USER GUIDE

Asterisk
Technical Application Notes
08/20/15

Contents:

ABOUT ASTERISK

Digium® created Asterisk® was by and released it as open source software under the GNU General Public License (GPL). It is available free of charge as a download from the Internet for developing advanced communication solutions. Asterisk can switch calls, manage call routing and connect calls over IP, POTS and digital connections, to list just a few of its capabilities. It runs on a variety of operating systems and can interoperate with almost all standards-based telephony equipment.

Asterisk supports Session Initiation Protocol (SIP), making it an ideal choice for use in conjunction with Fusion SIP Trunking. For more information about Asterisk, visit www.digium.com.

PURPOSE, SCOPE AND AUDIENCE

This technical application note describes the configuration of Asterisk for the Fusion SIP Trunking service. This document is suitable for use by anyone deploying the Fusion SIP Trunking service in conjunction with Asterisk. This document has a technical audience in mind – specifically IT professionals skilled in Linux with some experience in PBX administration and familiarity with VoIP technologies. This document is not for business administrators or people in other non-technical careers. In order to successfully use this document to deploy Fusion SIP Trunking service, you will need to possess the following skills, or have access to professionals or consultants with the following skills:

- Understanding of UNIX or Linux operating systems, including:
  - Understanding of file and directory structure on target OS
  - Understanding of firewall configuration on target OS
  - Understanding of network configuration on target OS
  - Understanding of service configuration on target OS
- Familiarity with network troubleshooting tools, including:
  - Wireshark/Ethereal
  - dig/nslookup
  - ping
  - traceroute
- Familiarity with PBX systems, including:
  - Trunk configuration
  - Calling plan configuration
  - Extension configuration
  - Mailbox configuration
- Familiarity with Session Initiation Protocol (SIP)
- An understanding of all seven layers of the Open System Interconnection (OSI) model
- A complete understanding of your internal network structure, Network Address Translation (NAT) setup, and firewall setup
- A complete understanding of your public Internet connectivity

Fusion can only provide support for Asterisk to the extent covered in this Technical Application Note and the included reference configuration, so if your level of technical expertise does not include the above skills, it is recommended that you obtain the services of an Asterisk professional.

ASTERISK DEPLOYMENT INFORMATION

Before you begin deploying Asterisk, please locate the following information. If you have questions about any item, refer to the descriptions and additional details provided on the pages that follow.

Asterisk External IP Address or DNS: _____

Preferred Codec: ulaw g729

Alternate Codec: ulaw g729 none

Is Asterisk NATd: Yes No

Is Asterisk Behind a Firewall: Yes No

Is There a Local Firewall: Yes No

ASTERISK EXTERNAL IP ADDRESS

Your Asterisk server will either use a public IP address or a private IP address. If the IP address on your Asterisk server is of the form 192.168.x.x, 172.16.x.x – 172.31.x.x, or 10.x.x.x, then your Asterisk server uses an internal, private IP address. This internal address is not routable on the public Internet. In order for your Asterisk server to connect to the Fusion Session Border Controller, you must either have a public IP address on your Asterisk server or you must translate your private IP address into a public IP address using a Network Address Translator (NAT).

If your Asterisk server is behind a NAT, your public IP address will typically be the public IP address of your NAT. You may also have a static, one-toone mapping of a public IP address to your private IP address. In this case, your public IP address will not match the IP address of your NAT, but you can look up the correct public IP address in your NAT configuration. If in doubt, you can perform a network packet capture using Wireshark (previously called Ethereal) on the public side of your NAT while simultaneously issuing some form of Internet request on your Asterisk server.

SENDING CALLS TO FUSION

In your Welcome letter, Fusion provides DNS records to which you may send calls, and from which you should be prepared to receive calls. Asterisk supports DNS A records, DNS SRV records, and IP addresses. Please note, however, than Asterisk only resolves the DNS records during startup and will only utilize the first IP address in any multiple-IP record.

At the top of your technical welcome letter, you will see a table like this one which shows your account number, turn-up ticket number, and trunk number. This information should be provided to Fusion when you call for assistance to expedite support.

Account Number	Trunk turn-up Ticket Number	Trunk Number

Figure 1: Welcome Letter Account Information

The third page of the welcome letter contains a table of the IP addresses and ports you need to allow through your firewall. Note that the table included here is an example and may be out of date.

Traffic Type	IP Addresses	Protocol	Port Range
SIP	208.93.224.224/28 208.93.226.208/28 208.93.227.208/28	UDP and TCP	5060
SIPS (SIP over TLS)	208.93.224.224/28 208.93.226.208/28 208.93.227.208/28	TCP	5061
Media	208.93.224.224/28 208.93.226.208/28 208.93.227.208/28 69.60.209.4 69.60.209.5 216.86.41.4 216.86.41.5	UDP	1024-65536

Figure 2: Firewall Configuration Information

The third page also contains the IP address and DNS information you should use for configuring your trunk. We recommend you utilize the DNS A record entries for Asterisk unless you have specific reasons not to.

City	DNS A Record	DNS SRV Record	IP Address
New York City, NY	nyc01-01.fs.broadvox.net	nyc01-01.fs.broadvox.net	208.93.226.212
Dallas, TX	dfw01-01.fs.broadvox.net	dfw01-01.fs.broadvox.net	208.93.224.228
Los Angeles, CA	lax01-01.fs.broadvox.net	lax01-01.fs.broadvox.net	208.93.227.212

Figure 3: Trunk Destination Information

Also on the third page, you will find a section containing information about how your trunk is configured on the Fusion side. You should carefully review this information to ensure it is configured properly.

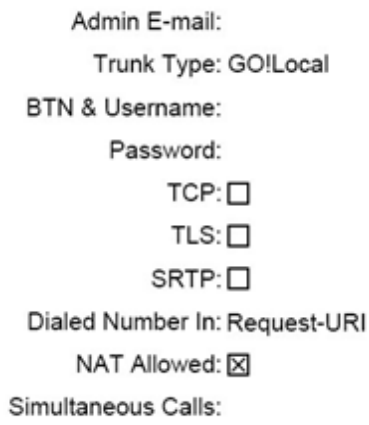


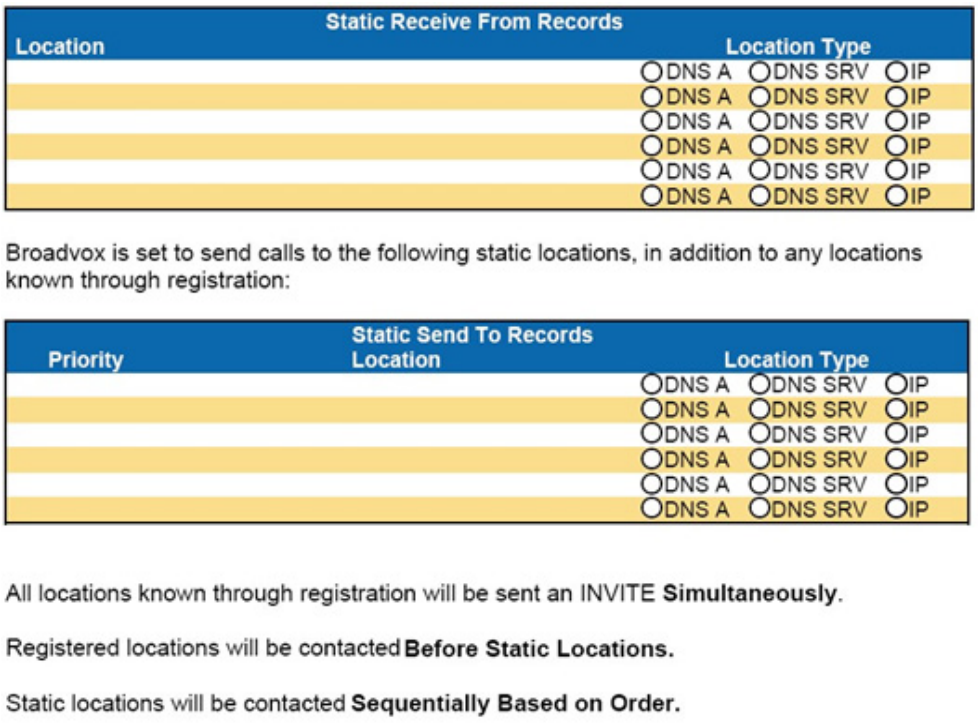
Figure 4: Configuration of Fusion Side

The 'Admin E-mail ' lists the E-mail address which will receive alerts from the Fusion SIP Trunking platform when various recognizable events occur. These events include things such as calls being blocked because they would cause you to exceed the simultaneous call sessions you purchased.

Asterisk has been tested to support TLS with special configuration changes, however, as of July 2009, Asterisk does not yet support SRTP.

Finally, on the fourth page, you will find two sections that specify how Fusion is configured to send calls to your Asterisk box and how Fusion is configured to receive calls from your Asterisk box. These two sections are only utilized if you provided static IP address information or DNS information. Fusion can send calls to entirely separate systems from the ones it is configured to receive calls from. This allows you to split your inbound and outbound traffic for any reason you may have, including but not limited to load distribution over several systems or multiple Internet connections. In addition, Fusion can randomly loadbalance calls across several systems using an identical priority for the Send-To records.

These options should allow you to engineer your traffic flow to suite your particular needs.



Static Receive From Records	
Location	Location Type
	○DNS A ○DNS SRV ○IP
	○DNS A ○DNS SRV ○IP
	○DNS A ○DNS SRV ○IP
	○DNS A ○DNS SRV ○IP
	○DNS A ○DNS SRV ○IP
	○DNS A ○DNS SRV ○IP

Broadvox is set to send calls to the following static locations, in addition to any locations known through registration:

Static Send To Records		
Priority	Location	Location Type
		○DNS A ○DNS SRV ○IP
		○DNS A ○DNS SRV ○IP
		○DNS A ○DNS SRV ○IP
		○DNS A ○DNS SRV ○IP
		○DNS A ○DNS SRV ○IP
		○DNS A ○DNS SRV ○IP

All locations known through registration will be sent an INVITE **Simultaneously**.

Registered locations will be contacted **Before Static Locations.**

Static locations will be contacted **Sequentially Based on Order.**

Figure 5: Signaling Configuration

SRV RECORDS

Service records (SRV) are a form of Domain Name System (DNS) record. They contain information about where to send requests for a particular service offered at a specific domain. In the case of Fusion SIP Trunking, they provide the IP addresses, port numbers, and preferences to use for sending SIP calls over UDP, TCP, and TLS to Fusion. The SRV location to use for sending calls to Fusion for each of your trunk groups is in your Welcome letter.

There is one caveat with using DNS records on Asterisk. Asterisk, by design, performs the DNS query on initial startup (or reload) and uses only one IP address for signaling to/from a peer. To configure Asterisk to provide proper redundancy, you must configure multiple peers for each different Fusion gateway. If you use IP addresses instead of DNS and Fusion removes one of the servers from DNS to perform a scheduled maintenance, your Asterisk server will continue to try to target that IP. This will add a small amount of post dial delay to your calls. Post dial delay (PDD) is the period of time between when you finish dialing a number and you start to receive ringing. Typically, the added delay will be less than 3 seconds.

TESTING SRV RECORDS

Most Fusion customers like to ensure the DNS entries are functioning or they like to look up the actual IP addresses, however, performing a standard DNS query on the SRV records will fail. In a Windows environment, you can perform the query using the nslookup command at a command prompt, as shown in Figure 1.

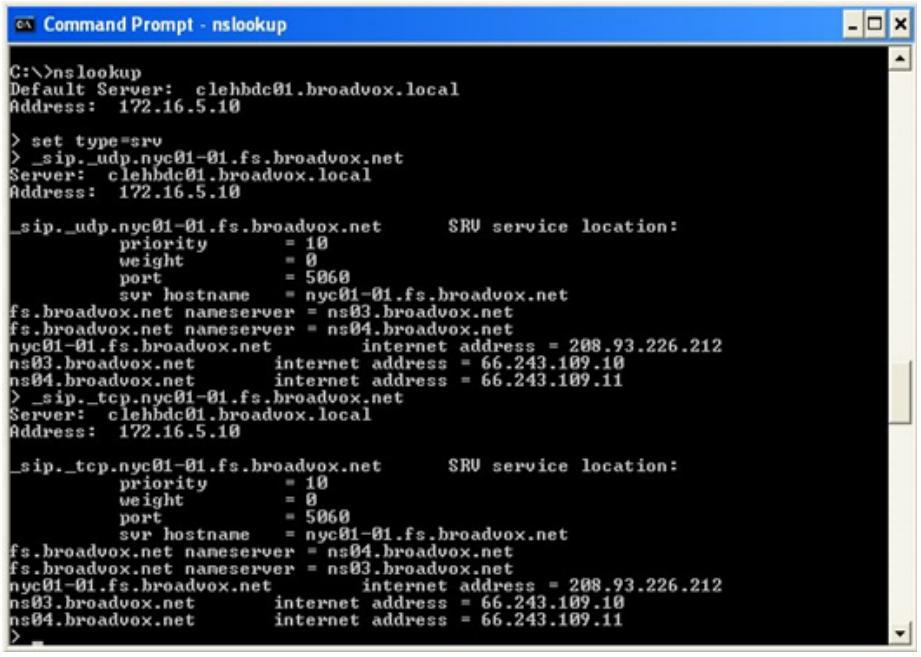


Figure 6: SRV Lookup in Windows XP

As you can see, a SRV record consists of a service type definition (_sip), a transport definition (_udp), and the domain (nyc01-01.fs.broadvox.net). Asterisk will automatically add the service and transport definitions as a prefix to the domain before performing the query. The query returns a priority, weight, port and hostname for each entry. The query also returns the "A record" entries for each hostname, which provides the IP address for each host.

In a UNIX or Linux environment, you can perform a query on our SRV records using the dig command:

```
$ dig srv _sip._udp.nyc01-01.fs.broadvox.net
; <<>> DiG 9.3.4-P1 <<>> srv _sip._udp.nyc01-01.fs.broadvox.net
;; global options:  printcmd ;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26443
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1
 ;; QUESTION SECTION:
;_sip._udp.nyc01-01.fs.broadvox.net. IN SRV
 ;; ANSWER SECTION:
_sip._udp.nyc01-01.fs.broadvox.net. 600 IN SRV  10 0 5060 nyc0101.fs.broadvox.net.
;; AUTHORITY SECTION: fs.broadvox.net.      600    IN     NS     ns03.broadvox.net. fs.broadvox.net.      600    IN     NS     ns04.broadvox.net.
;; ADDITIONAL SECTION:
nyc01-01.fs.broadvox.net. 600   IN     A      208.93.226.212
;; Query time: 95 msec
;; SERVER: 10.128.6.4#53(10.128.6.4)
;; WHEN: Thu Jul 30 13:59:26 2009
;; MSG SIZE  rcvd: 150
```

PREFERRED AND ALTERNATE CODECS

Fusion allows you to select preferred and alternate codecs to simultaneously meet your bandwidth requirements and provide greater end-to-end support. In the event that your destination party or your destination party's carrier cannot support your preferred codec or alternate codecs, Fusion will automatically transcode your call to a supported codec.

When configuring codecs, please keep in mind that G.711 µLaw (ulaw) consumes approximately 87.2 Kbps of bandwidth per simultaneous call over Ethernet. G.729 Annex A (g729) will consume approximately 31.2 Kbps of bandwidth per simultaneous call over Ethernet. Also, keep in mind that G.711 offers superior call quality when compared to G.729, but only if you have enough bandwidth to support all of your simultaneous calls.

IS ASTERISK NATD

If your Asterisk server uses an Internet-facing IP address of the form 192.168.x.x, 172.16.x.x – 172.31.x.x, or 10.x.x.x, then it is almost certainly behind a Network Address Translation (NAT) device. If your server uses an address of that form and is not behind a NAT, then it has no connectivity to the Internet. Even if your server uses an IP address that does not match the forms above, it is still possible (though very unlikely) that it is behind a NAT. If Asterisk is behind a NAT, you may need to perform port forwarding, set up a DMZ host or configure a one-toone static IP map.

IS ASTERISK BEHIND A FIREWALL

If Asterisk is behind a NAT, then it is almost certainly behind a firewall. It is also possible that Asterisk uses a public IP address but is still behind a firewall. If you use a Cisco PIX, SonicWALL, Shorewall, Firebox, or any other brand of firewall, you may need to perform additional configuration steps on the firewall device to allow Asterisk to function properly. Additionally, you may be using an Application Gateway such as an Ingate SIParator. These devices will also need additional configuration to allow Asterisk to function properly. Configuring your firewall or application gateway is beyond the scope of this document. In general, you will need to allow UDP port 5060 in both directions, as well as UDP ports 1024 to 65535 for RTP. However, you may need a larger range of ports for RTP.

IS THERE A LOCAL FIREWALL

In addition to being behind a firewall, it is also possible that the Asterisk server itself utilizes a local firewall. Typically, Asterisk is deployed on a UNIX or Linux operating system. These systems usually come with a firewall program installed, like iptables. If your server uses iptables, you can check to see if there are any rules in place by issuing the following commands:

```
$ iptables -L -v -n
Chain INPUT (policy ACCEPT 3549M packets, 4907G bytes)  pkts bytes target     prot opt in     out     source               destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 688M packets, 51G bytes)  pkts bytes target     prot opt in     out     source               destination
$ iptables -L -v -n -t nat
Chain PREROUTING (policy ACCEPT 1836K packets, 118M bytes)  pkts bytes target     prot opt in     out     source               destination
Chain POSTROUTING (policy ACCEPT 2247K packets, 136M bytes)  pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 2247K packets, 136M bytes)  pkts bytes target     prot opt in     out     source               destination
$ iptables -L -v -n -t mangle
Chain PREROUTING (policy ACCEPT 3551M packets, 4907G bytes)  pkts bytes target     prot opt in     out     source               destination
Chain INPUT (policy ACCEPT 3549M packets, 4907G bytes)  pkts bytes target     prot opt in     out     source               destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 688M packets, 51G bytes)  pkts bytes target     prot opt in     out     source               destination
Chain POSTROUTING (policy ACCEPT 688M packets, 51G bytes)  pkts bytes target     prot opt in     out     source
```

The output shown above indicates that there are no firewall rules configured on this server. If you are using a different type of firewall software on your Asterisk server, you will need to consult the documentation for that software to learn how to check whether it is enabled. If you have a local firewall enabled, you will need to configure it to allow the appropriate ports, as described in "Is Asterisk Behind a Firewall."

If you are using a standard iptables firewall setup, such as the one on Red Hat Enterprise Linux, CentOS, Gentoo Linux, or Slackware Linux, these rules may be of use to you in allowing the appropriate traffic from our Fusion platform:

```
# Allow SIP over UDP, TCP, and TLS:

iptables -I INPUT -p udp --dport 5060 -s 208.93.224.224/28 -j ACCEPT iptables -I INPUT -p tcp --dport 5060 -s 208.93.224.224/28 -j ACCEPT iptables -I INPUT -p tcp --dport 5061 -s 208.93.224.224/28 -j ACCEPT iptables -I INPUT -p udp --dport 5060 -s 208.93.226.208/28 -j ACCEPT iptables -I INPUT -p tcp --dport 5060 -s 208.93.226.208/28 -j ACCEPT iptables -I INPUT -p tcp --dport 5061 -s 208.93.226.208/28 -j ACCEPT iptables -I INPUT -p udp --dport 5060 -s 208.93.227.208/28 -j ACCEPT iptables -I INPUT -p tcp --dport 5060 -s 208.93.227.208/28 -j ACCEPT iptables -I INPUT -p tcp --dport 5061 -s 208.93.227.208/28 -j ACCEPT # Allow media:

iptables -I INPUT -p udp --dport 1024:65535 -s 208.93.224.224/28 -j ACCEPT iptables -I INPUT -p udp --dport 1024:65535 -s 208.93.226.208/28 -j ACCEPT iptables -I INPUT -p udp --dport 1024:65535 -s 208.93.227.208/28 -j ACCEPT iptables -I INPUT -p udp --dport 1024:65535 -s 64.158.162.71 -j ACCEPT iptables -I INPUT -p udp --dport 1024:65535 -s 64.158.162.100 -j ACCEPT iptables -I INPUT -p udp --dport 1024:65535 -s 64.152.60.71 -j ACCEPT iptables -I INPUT -p udp --dport 1024:65535 -s 64.152.60.164 -j ACCEPT iptables -I INPUT -p udp --dport 1024:65535 -s 209.249.3.71 -j ACCEPT iptables -I INPUT -p udp --dport 1024:65535 -s 209.249.3.81 -j ACCEPT iptables -I INPUT -p udp --dport 1024:65535 -s 64.156.174.71 -j ACCEPT iptables -I INPUT -p udp --dport 1024:65535 -s 208.93.227.5 -j ACCEPT iptables -I INPUT -p udp --dport 1024:65535 -s 208.93.226.5 -j ACCEPT
```

Please note, you may not be able to copy and paste these directly into a terminal program like SecureCRT, PuTTY, ZOC, etc. You may need to paste into Notepad or a similar text-only editor, and then copy and paste from there into the terminal program. This extra step should eliminate any hidden formatting characters that get copied along with the text (typically only applies when performing the copy and paste on a Microsoft platform).

Any rules you insert into iptables must be loaded each time the Asterisk server restarts. There are typically two methods to accomplish this. The first (and usually preferred) method is to use the iptables save and restore functionality. On most platforms, you can simply issue one of these two commands:

```
/etc/init.d/iptables save /etc/rc.d/iptables save
```

The second method is to use a start-up script to re-issue the commands that add the rules. Generally, you would create a file in /etc/init.d or the appropriate /etc/rc.d directory (based on your individual platform) that contains the commands to create the rules. You would then chmod the file so that it is executable. Next, you would either create a symbolic link in the appropriate /etc/rc.d directory, or you would add it to your 'local' script which is responsible for executing any custom start-up commands.

If you require any further assistance in modifying your local firewall, please consult the documentation appropriate for your OS distribution and firewall program.

CONFIGURING ASTERISK

Asterisk configuration files are typically stored in /etc/asterisk. The two files we are most concerned with are sip.conf and extensions.conf. Using a text editor such as vim, vi, emacs, pico, nano, jed, or joe, modify the sip.conf file to support the Fusion SIP Trunking service, as outlined in Appendix A. Asterisk Sip.conf File. After modifying the sip.conf file, modify the extensions.conf file as outlined in Appendix B. Asterisk Extensions.conf File.

The sip.conf file tells Asterisk how to interconnect with SIP peers. The top section of the sip.conf file (under the section [general]) contains global settings that you should apply to all of your peers. Some of these settings can be set on each individual peer, such as codecs. Individual peer settings override global settings.

The extensions.conf file creates dialing plans that allow you to configure how and where your calls are sent. Each section in the extensions.conf file is called a "context." You can include dialing rules from other contexts by using the include command. The default rules provided in the reference configuration will enable all 10-digit dialed and toll-free numbers to be sent to your Fusion Local trunk and all 1+10-digit dialed and international numbers to be sent to your Fusion Domestic trunk. You may modify the dialing rules to suit your needs.

After configuring the sip.conf and extensions.conf files, you must reload the configuration. You can do this by either reloading the Asterisk service, or by performing the following actions:

```
$ asterisk -r Asterisk 1.2.21.1, Copyright (C) 1999 - 2007 Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'show warranty' for details.
This is free software, with components licensed under the GNU General
Public
License version 2 and other licenses; you are welcome to redistribute it under certain conditions. Type 'show license' for details.
=========================================================================
Connected to Asterisk 1.2.21.1 currently running on localhost (pid =
26232)
localhost*CLI> set verbose localhost*CLI> reload
```

Either method will be sufficient to instate the new configuration, however using the Asterisk command prompt is the preferred method as it has less impact and provides more verbose output about the reload of the configuration files.

APPENDICES: REFERENCE CONFIGURATION FILES

A. Asterisk Sip.conf File for Fusion SIP Trunks

[general] ; The "default" context is where all unknown, inbound calls will be sent context=default ; Default context for incoming calls

; Broadvox supports port 5060 only

bindport=5060 ; UDP Port to bind to (SIP standard port is 5060)

; You may bind to all addresses on your Asterisk server, or whichever address

; is Internet-facing.

bindaddr=0.0.0.0 ; IP address to bind to (0.0.0.0 binds to all)

; Broadvox offers SRV records, but the default is to use DNS A records srvlookup=no ; Disable DNS SRV lookups on outbound calls
; Note: Asterisk only uses the first host

; in SRV records

; Disabling DNS SRV lookups disables the

; ability to place SIP calls based on domain ; names to some other SIP users on the Internet

; This is used by some routers to prioritize your voice packets for reduced

; latency and jitter

tos=lowdelay ; lowdelay,throughput,reliability,mincost,none

; Broadvox recommends you place your Asterisk box's external IP address in the ; 'fromdomain' field. Alternatively, you may place your FQDN for your Asterisk

; box in the 'fromdomain' field. fromdomain=____.____.____.____ ; When making outbound SIP INVITEs to

; non-peers, use your primary domain "identity"

; for From: headers instead of just your IP

; address. This is to be polite and

; it may be a mandatory requirement for some

; destinations which do not have a prior ; account relationship with your server.

; * DTMF and Codec Support **********

; * You may optionally specify these settings on your Broadvox-specific peer ; * settings. Broadvox supports G.711 uLaw and G.729 Annex B.

; ********** disallow=all ; First disallow all codecs

allow=ulaw ; Allow codecs in order of preference; G.711 uLaw allow=g729 ; Allow G.729 Annex B

; Broadvox supports RFC2833 DTMF events. This requires Asterisk 1.4.19 or

; higher due to prior bugs in Asterisk's DTMF implementation. dtmfmode=rfc2833 ; Set default dtmfmode for sending DTMF. Default: rfc2833

; Other options:

; info: SIP INFO messages

; inband: Inband audio; requires 64 kbit codec alaw, ulaw

; auto: Use rfc2833 if offered, inband otherwise

; **********

Fusion SIP Trunks support registration. The following line tells Asterisk to register to Broadvox using the BTN and Password provided in your Welcome letter. Be sure to fill out the BTN and password below, as well as the signaling IP or DNS address for the trunk that the BTN belongs to. If you have more than one trunk with a BTN that will register, you may enter multiple register lines here. Because Fusion trunks provide redundant platforms in three cities, you will need three register lines for ; each trunk.

****

register=>BTN:PASSWORD@dfw01-01.fs.broadvox.net register=>BTN:PASSWORD@nyc01-01.fs.broadvox.net register=>
BTN:PASSWORD@lax01-01.fs.broadvox.net

;register=>BTN2:PASSWORD2@dfw01-02.fs.broadvox.net

;register=>BTN2:PASSWORD2@nyc01-02.fs.broadvox.net

;register=>BTN2:PASSWORD2@lax01-02.fs.broadvox.net

;register=>BTN3:PASSWORD3@dfw01-03.fs.broadvox.net

;register=>BTN3:PASSWORD3@nyc01-03.fs.broadvox.net

;register=>BTN3:PASSWORD3@lax01-03.fs.broadvox.net

; ***

; * NAT SUPPORT ***

; The externip, externhost and localnet settings are used if you use Asterisk ; behind a NAT device to communicate with services on the outside.

; Broadvox recommends you place your external IP address in the 'externip' ; field.

; ** externip=____.____.____.____ ; Address to put in outbound SIP messages

; if we're behind a NAT

; The externip and localnet is used

; when registering and communicating with

; other proxies that we're registered with

;externhost=foo.dyndns.net ; Alternatively you can specify an

; external host, and Asterisk will

; perform DNS queries periodically. Not

; recommended for production

; environments! Use externip instead

; The nat= setting is used when Asterisk is on a public IP, communicating with devices hidden behind a NAT device (broadband router). If you have one-way audio problems, you usually have problems with your NAT configuration or your firewall's support of SIP+RTP ports. You configure Asterisk choice of RTP ports for incoming audio in rtp.conf

; You may need to adjust this setting to suite your particular environment. nat=route ; Global NAT settings (Affects all peers and users)

; yes = Always ignore info and assume NAT

; no = Use NAT mode only according to RFC3581 (;rport)

; never = Never attempt NAT mode or RFC3581 support

; route = Assume NAT, don't send rport

; (work around more UNIDEN bugs)

; ***

; * Peer Definitions **

; * The peers listed here are targeted in your extensions.conf file to send calls out. They also determine where inbound calls from certain peers will be directed in your extensions.conf file. In your welcome letter, you will find a line that tells you what IP address to use when sending your calls. You will want to place that IP address in the 'host' field for the particular peer you are defining. An example of a dual, GO!Domestic + GO!Local configuration is included here. If you have more than one GO!Local trunk (Broadvox supports up to 10 trunks to a single IP), you can define them all here. Each will have a different IP address to target in the 'host' field. On each ; * GO!Local trunk, you should set the call-limit value accordingly.

; ***

[GODOMESTIC1-NYC-OUT] type=peer

context=GODOMESTIC-INBOUND host=nyc01-01.fs.broadvox.net canreinvite=no

[GODOMESTIC1-DFW-OUT] type=peer

context=GODOMESTIC-INBOUND host=dfw01-01.fs.broadvox.net canreinvite=no

[GODOMESTIC1-LAX-OUT] type=peer

context=GODOMESTIC-INBOUND host=lax01-01.fs.broadvox.net canreinvite=no

; For brevity, only one GO!Local trunk is configured, but you can configure up to 10 trunks per origination IP that you ; use.

[GOANYWHERE1-NYC-OUT] type=peer

context=GOANYWHERE1-INBOUND host=nyc01-01.fs.broadvox.net canreinvite=no

[GOANYWHERE1-DFW-OUT] type=peer

context=GOANYWHERE1-INBOUND host=dfw01-01.fs.broadvox.net canreinvite=no

[GOANYWHERE1-LAX-OUT] type=peer

context=GOANYWHERE1-INBOUND host=lax01-01.fs.broadvox.net canreinvite=no

; **

; * Internal SIP Device Definitions **

; * You will also need to configure peer or friend definitions for your ; * internal SIP devices. An example Sipura configuration is given.

; **

[SIPURA-OUT]

type=friend ; peer+user

context=SIPURA-INBOUND ; Context for calls from Sipura

canreinvite=no ; Disallow re-INVITES to direct media around Asterisk username=JohnDoe ; Username for registration secret=MyPass1234 ; Password for registration

mailbox=1234@default ; mailbox 1234 in voicemail context “default” host=dynamic ; This device needs to register insecure=very

permit=192.168.0.0/255.255.0.0 ; Allow auth from these internal IP permit=172.16.0.0/255.224.0.0 ; addresses permit=10.0.0.0/255.0.0.0

; **

B. Asterisk Extensions.conf File for Fusion SIP Trunks

[GOANYWHERE1-INBOUND] include => ROUTES

[GODOMESTIC1-INBOUND] include => ROUTES

; This tells Asterisk to route calls based on the TO header field in the SIP INVITE instead of the Request-URI. This is needed when using registration in order to properly route calls based on the dialed number instead of the BTN. Fusion trunks support sending the dialed number in either the Request-URI or the To-URI for registered trunks. In either case, the dialed number will always be present in the To-URI, so we recommend you ; use this method of routing your calls.

[ROUTES]

exten=>s,1,Goto(DIDS,${SIP_HEADER(TO):5:10},1) exten=>s,n,Goto(AutoAttendant,s,1)

[DIDS]

exten => 5555398198,1,Dial(SIP/${EXTEN}@SIPURA1-OUT) exten => 5555398199,1,Dial(SIP/${EXTEN}@SIPURA2-OUT)

; This is where you would define your auto-attendant

[AutoAttendant]

;exten=>s,1,Answer

;exten=>s,n,Playback(aa-greeting)

; Any calls hitting sipura-inbound are dialed from our phone, so they are

; actually outbound calls. Here we tell how to send the calls out to ; Broadvox, including whether to use GO!Local or GO!Domestic.

[SIPURA-INBOUND]

; We are coming in from a phone, so include our extensions list include => extensions

; GO!Local should come first to catch toll-free and local calling rules include => GOANYWHERE1-OUT-PLAN include => GODOMESTIC1-OUT-PLAN ; This is how you would do an extension:

[extensions]

exten => 101,1,Dial(SIP/${EXTEN}@101)

; Notice that each pattern match has three rules. The first rule will attempt to send the call to the NYC gateway. If that fails for some reason, then the call will be attempted on the Dallas gateway. If that also fails, then then call will be attempted on the LA gateway. This provides redundancy for ; outbound calling in the event Fusion has an outage in one of the cities.

You may change the ordering of the cities. However, the first one listed should contain the '1' value for the order field while the other two should contain the 'n' value for the order field. Also note that the first rule on the 911 rule sets the caller ID to your BTN. You must ensure that calls to 911 use the correct outbound caller ID based on the address of phone making the call. If you have multiple offices using this PBX, you may need multiple ; dial plans or multiple 911 rule sets to accomplish this.

[GOANYWHERE1-OUT-PLAN]

exten => _411,1,Dial(SIP/${EXTEN}@GOANYWHERE1-NYC-OUT) exten => _411,n,Dial(SIP/${EXTEN}@GOANYWHERE1-DFW-OUT) exten => _411,n,Dial(SIP/${EXTEN}@GOANYWHERE1-LAX-OUT) exten => _711,1,Dial(SIP/${EXTEN}@GOANYWHERE1-NYC-OUT) exten => _711,n,Dial(SIP/${EXTEN}@GOANYWHERE1-DFW-OUT) exten => _711,n,Dial(SIP/${EXTEN}@GOANYWHERE1-LAX-OUT) exten => _911,1,Set(CALLERID(all)=My Company <my_btn_goes_here>) exten => _911,n,Dial(SIP/${EXTEN}@GOANYWHERE1-NYC-OUT) exten => _911,n,Dial(SIP/${EXTEN}@GOANYWHERE1-DFW-OUT) exten => _911,n,Dial(SIP/${EXTEN}@GOANYWHERE1-LAX-OUT) include => toll-free-out include => local-calling-areas

; Define local dialing patterns to map local calls to GO!Local trunk

; 10 digit dialing will attempt GO!Local trunk

[local-calling-areas]

exten => _NXXNXXXXXX,1,Dial(SIP/${EXTEN}@GOANYWHERE1-NYC-OUT) exten => _NXXNXXXXXX,n,Dial(SIP/${EXTEN}@GOANYWHERE1-DFW-OUT) exten => _NXXNXXXXXX,n,Dial(SIP/${EXTEN}@GOANYWHERE1-LAX-OUT)

; Patterns to send toll free to GO!Local trunk

; 11 digit toll-free dialing will attempt GO!Local trunk

[toll-free-out]

exten => _1800NXXXXXX,1,Dial(SIP/${EXTEN}@GOANYWHERE1-NYC-OUT) exten => _1800NXXXXXX,n,Dial(SIP/${EXTEN}@GOANYWHERE1-DFW-OUT) exten => _1800NXXXXXX,n,Dial(SIP/${EXTEN}@GOANYWHERE1-LAX-OUT) exten => _1866NXXXXXX,1,Dial(SIP/${EXTEN}@GOANYWHERE1-NYC-OUT) exten => _1866NXXXXXX,n,Dial(SIP/${EXTEN}@GOANYWHERE1-DFW-OUT) exten => _1866NXXXXXX,n,Dial(SIP/${EXTEN}@GOANYWHERE1-LAX-OUT) exten => _1877NXXXXXX,1,Dial(SIP/${EXTEN}@GOANYWHERE1-NYC-OUT) exten => _1877NXXXXXX,n,Dial(SIP/${EXTEN}@GOANYWHERE1-DFW-OUT) exten => _1877NXXXXXX,n,Dial(SIP/${EXTEN}@GOANYWHERE1-LAX-OUT) exten => _1888NXXXXXX,1,Dial(SIP/${EXTEN}@GOANYWHERE1-NYC-OUT) exten => _1888NXXXXXX,n,Dial(SIP/${EXTEN}@GOANYWHERE1-DFW-OUT) exten => _1888NXXXXXX,n,Dial(SIP/${EXTEN}@GOANYWHERE1-LAX-OUT)

; Long distance / international will go over GO!Domestic

; 11 digit dialing will attempt GO!Domestic

[GODOMESTIC-OUT-PLAN]

exten => _1NXXNXXXXXX,1,Dial(SIP/${EXTEN}@GODOMESTIC1-NYC-OUT) exten => _1NXXNXXXXXX,n,Dial(SIP/${EXTEN}@GODOMESTIC1-DFW-OUT) exten => _1NXXNXXXXXX,n,Dial(SIP/${EXTEN}@GODOMESTIC1-LAX-OUT) include => international-out

[international-out]

exten => _011X.,1,Dial(SIP/${EXTEN}@GODOMESTIC1-NYC-OUT) exten => _011X.,n,Dial(SIP/${EXTEN}@GODOMESTIC1-DFW-OUT) exten => _011X.,n,Dial(SIP/${EXTEN}@GODOMESTIC1-LAX-OUT)