IP Connect Global Service Schedule
Part B – Service Description

Section A – The Service

1. STANDARD COMPONENTS OF THE SERVICE

BT will provide the Customer with the following Services in accordance with the details set out in any applicable Order:

1.1 Access Line

1.1.1 The Customer may opt for Customer Provided Access ("**CPA**") or BT Provided Access.

1.1.2 If the Customer opts for BT Provided Access BT, or BT's agent, will arrange to connect the Site(s) to a Point of Presence ("**PoP**") on the BT Network using the type of Access Line chosen by the Customer and set out in the Order. The Access Line option(s) available at a Site may vary according to the location of the Site and not all are suitable for all the Customer applications. The available Access Line options available are:

(a) **Leased Line Access**. Leased Line Access is a dedicated Circuit from a Site to the nearest BT Network PoP, and is capable of carrying all Classes of Service (CoS).

(b) **DSL**. If DSL is selected in the Order;

(i) BT will provide the Customer with one of the following DSL packages, as set out in the Order:

a) Business DSL Premium;

b) Business DSL Plus;

c) Business DSL Standard (Managed Routers are mandatory); or

d) Basic DSL.

(ii) the Port speed is set to the DSL speed, and traffic may burst to the Access Line speed if bandwidth is available. The Contention Ratio limits the typical Throughput;

(iii) in some locations DSL is supplied using 'rate adaptive' broadband technology, which does not run at fixed speeds and is determined by the fastest speed that the Customerr analogue direct exchange line can support. BT will have no liability to the Customer for failing to reach any specific speeds.

(iv) following the Operational Service Date, for a period of up to 10 Business Days, BT will undertake dynamic line management to stabilise the line at the most appropriate speed. During this time short outages may occur, which are excluded from BT's Availability calculations;

(v) BT will deliver the DSL up to a defined demarcation point. Telephony services on the DSL will be disabled and the line may only be used with the Service;

(vi) BT may require a Site survey to determine if BT's supplier can deliver the DSL. If the initial enquiry shows that the Service is available but is later found to be undeliverable, BT will inform the Customer of alternative access options and prices. Under this circumstance, the Customer may order an alternative or cancel the Order for that Site; and

(vii) the following additional provisions apply to Basic DSL:

a) Basic DSL is connected to the BT Network via HVPN or DSL gateways;

b) as Basic DSL bundles are fixed, the Customer accept there is no option to change the speeds, Class of Service values, bundled Routers or the products of the local third party supplier;

c) Managed Routers are mandatory for all Basic DSL Sites. BT, or the third party Access Line/equipment supplier can manage the Routers; and

d) BT will only provide BT Network reports for Basic DSL sites. BT will not provide Site to Site or Router performance reporting as set out in this Schedule.

(c) **Ethernet.**

(i) The Customer may order one of following three Ethernet options from BT:

a) Standard Ethernet Access;

b) Ethernet Plus Access; and

c) Premium Ethernet Access.

(ii) Standard Ethernet Access has a Contention Ratio of 10:1 – 50:1 and is suitable for DE Class.

(iii) Ethernet Plus Access has a Contention Ratio <10:1 and is suitable for AF Class and DE Class.

(iv) Premium Ethernet Access provides a dedicated Ethernet access Circuit connecting a Site to the BT Network. It is suitable for all CoS. The following limitations apply:

a) framing overheads will reduce IP Throughput, by an average of 9 per cent (depending on CoS profile and average packet size) of the "headline" access speed; and

b) maximum EF Class traffic is 50 per cent of Port speed.

(d) **HVPN**

(i) With HVPN an IPsec Tunnel is created from a Managed Router at a Site to a secure network gateway to the BT Network. The Customer may access its VPN at the HVPN Port speed as set out in the Order.

(ii) For new Orders at a Site, one Managed Router is required. If the Customer replaces an existing access method with HVPN, it may be necessary either to replace an existing Managed Router, or to add an additional Managed Router. The Customer will be liable to pay for any additional Managed Router and for any installation and de-installation Charges.

(e) **Split Tunneling.**

(i) The Split Tunnelling feature includes two related capabilities:

a) **Internet Break-out (IBO)** – IBO will provide a way for the Customer to give restricted access to the Internet from the VPN site via the HVPN CPE. The Internet traffic is presented on the Customer LAN Port, and the CPE will route the Internet traffic onto the HVPN access without encryption so that the Internet traffic does not traverse the IPSec Tunnel; and

b) **iLAN** – iLAN provides an additional Port with unrestricted Internet access. The iLAN is typically used for a guest LAN or Wi-Fi access to the Internet. There is no access to the VPN from the iLAN Port. iLAN allows the Customer to provide internet access without the cost of additional hardware.

(ii) Both features provide security against intrusion from the Internet via a zone-based firewall.

(f) **BT Reach-In NNI**

(i) BT Reach-In NNI is a private, in-country IP-based VPN service delivered over a third party network that extends the reach of the Customer IP Connect Global network.

(ii) The BT Network is interconnected with BT's suppliers' networks in certain countries. The Customer may access its MPLS network via BT's supplier's IP VPN service via these interconnections.

(iii) BT Reach-In NNI consists of an Access Line, CoS, Port(s) and either Unmanaged BT Routers, Unmanaged Customer Routers, or Managed Router(s) at each Site. The Customer may order different configurations to provide the required level of resilience at the Site.

(iv) BT will provide the Access Line from the Site to a Port on a node in BT's supplier's network using one of the following, as set out in the Order:

a) Leased Line;

b) Premium Ethernet;

c) Business DSL Premium; or

d) Basic DSL.

(v) Managed Routers, Unmanaged BT Routers and Unmanaged Customer Routers connected to BT's supplier's network must conform to the CoS markings and classes available on BT's supplier's network. Managed Routers will perform CoS mapping and re-mark traffic from BT's standard six CoS (on the LAN side of the Managed Router) to the supplier-specific CoS. Customer Data will not be re-marked as it transits the Customer supplier's network.

1.1.3 If the Customer opts for Customer Provided Access;

(a) except with HVPN, BT will provide the Customer with an ISP-supplied modem or a data SIM for mobile connection, at the Customer's own expense;

(b) with HVPN, the Customer will provide an ISP-supplied modem at the Customer's own expense. Both the upstream and downstream broadband speed must be greater than, or equal to, the HVPN Port speed; and

(c) if the Customer provide DSL Access, the Customer is responsible for the functionality, maintenance and all Charges related to this DSL Access. BT will not provide the Service if the Customer Provided Access is connected to a private branch exchange (PBX) system or related equipment.

1.2 Port

1.2.1 The Port is the point where the Access is connected to the BT Network.

1.2.2 Where BT manage the router for the Service, a part of the bandwidth of the Port is used by BT for management purposes.

1.2.3 If the Access Line speed exceeds the Port speed, traffic shaping is used to limit the use of Access Line capacity to the Port speed.

1.2.4 For BT Reach-In NNI, the Port is the point on BT's supplier's network where the Access Line is connected to BT's supplier's IP VPN service.

1.3 Class of Service ("CoS")

1.3.1 CoS assists with congestion avoidance and management. BT's traffic may be either "**In-Contract**" or "**Out-of-Contract**". In-Contract traffic is data sent by the Customer within the configuration rules applied by BT and is supported by the Service Levels set out in Part A. Out-of-Contract traffic is data sent by the Customer outside of the configuration rules applied by BT and is not supported by the Network Performance Service Levels set out in Part A.

1.3.2 The Service has three types of application CoS (EF Class, AF Class and DE Class). The Customer may order up to four separate AF Classes, as well as one of each DE Class and EF Class - up to six Classes in total. CoS varies based on application type and speed, but the Access Line and the Port must have the same or greater bandwidth than the total contracted rate per CoS, (the contracted rate for each AF Class is counted separately). The Customer's applications mapping policy to the appropriate CoS, based on the applications operating across the Customer VPN, is set in consultation with BT. Any traffic not identified as part of a subscribed CoS is marked DE Class. The prioritisation of data within the Service is set out below:

(a) "**EF Class**" is for voice over IP applications. The Customer will specify the amount of EF Class traffic "**In-Contract rate**" required. There is no bursting capability for EF Class traffic and any traffic above the In-Contract rate is dropped.

(b) "**AF Class**" is for delay-sensitive data traffic. The Customer specify the amount of AF Class traffic ("**In-Contract"** bandwidth). Traffic may burst above the In-Contract rate if bandwidth is available ("**Out-of-Contract**" traffic). The assured Throughput for each AF Class is the In-Contract bandwidth for that CoS. Traffic in excess of the In-Contract bandwidth in any AF Class is marked Out-of-Contract.

(c) "**DE Class**" is for delay tolerant applications. DE Class is not ordered separately and is included in the Charge for the Port. DE Class can burst to Port speed if other Classes are not using the bandwidth. DE Class traffic is "bleached", which means the DSCP markings are set to zero. Some Access Line types allow the Customer to turn off this bleaching if set out in the Order.

1.3.3 For **BT Reach-In NNI** the number of CoS may be less than six depending on BT's supplier's network. It may be three, (only one AF Class) or one (DE Class only) if BT's supplier's network does not have six Classes of Service or it's CoS model is not fully compatible with BT's CoS model.

1.3.4 Class of Traffic Marking

(a) If the Customer are marking the Customerr own traffic (either the Customer have ordered Managed Routers with DSCP transparency or have Unmanaged BT or Unmanaged Customer Routers) then:

(i) only AF Class traffic that is marked as low drop probability ('afx1') or using the class selector ('csx') and is within the specified contract bandwidth is carried as "**In-Contract**". All other AF Class traffic is treated as "**Out-of-Contract**" even if the total traffic for that AF Class is less than the specified "**In-Contract**" bandwidth; and

(ii) the Customer will mark DE Class traffic with the DSCP marking used by BT before transmitting it to the BT Network.

(b) Customer Traffic Marking is not available with BT Reach-In NNI.

1.3.5 Standard Reports

(a) BT will provide access to one of BT's portals where the following reports are available.

(b) The following reports are available without additional Charge with the Service ("Basic Report Package"):

(i) Near Real Time utilization reports (PE Based port, VPN and COS utilization reports)

(ii) Core Network Round-Trip Delay, Packet Delivery and Jitter

(iii) Inventory report;

(iv) Planned Maintenance report;

(v) Order status;

(vi) Ticket status;

(vii) e-Notification - Initial Incident detection; and

(viii) e-Updates.

(c) Reports are unavailable for Sites with Business DSL Plus; Business DSL Standard; Basic DSL Access or HVPN unless otherwise agreed on the Order.

2. SERVICE OPTIONS

BT will provide the Customer with any of the following options as set out in any applicable Order and in accordance with the details as set out in that Order:

2.1 Routers

2.1.1 BT offers three different supply and support models for Routers:

(a) **Managed Routers**. If the Customer selects the Managed Router Service option, BT will:

(i) configure and install Managed Routers (both hardware and Software) and the Service at the Site(s) to deliver connectivity for the Customer traffic across the BT Network);

(ii) perform commissioning and acceptance testing (up to layer 3 of the Open Systems Interconnection reference model) before giving the Customer design and configuration details;

(iii) manage the Managed Router (including providing maintenance, monitoring and configuration) to make sure that the User has connectivity for its traffic across the Service. A number of maintenance service options are available for BT Managed Routers. These options vary from country to country and must be selected for each Site and specified in the Order;

(iv) be responsible for network design and will ensure that any proposed reconfigurations of Managed Routers do not conflict with the Customer existing network. If any network changes are required, BT will make the network changes at the same time as the reconfiguration of the Managed Routers;

(v) archive Managed Router configuration files and restore configurations if a Managed Router fails. BT will store copies of the three most recent configurations for each Managed Router;

(vi) provide Software maintenance for Managed Routers ensuring that the level of Software is appropriate. Before any upgrade, BT will evaluate the impact to the Customer network;

(vii) provide upgrades to OS versions if changes to the Service required by the Customer require a later release of Software;

(viii) configure the Managed Routers so that the Customer may download new Software to the Managed Router from BT's relevant systems, in addition to the existing Managed Router configuration; and

(ix) own the Managed Router at all times.

(b) **Unmanaged BT Routers.** If the Customer selects the Unmanaged BT Router Service option, BT will:

(i) install the Unmanaged Router(s) at the Site(s); and

(ii) subject to the Customer informing BT that the Unmanaged BT Router is faulty, physically maintain (hardware only) it but the Customer will monitor, configure and commission the Unmanaged BT Routers.

(c) **Unmanaged Routers.** If the Customer selects the Unmanaged Router Service option, the Customer will be responsible to install, monitor, configure, commission and physically maintain the Unmanaged Routers**.**

2.1.2 With the Managed Router option, the Customer may order change management in which BT will perform routine Software configuration and upgrade tasks remotely on Managed Routers. The Customer may order change management with up to five defined changes per Managed Router, per year for a Monthly Charge (as set out in the Order).

2.2 Access Line Resilience

2.2.1 The Customer may select one of the following Access Line resilience options as set out in the Order. Not all options are available in all locations (which is set out in the BT quote) and Managed Routers are required for "**Access Backup**", "**Secure**" and "**SecurePlus**" resiliency options:

(a) **'Standard'** – BT, or BT's agent will arrange for a single Access Line to connect the Site(s) to a BT PoP via a single router at the Site(s);

(b) **'Access Backup'** BT, or BT's agent will arrange for a second Access Line (either a DSL or HVPN Access Line) to connect the Site(s) to either the same or a different PoP as the original Access Line via a single CPE or via two routers at the Site(s);

(c) **'Secure'** – BT, or BT's agent will arrange for a second Access Line to connect the Site(s) to the same PoP as the original Access Line via two routers at the Site(s);

(d) **'SecurePlus'** – BT, or BT's agent will arrange for a second Access Line to connect the Site(s) to a separate PoP from the original Access Line via two routers at the Site(s).

2.2.2 Except for Standard Access Lines, if the Primary Access Line (or Managed Router or PoP as appropriate) fails, traffic is re-routed to the Secondary Access Line. The Secondary Access Line may be of equal or less bandwidth than the Primary Access Line. If the Customer orders different CoS on the Primary Access Line and the Secondary Access Line, it may not be possible to carry all traffic effectively on the Secondary Access Line.

2.2.3 Unless the Customer purchases the load balancing option as set out in Paragraph 2.2.4 below, the Customer may only use the Secondary Access Line during a failure of the Primary Access Line.

2.2.4 Depending on the configuration, routing protocol and speed of the Customer network, the Customer may select one of the following Access Line resilience configurations:

(a) **'Failover'** – BT, or BT's agent, will configure the Secondary Access Line as a backup to the Primary Access Line, if the Primary Access Line fails traffic will route via the Secondary Access Line; or

(b) **'Load balancing'** – BT, or BT's agent, will configure the Secondary Access Line for dual running with the Primary Access Line. If one Access Line fails, subject to sufficient capacity being available on the other, traffic can flow over the other.

2.3 Multiple VPN

2.3.1 The Customer may order Multiple VPN for Sites with Access Lines connecting directly to the BT Network. Multiple VPNs enables the Customer to define more than one VPN within its network and connect Sites to a number of VPNs. BT cannot provide Multiple VPN over DSL or HVPN Access Lines.

2.3.2 The Customer may partition routing and traffic between Sites securely right up to the LAN Port. Each Site may be a member of some or all of these VPNs allowing communities of interest to be set up. BT will not provide any connectivity between the VPNs.

2.3.3 A Managed Router, Unmanaged BT Router or Unmanaged Customer Router supports connectivity to Multiple VPNs, traffic from each VPN is routed to a dedicated LAN or sub interface on that Router.

2.3.4 Each Site will have one VPN connection designated as the primary VPN for management connectivity.

2.3.5 CoS specifications may be aggregated either across the Port or per VPN at each Site.

2.3.6 For Leased Line Access, frame relay protocol is used to present each VPN logically as a dedicated frame relay PVC over the Access Line.

2.3.7 For Ethernet Access, the same as for Leased Line Access above, is achieved through the use of 802.1q virtual LAN standards, issued by the Institute of Electrical and Electronics Engineers Standards Association.

2.3.8 The Customer is responsible for the selection and configuration of the Router if the Customer orders the Service with Unmanaged BT Routers or Unmanaged Customer Routers.

2.3.9 If the Customer orders Multiple VPNs to a Site, then the CoS policy may be applied to the whole of the Customer access ("**CoS Policy per Access**" or "**CPpA**") or it may be applied to the individual VPN connections ("**CoS Policy per Connection**" or "**CPpC**"). In some locations, there is no choice and only CPpA or CPpC is available. In such event this will be set out on the Order.

2.4 Multiple Routes

2.4.1 The Multiple Default Route feature allows the Customer VPN to support up to five default routes (typically for Internet access). This allows the Customer to have regional Internet break-out (or access to other networks).

2.4.2 The Multiple Specific Route feature uses the same technology as the Multiple Default Route feature and allows the Customer VPN to support up to five routes to the same specific IP Addresses.

2.4.3 Multiple Routes are not available with the BT Reach-In NNI Access type.

2.4.4 The Customer may order either or both of the following options, but the aggregate number of preferred routes will not exceed five.

2.4.5 Multiple Default Routes. If the Customer is using a routing gateway to other services, such as the Internet, the Customer may select up to five Sites through which connection to the other service occurs. This enables the Customer to provide regional access to those services.

2.4.6 Multiple Specific Routes. The Customer may order up to five routes to the same IP Addresses to manage traffic loads to Site(s) with multiple Access Lines. Each of the Access Lines is declared a routing gateway.

2.4.7 For both options, all other Sites select a preferred routing gateway. If the preferred gateway fails, the Service automatically redirects traffic to another routing gateway.

2.5 Multicast VPN

2.5.1 Multicast VPN enables packet replication, which is required by applications such as: video conferencing, IP TV, corporate communication, software distribution, stock quotation and news feeds. It enables the Customer traffic to be sent from a 'source' Site to multiple 'receiver' Sites.

2.5.2 Multicast VPN is not available with BT Reach-In NNI.

2.5.3 Multicast VPN is available over the Customer intranet VPN(s) at Sites with either Leased Line Access or Ethernet Access to the BT Network. It does not support EF Class. In the Order, the Customer will state the amount of bandwidth that is used at each Site for Multicast VPN. The Customer may order either or both of the following options as set out in the Order:

(a) **Protocol Independent Multicast ("PIM") Sparse Mode** – This option ensures that the Multicast VPN application flows are sourced only to Users that form part of a Multicast VPN group. To become part of a Multicast VPN group, Users will register to a Rendezvous Point ("**RP**"), from where Multicast VPN traffic will flow via a "shared" distribution tree, rooted at the RP associated with the Multicast VPN group. BT will provide either the auto RP or static RP mechanism for distribution of RP information, as set out in the Order.

(b) **Source Specific Multicast ("SSM")** – This option provides a higher layer protocol, IGMPv3, enabling Users to receive information from a Router (either a Managed Router, Unmanaged BT Router or Unmanaged Customer Router).

2.6 Internet Gateway Regional feature

2.6.1 The Internet Gateway Regional feature offers the Customer access to Internet based applications from their VPN(s). All Internet traffic from Sites in that VPN follows a default route to the Internet, in general using the nearest Internet Gateway (selected based upon BT Network topology) to take them to the Internet via the Service.

2.6.2 The Customer may order at least two or more gateways per VPN if the Customer requires resiliency. When more than one Internet Gateway is selected, all of them are available. In case one fails, all Internet traffic from that VPN is dynamically routed via the alternate(s) Internet Gateway(s) in the event of network outage

2.6.3 The Multiple Default Routes feature described in Paragraph 2.4 can be used to influence the Internet Gateway used by specific Site(s).

2.6.4 In addition to the advertisement of a default route from each Internet Gateway, the Customer may also opt to receive routes for specific destinations, such as an Internet service provider, from any of their Internet Gateways ("**Customer Defined IP Routing Policy**"). The Customer may specify up to 100 specific routes unless otherwise agreed with us.

2.6.5 The Customer will have the ability to select a fixed capacity for the Internet Gateway Regional feature and that Internet Gateway bandwidth is shared by all Sites on that VPN for accessing the Internet.

2.6.6 BT will deliver the Internet Gateway Regional feature with a Cloud Firewall feature, as set out in Paragraph 2.9.

2.6.7 The Customer may order the Internet Gateway Regional feature at the same time as a "**new provide**" Order for the Service or as a standalone feature if the Service already exists.

2.7 Cloud Connect to Data Centre feature

2.7.1 The Customer may order the Cloud Connect to Data Centre feature at the same time as a "**new provide**" Order for the Service or as a standalone feature if the Service already exists. BT will only provide connectivity to the Data Centre and will have no liabilities relating to such third party patch service provider services, including but not limited to any liability relating to performance, availability, data protection and any security issues.

2.7.2 The Cloud Connect to Data Centre feature offers the Customer private access directly to a set of pre-connected Data Centres on the BT Network.

2.7.3 Those connections are built as an extension of the Customer VPN to the point of interconnection with the Data Centre provider. Cloud Connect to Data Centre feature includes:

(a) Connectivity to the Data Centre; and

(b) The management of the Cloud Connect to Data Centre feature.

2.7.4 If requested in the Order, BT will provide connectivity inside the Data Centre, or within the campus according to available solutions in place with the Data Centre provider. The solution available will vary according to both the Data Centre provider and location, and will be determined on a case by case basis. BT will notify the Customer as soon as is reasonably practicable of any additional requirements, including, but not limited to, a need for the Customer to order internal Data Centre cabling directly from the Data Centre provider, or any additional Charges becoming payable for connection.

2.8 Cloud Connect Direct feature

2.8.1 The Cloud Connect Direct feature offers the Customer private access direct to a third party cloud service provider with whom BT have built one or more interconnection points globally on the BT Network.

2.8.2 The Customer is responsible for entering into an agreement with a third party cloud service provider for any usage of that service. BT will only provide connectivity to the third party cloud service provider.

2.8.3 The Customer may order more than one connection to have geographical resilience in place or to align to the Service being consumed with the third party cloud services.

2.8.4 The Cloud Connect Direct feature is built as an extension of the Customer VPN to the point of interconnection with the third party cloud service provider. Cloud Connect Direct includes:

(a) connectivity to the service associated to this connection; and

(b) the management of the Cloud Connect Direct feature.

2.8.5 The Port speed will depend upon the offering of the third party cloud service provider that the Customer have contracted with.

2.9 Cloud Firewall feature

2.9.1 The Cloud Firewall feature provides network protection and optimisation hosted at a BT PoP. The Cloud Firewall feature controls inbound and outbound access from either:

(a) the Cloud Connect Direct feature; or

(b) the Internet Gateway Regional feature.

2.9.2 BT will provide the Cloud Firewall feature automatically if the Customer purchase the Internet Gateway Regional feature. In addition, the Customer may choose to order the Cloud Firewall feature with the Cloud Connect Direct feature.

2.9.3 BT provide the Customer with the following elements for the Cloud Firewall feature:

(a) **security platform**: BT will provide the Cloud Firewall feature on the chosen third party partner technology (hardware and applications). The Cloud Firewall feature is virtualised, and multiple customers will share the same physical platform;

(b) **security consultancy**: BT will provide support to the Customer in producing the Customer Customer Security Policy ("**CSP**"), and/or its network design if requested by the Customer and set out in the Order;

(c) **fault management**: BT will provide a helpdesk available during 24 hours a day, seven days per week to respond to Incidents, platform support backed off to appliance and application vendors, and continuous real-time service monitoring; and

(d) **configuration management**: BT will implement reasonable Customer-requested changes to the CSP, and upgrade the Cloud Firewall feature according to recommended and tested vendor patches.

2.9.4 The Cloud Firewall feature is resilient to failure of any single element, to the extent that traffic is re-routed around a failed service element via an alternative service element, until such time as the failed service element is restored. In such cases:

(a) there will be a temporary interruption of the Cloud Firewall feature and active sessions will need to be re-established; and

(b) the Customer re-routed traffic will egress to the Internet in other geographic locations. (For example, in the case of UK and US locations, and the US location experience a failure, then the Customer US traffic would be re-directed to the UK location.)

2.10 Shared Access

Shared access enables the Customer to share the Customer Access Line(s) with, or share the Access Line(s) of, another IP Connect Global customer in order to create mutual VPNs, as agreed between the relevant parties under a separate agreement. The terms and conditions which apply to shared access are specified in the "**Shared Access Consent Form**", which both the Customer and the other customer will sign.

2.11 Additional Reports

2.11.1 The "**Advanced report package**" consists of:

(a) The Basic Report Package;

(b) Managed Router Performance;

(c) Port, VPN and CoS utilisation;

(i) CPU utilisation;

(ii) Free/used memory; and

(iii) CPE reachability.

(d) DSL Plus reporting package – this option adds reports per Site or for all Sites that have Business DSL Plus Access;

(e) Port errors and discards – provides information about the number of packets with errors and the number of discarded packets;

(f) Threshold reporting – provides a view of performance exceptions based on pre-set threshold for Ports, VPNs, CoS, routers and Site-to-Site paths.(if site to site reports are ordered); and

(g) Trending and forecasting reports package – provides a forecast view of Port, VPN utilisation and CoS usage based historical trends.

2.11.2 The "**Advanced+ report package**" consists of:

(h) 90th Percentile Reports – is a report that summarizes the network usage over a time period better than the average or peak utilisation;

(i) Baseline exception reports – is a report that shows when VPN usage is outside an expected usage pattern.

2.11.2 In addition, the following reports can be ordered in addition to the "**Advanced report package**" or "**Advanced+ report package**":

(a) Site-to -Site performance (for which the Customer will use BT Managed Routers) – provides network performance (Round-Trip Delay and Jitter) reporting between the Sites and is ordered in packs of ten Sites; and

(b) Simple Network Management Protocol ("SNMP") management feed – gives read-only SNMP access to network management information from the Managed Router. The Customer is responsible for providing the Customer own SNMP management tools. SNMP connectivity is provided between the Managed Routers and up to two hosts within the Customer LAN.

2.12 Regional Service Desk Support. The Customer may request and BT may agree to provide additional telephone numbers to give the Customer Contact access to up to three additional regional service desks, which can provide support in a small number of additional languages.

2.13 Multi-Service Access

2.13.1 Multi-Service Access is an option that provides both IP Connect Global and the right to access and use the Internet service that BT provides ("**Internet Connect Global**") over the same Access Line, router and Port ("**Multi-Service Access").**

2.13.2 The Multi-Service Access option is only available if confirmed in writing by BT.

2.13.3 Internet Connect Global, as part of the Multi-Service Access option, is only available at Sites in countries in which BT provides the Internet Connect Global service.

2.13.4 The Cloud Firewall feature is not available for the Internet Connect Global service as part of the Multi-Service Access option.

2.13.5 BT's monitoring obligations under this Schedule apply only to the IP Connect Global Services and do not apply to the Internet Connect Global Service as part of the Multi-Service Access option. There is no proactive monitoring of the Internet Connect Global service outside of the Access Line, Port and any Managed Router.

3. SERVICE MANAGEMENT BOUNDARY

3.1 BT's responsibility to provide and manage the Service is physically and logically limited to the following service management boundary as set out in the remainder of this Paragraph 3 (**"Service Management Boundary"**):

3.1.1 where BT provide the Customer with Managed Routers, the Service Management Boundary is the LAN Port on the Managed Router. This includes provision, maintenance and management of all elements up to this Service Management Boundary. The cable which connects to the Customer Equipment is the Customer responsibility;

3.1.2 where BT provide the Customer with Unmanaged BT Routers, or the Customer uses Unmanaged Customer Routers, the Service Management Boundary is the Network Terminating Unit ("NTU") of the Access Line that BT provides. This includes provisioning, maintenance and management of all elements up to this Service Management Boundary. The Customer is responsible for the cable connecting the NTU to the Unmanaged BT Router or Unmanaged Customer Router;

3.1.3 for the purposes of Paragraphs **Error! Reference source not found.** to 3.1.2 above, where the C ustomer provide any internal cabling, this will fall outside of the Service Management Boundary for the Service;

3.1.4 HVPN CPA falls outside of the Service Management Boundary;

3.1.5 for the Internet Gateway Regional feature, the Service Management Boundary is the port on the BT Equipment which provides connectivity to the Internet;

3.1.6 for the Cloud Connect to Data Centre feature, the Service Management Boundary is:

(a) in the case of Managed Routers, the LAN port on the Router; and

(b) in the case of Unmanaged BT Routers or Unmanaged Customer Routers, at the terminating patch panel port at the Data Centre.

3.1.7 in addition, for the Cloud Connect to Data Centre feature, where the Customer orders any internal Data Centre cabling directly from the Data Centre provider, this will fall outside of the Service Management Boundary for this feature;

3.1.8 for the Cloud Connect Direct feature, the Service Management Boundary is the interconnection between the third party cloud service provider router and the BT Managed Router;

3.1.9 for the Cloud Firewall feature, the Service Management Boundary is the interconnection between the third party cloud service provider router and the BT Managed Router. BT may make changes to the configuration of the Cloud Firewall feature within the Service Management Boundary. Unless otherwise agreed in writing, the Customer is responsible for making any necessary configuration changes outside the Service Management Boundary and for the in-life management of Service elements outside the Service Management Boundary. Under no circumstances will the Customer attempt to make direct changes to the physical or Software configuration of the Cloud Firewall feature without BT's prior written approval.

3.2 BT will have no responsibility for the Service outside the Service Management Boundary.

3.3 BT does not make any representations, whether express or implied, about whether the Service will operate in combination with any Customer Equipment or other equipment and software.

3.4 The Cloud Firewall feature cannot ensure prevention or detection of all threats and unauthorised actions.

4. COMMISSIONING OF THE SERVICE

4.1 Before the Operational Service Date, BT will:

4.1.1 deliver and configure the Service;

4.1.2 conduct a series of standard tests on the Service to ensure that it is configured correctly;

4.1.3 for Service with Managed Routers, configure the equipment, CoS and the Access Line, so that traffic can be transmitted from one Site to another, and conduct a set of standard tests to ping the Managed Router;

4.1.4 for Service with Unmanaged BT or Unmanaged Customer Routers, confirm delivery of the Access Line, configure the CoS and conduct a set of standard tests to ping the Port; and

4.1.5 on the date that BT has completed the activities in this paragraph 4.1, confirm to the Customer that the Service is available for performance of any Acceptance Tests.

5. ACCEPTANCE TESTS

5.1 The Customer will carry out the Acceptance Tests for the Service within five (5) Business Days after receiving notice from BT ("Acceptance Test Period").

5.2 The Service is accepted by the Customer if the Customer confirms acceptance in writing during the Acceptance Test Period or is treated as being accepted by the Customer if the Customer does not provide BT with notice to the contrary by the end of the Acceptance Test Period.

5.3 Subject to paragraph 5.1 and 5.2, the Operational Service Date will be the earlier of the following:

5.3.1 the date that the Customer confirms or BT deems acceptance of the Service in writing in accordance with paragraph 5.2;

5.3.2 the date of the first day following the Acceptance Test Period; or

5.3.3 the date the Customer starts to use the Service.

5.4 If, during the Acceptance Test Period, the Customer provides BT notice that the Acceptance Tests have not been passed, BT will remedy the non-conformance without undue delay and provide the Customer notice that BT has remedied the non-conformance and inform the Customer of the Operational Service Date. Minor defects in quality of the Service shall not prevent acceptance.

Section B – Service Responsibility Matrix

6. SERVICE MANAGEMENT

6.1 The Service Management Schedule as referred to in the Order will apply to this Service.