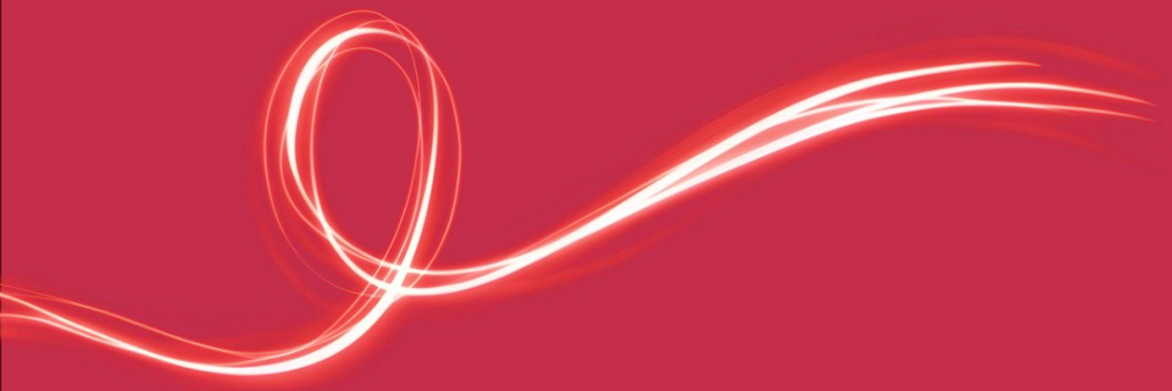
TalkTalk Business

TalkTalk Business DIA (Dedicated Internet Access)

Services Description



Contents

1. Dedicated Internet Access

DIA is TalkTalk Business' dedicated internet first, secure and resilient connectivity solution for public sector organisations. DIA offers high speed (up to 10GB) symmetrical bandwidth for customers who require significant upload and download capability. Our solution provides enhanced service levels with fast repair times. Bandwidth is uncontended, so customers get all their bandwidth all the time, meaning there's no slowdown in busy periods.

TalkTalk Business (TTB) provides a range of DIA services, offering guaranteed, uncontended speeds and enterprise grade reliability. Our DIA service is provided on dedicated circuits (bearers) to customer premises in a variety of sizes and technologies to suit their needs. We can provide routers as part of a managed service, opening up a wider range of features and benefits. Customers can also take a 'wires only' service and provide their own routers. It's what makes sense for them and their organisation. Additionally, we can provide managed firewalls to make sure connections are secure, if required.

Key terms:

'Symmetrical bandwidth' - Upload and download speeds are the same. (For example, broadband is asymmetrical meaning download speeds are higher than upload speeds).

'Uncontended' – Maintain the same speed throughout peak times as you are not sharing the service with other organisations in your local area, as with broadband services.

'Bearers' - The physical fibre/access circuits that bandwidth is delivered over. These usually have a maximum size of either 100Mb, 1Gb or 10Gb. Customers would traditionally have ordered 100Mb bearers for smaller sites, but TTB offers 1Gb bearers at the same price as 100Mb bearers, future-proofing any investment.

<u>Access Options</u>

TTB provides DIA services on the access technologies included in the table below. For more information about each specific access technology, please see the following sections.

Access Type	Bandwidths	Service Level
Ethernet Fibre (leased lines)	10Mb – 10Gb	Premium
Ethernet over Fibre to the Premises (EOFTTP)	Guaranteed 20Mb - 200Mb (symmetrical) Download burst available up to 1Gb	Express
Ethernet over Single Order Generic Ethernet Access (EOSOGEA)	Up to 20Mb (symmetrical)	Express

Ethernet Fibre (leased lines)

Ethernet Fibre, sometimes referred to as Ethernet Access Direct (EAD), offers a dedicated and symmetrical bandwidth service delivered on uncontended fibre access at speeds from 10Mb/s up to 10Gb/s. This is all backed up by our industry-leading SLAs. Bandwidth can be increased quickly and easily, in line with emerging business needs. Customers have a choice of fibre bearers to suit their bandwidth requirements and budgets. All speeds are symmetrical and uncontended.

Bearer	Available Bandwidths	Interface Options
1Gb	10MB, 20MB, 30MB, 50MB, 100MB, 200MB, 300MB, 500MB, 1GB	RJ45 (copper) Single-mode Fibre (SMF) Multimode Fibre (MMF)
10Gb	1GB, 2GB, 3GB, 5GB, 10GB	10GB Single-mode Fibre (SMF) 10GB Multimode Fibre (MMF)

Ethernet Over Fibre To The Premise (EOFTTP)

EoFTTP delivers Ethernet-style service capabilities (i.e., uncontended, symmetrical bandwidths) over low-cost ultrafast broadband access technology. EoFTTP access services are presented on RJ45 from 20Mbps or 200Mbps symmetrical bandwidth, depending on the access service ordered. Customers are also able to utilise any latent capacity of the access bandwidth over and above the symmetrical speed elements of the access circuit, i.e. where a 1Gb access circuit is used to deliver a 100Mb symmetrical service, customers can ‘burst’ above the 100Mb symmetrical speed and take advantage of the ‘up to 1Gb’ download capacity of the circuit. EoFTTP services are subject to geographic availability, with a footprint which is growing daily. They are ideal for small offices, branch sites, or as a low-cost backup to a primary EAD service. TTB is continually launching new EoFTTP speed variants to cater for customer technical requirements and budget.

Ethernet over SOGEA (EoSOGEA)

EoSOGEA delivers ethernet-style service capabilities (i.e., uncontended, symmetrical bandwidths) over low cost and widely available superfast broadband access technology. EoSOGEA access services are presented on RJ45 and provide up to 20Mb/s symmetrical bandwidths. Customers are also able to utilise any latent capacity of the access bandwidth over and above the symmetrical speed elements of the access circuit, i.e. where an 80Mb access circuit is used to deliver a 20Mb symmetrical service, customers can ‘burst’ above the available symmetrical speed and take advantage of the ‘up to 80Mb’ download capacity of the circuit. They are ideal for small offices, branch sites, or as a low-cost backup to a primary EAD service. EoSOGEA is

the strategic replacement product for EoFTTC, which will be phased out over the coming years in the UK.

Managed Router Services

TTB provides the option of a managed router with all DIA services for customers. As it's a 'managed' router, we will provide all support should there be any issues with the device, including device/parts replacement and engineering visits, should they be required, taking the hassle away from the customer. There are a range of routers available to cater for various speed and budget requirements.

We provide a wide range of managed routers including the following vendors:

- Cisco
- Meraki
- Juniper

Wires Only Services

Where customers wish to deploy their own technology, TTB can offer a wires only service based on the above products to provide this flexibility.

Firewalls

TTB understands how complex security can be for our customers, so we provide a range of options and templates to suit each customer's needs, from a basic rule set which allows all traffic out and nothing in, to project-managed tailored configurations. TTB can provide managed firewall services from a range of carefully curated vendors, including Cisco, Juniper and Sonicwall.

IP Addressing

All DIA services from TTB include a single static IPV4 address, and customers have the option to buy larger IP address blocks to suit their business requirements. The inclusive IP range is a /31 which gives end customers a single useable static IP address. The IP addresses assigned to a customer by TTB remain the property of TTB and will be recovered by TTB if a customer chooses to cease their service.

Network Resilience

TTB provide a variety of resilient options to meet the needs of any size business for whom internet access is critical. The most common method of ensuring end user uptime is to deploy dual access circuits into a location. Access circuits can be provided to meet the bandwidth requirements, so that service degradation is minimal; but also, cost-effective resilient solutions can be deployed when only a small amount of bandwidth is required in an emergency.

TTB can provide resilient circuits in several ways:

- **Diverse routing by single supplier** (e.g. Openreach's R02 service): This is where both primary and secondary circuits are provided by Openreach and each circuit is planned and delivered to be completely physically separate to the other. This includes the use of different exchanges / points of presence, separate ducts and separate entry points to customer's premises where practicable. So any event which affects the primary circuit (such as a fibre break) would not affect the operation of the secondary circuit, allowing the delivery of internet services to continue uninterrupted.

- **Diverse routing using multiple suppliers:** By providing a resilient service using access circuits from alternative network providers, (i.e., Virgin Media Business, COLT, City Fibre, and others). This provides carrier resilience, which means that if one carrier has a network issue, or there is a fault on one of the resilient circuits, then it is unlikely for the other carrier to be affected by the same event.

Hardware Resilience:

- **Single router resilient access** - TTB can offer two access services into a single CPE. Typically, these deployments incorporate an ethernet access primary circuit, with a secondary reduced bandwidth ethernet service.

- **Dual router resilient access** – In this design a primary ethernet circuit carries the traffic during normal operation. In the event of primary ethernet circuit failure, all services will be failed over to the secondary ethernet connection, via the secondary CPE. To ensure that a hardware failure of the managed CPE does not affect the uptime of the site connectivity, we will provide two managed routers (one for each circuit). We deploy Virtual Router Redundancy Protocol (VRRP) and Internal Border Gateway Protocol (iBGP) to ensure protection against circuit failure, and CPE failure when using Juniper managed routers.

Both resilience options offer an 'active – standby' failover service, where the primary circuit is active, and the secondary circuit lies dormant until there is an issue with the primary circuit, in which case the secondary circuit will kick into action

TTB can also provide an 'Active / Active' resilient service whereby two separate circuits are delivered using diverse and physically separate routing. This effectively gives a customer two primary services, each with its own distinct IP range. In this configuration TTB does not manage any failover of traffic between the two links. This is ideal for SD-WAN deployments where dynamic load sharing is used to send traffic across both active links. This can also be provided across different access technologies e.g., a mix of EAD or EoFTTP or EoSOGEA access circuits.

Additional Features

Bandwidth Boost

Bandwidth Boost is a feature which allows customers to temporarily increase the bandwidth of their service (subject to the maximum capacity of their access bearer and router) without having to re-contract their service. This is a benefit for customers who have seasonal peaks in bandwidth demand, and who do not want to pay for bandwidth through the year which they don't need. Customers can pay for their increased bandwidth on a daily rate and revert to their contracted bandwidth when they no longer need the extra speed just by letting us know. There is a two-working day lead time to change bandwidth up or down, and once a change has been made a customer must remain on the given bandwidth level for a minimum of seven days. Billing for bandwidth changes will commence on the first full day that the new bandwidth level is made available to the customer. Requests for bandwidth changes can be made through either our Sales or MAC (moves, adds and changes) Teams. The Bandwidth Boost feature is only available on services where we provide a managed Juniper router.

SIP Exchange

SIP Exchange allows our customers to enjoy the benefits of access to multiple SIP providers over their DIA service, without having to install dedicated physical connectivity. We provide the path between you and your chosen SIP provider, leaving you free to negotiate your commercial arrangement with your SIP service provider. SIP Exchange allows customers to segregate a portion of their DIA bandwidth specifically to SIP services so they enjoy the very best quality of voice by keeping your voice traffic off the public internet.

SIP Exchange delivers on-net access to the UK's leading SIP providers and is available as a standard part of our public internet portfolio. It includes key IP voice providers including Gamma, COLT, BT Wholesale IPVS, and Teleware to give our customers the choice of sending traffic to the very best SIP solutions. These interconnects are dedicated to voice traffic, which means all your voice traffic can be kept off the public internet, traversing our network from end to end, assuring both performance and security.

Cloud Exchange

Cloud Exchange is a service which offers on-net access to public cloud service providers, such as AWS, Google Cloud, Microsoft Azure, Office 365 and Oracle Cloud, without requiring dedicated connectivity solutions or traversing the public internet. Our interconnected approach allows you to boost cloud application performance, reduce latency and improve scale, network control and visibility to deliver a quality cloud experience to your end users. With business-critical applications now hosted in many different locations, Cloud Exchange keeps you safe by privately connecting with the

leading public cloud and SaaS providers to deliver a high-performing and secure solution. Customers can dedicate some of their DIA access bandwidth for exclusively connecting to the available cloud service providers.

Bandwidth Utilisation Reports

Customers can receive bandwidth utilisation reports. This will provide visibility of actual usage so customers can plan for any future networking requirements.

1.1 Disaster Recovery/Business Continuity

At TTB we undertake 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 P1 or 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.

Business Continuity, Crisis Management and Disaster Recovery Plans are in place for our key sites. Network resilience is assessed and monitored through testing on a regular 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 3rd party infrastructure, we have agreed competitive SLAs with our suppliers 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 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.

1.2 Onboarding Support

TTB has an onboarding model for all new customers, from SMEs through to major customers. All customers procuring services via public sector frameworks also have the support of a dedicated Account Manager.

In general all orders follow the process detailed below:

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, and credit checked and, once approved, put into the provisioning work in progress queue (WIP)

3. All orders are built within our Inventory System's 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.

1.3 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 to TTB unless otherwise agreed.

1.4 Service constraints

For all planned notices and maintenance, the customer will be notified 10 business days in advance to allow them to make suitable arrangements. Emergency maintenance is rarely required and is typically not customer-affecting, as it is usually confined to one part of a resilient system. In the event emergency maintenance is required that is likely to be customer affecting, the planning and risk assessment we undertake will include making provision to minimise the impact in terms of scope and duration. Where it is possible, advance notice will be given.

1.5 Service levels

Customer support is available 24x7x365.

Performance/Availability

The network performance targets for the TTB network are:

Internet Access Platform Matrix	Target
Availability	99.99%
Round Trip Delay	<30ms
Packet Loss	<0.1%

Target Service Level Agreements

The target SLAs we offer are linked to the type of access technology taken as part of your service. Our SLA on repair is industry leading, with clear and simple service credits available should we not meet expectations. This includes replacement of faulty hardware as detailed below.

SLA Level	**Incident Reporting Coverage**	**P1 Resolution Target**	**P2 Resolution Target**	**P3 Resolution Target**
Premium	24x7x365	4 Hours	8 Hours	24 Hours
Express	24/7/365	7 Hours	24 Hours	72 Hours

For example, for a P1 incident which is deemed to be due to faulty hardware, we offer a 4- hour replacement part and engineer to site resolution target.

Service Credits

After receiving report of an incident, we will aim to resolve the issue as per the target SLA table in the section above. For P1 incident types, once this period has elapsed (e.g. 4 hours for EAD or 7 hours for EoFTTC services), you are entitled to claim service credits. To keep things simple, we offer 50% of the monthly rental charge if we don't resolve it within 1 day after this initial period or 100% of the monthly rental if it is over 1 day.

Clock hours exceeding resolution target (per incident)	**(per incident) Credit (% of applicable monthly recurring charges)**
< 1 day	50%
≥ 1 day	100%

Service credits apply to P1 incidents only. More information on service credits is detailed in the TTB Managed Data Product Terms and Conditions.

1.6 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.

1.7 Technical Requirements

Customers are required to confirm the required location of where the service should terminate. Customers must ensure that there is an adequate power supply in the termination location. Customers will also require a compatible router and firewall service, which TTB is able to provide.

1.8 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 or MSO will follow a procedure whereby all necessary testing is completed within the Assurance and Technical Engineering teams. 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.

1.9 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.

1.10 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 by the use of smartcard and pin, video surveillance and personal escorts.

The datacentres provide for a grading of 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 to the facility. 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 on a needs basis. 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 the booking 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 data.

1.11 Access to Data upon Exit

Data is stored in a secure and resilient N+1 environment and, where applicable, is subject to near real time replication/mirroring across diverse geographic locations. In the event of an incident, including loss or degradation of resilience, the incident will be managed in line with an established procedure to ensure customer SLAs can continue to be supported. Should the customer require access to data upon exit, a plan will be put into place for requesting the data via the customer’s Account Manager.

1.12 Security

Should intelligence or alerting indicate any potentially malicious activity, TTB operates a robust security incident management programme, and has deployed industry-leading endpoint protection technology to defend against advanced threats as part of our incident response program. TTB has implemented an Information Security Management System based on industry good practice (NIST CSF, PCI DSS) and is externally certified to ISO 27001. This covers a range of policies and procedures to ensure the confidentiality, integrity and availability of information. Standard security protocols are followed for private network connectivity. The Ethernet Service has no additional security requirements as the security elements lie within the private network. The TTB Security Operations Centre (SOC) facilities are manned 24x7x365, providing a near real-time response to security events with an escalation process to senior management as required. Our 24/7 SOC has extensive monitoring of internal and external security controls, coupled with curated threat intelligence feeds. Incidents are triaged based on risk and impact and playbooks have been developed to focus on containment, eradication and recovery activities in-line with NIST best practices. TTB conducts security scanning of all its infrastructure on a bi-weekly basis. We also conduct weekly threat and vulnerability scanning of all our network assets via

InsightVM. Critical/high risk vulnerabilities patches are applied within 14 days. All other updates are applied as soon as possible using a monthly patching cycle. Security updates are assessed and prioritised based on threat level, likelihood of compromise, consequences of compromise, environmental characteristics and regulatory or accreditation-based requirements. TTB gets its information about potential threats from InsightVM for scanning, Altiris Patch Management.

Version Control

Document Amendment History Log						
Document Owner	Andrew Stokes					
Created Date	21-01-26					
Author	Paul Ducklin					
Next Review Date	21-01-27					
Version Number	**Modified date**	**Amendment history**	**Reviewed by**	**Approved by**	**Approval date**	**Approval evidence**