TELSTRA BUSINESS SIP®

CUSTOMER DETAILED INTEGRATION GUIDE

Table of Contents

1. About this Document

The purpose of this document is to communicate key information about the deployment and integration of the Business SIP® product.

The audiences may include Telstra pre-sales, Telstra partners and anyone involved with considering the Business SIP product.

> **Note:** This document does not constitute an IP Tel design but serves as a generic reference guide for the adoption of the Telstra Business SIP® product and applications only within the customer's environment.

1.1. Product architecture overview

The diagram below provides an overview of the Telstra Business SIP® product architecture.

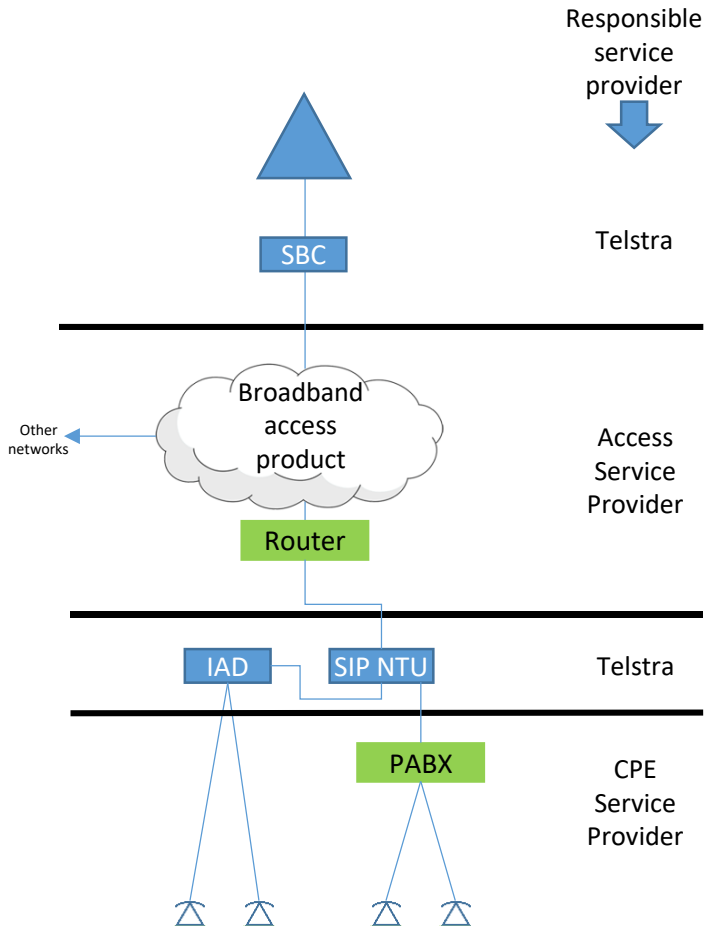

Figure 1 – Product architecture

The Telstra Business SIP® product is a voice-only product that resides over the top of a broadband access product. The broadband access product is a separately ordered product that should provide guaranteed voice bandwidth to ensure high quality of experience for calls.

Similarly, the PABX, phones and local networking environment is a separately ordered product. Only accredited providers/personnel should be involved in setting up the customer's local environment including performing installs and migrations.

The Telstra-supplied SIP NTU is an optional device for connecting ISDN or IP PBX's. Customers requiring an IAD for connecting analogue phones or voice-band data devices (e.g. fax) must order one of the available Telstra devices or use native capabilities of the PBX.

Due to the nature of the SIP protocol **only accredited IP PBX's can be connected**.

2. Customer environment

2.1. Bandwidth

The voice bandwidth of the broadband access product must be dimensioned using at least 100Kbit/s in each direction for each concurrent phone call provisioned on the service. See the table below for examples.

Number of concurrent calls	Minimum Downstream Voice Bandwidth	Minimum Upstream Voice Bandwidth
2	200 Kbit/s	200 Kbit/s
4	400 Kbit/s	400 Kbit/s
6	600 Kbit/s	600 Kbit/s
8	800 Kbit/s	800 Kbit/s
10	1 Mbit/s	1 Mbit/s
30	3 Mbit/s	3 Mbit/s
50	5 Mbit/s	5 Mbit/s
60	6 Mbit/s	6 Mbit/s
100	10 Mbit/s	10 Mbit/s
150	15 Mbit/s	15 Mbit/s

Table 1 – Bandwidth requirements

2.2. Router

2.2.1. Quality of Service

The WAN router must be designed and configured with a suitable QoS policy to categorise and prioritise VoIP traffic over data. The customer's access service provider is responsible for ensuring the router is appropriately configured. Where either a QOS aware gateway/router or Access QOS is not available, then it is recommended to dedicate the full link to voice only to maintain voice quality.

2.2.2. Router Configuration for Voice

Routers vary in their default configuration and implementation of the following features:

- Firewalls
- NAT (Network Address Translation)
- SIP ALG (SIP Application Layer Gateway)
- uPnP (Universal Plug and Play)
- Port Forwarding

There is no one size fits recommendation for all cases, but the following table has some examples and suggested steps when using different types of routers.

Example	Router / Gateway	SIP NTU Gets Config OK	SIP NTU Registers OK	Two Way Speech for Voice Calls OK	Remote Admin Works	Required Router Config Actions
1	Telstra Netgear V7610	Y	Y	Y	Y	No special action is required for Port forwarding or Remote Administration as these features are preconfigured
2	Generic Router	Y	Y	Y	N	Enable uPNP or configure Remote administration (as per 2.2.5)
3	Generic Router	Y	N	N	N	Disable SIP ALG + Add Port Forwarding (as per 2.2.4) + Configure Remote administration (as per 2.2.5) or Enable uPNP for Remote admin
4	Generic Router	Y	Y	N	N	Enable SIP ALG + uPnP + Add Port Forwarding (as per 2.2.4) + Configure Remote administration (as per 2.2.5)

Table 2 – Router configuration actions

2.2.3. Firewalls

Firewall misconfiguration can break VoIP. If the service appears to be partially working, e.g. one-way voice, then it is likely that some firewall re-configuration is required.

Telstra recommends that you allow the subnets listed in either the “Summarised routes” in section 2.2.3.2 or the “Detailed routes” listed in section 2.2.3.3 through the firewall, for all the ports/protocols listed in section 2.2.4. For customers looking for a “Quick firewall guidelines” refer to section 2.2.3.1. Although this will work, it is not recommended for customers with Telstra carriage. It is also worth noting that Telstra’s ability to support customers/partners is greatly enhanced when “Remote Administration” access is allowed to the NTU as per section 2.2.5.

2.2.4. Quick Firewall Guidelines – No Remote Admin

Activating encryption may simplify the process, as follows:

1. Enable Encryption in the Business SIP Customer Portal then reboot NTU. This reduces the SBCs involved from 4 SBC’s to 2 SBC’s which means less firewall rules
2. Set NTU with a Static IP (Requires NTU to be Factory reset and reprogrammed) or setup a static DHCP lease from DHCP server to ensure the NTU WAN IP never changes
3. Allow SIP/sRTP/sRTCP traffic to/from these SBC IP’s: 192.148.164.7/32 & 192.148.164.23/32
4. Allow SIP/sRTP/sRTCP Traffic to/from the NTU WAN IP and IAD WAN IP, if applicable
5. Voice RTP/sRTP will be UDP and use the full 16384-32768 between the NTU Northbound to SBC
6. SIP Signalling will be port 5061 both ends (SBC & NTU) when encrypted

However, if Telstra carriage is in place, activating encryption may increase latency, as encrypted SBC’s do not exist in every state. In this case, consider implementing the full firewall configuration as outlined below.

2.2.5. Summarised routes

The following tables list the routes required for Business SIP in a summarised form to simplify the number of entries.

NTU Remote Administration: (Telstra Admin Source IP's)

REMOTE ADMIN IP ADDRESS
203.35.135.0 / 24
203.35.82.0 / 24
203.213.78.50

Customer IT staff should allow Telstra remote admin access to the NTU from the listed IP addresses to the static IP of the NTU.

Telstra Core SBC's - Simplified Subnets:

SBC IP ADDRESS	DESCRIPTION
203.41.24.0 / 24	VIC / NSW / QLD / WA SBC's
203.41.29.0 / 24	SA SBC
192.148.164.0 / 24	Both i-SBC's used for encryption (and fall back for non-encrypted sites)

Telstra Configuration Servers: (used to get NTU/IAD configuration files)

CONFIGURATION SERVER IP ADDRESS
144.140.208.16 / 29
144.140.208.32 / 28
144.140.162.40 / 29
144.140.162.48 / 28

Devices will not install and will not pick up updated configuration files if these IP's are blocked.

2.2.6. Detailed routes

The following tables list the routes required for Business SIP showing specific IP addresses, if preferred.

NTU Remote Administration: (Telstra Admin Source IP's)

REMOTE ADMIN IP ADDRESS
203.35.135.0 / 24
203.35.82.0 / 24
203.213.78.50

Customer IT staff should allow Telstra remote admin access to the NTU from the listed IP addresses to the static IP of the NTU.

Telstra Core SBC's:

NTU HOME LOCATION	SBC IP ADDRESS
Encrypted – any state	192.148.164.7 192.148.164.23
QLD	203.41.24.132 203.41.24.164 192.148.164.8 192.148.164.24
NSW/ACT	203.41.24.68 203.41.24.100 192.148.164.8 192.148.164.24
VIC/TAS	203.41.24.4 203.41.24.36 192.148.164.8 192.148.164.24
SA/NT	203.41.24.196 203.41.29.4 192.148.164.8 192.148.164.24
WA	203.41.24.196 203.41.29.4 192.148.164.8 192.148.164.24

When encryption is enabled, then only the two IP addresses are required, independent of the state involved.

For the state where the NTU is homed, the NTU will try any of the addresses listed, so all 4 IP addresses should be allowed through firewalls.

Customer IT staff should allow internet traffic from the relevant SBC IP's to Port 5060/5061 of the Static IP of the WAN side of the NTU to allow call signalling.

Telstra Configuration Servers: (used to get NTU/IAD configuration files)

CONFIGURATION SERVER IP ADDRESS
144.140.208.16 / 29
144.140.208.32 / 28
144.140.162.40 / 29
144.140.162.48 / 28

Devices will not install and will not pick up updated configuration files if these IP's are blocked.

2.2.7. Ports and Protocols

Avoid the use of firewall devices before or after the SIP NTU device as they may cause issues such as one-way/no-way speech, SIP registration issues or block Telstra's remote access to the IAD which is used to assist with issues.

The following table provides a list of the protocols and ports used by Telstra Business SIP®. These are relevant to both Northbound and Southbound, except TLS, SRTP & SRTCP which are not employed Southbound.

SERVICE	PROTOCOL	PORT	DESCRIPTION
SIP	UDP/TCP/TLS	5060/5061	Signalling protocol used by SIP NTU
RTP	UDP	16384 - 32768	Real-time Transport Protocol (Media) used to deliver audio between VoIP end-points.
SRTP	UDP	16384 - 32768	Secure Real-time Transport Protocol (Media) used to deliver encrypted audio between VoIP end-points.
RTCP	UDP/TCP	16384 - 32768	Real-time Transport Control Protocol used to provide QoS status to end-points.
SRTCP	UDP/TCP	16384 - 32768	Secure Real-time Transport Control Protocol used to provide encrypted QoS status to end-points.
HTTPS	TCP	443	Hyper Text Transfer Protocol Secure used to provide encrypted sessions from customer computer browser to the Telstra Business SIP® Web Portal and remote access for Telstra support personnel.
SSH	TCP	22	Secure Shell used to provide encrypted sessions from Telstra support personnel to the SIP NTU.

Table 6 – Ports and Protocols

2.2.8. Remote administration

To enable Telstra support staff to remotely administer the SIP NTU, set up port forwarding on the router to the SIP NTU WAN IP address as follows:

TCP traffic inbound to port 59999, forward to SIP NTU IP Address, port 443

TCP traffic inbound to port 60999, forward to SIP NTU IP Address, port 22

For example, if the IP address of the SIP NTU was 192.168.190.2, then the port forwarding rule becomes:

TCP traffic inbound to port 59999, forward to 192.168.190.2:443

TCP traffic inbound to port 60999, forward to 192.168.190.2:22

It is highly recommended that a static DHCP assignment or fixed IP address be assigned to the SIP NTU to ensure the port forwarding is maintained. If this is not possible then power reset the router with no wired/wireless connections, then connect the SIP NTU and note the IP address assigned then use this as the IP referenced in the port forwarding. This will ensure the most likely IP to be assigned by DHCP after a power-reset of the router and SIP NTU is used.

If multiple devices exist on site then use the next port in sequence, counting down, e.g. for the 2nd device use:

TCP traffic inbound to port 59998, forward to SIP NTU IP Address, port 443

TCP traffic inbound to port 60998, forward to SIP NTU IP Address, port 22

2.2.9. DHCP Options to support IAD's

The following DHCP configuration is required for all routers (except the Telstra Netgear Gateway Pro V7610) if connecting an IAD such as the One Access 8-Port or the Cisco SPA122 directly to a router, and not via the recommended connection to ports (0/2 and 0/3) of the SIP NTU. Without access to these DHCP Options, the IAD's will not download their configuration files and will not function at all.

If the One100 8-port IAD is being used then DHCP Options must be configured as shown in the table.

DHCP OPTION	FIELD FORMAT	VALUE
Option 160	ASCII	http://polydms.digitalbusiness.telstra.com/dms/bootstrapV4

If the SPA-122 2-port IAD is being used then DHCP Options must be configured as shown in the table.

DHCP OPTION	FIELD FORMAT	VALUE
Option 66	ASCII	dms.digitalbusiness.telstra.com

It is recommended that these devices are connected to the LAN ports of the SIP NTU. Note that only the 3rd and 4th ports (0/2 and 0/3) of the SIP NTU are DHCP-enabled so these are the ports to be used for the IAD's.

If the IAD is connected via the SIP NTU in the recommended configuration, DHCP Opt 66 and DHCP Opt 160 will be handled by the SIP NTU.

2.3. SBC Pingable addresses

Below are the IP addresses to ping for testing which will also confirm SBC connectivity for both encrypted and non-encrypted services.

Note: The ping tests are only the segment from the customer to the Telstra core SBC's.

Telstra PoP's accessible to Telstra Business Broadband and Telstra 4G (Unencrypted)

SBC POP	PINGABLE IP ADDRESS
VIC/TAS POP 1	203.41.24.1
VIC/TAS POP 2	203.41.24.33
NSW/ACT POP 1	203.41.24.65
NSW/ACT POP 2	203.41.24.97
QLD POP 1	203.41.24.129
QLD POP 2	203.41.24.161
WA POP 1	203.41.24.193
WA POP 2	203.41.29.1
SA/NT POP 1	203.41.29.1
SA/NT POP 2	203.41.24.193

Internet-facing POP's & Encrypted

SBC POP	PINGABLE IP ADDRESS
POP 1	192.148.164.1
POP 2	192.148.164.17

3. Web Portal

Telstra Business SIP® has a web portal, accessible through the internet, for configuring elements of the service.

The url is https://portal.mycalling.telstra.com/

Username/passwords are supplied by email to the customer administrator at the time of service establishment.

It is mandatory to access the portal for the following actions:

- Retrieving device credentials for OneAccess devices (SIP NTU, One100 IAD) needed for initial installation.
- Performing number migration from the old ISDN/PSTN service to the new Telstra Business SIP® service.
- Assigning purchased feature packs to individual numbers
- Configuring Hunt Group or Virtual Receptionist, if purchased
- Activation/deactivation of Encryption. By default voice is not encrypted. If you wish to change this, then activation is performed via the Portal. Activate encryption only where the broadband access product traverses untrusted networks, e.g. the internet. When Non-Telstra Access is used, then the voice will traverse the Internet.

4. Appendices

4.1. Appendix A: Telstra IP-VPN for Business SIP

Telstra IP-VPN products: Business IP, Connect IP

Also known as: Telstra IP-VPN, Telstra MPLS

Telstra IP-VPN is the primary means for providing carriage for TIPT and SIP Connect customers. This carriage is supported for Business SIP.

The steps required to set up the IP-VPN for Business SIP can be summarised as follows:

1. Establish the IP-VPN
2. Establish the data/media interconnects
3. Establish the DNS forwarding rules
4. Set up firewall rules and routes
5. Test for connectivity

The following sections provide more detail on these topics.

4.1.1. Establish the IP-VPN

Order and build the Business IP or Connect IP service. Refer to your Telstra representative to arrange.

4.1.2. Establish the data/media interconnects

Interconnects to the TIPT core platform from the IP-VPN must be built. Interconnects are not automatically provisioned so need to be specifically ordered. Refer to your Telstra representative to arrange. If a TIPT or SIP Connect service is/was operational on this IP-VPN then interconnects are already in place.

Data interconnects: These enable the SIP NTU and IAD's to perform DNS look-ups and allow connectivity to the Telstra configuration servers needed by the SIP NTU and IAD's to retrieve their configurations.

Media interconnects: These provide connectivity to the Telstra SBC's for SIP and RTP for call signalling and media traffic.

4.1.3. Establish the DNS forwarding rules

The IP network must forward DNS look-ups for the following FQDN's to the Telstra DNS via the data interconnects:

- digitalbusiness.telstra.com
- nipt.telstra.com
- tipt.telstra.com

Primary Domain Forwarder: 203.52.0.221

Secondary Domain Forwarder: 203.52.1.222

4.1.4. Set up firewall rules and routes

The following tables list the routes required for Business SIP.

Data interconnects:

DATA INTERCONNECTS
203.52.0.0 / 23

Telstra Core SBC's:

STATE	SBC IP ADDRESS	PING-ABLE ADDRESS (FOR TESTING ONLY – NOT SBC IP)	SBC SUBNET
VIC/TAS	203.52.0.167	203.52.0.161	203.52.0.160 /28
	203.44.42.100	203.44.42.97	203.44.42.96 /28
NSW/ACT	203.52.1.167	203.52.1.161	203.52.1.160 /28
	203.44.42.116	203.44.42.113	203.44.42.112 /28
QLD	203.52.3.164	203.52.3.161	203.52.3.160 /28
	203.44.42.148	203.44.42.145	203.44.42.144 /28
SA/NT	203.44.43.164	203.44.43.161	203.44.43.160 /28
	203.44.42.164	203.44.42.161	203.44.42.160 /28
WA	203.52.2.164	203.52.2.161	203.52.2.160 /28
	203.44.42.132	203.44.42.129	203.44.42.128 /28

For the state where the NTU is homed, the NTU will try any of the addresses listed, so both IP addresses should be allowed through firewalls.

Customer IT staff should allow internet traffic from the relevant SBC IP's to Port 5060 of the Static IP of the WAN side of the NTU to allow call signalling.

Telstra Configuration Servers: (used to get NTU/IAD configuration files)

CONFIGURATION SERVER IP ADDRESS
144.140.208.16 / 29
144.140.208.32 / 28
144.140.162.40 / 29
144.140.162.48 / 28

Devices will not install and will not pick up updated configuration files if these IP's are blocked.

Refer to section 2.2.7 for allowed ports and protocols.

4.1.5. Test for connectivity

A traceroute to these hosts should be performed prior to deployment. The traceroute will only show the first few hops as ICMP is blocked inside the Telstra core. IP routing to these interconnects (POPs) must not occur via the Internet or via third party data-centres.

TELSTRA DNS SERVERS
tracert -d 203.52.0.221
tracert -d 203.52.1.222

TELSTRA CONFIGURATION SERVERS
tracert -d polydms.digitalbusiness.telstra.com

MEDIA INTERCONNECTS
tracert -d sbc-vic.nipt.telstra.com
tracert -d sbc-nsw.nipt.telstra.com
tracert -d sbc-qld.nipt.telstra.com
tracert -d sbc-sa.nipt.telstra.com
tracert -d sbc-wa.nipt.telstra.com

Only test to the state PoP to which the service is homed.

Validate that connectivity is via the IP-VPN SBC's, i.e., to 203.44.x.x or 203.52.x.x. If registration is successful, but connectivity does not exist to the IP-VPN SBC's, then the devices have discovered a route to the TBB SBC's (via NBN, ADSL or Telstra 4G) or to the internet-facing SBC's (via the internet or TID). This is undesirable if the expectation is the customer's IP-VPN is to be employed.

4.1.6. Encryption

Encryption is not available on the IP-VPN SBC's. If an attempt to activate encryption is performed on the Business SIP customer portal then this will force the devices to route to the internet-facing SBC's. If no route exists to the internet-facing SBC's then the devices will not register and the service will not work. Do not activate encryption if IP-VPN operation is required.

4.1.7. VLAN's

TIPT and SIP Connect recommendations include the use of VLAN's to separate voice traffic from data. This enhances voice quality and performance. It is recommended that VLAN separation be employed for Business SIP as well. If doing so, the SIP NTU and IAD WAN ports should be connected to untagged ports.

4.2. Appendix B: References

The following reference documents are available for installation and administration purposes.

DOCUMENT NAME
Business SIP - Installation Guide
Business SIP Portal - Administrator Guide
Business SIP Portal - End User Guide
Business SIP – IAD Installation Guide

Link to documentation repository: http://www.telstra.com/business-sip-support

Link to latest version of this document: Telstra Business SIP - Detailed Integration Guide

4.3. Appendix C: Glossary

The following terms, acronyms and abbreviations are referred to in this document.

TERM	DEFINITION
AS	Application Server
DHCP	Dynamic Host Configuration Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IAD	Integrated Access Device
IP	Internet Protocol
LAN	Local Area Network
NTU	Network Termination Unit
PABX	Private Automated Branch Exchange
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SBC	Session Border Controller
SIP	Session Initiation Protocol
sRTP	Secure Real-time Transport Protocol
TLS	Transport Layer Security
VoIP	Voice over Internet Protocol