



Adaptive Collaboration: Telstra Cloud Calling Integration Guide

September 2024



Table of Contents

Document Purpose	3
Intended Audience	3
Product Description	3
Product Variance	4
Architectural & Infrastructure Overview	4
IP Routing	5
LAN Environment	6
LAN & Internal Cabling	6
WAN Router	6
SD-WAN	6
LAN Switch	6
Power over Ethernet	7
Network Time Protocol	7
DHCP Server	7
DNS Server	7
Web Proxy (Caching) Server	8
Firewall and Ports	8
SIP ALG	10
Quality of Service	10
CPE Guide	11
Supplementary Information	12
Supported Codecs for Adaptive Collaboration: Telstra Cloud Calling	12
Troubleshooting & Quick tips	12
Device Management Platform (Provisioning server)	12
Connectivity test	
Glossary	13
Customer Support	13

Document Purpose

This document is designed to assist you with your Adaptive Collaboration: Telstra Cloud Calling integration and deployment activities.

Note: This document does not constitute the Telstra Cloud Calling solution design but serves as a generic reference guide for adopting Telstra Cloud Calling and applications within your environment.

Intended Audience

There are two specific targets for this document. The primary audience is those who will need to read, acknowledge acceptance and compliance for the sections noted in this document.

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

The Secondary audience is those who will assist you, representative, throughout this process.

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

Product Description

Adaptive Collaboration: Telstra Cloud Calling is a hosted telephony and UC application that requires access to users and devices on your network to work.

Handsets and other unified communications equipment require connectivity to your network or the internet using suitable internet access. Your Telstra MPLS or Internet access should already be in place before you attempt to set up your equipment.

Your network needs to be configured to be able to support Telstra Cloud Calling. Your network may be provided by Telstra or a third-party Internet provider. This guide provides high-level configuration requirements for networks to support Telstra Cloud Calling.

Given that there are many possible network service and equipment providers, this guide does not provide lower-level network equipment configuration details.

The Telstra Cloud Calling solution aims to deliver a full set of unified communication and collaboration services, including:



Voice



Video



Voicemail



Presence & Instant Messaging (Webex)



Compatible Mobility Services (Webex App on Mobile and Tablet)

Product Variance

Adaptive Collaboration: Telstra Cloud Calling is access agnostic. However, your network and equipment may need to be configured depending on your network access service, i.e. Telstra MPLS, Telstra Internet or the 3rd-party internet access.

Architectural & Infrastructure Overview

The following section will describe the high-level technology, common infrastructure, and architectural touchpoints for Telstra Cloud Calling – it is not designed to provide a complete detailed view of the Telstra Cloud Calling components.

At a high level, the end-to-end network “ecosystem” is comprised of 4 key areas, listed in order of their logical flow:

-  Customer Site (including onsite switches, routers, voice gateway, handsets, soft clients, and analogue devices)
-  Network Access – Telstra MPLS, Telstra Internet, 3rd-party internet access
-  Hosted Infrastructure – Application Servers, Provisioning Servers, Firewalls.
-  Call Routing/Flow – Session Border Controller (SBC) and BroadWorks Soft Switch.

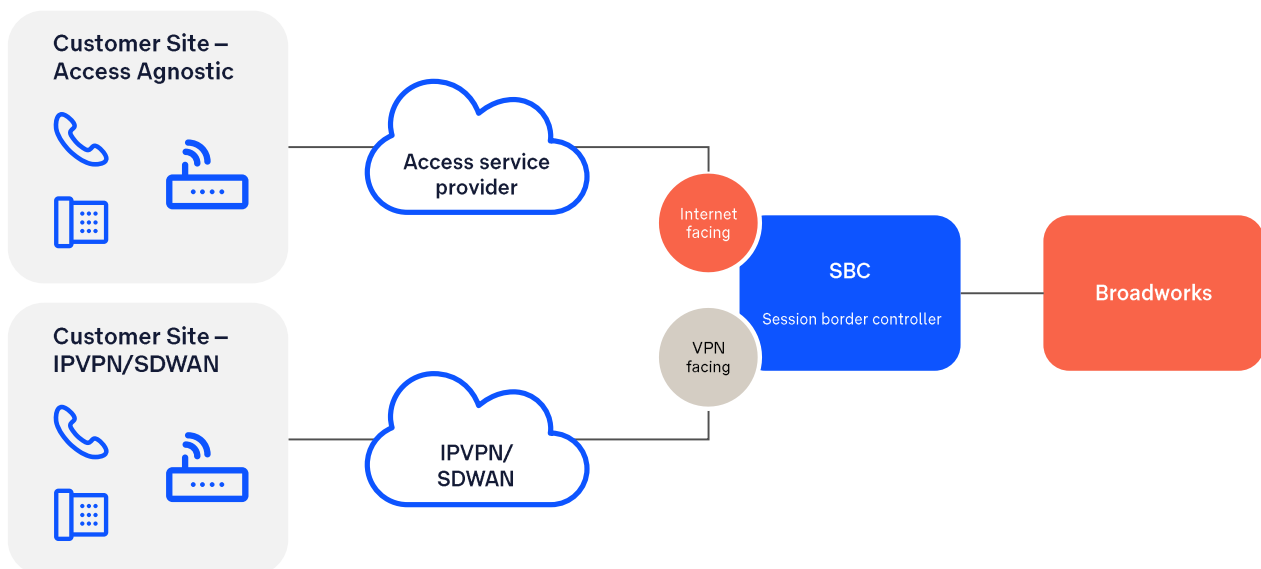


Figure 1: High-Level Network Architecture

IP Routing

Adaptive Collaboration: Telstra Cloud Calling is enabled by various applications and network structures.

For your Telstra Cloud Calling service to work, your devices (including softphones) need to be able to access those structures. Your network must be modified to be able to send information to, and receive information from, these subnets.

You must be able to route to these networks to reach the Telstra Cloud Calling platform.

IP routing can be configured via static or dynamic routing protocols at your edge device (BGP is preferred).

A **traceroute** to these hosts should be performed before 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 Telstra Cloud Calling.

Interconnects	Configuration	Description
All access types		
Data interconnects (Mandatory)	144.140.208.16/28	Device Management (DMS)
	144.140.208.32/28	Device Management (DMS)
	144.140.162.40/28	Device Management (DMS)
	144.140.162.48/28	Device Management (DMS)
	144.140.218.96/28	NSW – XSP Servers
	144.140.224.32/28	VIC – XSP Servers
Telstra MPLS access		
Data interconnects (Mandatory)	203.52.0.0/23	VIC & NSW – DNS
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 – 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
Telstra Internet access		
Media interconnects (As required)	192.148.131.103/32	NSW – SBC 1
	192.148.131.119/32	NSW – SBC 2
	192.148.131.135/32	QLD – SBC 1
	192.148.131.148/32	QLD – SBC 2
	192.148.131.164/32	WA – SBC 1
	192.148.131.196/32	SA – SBC 1

	192.148.131.71/32	VIC – SBC 1
	192.148.131.87/32	VIC – SBC 2
3rd-party internet access		
	192.148.164.20/32	SA - SBC1
Media interconnects (As required)	192.148.164.24/32	SA - SBC2
	192.148.164.4/32	VIC - SBC1
	192.148.164.8/32	VIC - SBC2

LAN Environment

LAN & Internal Cabling

As a rule, your LAN environment (routers/desktops and endpoints) must have structured cabling of CAT5e or better. However (CAT 6) is recommended to support Telstra Cloud Calling for voice, data, and video transmission. All cabling, including network patching, is your responsibility and must be completed before deploying Telstra Cloud Calling.

WAN Router

WAN router must be designed and configured with a suitable QoS policy to categorise and prioritise VoIP traffic to maintain Grade of Service. A LAN design must be undertaken so that the converged solution meets Adaptive Collaboration: Telstra Cloud Calling requirements. Site documentation (e.g. network diagrams) should be updated to support the IP Telephony solution.

For Telstra Cloud Calling customers connecting over the internet, QoS is not mandatory. However, a separate prioritised voice VLAN should be implemented where possible.

SD-WAN

If using SD-WAN, make sure the SD-WAN design routes natively into underlay, i.e. allows MPLS native access for Telstra Cloud Calling.

Using a mix of SD-WAN and MPLS, make sure the routing is in place from SD-WAN sites to the remaining MPLS sites. This needs to be confirmed with the Telstra Project delivery team.

LAN Switch

IP Telephony enabled LAN switches supporting VLANs, IEEE802.1Q (VLAN Tagging), IEEE 802.3af (Power over Ethernet), Quality of Service (QoS) must be used. VLAN segmentation is required to allow prioritisation of voice traffic. VLAN ID 100 is recommended as the Voice VLAN to achieve configuration consistency across all sites.

The key benefits of having separate data and voice VLAN's are:



Logical separation of the network



Broadcast packets from the data network are not sent to the voice network



Easier to implement Access Control Lists



Provides a control point for management traffic

In a Cisco LAN switch environment, with CDP enabled, the VLAN assignment is automatic.

In a non-Cisco LAN switch environment, the voice VLAN ID will need to be manually configured unless the IP device supports LLDP.

Note: All our Telstra devices support LLDP, so LLDP will need to be configured on the switch.

Power over Ethernet

IP Telephony enabled LAN switches supporting VLANs, IEEE802.1Q (VLAN Tagging), IEEE 802.3af (Power over Ethernet), Quality of Service (QoS) must be used. VLAN segmentation is required to allow prioritisation of voice traffic. VLAN ID 100 is recommended as the Voice VLAN to achieve configuration consistency across all sites.

Network Time Protocol

Defining an NTP source is critical for displaying the correct time and date on the devices, for certificate validation, obtaining device configurations, and delivering firmware updates.

The NTP source can be specified using DHCP Option 42 and sourced from the following location:

- <https://www.pool.ntp.org/zone/au>.

DHCP Server

All Telstra Cloud Calling customers are required to provide their own DHCP server to facilitate the assignment of IP addresses to the endpoints for connectivity to UC applications.

The DHCP server used for the Telstra Cloud Calling Voice VLANs (local or centralised) at each site must be configured to provide the following DHCP Options.

DHCP Option	Purpose	Field format	Value
Option 42 (optional)	Time server	IP Address	IP Address of NTP Server
Option 66 (optional)			
Used to support Polycom SoundPoint IP Phones (capped at firmware version 3.1.3 rev C) and for Linksys IADs transitioning from TIPT, DOT	TFTP server	ASCII	dms.digitalbusiness.telstra.com
Option 160			
If Option 160 is not set, devices will discover Telstra's Device Manager Server from the device vendor's zero touch provisioning server	Device Management Server	ASCII	http://polydms.digitalbusiness.telstra.com/dms/bootstrap

DNS Server

For Telstra MPLS access, DNS server(s) must be configured for DNS conditional forwarding for "nipt.telstra.com" and "tipt.telstra.com" domains as per the table below.

Parameter	Configuration
Telstra MPLS access	
Forwarder – DNS Domain Name	nipt.telstra.com tipt.telstra.com
Primary Domain Forwarder	203.52.0.221
Secondary Domain Forwarder	203.52.1.222

Telstra Internet access

Primary Domain Forwarder	DNS info provided by Telstra or Google 8.8.8.8 or Cloudflare 1.1.1.1
Secondary Domain Forwarder	DNS info provided by Telstra or Google 8.8.8.8 or Cloudflare 1.1.1.1

3rd-party internet access

Primary Domain Forwarder	DNS info provided by your service provider or Google 8.8.8.8 or Cloudflare 1.1.1.1
Secondary Domain Forwarder	DNS info provided by your service provider or Google 8.8.4.4 or Cloudflare 1.0.0.1

Web Proxy (Caching) Server

Your Web Proxy Server should be configured for http(s) cache bypass for “*.telstra.com”.

If a cache bypass is not configured, Administrator’s may find that stale web pages are presented whilst trying to manage Telstra Cloud Calling via the Adaptive Collaboration Management Portal. This is especially critical when using an internal web proxy server to gain access to the Internet.

Alternatively, for a Windows PC, a User can press <Ctrl F5> to reload the page.

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 can impact performance (voice quality due to additional network delay) and service quality.

Service	Protocol	Port	Description	IP ranges	Comments	Inbound	Outbound
Telstra MPLS access							
SIP & RTP	UDP/TCP & UDP	5060 & Dynamic (16384-32767)	Signalling protocol used by IP Handsets and IADs Media protocol used to deliver audio and video between VoIP endpoints	203.52.0.160/28	VIC – SBC 1	Yes	Yes
				203.44.42.96/28	VIC – SBC 2		
				203.52.1.160/28	NSW – SBC 1		
	UDP			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	53	Used for Name Resolution DNS servers	203.52.0.221 203.52.1.222	DNS Server	Yes	Yes

Telstra Internet access							
SIP	UDP/TCP	5060	Signalling protocol used by IP Handsets and IADs	192.148.131.103/32	NSW – SBC 1	Yes	Yes
&	&	&		192.148.131.119/32	NSW – SBC 2		
				192.148.131.135/32	QLD – SBC 1		
				192.148.131.148/32	QLD – SBC 2		
RTP	UDP	Dynamic (16384-32767)	Media protocol used to deliver audio and video between VoIP endpoints	192.148.131.164/32	WA – SBC 1		
				192.148.131.196/32	SA – SBC 1		
				192.148.131.71/32	VIC – SBC 1		
				192.148.131.87/32	VIC – SBC 2		
3 rd -party internet access & Device signalling and media encryption with TLS							
SIP	UDP/TCP/ TLS	5060/ 5061	Signalling protocol used by IP Handsets and IADs	192.148.164.20/32	SA – SBC 1 (Encrypted)	Yes	Yes
&	&	&		192.148.164.24/32	SA – SBC 2 (Unencrypted)		
RTP/ SRTP	UDP/TCP	Dynamic (16384-32767)	Media protocol used to deliver audio and video between VoIP endpoints	192.148.164.4/32	VIC – SBC 1 (Encrypted)		
				192.148.164.8/32	VIC – SBC 2 (Unencrypted)		
All access types							
HTTPS	TCP	80,443	Phone configuration files for the Device Management Server	144.140.208.16/28 144.140.208.32/28 144.140.162.40/28 144.140.162.48/28	Device Management Server	Yes	Yes
			HTTP and SSL for Adaptive Collaboration Portal administration, Call Centre and miReception	144.140.208.80/28 144.140.162.80/28 144.140.181.80/28 144.140.218.96/28 144.140.222.32/28 144.140.224.32/28	Web server		
NTP	UDP	123	Handsets will obtain their NTP time source via a specified synchronised time source	Customer configured	Time server	Yes	Yes
Cisco's Zero Touch Provisioning (If DHCP Option 160 is not set)			Refer to Cisco documentation: https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/ip-phones/ztp-firewall-settings-ds.html				
Poly's Zero Touch Provisioning (If DHCP Option 160 is not set)			Refer to Poly documentation: https://info.ztp.poly.com/docs/begin/prerequisites				
Webex for BroadWorks			Refer to Webex documentation: https://help.webex.com/en-us/article/WBX000028782/Network-Requirements-for-Webex-Services#id_134137				

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 Telstra Cloud Calling Voice devices from:

-  Registering on the service.
-  Making internal calls.
-  Receiving incoming calls.
-  Voice quality issues.

Note: For Telstra Cloud Calling over 3rd-party Internet, make sure to turn off SIP ALG on the 3rd-party router.

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 for on-site switches and routers, is recommended so that voice receives prioritisation within the Local Area Network and that network congestion is avoided by implementing techniques such as “Modular QoS”.

Implementation of Telstra’s MPLS Dynamic CoS means that voice receives prioritisation within the Wide Area Network and that network congestion is avoided 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

To provide an enterprise grade of service for Telstra Cloud Calling, your network must support end-to-end QoS. The WAN edge router must be configured to categorise and prioritise the traffic accordingly.

Differentiated 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 (i.e. DNS, HTTP(s), FTP, TFTP)	

Note: For Adaptive Collaboration: Telstra Cloud Calling over the Internet sites, it's best effort as the traffic is coming through 3rd-party internet.

Bandwidth

Although there is no set bandwidth that is mandated you will still need to ensure there is enough WAN link bandwidth available for Telstra Cloud Calling traffic, as a guide you should nominally base your 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. See the table below for examples.

Voice Services		
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

CPE Guide

Please refer to the Adaptive Collaboration: Telstra Cloud Calling Device Guide found [here](#).

Supplementary Information

Supported Codecs for Adaptive Collaboration: Telstra Cloud Calling

To simplify the choice for our customers, Adaptive Collaboration: Telstra Cloud Calling recommends the use of G.722 codec where possible and G.711a as second option followed by G.729a. Below table contains sample calculations for the default voice payload sizes.

Codec Information				Bandwidth Calculations					
Codec & Bit Rate (Kbps)	Codec Sample Size (Bytes)	Codec Sample Interval (ms)	Mean Opinion Score (MOS)	Voice Payload Size (Bytes)	Voice Payload Size (ms)	Packets Per Second (PPS)	Bandwidth MP or FRF.12 (Kbps)	Bandwidth w/cRTP MP or FRF.12 (Kbps)	Bandwidth Ethernet (Kbps)
G.722_64k (64 Kbps)	80 Bytes	10ms	4.13	160 Bytes	20ms	50	82.8 Kbps	67.6 Kbps	87.2 Kbps
G.711a (64 Kbps)	80 Bytes	10ms	4.1	160 Bytes	20ms	50	82.8 Kbps	67.6 Kbps	87.2 Kbps
G.729 (8 Kbps)	10 Bytes	10ms	3.92	20 Bytes	20ms	50	26.8 Kbps	11.6 Kbps	31.2 Kbps
G.711u (64 Kbps)	80 Bytes	10ms	4.1	160 Bytes	20ms	50	82.8 Kbps	67.6 Kbps	87.2 Kbps

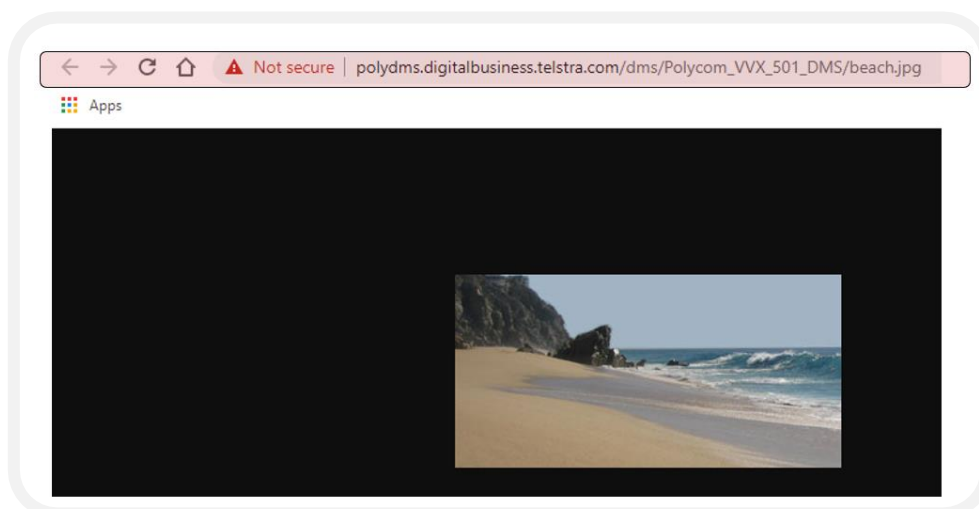
Troubleshooting & Quick tips

Device Management Platform (Provisioning server) Connectivity test

To check the routing has been established to Telstra's Device Management Platform, open a browser window via your PC using the following address:

- https://polydms.digitalbusiness.telstra.com/dms/Polycom_VVX_501_DMS/beach.jpg

A successful test should display the following picture:



Glossary

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

Term	Definition
CDP	Cisco Discovery Protocol
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 WAN	Internet Protocol Wide Area Network
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
NTP	Network Time Protocol

Customer Support

For any questions about your offer, technical support, service, or connection, you can visit [Telstra Connect](#), or call us on 1800 370 430. Assurance and fault calls are answered 24 hours / 7 days, all other calls are answered Monday to Friday, 9am to 5pm Eastern Standard Time (except national public holidays).

For escalations, contact your **Telstra Account Representative**.