MegaPath
A Fusion Company

snom ONE

IP PBX Provisioning Guide

Date: December 4, 2012
Author(s): Armando Lemus

Abstract:
snom ONE is a software-based IP PBX. The software is designed to run on the customer premise or in the cloud. This document will cover the case in which the snom ONE software-based IP PBX is installed as a server behind NAT.

INTRODUCTION

snom ONE is a software-based IP PBX. The software is designed to run on the customer premise or in the cloud. This document will cover the case in which the snom ONE software-based IP PBX is installed as a server behind NAT.

The R14 Identity/Device profile required for the snom ONE IP PBX is the “Generic SIP Trunk Single Registration” Identity/Device profile.

1. Standard Firewall LAN Topology

This configuration features a snom ONE build deployed behind a standard, third-party firewall. The firewall is configured to forward SIP and an RTP port range from the firewall WAN IP address to the internal IP address of the snom ONE server.

1.1 Server Behind NAT

Enterprises frequently want to run the PBX on a private network while at the same time giving remote users access to the system. The requirements to achieve this are as follows:

- A corporate firewall is available that filters traffic between intranet and Internet. This firewall is not SIP-aware, but it is able to send traffic to a DMZ (not performing NAT on this traffic).

- Most of the phone calls occur internally, and the company is running its own small data center. Therefore, the PBX should run in the private network.

- The firewall has at least one public IP address which is routable from anywhere in the Internet.

1.2 SIP Port Settings

These settings are located within Admin > Settings > Ports. In this section, you can provide specific port information for the SIP protocol. SIP can run on UDP, TCP, or TLS. TCP and UDP send the SIP packets unencrypted and therefore are considered insecure.

TLS is used for secure SIP communication since it encrypts the SIP signalling packets much like HTTPS encrypts HTTP traffic.

The default SIP port per RFC 3261 is 5060 for SIP and 5061 for SIPS. The snom ONE software is listening for and transmitting SIP requests and responses on these ports. (Changes to HTTP and SIP settings require a system restart.)

- SIP UDP Ports: If you are using SIP over UDP, you need to set this field. The default port for UDP is 5060. Multiple ports are permitted (e.g., 5060 5064).

- Maximum number of SIP connections per second: This setting specifies the number of SIP conversations the system will respond to in 1 second. This setting is useful for deterring against SIP attacks.

- Maximum number of SIP connections: This setting limits the total number of SIP connections the system will support. This setting must be configured in busy environments where resource limitation is an issue.

- SIP IP Replacement List: This setting applies to a system that is used in a DMZ zone with NAT (e.g., to connect remote phones to a system that is not on a public IP address). In this case, when the system builds the remote SIP packets, it will use the public IP address of the router. The setting should include a list of local IP addresses and their replacements. Whenever the system finds a local address in the list, it replaces the local address with the remote address, so the SIP messages from the system will look as if they were sent from the replaced IP address. The format of the list is LocalAddress/RemoteAddress [LAdr/RAdr]. Both the LAdr and the RAdr must be an IPv4 or IPv6 address (e.g., 192.168.1.2/203.4.5.12). DNS addresses are not resolved here.

1.3 RTP Port Settings

These settings are located within Admin > Settings > Ports. The Real Time Protocol (RTP) ports are used for sending and receiving media. Be sure to specify a reasonable port range so that you have enough ports for all open calls. A port range of 100 ports is not unusual. Most user agents send RTP media data from the same port on which they expect to receive data. This is useful when a user agent sends media from behind NAT. The system can use this mechanism to establish a two-way media path, even if the user agent is not able to determine its public IP address for media and is behind NAT.

- Port Range Start: This setting represents the starting RTP port that the system will use for media sessions. If the system is behind a firewall, these ports should be open.

- Port Range End: This setting represents the end RTP port that the system will use for the media sessions. RTP uses UDP for transport, whereas SIP can use UDP, TCP, and/or TLS.

- Follow RTP: Some user agents use different ports for sending and receiving. Although they will not be able to operate behind NAT, they are within the scope of the IETF standards. With this setting, these devices can be made compatible. By default, this flag is set to On. If you have trouble with devices that use different ports for sending and receiving, try turning this flag off. Some troublesome devices also have a flag that can be used to turn the usage of different ports off. This behavior can be controlled on a trunk level, as well. If only a specific trunk has this problem, use this setting only on the trunk level.

- Codec Preference: The Codec Preference setting allows you to select the codecs that will be supported on the system. The codecs that are allowed on the system are shown at the left. If you do not want to use a particular codec, click the codec, then click Remove. This will move the codec to the right-side selection box, removing it from use. The system comes with recommended high-quality codecs like G.711 µ-law (0), G.711 A-law (8), G.722 (9), G.726 (2), or GSM 6.10 FullRate (3). Codecs can be changed without restarting the service. G.729 is a royalty-based codec and requires a fee, and it is not enabled by default.

- Lock codec during conversation: In certain cases, the system can switch to a common codec (advertised by both end devices) to avoid the transcoding during the call setup. Even though this is legal from the protocol's point of view, many devices still cannot change codecs midstream. To avoid this problem, you must enable this feature. Once this is set, the system will not switch the codec during the call setup. This may introduce transcoding, which is a CPU-intensive job. Default is off.

- Packet length (in ms): This is the ptime parameter in the session description protocol (SDP). The default is 20 ms.

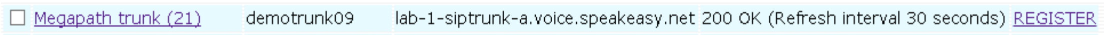
- Multicast IP Addresses: Set this to an IP address if you want the system to send and receive multicast IP addresses on this network interface. If this is set to 20 ms, then the system will send out packets every 20 ms, which equals 50 packets per second. If both sides of the call are set to different ptimes, then the system will have to transcode them, which will degrade performance.

- Bind to specific IP address (IPv4): The system opens RTP ports on this IP address only. This is useful if you have a dual NIC machine and want to use only on one interface for RTP. If this is left blank, then the system will use all the interfaces it sees in the machine.

- Bind to specific IP address (IPv6): IPv6 equivalent of the above field.

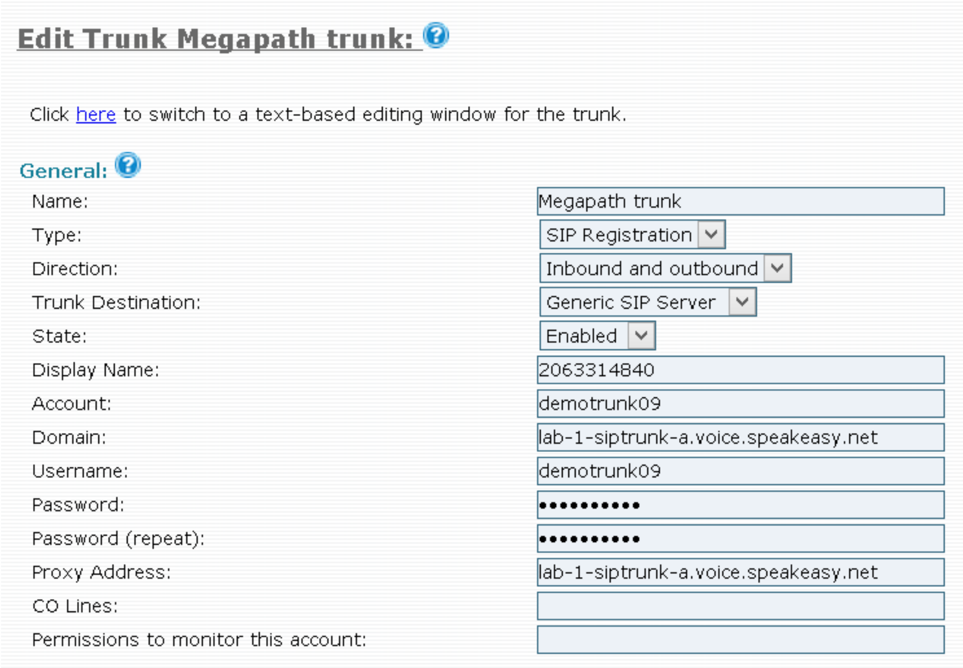
1.4 Megapath SIP Trunk Settings

- Create a trunk and name it “Megapath.”



☐ Megapath trunk (21)	demotrunk09	lab-1-siptrunk-a.voice.speakeasy.net	200 OK (Refresh interval 30 seconds)	REGISTER

- For the “Type” of trunk choose, “Registration.” Megapath will provide the registration account information to include authentication username, password, and proxy address. Save the configuration.



Edit Trunk Megapath trunk:

Click here to switch to a text-based editing window for the trunk.

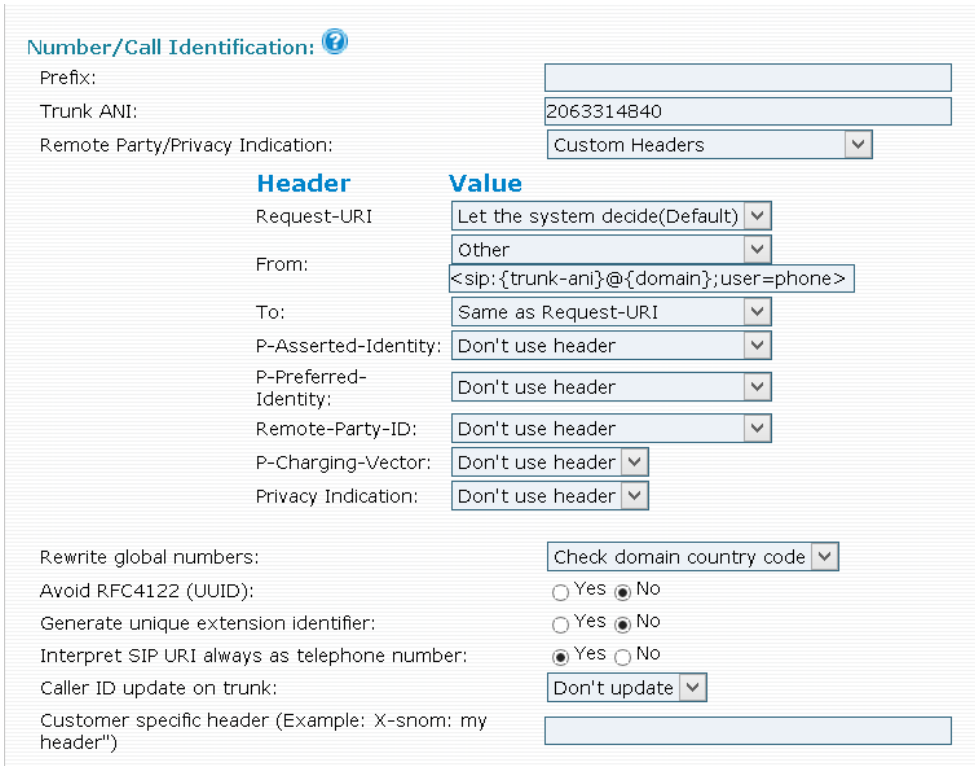
General:

Name:	Megapath trunk
Type:	SIP Registration
Direction:	Inbound and outbound
Trunk Destination:	Generic SIP Server
State:	Enabled
Display Name:	2063314840
Account:	demotrunk09
Domain:	lab-1-siptrunk-a.voice.speakeasy.net
Username:	demotrunk09
Password:	••••••••••
Password (repeat):	••••••••••
Proxy Address:	lab-1-siptrunk-a.voice.speakeasy.net
CO Lines:	
Permissions to monitor this account:	

- For call identification, Megapath authenticates the user by way of the “from” field when originating an outbound call on the snom ONE IP PBX. Here a quick snapshot:

  From:"HamletCollado<sip:2063314840@bostonpbx.snom.com;user=phone>;tag=470172627

- For Number/Call Identification



Number/Call Identification:

Prefix:	
Trunk ANI:	2063314840
Remote Party/Privacy Indication:	Custom Headers

Header	Value
Request-URI	Let the system decide(Default)
From:	Other <sip:{trunk-ani}@{domain};user=phone>
To:	Same as Request-URI
P-Asserted-Identity:	Don't use header
P-Preferred-Identity:	Don't use header
Remote-Party-ID:	Don't use header
P-Charging-Vector:	Don't use header
Privacy Indication:	Don't use header

Rewrite global numbers:	Check domain country code
Avoid RFC4122 (UUID):	○ Yes ● No
Generate unique extension identifier:	○ Yes ● No
Interpret SIP URI always as telephone number:	● Yes ○ No
Caller ID update on trunk:	Don't update
Customer specific header (Example: X-snom: my header")	

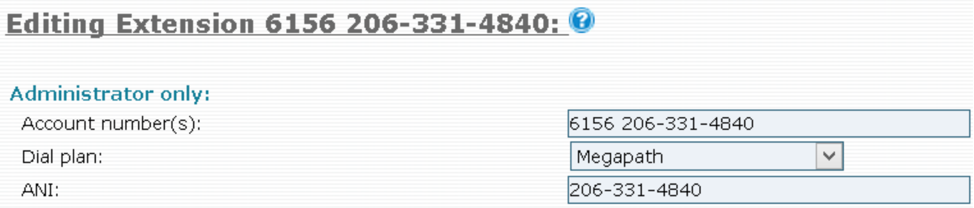
The in the custom header "From" field choose "other" and copy paste the following syntax.

"<sip:{trunk-ani}@{domain};user=phone>" to show the trunks ANI

or you can use

"<sip:{ext-ani}@{domain};user=phone>" to show the extensions ANI.

- To set the "Extension ANI" or if you have multiple DIDs for each extension, you will have to navigate to the users extension and assign the DID.



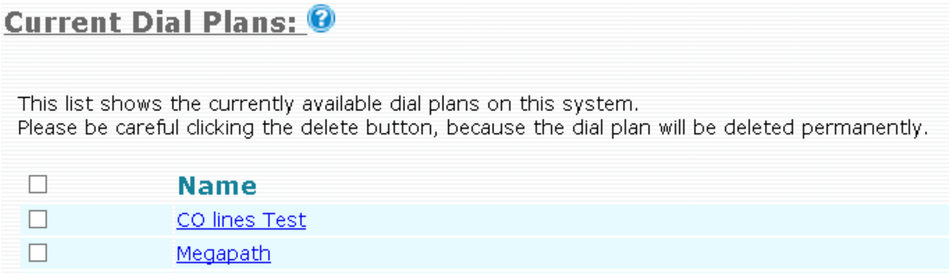
Editing Extension 6156 206-331-4840:

Administrator only:

Account number(s):	6156 206-331-4840
Dial plan:	Megapath
ANI:	206-331-4840

- Navigate to Admin---> Domain--> Choose a Domain and then a Dial Plan

- Create a new dial plan.

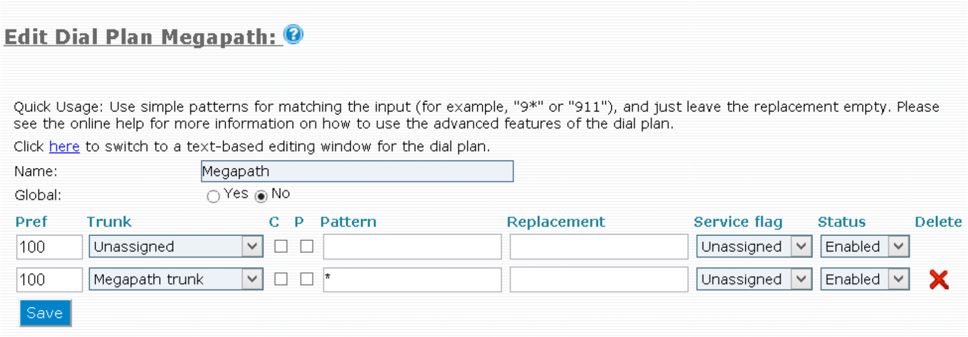


Current Dial Plans:

This list shows the currently available dial plans on this system.
Please be careful clicking the delete button, because the dial plan will be deleted permanently.

	Name
□	CO lines Test
□	Megapath

- Choose Megapath as your Trunk for the Pattern you can add a *



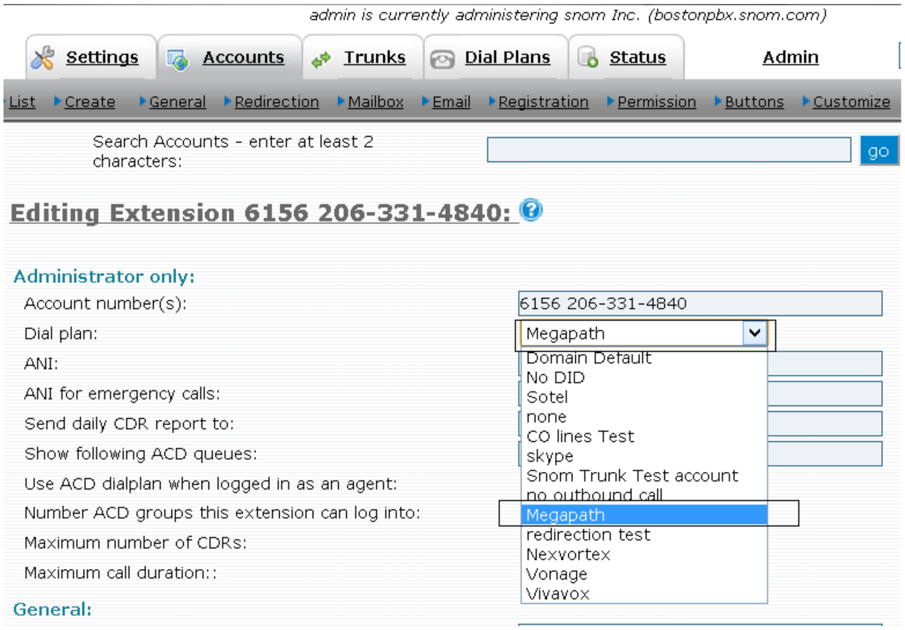
Edit Dial Plan Megapath:

Quick Usage: Use simple patterns for matching the input (for example, "9*" or "911"), and just leave the replacement empty. Please see the online help for more information on how to use the advanced features of the dial plan.
Click here to switch to a text-based editing window for the dial plan.

Name: Megapath
Global: ○ Yes ● No

Pref	Trunk	C	P	Pattern	Replacement	Service flag	Status	Delete
100	Unassigned	□	□			Unassigned	Enabled	
100	Megapath trunk	□	□	*		Unassigned	Enabled	✗

- You can navigate to the extension level and choose the newly created "MegaPath" dial plan in the drop down.



admin is currently administering snom Inc. (bostonpbx.snom.com)

Search Accounts - enter at least 2 characters:

Editing Extension 6156 206-331-4840:

Administrator only:

Account number(s): 6156 206-331-4840
Dial plan: Megapath
ANI:
ANI for emergency calls:
Send daily CDR report to:
Show following ACD queues:
Use ACD dialplan when logged in as an agent:
Number ACD groups this extension can log into:
Maximum number of CDRs:
Maximum call duration::

General: