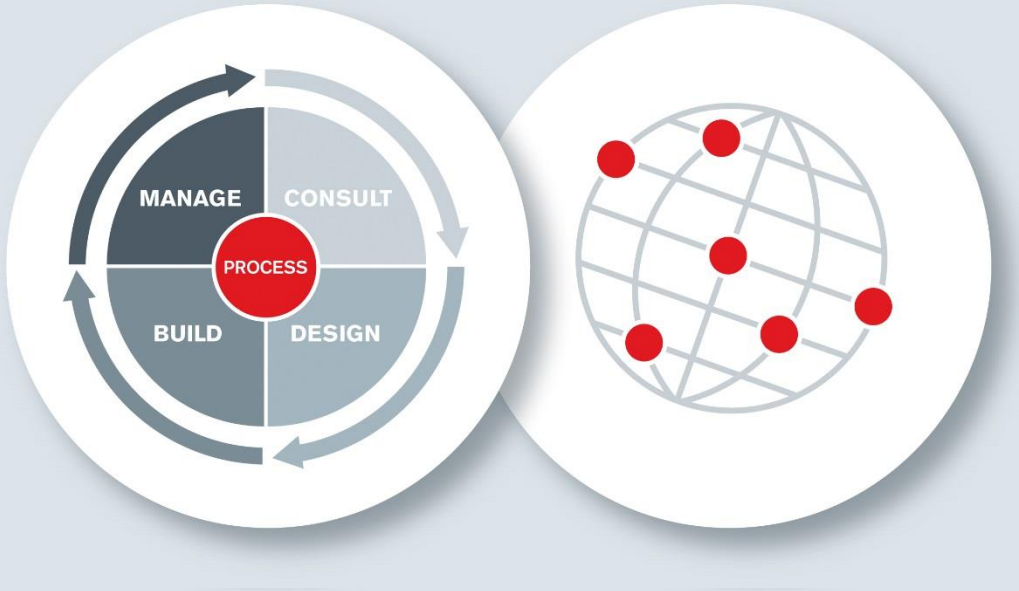
Claranet Service Description



MPLS Connectivity

Claranet MPLS solutions offer the ability to connect your national and international offices together into a private network. A range of connectivity options are available to suit any requirement from high availability Ethernet to Mobile Broadband. The latter connecting directly into your private MPLS network enabling temporary or fast start solutions.

Managed Firewalls in our data centres offer the ability to centralise your Internet connectivity and manage your Internet policies. In addition, you will benefit from our integrated cloud solutions by easy on-boarding services such as Cloud Connect, Hosted Voice and Data Backup.

Version 10.3

claranet
hosting | applications | networks

helping our customers
do amazing things

Contents

claranet

The Service Description

This Service Description describes the service Claranet provides and details your responsibilities in relation to this service. The Service Description forms part of the Agreement between the Parties and all terms used within this document are in accordance with the terms to be found in the Master Services Agreement.

Service overview

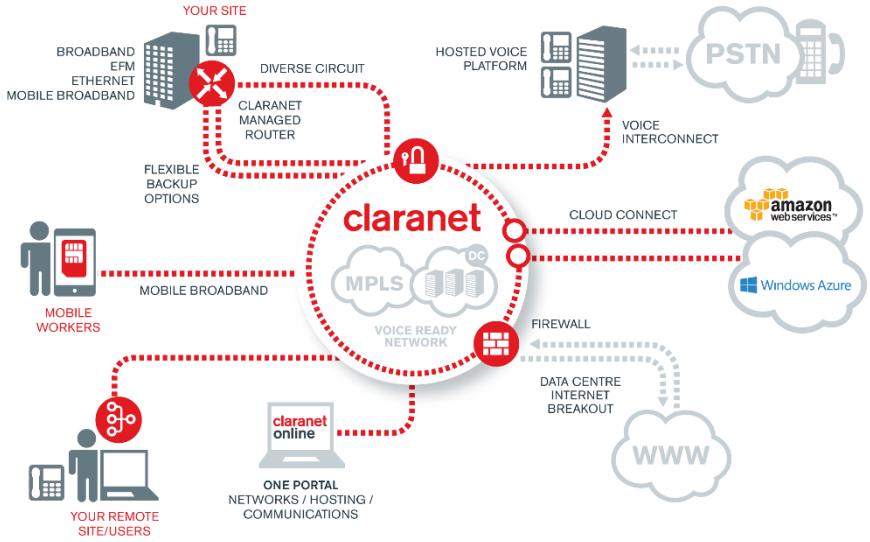
The primary function of Claranet's MPLS (Multiprotocol Label Switching) service is to provide you with a private networking service connecting your sites together. This will enable your IP based applications and services to communicate faster and more efficiently. The network is private as it is logically separated from other MPLS Services provided in the Claranet network, allowing you to define how the IP addressing and routing should work within your network.

Claranet's MPLS is a Virtual Private Network (VPN) service available across Claranet's international MPLS backbone. This solution provides you with a private network with any-to-any connectivity at IP layer 3 including Managed Routers. In addition, you can purchase value added services such as secure internet access through a managed firewall located in one of Claranet's Data Centres.

Options

Claranet MPLS provides physical connectivity to the MPLS backbone with logical private connectivity to one or many private VPN's using Ethernet, Ethernet First Mile, Broadband, FTTC, FTTP and Mobile Broadband Services. Layer 3 VPN's by default provide any-to-any connectivity between Customer Premises Equipment (CPE) nodes, but on request can be provisioned in a hub-and-spoke model.

An example of the various connectivity options can be seen in the diagram below and details of Ethernet sub-interfacing, EVC and Q-in-Q can be found in Appendix: Sub-Interfacing. **Full details of the various component options can be found in the Claranet Connectivity Component Description which acts as a support document to this one and should be read in conjunction with it.**



claranet

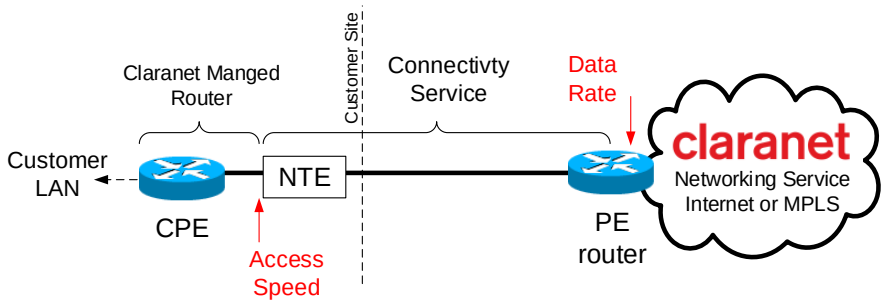
Component	Mobile Broadband	Broadband	FTTC	FTTP	EoFTTC	EFM Lite	EFM	Ethernet
Bandwidth	HSDPA	Up to 20Mbits/s download, 2.5Mbit/s upload	Up to 80Mbits/s download, 20Mbit/s upload	Up to 80Mbits/s download, 20Mbit/s upload	Up to 20Mbit/s		1-35 Mbit/s	2Mbit/s – 10Gb
Symmetric bandwidth					● [2]	● [2]	●	●
Guaranteed bandwidth					●	●	●	●
Dedicated bandwidth					●	●	●	●
Proactive monitoring – Up/Down status		Option [1]	Option [1]	Option [1]	●	●	●	●
Resiliency options		Broadband, Mobile Broadband	Broadband, FTTC, Mobile Broadband	Broadband, FTTC, FTTP, Mobile Broadband	Broadband, FTTC, FTTP, EoFTTC, Mobile Broadband	Broadband, FTTC, FTTP, EoFTTC, EFM, Mobile Broadband	Broadband, FTTC, FTTP, EoFTTC, EFM, Mobile Broadband	Broadband, FTTC, FTTP, EoFTTC, EFM, Ethernet, Mobile Broadband

[1] As part of the MPLS network

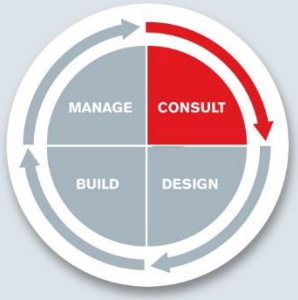
[2] Symmetric Bandwidth is available up to the maximum upstream speed achievable on the circuit.

There is considerable flexibility within the choice of connectivity (as can be seen in the table above). The Claranet MPLS service will cover the access link to your premises, up to and including the NTE and includes Managed Routers as standard A wires only Service is available to channel partners who wish to supply their own equipment. The following diagram outlines these demarcation points.

Claranet connectivity demarcation points



claranet



Consult

Claranet's consulting process ensures that you have the right information, the right recommendations, and the right service options available to you to achieve your business outcomes.

Understanding your business is paramount to ensuring that you have the right solution for your business outcomes. In the Consult stage, Claranet will discuss your business requirements with you prior to recommending a solution. In many cases, Claranet MPLS service may be part of a larger solution involving other connectivity or hosting services or both.

Depending on the complexity of requirements, one or more workshops between you and Claranet may be arranged in order to outline your requirements. These may be conducted by Network Consultants, Strategy Consultants, Solutions Architects and Enterprise Architects who will be applied at our discretion. It is in everyone's interests to ensure that the proposed solution will meet your requirements and one of our first roles is to focus on your business, your IT and connectivity requirements and to produce a high level scoping report, the High Level Options Analysis. This will allow you to make an informed choice as to the recommended path.

High Level Options Analysis

What Claranet will do

Deliverable: The High Level Options Analysis report is a short, high-level scoping document.

Time to complete: The High Level Options Analysis is a consulting based service and is included up to a maximum of 2 days work at Claranet's discretion. In some instances, the work required to produce a High Level Options Analysis could extend beyond this e.g. where the requirements need extensive discussion or the options are particularly complex. If this is the case, Claranet will agree with you a charge for the additional work required to produce a High Level Options Analysis to establish the requirement.

What Claranet will do

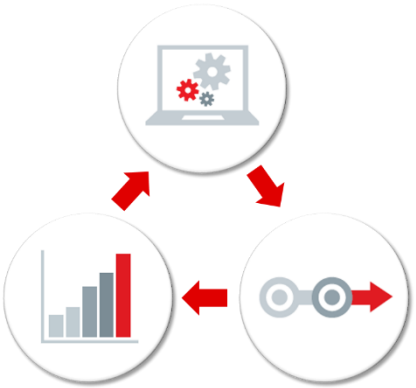
Technical Design: Technical work beyond this falls outside of the scope of the High Level Options Analysis and is carried out in the Design phase.

What you will do

Information sharing: Provide any requested information to allow Claranet to deliver a High Level Options Analysis. This will include full details of on-going technical contacts within your organisation. This information will form the basis of the Initial Configuration, so it is your responsibility to ensure the information provided is correct.

Packaged Consulting

Claranet has a number of pre-packaged assessments and audits that help to outline your readiness in respect of particular IT options. It may be that the completion of one or more of these packaged consultancy engagements is made as a result of the recommendations made in the High Level Options Analysis report. The completion of these assessments follow a general pattern:



Current State

Performing a real life assessment of your current environment and understanding where your business needs, and your current technical setup, may diverge.

Future State

A vision of the future for your company, taking into account strengths, weaknesses, opportunities and threats.

Transformation

The enablement program to be undertaken as a priority to advance your organisation to the desired level of maturity.

What Claranet will do

Examples of pre-packaged assessment options:

- Linux Infrastructure Maturity Assessment (LIMA)
- Infrastructure Maturity Assessment (IMA)
- Cloud Readiness Assessment
- Open Source Assessment

Pricing: This additional packaged consulting service is optional and is a chargeable event. Claranet provides three prices for each assessment depending on the size of your company and the complexity of your requirements: Small / Medium / Large.

Consulting

A packaged consulting approach can be of significant help to many organisations. However, Claranet also provide a specialist consulting service that can be used at any time (including pre-contract) to help you in areas outside of the packaged offering. This engagement is specific to you and can cover any area that is needed with regard to your business and technology.

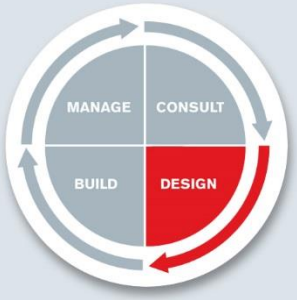
What Claranet will do

Specialist consulting: Provide a range of specialist expertise in a variety of areas. This includes a detailed focus on your business in order to ascertain the scoping requirement or where you are unsure as to the direction your business should take in the ever-changing IT environment.

Outcomes: Provide a full and detailed report on your available options along with recommendations of the next steps to take.

Pricing: This additional consulting service is optional and is a chargeable event and is based on a consultancy day rate.

claranet



Design

Your Claranet MPLS service will be designed to meet your requirements. The decision as to how this fits within any connectivity solution is made in the Design stage.

Claranet offers a comprehensive Solution Design Service as standard for all prospective MPLS customers. Claranet will discuss with you, your business and technical requirements, and will design a MPLS solution. Claranet will deliver where required a detailed description of the technical design including a network diagram and Statement of Works. It may be part of a larger document if the MPLS network is part of a larger solution. This forms part of your agreement and will provide the technical specifications for your solution.

The MPLS standard design service uses information provided by you as the primary influence to the proposed solution.

At this design phase it is your responsibility to ensure that Claranet has the correct site address, contact and technical information for the proposed MPLS solution. Although changes can generally be made during installation, delays and additional fees may be incurred.

What Claranet will do

Deliverable: A proposal document and a Statement of Works which may be part of a larger solution document, and which forms part of your agreement which is detailed enough to allow a full quotation.

Standard level of design work: Produce design work on your proposed solution at a level commensurate with that of the market. It will be sufficient to allow further decisions to be made and may include input from a Claranet Sales Specialist.

Additional components: In the event that additional components are required outside of the SoW, Claranet will levy additional charges for the implementation and management of the modified solution. If this is the case, a new proposal and SoW document is produced. This must then be signed by you to acknowledge and accept the changes before any work is performed.

What you will do

Outline: Outline the purpose of any requirements to Claranet, in order to ensure that Claranet may assess whether the solution is suitable for the requirement.

Information: Provide Claranet with the correct site address, contact and technical information for the proposed MPLS solution.

Network sales specialist

As part of your MPLS connectivity service, Claranet provides a Network sales specialist who has detailed knowledge within this particular field, or within your own specialist vertical industry, and will support your Account Manager and Solutions Architect with your proposal. Part of their role is also to help ensure that the proposed technical solution will fit your business and achieve the outcomes you are looking for.

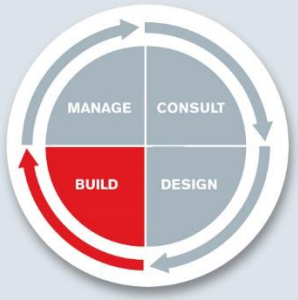
However, at times, the complexity of your solution design will require additional or specialist design work in order to detail your requirements.

What Claranet will do

Specialist level of design work: Produce technical design work on your proposed solution in order to specify your requirements fully. This may be completed by a Solutions Architect or a Claranet Technical Specialist in that particular field.

Pricing: This additional specialist solution design service is optional and is a chargeable event and is based on a day rate for the service.

claranet



Build

Once your order has been placed, Claranet will advise on installation and configuration of your MPLS network.

The Build section covers the steps involving the configuration and installation of the MPLS network according to the agreed specifications. At the completion of this phase. Once set up, any future changes are explained as part of In-Life Management, details of which can be found in the Manage section.

Specialist engineering

It may be that your particular setup requires additional specialist engineering work. This will be quoted individually and could include specialist change requests, work on piloting projects or prototyping.

What Claranet will do

Specialist engineering: Provide a quotation for specialist engineering work based on a day rate.

Project Management

Some Claranet projects are small, simple and very straightforward and the management of these is part of the normal operation carried out by your Account Manager, the Solution Architect and Project Co-ordinator who are already built into the cost of delivering your standard service. Other Claranet projects are much more complex and require more comprehensive project management to bring together the many elements that are needed. Claranet is conscious of the fact that the introduction of a Claranet Project Manager is a chargeable event but will suggest this when we believe it is justifiable and necessary.

In addition, it may be that only a short time needs to be spent by a Claranet Project Manager in overseeing and authorising the Claranet project e.g. at the start of the project, where the project is then managed by a Project Co-ordinator, helping to keep your costs to a minimum.

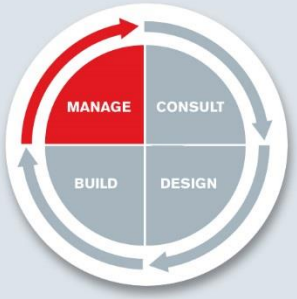
What Claranet will do

Project Management: Allocate a Claranet Project Manager who is PRINCE2 qualified who will ensure that the project is initiated, implemented, carried out and closed according to PRINCE2 methodology and will be responsible for the overall control and management of the Claranet project. Full details of this can be found in the Project Management Service Description and from your Account Manager.

Acceptance procedure

Once the MPLS solution is setup and connected, the ongoing management is under the process of the In-Life Management process.

claranet



Manage

Your solution is managed In-Life by our Service Operations team who provide a pro-active, ITIL aligned service.

In-Life Management

Once your MPLS network is up and running, Claranet will monitor your network against a number of performance and availability metrics to ensure that the network remains live and operational within the Service Levels.

Planned changes, emergency maintenance

What Claranet will do

Notice: Provide at least seven working days' notice of any planned maintenance work where an outage is expected, wherever possible.

Supplier planned Engineering: Notify you of any supplier planned engineering works where it is likely that you will experience an outage within one day of receipt of the notification from our supplier wherever possible.

Notification: Notify your nominated contacts through two primary channels, Claranet Online and by email notification. An email is sent to the nominated contact and details are announced through the notifications in Claranet Online. The notification will contain the date and time of the maintenance, the reason, the service affected and the likely impact to you.

Problems occurring during planned maintenance: The Major Incident process will be invoked during the maintenance window where a rollback or issue mitigation process does not exist, or should the planned work extend beyond the planned maintenance window.

Emergency maintenance: Provide as much notice as possible and we will seek to ensure minimal disruption. Wherever possible, changes will be made at periods of low service utilization. It may be necessary to make changes **without** prior notification to ensure the continued operation of the managed service.

What Claranet will do

Patching: Apply all critical patch updates on an as required basis.

Emergency outages: In some extreme cases, Claranet may require an emergency outage to rectify a problem. In such cases, Claranet will work with you to agree a mutually convenient time, but you agree that in such cases the problem cannot be rectified until the outage has taken place.

What you will do

Contact list: You will be responsible for providing and maintaining the contact details including the levels of authorisation that any individuals may have. Claranet will only provide any reporting information and change requests, to those personnel in accordance with this information. These details can be maintained within Claranet Online.

Changes requested by you

Where you require specific changes to be made or wish to request a help desk ticket, these can be made by raising a ticket through Claranet Online and details of how to do this can be found in the **Appendix: Help and Support**.

claranet

What you will do

Change control process: It is your responsibility to familiarise yourself with the official Claranet change control process and to follow this process every time a change to the Service is required. Details of this process can be found in **Appendix: Help and Support.**

Change request impact: It is your responsibility to ensure that any changes will not directly cause a service outage or other disruption of the service.

Change of services: If you request a new service, a change of service type, or a change in service features they must be requested via your Account Manager and may be subject to prevailing fees.

When a threshold is breached

What Claranet will do

Pro-active alerts: Set up pro-active alerts that are in place on the platform and network to ensure there are no bottlenecks.

What you will do

Contact support: If you do experience continued loss of performance, please contact the Claranet support desk and raise a support ticket so that it can be investigated.

If a threshold is breached or a service affecting event occurs, the Claranet Operations team are notified to raise a ticket and take appropriate action to resolve the issue. This could include troubleshooting and resolving the problem, or notifying you that your network has a specific problem. There are predefined response times to event notifications based on the severity of the issue. These are outlined below.

What Claranet will do

Severity response times: Respond to a threshold breach depending on the severity of the breach:

Major:
Claranet will acknowledge any alarms on the system within 30 minutes

Minor:
Claranet will acknowledge any alarms on the system within 60 minutes

Warning:
Claranet will acknowledge any alarms on the system within 1 day

Change to monitoring tools: Reserve the right to change its monitoring tools, methods, parameters and polling intervals over time

Help and support

Service Desk support

What Claranet will do

Support times and Service Desk: Provide support 24x7x365 once the MPLS service has been set up.

Raising tickets: Changes to your service configuration can be made through the Claranet Online ticket request and details of this can be found in the **Appendix: Help and Support**.

Escalation: In the event that an escalation is required, Claranet provides a clear escalation process to allow you to contact the appropriate person within the company. Details of this can be found in the **Appendix: Help and Support**.

Service Levels

The Service Level determines the parameters by which the service is accountable. Details of the metrics showing the expected service levels can be found in the **Appendix: Service Levels.**

What Claranet will do

Information delivery: Obtain the results for each of the metrics and contact you according to your list of authorised contacts in the event that any results fall outside of the acceptable parameters.

Archiving results: Retain an archive version of the monitoring results for up to 90 days which can be available to you on request through the Claranet Online portal.

Metrics exceeding the thresholds: In the event that a monitored metric exceeds the acceptable thresholds, Claranet will raise a support call to investigate the incident and contact you in accordance with the escalation details held.

claranet

Appendices

Here you will find further information regarding the technical specifications of the service as well as standard procedures and agreements.

Appendix: Sub-Interfacing

Sub-interfacing allows for multiple logical channels to be configured on the Ethernet circuit to keep traffic logically distinct for routing and/or security purposes. This is most commonly used to keep public Internet (insecure) and private MPLS (secure) traffic separate.

Where sub-interfaces are supported they can either be presented to the LAN as separate physical Ethernet interfaces (as long as the CPE has sufficient ports of the correct type) or as multiple VLANs on a single interface. Where Claranet is providing the router configuration, the default configuration provided will be the latter, unless specifically requested otherwise.

Sub-interfacing is available for the following Services:

Service	Sub-interfaces
Ethernet	Multiple EVC
Ethernet	Q-in-Q

Claranet offers two methods of delivering multiple VLANs:

- Multiple Ethernet Virtual Connection
- Q-in-Q

Multiple Ethernet Virtual Connection (EVC)

EVCs are logical pathways between your site and the Claranet core network. They have bandwidth associated with them that is then used to allow information exchange between sites. For example a 100Mbit/s Ethernet circuit may have an EVC with a bandwidth of 50Mbit/s.

When multiple EVCs are delivered on a single Ethernet circuit, the sum of all the EVCs must not exceed the capacity of the Ethernet circuit.

Q-in-Q

Q-in-Q is used to deliver multiple VLANs over a single Ethernet Virtual Circuit (EVC). Each sub-interface by default will contend for the full bandwidth of the EVC on an equal footing with no prioritisation of one over the other. Alternative QoS may be enabled to configure bandwidth profiles for each sub-interface.

The table below describes the Q-in-Q options available:

Service	Multiple EVCs / VLANs	Q-in-Q
Maximum number of VLANs	4	4
Delivered as standard on a single LAN Port	Yes	Yes
Option to deliver on multiple LAN ports	Yes	Yes
Dedicated bandwidth on each VLAN	Yes Bandwidth for each EVC is guaranteed. A VLAN will not consume the bandwidth of another.	Default - No By default bandwidth is shared across all VLANs. A VLAN can consume the full circuit bandwidth. QoS may be applied to allow bandwidth profiling.
Option to deliver each VLAN to different POPs	Yes	No
Bandwidth limitations	The sum of each VLAN cannot exceed the bearer size.	The sum of each VLAN cannot exceed the bearer size.
Quality of Service (QoS)	Yes	Yes
Bandwidth changes	Reconfiguration of other VLANs may be required	Yes

Appendix: Components

Default route

Claranet is able to configure a default route within your VPN, allowing access to IP networks outside of the realm of the MPLS. The most common use for a default route is to provide Internet access to the sites in the VPN.

The VPN default route can be used in conjunction with an Internet Breakout Service, where Claranet provide a gateway to the Internet, protected with a Managed Firewall generally located either at the your main office or in a Claranet data centre.

Internet connectivity

Internet connectivity from the MPLS network may be provided through Claranet data centres. This offers a centralised breakout from the MPLS network through a high availability data centre which reduces the risk of having an Internet breakout from a single site on the MPLS network.

Internet connectivity can be achieved via a number of Firewall options located within the data centre:

- Platform Firewall
- Physical firewalls
    - Single firewall
    - High Availability firewall
- Co-located firewall

Please refer to the Claranet Managed Firewall Service Description for details on the Managed Firewall options available.

Internet connectivity from the MPLS network to the internet may also be achieved from a site on the MPLS network. When this option is taken the site used to connect to the internet must be served by an Ethernet circuit from the MPLS network to the site. The internet connectivity from the site to the Internet may be in the form of Ethernet, Ethernet First Mile, EoFTTC, FTTP, FTTC or DSL.

The table below describes the connectivity bandwidth options available when breakout to the internet is from the data centre:

Part number	Description
Internet connectivity from data centre	Managed Internet Bandwidth: 20 Mbit/s
	Managed Internet Bandwidth: 50 Mbit/s
	Managed Internet Bandwidth: 100 Mbit/s
	Managed Internet Bandwidth: 200 Mbit/s
	Managed Internet Bandwidth: 300 Mbit/s
	Managed Internet Bandwidth: 400 Mbit/s
	Managed Internet Bandwidth: 500 Mbit/s
	Managed Internet Bandwidth: 1000 Mbit/s
MPLS port to centralised Firewalls	Managed Internet Bandwidth: 100 Mbit/s
	Managed Internet Bandwidth: 1000 Mbit/s

Appendix: Quality of Service

Quality of Service (QoS) is a data traffic classification and prioritisation feature available on a number of Claranet access services.

Quality of Service has two main functions; one is to identify and classify the IP data by application; the other is to prioritise certain application classes over others if the connectivity service becomes congested. QoS is enabled on the connectivity link between the equipment located at your site (Customer Premises equipment - CPE) and the equipment at the associated edge of Claranet's network (Provider Edge – PE). Depending on the type of access service, there are different levels of QoS available.

QoS on Broadband and FTTC/FTTP services offer up to three levels of application classification. Within this, the first class is given a priority over all traffic whilst the optional second class will take a precedence over standard traffic on any remaining bandwidth, which falls into the third class. QoS on Ethernet services (including the Ethernet Fist Mile products) offer up to six levels of application classification and prioritisation.

Quality of Service offers guarantees that the data traffic classified and prioritised at the edge of the network is transported over the Access Service and Claranet Core within a defined set of quality performance metrics. Claranet control the performance of the Core Network through a combination of capacity management and congestion management techniques.

Ethernet-QoS SLA performance metrics are Customer Site to Customer Site, based on a combination of the performance guarantees of the access services used to connect the Customer Site to the Claranet Core, and the performance guarantees within the Claranet Core. When an access service does not have performance guarantees (for example broadband or FTTC/FTTP services), QoS SLA performance metrics are not available for that link.

QoS is available only when a compatible CPE is provided by Claranet or a MPLS accredited partner, and where the connectivity service itself support QoS.

QoS access service compatibility

The following table highlights the access Service compatibility with Quality of Service (QoS):

Service	QoS available	QoS classes
Ethernet	Yes	6
Ethernet First Mile	Yes	6
Ethernet First Mile Lite	Yes	6
Ethernet over FTTC	Yes	3
FTTC / FTTP	Yes	3
Broadband	Yes	3
Broadband Core	No	None
Mobile Broadband (3G)	No	None

Ethernet QoS

Claranet Quality of Service offers up to six levels of application classification. In some circumstances (such as very high capacity links, or very complex networks) all six classes will be used, but in majority of cases no more than three separate classes are needed. This kind of QoS applies to Ethernet and Ethernet First Mile services. The table below illustrates the classes available:

Application classes	Queuing technique	Example application
Gold	Low Latency Queue	Voice over IP
Silver-1	Class Based Weighted Fair Queue	Citrix
Silver-2	Class Based Weighted Fair Queue	EPOS
Silver-3	Class Based Weighted Fair Queue	Intranet
Silver-4	Class Based Weighted Fair Queue	Internal Messaging
Default	Weighted Fair Queuing	Web browsing

Gold

The ‘Gold’ queue is a strict priority queue designed specifically for real-time voice and video applications. The purpose of a strict priority queue is that while the flow of data in question remains within pre-defined limit of bandwidth, no other traffic on the same link can affect the flow of the priority queue. All Gold data above the configured committed data rate (CDR) for this queue will be dropped.

It is very important that enough bandwidth is allocated to Gold, as dropping data from this application class will be highly detrimental to the real time applications that use this class.

Silver

The ‘Silver’ queue is a group of prioritised queues making use of Class Based Weighted Fair Queuing and Weighted Random Early Detection (WRED) congestion management techniques. This queue is preferred above Default and designed for non-real-time business critical applications.

All ‘Silver’ data above the configured committed data rate (CDR) for this queue will be dropped. If only one Silver Queue is configured, it will be given priority over the Default queue. If more than one ‘Silver’ queue is configured, each ‘Silver’ queue is given a priority weighting against the other ‘Silver’ queues within the bandwidth allocated for all ‘Silver’ queues.

The weighting used to determine how much bandwidth is available for each Silver Class is calculated based on a ratio of the total bandwidth allocated to Silver and the level of Silver used. For example, where two Silver classes are used, classifying one application as Silver-1 and another as Silver-4 will give far greater priority to Silver-1 than if one application is classified Silver-1 and the other Silver-2.

Default

The ‘Default’ queue can take advantage of the full access-link bandwidth if the Gold or Silver queues are not enabled or if there is available bandwidth not being utilized by the priority or weighted fair queues. Default also uses WRE

Allocation of bandwidth with QoS

Once a decision has been made on the applications that need to be prioritised, and in what classes they should sit, bandwidth will need to be allocated to each class. The amount of bandwidth allocated to each class will influence the prioritisation decisions that the network will need to make if the Connectivity Service were to become congested.

The following are limitations to how much bandwidth or ‘weighting’ each class can have in a Class of Service Prioritised link:

1. It is not possible to allocate more than 75% of the link bandwidth to the Silver Classes.
2. The maximum amount of bandwidth that can be allocated to a Gold class is 50% of the total link bandwidth.
3. The minimum amount of bandwidth that can be allocated to Gold is 100 Kbps.100Kbp/s.
4. Gold bandwidth allocation must always be configured by speed symmetrically, i.e. the same downstream allocation as upstream.
5. Silver bandwidth allocation can be configured asymmetrically, but the rules regarding maximum percentage allocation on a link must be honoured, in both directions.
6. Where a link has both Gold and Silver classes configured; the combined total of the bandwidth allocated to these Classes must not exceed 75%. The remaining 25% is used for CPE management and Default data.
7. The bandwidth value allocated to any Class must be based on 10 Kbps10Kbps increments.

There is no specific bandwidth allocated to Default applications, although applications in this class will have less congestion management (therefore better performance) if less of the total link is allocated to the prioritised Classes.

The following table summarises the above rules:

Application classes	Minimum bandwidth allocation per class	Maximum bandwidth allocation per class	Maximum total application
Gold	100 Kbps	50%	
Silver-1	N/A	75%	75%
Silver-2		75%	75%
Silver-3			
Silver-4			
Default	Not allocated	Not allocated	Not allocated

Application classification

Customer Application Traffic destined for either the Gold or Silver queues must be marked appropriately with either IP Precedence or DiffServ Code Point (DSCP), either by you yourselves on the client and server devices, or by the Claranet CPE. By default the following values will signal the traffic to be forwarded into the queues marked below:

DCSP value	IP precedence value		QoS class
EF	5	101	Gold
AF41	4	100	Silver-1
AF31	3	011	Silver-2
AF21	2	010	Silver-3
AF11	1	001	Silver-4
BE	0	000	Default

Claranet can support classification on the CPE by using either access lists to define the source or destination port and protocol used by the application, or by using Cisco NBAR (Network based Application Recognition) to define the application used. More information on Cisco NBAR and what applications it will recognise is available from Cisco's website.

All traffic marked with either IP precedence or DSCP values on non QoS enabled VPN tail circuits shall be remarked to zero at ingress and prioritised using the 'Default' queue.

Ethernet over FTTC QoS

Claranet Quality of Service offers up to three levels of application classification on Ethernet over FTTC. The table below illustrates the classes available:

Application classes	Queuing technique	Example application
Gold	Low Latency Queue	Voice over IP
Silver	Class Based Weighted Fair Queue	Citrix
Default	Weighted Fair Queuing	Web browsing

claranet

Gold

The ‘Gold’ queue is a strict priority queue designed specifically for real-time voice and video applications. The purpose of a strict priority queue is that while the flow of data in question remains within pre-defined limit of bandwidth, no other traffic on the same link can affect the flow of the priority queue. All Gold data above the configured committed data rate (CDR) for this queue will be dropped.

It is very important that enough bandwidth is allocated to Gold, as dropping data from this application class will be highly detrimental to the real time applications that use this class.

Silver

The ‘Silver’ queue is a group of prioritised queues making use of Class Based Weighted Fair Queuing and Weighted Random Early Detection (WRED) congestion management techniques. This queue is preferred above Default and designed for non-real-time business critical applications.

All ‘Silver’ data above the configured committed data rate (CDR) for this queue will be dropped. Traffic in the Silver Queue will be given priority over the Default queue.

Default

The ‘Default’ queue can take advantage of the full access-link bandwidth if the Gold or Silver queues are not enabled or if there is available bandwidth not being utilized by the priority or weighted fair queues. Default also uses WRED congestion management.

Broadband QoS

This type of QoS is aimed at prioritising voice traffic on Broadband and FTTC/FTTP access services. There are three levels of application classification. The first class is reserved for voice traffic and manages latency, packet loss and jitter to ensure voice applications run smoothly. A fixed assured bandwidth figure is set for this class and the class has priority over the remaining two classes.

The second class, which is an optional class designed for premium data, is then given a precedence over standard traffic on the remaining bandwidth. Standard traffic will fall into the default class (see below).

With QoS on Broadband, traffic traversing the carrier network is all equally weighted. The classification and prioritisation of traffic is managed on the Claranet core network and CPE router endpoints.

QoS class	DSCP value	Example application
Priority class	EF	Voice over IP
Precedence class	AF21	Citrix
Default class	Default	Web browsing

Priority class (EF)

The priority class is exclusively for voice traffic. The EF queue is a strict priority queue where data flow remains within a pre-defined bandwidth limit, no other traffic on the same circuit can affect the flow of the priority queue. Any EF data above the configured committed data rate (CDR) for this queue will be dropped. The bandwidth values that can be assigned to this class are as below, with an indication of how many concurrent voice calls this bandwidth will support (using the G.711 codec):

EF bandwidth value	Maximum number of concurrent calls (using G.711 code)
220 Kbps	2 calls
350 Kbps	3 calls
700 Kbps	6 calls
1000 Kbps	8 calls

Precedence class (AF21)

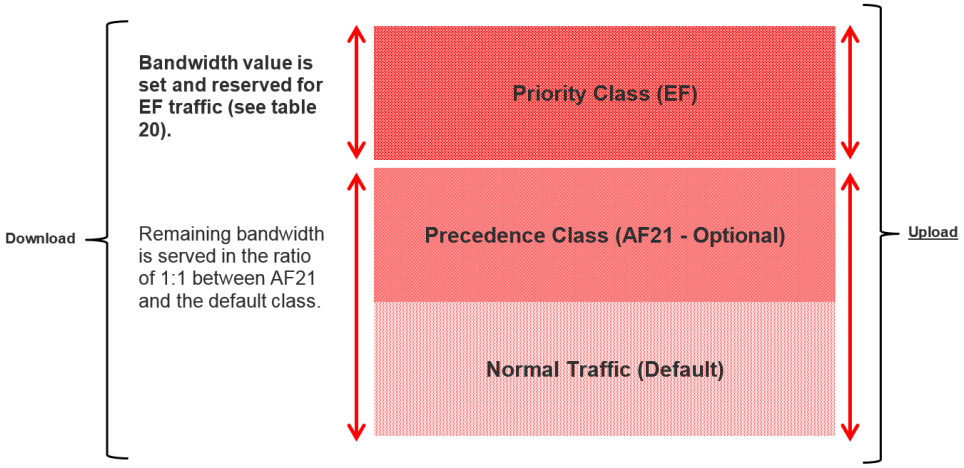
There are two options available for QoS on Broadband that determine the behaviour of the precedence class, Option A and Option B.

With Option A, the precedence class is given the same weighting as the default class. With Option B, the precedence class gets a higher weighting that the default class. In both cases, this does not affect the EF priory queue.

The use of the precedence class is optional. If no traffic is marked AF21 then all traffic (outside of the EF priority queue) will be treated the same regardless of which precedence option is used.

Option A (1:1 ratio)

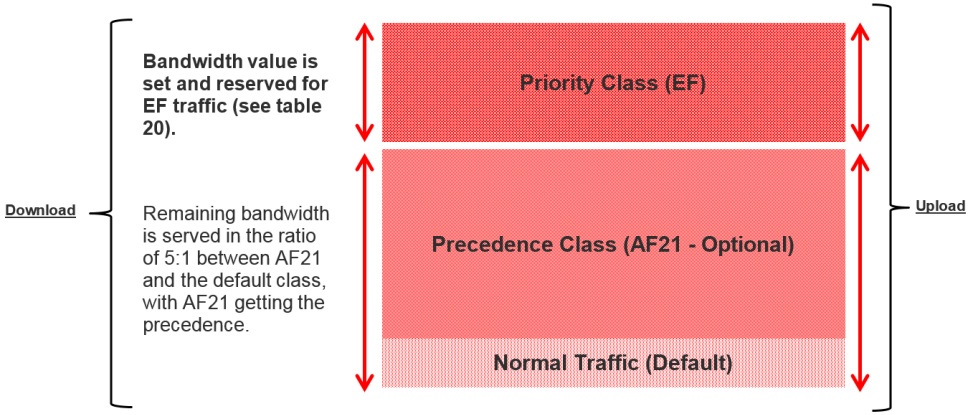
Option A assigns 100% of the prioritised bandwidth to the priority class (EF). The precedence class (AF21) has an equal weighting with the default class for any remaining bandwidth (remaining bandwidth is served in the ratio of 1:1 between AF21 and the default class).



If the amount of EF traffic exceeds the prioritised bandwidth profile then the excess EF traffic will be policed and discarded.

Option B (5:1 ratio)

Option B assigns 100% of the prioritised bandwidth to the priority class (EF). AF21 traffic has precedence over traffic in the default class for any remaining bandwidth in the ratio of 5:1 (remaining bandwidth is served in the ratio of 5:1 between AF21 and the default class).



Default class (Default)

Traffic that is not marked EF or AF21 will fall into the default queue. This queue will take advantage of the full circuit capacity if there is no EF or AF21 traffic utilising the priority or precedence queues.

Service restrictions for QoS on Broadband

- QoS on Broadband is only available on MPLS Broadband and FTTC/FTTP services with the Elevated Best Effort Traffic option.
- The use of the EF class for any traffic other than voice will not be supported by Claranet.

claranet

- Claranet are unable to provide any logging on QoS performance, real time or historical. QoS statistics from the CPE router will be used during troubleshooting to ensure and demonstrate the QoS service is working correctly.
- A compatible and approved Claranet managed Cisco router is required to run the QoS on Broadband service.
- In the event that the selected bandwidth for the Priority Class is greater than the achievable upstream bandwidth on the circuit, Claranet will select the highest value that the line will support instead.

Appendix: MPLS Core network

Service availability

Claranet guarantees **99.99% availability** of the MPLS Backbone, measured using the aggregate Provider Edge router to Provider Edge router network availability. Performance is measured as a monthly average in arrears from the Service Commencement Date and each month thereafter.

Network performance

The following details the performance metrics used to measure the performance of the MPLS core, and what targets and/or guarantees are available on these metrics.

There are different guarantees for traffic depending upon the class (Gold, Silver or Default) it has been allocated to on the network. All traffic is marked Default, unless you have purchased the optional Quality of Service (QoS) feature, in which the additional service levels applicable to Gold traffic can apply, but they can only be applied to the traffic that has been allocated to the Gold class, not to all traffic at a given site.

Gold traffic

Gold traffic - Round Trip Time (RTT)

Claranet offers the following maximum RTT guarantees for your data allocated to the optional Gold traffic class. These guarantees apply only to such traffic as has been allocated to this class, with all other traffic being subject to the core RTT guarantees in the previous section. Performance guarantees are based on provider edge to provider edge measurements. Performance is measured as a monthly average in arrears from the Service Commencement Date and each month thereafter.

Gold Round Trip Time Country provider edge to country provider edge RTT guarantee /ms						
	UK[1]					
UK[1]	10	**FR**				
FR	30	10	**ES**			
ES	50	40	10	**NL**		
NL	30	25	60	10	**DE**	
DE	45	30	70	40	20	**PT**
PT	40	60	75	65	75	10

[1] As measured from London Provider Edge Router

Gold traffic – packet loss

Claranet offers the following maximum packet loss guarantees for your data allocated to the optional Gold Service crossing the MPLS core network. Performance guarantees are based on Provider Edge to Provider Edge measurements. Performance is measured as a monthly average in arrears from the Service Commencement Date and each month thereafter.

claranet

Gold Packet Loss Country provider edge to country provider edge Packet Loss guarantee	
Any to Any	0.05%

Gold traffic - jitter

Claranet offers the following maximum jitter guarantees for your data allocated to the optional Gold Service crossing the MPLS core network. Performance guarantees are based on Provider Edge to Provider Edge measurements. Performance is measured as a monthly average in arrears from the Service Commencement Date and each month thereafter.

Gold Jitter Country provider edge to country provider edge Jitter guarantee /ms	
Any to Any	20 ms

Silver and Default traffic

Silver and Default – Round Trip Time (RTT)

Claranet offers the following guarantees relating to maximum backbone network Round Trip Time (RTT) across the MPLS core network. Performance guarantees are based on provider edge to provider edge measurements. Performance is measured as a monthly average in arrears from the Service Commencement Date and each month thereafter.

Silver and Default Round Trip Time Country provider edge to country provider edge RTT guarantee /ms						
	UK[1]					
UK[1]	15	**FR**				
FR	35	15	**ES**			
ES	55	45	15	**NL**		
NL	40	30	65	15	**DE**	
DE	50	35	75	45	25	**PT**
PT	45	65	35	70	80	15

[1] As measured from London Provider Edge Router

Silver and Default – packet loss

Claranet offers the following maximum packet loss guarantees for your data crossing the MPLS core network. Performance guarantees are based on provider edge to provider edge measurements. Performance is measured as a monthly average in arrears from the Service Commencement Date and each month thereafter.

Silver and Default Packet Loss Country provider edge to country provider edge Packet Loss guarantee	
Any to Any	0.1%

claranet

Appendix: Support

Help and Support

Change Control Process

Claranet's Change Management team are responsible for requests relating to any product and service configuration changes you wish to make that can't be made through the web portal. The team specialise in configuration and follow strict processes and ensuring that the changes are authorised. The Change Management team are also responsible for Claranet's Change Advisory Board (CAB), which discusses and approves changes raised internally. To make a change request, see the section below on "Raising a support ticket".

Raising a support ticket and a Request For Change (RFC)

Claranet provides two ways for your approved contacts to raise, track and update standard support tickets; through Claranet Online and by telephone. For security and audit reasons, you are required to make all requests for change through the Claranet Online portal and only portal users with the correct privileges can request a change. You will only see your services listed so please select the service relating to the request for change. In the event that the customer portal is unavailable, please contact Claranet by telephone, where an emergency procedure will be in place to log change requests on your behalf. Request for changes will not be accepted through this number at any other time.

What Claranet will do

Through Claranet Online: The most efficient way of raising support tickets is through the Claranet Online portal. The ticket you raise is assigned to the appropriate support team based on the service you need the support for. You will only see your services listed so please select the service relating to the incident or to the service request. The response time will start from as soon as your ticket has been submitted.

By telephone: When choosing to raise a support ticket using the telephone you must provide proof of identity following Claranet's standard security procedure. The response time will start from as soon as your telephone call has ended.

Escalating a ticket

In the event that you need to escalate a ticket, Claranet is ready and available to help you quickly bring your issue to closure. Within each level of the escalation path the person you speak with is responsible for evaluating your situation, facilitating the resolution plan and acting as your sponsor. The benefits of the escalation procedure are:

- ITIL accredited staff owning your escalation
- A focus on service recovery
- Improved communication
- Consistent process

An escalation may be initiated when, after working through our standard support processes and with our teams, you are not satisfied with the level or timeliness of the service you have received. Additionally, an escalation should be initiated when there is tangible impact to your production environment, or there is high risk to your business operations.

What Claranet will do

Escalation Manager: Assign an Escalation Manager who will deal with your escalation and collaborate with you to develop a communication plan. A technical plan of action may be needed to ensure resolution of a technical issue. Your Escalation Manager works as your advocate internally and will become a virtual member of your own problem resolution team. Should you feel dissatisfied with the escalation process, please contact your Account Manager directly.

Service Delivery – Fix levels and response times

The circumstances where a fix service level is deemed to be met are:

- When the service has been fixed within the standard and expected response time
- Where you receive a telephone call (within the service level response time) resulting in a fix over the telephone
- Where you receive a telephone call and you defer the visit of an engineer to a specific time, the fix time is measured from the specific time you specify
- Where it is subsequently discovered that the issue giving rise to the telephone call falls outside the Services agreed to be provided by Claranet

- When the equipment has been returned to an acceptable operational status or an item of loan equipment has been supplied
- Where the fault relates to an excepted Service

What you will do

Efforts to resolve an issue: You are responsible for providing reasonable efforts support and information to Claranet to help in the resolution of any technical issues.

Service outage: In the event of a Service outage, you are responsible for complying as quickly as possible with any requests from Claranet for help with diagnostics. Any delay in resolving the fault due to you not being available or not complying with Claranet's requests may impact the validity of any Service Levels.

Table: Service Level Response Times

Priority	Service Level Response	Description
1 – Critical	Within 1 hour	Total service is unavailable
2 – Major	Within 2 hours	Partial service, an element of the total service has failed
3 – Minor	Within 4 hours	Impaired service, no element has totally failed but there is a quality issue
4 – Request	Within 1 Business Day	The service is unaffected. Request for product related technical advice or configuration change

Service Levels

If Claranet fails to deliver the stated service level, Claranet agrees that you shall be entitled to receive, in lieu of all other remedies available to you, Service Credits as set forth in this section against the fees owing to Claranet under the Agreement.

Measure of availability

In the event of the service failing, we measure Non-availability as follows:

Non-availability is calculated from the time the service or part thereof experiences a failure to such time as the service is restored to you. Periods of Non-availability for your network platform will be measured by our internal system logs

Any time in which the Claranet monitoring system is unable to receive or process monitoring data shall not be assumed to be unscheduled downtime. If you initiate a Service Credit request, this will put into a process where Claranet coalesce the systems monitoring data and logs with your own record of when and where an outage occurred. The Service Credits will be available for that agreed window. You have the option to dispute records with Claranet, where upon systems monitoring data can be provided to you.

In the event that you and Claranet agree that Claranet has failed to meet any service level guarantee during any given calendar month, Claranet will credit your account with a Service Credit. Service Credits shall apply only to the fee(s) for the affected service(s). Service Credits shall be deducted from the relevant monthly fee due in respect of the second month following the month in which an agreed Service Credit is claimed. The maximum amount of Service Credit a Customer can receive in each calendar month relating to this agreement is fixed to 50% of the fee for the affected Service. The Service Credits issued are liquidated damages and, unless otherwise provided in this agreement, such Service Credits will constitute your sole and exclusive remedy with respect to the failure for which they are payable.

Compensation claims

Compensation claims must be submitted, in writing (email or letter), within 30 days from the service level guarantee breach to which they refer. All claims must be submitted to the appointed Account Manager and/or Service Manager. You agree to correct problems and to attempt to minimise the recurrence of problems for which you are responsible that may prevent Claranet from meeting the service level guarantees. Requests for support received by the Service Desk by means other than telephone or request ticket (for example, by fax) will be excluded when calculating service levels.

claranet

Exceptions

Claranet excludes responsibility for meeting any service levels to the extent that meeting the service levels is affected by the following items:

- if you are in default under the Agreement;
- in respect of any non-availability which results during any periods of scheduled maintenance or emergency maintenance;
- in the event that the Service is disrupted due to unauthorised users or hackers;
- in the event that the Service is unavailable due to changes initiated by you whether implemented by you or Claranet on behalf of a customer;
- in the event that the Service is unavailable as a result of you exceeding system capacity;
- in the event that the Service is unavailable due to viruses;
- in the event that the Service is unavailable due to the your failure to adhere to Claranet's implementation, support processes and procedures;
- in the event that the Service is unavailable due to the acts or omissions of you, your employees, agents, third party contractors or vendors or anyone gaining access to Claranet's network, control panel; or to your website at the request of a customer;
- in the event that the Service is unavailable due a Force Majeure Event;
- in the event that the Service is unavailable due to any violations of Claranet's Acceptable Use Policy;
- in the event that the Service is unavailable due to any event or situation not wholly within the control of Claranet;
- in the event that the service is unavailable due to your negligence or wilful misconduct of you or others authorised by you to use the Services provided by Claranet;
- in the event that the service is unavailable due to any failure of any component for which Claranet is not responsible, including but not limited to electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by you;
- in the event that the service is unavailable due to any failure local access facilities provided by you; and
- in the event that the service is unavailable due to any failures that cannot be corrected because you are inaccessible or because Claranet personnel are unable to access your relevant sites. It is your responsibility to ensure that technical contact details are kept up to date by submitting a request ticket to confirm or update the existing the technical contact details.