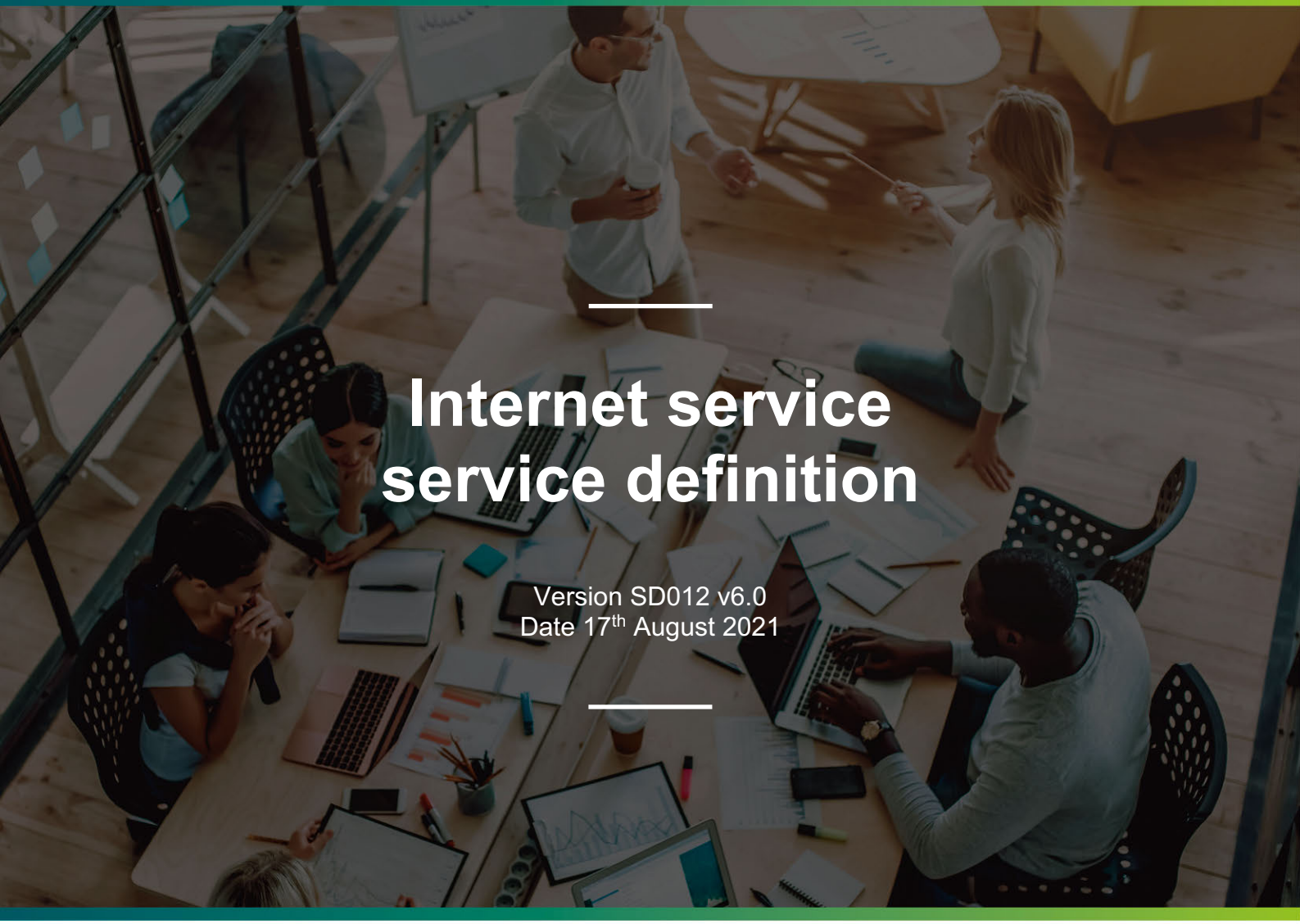

Internet service service definition

Version SD012 v6.0
Date 17th August 2021

redcentric

AGILE • AVAILABLE • ASSURED

1) Service Overview

1.1) Overview

Redcentric's Internet Service provides robust Internet connectivity to Customer sites using a variety of circuit options and to Customer environments within Redcentric data centres. Redcentric has fault-tolerant inter-connections with several Tier-1 transit providers at multiple sites across the UK. Several ancillary functions including domain name resolution and email store-and-forward are included in the service.

2) Service Description

2.1) Access Methods

Redcentric offers a variety of connectivity options to deliver the Internet Service to Customer sites, including Asymmetric Digital Subscriber Line (ADSL) and Ethernet. Please see the Service Definitions of the various connection options for details of available bandwidth, Service Levels etc.

The Internet Service is also available within Redcentric data centres. Customers subscribing to the Redcentric Colocation Service use data centre ports to access the Internet Service.

2.2) Secondary Email

The Redcentric Internet Service incorporates a secondary email server as a backup facility to the Customer's own Simple Mail Transfer Protocol (SMTP) email server. If the Customer's email server or network connection fails, incoming emails can be temporarily held on the Redcentric resilient secondary email server infrastructure. Stored mails will be sent to the Customer's email server when it is back online.

2.3) DNS Cache Servers

As part of the Internet Service, Redcentric provides highly available, resilient Domain Name Service (DNS) infrastructure to resolve Internet Protocol (IP) addresses for outgoing web, email and other requests from users of the Internet Service.

DNS cache servers do recursive queries to find the authoritative answer to an Internet DNS request made by a user and then cache the information for a finite set period or 'time to live'. Using DNS caching makes popular queries faster and reduces overall bandwidth usage.

2.4) Domain Name Registration and Hosting

Redcentric can manage domain name registration, renewal, transfer and release on behalf of the Customer.

In addition, Redcentric also provides the authoritative domain name resolution for any Customer domain names that are administered by Redcentric. A team is available to validate and implement Customer DNS change requests relieving the Customer of this often-understated business critical function.

Authoritative domain name resolution is a critical part of delivering web content and emails to end users. Domain name administration is a chargeable additional option, provided by Redcentric to enhance the Internet Service.

2.4.1) Registration

A domain name will be registered and established within 48 hours of placing an order if the correct information is provided.

2.4.2) Renewal

When registering the domain, Redcentric will mark the auto-renewal flag on the registrar's database. This means that under normal circumstances, after the registration period (ordinarily two years) elapses, the domain name will be automatically re-registered and Redcentric will charge the Customer for the renewal. 'Renewing by default' saves potentially serious disruption should a Customer forget to instruct Redcentric to renew the domain before it expires.

It is possible to opt out of auto-renewal; however, Redcentric urge Customers to consider the potential ramifications of domain name expiration before doing so. Customers who do not wish to renew should send instruction to Redcentric in writing at least six weeks prior to the end of the registration period.

If Redcentric has not received a written instruction to cancel auto-renewal, the registrar will renew the domain name and charge the Customer will be charged the amount published in the price-book for the renewal.

2.4.3) Transfer

Domain name hosting can either be transferred away from, or into Redcentric administration.

Redcentric service desk personnel are experts in the transfer process and will deal with the technical aspects of transfers. Redcentric will co-operate fully with requests to migrate a domain name into the administration of another registrant agent, and there is no cost associated with this process.

Please note that when administration of a domain is transferred to Redcentric from another registrant agent, a transfer charge applies.

2.5) Public IP Address Allocation

Redcentric is an Internet Registry partner of RIPE (Réseaux IP Européens) and has devolved authority for allocated IP address space. Redcentric also run a Border Gateway Protocol (BGP) routing Autonomous System (AS). For Internet connectivity, Redcentric assumes clients connecting to the Internet will use Network and Port Address Translation (NAT/PAT) to map internal RFC1918 private Internet addresses to a single public IPv4 Internet address. Customers requiring IPv4 provider aggregated (PA) IPv4 addresses are required to complete the RIPE IP address request form. Due to the well-publicised depletion of IPv4 addresses, Redcentric can allocate only the smallest prefix to meet immediate requirements. Subject to suitable design and when agreed by both parties in writing, Redcentric can route IPv4 provider independent (PI) address-space that has been allocated to the customer. Redcentric will also allocate PA IPv6 addresses following the same process, but allocation is not as restrictive.

2.6) Service Report

The Redcentric technical support desk personnel are available to respond to queries 24 hours a day, 365 days a year. Staff are trained to deal with Customer Internet Service queries, including those relating to mail relay, IP addressing, DNS resolution, etc.

2.7) Volumetric Denial of Service Attacks

In the context of Internet connectivity, a Denial of Service (DoS) attack occurs when an attacker sends traffic to a targeted organization with the intent of disrupting or making unavailable that organization's Internet connection, web or email servers, web-facing applications, IP telephony systems etc. Attack methods vary but the goal is usually to disrupt service, make resources unavailable or generate distraction for other nefarious purposes. Distributed Denial of Service (DDoS) attacks are generally characterised by the delivery of very large volumes of traffic to the targeted system. The greatly elevated traffic levels can overwhelm the network and/or infrastructure associated with the target system and make it inaccessible. In order to protect the majority of its customers, when Redcentric becomes aware that a Customer's system is being attacked, Redcentric staff implement changes that will stop all traffic entering the network destined for the targeted system(s). While this action is intended to protect the infrastructure as a whole, and therefore the majority of Customers, the targeted Customer will inevitably have service interruption. Customers hosting business critical, web facing applications and resources may wish to purchase Redcentric's DDOS Mitigation Service. This Service is based on an upstream filtering/scrubbing facility which aims to detect and discard malicious traffic and pass only legitimate traffic to the target system(s).

2.8) Delivery Timescales

Where new a new circuit is required, delivery timescale of the Internet Service is determined by the lead-time of the new access circuit. Please see the relevant Service Definition for details. Where the Internet Service is delivered to a data centre port or over an existing circuit to a Customer site with spare capacity, under normal circumstances, the Internet Service will be provisioned in 10 working days.

2.9) Exclusions

Unless specifically stated otherwise in this document, it should be assumed that no other ancillary services are included in the Internet Service including the provision of any of the following:

- web servers
- web storage space
- web software of any kind

- primary email servers
- web content filtering
- email checking
- perimeter firewall security
- denial of service attack remediation
- distributed denial of service mitigation

3) Implementation and Acceptance

3.1) Acceptance Criteria

The following Acceptance Criteria apply to the Internet Service:

- Communicate public IP address allocation to Customer (if provider independent address space is not to be used)
- Check the LAN connection to the CPE for speed and duplex mismatches and errors (where possible).
- Test IP connectivity by pinging devices on the web
- Test domain name resolution
- Test secondary email service if required

4) Service Levels and Service Credits

4.1) Service Levels

The Service Level applicable to the Internet Service is as follows:

Service Level: Availability **Measurement Period: Month**	
Service Level	Equal to the Availability Service Level of the access circuit or data centre port over which the Internet Service is delivered. Please see the appropriate Service Definition for details.

4.2) Exclusions from Availability

In calculating Availability, in addition to the exclusions listed in clause 6.7 of the General Terms the following shall be excluded:

- Unavailability due to malicious activity of any kind. E.g. a Denial of Service attack (DOS)

4.3) Floor Service Level

The Floor Service Level applicable to the Internet Service in respect of Availability is determined by the Availability Floor Service Level of the access circuit or data centre port over which the Internet Service is delivered. Please see the appropriate Service Definition for details.

4.4) Service Credits

The Service Credits applicable to the Internet Service shall be as specified in the Service Definition for the access circuit or data centre port over which the Internet Service is delivered, and shall be payable in addition to the Service Credits arising from the non-Availability of the circuit or port. Please see the appropriate Service Definition for details.

Example: Internet Service delivered over a Redcentric Data Centre port, and achieving 98% availability in the relevant Month. The Data Centre Port is covered by the Managed IP-VPN Core Service Definition. 98% Availability would lead to a Service Credit of 15% of the Monthly Charge for the Data Centre Port, as set out in the IP-VPN Core Service Definition; in addition, for the Internet Service delivered over that Data Centre port, an additional Service Credit would apply in respect of the Internet Service, being 15% of the monthly charge for the Internet Service.

5) Data Processing

5.1) Data processing scope

- Redcentric Internet Service delivers the transport of IP packets between Redcentric's Internet gateways and Customer locations.
- Redcentric Internet Service does not involve any storage or backing up of data.
- When requested by the Customer, the optional secondary email server function delivers temporary storage of emails on Redcentric systems when connectivity is interrupted.

5.2) Data Storage and Encryption

- Redcentric does not encrypt IP traffic destined for the Internet.
- Redcentric does not capture, inspect, analyse, store or share the customer's traffic/data under normal circumstances.
- Under certain circumstances, when managing a support ticket, Redcentric may capture, inspect, analyse and/or store a small sample of the customer's traffic in order to investigate and diagnose a very specific problem, e.g. to help resolve a problem relating to IP packet corruption. Such diagnosis would involve the examination of a small sample of IP packets.

5.3) Data Processing Decisions

- Redcentric does not make any data processing decisions in relation to the Internet Service. Any processing of data over Customer systems when using Redcentric Internet Service for transit is instigated, configured and managed by the Customer, including any decision to use encryption.
- Redcentric Support can be asked by the Customer to intervene in the event of an issue with the Redcentric Internet Service. In such a case Redcentric may make decisions that affect data processing, but such actions will only be undertaken at the request of and in conjunction with the Customer.

5.4) Sub-Processors

- Redcentric routes traffic between Customer locations and multiple upstream service providers (eg. Cogent, Level-3 and LINX etc.). Redcentric has no control of traffic that traverses the Internet with regard to integrity, confidentiality and/or reliability etc. Customers should take measures to protect data that is transmitted over this unsecure, public network.
- Redcentric's network, over which elements of the Internet Service is delivered, uses third party carriers (such as BT and Virgin Media Business) to provide connectivity.
- Redcentric works with various Internet Registrars to register and administer Internet Domain Names
- No other parties are involved in delivering the Redcentric Internet Service, and there are no sub-processors appointed by Redcentric.

5.5) Customer Access to Data

- The Customer control its own platforms which use Redcentric Internet Service to carry data, and the Customer therefore has full access to its own data.

5.6) Security Arrangements and Options

- The Redcentric Internet Service core is hosted at both Redcentric and third party locations. All locations meet physical security standard ISO27002 section 11.1 or equivalent.

HEAD OFFICE

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522
E sayhello@redcentricplc.com
W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED