SERVICE SPECIFICATION SCHEDULE (SSS)

Version BCLS_IPT_v1.1_20240701

.

1. GENERAL

1.1. This Service Specification Schedule (SSS) set forth the terms applicable to the Services that Supplier delivers to Customers, by means of the following sections outlined in this document:

1.1.1. Service Description: Technical and functional features of the Services

1.1.2. Service Level Agreement (SLA). Measurable performance service levels and the remedies available to Customer if these levels are not achieved

1.2. This Service Specification Schedule is incorporated and governed by certain Master Service Agreement ("MSA") and any applicable Service Orders entered into by and between the Customer and the Supplier, all of which are binding on the Customer. The provisioning of Services is contingent upon the full execution of the MSA.

1.3. This Service Specifications Schedule may be updated on a periodic basis to introduce, change, adjust, replace or discontinue any Services. These actions may be undertaken to, but not limited to, enhance technology, improve the performance of the Services, comply with industry trends, adhere to regulatory requirements, or for alternative business considerations, as deemed necessary. All such modifications will be promptly incorporated into updated versions of the relevant Service Specification Schedules (SSS). These updated SSS versions, along with their officially announced effective dates, are publicly available and readily accessible through the Supplier's website and/or Customer Portal, with reasonable advance notice.

2. DEFINITIONS

Unless the context otherwise requires, all capitalized terms used but not otherwise defined herein shall have the meanings as found in the MSA. Terms not capitalized will be given their plain English meaning, and those terms, acronyms, and phrases known in the information technology and telecommunications industries will be interpreted in accordance with their generally accepted meanings.

2.1. **Access Port:** mean the port on the Supplier Network through which the Service is provided to the Customer

2.2. **Applicable Law:** means law, regulation, binding code of practice, rule, order or requirement of any relevant government or governmental agency, professional or regulatory Authority, each as relevant to (i) Supplier in the provision of the Service and/or (ii) Customer in receipt of the Service or carrying out of its business

2.3. **Authority:** means those governments, agencies, courts of law, and professional and regulatory authorities that supervise, regulate, investigate, or enforce Applicable Law

2.4. **Authorized Contact:** means a person designated by the Customer to act on its behalf to place Service Incident Tickets

2.5. **Autonomous System (AS):** means a collection of connected IP routed prefixes, under the control of one or more entities that presents a common, clearly defined routing policy to the Internet. An AS is enabled to exchange routing information via BGP with other neighboring AS

2.6. **Autonomous System Number (ASN):** means a number that identifies uniquely an Autonomous System. The ASN is assigned by the relevant Internet Registry (IR)

2.7. **Back-Up Access Port:** means additional Access Ports that is connected to the Supplier Network, where the Customer can deliver data traffic as back-up of the main Access Port.

2.8. **BGP:** means Border Gateway Protocol

2.9. **Black Hole(ing):** means discarding all data destined for a particular IP Address so that it does not disrupt the flow of data to other IP Addresses

2.10. **Border Gateway Protocol**: It is the main protocol that determines the core routing decisions on the Internet to exchange and forward packets among all Autonomous Systems (AS)

2.11. **Business Day**: means any calendar day except: (i) Saturdays or Sundays or (ii) national, regional and local holidays in the jurisdiction in which the relevant notice is to be given or where the relevant activity is to be performed. If an obligation is to be performed on a day that is not a Business Day, the obligation will be performed on the following Business Day.

2.12. **Colocation Datacenter**: means a facility that provides leased spaces to install and operate equipment, along with supplies to operate such equipment, including power, environmental conditioning, connectivity and security control.

2.13. **Committed Data Rate (CDR):** means the fixed assured bandwidth (expressed in Gbps) for a designated Access Port to work under normal conditions up to which the Customer is entitled to use for the Service. Information rate is lower than CDR to take into account the overhead inherent with Ethernet and IP technology.

2.14. **Cross-Connect:** means a physical, hardwired cable that directly links the networks of two different tenants in a Colocation Datacenter.

2.15. **Customer**: means any individual or company with a contractual relationship with Supplier for the provision of any Service under the Master Service Agreement.

2.16. **Customer Equipment**: means all hardware and related software owned, leased, licensed or controlled by the Customer in connection with the use of the Service. Equipment sold by Supplier to Customer is considered Customer Equipment.

2.17. **Customer Network**: means a collection of IP networks and routers under a single Autonomous System administered by the Customer

2.18. **Customer Premises:** means an equipped and serviced area, building or facility used by, or belonging to the Customer, wherein the Customer has privative access to it.

2.19. **Data Protection Terms:** means the terms regarding data protection in the Master Service Agreement.

2.20. **Distributed Denial of Service (DDoS):** means a form of Internet threat or attack involving multiple computers, which send repeated false traffic or requests to a server (web site) to render it inaccessible to valid users.

2.21. **DDoS Mitigation Capacity**: means the size of DDoS attack which the Supplier's Scrubbing Centre(s) can receive from the Internet and mitigate it accordingly

2.22. **Diversity**: means a type of architecture that reduces single points of failure in a complex system by maintaining separation of paths, routes and/or equipment.

2.23. **Domain Name System (DNS):** means a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols

2.24. **Emergency Maintenance:** mean maintenance carried out by the Supplier to correct unforeseen circumstances under a condition or situation which poses danger to the system, equipment, network, facilities required for rendering the Service etc. as the case may be and has to be attended immediately.

2.25. **Excluded Event:** means an instance or reason for which the Service Level Objectives do not apply, and any associated Service failure does not constitute Service Downtime for purposes of a Service Credit.

2.26. **Force Majeure Event**: means an unforeseeable and uncontrollable event, as defined in the applicable Master Service Agreement (MSA).

2.27. **Gbps:** means Gigabit per second

2.28. **Inbound Traffic**: means the data or information flowing from external networks or sources towards the Customer Network

2.29. **Internet:** means a global system of interconnected networks that use a standard IP to link devices worldwide.

2.30. **Internet Registry (IR):** means an entity that assigns and manages Internet numbers assigned to Autonomous Systems

2.31. **IP Address:** means the unique public address used by the Internet and is controlled and assigned by an Internet Registry.

2.32. **IP Network Prefixes**: means specific blocks or ranges of IP Addresses that are allocated or designated for use by the Customer or the Supplier within their respective network infrastructures.

2.33. **IP Routing Table**: means a database maintained by network devices (routers) that contains information about the available paths, network destinations (IP Network Prefixes), and next-hop addresses to reach those destinations.

2.34. **Master Service Agreement (MSA):** means the contract signed and executed between the Customer and the Supplier that governs the terms in connection with the provision of Services, including delivery requirements, payment terms, intellectual property rights, confidential information, warranties, dispute resolution and termination

2.35. **Meet-Me Room:** means a dedicated and secured area within a Colocation Datacenter where telecommunication service providers can physically connect to one another and exchange data by means of fiber Cross-Connects.

2.36. **Monthly Recurring Charges (MRC):** means, in reference to a Service Fee, the amount automatically charged to Customer each month as Service subscription, and excludes taxes and all other fees which might be charged to Customer, such as, by way of example and not limitation, set-up fees, space rental fees or charges for additional services

2.37. **Monthly Measurement Period** means, in reference to a Service, the period from the its RFS Date up to the end of the calendar month and then each calendar month thereafter (save for the last month that will end upon the termination date of the Service).

2.38. **Non-Recurring Charges (NRC):** means, in reference to a Service Fee, the one-time non-recurring charges automatically charged to Customer for installing, commissioning and provisioning of the Service.

2.39. **Office Hours**: means 9.00 am to 6.00 pm local time Monday to Thursday, and 8:00 am to 3:00 pm local time Friday, each Business Day.

2.40. **Off-Net:** means a location or portion of network that is not on the Supplier Network

2.41. **On-Net:** means a location that is on the Supplier Network. Any Service which connects two On-net locations is provisioned entirely on the Supplier Network.

2.42. **Optical Distribution Frame (ODF):** means a frame used to terminate optical cables for connectivity management. More specifically, it is mainly used for fiber fusion splicing of the optical cable, the installation of optical connectors, the storage of excess pigtails, and the protection of optical fibers

2.43. **Outbound Traffic**: means the data or information flowing from Customer Network towards external networks

2.44. **Packet Loss**: means to the percentage of data packets that fail to reach their destination within Supplier Backbone Network. It is measured by taking an aggregate average of sample measurements taken during a calendar month between designated POPs as measured by Supplier

2.45. **Protected Asset:** means the Customer's Internet-facing asset, which is protected against DDoS attack by the Service

2.46. **Resource Public Key Infrastructure (RPKI):** means a security framework designed to secure the Internet's routing infrastructure by cryptographically binding IP Network Prefixes to their respective holders (Autonomous Systems).

2.47. **RFS Date**: means, in relation to a Service, the actual date when the Service is first made available to the Customer

2.48. **Round-Trip Time (RTT)**: means a performance metric that measures the average time it takes for a data packet to travel between two adjacent designated Supplier POPs on the selected portions of the Supplier Backbone Network during a calendar month, as measured by Supplier and then return back to the source

2.49. **SC-APC:** means an optical connector with an angle polished ending compliant with IEC 61754-4 standard

2.50. **Scrubbing Centre:** means the part of the Service system where potential malicious DDoS traffic is redirected to, and filtered, and from where the filtered traffic is routed to the Customer network.

2.51. **Service**: means a service offered and supplied by the Supplier to the Customer under the terms of the MSA.

2.52. **Service Affecting Issue**: means, in relation to a Service, an unscheduled period during which the Service performs irregularly or otherwise not up to normal specifications.

2.53. **Service Availability:** means the percentage of time a Service is available for use as set out in the Service Level Objectives. It is calculated as (1- Service Downtime)

2.54. **Service Credit**: means a refund mechanism levied on the Supplier as a consequence of its failure to meet the SLA levels.

2.55. **Service Delivery Location:** means the facility where the Service is delivered to the Customer

2.56. **Service Demarcation Point:** means, in relation to a Service, the physical demarcation point where Customer can access the Supplier Network and use the Service. It is the dividing line which determines responsibility for installation and maintenance between the Customer and the Supplier

2.57. **Service Downtime:** means that period of time for which the Service was unavailable to the Customer during the Monthly Measurement Period.

2.58. **Service Element**: means any of the individual components of a Service. Some elements may be optional and thus selectable at the Customer's discretion

2.59. **Service Fees**: means in relation to a Service, all the charges payable by the Customer to Supplier in exchange for the Service provided by the Supplier, exclusive of taxes, as specified in the applicable Service Order

2.60. **Service Incident** means, in relation to a Service, an unplanned interruption to, or a reduction in the quality of the Service or a Service Element, provided that such interruption or degradation is not the result of an Excluded Event.

2.61. **Service Incident Ticket**: means a formal report from an Authorized Contact of the Customer in relation to a Service Incident. Service Incident Tickets have a unique identification number that is used for all subsequent updates and communications

2.62. **Service Interface:** means the physical network interface by which the Customer connects to the Service in the Service Demarcation Point

2.63. **Service Level Agreement (SLA)**: means, in relation to a Service, an agreement between Customer and Supplier setting the minimum performance level to be achieved by Supplier with respect to that Service. An SLA will be binding in respect of all supplies of the Service to which it relates.

2.64. **Service Level Objectives (SLO)**: means, in relation to a Service, the target service performance levels applicable in the provision of the Service.

2.65. **Service Order:** means the document (hardcopy or electronic form) submitted by the Customer and accepted by the Supplier, requesting the provision of a Service.

2.66. **Service Specifications Schedule (SSS):** means, in relation to a Service, a schedule setting out the technical and operational specifications of the Service. An SSS will be binding in respect of all supplies of the Service to which it relates.

2.67. **Service Term**: means, in relation of a Service Order, the committed period of time that the Service is delivered to Customer since the RFS Date.

2.68. **Service Termination**: means, in relation to a Service, the cancellation of the Service provision, with inter alia a complete wipe off of data and deletion of access records (if applicable) kept on the Supplier Equipment. A terminated service can´t be resumed, unless it is provisioned under a new Service Order.

2.69. **Service Use Policies (SUP):** means the acceptable practices and applicable policies that sets out the rules with which the Customer is required to comply in relation to receipt and use of Services. The Supplier reserves the right to amend the SUP in its sole discretion from time to time.

2.70. **Site Survey**: means a survey of a Customer Site to assess whether (in Supplier's opinion) the existing infrastructure is sufficient to provide the Service at that Customer Site and an access line is feasible to connect to a Supplier's Point-of-Presence

2.71. **Supplier:** means AFR-IX Telecom

2.72. **Supplier Account Representative:** means a member of the Supplier´s commercial staff.

2.73. **Supplier Equipment**: means any apparatus, material equipment, telecommunications equipment, energy equipment, wires, cables, ports, switches, routers, cabinets, racks, trays and other hardware and software owned by or licensed to Supplier for the provision of Services.

2.74. **Supplier Infrastructure:** means collectively the space, buildings, facilities, outside plant, data centers owned or controlled by Supplier, together with all infrastructure systems, power capacity and systems relating thereto, in or from which Services are offered.

2.75. **Supplier Infrastructure Policies (SIP):** means the acceptable practices and applicable policies enforced to follow to any individual when in and using the Supplier Infrastructure, . The Supplier reserves the right to amend the SIP in its sole discretion from time to time.

2.76. **Supplier Network**: means all the Supplier's network, including network hardware such as routers, firewalls, switches and cabling that is essential to the provisioning of Services

2.77. **Supplier Backbone Network**: means Supplier operated IP routing infrastructure consisting solely of selected Designated POPs

2.78. **Supplier Point-of-Presence (PoP)**: means a Colocation Datacenter or similar facility where Supplier has the operational equipment that interfaces with the Supplier Backbone Network

2.79. **Supplier Router:** means a high-capacity routers located at the Supplier PoPs that interface with the Customer Network

2.80. **Suspicious DDoS Traffic:** means the traffic flowing towards the IP Address(es) of the Protected Asset that includes potential DDoS attack and the legitimate (non-DDoS) traffic.

2.81. **Third Party Provider**: means a third party contracted by either Customer or Supplier that provides a supply that connects to the Service.

2.82. **Trouble Ticket:** means the method specified by Supplier to be used by the Sustomer for advising Supplier of a perceived service Incident or SLA non-compliance

2.83. **User**: means an individual who uses the Service

INTERNET SERVICES

IP TRANSIT SERVICE DESCRIPTION

3. SERVICE DESCRIPTION

3.1. **Overview.** IP Transit is a Service that provides dedicated access to the Supplier Backbone Network. With capacity-based pricing, it enables Customers to send and receive traffic over the public Internet by leveraging the Supplier's extensive international connectivity and numerous public and private peering arrangements

3.2. **Standards compliance:** IP Transit Service ensures packet routing is done in accordance with the technical standards set by the Internet Engineering Task Force (IETF).

3.3. **Service Scope**: The scope of IP Transit Service extends from the Customer's entrance Access Port to any port on a Supplier Router within the Supplier Backbone Network.

3.4. **Integrated security:** IP Transit is provided with integrated security and filtering features to help protect the users from malicious sites and threats.

3.5. **Service Delivery Locations:** IP Transit can be delivered at two types of Service Delivery Locations:

- 3.5.1. ON-NET. Service delivered at a designated Meet-Me Room in a Colocation Datacenter.
- 3.5.2. OFF-NET. Service delivered at Customer Premises, subject to availability

3.6. **Target Customers:** IP Transit is addressed to Customers who have their own Autonomous System Number (ASN), such as:

- 3.6.1. Content delivery networks: Organizations that distribute large volumes of content across the Internet.
- 3.6.2. Regional carriers: Providers offering carrier-grade quality Internet services to their customers.

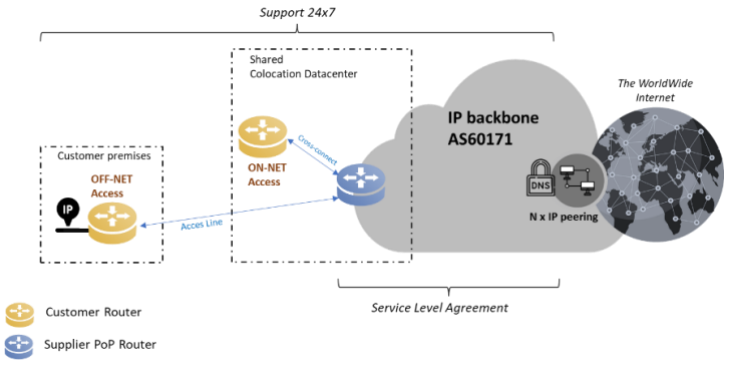
4. SERVICE ELEMENTS

4.1. **Core Service Elements**: IP Transit Service comprises the following essential elements:

- 4.1.1. Access Port: the network interface where the Service is delivered to the Customer.
- 4.1.2. Bandwidth: the data transfer speed at the Access Port, measured in bits per second, offered in a flexible bandwidth model.
- 4.1.3. Routing Configuration: the set of policies that governs the exchange of IP traffic from and to the Customer Network.
- 4.1.4. DDoS Blackholing
- 4.1.5. Service Monitoring and Service Support

4.2. **Optional Service Elements:** Customers can enhance their IP Transit Service with the following optional elements:

- 4.2.1. Dual-Homing
- 4.2.2. Access Line: A physical wiring that extends the Service Demarcation Point to the Customer Premises, required in OFF-NET configurations.
- 4.2.3. Extra Public IP Addresses: Allocation of extra public IP addresses to the Customer.
- 4.2.4. DDoS Mitigation.



5. SERVICE DELIVERY LOCATION

5.1. **Overview**: The IP Transit Service is delivered at a designated Service Delivery Location, configured according to one of the following options. The Service Demarcation Point specifies the exact location where the service is handed off to the Customer.

OPTION	SERVICE DELIVERY LOCATION	SERVICE DEMARCATION POINT
ON-NET	Any Supplier PoP location	Located in Meet-Me Room facilities in a Colocation Datacenter
OFF-NET with Access Line (*)	Customer Premises (**) An Access Line connects the Customer Premises with the Supplier PoP	Located in Optical Distribution Frame installed in the assigned area in Customer Premises

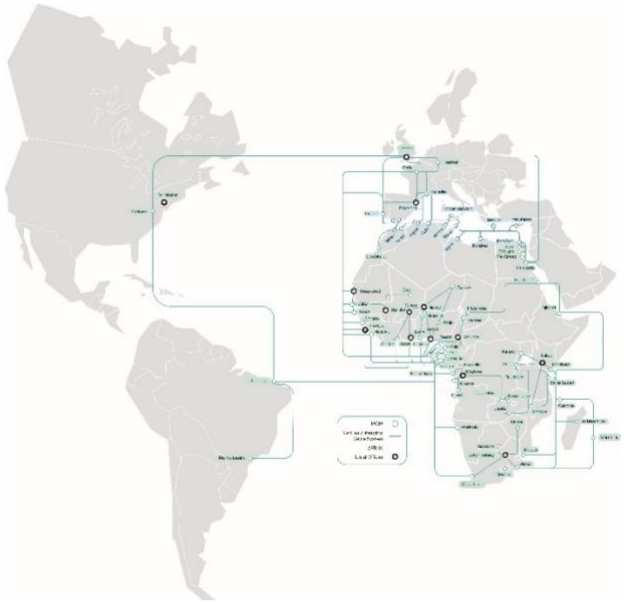
(*) Availability is contingent upon a positive feasibility assessment following a Site Survey conducted by the Supplier

(**) Only when Customer Premises are within **10Km** of the serving Supplier PoP

5.2. **Customer Responsibilities for Connectivity**: The Customer is responsible for procuring, installing and maintain, at their own expense, all necessary Customer Equipment, cabling, and patching required to connect to the Service Demarcation Point. If the Customer is unable to fulfill these duties, the Supplier can undertake them on his behalf and charge the Customer for any associated costs.

6. SUPPLIER POP LOCATIONS

Supplier Point-of-Presence (PoP) Network: The Supplier maintains a comprehensive and extensive worldwide network of Points-of-Presence (PoPs) strategically located, as indicated on the accompanying map. Customers have the flexibility to choose the Service Delivery Locations from any of the Supplier PoPs.



7. ACCESS PORT

7.1. **Overview**: Access Port is a Core Service Element of IP Transit Service, defining the point of connection where the Service is delivered to Customer. This Access Port is physically accessible at the Service Demarcation Point

7.2. **Access Port Configuration**:

7.2.1. Physical Interface

Single-mode fiber G652 terminated with an SC/APC connector. Additional interface options may be available upon the Customer's request to accommodate specific requirements.

7.2.2. Link Interface

Optical-based, standardized Ethernet interface. Customers can choose from a variety of available options, as detailed in the following table. Traffic is managed using IEEE 802.1Q tagged VLANs.

INTERFACE		SPEED	STANDARD	TYPICAL REACH
1000BaseLX		1 Gbps	802.3z	10 Km
10GBaseLR		10 Gbps	802.3ae	80 Km
100GBaseLR4		100 Gbps	802.3ba	8 Km
100GBaseER4		100 Gbps	802.3ba	28 Km

7.2.3. Frame Size

The standard Maximum Transmission Unit (MTU) frame size is 1,500 bytes but "jumbo" MTU frame sizes up to 9,500 bytes are also supported on request

7.3. **Traffic Symmetry**: The traffic in IP Transit Service shall be symmetric type only (e.g. Outbound Traffic and Inbound Traffic bandwidth shall be equal)

7.4. **Severability of Services in a single Access Port**. Customers can consolidate multiple Services onto a single Access Port. By using multiple tagged Virtual Local Area Network (VLAN) instances, several different Services, such as IP Transit, Dedicated Internet Access (DIA), Multiprotocol Label Switching (MPLS), and Virtual Private LAN Service (VPLS), can share the bandwidth of a single Access Port. Each Service may require a separate Committed Data Rate (CDR), which is implemented using a combination of Ethernet and networking technologies along with policy enforcement mechanisms.

8. ACCESS LINE IN OFF-NET DELIVERY

8.1. **Overview**: The Access Line is an optional Service Element of IP Transit Service required in OFF-NET delivery configuration. The Access Line facilitates a dedicated physical connection to deliver IP Transit Service at a designated Customer Premises.

8.2. **Provision of Access Line**: The Supplier will be responsible for enabling a fiber optic line that runs from the designated Supplier PoP to the Customer Premises. This line may be owned by the Supplier or leased by the Supplier from a Third-Party Provider.

Each Access Line provides connectivity to a single Access Port, ensuring there is a one-to-one correspondence between the Access Line and the Access Port.

8.3. **Network Interface Device (NID):** The Access Line will be terminated in a Network Interface Device (NID) at the Customer Premises which is installed by the Supplier. The NID is an active equipment that converts the native single-mode fiber delivery to the appropriate Service interface. The Supplier retains ownership of the installed NID and is responsible for its monitoring and maintenance throughout the Service Term

8.4. **Customer Responsibilities for OFF-NET Delivery**: When opting for OFF-NET delivery, the Customer is responsible for the following supplies and to ensure they are available in sufficient time to enable to achieve the planned RFS Date. All associated costs to these supplies are the sole responsibility of the Customer

8.4.1. Right of Way: The customer must grant to the Supplier all necessary rights of way and consents required for the installation of the Access Line inside the Customer Premises.

8.4.2. Access Permission: The Customer must provide access credentials to perform provisioning and maintenance tasks to designated Supplier's technicians

8.4.3. Rack Space: The Customer must provide rack space in a standard 19-inch cabinet to accommodate the Network Interface Device and associated hardware. This space must include a minimum of 3 contiguous rack units (3 x 1.75 inches in height) with a minimum width of 24 inches.

8.4.4. Electrical Power: The Customer must provide a secure, continuous and appropriate electrical power supply for the operation and maintenance of the NID and the Service at such points and with such connections as the Supplier specifies, adhering to all applicable safety regulations and wiring standards at the Service Delivery Location. It is recommended to use a power conditioner or an Uninterruptible Power Supply (UPS) to mitigate transients and fluctuations in the mains power

 2 x IEC320-C13	230 volt AC 10 Amp breaker Power: 100 Watt

8.4.5. Environmental Conditions. The Customer must ensure that the active Supplier Equipment installed at the Customer Premises operates within the following environmental parameters: (i) temperature between 15°C and 35°C, and (ii) relative humidity between 20% and 60%

9. BANDWIDTH

9.1. **Overview:** Bandwidth is a Core Service Element of IP Transit Service. The Bandwidth refers to the capacity of the network connection to transmit/receive data through an Access Port. It is typically measured in bits per second (bps) and its multiples (Kbps, Mbps, Gbps, etc.).

9.2. **Flexible Bandwidth Model**: The Service offers a flexible bandwidth model designed to accommodate dynamic bandwidth needs of Customers.

9.2.1. Committed Data rate (CDR): The CDR sets a baseline for guaranteed bandwidth, ensuring a minimum level of performance and reliability.

9.2.2. Bursting Capabilities: means the flexibility to temporarily exceed the CDR threshold, when necessary, up to the maximum capacity of the Access Port. This allows for the accommodation of peak traffic demands without the need for permanent bandwidth upgrades.

OPTION	CDR (Gbps)	Max Bursting (Gbps)
1G/0.5G	0.5 G	1
10G/1G	1 G	10 G
10G/2G	2 G	10 G
10G/5G	5 G	10 G
100G/20G	20 G	100 G
100G/50G	50 G	100 G

9.3. **Aggregate CDR**: The Service features the choice for an aggregate CDR bandwidth shared across multiple Access Ports. This configuration is particularly suited for solution architectures aimed at enhancing diversity or resilience.

9.4. **Disclaimer:**

9.4.1. Actual Throughput: CDR figures are calculated based on raw traffic bitstream. Actual information throughput is typically lower due to frame overheads and the inherent characteristics of IP transmission protocols

9.4.2. Bursting capability: Bursting is allowed up to the physical limit of the Access Port. However, bursting is only guaranteed up to two times the CDR. Bursting above that threshold is delivered on a best effort basis, which means that it might experience service quality issues if there is congestion in the network

9.4.3. Transmission performance disclaimer: The Supplier does not guarantee transmission performance beyond the Supplier Backbone Network

10. ROUTING CONFIGURATION

10.1. Overview

10.1.1. Routing Configuration is a Core Service Element of IP Transit Service. The IP Transit Service is established through the connection of two IP routers: one situated in the Customer Network (Customer Router) and the other in the Supplier Network (Supplier Router). Routing Configuration involves the implementation of specific policies and rules on these routers in a coordinated way, governing the IP traffic sent and received through this connection.

10.1.2. Each router enforces its respective policies to effectively manage Outbound Traffic and Inbound Traffic. However, the effectiveness of the IP Transit Service relies heavily on collaborative policy management between the Customer and the Supplier. Alignment of policies ensures seamless traffic flow, optimal performance and robust security.

10.2. Customer Routing Options

10.2.1. The Customer is responsible for defining and filtering which traffic originated within their network shall be routed to the Internet (Outbound Traffic) through the IP Transit Service. Additionally, the Customer is responsible for determining which incoming Internet traffic directed to their network (Inbound Traffic) shall be routed through the IP Transit Service. Routes for Inbound Traffic and Outbound Traffic are not necessarily the same.

10.2.2. To configure Outbound Traffic, the Customers have the following options to manage their network traffic effectively:

OPTION	DESCRIPTION
Default Routing	IP Supplier Network is the default route for all Outbound Traffic
Static Routing	IP Supplier Network routes Outbound Traffic for some selected IP Network Prefixes set statically by the Customer
BGP Routing	IP Supplier Network routes Outbound Traffic dynamically as indicated by BGP operation

10.2.3. Default Routing: Default Routing involves configuring the Customer Router to use a default IP route provided by the Supplier for all Outbound Traffic. This approach simplifies routing tables by providing a catch-all mechanism. It directs traffic destined for any unknown or unspecified destination towards the Supplier Backbone Network, ensuring connectivity without the need for detailed routing table entries.

10.2.4. Static Routing**:** Static Routing involves configuring the Customer Router to use a default IP route provided by the Supplier for the Outbound Traffic of only selected IP Network Prefixes configured by Customer. These routes remain fixed and do not dynamically update. Failover scenarios require additional manual intervention to redirect traffic to alternate paths, making this option suitable for environments where network topology remains stable and predictable.

10.2.5. BGP Routing. Border Gateway Protocol (BGP) Routing facilitates a routing environment where the Customer Router dynamically takes routing decisions based on a Routing Table received from the Supplier Network through a BGP session. This allows for dynamic selection of the best routing paths based on real-time network conditions.

10.2.6. Combining Routing Approaches: BGP Routing and Static Routing can complement each other to create a robust and flexible routing environment. Static Routes ensure stability and predictability for critical paths and BGP Routing offers dynamic control and optimization.

10.3. BGP Description

10.3.1. Overview: Border Gateway Protocol (BGP) is a standardized and well-established routing protocol that enables the exchange of network reachability information between different Autonomous Systems on the Internet. BGP also facilitates the establishment of routing policies that govern the exchange of traffic between Autonomous Systems.

10.3.2. Standardization and Implementation: IP Transit Service implements BGP-4, adhering to the standards outlined in RFC 4271.

10.3.3. Capacity: Implementing BGP requires routers with sufficient memory, processing power, and bandwidth to handle the large volume of routing information. It also demands expertise in BGP configuration and operation to optimize routing performance effectively.

10.4. BGP Operation in IP Transit

10.4.1. Configuration: the BGP interface must be first configured manually in both designated BGP-peer routers.

10.4.2. BGP Session: To operate the BGP protocol, a BGP session must be established and maintained between both designated BGP-peer routers. This BGP session is established over a TCP connection on port 179 and is typically transported within a tagged VLAN. BGP-peers exchange "keepalive" messages at regular intervals to maintain the active status of BGP sessions. If a BGP peer becomes unreachable or fails to respond within a specified time frame, the session is terminated, and routes learned from that peer are withdrawn to prevent routing loops or blackholing of traffic.

10.4.3. Routing Information Exchange: Along the BGP session, BGP-peers exchange routing information by advertising the IP Network Prefixes they can reach each side.

IP Network prefixes advertised to Customer Router by IP Transit Service can come with two options:

i. Full Routing Table: Details routes to every destination on the Internet

ii. Partial Routing Table: Details routes to a subset of IP Network Prefixes, filtered by the Supplier, corresponding to the most common IP destinations. Partial Routing Table reduce the complexity of routing, enhancing efficiency and scalability, and reducing overhead.

IP Network Prefixes advertisements may be aggregated using Classless Inter-Domain Routing (CIDR) to reduce the size of Routing Tables

10.4.4. Route Selection and IP Routing Table: Each route advertisement includes various BGP attributes such as Next-Hop, AS-Path, Local Preference, Multi-Exit Discriminator (MED), and Community. These attributes play a crucial role in influencing route selection and managing traffic flow at each BGP-peer, allowing for sophisticated traffic engineering and policy enforcement. In scenarios where multiple routes to the same destination exist, BGP-peers utilize the attributes to determine the optimal path. The selected routes are then installed in the IP Routing Table of the router.

10.4.5. Network Topology and Convergence: BGP-peers exchange periodic updates to reflect changes in network topology, such as new routes becoming available or existing routes being withdrawn. Achieving consistent routing information across all BGP routers may require a convergence time, during which routers synchronize their IP Routing Tables to ensure network stability and optimal performance.

10.5. Routing Security Features

IP Transit Service offers robust capabilities to enhance the security of BGP sessions, ensuring the integrity and reliability of routing operations

10.5.1. BGP Route Filtering: Implement route filters based on BGP attributes to control which IP Network Prefixes are accepted and advertised. This ensures that only legitimate traffic is propagated.

10.5.2. MD5 Authentication: Implement MD5 authentication for BGP sessions to authenticate peers and prevent unauthorized route injections by unauthorized or malicious devices, mitigating the risk of session hijacking or spoofing attacks.

10.5.3. Route Origin Validation (ROV) with RPKI: Verify the origin of BGP routes using Route Origin Validation (ROV) with Resource Public Key Infrastructure (RPKI). This validation process ensures that the origin AS for a BGP route is authorized to advertise the IP Network Prefix. To operate this feature, Customers are required to create a Route Origin Authorization (ROA) record with the respective Internet Registry (IR) to validate their IP routes. Invalid BGP announcements are discarded, protecting against routing leaks and hijacks and ensuring that Customer traffic is routed only to legitimate destinations.

10.5.4. Monitoring and Logging: Implement comprehensive monitoring and logging mechanisms to detect and respond to suspicious activities and traffic anomalies in real-time. Monitoring tools provide visibility into BGP session activities, traffic patterns, and routing changes, enabling proactive security management and rapid incident response.

10.5.5. BGP session protection with ACL: Restrict access to BGP sessions using Access Control Lists (ACLs) to allow sessions only from trusted IP addresses or peers. ACLs define permitted and denied access policies based on source IP addresses or port numbers.

10.6. Redundant BGP Sessions

10.6.1. Overview: IP Transit Service offers Customers the capability to establish redundant BGP sessions to create diversity architectures. Redundant BGP peering enables several solution architectures and provides several benefits to Customers such as failover capabilities, load balancing of traffic or geographic redundancy

10.7. Customer Obligations

10.7.1. BGP Maintenance and Configuration: The Customer is solely responsible for the maintenance and configuration of BGP protocol on their equipment. This includes ensuring the proper setup and ongoing management of BGP sessions, route advertisements, and policy configurations.

10.7.2. Registration with Internet Registries: The Customer must register all routes and downstream Autonomous System (AS) Numbers with Internet Registries from which they wish to receive traffic via IP Transit Service. Additionally, the Customer must ensure timely payment of all fees owed to relevant Internet Registries for his IP space

10.7.3. IP Network Prefixes: IP Network Prefixes advertised by the Customer must be at least a /24 in size to be globally routable. For smaller prefixes, the Customer must advertise them with the "no-export" COMMUNITY attribute and advertise an aggregate prefix of /24 or larger covering all smaller prefixes over each BGP session.

10.7.4. Full BGP Routing Table Capability: If opting to receive a full BGP Routing Table, the Customer must ensure their equipment is capable of supporting the current table size and its future growth. This includes sufficient memory, processing power, and bandwidth to handle the volume of routing information exchanged.

10.7.5. Inbound and Outbound Filtering: The Customer must implement and maintain appropriate inbound and outbound filtering to protect both the Customer Network and the Supplier network

10.7.6. Communication and Coordination: Regular communication and coordination between Customer and Supplier is essential. This ensures that policies are adapted promptly in response to evolving network conditions, changes in traffic patterns, and emerging security threats.

10.8. Routing Operation Disclaimer

Note the following important disclaimers regarding routing operations:

10.8.1. Upstream Transit Providers: Supplier makes no guarantee that its upstream IP transit providers will update their filters within a short timeframe

10.8.2. Routing Policies of Upstream Providers: Supplier makes no guarantees, explicit or implicit, about the routing policies of other upstream transit providers and the routes that they accept into their routing tables

10.8.3. Public AS Numbers: Supplier will not provide public AS numbers to Customers. Customers should contact the correspondent regional Internet Registry for allocation of such resources.

10.8.4. IP Network Prefix Ownership: By requesting the registration of a prefix or AS Number, the Customer warrants that it is the legitimate owner or leaseholder of those resources, or has authorization from the owner or leaseholder to use them. Supplier will only accept IP Network Prefixes that the Customer is entitled to originate. In case of a complaint regarding the Customer's use of an Internet resource (such as an IP block or AS number), Supplier will resolve such complaints in accordance with the organization listed in the Internet Registry WHOIS database. In disputes, the burden of proof lies with the Customer to demonstrate ownership of the resource. If unable to do so, any decision by Supplier to deny a prefix announcement will not be considered a breach of the Service Level Agreement (SLA).

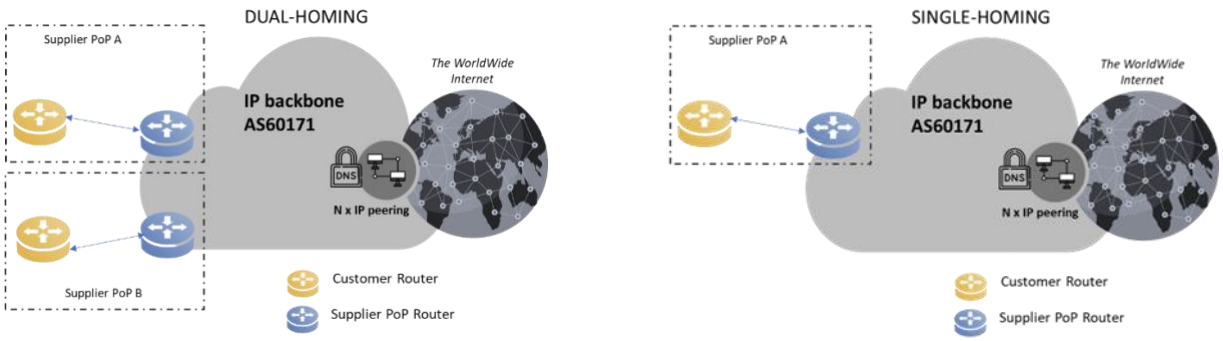
11. SOLUTION ARCHITECTURES

11.1. **Service delivery options: Single-Homing and Dual-Homing**

The IP Transit Service can be delivered according to the configurations as detailed in the table below, which the Customer can select based on their specific requirements and redundancy needs. All mechanisms outlined in this section deal only with the traffic towards the Customer Network. Outbound traffic path to Internet should also be adjusted by the Customer by tuning the routing decision policies of the Customer routers

OPTION	DESCRIPTION
Single-Homing	Service is delivered in a unique Service Delivery Location
Dual-Homing	Service is delivered in two distinct Service Delivery Location

Single Homing refers to the connection of the Customer Network to the Supplier Network through a single Service Delivery Location. Dual-Homing involves connecting the Customer Network to the Supplier Network through two different Service Delivery Locations situated in distinct Supplier Points of Presence (PoPs). This setup typically includes multiple BGP sessions, which are essential for ensuring optimal routing and redundancy. This configuration enhances reliability and redundancy, ensuring that traffic can be rerouted in case one connection fails and facilitates load balancing. On the other side has a higher cost and more complex configuration.



11.2. Service delivery options: Single circuit or Multiple circuits

The connectivity to the Service Delivery Location can be implemented:

11.2.1. Using a Single circuit. Static routing would be sufficient. BGP is optional. This option provides a straightforward and cost-effective solution for Customers who have minimal requirements in terms of traffic engineering and redundancies.

11.2.2. Using Multiple circuits. BGP is enabled for automatic fail-over. The IP Transit Service supports several multi-circuit configuration options:

i. BGP Multipath: Allows to install multiple equal-cost BGP circuits with the Supplier Backbone Network that can be used simultaneously. For each additional circuit, a separate BGP session is established. This approach provides greater flexibility and redundancy, improving fault tolerance and load distribution.

ii. Link Aggregation. Allows to install multiple Ethernet circuits bonded together using LACP to form a single logical link and a single one-hop BGP session.

iii. Active-Backup. Allows to install multiple BGP circuits with the Supplier Backbone Network, one path as the primary (active) path and one or more paths as backups. The backup paths are only used if the primary path fails.

iv. Active-Active. Allows to install multiple BGP circuits with the Supplier Backbone Network that can be used simultaneously. Each circuit is preferred for a subset of Customer IP Network Prefixes, and the other circuits preferred to a different set of Customer IP Network Prefixes.

12. SERVICE MONITORING AND SERVICE SUPPORT

12.1. **Overview:** Service Monitoring is a Core Service Element of IP Transit Service. IP Transit Service offers comprehensive monitoring capabilities for Customers, ensuring visibility, control, and proactive management of network performance and service availability. The following are the key monitoring capabilities offered:

12.2. **Traffic Utilization Monitoring**:

12.2.1. Bandwidth Usage: Real-time and historical data on bandwidth consumption, both inbound and outbound.

12.2.2. Traffic Patterns: Analysis of traffic patterns over time, including peak usage periods and trends.

12.3. **BGP Routing Monitoring**:

12.3.1. BGP Route Visibility: Visibility into BGP routing updates and the status of advertised routes.

12.3.2. Route Convergence: Monitoring BGP route convergence times to ensure efficient routing updates and minimal impact on network performance.

12.4. **Network Performance Metrics**:

12.4.1. Latency Monitoring: Measurement of network latency across different destinations and over time.

12.4.2. Packet Loss: Monitoring packet loss rates to identify network congestion or quality issues.

12.5. **Service Availability and Uptime**:

12.5.1. Service Monitoring: Monitoring of Service availability and uptime based on SLA commitments.

12.5.2. Incident Reporting: Notification of Service Incidents, along with status updates and resolution timelines.

12.6. **Customer Portal and Reporting**:

12.6.1. Dashboard: Access to a web-based Customer Portal displaying network performance metrics and status updates.

12.6.2. Custom Reports: Generation of customized reports on network utilization, performance trends, and SLA compliance.

12.7. **Support and Troubleshooting Tools**:

12.7.1. Troubleshooting Assistance: Access to diagnostic tools and utilities to troubleshoot connectivity issues and analyze network performance metrics.

12.7.2. Technical Support: Availability of technical support resources, including access to network engineers for assistance with configuration or troubleshooting.

13. DDOS DETECTION AND DDOS MITIGATION

13.1. **Overview**. Distributed Denial of Service ("DDoS") attacks may from time to time affect the Service by flooding Customer's system with undesired incoming traffic. To safeguard the Customer's Protected Assets, the IP Transit Service includes DDoS Detection and offers DDoS Mitigation as an optional capability

13.1.1. DDoS Detection continuously monitors incoming and outgoing traffic to and from the Protected Assets. It identifies potential DDoS attacks and helps block malicious traffic. DDoS detection is a Core Service Element of IP Transit and is included in the standard service delivery

13.1.2. DDoS Mitigation is an Optional Service Element that provides an DDoS protection enhancement, available at an additional cost

13.2. **DDoS Blackholing**. DDoS Blackholing offers comprehensive measures to safeguard against DDoS attacks. The key components include:

13.2.1. Protection Configuration. Customer and Supplier agreement on a list of IP Protected Assets to which the DDoS Blackholing applies.

13.2.2. Real-time traffic monitoring. Continuous monitoring of traffic patterns by different metrics (bandwidth utilization, packet pattern, etc.) is conducted to detect anomalies that may indicate a DDoS attack

13.2.3. Detection of Suspicious DDoS Traffic. If the Supplier detects traffic containing a DDoS attack toward the Protected Asset, such traffic is considered Suspicious DDoS Traffic. Additionally, the Customer may contact the Supplier to request DDoS Blackholing if an attack is not detected by the Supplier or directly apply the correct BGP community tag to the impacted IP Protected Asset

13.2.4. Traffic Diversion Response. Upon detection of an anomaly that is indicative of a DDoS attack, the Suspicious DDoS Traffic is diverted to the Supplier's null-route or "black hole".

i. DNS Mode. The Protected Asset is considered a protected domain. Traffic is diverted via a change in the DNS setting

ii. BGP Mode. The Protected Asset is considered IP address. Traffic is diverted via BGP routing protocol

13.3. **DDoS Mitigation.** DDoS Mitigation provides advanced mechanisms to protect against and mitigate the effects of DDoS attacks. Key features include:

13.3.1. Advanced filtering techniques. Utilizes sophisticated algorithms and filtering methods to distinguish between malicious and legitimate traffic.

13.3.2. Scrubbing Centers. A Scrubbing Center is a specialized facility used by DDoS mitigation services to filter and clean incoming network traffic. When DDoS mitigation feature is active, Suspicious DDoS Traffic is redirected to Supplier's Scrubbing Centers where it undergoes thorough cleansing to remove malicious traffic. Traffic is subjected to multiple layers of statistical analysis, active verification, and anomaly recognition to identify and eliminate malicious packets, ensuring that only clean traffic reaches the Customer Network

13.3.3. DDoS Mitigation Capacity. The Service provides different level of DDoS Mitigation Capacity ranging from 20 Gbps, 50 Gbps and 100Gbps peak throughput.

13.3.4. Traffic Rerouting. The filtered traffic from the Supplier's Scrubbing Centers will then be routed back to the Customer's Protected Asset

13.3.5. Comprehensive reporting. Detailed reports on detected and mitigated DDoS attacks. Includes information on attack vectors, duration, volume, and mitigation measures taken

13.3.6. Support and guidance. Access to the Supplier's security experts for support and guidance during and after an attack. Offers insights and recommendations to improve future resilience and enhance overall security posture

13.4. **Performance Disclaimer**

13.4.1. DDoS Monitoring and Mitigation. DDoS attack monitoring, detection, and filtering are provided on a best effort basis. Due to the unpredictable nature of DDoS attacks, the Supplier cannot guarantee complete mitigation or elimination of all DDoS attacks, nor guarantee identification and blocking of all malicious traffic on every occasion. It is acknowledged that during mitigation, some potentially legitimate traffic may be discarded, even if it appears to conform to normal traffic patterns

13.4.2. Actions Against Adverse Impact. In the event that the Supplier has reason to believe that the DDoS attack associated with the Protected Asset will cause adverse impact to the Supplier Backbone Network, the Supplier will, at its sole discretion and without prior notice, implement necessary actions to reduce the impact of such DDoS attack. These actions include, but are not limited to, black hole of the IP Addresses being attacked, or alteration to the routing of the traffic destined to the IP Addresses being attacked.

13.4.3. Limitations of Scrubbing Capacity. Scrubbing of DDoS traffic as an action to mitigate a DDoS attack is limited to the current capacity of the on-net scrubbing system within the Supplier Network. At any given time, the current capacity will depend on the source of the attack traffic, the ingress route and type of traffic destined for the host under attack, the volume of concurrent traffic being scrubbed and other factors. Where a DDoS attack is larger than the scrubbing capacity, the Supplier may black hole traffic or use other methods at its disposal to mitigate the attack.

13.4.4. Supplier's Liability Disclaimer. With respect to the DDoS Protection, the Supplier is not liable and otherwise excludes all liability in negligence or otherwise in connection with:

i. Traffic rerouted away from the Customer or any resulting delays caused by routing, filtering, or cleaning of Customer traffic.

ii. DDoS events that are not detected or mitigated by the Supplier.

iii. Any traffic to or from the Customer's Service that may experience delays, drops, or other forms of impact

13.4.5. Scope of DDoS Mitigation. DDoS Mitigation does not include: load balancing of traffic, permanent archival/storage of log files, forensics or investigations, legal case preparation, security consulting services or disaster recovery planning.

13.4.6. Data Processing Terms. The Supplier is not the data processor for the Customer traffic passing through the Supplier's Scrubbing Centers under Data Protection Terms

13.4.7. Types of DDoS Protection Provided. The DDoS Protection provides volumetric DDoS protection, not protection against application-level attacks.

13.4.8. Exclusion of Indirectly Affected Services. Attacks that target third-party services or infrastructure not directly under the control of the Customer or Supplier, affecting the service indirectly, are excluded from coverage.

14. PUBLIC IP ADDRESSES ALLOCATION

14.1. Overview

14.1.1. Supplier Public IP Addresses. Public IP Addresses are an optional Service Element of the IP Transit Service. While IP Transit connectivity and the establishment of BGP sessions can technically be implemented using private IP addressing, private IPs are not routable on the public Internet. Consequently, they cannot be used for advertising routes intended to be accessible globally.

To address this limitation, the Supplier provides a public IP Address subnet as part of the standard IP Transit Service delivery. Public IP addresses enable seamless communication between the Customer and the Supplier over the public Internet, facilitating the exchange of routing information. The Supplier will advertise these public IP addresses assigned to the Customer to the global Internet, ensuring their reachability.

14.1.2. Customer-supplied IP Addresses. Customers also have the option to use their own public IP Addresses. In such cases the Customer must also handle the necessary administrative tasks related to the management and upkeep of their IP address allocations to maintain their validity and global routability.

14.2. Scope

14.2.1. Standard Allocation. The standard allocation of Public IPv4 addresses in IP Transit is listed in the following table.

OPTION	IPv4	IPv6
Single-Homing architecture	/30 subnet	/64 subnet
Dual-Homing architecture	/29 subnet	/64 subnet

14.2.2. Extra Allocation. The Customer may request at an additional charge the reallocation of additional contiguous IP Addresses, which is subject to Supplier's approval. Depending on the size of the address reallocation, additional information may be required from the Customer in order for the Supplier to fulfil the request. Additional IP Addresses allocation can be provided according to the following offering. These Addresses can be purchased as IPv4 only, IPv6 only, or as a dual stack where IPv4 and IPv6 are combined.

IPv4	IPv6
/30 subnet	/64 subnet
/29 subnet	/48 subnet
/28 subnet	
/27 subnet	
/26 subnet	
/25 subnet	
/24 subnet	

14.3. Disclaimer

14.3.1. Ownership and Transfer of IP Addresses. Any Public IP addresses allocated to the Customer by the Supplier remain the property of the Supplier and are not transferable.

14.3.2. Termination of IP Address Usage. The Customer's right to use the Supplier delivered IP addresses ceases upon the termination of the agreement for supply of the Service, cancellation of the Service, or where the Supplier discontinues providing the Service to the Customer

14.3.3. IP Address Changes. The Supplier reserves the right to change any Supplier-delivered IP addresses allocated to the Customer with at least 7 days' notice, or immediately in urgent situations necessary to maintain Supplier backbone Network availability, stability, or to rectify faults. The Supplier will collaborate with the Customer to minimize service disruption during such changes

14.3.4. Subnet Requests. Requests for more than /24 subnet Public IPv4 Addresses are not generally available from the Supplier and should be referred to the relevant Internet Registry.

14.3.5. Payment Responsibilities. In the event the Supplier is aware that the Customer has failed to make payment of any fee due and payable, the Supplier may be entitled to terminate the relevant Service Order

15. SERVICE CONFIGURATION PROCEDURE

15.1. **Network Assessment and Design**:

15.1.1. Define Requirements: Understand the Customer network requirements, including traffic volume, and expected growth.

15.1.2. Topology Design: Determine the physical and logical topology. This includes selecting the appropriate Access Port(s), Access Line(s), and Service Delivery Location(s)

15.1.3. Addressing Plan: Plan IP addressing schemes, ensuring they comply with Internet registry (IR) guidelines.

15.2. **Access Port Configuration**

15.2.1. Define Architecture: Choose between single/dual homed and single/multiple circuits

15.2.2. Interface Selection: Choose the appropriate physical interface for the Access Port and Bandwidth

15.2.3. VLAN Configuration: Implement IEEE 802.1Q tagged VLANs to segregate different types of traffic on the same Access Port.

15.3. **Routing Protocol Selection**

15.3.1. ASN Assignment: Ensure the Customer has an Autonomous System Number (ASN) assigned

15.3.2. BGP Configuration: If using BGP, configure BGP sessions between the Customer Router and the Supplier Router. Alternatively, configure static routes if BGP is not used or for specific routes that do not need dynamic updates

i. The Customer must set in the IP-Configuration Form all routes and downstream ASN from which it wishes to receive traffic from the Supplier Network. The Supplier will update its own filters and advise its upstream providers and peers accordingly.

ii. The Customer must set in the IP-Configuration Form the list of IP Network Prefixes that they want to announce, ensuring that the prefixes are registered in an appropriate Internet Registry

15.3.3. BGP Peering: Configure parameters and establish BGP sessions over TCP port 179.

15.3.4. Address Family Configuration: Define address families (IPv4 or IPv6) and configure route advertisements and filters.

15.4. **Routing Policies and Filters**

15.4.1. Prefix Filtering: Implement prefix lists or route maps to filter inbound and outbound routes based on specific criteria (prefix length, AS path, community attributes).

15.4.2. Route Aggregation: Use route aggregation (CIDR) to reduce the size of routing tables, especially when advertising multiple smaller prefixes as a single larger prefix.

15.5. **Security Considerations**

15.5.1. ACLs: Apply Access Control Lists (ACLs) to BGP sessions to control which IP addresses or networks are allowed to establish BGP peering sessions.

15.5.2. BGP Session Protection: Use ACLs or firewall rules to protect BGP sessions from unauthorized access or attacks.

15.6. **Monitoring and Optimization**

15.6.1. Performance Monitoring: Set up monitoring tools to track BGP session status, route updates, and traffic metrics.

15.6.2. Traffic Engineering: Use BGP attributes (e.g., MED, local preference) for traffic engineering to influence path selection and optimize traffic flow.

15.6.3. Regular Review: Periodically review routing configurations to ensure they align with network requirements and security policies.

15.7. **Testing and Validation**

15.7.1. Functional Testing: Conduct thorough testing of the routing configuration to verify connectivity, route propagation, and failover mechanisms.

15.7.2. Validation: Validate that traffic is flowing correctly according to routing policies and that failover mechanisms work as expected in case of link or router failures.

15.8. **Documentation and Handover**

15.8.1. Documentation: Document the routing configuration, including diagrams, IP addressing schemes, BGP configurations, ACL rules, and any special configurations.

15.8.2. Handover: Provide documentation to the Customer along with training or guidance on monitoring tools and maintenance procedures.

16. SERVICE FEES AND MINIMUM SERVICE TERM.

16.1. **Overview**. The Service is charged based on the following items. Rates are specified in the applicable Service Order. Non-Recurring Charges (NRC) are incurred to cover the materials and labor associated with installation. Monthly Recurring Fees (MRC) are associated to the operation of the Service.

	NRC	MRC	Use On demand	Comment
Access Port	X			Multiple Access Ports provisioned in dual-homed architectures
Bandwidth CDR		X		Bandwidth is associated to each Access Port. Aggregated Bandwidth can be used in dual-homed architectures
Bandwidth Burst			X	When usage above the CDR. If the IP Burst Fee is not listed in the Service Order, it will be 25% more than the per Mbps fee for the CDR
Cross-Connection	X	X		Chargeable when provided by the Supplier
DDoS Mitigation	X	X	X	Optional feature. DDoS Blackholing is included in the standard delivery. Offered as: (i) Flat rate independent of number and size of attacks (ii) On demand usage-based billing
Extra allocation IP Addresses	X	X		Optional Extra IP addresses requested in addition of the standard allocation.
Access Line	X	X		Only in OFF-NET delivery and chargeable when delivered by the Supplier
Professional Services			X	Site Survey, technical support, etc.

16.2. **Bandwidth Burst calculation**. If the actual Service bandwidth utilization by Customer exceeds the CDR in a particular month, the MRC in that particular month is set according to the 95th percentile method, with the following procedure:

16.2.1. Samples of average Bandwidth utilization rates of both Inbound and Outbound Traffic from Customer Access Ports are regularly collected in five (5) minute intervals over a calendar month

16.2.2. The higher of such samples (Inbound or Outbound) are sorted from highest to lowest

16.2.3. The highest five percent (5%) of the samples are discarded and the next highest sample is chosen to represent the 95th bandwidth utilization of that month.

17. BUSINESS OPERATIONS.

17.1. Service Termination before Service Term expiration may be subject to Early Termination Charges as set forth in the Service Order and/or the MSA.

Service Element	Request	Change during Service Term	Termination before Service Term expiration
Access Port	Through the Supplier Account Representative	Not permitted. Existing Service shall be terminated and implement the changes in a new Service Request	Through Supplier Account Representative
Bandwidth	Through the Supplier Account Representative	Through the Supplier Account Representative	Through Supplier Account Representative
Cross-Connection	Through the Supplier Account Representative	Through the Supplier Account Representative	Through Supplier Account Representative
DDoS Mitigation	Through the Supplier Account Representative	Through the Supplier Account Representative	Through Supplier Account Representative
Extra allocation of IP addresses	Through the Supplier Account Representative	Through the Supplier Account Representative	Through Supplier Account Representative
Access Line	Through the Supplier Account Representative	Not permitted. Existing Service shall be terminated and implement the changes in a new Service Request	Through Supplier Account Representative

SERVICE LEVEL AGREEMENT

18. GENERAL SCOPE

18.1. **Scope**

This Service Level Agreement (SLA) is an agreement between the Supplier and the Customer wherein are set out the committed Service Level Objectives (SLO) in the provision of Services. The SLO contains the qualitative and quantitative performance levels by which Supplier ensures to deliver and support the Services to Customer, and the Service Credits, if any, for failure to meet these performance levels. Unless otherwise stated in the relevant Service Order, these performance levels shall apply.

The Supplier will maintain sufficient capability, systems, and processes to promptly respond to and address Service Incidents that affect, or have the potential to affect, the Services or the operation of the facility. The Supplier monitors the critical equipment providing the alerts staff to investigate and take appropriate and timely corrective action.

19. TERMS AND EXCLUSIONS

19.1. **SLO Excluded Events**. Service Level Objectives shall not take in account Service Incidents, Service Outages or any Service Affecting Issue caused by or connected to any of the following events (each one an "Excluded Event").

19.1.1. Events associated with failures of systems, software, hardware, wiring, power, networks (including consumption of services over the Internet) which are not operated or provided by Supplier.

19.1.2. Events due to failures located further than the Demarcation Points of the affected Service

19.1.3. Events attributable to the negligence, act, or omission of Customer (including any of its representatives) or a Third-Party Provider not within Supplier's direct control.

19.1.4. Events associated with Customer's delay or non-performance of any of Customer's obligations set out in the MSA

19.1.5. Events as consequence of any Force Majeure Events stipulated in the MSA.

19.1.6. Events associated to Planned Maintenance, up to an accumulated total of eight (8) hours per calendar month.

19.1.7. Events associated to Emergency Maintenance, if announced at least sixty (60) minutes in advance, up to an accumulated total of two (2) hours per calendar month.

19.1.8. Events during Support Hold or Service Suspension periods set by the Supplier according to the terms of the MSA

19.1.9. Events caused by the inability, refusal or delay by a Third-Party Provider to provide the Access Line at Customer Premises

19.1.10. Events caused by a service failure at any other Customer Premises

19.1.11. Events associated to the Customer failing to agree to the installation of an upgrade, patch or change recommended by Supplier, such as security or other fixes.

19.1.12. Events associated to any misuse of the Services that violates the terms of service or acceptable use policies

19.1.13. False SLO breaches reported as a result of outages or errors of any measurement system.

19.1.14. Events subsequent to any Customer-initiated action in a Customer Equipment, including testing.

19.2. **SLO eligibility period**.

The eligibility period to measure Service Level Objectives is one (1) calendar month. When a Service has been used for less than 30 days in a calendar month, the SLA eligibility period is still 30 days, but any days prior or after to Customer's use of the Service will be deemed to have had 100% availability.

19.3. **SLO measurements**.

All measurements performed by Supplier serve as compelling evidence concerning the compliance of the any Service Level Objectives. Measurements performed by Supplier are therefore always leading and prevailing in the SLA.

19.4. **Service Downtime duration.**

Any Service Downtime produced as a result of a Service Incident will be measured from the earlier of:

(i) the time Supplier becomes aware of the Service Incident evidenced by Supplier's systems or logs or data, monitoring systems or applicable Incident report; or

(ii) Customer's notification to the Supplier of the Service Incident (Customer opens a Service Incident Ticket), provided that Supplier can confirm the Service Incident began when the Customer claims it did;

until the incident has been remediated and the Service Incident Ticket is closed.

Service Downtime duration will not include any time required to remedy any issues in the Customer Equipment resulting from the Service Incident

20. MAINTENANCE

20.1. **Planned Maintenance**.

20.1.1. Planned Maintenance is scheduled work performed by Supplier to ensure the integrity, supportability, security, performance or availability of any infrastructure that supports the Services. Planned Maintenance may temporarily interrupt the Service delivery.

20.1.2. The Supplier will notify by email to the Authorized Contacts of Customer any Planned Maintenance, with the advanced notice herewith:

Type of Scheduled Outage	Notice period	Length of scheduled Service Outage	Hours to carry out the Service Outage
Emergency	As soon as reasonably practical	As short as reasonably practical	Undetermined
Major scheduled Service Outages (more than 60 min)	10 Business Days	More than 60 min	1:00 A.M. to 5:00 A.M. (CET) Monday to Sunday
Minor scheduled Service Outages (less than 60 min) or Service Affecting Issues only	5 Business Days	Less than 60 min	1:00 A.M. to 5:00 A.M. (CET) Monday to Sunday
Low risk activities	No obligation	Undetermined	Undetermined

20.1.3. The Supplier will use reasonable endeavors to minimize the number of instances of Planned Maintenance and to limit any disruptive work into the range between 1:00 A.M. to 5:00 A.M. (CET) Monday to Sunday.

20.1.4. The Customer may object the planned date/time within 24 hours after receiving the announcement. The Supplier will take the objection into consideration, but has the right to still carry out the work on the planned date and time.

20.1.5. Supplier reserves the right to perform Emergency Maintenance as needed outside the Planned Maintenance window, in which case Supplier will make a reasonable effort to notify the Customer with a minimum of two (2) hours in advance, if feasible under the circumstances

21. CUSTOMER SUPPORT SERVICE

21.1. **Customer Support Service scope**.

Support Service is available to Customers to:

21.1.1. Report any Service Incident

21.1.2. Report any account or billing problem

21.1.3. Request Information

21.2. **Incident Reporting Procedure and Escalation Matrix:**

Supplier will notify the Customer the Service Incident reporting procedures and escalation matrix. Such matrix includes email addresses and telephone access numbers for operations and senior management points of contact, who are available and authorized to address and resolve performance issues and Service Incidents.

21.3. **Incident Log**:

Supplier will maintain a log of Service Incidents reported by the Customer. Upon request from the Customer, Supplier will furnish the Customer a copy of such Incident Log.

21.4. **Customer Support Service timeframe**.

Customer Support Service will be available according to the following table:

Support Service	Reporting Cover Period	Response and Restoration Cover Period
Service Incident Management - Incidents Priority 1	24/7/365	24/7/365
Service Incident Management - Incidents Priority 2	24/7/365	Office Hours
Service Incident Management - Incidents Priority 3 & 4	24/7/365	Office Hours
Account or billing problems or information request	Office Hours	Office Hours

21.5. **Customer Support Service contact**.

The Supplier provides reliable and secure Service Incident Management support by requiring that all Service Incident requests come only from Authorized Contacts of Customer. Customer shall provide an "Authorized Contact List" with the appointed individuals' identity and level of access, which will contain a minimum of one (1) primary Administrative/Billing Contact and one (1) Emergency Contact. The Authorized Contact List will include the name, email address and phone number for each Authorized Contact. The Emergency Contact will receive Emergency Maintenance or Service-related correspondence from Supplier. Customer is responsible for ensuring the Authorized Contact List is accurate and maintained.

The Customer shall ensure that Support Authorized Contacts are available during the Respond Cover Periods and Restoration Cover Periods. Customer acknowledges that if the Support Authorized Contacts are not available at all such times, Supplier may not be able to meet the applicable Response Time and Restoration Times stipulated in the SLA.

The Supplier reserves the right to delay response on Service Incidents requests by anyone other than an Authorized Contact.

21.6. **Support limitations.**

Supplier is not responsible for Customer's end-user support.

21.7. **Support language**.

Support service is available in English, Spanish and French

22. PRIORITY OF SERVICE INCIDENTS

22.1. The following Priority Levels are applied to Service Incidents:

Priority Level	Priority Level Definition	Priority Level Definition	Support Service Hours	Response Time SLO	Status Update	Restoration Time SLO
1	Service Outage	Total loss of Service	24/7/365	15 min	Every 1 Hour	*defined for each Service in the SLA*
2	Service Affecting Issue	Service not performing in accordance with the Service Level Objectives	Office Hours	1 hour during Office Hours	Every 2 Hours	*defined for each Service in the SLA*
3	Service Event	Service is partially unavailable but cause little effect on the Service performance	Office Hours	4 hours	Every 4 Hours	Next Business Day
4	Informational Event	Issue that not materially affect the Service	Office Hours	Next Business Day	No intermediate updates	3 Business Days

22.2. **Response Time** is defined as the duration between the moment a Service Incident is reported by the Customer (through the opening of a Service Incident Ticket) and the point at which the Supplier's technician acknowledges receipt of the report. Any communication exchanged between the Supplier and Customer regarding the request will be deemed a satisfactory response.

22.3. **Restoration Time** is defined as the span between the reporting of a Service Incident by the Customer (initiating the opening of a Service Incident Ticket) and the resolution of the issue, indicated by the closure of the Service Incident Ticket by the Supplier. Excluded from the calculation of Restoration Time are delays arising due to: (i) inaccessibility of the Customer to the Supplier; (ii) inaccuracies or incompleteness in the information provided by the Customer regarding the Service Incident; or (iii) the Supplier's inability to perform necessary work at, or gain access to an asset controlled by the Customer, if such access were required.

23. NOTIFICATION OF SERVICE INCIDENTS

23.1. **Service Incident prediagnosis**.

Before reporting a suspected Service Incident to Supplier, the Customer shall carry out such testing and investigations as may be necessary to ascertain and ensure that: (i) such Service Incident does not lie with or is primarily caused by the Customer Equipment and (ii) such Service Incident has not arisen as a result of any matter that is not Supplier's responsibility or is caused by an Excluded Event.

If the result of the Service Incident prediagnosis lead the Customer to the reasonable belief that the Service Incident lies within the Supplier Network or Supplier Equipment, Customer shall report the Incident to Customer Support Service by opening a Service Incident Ticket (available via Customer Portal, telephone or email);

23.2. **Service Incident reporting information**.

Customer shall provide all adequate information in the Service Incident Ticket to enable Supplier to diagnose and resolve. This information will include:

23.2.1. The name, telephone number and email address of the person reporting the Service Incident;

23.2.2. The physical location of the Service Incident and the Service affected;

23.2.3. The identification of the Service(s) assets or components the incident is being reported against, hardware reference, or similar identifiers; and

23.2.4. any other details that may be relevant to the diagnosis of the Service Incident (including symptoms, events or actions leading up to the incident, any tests already carried out, any environmental conditions that may be causing the Service Incident, etc.)

If the Supplier becomes aware of a Service Incident that affects any Services, the Supplier will inform and advise the affected Customers of the nature of the Service Incident within thirty (30) minutes of discovery, or as soon as is practicable given the circumstances.

23.3. **Service Incident Management process**.

Upon the initiation of a Service Incident Ticket by the Customer or upon the Supplier's awareness of the Service Incident, whichever occurs first

23.3.1. The Supplier will furnish the Customer with a unique reference number for the Service Incident Ticket.

23.3.2. The Supplier will diligently and responsibly investigate the cause of the Service Incident, keeping the Customer informed of any changes in the investigation/rectification status and actions taken. The Customer can track the progress of the incident through the Customer Portal.

23.3.3. If, after thorough investigations, the Supplier is unable to identify the cause of the Service Incident, the Customer is required to participate in a fault identification coordination meeting if requested by the Supplier. The Customer is expected to cooperate with the Supplier in resolving the issue at no additional cost.

23.3.4. If deemed necessary by the Supplier, the Customer must authorize the interruption of the Service to address Priority Level 2 Service Incidents. Failure to do so will result in the downgrade of the Service Incident to a Priority Level 3.

23.3.5. In cases where, after investigations, no Service Incident is identified, or the Supplier determines that the Service Incident is not related to the Supplier Network or is caused by an Excluded Event, the Supplier may, at its discretion, charge the Customer for reasonable expenses associated with the actions taken following the Service Incident Ticket.

23.3.6. The Supplier will notify the Customer upon believing that the Service Incident has been resolved. The Service Incident Ticket will be closed when

(i) The Customer confirms resolution within 24 hours of notification; or

(ii) The Supplier unsuccessfully attempts to contact the Customer, as agreed, and receives no response within 24 hours of the attempt

If the Customer objects to the resolution within 24 hours of notification, the Service Incident Ticket will remain open, and the Supplier will continue efforts to resolve the Service Incident.

23.3.7. Upon Customer request, the Supplier will provide a final report within five (5) Business Days of the Service Incident detailing the reason and remediated actions practiced.

24. SERVICE CREDITS

24.1. **Scope**.

If, at any point during the Service Term, the Service fails to meet the specified Service Level Objectives, the Supplier commits to issuing a Service Credit to the Customer as outlined in the Service Level Agreement.

Service Credits represent the exclusive and sole remedy available to the Customer for any failure in the performance of the Services

24.2. Service Credit Entitlement

24.2.1. Service Incidents must be promptly reported to the Supplier within seven (7) days of their occurrence to be considered eligible for Service Credit

24.2.2. Service Credits are not accumulative. In cases where multiple Service Level Objectives (SLOs) are breached due to the same incident, the Customer is entitled only to the highest applicable Service Credit amount

24.2.3. The maximum cumulative Service Credits that the Customer may qualify for in any given calendar month, along with all other refunds or guarantees, will not surpass 100% of the Monthly Recurring Charges (MRC) for the affected Services during that month.

24.2.4. Service Credits are solely based on Monthly Recurring Charges (MRCs) and do not extend to other fees, including but not limited to usage charges, energy consumption, third-party fees, taxes, or government-related charges.

24.2.5. The calculation of Service Credits is performed after deducting all applicable discounts and any special pricing arrangements agreed upon with the Customer.

24.2.6. Service Credits are granted to the Customer in alignment with the Service Level Agreement (SLA) only if the Customer is not in default, as defined in the applicable Master Services Agreement (MSA), during the period when the Service Incident occurred.

24.2.7. Service Incidents that occurred before a successful Service Credit claim cannot be utilized for any subsequent Service Credit claims

24.3. Service Credit request and payment

24.3.1. To initiate a Service Credit request, the Customer is required to formally notify the Supplier in writing within thirty (30) days from the point of becoming eligible for compensation. Failure to adhere to this notification period will result in the waiver of the Customer's entitlement to any compensation

24.3.2. Service Credit requests must be submitted using the Supplier's designated form, accessible on the website (http://afr-ix). The Customer will provide the reference numbers of all Service Incident Tickets linked to the request, along with relevant details facilitating the Supplier's evaluation.

24.3.3. Within seven (7) days following the request submission, the Supplier will assess and communicate the approved Service Credit amount to the Customer, excluding any Service Downtime not adequately accredited or arising from an Excluded Event.

24.3.4. The Supplier will disburse the applicable Service Credits in the invoice of the subsequent month following the approval of the Service Credit. The transfer of monetary resources to the Customer is only applicable upon Service Termination within a reasonable timeframe.

25. SERVICE LEVEL OBJECTIVES (SLO) FOR IP TRANSIT

25.1. **Service Incident scope**.

25.1.1. The Service Incident scopes is defined by the occurrence of the significant degradation or impairment of Service performance beyond the following acceptable thresholds:

	Condition	
Service Outage	(i)	Complete interruption of data transmission for a period > 60 seconds
Service Affecting Issue	(i)	Bandwidth < 50% of the CDR
Service Event	(i)	Bandwidth < 75% of the CDR

25.2. **Service Downtime calculation.**

25.2.1. Service Downtime is calculated as the aggregate number of whole minutes in the relevant calendar month during which:

	Monthly calculation	
Service Downtime	(i)	Periods of Service Outage > 15 consecutive minutes, and/or
	(ii)	Periods of Service Affecting Issue > 120 consecutive minutes

25.2.2. Service Downtime conditions and restrictions:

i. In Dual-Homed architectures, Service Outages or Service-Affecting Issues occurring at one Service Delivery Location are not considered if the committed traffic can be seamlessly handled by the other Service Delivery Location(s).

ii. Service Downtime resulting from incidents affecting the Access Line or issues caused by power failures, cooling system failures, or other environmental problems at the Customer Premises is excluded from the calculation

25.3. **SLO Restoration Time objective**:

25.3.1. The target Service Restoration Time is:

	Restoration Time objective
Service Outage	< 2 hours
Service Affecting Issue	< 8 hours
Service Event	Next Business Day

25.4. **SLO Fulfillment objective**.

25.4.1. The target Service Fulfillment when the Estimated RFS Date is not stipulated in the Service Order, is:

	Service Fulfillment objective
ON-NET Delivery	< Ten (10) Business Days
OFF-NET Delivery	Undetermined. Varies by project

25.5. **SLO Availability objective**

25.5.1. The target Service Availability is

Service Level Objective	Service Availability
IP Transit	Single-Homing (Europe, UK & US): 99.98% Dual-Homing (Europe, UK & US): 99.99% Single-Homing (rest): 99.60% Dual-Homing (rest): 99.90%
$$P = (T - U)/T \ x\ 100$$ Where: P = Service Availability (percentage) T = number of minutes in the relevant calendar month U = Service Downtime in the relevant calendar month.	

25.6. **SLO DDoS Mitigation objective**

25.6.1. The target DDoS Mitigation objective is:

	Service DDoS Mitigation objective
Detection The time taken to detect a DDoS attack once it begins.	< 60 seconds
Efficiency	> 95% of malicious traffic
Availability	> 99.99%

25.6.2. Conditions and restrictions:

i. The Service Level Objective (SLO) does not cover issues resulting from incorrect or improper configurations by the Customer, including but not limited to incorrect BGP announcements, routing configurations, or improper use of mitigation settings

ii. Any DDoS attack that exceeds the specified capacity or limits outlined in the SLA (e.g., bandwidth capacity, number of concurrent attacks) is excluded from coverage.

iii. Attacks targeting third-party services or infrastructure not directly under the control of the Customer or Supplier, which indirectly affect the service, are excluded

iv. The DDoS mitigation service is focused on volumetric attacks and does not extend to application-level attacks. Customers need to implement additional security measures for protection against such attacks

25.7. **SLO RTT and Packet Loss objective**

25.7.1. The target Round-Trip Time (RTT) and Packet Loss objectives are:

	Service objective
Round Trip Time between any pair of Supplier PoPs	According to RTT table
Monthly average Packet Loss rate	< 0.5%

i. RTT is measured as the average round-trip time between designated points within the Supplier Backbone Network. Thresholds vary based on geographical distances between measured end-points. Average RTT is measured as the average of fifteen (15) minute samples as taken throughout a calendar month

ii. Packet Loss rate is measured by averaging the packet loss percentage across all monitored paths between the Access Ports of Customer and the Supplier PoP. Measurements are taken using industry-standard tools and methodologies.

26. SERVICE CREDITS FOR IP TRANSIT.

26.1. **Entitlement**

26.1.1. The Customer is entitled to Service Credits for any failure to meet the Service Level Objectives (SLO), with the credits varying based on the contracted SLA option: Platinum or Gold.

26.1.2. Service Credits are formulated as per the NRC and/or MRC of the individual instances of Service Elements affected by the SLO compliance

SLO Compliance	RFS Date delay	Platinum	Gold
Fulfillment ON-NET Delivery	< 5 Business Days	15% of NRC	
	> 5 Business Days	25% of NRC	15% of NRC

SLO Compliance	Aggregated Monthly Service Downtime	Platinum	Gold
Availability Single-Home (UK,EU,US)	> 9 min but <= 60 min	10% of MRC	5% of MRC
	> 60 min but <= 120 min	30% of MRC	10% of MRC
	> 120 min but <= 360 min	50% of MRC	30% of MRC
	> 360 min	80% of MRC	50% of MRC
Availability Single-Home (rest world)	> 5 min but <= 30 min	10% of MRC	5% of MRC
	> 30 min but <= 60 min	30% of MRC	10% of MRC
	> 60 min but <= 120 min	50% of MRC	30% of MRC
	> 120 min	80% of MRC	50% of MRC
Availability Dual-Home (UK,EU,US)	> 180 min but <= 1 day	10% of MRC	5% of MRC
	> 1 day but <= 2 day	30% of MRC	10% of MRC
	> 2 day but <= 5 day	50% of MRC	30% of MRC
	> 5 day	80% of MRC	50% of MRC
Availability Dual-Home (rest world)	> 45 min but <= 5 hours	10% of MRC	5% of MRC
	> 5 hours but <= 10 hours	30% of MRC	10% of MRC
	> 10 hours but <= 1 day	50% of MRC	30% of MRC
	> 1 day	80% of MRC	50% of MRC

SLO Compliance	Monthly average RTT in excess	Platinum	Gold
Round Trip Time between Supplier PoPs	> 15%	10% of NRC	
	> 30%	25% of NRC	

SLO Compliance	Monthly average Packet Delivery rate	Platinum	Gold
Packet Loss rate	< 99.5% but > 99.0%	10% of NRC	
	< 99.0% but > 98.0%	20% of NRC	
	< 98.0%	40% of NRC	

SLO Compliance	Aggregated Monthly Service Downtime	Platinum	Gold
DDoS Mitigation Availability	> 5 min but <= 30 min	10% of NRC	10% of NRC
	> 30 min	25% of NRC	25% of NRC