Business Talk & BTIP
For IPBX Unify OpenScape Voice and Unify OpenScape Branch

Versions addressed in this guide: OpenScape Voice V9R4 with OpenScape Branch V9R4 & OpenScape Voice V9 R1

Information included in this document is dedicated to customer equipment (IPBX, TOIP ecosystems) connection to Business Talk IP service: it shall not be used for other goals or in another context.

Document Version

Version of 23/09/2019

1. Table of Contents

2. Goal of this document

The aim of this document is to list technical requirements to ensure the interoperability between Unify OpenScape Voice IPBX with Orange Business Services Business Talk / Business Talk IP SIP services, hereafter so-called “service”.

3. OpenScape Voice V9R4 & OpenScape Branch V9R4

3.1. Architecture overview

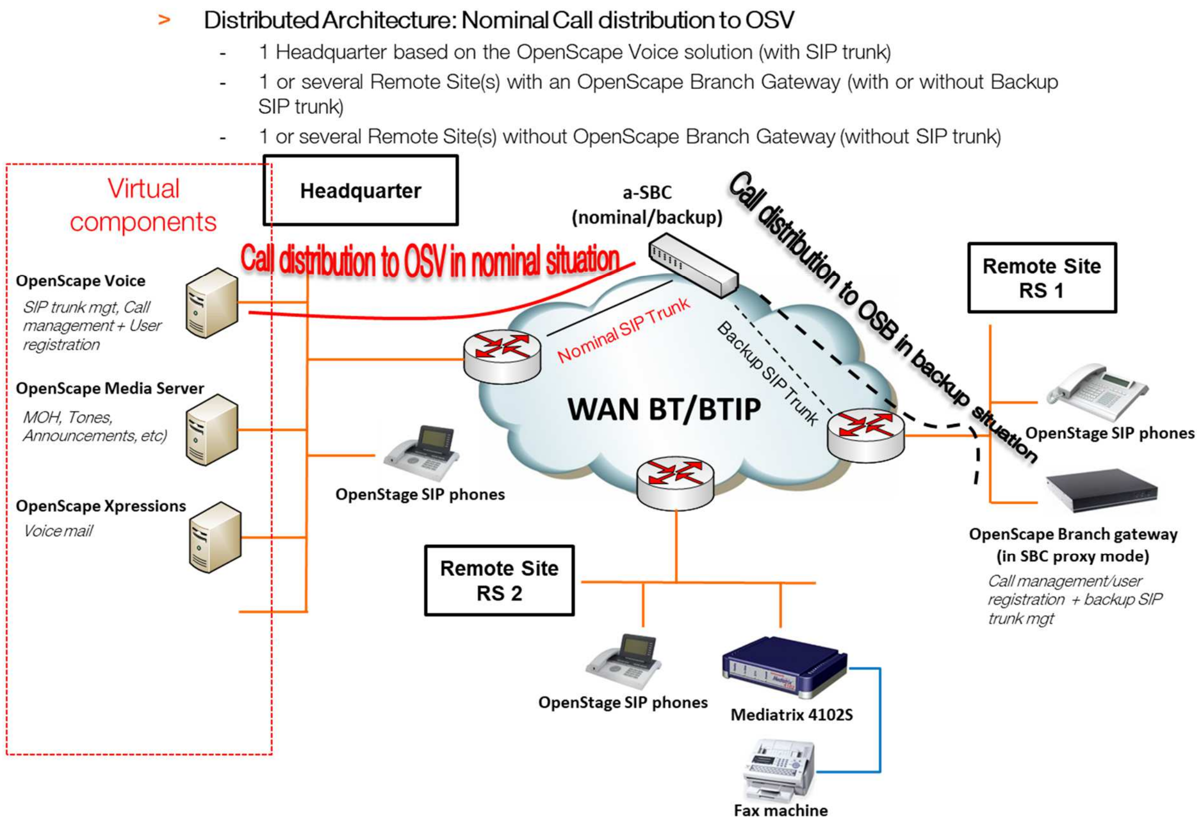
Access to BT/BTIP service required to be connected to 2 Orange a-SBC platforms (nominal and backup platforms).

In nominal situation, call distribution is performed to OpenScape Voice (OSV) solution connected via SIP trunks to Orange infrastructure (§3.1.1).

For remote sites equipped with OpenScape Branch (OSB) configured in SBC proxy mode, call distribution can be directly performed to Orange infrastructure via backup SIP trunks when connection with OSV is lost. Thus OSB runs in survivability mode (§3.1.1).

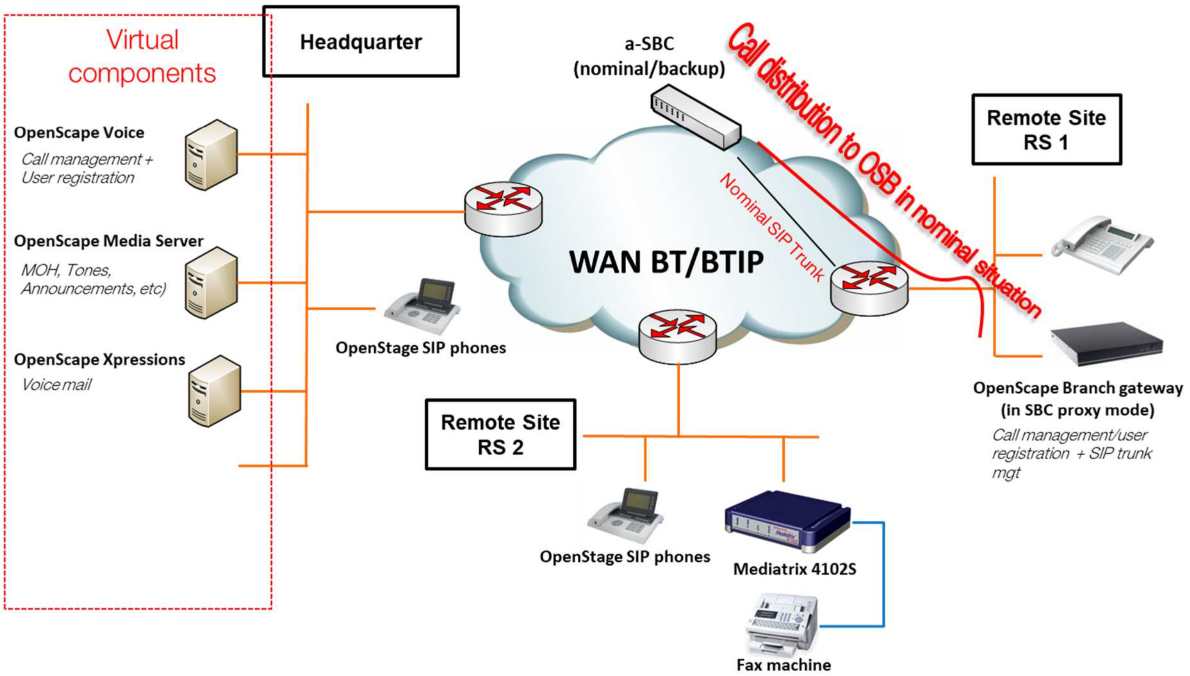
In nominal situation, local call distribution can be also performed to OSB solution (configured in SBC proxy mode) via local SIP trunks connected to Orange a-SBC. In this architecture, OSV platform is usually not connected to Orange a-SBC and OSB runs in nominal mode (§3.1.2).

3.1.1. Distributed architecture: Nominal call distribution to OSV



3.1.2. Distributed architecture: Nominal local call distribution to OSB

> Distributed Architecture: Nominal local distribution to OSB
  - 1 Headquarter based on the OpenScape Voice solution (without SIP trunk)
  - 1 or several Remote Site(s) with an OpenScape Branch Gateway (with SIP trunk)
  - 1 or several Remote Site(s) without OpenScape Branch Gateway (without SIP trunk)



3.2. Sizing consideration

Specific sizing approach has to be considered with OSV/OSB solution due to the fact that:

- In nominal situation, phones located on remote sites with OSB in SBC proxy mode register both to OSB but also to OSV. Consequently for calls from or to these phones, the SIP signaling flow is routed via OSB to OSV and back to OSB.
- OSB in nominal or survivability mode anchors systematically the RTP flow for calls to/from Orange a-SBC. Therefore, the RTP flow is not direct between Unify phones and Orange a-SBC.

3.3. Resiliency consideration

OSV consists in co-located two-nodes cluster in active-backup mode.

Switchover between the active OSV node to the second node in case of a failure is done by a monitoring process named *Survival Authority* on an external server.

Same resiliency also exists for OSB.

3.4. CAC & Codec consideration

G729 codec usage is not supported in the scope of Unify OSV or OSB SIP trunking interoperability with Orange Business Services. Only G711a codec is supported.

Configuration of Internal CAC solution in Openscape Voice is required to restrict only G711A 20ms Voice codec. Refer to 3.8.Annex 1 « CAC management rules on OpenScape Voice system » for more information.

3.5. Parameters to be provided by customer to access BT/BTIP service

IP addresses marked in red have to be indicated by the Customer, depending on Customer architecture scenario.

Head Quarter (HQ) architecture	Level of Service	Customer IP addresses used by the service	
		Nominal	Backup
OSV - Local redundancy-Duplex integration	Local redundancy: two OSV servers in a redundant two-node cluster that executes in an active-standby mode and sharing the same IP@.	VIP@	N/A
2 OSV servers (active/active) - 2 NUMBERING PLANS 2 OSV servers (active/active) hosted by 2 different physical sites. Local redundancy (Duplex integration) possible on each physical sites Each OSV server manages a range of users (2 numbering plans). Each OSV server (OSV1 and OSV2) has its own SIP trunk and each manages its own group of users in nominal mode. - Nominal mode: All HQ1 users register with OSV1 HQ1 All HQ2 users register with OSV2 HQ2 - Backup mode: In case of OSV1 HQ1 crash, all HQ1 users re-register onto OSV2 HQ2 In case of OSV2 HQ2 crash, all HQ2 users re-register with OSV1 HQ1 warnings: - Both HQ accesses capacity to be sized adequately	**For OSV1 HQ1** User registration redundancy (IP phones only) Rerouting at AS level	OSV1 HQ1 IP@ or OSV1 HQ1 VIP@ (if duplex integration)	N/A
	For OSV2 HQ2 User registration redundancy (IP phones only) Rerouting at AS level	OSV1 HQ2 IP@ or OSV2 HQ2 VIP@ (if duplex integration)	N/A
OSB (in SBC proxy mode) - Local redundancy-Duplex integration In this configuration, the OSBranch servers are connected to OSV servers but only the OSBranch servers are connected to Orange infrastructure via local SIP trunks	Local redundancy: two OSB servers in a redundant mode and sharing the same IP@.	VIP@	N/A

Remote Site (RS) architecture – OSV Local redundancy	Level of Service	Customer IP addresses used by the service	
		Nominal	Backup
Remote site with OpenScape Branch gateway	Local user survivability, trunk redundancy via PSTN only	N/A	N/A
Remote site with OpenScape Branch gateway (in SBC proxy mode) + SIP trunk as backup	Local survivability for the remote site hosting the OSB/SIP Trunk in case of non-access to HQ (OSV crash) Nominal outgoing and incoming traffic goes through HQ	OSB VIP@	N/A
Remote site without media gateway	No survivability, no trunk redundancy	N/A	N/A

Remote Site (RS) architecture - 2 OSV servers (active/active)	Level of Service	Customer IP addresses used by the service	
		Nominal	Backup
Remote site with OpenScape Branch gateway	Local user survivability, trunk redundancy via PSTN only	N/A	N/A
Remote site with OpenScape Branch gateway + SIP trunk as backup	Local survivability for the remote site hosting the OSB/SIP Trunk in case of non-access to HQ (OSV crash) Nominal outgoing and incoming traffic goes through HQ	OSB VIP@	N/A
Remote site without media gateway	No survivability, no trunk redundancy	N/A	N/A

3.6. Business Talk & BTIP certified versions

To get more details about the versions supported by Unify, Unify product Lifecycle notifications can be provided via Unify's standard communication channels (e.g. account teams, partner portal).

3.6.1. Unify OpenScape Voice/Branch IPBX

Unify OpenScape Voice / Branch IPBX – software versions			
Reference product	Software version	Certification ✓: Certified NS : No supported	Restrictions/Comments
OpenScape Voice software	V9R4.39.3	✓	User-Agent header contains: OpenScape Voice V9R4
OpenScape Branch software	V9R4.11	✓	User-Agent header contains: OpenScape-Branch-V9R4

3.6.2. Unify OpenScape Voice/Branch endpoints and applications

Unify OpenScape Voice / Branch IBX - Endpoints and applications					
Reference product		Software version NA: not applicable	Certification ✓: Certified NS : No supported	OSV version / OSB version	Restrictions/Comments
SIP endpoints	OpenStage SIP 15, 20, 40, 60, 80	V3 R5.13.0	✓	V9R4.39.3/ V9R4.11	
Unify Gateway	OpenScape Branch	V9R4.11	✓	V9R4.39.3/ V9R4.11	
Voice Mail	OpenScape Xpressions	V7 R1.5.0	✓	V9R4.39.3/ V9R4.11	
Third party Gateway	Mediatrix 4102S	Dgw 42.2.954	✓	V9R4.39.3/ V9R4.11	
Analog Fax	Connected to Mediatrix 4102S	NA	✓	V9R4.39.3/ V9R4.11	Only T.38 protocol is supported for FAX.

3.7. SIP trunking configuration checklist

Refer to the document written by Unify, in sections 3.10 and 4.9 of this document.

For the configuration of OpenScape Voice V9R4, the Unify document in section 4.9 has to be considered. The Unify document in section 3.10 describes the OpenScape Branch V9R4 configuration to ensure the interoperability with Orange Business Services.

3.8. CAC management rules on OpenScape Voice system

See paragraph 3.8.

3.9. Configuration of OpenScape Voice V9R4 and OpenScape Branch V9R4 with Orange Business Services SIP Trunk

OpenScape Voice V9R4

OpenScape Branch V9R4

Configuration of OpenScape Voice V9R4 and OpenScape Branch V9R4 with Orange Business Services SIP Trunk

Version 1.1– 11th July 2019

Table of Contents

1. Goal of this document

This document describes the Unify OpenScape Voice V9R4 and OpenScape Branch V9R4 configuration to ensure the interoperability with Orange Business Services.

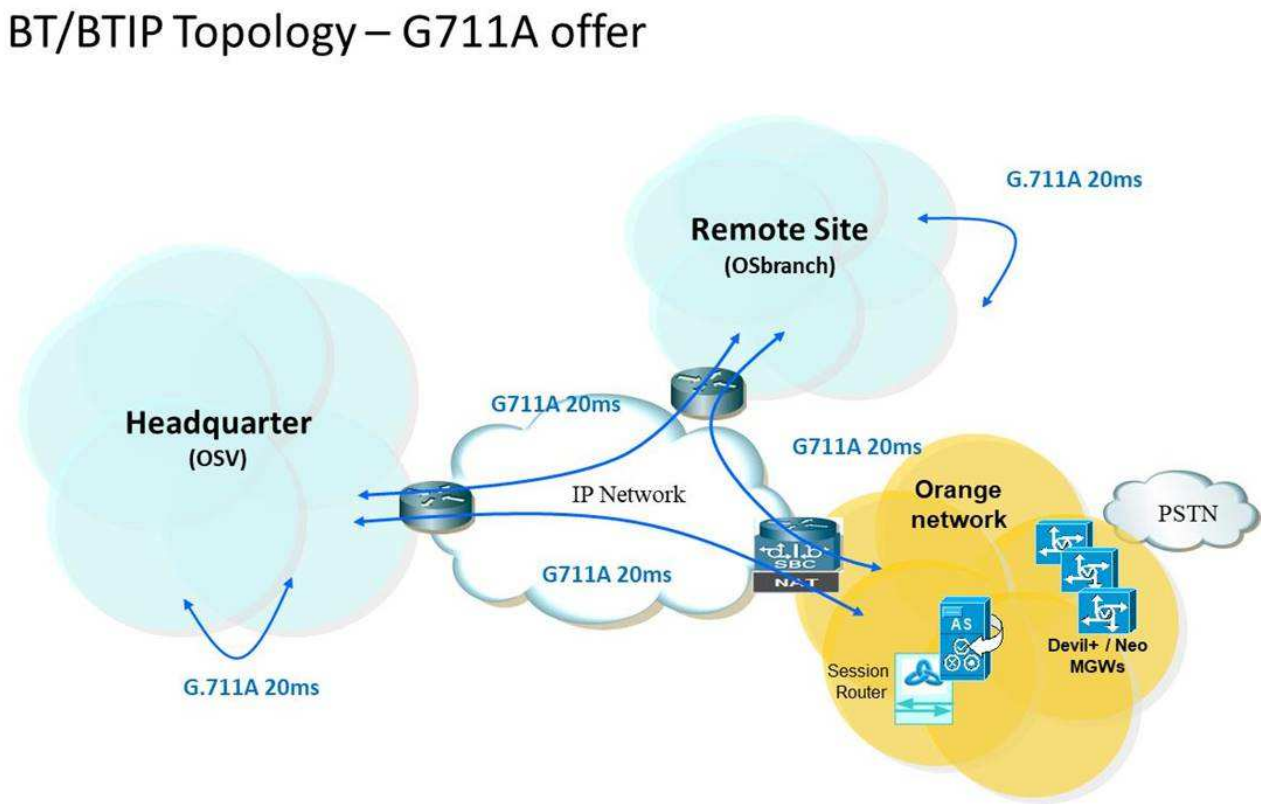
2. Certified Hardware and Software

The table below show the tested versions:

Device	**SW / Release**
OpenScape Voice, virtualized	V9 R4.39.3
OpenScape Branch, virtualized SBC Proxy mode	Tested: V9 R4.09.02 Release to be Orange compatible: V9R4.11
OpenStage SIP phone	V3 R5.13.0

3. Customer Network Topology

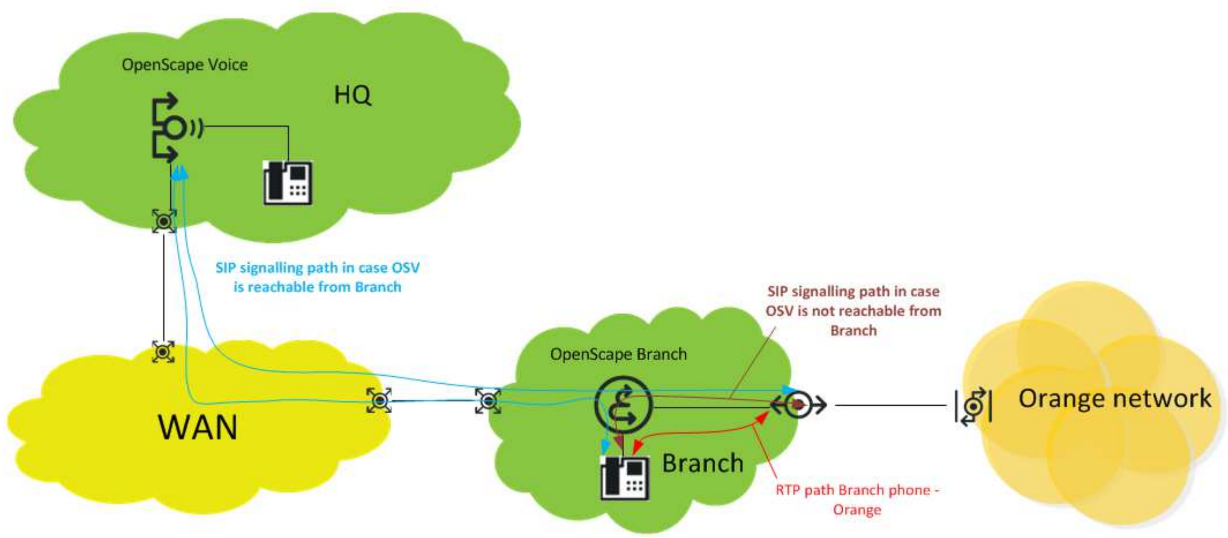
The figure below shows the connection between the Orange network, the customer's headquarter and a customer's remote site. The customer's headquarter and his remote sites are connected also via Orange network.
Orange doesn't want a codec change without codec renegotiation. Therefore G711A should be configured as one and only codec to be supported by OS Branch because OS Branch cannot select only one codec in its SDP answer.



Call routing on OS Branch is as follows. The phone is registered via OS Branch with OS Voice so the phone is registered with both servers.

- <u>OS Branch Nominal Mode (NM)</u>
  OS Branch has a connection to OS Voice. Calls from or to the phone are routed via OS Branch to OS Voice and back to OS Branch.
- <u>OS Branch Survival Mode (SM)</u>
  OS Branch has no connection to OS Voice. OS Branch connects directly the Orange SBC and the phone.

Calls from testlab to Orange network when OSV is/is not reachable

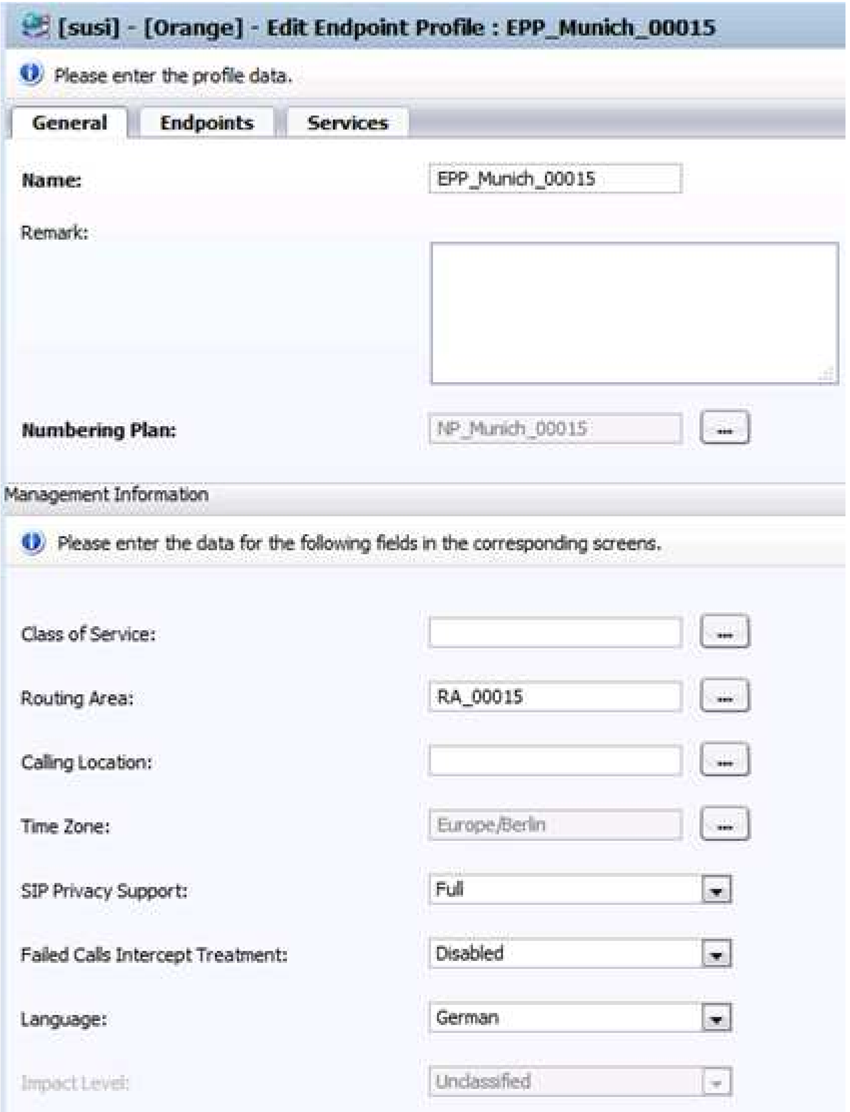


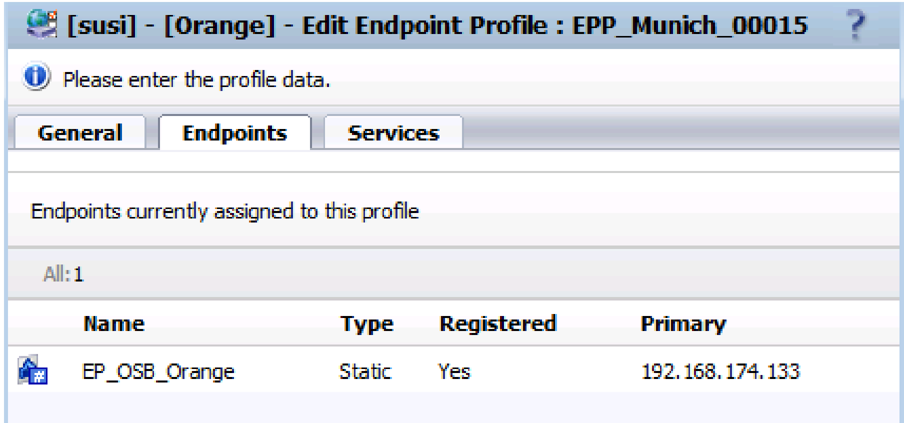
4. Configuration of the SIP Devices

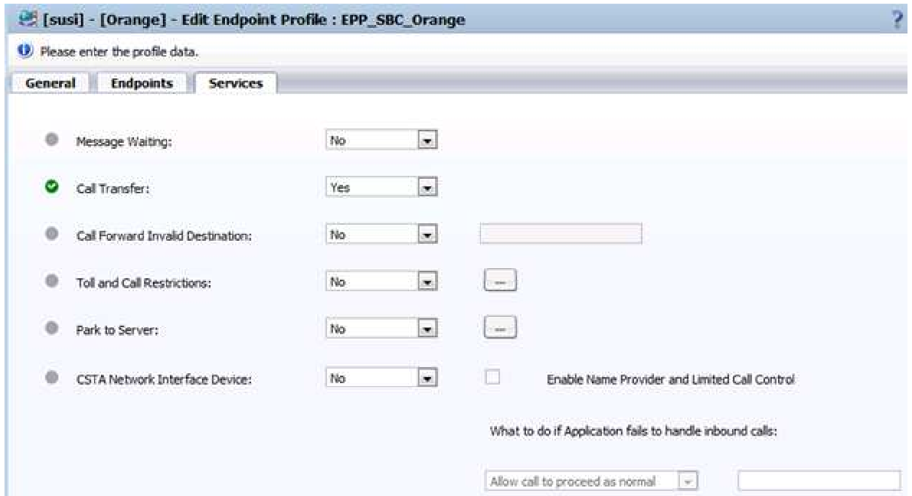
4.1. Configuration of OpenScape Voice

The following describes the configuration of OpenScape Voice for the Orange Business Services SIP Trunk compliancy. OpenScape Voice has been installed and configured based on the OpenScape Voice Installation and Configuration Guide. Additionally an Orange Branch endpoint and endpoint profile configuration is required.

4.1.1. OpenScape Branch Endpoint Profile Configuration

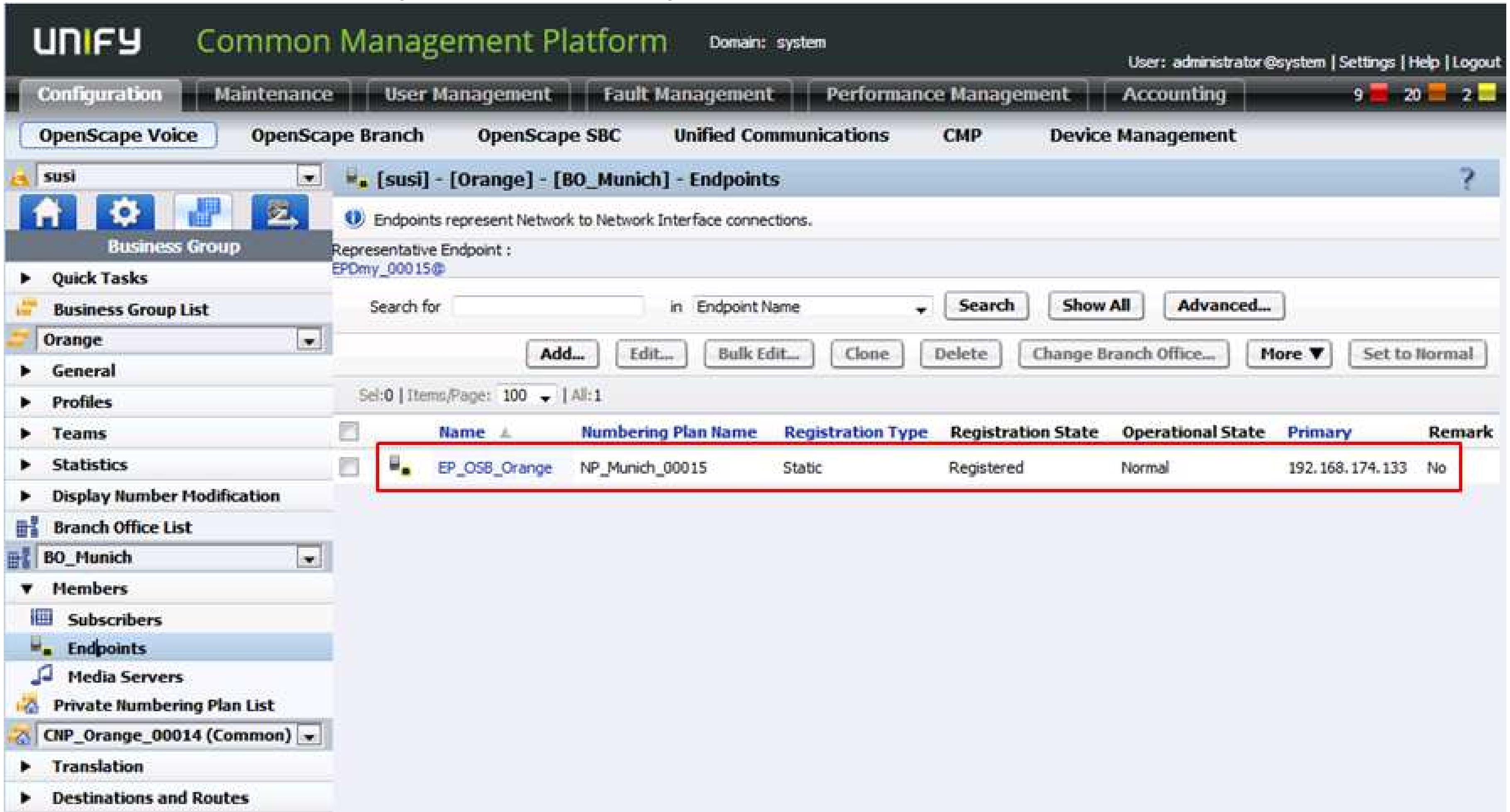




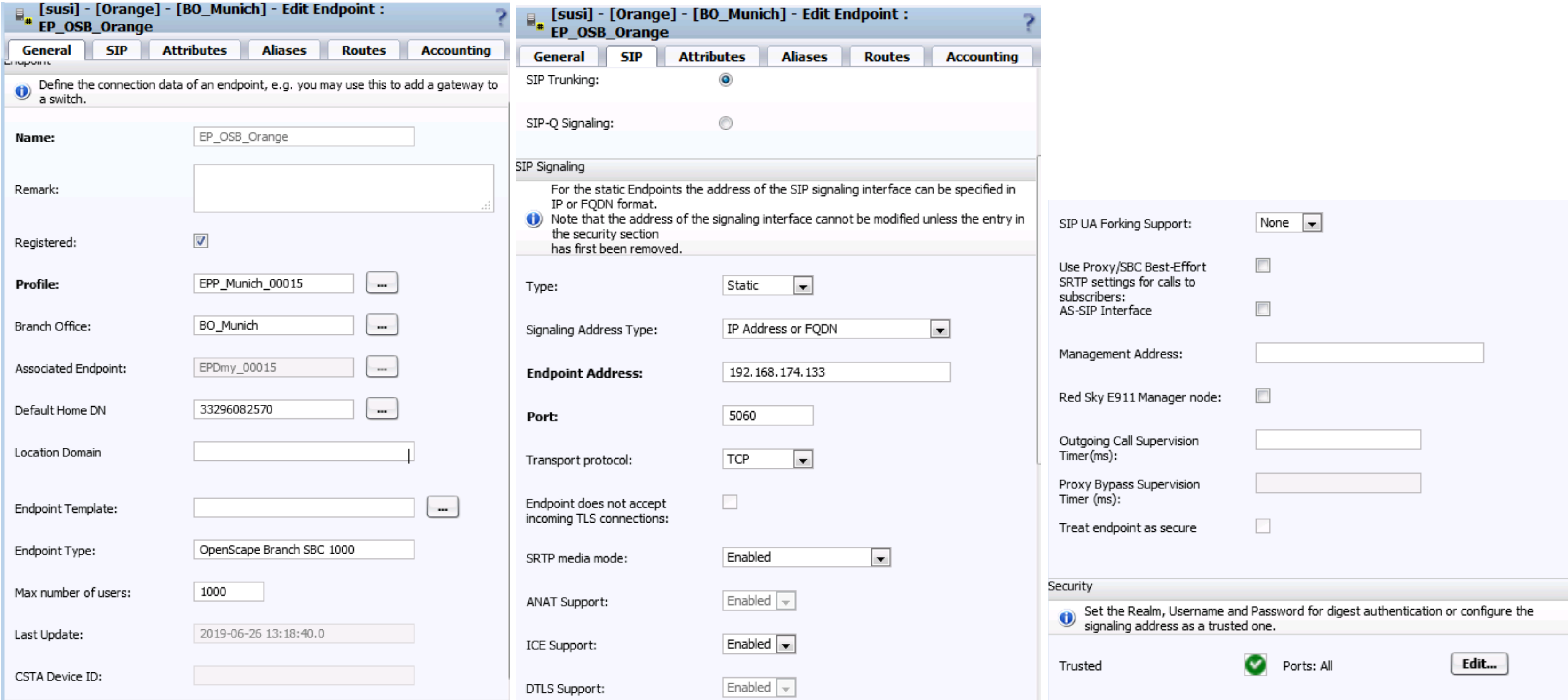


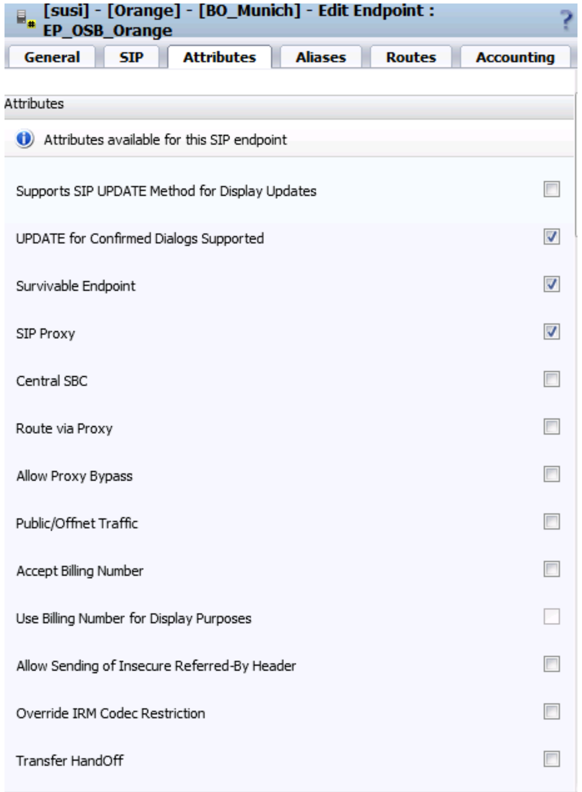
4.1.2. OpenScape Branch Endpoint Configuration

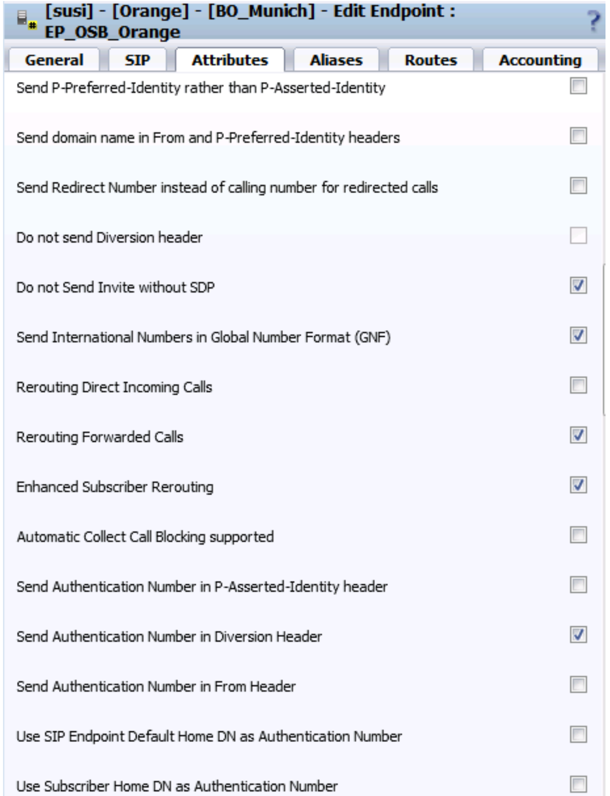
The OpenScape Branch endpoint is configured in the Common Management Platform in the Business Group area:

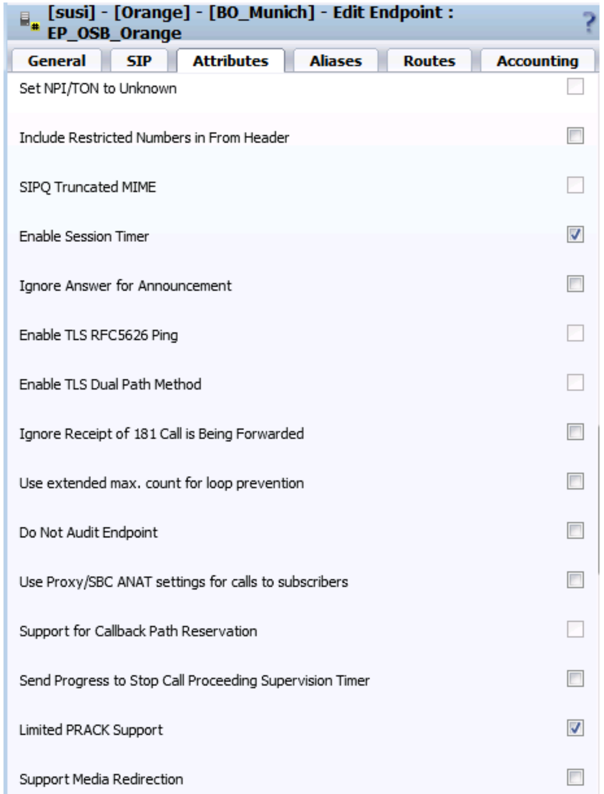


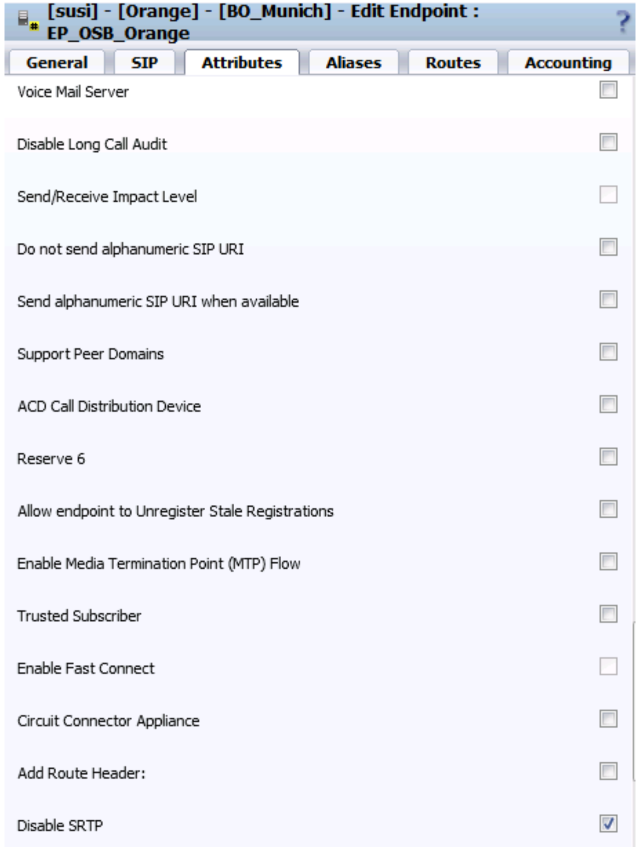
Below is shown the configuration of the OpenScape Branch endpoint for the virtual LAN IP:

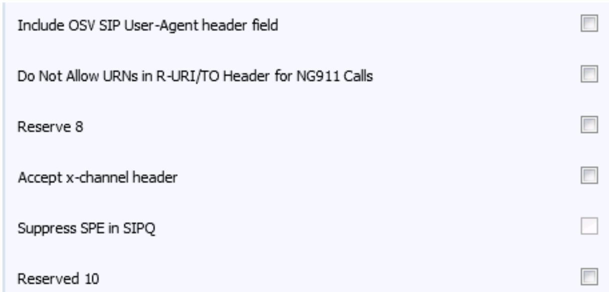

[susi] - [Orange] - [BO_Munich] - Edit Endpoint : EP_OSB_Orange
General
SIP
Attributes
Aliases
Routes
Accounting
Define the connection data of an endpoint, e.g. you may use this to add a gateway to a switch.
Name: EP_OSB_Orange
Remark:
Registered:
Profile: EPP_Munich_00015
Branch Office: BO_Munich
Associated Endpoint: EPDmy_00015
Default Home DN 33296082570
Location Domain
Endpoint Template:
Endpoint Type: OpenScape Branch SBC 1000
Max number of users: 1000
Last Update: 2019-06-26 13:18:40.0
CSTA Device ID:
[susi] - [Orange] - [BO_Munich] - Edit Endpoint : EP_OSB_Orange
SIP Trunking:
SIP-Q Signaling:
SIP Signaling
For the static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format.
Note that the address of the signaling interface cannot be modified unless the entry in the security section
has first been removed.
Type: Static
Signaling Address Type: IP Address or FQDN
Endpoint Address: 192.168.174.133
Port: 5060
Transport protocol: TCP
Endpoint does not accept incoming TLS connections:
SRTP media mode: Enabled
ANAT Support: Enabled
ICE Support: Enabled
DTLS Support: Enabled
SIP UA Forking Support: None
Use Proxy/SBC Best-Effort SRTP settings for calls to subscribers:
AS-SIP Interface
Management Address:
Red Sky E911 Manager node:
Outgoing Call Supervision Timer(ms):
Proxy Bypass Supervision Timer (ms):
Treat endpoint as secure
Security
Set the Realm, Username and Password for digest authentication or configure the signaling address as a trusted one.
Trusted
Ports: All
Edit...

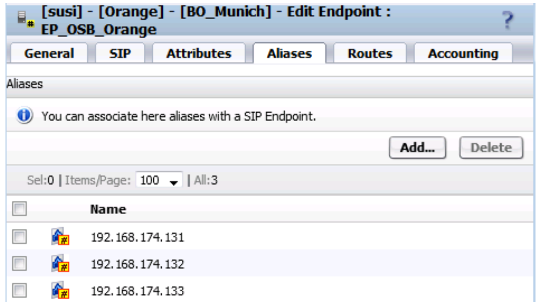

[susi] - [Orange] - [BO_Munich] - Edit Endpoint : EP_OSB_Orange
General
SIP
Attributes
Aliases
Routes
Accounting
Attributes
Attributes available for this SIP endpoint
Supports SIP UPDATE Method for Display Updates
UPDATE for Confirmed Dialogs Supported
Survivable Endpoint
SIP Proxy
Central SBC
Route via Proxy
Allow Proxy Bypass
Public/Offnet Traffic
Accept Billing Number
Use Billing Number for Display Purposes
Allow Sending of Insecure Referred-By Header
Override IRM Codec Restriction
Transfer HandOff


[susi] - [Orange] - [BO_Munich] - Edit Endpoint : EP_OSB_Orange
General
SIP
Attributes
Aliases
Routes
Accounting
Send P-Preferred-Identity rather than P-Asserted-Identity
Send domain name in From and P-Preferred-Identity headers
Send Redirect Number instead of calling number for redirected calls
Do not send Diversion header
Do not Send Invite without SDP
Send International Numbers in Global Number Format (GNF)
Rerouting Direct Incoming Calls
Rerouting Forwarded Calls
Enhanced Subscriber Rerouting
Automatic Collect Call Blocking supported
Send Authentication Number in P-Asserted-Identity header
Send Authentication Number in Diversion Header
Send Authentication Number in From Header
Use SIP Endpoint Default Home DN as Authentication Number
Use Subscriber Home DN as Authentication Number


[susi] - [Orange] - [BO_Munich] - Edit Endpoint : EP_OSB_Orange
General
SIP
Attributes
Aliases
Routes
Accounting
Set NPI/TON to Unknown
Include Restricted Numbers in From Header
SIPQ Truncated MIME
Enable Session Timer
Ignore Answer for Announcement
Enable TLS RFC5626 Ping
Enable TLS Dual Path Method
Ignore Receipt of 181 Call is Being Forwarded
Use extended max. count for loop prevention
Do Not Audit Endpoint
Use Proxy/SBC ANAT settings for calls to subscribers
Support for Callback Path Reservation
Send Progress to Stop Call Proceeding Supervision Timer
Limited PRACK Support
Support Media Redirection

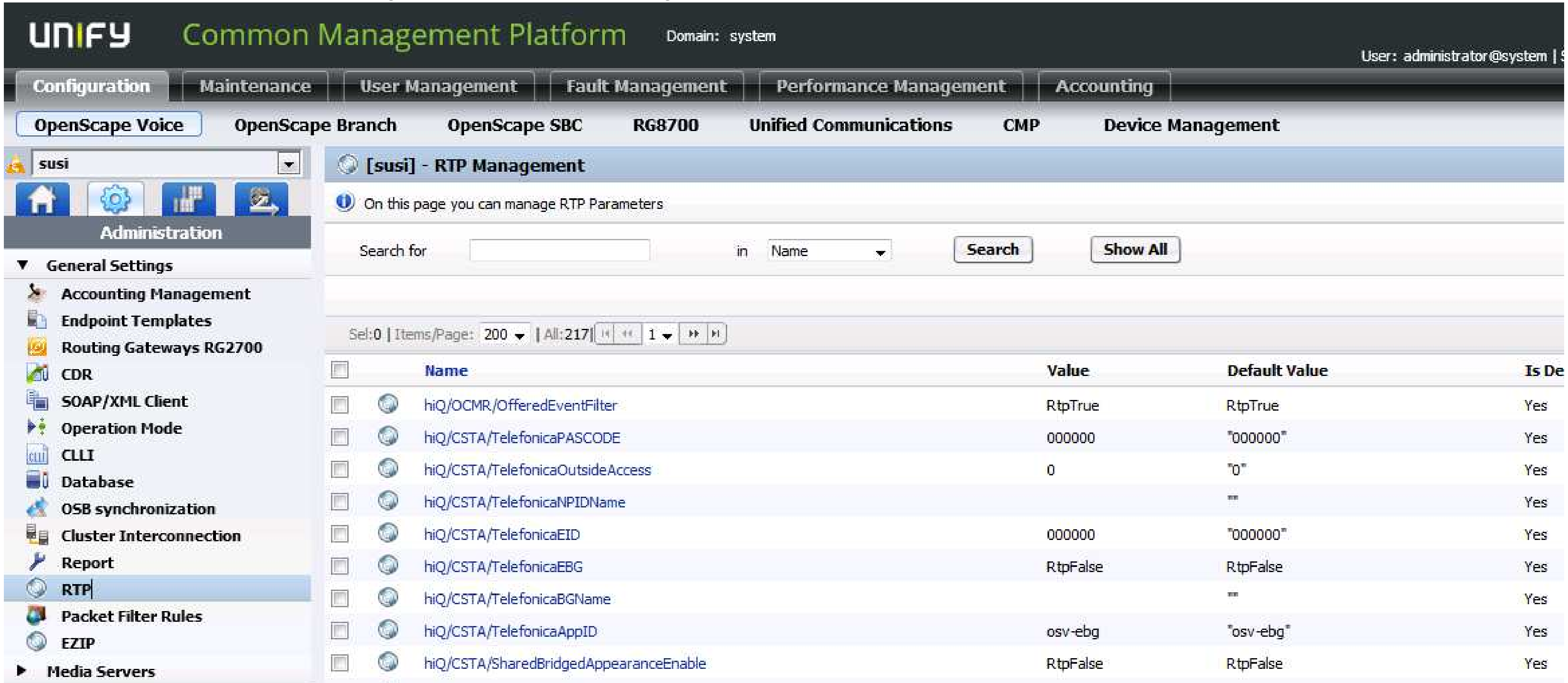

[susi] - [Orange] - [BO_Munich] - Edit Endpoint : EP_OSB_Orange
General
SIP
Attributes
Aliases
Routes
Accounting
Voice Mail Server
Disable Long Call Audit
Send/Receive Impact Level
Do not send alphanumeric SIP URI
Send alphanumeric SIP URI when available
Support Peer Domains
ACD Call Distribution Device
Reserve 6
Allow endpoint to Unregister Stale Registrations
Enable Media Termination Point (MTP) Flow
Trusted Subscriber
Enable Fast Connect
Circuit Connector Appliance
Add Route Header:
Disable SRTP


Include OSV SIP User-Agent header field
Do Not Allow URNs in R-URI/TO Header for NG911 Calls
Reserve 8
Accept x-channel header
Suppress SPE in SIPQ
Reserved 10


[susi] - [Orange] - [BO_Munich] - Edit Endpoint : EP_OSB_Orange
General
SIP
Attributes
Aliases
Routes
Accounting
Aliases
You can associate here aliases with a SIP Endpoint.
Add...
Delete
Sel:0 | Items/Page: 100 | All:3
Name
192.168.174.131
192.168.174.132
192.168.174.133

4.1.3. OpenScape Voice Resilient Telco Platform (RTP) Parameters

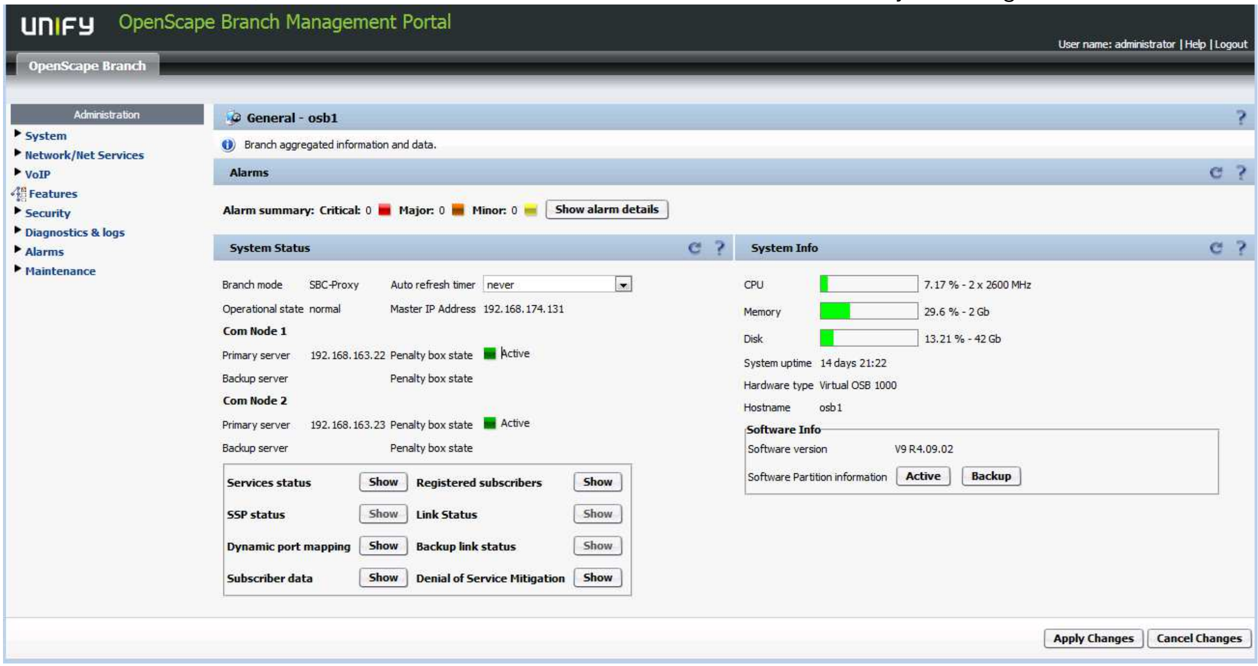
The required RTP parameters are configured in the Common Management Platform in the Administration area:



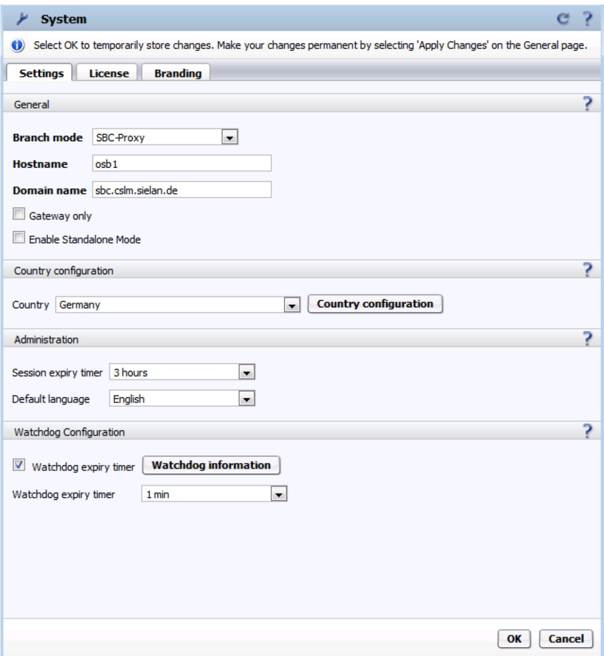
Parameter Name	Value	Description
Srx/Sip/Min_Session_Timer_Value	7101000	OSV will send a re-INVITE every 59.175 minutes (session refresh timer)
Srx/Sip/Session_Timer	ON	
Srx/Sip/sdpSessionMaintainer	RtpTrue	This parameter forces OSV to send the o-line value unchanged in SDP as received from the phone when set to RtpTrue.
Srx/Sip/IncludeOsvUserAgentVersionInfo	RtpTrue	This enables the inclusion of the OSV version in the User-Agent header when set to RtpTrue.

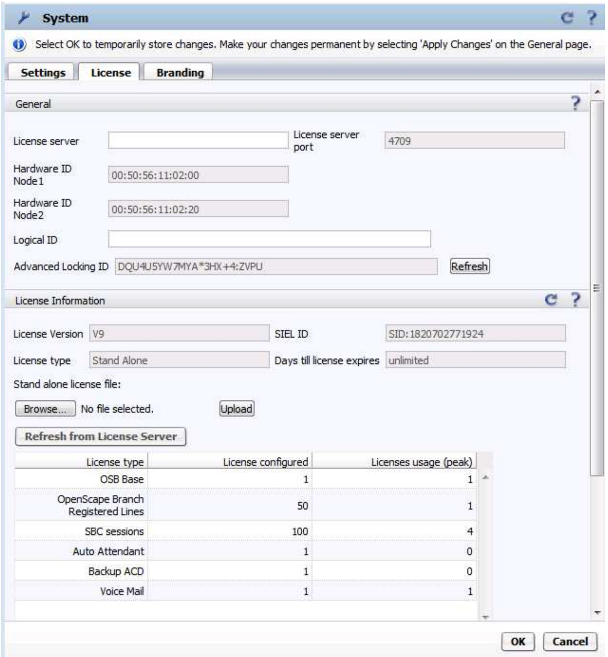
4.2. Configuration of OpenScape Branch

OS Branch is configured to run in SBC Proxy mode. In this mode OS Branch has two interfaces. One interface connects to OS Voice, and the second interface connects via SBC functionality to Orange.

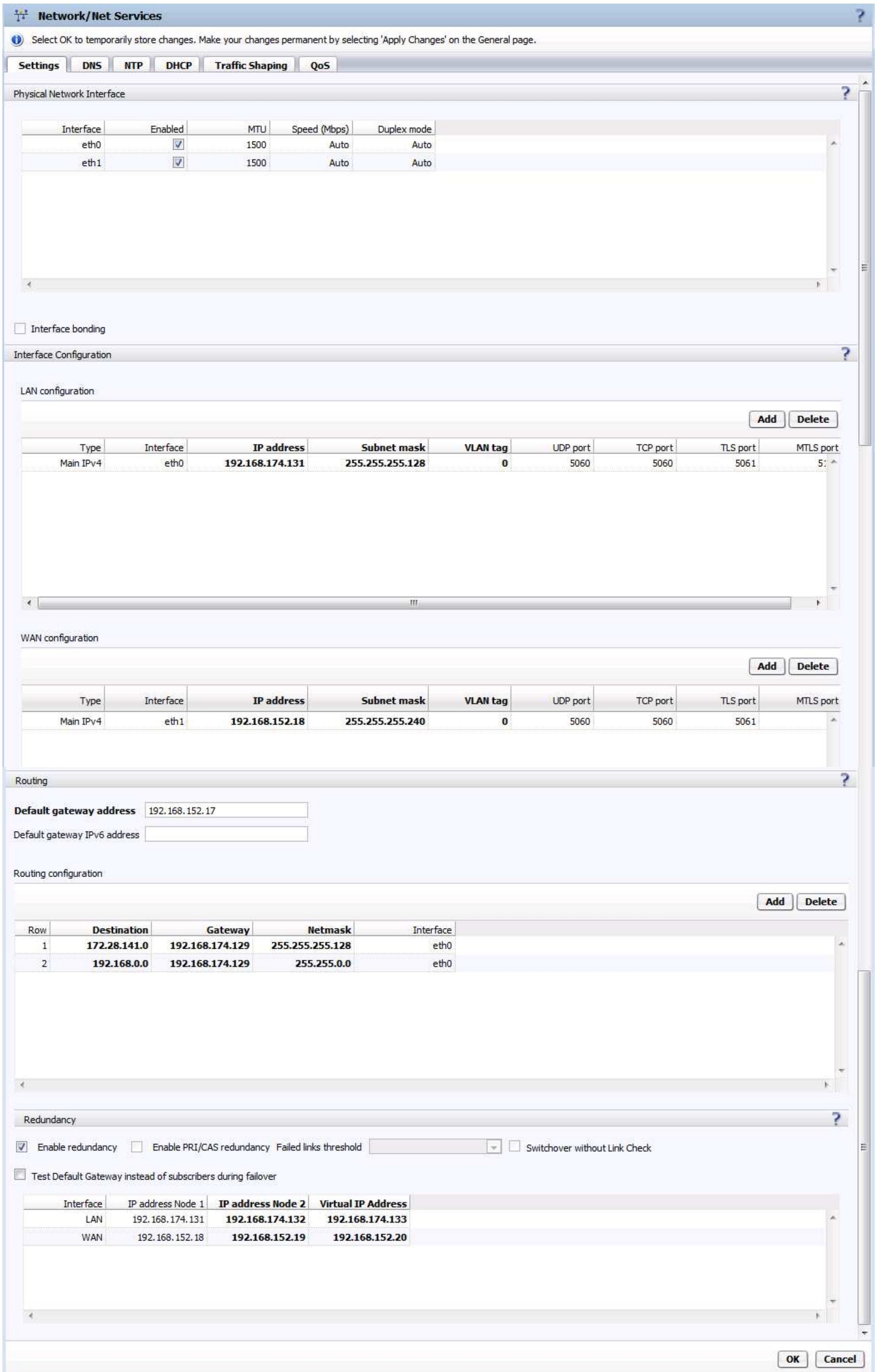


System -> Settings: System -> License:

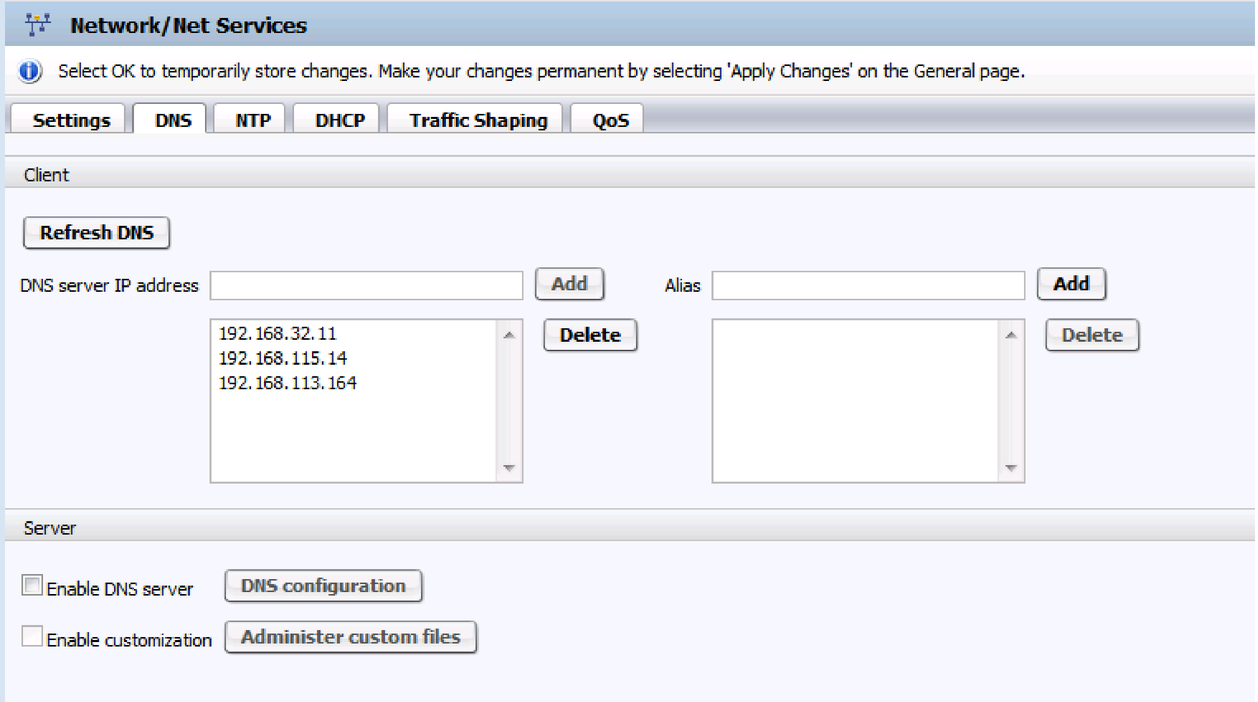




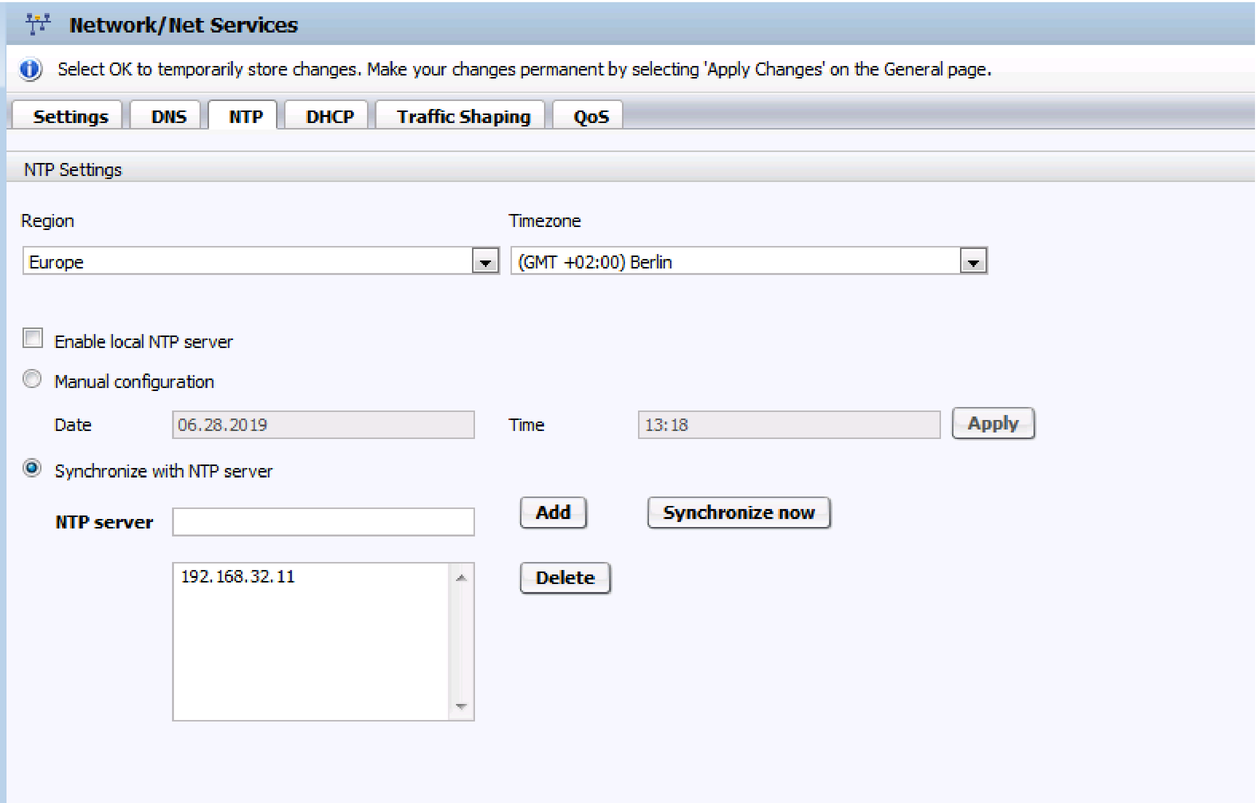
Network/Net Services -> Settings:



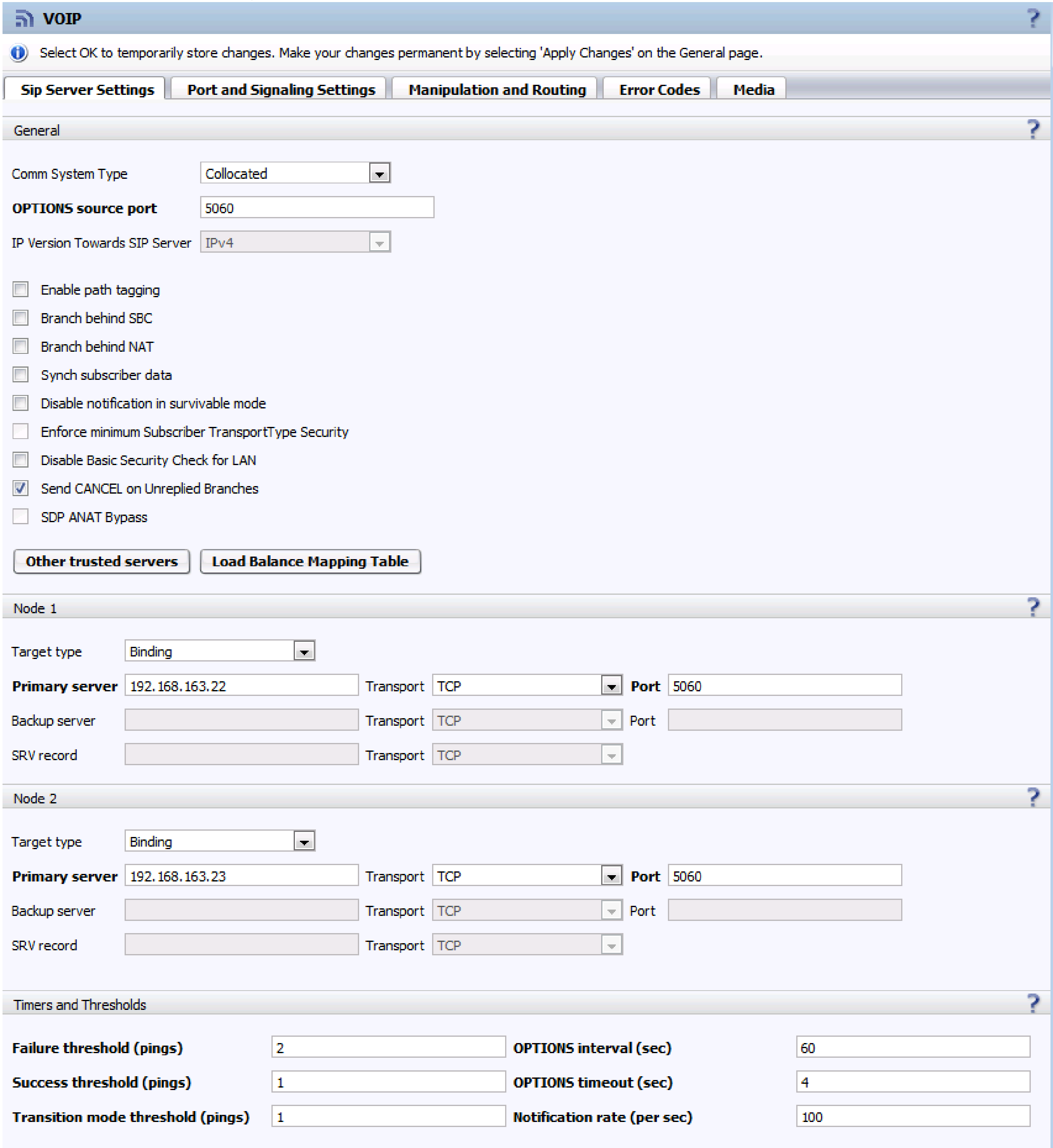
Network/Net Services -> DNS:



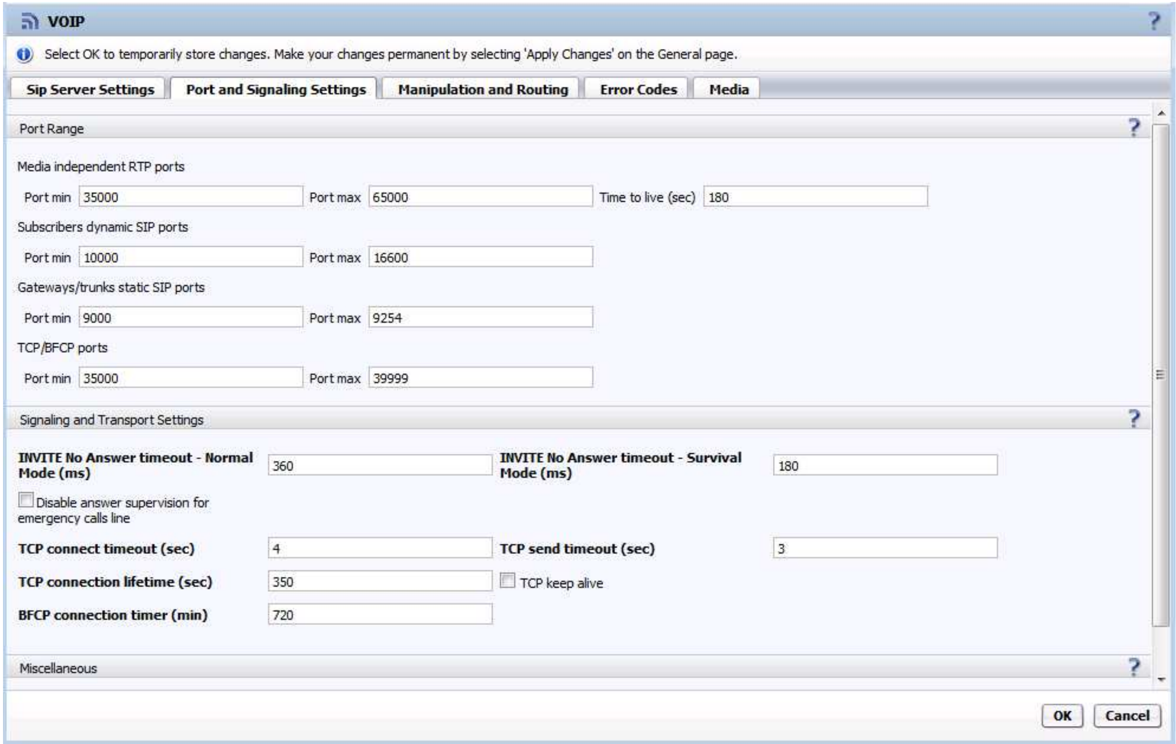
Network/Net Services -> NTP:



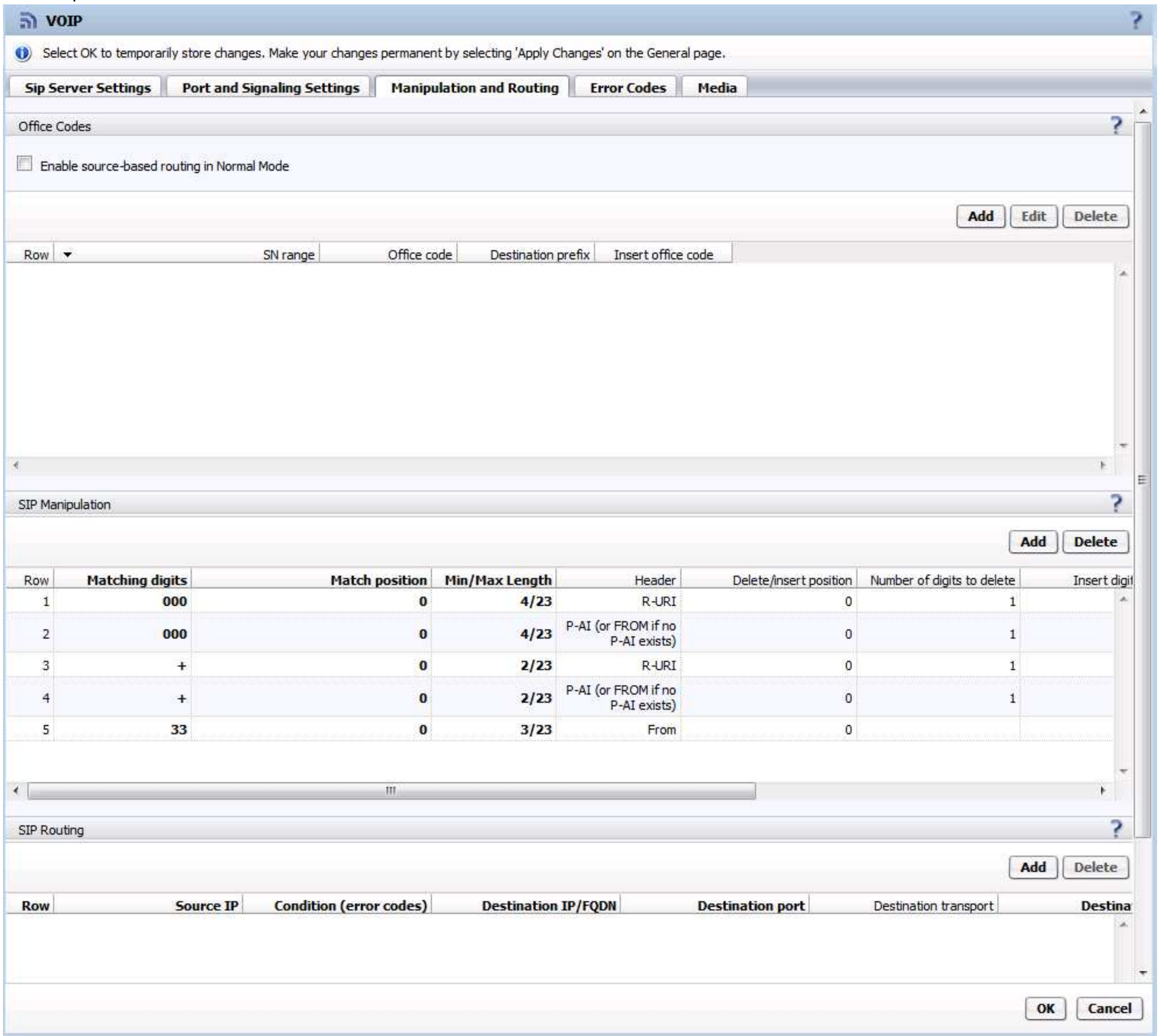
VOIP -> Sip Server Settings:



VOIP -> Port und Signaling Settings:

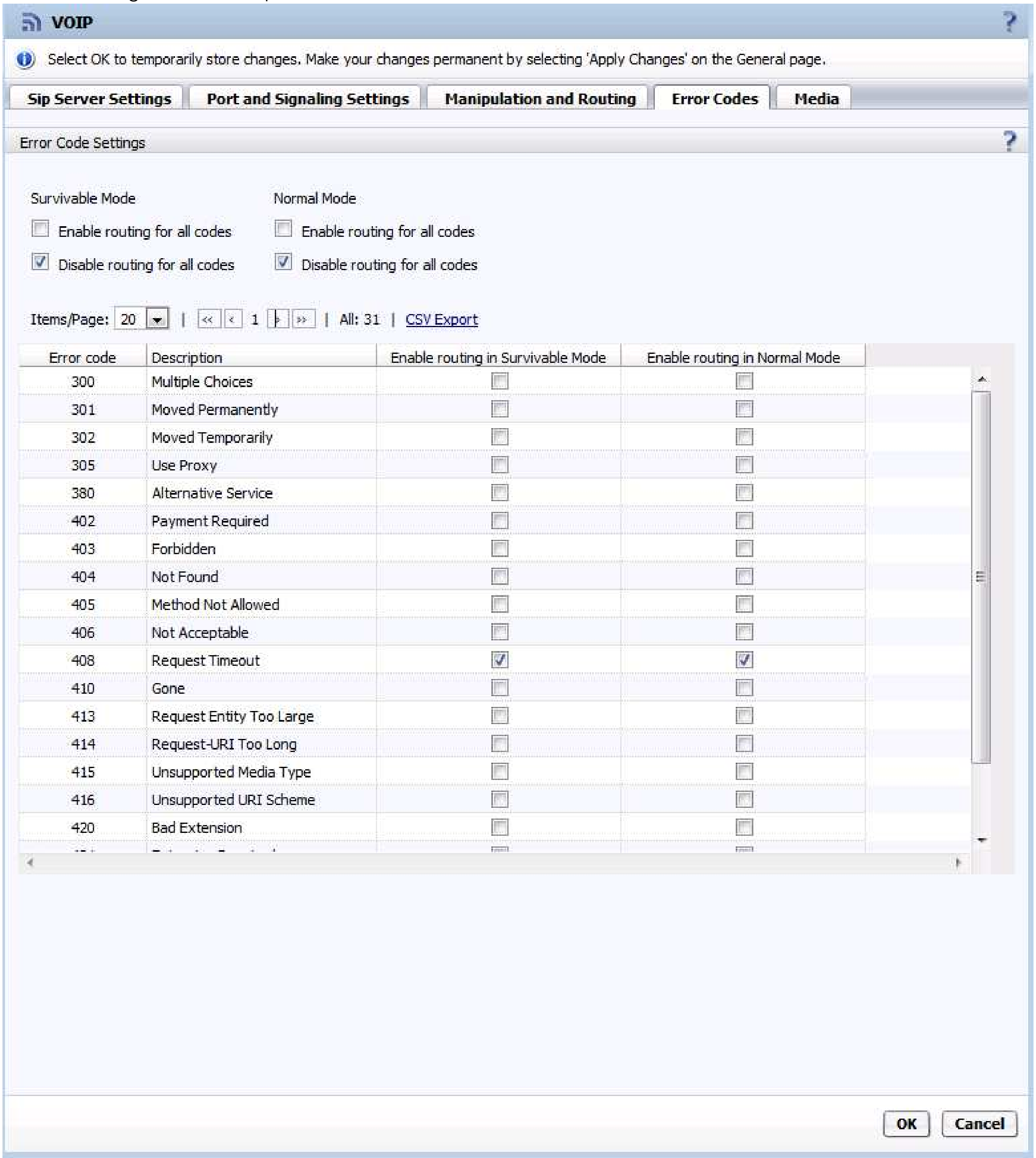


VOIP -> Manipulation and Routing:
Here must be configured SIP Manipulation rules to modify numbers dialed on the phone to be sent to Orange in the expected number format when OS Branch is in Survival Mode:

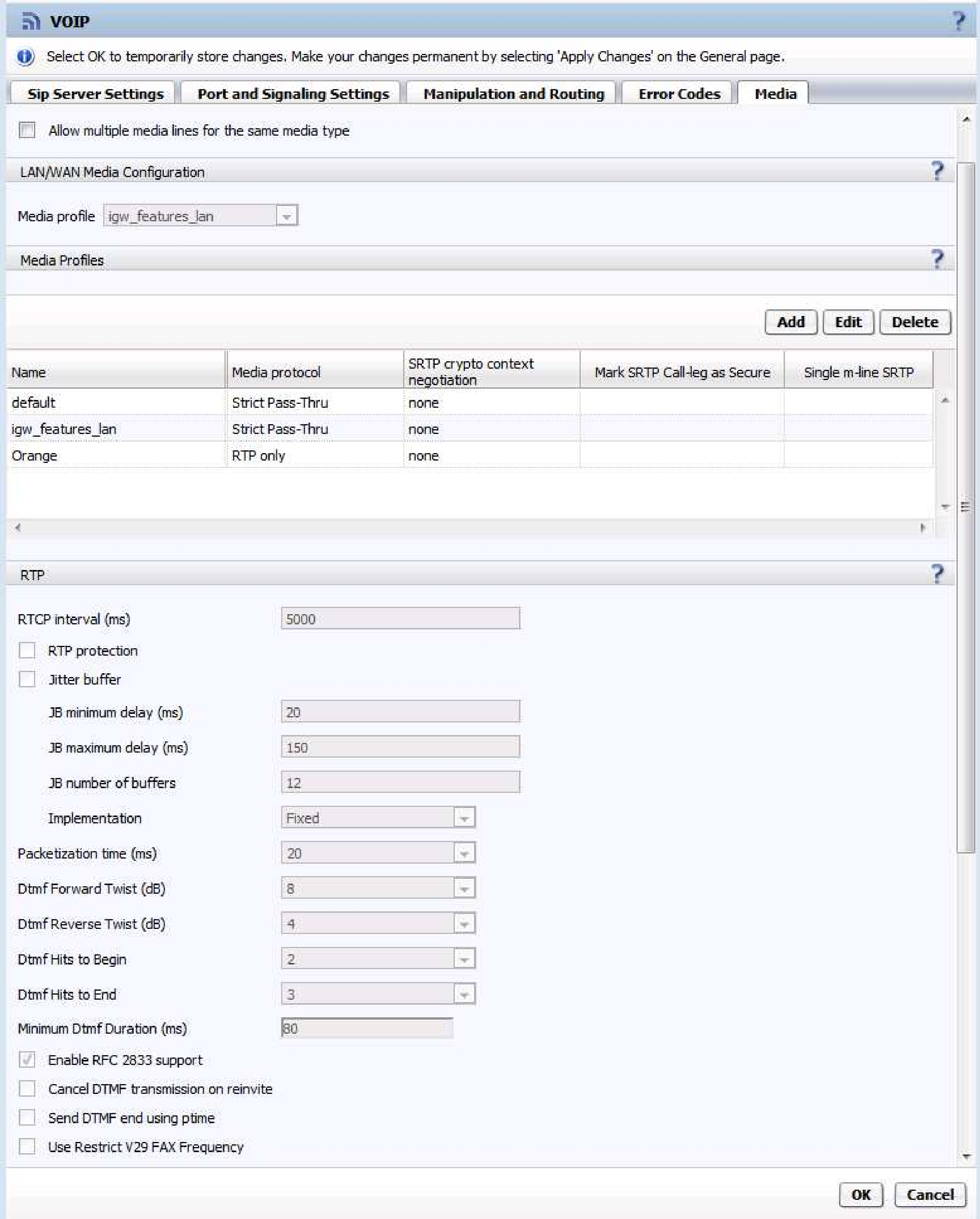


Row	Matching digits	Match position	Min/Max Length	Header	Delete/insert position	Number of digits to delete	Insert digit
1	000	0	4/23	R-URI	0	1	
2	000	0	4/23	P-AI (or FROM if no P-AI exists)	0	1	
3	+	0	2/23	R-URI	0	1	
4	+	0	2/23	P-AI (or FROM if no P-AI exists)	0	1	
5	33	0	3/23	From	0		

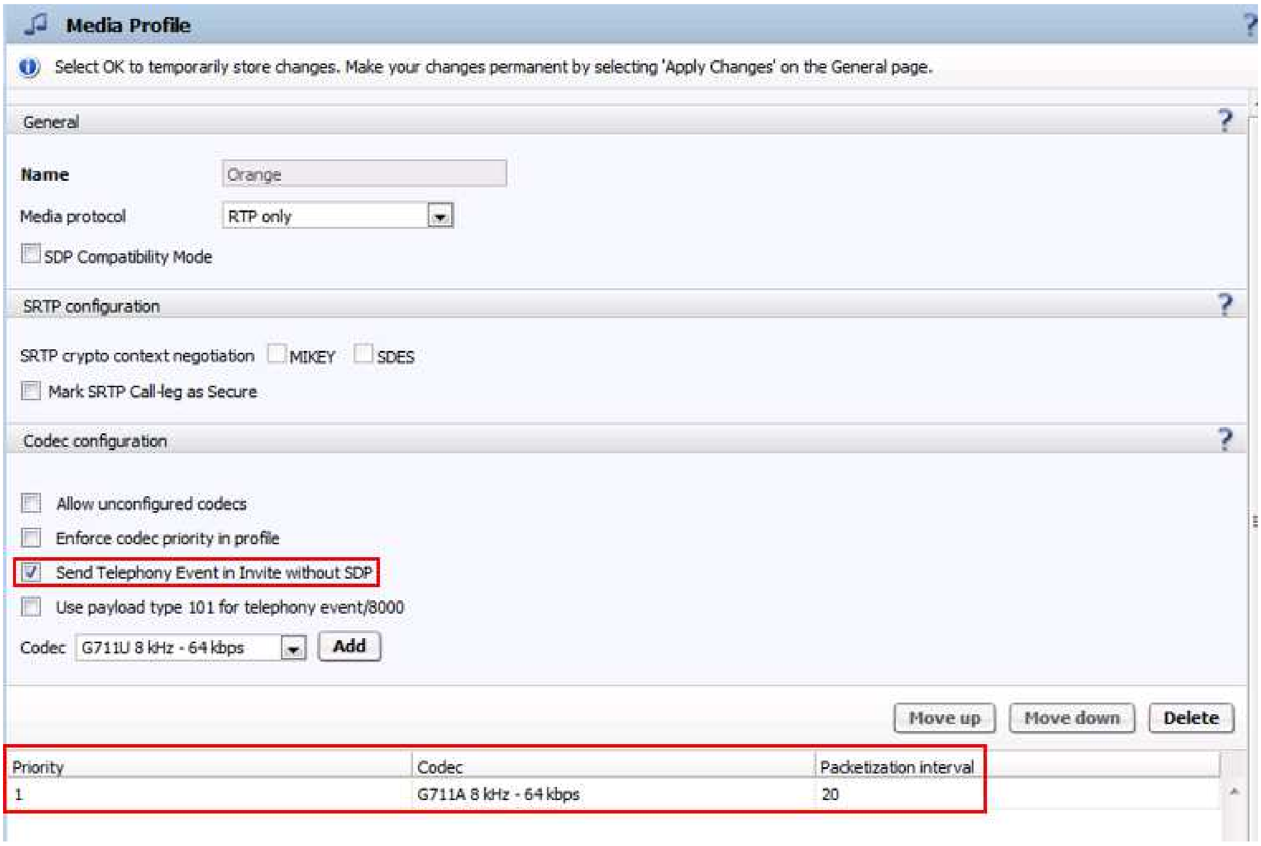
VOIP -> Error Codes:
Error code 408 must be enabled here for both modes in case the nominal Orange SBC does not respond to allow rerouting to the backup SBC.



VOIP -> Media:
For the test was used in the dialog Gateway/Trunks a Media Profile named Orange to support media protocol *RTP only*.

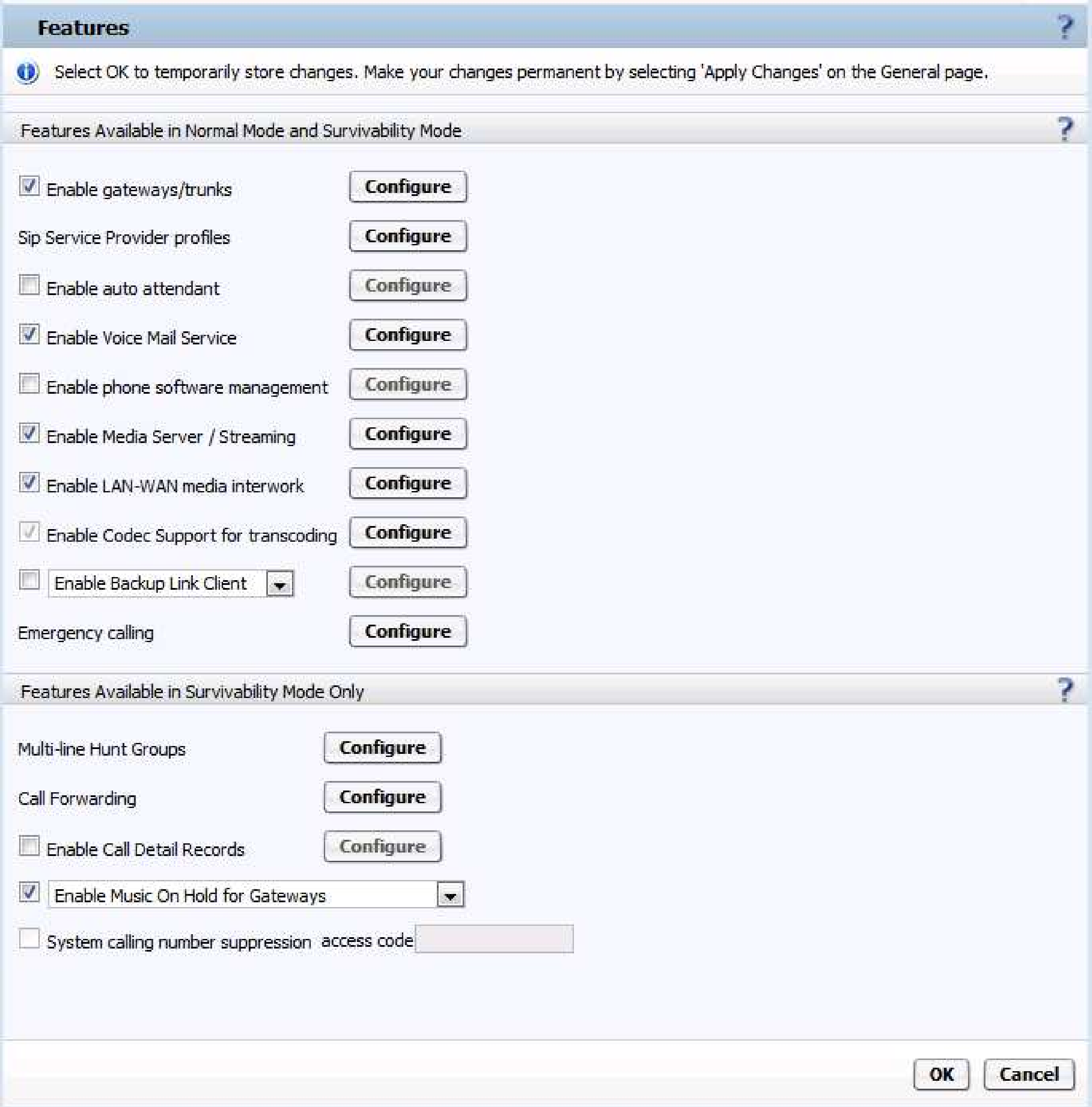


In the used Media Profile *Orange* must be configured the settings below to meet Orange requirements.

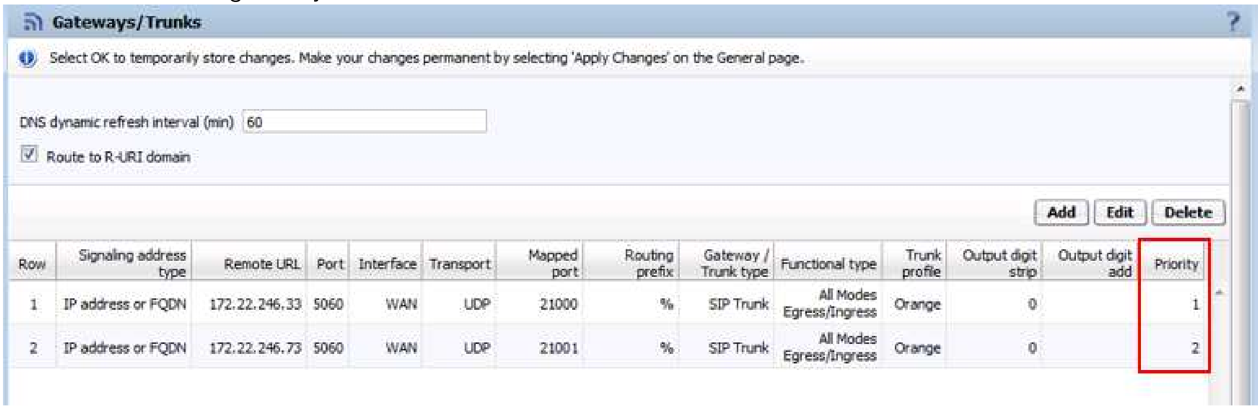


Codec G711A must be configured here to restrict OpenScape Branch supporting this one codec only.

Features:


Features
Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.
Features Available in Normal Mode and Survivability Mode
Enable gateways/trunks
Configure
Sip Service Provider profiles
Configure
Enable auto attendant
Configure
Enable Voice Mail Service
Configure
Enable phone software management
Configure
Enable Media Server / Streaming
Configure
Enable LAN-WAN media interwork
Configure
Enable Codec Support for transcoding
Configure
Enable Backup Link Client
Configure
Emergency calling
Configure
Features Available in Survivability Mode Only
Multi-line Hunt Groups
Configure
Call Forwarding
Configure
Enable Call Detail Records
Configure
Enable Music On Hold for Gateways
System calling number suppression
access code
OK
Cancel

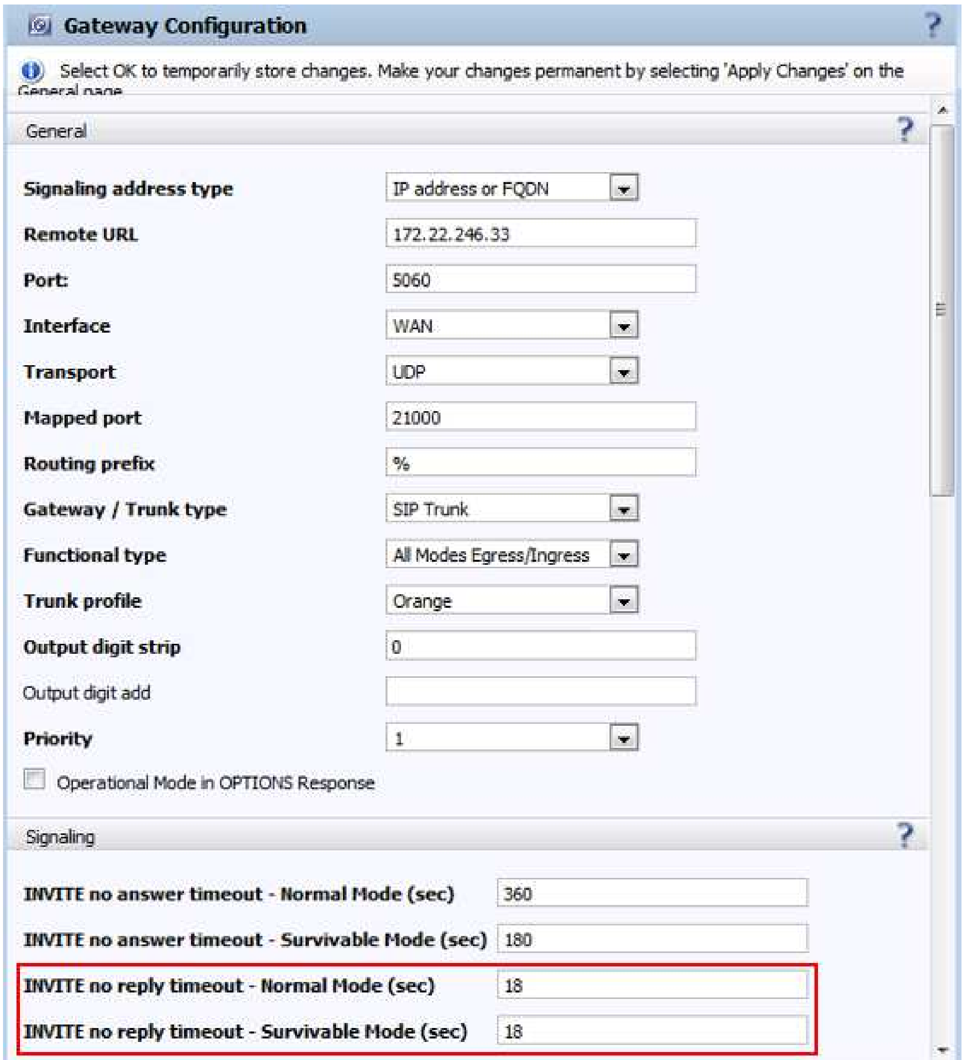
Features -> Enable gateways/trunks:

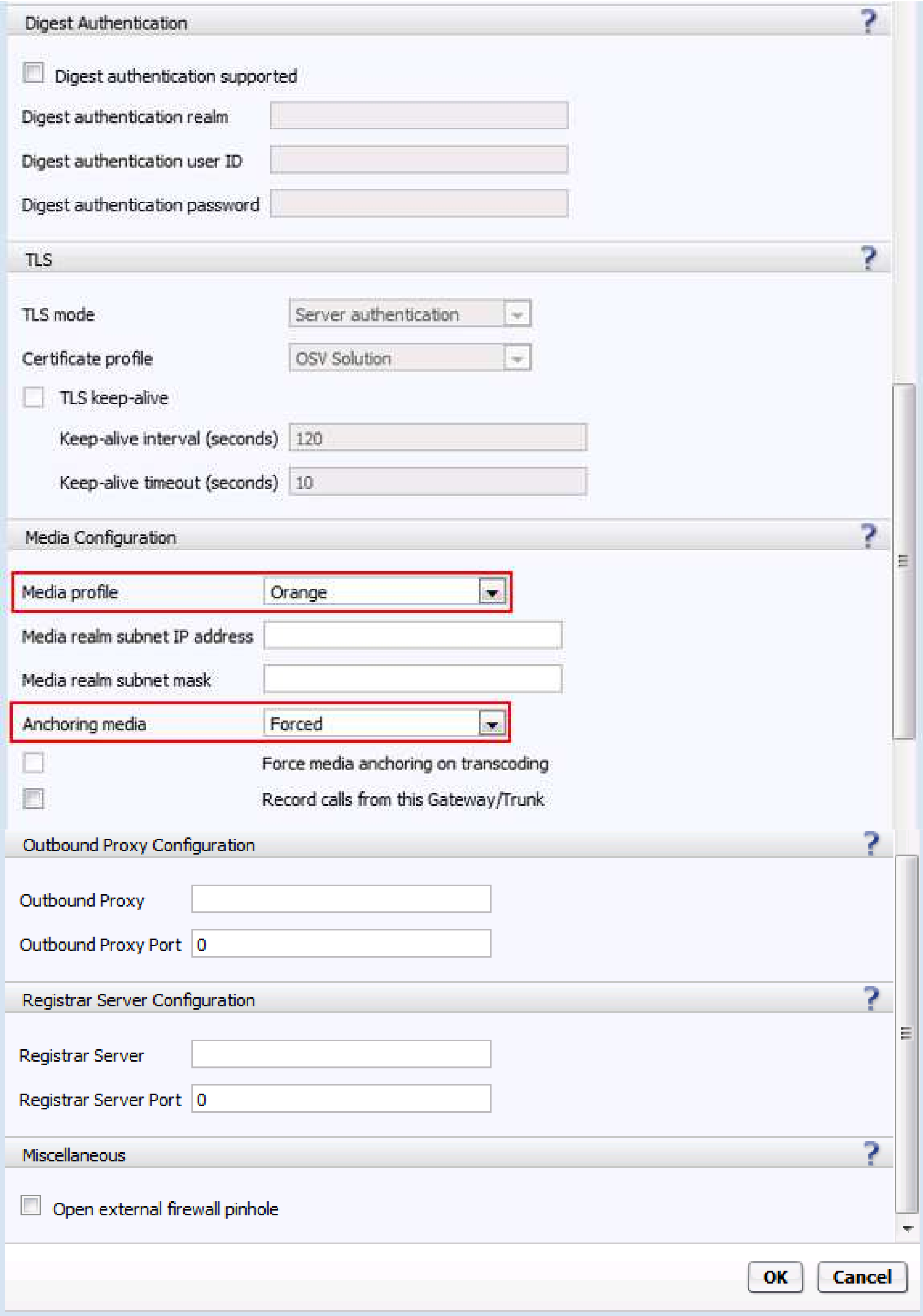


Row	Signaling address type	Remote URL	Port	Interface	Transport	Mapped port	Routing prefix	Gateway / Trunk type	Functional type	Trunk profile	Output digit strip	Output digit add	Priority
1	IP address or FQDN	172.22.246.33	5060	WAN	UDP	21000	%	SIP Trunk	All Modes Egress/Ingress	Orange	0		1
2	IP address or FQDN	172.22.246.73	5060	WAN	UDP	21001	%	SIP Trunk	All Modes Egress/Ingress	Orange	0		2

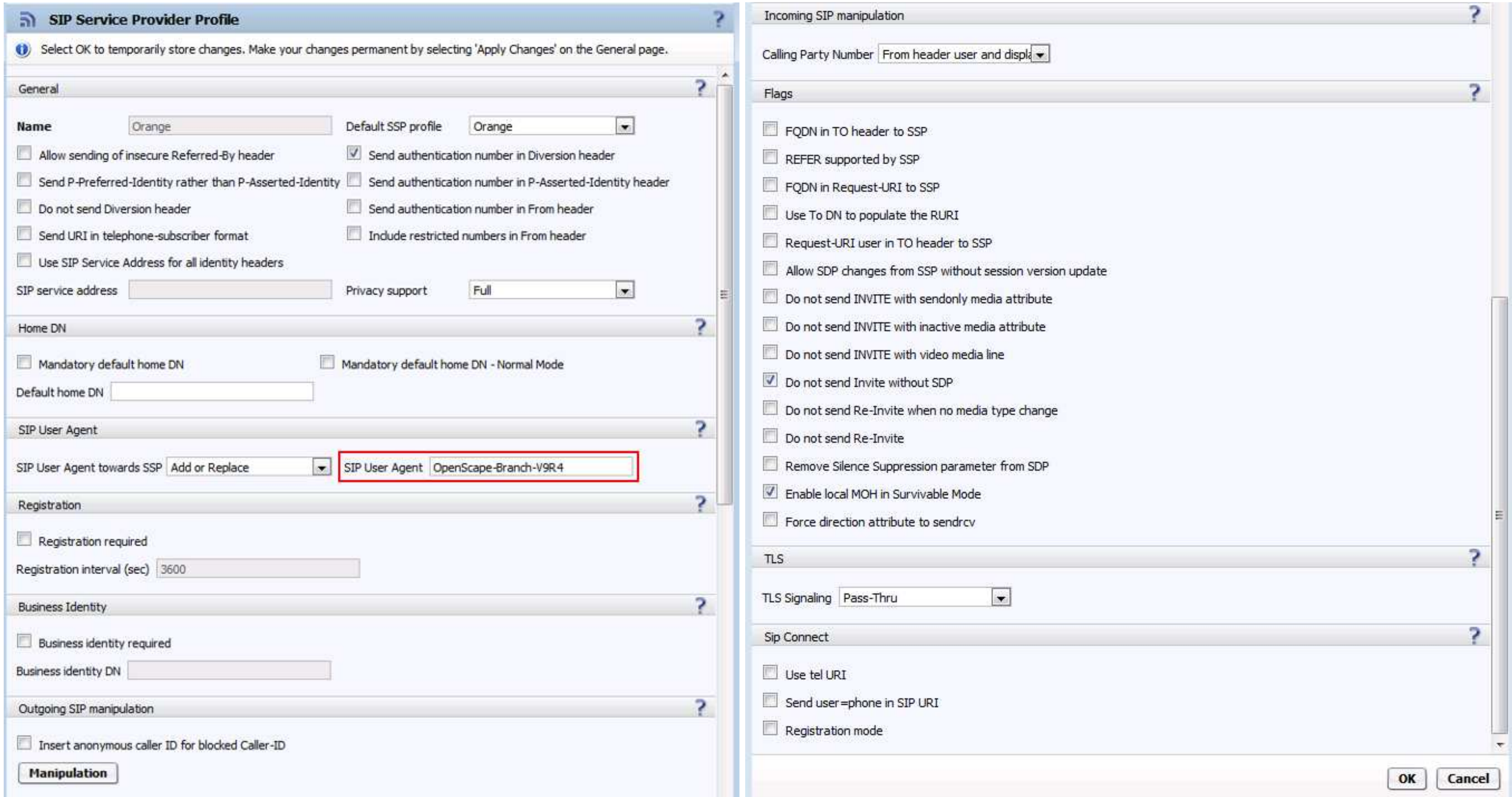
In this configuration the nominal Orange SBC 172.22.246.33 has priority 1 and the seconds Orange SBC 172.22.246.73 has priority 2.

In the *INVITE no reply timeout - Normal Mode / Survivable Mode (sec)* fields are specified 18 seconds. This means that a not replied Invite to the nominal Orange SBC is resend after 18 seconds to the backup Orange SBC.



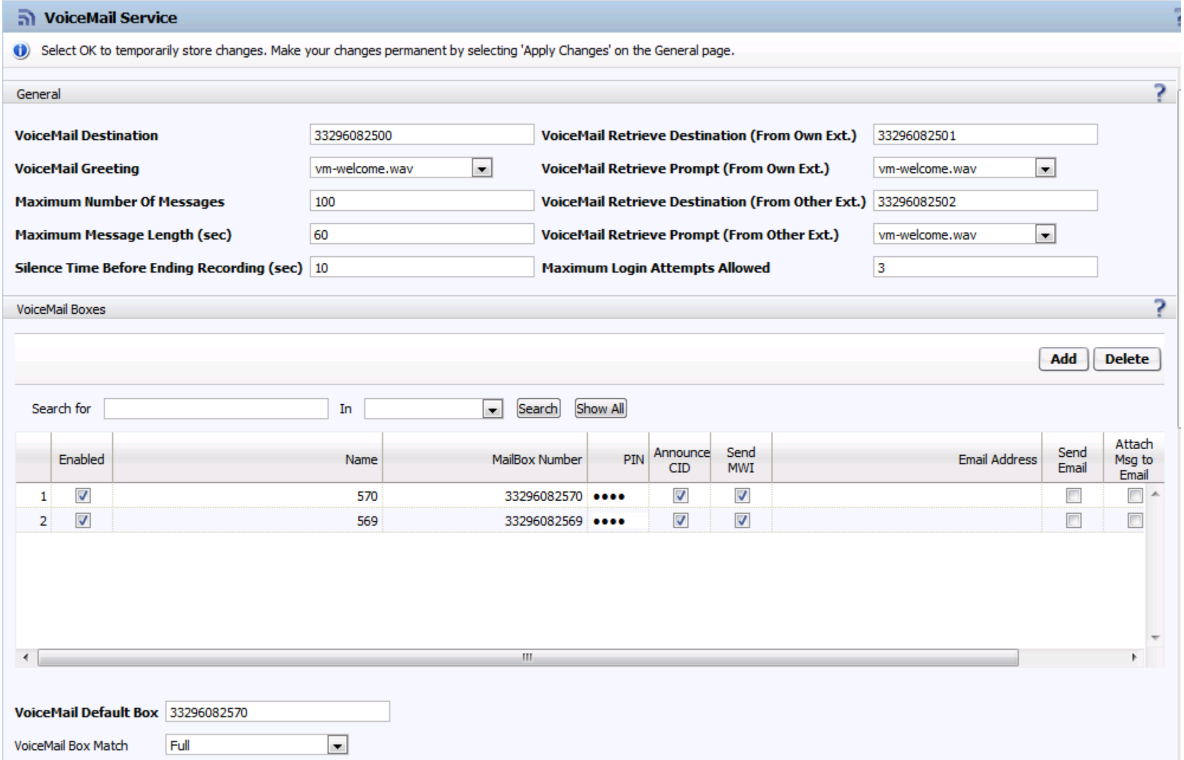

Digest Authentication
Digest authentication supported
Digest authentication realm
Digest authentication user ID
Digest authentication password
TLS
TLS mode
Server authentication
Certificate profile
OSV Solution
TLS keep-alive
Keep-alive interval (seconds)
120
Keep-alive timeout (seconds)
10
Media Configuration
Media profile
Orange
Media realm subnet IP address
Media realm subnet mask
Anchoring media
Forced
Force media anchoring on transcoding
Record calls from this Gateway/Trunk
Outbound Proxy Configuration
Outbound Proxy
Outbound Proxy Port
0
Registrar Server Configuration
Registrar Server
Registrar Server Port
0
Miscellaneous
Open external firewall pinhole
OK
Cancel

Features -> Sip Service Provider profiles:

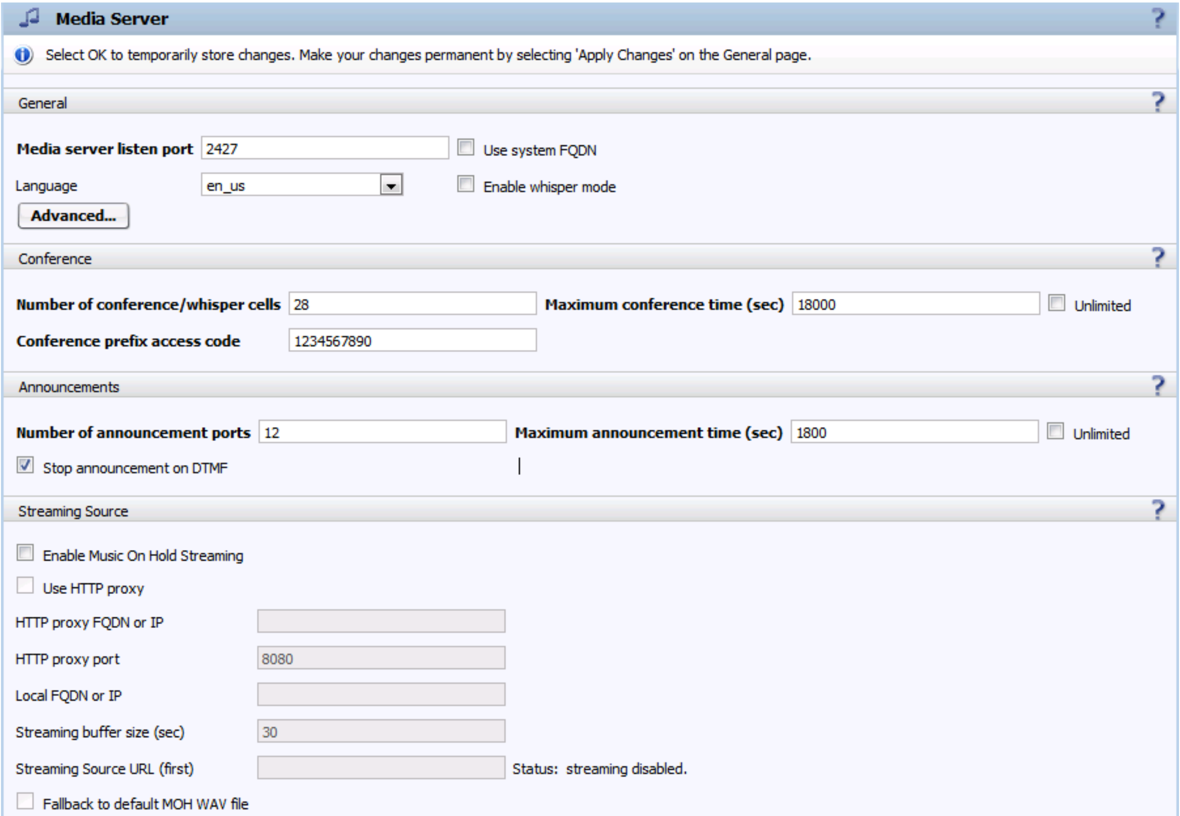


In the *SIP User Agent towards SSP* field must be configured the OS Branch version as string to meet an Orange requirement.

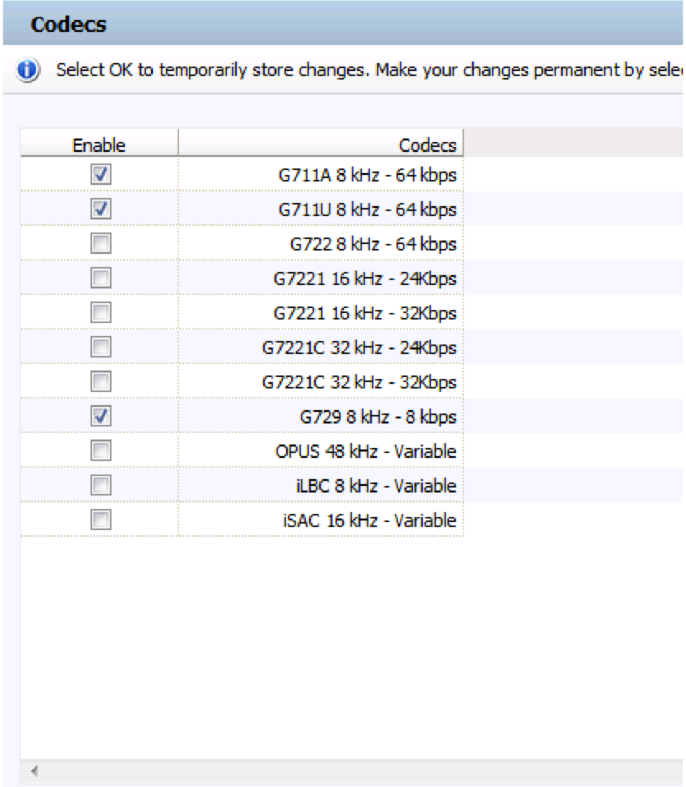
Features -> VoiceMail Service:
Here should be configured the OS Branch internal VoiceMail Service in case OS Branch is in Survival Mode having to connection to the Voice Mail server in the head quarter.



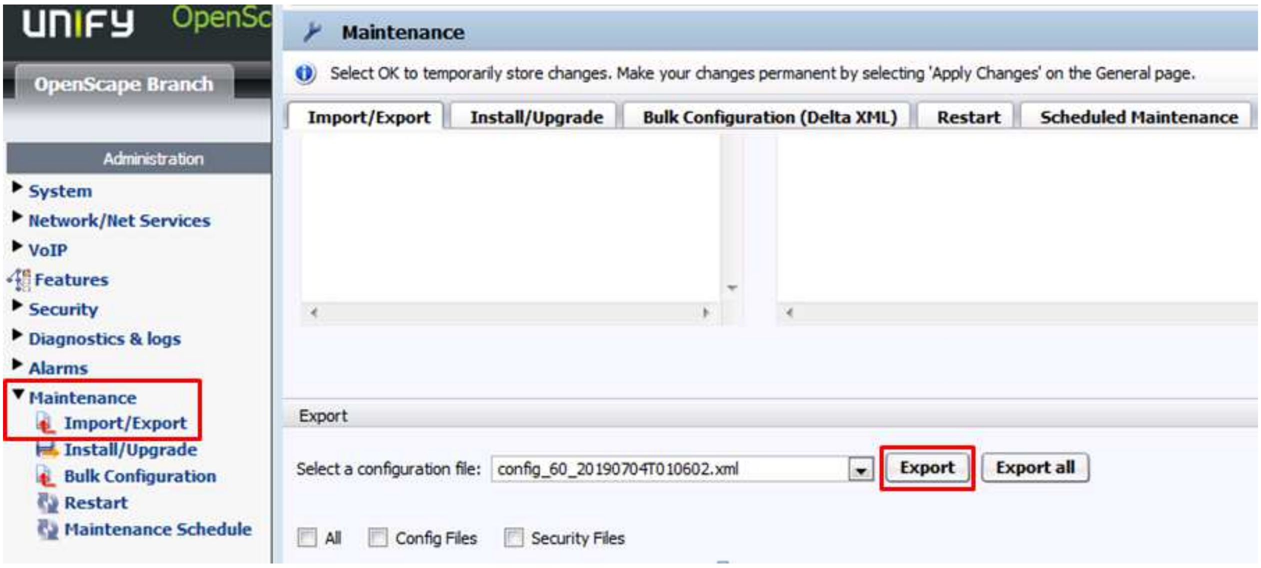
Features -> Media Server:



Features -> Enable Codec Support for transcoding:
Here must be enabled codec G711A to be used in the Media Profile.



To apply the behavior on OS Branch required by Orange a flag must be enabled in the configuration. To do so the configuration file must be exported and the *orangeCompliance* flag in section set to 1. Afterwards the modified configuration file must be imported again.




```
    <extFwPinholeEnable/>
    <trackCseqUpdatesEnable>1</trackCseqUpdatesEnable>
    <orangeCompliance>1</orangeCompliance>
</voipData>
```

In case the exported configuration file does not show the *orangeCompliance* flag the auto refresh timer on GUI must be changed and applied by clicking on Apply Changes, and afterwards the export must be done again.

4. OpenScape Voice V9 R1

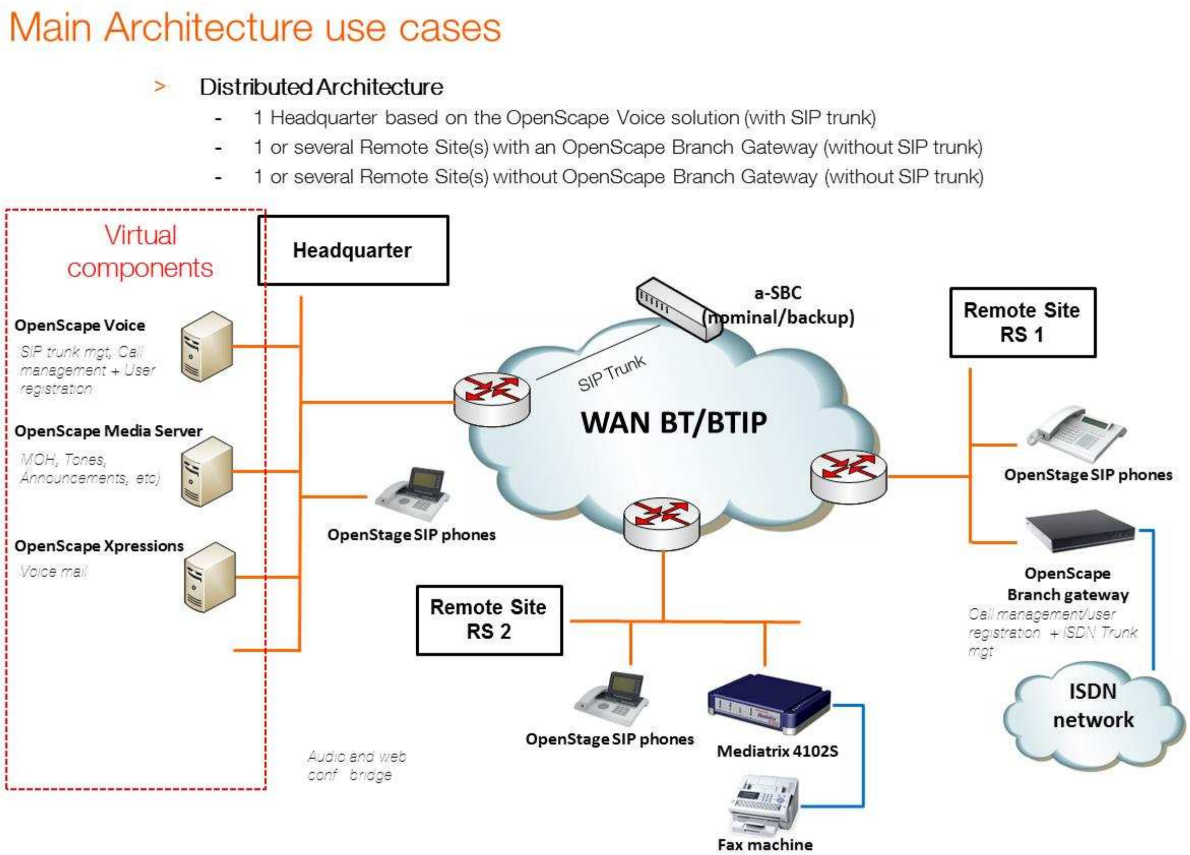
4.1. Architecture overview

Access to BT/BTIP is performed through 2 a-SBC (nominal and backup).

Only OpenScape Voice solution is connected via SIP trunks to Orange infrastructure for call distribution.

Customer shall pay attention to get proper IPBX licencing.

4.2. Distributed architecture (virtual + hardware) components



4.3. Resiliency consideration

Co-located two-nodes cluster in active-backup mode.

Switchover between the active OSV node to the second node in case of a failure is done by a monitoring process named *Survival Authority* on an external server.

4.4. CAC & Codec consideration

G729 codec usage is not supported in the scope of Unify OpenScape Voice SIP trunking interoperability with Orange Business Services. Only G711a codec is supported.

Configuration of Internal CAC solution in Openscape Voice is required to restrict only G711A 20ms Voice codec. Refer to 3.8.Annex 1 « CAC management rules on OpenScape Voice system » for more information.

4.5. Parameters to be provided by customer to access BT/BTIP service

IP addresses marked in red have to be indicated by the Customer, depending on Customer architecture scenario.

Head Quarter (HQ) architecture	Level of Service	Customer IP addresses used by service	
		Nominal	Backup
Duplex integration	Local redundancy: two OSV servers in a redundant two-node cluster that executes in an active-standby mode and sharing the same IP@.	VIP@	N/A
Remote Site (RS) architecture	**Level of Service**		
		Nominal	**Backup**
Remote site with OpenScape Branch gateway	Local user survivability and trunk redundancy via PSTN only	N/A	N/A
Remote site without media gateway	No survivability, no trunk redundancy	N/A	N/A

4.6. Business Talk & BTIP certified versions

To get more details about the versions supported by Unify, Unify product Lifecycle notifications can be provided via Unify's standard communication channels (e.g. account teams, partner portal).

4.6.1. Unify OpenScape Voice IPBX

Unify OpenScape Business IPBX – software versions			
Reference product	Software version	Certification ✓: Certified NS : No supported	Restrictions/Comments
OpenScape Voice software	V9R1.21	✓	User-Agent header contains: OpenScape Voice V9R1

4.6.2. Unify OpenScape Voice endpoints and applications

Unify OpenScape Business IBX - Endpoints and applications					
Reference product		Software version NA: not applicable	Certification ✓: Certified NS : No supported	OpenScape Voice version	Restrictions/Comments
SIP endpoints	OpenStage SIP 15, 20, 40, 60, 80	V3 R5.3.0	✓	V9R1.21	
Unify Gateway	OpenScape Branch	V9 R1.01.00	✓	V9R1.21	
Voice Mail	OpenScape Xpressions	V7 R1.3.1	✓	V9R1.21	
Third party Gateway	Mediatrix 4102S	Dgw 2.0.36.672	✓	V9R1.21	
Analog Fax	Connected to Mediatrix 4102S	NA	✓	V9R1.21	Only T.38 protocol is supported for FAX.

4.7. SIP trunking configuration checklist

Refer to the document written by Unify, in 3.9.of this document.
The Unify document describes the Unify OpenScape Voice V9 and Mediatrix 4102S Analog VoIP Adapter configuration to ensure the interoperability with Orange Business Services.

4.8. CAC management rules on OpenScape Voice system

CAC is controlled on OpenScape Voice IPBX for each geographical site.

CAC groups & CAC policies have to be defined.

A CAC Group represents the group of endpoints being served by each bandwidth-limited link which needs to be monitored.
A CAC Group will be defined based on IP subnets.

A CAC Policy is assigned to a CAC Group and represents the characteristics for the bandwidth-limited link being monitored.
Each CAC Policy contains:

- The CAC Group to which the policies applies. The CAC Policy applies to all calls to and from the CAC Group.
- the traffic type controlled by the CAC Policy: only Voice
- The bandwidth limit
- The permitted voice codecs : only G711a

Please find below the different CAC groups to be configured and their associated CAC policy.

<u>CAC Group *Branch 1* based on Headquarter subnet</u>
CAC Policy: From/To *Branch 1*, Voice, Bandwidth: xxxx Kbps, Allowed Codecs: G711a – In order to restrict G711a codec and apply some CAC for the Headquarter site

<u>CAC Group *Branch 2* based on Remote Site 1 subnet</u>
CAC Policy: From/To *Branch 2*, Voice, Bandwidth: yyyy Kbps, Allowed Codecs: G711a - In order to restrict G711a codec and apply some CAC for the Remote Site 1

<u>CAC Group: *Branch 3* based on Remote Site 2 subnet</u>
CAC Policy: From/To *Branch 3*, Voice, Bandwidth: zzzz Kbps, Allowed Codecs: G711a - In order to restrict G711a codec and apply some CAC for the Remote Site 2

<u>CAC Group: *Branch 4* based on Orange SBC IP@</u>
CAC Policy: From/To *Branch 4*, Voice, Allowed Codecs : G711a - In order to restrict G711a codec only – It is not required to define Bandwidth or Number of Calls restriction for this CAC Group

4.9. Configuration of Orange Business Services SIP Trunk with OpenScape Voice V9

OpenScape Voice V9

Configuration of Orange Business Services
SIP Trunk with OpenScape Voice V9

Version 1.2

Table of Contents

1. Goal of this document

This document describes the Unify OpenScape Voice V9 and Mediatrix 4102S Analog VoIP Adapter configuration to ensure the interoperability with Orange Business Services.

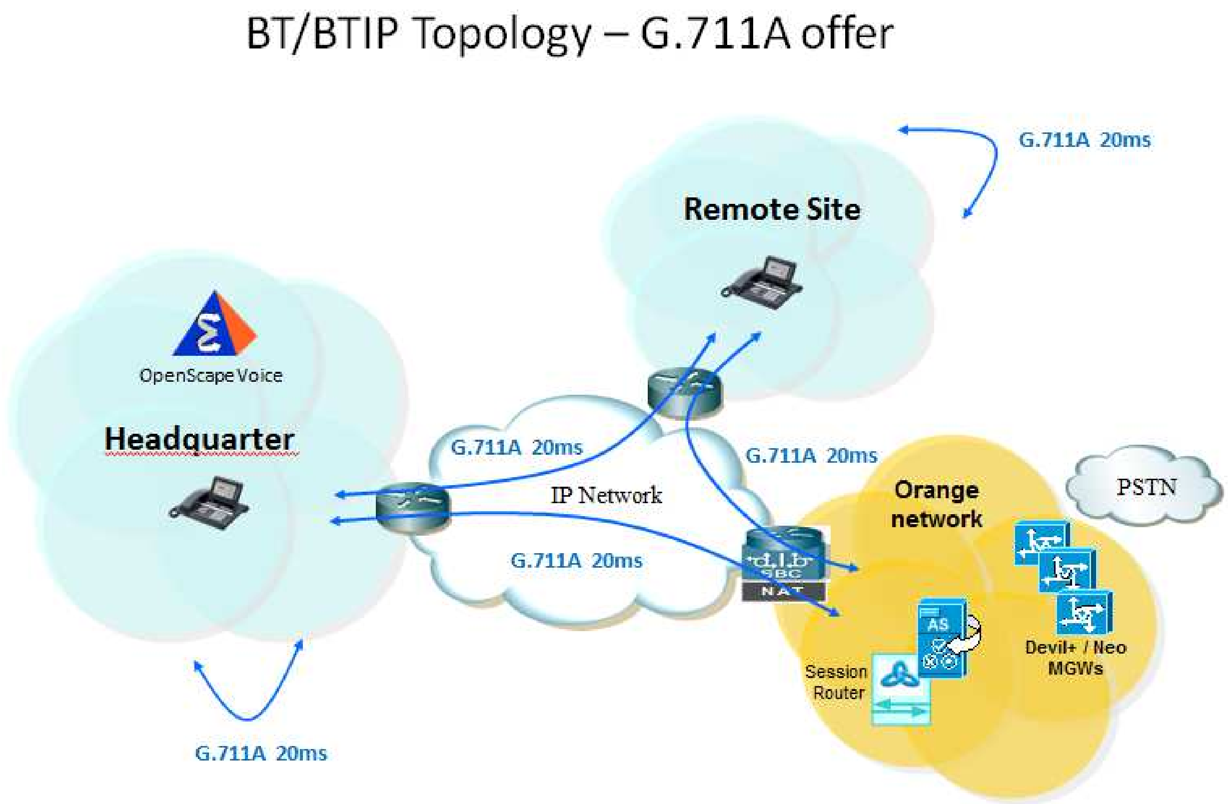
2. Certified Hardware and Software

The table below show the certified firmware versions of the SIP devices to be compliant with Orange Business Services:

HW / SW	SW / Release
OpenScape Voice	V9 R0.12.4 and V9 R2.24.1
Mediatrix 4102S	Dgw 2.0.28.504 and Dgw 2.0.36.672
OpenScape Branch, native	V9 R1.01.00
OpenStage SIP phones	V3 R4.10.0 and V3 R5.6.0

3. Customer Network Topology

The figure below shows the connection between the Orange network, the customer's headquarter and a customer's remote site. The customer's headquarter and his remote sites are connected also via Orange network.



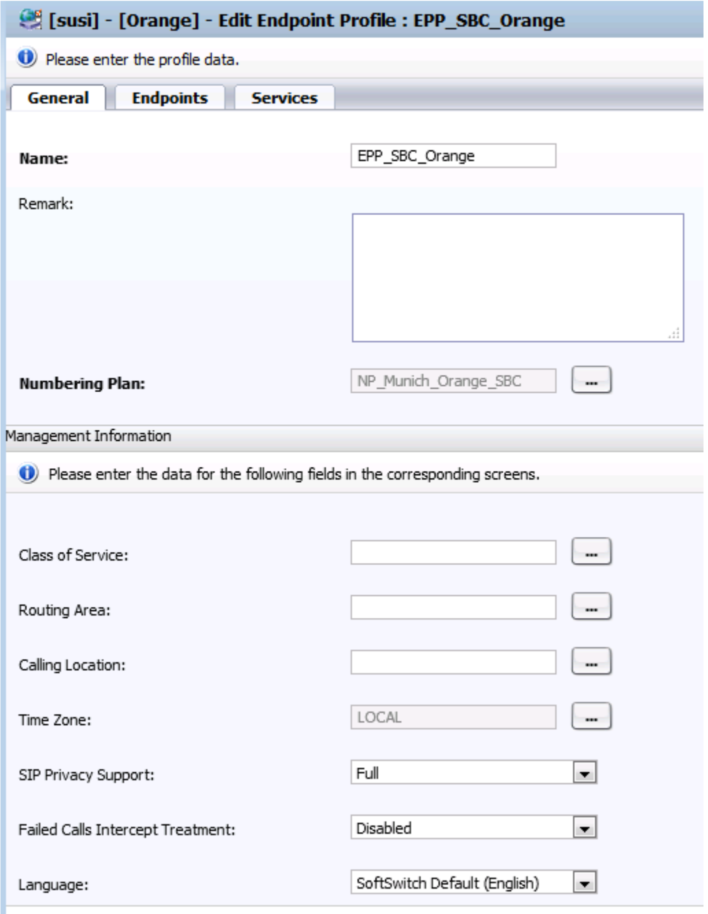
4. Configuration of SIP Devices

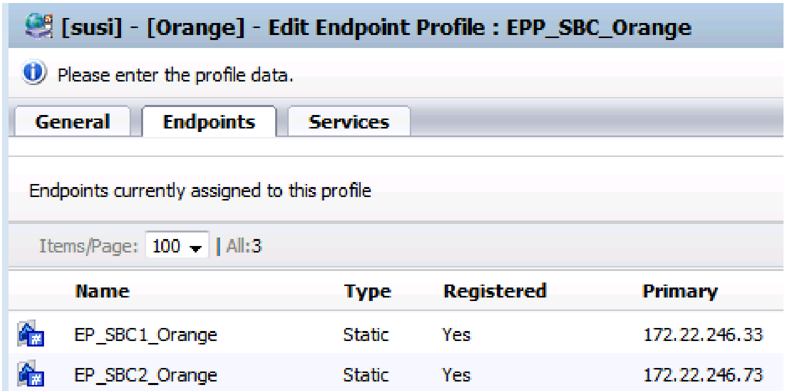
4.1. Configuration of OpenScape Voice

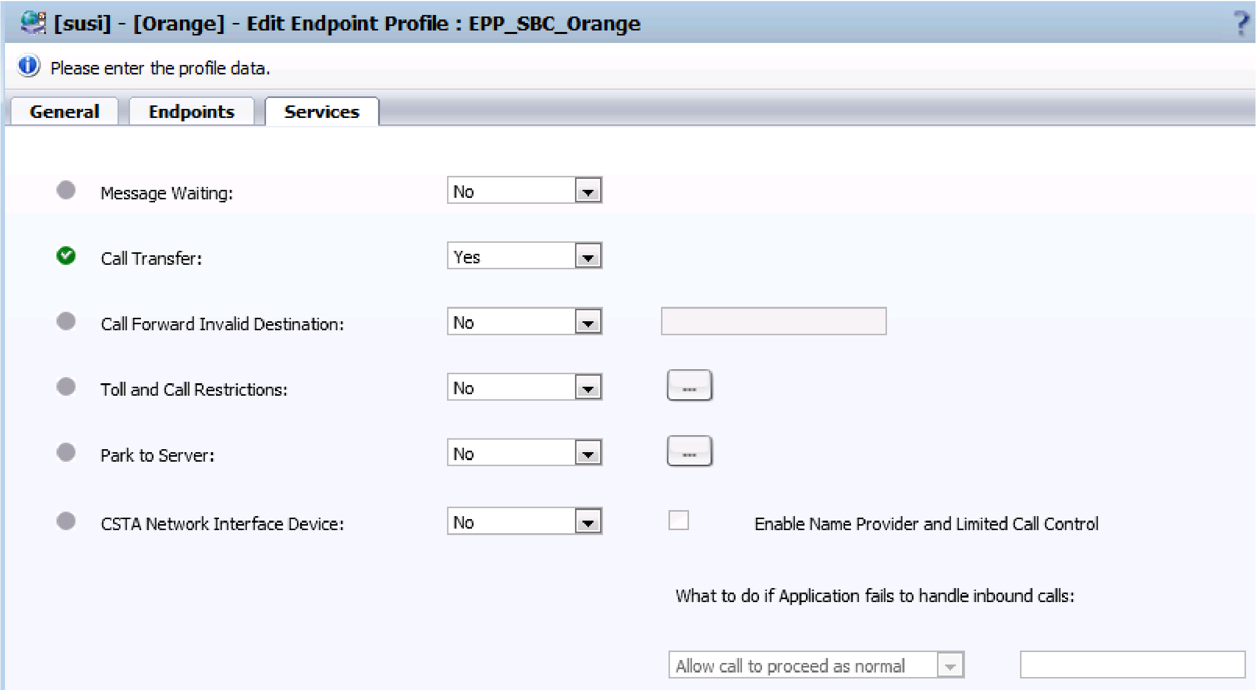
The following describes the configuration of OpenScape Voice for the Orange Business Services SIP Trunk compliancy. OpenScape Voice has been installed and configured based on the OpenScape Voice Installation and Configuration Guide. Additionally Orange SBC endpoints and endpoint profile configuration is required.

4.1.1. Orange SBC Endpoint Profile Configuration

The Orange SBC endpoints are configured in the Common Management Platform.

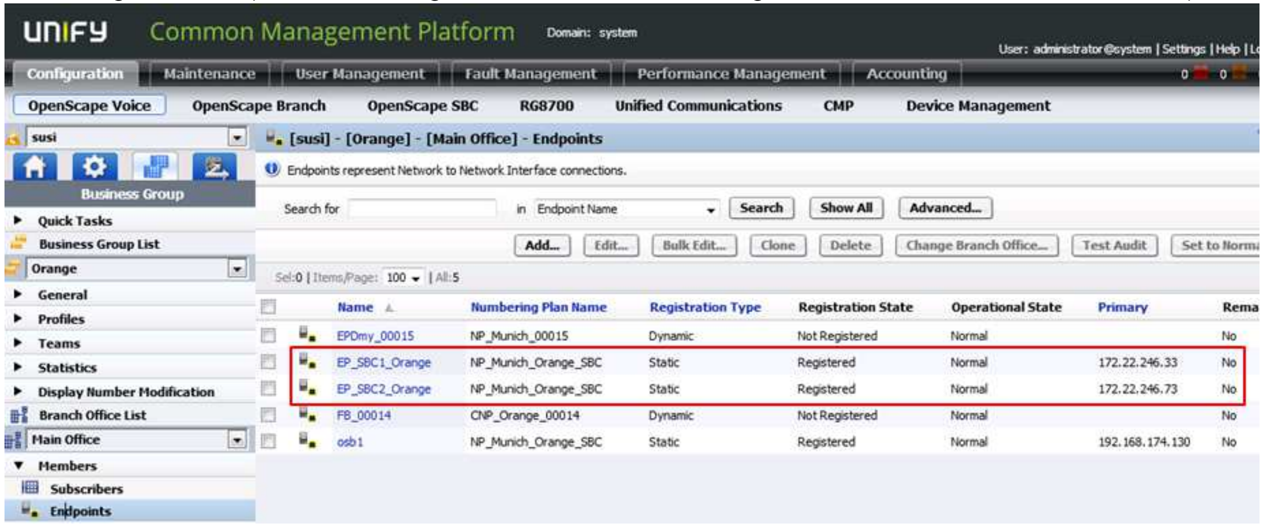





[susi] - [Orange] - Edit Endpoint Profile : EPP_SBC_Orange
Please enter the profile data.
General
Endpoints
Services
Message Waiting:
No
Call Transfer:
Yes
Call Forward Invalid Destination:
No
Toll and Call Restrictions:
No
Park to Server:
No
CSTA Network Interface Device:
No
Enable Name Provider and Limited Call Control
What to do if Application fails to handle inbound calls:
Allow call to proceed as normal

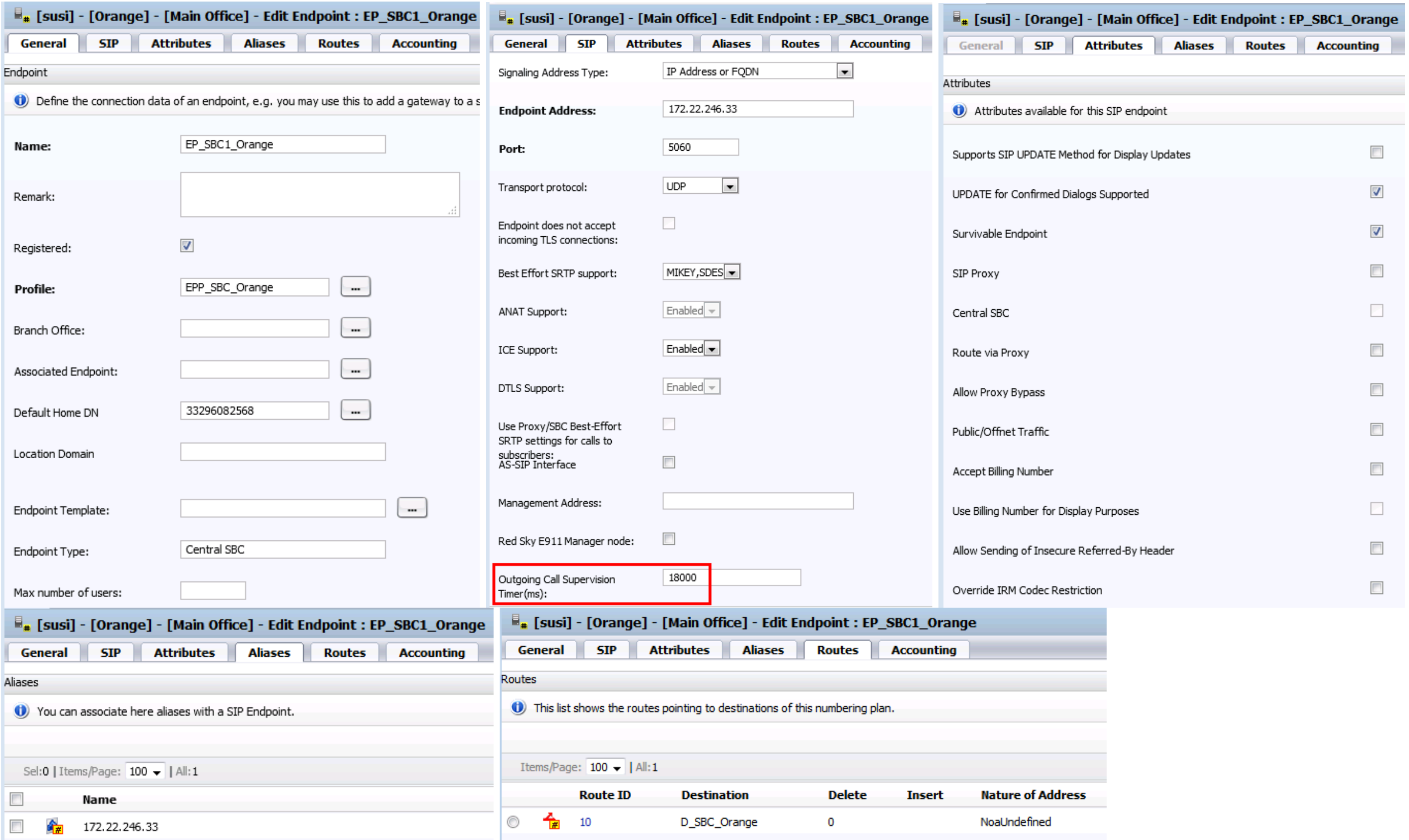
4.1.2. Orange SBC Endpoint Configuration

The Orange SBC endpoints are configured in the Common Management Platform in the Business Group area:



The backup SBC is used in case the nominal SBC does not respond within the time specified in the *Outgoing Call Supervision Timer*, see below.

Below is shown the configuration of the nominal Orange SBC endpoint. A similar configuration has to be made for the backup Orange SBC. In the nominal SBC endpoint is configured an Outgoing Call Supervision Timer with its value of 18000 ms. The Outgoing Call Supervision Timer supervises the time between sending an INVITE request and receiving a provisional (non-100 Trying) or final response from the SBC. After expiration of this timer the backup SBC is called instead of the nominal SBC.



4.1.3. OpenScape Voice SIP Parameters for Orange SBC Endpoints

The following SIP attributes are configured in both Orange SBC endpoints on the Attributes tab shown above:

SIP attribute	Description	Value to set in the scope of OSV v9 certification
Supports SIP UPDATE Method for Display Updates	This attribute indicates whether the SIP Trunking endpoint supports receiving a SIP UPDATE method without SDP and with a P-Asserted-Identity (or P-Preferred-Identity) header field for display updates. This attribute is only applicable for SIP Trunking endpoints and it is automatically enabled for SIP Private Networking endpoints. In addition, this attribute only makes a difference if the SIP Trunking Endpoint Profile has Privacy Support set to Full or Full-Send.	OFF
UPDATE for Confirmed Dialogs Supported	If selected (enabled), update for confirmed dialogs is specified. (We assume this is linked to the session refresh…)	ON
Survivable Endpoint	If selected (enabled), the endpoint provides survivability in a branch office. Note : This attribute is required for the "Subscriber Rerouting" feature. Subscriber rerouting is only executed for subscribers whose Associated Endpoint has this attribute set; applicable only to SIP endpoint.	ON
SIP Proxy	If selected (enabled), the endpoint is a SIP proxy (e.g. Comdasys, RG2700); applicable only to SIP endpoint. This attribute is not applicable for SIP Private Networking.	
Central SBC	This attribute is introduced from OSV V8 onwards for proxy/SBC endpoints and can be selected (enabled) only if the SIP Proxy attribute is enabled. Central SBC attribute and Allow Proxy Bypass attribute are mutually exclusive so if one is checked the other automatically is unchecked. If the attribute is selected (enabled) it indicates that the endpoint is a Central SBC and any subscriber associated to this endpoint is considered a remote user from the SIP-Registar and is allowed to register only if the respective check box Registration via Central SBC Allowed is ticked. NOTICE: From V8 onwards in order to be able to control whether a subscriber is allowed or not to register via a Central SBC, the endpoint attribute Central SBC must be set for all endpoints that are central SBCs. If this precondition is met, whether a subscriber is allowed or not to register via the central SBC can be controlled via the subscriber checkbox Registration via Central SBC Allowed	OFF

Route via Proxy	If selected (enabled), the endpoint which must be a SIP proxy (i.e. the IP Proxy attribute must be selected) requests to be on the route when the OpenScape Voice is making an outbound call to a subscriber that has this endpoint as their Associated Endpoint. IMPORTANT: The parameter Srx/Sip/CentralSbcSupport related to Route via Proxy attribute is by default set to RtpTrue. If it is changed to RtpFalse the attribute under the Endpoint configuration will have no effect and routing problems may also be created. This attribute should always be set if the SIP Proxy attribute is set; applicable only to SIP endpoint.	
Allow Proxy Bypass	Proxy Bypass is a system-wide OSV feature that is turned on per default. It is only used when deploying Type 2 or 5 branch offices. If selected (enabled), Proxy Bypass allows OpenScape Voice to bypass the recorded proxy in a contact if an INVITE request to the contact's recorded proxy does not receive a response within a specified time. This attribute is not applicable for SIP Private Networking.	
Public/Offnet Traffic	If selected (activated), this attribute allows the subscriber marking all calls from/to an endpoint as external regardless whether the called or calling is intra-BG or not Note : This attribute is only configurable for SIP Trunking endpoints and it is automatically disabled for SIP Private Networking endpoint or not.	**OFF**
Accept Billing Number	If selected (activated), this attribute makes sure that calls get charged to the right call account. This attribute is achieved by transporting the user number in the additional SIP CDR header field	**OFF**

Use Billing Number for Display Purposes	This attribute can be activated only if the attribute Accept Billing Number is activated. The combination of both attributes is used on endpoints that send charge numbers for outbound calls or blind transfers and where the Administrator wishes to use this number for display purposes. Currently OpenScape Xpressions and OpenScape UC conference bridge send a charge number for outbound calls. The possible combination of these two attributes (Accept Billing Number and Use Billing Number for Display Purposes) have the following result: – Not having either attribute set, means that the charge number in a received X-Siemens-CDR header is ignored. – Having only Accept Billing Number set but not Use Billing Number for Display Purposes, means that the charge number is used for authorization and authentication purposes and will show up in CDR records.If however the "charge number" and "From number" of the incoming INVITE request have different formats of the same subscriber number, the charge number is used as display number (e.g. when setting up Xpressions mailbox using extensions of subscribers). – Having both Accept Billing Number and Use Billing Number for Display Purposes set, means that the charge number is used for authorization and authentication purposes and will show up in CDR records and is used for display purposes as well.	**OFF**
Allow Sending of Insecure Refered-By Header	If selected (activated), this attribute makes sure that calls get charged to the right call account. NOTICE: This attribute is achieved by transporting the user number in the additional SIP CDR header field "X-Siemens-CDR" for the endpoint used.	**OFF**
Override IRM Codec Restriction	It brings the potential for multicodec scenarios to set up an advanced codec restriction policy If selected (enabled), the Override IRM Codec Restrictions attribute will be assigned to the selected subscriber.	**OFF**
Transfer HandOff	If selected (enabled), during transfer handoff, REFER and NOTIFY transactions will be passed transparently through OpenScape Voice. Used for TRANSFER_HANDOFF for Genesys	**OFF**
Send P-Preferred-Identity (PPI) rather than P-Asserted-Identity	If selected (enabled), a P-Preferred-Identity header field will be sent whenever a P-Asserted-Identity header field would normally be sent.	**OFF**

(PAI)	This attribute is primarily intended for use when connecting to a SIP Service Provider that does not accept a P-Asserted-Identity SIP header field. NOTICE: This attribute can only be configurable for SIP Trunking endpoints. This attribute is automatically disabled for SIP Private Networking endpoints. The Diversion header field is used on the SIP Private Networking interface to transport the diverting/re-directing party number and the reason for the diversion.	
Send domain name in From and P-Preferred-Identity headers	If selected (enabled), the host part of the From and P-Preferred-Identity (or P-Asserted-Identity) SIP header fields will contain the domain name of the OpenScape Voice node. Note: If calling number presentation restrictions apply the host part of the From header field will contain 'anonymous.invalid'. Note: This attribute is primarily intended for use when connecting to a SIP Service Provider that does not accept dotted IP addresses in calling user identification SIP header fields.	**OFF**
Send Redirect Number instead of calling number for redirected calls	If selected (enabled), a call that is redirected to the endpoint will have the last redirecting or transferring party's identity in the From and P-Asserted-Identity (or P-Preferred-Identity) SIP header fields. This attribute is primarily intended for use when connecting to a SIP Service Provider that does not understand the Diversion header field. Note: This attribute can only be configured for SIP Trunking endpoints. This attribute is automatically disabled for SIP Private Networking endpoints.	**OFF**
Do not send Diversion header	If selected (enabled), a SIP Diversion header field will not be sent. This attribute is primarily intended for use when connecting to a SIP Service Provider that cannot accept a Diversion SIP header field. When this attribute is selected the 'Send forwarding number rather than calling number for forwarded calls' attribute will generally also be required. This attribute is normally used in conjunction with one of the following attributes: Send redirecting number rather than calling number for redirected calls Send authentication number in P-Asserted-Identity header Send authentication number in From header Note: This attribute can only be configured for SIP Trunking endpoints. This attribute is automatically disabled for SIP Private Networking endpoints	**OFF**

Do not Send Invite without SDP	If selected (enabled), SIP reINVITE requests that do not include SDP will not be sent during redirection procedures. OpenScape Voice will reuse the SDP previously received from the endpoint to send as an SDP offer to the new partner endpoint. When the SDP answer is received the new SDP will be sent in a reINVITE and the 200 OK answer will be consumed by OpenScape Voice. Note : This attribute is primarily intended for use when connecting to a SIP Service Provider that cannot accept a reINVITE request without SDP.	**ON (with OSV RTP parameter set: Srx/Sip/sdpSessionMaintainer = RtpTrue)**
Send International Numbers in Global Number Format (GNF)	If selected (enabled), the OpenScape Voice adds a '+' in front of all numbers which have NPI =PUBLIC and NOA = INTERNATIONAL. In order to do this, both Translation and the Display Number Modification tables MUST be provisioned to send numbers with NPI = PUBLIC and NOA= INTERNATIONAL to this endpoint. NOTICE: This attribute can be configured both for SIP Trunking and for SIP Private Networking endpoints. If the endpoint attribute Send International Numbers in Global Number Format (GNF) is set to true on a SIP Private Networking endpoint, then all public numbers are sent to this endpoint in GNF format. BT/BTIP Recommendation is to send E.164 (if GNF = E.164 -> On) Global numbering format i.e. starting with a plus sign followed by the complete international number e.g. +49891000100	**ON**
Rerouting Direct Incoming Calls	An OpenScape Voice subscriber that is forwarded to another user located at another OpenScape Voice or QSIG-compliant PINX will perform rerouting where the calling user's system is requested to perform the forwarding to the forwarded to party. If the rerouting request is rejected, OpenScape Voice shall perform forward-switching on behalf of the calling party. Subscriber rerouting may be triggered when a call destined for a remote subscriber - for example, in a branch office - is blocked by congestion or outage of the LAN/WAN link. When subscriber rerouting occurs, it may or may not lead to gateway rerouting. Beginning in V4, subscriber rerouting accommodates the needs of customers that need access to certain OpenScape Voice features - for example, group features that are needed by subscribers in a branch.	**OFF**

	Select this attribute to allow subscriber rerouting of incoming calls through the SIP endpoint (that are not forwarded). This attribute is not commonly used, and should not be selected for gateway endpoints. Check this checkbox to enable the rerouting of direct incoming calls through the PSTN. Values: Enabled/Disabled. Note: Although using Subscriber Rerouting through the PSTN is useful during WAN failures and CAC bandwidth restrictions, it can also lead to additional charges for the PSTN calls.	
Rerouting Forwarded Calls	If selected (enabled), this attribute allows subscriber rerouting of incoming calls through the SIP endpoint that are forwarded to a survivable SIP subscriber. Note : Although using Subscriber Rerouting through the PSTN is useful during WAN failures and CAC bandwidth restrictions, it can also lead to additional charges for the PSTN calls.	ON
Enhanced Subscriber Rerouting	This is the ability to reroute forwarded calls and hunt group calls. If selected (enabled), this attribute enables enhanced subscriber routing, which pertains to the ability to reroute forwarded calls and hunt group calls.	ON
Automatic Collect Call Blocking Supported	A collect call is a telephone call in which the calling party wants to place a call at the called party's expense and billed on their home telephone bill. When this option is enabled, calls from a PSTN Gateway (e.g. AudioCodes) to the subscriber result in additional SIP signaling (SIP INFO request) between OpenScape Voice and the PSTN Gateway. Note: The PSTN Gateway recognizes this additional SIP signaling as an indication that collect calls are not allowed to this subscriber and initiates special CAS/ISDN signaling procedures ('double answer') towards the PSTN central office. These CAS/ISDN signaling procedures result in the call being cleared by the central office if the incoming call is a collect call. If the incoming call is not a collect call then the call proceeds as normal.	OFF
Send Authentication Number in P-		OFF

Asserted-Identity header	The authentication number is the number that the PSTN provider expects in order to allow the call to proceed. It depends on the provider which Authentication Header is used to get the authentication information. Three different parameters can be set to give the provider the required diverting or transferring party to appear in one of the following headers:	
Send Authentication Number in Diversion Header	If this attribute is enabled, the Do Not Send Diversion Header attribute must be disabled. Note: This attribute only applies to SIP Trunking endpoints.	**ON (required in the scope of Call transfer, to send to Orange the number of the site which performs the call transfer)**
Send Authentication Number in From Header	The authentication number is the number that the PSTN provider expects in order to allow the call to proceed. It depends on the provider which Authentication Header is used to get the authentication information. Some providers only use the From header and therefore require the diverting or transferring party to appear in the From header. Others look in the P-Asserted-Identity for this information. Others again look in the Diversion header. Note: This attribute can only be configured for SIP Trunking endpoints. This attribute is automatically disabled for SIP Private Networking endpoints. SIPQ Truncated MIME The private network allows 8k registered user agents/clients to communicate with other users/resources in the private network connected via LAN/WAN using SIP protocol, or, for migrating customers, SIPQ protocol (i.e., SIP signaling with QSIG protocol embedded as a MIME for call control and supplementary service interoperability) for interworking with legacy QSIG private networks. SIP Trunking is used to interwork calls over the public network (IP or non-IP based) via "mediating GWs" (e.g., RG8700, SBC) which provide functions such as Network Address Translation (NAT), proxy services, media conversion.	**OFF**
Use SIP Endpoint Default Home DN as Authentication Number	If this attribute is set, the Default Home DN provisioned for the SIP endpoint is used to populate the authenticated number.	No impact on the SIP trunk - No Orange recommendation

Use Subscriber Home DN as Authentication Number	If this attribute is set, the OSV call originator or feature subscriber's Home DN is used to populate the authenticated number. NOTICE: The attributes Use SIP Endpoint Default Home DN as Authentication Number and Use Subscriber Home DN as Authentication Number are used to control what authentication identity is to be used when sending the INVITE requests towards a SIP endpoint. They are mutually exclusive. The default (unselected or unchecked) identifies that the existing OSV identity field selection logic applies.	No impact on the SIP trunk - No Orange recommendation
Set NPI/TON to Unknown	This endpoint attribute only applies to SIP-Q Private Networking endpoints. It is unchecked and grayed out for SIP Private Networking and SIP Trunking endpoints. When set, all presentation numbers sent to the SIP-Q PBX or gateway will have their numbering plan identifier and type of number reset to Unknown. This is necessary in case the SIP-Q network was set up using an unknown numbering plan. This attribute will be checked by SIPSM.	No impact on the SIP trunk - No Orange recommendation
Include Restricted Numbers in From Header	If the SIP Trunking Endpoint Profile's Privacy Support is set to Full (or Full-Send) and the SIP endpoint has the "Include Restricted Numbers in From Header" attribute, the OpenScape Voice SHALL NOT anonymize the Name and User portion of the From header field when the calling party identity is restricted. Note: This attribute is only be configurable for SIP Trunking endpoints and it is automatically disabled for SIP Private Networking endpoints. In addition, this attribute makes only a difference if the SIP Trunking Endpoint Profile has Privacy Support set to Full or Full-Send.	**OFF**
SIPQ Truncated MIME	The private network allows 8k registered user agents/clients to communicate with other users/resources in the private network connected via LAN/WAN using SIP protocol, or, for migrating customers, SIPQ protocol (i.e., SIP signaling with QSIG protocol embedded as a MIME for call control and supplementary service interoperability) for interworking with legacy QSIG private networks. SIP Trunking is used to interwork calls over the public network (IP or non-IP based) via "mediating GWs" (e.g., RG8700, SBC) which provide functions such as Network Address Translation (NAT), proxy services, media conversion.	**OFF**
Enable Session Timing	SIP SM provides the Session Timing endpoint attribute (Endpoint_Session_Timer) that will identify the Session Timing option per SIP-NNI/SIPQ endpoint.	**ON**

When enabled, session timing will be possible on the SIP-NNI/SIPQ interface for all calls that exist on that link.

Enable/disable session timing on a specific endpoint:

If system wide session timing is disabled then the session timing on the endpoint depends on the value of the "Enable Session Timer" attribute:

> When the last attribute is true session timing is invoked

> When the last attribute is false session timing is not invoked.

If session timing is enabled the SIP INVITE request to NNI and SIP endpoints will include the tags to enable session timer for that call. OpenScape Voice and the endpoint will negotiate who will refresh the session during the call (usually OpenScape Voice ends up being the refresher).

The RTP parameter Srx/Sip/Session_Timer must be set to YES for this attribute to work. If it's set to NO, OpenScape Voice will never attempt to refresh the SIP sessions, even this attribute is enabled for a specific endpoint.

There will be no linkage between the switch wide session timing attribute (via RTP parameter) and the endpoint attribute to control session timing.

The following rules to enable/disable session timing will apply for various endpoints

Switch-wide optionRTP parameter	SIPNNI/SIPQ Endpoint attribute	Session timing on subscriber devices	Session timing on SIP-NNI/SIPQ Endpoint
Session Timing Enabled	Session Timing Disabled	Session Timing Enabled	Session Timing Disabled
	Session Timing Enabled	Session Timing Enabled	Session Timing Enabled
Session Timing Disabled	Session Timing Disabled	Session Timing Disabled	Session Timing Disabled
	Session Timing Enabled	Session Timing Disabled	Session Timing Enabled

Note:

	There is no linkage between the RTP parameter to control session timing and the endpoint attribute (applicable per endpoint). RTP parameter applies to subscribers only. Endpoint attribute applies per endpoint (SIP or SIPQ). Default value for the attributes is false which is applied during upgrades.	
Ignore Answer for Announcement		**OFF**
Enable TLS RFC5626 Ping	The attribute enables the RFC5626 connectivity check feature for outgoing TLS connections. The default value for this attribute is disabled/unchecked.	**OFF**
Enable TLS Dual Path Method	The attribute enables the 'Dual Path' method, in which a client to server TLS connection is used for all outgoing SIP requests. SIP responses are expected to be received on the same TLS connection as the SIP request that is responded to. The default value for this attribute is disabled/unchecked. IMPORTANT: The attributes Enable TLS RFC5626 Ping and Enable TLS Dual Path Method can be selected only for MTLS endpoints. To set an Endpoint as MTLS the Transport protocol value must be set to MTLS.	**OFF**
Reserve Attributes for Endpoints	The intention of the reserved attributes is to use them only in exceptional cases where the regular process of adding endpoint attributes can not be applied due to time constraints. Usage of these reserve attributes must be explicitly approved by development management before proceeding. There are three Reserve Attributes available: – Reserve 4 – Reserve 5 – Reserve 6 INFO: Once a Reserve Attribute has been used then it should be replaced with a proper named attribute as soon as practical.	**OFF**
Use extended max count for loop prevention	The attribute is used for Endpoints that common numbers terminate too and you want to allow common numbers to use a higher max CFLoop counter (i.e. RTP parameter Srx/Service/CFLoopMaxCountExtended) while maintaining a low max counter for the overall system (i.e. RTP Parameter Srx/Service/CFLoopMaxCount). When the attribute is set then the extended max counter has the value of RTP parameter Srx/Service/CFLoopMaxCountExtended.	No impact on the SIP trunk - No Orange recommendation

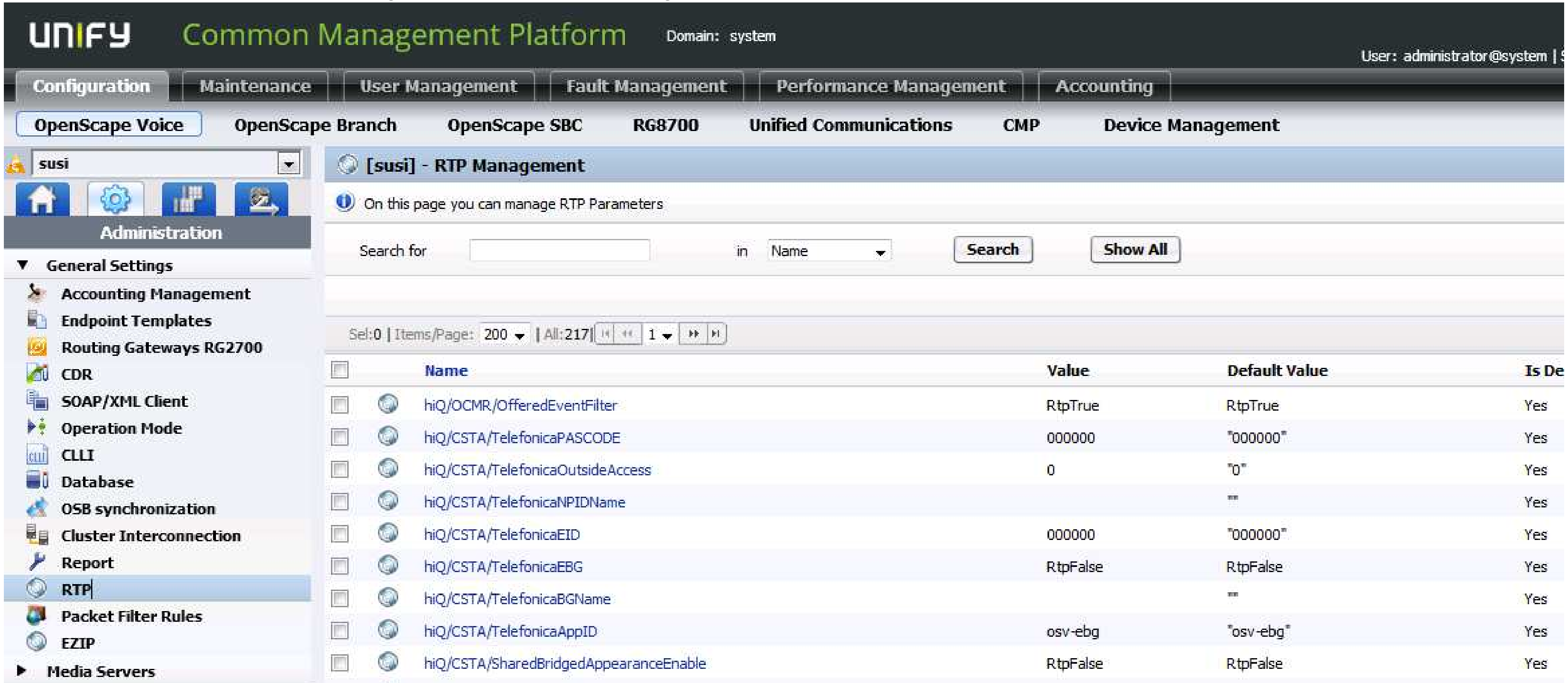
Do Not Audit Endpoint	Support for OPTIONS within OpenScape Voice is limited to sending OPTIONS requests as an audit mechanism or as a heartbeat mechanism between a network elements. OpenScape Voice does not currently use OPTIONS to discover UA capabilities OpenScape Voice is able to process OPTIONS requests received from the Service Provider, according to RFC3261. By setting this attribute, the audit of that specific Endpoint can be turned off. The default value is enabled. INFO: The Do Not Audit Endpoint attribute should only be used for dummy Endpoints.	**OFF**
Use Proxy/SBC ANAT settings for calls to subscribers	This attribute can be selected only for proxy endpoints ('SIP proxy' attribute set).	**OFF**
Support for Callback Path Reservation		No impact on the SIP trunk - No Orange recommendation
Send Progress to Stop Call Processing Supervision Timer	In case of an incoming call to OSV to send a 183 Session Progress message before 180 is send to prevent from timeout.	**OFF**
Limited PRACK Support	The PRACK-Lite feature provides a limited form of RFC3262 PRACK within OSV, supporting PRACK on a half-call basis and only for SIP network-network interfaces: – There is no end-to-end PRACK behavior - OSV as a B2BUA supports all requirements for PRACK as a SIP UAC or SIP UAS, i.e., with PRACKLite,	**ON**

	PRACK interworking is always performed on each interface independently. – OSV does not support PRACK for SIP subscriber interfaces. A SIP Subscriber will not receive any indications that PRACK is used in the network. – CSTA, SIP-Q and OSV Services are not aware of any PRACK communication requirements – PRACK interworking is supported only if enabled on a per-SIP network-network interface basis. Only if PRACK support is enabled will a SIP network-network interfaces receive indications from OSV that PRACK is supported or required.	
Support Media Redirection		No impact on the SIP trunk - No Orange recommendation
Voice Mail Server	The attribute is used to indicate whether Message Waiting Indication messages (SIP NOTIFY messages) are allowed to be sent towards the Endpoint.	No impact on the SIP trunk - No Orange recommendation
Disable Long Call Audit	When calling or called party has this attribute set to true, long call audit is disabled for this call. Default value is unchecked. If the attribute is checked then it will eliminate the impact of the long call duration timer on Hoot and ARD (Automatic Ring Down) lines used in trading solutions. It will also use RTP Srx/Sip/Reduced_Session_Timer_Value to define the minimum session refresh value for calls to/from the SIP endpoint with this attribute checked. The default value for Srx/Sip/Reduced_Session_Timer_Value is 90000 (90 seconds). The allowed range for the parameter is 60000-1800000.	No impact on the SIP trunk - No Orange recommendation
Send/Receive Impact Level	The attribute is used to control the 'Impact Level' notifications that the endpoint sends/receives to/from other endpoints. 'Impact Level' notifications inform the user when an incoming call originates from a lower security zone, or when an outgoing call terminates in a lower security zone. Possible values: Checked and Unchecked. Default value: unchecked (false). NOTICE: The attribute is applicable only for SIP-Q endpoints. In addition appropriate SIP settings must be configured in order for the attribute to be enabled.	No impact on the SIP trunk - No Orange recommendation
Allow endpoint to Unregister Stale Registrations	When this endpoint attribute is set, unregistration messages initiated by the endpoint will not be challenged by OSV with digest authentication as long as the endpoint is recorded to have been on the path that was taken on the initial registration of the contact which expired at this endpoint.	No impact on the SIP trunk - No Orange recommendation
Enable Media Termination Point (MTP) Flow	This EP attribute must be set when interworking with Cisco™ endpoints that have the Media Termination Point (MTP) feature enabled.	No impact on the SIP trunk - No Orange recommendation

Video Call Allowed	If the Video Call Allowed check mark is turned ON (default), then the OpenScape Voice will allow video calls across the server. If the Video Call Allowed check mark is turned OFF, then even if endpoint makes video calls, the port of all video m-lines will be set to zero by the OpenScape Voice server before routing the call to intended receiver.	**OFF**
Trusted Subscriber	When this SIP subscriber endpoint attribute is set then OSV offers the capability to verify whether the IP address used by the SIP subscriber in the bottom Via header is trusted. The attribute is used to support backward compatibility of RTP flag Srx/Main/AuthTraverseViaHdrs with the RtpTrue setting.	No impact on the SIP trunk - No Orange recommendation
Enable Fast Connect	This Endpoint attribute is available only for SIP-Q endpoints and when checked it enables a fast connection for SIP-Q connections in direct call scenarios.	No impact on the SIP trunk - No Orange recommendation
Circuit Connector Appliance	This Endpoint is applicable only to non-subscriber endpoints and when checked OSV supports sending/receiving ansible client API json mime objects in the body of SIP messages over the SIP trunking interface.	No impact on the SIP trunk - No Orange recommendation
Add Route Header	This Endpoint SIP attribute is applicable only for SIP Trunking endpoints and, when checked, enables adding a Route Header to SIP requests other than the initial INVITE.	**OFF**
Disable SRTP	When the attribute is checked, then SRTP is not offered to the endpoint and removed when offered by the endpoint. An Encryption license is not checked out with this setting. When the attribute is unchecked SRTP is allowed to and from the endpoint, and If Encryption license checking is enabled in the OSV license file, an Encryption license is checked out when a subscriber registers a contact using TLS. By default the attribute is unchecked.	**ON**
Include OSV SIP User-Agent header field	It allows the SIP Provider to use this SIP attribute to be able to recognize a SIP soft switch and apply dynamically a profile to this SIP soft switch and monitor it.	**ON**
Accept x-channel header	When this attribute is checked, the Endpoint accepts and parses the SIP proprietary X-Channel header	**OFF**

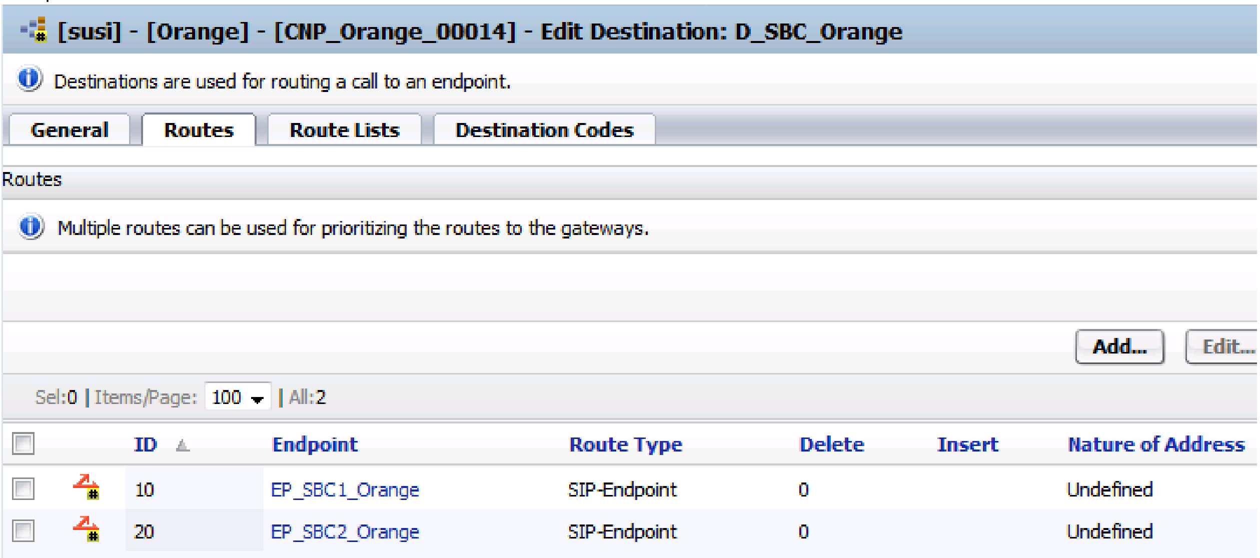
4.1.4. OpenScape Voice Resilient Telco Platform (RTP) Parameters

The required RTP parameters are configured in the Common Management Platform in the Administration area:



Parameter Name	Value	Description
Srx/Sip/Min_Session_Timer_Value	7101000	OSV will send a re-INVITE every 59.175 minutes (session refresh timer)
Srx/Sip/Session_Timer	ON	
Srx/Sip/sdpSessionMaintainer	RtpTrue	this parameter forces OSV to send the o-line value unchanged in SDP as received from the phone when set to RtpTrue.
Srx/Sip/IncludeOsvUserAgentVersionInfo	RtpTrue	This enables the inclusion of the OSV version in the User-Agent header when set to RtpTrue.

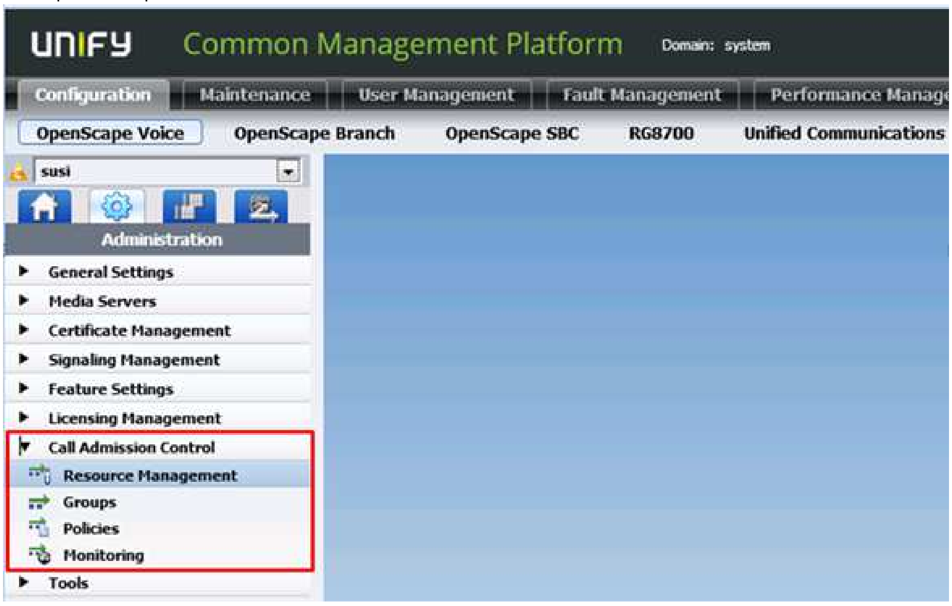
The Destination Code to be routed over the SIP trunk to Orange is forwarded to a Destination which have the both Orange SBC endpoints with different priorities (ID) configured. The lower priority value (ID) specifies the SBC endpoint to be addressed first for an outgoing call over the SIP trunk. If unavailable, the second SBC endpoint is addressed.

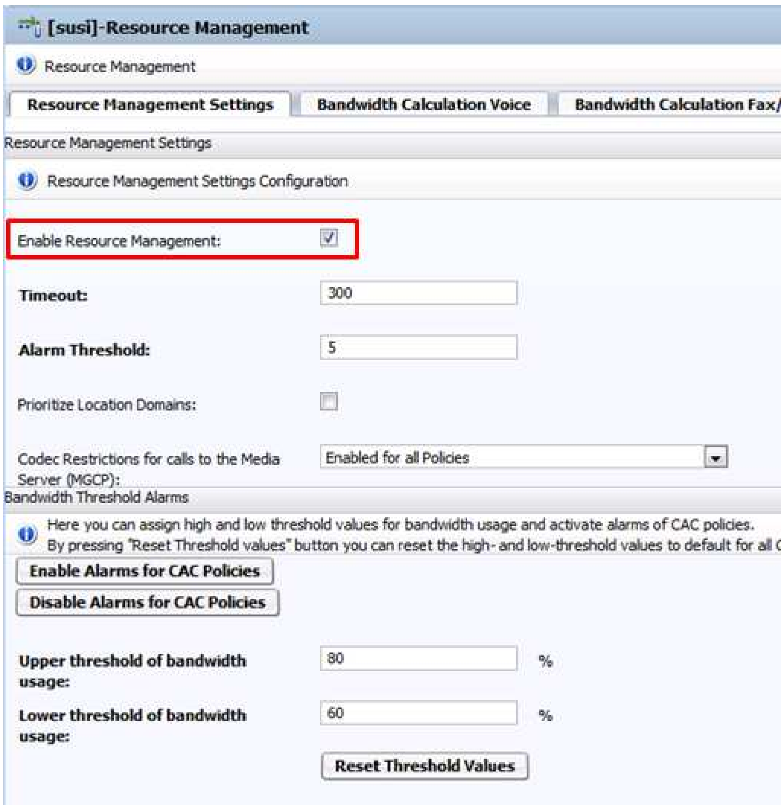


4.1.5. Call Admission Control Configuration

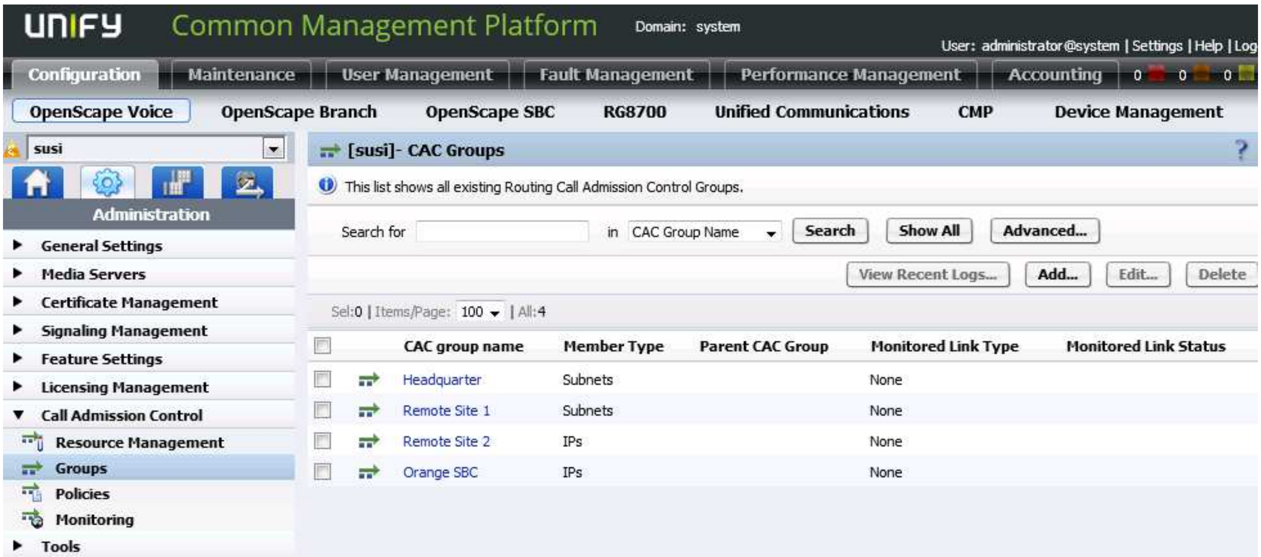
Call Admission Control (CAC) is used in OpenScape Voice to meet Orange's requirement allowing in SDP only one codec preventing a codec change without codec renegotiation.
CAC restrict beside specific allowed codecs bandwidth and/or number of calls to specific IPs, subnets, or directory numbers.
OpenScape Voice is located in the Headquarter monitoring connections to different sites via CAC.

CAC is enabled in the Common Application Platform connected to OpenScape Voice by selecting Configuration -> OpenScape Voice -> Administration -> Call Admission Control -> Resource Management, see figures below.





The exemplary CAC configuration below shows four CAC groups monitoring the connection of OpenScape Voice to different sites:
CAC Group Headquarter: Here is configured CAC monitoring connection to devices in the Headquarter specified by the Headquarter subnet as CAC Group Member.
CAC Group Remote Site 1: Here is configured CAC monitoring connection to devices in the Remote Site 1 specified by the Remote Site 1 subnet as CAC Group Member.
CAC Group Remote Site 2: Here is configured CAC monitoring connection to OpenScape Branch in the Remote Site 2 specified the OpenScape Branch IP address as CAC Group Member.
CAC Group Orange SBC: Here is configured CAC monitoring connection to the Orange SBC's specified by the SBC IP addresses as CAC Group Member.

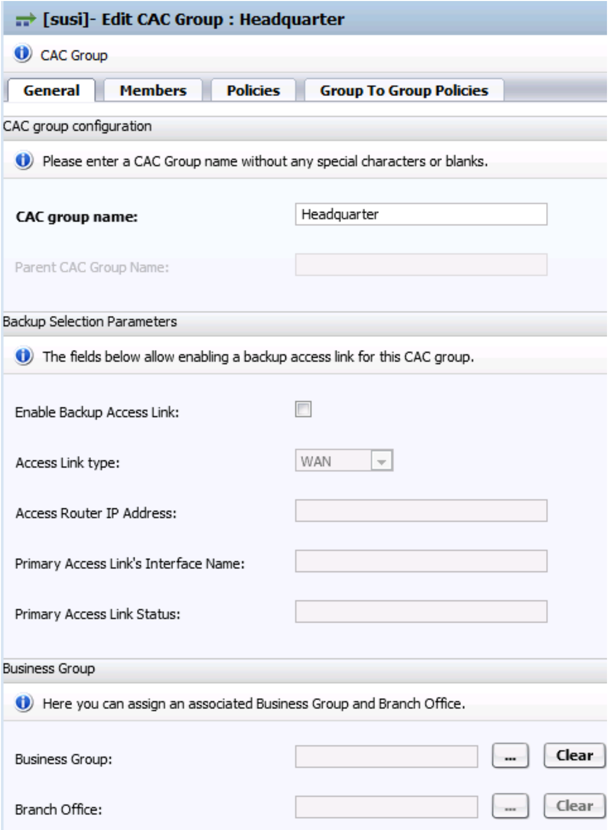


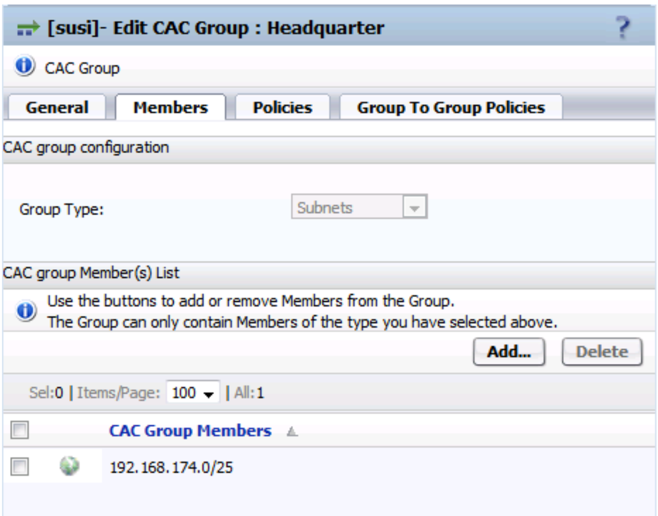
For each CAC Group is configured codec restriction to G.711 A-law and Voice and Fax as Traffic Type. If no restriction of bandwidth is required in a CAC Group its value should be set to the highest value possible.

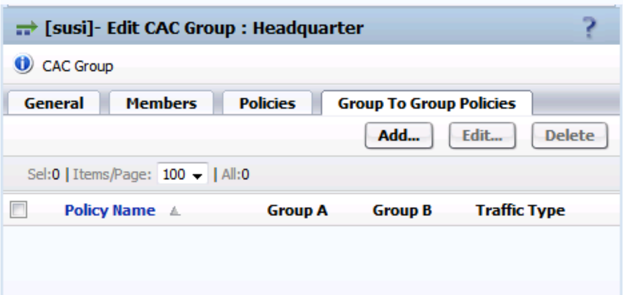
The CAC Group configuration tabs are:
General tab: Here is configured the CAC Group name
Members tab: Here is configured the monitored subnet or IP addresses as Group type *Subnet* to be monitored by CAC
Policies tab: Here is configured the monitored Traffic Type Voice and Fax. Further setting is configured in subdialogs:

General tab: Here is configured the Limit Type Bandwidth and Max Bandwidth
Voice Codecs tab: Here is configured the allowed codec, e.g. G.711 A-law.

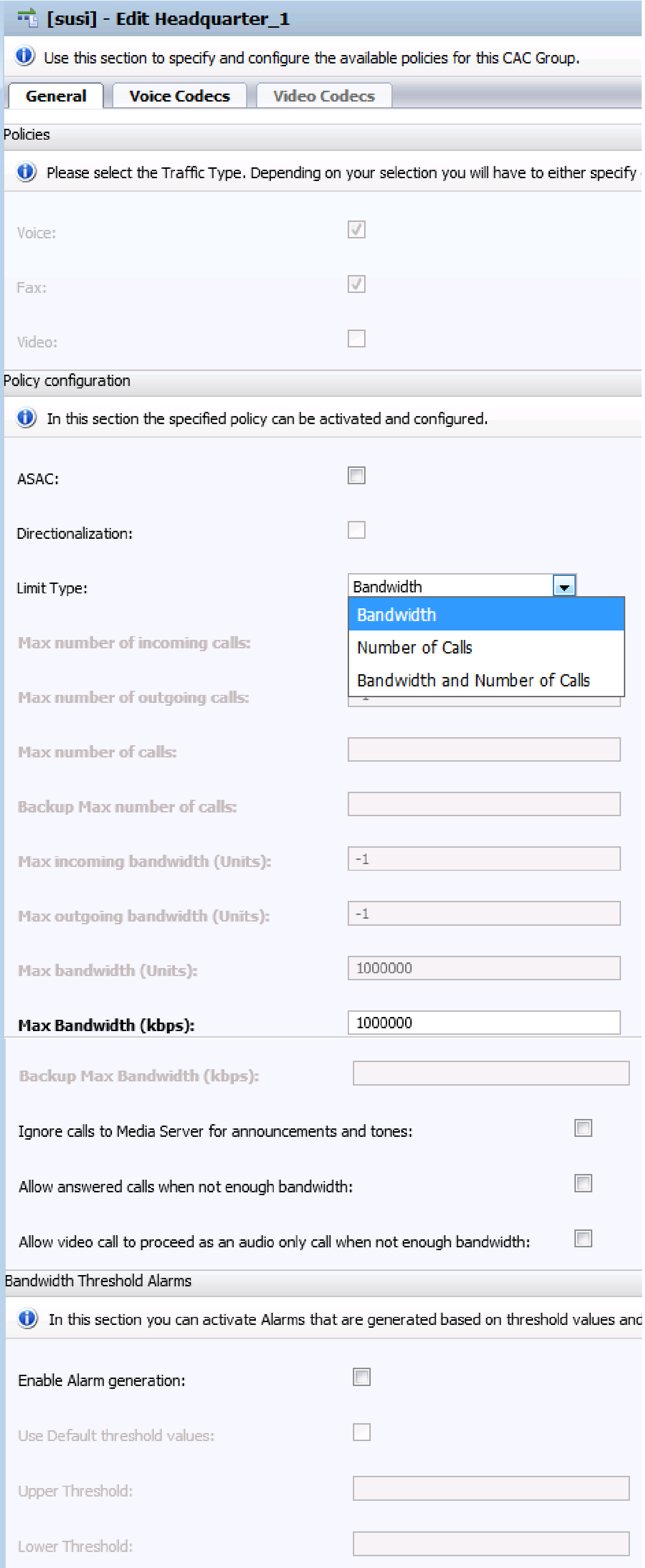
CAC Group Headquarter configuration:



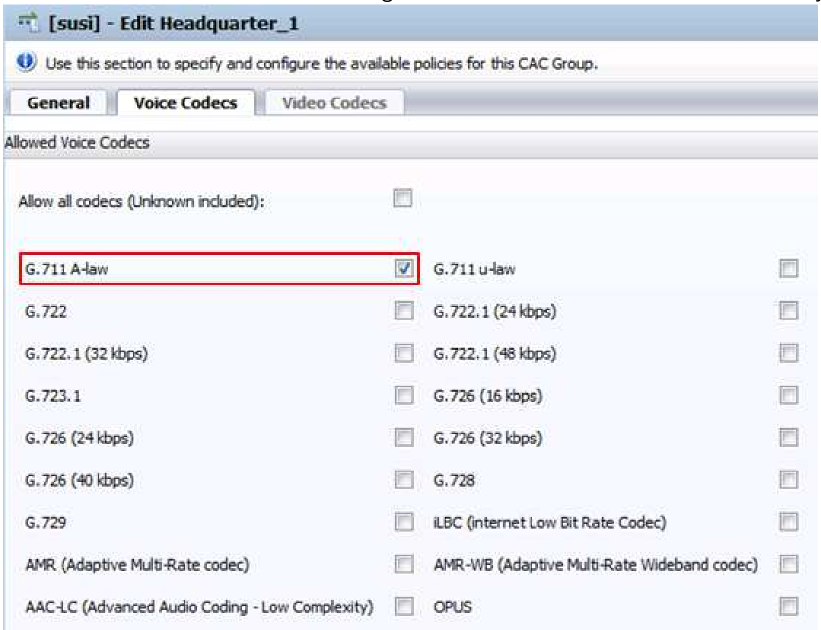




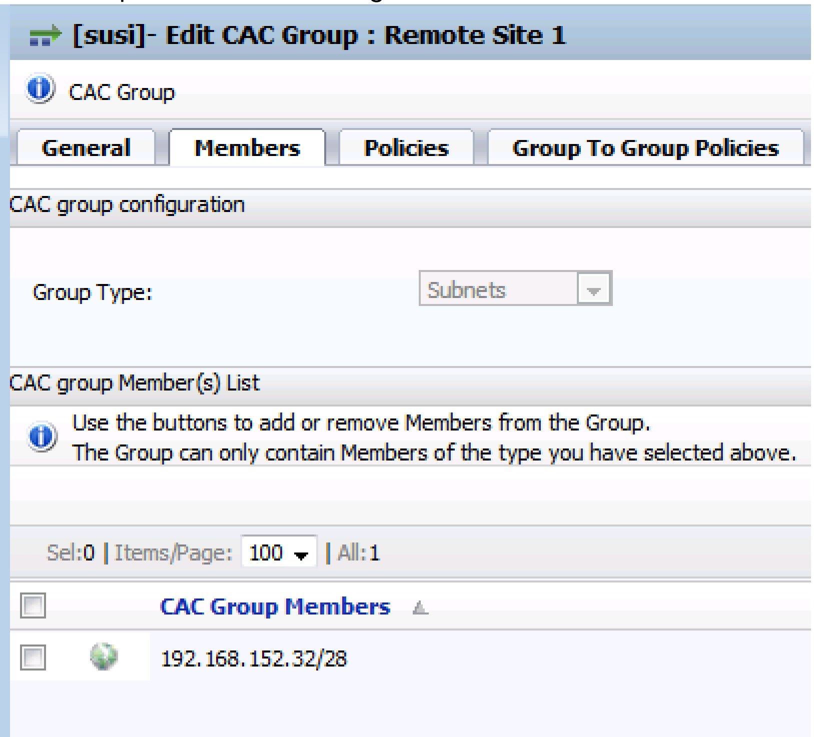
Adding or opening the **Traffic Type** entry on the Policies tab the **Limit Type** and **Max Bandwidth** can be configured:



On the Voice Codecs tab is configured to allow codec G.711 A-law only.

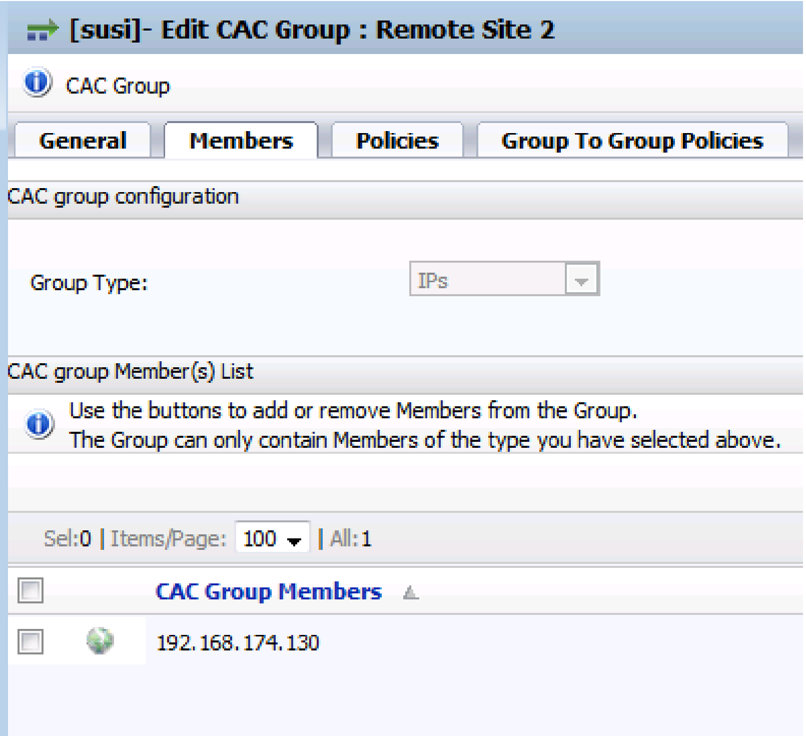


CAC Group Remote Site 1 configuration:



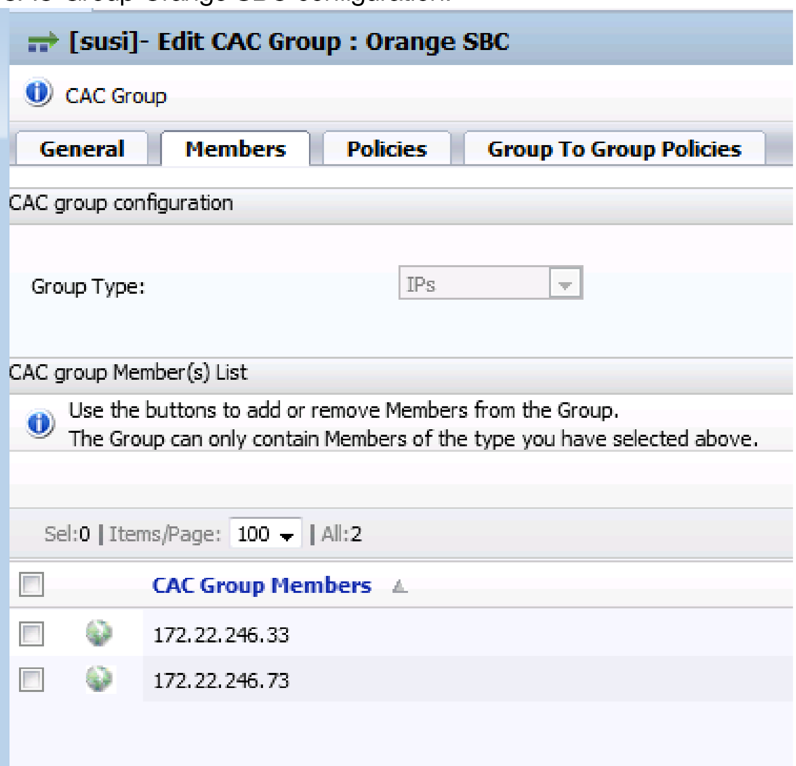
Here is configured the phone's subnet as Group Type Subnets.

CAC Group Remote Site 2 configuration:



Here is configured the OpenScape Branch IP address as Group Type IPs.

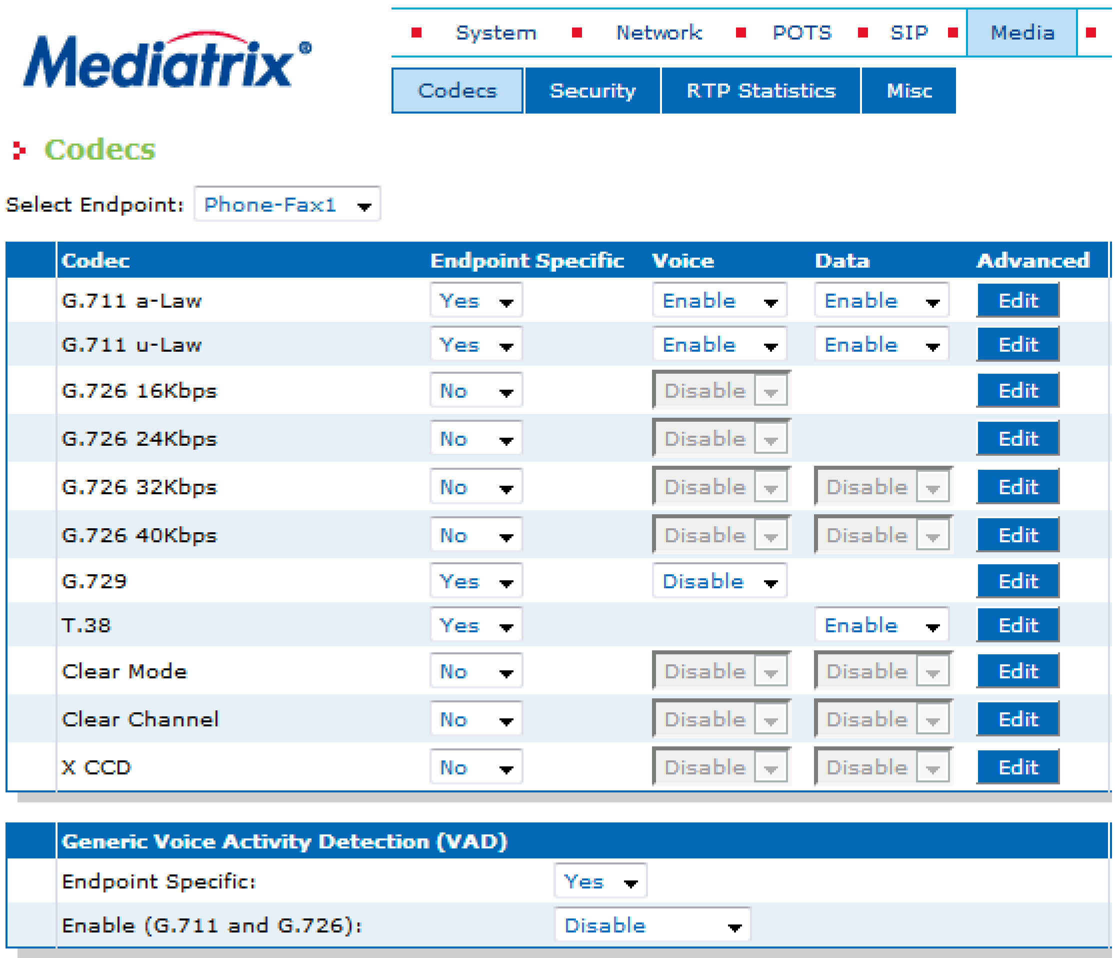
CAC Group Orange SBC configuration:

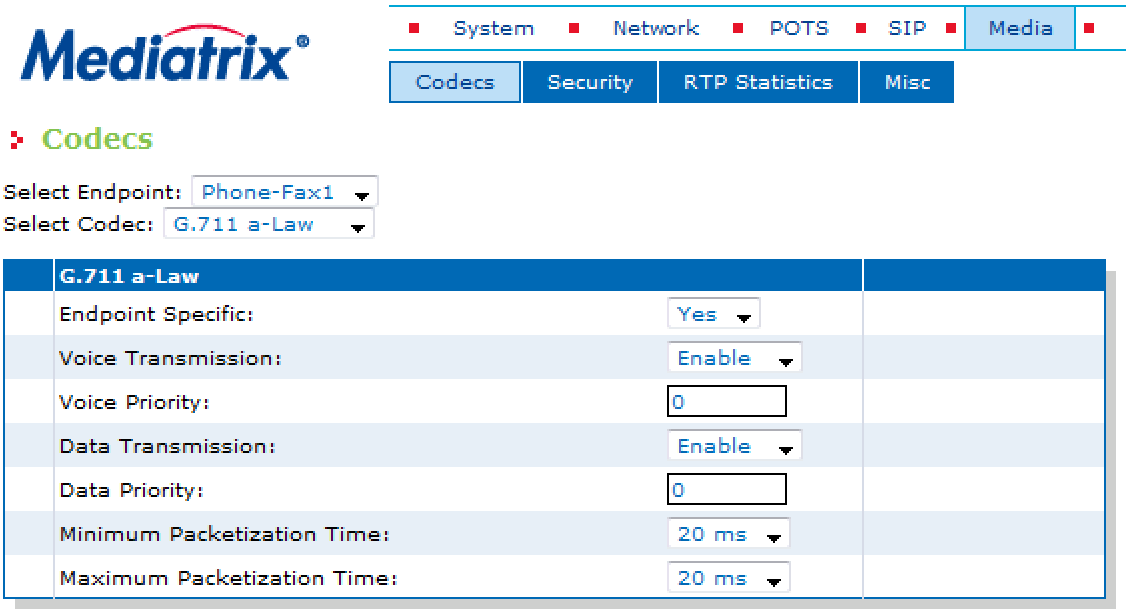


Here are configured the IP addresses of both Orange SBC's as Group Type IPs.

4.2. Configuration of Mediatrix 4102S Analog VoIP Adapter

The Mediatrix 4102S Analog VoIP Adapter is used to connect a fax machine to VoIP.





The Redundancy Level was set to 1 for the T.38 codec: