TalkTalk Business

TalkTalk Business

SIP (Session Initiation Protocol) Trunks

Service Definition

Contents

1. SIP (Session Initiation Protocol)

SIP (Session Initiation Protocol) Trunks

TalkTalk Business (TTB) SIP Trunking is a cloud-ready, cost-effective replacement for traditional ISDN, enabling public-sector organisations to modernise voice services without replacing existing PBXs. Operating across new or existing IP connectivity, it offers high-quality voice, automatic traffic prioritisation, flexible channel growth, detailed call analytics and robust resilience options. Integrated spend-management tools help protect against unexpected usage, while the optional Call Manager portal provides full control over routing, diverts and inbound call handling. Designed for reliability and scalability, it supports the communication needs of councils, NHS trusts, education organisations, local government, housing providers and emergency services.

TTB's SIP Trunks are deployed as two or more channels. Each SIP channel has the capability to support one incoming or outgoing call. SIP channels are sometimes called sessions, lines or concurrent calls. SIP Trunks operate over an IP connection, which connects over DIA or public or private cloud.

Benefits of SIP Trunks

Supports business continuity:

- Offers flexibility that is not available through traditional ISDN
- As SIP trunks work via IP networks, resilience can be provided with fail-over options if problems occur
- SIP can automatically reroute any calls to back up sites in seconds - so there is no customer disruption

Number flexibility:

- SIP trunking allows customers to decide which number they want to display on a call-by-call basis.
- SIP trunking allows out-of-area geographic number ranges to be used - showing businesses as local, despite being physically located elsewhere.
- The impact of changing office location is minimised and growing business without opening more regional offices is enabled as SIP hosts geographic numbers, granting more flexibility while maintaining geographic numbers

Saves money:

- No need for a separate dedicated voice connection as SIP can be accommodated on the data connection
- SIP trunking allows free calls between connected sites

Greater flexibility to meet seasonal peaks:

- Customers can add more channels when demand is high, reduce them when there is little demand and split calls to make handling more efficient.

SIP Trunk Call Manager (Add-on)

SIP Trunk Call Manager offers a comprehensive suite of inbound call handling tools. It's ideally suited to a business highly dependent on customer service. It supports organisations looking to deal with incoming sales enquiries effectively without missing a call or make a step change in the way they handle business continuity. Advanced call handling features can be tailored to customer needs and adapted instantly via web and app control, supporting callers.

SIP Trunk Call Manager is deployed at endpoint level. Each deployment, alongside the Call Manager (and any optional add-ons/Direct Dia Ins (DDI) managed by it), is subject to a 12-month minimum term and a monthly rental charge. New DDIs can be added or removed as required.

The tools include:

- Change Inbound call routing via a password protected website
- Implement additional routing features such as call diverts according to time of day/day of week, system announcements and network-based queuing
- Set up a range of online inbound reporting on a per number basis for all, some or individual DDI Numbers
- Detailed inbound call analysis

Upon entering the correct Username and Password the administrator can access the SIP Trunk Call Manager via a password protected website: www.siptrunkcallmanager.co.uk

Features and Benefits of SIP Trunk Call Manager

End User Control of:	Business Benefits
Geo or NGN Termination or SIP	Control entire number estate via an intuitive online portal.
Termination on number	Redirect inbound calls to achieve business continuity and flexible working.
Time/day of week routing	Schedule call routing in advance according to business hours and call handling.
Divert on busy/OOH/no	Maximise call handling potential and provide improved service to the caller.
Snapshot Management	View call handling performance at a glance and monitor inbound call handling
Email alert on missed call	Ensure you are proactively notified of any unanswered/engaged calls –ideal
'One Touch' Business Continuity	Pre-build designated Business Continuity call plans for your Inbound number(s) with the ability to invoke/restore the last active call plan instantly – immediate business continuity in the event of office evacuations.
Date routing	Set up date-specific routing in advance –e.g. Bank Holidays.

SIP Trunk Call Manager App -access to call plan routing changes via a handheld smartphone/device	Provides a DDI user with quick access to key functionality and the ability to view essential call stats whilst on the move.
Hunt Groups	Enable calls to be answered by Serial, random, prioritised or simultaneous hunt groups
Call Queuing	Queue incoming calls on a destination number to assist with call handling during peak busy periods. End user configurable announcements, breakout and overflow options. Live queue stats enable effective queue management.
Call Distribution	Serial, hunt group and % based routing enables load balancing of calls across sites
Voicemail	Demonstrate excellent customer service by providing callers with an option to leave a message when unavailable. Customise voicemail messages to prompt users to leave details for a call back.

End User Control of:	Business Benefits
Advanced Statistics	Online access to comprehensive call statistics which enable informed business decisions. Advanced management information relating to call handling efficiencies; productivity, call patterns and caller behaviour. Data includes time to answer, calling time, call outcome and caller details.
Call Whisper agent notifications	Popular applications include the ability to tailor greetings to the number dialled. The end user can record an announcement to be played as a prompt to the call answering agent. Seamless to the caller, the call whisper announcement may be used to provide the agent with information from which they may tailor their call answering according to the particular SIP Trunk number that the caller has dialled.
Push Reports - Advanced	Provides recipients with full or summarised advanced statistics reports via email for daily, weekly or monthly periods.
Shared Values	Create global schedules which can be shared across many call plans. This saves users from having to make the same date/time or day/time change in many places.
Aliasing	Aliasing eliminates the need to create two or more identical call plans when all that is required is a new callable inbound

Optional SIP Trunk Call Manager Add-ons

A number of SIP Trunk Call Manager add-ons are available. These features are optional, chargeable extras. They can be provisioned on an End User account at the point of ordering SIP Trunk Call Manager or to an existing account.

Add-on Announcement	Announcements either from a personalised uploaded file by the user or from a selection of default system announcements. This allows incoming callers to hear a customer-facing spoken message ahead of calls being connected, improving customer service.
Add-on Area Based Routing	Used to define call routing, based on the originating telephone number or area code. This allows, for example, a branch office in a particular location to be routed all calls from a specific area. E.g. all calls starting 0161 can be routed to the Manchester branch office. This improves efficiency and
Add-on Standard Auto Attend	Personalised menu announcements with up to 10 options to be played to the caller, each leading to defined call routing/action based on the caller's key press on their keypad. This allows calls to be internally routed according to a caller's needs, improving efficiency and customer service.
Add-on Limit Caller Admission	Restrict the number of calls allowed to a configured destination across the entire SIP Trunk Call Manager account and prevent further calls being presented if the threshold is exceeded. Limit Caller Admission is ideal for restricting incoming call capacity during a period of high-volume of inbound calls. The total number of allowable inbound calls can be restricted, ensuring your total capacity is not fully utilised and allowing capability to make outgoing calls as necessary.

Resilience

SIP trunks connect customer call-connect systems, and the main requirement for them is to offer additional resilience options in the event of failure either in the calling system or underlying connection.

All SIP services are available in one of three resilience options (see Figure 1 below):

Single This is the default option. It provides a single internet connection between your SIP- enabled PBX and the carrier network. You can deploy minimum of two channels across the connection: each channel allows a single inbound or outbound telephone (or video) call.

Active standby – failover. This provides a second, standby SIP trunk which is activated if the primary trunk becomes unavailable. This option provides a cost-effective solution for customers wishing to ensure a degree of resilience for the service. Note that failover may need a small amount of downtime and customers will need two active, single connectivity circuits in this scenario.

Active active – load-balanced. Traffic is split between two active SIP trunks. The service automatically routes calls through two distinct connectivity services and traffic will be managed to ensure load-balancing across each. If either trunk becomes

unavailable, then all traffic will automatically route across the other until the unavailable trunk is active once again.

Note that in this scenario customers will need two active connectivity circuits and the same number of channels across each.

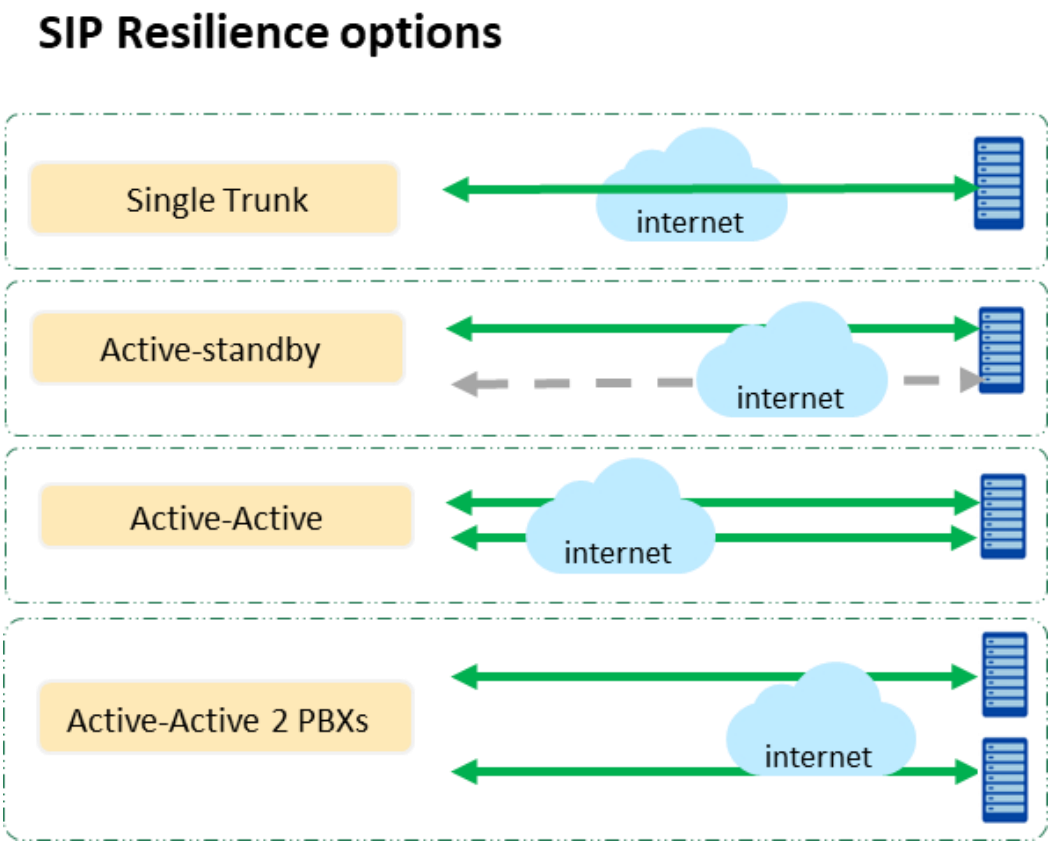

Figure 1: SIP resilience options

1.1 Data backup and restore

Providers and SIP platforms implement failover as back up to ensure continuity during network, server, or ISP failures.

Typical failover mechanisms include:

- Automatic call forwarding to backup routes or locations
- Separate trunks for critical vs. non-critical services
- Load balancing across multiple SIP trunks or servers
- Fallback to PRI (traditional phone lines) if SIP fails

These approaches are documented as common SIP failover solutions.

Some providers offer multiple SIP gateways, with SRV (DNS) records allowing SIP devices to automatically try alternate servers.

This redundancy includes:

- Multiple gateway endpoints
- Automatic rerouting to another gateway if one fails
- SIP devices registering to backup gateways

Levels:

- P1: Critical Fault – loss of service. 9 clock-hours' resolution, 24/7- Restoration time 9 hours
- P2: Partial loss of service. Restoration 3 working days
- P3: Degradation of service. Restoration 7 working days

1.2 Disaster Recovery

SIP trunks allow disaster recovery options in addition to connectivity above. SIP Trunk Call Manager allows customers control of their numbers so the Customer Admin can implement call forwarding in addition to connectivity and hardware resilience.
Business Continuity, Crisis Management and Disaster Recovery Plans are in place for all sites. Network resilience is assessed and monitored through testing on an annual basis. Continuous monitoring of network availability through the Technical Support Centre team will ensure any issues are identified in a timely manner.

Where an incident does occur, a robust incident response process is in place and is exercised to ensure an effective response, followed by a problem management review linked to service improvement. TTB recognises that network resilience is also reliant on Openreach for the last mile. If an outage was to occur on the Openreach infrastructure, we have agreed competitive SLAs with Openreach to mitigate risk. Other prioritised critical processes, systems and third parties are identified, and business owners are assigned accountability for assessing resilience and implementing business continuity plans to enable continuity of operations in the event of an incident.

TTB undertakes best ITIL practices throughout the business and technology teams. The Service Desk team has a problem management and change process to ensure that root cause and preventative actions are managed effectively, in line with service levels. In addition, root cause investigations are completed as part of our problem management process, where change and incident information is analysed and collected to suggest preventative actions. Reason for Outage (RFO) for network incidents are distributed to impacted customers within 10 working days from root cause following a Priority 1(P1) or Major Service Outage (MSO).

Where the priority of a TTB Network Incident is MSO or P1, a Major Incident Manager is assigned to document and communicate the progress of an incident. A multi-disciplinary team will work collaboratively to resolve the incident as quickly as possible and with minimal impact on the business. The IT Service Management (ITSM) team record of the incident is updated throughout and resolved using defined metrics to drive post-incident analysis activities.

Major Incident notifications are distributed during the life of the incident via a dedicated Incidents Team. If the customer has any questions related to an RFO notification, or requires additional detail, these can be referred to the ITSM team via your Account Manager.

TTB also continues to invest in supporting appropriate resilience of critical systems. Relationship owners are assigned accountability for requiring critical third parties to have adequate business continuity plans in place and obtaining third party assurance, where appropriate, that their plans have been reviewed and tested annually.

With usage consistently on the rise, we constantly monitor the network, forecasting and responding to the ongoing demand to maintain stability and minimise any congestion. Despite download usage increasing 40% year-on-year, our network has remained resilient. Additionally, due to Covid-19, further measures have been implemented to ensure the health and safety of our workforce and customers whilst we successfully continue our provision of critical services, which involves enabling the remote working of both our workforce and third parties.

1.3 Onboarding support

All customers procuring through a public sector framework will be allocated a TTB Account Manager who will support all onboarding, in-life and offboarding processes.

The TTB Account Manager will be responsible for the following:

- Serve as the main single point of contact for assigned public sector clients
- Build long-term, trusted relationships
- Understand each client's business goals and challenges
- Ensure clients feel supported and valued
- Run regular check-ins, calls, or business reviews

TTB has an onboarding model for all new customers, from SMEs through to major customers, undertaking the following process:

1. The customer order is received by the salesperson, along with a copy of the terms and conditions (signed using DocuSign)
2. All customer orders are verified, credit checked and, once approved, put into the provisioning work in progress queue (WIP)
3. All orders are built within our Inventory Systems billing system by the Delivery team
4. All updates and communication on installation dates will be provided to the customer via email by the Delivery Team
5. Should a router be requested as part of the solution, TTB will provide engineering resource for onsite installation.

1.4 Offboarding support

If a customer chooses to cease their TTB service, clear timescales will be mutually agreed between TTB and the end customer. Any managed CPE provided as part of the managed service remains the property of TTB and must be returned unless otherwise agreed. TTB Account Managers will be on hand to support customers through any offboarding activities, including any contractual elements around termination fees, providing a full inventory of all estate products and services and any general updates.

1.5 Service Constraints

SIP Trunks are only available to approved Call-Connect Systems. TTB can check and verify customers system compatibility during engagement.

1.6 Service Levels

TTB' service support hours for incident reporting, maintenance notifications, and hours of support are shown below:

Support Hours and Maintenance notification			**Response Targets (clock hours)**
Incident reporting	Priority 1	24x7x365	4
	Priority 2	Business Days 08:30 – 17:15	8
	Priority 3	Business Days 08:30 – 17:15	48
Maintenance notification	TTB initiated changes	Minimum of 10 business days	

Support hours

Faults can be raised 24x7, 365.

In hours – M-F (excl. BH) 8:30 to 17:15	**Out Of Hours**
Email: **systemsupport@talktalkbusiness.co.uk**	Email: b2booh@talktalkbusiness.co.uk
Phone: **0191 493 1120, option 1 or 0800 4661234, option 1 then option 3**	Phone: 0800 5426753

Your case will be allocated to an engineer who will investigate the issue and either resolve the fault directly or raise and track a support case with our suppliers. Tickets will be prioritised according to the severity of the fault reported and will be tracked and managed through our established fault management process.

1.7 Service Levels Agreements

Priority	Description	Definition	Resolution SLA
P1	Critical Fault Loss of service (TLOS)	For incident conditions which have existed for 5 minutes or more and comprise one or more of the following: • Total loss of voice service • Dial tone not available • Outbound or inbound calling not unavailable • No outbound calls connecting • All outbound or inbound calls in progress drop mid call	9 clock-hours' resolution, 24/7
P2	Partial loss of service (PLOS)	Intermittent or partial loss of voice service at an installation site with a high degree of service impact and where the intermittence can be demonstrated repeatedly within a 1-hour period.	3 working days In hours – M-F (excl. BH) 8:30 to 17:15
P3	Degradation of service	Intermittent or partial loss of voice service at an installation site with a low degree of service impact and where the intermittence cannot be demonstrated repeatedly within a 1-hour period.	7 working days In hours – M-F (excl. BH) 8:30 to 17:15

Service Credits

Service credits are available for P1 incidents not resolved to target. Details can be provided on request.

1.8 After Sales support

Incident reporting and support requests should be raised by telephone on 0333 003 4333 or via email ttbenterpriseassurance@talktalk.business. Our team aims to diagnose faults within 30 minutes. Support requests which are less time-sensitive should be raised by email.

1.9 Technical Requirements

- **System Requirements:** Users must have compatible call-connect system (PBX), sufficient connectivity bandwidth (high-speed recommended), and the current software version to access full functionality.
- **Network access:** Firewalls, proxy servers, or web security gateway settings can block access to the service, so checking network configurations is important.

1.10 Outage and Maintenance Management

For all planned notices and maintenance, the customer will be notified 10 business days in advance. In regard to all unplanned disruption or major failures, all TTB staff will receive email notification internally, informing them of the exact nature of the disruption and the details of the known failure. At this stage it will be the responsibility of the Assurance Desk to inform all affected customers via email and/or text message. Updates will be provided on a regular basis (every four hours) until fault restoration. For all Major Service Outages (MSOs) a full RFO report will be provided as part of the communication.

Reverting to a normal service in the event of a failure of MSO will follow a procedure whereby all necessary testing is completed within the Assurance and Technical Engineering teams. This includes ensuring calls can be made and received, call features are restored and any underlying connectivity is restored. These teams will initially follow up through direct contact with named representatives within the customer's organisation. All relevant checks will be completed by both parties to ensure all services and deliverables are working correctly prior to any buyer sign-off.

1.11 Hosting Options

TTB currently has multiple datacentre facilities, notably Corsham and Milton Keynes. We also have data centre space in Virtus 2 in Hayes, and Virtus 5 in Stockley Park, both in west London.

Corsham

The functionality and operation of the TTB Corsham datacentre facility is designed to act as a single point of reference for customers to understand both the facilities provided and also how to access/manage their services with TTB. The datacentre combines Tier 3 high-availability with very low additional energy used in the cooling and power system losses, resulting in an annualised power usage effectiveness (PUE) of less than 1.3 within an IL3 security environment.

The systems employed ensure that Corsham is highly scalable, ensuring an unusually low PUE is achievable at low IT loads as well as when the facility is at its maximum capacity. This results in a carbon footprint that is nearly half the industry norm, providing customers with additional green credentials. Based in a multi-layered security complex with multiple levels of redundancy at both a power and network level, this facility ensures continuity of service delivery for customers hosting their equipment.

Milton Keynes

The Milton Keynes data centre consists of a purpose-built facility with N+1 redundancy throughout. Formerly the data centre for the Trustee Savings Bank (TSB), the Milton Keynes site has been built with attention focused on high availability. The data centre is secure and available 24x7x365. TTB provides a standard availability of 99.9% on all of the components of its co-location services: power, bandwidth, HVAC and fire suppression. Co-location services can be purchased as a standalone item, or as part of an IPVPN Service. These services may be used to extend service directly into a private MPLS cloud and/or to provide internet breakout.

Security

Our Data Centre facilities provide a multi-layered physical security model to maximise security. The overall site is controlled and patrolled with no unauthorised access being permitted. The data centre building has its own controlled security perimeter. Internally within the facility, all access is restricted and monitored through smartcard and pin, video surveillance and personal escorts.

The datacentres are protected by graded security access. Personnel are only permitted to access the areas they require and only during the time periods agreed. In addition to standard physical access controls, photographic identification and biometric fingerprinting is required to access critical areas. Sites have security and technical staff on-site 24/7, 365 days a year. Access to the buildings is controlled by an air lock which only allows one person through at a time. Access to all internal doors and equipment aisles are controlled by card and pin code locks. The cards are configured to allow each individual access to only the areas they require and only for the length of time they require it. Access to the data rooms and build areas also have biometric scanners for additional security.

Access to the datacentre facilities is covered by digital video surveillance both inside and out which records all movement and stores the data externally. This video data is stored offsite for three months. The physical building is covered by both passive and active sensors that are linked into local security response and emergency services. These sensors cover all areas with additional levels of coverage for critical zones. As additional security, all building alarm systems have built-in wireless notification systems as well as traditional telephone-based notifications to provide coverage in the event of physical links being tampered with.

The data centres are manned 24x7 and has 24-hour security at reception. The security desk is equipped with CCTV screens monitoring all access points, corridors and sensitive areas. All staff carry photo ID cards. Swipe cards are required to enter the data centre and to pass between rooms and enter hosting areas. Access to server rooms is only provided when required. All rooms, corridors and service areas are equipped with PIR detectors so that movement can be detected anywhere in the building. All external windows have “break glass” detectors, and all external doors including service areas trigger an alert when opened. The building is protected by an invisible fence, which will detect motion around close proximity of the building.

Client access to the data centre must be booked in advance and confirmed by TTB. Any person arriving at the data centre without prior confirmation will be refused access. Anyone attending the data centre must show a valid legal form of photo ID. Using the “Authorised Contact Form”, it is possible for customers to restrict access to a pre-determined group of personnel. Please note that it is the customer’s responsibility to ensure this form is kept up to date.

1.12 Access to data (upon exit)

When the customer wishes to cancel their service, all service-related data will be deleted via our data cleanse processes. The end of contract process will be supported by the customer’s dedicated Account Manager and TTB Customer Services, who will assist them to access to their data along with any queries or requirements. We will also raise a data deletion request with our supplier. Former customers can initiate a right-to-be-forgotten request to remove their data held on our customer database. Contact details are published on our website and in any service documentation provided following service initiation.

1.13 Security

SIP is an established and mature service within the UK market. Customers who require additional security can deploy SIP trunks through private networking connections where the path does not touch the public internet.

Infrastructure and network security

- **Private access circuits:** For higher security, you can connect your site to our providers network using a private circuit instead of the public internet.
- **Network monitoring:** Our providers network is monitored for traffic patterns to help prevent fraud and ensure service quality.

- **Quality of Service (QoS):** QoS assurance is provided to guarantee voice quality and end-to-end availability.
- **Internal network security:** Integrating firewalls and using IP authentication can protect your internal network from external threats.

Fraud protection

- **Anti-fraud software:** Our provider uses sophisticated anti-fraud software to combat malicious activity.
- **Fraud management portal:** Administrators can access a portal to set spending thresholds and receive alerts for unusual activity, such as a spike in calls to premium numbers.
- **Blocking unauthorised calls:** Our providers software can immediately flag and block unauthorised calls, minimising damage to a company's assets.

Version Control

Document Amendment History Log						
Document Owner	Jay Bhickhabai					
Created Date	20-01-26					
Author	Jay Bhickhabai					
Next Review Date	20-01-27					
Version Number	**Modified date**	**Amendment history**	**Reviewed by**	**Approved by**	**Approval date**	**Approval evidence**