

1. Service Overview

Our Managed WAN Service provides you with a private layer 3 network that enables you to connect between multiple sites and/or the Internet through a resilient, QoS-enabled MPLS core.

The Managed WAN Service can cover UK, European and international access, and can provide remote access, resilience options, routing, VPN configuration options and QoS. We will deliver Managed WAN Service to your Site(s) or from one of our Points of Presence ("PoP").

We will deliver the Managed WAN Service using our resilient NGN to interconnect any number of your Site(s), independent of their location and their bandwidth requirements.

Additional information is included in your Order Form and Statement of Work.

2. Service Features

This section describes the key features of the Managed WAN Service.

The features of the Managed WAN Service are described in the table below. The optional features are available upon request for an additional Fee, which will be defined in your Order Form and/or SoW.

Feature	Description	Standard	Optional
Access Service	As described in Section 2.1.	•	
Standard Access	As described in Section 2.2(a).	•	
Resilient Access	As described in Section 2.2(b).		•
Standard QoS setup	As described in Section 2.4.	•	
Optional QoS packages	As described in Section 2.4.		•
Up/Down Alerting	As described in Section 2.5.	•	
Critical Patch Management	As described in Section 2.9.	•	
MSDD Configuration Backup	We will add the MSDD to our configuration management platform in order to maintain up-to-date configurations where reachability permits.	•	
Data Rate Usage Graphing	We will monitor the Managed WAN Service for bandwidth utilisation statistics. You will be able to view the reports based on bits per second samples taken every five (5) minutes via SNMP.	•	



Feature	Description	Standard	Optional
Data Usage Alerting	We will monitor managed devices for data usage and you will receive an automatic alert in the event of a critical link exceeding seventy-five percent (75%) of utilisation. Data usage samples are taken every five (5) minutes via SNMP.		•
Enhanced Response (Six Degrees Care Level 4)	Applicable to type C broadband service(s) only (see Access Service table in Section 2.1), enhanced response provides a fix to PSTN copper-based lines within six (6) hours of a fault being reported to the third party vendor.		•

2.1 Access Service

We provide a dedicated Access Service to connect each of your Site(s) to one of our core network's PoPs. We offer connectivity options range up to >10Gbps.

Each Access Service is provided using at least one (1) of the following types of physical access solutions:

Access Service	Type	Description
Fibre Service	A	A High-Speed dedicated fibre access connection from our PoP to your Site(s).
Copper Service	B	Ethernet First Mile (EFM) or Generic Ethernet Access (GEA) copper service or similar symmetric copper product from our PoP to your Site(s).
Broadband Service	C*	Standard broadband connectivity service, such as ADSL, FTTC, SoGEA, FTTP, 3G, 4G, or similar variant from your Site(s).
Data Centre Service	D	Ethernet port available within any PoP.

* (C). Please note that the line speed (Mbps) performance of may vary depending on the distance from the telephone exchange, proximity to cellular network and or device placement and building surrounding.

Your choice will be indicated on your Order Form.

2.2 Resilience Option(s)

We offer two resilience options for the Managed WAN Service:

- Standard Access** (standard) – a single Access Service is provided from your Site(s) to one of our PoPs. This service is defined as the primary Access Service; or
- Resilient Access** (optional) – two (2) Access Services are provided with different types and bandwidth, defined as the primary Access Service and secondary Access Service. These are configured in an active/passive set-up whereby the primary Access Service is used by default. If the MSDD Router detects an issue with the primary Access Service,



the secondary Access Service will be utilised until the primary Access Service is re-established. The resilient access can be deployed using the following combinations:

- (i) A+A;
- (ii) A+B;
- (iii) A+C;
- (iv) B+C; and
- (v) D+D.

Resilient access uses a router redundancy protocol to switch between the dual MSDD devices for access types A+A, A+B, A+C or B+C.

Your choice will be indicated on your Order Form.

2.3 Managed WAN Service Configuration Options

Each Managed WAN Service is set up with one or multiple virtual routing and forwarding tables, allowing multiple Managed WAN Service networks to share the Access Services. We will deploy each virtual routing and forwarding ("VRF") in an any-to-any configuration such that each site within the VRF can reach all other sites within the VRF.

Your IP addressing within the Managed WAN Service will use private ranges as defined per RFC1918 or IP addressing registered to you in a local internet registry's database. The following IP address ranges should be avoided as they are used by us to manage the network: 10.204.0.0/15, 172.31.0.0/16, 172.30.0.0/16, 172.16.0.0/16. If these ranges are configured and in use by you, we can arrange a meeting, at your request, to evaluate design variations to accommodate their use.

We support both IPv4 and/or IPv6 configured as static or BGP routing protocols option.

Please note the Managed WAN Service does not include encryption. Should you require encryption, this item will be described in a separate Order Form and/or SoW and will be subject to an additional Fee.

2.4 QoS Options

QoS is based on differentiated service enhancements and associated traffic classes as described in the IETF RFC2474. Standard QoS setup will map all traffic into a default QoS class. For an additional Fee, you can opt for one of our three QoS packages:

- (a) 4-Class QoS package (the default and standard);
- (b) Premium 8-Class QoS package; or
- (c) Custom QoS package.

Please refer to the sections below for further details on each QoS package.



Please note, you are responsible for marking all traffic at the LAN port of our MSDD. If no QoS is marked, traffic is placed into the default QoS queue.

DSCP is used for classifying and managing network traffic and for providing QoS on the Managed WAN Service. The DSCP parameters are defined per the QoS classes described below.

(d) 4-Class QoS Options

The 4-Class QoS configuration uses the policies set out below:

QoS Class	4-Class QoS Model DSCP	Traffic Ratio
Voice	EF	33%
Network Control – NC and Signalling	CS5, CS6	7%
Data	AF2X	35%
Default	DF (and others)	25%

(e) Premium 8-Class QoS Options

The Premium 8-Class QoS configuration uses the policies set out below:

QoS Class	8-Class QoS Model DSCP	Traffic Ratio
Voice	EF	10%
Video	AF4	23%
Streaming	AF3	10%
Network Control	CS6	5%
Signalling	CS5	2%
Data	AF2X	24%
Default	DF (and others)	25%
Scavenger	CS1	1%

(f) Custom QoS

Should you require a custom QoS set-up, this item will be described in a separate SoW and will be subject to an additional Fee.

The custom QoS Package contains up to eight (8) QoS classes.

2.5 Up/Down Alerting

We will provide proactive email alerting for up/down notification(s) of the MSDD availability via ICMP. Upon an alert and investigation to confirm a fault, we will initiate the incident management process as described in our Operations Manual.



2.6 Internet Gateway

If you take this option, we will provide Dedicated Internet Access breakout from the Managed WAN Service using Access Service, as defined in section 2.1 above. For more information on Internet Gateway options, please refer to the Dedicated Internet Access (DIA) Service Description. We can provide DIA at one or multiple locations. DIA is delivered from a site as a VLAN or injected into a VRF.

Managed Firewalls are also available as an add-on service for internet border protection and remote access. For more information on managed firewall options, please refer to the NGFW Service Description.

2.7 Complementary Service Options

Where you have subscribed to our other services such as Cloud services, Colocation, SIP Trunking or other managed network services, we can inject these services into your VRF facilitating two-way private connectivity to our service platforms. This is optional, with no additional Fee.

2.8 Managed Service Demarcation Device and Network Termination Equipment

For Access Service types A, B and C, you will need a MSDD. The MSDD controls the routing, failover and control of traffic between your network and our core network. The MSDD also allows our Support Team to monitor the Service and provide Data Rate Usage Graphing and Up/Down Alerting as listed in the Service Features table in section 2. The MSDD is owned, managed and maintained by us during the life of the Service. We will maintain it *in situ* (this could be a firmware upgrade/reboot). If we cannot ensure that normal service has resumed with the MSDD, we will replace the hardware with the same or equivalent model, with the latest applicable and approved firmware.

For Access Service types A and B, we can configure a SIP assured DIA profile on the MSDD for you. This configuration ensures that traffic destined to the supplier's public SIP gateways will be mapped by the MSDD into a priority traffic queue and ensures that this real-time traffic is prioritised across the access circuit.

For access type D, no MSDD is required. The demarcation point of the Service is the port within our PoP, delivered as a copper or optical fibre ethernet port. We will not provide you any cross-connect cable as part of this Service. You can either obtain cross-connect cables via the data centre provider or by us, subject to an additional Fee that will be specified in your Order Form. Please contact us if you require pricing information.

2.9 Patch Management

We will review your estate quarterly and check that patching is aligned to our recommended baseline. Where patching is required, we will arrange a maintenance window to carry out the work.*

The applicable MSDD will require a hardware refresh if the hardware is forecast to reach the end of vendor's support after the end of your Initial Service Term. Hardware refresh is outside the scope of this Service and is a chargeable activity.



We will identify and validate vulnerability with Critical and High severity (CVSS 3.0 7.0+) in the deployed firmware and evaluate the applicability of such vulnerability. If exploitable, we will remediate Critical (CVSS 9.0+) vulnerabilities within fourteen (14) days from our assessment, and High (CVSS 7.0+) vulnerabilities within thirty (30) days. Critical-severity vulnerabilities that cannot be remediated without interruption to your Service will require emergency maintenance, for which we may not be able to provide advanced notice of any service interruption, especially if it is reported that the vulnerability is already being exploited by threat actors. If we become aware that a specific critical vulnerability is being maliciously exploited anywhere in the world, we will use reasonable endeavours to remediate such vulnerability within two (2) Business Days of our initial assessment, provided that the vendor has made available an updated software version or alternative remediation is technically possible.

*Please note that, if you are unable agree a maintenance window with us for a scheduled patch update following our notification, we cannot guarantee the patching will take place in the above timeline.

3. Service Implementation

After order acceptance, we will implement the Service as follows:

Service Implementation	Us	You
We will send out Welcome Pack and a Technical Data Capture Form to you.	•	
We will place orders with our third parties to fulfil the Access Service(s) for you.	•	
We will schedule site survey(s) with you, where required. Please refer to Section 3.1 for more detail.	•	
Following the site survey(s) we confirm any additional work required and the relevant ECC, if applicable. Please refer to Section 3.1 for more detail.	•	
We will confirm your commit date(s) with you.	•	
We will preconfigure and dispatch MSDD routers to your preferred address(es).	•	
We will install Access Service(s) for you.	•	
We will confirm Ready for Service, including providing you with our Handover Pack.	•	
We will jointly activate the Access Service(s) with you.	•	•

All implementation work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional fees for any change in your requirements occurring after the implementation of the Service and outside the scope of your contract.

3.1 Excess Construction Charge(s)

If, following a site survey, we determine that additional work is required to provision the Service(s) (for example, due to a lack of existing infrastructure or capacity at the installation site), we will advise you in advance and you may decide whether to proceed or to cancel the order. If you decide to cancel the order, we reserve the right to charge a reasonable Fee for the



work performed prior to cancellation. If you decide to proceed, you will be responsible for the associated costs (the “Excess Construction Charges” or “ECCs”).

3.2 Scheduled Visits

If we have booked a visit to your site with you to carry out a site survey, installation or activation of equipment, and you wish to reschedule your appointment, please ensure that written notification is provided to us at least two (2) Business Days prior to the appointment date and time.

We reserve the right to pass on to you any third-party costs that we incur as a result of your failure to:

- (a) Notify us of your intention to reschedule an appointment in accordance with this Section 3.2;
- (b) Provide us or our third-parties access to your site at the scheduled date and time; or
- (c) Ensure that your nominated contact is available on-site during the scheduled appointment where, as a result of such failure, we are unable to carry out the site survey, installation or activation of equipment.

3.3 Ready for Service

The Ready for Service Date for the Managed WAN Service will be based on the delivery of each Access Service and defined as the latter of the completion of the following:

- (a) Activation of the Access Service to a Managed WAN Reference Site designated by you at order acceptance (usually your headquarter offices or a data centre);
- (b) Installation of each Access Service’s individual line to your site or to our PoP, as appropriate;
- (c) For Access Service Types A, B and C, delivery of the MSDD for use on your Site(s) or in our PoP; or
- (d) For Access Service Type D, the Ready for Service Date is the date when we have communicated successful testing of the network port(s) in our PoP to you.

Please note that for Resilient Access, the Ready for Service Date of one Access Service may be different from Ready for Service Date of the other Access Service.

4. Billing

The Service will be billed as a Set-Up Fee and a Recurring Fee as described in our Billing Guide, using the definition of the Ready for Service Date in Section 3.3 of this Service Description.

Please refer to Section 3.1 for more detail on ECCs. Any ECCs will be payable as Set-Up Fees as described in our Billing Guide.



4.1 Additional Charges

We reserve the right to charge additional fees in the following situations:

- (a) Implementation work carried out outside Business Hours;
- (b) Any change in your requirements occurring after the implementation of the Service and outside the scope of the contract (as described in the MSA);
- (c) Any third-party costs incurred as a result of your failure to comply with section 3.2.

5. Service Operations

Please refer to our Operations Manual for further information on incident management, requests for change and information requests.

After Ready for Service date, we will operate the service as follows:

Service Operations	Us	You
We will monitor the Managed WAN Service and its associated core network for availability and uptime for you.	•	•
We will notify you should we detect loss of service to the MSDD.	•	
You will confirm first line checks.		•
We will provide you access to a data rate usage graphing tool.	•	
We will troubleshoot and resolve Managed WAN issues for you.	•	•
We will maintain backups of all MSDD for you.	•	
We will follow change control process.	•	
We will carry out reporting in line with your chosen Service as indicated on your Order Form or SoW.	•	

5.1 Request for Change

To change your Service, you must raise a request for change, following the approach set out in our Operations Manual.

Changes included in this Service:

Item	Description
LAN Port Changes	Changes to MSDD Ethernet ports that face your LAN.
Application Identification Changes	Application WAN Selection Changes.
Routing changes	Add or modify an internal / external routing change affecting single / multiple destinations.
LAN Port Changes	Changes to MSDD Ethernet ports that face your LAN.
LAN IP Address Changes	IP changes to the ethernet ports that face your LAN.



LAN-facing VLAN Changes	VLAN changes to the ethernet ports that face your LAN.
DHCP Scope Changes	DHCP scope changes on MSDD.
DHCP Relay Address Changes	DHCP Relay address changes on MSDD.
QoS Policy Changes	Changes to QoS policies applied to the MSDD.

We will perform the changes listed above as and when required during normal Business Hours and subject to your monthly allowance. Please note that we can perform changes outside Business Hours upon request subject to an additional Fee calculated on a time and materials basis.

By default, this Service includes a monthly allowance of forty-five (45) minutes for the performance of requested changes. If you require a higher monthly allowance, we can include this in your Service subject to an additional Fee, details of which will be included in your Order Form and/or SoW. Please refer to Section 9 for our operational targets in relation to change requests.

If the time necessary to implement the changes that you require exceeds the standard monthly allowance of forty-five (45) minutes (or any higher allowance that you may have contracted with us), we will charge you on a time and materials basis for the remainder of the time needed to carry out the work.

5.2 Decommissioning Process

The decommissioning of the Service will follow the following process:

Decommissioning Process	Us	You
You will inform us of your request to decommission your Managed WAN Service. <i>NOTE: you may be charged an early termination Fee in accordance to the terms of your MSA if the Services are in-contract.</i>		•
We will confirm to you your termination date.	•	
You will return the equipment back to us for disposal.		•
We will confirm the location for the return of equipment upon termination by you	•	
We will delete relevant data on the target site via the portal. <i>NOTE: This process is irreversible once initiated.</i>	•	
We will delete all your backup data, related components and the environment.	•	

6. Dependencies

We will provide the Managed WAN Service subject to the following dependencies:

6.1 Prerequisites

- (a) A site survey is required as described in Section 3.1 (except for Access Service type D).



6.2 Client Obligations

- (a) You will designate a project lead and technical contacts with the appropriate level of expertise to support the successful implementation and operation of the Service;
- (b) You will provide us with all of the information needed to complete the configuration of the Service;
- (c) You will manage any of your own third parties during service implementation or service operations;
- (d) You will provide us or our third parties with access to your site(s) for set up and maintenance of the Access Service and for maintenance of the MSDD;
- (e) You will ensure that your nominated contact is available on-site during a scheduled visit;
- (f) During the installation of the service, it is your responsibility to show our installation engineer (or our third-party engineer) to the installation point;
- (g) You will ensure that structured cabling and appropriate LAN connectivity are in place on your site(s);
- (h) You will provide Comms Room space in your site(s) for the MSDD and/or NTE;
- (i) You will unbox, install and connect MSDD routers to power as well as to the connectivity that we provide;
- (j) Should you wish to reschedule or cancel a scheduled visit, you are responsible for notify us of your intention to reschedule an appointment in accordance with Section 3.2.

6.3 Service Dependencies

- (a) In instances where there is insufficient infrastructure, we reserve the right to charge ECCs. In these instances, lead-times may increase depending on the nature of the works required; and
- (b) Hardware refresh for MSDD End of Life (please see Section **Error! Reference source not found.** for further details).

7. Exclusions

- (a) Please note the Managed WAN Service does not include encryption. Should you require encryption, we will provide this service subject to an additional Fee, details of which will be included in your Order Form and/or SoW;
- (b) For Managed Service MSDD and NTE, any cross-connect cable is not part of this Managed WAN Service. If you are interested in a cross-connect, please contact your Account Manager for more detail.
- (c) For custom Quality of Service (QoS), if you require a custom QoS set-up, this item will be an additional Fee and will be described in a separate SoW.



- (d) Please note that we require an active licence with the relevant vendors MSDD to be able to apply patching in accordance with Section 2.9. If such licence is not in place, we will use reasonable endeavour to patch your MSDD, but our ability to apply patching may be limited.

8. Definitions and Acronyms

8.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
Access Service	A service used to provide access to connect each of your Site(s) to one of our core network's PoPs.
Excess Construction Charges	Charges applicable where the findings of a third party survey on the installation location establishes the need for additional work in order to provision the Services (e.g. lack of infrastructure at the installation site).
Managed Service Demarcation Device	This device marks the handover of the Service from us to you.
Point of Presence	Geographically diverse and resilient facilities (PoPs) spread across our NGN.
Statement of Work	A document which defines project-specific or client-specific activities, deliverables and/or timelines for providing services to that client.
VRF Any-to-Any Configuration	All sites are put within a secure technical grouping within the NGN. As standard, each site is permitted to see the other sites within the same group.

8.2 Acronyms

Acronym	Meaning
ADSL	Asymmetric Digital Subscriber Line
BGP	Border Gateway Protocol
DIA	Dedicated Internet Access
DSCP	Differentiated Services Code Point
ECCs	Excess Construction Charges
EFM	Ethernet First Mile
EoL	End of Life
FTTC	Fibre to The Cabinet
FTTP	Fibre to the Premise
GEA	Generic Ethernet Access
ICMP	Internet Control Message Protocol



Acronym	Meaning
MSDD	Managed Service Demarcation Device
MPLS	Multiprotocol Label Switching
NGN	Next Generation Network
NTE	Network Termination Equipment
PoP	Point of Presence
QoS	Quality of Service
RFC 1918	Definition of reserved IPv4 subnets for use only in private networks
SIP	Session Initiation Protocol
SoGEA	Single order Generic Ethernet Access
SoW	Statement of Work
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding



9. Operational Targets

Product		P1	P2	P3	P4
Resilient Access A+A	Response	30 mins	30 mins	1 hour	Next Business Day
Resilient Access A+B	Fix	4 hours	6 hours*	8 hours	3 Business Days
Resilient Access D+D					
Resilient Access A+C*	Hours of Support	24x7	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days
Resilient Access B+C*					
Standard Access D Type 1					
Standard Access A	Response	30 mins	30 mins	1 hour	Next Business Day
Standard Access B Type 3	Fix	6 hours	12 hours	24 hours	3 Business Days
	Hours of Support	24x7	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days
Standard Access C Type 5	Response	30 mins	30 mins	1 hour	Next business day
	Vendor Fix	Next Business Day	Next Business Day	Next Business Day	3 Business Days
	Hours of Support	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days
	Description	- For Resilient Access only, total loss of both Primary Access Service and Secondary Access; - For Standard Access D only, total loss of Primary Access Service.	- For Resilient Access Only, total loss of either Primary Access Service or Secondary Access; - Performance issues.	Non-service-affecting issue.	- Service Requests; - Non-Service affecting work and reports; - A required change or configuration alteration to a service.

* For Resilient Access A+C and B+C, the standard Fix Time Target is applicable to the resolution of issues solely attributable to Primary Access Service (A). For all other issues, the Fix Time Target is 40 hours.

The implementation of the service depends on our third-party' delivery time. The following target implementation times are exclusive of any time reasonably beyond the control of the Supplier:

- Up to 65-85 Business Days from Order Acceptance for Fibre Service (A);
- Up to 45-65 Business Days from Order Acceptance for Copper Service (B); and
- Up to 15 Business Days from Order Acceptance for Broadband Service (C) and Data Centre Service (D).



10. Service Levels and Service Credits

The Service will be delivered at the target level set out below for the percentage level described, against which service credits will be paid (as set out in the Billing Guide).

Service	Measurement	Period	Target	Service Level	Service Credit
Standard Access Service (A) and (D) only Resilient Access Service (A + C) Standard Access Service (B) only	Availability - The ability to transmit a 64-byte IP data packet from the MSDD to the Designated Reference Router over the active Access Service and receive the response whilst not Congested. The KPI is defined as the percentage of packets successfully received. The Service is Congested when the utilization of the available bandwidth is greater than 75%.	Calendar Month	99.9%	99.9% - 99.3% 99.3% - 98.85% Less than 98.85%	5% of monthly value of Recurring Fees 10% of monthly value of Recurring Fees 15% of monthly value of Recurring Fees
Resilient Access Service (A + A) and (A + B) and (D + D) only			100% exclusive of the time taken to technically switch between the primary and secondary connection	100% - 99.9% 99.9% - 99.3% 99.3% - 98.85% Less than 98.85%	5% of monthly value of Recurring Fees 10% of monthly value of Recurring Fees 15% of monthly value of Recurring Fees 20% of monthly value of Recurring Fees
Standard Fibre Service (A) Standard Access Data Centre Service (D) Resilient Access Copper Service (B and C)			99.9% For Resilient Access Copper Service (B and C), the target is exclusive of the time taken to technically switch between the primary and secondary connection.	99.9% - 99.3% 99.3% - 98.85% Less than 98.85%	5% of monthly value of Recurring Fees 10% of monthly value of Recurring Fees 15% of monthly value of Recurring Fees
Standard Access Copper Service (B)			99.15%	99.15% - 98.85% Less than 98.85%	5% of monthly value of Recurring Fees 10% of monthly value of Recurring Fees
Standard Access Broadband Service (C)			Best Endeavours		