SIP Trunking Specification

SMB Platform Interoperability for IP PBXs

Document Number: VSEST2090831

Rev: 1.8

Release: September 16th, 2011
Supersedes: Rev 1.7

Revision History

Number	Date	Description
0.5	02/03/09	First draft by Markus Bojarski, Tim Flowers, Shawn Wade
0.9	05/12/09	Final draft by Markus Bojarski, Tim Flowers, Shawn Wade
1.0	05/14/09	Release 1.0 by Adam Morris
1.1	08/31/09	Updates and formatting changes by Larry Corvari
1.2	09/14/09	Update 3cx figures by Larry Corvari
1.3	12/07/09	Added table of Speakeasy defaults & minor edits.
1.4	03/12/2010	Updates to IP-PBX configs to include Edgemarcs by Jason Morgan
1.5	04/12/2010	Update to include Adtran NetVanta 7100 IP-PBX by Jason Morgan
1.6	06/04/10	Update 3cx versioning
1.7	01/28/2011	Update to include Cisco UC500 IP-PBX, merged v1.5 & 1.6. Updated branding from Speakeasy to Megapath - by Aaron Stevens
1.8	09/16/2011	Update to include Samsung OfficeServ 7100/7200 by Jason Morgan

Contents

List of Figures

List of Tables

1. Definitions

1.1 Acronyms & Definitions

The following table provides a list of Megapath used acronyms and definitions.

Table 1-1 - Megapath Acronyms and Definitions

Acronym	Definition
B2BUA	Back-to-back User Agent
CLID	Calling Line Identification
EMI	Enterprise Media Interface – The interconnection point with the Megapath Media Interface (SMI) for sending and receiving media.
FQDN	Fully Qualified Domain Name
NAT	Network Address Translation
PCMU	Pulse Code Modulation with mu-Law scaling
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request for Comment
RTP	Real-time Transport Protocol
RTCP	RTP Control Protocol
SBC	Session Border Controller
SIP	Session Initiation Protocol
SMI	Megapath Media Interface – The interconnection point with EMI for sending and receiving media
TCP	Transport Control Protocol
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol

1.2 RFC Support

The following table provides the list of RFCs that Megapath supports. The RFC can be found at http://www.ietf.org.

Table 1-2 RFC Support

RFC	Description
1889	RTP: A Transport Protocol for Real-Time Applications
2327	SDP: Session Description Protocol
2833	RTP: Payload for DTMF Digits, Telephony Tones and Telephony Signals
3261	SIP: Session Initiation Protocol
3262	Reliability of Provisional Responses in Session Initiation Protocol
3263	Session Initiation Protocol (SIP): Locating SIP Servers
3264	An Offer/Answer Model with Session Description Protocol
3326	The Reason Header Field for the Session Initiation Protocol
3824	Using E.164 numbers with the Session Initiation Protocol
3891	The Session Initiation Protocol (SIP) “Replaces” Header
3892	The Session Initiation Protocol (SIP) Referred-By Mechanism
3986	Uniform Resources Identifier (URI): Generic Syntax
4028	Session Timers in the Session Initiation Protocol

1.3 SIP Method Support

The following table documents the SIP Methods supported by Megapath.

Table 1-3 SIP Method Support

SIP Method	RFC	Receive	Send
INVITE	3261	Y	Y
ACK	3261	Y	Y
CANCEL	3261	Y	Y
BYE	3261	Y	Y
REGISTER	3261	Y	N
OPTION	3261	NS*	N
PRACK	3262	Y	Y
INFO	2976	N	N
UPDATE	3311	NS*	NS*
SUBSCRIBE	3365	N	N
NOTIFY	3265	N	Y
REFER	3515	NS*	N
MESSAGE	3428	N	N
PUBLISH	3903	N	N

Note – NS* = Not supported at this time

2. Overview

2.1 Scope and Assumptions

The purpose of this document is to show how the Megapath SMB Service interoperates with IP PBXs via SIP trunking. It is not an exhaustive list of all possible SIP Trunking techniques, rather a subset that Megapath supports. This document and the language used imply that the reader is familiar with SIP and/or VoIP technologies and standards.

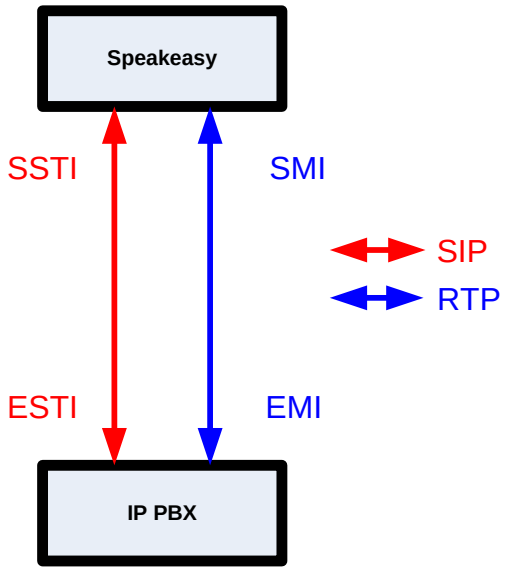
2.2 Terminology

In this document, the key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' are to be interpreted as described in RFC 2119 and indicate requirement levels for compliant SIP implementations.

2.3 Reference Architecture

The diagram below, Figure 2-1 Reference Architecture, depicts the points of interconnection between the Megapath Interfaces and the Enterprises Interfaces for SIP signaling and RTP media.

Figure 2-1 Reference Architecture



2.4 Megapath Configuration Data

Table 2-1 - Megapath Configuration Data

SIP Method	Value
REGISTER	60 seconds

2.5 DNS

Megapath provides the Enterprise SIP Trunk Interface with either 1 SRV record or 2 A records for locating the Megapath SIP Trunk Interfaces. The SRV record will have a 2 character state indicating the ETSI geographic State.

In the example SRV record below, the 2 character State “wa” indicates Washington State.

```
_sip._udp.wa1-siptrunk-srv.voice.speakeasy.net.
```

That SRV record will resolve to 2 (two) A records.

```
14400 IN SRV 1 50 5060 ca1-siptrunk-a.voice.speakeasy.net.
14400 IN SRV 2 50 5060 ny1-siptrunk-a.voice.speakeasy.net.
```

The result reads, from left to right:

- Time-To-Live (seconds)
- Class (IN = Internet)
- SRV
- Priority (1-9, lower # = higher priority)
- weight (not used)
- port number (5060)
- target (A record)

The Enterprise SIP Trunk Interface should resolve the SRV record, then resolve the 2 A records, then register with the highest priority first and cache the second for redundancy. In this case, ***ca1-siptrunk-a.voice.speakeasy.net***. would be the first target because it has the higher priority and it is closer to the Enterprise SIP Trunk Interface.

Note – It is required to use DNS names as opposed to IP addresses in all IP PBX configurations.

2.6 Redundancy

Megapath provides a means for Enterprise SIP Trunk Interfaces to have redundant access to the Megapath network by implementing two Megapath SIP Trunk Interfaces. The Megapath SIP Trunk Interfaces are exactly the same, however, for some, one will be primary and the other will be secondary.

Redundancy is achieved by the Enterprise SIP Trunk Interface noticing a failure or timeout of some sort at their primary Megapath SIP Trunk Interface and then registering with their secondary Megapath SIP Trunk Interface. When their primary Megapath SIP Trunk Interface comes back, the Enterprise SIP Trunk Interface can fail back to their primary Megapath SIP Trunk Interface.

The preferred method of failover is via DNS SRV records per RFC 2782. If SRV records are not supported at the Enterprise SIP Trunk Interface, customers may use one of the A records as a primary and the other as a secondary if that is supported at their IP PBX.

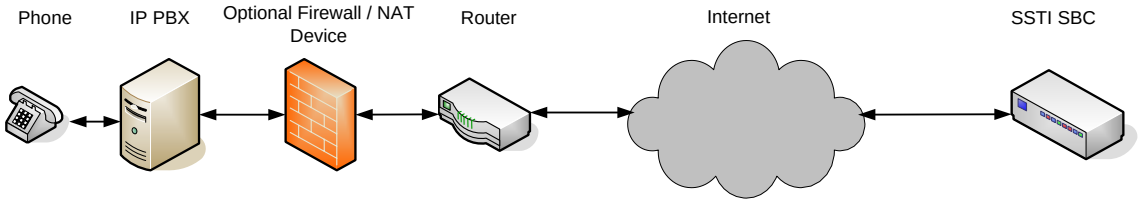
2.7 Supported Transport Methods

Megapath **ONLY** supports encrypted UDP for SIP transport.

2.8 LAN Design

Below, Figure 2-2 Sample LAN, is a sample LAN architecture showing the path from a phone through the IP PBX and to the Megapath SIP Trunk Interface.

Figure 2-2 Sample LAN



2.9 Firewalls and NAT

Firewalls are designed to prevent unauthorized access to a network. Firewalls can also perform Network Address Translations, Application Layer Gateway or proxy functions and intrusion detection to name a few. They usually protect a trusted domain, such as a private network, from an un-trusted domain like the public internet.

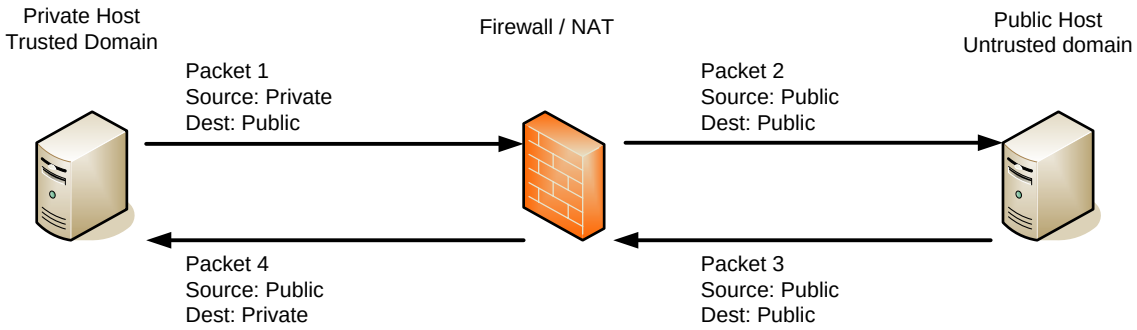
Network Address Translation or NAT is a mechanism for changing layers 3 and 4 information in IP packets. Throughout this document, the term NAT will imply changing any source or destination IP address as well any source or destination UDP port number unless noted otherwise. The main purpose of NAT is to bridge two different networks.

There are many types of NAT techniques such as full-cone or one-to-one NAT, address-restricted or port-restricted NAT, Bi-directional and symmetrical NAT. There are also protocols created to discover and traverse NATs such as STUN, TURN and

ICE. None of these methods are supported, thus the details of each are outside the scope of this document.

In a typical scenario, where a firewall is performing both security and translation functions, the firewall will be configured with interfaces in both the trusted and un-trusted domains. In normal operation, the firewall will allow the private network to make connections out to the un-trusted domain and disallow connections from the un-trusted domain into the private network. Figure 2-3 Firewall NAT Operation, depicts a firewall in this typical scenario.

Figure 2-3 Firewall NAT Operation



1. The firewall changes the source address of the initial connection request from the private network to look as if it came from the public network and sends it to the destination address.
2. The firewall will cache the change it has made into a mapping for later use.
3. When the destination responds, the firewall compares the source address of the packet to its mappings. If it matches the mapping in its cache, it lets it through. This is also called a pinhole.
4. At this point, the firewall will change the destination address of the packet back to the private address.

At this point, the two hosts can communicate freely as long as the source & destination addresses don't change and there is enough periodic traffic to keep the firewall from closing the pinhole.

Some firewalls have "SIP aware" features designed to make modifications to application layer information in SIP packets. The use of these features is not recommended, but is permitted as long as it works. Megapath has seen situations where registration, inbound calls and early media have been disrupted due to SIP aware firewalls. It is best to not use the SIP aware features of the firewall in this case.

The SBC is the best choice for modifying SIP packets, but they are not required at the Enterprise SIP Trunk Interface. The Megapath SIP Trunk Interface deploys SBCs to discover NATs and respond accordingly.

Note – The Megapath SIP Trunk Interface will use the source IP address and source UDP port number from the registration and reply back to them for responses and new call setup.

Whatever security and or NAT method used, the firewall/NAT device SHOULD keep track of the source UDP ports especially if it changes them or uses something other than 5060. The firewall/NAT device MUST keep the pinhole open for at least 60 seconds of inactivity.

Note – To keep the pinhole open at the Enterprise SIP Trunk Interface, the Megapath SIP Trunk Interface will request that the Enterprise SIP Trunk Interface re-register every 60 seconds.

2.10 Quality of Service

Quality of Service is a mechanism designed to prioritize and transmit IP packets based on user defined criteria. It consists of two basic concepts, marking and queuing.

There are two formats in terms of marking

- TOS – Type of Service
- DSCP – Differentiated Services Code Point).

The differences lie in the interpretation of that 3rd byte in the IP header. TOS uses 3 bits for Precedence and 1 bit for each Delay, Throughput, Reliability and Cost parameters. DSCP is similar to TOS in that it uses 6 bits for a classification/marking and the last two bits for congestion notification.

There are many mechanisms for queuing and these depend on vendor or configuration. Most common and simple is to have a queue for high priority traffic and a queue for low priority traffic on a particular interface. That interface may have a certain amount of the total bandwidth allocated on that interface for the high priority queue and the leftover bandwidth for the low priority queue. It may also let other traffic use the high priority queue/bandwidth if it is empty. Most of the time, traffic may flow out an interface in a first-in-first-out fashion until a queue fills or the link becomes otherwise saturated. At that point the device will enact its queuing strategy and delay or discard lower priority traffic ensuring the higher priority traffic gets transmitted.

It is a good idea to mark and queue at the transmitting source of the packet or by another device as close to the source as possible. When going from one provider's network to another, the packets may be remarked and queued to that network's scheme.

Note – If Megapath is your Internet service provider, please feel free to mark and queue your own VOIP traffic with a TOS precedence of 5 for signaling and media. Other received markings will be overwritten

2.11 E.164 Compliance

E.164 is an ITU specification stating the format and numbering plan for telephone numbers. In the context of SIP and E.164 compliance, it means prefixing digits with a "+" and including the CC (Country Code) and the NDC (National Destination Code)

in digits strings. Below is an example of a U.S. number with the "+", the Country Code (1), the NPA (206) then the station digits in E.164 format.

```
+12063334444
```

Megapath tests with and prefers sending and receiving digit strings in E.164 format. The Megapath SIP Trunk Interface will send all digit strings in E.164 format. The Enterprise SIP Trunk Interface SHOULD send all digit strings in E.164 format.

2.12 Uniform Resource Identifiers

Uniform Resource Identifiers, URI, are simply a string of characters used to identify or name a resource on the Internet. There are many kinds of URIs for locating and communicating with resources such as web pages (http:) and mail (mailto:). A SIP URI (sip:) contains specific syntax to identify and initiate a communications session with a resource. RFC 3261 section 19 outlines the SIP URI format supported by the Megapath SIP Trunk Interface. The Megapath SIP Trunk Interface does not support the other URIs such as sips: and tel:. Here is an example of a supported SIP URI.

```
sip:+12063334444@192.168.100.1:5060;user=phone
```

2.13 Caller-ID

Caller-ID is a mechanism for displaying the name and number of the person calling. Typically, when a switch receives a call with only the calling number, the switch will lookup the name for that number. The switch then includes that name in the subsequent setup message. Names can also be assigned to numbers locally within a switch and sent out with call setup message thus not requiring a lookup to be performed by the far end.

Megapath includes the display name for all the numbers it is authoritative for. For calls from the Megapath SIP Trunk Interface to the Enterprise SIP Trunk Interface, the Megapath SIP Trunk Interface will send the Caller-ID information in the FROM header. For calls from the Enterprise SIP Trunk Interface to the Megapath SIP Trunk Interface, the FROM must be one of the DIDs. The display name sent to the PSTN will be taken from the name assigned to the DID in our switch.

2.14 Privacy

In the context of VoIP, privacy is a mechanism for concealing the name and number of the calling party from the called party. For calls from the Megapath SIP Trunk Interface to the Enterprise SIP Trunk Interface, the FROM header will contain anonymous@anonymous.invalid.com per RFC 3261 if the calling party has requested privacy.

Note – Privacy from the Enterprise SIP Trunk Interface to the Megapath SIP Trunk Interface is not supported via RPID or PAI.

2.15 SIP Timers

The table below shows the SIP timers from RFC 3261, their default values, where they can be found in the RFC and a brief description.

Table 2-2 SIP Timers

Timer	Value	Section	Meaning
T1	500ms default	Section 17.1.1.1	RTT Estimate
T2	4s	Section 17.1.2.2	The maximum retransmit interval for non-INVITE requests and INVITE responses
T4	5s	Section 17.1.2.2	Maximum duration a message will remain in the network
Timer A	initially T1	Section 17.1.1.2	INVITE request retransmit interval, for UDP only
Timer B	64*T1	Section 17.1.1.2	INVITE transaction timeout timer
Timer C	> 3min	Section 16.6 bullet 11	proxy INVITE transaction timeout
Timer D	> 32s for UDP 0s for TCP/SCTP	Section 17.1.1.2	Wait time for response retransmits
Timer E	initially T1	Section 17.1.2.2	non-INVITE request retransmit interval, UDP only
Timer F	64*T1	Section 17.1.2.2	non-INVITE transaction timeout timer
Timer G	initially T1	Section 17.2.1	INVITE response retransmit interval
Timer H	64*T1	Section 17.2.1	Wait time for ACK receipt
Timer I	T4 for UDP 0s for TCP/SCTP	Section 17.2.1	Wait time for ACK retransmits
Timer J	64*T1 for UDP 0s for TCP/SCTP	Section 17.2.2	Wait time for non-INVITE request retransmits
Timer K	T4 for UDP 0s for TCP/SCTP	Section 17.1.2.2	Wait time for response retransmits

3. Detailed SIP Method Reference

3.1 INVITE

This method is used to initiate call setup, to modify an existing call, and to refresh a session.

Sample INVITE:

```
INVITE sip:bob@domainname.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKkjshdyff
To: Bob <sip:bob@domainname.com>
From: Alice <sip:alice@ip-pbx-domainname.com>;tag=88sja8x
Max-Forwards: 70
Call-ID: 001280f3-abfb0071-4925fefd-3ea924bb@192.168.1.8
CSeq: 101 INVITE
```

The INVITE example shows the INVITE line with username@domain. This needs to be the username of the credentials which have been provided by Megapath. The initial INVITE will in turn be rejected with a 401 Unauthorized message and the IP-PBX will need to resend the INVITE with the correct digest credentials

The Allow header in the INVITE is mandatory and needs to be populated with at least these methods: The Megapath SIP Trunk Interface will offer a minimum of these methods when sending to an IP-PBX:

```
Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, REGISTER
```

Example of a call setup and tear down starting with the initial INVITE:

```
       IP-PBX . . . . . . . . . . Megapath SIP Trunk Interface . . . . . . .
. . . CALLEE
         |                         |                          |
         |-------- INVITE -------->|                          |
         |                         |                          |
         |<-- 401 Unauthorized ----|                          |
         |                         |                          |
         |---------- ACK --------->|                          |
         |                         |                          |
         |-------- INVITE -------->|                          |
         |                         |--------- INVITE -------->|
         |<------- 100 Trying -----|                          |
         |                         |<------ 180 Ringing ------|
         |<---- 180 Ringing -------|                          |
         |                         |<-------- 200 OK ---------|
         |<------- 200 OK ---------|                          |
         |                         |                          |
         |---------- ACK --------->|                          |
         |                         |                          |
         |<================= Media Session ==================>|
         |                         |                          |
         |                         |<---------- BYE ----------|
         |                         |                          |
         |<--------- BYE ----------|                          |
         |                         |                          |
```

```
        |-------- 200 OK -------->|                          |
        |                         |--------- 200 OK -------->|
        |                         |                          |
```

3.1.1 Megapath SIP Trunk Interface Compliancy Rules

1. An Initial INVITE sent by the Megapath SIP Trunk Interface always contains an SDP offer and the SDP answer is expected in the first response.
2. An Initial INVITE sent by the Megapath SIP Trunk Interface contains Allow and Supported headers.
3. Session timers must be used as discussed in RFC 3261.
4. A re-INVITE can be used to update the current session without stopping the call.
5. The initial INVITE will be challenged with a 401 Unauthorized for a request of authorization. The caller will need to re-attempt an INVITE with the correct authorization credentials for the call flow to continue.
6. The initial INVITE and all subsequent INVITEs are required to have the supported headers populated in the “Allow:” field.

3.2 ACK

The ACK method is used to acknowledge receipt of a final response (2xx, 3xx, 4xx, 5xx, or 6xx) to an INVITE request and MUST be supported. The ACK message is the final part of a three-way handshake establishing a session.

3.3 CANCEL

The CANCEL method is used to stop the processing of an INVITE and MUST be supported.

3.4 BYE

The BYE method is used to terminate a session and MUST be supported.

3.5 REGISTER

A REGISTER method allows a SIP device with a dynamic IP or behind a NAT firewall to receive calls. When set up correctly, the IP-PBX registers to the Megapath SIP Trunk Interface, and renews the registration every 60 seconds to keep the server up to date with its current location and the Megapath SIP Trunk Interface will be able to send subsequent signaling, like an INVITE to the device. Also, the Megapath SIP Trunk Interface will not accept any other SIP signaling request without first registering.

The first registration attempt by the IP-PBX will be returned with a 401 Unauthorized from the Megapath SIP Trunk Interface. The IP-PBX will then need to send a second REGISTER in dialogue with the proper credentials

Example initial REGISTER:

```
REGISTER sip:speakeasy.net SIP/2.0
Via: SIP/2.0/UDP 22.33.44.55
From: “2065555555” <sip:5555@speakeasy.net>;tag=ed4f6b4f8f8b44ao2
To: “2065555555” <sip:5555@speakeasy.net>
Call-ID: 6fd4932-96842@22.33.44.55
CSeq:  52486 REGISTER
Max-Forwards: 70
Contact: “2065555555” <sip:5555@22.33.44.55>;expires=60
User-Agent:  Linksys/SPA962-5.1.18(SC)
Content-Length: 0
Allow:  ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS
Supported: replaces
```

Example of a REGISTER responding to a 401 Unauthorized sent from Megapath SIP Trunk Interface. The only difference is it has an Authorization header and the CSeq has incremented:

```
REGISTER sip:speakeasy.net SIP/2.0
Via: SIP/2.0/UDP 22.33.44.55
From: “2065555555” <sip:5555@speakeasy.net>;tag=ed4f6b4f8f8b44ao2
To: “2065555555” <sip:5555@speakeasy.net>
Call-ID: 6fd4932-96842@22.33.44.55
CSeq:  52487 REGISTER
Max-Forwards: 70
Authorization: Digest
username="2065555555",realm="BroadWorks",nonce="BroadWorksXfsgbof1vT6zc5jiBW
",uri="sip:speakeasy.net",algorithm=MD5,response="e7b19051ccdce503655b360a90
32a72d",qop=auth,nc=00000001,cnonce="6f81ed02"
Contact: “2065555555” <sip:5555@22.33.44.55>;expires=60
User-Agent:  Linksys/SPA962-5.1.18(SC)
Content-Length: 0
Allow:  ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS
Supported: replaces
```

If behind a NAT firewall the IP-PBX will need to register often to keep the connection state (pinhole) establish through the firewall for inbound calls to succeed. The Megapath SIP Trunk Interface will send a timer setting of 60 seconds for re-registering of the IP-PBX.

Example of the dialog for a REGISTER in a flow diagram:

```
IP-PBX                   Megapath SIP Trunk Interface
    |                      |
    |                      |
    |----- REGISTER ------>|
    |                      |
    |<---401 Unauthorized--|
    |                      |
    |----- REGISTER ------>|
    |                      |
    |<----- 200 OK --------|
```

Upon a successful REGISTER the IP-PBX will receive a 200 OK. If the credentials are not correct the Megapath SIP Trunk Interface will return at 401 Unauthorized until the correct credentials are provided.

3.5.1 Megapath SIP Trunk Interface Compliancy Rules

1. The IP-PBX provides its SIP signaling credentials to the Megapath SIP Trunk Interface using the SIP registration procedure for successive signaling to occur.
2. The IP-PBX MUST support the digest authentication mechanism using a username and password agreed upon by both parties.
3. A successful REGISTER MUST be completed before and INVITE will be accepted for processing.
4. A successful REGISTER MUST be completed before the caller may place a call.
5. If an IP-PBX does not successfully register to the Megapath SIP Trunk Interface all other SIP signaling from that IP-PBX will be ignored by the Megapath SIP Trunk Interface until a successful register has occurred.
6. A single reg for a trunk group is recommended/supported, multiple line reg may work but is not supported.
7. The Megapath SIP Trunk Interface will never send a REGISTER request.

3.6 OPTIONS

The OPTIONS method is used to retrieve capabilities from an endpoint.

An OPTIONS request SHOULD NOT be used as a service ping or a session keep-alive mechanism.

The Megapath SIP Trunk Interface will never send an OPTIONS request.

3.7 PRACK

The PRACK method is used to acknowledge reliable provisional responses.

3.8 INFO

The INFO method is NOT supported by the Megapath SIP Trunk Interface.

3.9 UPDATE

The UPDATE method is NOT supported by the Megapath SIP Trunk Interface at this time.

3.10 SUBSCRIBE

The SUBSCRIBE method is NOT supported by the Megapath SIP Trunk Interface.

3.11 NOTIFY

This method is used to send state information about a resource. The Megapath SIP Trunk Interface supports NOTIFY as part of REFER.

A NOTIFY method SHOULD NOT be sent to the Megapath SIP Trunk Interface.

All call flows that require a NOTIFY to be sent from the Megapath SIP Trunk Interface are not supported at this time.

3.12 REFER

This method is used to send state information about a resource. The Megapath SIP Trunk Interface supports NOTIFY as part of REFER.

A REFER method SHOULD NOT be sent to the Megapath SIP Trunk Interface.

All call flows that require a REFER to be sent from the Megapath SIP Trunk Interface are not supported at this time.

3.13 MESSAGE

The MESSAGE method is not supported by the Megapath SIP Trunk Interface.

3.14 PUBLISH

The PUBLISH method is not supported by the Megapath SIP Trunk Interface.

3.15 Unknown Method

Any method not specifically described in Table 1-3 SIP Method Support, is considered an unknown method and will not be processed by the Megapath SIP Trunk Interface appropriately.

4. SIP Header Support

Table 4-1 SIP Header Support, delineates the headers and the directions in which they are supported at the Megapath SIP Trunk Interface. Per RFC 3261, if a UAS does not understand a header field in a request (that is, the header field is not defined in this specification), the server MUST ignore that header field and continue processing the message. A UAS SHOULD ignore any malformed header fields that are not necessary for processing requests. This list of SIP headers is not a complete list of all the SIP headers. It is just a list of the headers used in SIP Trunking with Megapath.

Table 4-1 SIP Header Support

Header	RFC	Receive	Send
Accept	3261	Y	Y
Allow	3261	Y	Y
Authorization	3261	Y	N
Call-ID	3261	Y	Y
Call-Info	3261	Y	N
Contact	3261	Y	Y
Content-Length	3261	Y	Y
Content-Type	3261	Y	Y
CSeq	3261	Y	Y
Diversion	Draft-levy-sip-diversion-08	Y	Y
Expires	3261	Y	Y
From	3261	Y	Y
Max-Forwards	3261	Y	Y
Reason	3261	Y	Y
Record-Route	3261	Y	Y
Reply-To	3261	Y	N
Require	3261	Y	Y
Retry-After	3261	Y	Y
Request	3261	Y	Y
Route	3261	Y	Y
Server	3261	Y	N
Subject	3261	Y	N
Supported	3261	Y	Y
Timestamp	3261	Y	N
To	3261	Y	Y
Unsupported	3261	Y	Y
User-Agent	3261	Y	Y
Via	3261	Y	Y
Warning	3261	Y	N
WWW-Authenticate	3261	Y	N

4.1 Accept

The Accept request-header field can be used to specify content-types which are acceptable for the response. Accept headers can be used to indicate that the request is specifically limited to a small set of desired types. If no Accept header field is present, the Enterprise SIP Trunk Interface SHOULD assume a default value of application/sdp. The Megapath SIP Trunk Interface only supports the application/sdp content-type.

Example Accept:

```
Accept: application/sdp
```

4.2 Allow

The Allow header lists the set of methods supported by the UA generating the message. It is mostly used in INVITEs, OPTIONS or as a list included in a 405 (Method Not Allowed) response.

All methods, including ACK and CANCEL, understood by the UA MUST be included in the list of methods in the Allow header field, when present. The absence of an Allow header field MUST NOT be interpreted to mean that the UA sending the message supports no methods. Rather, it implies that the UA is not providing any information on what methods it supports. Supplying an Allow header field in responses to methods other than OPTIONS reduces the number of messages needed.

Example Allow:

```
Allow: ACK,BYE,CANCEL,INVITE
```

4.3 Authorization

The Authorization header contains authentication credentials of a UA. Its contents are therefore dependent on the challenge of the WWW-Authenticate header in the 401 Response. The Megapath SIP Trunk Interface uses HTTP Digest Access Authentication Scheme per RFC 2617. A valid response contains a MD5 checksum of the username, the password, the given nonce value, the HTTP/SIP method, and the requested URI. In this way, the password is never sent in clear text.

This header is most commonly seen in REGISTER and INVITE requests that have been challenged by the registrar or the UAS processing the INVITE. Its use in the ACK and CANCEL methods are only for maintaining authentication and are not challenged or recalculated since the contents should be the same as the initial INVITE. The Megapath SIP Trunk Interface requests authentication in all REGISTER and INVITE requests.

1. The Enterprise SIP Trunk Interface will request registration:

```
REGISTER sip:speakeasy.net:5060 SIP/2.0
From: <sip:10000311@speakeasy.net:5060;transport=UDP>;tag=2b49570-4ad3eb93
To: <sip:10000311@speakeasy.net:5060;transport=UDP>
Call-ID: 2baed10-45114f3a-13c4-4f-313a1e8b-4f
CSeq: 9441 REGISTER
Via: SIP/2.0/UDP 74.211.235.147:5060;branch=z9hG4bK-5196c
Max-Forwards: 70
Supported: 100rel,replaces
Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, PRACK, REFER, REGISTER
Contact: <sip:10000311@74.211.235.147:5060;transport=UDP>
Expires: 1700
Content-Length: 0
```

2. The Megapath SIP Trunk Interface then challenges the request with a 401 Response and includes the WWW-Authenticate header:

```
SIP/2.0 401 Unauthorized
```

```
From: <sip:10000311@speakeasy.net:5060;transport=UDP>;tag=2b49570-4ad3eb93
To: <sip:10000311@speakeasy.net:5060;transport=UDP>;tag=SD21k6e99
Call-ID: 2baed10-45114f3a-13c4-4f-313a1e8b-4f
CSeq: 9441 REGISTER
Via: SIP/2.0/UDP 74.211.235.147:5060;branch=z9hG4bK-5196c
WWW-Authenticate: DIGEST
realm="BroadWorks",qop="auth",algorithm=MD5,nonce="BroadWorksXfuh3assrTmvdbj
vBW"
Content-Length: 0
```

3. The Enterprise SIP Trunk Interface would then calculate the response and send the new REGISTER with Authorization:

```
REGISTER sip:speakeasy.net:5060 SIP/2.0
From: <sip:10000311@speakeasy.net:5060;transport=UDP>;tag=2b49570-4ad3eb93
To: <sip:10000311@speakeasy.net:5060;transport=UDP>
Call-ID: 2baed10-45114f3a-13c4-4f-313a1e8b-4f
CSeq: 9442 REGISTER
Via: SIP/2.0/UDP 74.211.235.147:5060;branch=z9hG4bK-5196c
Max-Forwards: 70
Supported: 100rel,replaces
Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, PRACK, REFER, REGISTER
Contact: <sip:10000311@74.211.235.147:5060;transport=UDP>
Expires: 1700
Authorization: Digest
username="10000311",realm="BroadWorks",nonce="BroadWorksXfuh3assrTmvdbjvBW",
uri="sip:speakeasy.net:5060",response="a5d083512c28b262d30a14861cd8cbbe",alg
orithm=MD5,cnonce="13eb507a",qop=auth,nc=00000001
Content-Length: 0
```

4. If the credentials are valid, the user is registered at the Megapath SIP Trunk Interface and it replies with a 200 OK:

```
SIP/2.0 200 OK
From: <sip:10000311@speakeasy.net:5060;transport=UDP>;tag=2b49570-4ad3eb93
To: <sip:10000311@speakeasy.net:5060;transport=UDP>;tag=SD21k6e99-
Call-ID: 2baed10-45114f3a-13c4-4f-313a1e8b-4f
CSeq: 9442 REGISTER
Via: SIP/2.0/UDP 74.211.235.147:5060;branch=z9hG4bK-5196c
Contact: <sip:10000311@74.211.235.147:5060;transport=UDP>;expires=60;q=0.5
Content-Length: 0
```

4.4 Authorization Header Requirements

4.4.1 Authentication

There are two schemes BASIC and DIGEST. The BASIC scheme allows for clear text passwords and DIGEST does not. The Megapath SIP Trunk Interface only supports the DIGEST scheme.

Example Authentication:

```
Authentication Scheme: Digest
```

4.4.2 Username

The user's name in the specified realm. This will be provided to the Enterprise SIP Trunk Interface

Example Username:

```
username="10000311"
```

4.4.3 Realm

A string displaying which username and password were used to calculate the Response. The Megapath SIP Trunk Interface specifies “Broadworks” as the realm.

Example Realm:

```
realm="BroadWorks"
```

4.4.4 Nonce

A string displaying which username and password were used to calculate the Response. The Megapath SIP Trunk Interface specifies “Broadworks” as the realm

Example Nonce:

```
nonce="BroadWorksXfuh3assrTmvdbjvBW
```

4.4.5 Authentication URI

The URI from the Request-URI of the Request-Line. The Enterprise SIP Trunk Interface would include this to show that no proxy had changed the Request-Line in transit.

Example Authentication URI:

```
uri="sip:speakeasy.net:5060"
```

4.4.6 Digest Authentication Response

A string of 32 hex digits denoting the MD5 checksum of the username, the password, the given nonce value, the HTTP method, and the requested URI.

Example Digest Authentication Response:

```
response="a5d083512c28b262d30a14861cd8cbbe"
```

4.4.7 Algorithm

This field denotes hash function used in calculating the response.

Example Algorithm:

```
algorithm=MD5
```

4.4.8 CNonce

The CNonce-value is an opaque quoted string value provided by the client and used by both client and server to avoid chosen plaintext attacks, to provide mutual authentication, and to provide some message integrity protection.

Example CNonce:

```
cnonce="13eb507a"
```

4.4.9 QOP

The QOP field is reused from the 401 to show the protection used. It is a quoted string of one or more tokens indicating the "quality of protection" values supported by the server. The value "auth" indicates authentication; the value "auth-int" indicates authentication with integrity protection. These values affect the computation of the request-digest. The Megapath SIP Trunk Interface uses a QOP of “auth”.

Example QOP:

```
qop=auth
```

4.4.10 Nonce Count

The Nonce Count value is the hexadecimal count of the number of requests (including the current request) that the client has sent with the nonce value in this request.

Example Nonce Count:

```
nc=00000001
```

4.4.11 Call-ID

The Call-ID header contains a globally unique identifier for a particular invitation or all registrations of a particular client. An INVITE from the Speakeasy SIP Trunk Interface usually starts with an SD and looks similar to the example below.

Example Call-ID:

```
Call-ID: SDckina01-b6038671ba7e9274b9bec2197791db00-v3000v3
```

4.4.12 Call-Info

The Call-Info header field provides additional information about the caller or callee, depending on whether it is found in a request or response. There are several parameters within this header that can carry information such as icons and business cards. Use of the Call-Info header field can pose a security risk. If a callee fetches the URIs provided by a malicious caller, the callee may be at risk for displaying inappropriate or offensive content, dangerous or illegal content, and so on. Therefore, it is RECOMMENDED that a UA only render the information in the Call-Info header field if it can verify the authenticity of the element that originated the header field and trusts that element. This need not be the peer UA; a proxy can insert this header field into requests. The Speakeasy SIP Trunk Interface does not send this header.

Example Call-Info:

```
Call-Info: <http://wwww.example.com/alice/photo.jpg> ;purpose=icon,
<http://www.example.com/alice/> ;purpose=info
```

4.4.13 Contact

The Contact header contains a URI that is to be used by the UAS as a place to send future requests. A Contact header field value can contain a display name, a URI with

URI parameters, and header parameters. These parameters such as are only used when the Contact is present in a REGISTER request or response, or in a 3xx response.

When the header field value contains a display name, the URI including all URI parameters is enclosed in "<" and ">". If no "<" and ">" are present, all parameters after the URI are header parameters, not URI parameters.

The display name can be tokens, or a quoted string, if a larger character set is desired. There may or may not be LWS between the display-name and the "<". These rules for parsing a display name, URI and URI parameters, and header parameters also apply for the header fields To and From.

Example Contact:

```
Contact: <sip:2067343080@192.168.1.27:5060;transport=udp>
```

4.4.14 Content Length

The Content-Length header field indicates the size of the message- body, in decimal number of octets, sent to the recipient. Applications SHOULD use this field to indicate the size of the message-body to be transferred, regardless of the media type of the entity. If a stream-based protocol (such as TCP) is used as transport, the header field MUST be used. If no body is present in a message, then the Content-Length header field value MUST be set to zero.

Example Content Length:

```
Content-Length: 349
```

4.4.15 Content Type

The Content-Type header field indicates the media type of the message-body sent to the recipient. The Content-Type header field MUST be present if the body is not empty. If the body is empty, and a Content-Type header field is present, it indicates that the body of the specific type has zero length (for example, an empty audio file). The Megapath SIP Trunk Interface only supports application/sdp.

Example Content Type:

```
Content-Type: application/sdp
```

4.4.16 CSeq

The sequence number MUST be expressible as a 32-bit unsigned integer. The method part of CSeq is case-sensitive. The CSeq header field serves to order transactions within a dialog, to provide a means to uniquely identify transactions, and to differentiate between new requests and request retransmissions. Two CSeq header fields are considered equal if the sequence number and the request method are identical.

Example CSeq:

```
CSeq: 4711 INVITE
```

4.4.17 Diversion

The Diversion header is used to implement certain features such as third-party voicemail, Automatic Call Distribution (ACD) or call forwarding, where the feature changes the Request URI. This header displays who and why the call was diverted.

Example Diversion:

```
Diversion: <sip:esti@example.com>;reason=unconditional
```

4.4.18 Expires

The Expires header gives the relative time after which the message (or content) expires. It is mostly used in registrations as part of the Contact header to indicate when that registration will expire. The precise meaning of this is method dependent. The expiration time in an INVITE does not affect the duration of the actual session that may result from the invitation. Session description protocols may offer the ability to express time limits on the session duration, however. The value of this field is an integral number of seconds (in decimal) between 0 and (2**32)-1, measured from the receipt of the request.

Example Expires:

```
expires=60
```

4.4.19 From

The From header field indicates the logical identity of the initiator of the request. It contains a URI and optionally a display name. The Enterprise SIP Trunk Interface SHOULD use the display name "Anonymous", along with a syntactically correct, but otherwise meaningless URI (like sip:anonymous@anonymous.invalid), if the identity of the client is to remain hidden. A tag is added to the From header by the transmitting UAC as a means of identifying itself in establishment of a dialog with the UAS.

Example From:

```
From: "2063844840" <sip:2063844840@speakeasy.net>;tag=as1166d37d
```

4.4.20 Max-Forwards

The Max-Forwards header field SHOULD be used with any SIP method to limit the number of proxies or gateways that can forward the request to the next downstream server. This can also be useful when the client is attempting to trace a request chain that appears to be failing or looping in mid-chain.

The Max-Forwards value is an integer in the range 0-255 indicating the remaining number of times this request message is allowed to be forwarded. This count is decremented by each server that forwards the request. The recommended initial value is 70.

This header field should be inserted by elements that can not otherwise guarantee loop detection. For example, a B2BUA should insert a Max-Forwards header field.

Example Max-Forwards:

```
Max-Forwards: 70
```

4.4.21 Record Route

The Record-Route header is inserted by proxies in a request to force future requests in the dialog to be routed through the proxy.

Example Record Route:

```
Record-Route: <sip:proxy.example.com;lr>
```

4.4.22 Request

The Request header contains the desired user or service to which the request is being addressed. SIP Requests are distinguished by having a Request-Line for a start line as opposed to a Response which has a status line. A Request-Line contains a method name, a Request-URI, and the protocol version separated by a single space (SP) character.

The initial Request-URI of the message SHOULD be set to the value of the URI in the To field. In terms of SIP trunking with the Megapath SIP Trunk Interface, the host name should be the value provided by Megapath. Depending on the IP PBX implementation and support for outbound proxy at the IP PBX, that hostname could be either be speakeasy.net or an A record for the Megapath SIP Trunk Interface.

Example Request:

```
Request-Line: INVITE sip:+12063844840@speakeasy.net SIP/2.0
```

4.4.23 Route

The Route header field is used to force routing for a request through the listed set of proxies. There are two forms of routing of requests in SIP. Loose routing is when a proxy will add or remove its route line from the list as the request propagates and is denoted by “lr”. Strict routing is when a proxy will add or remove its route line from the list as the request propagates but overwrites the Request line with the next route in the list. Since the Megapath SIP Trunk Interface is a B2BUA, it does not generate a Route header but will follow RFC 3261 for handling of the Route header. The Enterprise SIP Trunk Interface can include a Route header.

Example Route:

```
Route: <sip:1986@example.com;lr>,
```

4.4.24 Server

The Server header field contains information about the software used by the UAS to handle the request. Revealing the specific software version of the server might allow the server to become more vulnerable to attacks against software that is known to contain security holes. Implementers SHOULD make the Server header field a configurable option.

Example Server:

```
Server: HomeServer v2
```

4.4.25 Supported

The Supported header enumerates all the extensions supported by the UAC or UAS. The Supported header field contains a list of option tags, described in RFC 3261, that are understood by the UAC or UAS. A UA compliant to this specification MUST only include option tags corresponding to standards-track RFCs. If empty, it means that no extensions are supported.

Example Supported:

```
Supported: replaces
```

4.4.26 Timestamp

The Timestamp header field describes when the UAC sent the request to the UAS. See Section 8.2.6 for details on how to generate a response to a request that contains the header field. Although there is no normative behavior defined here that makes use of the header, it allows for extensions or SIP applications to obtain round trip time estimates.

Example Timestamp:

```
Timestamp: 54
```

4.4.27 To

The To header specifies the logical recipient of the request. In most cases, this is the dialed number. It may also contain an optional display-name if the requestor knows the name of the destination. A tag is added to the To header by the receiving UAS as a means of identifying the UAS and establishing a dialog with the UAC. The Megapath SIP Trunk Interface recommends using E.164 formatted numbers in the To header.

Example To:

```
To: <sip:+12067553872@speakeasy.net>
```

4.4.28 Unsupported

The Unsupported header lists the features not supported by the UAS. See Section 8.1.25 of this specification for more information,

Example Unsupported:

```
Unsupported: foo
```

4.4.29 User-Agent

The User-Agent header field contains information about the UAC originating the request. The semantics of this header field are defined in RFC 3261. Deployments that use this header SHOULD make the User-Agent field configurable due to revealing potential vulnerabilities.

Example User-Agent:

```
User-Agent: X-Lite release 11001 stamp 47546
```

4.4.30 Via

The Via header indicates the path taken by the request so far and indicates the path that should be followed in routing responses. A Via header field value contains the transport protocol used to send the message, the client's host name or network address, and possibly the port number at which it wishes to receive responses. The branch ID parameter in the Via header field values serves as a transaction identifier, and is used by proxies to detect loops. There is a “magic cookie” of z9hG4bK prefixing the branch parameter that implies SIP 2.0.

Example Via:

```
Via: SIP/2.0/UDP 66.93.179.239:5060;branch=z9hG4bK0a0d2fa5;
```

4.4.31 Warning

The Warning header is used to carry additional information about the status of a response. Warning header field values are sent with responses and contain a three-digit warning code, host name, and warning text. The "warn-text" should be in a natural language that is most likely to be intelligible to the human user receiving the response. This decision can be based on any available knowledge, such as the location of the user, the Accept-Language field in a request, or the Content-Language field in a response. The default language is i-default. For a more complete list of the warning codes see RFC 3261. The Megapath SIP Trunk Interface does not include a Warning header in its responses and may return unexpected results if received.

Example Warning:

```
Warning: 307 isi.edu "Session parameter 'foo' not understood"
Warning: 301 isi.edu "Incompatible network address type 'E.164'"
```

4.4.32 WWW-Authenticate

The WWW-Authenticate header consists of a challenge that indicates the authentication scheme and parameters applicable to the realm. The Megapath SIP Trunk Interface uses HTTP Digest Access Authentication Scheme per RFC 2617. This header is used in a 401 Unauthorized Response to Initial and expired registrations, as well as INVITEs.

Example WWW-Authenticate:

```
SIP/2.0 401 Unauthorized
From: <sip:10000311@speakeasy.net:5060;transport=UDP>;tag=2b49570-4ad3eb93
To: <sip:10000311@speakeasy.net:5060;transport=UDP>;tag=SD21k6e99
Call-ID: 2baed10-45114f3a-13c4-4f-313a1e8b-4f
CSeq: 9441 REGISTER
Via: SIP/2.0/UDP 74.211.235.147:5060;branch=z9hG4bK-5196c
WWW-Authenticate: DIGEST
realm="BroadWorks",qop="auth",algorithm=MD5,nonce="BroadWorksXfuh3assrTmvdbj
BW"
Content-Length: 0
```

5. SIP Responses

The SIP responses codes are messages sent in response to a request. Some responses are provisional and others are final. SIP responses are distinguished from requests by having a Status-Line as their start-line.

A Status-Line consists of the protocol version followed by a numeric Status-Code and its associated textual phrase. The first digit of the Status-Code defines the class of response. The last two digits do not have any categorization role. For this reason, any response with a status code between 100 and 199 is referred to as a "1xx response", any response with a status code between 200 and 299 as a "2xx response", and so on.

SIP/2.0 allows six values for the first digit:

- 1xx: Provisional -- request received, continuing to process the request.
- 2xx: Success -- the action was successfully received, understood, and accepted.
- 3xx: Redirection -- further action needs to be taken in order to complete the request.
- 4xx: Client Error -- the request contains bad syntax or cannot be fulfilled at this server.
- 5xx: Server Error -- the server failed to fulfill an apparently valid request.
- 6xx: Global Failure -- the request cannot be fulfilled at any server.

All SIP response Codes are defined in RFC 3261 for both send and receive.

5.1 SIP Response Support

Table 5-1 SIP Response Support

SIP Response Code	Description
1xx Provisional Response	Provisional responses are also known as informational responses, indicating that the server contacted is performing some further action and does not yet have a definitive response. A server sends a 1xx response if it expects to take more than 200 ms to obtain a final response. Note that 1xx responses are not transmitted reliably. They never cause the client to send an ACK. Provisional (1xx) responses MAY contain message bodies, including session descriptions
100 Trying	This response indicates that the request has been received by the next-hop server and that some unspecified action is being taken on behalf of this call (for example, a database is being consulted). This response, like all other provisional responses, stops retransmissions of an INVITE by a UAC. The 100 Trying response is different from other provisional responses, in that it is never forwarded upstream by a state-full proxy

SIP Response Code	Description
18X Ringing / Session Progress	These responses are used to show that the UA receiving the INVITE is trying to alert the user. They MAY be used to initiate local ringback or used to convey information about the progress of the call that is not otherwise classified. The Reason-Phrase, header fields, or message body (SDP) MAY be used to convey more details about the call progress
2xx Successful Response	A 2xx message indicates success. 2xx messages also require an acknowledgement (ACK Method)
200 OK	In most cases a 200 OK is used to signify an answer by the called user. They may or may not have a message body (SDP)
4xx Request Failure Response	4xx responses are definite failure responses from a particular server. The client SHOULD NOT retry the same request without modification (for example, adding appropriate authorization)
400 Bad Request	The request could not be understood due to malformed syntax. The Reason-Phrase SHOULD identify the syntax problem in more detail, for example, "Missing Call-ID header field"
401 Unauthorized	The request requires user authentication. This response is issued by UASs and registrars, while 407 (Proxy Authentication Required) is used by proxy servers
403 Forbidden	The server understood the request, but is refusing to fulfill it. Authorization will not help, and the request SHOULD NOT be repeated
404 Not Found	The server has definitive information that the user does not exist at the domain specified in the Request-URI. This status is also returned if the domain in the Request-URI does not match any of the domains handled by the recipient of the request
408 Request Timeout	The server could not produce a response within a suitable amount of time, for example, if it could not determine the location of the user in time. The client MAY repeat the request without modifications at any later time
480 Temporarily Unavailable	The called's end system was contacted successfully but the callee is currently unavailable (for example, is not logged in, logged in but in a state that precludes communication with the callee, or has activated the "do not disturb" feature). This status is also returned by a redirect or proxy server that recognizes the user identified by the Request-URI, but does not currently have a valid forwarding location for that user
482 Loop Detected	The server has detected a loop. If the request contains a Via header field with a sent-by value that equals a value placed into previous requests by the proxy, the request has been forwarded by this element before. The request has either looped or is legitimately spiraling through the element. To determine if the request has looped, the element MAY perform the branch parameter calculation and compare it to the parameter received in that Via header field. If the parameters

SIP Response Code	Description
	match, the request has looped
486 Busy Here	The called's end system was contacted successfully, but the callee is currently not willing or able to take additional calls at this end system
487 Request Terminated	The request was terminated by a BYE or CANCEL request. This response is never returned for a CANCEL request itself
5xx Server Failure Responses	5xx responses are failure responses given when a server itself has encountered an error
500 Server Internal Error	The server encountered an unexpected condition that prevented it from fulfilling the request. The client MAY display the specific error condition and MAY retry the request after several seconds. If the condition is temporary, the server MAY indicate when the client may retry the request using the Retry-After header field
503 Service Unavailable	The server is temporarily unable to process the request due to a temporary overloading or maintenance of the server. The server MAY indicate when the client should retry the request in a Retry-After header field. If no Retry-After is given, the client MUST act as if it had received a 500 (Server Internal Error) response. A client (proxy or UAC) receiving a 503 (Service Unavailable) SHOULD attempt to forward the request to an alternate server. It SHOULD NOT forward any other requests to that server for the duration specified in the Retry-After header field, if present. Servers MAY refuse the connection or drop the request instead of responding with 503 (Service Unavailable)
6xx Global Failures 6xx	6xx responses indicate that a server has definitive information about a particular user, not just the particular instance indicated in the Request-URI
600 Busy Everywhere	The called's end system was contacted successfully but the callee is busy and does not wish to take the call at this time. The response MAY indicate a better time to call in the Retry-After header field. If the callee does not wish to reveal the reason for declining the call, the callee uses status code 603 (Decline) instead. This status response is returned only if the client knows that no other end point (such as a voice mail system) will answer the request. Otherwise, 486 (Busy Here) should be returned
603 Decline	The calleds machine was successfully contacted but the user explicitly does not wish to or cannot participate. The response MAY indicate a better time to call in the Retry-After header field. This

SIP Response Code	Description
	status response is returned only if the client knows that no other end point will answer the request
604 Does Not Exist Anywhere	The server has authoritative information that the user indicated in the Request-URI does not exist anywhere
606 Not Acceptable	The user's agent was contacted successfully but some aspects of the session description such as the requested media, bandwidth, or addressing style were not acceptable. A 606 (Not Acceptable) response means that the user wishes to communicate, but cannot adequately support the session described. The 606 (Not Acceptable) response MAY contain a list of reasons in a Warning header field describing why the session described cannot be supported.

6. Session Description Protocol

The Session Description Protocol (SDP), described in RFC 2372, is used by the Megapath SIP Trunk Interface as part of establishing a voice call, or other multimedia session. The purpose of SDP is to convey critical information about media streams such as port, ip, codec, type of media, and sampling rate so that all recipients can participate in a session. SDP is transmitted as the body of a SIP message.

The Megapath SIP Trunk Interface utilizes the Offer/Answer Model defined in RFC 3264 to negotiate a media session.

6.1 SDP Support

The following table shows the Megapath SIP Trunk Interface SDP support. Optional items are marked with an "*".

Table 6-1 SDP Supported Parameters

SDP keyword	Megapath SIP Trunk Interface support
v= (protocol version)	Required (Sent/Received)
o= (owner/creator and session identifier)	Required (Sent/Received)
s= (session name)	Required (Sent/Received)
i=* (session information)	Optional (Received)
u=* (URI of description)	Optional (Received)
e=* (email address)	Optional (Received)
p=* (phone number)	Optional (Received)
c=* (connection information - not required if included in all media sections)	Optional (Received)
b=* (bandwidth information)	Optional (Received)
One or more time descriptions	Required (Sent/Received)
z=* (time zone adjustments)	Optional (Received)
k=* (encryption key)	Optional (Received)
a=* (zero or more session attribute lines)	Optional (Received)
One or More media descriptions (See Below)	Required (Sent/Received)
Time Description	
t= (time the session is active)	Required (Sent/Received)
r=* (zero or more repeat times)	Optional (Received)
Media Description	
m= (media name and transport address)	Required (Sent/Received)
i=* (media title)	Optional (Received)
c=* (connection information - optional if included at session-level)	Optional (Received)

SDP keyword	Megapath SIP Trunk Interface support
b=* (zero or more bandwidth information lines)	Optional (Received)
k=* (encryption key)	Optional (Received)
a=* (zero or more media attribute lines)	Optional (Received)

6.2 Media Negotiation

6.3 The Offer/Answer Model

The Megapath SIP Trunk Interface uses the Offer/Answer Model defined in RFC 3264 to negotiate media characteristics of a media session. Any media endpoint that originates and/or terminates RTP to the SMI MUST utilize SDP in conjunction with the Offer/Answer Model to exchange critical information about media streams.

6.4 Media Types

6.4.1 Audio Media

The following Audio codecs are supported:

- G.711 (PCMU) SDP Payload type of 0, and ptime size of 20ms
- G.729A SDP Payload type of 8

6.4.2 DTMF

The Enterprise SIP Trunk Interface MUST support RFC 2833 style DTMF Tones (dynamic payload type of 101). The Following SDP body demonstrates the use of G.729 along with the DTMF payload.

Example DTMF:

```
v=0
o=- 4321 1234 IN IP4 192.168.4.122
s=ApplicationServer
c=IN IP4 192.168.3.122
t=0 0
m=audio 5106 RTP/AVP 18 101
a=maxptime:20
a=fmtp:18 annexb=no
a=rtpmap: 101 telephone-event/8000
a=fmtp: 101 0-15
```

6.4.3 Fax/Modem Media

All Faxes MUST be sent using G.711. If the call was setup using another codec the Enterprise SIP Trunk Interface MUST either send a reINVITE as described in RFC 3261.

6.4.4 Other Media

Video, Application, and data media types are not supported by the Megapath Network. These media types will be ignored.

6.5 Modifying and Existing SIP Session

The Megapath SIP Trunk Interface supports the reINVITE (RFC 3261) method for modifying a session. Once the dialog is established between the Enterprise SIP Trunk Interface and Megapath SIP Trunk Interface, either side MAY send a reINVITE to update any media attribute of a session. If negotiation fails, the Megapath SIP Trunk Interface will return a 488 status code and the original session will remain intact.

6.6 SIP Message Body Types

The Megapath SIP Trunk Interface only supports one SIP Message Body type at this time, all other message body types will be ignored.

SDP (Session Description Protocol) is fully supported.

Example of a fragment of a sip message containing a SDP Body follows:

```
Content-Type: application/sdp
Content-Length: 137

v=0
o=- 4321 1234 IN IP4 192.168.4.123
s=Speakeasy SIP Trunk Interface VoIP Call
c=IN IP4 192.168.3.123
t=0 0
m=audio 20000 RTP/AVP 0
a=ptime:20
```

7. RTP and RTCP Support

7.1 RTP

SIP utilizes RTP (real-time transport protocol) defined by RFC 1889, for transporting real-time session data. RTP provides the end-to-end network transport functions used by applications that need to transmit real-time data, such as audio or video over multicast and unicast network services.

The SMI only supports RTP in a symmetric unicast manner with packetization rate of 20ms. The SMI (refer to Table 7-1 RTP Headers and SMI Support) uses UDP ports in the range 49152 to 65535 for receiving RTP media streams. The SMI does not support encryption.

Table 7-1 RTP Headers and SMI Support

SMI	Description
Version	This field indicates the version of RTP. The SMI supports version 2
Padding	If the padding bit is set, the packet contains one or more additional padding octets at the end which are not part of the payload. The SMI supports padding
Extension	This header is for experimental use and is not supported at the SMI
CSRC	The CSRC (Contributing Source Count) count contains the number of CSRC identifiers that follow the fixed header. In most cases, RTP from the SMI will be 0. If a different value is received, the SMI will pass it on along with the list of CSRCs
Marker	The interpretation of the marker is defined by an audio/video profile. It is intended to allow significant events such as frame boundaries to be marked in the packet stream. The SMI does not support use of the marker bit as the supported codecs do not use them
Payload Type	This field identifies the format of the RTP payload and determines its interpretation by the application. A profile MAY specify a default static mapping of payload type codes to payload formats. The SMI supports PCMU, G.729 and telephone-event 101 (DTMF digits). See section 10.2 for more details of supported codecs
Sequence Number	Indicates the order of the RTP packets as they are generated. The sequence number is a 16 bit integer and increments by one for each RTP data packet sent. It may be used by the receiver to detect packet loss and to restore packet sequence. The initial value of the sequence number from the SMI will be random
Extended Sequence Number	This is usually only seen by a monitoring application. It is a 32 bit integer used by applications and codecs to keep an overall sequence number as a typical 20ms call will wrap to zero about every 20 minutes and a 32 bit integer would wrap about every 2 years. This sequence number contains the number of wraps and the sequence number from the RTP header
Timestamp	The timestamp reflects the sampling instant of the first octet in the RTP data packet. The sampling instant is derived from a clock that increments

SMI	Description
	monotonically and linearly in time to allow synchronization and jitter calculations. As an example, for fixed-rate audio the timestamp clock would likely increment by one for each sampling period. If an audio application reads blocks covering 160 sampling periods from the input device, the timestamp would be increased by 160 for each such block, regardless of whether the block is transmitted in a packet or dropped as silent. The initial value of the timestamp from the SMI is random and increment by 160 for each packet
SSRC	The SSRC field identifies the synchronization source. This identifier is chosen randomly, with the intent that no two synchronization sources within the same RTP session will have the same SSRC identifier. This is a constant in each RTP packet and is used for mixing streams. The SMI will create a new SSRC for each stream to the EMI
CSRC list	The CSRC list identifies the contributing sources for the payload contained in this packet. The number of identifiers is given by the CSRC field. CSRC identifiers are inserted by mixers using the SSRC identifiers of contributing sources. RTP from the SMI will not contain a CSRC list

7.2 RTCP

The RTP Control Protocol (RTCP) is based on the periodic transmission of control packets to all participants in the session to provide feedback on the quality of the data distribution. RTCP is not supported at the SMI and will be silently discarded.

8. Sample Call Flows

8.1 Outbound from Enterprise to Megapath

Call displayed as ladder diagram:

```
Enterprise SIP Trunk Interface      Megapath SIP Trunk Interface
                 |   INVITE SDP           |
                 |   ------------------>  |
                 |   100 Trying           |
                 |   <------------------  |
                 |   401 Unauthorized     |
                 |   <------------------  |
                 |   ACK                  |
                 |   ------------------>  |
                 |   INVITE SDP           |
                 |   ------------------>  |
                 |   100 Trying           |
                 |   <------------------  |
                 |   183 Sess Prog SDP    |
                 |   <------------------  |
                 |   200 OK SDP           |
                 |   <------------------  |
                 |   ACK                  |
                 |   ------------------>  |
                 |   BYE                  |
                 |   <------------------  |
                 |   200 OK               |
                 |   ------------------>  |
```

Same call displayed as packets:

```
    Request-Line: INVITE sip:+12067343080@speakeasy.net SIP/2.0
    Message Header
        Via: SIP/2.0/UDP 66.93.179.239:5060;branch=z9hG4bK05aa8e3c;rport
        From: "2063844840" <sip:2063844840@speakeasy.net>;tag=as1166d37d
        To: <sip:+12067343080@speakeasy.net>
        Contact: <sip:2063844840@66.93.179.239>
        Call-ID: 350ea0d70528e4676c1574957d6ca03d@speakeasy.net
        CSeq: 102 INVITE
        User-Agent: Asterisk PBX
        Max-Forwards: 70
        Date: Tue, 10 Feb 2009 22:56:39 GMT
        Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
        Supported: replaces
        Content-Type: application/sdp
        Content-Length: 184
    Message Body
        Session Description Protocol
            Session Description Protocol Version (v): 0
            Owner/Creator, Session Id (o): root 3042 3042 IN IP4
66.93.179.239
            Session Name (s): session
            Connection Information (c): IN IP4 66.93.179.239
            Time Description, active time (t): 0 0
            Media Description, name and address (m): audio 14870 RTP/AVP 0
            Media Attribute (a): rtpmap:0 PCMU/8000
            Media Attribute (a): silenceSupp:off - - - -
```

```
            Media Attribute (a): ptime:20
            Media Attribute (a): sendrecv

    Status-Line: SIP/2.0 100 Trying
    Message Header
        Via: SIP/2.0/UDP
66.93.179.239:5060;branch=z9hG4bK05aa8e3c;rport=5060
        From: "2063844840" <sip:2063844840@speakeasy.net>;tag=as1166d37d
        To: <sip:+12067343080@speakeasy.net>
        Call-ID: 350ea0d70528e4676c1574957d6ca03d@speakeasy.net
        CSeq: 102 INVITE

    Status-Line: SIP/2.0 401 Unauthorized
    Message Header
        Via: SIP/2.0/UDP
66.93.179.239:5060;branch=z9hG4bK05aa8e3c;rport=5060
        From: "2063844840" <sip:2063844840@speakeasy.net>;tag=as1166d37d
        To: <sip:+12067343080@speakeasy.net>;tag=SDv0gdd99-536245398-
1234306631439
        Call-ID: 350ea0d70528e4676c1574957d6ca03d@speakeasy.net
        CSeq: 102 INVITE
        WWW-Authenticate: DIGEST
realm="BroadWorks",qop="auth",algorithm=MD5,nonce="BroadWorksXfr16as5rTf053g
1BW"
        Content-Length: 0

    Request-Line: ACK sip:+12067343080@speakeasy.net SIP/2.0
    Message Header
        Via: SIP/2.0/UDP 66.93.179.239:5060;branch=z9hG4bK05aa8e3c;rport
        From: "2063844840" <sip:2063844840@speakeasy.net>;tag=as1166d37d
        To: <sip:+12067343080@speakeasy.net>;tag=SDv0gdd99-536245398-
1234306631439
        Contact: <sip:2063844840@66.93.179.239>
        Call-ID: 350ea0d70528e4676c1574957d6ca03d@speakeasy.net
        CSeq: 102 ACK
        User-Agent: Asterisk PBX
        Max-Forwards: 70
        Content-Length: 0

    Request-Line: INVITE sip:+12067343080@speakeasy.net SIP/2.0
    Message Header
        Via: SIP/2.0/UDP 66.93.179.239:5060;branch=z9hG4bK0a0d2fa5;rport
        From: "2063844840" <sip:2063844840@speakeasy.net>;tag=as1166d37d
        To: <sip:+12067343080@speakeasy.net>
        Contact: <sip:2063844840@66.93.179.239>
        Call-ID: 350ea0d70528e4676c1574957d6ca03d@speakeasy.net
        CSeq: 103 INVITE
        User-Agent: Asterisk PBX
        Max-Forwards: 70
        Authorization: Digest username="9000000743", realm="BroadWorks",
algorithm=MD5, uri="sip:+12067343080@speakeasy.net",
nonce="BroadWorksXfr16as5rTf053g1BW",
response="624c5706d246823adbed5e0b955449ed", qop=auth, cnonce="444d9235",
nc=000000
        Date: Tue, 10 Feb 2009 22:56:39 GMT
        Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
        Supported: replaces
        Content-Type: application/sdp
        Content-Length: 184
    Message Body
```

```
        Session Description Protocol
            Session Description Protocol Version (v): 0
            Owner/Creator, Session Id (o): root 3042 3043 IN IP4
66.93.179.239
            Session Name (s): session
            Connection Information (c): IN IP4 66.93.179.239
            Time Description, active time (t): 0 0
            Media Description, name and address (m): audio 14870 RTP/AVP 0
            Media Attribute (a): rtpmap:0 PCMU/8000
            Media Attribute (a): silenceSupp:off - - - -
            Media Attribute (a): ptime:20
            Media Attribute (a): sendrecv

    Status-Line: SIP/2.0 100 Trying
    Message Header
        Via: SIP/2.0/UDP
66.93.179.239:5060;branch=z9hG4bK0a0d2fa5;rport=5060
        From: "2063844840" <sip:2063844840@speakeasy.net>;tag=as1166d37d
        To: <sip:+12067343080@speakeasy.net>
        Call-ID: 350ea0d70528e4676c1574957d6ca03d@speakeasy.net
        CSeq: 103 INVITE

    Status-Line: SIP/2.0 183 Session Progress
    Message Header
        Via: SIP/2.0/UDP
66.93.179.239:5060;branch=z9hG4bK0a0d2fa5;rport=5060
        From: "2063844840" <sip:2063844840@speakeasy.net>;tag=as1166d37d
        To: <sip:+12067343080@speakeasy.net>;tag=SDv0gdd99-1550287726-
1234306632611
        Call-ID: 350ea0d70528e4676c1574957d6ca03d@speakeasy.net
        CSeq: 103 INVITE
        Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
        Supported:
        Contact: <sip:+12067343080@69.17.110.135:5060;transport=udp>
        Session: Media
        Remote-Party-ID:
<sip:2067343080@66.92.30.132;user=phone>;screen=yes;party=called;privacy=off
;id-type=subscriber
        Content-Type: application/sdp
        Content-Length: 145
    Message Body
        Session Description Protocol
            Session Description Protocol Version (v): 0
            Owner/Creator, Session Id (o): - 1642594582 1 IN IP4
69.17.110.135
            Session Name (s): -
            Connection Information (c): IN IP4 69.17.110.135
            Time Description, active time (t): 0 0
            Media Description, name and address (m): audio 50102 RTP/AVP 0
            Media Attribute (a): ptime:20
            Media Attribute (a): bsoft: 1 image udptl t38

    Status-Line: SIP/2.0 200 OK
    Message Header
        Via: SIP/2.0/UDP
66.93.179.239:5060;branch=z9hG4bK0a0d2fa5;rport=5060
        From: "2063844840" <sip:2063844840@speakeasy.net>;tag=as1166d37d
        To: <sip:+12067343080@speakeasy.net>;tag=SDv0gdd99-1550287726-
1234306632611
        Call-ID: 350ea0d70528e4676c1574957d6ca03d@speakeasy.net
```

```
        CSeq: 103 INVITE
        Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
        Supported:
        Contact: <sip:+12067343080@69.17.110.135:5060;transport=udp>
        Remote-Party-ID:
<sip:206734308 0@66.92.30.132;user=phone>;screen=yes;party=called;privacy=off
;id-type=subscriber
        Accept:
multipart/mixed,application/media_control+xml,application/sdp
        Content-Type: application/sdp
        Content-Length: 145
    Message Body
        Session Description Protocol
            Session Description Protocol Version (v): 0
            Owner/Creator, Session Id (o): - 1642594582 1 IN IP4
69.17.110.135
            Session Name (s): -
            Connection Information (c): IN IP4 69.17.110.135
            Time Description, active time (t): 0 0
            Media Description, name and address (m): audio 50102 RTP/AVP 0
            Media Attribute (a): ptime:20
            Media Attribute (a): bsoft: 1 image udptl t38

    Request-Line: ACK sip:+12067343080@69.17.110.135:5060;transport=udp
SIP/2.0
    Message Header
        Via: SIP/2.0/UDP 66.93.179.239:5060;branch=z9hG4bK1e948ba7;rport
        From: "2063844840" <sip:2063844840@speakeasy.net>;tag=as1166d37d
        To: <sip:+12067343080@speakeasy.net>;tag=SDv0gdd99-1550287726-
1234306632611
        Contact: <sip:2063844840@66.93.179.239>
        Call-ID: 350ea0d70528e4676c1574957d6ca03d@speakeasy.net
        CSeq: 103 ACK
        User-Agent: Asterisk PBX
        Max-Forwards: 70
        Content-Length: 0


    Request-Line: BYE sip:2063844840@66.93.179.239 SIP/2.0
    Message Header
        Via: SIP/2.0/UDP
69.17.110.135:5060;branch=z9hG4bKb16dg0202oghga0up040sdh1d6472.1
        From: <sip:+12067343080@speakeasy.net>;tag=SDv0gdd99-1550287726-
1234306632611
        To: "2063844840" <sip:2063844840@speakeasy.net>;tag=as1166d37d
        Call-ID: 350ea0d70528e4676c1574957d6ca03d@speakeasy.net
        CSeq: 825508750 BYE
        Max-Forwards: 9
        Content-Length: 0

    Status-Line: SIP/2.0 200 OK
    Message Header
        Via: SIP/2.0/UDP
69.17.110.135:5060;branch=z9hG4bKb16dg0202oghga0up040sdh1d6472.1;received=69
.17.110.135
        From: <sip:+12067343080@speakeasy.net>;tag=SDv0gdd99-1550287726-
1234306632611
        To: "2063844840" <sip:2063844840@speakeasy.net>;tag=as1166d37d
        Call-ID: 350ea0d70528e4676c1574957d6ca03d@speakeasy.net
        CSeq: 825508750 BYE
```

```
        User-Agent: Asterisk PBX
        Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
        Supported: replaces
        Contact: <sip:2063844840@66.93.179.239>
        Content-Length: 0
```

8.2 Inbound to Enterprise from Megapath

Call displayed as a ladder diagram:

```
Megapath SIP Trunk Interface    Enterprise SIP Trunk Interface
          | INVITE SDP           |
          | ------------------>  |
          | 100 Trying           |
          | <------------------  |
          | 180 Ringing          |
          | <------------------  |
          | 200 OK SDP           |
          | <------------------  |
          | ACK                  |
          | ------------------>  |
          | BYE                  |
          | ------------------>  |
          | 200 OK               |
          | <------------------  |
```

Same call displayed as packets:

```
    Request-Line: INVITE sip:2063844840@66.93.179.239 SIP/2.0
    Message Header
        Via: SIP/2.0/UDP
69.17.110.135:5060;branch=z9hG4bK6p9dul20a860fbs1s0c0.1
        From: "SEATTLE
WA"<sip:2067343080@69.17.110.135;user=phone>;tag=SDckina01-1058286018-
1234307108806-
        To: "DID 1"<sip:2063844840@speakeasy.net>
        Call-ID: SDckina01-b6038671ba7e9274b9bec2197791db00-v3000v3
        CSeq: 825747428 INVITE
        Contact: <sip:2067343080@69.17.110.135:5060;transport=udp>
        Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
        Accept:
multipart/mixed,application/media_control+xml,application/sdp
        Supported:
        Max-Forwards: 9
        Content-Type: application/sdp
        Content-Length: 192
    Message Body
        Session Description Protocol
            Session Description Protocol Version (v): 0
```

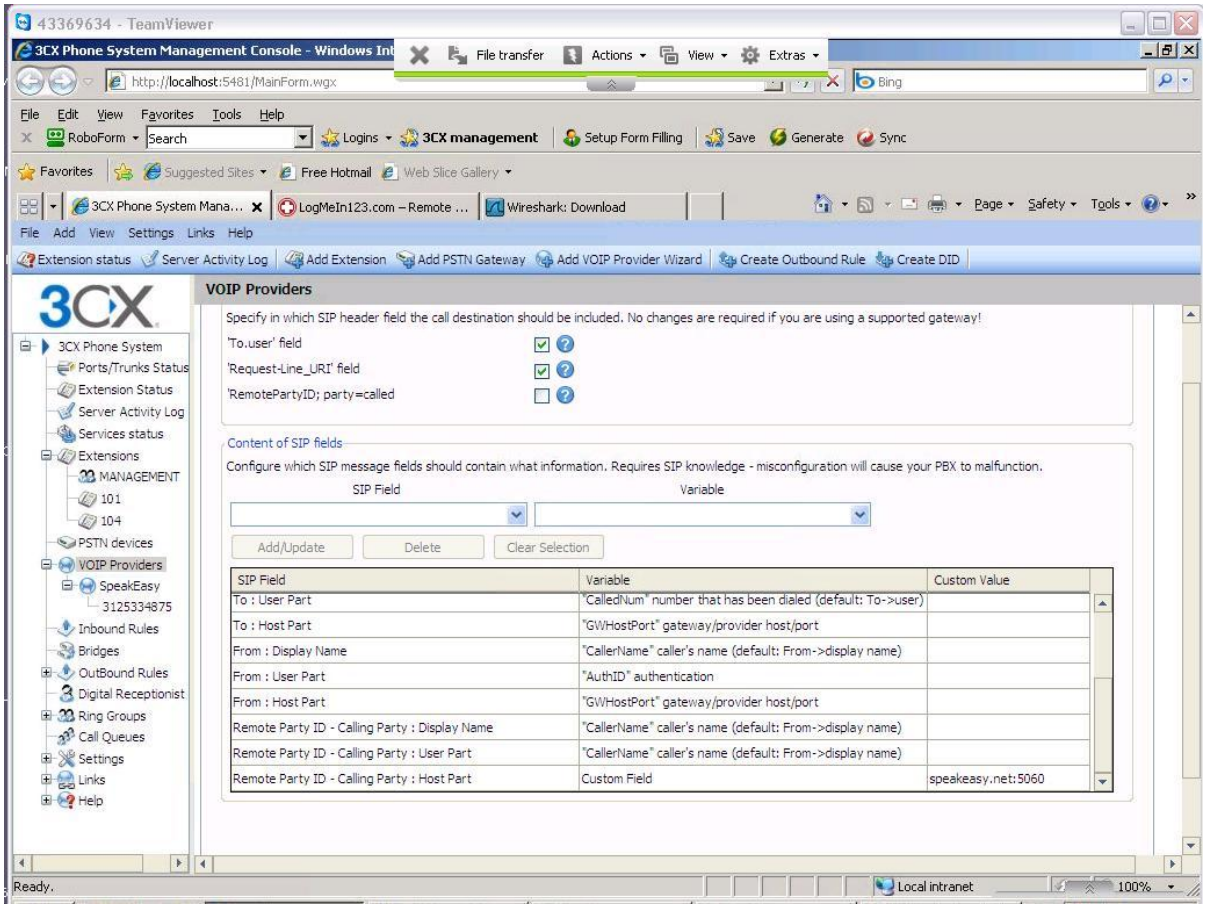
```
            Owner/Creator, Session Id (o): - 2179465473 1 IN IP4
69.17.110.135
            Session Name (s): -
            Connection Information (c): IN IP4 69.17.110.135
            Time Description, active time (t): 0 0
            Media Description, name and address (m): audio 50110 RTP/AVP 0
18 101
            Media Attribute (a): rtpmap:101 telephone-event/8000
            Media Attribute (a): fmtp:101 0-15
            Media Attribute (a): bsoft: 1 image udptl t38

    Status-Line: SIP/2.0 100 Trying
    Message Header
        Via: SIP/2.0/UDP
69.17.110.135:5060;branch=z9hG4bK6p9dul20a860fbs1s0c0.1;received=69.17.110.1
35
        From: "SEATTLE
WA"<sip:2067343080@69.17.110.135;user=phone>;tag=SDckina01-1058286018-
1234307108806-
        To: "DID 1"<sip:2063844840@speakeasy.net>
        Call-ID: SDckina01-b6038671ba7e9274b9bec2197791db00-v3000v3
        CSeq: 825747428 INVITE
        User-Agent: Asterisk PBX
        Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
        Supported: replaces
        Contact: <sip:2063844840@66.93.179.239>
        Content-Length: 0

    Status-Line: SIP/2.0 180 Ringing
    Message Header
        Via: SIP/2.0/UDP
69.17.110.135:5060;branch=z9hG4bK6p9dul20a860fbs1s0c0.1;received=69.17.110.1
35
        From: "SEATTLE
WA"<sip:2067343080@69.17.110.135;user=phone>;tag=SDckina01-1058286018-
1234307108806-
        To: "DID 1"<sip:2063844840@speakeasy.net>;tag=as1f9b414d
        Call-ID: SDckina01-b6038671ba7e9274b9bec2197791db00-v3000v3
        CSeq: 825747428 INVITE
        User-Agent: Asterisk PBX
        Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
        Supported: replaces
        Contact: <sip:2063844840@66.93.179.239>
        Content-Length: 0

    Status-Line: SIP/2.0 200 OK
    Message Header
        Via: SIP/2.0/UDP
69.17.110.135:5060;branch=z9hG4bK6p9dul20a860fbs1s0c0.1;received=69.17.110.1
35
        From: "SEATTLE
WA"<sip:2067343080@69.17.110.135;user=phone>;tag=SDckina01-1058286018-
1234307108806-
        To: "DID 1"<sip:2063844840@speakeasy.net>;tag=as1f9b414d
        Call-ID: SDckina01-b6038671ba7e9274b9bec2197791db00-v3000v3
        CSeq: 825747428 INVITE
        User-Agent: Asterisk PBX
        Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
        Supported: replaces
        Contact: <sip:2063844840@66.93.179.239>
```

```
        Content-Type: application/sdp
        Content-Length: 184
    Message Body
        Session Description Protocol
            Session Description Protocol Version (v): 0
            Owner/Creator, Session Id (o): root 3042 3042 IN IP4
66.93.179.239
            Session Name (s): session
            Connection Information (c): IN IP4 66.93.179.239
            Time Description, active time (t): 0 0
            Media Description, name and address (m): audio 12152 RTP/AVP 0
            Media Attribute (a): rtpmap:0 PCMU/8000
            Media Attribute (a): silenceSupp:off - - - -
            Media Attribute (a): ptime:20
            Media Attribute (a): sendrecv

    Request-Line: ACK sip:2063844840@66.93.179.239 SIP/2.0
    Message Header
        Via: SIP/2.0/UDP
69.17.110.135:5060;branch=z9hG4bK71nhi830a8khoa4ud1c0.1
        From: "SEATTLE
WA"<sip:2067343080@69.17.110.135;user=phone>;tag=SDckina01-1058286018-
1234307108806-
        To: "DID 1"<sip:2063844840@speakeasy.net>;tag=as1f9b414d
        Call-ID: SDckina01-b6038671ba7e9274b9bec2197791db00-v3000v3
        CSeq: 825747428 ACK
        Contact: <sip:2067343080@69.17.110.135:5060;transport=udp>
        Max-Forwards: 9
        Content-Length: 0

    Request-Line: BYE sip:2063844840@66.93.179.239 SIP/2.0
    Message Header
        Via: SIP/2.0/UDP
69.17.110.135:5060;branch=z9hG4bK71nhi830a8khoa4ud1c0cdhpdeui3.1
        From: "SEATTLE
WA"<sip:2067343080@69.17.110.135;user=phone>;tag=SDckina01-1058286018-
1234307108806-
        To: "DID 1"<sip:2063844840@speakeasy.net>;tag=as1f9b414d
        Call-ID: SDckina01-b6038671ba7e9274b9bec2197791db00-v3000v3
        CSeq: 825747429 BYE
        Max-Forwards: 9
        Content-Length: 0

    Status-Line: SIP/2.0 200 OK
    Message Header
        Via: SIP/2.0/UDP
69.17.110.135:5060;branch=z9hG4bK71nhi830a8khoa4ud1c0cdhpdeui3.1;received=69
.17.110.135
        From: "SEATTLE
WA"<sip:2067343080@69.17.110.135;user=phone>;tag=SDckina01-1058286018-
1234307108806-
        To: "DID 1"<sip:2063844840@speakeasy.net>;tag=as1f9b414d
        Call-ID: SDckina01-b6038671ba7e9274b9bec2197791db00-v3000v3
        CSeq: 825747429 BYE
        User-Agent: Asterisk PBX
        Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
        Supported: replaces
        Contact: <sip:2063844840@66.93.179.239>
        Content-Length: 0
```

Appendix A: 3CX

Navigate and Login to the admin section of the 3CX System Management Console/

1. Select 3CX Phone System and expand the menu.
2. Select "VOIP Providers", run the Add VOIP Provider Wizard
3. Add the fields to match the figure below.



Edit VOIP Provider Settings

Provider Details:

1. SIP server hostname or IP (Enter value here provided by Megapath)
   - If using an Edgemarc, enter Edgemarc's LAN IP address
2. SIP server port MUST be 5060
3. Outbound proxy hostname or IP (Enter value here provided by Megapath)
   - If using an Edgemarc, enter Edgemarc's LAN IP address

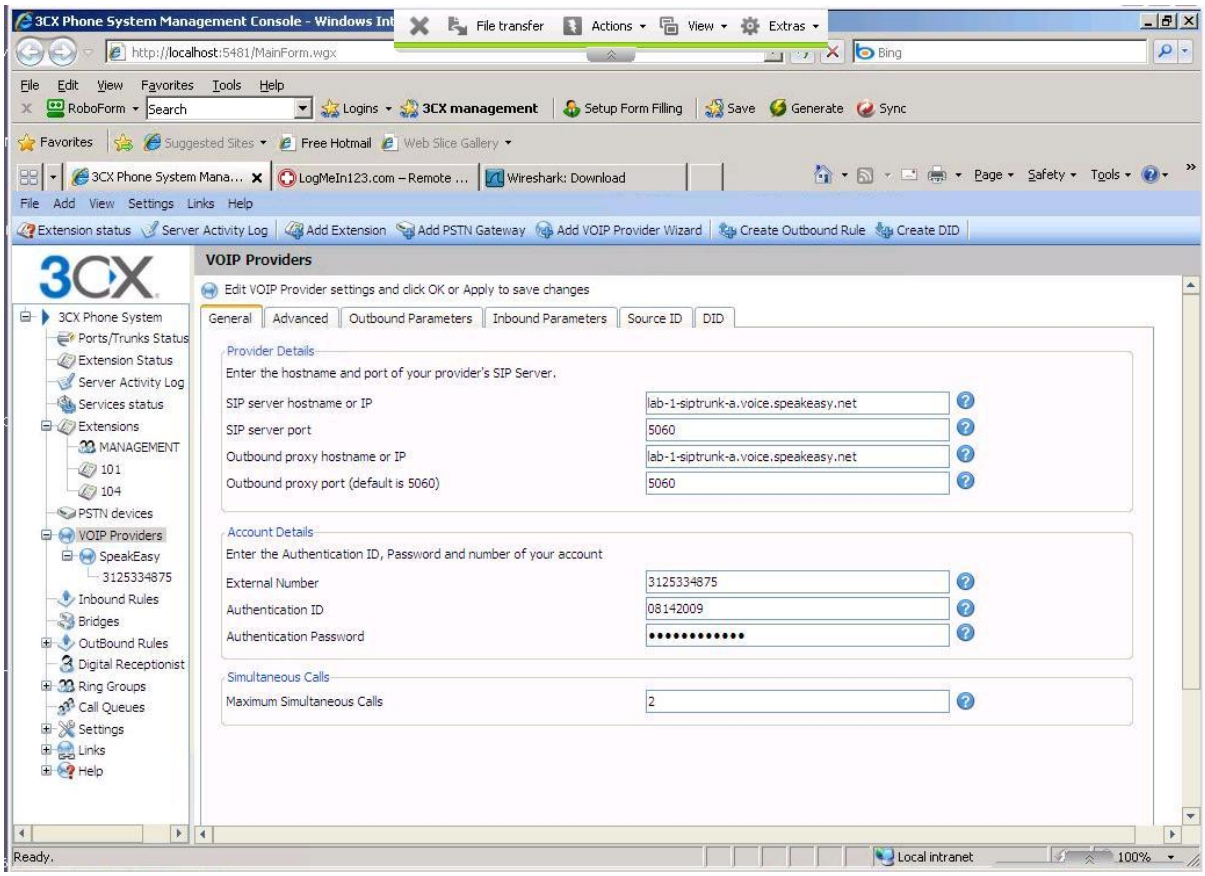
4. Outbound proxy port (default is 5060) MUST be 5060

Account Details:

1. External Number (Enter agreed upon value)
2. Authentication ID (Enter value here provided by Megapath)
3. Authentication Password (Enter value here provided by Megapath)

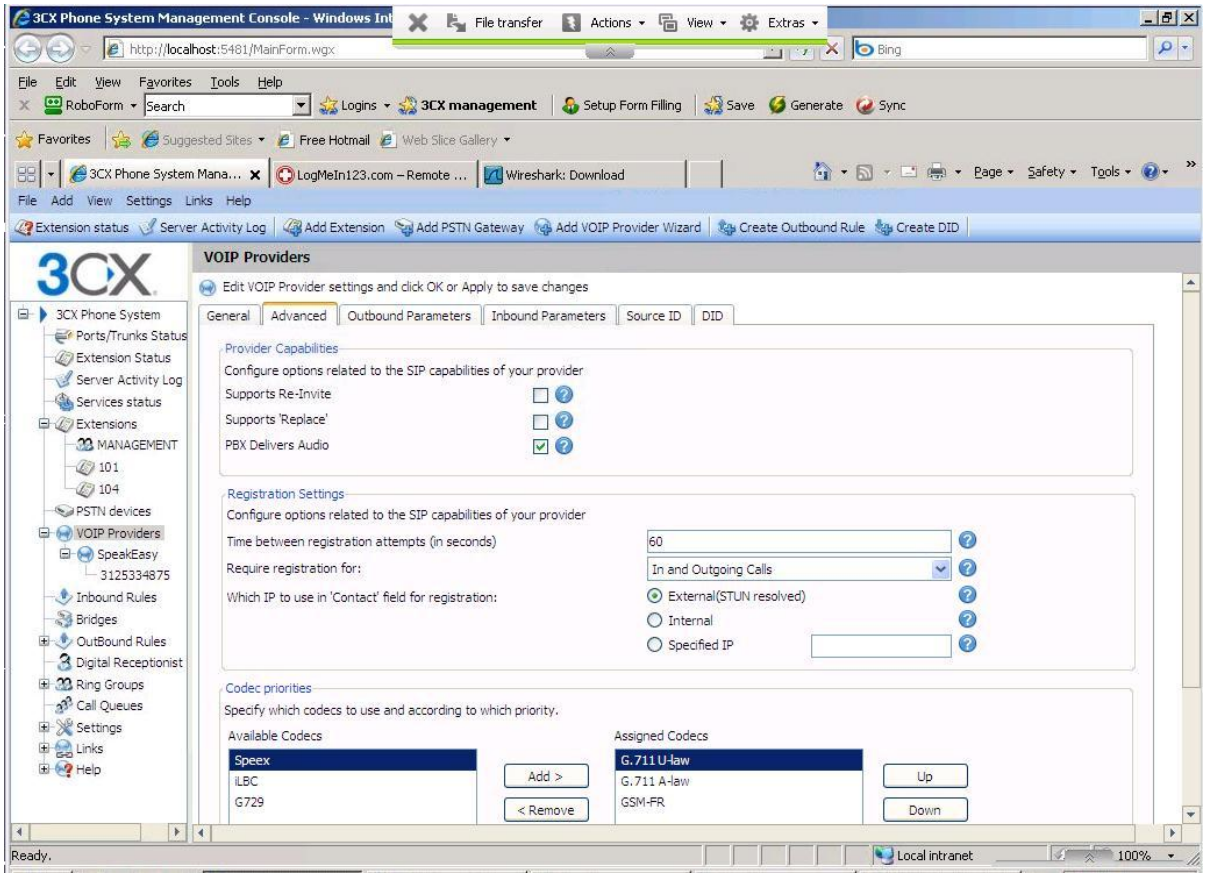
Simultaneous Calls:

1. Maximum Simultaneous Calls (Enter value here provided by Megapath)



Select “Advanced” tab;

- Enter values indicated in below figure



A.1. Broadworks CPE Type

3CX was tested using **Generic SIP PBX Single Registration** as the CPE device type within Broadworks.

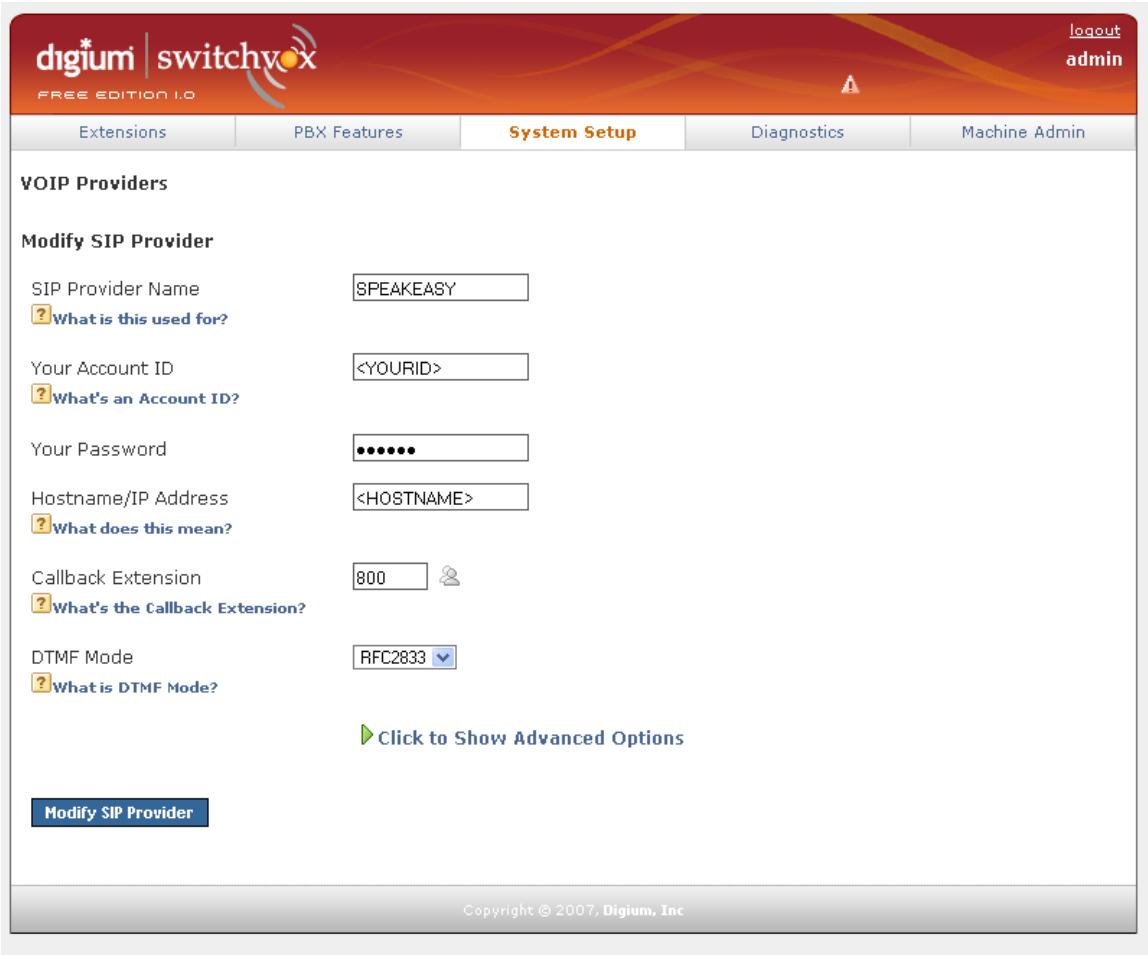
A.2. Tested Software Versions

This was tested with 3CX version 8.0.9342.

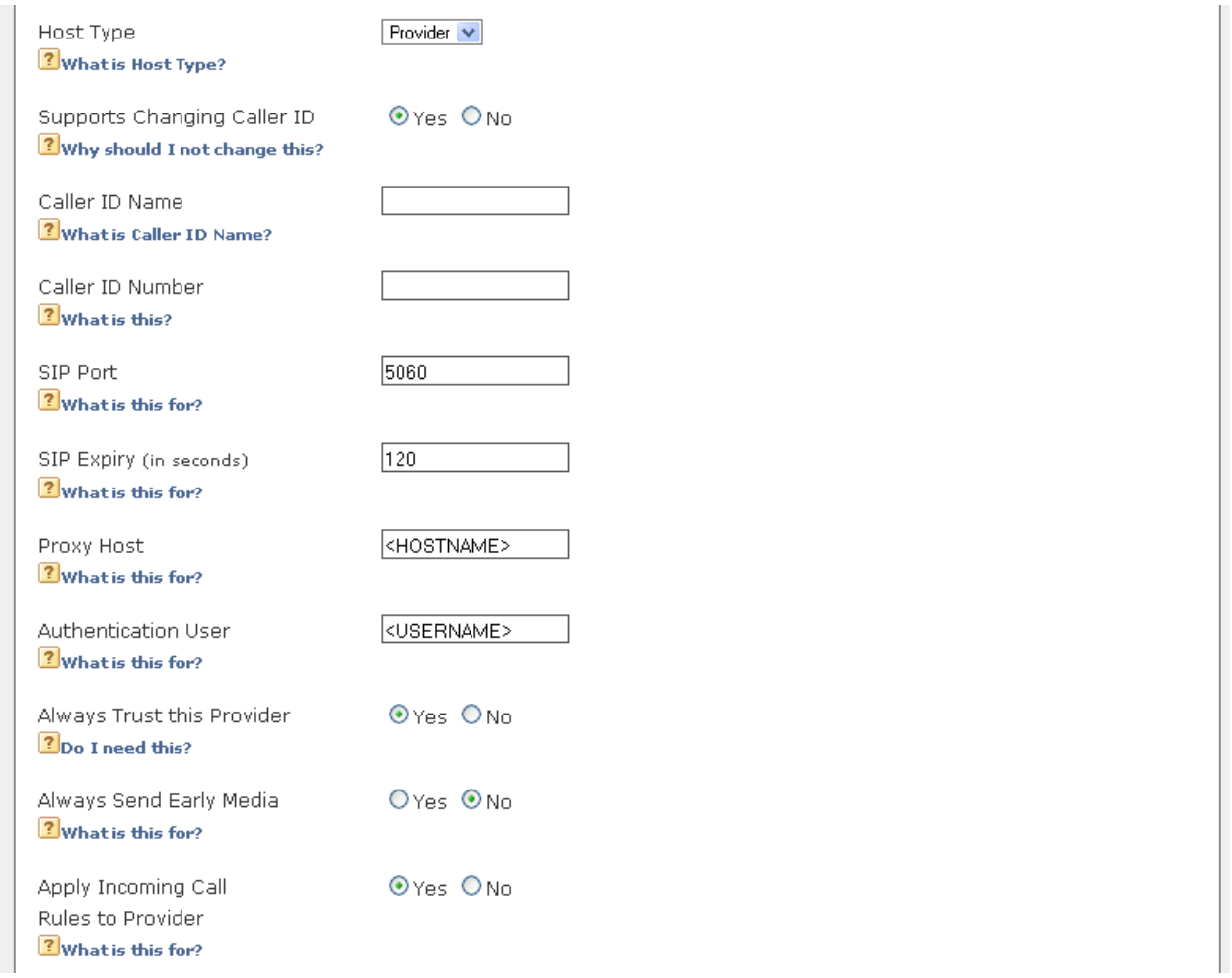
Appendix B: Digium Switchvox

Navigate and Login to the admin section of the web portal https://<IP ADDRESS>/admin/

4. Click "System Setup", and then click "VOIP Providers"
5. Select Add new SIP Provider, and click the Go button and fill out the following Fields



- Set "SIP Provider Name" to MEGAPATH (Any Name will do here it is just a name)
- Set "Your Account ID" To the trunk group username
- Set "Your Password" To The Trunk group password
- Set "Hostname/IP Address" to the Host name assigned to account (SIP Trunk Host provided by Moses)
    - If using en Edgemarc, enter the Edgemarc's LAN IP address
- Select RFC2833 for "DTMF Mode"
- Click the link titled "Click to show advanced options



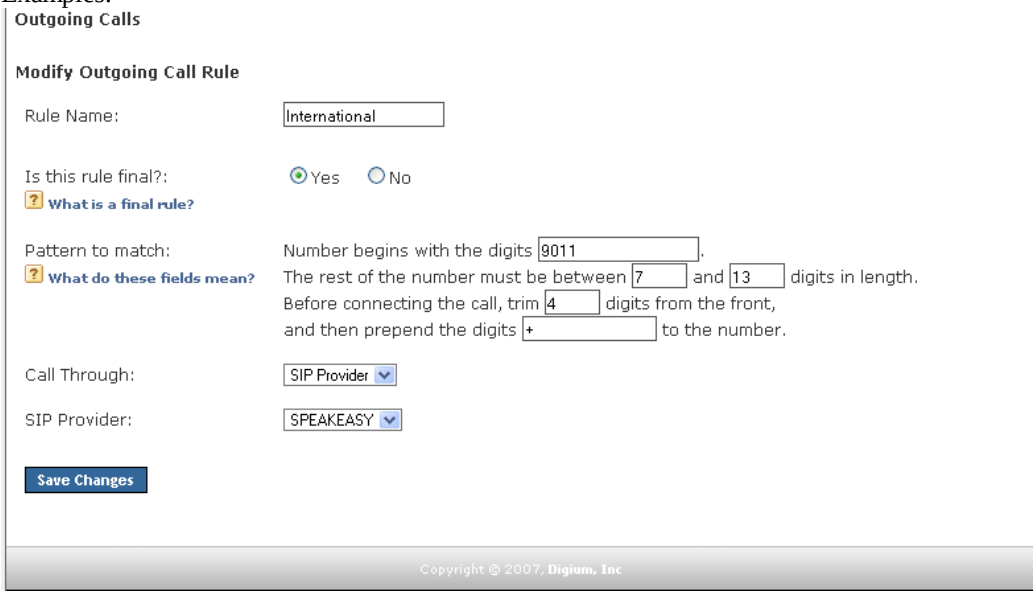
- Set "Supports Changing Caller ID" to Yes
- Set "Proxy Host" to provided hostname
  - If using an Edgemarc, specify the Edgemarc's LAN IP address
- Set "Authentication User to provided username
- Select the appropriate codec -- NOT SHOWN -> at bottom of page

B.1. Routing – Outgoing Calls

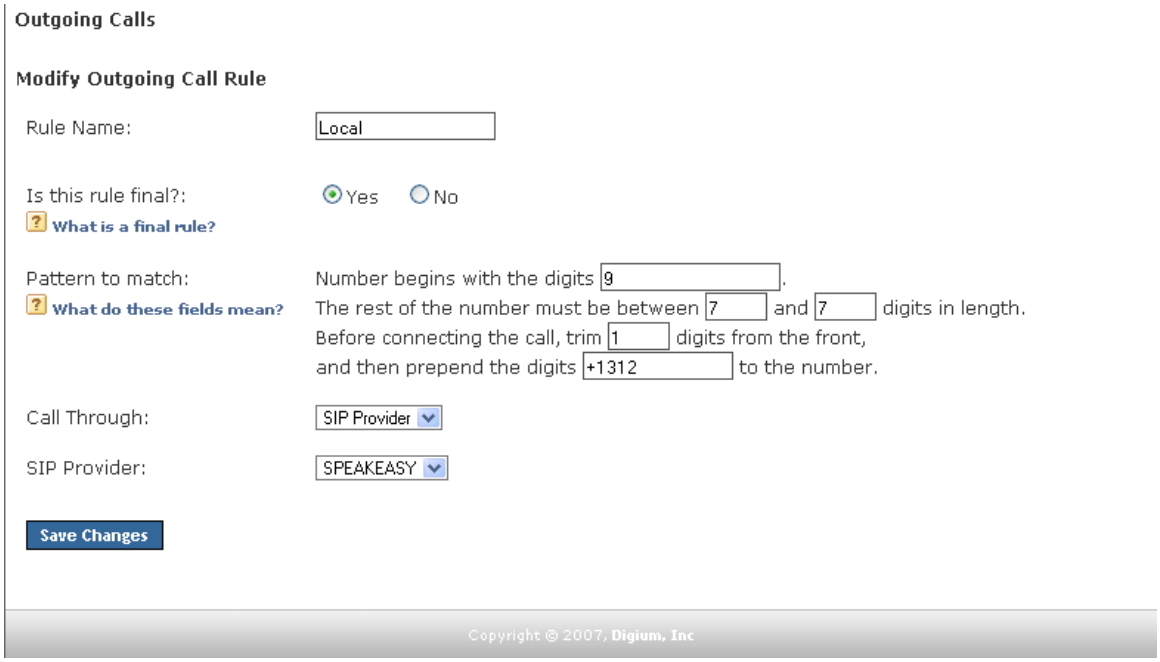
Go to "**System Setup**" then to "**Outgoing Calls**"

All existing routes need to be modified by clicking the Modify button next to the route so that they send calls to the MEGAPATH VoIP provider defined in the previous section, and to send calls out with the appropriate E.164 formatting (+1NPANXXXXXX, or +CCXXXXXXXX for International calls)

Examples:



- Add a "+" in the "prepend the digits" field
- Change "Call Through" to SIP Provider
- Change "SIP Provider" to MEGAPATH (or whatever name used in previous section)



- Add a "+1NPA" in the "prepend the digits" field
- Change "Call Through" to SIP Provider

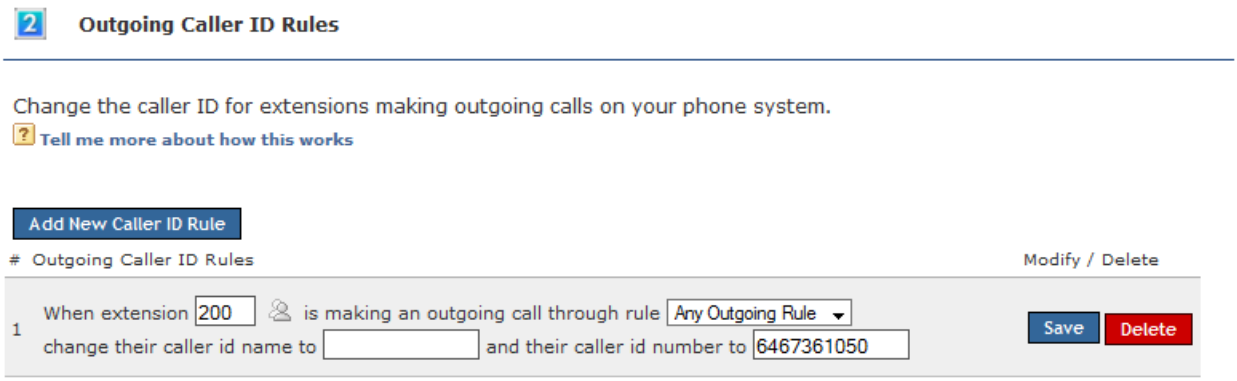
- Change "SIP Provider" to MEGAPATH (or whatever name used in previous section

This process should be repeated for all outgoing dialing patterns that the customer wishes to send to Megapath.

Note – BY DEFAULT THERE IS NO OUTBOUND 911 ROUTE, PLEASE REMIND CUSTOMER TO SET THIS UP

B.2. Routing – Outbound Caller-ID

Go to "**System Setup**", "**Outgoing Calls**", then to "**Outgoing Caller ID Rules**".



Specify Extension number, and specify a Caller ID Number for this extension.

Note – Each extension should have a Caller ID number specified in this manner

B.3. Routing – Incoming Calls

Go to "**System Setup**" then to "**Incoming Calls**"

Every DID needs either an Incoming Call Rule (IE transfer to another number) or An Incoming Call Route (IE Route to an extension). Most cases will use an Incoming call route to send a call to an existing extension.

Click the "Add Route" Button:

- Enter DID in the "Route Number" field
- Enter the extension you want the DID routed to in the "Extension" field
- Click the Save button

B.4. Blind Transfers

Blind Transfer's do not work with Asterisks based systems. This issue can be resolved by setting CLID override on the trunk group.

B.5. Broadworks CPE Type

Digium Switchvox was tested using **Generic SIP PBX Single Registration** as the CPE device type within Broadworks.

B.6. Tested Software Versions

This was tested with Digium Switchvox free addition version 8634.

B.7. Outbound Caller ID

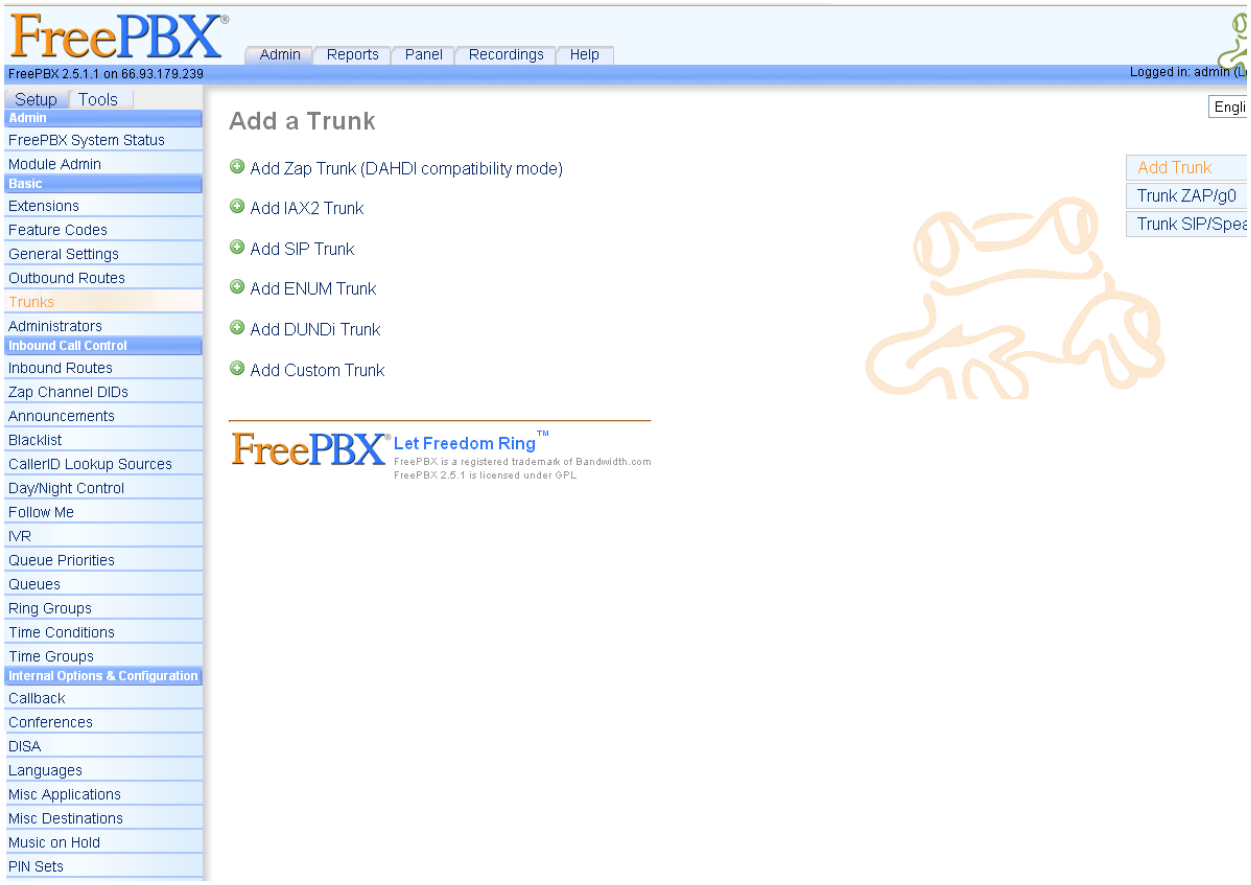
Recommended Outbound Caller ID settings are to be configured using the Outgoing Caller ID Rules. This will allow the customer to configure Outbound Caller ID on a per user (extension) basis. Switchvox does support Global Caller ID settings which is not recommended as remote users may need to have a different 911 address displayed for 911 calls.

Appendix C: Free PBX

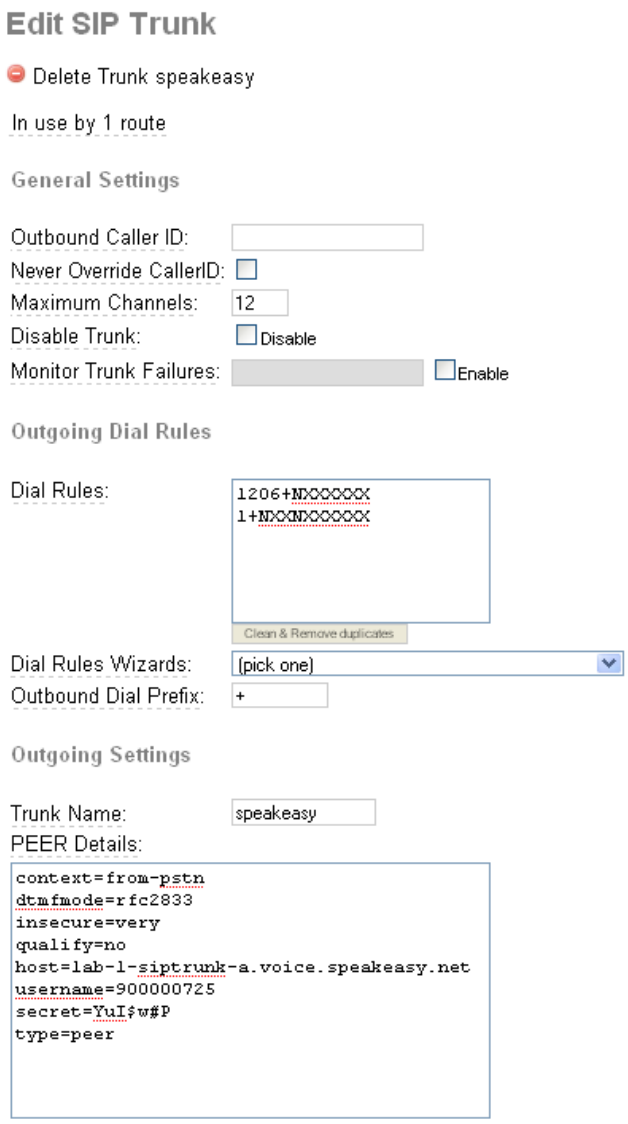
C.1. SIP Trunk

Navigate and login to the FreePBX 2.5 administration page via HTTP (IP address of the FreePBX machine).

Click "**Trunks**" then "**Add SIP Trunk**"



Enter the below information for the SIP Trunk Configuration



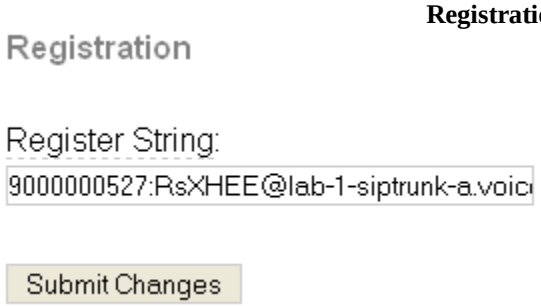
- Set the "**Outbound Caller ID**" if all routes that use this trunk should show a specific caller ID. Example is a company that wants all outbound calls to show the main company number for caller ID.
- Set the "**Maximum Channels**" to the number of SIP Trunks purchased from Megapath.
- **Dial Rules** will set how the calls will be sent from the trunk to Megapath. All outbound calls must be sent as +1NPANXXXXXX. To allow 7 digit and 10 digit dialing, configure as below:
  - **Local Calling:** 1(NPA)+NXXXXXX (NPA is the local area code)
  - **10 Digit Dialing:** 1+NXXNXXXXXX
- **Outbound Dial Prefix:** This option will add the "+" into the outbound call to comply with Megapath's E.164 requirement.

- **Trunk Name:** Name of the SIP Trunk, in this example Megapath is used.
- **Peer Details:** Add the below lines verbatim, except for the username, secret, and host entries. Please use the information provided from Moses for these entries.
  - If using an Edgemarc, enter the Edgemarc's LAN IP address for the Host entry.

```
context=from-pstn
dtmfmode=rfc2833
insecure=very
qualify=no
host=<Host from Moses>
username=<SIP Trunk Username>
secret=<SIP Trunk Password>
type=peer
```

Note – Within Asterisk version 1.4, there is a bug which prevents DNS SRV lookups from functioning properly. Due to this, the hostname used for Asterisk based IP PBXs MUST only use DNS A record associated to it. This hostname can be found in Moses device configuration page.

- At the bottom of the "**Edit SIP Trunk**" page, also enter the **Registration String**:



Registration format:

<username>:<password>@<hostname>/<username>

Username is the SIP Trunk username from Moses. Password is the SIP Trunk password from Moses. XX will need to be replaced with the customer's state code.

Example Register string:

```
9000000527:RsXHEE@wa1-siptrunk-a.voice.speakeasy.net/9000000527
```

"**Submit Changes**" at the bottom of this page and make sure to click the orange "**Apply Configuration Changes**" at the top of the screen.

If using an Edgemarc, the Register string will include the Edgemarc's LAN IP address instead of hostname.

Example Register string using an Edgemarc:

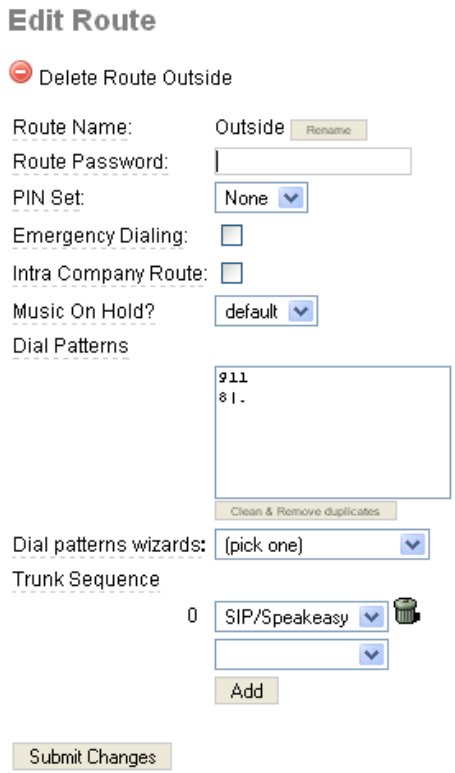
```
9000000527:RsXHEE@192.168.1.1/9000000527
```

C.2. Routing

Inbound/Outbound routes need to be configured within Asterisk to properly route calls.

Note – The below information is only an example of how these routes may be configured. Customer configurations may vary as customers may choose to have multiple SIP providers and configure different routes for each or possibly other routing configurations.

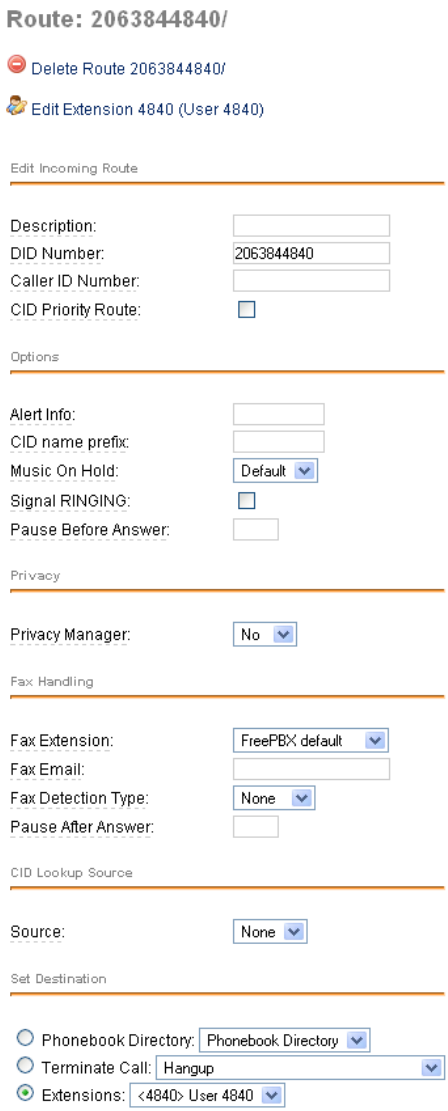
Go to "**Outbound Routes**" then to "**Add Route**"



- "**Route Name**" may be set to anything you'd like. In this example, "Outside" is used.
- "**Dial Patterns**" identify what calls will be sent over the route.
  - 911 - will send 911 calls as dialed
  - 8|. - will send all calls that start with an 8, strip the 8 and pass to the trunk
- "**Trunk Sequence**" specifies what trunk this outbound route will use.

Note – This example would require a user to dial an 8 for an outside line. This is not required and customers may configure this as they would like.

Select "**Inbound Routes**" then "**Add Route**"



- Choose the person, group, or queue to route the call to under "**Set Destination**".

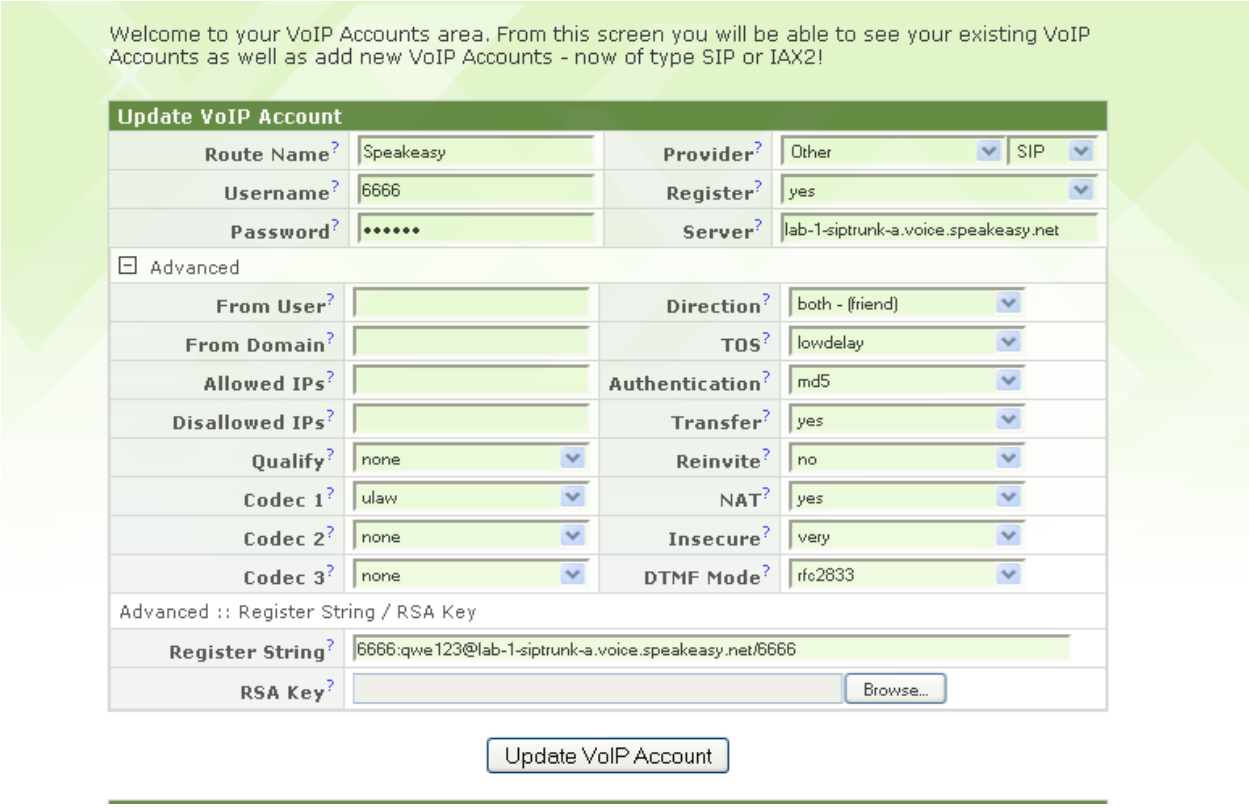
Note – Each DID will need to have an inbound route built.

Appendix D: Trixbox Pro

Navigate and Login to the Trixbox Pro via the Fonality Portal using URL and Username / password

Click "Options" and then click "VoIP"

Click The "Add VoIP Account" Button



- Set "Route Name" to Megapath (or any other name, this will be used later in the config)
- "Provider" to Other
- Set "Username" To Megapath provided Username
- Set "Password" To The Trunk group password
- Set "Register to yes
- Set "Server" to the Host name assigned to account
- Set "Authentication" to md5
- Set "DTMF Mode" to RFC2833
- "Register String" should be auto populated, but if not format is: <UN>:<PW>@<HOST>/<UN>

When using an Edgemarc in front of the Trixbox Pro, some settings will vary from the above configuration.

- Set “Server” to the LAN IP address of the Edgemarc
- Set “From Domain” to the LAN IP address of the Edgemarc
- Set “Outbound Proxy” to the LAN IP address of the Edgemarc
- Verify “Register String” is properly formatted as follows:
  <UN>:<PW>@<Edgemarc LAN IP >/<UN>

D.1. Routing

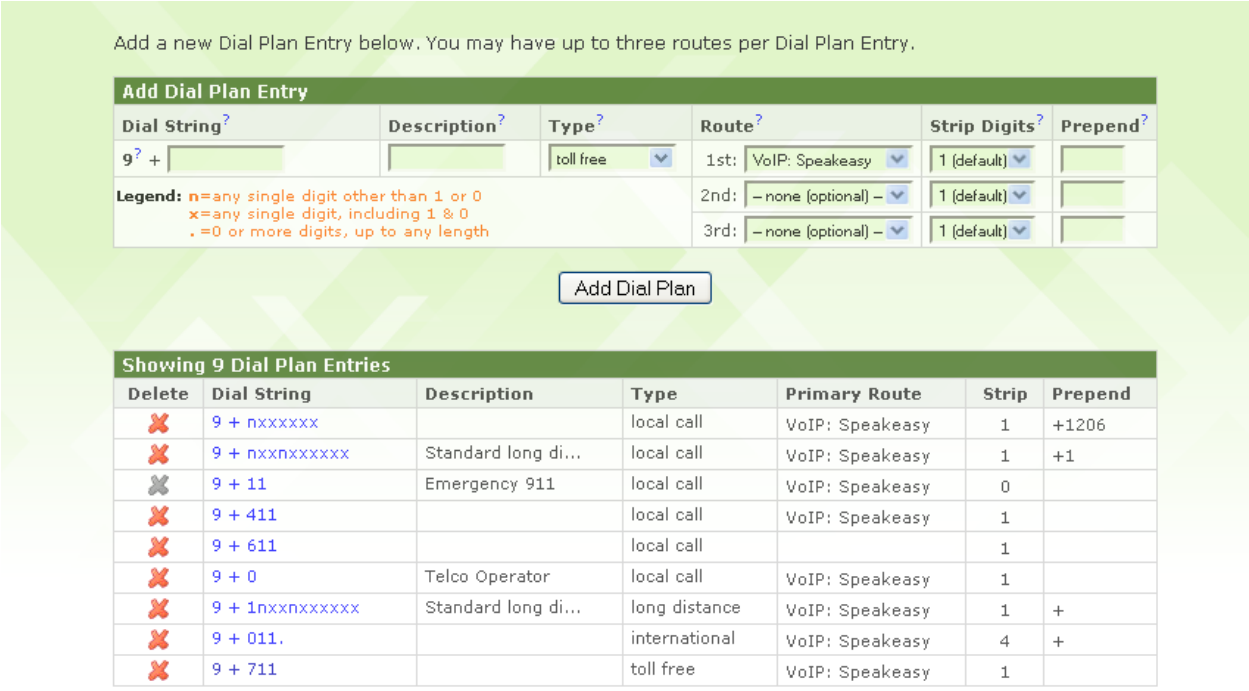
Inbound/Outbound routes need to be configured within Trixbox Pro to properly route calls.

Note – The information following is only an example of how these routes may be configured. Customer configurations may vary as customers may choose to have multiple SIP providers and configure different routes for each or possibly other routing configurations.

D.2. Dial Plan

Go to "**Options**" then to "**Dial Plan**"

The Dial Plan need to be modified by clicking the Modify button next to the route so that they send calls to the MEGAPATH VoIP provider defined in the previous section, and to send calls out with the appropriate E.164 formatting (+1NPANXXXXXX, or +CCXXXXXXXX for International calls).

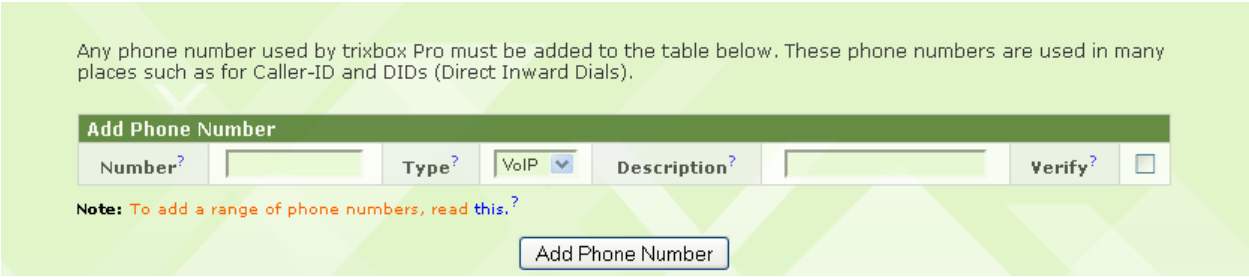


- Existing entries need to be modified to add a "+" in the "prepend" field.

Note – BY DEFAULT THERE IS NO OUTBOUND 911 ROUTE, PLEASE REMIND CUSTOMER TO SET THIS UP

D.3. Phone Numbers

Go To "Extensions" then go to "Phone Numbers"



- Add the DID to the "Number" field

Once Number is added it should be assigned as "Inbound Phone number" and "Outbound Caller ID" to an extension.

D.4. Known Issues

Blind Transfer's do not work with Asterisks based systems. This can be mitigated by using CLID override at the trunk group level.

D.5. Broadworks CPE Type

Trixbox Pro was tested using "Generic SIP PBX Single Registration" as the CPE device type within Broadworks.

D.6. Software Version

This was tested with Trixbox Pro version 2.0.1

Appendix E: Adtran NetVanta 7100

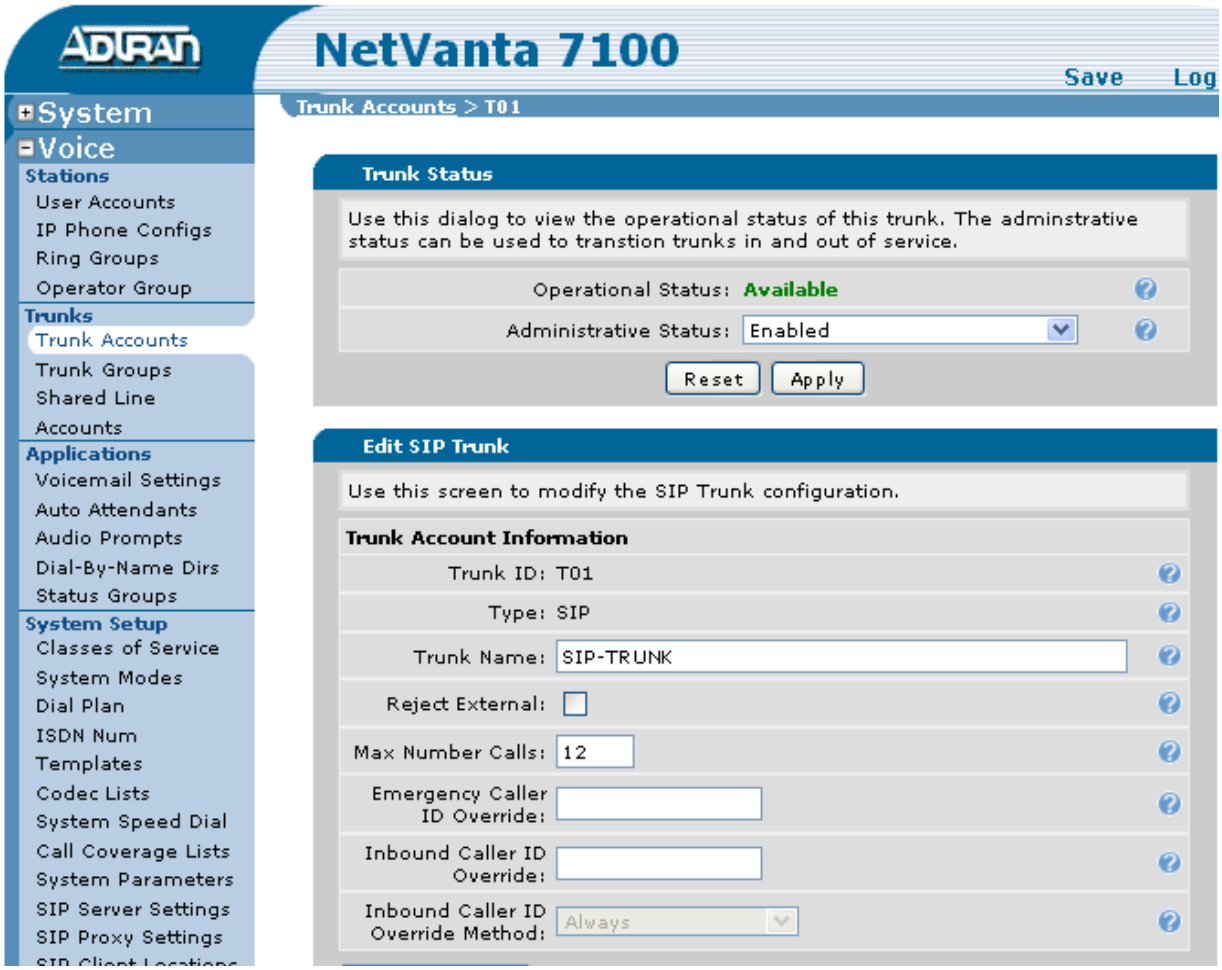
E.1. Trunk Accounts

Browse to the management IP address of the Netvanta 7100 via HTTPS.

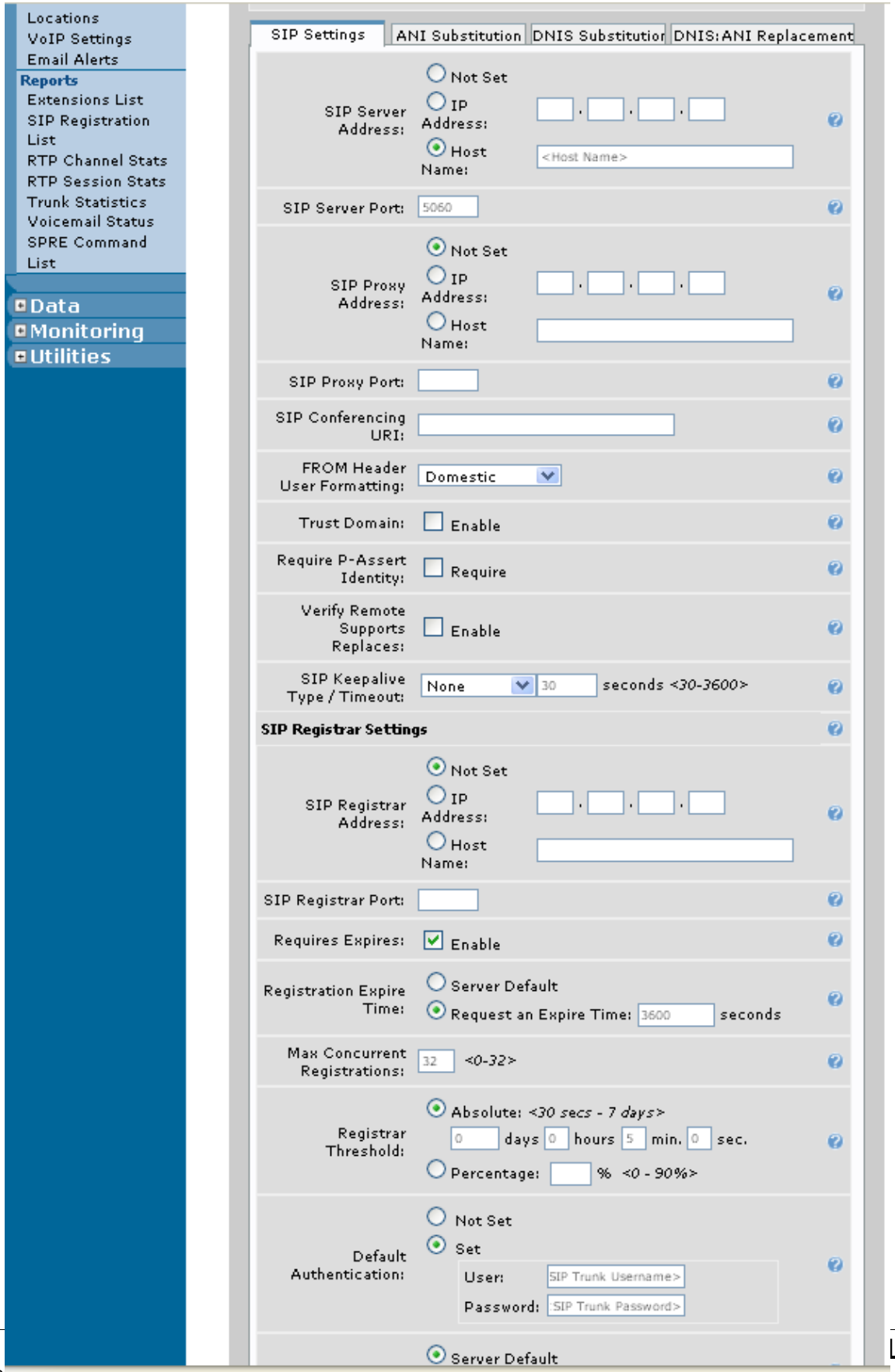
https://<management IP address>/admin

Navigate to “Voice” on the left hand column, then “Trunk Accounts”.

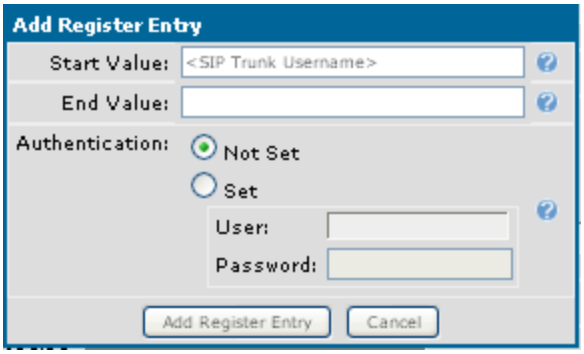
- Type in a name under “Trunk Name”.
- Under Type, choose “SIP”. Then click “Add”. This will bring you to the “Edit SIP Trunk” page



- Uncheck the option for “Reject External”
- Set “Max Number Calls” to the number of SIP trunks the customer has purchased


Locations
VoIP Settings
Email Alerts
Reports
Extensions List
SIP Registration List
RTP Channel Stats
RTP Session Stats
Trunk Statistics
Voicemail Status
SPRE Command List
Data
Monitoring
Utilities
SIP Settings
ANI Substitution
DNIS Substitution
DNIS:ANI Replacement
SIP Server Address:
Not Set
IP Address:
Host Name:
<Host Name>
SIP Server Port:
5060
SIP Proxy Address:
Not Set
IP Address:
Host Name:
SIP Proxy Port:
SIP Conferencing URI:
FROM Header User Formatting:
Domestic
Trust Domain:
Enable
Require P-Assert Identity:
Require
Verify Remote Supports Replaces:
Enable
SIP Keepalive Type / Timeout:
None
30
seconds <30-3600>
SIP Registrar Settings
SIP Registrar Address:
Not Set
IP Address:
Host Name:
SIP Registrar Port:
Requires Expires:
Enable
Registration Expire Time:
Server Default
Request an Expire Time:
3600
seconds
Max Concurrent Registrations:
32
<0-32>
Registrar Threshold:
Absolute: <30 secs - 7 days>
0 days 0 hours 5 min. 0 sec.
Percentage:
% <0 - 90%>
Default Authentication:
Not Set
Set
User:
SIP Trunk Username>
Password:
SIP Trunk Password>
Server Default

- Select the radio button under “SIP Server Address” to “Host Name” and specify the Moses provided Host name
  - If using an Edgemarc, select the radio button under “IP Address” and specify the LAN IP address of the Edgemarc.
- Set the “SIP Server Port” to “5060”
- Select the radio button for “Default Authentication” to “Set”
  - Specify the User using the SIP Trunk Username provided by Moses
  - Specify the Password using the SIP Trunk Password provided by Moses
- At the very bottom of this window, click on “Add Register Entry” – Not Shown
- This will bring up the “Add Register Entry” dialog box

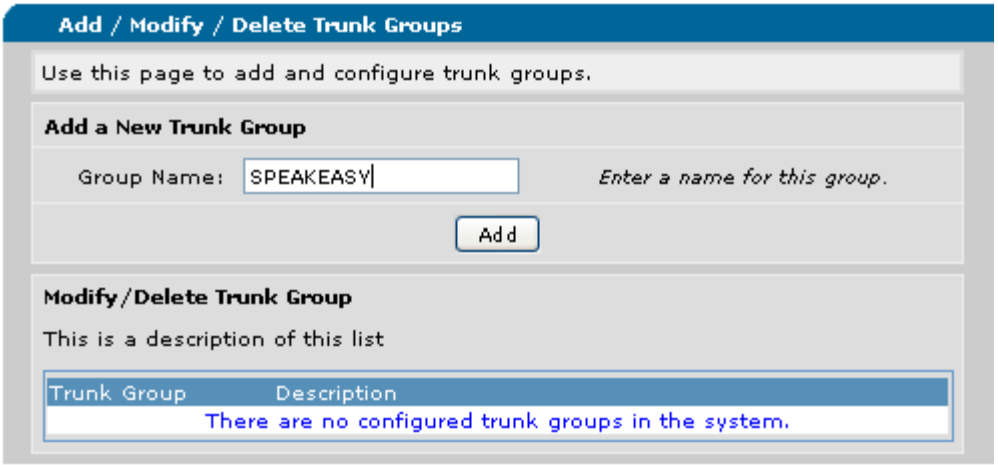


- For “Start Value”, enter the SIP Trunk Username provided by Moses
- Do not specify any End Value or Authentication settings.

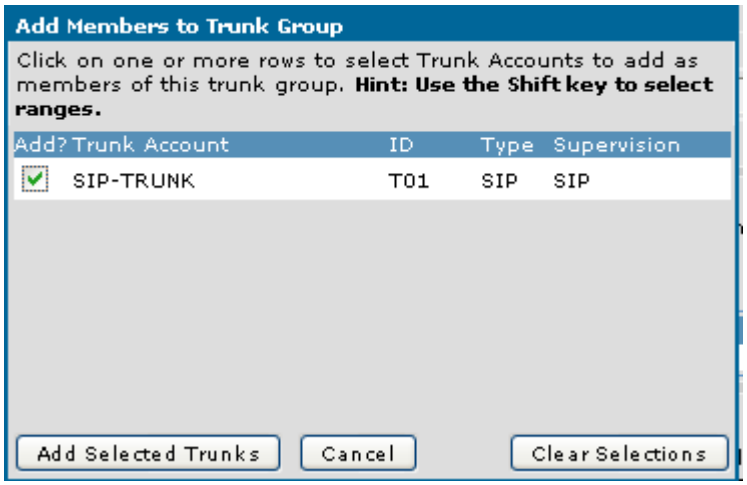
E.2. Trunk Groups

Navigate to “Voice” → “Trunk Groups” on the left hand column.

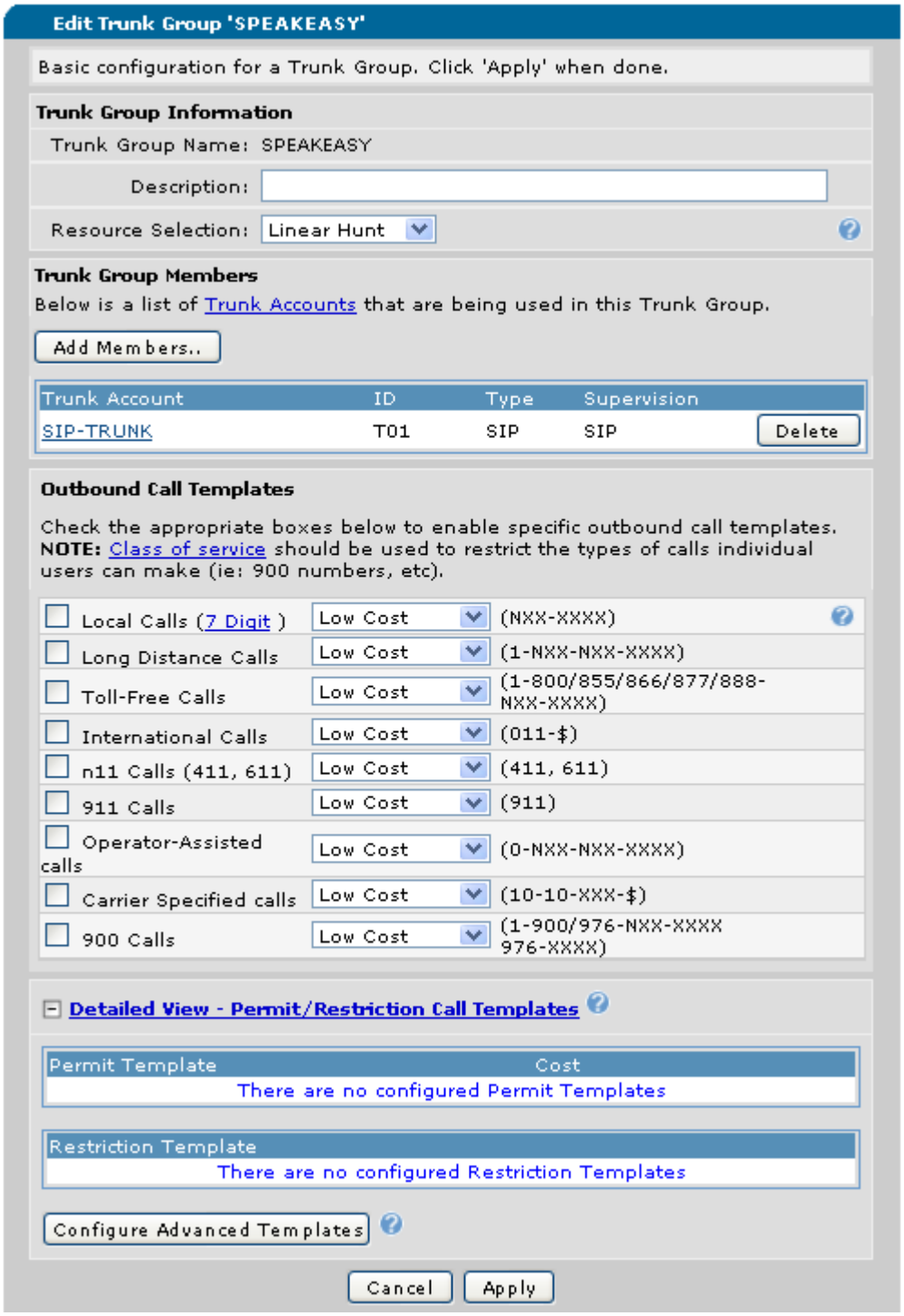
Type in a “Group Name” and click Add



Click on the "Add Members" button

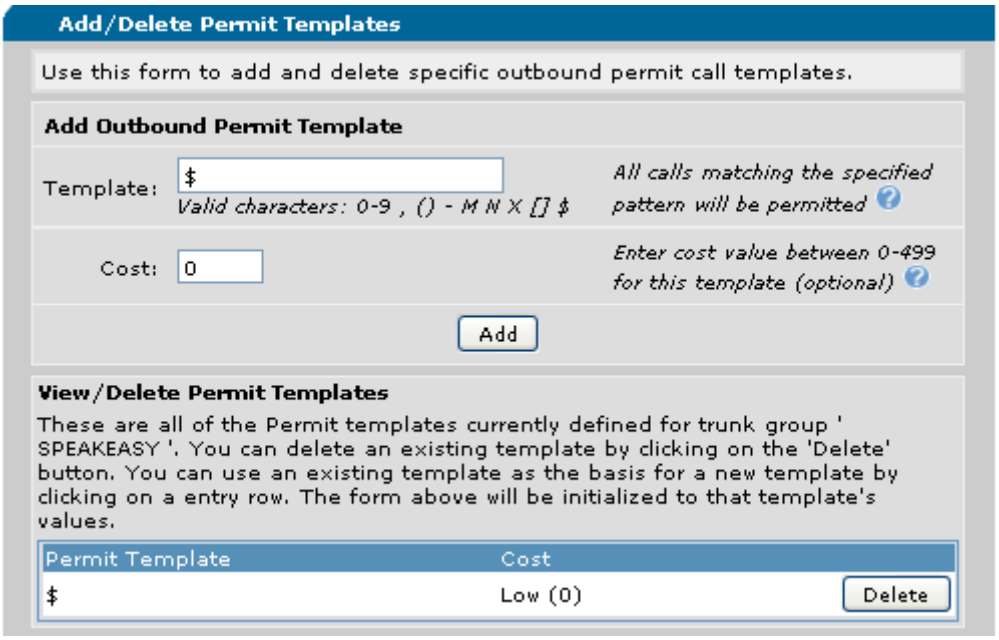


Check the box for the SIP Trunk you previously added. Then click on "Add Selected Trunks".



Verify that the selected Trunk Account is listed as a Trunk Group Member. Click on Apply at the bottom of the page.

Click on “Configure Advanced Templates”



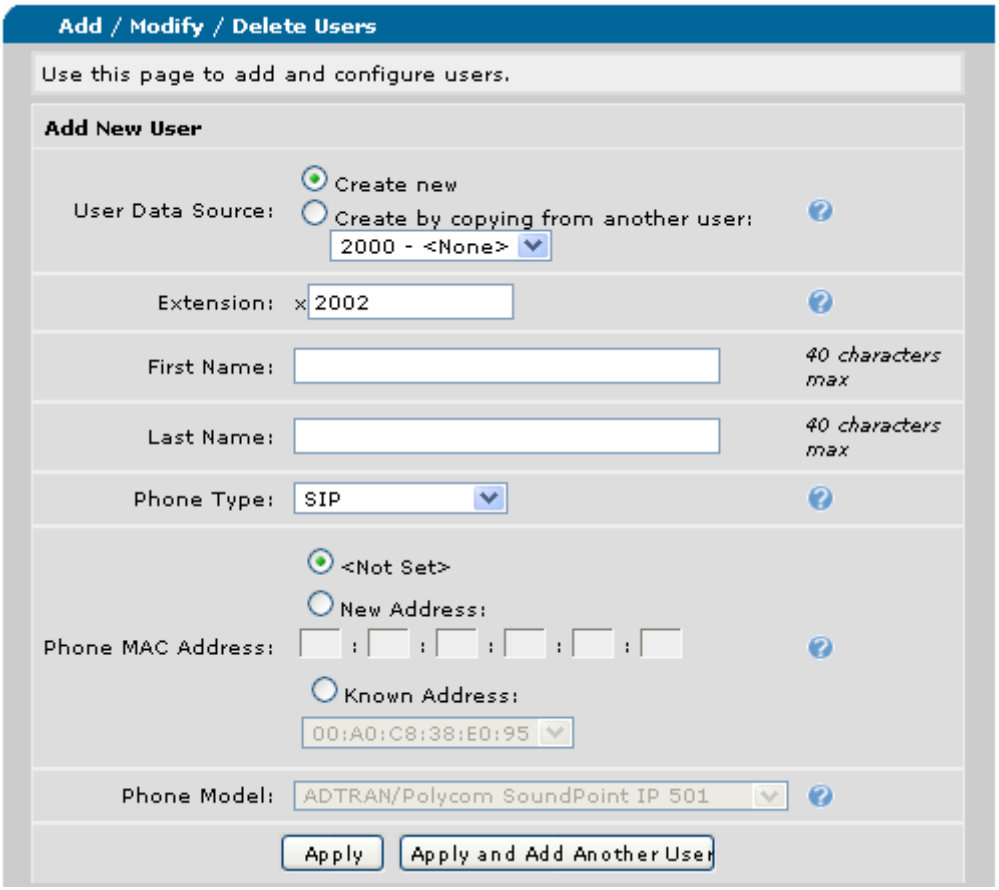
For “Outbound Permit Template”, specify “$” for Template variable and Cost “0”. Click “Add”. Verify Permit Template is listed under “View/Delete Permit Templates”.

E.3. User Accounts

User Accounts will need to be configured and would generally be assigned to a phone by MAC address. However, customers may have additional configurations.

Note The below information is only an example of how these user accounts may be configured. Customer configurations may vary.

User Accounts is accessed under “Voice” → “User Accounts” on the left hand column.



Create a new user and assign an extension to the user. Also specify the Phone MAC Address if this extension is to be assigned to a specific phone. Under "Phone Model", specify the device type.

E.4. Known Issues

Moses device type adds incorrect device. Choosing Adtran 7100 via Moses will assign a "Generic SIP PBX" device to the trunk group. This is known to cause inbound call routing failures.

E.4.1 Transfer to Auto Attendant

Setup

• Endpoint A's call coverage set to AA

Execution

• Endpoint B calls Endpoint A
• A is alerted
• B hears audible ringing
• A does not answer call
• B is sent to AA
• B dials valid extension and is transferred

Expected Results
• B hears AA prompt after transfer
• B can enter digits into AA and be transferred

Result of Test Case Execution: Fail

Observations: This fails because after the call is transferred to the AA, SDP from network does not include RFC 2833 parameters. 7100 does not handle this case gracefully in A2.02, causing the caller to not be able to enter digits into the AA. This bug will be fixed in A2.03.

E.4.2 Voicemail Notification

Setup
• Endpoint A's call coverage set to voicemail.

Execution
• Endpoint B calls Endpoint A
• A is alerted
• B hears audible ringing
• A does not answer
• B is sent to A's voicemail
• B leaves message
• A logs into voicemail and listens to message
• A deletes message

Expected Results
• A receives MWI after message is left
• MWI is cleared after message deleted

Result of Test Case Execution: Fail

Observations: This fails because after the call is transferred to VM, SDP from network does not include RFC 2833 parameters. 7100 does not handle this case gracefully in A2.02, causing the caller to not hear the beep from the VM to start the message. This bug will be fixed in A2.03.

E.5. Broadworks CPE Type

The Adtran Netvanta 7100 was tested using "Generic SIP PBX Single Registration" as the CPE device type within Broadworks.

E.6. Firmware

Testing for the Adtran Netvanta 7100 was done using Adtran's A2.02.00 firmware release.

Appendix F: Cisco Unified Communications 500 Series

The Cisco Unified Communications 500 Series is comprised of three primary models with numerous options and configurations available to each. Below is a high-level comparison of the Unified Communications 520, 540 and 560.

Note – Testing was limited to the Cisco Unified Communications 540 model

Model	 **Cisco UC 520**	 **Cisco UC 540**	 **Cisco UC 560**
Feature Highlights	• Eight to 64 IP phone station support • Four to 8 analog trunks or two to 4 BRI digital trunks • Optional single T1/E1 voice interface (PRI and CAS) • Integrated voicemail • 16 hours voicemail storage • Automated attendant • Integrated business productivity applications • Integrated security • Music on hold • Optional on board wireless access • Simple system configuration and management	• Eight to 32 phone station support • Four to 8 analog trunks or two to 4 BRI digital trunks • Optional single T1/E1 voice interface (PRI and CAS) • Integrated voicemail • 32 hours voicemail storage • Automated attendant • Integrated business productivity applications • Integrated security • Music on hold • On board wireless included • Simple system configuration and management	• 16 to 104 phone station support • Four to 12 analog trunks or two to 6 BRI digital trunks • Optional one or two T1/E1 voice interface (PRI and CAS) • Integrated voicemail • 32 or 64 hours voicemail storage • Automated attendant • Integrated business productivity applications • Integrated security • Music on hold • Wireless support with the Cisco AP 500 Series Wireless Access Point • Simple system configuration and management

F.1. Cisco Configuration Assistant Setup

To use the Cisco Configuration Assistant to create and save the initial software configuration, please follow the steps below:

1) If necessary, install Configuration Assistant on a PC to be used to manage the configuration of the UC 500. For information, see the Getting Started with Cisco Configuration Assistant document at http://www.cisco.com/go/configassist or on the CD-ROM that shipped with your product.

2) Launch Configuration Assistant. For information, see the Getting Started with Cisco Configuration Assistant document at http://www.cisco.com/go/configassist or on the CD-ROM that shipped with your product.

   a) Factory default username and password are cisco/cisco

3) Using an RJ-45-to-RJ-45 Ethernet cable, connect the Ethernet port of the PC on which the Cisco Configuration Assistant is installed to a PoE port on the front panel of the UC 500.

4) Use the Configuration Assistant to perform the following tasks. For more information, see online help.

   a) Connect to a New Community.

   b) Accept the default values to create the initial configuration.

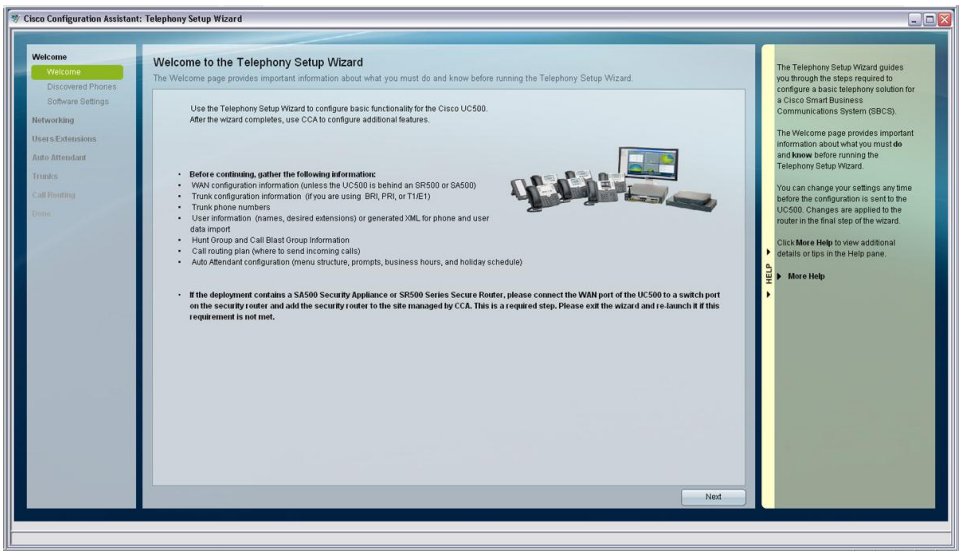
Note – If you are installing a single-site key system configuration, change the "Voice System Type" setting from PBX to Key System Configuration.

   c) Save the configuration

5) Confirm that the UC 500 appears in the Topology View.

F.2. Telephony Setup Wizard

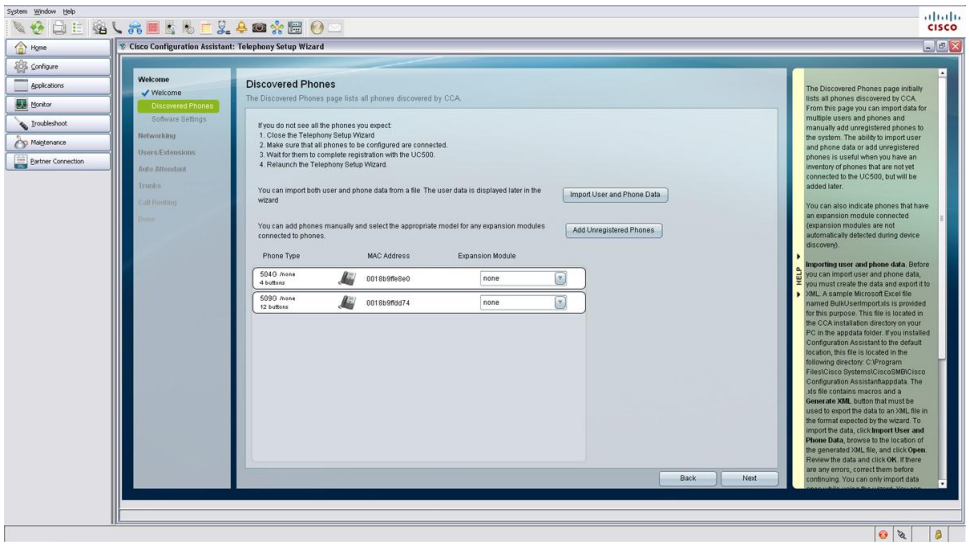
When running Cisco Configuration Assistant for the first time, the Telephony Setup Wizard will start automatically and guide you through configuring basic settings on the Cisco UC500



Welcome and Overview

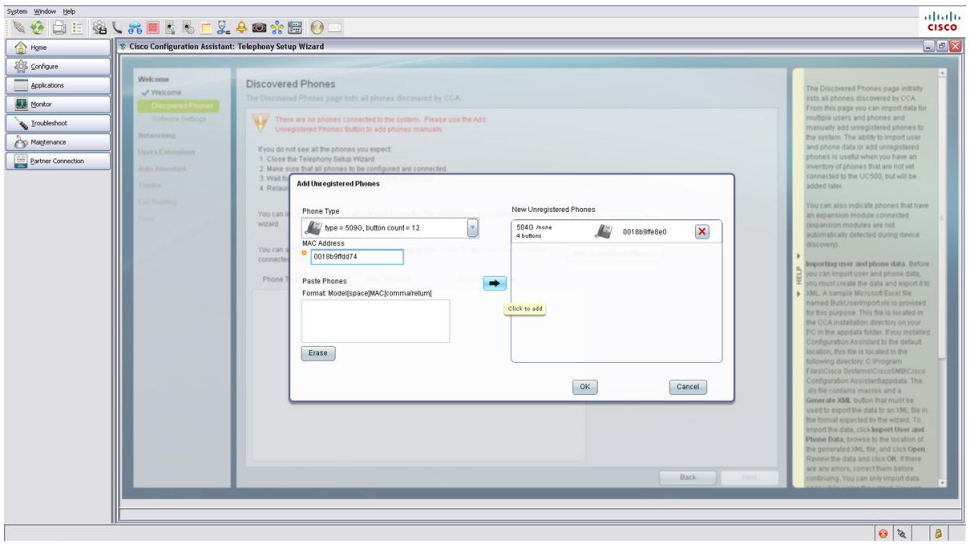
F.2.1 Welcome - Discovered Phones

If compatible phones are connected to the UC500 it will automatically discover and display them here.



Discovered/added phones

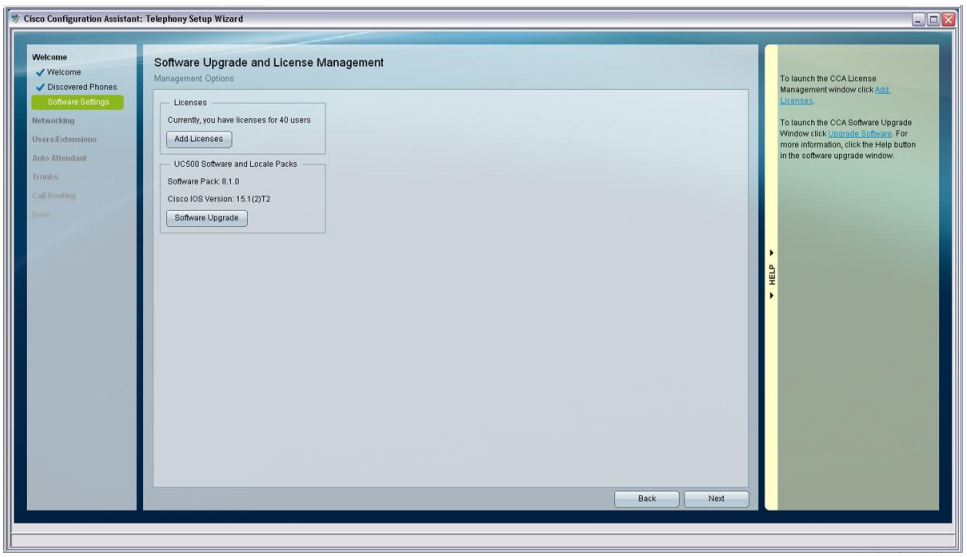
If no phones are connected or will be connected later, they may be added here for later use.



Adding phones

F.2.2 Welcome - Software Settings

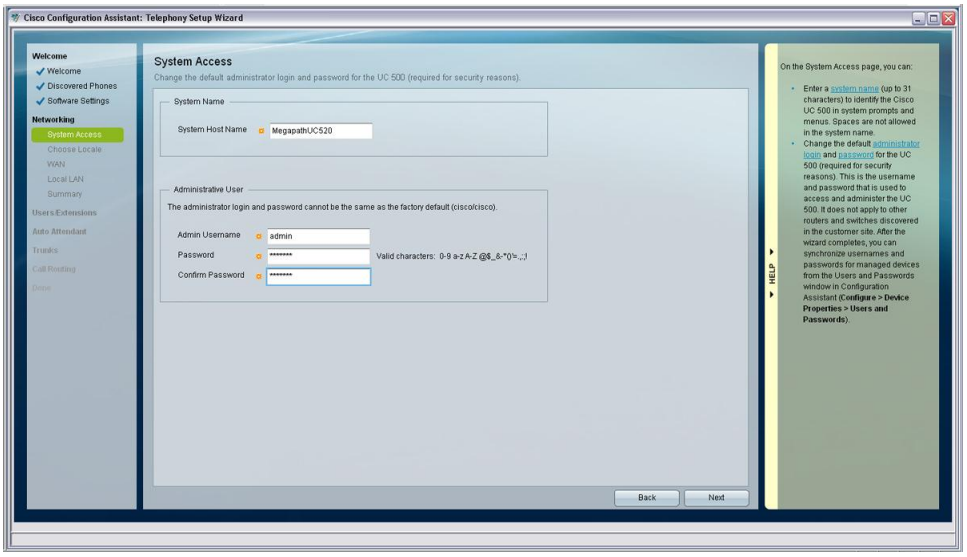
This screen displays licensing and software version information. Additional user licenses can be added and the system software version can be upgraded here.



Software Upgrade and License Management

F.2.3 Networking – System Access

Configure the UC500 system hostname and administrator access credentials on this screen.

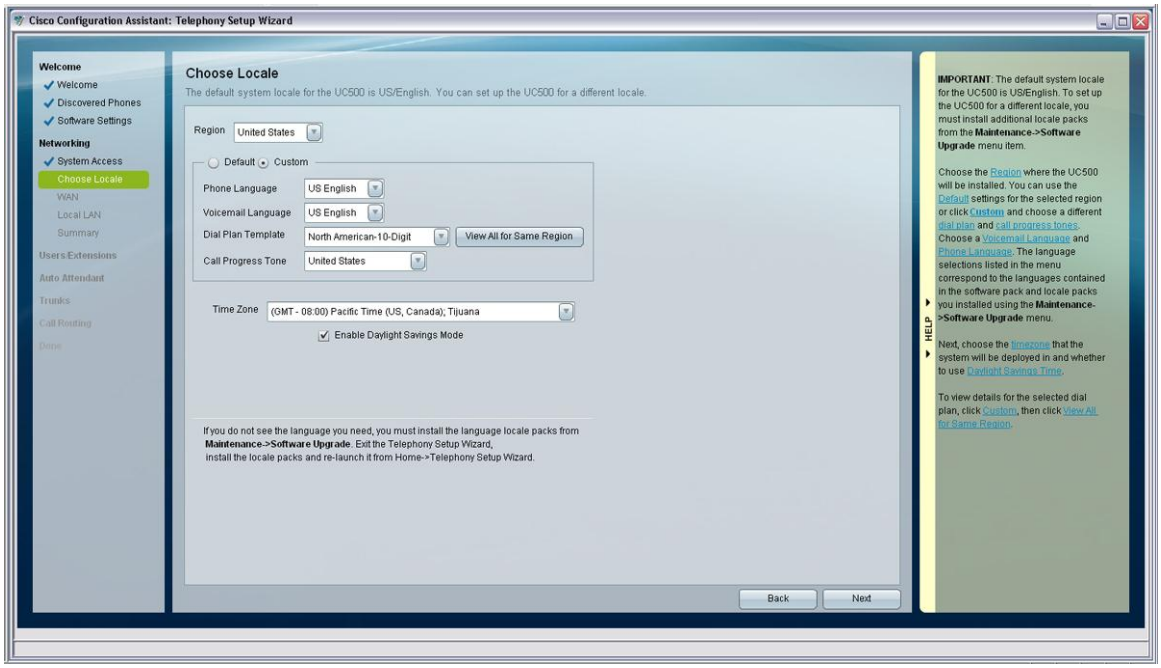


Configuring System Access settings

Note – Login credentials configured here apply to both Cisco Configuration Assistant and CLI access.

F.2.4 Networking – Choose Locale

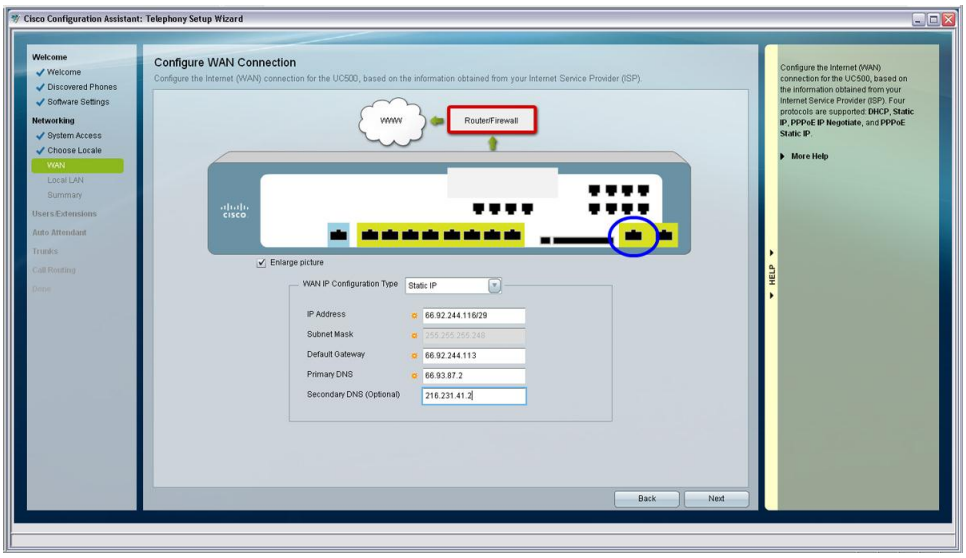
Select “Custom” and choose the “North American-10-Digit” dial plan template.



Choose Locale

F.2.5 Networking – WAN

Configure WAN Internet settings here, making sure to specify CIDR notation in the "IP Address" field which will automatically populate the "Subnet Mask" field.

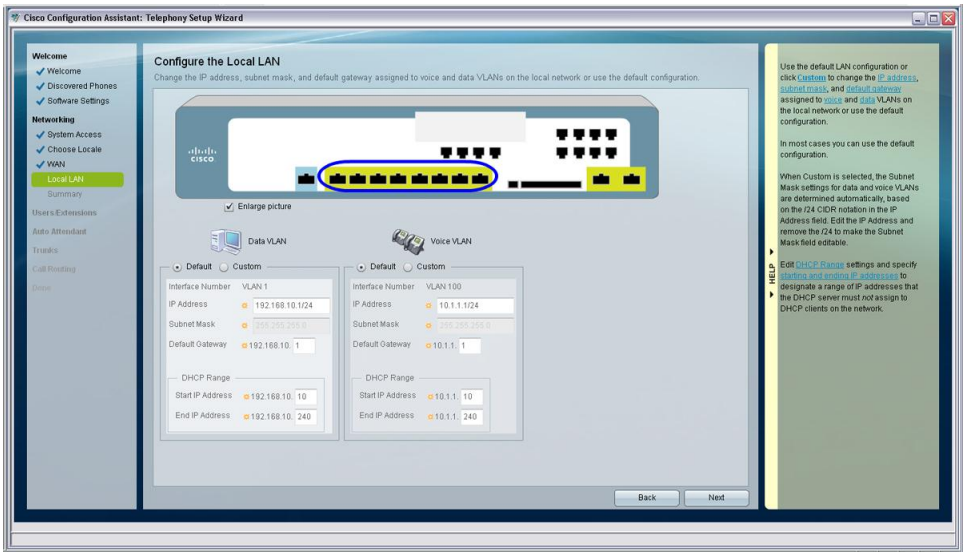


Configuring WAN settings

Note – Using a static IP address is highly recommended. No testing or verification of behavior using a DHCP assigned IP address was completed.

F.2.6 Networking – Local LAN

If needed, configure Local LAN settings here including voice and data VLANs. This step is optional and these settings will function with the default configuration.

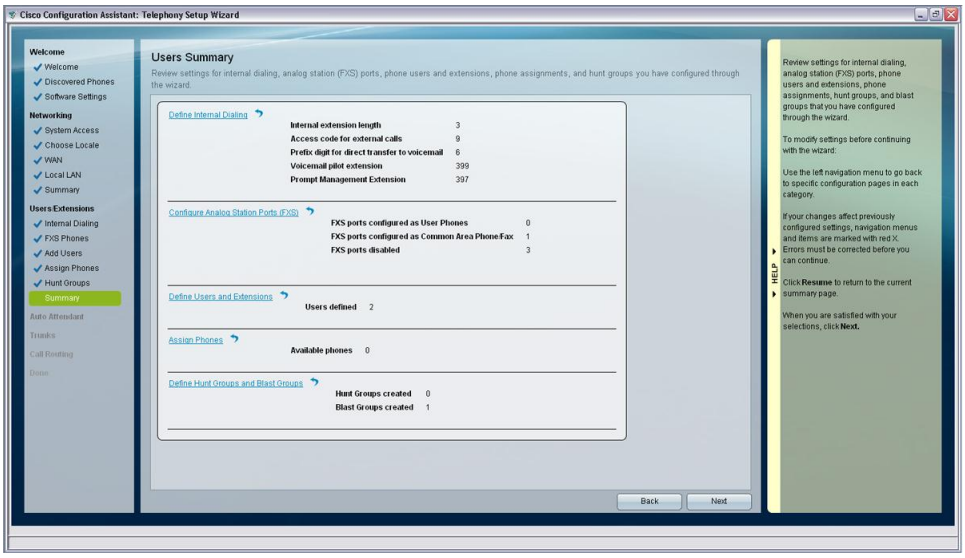


Configuring Local LAN settings

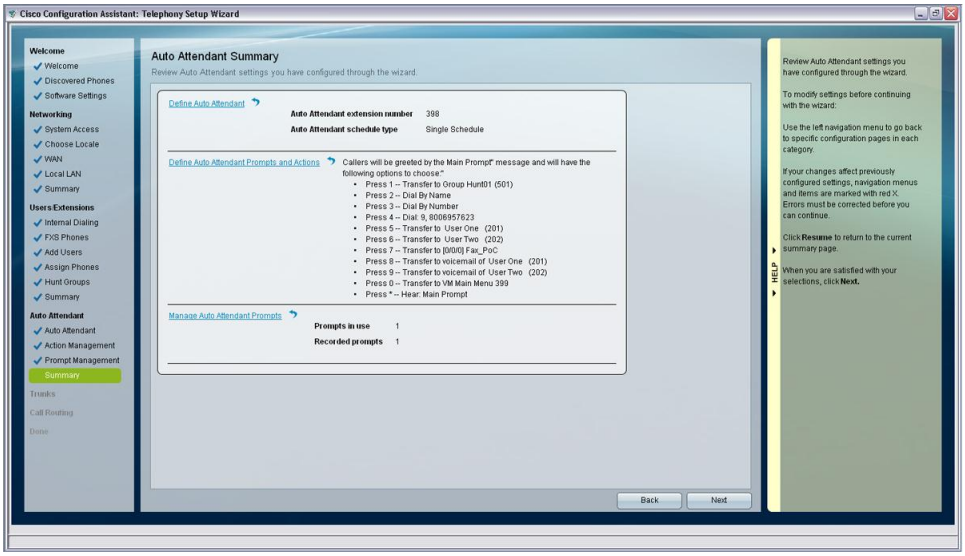
F.2.7 Users/Extensions and Auto Attendant

Options in this section are customer specific and configuration will not be covered. Navigate through this section to configure the following:

- Extension digit length
- Access Code for outside dialing
- Voicemail extension
- Create and configure an Auto Attendant, customize prompts and actions
- Configure FXS (analog) ports
- Create Users
    - Assign User extensions
    - Assign User phones
- Create and configure Hunt Groups



Users Setup Summary



Auto Attendant Setup Summary

F.2.8 Trunks – FXO Ports

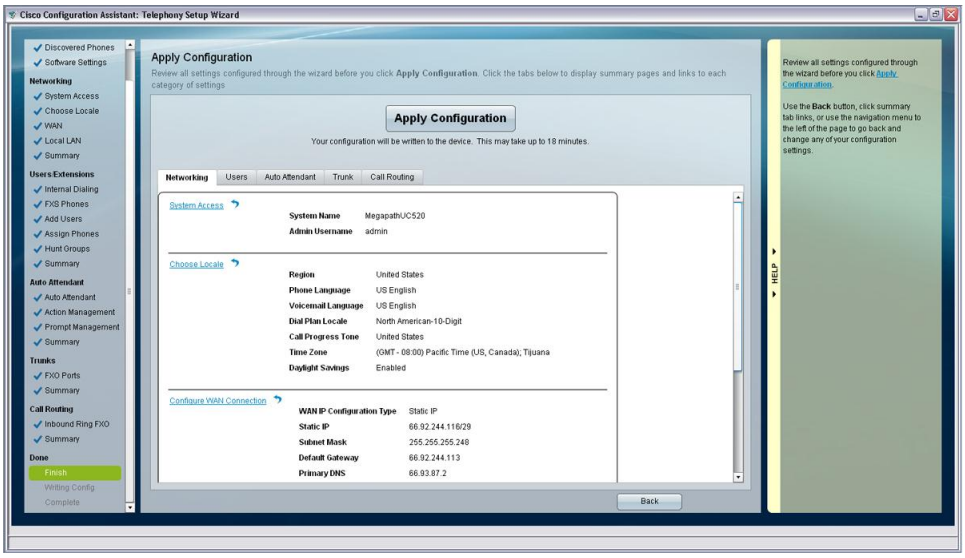
Configure FXO (analog) Trunk settings here. SIP Trunk settings are not included in the wizard and will be covered later in this document.

Note – At least one FXO port must remain active during setup or the error displayed below will be received. This port can be disabled once the configuration wizard is complete.

Error displayed when all FXO ports have been disabled

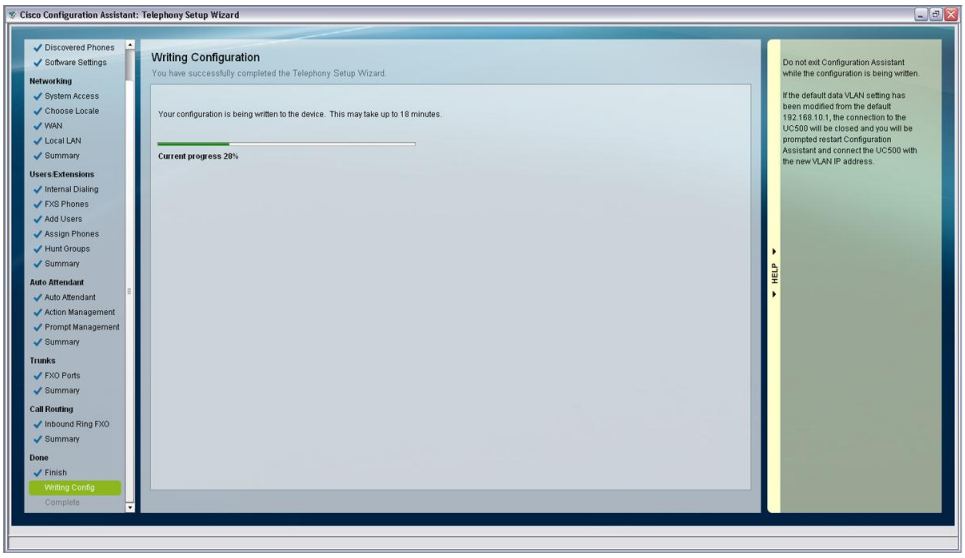
F.2.9 Done – Applying and Saving the Configuration

Now that the Telephony Setup Wizard is complete, click "Apply Configuration" to apply the settings to the running configuration.



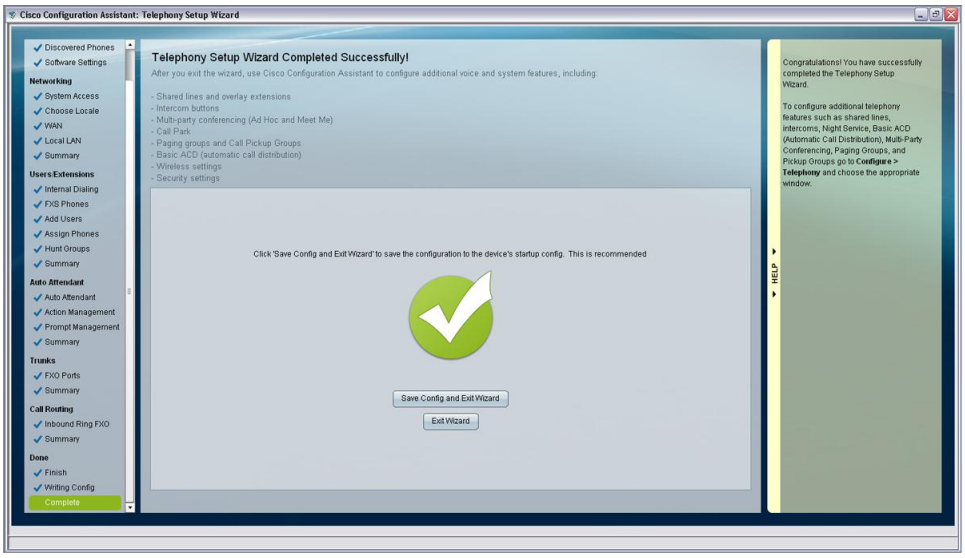
Wizard Summary – Apply Configuration

Writing the configuration can take some time, please allow it to complete and do not close Cisco Configuration Assistant while in process.



Writing settings to the running configuration

Telephony Setup Wizard is now complete! Click “Save Config and Exit Wizard” to save the running configuration to the startup configuration and exit the wizard.



Completed Telephony Setup Wizard

F.3. Additional Voice Configuration

To finish configuration for SIP Trunking on the UC 500 Series IP-PBX, additional settings must be entered outside of the Telephony Setup Wizard and SIP Trunk sections. **Please complete these steps prior to configuring the SIP Trunk.**

F.3.1 DNS Server and Domain Hostname

1. Navigate to Configure → Routing → IP Addresses

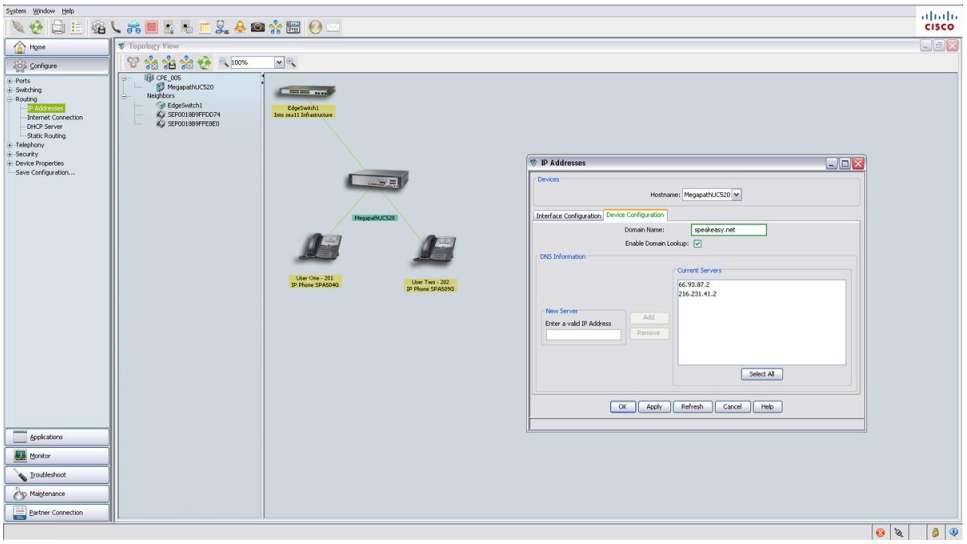
2. Select the "Device Configuration" tab

   a. Domain Name: speakeasy.net

   b. Enable Domain Lookup: Checked

   c. Current Servers: These should have been configured during Telephony Setup Wizard and the primary and secondary DNS server addresses should appear here. If not, enter DNS server IP information under New Server → Enter a valid IP Address then click "Add".

3. Click "OK" to save the settings



Adding DNS and Domain Hostname

F.3.2 QoS/Traffic Shaping

The Cisco Unified Communications 500 Series IP-PBX supports DSCP and will mark packets for prioritization if Traffic Shaping is configured and active. Once enabled, signaling (SIP) is marked with DSCP CS4 and media (RTP) is marked with DSCP CS5.

DSCP QoS is honored through Megapath's network. If Internet connectivity is provided by an off-net third party then Quality of Service cannot be guaranteed. Other providers may or may not honor DSCP packet marking and standard best practice is to strip the ToS byte at the provider's network edge.

Note – Traffic Shaping MUST be configured and active in order to activate DSCP marking and utilize QoS prioritization across Megapath's network.

To configure the Cisco UC 500 Series for DSCP marking, please follow the steps outlined below:

1. Navigate to Configure → Routing → Internet Connection

2. Under "WAN Interfaces", FastEthernet0/0 should be listed, select this interface and click "Modify"

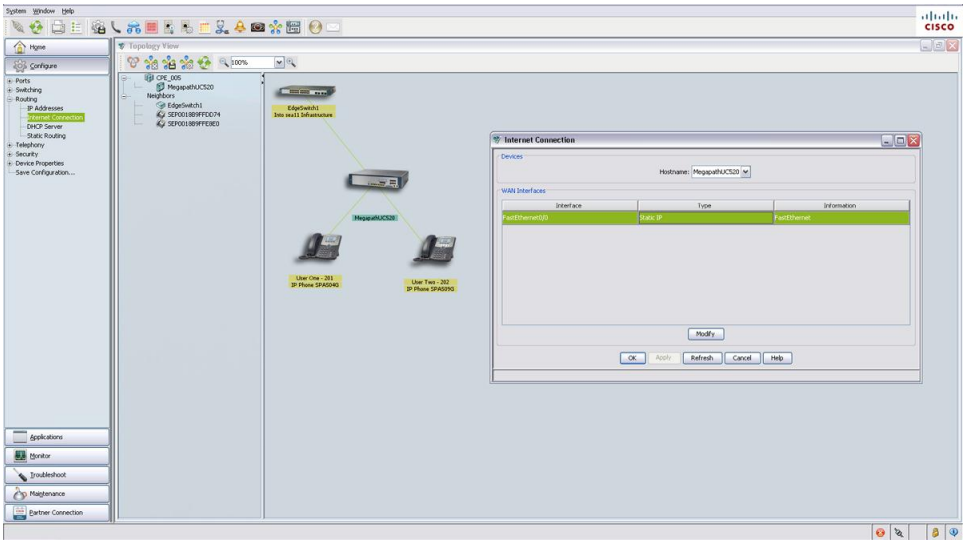
3. The "Modify Internet Connections" window should display, click the "Traffic Shaping" tab

   a. Traffic Shaping: Checked

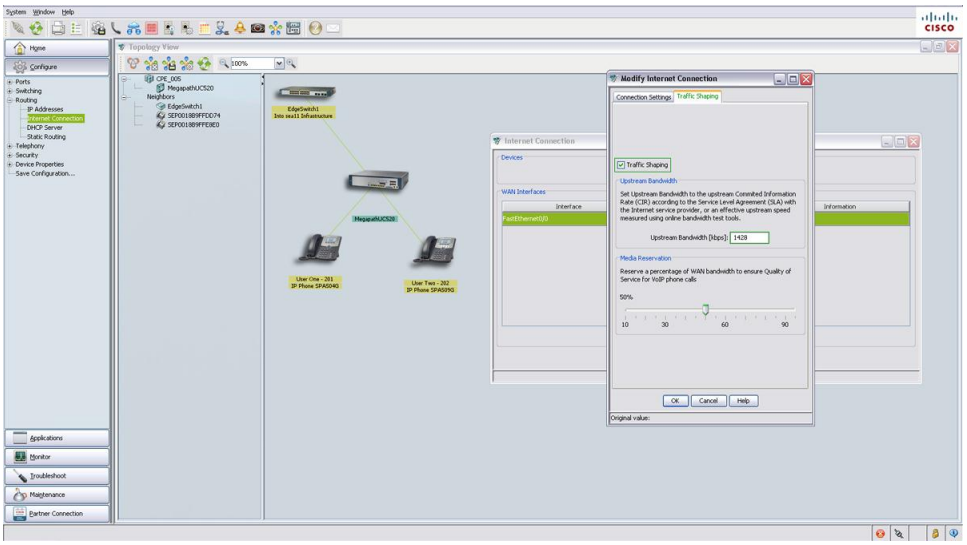
   b. Upstream Bandwidth [kbps]: Approximately 92% of actual upstream bandwidth as defined by speed tests. For example, a T1 circuit at 1536k would be set at 1428k to account for IP overhead.

   c. Media Reservation: Testing was completed with the default setting of 50% WAN bandwidth reservation however this may be adjusted as needed to meet customer requirements.

4. Click "OK" in the "Modify Internet Connection" window, then once more in the "Internet Connection" window to save the new settings.



Select and Modify WAN Interface



Setting and Activating Traffic Shaping/QoS

F.4. SIP Trunk Configuration

The Cisco Unified Communications 500 Series IP-PBX can be configured for different types LAN/WAN topologies and different methods of communicating with the SIP server. Testing was focused on the following:

1. Direct Internet connection on public IP (UC500 → Router → Internet)

    a. Using SRV record resolution for SIP Server address

    b. Using A record resolution for SIP Server address

2. SIP Proxy connection using NAT (UC500 → Edgemarc 4552 as SIP Proxy → Router → Internet)

Configuration and behavior varies between the different methods/topologies and is outlined when necessary in this guide.

F.4.1 Configure SIP Trunk

1. Navigate to Configure → Telephony → Ports and Trunks → SIP Trunk

2. Select the "Generic SIP Trunk Provider" template from the "Service Provider" dropdown menu which configures the following default settings:

    a. Voice Codec: G.711-ulaw only. Secondary codecs are not included in this template and must be configured using the CLI.

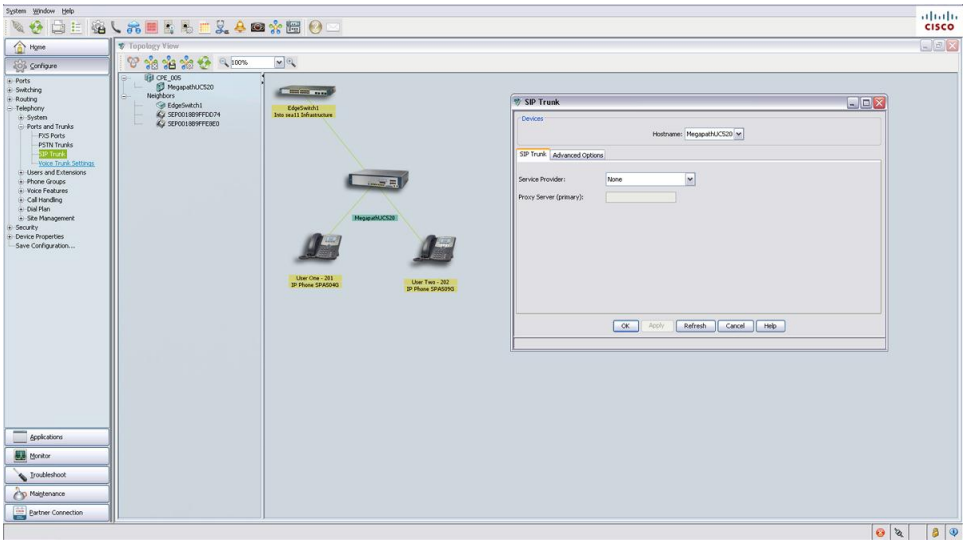
    b. Fax Codec: G.711

c. DTMF (dual-tone multi-frequency) payload: 101

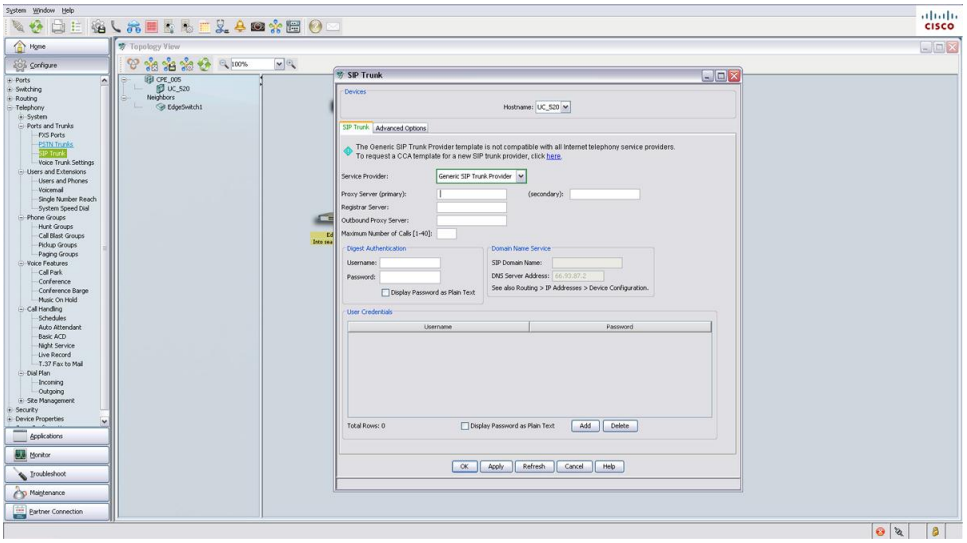
d. SIP Registration: Registers main number only. Additional DID registration is not included in this template and must be configured using the CLI.

e. SIP Registration Expiry Timer: Set at 3600 seconds. The Edgemarc 4552 SIP Proxy and Megapath SBCs reply with a reset expiry timer of 60 seconds in the 200 OK response to a successful registration so the UC500 will re-register every 60 seconds regardless of the configured timer value.

3. Configure as outlined below based on the solution in use at the customer site.



SIP Trunk Service Provider Selection



Generic SIP Trunk Provider Configuration

F.4.1.1 Direct Internet Connection – SRV Resolution

Using SRV records as the SIP server/registrar allows for redundancy in the case that the primary server is not reachable. This is the recommended configuration, however if A record resolution is preferred or required please refer to the next section titled "Direct Internet Connection – A Record Resolution" for configuration instructions.

The UC 500 Series is configured by default to attempt and resolve the SIP server address as both A and SRV records, input the SRV address as follows:

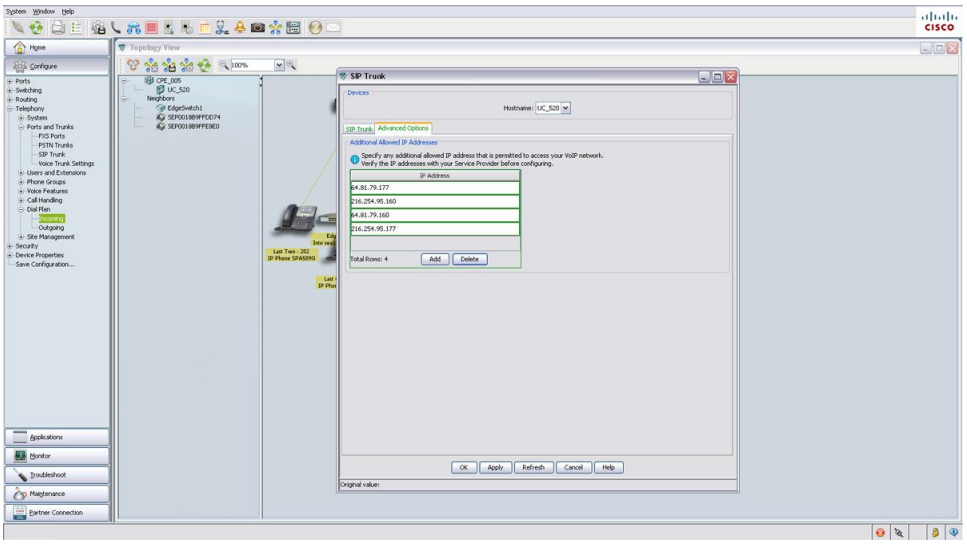
1. Proxy Server (primary): <st>1-siptrunk-srv.voice.speakeasy.net (replace <st> with the state abbreviation of the customer site, for example Washington state would be wa1-siptrunk-srv.voice.speakeasy.net)
2. (secondary): Leave blank
3. Registrar Server: <st>1-siptrunk-srv.voice.speakeasy.net
4. Outbound Proxy Server: <st>1-siptrunk-srv.voice.speakeasy.net
5. Maximum Number of Calls: The number of SIP Trunks assigned to the customer
6. Digest Authentication
    a. Username: provisioned trunk group username
    b. Password: provisioned trunk group password
7. Domain Name Service
    a. SIP Domain Name: speakeasy.net (input this if blank)
    b. DNS Service Address: Primary DNS server address (input this if blank)
8. User Credentials: Leave blank, this is only used if each DID requires a unique username and password to authenticate.

Due to the way that SRV resolves, the Cisco UC500 needs to be explicitly configured to allow the SBC IP addresses. The following step should only apply when using SRV. If skipped, registrations will fail as the UC500 will not recognize the server as authorized and therefore will not respond.

9. Within the SIP Trunk window, click the "Advanced Options" tab. Click "Add" and input each of the following addresses:
    a. 64.81.79.177
    b. 216.254.95.160
    c. 64.81.79.160

d. 216.254.95.177

Note – These IP addresses may change at any time without prior notice!



Allowing SBC IP Addresses

10. Click “OK” to apply settings

11. A “User Confirmation” window will display, enter the following information:

    a. SIP Trunk → Add Generic SIP Trunk Provider as a SIP Trunk options to Outgoing Numbers in the Dial Plan?: Checked

    b. Caller ID → Company Main Number: Enter primary DID, this will be used as the primary register number as well as for outbound CLID

    c. Click “OK”

Outbound SIP Trunk and CLID/Main Number Configuration

12. Due to the use of SRV DNS, the UC 500 produces an error that the SIP server is not reachable although registration has likely succeeded. This error may appear one or more times, ignore it and click “OK” to continue.

Invalid SIP Server Reachability Error

13. SIP Trunk configuration using SRV is now complete. Please continue to configuring Dial Plans.

F.4.1.2 Direct Internet Connection – A Record Resolution

Configuring a SIP Trunk to use A records instead of SRV is much simpler, however there is no redundancy since the record points to a single IP address. If there is a failover scenario where the SIP server is no longer reachable then registration will be lost and no calls will complete over the SIP Trunk.

1. Proxy Server (primary): Hostname provided by Moses

   a. <st>1-siptrunk-a.voice.speakeasy.net (replace <st> with the state abbreviation of the customer site, for example Washington state would be wa1-siptrunk-a.voice.speakeasy.net). Note that this may change so it’s strongly encouraged to use the Moses provided information.

2. (secondary): Leave blank

3. Registrar Server: Hostname provided by Moses, same as Proxy Server (primary)
4. Outbound Proxy Server: Hostname provided by Moses, same as Proxy Server (primary)
5. Maximum Number of Calls: The number of SIP Trunks assigned to the customer
6. Digest Authentication
    a. Username: provisioned trunk group username
    b. Password: provisioned trunk group password
7. Domain Name Service
    a. SIP Domain Name: speakeasy.net (input this if blank)
    b. DNS Service Address: Primary DNS server address (input this if blank)
8. User Credentials: Leave blank, this is only used if each DID requires a unique username and password to authenticate.
9. The Cisco UC 500 Series should resolve the SIP server hostname and automatically add it to the firewall as an allowed source. If this is not the case, please refer to step 9 under "Direct Internet Connection – SRV Resolution" to configure additional allowed IP addresses.
10. Click "OK" to apply settings
11. A "User Confirmation" window will display, enter the following information:
    a. SIP Trunk → Add Generic SIP Trunk Provider as a SIP Trunk options to Outgoing Numbers in the Dial Plan?: Checked
    b. Caller ID → Company Main Number: Enter primary DID, this will be used as the primary register number as well as for outbound CLID
    c. Click "OK"

Outbound SIP Trunk and CLID/Main Number Configuration

12. SIP Trunk configuration using A records is now complete. Please continue to configuring Dial Plans.

F.4.1.3 Edgemarc 4552 as SIP Proxy

The Edgewater Edgemarc 4552 ALG has been certified for use as a SIP Proxy for IP-PBX SIP Trunk solutions. The UC 500 Series will register to the LAN interface of the Edgemarc which then proxies registrations to the SIP servers. In this case, the Edgemarc can be configured with the SRV SIP server addresses which would provide redundancy in a failover scenario. For additional information on Edgemarc 4552 configuration, please see the Edgemarc 4552 Certification Guide.

1. Proxy Server (primary): LAN IP of SIP Proxy (Edgemarc 4552)
2. (secondary): Leave blank
3. Registrar Server: LAN IP of SIP Proxy (Edgemarc 4552)
4. Outbound Proxy Server: LAN IP of SIP Proxy (Edgemarc 4552)
5. Maximum Number of Calls: The number of SIP Trunks assigned to the customer
6. Digest Authentication
    a. Username: provisioned trunk group username
    b. Password: provisioned trunk group password
7. Domain Name Service
    a. SIP Domain Name: speakeasy.net (input this if blank)

b. DNS Service Address: Primary DNS server address (input this if blank)

8. User Credentials: Leave blank, this is only used if each DID requires a unique username and password to authenticate.

9. Click “OK” to apply settings

10. A “User Confirmation” window will display, enter the following information:

    a. SIP Trunk → Add Generic SIP Trunk Provider as a SIP Trunk options to Outgoing Numbers in the Dial Plan?: Checked

    b. Caller ID → Company Main Number: Enter primary DID, this will be used as the primary register number as well as for outbound CLID

    c. Click “OK”

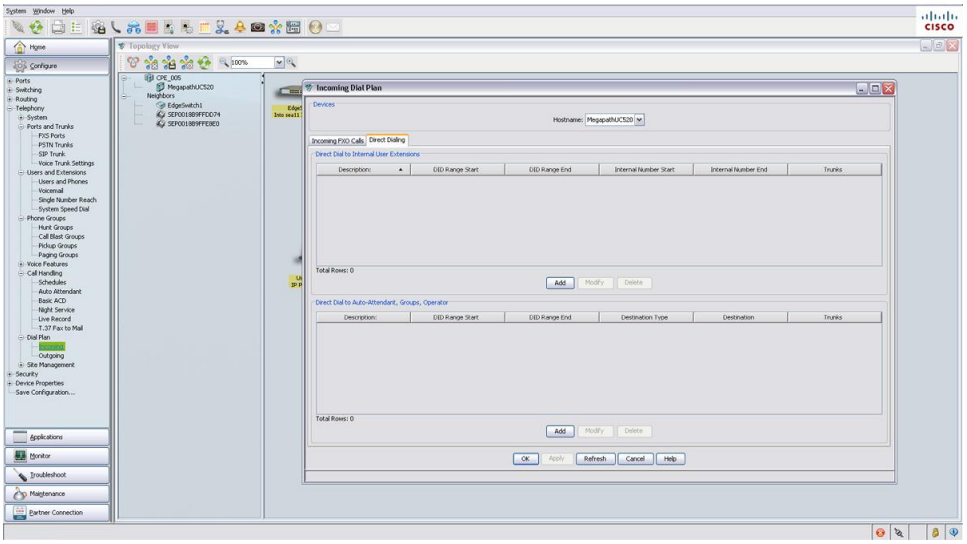
Outbound SIP Trunk and CLID/Main Number Configuration

11. SIP Trunk configuration using the Edgemarc 4552 as SIP Proxy is now complete. Please continue to configuring Dial Plans.

F.5. Dial Plans

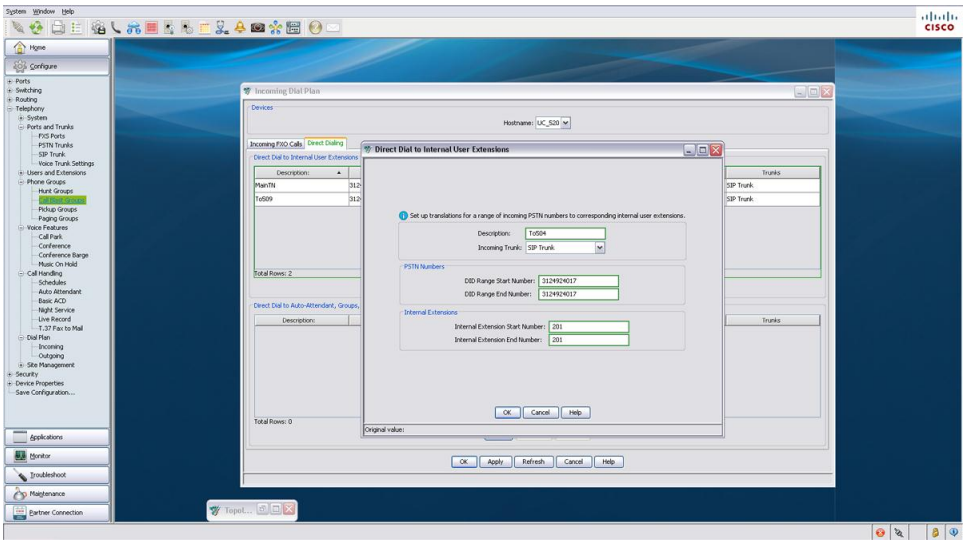
Note – By default, the UC 500 Series will only register a single DID which is used as the main number and for CLID for the site. Additional DIDs can be configured to register via the CLI, please refer to Cisco documentation for further information.

F.5.1 Incoming Dial Plan



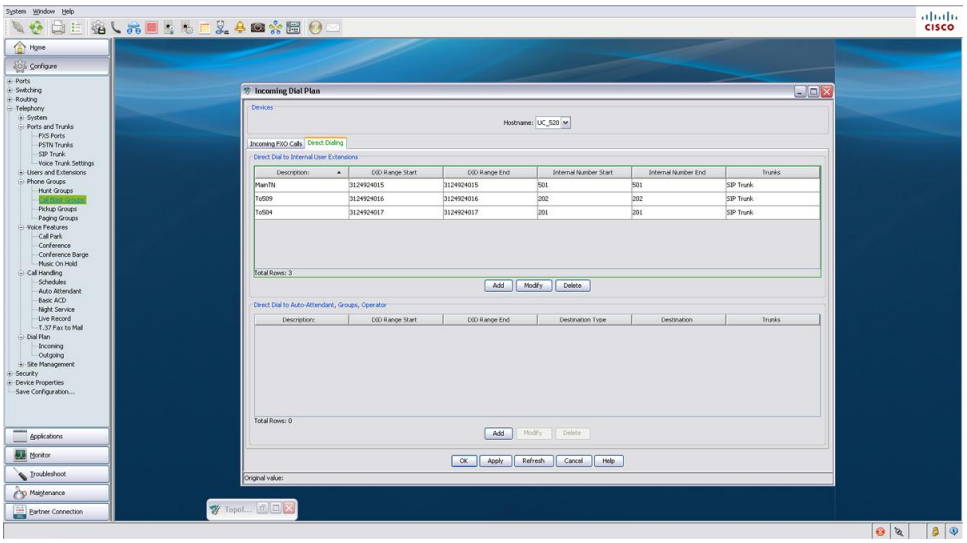
Unconfigured Incoming Dial Plan

1. Navigate to Configure → Telephony → Dial Plan → Incoming Dial Plan
2. Select the "Direct Dialing" tab
3. Select if calls should route directly to a user or to a service such as Auto Attendant, click "Add" in the chosen section.
4. Input the following:
   a. Description: Description of the Direct Dial route
   b. Incoming Trunk: SIP Trunk
   c. PSTN Numbers
      i. DID Range Start Number: Main DID
      ii. DID Range End Number: Main DID
   d. Internal Extensions
      i. Internal Extension Start Number: Internal extension to route the DID to
      ii. Internal Extension End Number: Internal extension to route the DID to
5. Click "OK" to add the incoming Direct Dial



Add Incoming Direct Dial

6. Once all incoming Dial Plans have been added, click “OK” on the “Incoming Dial Plan” window to apply the changes.



Incoming Dial Plan with Multiple DIDs

F.5.2 Outgoing Dial Plan

The default Outgoing Dial Plan should require no changes for basic functionality as long as “North American-10-Digit” was selected during the Telephony Setup Wizard. To verify configuration or add outbound Dial Plan rules, please follow the steps below.

1. Navigate to Configure → Telephony → Dial Plan → Outgoing

2. Select the “Outgoing Call Handling” tab

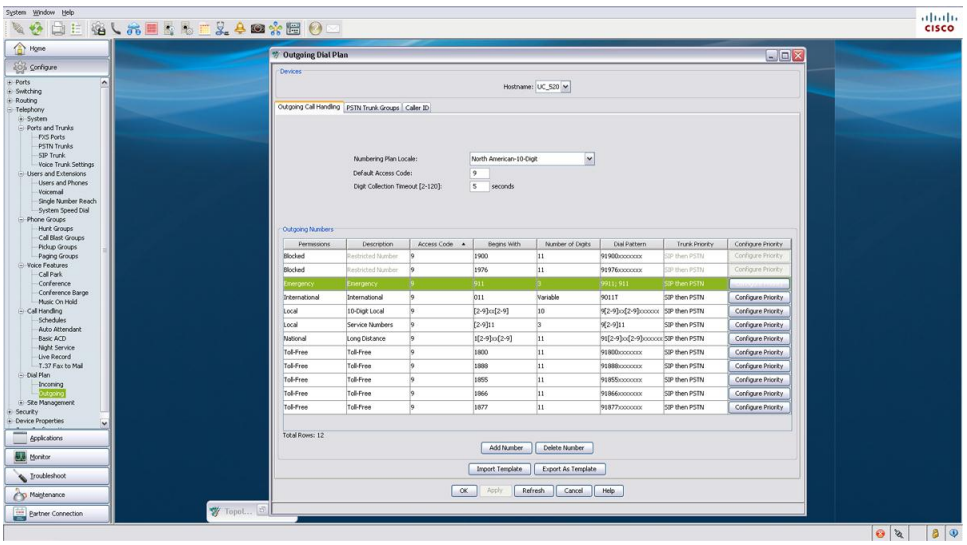
   a. Verify that “Numbering Plan Locale” is set to “North American-10-Digit

   b. Verify that a Default Access Code is configured (default is 9)

   c. Verify that a Digit Collection Timeout is set (default 5)

3. Verify that all routes have “Trunk Priority” set as SIP then PSTN or SIP Only. If they do not then please configure each so the SIP Trunk is the priority route.

4. Click “OK” to apply any changes



Default Outgoing Dial Plan

F.6. Completion

Navigate to Configure → Save Configuration to apply all changes

F.7. Broadworks CPE Type

The Cisco Unified Communications 500 Series was tested using **Cisco UC500** as the CPE device type within Broadworks

F.8. Software/Hardware Versions Tested

- The specific model tested was a Cisco UC520
- Cisco Configuration Assistant: v3.0
- Cisco Software Pack: v8.1.0

- Cisco IOS: (UC500-ADVIPSERVICESK9-M), v15.1(2)T2
- System Bootstrap ROM: v12.4(11r)XW3

F.9. Additional Information

Although CLI configuration is not outlined in this document or supported, the following items were tested successfully:

1. G.711ulaw Codec Only
2. G.729a Codec Only
3. G.711ulaw as first priority with G.729a as second priority
4. G.729a as first priority with G.711ulaw as second priority
5. With Traffic Shaping applied, SIP and RTP packets are correctly marked as configured.
6. During configuration change testing, the SBC IPs were removed from the allowed list which caused the UC 500 to lose registration. During this time, SRV records were configured and successful failover/failback behavior was witnessed. Since neither IP was allowed, registration was not successful until added back into the firewall however the UC 500 acted correctly which verifies the validity of SRV registration.

Appendix G: Samsung OfficeServ 7200

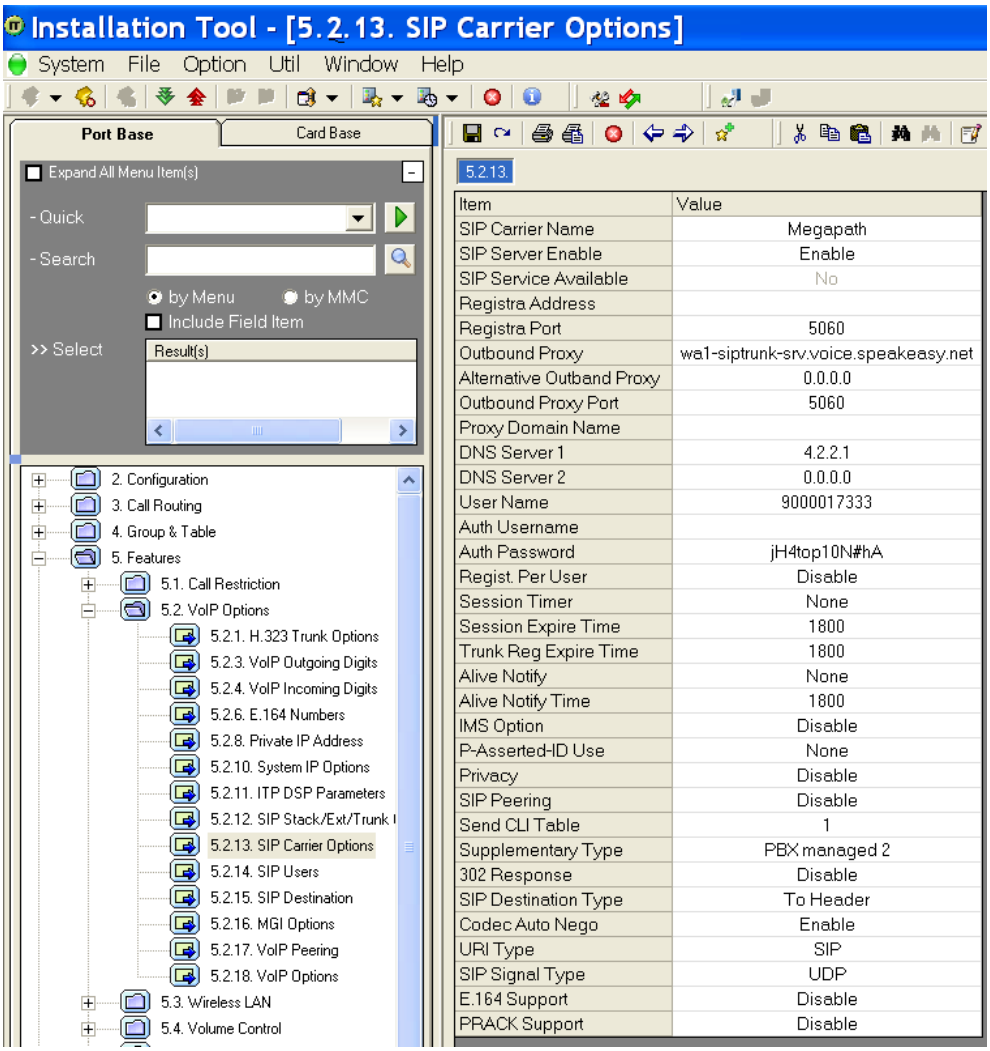
G.1. Overview of OfficeServ 7200 deployments

Samsung OfficeServ 7200 installations will be deployed using a Samsung iBG1000 router only. IP-PBX (OfficeServ 7200) connects to the iBG1000 directly via Ethernet. Below configuration of this IP-PBX is done using the Samsung OfficeServ Installation Tool utility.

Note – Using this IP-PBX behind an Edgemarc ALG is not a supported configuration.

G.2. 5.2.13 SIP Carrier Options

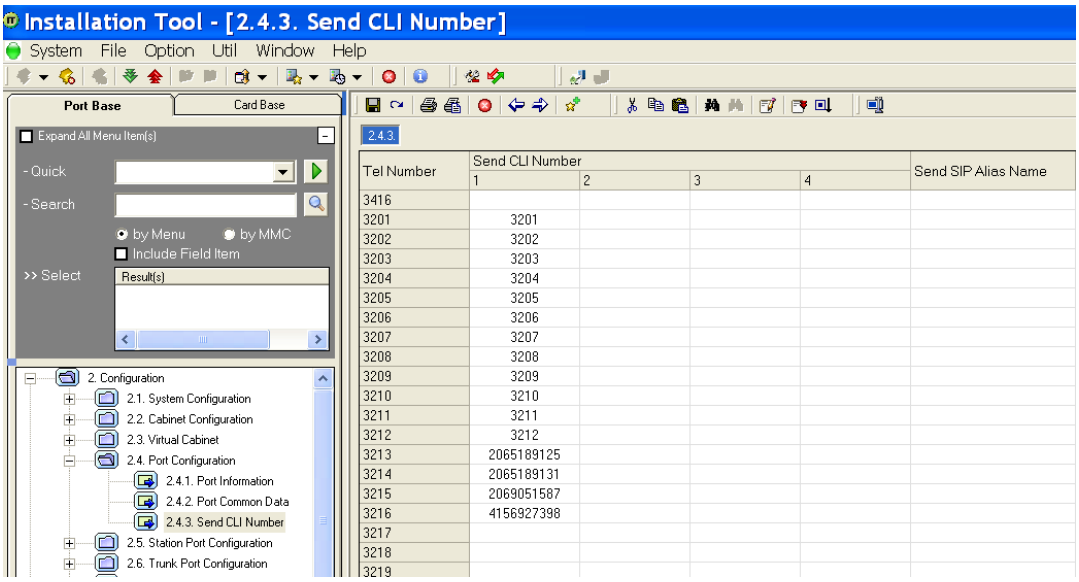
Configure the SIP Carrier Options within the Samsung Installation Tool utility



- Set "SIP Carrier Name" to Megapath
- Set “SIP Server Enable” to “Enable”
- Set Registra Port to 5060
- Set "Outbound Proxy” to Host address from Moses
- Set “Outbound Proxy Port” to 5060
- Set “DNS Server 1” and “DNS Server 2” to service provider’s DNS servers
- Set "User Name” to SIP Trunk Username from Moses
- Set "Auth Password” to SIP Trunk password from Moses
- Set "SIP Destination Type” to “To Header”
- Set "URI Type” to “SIP”
- Set "SIP Signal Type” to “UDP”

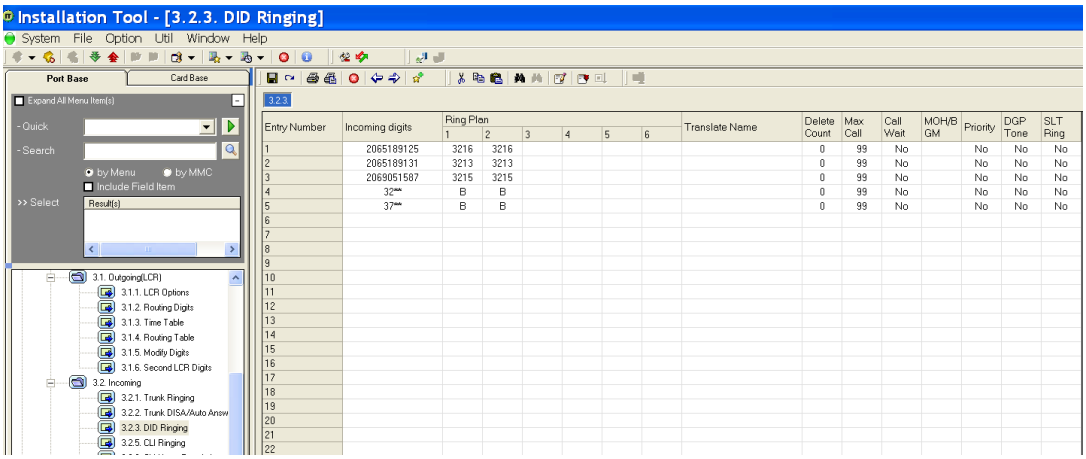
G.3. Send CLI Number

Configure Send CLI Number options within the Samsung Installation Tool utility.



G.4. DID Ringing

Configure DID Ringing options within the Samsung Installation Tool utility.



G.5. Broadworks CPE Type

Samsung OfficeServ 7200 was tested using **Generic SIP PBX Single Registration** as the CPE device type within Broadworks.

G.6. Tested Software Versions

This was tested with Samsung OfficeServ system version 11.03.18 V4.53c