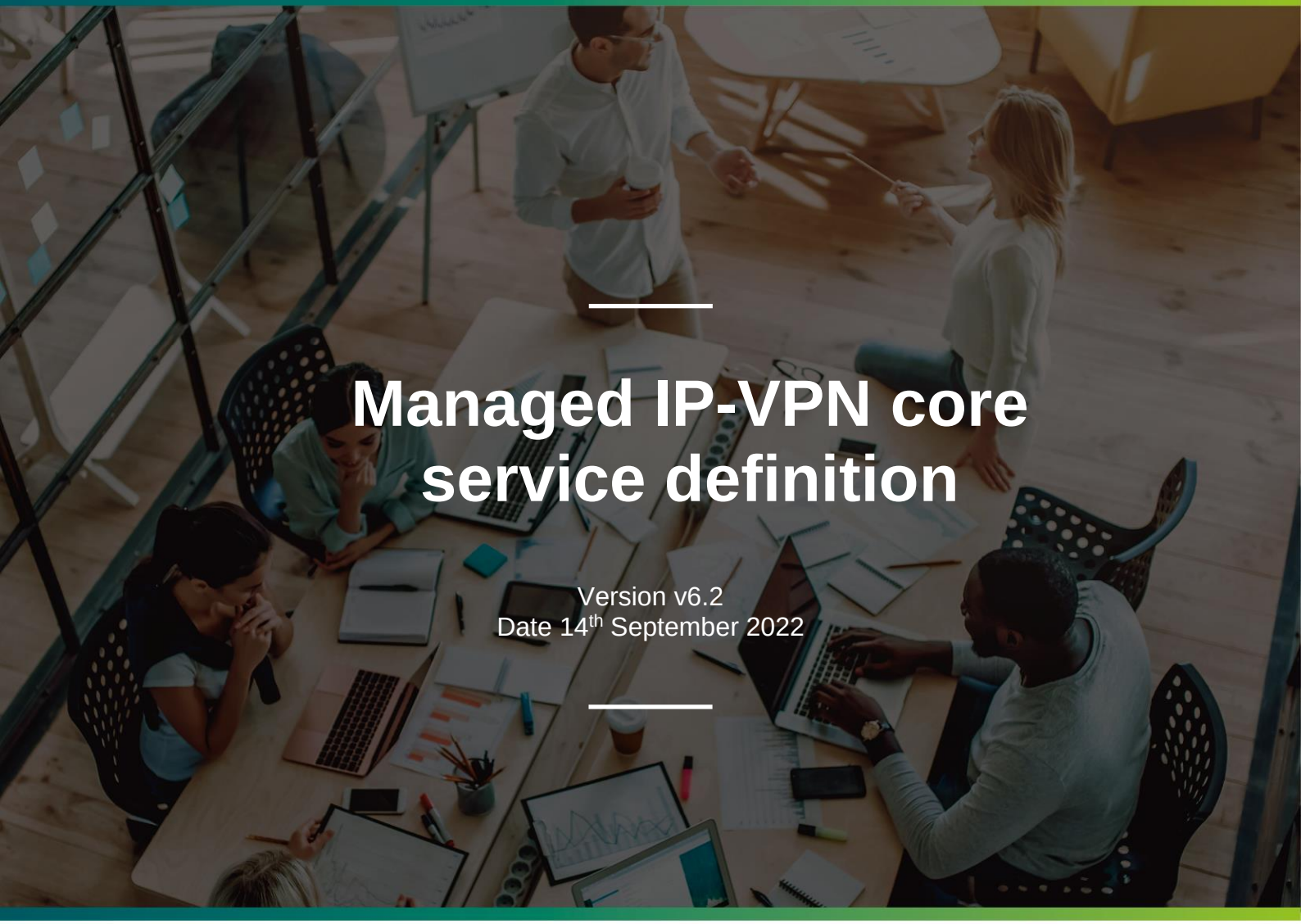

Managed IP-VPN core service definition

Version v6.2
Date 14th September 2022

redcentric

AGILE • AVAILABLE • ASSURED

1. Service Overview

1.1 Introduction

Managed IP-VPN is Redcentric's wide area network connectivity service.

Redcentric offers a suite of cost-effective, value-add voice and data services from within the core of the network. These include data centre co-location facilities, telephony services, data storage and virtual infrastructure solutions. The Managed IP-VPN Service can link individuals and sites, allowing users to access centralised services and access information and applications hosted at other company locations.

Customer sites can be connected to the Redcentric core using various access circuit connectivity options. The default Internet Protocol - Virtual Private Network (IP-VPN) service provides communication between devices (PCs, printers, and application servers etc.) at various Customer locations. Other service VPNs can also be delivered on the access circuits including Internet access and IP telephony.

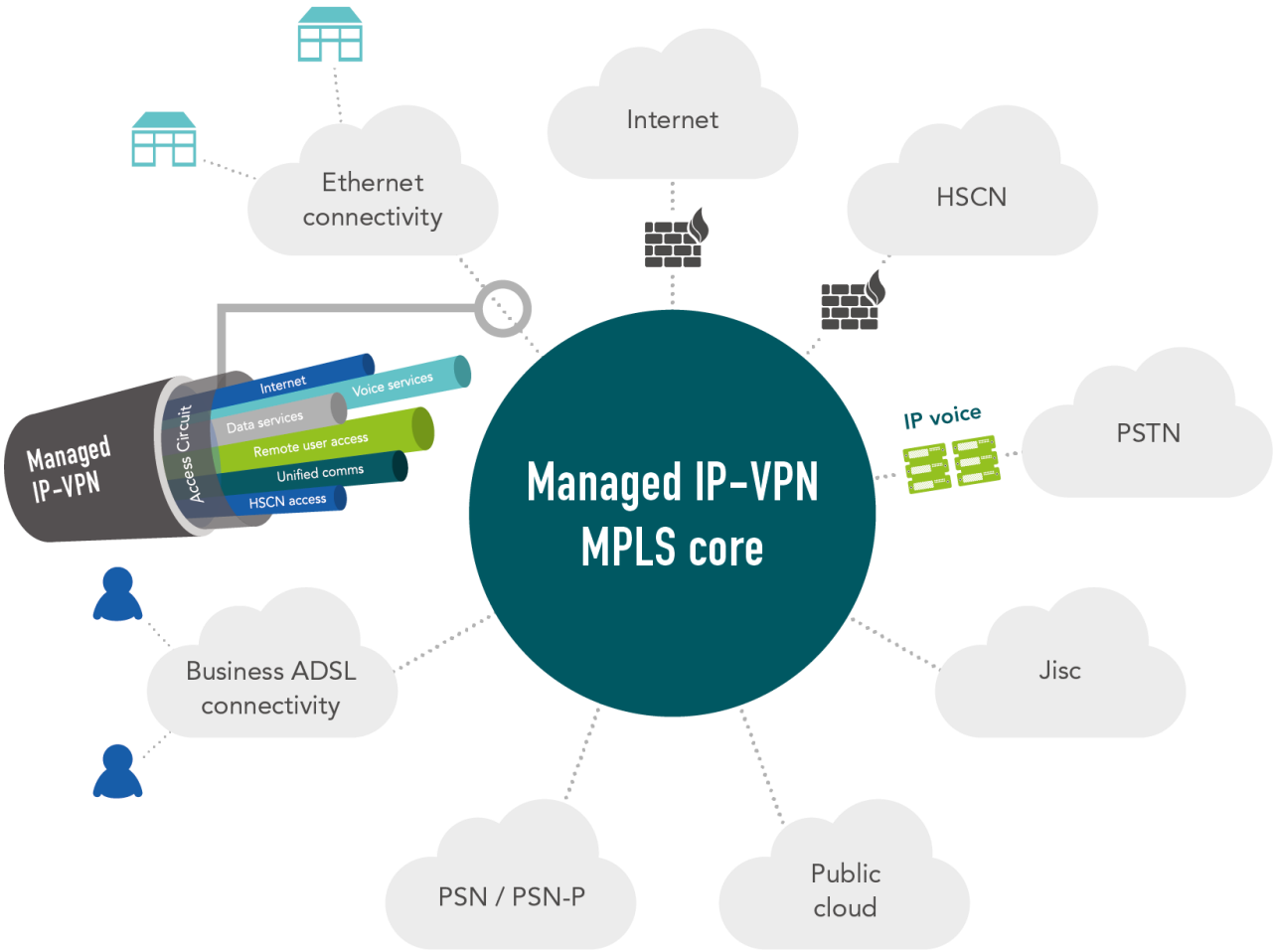

Diagram 1 – Redcentric core illustrating a range of connectivity options

1.2 Features

- Multiple circuit options - A choice of broadband, Ethernet and data-centre cross-connect circuits can be used on a mix-and-match basis to offer connectivity solutions to Customer sites with differing requirements. (Diagram 1)
- Multiple services - Each of the connectivity options can support multiple services (e.g. Internet, VPN etc.), which makes the Managed IP-VPN Service both flexible and scalable. (Diagram 2)
- Managed and Monitored – The network devices are monitored from Redcentric's network operations centre which operates 24 hours a day, 365 days a year.
- The Managed IP-VPN Service provides private, secure, IP connectivity between various company locations, data centres etc.
- Internet connectivity can be provided to one or more Customer company locations
- Redcentric is certified to connect qualifying Customers to several closed user groups networks including the NHS healthcare network and the JANET academic network
- The Online service portal gives Customers access to a variety of time-saving functions and also network performance reporting information

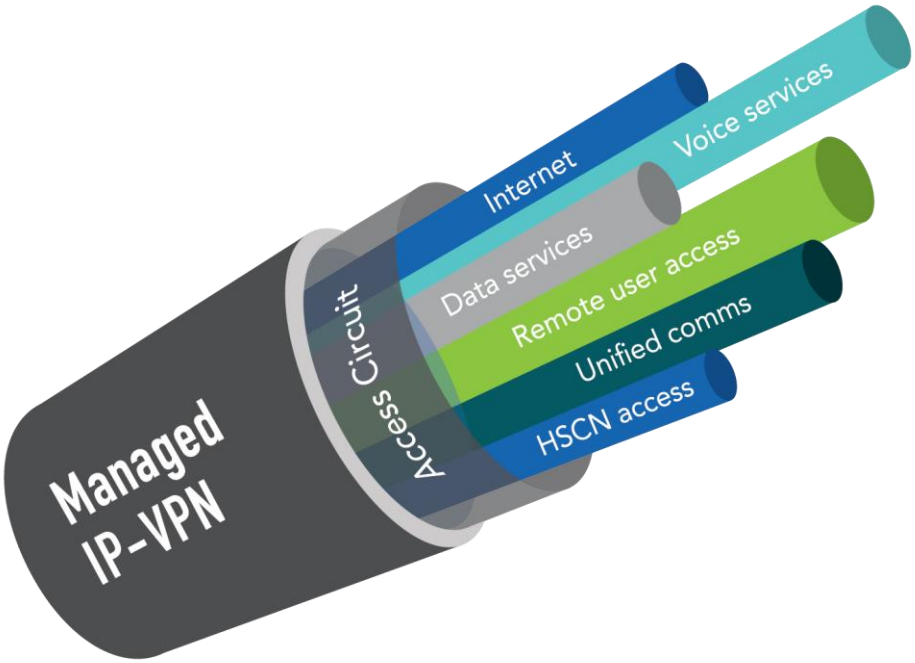

Diagram 2 – Representation of multiple services delivered over a Managed IP-VPN access circuit

2. Service description

2.1 Introduction

Redcentric offers various circuit options that connect Customer sites to the Redcentric core. The various circuit types can be considered for suitability according to several characteristics including cost, capacity, scalability, geographic availability, delivery timescales, Service Levels and so on. The details of each option can be found in their respective Service Definitions, which are available separately and must be read in conjunction with this document.

2.2 Access circuit options

Access circuit options are listed and detailed briefly below:

- Ethernet - An Ethernet circuit connects the Customer's site either directly to a Redcentric Point of Presence (POP) or to a Redcentric POP via a 3rd party IP network.
- Broadband – This typically asymmetric service makes use of low-cost broadband lines. Customer traffic goes over the lines to the nearest telephone exchange and is then switched across a shared infrastructure to Redcentric's core. The shared infrastructure is connected to the Redcentric core at several locations to offer increased availability.
- Mobile cellular - Provides low bandwidth primary and backup connections. This option utilises the mobile operators' network and either a private link to the Redcentric core or a secured tunnel over Internet connectivity provided by the cellular connectivity suppler.
- Data centre ports - this option provides connectivity into a Customer's rack or suite within a Redcentric data centre

Circuit types can be combined to offer a comprehensive single network solution meeting complex communication requirements.

2.3 Customer premises equipment

Customer Premises Equipment (CPE) refers to any device located on the Customer site that is used to deliver a fully managed, converged IT and communications solution.

CPE is provided with all Managed IP-VPN Service options with the exception of unmanaged broadband and connectivity to some 3rd-party cloud service providers (CSP), e.g., Microsoft Azure, Amazon Web Services and Google Cloud Platform.

To identify failures promptly, CPE is polled periodically so that Redcentric can automatically identify and begin to address any problems that arise.

The CPE serves as the service demarcation point for the Managed IP-VPN Service, and as such is designed to provide a straightforward means of delivering multiple services (e.g., a combination of Internet, Private VPN and IP telephony, etc.) to a single site. For sites with more than one circuit, where the objective is to increase bandwidth delivery, the circuits are bonded and are delivered to a single CPE device. Where multiple circuits are delivered to a site to offer enhanced resilience, it is standard practice to have a separate piece of CPE terminating each circuit.

CPE specification is largely determined by the type of circuit(s) it will be used to terminate. More details can be found in the various access circuit Service Definitions.

If Redcentric determines that a piece of CPE has developed a fault, Redcentric will arrange to have it replaced. Specific details can be found in the various Circuit Service Definitions, but the standard service offers 'next business day' CPE replacement in most instances. Customers can choose an expedited CPE replacement option, which offers a target hardware replacement timeframe of 4 hours from the point that Redcentric determines a replacement is required. This timeframe is not practical for certain remote UK locations; Redcentric will notify the Customer of alternative target timeframes for these locations. Naturally, expedited CPE replacement will not improve repair times for faults caused by anything other than faulty CPE hardware. The expedited CPE replacement option is charged monthly in advance and is applicable regardless of the number of times it is called upon.

If the firmware or hardware version of your CPE is forecast to become End of Support (EoS) / End of Life (EoL) during an initial contract term or a renewal of that contract term, Redcentric will no longer be able to provide security or critical firmware updates for that EoS or EoL CPE.

In order to continue to receive security and critical updates, a hardware refresh of the CPE will be required. Any hardware refresh, including the provision of new CPE, is outside the scope of this Service and will be chargeable. New CPE would need to be provided by Redcentric for an additional charge.

The Managed IP-VPN Service includes monitoring and reporting; however, Redcentric will configure CPE for read-only Simple Network Management Protocol (SNMP) access so that Customers can use their own monitoring terminals if required. SNMP read-only access incurs an additional charge.

2.4 Improved resilience

Redcentric recommends the provision of multiple circuits to sites that require enhanced resilience and availability. If the primary circuit or CPE fails, Customer data traffic will be routed over the back-up circuit instead. Most commonly, Redcentric uses a layer 3 routing protocol to automatically route traffic down the back-up link.

For most circuit combinations, an outage of around five minutes may be experienced as the network detects failure and routes traffic via the alternative connection. For certain circuit combinations and CPE configurations, this can be as low as 30 seconds. Please see the various access circuit Service Definitions for details.

2.5 Services delivered

Redcentric can deliver one or more bandwidth services over each access circuit as the basis of a converged Wide Area Network (WAN). The number of services supported, and the available bandwidth of each service varies for the different access circuit options. The available bandwidth services are detailed below:

- Private VPN - This provides connectivity between a Customer's locations allowing, for example, users in one location to access applications hosted at another. VPN traffic is private and moves only within Redcentric's managed network. Redcentric can deliver multiple private VPNs on a single circuit if required.
- Real-time bandwidth - This is essentially the same as a private VPN but traffic is given priority over other services and is suited to real-time applications like telephony and interactive video.
- Internet - Internet bandwidth allows users across the Internet to access the company's web-facing resources (eg. email servers and web servers). It can also be used to allow staff to access resources on the Internet (eg. external websites). Please see the Redcentric Internet Service Definition for more details.
- N3/HSCN - N3/HSCN is essentially a private VPN for a closed user group. Only Customers with the appropriate level of approval can connect to this government healthcare network. Please see the Redcentric N3/HSCN Service Definition for more details.

In most cases, each service is delivered on a separate port on the CPE. For example, the Redcentric Internet Service might be delivered to one port, the corporate private VPN to another and the Redcentric IP telephony Unity Service to a third. (Diagram 3)

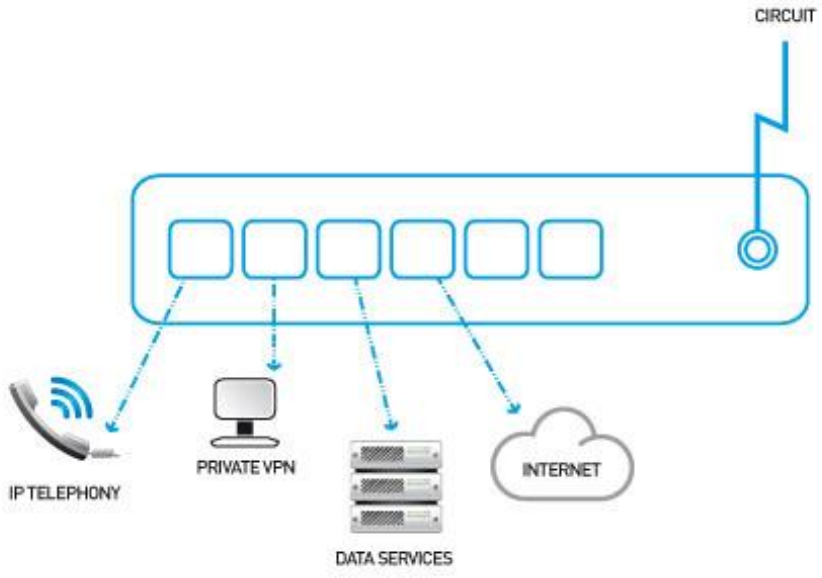

Diagram 3 – CPE showing various services delivered to separate ports

If the Redcentric CPE has seemingly spare or unused interfaces, they cannot be used to provide connectivity to end-user devices. In almost all circumstances, the Customer will need to provide a Local Area Network (LAN) switch on Customer sites to facilitate connectivity of end-user devices. Redcentric offers separately a Managed LAN Service; please see the relevant Service Definition for details.

In certain circumstances, Redcentric can provide several (or all) bandwidth services on a single port that is configured as an Ethernet 802.1Q trunk.

Please note that a requirement for several (or all) services to be delivered on a single port must be agreed in writing in advance of contract signature.

2.6 Service interface

For all circuit options except unmanaged broadband and 3rd-party Cloud Service Provider connections, the Ethernet LAN port interface(s) on the CPE represent(s) the Service demarcation point. The Service demarcation point for the unmanaged Broadband Service is the master telephone socket. The Service demarcation point for 3rd-party CSP connections is the wire connection into the 3rd-party CSP's interface.

2.7 IP addressing and routing

Details of IP addressing schemes for the various services are provided below:

Service	IP address ranges provided and managed by:	Private / public
Corporate private VPN	Customer	Either but Customers usually use RFC1918
Customer telephony VPN	Customer	Either but Customers usually use RFC1918
Redcentric IP telephony (Unity)	Redcentric	Private RFC1918 space
Internet	Redcentric	Public

Software in the CPE (excluding CPE on broadband links) makes it possible for different services to share the same IP address space if necessary. For example, a Customer could have both a production VPN and a

test/development VPN, each delivered to the same sites over the same circuits. These would terminate on the same CPE using identical IP address space without issues.

Redcentric uses a variety of routing protocols between CPE and the core network to provide the Managed IP-VPN Service. Redcentric uses static routing on the CPE to point to non-directly connected subnets on the Customer's LAN. Any requirement to run a dynamic routing protocol with devices on the Customer's LAN must be agreed prior to contract signature. Cisco System's proprietary Hot Standby Routing Protocol (HSRP) and occasionally the standards based Virtual Router Redundancy Protocol (VRRP) are offered to provide a single gateway address when multiple Redcentric circuits / routers are deployed on a site.

2.8 Exclusions

The following limitations and exclusions apply to Managed IP-VPN:

- Managed IP-VPN Service does not include encapsulation of non-IP packets
- Managed IP-VPN Service does not currently support IPv6
- Traffic filtering is not supported
- No firewall features or functions are offered as part of the service. Redcentric offers, separately, a Managed Firewall Service. Please see the relevant Service Definition for details
- Network Address Translation (NAT) will not be supported without prior written agreement

2.9 Quality of service

Redcentric applies Quality of Service (QoS) configuration as necessary, to support some of its bandwidth services.

The various Redcentric access options (e.g., broadband, Ethernet and data-centre cross-connects) have different QoS capabilities, largely determined by the underlying infrastructure. Details of these are included in the respective Service Definitions and should be read in conjunction with this document.

Traffic requires end-to-end QoS support. That means that any traffic moving between two locations effectively has the QoS capability equal to the lower of the links. For instance, traffic travelling from a broadband connected site to an Ethernet connected site, and vice versa, will have the end-to-end QoS capability of the broadband line.

When required, Redcentric technical consultants will work with a Customer to gather QoS requirements, then design and document a policy that will be implemented on the Redcentric network devices.

QoS performance reporting is available for certain CPE; please see section 2.13 below.

2.10 Provisioning timescales

The various circuit options have different delivery lead times, typically ranging between 10 and 75 days depending on the availability of existing infrastructure at a particular site. Redcentric will provide details of estimated delivery timescales on request.

2.11 Support

The Managed IP-VPN Service is underpinned by a comprehensive support, monitoring and management package, which includes 24/365 monitoring of all hardware, software and network elements by staff in the UK Network Operation Centre (NOC). These include:

- Event reporting and analysis
- Response to systems alerts
- Customer notification of systems alerts

Under normal circumstances, for monitored and managed connectivity options, the Redcentric systems poll the CPE every 5 minutes to confirm that the circuit and CPE are available. This is in line with industry standard network management best practices. If the CPE does not respond to several successive polls, an automatic alert

is forwarded to the Redcentric network fault management system. This automatically raises an incident, which is placed in the technical support queue. Technical support engineers investigate these incidents 24 hours a day, 365 days a year.

Customers can become aware of network problems in the short window before the polling procedures verify a problem and issue an alert. Redcentric provides additional means for Customers to raise faults, i.e. via telephone, email and the web portal. Experience shows that fault resolution times are largely independent of the fault identification and reporting method.

Redcentric classifies problems according to severity. This allows the prioritisation of resource on issues that have the most impact on Customers' businesses. Further details of the classifications can be found in Redcentric's Customer Welcome Pack which is available on request.

Redcentric is committed to continually improving and expanding its core network, and to facilitate these improvements, it is necessary to carry out essential work from time to time. In accordance with Information Technology Infrastructure Library (ITIL) service management standards, these activities are carefully scheduled using an internal change control process; this gives Customers maximum visibility of any given change and thereby ensures that planning and implementation is carried out to minimise the effect on Customers using Redcentric network services.

Maintenance windows and procedures for communicating emergency outages are detailed in the Customer Welcome Pack.

2.12 Redcentric Inform portal

One of the major features of the Managed IP-VPN Service is an online portal that provides easy access to performance and usage information. The portal gives access to:

- Customer self-service - Management of contact database for planned and emergency works, fault logging etc.
- View of the current status of open tickets - This gives Customers the ability to log new calls and update existing issue statuses
- Storage utilisation and trending information - This enables accurate gauging of usage-to-capacity ratio and traffic patterns
- Online access to billing data
- Access to project management team, plus latest status and date information - This lets Customers see how a service delivery project is progressing
- Enterprise class reporting and management suite - Info Vista is an enterprise class reporting system which can provide detailed information on network and data services. Please see section 2.13 on Monitoring and Reporting.

All products and tools used by Redcentric are regularly reviewed and Redcentric reserves the right to change systems and applications without prior notice.

2.13 Monitoring and reporting

The Redcentric system periodically polls CPE for information using SNMP. Assuming standards compliant SNMP Management Information Base (MIB) structures are available for the model of CPE chosen, both system-wide and Interface specific statistics can be presented including:

- Network information on availability, performance and utilisation as measured over selectable periods of time
- Near real-time information – useful for diagnostics
- QoS performance reporting where QoS is deployed
- One-off and scheduled reports covering services/devices/sites with the ability to summarise

For most models of Cisco and Huawei CPE, the following system-wide information is presented:

- Device availability
- CPU utilisation
- Memory usage

- Poll latency

And for WAN, and LAN interfaces delivering a Service Bandwidth on Cisco and Huawei CPE, the following information is presented:

- Interface availability
- Interface contracted bandwidth
- Interface utilisation
- For certain rate adaptive broadband services, the synchronisation rate of the line

Unless specific details are provided in the Statement of Work to the contrary, for other CPE (where MIB information is unavailable, incomplete, or is malformed), it should be assumed that only device availability will be available.

Additionally Enhanced Service Monitoring may be available in certain circumstances in conjunction with some models of CPE. For example, it may be possible to set a threshold and perform actions when the threshold is met (e.g. Reset the broadband line if there is a significant reduction in sync. speed). Specific deliverables must be detailed in the Statement of Work. Enhanced Service Monitoring incurs an additional Service Charge.

2.14 Connections to 3rd-party cloud service providers

Redcentric can provide connectivity to several of the major 3rd-party Cloud Service Providers including Microsoft Azure and Amazon Web Services. The Customer generally contracts directly with the CSP for services – including the private connectivity port(s). The Customer contracts with Redcentric to extend their WAN into the CSP environment. In most CSP implementations, Redcentric is unable to deploy CPE. The functions traditionally associated with CPE, i.e., traffic routing across primary/back-up links, QOS, and availability monitoring point become part of the CSP's offering. In most cases, the Customer exclusively administers their own CSP environment and consequently, the Customer is required to configure and support these CPE functions with guidance from Redcentric. Please see the Service Level section for details of the implications associated with this.

3. Implementation and acceptance

3.1 Acceptance criteria

The following are the Acceptance Criteria applicable to the Managed IP-VPN Service:

- Confirm Redcentric Support contact details have been supplied
- Confirm logon credentials have been supplied for the Inform portal
- Customer confirms access to Inform Portal
- For DC ports:
  - Check LAN connection to CPE for speed and duplex mismatches and also errors (where possible).
  - Test IP connectivity by pinging devices on remote sites (VPN service) and/or a known web address (Internet)
  - Failover testing where resilient solution is offered

4. Service levels and service credits

4.1 Service levels

The service level applicable to the managed IP-VPN service is as follows:

Service Level: Availability **Measurement Period: Month**	
Service Level for core network	Not less than 99.95%
Service Level for data centre ports	Not less than 99.95%
Service Level for connectivity to Microsoft	Not less than 99.9%
Service Level for resilient connectivity to AmazonWS	Not less than 99.9%
Service Level for non-resilient connectivity to AmazonWS	Not less than 99.8%

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:

- In the case of CSP connectivity, failure of any element not supplied by Redcentric which prevents Redcentric from measuring Availability
- In the case of CSP connectivity, any impact caused in-whole or in-part by actions of the Customer; for example misconfiguration of CPE functions in their environment

4.3 Floor service level

The Floor Service Level applicable to the Managed IP-VPN Service in respect of Availability shall be 85% in any given Month.

4.4 Service credits

The Service Credits applicable to the Managed IP-VPN Service shall be calculated as follows:

In the following table:

“≥” means “greater than or equal to”

< means “less than”

“MS” means the total Charges payable in respect of the Managed IP-VPN Service for the same Month

Applicable Managed IP-VPN Service	Service Availability	Service Credit
Core Network DC Port	≥99.95%	none
	≥99.0% but <99.95%	5% of MS
	≥96.5% but <99.0%	15% of MS
	<96.5%	20% of MS
Connectivity to Microsoft Resilient connectivity to Amazon Web Services	≥99.9%	none
	≥99.0% but <99.9%	5% of MS
	≥96.0% but <99.0%	15% of MS
	<96.0%	20% of MS
Non-resilient connectivity to Amazon Web Services	≥99.8%	none
	≥99.0% but <99.8%	5% of MS
	≥95.0% but <99.0%	15% of MS
	<95.0%	20% of MS

5. Data processing

5.1 Data processing scope

- Managed IP-VPN delivers the transport of IP packets between locations.
- Managed IP-VPN does not involve any storage or backing up of data.

5.2 Data storage and encryption

- Redcentric does not encrypt IP-VPN inter-site traffic, nor traffic destined for external networks.
- 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 Managed IP-VPN Service. Any processing of data over Customer systems when using Managed IP-VPN 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 Managed IP-VPN 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

- The Managed IP-VPN Service supports the connectivity needs of the Customer to third parties. Products and services of third parties are contracted to the Customer, and not to Redcentric unless stated to the contrary in an Order.
- Redcentric's network over which elements of the Managed IP-VPN Service is delivered uses third party carriers (such as BT and Virgin Media Business) to provide connectivity. These third parties are conduits only for data, and have no involvement in the processing or storing of data transmitted over Managed IP-VPN.
- No other parties are involved in delivering the Managed IP-VPN Service, and there are no sub-processors appointed by Redcentric.

5.5 Customer Access to Data

- The Customer controls its own platforms which use Managed IP-VPN to carry data, and the Customer therefore has full access to its own data.

5.6 Security Arrangements and Options

- The Managed IP-VPN 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