



AudioCodes

Configuration Guide for

TransNexus NexOSS-FC

April 13, 2015

1	Introduction.....	3
2	NexOSS-FC Solution	3
3	AudioCodes Configuration	4
3.1	SIP Message Manipulation.....	4
3.2	Proxy Sets.....	5
3.3	IP Group	8
3.4	IP-to-IP Routing	10
4	Unclassified Calls	11
4.1	Enable Unclassified Calls.....	12
4.2	SRD (Signaling Routing Domains).....	12
4.3	SIP Interface.....	13
4.4	Proxy Sets.....	13
4.5	IP Group	14
5	Test Cases	14
5.1	Fraud Detected - SBC Blocks the Call - 603 Decline	15
5.2	Fraud Detected - SBC Divert the Call - SIP 300 Redirect	17
5.3	No Fraud Detected - SBC Routes Call - 404 Not Found	19

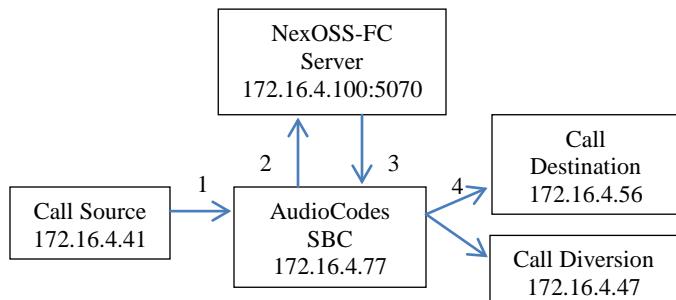
TransNexus and NexOSS-FC are trademarks of TransNexus, Inc.

1 Introduction

NexOSS-FC is a TransNexus product designed to provide real time telecom fraud prevention for enterprises and services providers. NexOSS-FC complements the AudioCodes Session Border Controller (SBC) as a SIP redirect server that identifies and blocks fraudulent calls. If no changes are made in the SBC, NexOSS-FC will detect and block fraudulent calls based on the telephone number of the calling party. However, NexOSS-FC can also provide telecom fraud detection based on the source IP address of the calling party if this information is available. This document provides instructions on how to configure AudioCodes SBC to pass the source IP address to NexOSS-FC for enhanced fraud protection.

2 NexOSS-FC Solution

NexOSS-FC solution is configured as a SIP redirect server. The following diagram illustrates how NexOSS-FC interoperates with the AudioCodes SBC.



Devices in test bed:

Call Source: 172.16.4.41
AudioCodes SBC: 172.16.4.77
NexOSS-FC Server: 172.16.4.100:5070
Call Destination: 172.16.4.56
Call Diversion: 172.16.4.47
(Call diversion can be used to route fraudulent calls to specific IP address for additional security measures, such as call recording, to collect additional information about the fraudulent call and calling party.)

SIP Messages:

1. Call Source sends a SIP INVITE to AudioCodes SBC.
2. AudioCodes forwards the SIP INVITE to NexOSS-FC Server.
Note: This call scenario requires the call source IP address (as P-Source-Device header) be added in the SIP INVITE sent to NexOSS-FC. This document explains the required SBC configuration changes.
3. NexOSS-FC analyzes SIP INVITE to determine risk of toll fraud.
 - a. If fraud is detected, SIP 603 Decline or SIP 300 Redirect (NexOSS-FC can also be configured to return SIP 302 Moved Temporarily instead of SIP 300 Redirect) is returned.
 - b. If no fraud is detected, a SIP 404 Not Found is returned to the SBC.
4. AudioCodes handles the response from NexOSS-FC
 - a. If SIP 603, call is blocked.

- b. If SIP 300, SBC send SIP INVITE to the diversion device in the redirect message contact header. This feature is used for call diversion.

- c. If SIP 404, SBC sends SIP INVITE to the next destination in local routing table.

Note: Step 4b and 4c require that the call source IP address added for step 2 (P-Source-Device header) be removed. This document explains the configuration changes.

3 AudioCodes Configuration

The configuration includes two parts, SIP message manipulation configuration and redirect routing configuration. The SIP message manipulation rules are the primary configuration for this project.

3.1 SIP Message Manipulation

Two SIP Message Manipulation rules should be configured.

1. SIP Manipulation rule InSMM is created to insert inbound SIP INVITE first Via header host (IP address of Source) as P-Source-Device header into the SIP INVITE messages to NexOSS-FC Server. This rule should be applied for the IP group of Source.

Index	Manipulation Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
1	InSMM	1	INVITE.request		header.P-Source-Device	Add	header.via.host
2	OutSMM	2	INVITE.request		header.P-Source-Device	Remove	

Manipulation Name:	InSMM	Action Subject:	header.P-Source-Device
Manipulation Set ID:	1	Action Type:	Add
Message Type:	INVITE.request	Action Value:	header.via.host
Condition:		Row Role:	Use Current Condition

2. SIP Manipulation rule OutSMM is created to remove P-Source-Device header from the SIP INVITE messages to destinations to prevent leaking source device information. This rule should be applied for the IP group of destinations.

Index	Manipulation Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
1	InSMM	1	INVITE.request		header.P-Source-Device	Add	header.via.host
2	OutSMM	2	INVITE.request		header.P-Source-Device	Remove	

Index	Manipulation Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
1	InSMM	1	INVITE.request		header.P-Source-Device	Add	header.via.host
2	OutSMM	2	INVITE.request		header.P-Source-Device	Remove	

3.2 Proxy Sets

Four Proxy sets should be configured in the SBC.

1. Proxy set for the Call Source - 172.16.4.41.

The screenshot shows the configuration interface for an AudioCodes device. The main window title is "AudioCodes Configuration for 100mg Standard - Microsoft Internet Explorer". The URL is "http://172.16.4.77". The top navigation bar includes "Submit", "Burn", "Device Actions", "Home", "Help", and "Log off". The left sidebar menu under "Configuration" includes "Basic" and "Advanced" tabs, with "Advanced" selected. The "Advanced" tab has several sections: System, VoIP, Network, Security, Media, Quality of Experience, Applications Enabling, VoIP Network, Media Realm Table, ISRO Table, IP Group Table, Proxy Sets Table, NAT Translation Table, SIP Definitions, Coders and Profiles, SBC, and Services.

The "Proxy Sets Table" section displays a table with columns "Proxy Set ID" (dropdown with value 1), "Proxy Address" (text input with value 172.16.4.41), and "Transport Type" (dropdown with value UDP). Rows 2 through 5 are empty.

The "Proxy Set ID" section displays a table with columns "Proxy Address" (text input with value 172.16.4.41) and "Transport Type" (dropdown with value UDP). Rows 2 through 10 are empty.

The bottom section contains configuration parameters:

Proxy Name	41ProxySet
Enable Proxy Keep Alive	Disable
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	0
Classification Input	IP only

2. Redirect server proxy set for NexOSS-FC.

Proxy Set ID: 2

	Proxy Address	Transport Type
1	172.16.4.100:5070	UDP
2		
3		
4		
5		
6		
7		
8		
9		
10		

Proxy Name: 100-5070ProxySet

Enable Proxy Keep Alive: Disable

Proxy Keep Alive Time: 60

Proxy Load Balancing Method: Disable

Is Proxy Hot Swap: No

Proxy Redundancy Mode: Not Configured

SRD Index: 1

Classification Input: IP only

Submit

3. Destination proxy set for destination.

Proxy Set ID: 3

	Proxy Address	Transport Type
1	172.16.4.56	UDP
2		
3		
4		
5		
6		
7		
8		
9		
10		

Proxy Name: 56ProxySet

Enable Proxy Keep Alive: Disable

Proxy Keep Alive Time: 60

Proxy Load Balancing Method: Disable

Is Proxy Hot Swap: No

Proxy Redundancy Mode: Not Configured

SRD Index: 1

Classification Input: IP only

Submit

4. Diversion proxy set for diversion device.

Index	Proxy Address	Transport Type
1	172.16.4.47	UDP
2		
3		
4		
5		
6		
7		
8		
9		
10		

Selected Row #4

Proxy Name	47ProxySet
Enable Proxy Keep Alive	Disable
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	1
Classification Input	IP only

3.3 IP Group

Four IP groups should be configured.

1. Source IP group for Source proxy set. Inbound message manipulation set should be configured as 1, InSMM.

Index	Type	Description	Proxy Set ID	SIP Group Name	Contact User
1	Server	411PGroup	1		
2	Server	100-50701PGroup	2		
3	Server	561PGroup	3		
4	Server	471PGroup	4		

Selected Row #1

Common	SBC
Types:	Server
Description:	411PGroup
Proxy Set ID:	1
SIP Group Name:	
Contact User:	
SRD:	0
Media Realm Name:	None
IP Profile ID:	1
Local Host Name:	
UII Format:	Disable
QoS Profile:	None
Bandwidth Profile:	None
Media Enhancement Profile:	None
Always Use Source Address:	No
Classify By Proxy Set:	Enable
Max. Number of Registered Users:	-1
Inbound Message Manipulation Set:	1
Outbound Message Manipulation Set:	-1
Registration Mode:	User Initiates Registration
Authentication Mode:	User Authenticates
Authentication Method List:	
SBC Client Forking Mode:	Sequential
Source URI Input:	FROM
Destination URI Input:	Request-URI
Username:	
Password:	
Msg Man User Defined String1:	
Msg Man User Defined String2:	

2. Redirect server IP group for redirect proxy set.

3. Destination IP group for destination proxy set. Outbound message manipulation set should be configured as 2, OutSMM.

4. Diversion IP group for diversion proxy set. Outbound message manipulation set should be configured as 2, OutSMM.

3.4 IP-to-IP Routing

Redirect routing rule is configured.

Index	Route Name	Source Host	Destination Username Prefix	Destination Host	Message Condition	ReRoute IP Group ID	Call Trigger	Call Setup Rules Set ID	Destination Type	Destination ID
20	Redirect	*	*	*	None	-1	Initial only	-1	IP Group	None
21	NoFraudDestination	*	*	*	None	-1	Any	-1	IP Group	None
22	FraudDiversion	*		172.16.4.47	None	-1	3xx	-1	IP Group	None

Index	Route Name	Source Host	Destination Username Prefix	Destination Host	Message Condition	ReRoute IP Group ID	Call Trigger	Call Setup Rules Set ID	Destination Type	Destination ID
20	Redirect	*	*	*	None	-1	Initial only	-1	IP Group	None
21	NoFraudDestination	*	*	*	None	-1	Any	-1	IP Group	None
22	FraudDiversion	*		172.16.4.47	None	-1	3xx	-1	IP Group	None

4 Unclassified Calls

It is possible to configure AudioCodes SBC to accept unclassified calls that their source devices are not configured in SBC explicitly. The logic is

1. Unclassified calls come in from SIP Interface configured with SRD UnclassifiedSRD.
2. AudioCodes SBC classifies the calls to the first Proxy Set/IP group configured with UnclassifiedSRD.
3. AudioCodes SBC routes the calls according to the IP group.

4.1 Enable Unclassified Calls

Unclassified calls must be allowed.

The screenshot shows the 'SBC General Settings' configuration page. The left sidebar lists various system and network settings. The main panel displays several configuration parameters:

Setting	Value
Transcoding Mode	Only If Required
No Answer Timeout [sec]	600
GRUU Mode	As Proxy
Minimum Session-Expires [sec]	90
BroadWorks Survivability Feature	Disable
BVE Authentication	Disable
User Registration Time [sec]	0
Proxy Registration Time [sec]	0
Survivability Registration Time [sec]	0
Forking Handling Mode	Latch On First
Unclassified Calls	Allow
Session-Expires [sec]	180
Direct Media	Disable
Preferences Mode	Doesn't Include Extensions
User Registration Grace Time [sec]	0
Fax Detection Timeout [sec]	10
Max Forwards Limit	10
SBC Enable Subscribe Trying	Disable
RTCP Mode	Transparent
Server Authentication	
Lifetime of nonce [sec]	300
Authentication Challenge Method	0
Authentication Quality of Protection	2

4.2 SRD (Signaling Routing Domains)

A SRD for the unclassified calls is configured.

The screenshot shows the 'SRD Table' configuration page. The left sidebar lists various tables and interfaces. The main panel displays a table of SRD entries:

Index	Name	Media Realm Name	Media Anchoring
0	SrcSRD	DefaultRealm	Enable
1	DestSRD	DefaultRealm	Enable
3	UnclassifiedSRD	DefaultRealm	Enable

Below the table, a 'Selected Row #3' details the configuration for the 'UnclassifiedSRD' entry:

Name:	UnclassifiedSRD	Block Unregistered Users:	NO
Media Realm Name:	DefaultRealm	Max. Number of Registered Users:	-1
Media Anchoring:	Enable	Enable Uni-Authenticated Registrations:	Enable

4.3 SIP Interface

The SIP Interface receiving the unclassified calls should be configured with SDR 3, UnclassifiedSRD.

The screenshot shows the AudioCodes configuration interface for a Mediant SW device. The left sidebar contains a navigation tree with sections like System, VoIP, Network, Security, Media, Quality of Experience, Applications Enabling, VoIP Network, SIP Definitions, Coders and Profiles, SBC, and Services. The main panel displays the 'SIP Interface Table' with two entries:

Index	SIP Interface Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
1	SrcSIPInterface	MainIPInterface	SBC	5060	5060	5061	3
2	DestSIPInterface	MainIPInterface	SBC	5070	5070	5071	1

A yellow box highlights the first row, labeled 'Selected Row #1'. The details for this row are shown in a callout box:

SIP Interface Name:	SrcSIPInterface	SRD:	3
Network Interface:	MainIPInterface	Message Policy:	None
Application Type:	SBC	TLS Context Name:	None
UDP Port:	5060	TLS Mutual Authentication:	None
TCP Port:	5060	Enable TCP Keepalive:	Disable
TLS Port:	5061	Classification Failure Response Type:	500

4.4 Proxy Sets

A Proxy Set with UnclassifiedSRD, 3, should be configured.

The screenshot shows the AudioCodes configuration interface for a Mediant SW device. The left sidebar contains a navigation tree with sections like System, VoIP, Network, Security, Media, Quality of Experience, Applications Enabling, VoIP Network, SIP Definitions, Coders and Profiles, SBC, and Services. The main panel displays the 'Proxy Sets Table' with a table for 'Proxy Set ID' 1:

	Proxy Address	Transport Type
1	172.16.4.41	UDP
2		
3		
4		
5		
6		
7		
8		
9		
10		

Below the table is a detailed configuration section for 'Proxy Set ID 1' with the following values:

Proxy Name	41ProxySet
Enable Proxy Keep Alive	Disable
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	3
Classification Input	IP only

A checkmark icon with the word 'Submit' is located at the bottom right of the configuration area.

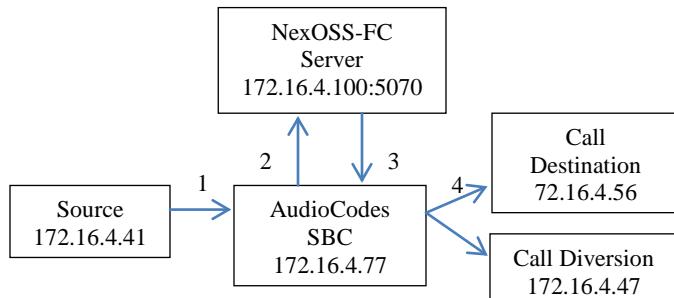
4.5 IP Group

A IP Group with UnclassifiedSRD, 3, and the proxy set with the same SRD should be configured.

Index	Type	Description	Proxy Set ID	SIP Group Name	Contact User
1	Server	41IPGroup	1		
2	Server	100-5070IPGroup	2		
3	Server	56IPGroup	3	3	
4	Server	47IPGroup	4		

5 Test Cases

Network Diagram:



Data Flow:

1. Source sends a SIP INVITE to AudioCodes SBC
2. AudioCodes forwards the SIP INVITE to NexOSS-FC Server
3. NexOSS-FC test cases
 - a. Fraud is detected - block call, SIP 603 Decline is returned
 - b. Fraud is detected - divert call, SIP 300 Redirect is returned.
 - c. No fraud detected, SIP 404 Not Found returned
4. AudioCodes SBC routes, blocks or diverts the call based on the SIP message returned by NexOSS-FC.

5.1 Fraud Detected - SBC Blocks the Call - 603 Decline

In this test case, NexOSS-FC analysis determines high risk of fraud and returns a 603 Decline messages to the SBC. The SBC should block the call. The following SBC log documents the SIP messages for the fraud - block call use case.

1. SIP INVITE from Source to SBC.

```
12d:7h:50m:40s INVITE sip:14040000020@172.16.4.77:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.4.41:5060;branch=z9hG4bK-5372-1-0
From: sipp <sip:1234567890@172.16.4.41:5060>;tag=5372SIPpTag001
To: sut <sip:14040000020@172.16.4.77:5060>
Call-ID: 1-5372@172.16.4.41
CSeq: 1 INVITE
Contact: sip:1234567890@172.16.4.41:5060
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 133

v=0
o=user1 53655765 2353687637 IN IP4 172.16.4.41
s=-
c=IN IP4 172.16.4.41
t=0 0
m=audio 6000 RTP/AVP 8
a=rtpmap:8 PCMA/8000
```

2. SIP 100 Trying from SBC to Source

```
12d:7h:50m:40s SIP/2.0 100 Trying
Via: SIP/2.0/UDP 172.16.4.41:5060;branch=z9hG4bK-5372-1-0
From: sipp <sip:1234567890@172.16.4.41>;tag=5372SIPpTag001
To: sut <sip:14040000020@172.16.4.77>;tag=1c502521130
Call-ID: 1-5372@172.16.4.41
CSeq: 1 INVITE
Server: Mediant SW/v.6.80A.216.008
Content-Length: 0
```

3. SIP INVITE from SBC to NexOSS-FC

P-Source-Device header has been added to SIP INVITE

```
12d:7h:50m:40s INVITE sip:14040000020@172.16.4.77 SIP/2.0
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac504682112
Max-Forwards: 10
From: sipp <sip:1234567890@172.16.4.41>;tag=1c504590555
To: sut <sip:14040000020@172.16.4.77>
Call-ID: 504579371123201575040@172.16.4.77
CSeq: 1 INVITE
Contact: <sip:1234567890@172.16.4.77:5070>
User-Agent: Mediant SW/v.6.80A.216.008
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 133
P-Source-Device: 172.16.4.41:5060
```

```
v=0
o=user1 504529370 504529337 IN IP4 172.16.4.77
s=-
c=IN IP4 172.16.4.77
t=0 0
m=audio 6010 RTP/AVP 8
```

a=rtpmap:8 PCMA/8000

4. SIP 100 Trying from NexOSS-FC to SBC

```
12d:7h:50m:40s SIP/2.0 100 Trying
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac504682112
From: sipp <sip:1234567890@172.16.4.41>;tag=lc504590555
To: sut <sip:14040000020@172.16.4.77>
Call-ID: 504579371123201575040@172.16.4.77
CSeq: 1 INVITE
Server: OpenSIPS (1.8.2-notls (x86_64/linux))
Content-Length: 0
```

5. SIP 603 Decline from NexOSS-FC to SBC

```
12d:7h:50m:40s SIP/2.0 603 Decline
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac504682112
From: sipp <sip:1234567890@172.16.4.41>;tag=lc504590555
To: sut <sip:14040000020@172.16.4.77>;tag=7cb6f5a1787856c92fdb341051634cd0.b445
Call-ID: 504579371123201575040@172.16.4.77
CSeq: 1 INVITE
Server: OpenSIPS (1.8.2-notls (x86_64/linux))
Content-Length: 0
```

6. SIP ACK from SBC to NexOSS-FC

```
12d:7h:50m:40s ACK sip:14040000020@172.16.4.77 SIP/2.0
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac504682112
Max-Forwards: 10
From: sipp <sip:1234567890@172.16.4.41>;tag=lc504590555
To: sut <sip:14040000020@172.16.4.77>;tag=7cb6f5a1787856c92fdb341051634cd0.b445
Call-ID: 504579371123201575040@172.16.4.77
CSeq: 1 ACK
Contact: <sip:1234567890@172.16.4.77:5070>
User-Agent: Mediant SW/v.6.80A.216.008
Content-Length: 0
```

7. SIP 603 Decline from SBC to Source

```
12d:7h:50m:40s SIP/2.0 603 Decline
Via: SIP/2.0/UDP 172.16.4.41:5060;branch=z9hG4bK-5372-1-0
From: sipp <sip:1234567890@172.16.4.41>;tag=5372SIPpTag001
To: sut <sip:14040000020@172.16.4.77>;tag=lc502521130
Call-ID: 1-5372@172.16.4.41
CSeq: 1 INVITE
Server: Mediant SW/v.6.80A.216.008
Content-Length: 0
```

8. SIP ACK from Source to SBC

```
12d:7h:50m:40s ACK sip:14040000020@172.16.4.77 SIP/2.0
Via: SIP/2.0/UDP 172.16.4.41:5060;branch=z9hG4bK-5372-1-0
From: sipp <sip:1234567890@172.16.4.41>;tag=5372SIPpTag001
To: sut <sip:14040000020@172.16.4.77>;tag=lc502521130
Call-ID: 1-5372@172.16.4.41
CSeq: 1 ACK
Contact: <sip:sipp@172.16.4.41:5060;transport=UDP>
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0
```

5.2 Fraud Detected - SBC Divert the Call - SIP 300 Redirect

In this test case, NexOSS-FC determines the call is fraudulent, but has been configured to instruct the SBC to divert the call, not block the call. The following SBC log documents the SIP messages for this test case.

1. SIP INVITE from Source to SBC.

```
10d:3h:8m:2s INVITE sip:14040000022@172.16.4.77:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.4.41:5060;branch=z9hG4bK-2690-1-0
From: sipp <sip:1234567890@172.16.4.41:5060>;tag=2690SIPpTag001
To: sut <sip:14040000022@172.16.4.77:5060>
Call-ID: 1-2690@172.16.4.41
CSeq: 1 INVITE
Contact: sip:1234567890@172.16.4.41:5060
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 133

v=0
o=user1 53655765 2353687637 IN IP4 172.16.4.41
s=-
c=IN IP4 172.16.4.41
t=0 0
m=audio 6000 RTP/AVP 8
a=rtpmap:8 PCMA/8000
```

2. SIP 100 Trying from SBC to Source

```
10d:3h:8m:2s (      lgr_flow)(      1744) ---- Outgoing SIP Message to
172.16.4.41:5060 from SIPInterface #1 UdpTransportObject(#1) ----

10d:3h:8m:2s SIP/2.0 100 Trying
Via: SIP/2.0/UDP 172.16.4.41:5060;branch=z9hG4bK-2690-1-0
From: sipp <sip:1234567890@172.16.4.41>;tag=2690SIPpTag001
To: sut <sip:14040000022@172.16.4.77>;tag=lc549823236
Call-ID: 1-2690@172.16.4.41
CSeq: 1 INVITE
Server: Mediant SW/v.6.80A.216.008
Content-Length: 0
```

3. SIP INVITE from SBC to NexOSS-FC

P-Source-Device header has been added to SIP INVITE

```
10d:3h:8m:2s INVITE sip:14040000022@172.16.4.77 SIP/2.0
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac553199308
Max-Forwards: 10
From: sipp <sip:1234567890@172.16.4.41>;tag=lc552885972
To: sut <sip:14040000022@172.16.4.77>
Call-ID: 5528631081032015382@172.16.4.77
CSeq: 1 INVITE
Contact: <sip:1234567890@172.16.4.77:5070>
User-Agent: Mediant SW/v.6.80A.216.008
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 133
P-Source-Device: 172.16.4.41:5060
```

```
v=0
o=user1 552761828 552761732 IN IP4 172.16.4.77
s=-
```

```
c=IN IP4 172.16.4.77
t=0 0
m=audio 6000 RTP/AVP 8
a=rtpmap:8 PCMA/8000
```

4. SIP 100 Trying from NexOSS-FC to SBC

```
10d:3h:8m:2s SIP/2.0 100 Trying
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac553199308
From: sipp <sip:1234567890@172.16.4.41>;tag=1c552885972
To: sut <sip:14040000022@172.16.4.77>
Call-ID: 5528631081032015382@172.16.4.77
CSeq: 1 INVITE
Server: OpenSIPS (1.8.2-notls (x86_64/linux))
Content-Length: 0
```

5. SIP 300 Redirect from NexOSS-FC to SBC

```
10d:3h:8m:2s SIP/2.0 300 Redirect
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac553199308
From: sipp <sip:1234567890@172.16.4.41>;tag=1c552885972
To: sut <sip:14040000022@172.16.4.77>;tag=7cb6f5a1787856c92fdb341051634cd0.880d
Call-ID: 5528631081032015382@172.16.4.77
CSeq: 1 INVITE
Contact: <sip:14040000022@172.16.4.47>
Server: OpenSIPS (1.8.2-notls (x86_64/linux))
Content-Length: 0
```

6. SIP ACK from SBC to NexOSS-FC

```
10d:3h:8m:2s ACK sip:14040000022@172.16.4.77 SIP/2.0
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac553199308
Max-Forwards: 10
From: sipp <sip:1234567890@172.16.4.41>;tag=1c552885972
To: sut <sip:14040000022@172.16.4.77>;tag=7cb6f5a1787856c92fdb341051634cd0.880d
Call-ID: 5528631081032015382@172.16.4.77
CSeq: 1 ACK
Contact: <sip:1234567890@172.16.4.77:5070>
User-Agent: Mediant SW/v.6.80A.216.008
Content-Length: 0
```

7. SIP INVITE from SBC to Destination

P-Source-Device is not included in INVITE message.

```
10d:3h:8m:2s INVITE sip:14040000022@172.16.4.47 SIP/2.0
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac618660440
Max-Forwards: 10
From: sipp <sip:1234567890@172.16.4.41>;tag=1c618504784
To: <sip:14040000022@172.16.4.47>
Call-ID: 6184808001032015382@172.16.4.77
CSeq: 1 INVITE
Contact: <sip:1234567890@172.16.4.77:5070>
User-Agent: Mediant SW/v.6.80A.216.008
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 167

v=0
o=user1 618368408 618368312 IN IP4 172.16.4.77
s=-
c=IN IP4 172.16.4.77
t=0 0
m=audio 6020 RTP/AVP 8
```

```
c=IN IP4 172.16.4.77  
a=ptime:20  
a=rtpmap:8 PCMA/8000
```

8. SIP 408 Request Timeout from SBC to Source

```
10d:3h:8m:3s (      lgr_flow)(      1764) ---- Outgoing SIP Message to  
172.16.4.41:5060 from SIPInterface #1 UdpTransportObject(#1) ----  
  
10d:3h:8m:3s SIP/2.0 408 Request Timeout  
Via: SIP/2.0/UDP 172.16.4.41:5060;branch=z9hG4bK-2690-1-0  
From: sipp <sip:1234567890@172.16.4.41>;tag=2690SIPpTag001  
To: sut <sip:14040000022@172.16.4.77>;tag=1c549823236  
Call-ID: 1-2690@172.16.4.41  
CSeq: 1 INVITE  
Server: Mediant SW/v.6.80A.216.008  
Content-Length: 0
```

9. SIP ACK from Source to SBC

```
10d:3h:8m:3s (      lgr_flow)(      1776) ---- Incoming SIP Message from  
172.16.4.41:5060 to SIPInterface #1 UdpTransportObject(#1) ----  
  
10d:3h:8m:3s ACK sip:14040000022@172.16.4.77 SIP/2.0  
Via: SIP/2.0/UDP 172.16.4.41:5060;branch=z9hG4bK-2690-1-0  
From: sipp <sip:1234567890@172.16.4.41>;tag=2690SIPpTag001  
To: sut <sip:14040000022@172.16.4.77>;tag=1c549823236  
Call-ID: 1-2690@172.16.4.41  
CSeq: 1 ACK  
Contact: <sip:sipp@172.16.4.41:5060;transport=UDP>  
Max-Forwards: 70  
Subject: Performance Test  
Content-Length: 0
```

5.3 No Fraud Detected - SBC Routes Call - 404 Not Found

The following SBC log documents the SIP messages for the test case when no fraud is detected. NexOSS-FC will return a SIP 404 message to the SBC. The SBC should route the call to the next destination in its local routing policy.

1. SIP INVITE from Source to SBC.

```
19d:2h:28m:37s INVITE sip:14040000027@172.16.4.77:5060 SIP/2.0  
Via: SIP/2.0/UDP 172.16.4.41:5060;branch=z9hG4bK-9135-1-0  
From: sipp <sip:1234567890@172.16.4.41:5060>;tag=9135SIPpTag001  
To: sut <sip:14040000027@172.16.4.77:5060>  
Call-ID: 1-9135@172.16.4.41  
CSeq: 1 INVITE  
Contact: sip:1234567890@172.16.4.41:5060  
Max-Forwards: 70  
Subject: Performance Test  
Content-Type: application/sdp  
Content-Length: 133  
  
v=0  
o=user1 53655765 2353687637 IN IP4 172.16.4.41  
s=-  
c=IN IP4 172.16.4.41  
t=0 0  
m=audio 6000 RTP/AVP 8  
a=rtpmap:8 PCMA/8000
```

2. SIP 100 Trying from SBC to Source

```
19d:2h:28m:37s SIP/2.0 100 Trying
Via: SIP/2.0/UDP 172.16.4.41:5060;branch=z9hG4bK-9135-1-0
From: sipp <sip:1234567890@172.16.4.41>;tag=9135SIPpTag001
To: sut <sip:14040000027@172.16.4.77>;tag=1c513360168
Call-ID: 1-9135@172.16.4.41
CSeq: 1 INVITE
Server: Mediant SW/v.6.80A.216.008
Content-Length: 0
```

3. SIP INVITE from SBC to NexOSS-FC

P-Source-Device header has been added to SIP INVITE

```
19d:2h:28m:37s INVITE sip:14040000027@172.16.4.77 SIP/2.0
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac516092414
Max-Forwards: 10
From: sipp <sip:1234567890@172.16.4.41>;tag=1c515905990
To: sut <sip:14040000027@172.16.4.77>
Call-ID: 515881014193201522837@172.16.4.77
CSeq: 1 INVITE
Contact: <sip:1234567890@172.16.4.77:5070>
User-Agent: Mediant SW/v.6.80A.216.008
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 133
P-Source-Device: 172.16.4.41:5060
```

```
v=0
o=user1 515777518 515777422 IN IP4 172.16.4.77
s=-
c=IN IP4 172.16.4.77
t=0 0
m=audio 6010 RTP/AVP 8
a=rtpmap:8 PCMA/8000
```

4. SIP 100 Trying from NexOSS-FC to SBC

```
19d:2h:28m:37s SIP/2.0 100 Trying
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac516092414
From: sipp <sip:1234567890@172.16.4.41>;tag=1c515905990
To: sut <sip:14040000027@172.16.4.77>
Call-ID: 515881014193201522837@172.16.4.77
CSeq: 1 INVITE
Server: OpenSIPS (1.8.2-notls (x86_64/linux))
Content-Length: 0
```

5. SIP 404 Not Found from NexOSS-FC to SBC

```
19d:2h:28m:37s SIP/2.0 404 Route Not Found
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac516092414
From: sipp <sip:1234567890@172.16.4.41>;tag=1c515905990
To: sut <sip:14040000027@172.16.4.77>;tag=7cb6f5a1787856c92fdb341051634cd0.a7da
Call-ID: 515881014193201522837@172.16.4.77
CSeq: 1 INVITE
Server: OpenSIPS (1.8.2-notls (x86_64/linux))
Content-Length: 0
```

6. SIP ACK from SBC to NexOSS-FC

```
19d:2h:28m:37s ACK sip:14040000027@172.16.4.77 SIP/2.0
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac516092414
Max-Forwards: 10
```

```

From: sipp <sip:1234567890@172.16.4.41>;tag=lc515905990
To: sut <sip:14040000027@172.16.4.77>;tag=7cb6f5a1787856c92fdb341051634cd0.a7da
Call-ID: 515881014193201522837@172.16.4.77
CSeq: 1 ACK
Contact: <sip:1234567890@172.16.4.77:5070>
User-Agent: Mediant SW/v.6.80A.216.008
Content-Length: 0

```

7. SIP INVITE from SBC to Destination

P-Source-Device is not included in INVITE message.

```

19d:2h:28m:37s INVITE sip:14040000027@172.16.4.77 SIP/2.0
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac580612558
Max-Forwards: 10
From: sipp <sip:1234567890@172.16.4.41>;tag=lc580444678
To: sut <sip:14040000027@172.16.4.77>
Call-ID: 580419470193201522837@172.16.4.77
CSeq: 1 INVITE
Contact: <sip:1234567890@172.16.4.77:5070>
User-Agent: Mediant SW/v.6.80A.216.008
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 167

v=0
o=user1 580311606 580311518 IN IP4 172.16.4.77
s=
c=IN IP4 172.16.4.77
t=0 0
m=audio 6000 RTP/AVP 8
c=IN IP4 172.16.4.77
a=rtpmap:8 PCMA/8000

```

8. SIP 180 Ringing from Destination to SBC

```

19d:2h:28m:37s SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac580612558
From: sipp <sip:1234567890@172.16.4.41>;tag=lc580444678
To: sut <sip:14040000027@172.16.4.77>;tag=5876SIPpTag012914244
Call-ID: 580419470193201522837@172.16.4.77
CSeq: 1 INVITE
Contact: <sip:172.16.4.56:5060;transport=UDP>
Content-Length: 0

```

9. SIP 180 Ringing from SBC to Source

```

19d:2h:28m:37s SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 172.16.4.41:5060;branch=z9hG4bK-9135-1-0
From: sipp <sip:1234567890@172.16.4.41>;tag=9135SIPpTag001
To: sut <sip:14040000027@172.16.4.77>;tag=lc513360168
Call-ID: 1-9135@172.16.4.41
CSeq: 1 INVITE
Contact: <sip:172.16.4.77:5060>
Server: Mediant SW/v.6.80A.216.008
Content-Length: 0

```

10. SIP 200 OK from Destination to SBC

```

19d:2h:28m:37s SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac580612558
From: sipp <sip:1234567890@172.16.4.41>;tag=lc580444678
To: sut <sip:14040000027@172.16.4.77>;tag=5876SIPpTag012914244

```

```

Call-ID: 580419470193201522837@172.16.4.77
CSeq: 1 INVITE
Contact: <sip:172.16.4.56:5060;transport=UDP>
Content-Type: application/sdp
Content-Length: 133

v=0
o=user1 53655765 2353687637 IN IP4 172.16.4.56
s=-
c=IN IP4 172.16.4.56
t=0 0
m=audio 6000 RTP/AVP 8
a=rtpmap:8 PCMA/8000

```

11. SIP ACK from SBC to Destination

```

19d:2h:28m:37s ACK sip:172.16.4.56:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac706049854
Max-Forwards: 10
From: sipp <sip:1234567890@172.16.4.41>;tag=1c580444678
To: sut <sip:14040000027@172.16.4.77>;tag=5876SIPpTag012914244
Call-ID: 580419470193201522837@172.16.4.77
CSeq: 1 ACK
Contact: <sip:1234567890@172.16.4.77:5070>
User-Agent: Mediant SW/v.6.80A.216.008
Content-Length: 0

```

12. SIP BYE from SBC to Destination

```

19d:2h:28m:37s BYE sip:172.16.4.56:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac706526182
Max-Forwards: 10
From: sipp <sip:1234567890@172.16.4.41>;tag=1c580444678
To: sut <sip:14040000027@172.16.4.77>;tag=5876SIPpTag012914244
Call-ID: 580419470193201522837@172.16.4.77
CSeq: 2 BYE
User-Agent: Mediant SW/v.6.80A.216.008
Reason: SIP ;cause=488 ;text="488 Not Acceptable Here"
Content-Length: 0

```

13. SIP 488 Not Acceptable from SBC to Source

```

19d:2h:28m:37s SIP/2.0 488 Not Acceptable Here
Via: SIP/2.0/UDP 172.16.4.41:5060;branch=z9hG4bK-9135-1-0
From: sipp <sip:1234567890@172.16.4.41>;tag=9135SIPpTag001
To: sut <sip:14040000027@172.16.4.77>;tag=1c513360168
Call-ID: 1-9135@172.16.4.41
CSeq: 1 INVITE
Server: Mediant SW/v.6.80A.216.008
Reason: SIP ;cause=488 ;text="488 Not Acceptable Here"
Content-Length: 0

```

14. SIP ACK from Source to SBC

```

19d:2h:28m:37s ACK sip:14040000027@172.16.4.77 SIP/2.0
Via: SIP/2.0/UDP 172.16.4.41:5060;branch=z9hG4bK-9135-1-0
From: sipp <sip:1234567890@172.16.4.41>;tag=9135SIPpTag001
To: sut <sip:14040000027@172.16.4.77>;tag=1c513360168
Call-ID: 1-9135@172.16.4.41
CSeq: 1 ACK
Contact: <sip:sipp@172.16.4.41:5060;transport=UDP>
Max-Forwards: 70
Subject: Performance Test

```

Content-Length: 0

15. SIP 200 OK from Destination to SBC

```
19d:2h:28m:37s SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.16.4.77:5070;branch=z9hG4bKac706526182
From: sipp <sip:1234567890@172.16.4.41>;tag=1c580444678
To: sut <sip:14040000027@172.16.4.77>;tag=5876SIPpTag012914244
Call-ID: 580419470193201522837@172.16.4.77
CSeq: 2 BYE
Contact: <sip:172.16.4.56:5060;transport=UDP>
Content-Length: 0
```