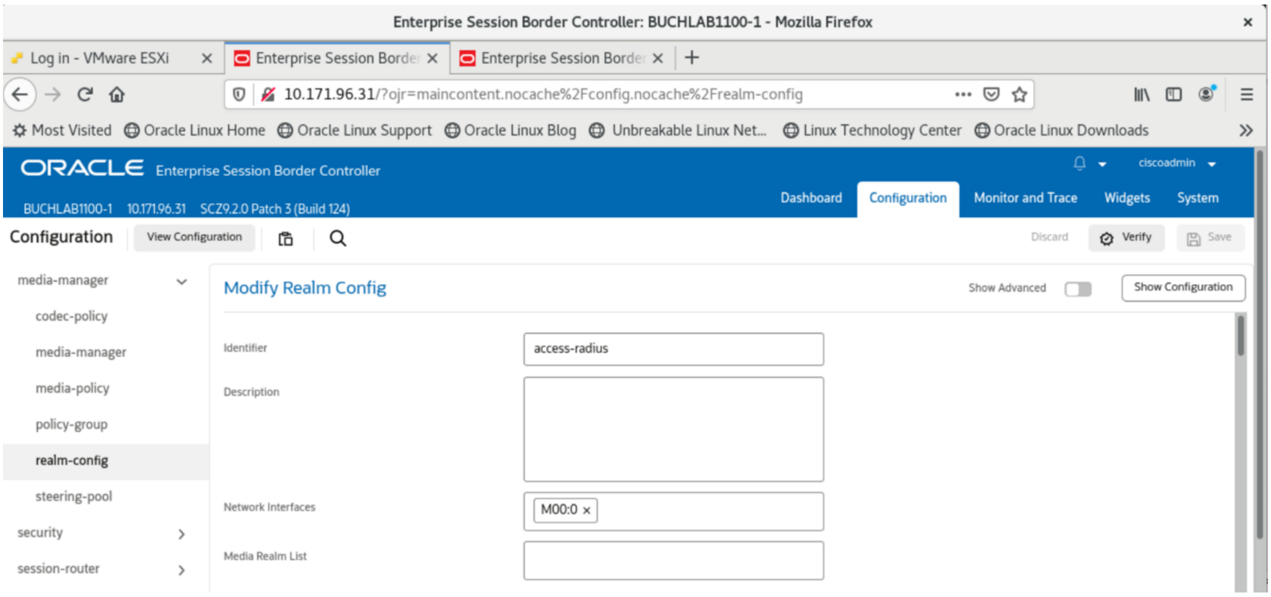
Figure 6 - location of realm-config instances



Select	Action	Identifier	Description	Addr Prefix	Network Interfaces	Media Realm List	Mm In Realm	Mm In Network
☑	⋮	access-radius		0.0.0.0	M00:0		disabled	enabled

For brevity Figure 7 & Figure 8, are intended to show the settings of the non-default parameters.

Figure 7 - Example realm-config instance for radius authentication via a media/signaling interface pt1



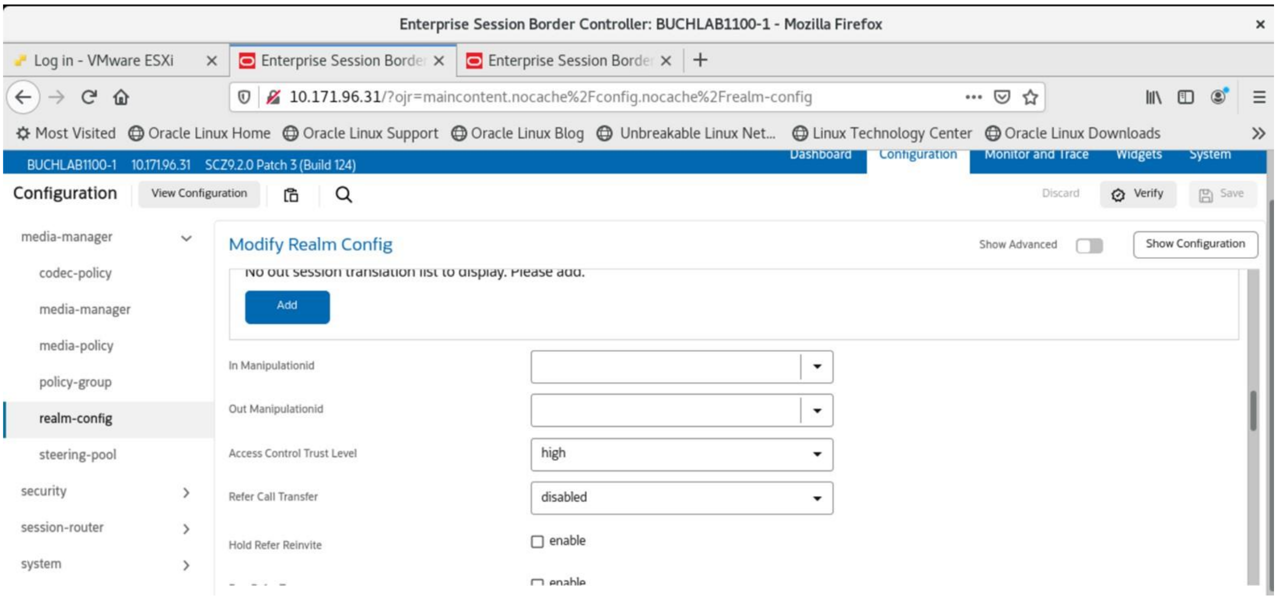
Identifier: access-radius

Description:

Network Interfaces: M00:0 ×

Media Realm List:

Figure 8 - Example realm-config instance for radius authentication via a media/signaling interface pt2



No out session translation list to display. Please add.

In Manipulationid:

Out Manipulationid:

Access Control Trust Level: high

Refer Call Transfer: disabled

Hold Refer Reinvite: □ enable

□ enable

5. OCSBC-RADIUS Server Example Exchanges

This section's sub-sections provide examples of different RADIUS authentications. Cisco Vendor Specific Attributes (VSAs) & Acme VSAs are configured on the RADIUS server. Section 5.1 provides information regarding the different account credentials.

5.1. RADIUS Server – clients.conf

Below are example entries from '/etc/raddb/clients.conf' that FreeRADIUS instances use to authenticate NAS devices (e.g. OCSBC).

```
client buchlab-management-network {
       ipaddr        = 10.171.96.0/24
       secret        = xABCdef123
}
client buchlab-10-171-98-0-network {
        ipaddr           = 10.171.98.0/24
        secret           = xABCdef123
}
```

5.2. RADIUS Server – account credentials

This section contains information from file '/etc/raddb/users'. FreeRADIUS instances use this file to authenticate users. For brevity only accounts relevant to this document are shown below:

```
# more /etc/raddb/users | awk '/^[^#]/ && !/^DEFAULT/ && !/Framed/ {print}'
ciscouser Cleartext-Password := "userRad1$"
       Cisco-AVPair += "shell:priv-lvl=1"
ciscoadmin Cleartext-Password := "adminRad2#"
        Cisco-AVPair += "shell:priv-lvl=15"
oracleuser Cleartext-Password := "userRad3$"
       Acme-User-Class = user
oracleadmin Cleartext-Password := "adminRad4#"
       Acme-User-Class = admin
oracleblocked Cleartext-Password := "abc123"
       Acme-User-Class = "none" # block access (to the SBC) for this account
#
```

5.3. OCSBC User level account – Cisco-AVPair

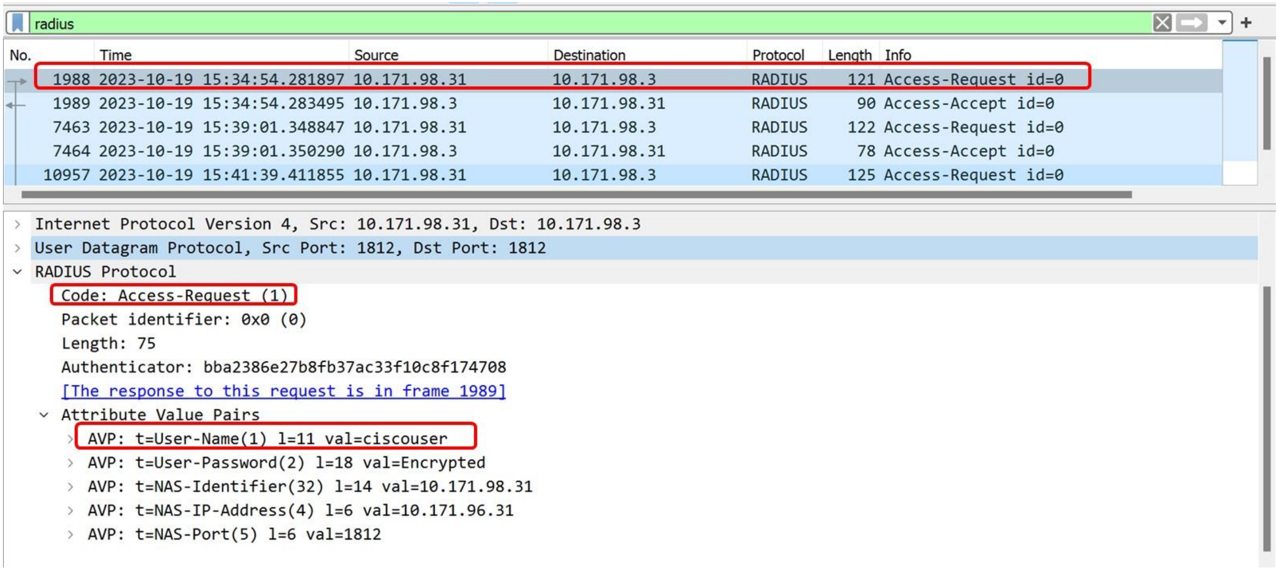
This section provides information of an OCSBC user level account being authenticated. In this scenario the RADIUS server will reply with Cisco-AVPair "shell:priv-lvl=1 VSA, when provided with the correct credentials. Figure 9 & Figure 10, show RADIUS packets exchanged during a successful authentication.

```
$ ssh ciscouser@10.171.96.31
WELCOME TO BUCHLAB1100-1

RESERVED IPs:
Mgmt:        10.171.96.31
Access(M00): 10.171.98.31
Core(M10)  : 10.171.99.31
Password:
BUCHLAB1100-1> enable
This "user" does not have privilege to be an "admin"

BUCHLAB1100-1>exit
Connection to 10.171.96.31 closed.
$
```

Figure 9 - Example - RADIUS Access-Request (user level account)

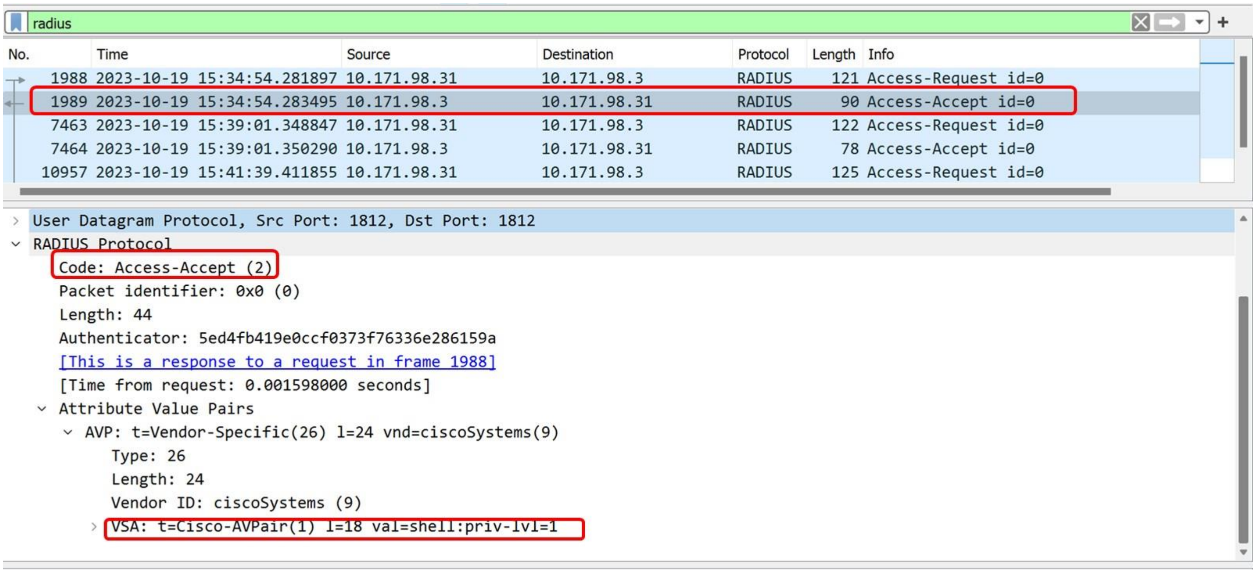


radius

```
No.    Time                       Source         Destination    Protocol  Length Info
 1988 2023-10-19 15:34:54.281897 10.171.98.31   10.171.98.3    RADIUS     121 Access-Request id=0
 1989 2023-10-19 15:34:54.283495 10.171.98.3    10.171.98.31   RADIUS      90 Access-Accept id=0
 7463 2023-10-19 15:39:01.348847 10.171.98.31   10.171.98.3    RADIUS     122 Access-Request id=0
 7464 2023-10-19 15:39:01.350290 10.171.98.3    10.171.98.31   RADIUS      78 Access-Accept id=0
10957 2023-10-19 15:41:39.411855 10.171.98.31   10.171.98.3    RADIUS     125 Access-Request id=0
```

```
> Internet Protocol Version 4, Src: 10.171.98.31, Dst: 10.171.98.3
> User Datagram Protocol, Src Port: 1812, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 75
    Authenticator: bba2386e27b8fb37ac33f10c8f174708
    [The response to this request is in frame 1989]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=11 val=ciscouser
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=NAS-Identifier(32) l=14 val=10.171.98.31
    > AVP: t=NAS-IP-Address(4) l=6 val=10.171.96.31
    > AVP: t=NAS-Port(5) l=6 val=1812
```

Figure 10 - Example – RADIUS Access-Accept, Cisco-AVPair priv-lvl=1 reply



radius

```
No.    Time                       Source         Destination    Protocol  Length Info
 1988 2023-10-19 15:34:54.281897 10.171.98.31   10.171.98.3    RADIUS     121 Access-Request id=0
 1989 2023-10-19 15:34:54.283495 10.171.98.3    10.171.98.31   RADIUS      90 Access-Accept id=0
 7463 2023-10-19 15:39:01.348847 10.171.98.31   10.171.98.3    RADIUS     122 Access-Request id=0
 7464 2023-10-19 15:39:01.350290 10.171.98.3    10.171.98.31   RADIUS      78 Access-Accept id=0
10957 2023-10-19 15:41:39.411855 10.171.98.31   10.171.98.3    RADIUS     125 Access-Request id=0
```

```
> User Datagram Protocol, Src Port: 1812, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x0 (0)
    Length: 44
    Authenticator: 5ed4fb419e0ccf0373f76336e286159a
    [This is a response to a request in frame 1988]
    [Time from request: 0.001598000 seconds]
  v Attribute Value Pairs
    v AVP: t=Vendor-Specific(26) l=24 vnd=ciscoSystems(9)
        Type: 26
        Length: 24
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=18 val=shell:priv-lvl=1
```

5.4. OCSBC Superuser (‘admin’) level account – Cisco-AVPair

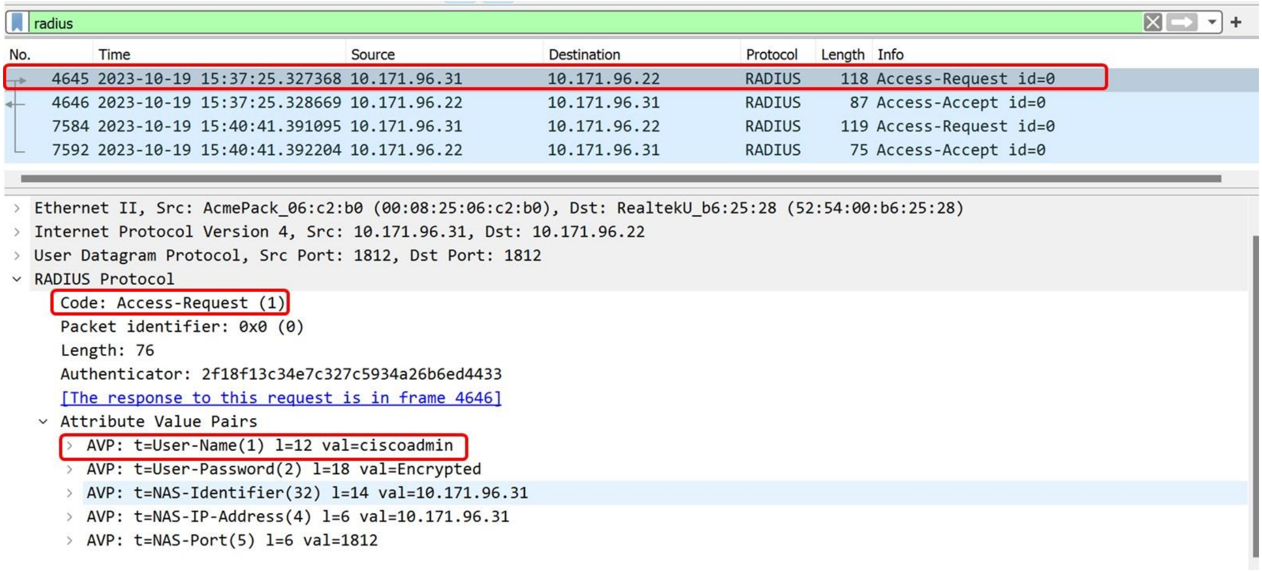
This section provides information of an OCSBC Super-user level account being authenticated. In this scenario the RADIUS server will reply with Cisco-AVPair "shell:priv-lvl=15 VSA, when the correct credentials are provided. Figure 11 & Figure 12, show RADIUS packets exchanged during a successful authentication.

```
$ ssh ciscoadmin@10.171.96.31
WELCOME TO BUCHLAB1100-1

RESERVED IPs:
```

```
Mgmt:         10.171.96.31
Access(M00): 10.171.98.31
Core(M10)   : 10.171.99.31
Password:
Password:
Password:
BUCHLAB1100-1# exit
BUCHLAB1100-1> exit
Connection to 10.171.96.31 closed.
$
```

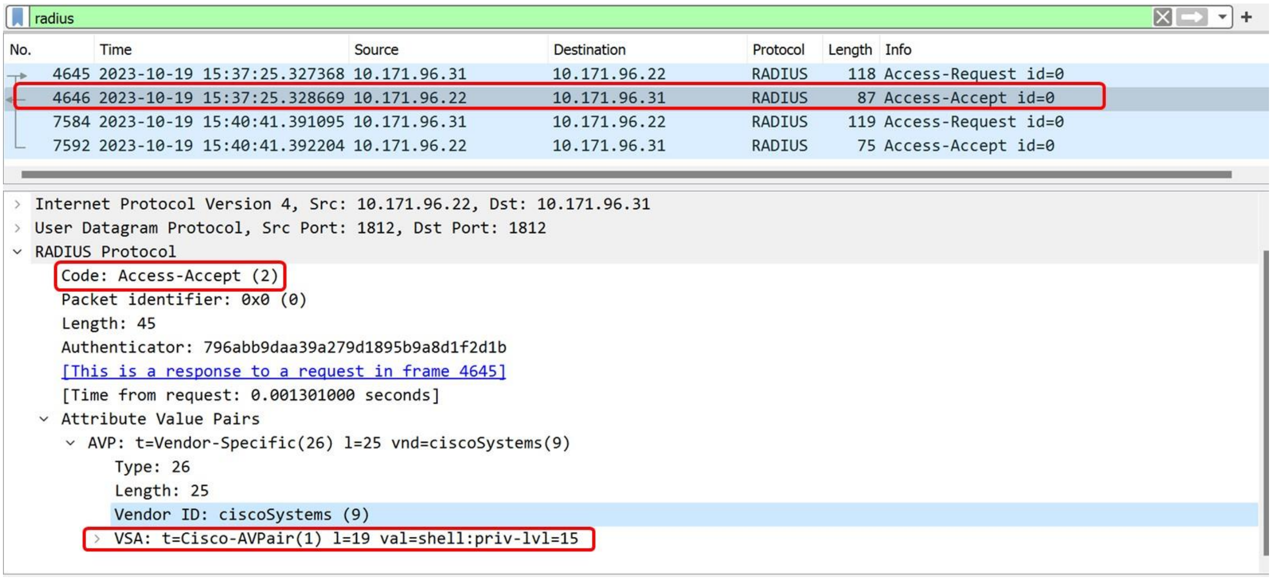
Figure 11 – Example - RADIUS Access-Request (super-user level account)



```
No.   Time                        Source          Destination     Protocol  Length  Info
4645 2023-10-19 15:37:25.327368 10.171.96.31    10.171.96.22    RADIUS     118 Access-Request id=0
4646 2023-10-19 15:37:25.328669 10.171.96.22    10.171.96.31    RADIUS      87 Access-Accept id=0
7584 2023-10-19 15:40:41.391095 10.171.96.31    10.171.96.22    RADIUS     119 Access-Request id=0
7592 2023-10-19 15:40:41.392204 10.171.96.22    10.171.96.31    RADIUS      75 Access-Accept id=0

> Ethernet II, Src: AcmePack_06:c2:b0 (00:08:25:06:c2:b0), Dst: RealtekU_b6:25:28 (52:54:00:b6:25:28)
> Internet Protocol Version 4, Src: 10.171.96.31, Dst: 10.171.96.22
> User Datagram Protocol, Src Port: 1812, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 76
    Authenticator: 2f18f13c34e7c327c5934a26b6ed4433
    [The response to this request is in frame 4646]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=12 val=ciscoadmin
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=NAS-Identifier(32) l=14 val=10.171.96.31
    > AVP: t=NAS-IP-Address(4) l=6 val=10.171.96.31
    > AVP: t=NAS-Port(5) l=6 val=1812
```

Figure 12 - Example – RADIUS Access-Accept, Cisco-AVPair priv-lvl=15 reply



```
No.   Time                        Source          Destination     Protocol  Length  Info
4645 2023-10-19 15:37:25.327368 10.171.96.31    10.171.96.22    RADIUS     118 Access-Request id=0
4646 2023-10-19 15:37:25.328669 10.171.96.22    10.171.96.31    RADIUS      87 Access-Accept id=0
7584 2023-10-19 15:40:41.391095 10.171.96.31    10.171.96.22    RADIUS     119 Access-Request id=0
7592 2023-10-19 15:40:41.392204 10.171.96.22    10.171.96.31    RADIUS      75 Access-Accept id=0

> Internet Protocol Version 4, Src: 10.171.96.22, Dst: 10.171.96.31
> User Datagram Protocol, Src Port: 1812, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x0 (0)
    Length: 45
    Authenticator: 796abb9daa39a279d1895b9a8d1f2d1b
    [This is a response to a request in frame 4645]
    [Time from request: 0.001301000 seconds]
  v Attribute Value Pairs
    v AVP: t=Vendor-Specific(26) l=25 vnd=ciscoSystems(9)
        Type: 26
        Length: 25
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=19 val=shell:priv-lvl=15
```

5.5. OCSBC User level account – Acme-User-Class

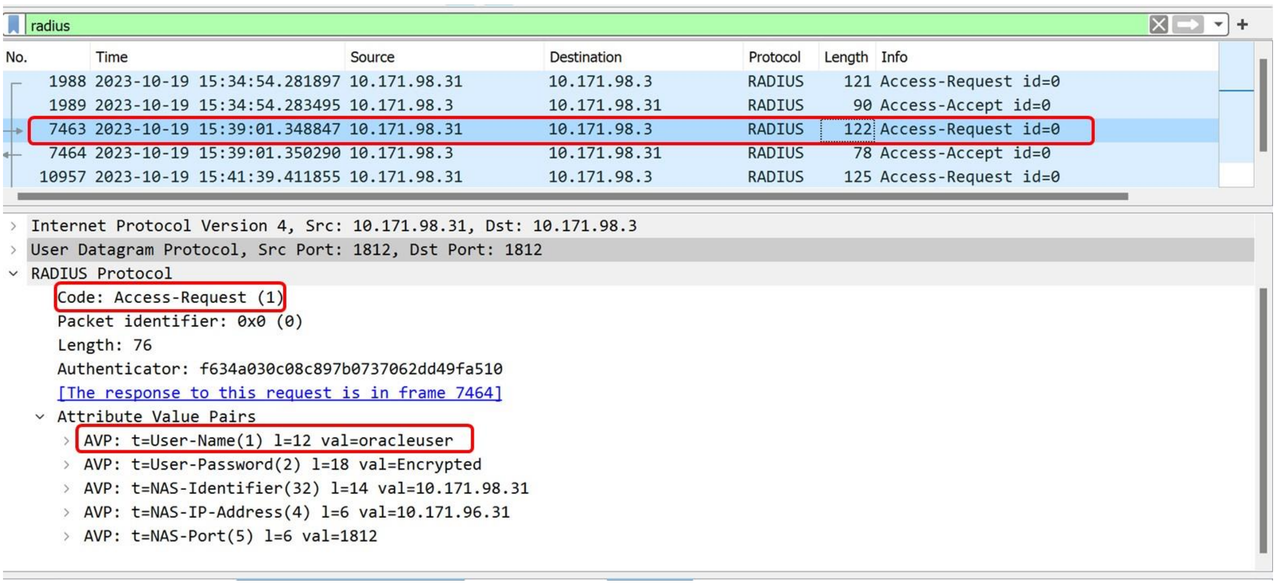
This section provides information of an OCSBC user level account being authenticated. In this scenario the RADIUS server will reply with ACME-USER-CLASS VSA, when provided with the correct credentials. Figure 13 & Figure 14, show RADIUS packets exchanged during a successful authentication.

```
$ ssh oracleuser@10.171.96.31
WELCOME TO BUCHLAB1100-1

RESERVED IPs:
Mgmt:         10.171.96.31
Access(M00): 10.171.98.31
Core(M10)   : 10.171.99.31
Password:
BUCHLAB1100-1> enable
This "user" does not have privilege to be an "admin"

BUCHLAB1100-1> exit
Connection to 10.171.96.31 closed.
$
```

Figure 13 - Example - RADIUS Access-Request (user level account)

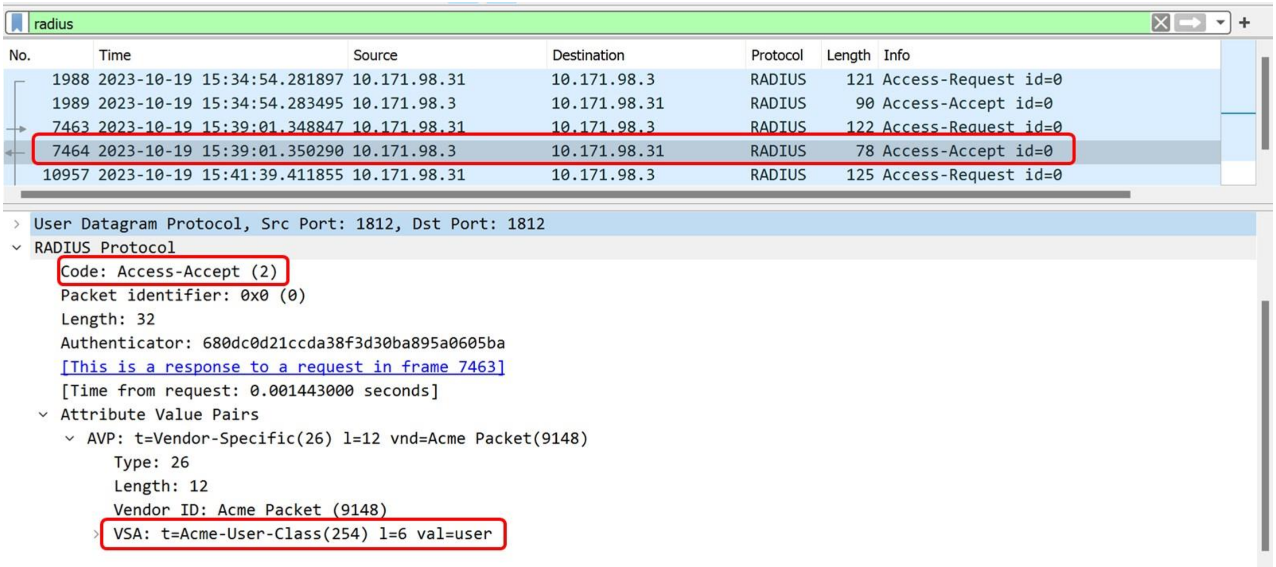


```
radius

No.    Time                        Source         Destination    Protocol  Length  Info
 1988 2023-10-19 15:34:54.281897 10.171.98.31   10.171.98.3    RADIUS     121 Access-Request id=0
 1989 2023-10-19 15:34:54.283495 10.171.98.3    10.171.98.31   RADIUS      90 Access-Accept id=0
 7463 2023-10-19 15:39:01.348847 10.171.98.31   10.171.98.3    RADIUS     122 Access-Request id=0
 7464 2023-10-19 15:39:01.350290 10.171.98.3    10.171.98.31   RADIUS      78 Access-Accept id=0
10957 2023-10-19 15:41:39.411855 10.171.98.31   10.171.98.3    RADIUS     125 Access-Request id=0

> Internet Protocol Version 4, Src: 10.171.98.31, Dst: 10.171.98.3
> User Datagram Protocol, Src Port: 1812, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 76
    Authenticator: f634a030c08c897b0737062dd49fa510
    [The response to this request is in frame 7464]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=12 val=oracleuser
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=NAS-Identifier(32) l=14 val=10.171.98.31
    > AVP: t=NAS-IP-Address(4) l=6 val=10.171.96.31
    > AVP: t=NAS-Port(5) l=6 val=1812
```

Figure 14 - Example – RADIUS Access-Accept, ACME-USER-CLASS 'user' reply



```
radius

No.    Time                        Source         Destination    Protocol  Length  Info
 1988 2023-10-19 15:34:54.281897 10.171.98.31   10.171.98.3    RADIUS     121 Access-Request id=0
 1989 2023-10-19 15:34:54.283495 10.171.98.3    10.171.98.31   RADIUS      90 Access-Accept id=0
 7463 2023-10-19 15:39:01.348847 10.171.98.31   10.171.98.3    RADIUS     122 Access-Request id=0
 7464 2023-10-19 15:39:01.350290 10.171.98.3    10.171.98.31   RADIUS      78 Access-Accept id=0
10957 2023-10-19 15:41:39.411855 10.171.98.31   10.171.98.3    RADIUS     125 Access-Request id=0

> User Datagram Protocol, Src Port: 1812, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x0 (0)
    Length: 32
    Authenticator: 680dc0d21ccda38f3d30ba895a0605ba
    [This is a response to a request in frame 7463]
    [Time from request: 0.001443000 seconds]
  v Attribute Value Pairs
    v AVP: t=Vendor-Specific(26) l=12 vnd=Acme Packet(9148)
        Type: 26
        Length: 12
        Vendor ID: Acme Packet (9148)
      > VSA: t=Acme-User-Class(254) l=6 val=user
```

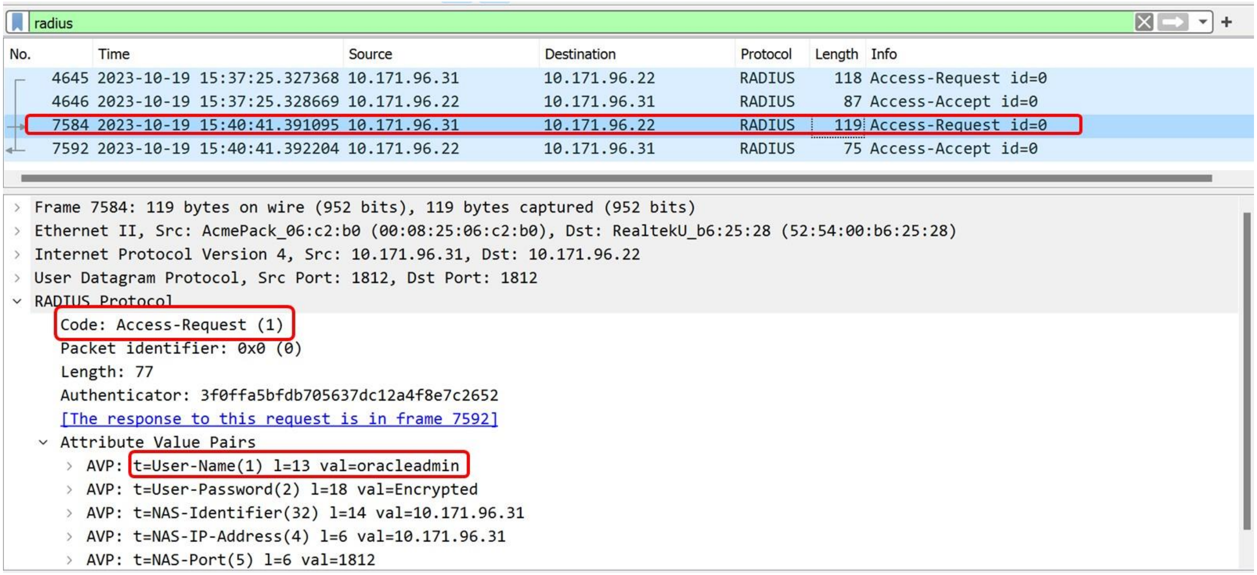
5.6. OCSBC Superuser (‘admin’) level account – Acme-User-Class

This section provides information of an OCSBC super-user level account being authenticated. In this scenario the RADIUS server will reply with ACME-USER-CLASS VSA, when provided with the correct credentials. Figure 15 & Figure 16, show RADIUS packets exchanged during a successful authentication.

```
$ ssh oracleadmin@10.171.96.31
WELCOME TO BUCHLAB1100-1

RESERVED IPs:
Mgmt:         10.171.96.31
Access(M00): 10.171.98.31
Core(M10)   : 10.171.99.31
Password:
BUCHLAB1100-1# exit
BUCHLAB1100-1> exit
Closing Session
Connection to 10.171.96.31 closed.
$
```

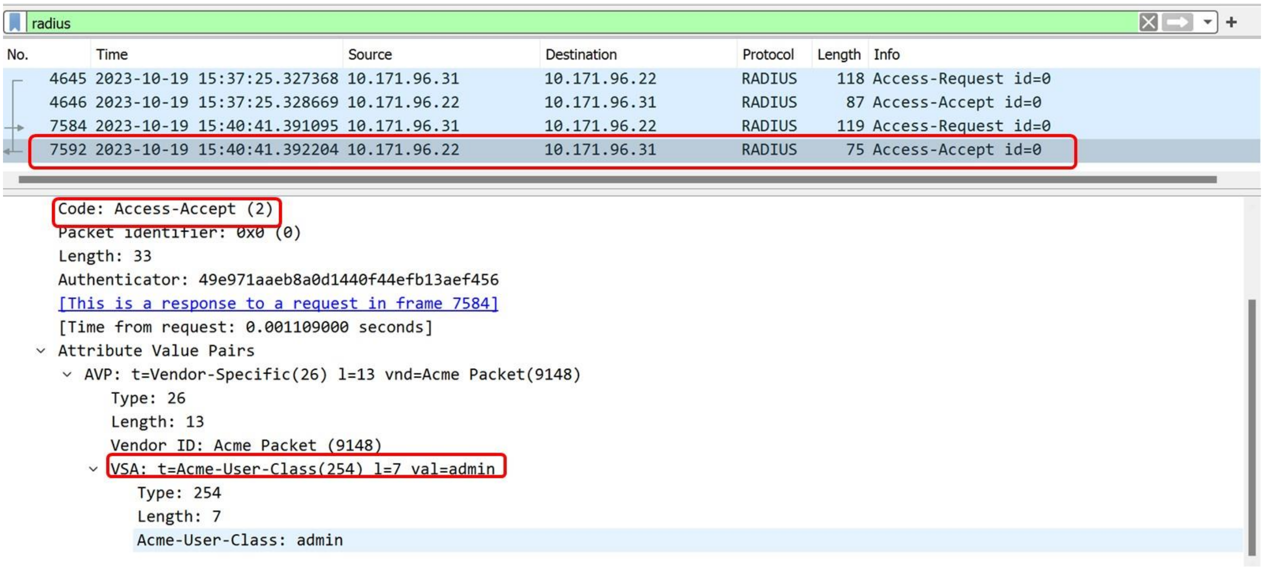
Figure 15 - Example - RADIUS Access-Request (super-user level account)



```
No.   Time                       Source        Destination   Protocol  Length Info
 4645 2023-10-19 15:37:25.327368 10.171.96.31  10.171.96.22  RADIUS    118 Access-Request id=0
 4646 2023-10-19 15:37:25.328669 10.171.96.22  10.171.96.31  RADIUS     87 Access-Accept id=0
 7584 2023-10-19 15:40:41.391095 10.171.96.31  10.171.96.22  RADIUS    119 Access-Request id=0
 7592 2023-10-19 15:40:41.392204 10.171.96.22  10.171.96.31  RADIUS     75 Access-Accept id=0

> Frame 7584: 119 bytes on wire (952 bits), 119 bytes captured (952 bits)
> Ethernet II, Src: AcmePack_06:c2:b0 (00:08:25:06:c2:b0), Dst: RealtekU_b6:25:28 (52:54:00:b6:25:28)
> Internet Protocol Version 4, Src: 10.171.96.31, Dst: 10.171.96.22
> User Datagram Protocol, Src Port: 1812, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 77
    Authenticator: 3f0ffa5bfdb705637dc12a4f8e7c2652
    [The response to this request is in frame 7592]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=13 val=oracleadmin
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=NAS-Identifier(32) l=14 val=10.171.96.31
    > AVP: t=NAS-IP-Address(4) l=6 val=10.171.96.31
    > AVP: t=NAS-Port(5) l=6 val=1812
```

Figure 16 - Example – RADIUS Access-Accept, ACME-USER-CLASS 'admin' reply



```
radius
No.   Time                        Source          Destination     Protocol  Length  Info
 4645 2023-10-19 15:37:25.327368 10.171.96.31    10.171.96.22    RADIUS      118 Access-Request id=0
 4646 2023-10-19 15:37:25.328669 10.171.96.22    10.171.96.31    RADIUS       87 Access-Accept id=0
 7584 2023-10-19 15:40:41.391095 10.171.96.31    10.171.96.22    RADIUS      119 Access-Request id=0
 7592 2023-10-19 15:40:41.392204 10.171.96.22    10.171.96.31    RADIUS       75 Access-Accept id=0

      Code: Access-Accept (2)
      Packet identifier: 0x0 (0)
      Length: 33
      Authenticator: 49e971aaeb8a0d1440f44efb13aef456
      [This is a response to a request in frame 7584]
      [Time from request: 0.001109000 seconds]
    ⌄ Attribute Value Pairs
      ⌄ AVP: t=Vendor-Specific(26) l=13 vnd=Acme Packet(9148)
          Type: 26
          Length: 13
          Vendor ID: Acme Packet (9148)
        ⌄ VSA: t=Acme-User-Class(254) l=7 val=admin
            Type: 254
            Length: 7
            Acme-User-Class: admin
```

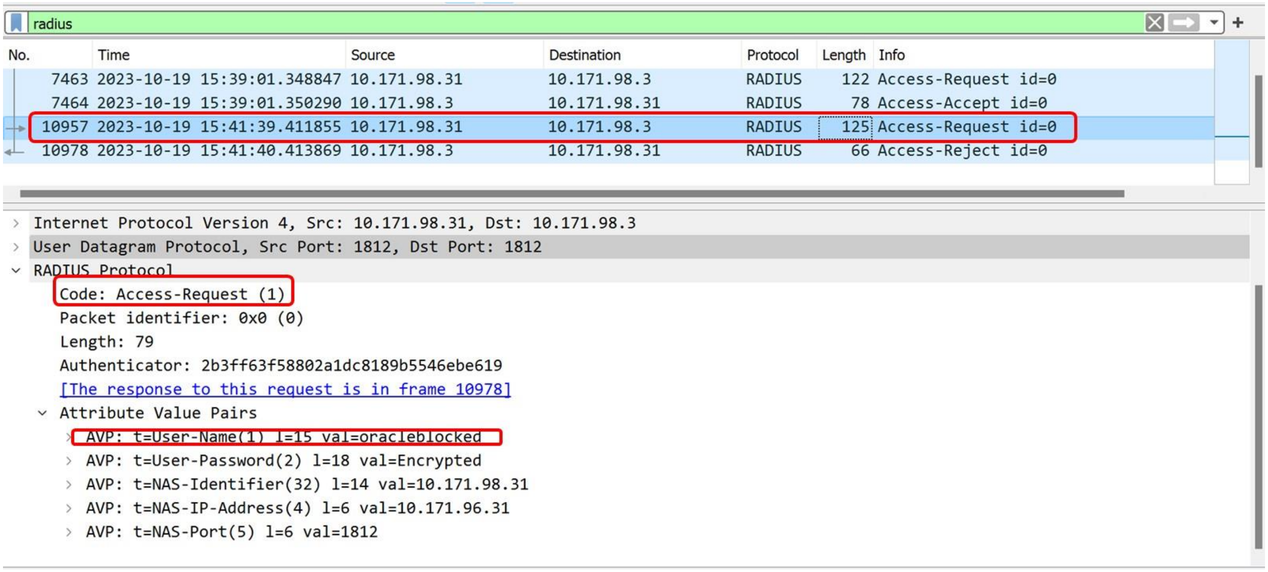
5.7. OCSBC RADIUS blocked account – Acme-User-Class

This section provides information for a blocked account. In this scenario the RADIUS server will reply with ACCESS-REJECT message. Figure 17 & Figure 18, show RADIUS packets exchanged during an authentication attempt.

```
$ ssh oracleblocked@10.171.96.31
WELCOME TO BUCHLAB1100-1

RESERVED IPs:
Mgmt:         10.171.96.31
Access(M00): 10.171.98.31
Core(M10)   : 10.171.99.31
Password:
Password:
Password:
Permission denied (publickey,keyboard-interactive).
$
```

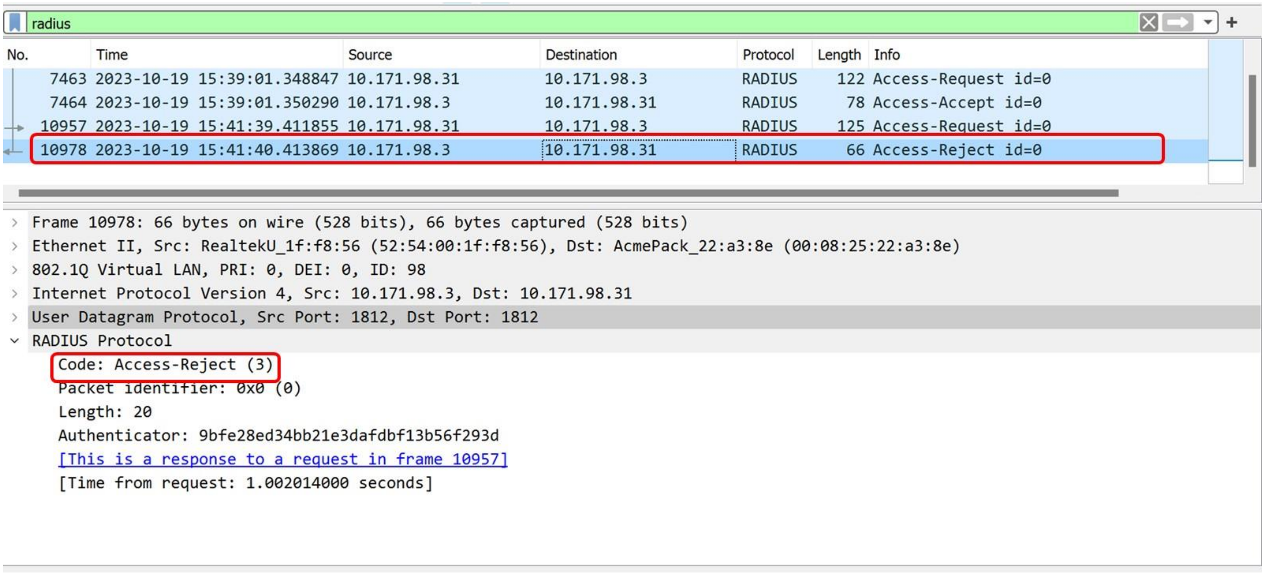
Figure 17 - Example - RADIUS Access-Request (blocked account)



```
radius
No.   Time                        Source          Destination     Protocol  Length  Info
 7463 2023-10-19 15:39:01.348847 10.171.98.31    10.171.98.3     RADIUS      122 Access-Request id=0
 7464 2023-10-19 15:39:01.350290 10.171.98.3     10.171.98.31    RADIUS       78 Access-Accept id=0
10957 2023-10-19 15:41:39.411855 10.171.98.31    10.171.98.3     RADIUS      125 Access-Request id=0
10978 2023-10-19 15:41:40.413869 10.171.98.3     10.171.98.31    RADIUS       66 Access-Reject id=0

› Internet Protocol Version 4, Src: 10.171.98.31, Dst: 10.171.98.3
› User Datagram Protocol, Src Port: 1812, Dst Port: 1812
⌄ RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 79
    Authenticator: 2b3ff63f58802a1dc8189b5546ebe619
    [The response to this request is in frame 10978]
  ⌄ Attribute Value Pairs
    › AVP: t=User-Name(1) l=15 val=oracleblocked
    › AVP: t=User-Password(2) l=18 val=Encrypted
    › AVP: t=NAS-Identifier(32) l=14 val=10.171.98.31
    › AVP: t=NAS-IP-Address(4) l=6 val=10.171.96.31
    › AVP: t=NAS-Port(5) l=6 val=1812
```

Figure 18 - Example – RADIUS Access-Reject reply



```
No.    Time                       Source        Destination   Protocol  Length Info
 7463 2023-10-19 15:39:01.348847 10.171.98.31  10.171.98.3   RADIUS      122 Access-Request id=0
 7464 2023-10-19 15:39:01.350290 10.171.98.3   10.171.98.31  RADIUS       78 Access-Accept id=0
10957 2023-10-19 15:41:39.411855 10.171.98.31  10.171.98.3   RADIUS      125 Access-Request id=0
10978 2023-10-19 15:41:40.413869 10.171.98.3   10.171.98.31  RADIUS       66 Access-Reject id=0
```

```
> Frame 10978: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: RealtekU_1f:f8:56 (52:54:00:1f:f8:56), Dst: AcmePack_22:a3:8e (00:08:25:22:a3:8e)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 98
> Internet Protocol Version 4, Src: 10.171.98.3, Dst: 10.171.98.31
> User Datagram Protocol, Src Port: 1812, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Reject (3)
    Packet identifier: 0x0 (0)
    Length: 20
    Authenticator: 9bfe28ed34bb21e3dafdbf13b56f293d
    [This is a response to a request in frame 10957]
    [Time from request: 1.002014000 seconds]
```

6. Appendix A – OCSBC ‘show run short’

The CLI output of ‘show running-config short’ command is shown below.

```
# show running-config short
authentication
        type                                    radius
        management-strategy                     round-robin
        management-servers                      10.171.96.22
                                                10.171.96.85
                                                10.171.98.3
                                                10.171.98.85
        radius-server
                address                                 10.171.96.22
                secret                                  ********
                nas-id                                  10.171.96.31
        radius-server
                address                                 10.171.98.3
                secret                                  ********
                nas-id                                  10.171.98.31
                realm-id                                access-radius
        radius-server
                address                                 10.171.96.85
                secret                                  ********
                nas-id                                  10.171.96.31
        radius-server
                address                                 10.171.98.85
                secret                                  ********
                nas-id                                  10.171.98.31
                realm-id                                access-radius
http-server
        name                                    webServerInstance
        http-interface-list                     GUI
media-manager
network-interface
        name                                    M00
        ip-address                              10.171.98.31
        netmask                                 255.255.255.0
        gateway                                 10.171.98.2
        gw-heartbeat
                state                                   enabled
                heartbeat                               10
                retry-count                             3
                retry-timeout                           3
                health-score                            30
        hip-ip-list                             10.171.98.31
        icmp-address                            10.171.98.31
network-interface
        name                                    M01
        ip-address                              10.171.99.31
        netmask                                 255.255.255.0
        gateway                                 10.171.99.2
        gw-heartbeat
                state                                   enabled
                heartbeat                               10
                retry-count                             3
                retry-timeout                           3
                health-score                            30
        hip-ip-list                             10.171.99.31
        icmp-address                            10.171.99.31
network-interface
```

```
        name                                    wancom0
        sub-port-id                             2
        pri-utility-addr                        169.254.1.1
        sec-utility-addr                        169.254.1.2
        netmask                                 255.255.255.252
ntp-config
        server                                  10.171.0.32
phy-interface
        name                                    M00
        operation-type                          Media
        virtual-mac                             00:08:25:22:a3:8e
        duplex-mode
        speed
phy-interface
        name                                    M01
        operation-type                          Media
        port                                    1
        virtual-mac                             00:08:25:22:a3:8f
        speed                                   1000
phy-interface
        name                                    wancom0
        duplex-mode
        speed
        wancom-health-score                     8
realm-config
        identifier                              access-radius
        network-interfaces                      M00:0
        access-control-trust-level              high
system-config
        hostname                                BUCHLAB1100-1
        mib-system-name                         BUCHLAB1100-1
        enable-snmp-auth-traps                  enabled
        enable-snmp-syslog-notify               enabled
        enable-snmp-monitor-traps               enabled
        enable-env-monitor-traps                enabled
        snmp-syslog-level                       INFO
        system-log-level                        INFO
        process-log-level                       INFO
        comm-monitor
                state                                   enabled
                monitor-collector
                        address                                 10.171.96.45
                monitor-collector
                        address                                 10.171.96.158
        default-gateway                         10.171.96.1
        snmp-agent-mode                         v1v2
#
```

7. References

Ref 1 - https://docs.oracle.com/en/industries/communications/session-border-controller/9.2.0/aclireference/acli-reference-guide.pdf