SIP Connect Customer Integration Guide

Table of Contents

1. Document Purpose

This document refers to Telstra's "SIP Connect" product and the capability allowing it to be employed over:

- A Telstra IPVPN (MPLS) service
- A Telstra NBN service (using the Telstra Business Broadband product), or
- A Telstra Internet Direct (TID) service, or
- An internet service

They will be referred to as "SIPC on IPVPN", "SIPC on TBB", "SIPC on TID" or "SIPC on Internet" in this document, SIP Connect with ISDN IAD is referred to as "SIP IAD".

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

Note: This document does not constitute a VoIP solution design but serves as a generic reference guide for the adoption of the SIP Connect product and applications within the customer's environment.

Important notes

If migrating from SIP Connect on IP VPN/MPLS, to TBB/TID/Internet, not only do the Outbound Proxy details change but so does DNS. The old DNS will not be accessible – use internet-based DNS servers.

When using an Internet Based Carriage using NATing, you may need to update your NAT IP settings in the PABX/CPE with your Public Internet Static IP to ensure the SIP Contact Header IP & SDP Connection IP's are presented with the correct value.

It is recommended that a Telstra commissioning appointment is made for the time of cutover, to reduce impact of downtime and to help with items such as the aforementioned points. Contact your Telstra representative to arrange a commissioning appointment.

Also, please note that the PABX configuration guides, which are available for all accredited PABX's, should be read in conjunction with this document **(see section 8 for the link).** Due to the nature of the SIP protocol **only accredited IP PBX's can be connected.**

Applicability of SIP Connect variants:

SIP Connect Availability		SIP Connect with ISDN IAD (SIP IAD)	SIP Connect Dedicated (Accredited IPPBX)	Enterprise Trunking (Accredited IPPBX)
Category	Eligible Access Services			
Enterprise Access Service	Telstra IPVPN (Next IP, MPLS)	Yes	Yes	Yes
Internet Access Services	Telstra Internet Direct (TID)	Yes	Yes	Yes
	Telstra Business Broadband (NBN)	Yes	Yes	Yes
	Other Internet Access types	No	Yes	Yes

Important excerpt to note from the "Our Customer Terms" document:

You acknowledge and agree:

a. To get the best out of the Telstra SIP Connect service we recommend use of a Telstra Next IP service.

b. When Telstra SIP Connect service is provided over any other service type, the voice and video quality of a call can be reduced as the service may be impacted by:

   i. Packet loss;
   ii. Variable delay; and
   iii. Variable data throughput rates,

c. The Telstra SIP Connect service will not work if there is an interruption to your underlying Eligible Access Service and as a result you may be unable to dial emergency services numbers such as 000. A Telstra SIP Connect Service over an Internet Access Service is not suitable for people with life threatening medical conditions that require priority assistance.

d. When using the Telstra SIP Connect service over an Internet Access Service:

   i. We recommend that your Internet Access Service provides a minimum of 100Kbps uncontended bandwidth per voice line in each direction to maintain your voice quality; and
   ii. We do not make any guarantees about the quality of your Telstra SIP Connect service experience when used over the Internet or mobile data network.
   iii. All the Voice Packets when traversing via Internet Access Services will be unencrypted, unless special arrangements have been made.

2. Intended Audience

There are two specific targets for this document. The primary audience are:

- Customer Network Administrators
- Customer Authorised Representative
- Customer ICT Managers
- Customer Project Managers
- Telstra Project Managers

The secondary audience are those who will assist the customer representative throughout this process:

- Solution Consultants/Communication Consultant
- UC Sales Specialists/Architects

3. Architectural & Infrastructure Overview

The following section will describe the high-level technology, common infrastructure and architectural touch points for SIP Connect.

At a high-level overview, the End to End Network "Ecosystem" comprises of 4 key areas, listed in order of their logical flow:

1. Customer Premises (including onsite switches, routers, PABX, handset, soft clients, analogue devices)
2. Broadband access service
3. Hosted Infrastructure – Application Servers, Provisioning servers, Firewalls etc.
4. Call Routing/Flow - SBC and Broadsoft softswitch, IMS etc

The following diagrams are labelled TIPT but the same architecture & infrastructure is employed for SIP Connect.

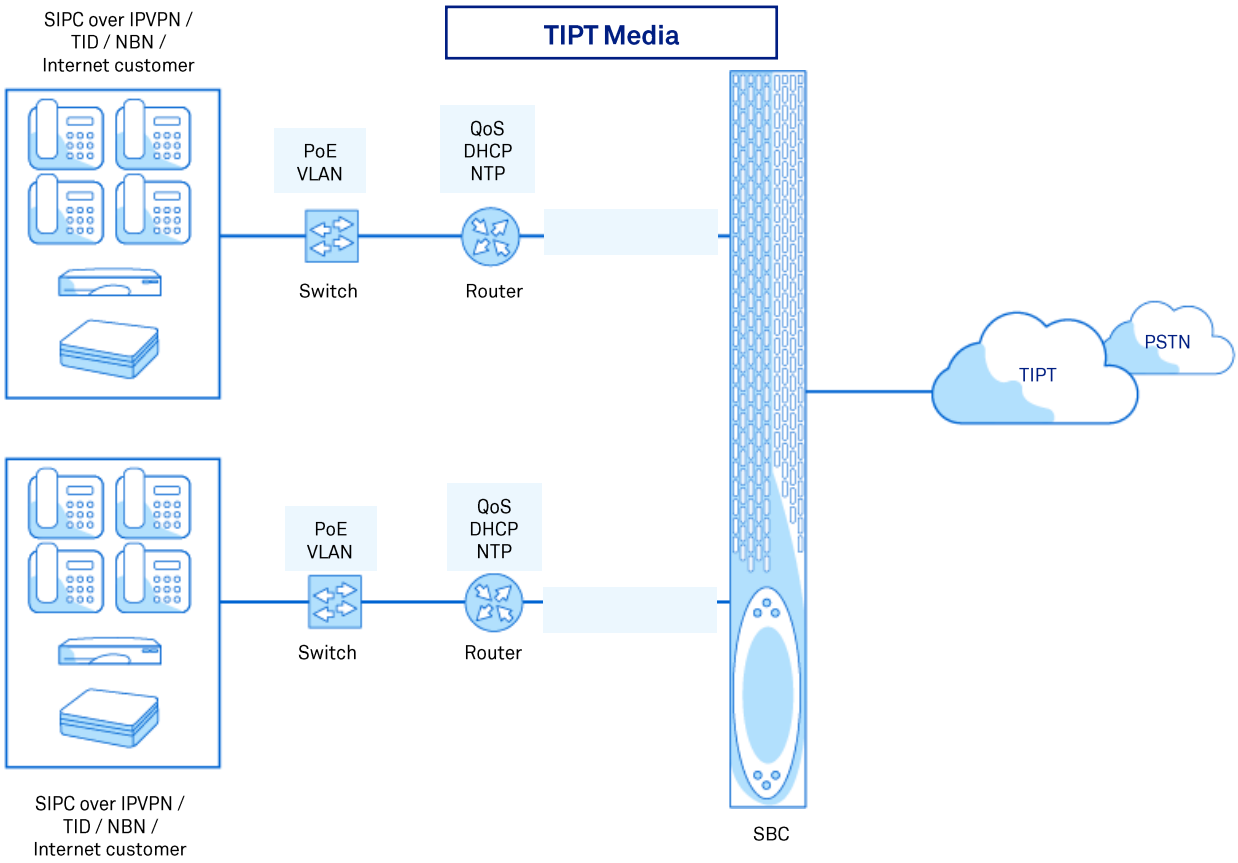


Figure 01: SIPC Media Interconnect High Level Network Diagram

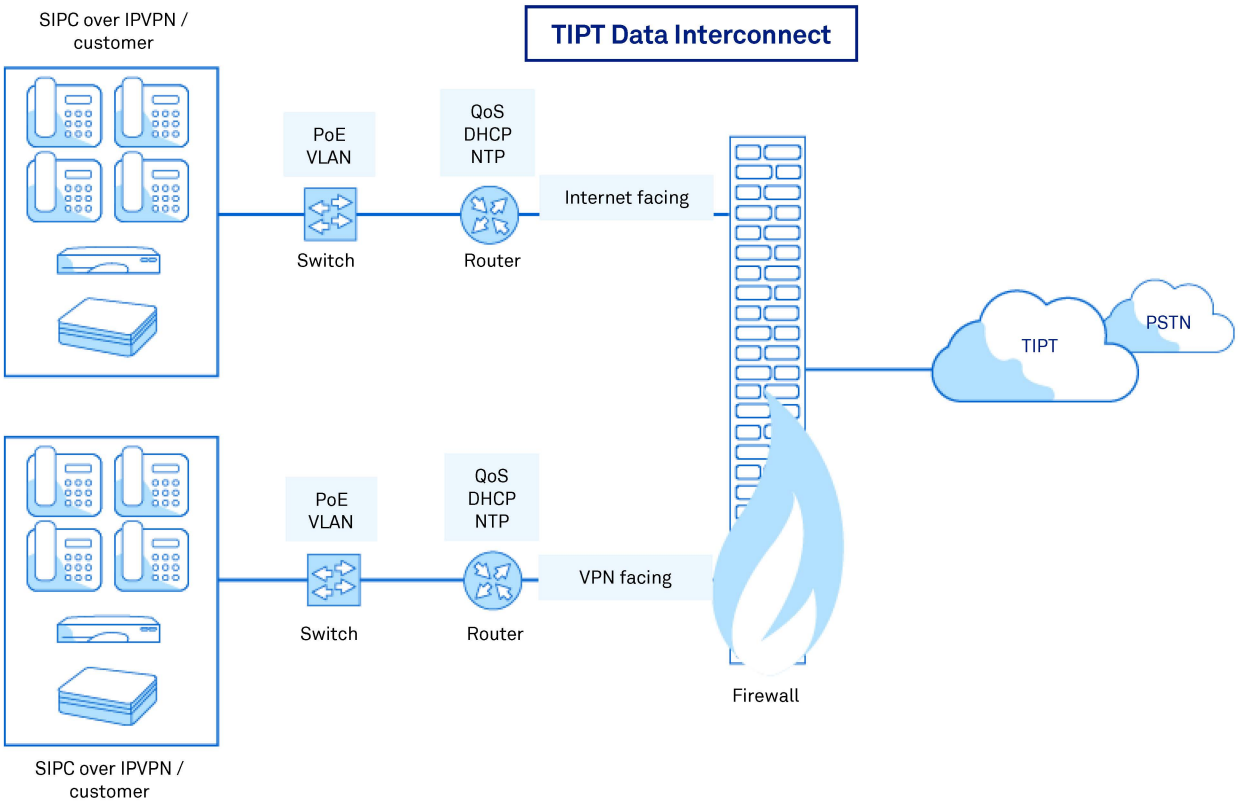


Figure 02: SIPC Data Interconnect High Level Network Diagram (IPVPN only)

4. Scalability & traffic type

The Core SBC's used by SIPC Over Internet / TID and SIPC Over TBB have extra controls in place to protect against Denial Of Service or similar attacks. This results in scalability limits for calls appearing to be emanating from the same Public IP address. This is not an issue for SIPC Over IPVPN as those PoP's do not have public accessibility.

The limit per Public IP address is 1,000 concurrent calls.

There are situations where multiple trunk groups may emanate from a single Public IP address to the one Telstra core SBC, and in these instances, combined capacity of the multiple trunk groups must be no more than 1,000 concurrent calls.

Traffic must be normal business traffic with average holding times of 120 seconds or greater.
High intensity traffic such as automated outbound calling campaigns and radio station competitions are not supported.

Failure to observe these restrictions may result in traffic being suspected as being faulty or malicious which would then cause calls to be automatically blocked.

5. IP Routing

SIP Connect is enabled by a range of applications and network structures.

For your SIP Connect service to work, your PABX or SIP IAD need to be able to access those structures. Your network may need to be modified to be able to send information to, and receive information from, the subnets within these structures.

The customer must be able to route to these networks to reach the TIPT platform. IP routing can be configured via static or dynamic routing protocols at the customer edge device (BGP is preferred).

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.

The following table shows the subnet accesses that are required for SIP Connect.

Interconnects	Configuration	Description
SIPC/SIP IAD Over IPVPN (Next IP / MPLS) Customers		
Data interconnects	203.52.0.0/23	VIC and NSW DNS
	144.140.208.16/29	SIP IAD Configuration servers
	144.140.162.40/29	
Signalling & Media interconnects (as required)	203.52.0.160/28	VIC – SBC 1
	203.44.42.96/28	VIC – SBC 2
	203.52.1.160/28	NSW/ACT – SBC 1
	203.44.42.112/28	NSW/ACT – SBC 2
	203.52.3.160/28	QLD – SBC 1
	203.44.42.144/28	QLD – SBC 2
	203.44.43.160/28	SA/NT – SBC 1
	203.44.42.160/28	SA/NT – SBC 2
	203.52.2.160/28	WA – SBC 1
	203.44.42.128/28	WA – SBC 2

SIPC Over Internet / TID Customers		
Signalling & Media interconnects (as required)	192.148.164.24/32	SA Internet facing – Unencrypted
	192.148.164.8/32	VIC Internet facing – Unencrypted
SIPC/SIP IAD Over TBB Customers		
Data interconnects	144.140.208.16/29	SIP IAD Configuration servers
	144.140.162.40/29	
Signalling & Media interconnects (as required)	203.41.24.0/24	VIC / NSW / QLD / WA DOT SBC's – Unencrypted
	203.41.29.0/24	SA DOT SBC – Unencrypted

Outbound Proxy / Core SBC addressing – SIPC over IPVPN

Telstra Core SBC's are positioned between the customer network and the TIPT core. They provide firewalling features and a logical separation between the networks. The SBC is treated as the SIP Server from the perspective of the PBX Gateway instead of the actual BroadWorks application server.

As part of Telstra's geo-redundancy network plan, 2 SBCs are available in each state. Care must be taken when configuring the customer CPE to ensure that the correct SBC FQDNs are entered to ensure the best possible SBC redundancy is available.

In all cases the SBC address MUST be entered as an FQDN, not an IP address.

Telstra DNS servers for IPVPN customers:

Primary 203.52.0.221
Secondary 203.52.1.222

SIP Connect Dedicated & Enterprise trunk - Single Trunk Registration:

Use the appropriate state SBC FQDN for the Outbound Proxy setting.

State	SBC FQDN	SBC IP	Ping-able Address
VIC and TAS	sbc-vic.nipt.telstra.com	203.52.0.167	203.52.0.161
NSW and ACT	sbc-nsw.nipt.telstra.com	203.52.1.167	203.52.1.161
QLD	sbc-qld.nipt.telstra.com	203.52.3.164	203.52.3.161
SA and NT	sbc-sa.nipt.telstra.com	203.44.43.164	203.44.43.161
WA	sbc-wa.nipt.telstra.com	203.52.2.164	203.52.2.161

SIP Connect Enterprise Trunk – Multiple Trunk Registration:

Use the appropriate state SBC FQDNs 1 and 2 for each trunk in the Enterprise Trunk configuration. Incoming call will be distributed across both SBCs within the state depending on the Enterprise Trunk routing configuration, outgoing call distribution is handled by the customer CPE configuration.

State	SBC Pair No.	SBC FQDN	SBC IP	Ping-able Address
VIC/TAS	1	sbc-vic-1.nipt.telstra.com	203.52.0.167	203.52.0.161
	2	sbc-vic-2.nipt.telstra.com	203.44.42.100	203.44.42.97
NSW/ACT	1	sbc-nsw-1.nipt.telstra.com	203.52.1.167	203.52.1.161
	2	sbc-nsw-2.nipt.telstra.com	203.44.42.116	203.44.42.113
QLD	1	sbc-qld-1.nipt.telstra.com	203.52.3.164	203.52.3.161
	2	sbc-qld-2.nipt.telstra.com	203.44.42.148	203.44.42.145
SA/NT	1	sbc-sa-1.nipt.telstra.com	203.44.43.164	203.44.43.161
	2	sbc-sa-2.nipt.telstra.com	203.44.42.164	203.44.42.161
WA	1	sbc-wa-1.nipt.telstra.com	203.52.2.164	203.52.2.161
	2	sbc-wa-2.nipt.telstra.com	203.44.42.132	203.44.42.129

Outbound Proxy / Core SBC addressing – SIPC over Internet / TID

IP-PBX's require configuration to enable connectivity to the Telstra Session Border Controllers (SBC's), also known as outbound proxy.

It is required that DNS look-up is employed by the IP-PBX to discover the appropriate Outbound Proxy IP addresses. Use the Fully Qualified Domain Names (FQDN's) as shown in the table below. There is no special DNS server requirement for these SBC FQDN's, so standard DNS servers can be used to resolve them.

Examples of some common DNS sites:

Google	8.8.8.8	8.8.4.4
Cloudflare	1.1.1.1	1.0.0.1
Quad9	9.9.9.9	149.112.112.112
OpenDNS	208.67.222.222	208.67.220.220

Sites converting from IPVPN must also change DNS servers to public DNS servers, such as TBB / TID / Google servers, as the TIPT DNS servers are only reachable via IPVPN.

There are two POP's available. If multiple trunk groups are being configured then distribute the registrations over the two POP's. The .8 PoP is VIC and the .24 PoP is SA.

State	SBC Pair No.	SBC FQDN	SBC IP	Ping-able Address
VIC/TAS	1	eims-asd-201and202-trunk.business.connect.telstra.com	192.148.164.8	192.148.164.1
	2	im8a-asd-201and202 trunk.business.connect.telstra.com	192.148.164.24	192.148.164.17
NSW/ACT	1	eims-asd-201and202-trunk.business.connect.telstra.com	192.148.164.8	192.148.164.1
	2	im8a-asd-201and202-trunk.business.connect.telstra.com	192.148.164.24	192.148.164.17
QLD	1	eims-asd-201and202-trunk.business.connect.telstra.com	192.148.164.8	192.148.164.1
	2	im8a-asd-201and202-trunk.business.connect.telstra.com	192.148.164.24	192.148.164.17
SA/NT	1	im8a-asd-201and202-trunk.business.connect.telstra.com	192.148.164.24	192.148.164.17
	2	eims-asd-201and202-trunk.business.connect.telstra.com	192.148.164.8	192.148.164.1
WA	1	im8a-asd-201and202-trunk.business.connect.telstra.com	192.148.164.24	192.148.164.17
	2	eims-asd-201and202-trunk.business.connect.telstra.com	192.148.164.8	192.148.164.1

Outbound Proxy / Core SBC addressing – SIPC over Internet / TID encrypted

Only PBXs that have been accredited through the SIP Connect vendor self-accreditation programme can employ encryption.

IP-PBX's require configuration to enable connectivity to the Telstra Session Border Controllers (SBC's), also known as outbound proxy.

It is required that DNS look-up is employed by the IP-PBX to discover the appropriate Outbound Proxy IP addresses. Use the Fully Qualified Domain Names (FQDN's) as shown in the table below. There is no special DNS server requirement for these SBC FQDN's, so standard DNS servers can be used to resolve them.

Examples of some common DNS sites:

Google	8.8.8.8	8.8.4.4
Cloudflare	1.1.1.1	1.0.0.1
Quad9	9.9.9.9	149.112.112.112
OpenDNS	208.67.222.222	208.67.220.220

Sites converting from IPVPN must also change DNS servers to public DNS servers, such as TBB / TID / Google servers, as the TIPT DNS servers are only reachable via IPVPN.

There are two POP's available. If multiple trunk groups are being configured then distribute the registrations over the two POP's. The .8 PoP is VIC and the .24 PoP is SA.

State	SBC Pair No.	SBC FQDN	SBC IP	Ping-able Address
VIC/TAS	1	eims-asd-201and202.itrunk.business.connect.telstra.com	192.148.164.7	192.148.164.1
	2	im8a-asd-201and202.itrunk.business.connect.telstra.com	192.148.164.23	192.148.164.17
NSW/ACT	1	eims-asd-201and202.itrunk.business.connect.telstra.com	192.148.164.7	192.148.164.1
	2	im8a-asd-201and202.itrunk.business.connect.telstra.com	192.148.164.23	192.148.164.17
QLD	1	eims-asd-201and202.itrunk.business.connect.telstra.com	192.148.164.7	192.148.164.1
	2	im8a-asd-201and202.itrunk.business.connect.telstra.com	192.148.164.23	192.148.164.17
SA/NT	1	im8a-asd-201and202.itrunk.business.connect.telstra.com	192.148.164.23	192.148.164.17
	2	eims-asd-201and202.itrunk.business.connect.telstra.com	192.148.164.7	192.148.164.1
WA	1	im8a-asd-201and202.itrunk.business.connect.telstra.com	192.148.164.23	192.148.164.17
	2	eims-asd-201and202.itrunk.business.connect.telstra.com	192.148.164.7	192.148.164.1

Outbound Proxy / Core SBC addressing – SIPC/SIP IAD over TBB

IP-PBX's require configuration to enable connectivity to the Telstra Session Border Controllers (SBC's), also known as outbound proxy.

It is required that DNS look-up is employed by the IP-PBX to discover the appropriate Outbound Proxy IP addresses. Use the Fully Qualified Domain Names (FQDN's) as shown in the table below. There is no special DNS server requirement for these SBC FQDN's, so standard DNS servers can be used to resolve them.

Examples of some common DNS sites:

Google	8.8.8.8	8.8.4.4
Cloudflare	1.1.1.1	1.0.0.1
Quad9	9.9.9.9	149.112.112.112
OpenDNS	208.67.222.222	208.67.220.220

Sites converting from IPVPN must also change DNS servers to public DNS servers, such as TBB / TID /Google servers, as the TIPT DNS servers are only reachable via IPVPN.

There are two POP's available per state. If multiple trunk groups are being configured then distribute the registrations over the two POP's.

State	SBC Pair No.	SBC FQDN	SBC IP	Ping-able Address
VIC/TAS	1	eims-asd-003and004 trunk.business.connect.telstra.com	203.41.24.4	203.41.24.1
	2	vims-asd-003and004-trunk.business.connect.telstra.co m	203.41.24.36	203.41.24.33
NSW/ACT	1	im2k-asd-011and012-trunk.business.connect.telstra.com	203.41.24.68	203.41.24.65
	2	im2t-asd-011and012-trunk.business.connect.telstra.com	203.41.24.100	203.41.24.97
QLD	1	im7w-asd-003and004-trunk.business.connect.telstra.com	203.41.24.132	203.41.24.129
	2	im7h-asd-001and002-trunk.business.connect.telstra.com	203.41.24.164	203.41.24.161
SA/NT	1	im8a-asd-001and002-trunk.business.connect.telstra.com	203.41.29.4	203.41.29.1
	2	im8e-asd-001and002-trunk.business.connect.telstra.com	203.41.24.196	203.41.24.193
WA	1	im8e-asd-001and002-trunk.business.connect.telstra.com	203.41.24.196	203.41.24.193
	2	im8a-asd-001and002-trunk.business.connect.telstra.com	203.41.29.4	203.41.29.1

6. LAN Environment

LAN & Internal Cabling

As a rule, the customer's LAN environment (routers/desktops and end points) must have structured cabling of CAT5e or better, though (CAT 6) is recommended in order to support TIPT for voice, data and video transmission. All cabling including network patching is the responsibility of the customer and must be completed prior to the deployment of the SIP Connect solution.

SIP IAD or Analogue TIPT IAD (for fax) DHCP requirements

The SIP IAD solution requires a DHCP server assigned address, static IP configuration is not supported. As the SIP IAD can require specific DNS servers (in the case of IPVPN), specific DHCP boot server options and QoS policy. Often this is best achieved using a separate VLAN and/or a specific scope for this device. A long lease time is also recommended to avoid unnecessary DHCP renewals. See example below for requirements (options 42, 66 and 160). Also note if your SIPC solution includes a TIPT based analogue IAD (for fax) this DHCP configuration is also required.

```
ip dhcp pool SIPIAD_VLAN
   network 172.16.200.0 255.255.255.0
   default-router 172.16.200.1
   dns-server 203.52.0.221 203.52.1.222
   option 42 ip 172.16.200.1
   option 66 ascii dms.digitalbusiness.telstra.com
   option 160 ascii http://polydms.digitalbusiness.telstra.com/dms/bootstrap
   lease 7
```

WAN Router

WAN router must be designed and configured with a suitable QoS policy to categorise and prioritise VoIP traffic to ensure Grade of Service. A LAN design must be undertaken to ensure that the converged solution meets IP telephony requirements. Site documentation (e.g. network diagrams) should be updated to support the IP telephony solution.

For SIP Connect customers connecting over the internet, QoS is not mandatory, however a separate prioritised voice VLAN should be implemented where possible.

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 all recommendation for all cases, but the following table has some examples and suggested steps when using different types of routers. Remote administration applies only to the SIP IAD, where Telstra assurance personnel may need access to the device remotely.

Example	Router/Gateway	SIP IAD Gets Config OK	SIP IAD/IP PBX Registers OK	Two Way Speech for Voice Calls Ok	SIP IAD 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 uPNP is preconfigured
2	Generic Router	Y	Y	Y	N	Enable uPNP or configure Remote administration (as per 3.2.12)
3	Generic Router	Y	N	N	N	Disable SIP ALG + Add Port Forwarding (as per 3.2.11) + Configure Remote administration (as per 3.2.12) or Enable uPNP for Remote admin
4	Generic Router	Y	Y	N	N	Enable SIP ALG + uPnP + Add Port Forwarding (as per 3.2.11) + Configure Remote administration (as per 3.2.12)

SDWAN

If using SDWAN, need to make sure the SDWAN design routes natively into underlay, i.e. allows MPLS native access for SIP Connect.© Telstra Corporation Limited (ABN 33 051 775 556) 2022. All rights reserved. SIP Connect Customer Integration Guide, Feb 22 13

If it is a mix of SDWAN and MPLS, make sure the routing is in place from SDWAN site to the remaining MPLS sites. This needs to be confirmed with the Telstra Project delivery team.

4G Access

Telstra doesn't recommend consumer-grade 4G devices, If there is no choice then make sure:

- The device is placed in the best location for 4G signal
- Any sleep functions are deactivated

Firewall and Ports

The use of customer firewalls (or NAT devices) to limit Voice Traffic - SIP (signalling) and dynamic RTP (Media) is not recommended and should be avoided. VoIP firewall traversal has the potential to impact performance (voice quality due to additional network delay) and service quality. If a firewall must be employed, refer to the following tables.

For SIP IAD over TBB, for Telstra staff connectivity to the SIP IAD, customer IT staff should allow inbound access to the device from the listed source IP addresses to the LAN IP address of the SIP IAD.

Service	Protocol	Port	Remote admin IP address
SSH HTTPS	TCP TCP	22 443	203.35.135.0 / 24 203.35.82.0 / 24 203.213.78.50

Service	Protocol	Destination Port	Description	IP ranges	Comment	In bound	Out bound
SIPC/SIP IAD over IPVPN (MPLS/Next IP)							
SIP RTP	UDP UDP	5060 Dynamic (16384-32767)	Signalling protocol used by IP PBX's and IAD's. Real-time Transport Protocol (Media) used to deliver audio between VoIP endpoints	203.52.0.160/28 203.44.42.96/28	VIC – SBC 1 VIC – SBC 2	Yes	Yes
				203.52.1.160/28	NSW – SBC 1		
				203.44.42.112/28	NSW – SBC 2		
				203.52.3.160/28	QLD – SBC 1		
				203.44.42.144/28	QLD – SBC 2		
				203.44.43.160/28	SA – SBC 1		
				203.44.42.160/28	SA – SBC 2		
				203.52.2.160/28	WA – SBC 1		
				203.44.42.128/28	WA – SBC 2		
DNS	UDP/ TCP	53	Used for Name Resolution via TIPT DNS servers	203.52.0.221 203.52.1.222	DNS SERVERS	Yes (return traffic)	Yes Yes
HHTTP/ HTTPS	TCP	80,443	SIP IAD configuration files for the Device	144.140.208.16/29	Exhibition St – TIPT DMS	Yes (return traffic)	Yes
				144.140.162.40/29	Pitt St – TIPT DMS		

			Management Solution				
SIPC over Internet/TID							
SIP	UDP	5060	Signalling protocol used by IP PBX's and IAD's. Real-time Transport Protocol (Media) used to deliver audio between VoIP endpoints Secure encrypted signalling protocol used by IP PBX's	192.148.164.23 /32	SA - Internet facing SBC – Encrypted	Yes	Yes
				192.148.164.24/32	SA - Internet facing SBC – Unencrypted		
RTP	UDP	Dynamic (16384-32767)		192.148.164.7/32	VIC Internet facing SBC – Encrypted		
SIP TLS	TCP	5061		192.148.164.8/32	VIC Internet facing SBC – Unencrypted		
DNS	UDP/TCP	53	Used for Name Resolution via Internet DNS servers	Any internet DNS	DNS SERVERS	Yes (return traffic)	Yes
SIPC/SIP IAD over TBB							
SIP	UDP	5060	Signalling protocol used by IP PBX's and IAD's.	203.41.24.0/24	VIC / NSW / QLD / WA SBC's	Yes	Yes
RTP	UDP	Dynamic (16384-32767)	Real-time Transport Protocol (Media) used to deliver audio between VoIP endpoints	203.41.29.0/24	SA SBC		
DNS	UDP/TCP	53	Used for Name Resolution	Any internet DNS	DNS SERVERS	Yes (return traffic)	Yes

			via Internet DNS servers				
HTTP/HTTPS	TCP	80, 443	SIP IAD configuration files for the Device Management Solution	144.140.208.16/29 144.140.162.40/29	IAD Configuration server	Yes (return traffic)	Yes

SIP ALG

What is SIP ALG?

SIP (Session Initiation Protocol) ALG (Application Layer Gateway) is an application within many routers. It inspects any VoIP traffic to prevent problems caused by firewalls and if necessary, modifies the VoIP packets. Routers will often have SIP ALG activated by default.

What problems can SIP ALG cause?

This can stop your TIPT Voice devices from:

- Registering on the service
- Making outgoing calls
- Receiving incoming calls
- and, can cause voice quality issues

In most cases where a SIP ALG is present in a router/firewall it is best for this to be disabled..

Quality of Service

Quality of Service (QoS) is the ability to provide differential levels of treatment to specific classes of traffic. This traffic, being voice, video or data, must be identified and sorted into different classes to which differential treatment is applied.

Implementation of a network wide QoS design on site switches and routers is recommended to ensure that voice receives prioritisation within the Local Area Network.

For SIPC over IPVPN, implementation of Telstra's IP MAN/IP WAN Dynamic CoS will ensure that voice receives prioritisation within the Wide Area Network and that network congestion is obviated through the implementation of techniques such as "Egress Queuing".

A Quality of Service Policy will address the key issues of:

- Classification and Marking
- Congestion Management
- Congestion Avoidance
- Traffic Policing and Shaping, and
- Link Efficiency

In order to provide an enterprise grade of service for SIPC over IPVPN, the customer's network must support end-to-end QoS. The WAN edge router must be configured to categorise and prioritise VoIP traffic accordingly.

Differentitated Service (DSCP)	Class of Service (COS)	Value	Queuing Method
EF	5	RTP Audio	Bandwidth allocation

			Strict Priority Queuing (LLQ)
AF (31) Video Endpoints	3	RTP Video H.264	Bandwidth %
CS3	3	SIP (Signalling), RTCP	Bandwidth %
BE (0)	0	Other (that is: DNS, HTTP(s), FTP, TFTP)	

Bandwidth:

Although there is no set bandwidth that is mandated the customer will still need to ensure there is enough WAN link bandwidth available for SIPC traffic. As a guide customers should nominally base their total voice bandwidth requirement around the 30% mark.

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

Where a TBB Voice Priority Pack or TBB Dedicated Data Pack is to be employed, use the following guidelines:

> TBB Voice Priority Pack: These packs are designated by concurrent call capacity, e.g. VPP10 provides up to 10 concurrent calls. It is not necessary to do any bandwidth calculations. Simply ensure the SIP Connect concurrent calls purchased is equal to or less than the purchased Voice Priority Pack.
>
> TBB Dedicated Data Pack: These packs are not designated by concurrent call capacity. They are designated as either “S”, “M” or “L”. Assume “S” (9Mbps) provides up to 90 concurrent calls, “M” (18Mbps) provides 180 and “L” (45Mbps) provides 450. As these are based on typical speeds is would be prudent to provide a safety buffer of 20%, i.e., “S” = 72 concurrent calls, “M” = 144 concurrent calls and “L” = 360. Ensure the SIP Connect concurrent calls purchased is equal to or less than these values.

Wireless access:

It is recommended that wireless, e.g. NBN Fixed Wireless or Satellite, is not employed due to the unreliable nature of radio technology.

Remote administration

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

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

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

For example (see Figure below), if the IP address of the SIP IAD was 192.168.190.2, then the port forwarding rule becomes:

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

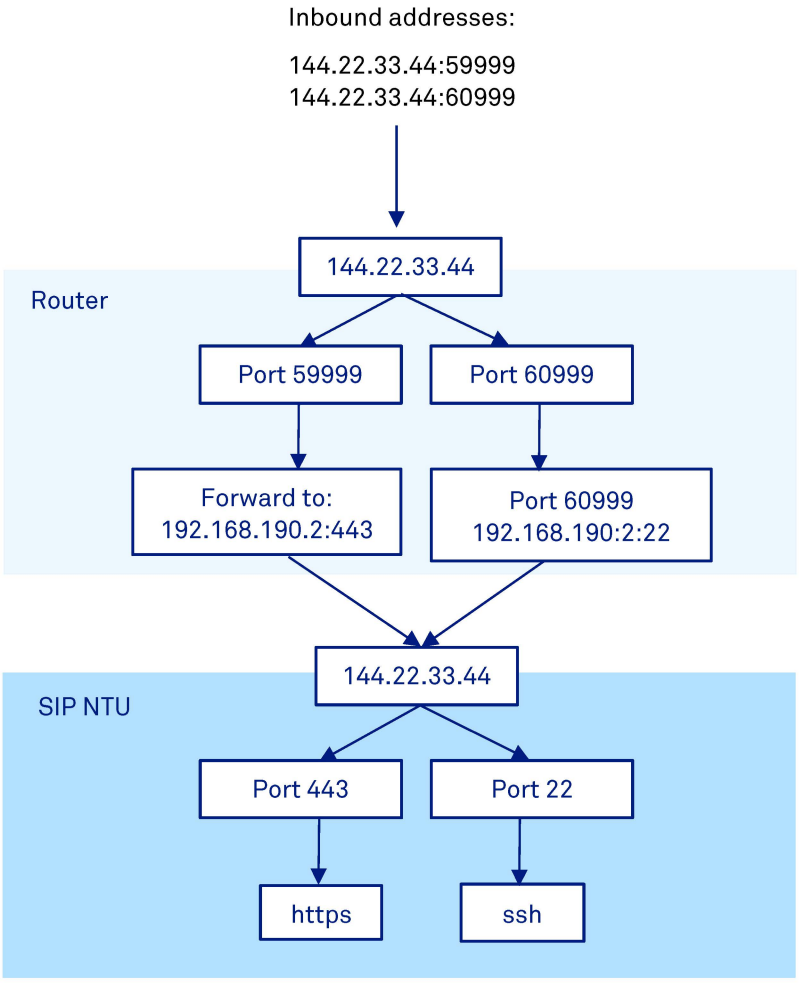
TCP traffic inbound to port 60999, forward to 192.168.190.2:22

It is highly recommended that a static DHCP lease be assigned to the SIP IAD 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 IAD 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 IAD 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 IAD IP Address, port 443

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



7. Supplementary Information

Telstra UC Self-service portal

Telstra's UC Self-Service Portal for TIPT and SIP Connect customers allows customers to submit change requests that will be implemented in near real-time!

https://ucp.tipt.telstra.com/

The UC Self Service Portal allows:

SIP Connect:

- Manage channel capacity on both Enterprise and Standard SIP Connect Trunks
- Increase capacity in near real time

Manage Business Connect:

- Assign the Business Connect soft client to any users in your group that has a standard or an executive pack but has not had Business Connect assigned

Malicious Call Trace

SIP Connect customers can initiate a "Customer Originated Trace (COT)" from a "handset" for MCT purposes, on the last incoming answered or unanswered (abandoned during ring) call received, by:

- If the incoming call was answered, they must go on-hook to end the call (hang up) or if the "Unwelcome call" was unanswered
- Then go off-hook (before a subsequent call 'ring' is received)
- At dial tone, enter the *57 Feature Activation Code (FAC).
- Then they will receive an RVA from the network stating that a trace has been performed on the last incoming call.
- They should also manually record the date, time & duration of the call

Note: It is also necessary that the customer PBX must have been pre-configured to pass any *57 Feature Activation code to the Telstra application server.

Initiation of the *57 Feature Activation Code (FAC) for COT, will result in the Telstra application server generating several data records which will be accessible to the Telstra Trace Control Centre & National Unwelcome Call Centre.

8. Useful links

Description	URL/Link
AMC Portal	**https://ucp.tipt.telstra.com/login**
Liberate Portal	**https://liberate.telstra.com/login**
TIPT Guides & Docs	**https://enterprise-support.telstra.com.au/t5/Telstra-IP-Telephony-TIPT/ct-p/TIPT**
SIPC Guides, Docs & Accreditation	**https://partners.enterprise.telstra.com.au/s/**

9. Glossary

The following words, acronyms and abbreviations are referred to in this document:

Term	Definition
BEM	Backlit Expansion Module
CAP	Client Access Protocol
CDP	Cisco Discovery Protocol
CIP	Connect IP
CoS	Class of Service
DHCP	Dynamic Host Configuration Protocol
DMS	Device Management Solution
DNS	Domain Name Services
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IAD	Integrated Access Device
IP	Internet Protocol
IP MAN	Internet Protocol Metropolitan Area Network
IP WAN	Internet Protocol Wide Area Network

LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MWAN	Managed Wide Area Network
NIPT	Network Internet Protocol Telephony
NTP	Network Time Protocol

10. Customer Support

For How-to support the How-to Help Desk can be contacted on **1800 648 116**

Telstra IP Telephony Helpdesk - **1800 287 289**

For escalations Contact your **Telstra Account Executive**