

SBC Advance Configuration Practice Guide

Copyright@2024 Shenzhen Dinstar Co., Ltd All rights reserved



- This course will introduce some common advanced features of SBC, and will describe the scenarios and configuration of these features.

Course Objective

Through this course
you will be able to



Understand some of the advanced configurations of SBC.



Understand the application scenarios of the features.



Understand the configuration of the features.

Contents

1 Number Profile

4 SIP Account

7 Trunk Group

2 Number Manipulation

5 SIP Header Manipulation

8 SIP Security

3 Number Pool

6 SIP Header Passthrough

9 Other

Number Profile

01



1.1 Application Scenarios of Number Profile

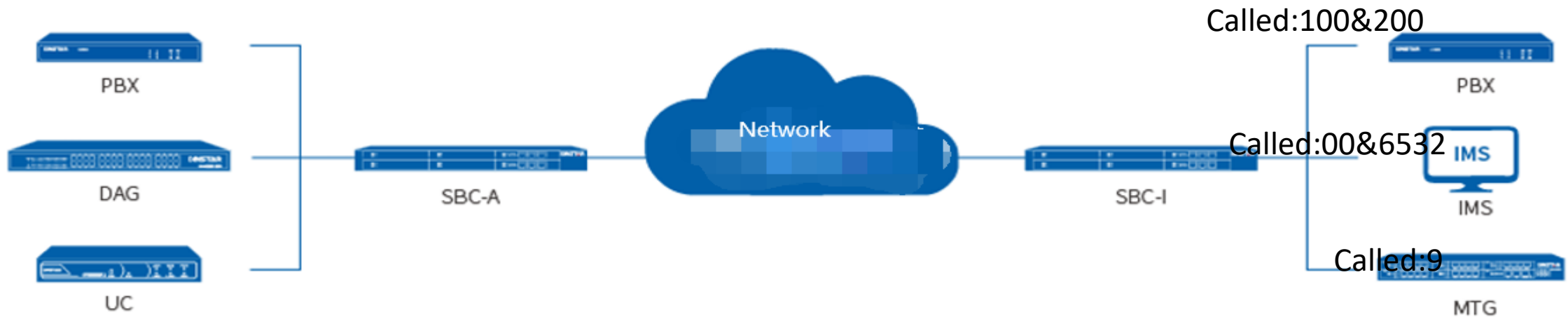


1.2 Configuration of Number Profile

Application scenarios of Number Profile

Number Profile is an important feature in SBC which is mainly used for calling/called number prefix matching during call routing. Then different call routes are applied according to the matched prefixes.

SBC may trunk to multiple platforms or devices. Then you can use the number prefix to match different routes and select different destinations.



Number Profile

Configuration of Number Profile

- Add Number Profile

1. Click on Service-Number Profile
2. Custom name
3. Configure called prefix
4. Configure other number Profile using the same method

The screenshot shows the SBC web interface with the 'Number Profile' configuration page. The 'Name' field is set to 'toPBX'. The 'Callee Prefix' field is set to '100,200'. The 'Number Profile' menu item is highlighted in the left sidebar. Below the form is a table listing existing number profiles.

Name	Description	Caller Prefix	Callee Prefix
toIMS			6532,00
toMTG			9
toPBX			100,200

Number Profile

Configuration of Number Profile

- Routing Configuration

1. Click on Service-Routing Profile-
Call Routing
2. Select number profile
3. Select source
4. Select the destination corresponding
to the number profile

The screenshot shows the SBC configuration interface. The sidebar on the left contains the following items: TransPort Endpoint, Access Network, Access SIP Trunk, Core SIP Trunk, Routing Profile, SIP Trunk Group, Call Routing (highlighted), Media Detection, CDR, Codec Profile, TLS Configuration, Recording configuration, Advanced, Number Profile, Black&White List, and Number Manipulation. The main configuration area is titled 'Call Routing' and includes the following sections:

- Media Payload Value Adaptation:** Normal(2833&rtsp)
- Secondary routing:** ☐
- Condition:** Number Profile (highlighted), toPBX
- Time Profile:** (empty)
- Caller SIP URL:** (empty)
- Callee SIP URL:** (empty)
- Source:** (highlighted), Access SIP Trunk
- SIP Methods:** (empty)
- Request URI:** (empty)
- The source of ring back tone:** remote
- Destination:** (highlighted), Core SIP Trunk
- Outbound Manipulation:** 7<PBX>

Below the configuration fields is a table titled 'Call Routing' with the following data:

Priority	Description	Condition	Destination/Manipulation Rule
1007	-	1<SIPTrunktoUC200> , toMTG	9<MTG> /
1008	-	1<SIPTrunktoUC200> , toIMS	8<IMS> /
1009	-	1<SIPTrunktoUC200> , toPBX	7<PBX> /

Contents

1 Number Profile

4 SIP Account

7 Trunk Group

2 Number Manipulation

5 SIP Header Manipulation

8 SIP Security

3 Number Pool

6 SIP Header Passthrough

9 Other

Number Manipulation

02

 2.1 Application Scenarios of Number Manipulation

 2.2 Configuration of Number Manipulation

Application scenarios of Number Manipulation

Number Manipulation is used to transform the calling/called number into a specified calling/called number according to rules.

The Number Manipulation rule processes the number sequentially Delete Prefix, Delete Suffix, Add Prefix, Add Suffix, and then matches the replacement condition

Example: Incoming call to IPPBX through SBC, the called number is 07976xxx of the line, and it is requested to be converted to 9xxx, and then sent to IPPBX



Number Manipulation

Configuration of Number Manipulation

1. Click on Service-Number Manipulation
2. Custom name
3. Select the callee number, delete prefix fill in 07976, add prefix fill in 9

The screenshot displays the SBC configuration interface. The left sidebar contains a menu with the following items: TransPort Endpoint, Access Network, Access SIP Trunk, Core SIP Trunk, Routing Profile, Media Detection, CDR, Codec Profile, TLS Configuration, Recording configuration, Advanced, Number Profile, Black&White List, Number Manipulation (highlighted with a red box and a circled '1'), and Number Pool. The main content area is titled 'Number Manipulation' and contains the following fields:

- Name:** 07976 (highlighted with a red box and a circled '2')
- Description:** (empty field)
- Caller Number:** (empty field with a '+ Add' button)
- Callee Number:**
 - Delete Prefix:** 07976 (highlighted with a red box and a circled '3', with a 'Delete' button next to it)
 - Delete Suffix:** Support RegExp
 - Add Prefix:** 9
 - Add Suffix:** (empty field)
 - Condition:** Support RegExp
 - Replacement:** (empty field)
- Synchronize the request-uri username:** (checked checkbox)
- Buttons:** Submit and Cancel

Number Manipulation

Configuration of Number Manipulation

- Method 1

1. Click on Service-Access SIP Trunk
2. Inbound Manipulation Select the corresponding number manipulation

The screenshot displays the SBC configuration interface. The left sidebar contains a menu with the following items: TransPort Endpoint, Access Network, Access SIP Trunk (highlighted with a red box), Core SIP Trunk, Routing Profile, Media Detection, CDR, Codec Profile, TLS Configuration, Recording configuration, Advanced, Number Profile, Black&White List, Number Manipulation, Number Pool, and Sip Account. The main content area shows the configuration for the selected 'Access SIP Trunk'. The configuration is divided into two sections. The top section includes: Bandwidth Limit (0 Mbit/s), Audio Media DSCP (BE), Video Media DSCP (BE), Near-end NAT, Refresh Media Penetration (checked), Respond to Media Refresh, Initial Invite Message Carrying SDP, local unregister, Passthrough RFC2833, ssrc change sync, and Without sdp Update Penetration. The bottom section includes: Rate Limit (default), Caller Blacklist, Caller Whitelist, Callee Blacklist, Callee Whitelist, Inbound Manipulation (highlighted with a red box, showing 'Number Manipulation' selected), and Inbound SIP Header Manipulation.

Number Manipulation

Configuration of Number Manipulation

Method 2

1. Click on **Service-Routing Profile-Call Routing**
2. Select the corresponding route
3. Outbound Manipulation Select the corresponding number manipulation

The screenshot displays the DINSTAR SBC configuration interface. The top navigation bar includes 'Overview', 'Service' (highlighted), 'Security', 'System', and 'Maintenance'. The left sidebar lists various configuration options: 'TransPort Endpoint', 'Access Network', 'Access SIP Trunk', 'Core SIP Trunk', 'Routing Profile', 'SIP Trunk Group', 'Call Routing' (highlighted), 'Media Detection', 'CDR', 'Codec Profile', and 'TLS Configuration'. The main content area shows the 'Call Routing' configuration for a 'Core SIP Trunk'. A red box highlights the 'Outbound Manipulation' section, which includes the following fields:

Field	Value
Destination	Core SIP Trunk
	2<IPPBX>
Outbound Manipulation	Number Manipulation
	07976

Other visible fields in the configuration include:

- Source: Core SIP Trunk
- 13<sbcsipserver> (with a 'Del' button)
- + Add button
- SIP Methods
- Request URI
- The source of ring back tone: remote
- SIP Header Passthrough

Contents

1 Number Profile

4 SIP Account

7 Trunk Group

2 Number Manipulation

5 SIP Header Manipulation

8 SIP Security

3 Number Pool

6 SIP Header Passthrough

9 Other

Number Pool

03



3.1 Application Scenarios of Number Pool



3.2 Configuration of Number Pool

Application scenarios of Number Pool

In Inbound Manipulation and Outbound Manipulation, we can select Number Pool. When selected, the calling or called number will be randomly replaced by the number in the number pool.

For example, for an outbound call to IMS, the caller must be provided by IMS. The case range is 6123000-6123999, 6223100-6223222.



Number Pool

Configuration of Number Pool

1. Click on Service-Number Pool
2. Custom name
3. Select the caller number, Configure prefix, starting number, and ending number

The screenshot shows the DINSTAR SBC configuration interface. On the left sidebar, the 'Number Pool' option is highlighted with a red box and a circled '1'. The main configuration area is titled 'Number Pool' and contains the following fields:

- Name:** A text field containing 'IMScaller', highlighted with a red box and a circled '2'.
- Description:** An empty text field.
- Caller Number:** A section containing two rows of configuration, each with a 'Prefix', 'Start Number', and 'End Number' field, and a 'Delete' button. The first row is highlighted with a red box and a circled '3'. The values are: Prefix 6123, Start Number 000, End Number 999. The second row has: Prefix 6223, Start Number 100, End Number 222.
- + Add:** A button to add a new caller number entry.
- Callee Number:** A section with a '+ Add' button.
- Synchronize the request-uri username:** A checkbox that is checked.
- Submit and Cancel:** Two green buttons at the bottom right.

Number Pool

Configuration of Number Pool

- Method 1

1. Click on Service-Routing Profile-Call Routing
2. Select the corresponding route, Outbound Manipulation Select Number Pool

SBC Overview Service Security System Maintenance Urgent Note! ! !

TransPort Endpoint

Access Network

Access SIP Trunk

Core SIP Trunk

Routing Profile

SIP Trunk Group

Call Routing ①

Media Detection

CDR

Codec Profile

TLS Configuration

Recording configuration

Advanced ^

Number Profile

Call Routing

Source Core SIP Trunk

7<PBX> Del

+ Add

SIP Methods

Request URI

The source of ring back tone remote

Destination Access SIP Trunk

6<ims>

② Outbound Manipulation

SIP Header Passthrough

request-uri Username to inManipulation user

request-uri IP Addr. remote address

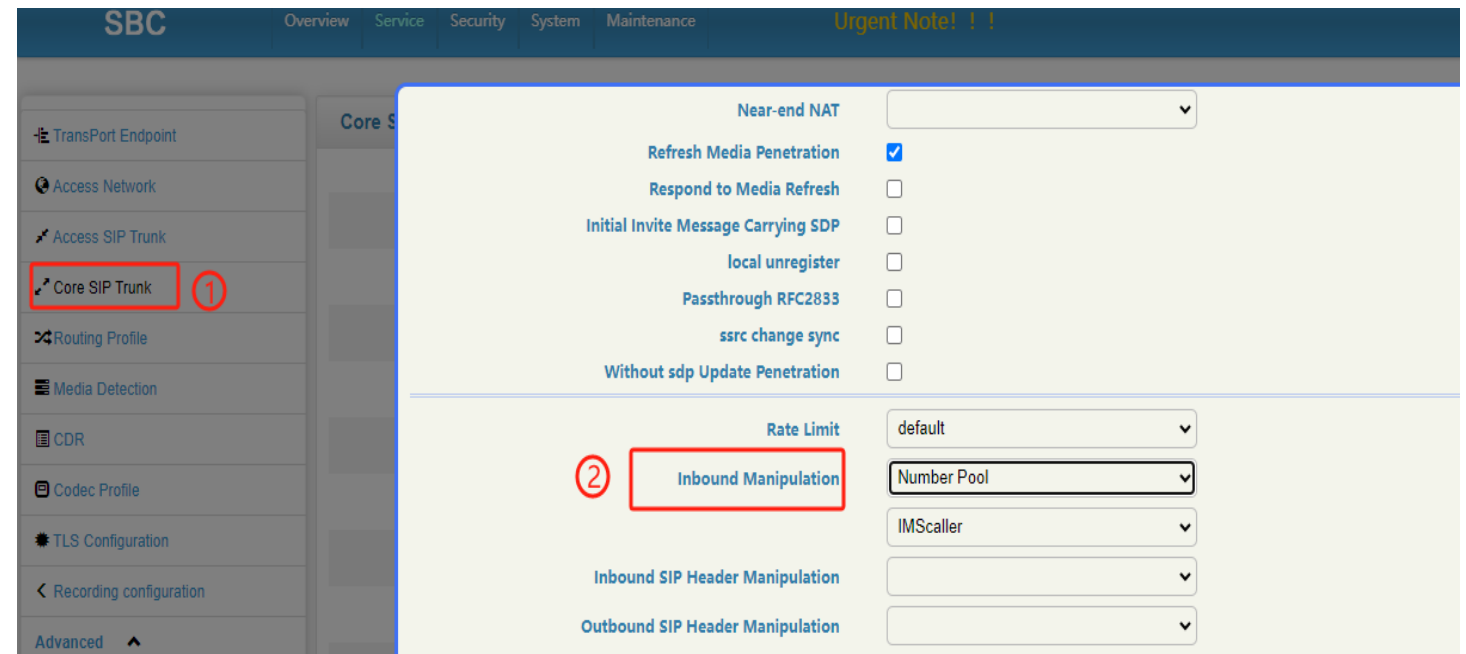
to Username to inManipulation user

Number Pool

Configuration of Number Pool

- Method 2

1. Click on Service-Core SIP Trunk
2. Select PBX, Inbound
Manipulation Select Number
Pool



Contents

1 Number Profile

4 SIP Account

7 Trunk Group

2 Number Manipulation

5 SIP Header Manipulation

8 SIP Security

3 Number Pool

6 SIP Header Passthrough

9 Other

SIP Account

04



4.1 Application Scenarios of SIP Account



4.2 Configuration of SIP Account

Application scenarios of SIP Account

SIP Account, used to configure the account that the SBC registers with the server.

SIP Account can be configured with many accounts, while Registration in Trunk can only be configured with one account.

When SIP Account is selected in Trunk, it is registered as a SIP client to SIP Server, and the caller will be replaced by the value of SIP account when calling to SIP Server.

The Registration in the Trunk is registered to the Server, and the caller will not be replaced by the SIP account value when calling to the SIP Server, it is the caller of the source.

SIP Account

Configuration of SIP Account

For example, if the account number provided by IMS is 987100--987129 and the password is admin987#, we can set it as follows

1. Click on **Service-SIP Account**
2. Configure name and flow control
3. Click add to add SIP account

SBC Overview Service Security System Maintenance Urgent Note! ! ! 28 579 0 0 0 Sync File Administ

Transport Endpoint Sip Account

Access Network

Access SIP Trunk

Core SIP Trunk

Routing Profile

Media Detection

CDR

Codec Profile

TLS Configuration

Recording configuration

Advanced ^

Number Profile

Black&White List

Number Manipulation

Number Pool

Sip Account

Name * IMSAccount

Description

Flow Count * 30

Unit Time for Flow Control * 10

Note: (Total number of accounts/flow control number) * flow control unit time < 50%-90% of the registration cycle. Otherwise, some users aren't registered, and the flow control only applies to register message. All group member accounts must follow the same registration cycle.

Account Delete All Modify All

Username Authentication ID Registered Interval Max Media Sessions

Submit Cancel

Add

SIP Account

Configuration of SIP Account

- 4. Configure username, authentication ID, and password
- 5. Configure start number, increment and number of SIP accounts

Username * 987\$1

Authentication ID * 987\$1

Password *

Registered Interval * 1800

Max Media Sessions * 30

Start Number * 100

Increment * 1

Number of SIP Accounts * 30

Submit Cancel

Note: If you want to add SIP accounts by batch, you can use the variable symbol \$1 to fill in the fields of 'Username' 'Authentication ID' 'Password'

Rule: Except \$1, all other characters filled in the fields of 'Username' 'Authentication ID' 'Password' will remain unchanged. \$1 will vary based on the configured start number, step and number of SIP accounts

Example: if you want to batch add SIP accounts from 10001000 to 10003000, you can enter 1000\$1 in the fields of 'Username' 'Authentication ID' 'Password' 1000 in the 'Start Number' field, 1 in the 'Step' field and 3000 in the Number of SIP Accounts

SIP Account

Configuration of SIP Account

6. Check if the account is correct

DINSTAR SBC

OverviewServiceSecuritySystemMaintenance

0416000Sync FileAdministrator

Transport Endpoint

Access Network

Access SIP Trunk

Core SIP Trunk

Routing Profile

Media Detection

CDR

Codec Profile

TLS Configuration

Recording configuration

Advanced

Number Profile

Black&White List

Number Manipulation

Number Pool

Sip Account

Time Profile

You have

Sip A

Account

Delete All

Modify All

Add

Username	Authentication ID	Registered Interval	Max Media Sessions	
987120	987120	1800	30	 
987121	987121	1800	30	 
987122	987122	1800	30	 
987123	987123	1800	30	 
987124	987124	1800	30	 
987125	987125	1800	30	 
987126	987126	1800	30	 
987127	987127	1800	30	 
987128	987128	1800	30	 
987129	987129	1800	30	 

<<123>>

SubmitCancel

cycle.

Otherwise, some users aren't registered, and the flow control only applies to register message.

SIP Account

Configuration of SIP Account

7. Click on Service - Core SIP Trunk, select the new account name under SIP Account

The screenshot displays the DINSTAR SBC configuration interface. The top navigation bar includes 'Overview', 'Service', 'Security', 'System', and 'Maintenance'. The left sidebar lists various configuration options: 'TransPort Endpoint', 'Access Network', 'Access SIP Trunk', 'Core SIP Trunk', 'Routing Profile', 'Media Detection', 'CDR', 'Codec Profile', 'TLS Configuration', 'Recording configuration', and 'Advanced'. The main content area is titled 'Core SIP Trunk' and contains several configuration fields. A red box highlights the 'Sip Account' dropdown menu, which is currently set to 'IMSAccount'. Below it, the 'Matching Mode' is set to 'Polling'. Other visible fields include 'Passthrough RFC2833' (unchecked), 'ssrc change sync' (unchecked), 'Rate Limit' (default), 'Inbound Manipulation', 'Inbound SIP Header Manipulation', 'Outbound SIP Header Manipulation', 'Remote Server Domain', 'Access ACL table' (with a '+ Add' button), 'Registration' (unchecked), and 'OutBound Proxy'.

Contents

1 Number Profile

4 SIP Account

7 Trunk Group

2 Number Manipulation

5 SIP Header Manipulation

8 SIP Security

3 Number Pool

6 SIP Header Passthrough

9 Other

SIP Header Manipulation

05



5.1 Application Scenarios of SIP Header Manipulation



5.2 Configuration of SIP Header Manipulation

Application scenarios of SIP Header Manipulation

When the SBC is used as a device that connects multiple platforms, for example, platform1---SBC---platform2, some Platform2 requires that incoming calls carry a certain SIP header & value, but Platform1 may not carry it. In this case, the SIP header can be modified on the SBC side to satisfy Platform2's special SIP header requirements.

SIP Header Manipulation

Configuration of SIP Header Manipulation

For example: IPPBX - SBC - IMS, IMS platform requires source messages to have rport values.

There is no rport in the message sent by IPPBX.

The rport String can be added on the SBC side.

The following is an example of an invite with rport.

```
▶ Frame 22: 949 bytes on wire (7592 bits), 949 bytes captured (7592 bits)
▶ Ethernet II, Src: 68:57:00:10:02:54 (68:57:00:10:02:54), Dst: DinstarTechn_40:e8:22 (f8:a0:3d:40:e8:22)
▶ Internet Protocol Version 4, Src: 10.133.1.253, Dst: 10.129.10.106
▶ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
▼ Session Initiation Protocol (INVITE)
  ▶ Request-Line: INVITE sip:018521051005@10.129.10.106 SIP/2.0
  ▼ Message Header
    ▶ Via: SIP/2.0/UDP 10.133.1.253;branch=z9hG4bKf64a080846ebdfaed0ed7de839e3bba9;rport
    ▶ From: "01063245669" <sip:01063245669@10.133.1.253>;tag=7c1e8438eac3247b36a1e98547199095
    ▶ To: <sip:018521051005@10.129.10.106>
      Call-ID: cdebfc6ac822281b50451785a802476c@10.133.1.253
      [Generated Call-ID: cdebfc6ac822281b50451785a802476c@10.133.1.253]
    ▶ CSeq: 717891891 INVITE
    ▶ Contact: <sip:01063245669@10.133.1.253;transport=UDP>
      Supported: 100rel,replaces
      Allow: INVITE, ACK, CANCEL, BYE, OPTIONS, INFO, UPDATE, PRACK, REFER
      Content-Type: application/sdp
      Max-Forwards: 70
      Content-Length: 342
  ▶ Message Body
```

SIP Header Manipulation

Configuration of SIP Header Manipulation

1. Click on Service-SIP Header Manipulation
2. Custom name
3. Click add to add operation

The screenshot displays the SBC (Softswitch Board Controller) configuration interface. The sidebar on the left contains various configuration options, with 'SIP Header Manipulation' highlighted at the bottom. The main panel shows the 'Add' operation configuration. The 'Name' field is set to 'via_add_rport', and the 'SIP Header Type' is set to 'header'. The 'Value' field contains the expression 'Svia.\$param.\$rport'. The 'Add' button is located in the top right corner of the main panel.

Name	Description	Type	Condition	Value
rport		header		Svia.\$param.\$rport

Buttons: Save, Cancel

SIP Header Manipulation

Configuration of SIP Header Manipulation

4.Type selection header

5.Click add to add operation, Configure according to the image

Destination ID

via

\$via.\$param

\$rport

Action

add

Value Type

Token

Value

Base64

Save

Cancel

Name

rport

Description

4

Type

Header

Condition

Add

Source ID

Match

Value

Operation

Add

Destination ID

Action

Value

Value Type

Match

Rule

\$via.\$param.\$rport

add

token

-

-

Save

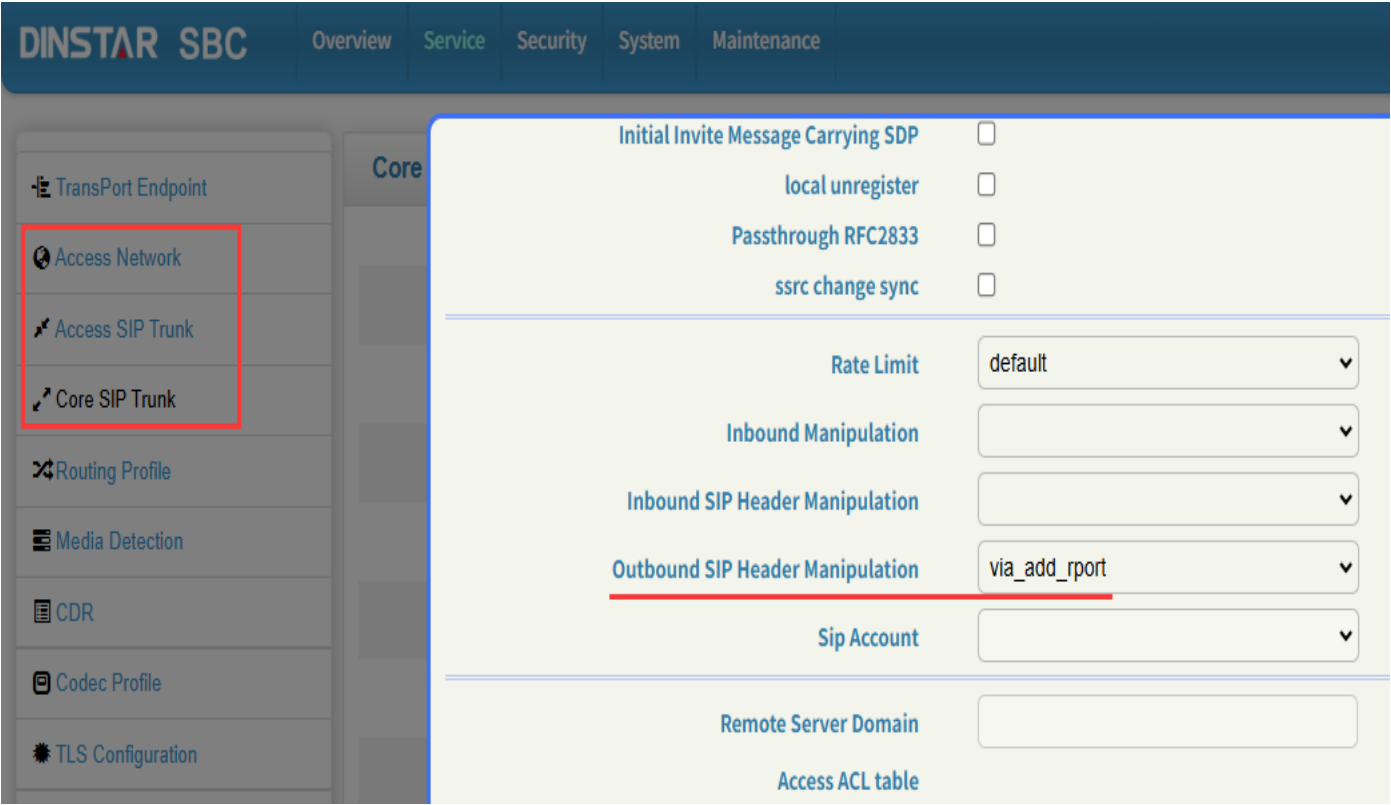
Cancel

SIP Header Manipulation



Configuration of SIP Header Manipulation

6.Check service-core SIP Trunk ,
outbound SIP Header Manipulation
Select the corresponding header
Manipulation



Contents

1 Number Profile

4 SIP Account

7 Trunk Group

2 Number Manipulation

5 SIP Header Manipulation

8 SIP Security

3 Number Pool

6 SIP Header Passthrough

9 Other

SIP Header Passthrough

06

SIP Header Passthrough

Configuration of SIP Header Passthrough

1. Click on Service-SIP Header Passthrough
2. Custom name and Fill in the header to be passthrough

The screenshot shows the SBC (Session Border Controller) configuration interface. The left sidebar contains a list of configuration options, with 'SIP Header Passthrough' highlighted at the bottom, marked with a red circle and the number 1. The main area displays the configuration form for 'SIP Header Passthrough'. The form has a 'Name' field with the value 'UserAgent' and a 'Description' field. Below these is a 'SIP Header' field with a text area containing 'User-Agent'. A red box highlights the 'Name' and 'SIP Header' fields, with a red circle and the number 2 next to it. At the bottom right of the form are 'Save' and 'Cancel' buttons. A 'Note' section at the bottom right of the interface provides a warning: 'Please think twice before you use headers of 'Allowed' and 'Sup'. The following headers can't be used for passthrough: Network, To, From, Contact, Cseq, Max-Forwards, Content-Length, Content-Type, Via, Require, Proxy-Require, Unsupported, Authorization, Proxy-Authorization, Www-Authenticate, Proxy-Authenticate, Accept, Route, Record-Route'.

SBC

Overview Service Security System Maintenance Urgent Note ! ! !

TransPort Endpoint

Access Network

Access SIP Trunk

Core SIP Trunk

Routing Profile

Media Detection

CDR

Codec Profile

TLS Configuration

Recording configuration

Advanced

Number Profile

Black&White List

Number Manipulation

Number Pool

Sip Account

Time Profile

Rate Limit

SIP Header Manipulation

SIP Header Passthrough

SIP Header

Name * UserAgent

Description

SIP Header

User-Agent

Save Cancel

Note: Please think twice before you use headers of 'Allowed' and 'Sup'. The following headers can't be used for passthrough: Network, To, From, Contact, Cseq, Max-Forwards, Content-Length, Content-Type, Via, Require, Proxy-Require, Unsupported, Authorization, Proxy-Authorization, Www-Authenticate, Proxy-Authenticate, Accept, Route, Record-Route

SIP Header Passthrough

Configuration of SIP Header Passthrough

3. Click on Service-Routing Profile-
Call Routing

4. Select the corresponding name
for SIP header Passthrough

The screenshot displays the SBC (Session Border Controller) configuration interface. The left sidebar contains a list of configuration categories: TransPort Endpoint, Access Network, Access SIP Trunk, Core SIP Trunk, Routing Profile, SIP Trunk Group, Call Routing (highlighted with a red box), Media Detection, CDR, Codec Profile, TLS Configuration, Recording configuration, Advanced, Number Profile, and Black&White List. The main panel shows the 'Call Routing' configuration for a specific profile. It includes fields for 'Callee SIP URL', 'Source' (set to 'Access SIP Trunk'), and a list of SIP methods. The 'SIP Methods' section is expanded, showing 'SIP Header Passthrough' selected from a dropdown menu (also highlighted with a red box). Other fields include 'Request URI', 'The source of ring back tone' (set to 'remote'), 'Destination' (set to 'Core SIP Trunk'), and 'Outbound Manipulation' (set to '9<MTG>'). The 'request-uri Username' and 'request-uri IP Addr.' fields are set to 'to inManipulation user' and 'remote address' respectively. The 'to Username' field is also set to 'to inManipulation user'.

Contents

1 Number Profile

4 SIP Account

7 Trunk Group

2 Number Manipulation

5 SIP Header Manipulation

8 SIP Security

3 Number Pool

6 SIP Header Passthrough

9 Other

Trunk Group

07

Trunk Group

Configuration of Trunk Group

1. Click on Service-Routing
Profile-SIP Trunk Group
2. Custom name
3. Select trunk type
4. Select routing mode
5. Select SIP trunk name and set capacity allocation

The screenshot shows the DINSTAR SBC configuration interface. The left sidebar contains a menu with the following items: TransPort Endpoint, Access Network, Access SIP Trunk, Core SIP Trunk, Routing Profile, SIP Trunk Group (highlighted with a red box and circled 1), Media Detection, CDR, Codec Profile, TLS Configuration, Recording configuration, and Advanced. The main content area displays the configuration for a SIP Trunk Group. The top section includes fields for Name (server), Description, Type (Core SIP Trunk Group), Routing Mode (Backup), Max Current InCalls (0), Max Current OutCalls (0), and Secondary routing (unchecked). The bottom section, highlighted with a red box and circled 5, shows a list of SIP Trunk Groups with columns for SIP Trunk Name and Capacity Allocation. The first entry is 3<uc> with a capacity of 300, and the second is 7<PBX> with a capacity of 300. Each entry has a Delete button. At the bottom of the list is an + Add button. Below the list are Save and Cancel buttons. A note at the bottom states: Note: The Max Current InCalls and OutCalls can be set to 0 for no limit.

DINSTAR SBC

Overview Service Security System Maintenance Urgent Note ! ! !

The configuration of SIP Trunk Group

① SIP Trunk Group

② Name: server

Description

③ Type: Core SIP Trunk Group

④ Routing Mode: Backup

Max Current InCalls: 0

Max Current OutCalls: 0

Secondary routing: ☐

⑤

SIP Trunk Name	Capacity Allocation
3<uc>	300
7<PBX>	300

+ Add

Save Cancel

Note: The Max Current InCalls and OutCalls can be set to 0 for no limit.

Trunk Group

Configuration of Trunk Group

- **Routing Mode:**

Backup mode--If the Capacity Allocation value same, all traffic to primary one, unless the trunk disconnect. If the Capacity Allocation value different, all traffic to primary one till it full

Load Balance mode--The SBC will base weight to dispatch call to different trunk, like Trunk A received 70%, other one 30%

Polling-- Polling and sending to various trunks during outgoing calls

The screenshot displays the configuration page for a SIP Trunk Group in the DINSTAR system. The left-hand navigation pane lists various configuration categories, with 'SIP Trunk Group' being the active section. The main configuration area on the right includes fields for 'Name' (set to 'server'), 'Description', 'Type' (set to 'Core SIP Trunk Group'), 'Routing Mode' (highlighted with a red box and showing a dropdown menu with 'Backup', 'Load Balance', and 'Round-Robin' options), 'Max Current InCalls', and 'Max Current OutCalls' (set to 0).

Contents

1 Number Profile

4 SIP Account

7 Trunk Group

2 Number Manipulation

5 SIP Header Manipulation

8 SIP Security

3 Number Pool

6 SIP Header Passthrough

9 Other

SIP Security

08

SIP Security

Configuration of SIP Security

SIP Security for protect the SBC and block the SIP attack.

1.Click on **Security - Security Policy-SIP Security**

2.Click on add or modify

3.Select attacked : IP Anti Attacking
Attacking/user attack

4.Select detected and Set value

The screenshot displays the DINSTAR SBC web interface. The top navigation bar includes 'Overview', 'Service', 'Security', 'System', and 'Maintenance'. The 'Security' menu is expanded, showing 'IP Security' and 'SIP Security' (highlighted with a red box and a circled '1'). The 'SIP Security' page shows a table of security policies. The 'Add' button (highlighted with a red box and a circled '2') is used to create a new policy. The 'Add' form shows the following fields: 'Priority' (123), 'Description' (empty), 'Attacked' (IP Anti Attacking, highlighted with a red box and a circled '3'), 'Detected' (Number Of Calls, highlighted with a red box and a circled '4'), 'Endpoint source' (empty), and 'Action' (Log Record). The 'Submit' and 'Cancel' buttons are at the bottom.

Priority	Description	Attacked	Detected	Action	Protected Time
124	detect register counts per ip	IP Anti Attacking	Number Of Registrations/30	Log Record	-
125	detect call counts per ip	IP Anti Attacking	Number Of Calls/10	Log Record	-
126	detect register counts per user	User Attack	Number Of Registrations/5	Log Record	-
127	detect call counts per user	User Attack	Number Of Calls/5	Log Record	-

Contents

1 Number Profile

4 SIP Account

7 Trunk Group

2 Number Manipulation

5 SIP Header Manipulation

8 SIP Security

3 Number Pool

6 SIP Header Passthrough

9 Other

Other

09

Other

Black/White List

- **Application scenarios**

The Black/White list use for Access Trunk and Access Network level.

Limit the external register/call to SBC, decrease the heavy of SBC and IPPBX

- **configuration**

1. Click on **Service-Black/White List**
2. Custom name and description
3. Configuration number

The screenshot shows the DINSTAR SBC configuration interface. The sidebar on the left contains the following menu items: TransPort Endpoint, Access Network, Access SIP Trunk, Core SIP Trunk, Routing Profile, Media Detection, CDR, Codec Profile, TLS Configuration, Recording configuration, Advanced, Number Profile, and Black&White List. The 'Black&White List' item is highlighted with a red circle (1). The main content area is titled 'Whitel' and contains a form for adding a new whitelist entry. The form has two main sections: 'Whitelist Group' and 'Description' (highlighted with a red box and circle 2), and a table for adding individual numbers. The table has columns for 'Number' and 'Description'. The first row shows '2235011' and '2235011[41-60]'. The second row shows '223501160' and an empty description field. The third row shows '22350114[1-9]' and an empty description field. The fourth row shows '22350115[0-9]' and an empty description field. Each row has a 'Delete' button next to the number field. A red box and circle (3) highlight the 'Number' and 'Description' fields for the second row. At the bottom of the form, there is a '+ Whitelist' button, a 'Submit' button, and a 'Cancel' button.

Rate Limit

- **Configuration**

1. Click on **Service-Rate Limit**

2. Click on add or modify

3. Custom name and description

4. RPS: Max SIP Register request per

seconds from remote side to this Trunk.

CPS: Max SIP Call request per seconds from remote side to to this Trunk.

Max Media Sessions: Max concurrent call in this trunk.

Note: the value should not overtop the license of SBC

The screenshot displays the DINSTAR SBC web interface. On the left sidebar, the 'Rate Limit' option is highlighted with a red box and a circled '1'. The main content area shows a modal form for adding or modifying a rate limit. The form includes a 'Name' field (circled '3'), a 'Description' field, and three rows of configuration: 'RPS' (circled '4'), 'CPS', and 'Max Media Callin Sessions', each with a numeric input field. The 'Max Media Callout Sessions' field is set to '5000'. At the bottom of the form are 'Submit' and 'Cancel' buttons. In the top right corner of the interface, there is an '+ Add' button (circled '2') and a 'Sync File' link.

Other

Codec Profile

- Configuration

1. Click on Service-Codec Profile
2. Click on add
3. Custom name
4. Select codec

The screenshot displays the DINSTAR SBC web management interface. On the left sidebar, the 'Codec Profile' menu item is highlighted with a red box and a circled '1'. The main content area shows a modal window for adding a new codec profile. This modal contains several fields: 'Name' (with 'opus' entered, circled '3' and red box), 'Description', 'Max Packetizing Time' (set to 60), 'Codec' (a list box with 'G723', 'G729', 'ILBC_13K', 'ILBC_15K', 'AMR', and 'G722' selected, circled '4' and red box), 'Payload' (set to 106), 'Packetizing Time' (set to 20), and checkboxes for 'Video Media Forbidden' and 'Penetrate MIME'. At the bottom of the modal are 'Submit' and 'Cancel' buttons. In the top right corner of the modal, there is a red box containing a question mark icon and a green '+ Add' button.

Other

Codec Profile

- Configuration

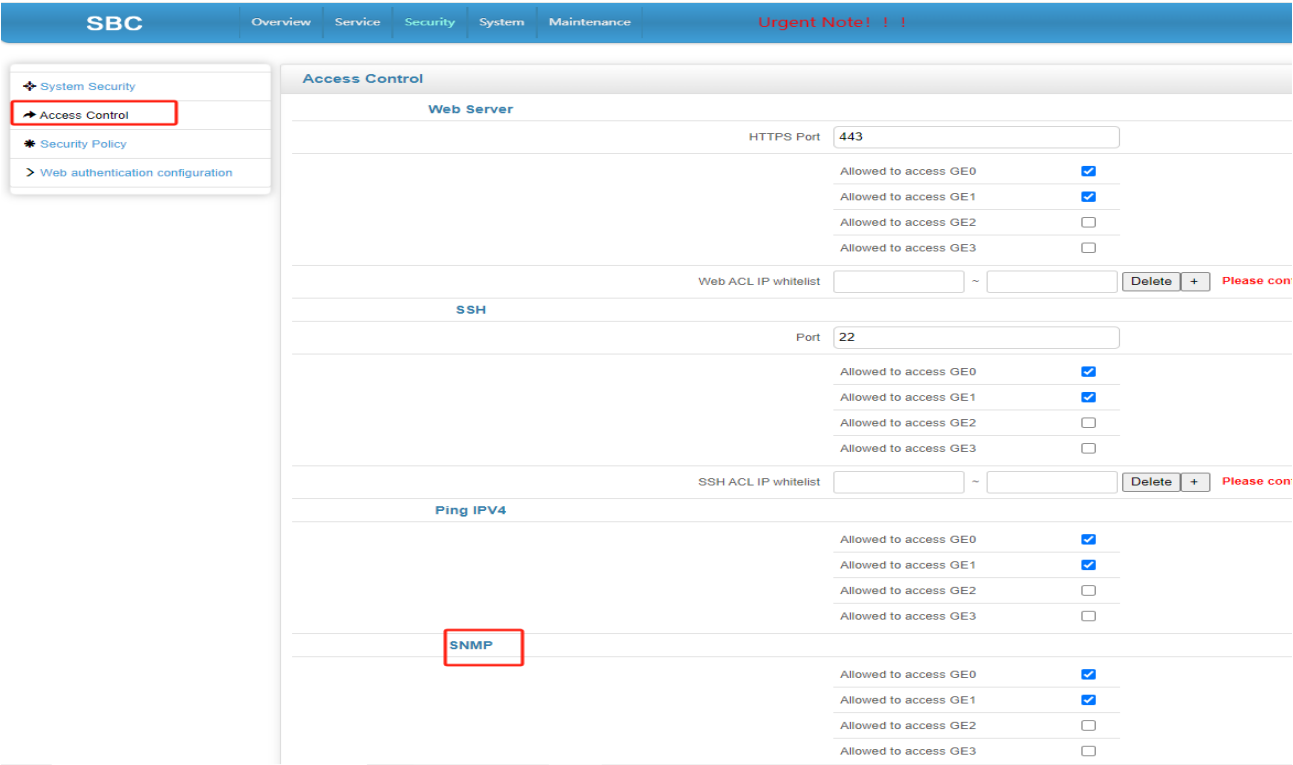
5. Click on the **Service – SIP Trunk/Access Network** according to the requirements, and select the profile name for the codec

The screenshot displays the DINSTAR SBC web interface. The left sidebar contains a menu with the following items: TransPort Endpoint, Access Network, Access SIP Trunk, Core SIP Trunk, Routing Profile, Media Detection, CDR, Codec Profile, TLS Configuration, Active And Standby, Recording configuration, Advanced, Number Profile, Black&White List, and Number Manipulation. The 'Access Network' item is highlighted with a red box. The main content area shows the configuration form for the selected item. The form includes fields for ID (10), Name, Description, Valid (checked), and Enable radius (unchecked). Below these are dropdown menus for media interface (GE0), TransPort Endpoint (GE0_1_UDP_7001), Codec (opus), DTMF Priority (local), and DTMF (RFC2833). There is also a text field for RFC2833 (101), a dropdown for Trunk Mode (Static), and a text field for Remote IP :Port. At the bottom right, there are 'Submit' and 'Cancel' buttons, and an 'Advanced' dropdown menu.

SNMP

- SBC Configuration

1. SNMP is enabled by default for the management port, and SNMP access permissions need to be enabled for other network ports in the **Security-Access Control**



The screenshot displays the SBC configuration interface. The top navigation bar includes 'SBC', 'Overview', 'Service', 'Security', 'System', and 'Maintenance'. An 'Urgent Note' is visible on the right. The left sidebar shows a tree structure with 'System Security' expanded, and 'Access Control' selected. The main content area is titled 'Access Control' and contains four sections: 'Web Server', 'SSH', 'Ping IPV4', and 'SNMP'. Each section has a 'Port' field and a table of checkboxes for 'Allowed to access GE0', 'GE1', 'GE2', and 'GE3'. The 'Web Server' section has a 'HTTPS Port' of 443. The 'SSH' section has a 'Port' of 22. The 'Ping IPV4' section has an 'SSH ACL IP whitelist' field. The 'SNMP' section is highlighted with a red box. Each section also has a 'Delete' button and a '+ Please confirm' link.

Service	Port	Allowed to access GE0	Allowed to access GE1	Allowed to access GE2	Allowed to access GE3
Web Server	443	☒	☒	☐	☐
SSH	22	☒	☒	☐	☐
Ping IPV4		☒	☒	☐	☐
SNMP		☒	☒	☐	☐

Other

SNMP

- SBC Configuration

2. Click on **Maintenance- SNMP Configuration**
3. Select SNMP version and click Edit
4. Configure SNMP port and community, and fill in the IP address for trap configuration

The screenshot displays the Dinstar SBC web interface. At the top, a navigation bar shows 'SBC' and various system status icons. A left sidebar contains a 'Log' menu with options like 'Reset', 'Ping', 'Tracer', 'Capture', 'Regular Expression', 'Warning', 'SNMP configuration', 'DRP configuration', 'NMS service configuration', 'Signal Track configuration', and 'WebRTC'. The main content area shows a success message 'The configurations has been applied successfully.' followed by two tables for 'SNMP configuration 1.0' and 'SNMP configuration 2.0'. Below these is a detailed configuration form for 'SNMP configuration 2.0' with fields for 'Open SNMP', 'SNMP Version', 'SNMP port', 'EngineID', 'Community configuration', and 'Trap configuration'. Red boxes highlight the 'SNMP configuration' menu item, the 'Community' field, and the 'IP Address' and 'Port' fields in the 'Trap configuration' section.

SNMP configuration 1.0

Open SNMP	SNMP port
Close	-

SNMP configuration 2.0

Open SNMP	SNMP port
Open	161

SNMP configuration 2.0

Open SNMP: Yes ☒ No ☐

SNMP Version: v2c

SNMP port: 161

EngineID: 0x80001f8880511226707761736700000000

Community configuration

Community	Source address
public	default

Note: The default value of the source address is default. If not, input the IP address!

Trap configuration

Trap Type	IP Address	Port	Community	Trap Language
v2c	172.28.7.49	162	public	English

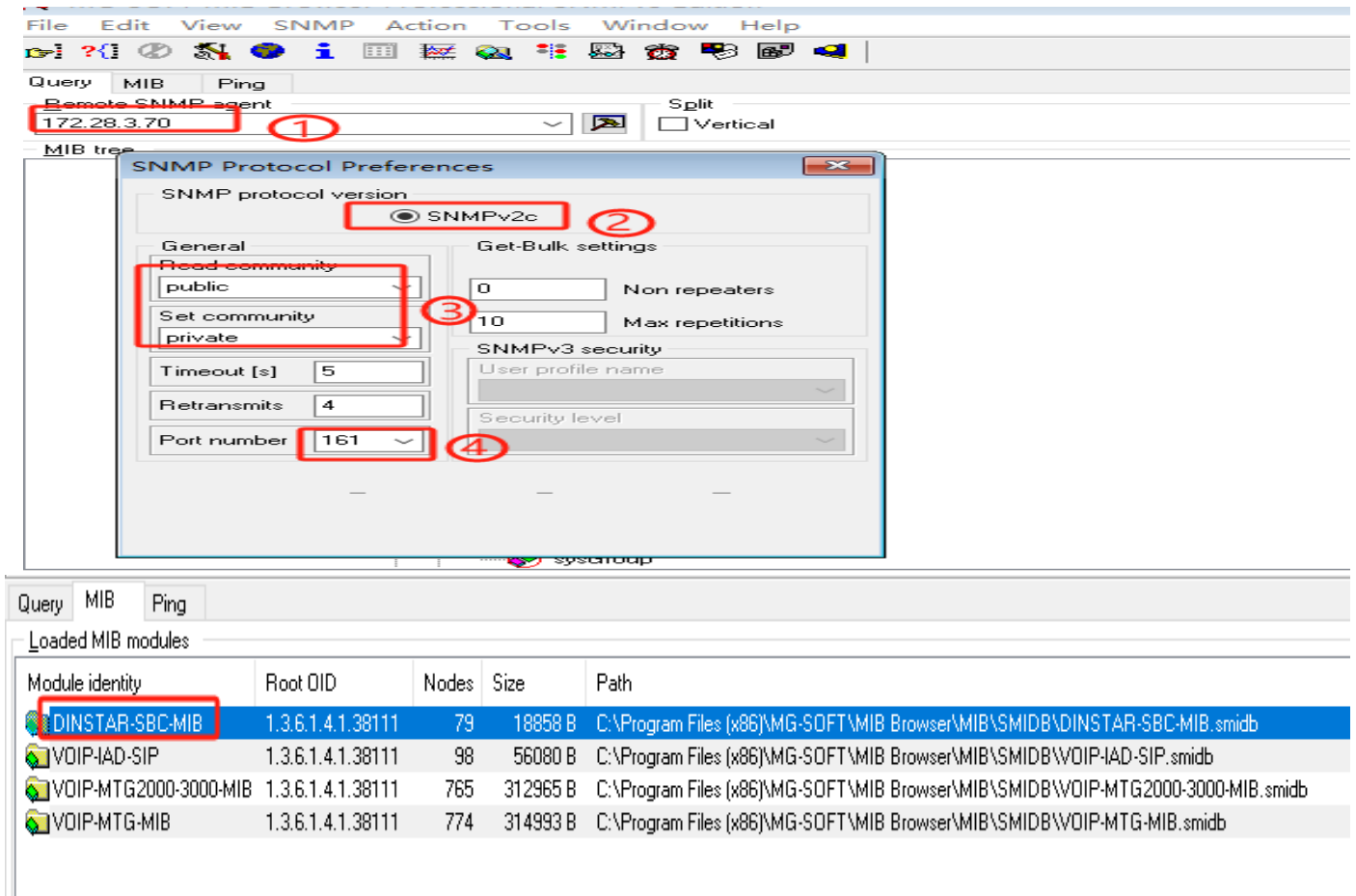
Save Cancel

Other

SNMP

- SNMP Server Configuration

1. Fill in the SBC network port IP
2. Choose SNMP version, keep the server and SBC consistent
3. Configure the community
4. Configure SBC listening port
5. Import the MIB file of SBC



Other

SNMP

- SNMP Server Retrieves SBC Information

Method 1: Find the information to be obtained on the MIB tree, right-click GET, and results will display the obtained information

Method 2: Knowing the OID of the corresponding information, one can directly query it

172.28.3.70

MIB tree

- internet
- private
- enterprises
- Dinstar
- netSnmpObjects
- netSnmpEnumerations
- netSnmpNotificationPrefix
- netSnmpConformance
- DAGParam
- MTGParam
- sbc
- device
- sbcProduct
- intflow
- system
- sysUptime
- sysCpuUsed
- sysMemoryUsed
- sysDiskUsed
- sysTemperature
- sysBootloaderVersion
- sysImageVersion
- sysAppVersion
- sysGroup

Query results

Remote address: 172.28.3.70 port: 161 transport: IP/UDP
Local address: 172.28.7.49 port: 64798 transport: IP/UDP
Protocol version: SNMPv2c
Operation: Get
Request binding:
1: sysUptime.0 (null) null
Response binding:
1: sysUptime.0 (octet string) 1days 01h:42m:18s

172.28.3.70

MIB tree

- internet
- private
- enterprises
- Dinstar
- netSnmpObjects
- netSnmpEnumerations
- netSnmpNotificationPrefix
- netSnmpConformance
- DAGParam
- MTGParam
- sbc
- device
- sbcProduct
- intflow
- system
- sysUptime
- sysCpuUsed
- sysMemoryUsed
- sysDiskUsed
- sysTemperature
- sysBootloaderVersion
- sysImageVersion
- sysAppVersion
- sysGroup

Prompt For OID - 172.28.3.70:sysCpuUsed.0

Remote SNMP agent: 172.28.3.70

OID: 1.3.6.1.4.1.38111.10.2.2.0

Get

Get Next

Get Bulk

Log only responses

Log response marker

Reuse result OID

Close after response is received

Abort

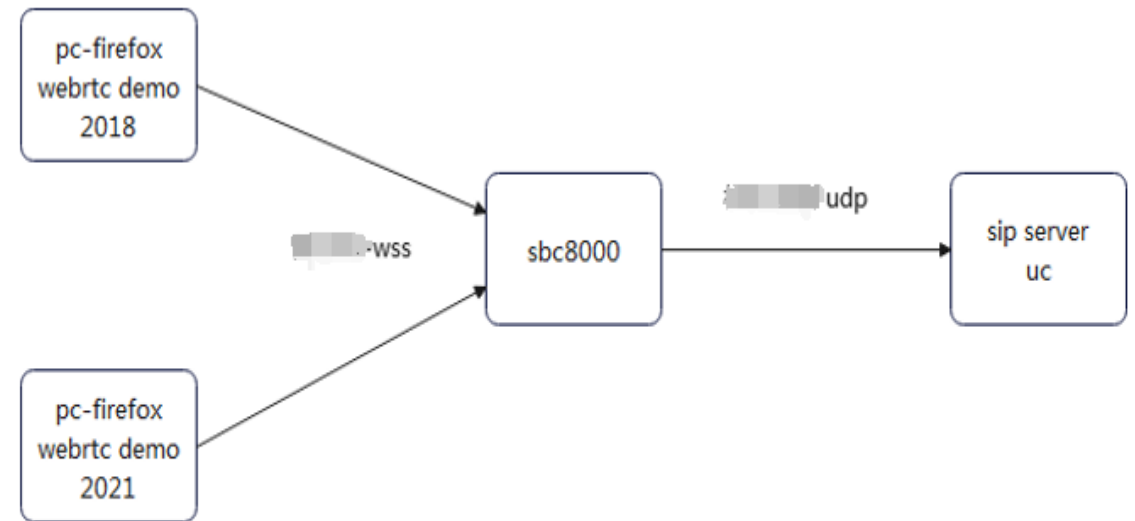
Close

Query results

Remote address: 172.28.3.70 port: 161 transport: IP/UDP
Local address: 172.28.7.49 port: 64798 transport: IP/UDP
Protocol version: SNMPv2c
Operation: Get
Request binding:
1: sysUptime.0 (null) null
Response binding:
1: sysUptime.0 (octet string) 1days 01h:42m:18s
***** SNMP PROMPT FOR OID-RESPONSE START *****
1: sysCpuUsed.0 (integer) 1
***** SNMP PROMPT FOR OID-RESPONSE END *****

WEBRTC

- SBC serves as the core network boundary proxy server (B2BUA), and users use WSS clients to initiate registration by listening to SBC's access network address
- After receiving the registration message, SBC transfers it to the server of the core SIP trunk
- The registration account and password are provided by the core network server, and SBC is a back-to-back proxy registration



Other

WEBRTC

•SBC configuration

- 1.Upload WSS certificate: Click on **System - Certificate**, upload CRT file and KEY file
- 2.Configure transport endpoint: Click on **Service - Transport Endpoint**, select interface, transport, and corresponding certificate
- 3.Configure the transport endpoint connected to IPPBX using the same method

ID	Name	Description	Interface	Port	IPv4/IPv6	Transport	Dedicated To Access Network
1	GEO_UDP_5065		GEO	5065	ip4	udp	false
2	GEO_WSS_5078		GEO	5078	ip4	wss	true

DINSTAR SBC Overview Service Security System Maintenance Urgent Notice 1/1

System Management
Web Configuration
Network
Port Mapping
Static Route
User
Date&Time
Upgrade
Backup & Restore
License
Certificate
UserBoard

Name: wss

CRT File: select file no files selected

KEY File: select file no files selected

CA File: select file no files selected

Save Cancel

Crt File List

Name	Begin Time	End Time	
crt_server.crt	2025-06-05 14:55:34 UTC	2035-06-03 14:55:34 UTC	⬆

Key File List

Name	
key_server_private.key	⬆

CA File List

Name	
------	--

DINSTAR SBC Overview Service Security System Maintenance Urgent Notice !!

TransPort Endpoint

Access Network
Access SIP Trunk
Core SIP Trunk
Routing Profile
Media Detection
CDR
Codec Profile
TLS Configuration
Recording configuration

Advanced

ID: 2

Name: GEO_WSS_5078

Description:

Valid: ☒

Dedicated To Access Network: ☒

Interface: GEO

Transport: WSS

TLS Bidirectional Verification: ☐

PEM File: wss/crt_server.crt

KEY File: wss/key_server_private.key

Port: 5078

IPv4/IPv6: IPV4

Signaling DSCP: BE

Save Cancel

Other

WEBRTC

•SBC configuration

4.Access Network: Click on **Service - Access Network**, select the media interface and transport endpoint

5.Core SIP Trunk: Click on **Service - Core SIP Trunk**, select the media interface and transport endpoint, and fill in the IP and port of the IPPBX

The screenshot shows the 'Access Network' configuration page in the DINSTAR SBC web interface. The left sidebar has a menu with 'Access Network' highlighted. The main panel contains the following fields:

- ID: 1
- Name: webrtc
- Description: (empty)
- Valid: ☒
- Enable radius: ☐
- media interface: GE0
- Transport Endpoint: GE0_WSS_5078
- IP Range: (empty) ~ (empty)
- Subnet Mask: (empty)
- + IP Range: (empty)
- Codec: default
- DTMF Priority: local
- DTMF: RFC2833
- RFC2833: 101
- Advanced: (dropdown arrow)
- Buttons: Save, Cancel

The screenshot shows the 'Core SIP Trunk' configuration page in the DINSTAR SBC web interface. The left sidebar has a menu with 'Core SIP Trunk' highlighted. The main panel contains the following fields:

- ID: 7
- Name: PBX
- Description: (empty)
- Valid: ☒
- Enable radius: ☐
- media interface: GE0
- Transport Endpoint: GE0_UDP_5065
- Codec: default
- DTMF Priority: local
- DTMF: RFC2833
- RFC2833: 101
- Trunk Mode: Static
- Remote IP :Port: 172.28.7.49:5060
- Advanced: (dropdown arrow)
- Buttons: Save, Cancel

Other

WEBRTC

- SBC configuration

6.Click on Service - Routing Profile -call Routing, configure bidirectional routing between core SIP TRUNK and access network

Transport Endpoint

Access Network

Access SIP Trunk

Core SIP Trunk

Routing Profile

SIP Trunk Group

Call Routing

Media Detection

CDR

Codec Profile

TLS Configuration

Recording configuration

Advanced

DINSTAR SBC

OverviewServiceSecuritySystemMaintenance

Urgent Note! ! !

Media Payload Value Adaptation

Normal(2833&rtp)

Secondary routing

Condition

Number Profile

Caller Username

Callee Username

Time Profile

Caller SIP URL

Callee SIP URL

Source

Core SIP Trunk

7<PBX>

Del

+ Add

SIP Methods

Request URI

The source of ring back tone

remote

Destination

Access Network

1<webrtc>

Outbound Manipulation

The configurations has been applied successfully.

Priority	Description	Condition	Destination/Manipulation Rule	
1002	uclovs	7<PBX>	1<webrtc> /	  
1003	wsstouc	1<webrtc>	7<PBX> /	  
1004	in	14<IMS>	7<PBX> /	  

WEBRTC

- WSS Terminal Registration

- 1.Fill in the network port IP and port selected for the SBC access network transport endpoint
- 2.Fill in the registered account and password assigned by the core network server

Server

172.28.3.11

["wss://172.28.3.11:5078"]

optional STUN/TURN servers

Account

6005

6005

.....

optional authorization name

Login

Other

WEBRTC

- WSS Terminal Registration

3. There will be corresponding prompts after successful registration

"6005" is logged in "172.28.3.11:5078"

Settings

Enable sound

call

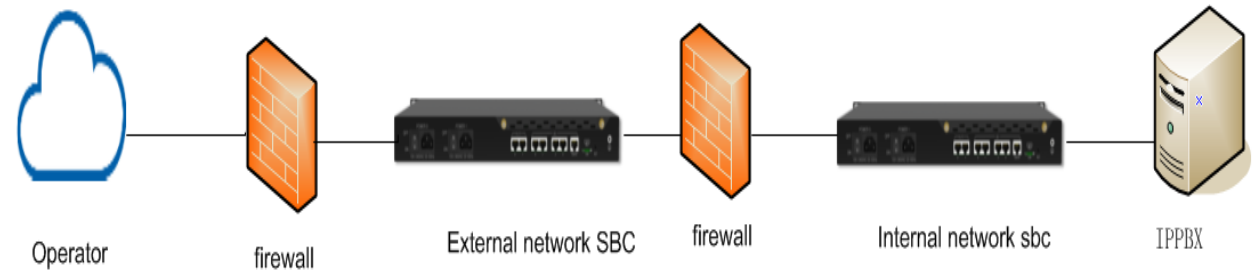
Audio

Video

Other

NAT

- There are firewalls between the internal network SBC and the external network SBC, as well as between the external network SBC and the operator equipment, to provide security protection
- The IP address of the external SBC is not in the same network segment as the operator's device, and the external SBC needs to configure NAT



Other

NAT

NAT configuration

1. Click on **Service - Access SIP Trunk**, find the access SIP trunk corresponding to the operator
2. Enable near end NAT and fill in the IP address required by the operator

The screenshot displays the SBC configuration interface. On the left, a sidebar menu lists various configuration options: TransPort Endpoint, Access Network, Access SIP Trunk (highlighted with a red box), Core SIP Trunk, Routing Profile, Media Detection, CDR, Codec Profile, TLS Configuration, Recording configuration, and Advanced. The main panel shows the configuration for the selected 'Access SIP Trunk'. It includes fields for Trunk Mode (Static), Remote IP :Port (172.27.10.10:5060), Bandwidth Limit (0 Mbit/s), Audio Media DSCP (BE), and Video Media DSCP (BE). A red box highlights the 'Near-end NAT' section, which contains a dropdown menu set to 'Static', an 'IP' field, and a 'Port' field. Below this, there are checkboxes for 'Start RTP Port under NAT', 'Refresh Media Penetration' (checked), 'Respond to Media Refresh', 'Initial Invite Message Carrying SDP', and 'local unregister'.

Summary

- The course describes application scenarios for some common advanced features of SBC and illustrates basic configuration with simple examples.

Abbreviation

- SIP: Session Initiation Protocol
- SBC: Session Border Controller



THANKS



sales@dinstar.com



www.dinstar.com



+86 755 6191 9966