

Colt IP VPN Service Guide

Note: This document is not legally binding.

Contents

1	Overview.....	5
2	Benefits.....	5
2.1	Extensive network reach	5
2.2	Reliability.....	6
2.3	Range of cost-effective connection options	6
2.4	Prioritised traffic	6
2.5	Quality and service guaranteed.....	6
2.6	Outstanding customer service	6
3	Description.....	7
3.1	IP VPN Plus	7
3.2	IP VPN Access.....	8
3.3	IP VPN Mobility	8
3.3.1	Encryption options.....	8
3.3.2	Public Internet access options.....	10
3.3.3	User Bundles	10
3.3.4	Authentication options.....	11
3.4	IP VPN Remote Fixed Access.....	12
3.5	Colt's network coverage	13
3.6	Network access.....	14
3.6.1	Colt access types.....	15
3.6.2	Partner access types.....	16
3.7	Bandwidth options.....	17
3.8	Technical attributes	18
3.8.1	IP layer and routing protocols.....	18
3.8.2	IP addressing	20
3.8.3	Interface options	20
3.8.4	Latency	21

3.8.5	Packet loss ratio.....	21
3.8.6	Jitter.....	21
4	Features.....	21
4.1	Enhanced resilience.....	22
4.1.1	Dual access – primary and backup.....	22
4.1.2	Dual access - load balancing.....	23
4.1.3	ISDN backup.....	23
4.1.4	DSL backup.....	24
4.1.5	Backup over the public Internet.....	24
4.1.6	Backup over 3G public Internet.....	25
4.2	Multiple Ethernet Interface.....	27
4.3	Multicast.....	27
4.4	Integrated Internet Access (IIA) CPE-based.....	28
4.4.1	Single Ethernet interface.....	28
4.4.2	Dual Ethernet interface.....	28
4.5	Integrated Internet Access network-based.....	29
4.6	Hybrid MPLS and Ethernet networking.....	29
4.7	CoS.....	30
4.8	SNMP read-only access.....	31
4.9	IP Sec over IP VPN Plus.....	31
4.10	Dynamic Host Configuration Protocol (DHCP).....	31
4.11	Multi VPN.....	32
4.12	Hybrid Networking.....	32
4.13	Performance Reporting.....	34
4.13.1	Silver.....	34
4.13.2	Gold.....	35
4.14	Application Aware VPN.....	37
5	Coverage.....	39
6	Security.....	40
7	Service delivery.....	40

7.1	New service order	40
7.2	Modifying an existing service.....	40
7.3	Out-of-hours changes	41
7.4	Cessation or cancellation of service	41
7.5	Demarcation point	42
8	Service assurance	42
8.1	Customer service	42
8.2	Service Level Agreement	42
8.3	Colt Online	43
8.4	Service monitoring	43
8.5	Planned maintenance	43
9	Commercials.....	44
9.1	Contract period	44
9.2	Billing	44
9.3	Installation charges	44
9.4	Rental charges.....	44
10	Colt Professional Services	44
11	Glossary.....	45
12	Certifications and industry standards.....	45
Appendix A	Colt Online.....	46
Appendix B	Service delivery timeframes.....	48
Appendix C	Order to delivery overview	49

1 Overview

Colt IP VPN is an IP-based virtual private network (VPN) service that provides customers with the security expected of a private network, while at the same time offering significant benefits of a shared network in terms of cost and optimal connectivity.

Any-to-any connectivity of sites, regardless of their sizes, into a customer's network can be achieved easily, efficiently and securely, whether these sites are located within a single country or at diverse locations around the world.

Class of Service (CoS) options ensure that customer traffic can be prioritised so that data streams with stringent requirements such as voice and video take precedence. In addition, remote access options give customers the flexibility to connect staff members who are on the move or working from home.

With Colt's IP VPN, other than the remote access options that are delivered using secure tunnels over the public Internet, all sites are connected using a private network and do not traverse the public Internet.

Colt's ability to provide end-to-end managed networks ensures that we can offer customers a high quality, cost-effective solution backed by comprehensive service level agreements (SLAs) and award-winning customer service.

2 Benefits

IP VPN offers customers extensive coverage, reliability, CoS and traffic prioritisation and a wealth of flexible and cost-effective service options.

Benefits include:

- [Extensive network reach](#)
- [Reliability](#)
- [Range of cost-effective connection options](#)
- [Prioritised traffic](#)
- [Quality and service guaranteed](#)
- [Outstanding customer service](#)

2.1 Extensive network reach

With one of the largest European fibre and DSL networks, Colt can deliver IP VPN

directly to customer premises in all of the major European cities and to locations around the world through partnership agreements. In many cases, customer service will be delivered end-to-end over our own network, ensuring the highest quality and availability at all times.

The Colt IP VPN backbone network is highly resilient and offers very high availability. The availability targets and guarantees offered for each access type are detailed in the IP VPN SLA.

See [Coverage](#) for more information.

2.2 Reliability

With a target availability of 99.95% for sites that are directly connected with Colt Fibre, the service is extremely reliable. Enhanced resilience options enable customers to further ensure that VPN traffic is not interrupted and to increase the service availability up to 99.99%.

2.3 Range of cost-effective connection options

Colt offers a wide range of flexible and cost-effective connectivity options so that customers seamlessly connect headquarters and branch sites as well as remote sites and mobile workers to the same IP VPN. By converging voice and data traffic onto a single network, operating costs associated with running two separate networks are reduced.

2.4 Prioritised traffic

Five CoS levels give customers the ability to prioritise business-critical or time-sensitive traffic such as voice over IP (VoIP) or Enterprise Resource Planning (ERP) traffic.

2.5 Quality and service guaranteed

Colt offers an industry-leading SLA with the IP VPN service covering service delivery, service availability and fault resolution. We are confident of the quality and reliability of our service and offer compensation if our service targets are not met.

See [Service assurance](#) for more information.

2.6 Outstanding customer service

With Colt's best-in-industry customer service, customers can be assured that their Colt IP VPN service will be delivered on time. The customer network will be

managed proactively and repaired rapidly should any faults occur. Our customer care centres provide support 24 hours a day, seven days a week.

See [Customer service](#) for more information.

3 Description

Two different access options are available for any site:

- Fixed access options provide direct connections to customer premises and provide customers with dedicated bandwidth and high quality of service. The IP VPN services based on a fixed access include:
 - [IP VPN Plus](#)
 - [IP VPN Access](#)
- Remote access options enable secure access to a customer's VPN over the public Internet. This has the advantage of giving a customer's staff mobility and flexibility using the ubiquity of the Internet; however, the use of this shared medium means that quality of service and performance cannot be guaranteed end to end. The IP VPN services based on a remote access include:
 - [IP VPN Mobility](#) (enhancement of the former IP VPN Remote User option)
 - [IP VPN Remote Fixed](#)

More detail on these services can be found in the following sections.

3.1 IP VPN Plus

IP VPN Plus supports the greatest combination of service features while presenting a standard Ethernet interface on the local area network (LAN) port of the Colt managed CPE router.

This service is based on Multi Protocol Label Switching (MPLS) and offers the best solution if customers require full mesh any-to-any connectivity, but customers can also use it for partial mesh or star network topologies. A Colt managed CPE router at the customer premises is always included with the service.

With MPLS, customers benefit from traffic separation, a high level of security, quality of service (QoS) and scalability. This gives customers the flexibility to optimise the design of their wide area network (WAN) in terms of cost effectiveness and to support new applications that require full mesh connectivity and are time-critical.

3.2 IP VPN Access

IP VPN Access is delivered on the access circuit (wires only). This service is also MPLS-based, and so again, IP VPN Access is a good solution for full mesh any-to-any connectivity or, if required, partial mesh or star network topologies. As a Colt managed CPE router is **not** included at the customer premises, this option is best suited to those customers who have the internal skills to manage their own network.

As an option on top of IP VPN Access, Colt can provide a Colt unmanaged CPE router (Colt CPE Solutions) and provide the on-site install and CPE router hardware maintenance, while the customer is responsible for the configuration and monitoring of the CPE router.

The following figure provides a schematic overview of the different service options.

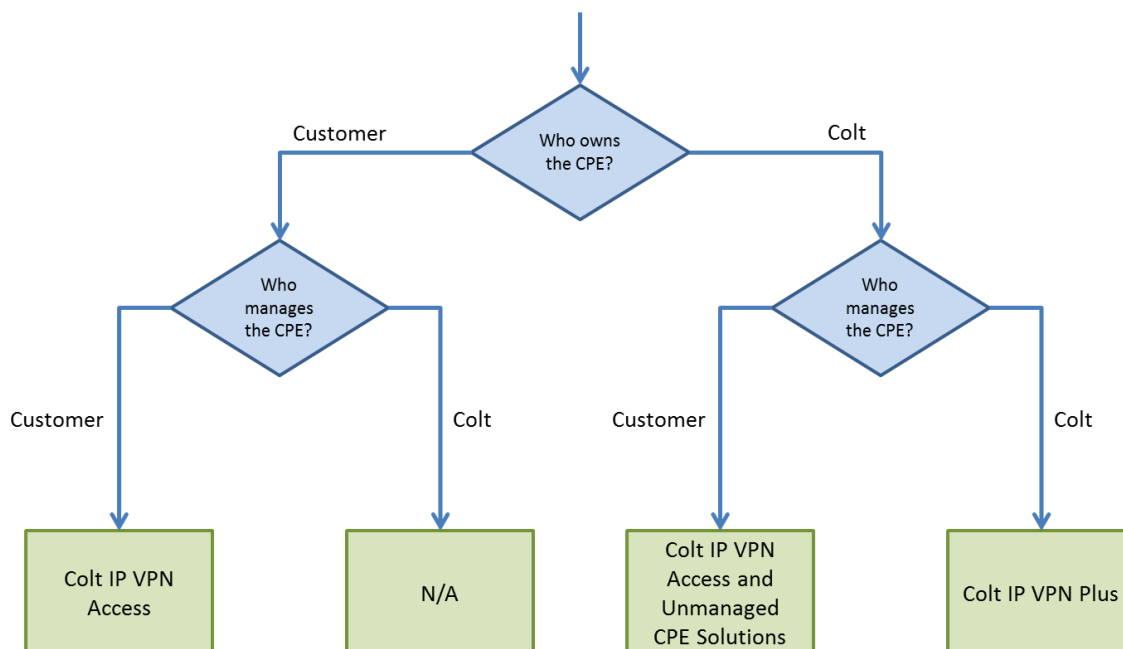


Figure 1: IP VPN structure

3.3 IP VPN Mobility

IP VPN Mobility enables staff members (the end-users) to access the customer's IP VPN in a secured way over the public Internet. IP VPN Mobility can be configured in various ways and the main options are described below.

3.3.1 Encryption options

All data sent over the public Internet is encrypted. IPVPN Mobility can be configured

with one of the following data transport encryption methods:

- **IPsec (Internet Protocol Security).** IPsec provides data encryption over the public Internet between the end-user laptop and the IPVPN router at the hub site. A VPN software client for the end-user laptop is provided to set up, maintain and terminate the secured tunnel. The VPN software client is simple to deploy and operate. Customers can pre-configure the client for deployment to large numbers of users. VPN access policies and configurations are downloaded from the central gateway and pushed to the client when a connection is established, making the client simple to install and manage, with high scalability.

The VPN client supports Windows 7, Windows 2000, XP and Vista (x86/32-bit only); Linux (Intel); Mac OS X 10.4 and 10.5; and Solaris UltraSparc (32 and 64-bit).

- **SSL (Secured Socket Layer).** SSL provides encryption of data between the end user laptop and the Central Network Gateway (CNG) in the Colt network, which is connected to the customer's VPN. Customers can define several user group roles with different access levels to network resources. End-point health checks like anti-virus and firewall can be configured.

SSL supports Window 7, Vista (SP1 and SP2), and XP (SP2 and SP3) in combination with the Internet Explorer (IE) and Firefox browser. For Mac OS X, version 10.5 and 10.6 are supported when using Firefox and Safari. On Linux, various distributions are supported when using the Firefox browser.

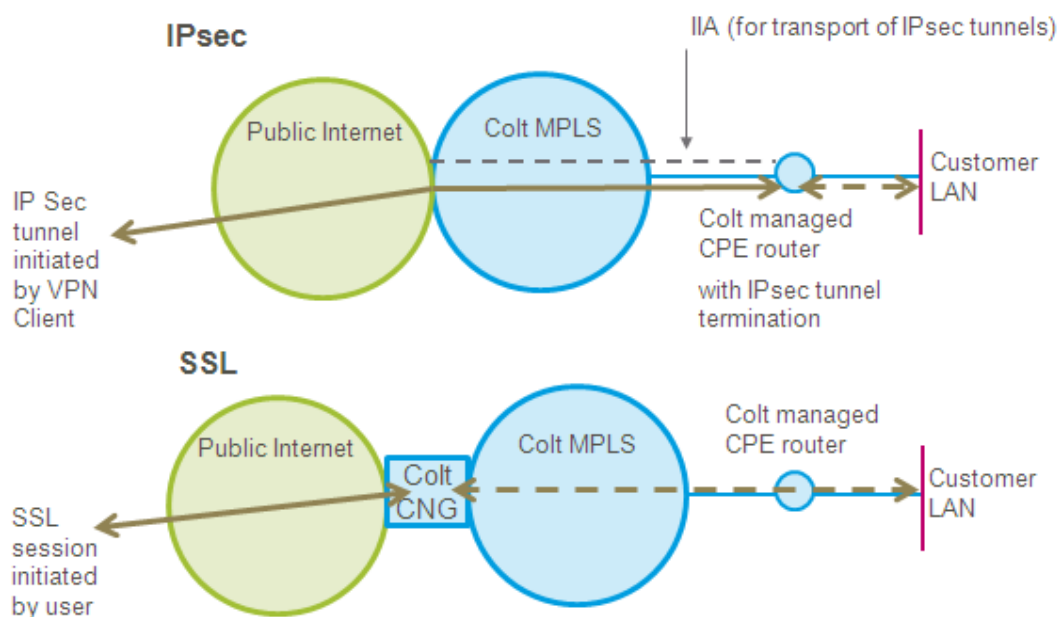


Figure 2: IP VPN Mobility encryption options

Operational conditions

For the operation of IPsec encryption, the public Internet connection for the remote access must support the configuration and transport of IPsec tunnels. This includes passing the following protocol types and port numbers:

- **Protocols** - 47 (GRE), 50 (ESP), 51 (AH)
- **Ports** - UDP Port 500 (ISAKMP)

For the operation of SSL encryption, the public Internet connection for the remote access must support the configuration and transport of SSL sessions. This includes the following port numbers:

- **Ports** - TCP Port 443 (HTTPS)

3.3.2 Public Internet access options

The public Internet access can be provided by the customer or by Colt. This results in the following two configurations:

- **Partially Inclusive** - Customer provides the underlying Internet Access for the remote users
- **Fully Inclusive** - Colt provides the underlying Internet Access to remote workers and business travellers

3.3.3 User Bundles

For the Fully Inclusive option, the following User Bundles are available for end-users:

- **User Bundle A** - Unlimited global dial-in and unlimited global WiFi access to the public Internet via the iPass network for laptops and smart phones.
- **User Bundle B** – Offers the same access as User Bundle A plus national mobile (3G/UMTS/HSDPA) wireless access to the public Internet via the iPass network for laptops. For the mobile access, a fair use policy applies with a maximum of 5GB per end-user per month. The mobile cards / dongles and SIM cards for the end-user laptops are provided by Colt. The national

mobile coverage is available in UK. The mobile coverage is national within the country that is selected for the service.

For all User Bundles, Colt provides an iPass software client for the end user laptops to set up, maintain and close the public Internet connection. The iPass software client first authenticates the end user (by login and password) before access to the Internet is granted. The iPass software client can start the VPN client automatically when the Internet connection is established in order to minimize the end-user effort.

For all user bundles, Colt will provide a standard configuration of the iPass software client. The iPass software client for laptops supports Windows XP, Windows Vista, Windows 7, MAC OSX 10.5, and Mac OSX 10.6. These configurations can be customized. iPass software clients for smart phones can be used for the service and support Apple iOS 2.1 or higher, Google Android 2.1 or higher, and RIM Blackberry OS 4.5 or higher. iPass software clients for smart phones come in a fixed configuration.

Each user bundle (A and B) also supports:

- Integration of home broadband Internet. This gives the end user identical access to the public Internet for all access types (Home broadband, Dail-in, WiFi and Mobile). Note that any cost related to home broadband need to be paid separately and are not included in the Colt invoices.
- Integration of non-iPass WiFi hotspots. Note that any cost related to these non-iPass hotspots need to be paid separately and are not included in the Colt invoices.

The software and hardware is provided by Colt to the IT manager. Customers must provide all end-user support for the hardware and software provided by Colt for the end-user laptops and smartphones. The customer is responsible for the installation, maintenance, and de-installation of software on the end-users laptops and smart phones. The customers is also responsible for distributing the mobile cards and SIM cards to the end-users and maintaining an up to date inventory of these devices. Colt service provisioning and assurance is available to the customer's IT department only.

3.3.4 Authentication options

End-users need to be authenticated before they can access the IP VPN and the iPass network. Authentication of end-users for IPVPN Mobility can be setup in two ways:

- Colt Authentication – Colt owns and manages all systems for authentication

and provides an online web-portal to manage end-user access rights.

- Customer Authentication – Customer owns and manages all systems for validating authentication requests. Colt forwards all authentication requests to the customer systems.

3.4 IP VPN Remote Fixed Access

IP VPN Remote Fixed Access is a remote access option that connects sites via IP Sec tunnels across the public Internet back to a customer's IP VPN fixed network. A Colt managed CPE router is placed at the remote site and a tunnel is built back to a customer's fixed IP VPN via a gateway on the Colt network. We will also manage the encryption keys for the tunnels from the remote router.

Two options are available:

- Customers provide the Internet Access at the customer site
- Colt provides the Internet Access at the customer site

Ethernet and E1 interfaces are supported to connect the Colt managed remote router to the Internet service provider's (ISP) network. Customers must make sure that legislation and regulation allow the use of IP Sec tunnels can be used at the customer site.

The following must be supported for the ISP Internet Access component of the Remote Fixed service:

- A fixed IP address on the WAN side of the router
- A fixed loop-back IP address
- Protocol and port transparency as noted

For the operation of Remote Fixed Access, the Internet connection for the remote site must support the configuration and transport of IP Sec tunnels. This includes passing the following protocol types and port numbers:

- **Protocols** - 47 (GRE), 50 (ESP), 51 (AH)
- **Ports** - UDP Port 500 (ISAKMP)

The following figure shows IP VPN Remote Fixed Access.

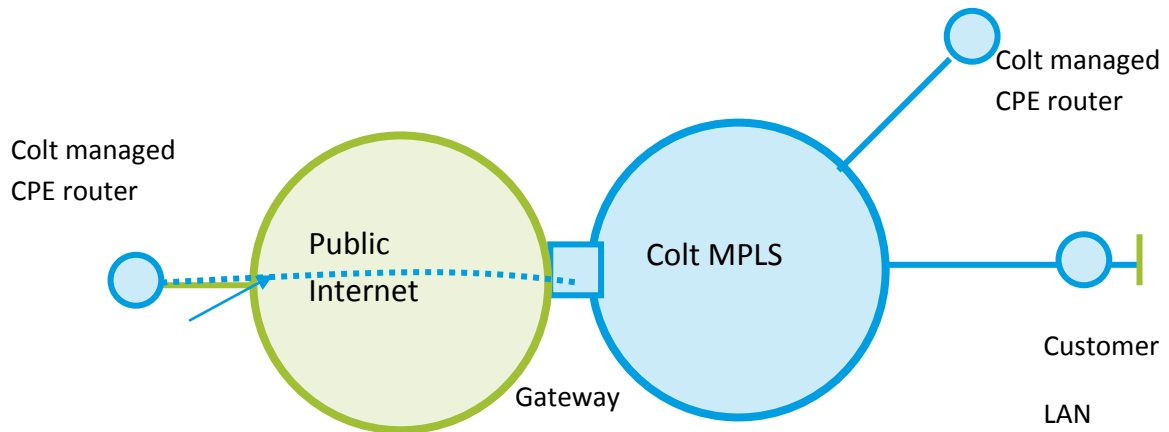


Figure 3: IP VPN Remote Fixed Access

Additionally, the following sections further describe the IP VPN service:

- [Colt's network coverage](#)
- [Network access](#)
- [Bandwidth options](#)
- [Technical attributes](#)

3.5 Colt's network coverage

Our secure and reliable network provides unrivalled reach across 19 countries with fibre-based metropolitan area networks (MANs) in 34 major cities. More than 17,000 buildings are directly connected to this network.



Figure 4: Colt network map

3.6 Network access

Colt has a comprehensive range of options for connecting customer sites to the Colt IP VPN backbone. Whichever access method type is used, the customer's solution will be created and managed by Colt under a single end-to-end SLA.

The maximum bandwidth of Colt services using DSL and EFM depend on copper line distance. For all DSL types (for example, ADSL and SDSL), the maximum bandwidth depends on the length of the copper line between the PTT Central Office (CO) and the customer site. If the copper line length is longer, the maximum bandwidth is lower. Therefore, the best maximum bandwidth is achieved if the customer site is very near the CO. Colt always lists the maximum bandwidth with minimal copper line distance. As a result, the maximum bandwidth can be lower than the listed bandwidth.

For ADSL, the download bandwidths (Colt network to customer site) above 2Mbps are mostly affected by the copper line length. For SDSL, the identical upload and download bandwidths are both affected by the copper line length. In general, bandwidths up to 2Mbps are possible if the copper line length is less than 2km.

In the case of ADSL and ADSL2+ lines in the UK, an additional line stabilization period of 10 days applies after delivery of the service. The purpose of the stabilization period is to optimize the line performance. During the stabilization period (especially during the first days), the line can be unstable and cause errors.

3.6.1 Colt access types

Customer sites can be directly connected to the Colt network using the following access types:

- [Fibre](#)
- [Unbundled local loop \(ULL\) DSL](#)
- [Ethernet in the First Mile \(EFM\)](#)

3.6.1.1 Fibre

Colt's MANs deliver high capacity, high speed bandwidth services to Europe's major business centres, which are interconnected via a European fibre-optic network delivering high quality reliable services door to door.

Each access to a customer's site uses ring architecture and diversely routed fibres where possible. SDH, Ethernet over SDH (EoSDH) and Multi Service Platform (MSP) provide the capability to switch between circuits where there are two separate circuits. This is known as automatic protection switching. Access connectivity can be restored within 50ms in case of failure.

Within the core, each node is parented to at least two other nodes using Colt's own backbone. These two nodes are protected using the same method as in the access network to ensure high resiliency. The core network typically runs at availability levels of 99.999%.

3.6.1.2 Unbundled local loop (ULL) DSL

Colt has invested in unbundled local loop (copper pair connections from the incumbent operator) with more than 600 central offices in 45 cities and 12 countries. Colt uses this to provide Symmetrical Digital Subscriber Line (SDSL) connections to customer sites. Colt owns the SDSL equipment with the copper provided by the incumbent PTT. The bandwidth provided is uncontended (bandwidth is not shared with other customers and therefore constant) and symmetrical (same speeds in both directions).

3.6.1.3 Ethernet in the First Mile (EFM)

Colt also uses ULL to provide Ethernet in the First Mile (EFM) connections to customer sites. EFM is a cost-effective access technology based on Ethernet protocol that allows high bandwidth connections over copper lines. Bandwidths are available at a maximum speed of 40Mbps, if the Colt service and the length of the

copper line permits.

Colt is able to provide on top of the minimum required number of copper pair for the respective bandwidth an additional copper pair, so that there is a much higher resilience against any change of line quality or outage of a single copper line. This option is called EFM Enhanced Bandwidth Availability. If there are no increased requirements on the bandwidth stability or resiliency, the standard deployment is sufficient. The choice which provisioning rule should be applied for the respective site can be selected on the order form.

3.6.2 Partner access types

Colt interconnects with and manages more than 85 partners in order to connect sites that are outside the reach of the Colt network in Europe or in other global locations.

Colt will order a circuit or circuits from the partner carrier on the customer's behalf, and customers will still be dealing directly with Colt at all times. Colt also takes responsibility for testing the interface between our network and the OLO's circuit to ensure that the customer's overall IP VPN service operates seamlessly.

Customer sites can be connected through partner networks using the following access types:

- [Wholesale DSL \(wDSL\)](#)
- [Leased lines \(SDH\)](#)
- [Ethernet tails](#)
- [MPLS NNIs](#)

3.6.2.1 Wholesale DSL (wDSL)

Colt interconnects with and manages 17 partners providing wDSL coverage in 12 European countries. wDSL can be used to provide SDSL and ADSL access at Off-Net sites. Wholesale DSL provides cost-effective reliable access underpinned by an SLA.

Where a PSTN or DSL line is provided by the customer for service delivery, this line must be maintained during the term of the service. If customers are reusing an existing line, which is possible in some countries, then customers must also maintain this line for the period of the IP VPN service. Any disruption to service caused by changes or faults related to the PSTN or DSL service does not constitute unavailable service in terms of IP VPN and also does not invoke IP VPN service compensation schemes of any kind.

Although DSL has excellent coverage, due to distance limitations and country

variations, the exact speed and availability can not always be confirmed at time of ordering. This means that orders are generally not confirmed until a Colt Promise Date (CPD) is issued, and any orders are provisional until DSL testing is confirmed. Delivery times are specified as indicative and, until a CPD is issued, the price and delivery mechanism may be subject to change.

3.6.2.2 Leased lines (SDH)

Leased lines are circuits or combination of circuits designated to be at the exclusive permanent disposal of a given subscriber. The interconnects to our partner networks consist of highly resilient, SDH-based Network-to-Network (NNI) connections.

3.6.2.3 Ethernet tails

Both protected and unprotected Ethernet circuits can be used to extend Colt's network to customer sites. Partner services are technically validated for compliance with key Ethernet technology standards and Colt's own product specification.

Integration is achieved using both simple cross-connected point-to-point services and Ethernet NNI connections. E-NNIs offer many advantages in terms of manageability, cost and deployment. Colt adheres to developing MEF standards and now has E-NNIs in the UK, France, Austria, Spain, Germany and Switzerland.

Colt uses Ethernet demarcation devices to provide sophisticated standards-based Operations Administration and Maintenance (OAM) end-to-end.

3.6.2.4 MPLS NNIs

Colt has agreements with a number of MPLS carriers to deliver connectivity outside of Western Europe via MPLS NNI – meaning the Colt MPLS network and the carrier MPLS network are connected together in a highly resilient setup. Colt is managing the end-to-end connection, including any CPE routers. Some features are not available via MPLS NNI-connected sites.

3.7 Bandwidth options

The IP VPN service is able to support different bandwidths as described in the following table for Colt Fibre access.

Table 1: IP VPN bandwidth options

IP bandwidths available

64kbps – 2Mbps

2Mbps – 20Mbps with increments of 1Mbps

IP bandwidths available

20Mbps – 50Mbps with increments of 5Mbps

50Mbps – 150Mbps with increments of 10Mbps

200Mbps – 1Gbps with increments of 100Mbps

Above 1Gbps available on request

Bandwidth is inclusive of underlying transport. For example, if MPLS is the underlying transport, then the IP packet throughput may be lower due to the protocol overhead.

On DSL, other bandwidths are available.

3.8 Technical attributes

Technical data consists of:

- [IP layer and routing protocols](#)
- [IP addressing](#)
- [Interface options](#)
- [Latency](#)
- [Packet loss ratio](#)
- [Jitter](#)

3.8.1 IP layer and routing protocols

The IP VPN service delivers and accepts IP version 4 packets only. It routes packets between customer sites based on the destination IP address either by static routes or by routing protocols.

Dynamic routing can be present at three different places in the Colt IP VPN network:

- Between Colt managed CPE and customer LAN
- Between physical edge (PE) router and Colt managed CPE
- In the Colt managed VPN core (PE to PE)

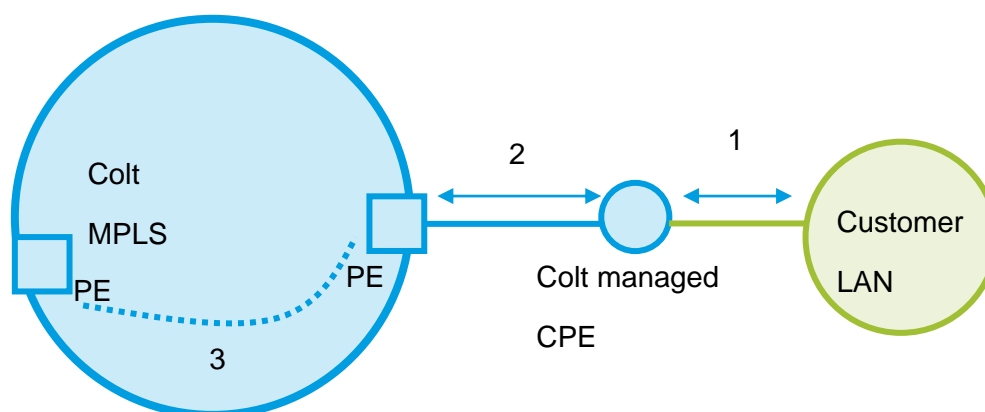


Figure 5: Dynamic routing

3.8.1.1 Dynamic routing between Colt managed CPE and customer LAN

Dynamic routing is exchanged between the Colt managed CPE router and the customer's own management equipment so that when the customer changes something in the LAN (for example, adding new segments), this is then propagated automatically. This feature is available on a customer case-by-case basis with IP VPN Plus (allowing us to check the technical feasibility). The following table describes the dynamic routing between Colt managed CPE and customer LAN.

Table 2: Dynamic routing between Colt managed CPE and customer LAN

	IPVPN Plus	IPVPN Access
BGP	Case-by-case	N/A
RIP	Case-by-case	N/A
OSPF	Case-by-case	N/A
EIGRP	Case-by-case	N/A
Static	Yes	N/A

3.8.1.2 Dynamic routing between PE router and customer managed CPE

Dynamic routing between PE router and customer managed CPE is only available for IP VPN Access services and allows routes between the Colt PE router and the customer managed CPE to be exchanged. Routing protocols available are BGP (default), RIP and Static.

3.8.1.3 Dynamic routing in the Colt managed MPLS VPN core (PE to PE)

BGP is used in the core for IP VPN Plus and IP VPN Access.

3.8.2 IP addressing

In order to manage the customer-located equipment and provide WAN connectivity across the network, Colt uses the IP addresses described in the following table. Customers cannot use any of these addresses on their own network.

Table 3: Excluded LAN IP addresses

Excluded LAN IP Addresses

192.168.99.0/24 to 192.168.255.0/24
10.82.20.0/22

In addition, Colt uses the following two ranges to assign addresses for point-to-point WAN links. Customers may use only one of these ranges on their own network and Colt will use the other range for WAN links. Customers cannot use addresses from both ranges.

The following table describes IP addresses for WAN links for IP VPN Plus.

Table 4: IP addresses for WAN links for IP VPN Plus

IP addresses for WAN links for IP VPN Plus

10.255.0.0/16
172.20.0.0/16
172.21.0.0/16
172.22.0.0/16

3.8.3 Interface options

The demarcation for IP VPN Plus is the LAN port on the Colt managed CPE router. The interface provided is Ethernet 10BASE-T or 100BASE-T, both of which are conformant to IEEE 802.3 (the physical connection is RJ45). As a standard service, this is a single interface. Half or full duplex is available; however, full duplex is the default.

With IP VPN Access, there is no Colt managed CPE router. Therefore, this service can be delivered with the interfaces described in the following table.

Table 5: IP VPN Access interface options

Access bandwidth	Presentation/Interface
------------------	------------------------

Access bandwidth	Presentation/Interface
E1	G.703/G.704
E3, DS3	G.703
STM1	Packet/SONET OC3c/STM1 Single mode (IR) Port
Ethernet Circuits	Ethernet 10BASE-T RJ45, 100BASE-T RJ45

3.8.4 Latency

Latency, or round trip delay, is the time taken for a 32 byte packet to traverse from Network Termination Point (NTP) to destination NTP and back again. It is made up of three elements:

- Delay between the service interface and the Colt Point of Presence (PoP)
- Delay across the core network between Colt PoPs
- Delay between the core PoP and the NTP

For more information on Colt's guarantees, please refer to the IP VPN SLA.

3.8.5 Packet loss ratio

Packet loss is measured across the Colt network over a calendar month. For more information on Colt's guarantees, please refer to the IP VPN SLA.

3.8.6 Jitter

Jitter is measured from PE router to PE router path and is defined on a monthly basis. For more information on Colt's guarantees, please refer to the IP VPN SLA.

4 Features

Features include:

- [Enhanced resilience](#)
- [Multiple Ethernet Interface](#)
- [Integrated Internet Access \(IIA\) CPE-based](#)
- [Integrated Internet Access network-based](#)
- [CoS](#)
- [SNMP read-only access](#)

- [IP Sec over IP VPN Plus](#)
- [Dynamic Host Configuration Protocol \(DHCP\)](#)
- [Multi VPN](#)
- [Performance Reporting](#)
- [Application Aware VPN](#)

Note that not all features are available on all services in all countries and some features are mutually exclusive.

4.1 Enhanced resilience

Colt offers a number of options to help customers increase the resilience of their IP VPN Plus service. These include:

- [Dual access – primary and backup](#)
- [Dual access - load balancing](#)
- [ISDN backup](#)
- [DSL backup](#)
- [Backup over the public Internet](#)
- [Backup over 3G public Internet](#)

4.1.1 Dual access – primary and backup

In the dual access configuration described in the following figure, two CPE routers and two separate circuits are provisioned at the customer site. This provides two traffic paths – a primary and a secondary route – into diverse routers on the Colt network. In the event that the primary circuit fails, traffic will be sent via the secondary route.

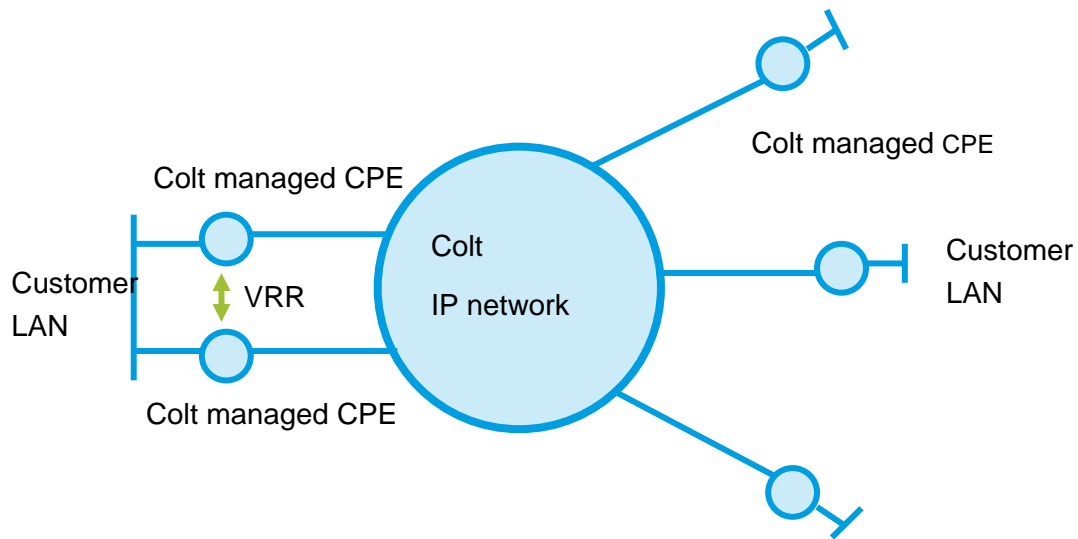


Figure 6: Dual homed configuration

BGP routing is used between the different sites to ensure network resiliency is effective. At the customer site, Virtual Router Redundancy Protocol (VRRP) is used as a failover mechanism between the two Colt managed CPEs. The two CPEs act as primary and secondary routers, but a single IP address is presented to the customer.

Dual access – primary and backup is not available for IP VPN Access services.

4.1.2 Dual access - load balancing

Dual access load balancing enables customers to use up to the full service bandwidth of the primary and secondary circuits. If one path fails, traffic will continue uninterrupted over the second path. Service bandwidth of each traffic path must be identical to ensure traffic is balanced equally across each traffic path.

Load balancing is implemented on a per packet basis. It is not available as standard for IP VPN Plus or IP VPN Access.

4.1.3 ISDN backup

There are three ISDN backup options available with IP VPN. This flexible range of options covers a number of scenarios, from ordering the customer ordering the ISDN line up to an all-inclusive ISDN backup service fully managed by Colt. Dial around the network options are available.

The following table shows the available ISDN backup options.

Table 6: ISDN backup service

ISDN Option	Dial around the network	ISDN line managed by	ISDN Backup number type
Option One	Yes	Customer	Non-freephone
Option Two	Yes	Customer	Freephone
Option Four	Yes	Colt	N/A

Note: the Dial through the network options three and five are no longer available.

If customers order the ISDN line themselves from another supplier, then they must ensure that the line is available when the IP VPN service is installed. If the line is not available when the fixed line is installed, then Colt will not commission the full ISDN backup service as part of installation. Full ISDN backup service must be requested as a Category B modification when the line is installed. Colt has no responsibility for the installation or repair of ISDN lines from other suppliers. See [Modifying an existing service](#) for information about Category B modifications.

Rerouting time is approximately 120 seconds for MPLS-based connections and 60 seconds for ATM or Frame Relay connections. Timings include identification of route failure, route propagation and convergence in addition to ISDN dial-up time.

4.1.4 DSL backup

DSL backup offers network diversity as well as a backup method that provides a lower cost than a second fixed circuit. DSL backup can back up a primary circuit based on either fibre or third-party leased line.

Primary and backup circuits terminate on different Colt MPLS PoPs in the Colt node whenever possible. The exception to this is if both primary and backup circuits are based on DSL because it is possible that both of these circuits will terminate on the same MPLS PoP.

DSL backup supports unequal primary and backup service bandwidths; for example, 4Mbps access and 1Mbps/1Mbps DSL backup.

4.1.5 Backup over the public Internet

Since public Internet access is available nearly everywhere, it is a widely available and cost-effective way to deliver a backup path to a primary circuit. A secure tunnel based on the IP Sec protocol is built across the public Internet to deliver the backup path. Colt manages the CPE router that interfaces to the customer's LAN.

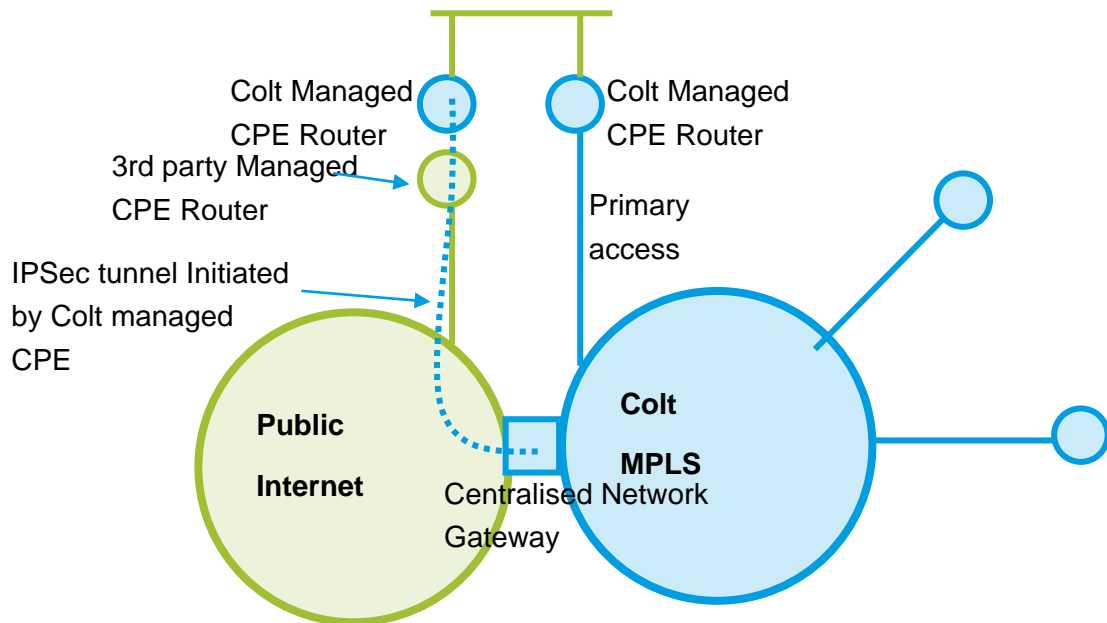


Figure 7: Backup over the public Internet

Customers must make sure that local legislation and regulation allow the use of IP Sec tunnels at the customer site.

Depending on the geography, there are two options for the delivery of the Internet access:

- **Partially Inclusive** - Customers provide and manage the Internet access. This service is available in Colt countries and Luxemburg
- **Fully Inclusive** - Colt does provide and manage the Internet access. This service is available nearly worldwide (including Colt countries)

In case of backup conditions, it is possible to request for the filtering of traffic so that only important traffic makes use of the backup path.

Note that the Internet access is available only as bearer for the IP Sec tunnel, not as local access to the Internet.

4.1.6 Backup over 3G public Internet

Backup over 3G public Internet is a backup mechanism based on 3G wireless transmission. It is independent of the fixed wireline infrastructure ensuring true resilience and disaster recovery preparedness. While DSL, ISDN, and backup over the Internet are common choices for backup in the event of primary WAN link failure and can provide higher throughputs, a non-terrestrial data path such as 3G wireless provides enhanced WAN diversity.

Colt will provide:

- CPE router, including (3G) wireless card
- Installation on-site of the CPE router, including (3G) wireless card
- Management of the CPE router, including (3G) wireless card
- Setup, termination and management of the IP Sec tunnel over the wireless Internet access
- Termination of the IP Sec tunnel and insertion of traffic into the customer IP VPN

For this option, customers have to provide:

- 3G wireless contract, signed directly between customer and the wireless provider (or MVNO)
- Access to the public Internet has to be provided as part of the wireless contract
- An activated Subscriber Identity Module (SIM) card, as part of the wireless contract

The 3G wireless WAN service supports the following 3G and 2.5G technologies: HSPA, UMTS, EDGE, and GPRS.

Note that it is the customer's responsibility to check the 3G coverage at the exact location that the Colt CPE router (including 3G antenna) will be installed. Colt advises against putting the Colt CPE in a basement or closed room without windows. Attention needs to be given to the internal cabling needed to connect the Colt managed CPE to the access circuit, as the Colt managed CPE has to be located outside of the (closed) IT room.

The 3G antenna can be positioned at a maximum of 15 metres from the Colt Managed CPE router. Colt will provide the coax cabling to connect the 3G antenna to the Colt Managed CPE router. It is crucial that the 3G antenna is positioned in a location with good 3G coverage.

The 3G bandwidths quoted by mobile operators are in general maximum, theoretical speeds. The 3G bandwidths seen in reality can be a lot lower (up to half or less in some cases). Colt can not control or guarantee this 3G bandwidth. Most of the wireless technologies are intrinsically asymmetric in speeds with a lower upload.

In order to be used with the IP VPN service as a backup, the 3G wireless contract must fulfil at least the following requirements:

- Should support full public Internet Access
- Should allow to connect a LAN site with multiple users, without restriction on the number of PCs / hosts attached to the LAN

- With a suitable rate plan designed for machine-to-machine (M2M) applications, preferably without data transfer limitations as otherwise the backup might not work when needed due to exceeded data rate limits.
- 3G wireless service should have preferably a fixed IP address. In case a fixed IP @ is not possible, Colt will make use of dynamically assigned IP@ and NAT. It should be noted that NAT is restricted in supporting some applications.
- The 3G service should allow IPSec traffic (i.e. allow UDP port 500, 4500, allow IP protocol 50, 51) and not block or filter this.
- Contact details of a person at the implementation site can be provided in the order form. The Colt installation engineer will retrieve the SIM card from that contact person.
- In case of backup conditions, it is possible to request for the filtering of traffic, so that only important traffic makes use of the backup path.
- Note that the Internet access is available only as bearer for the IP Sec tunnel, not as local access to the Internet.

4.2 Multiple Ethernet Interface

Multiple Ethernet Interface allows the NTP to be multiple Ethernet ports on the Colt managed CPE router. This service is aimed at satisfying switching requirements at the head office and the branch office by adding more LAN switching interfaces to the installed Colt managed router. Depending on the service bandwidth, several combinations are possible:

- Two LAN ports
- One LAN port and 16 switch ports
- Two LAN ports and 16 switch ports

4.3 Multicast

The Multicast feature is intended for customers who want to run multicast applications over their VPN network, such as video streaming. Multicast utilizes network infrastructure efficiently by requiring the source to send a packet only once, even if it needs to be delivered to a large number of receivers. The nodes in the network take care of replicating the packet to reach multiple receivers. This replication is done only where necessary.

Multicast is available on IP VPN Plus. It is not available on IP VPN Access.

4.4 Integrated Internet Access (IIA) CPE-based

Colt provides IIA CPE-based as a service option for sites that are connected via IP VPN Plus. This option allows combining two logical data streams (IP VPN traffic and Internet Access traffic) on the same physical access circuit. The service bandwidth for the Internet Access is defined separately from the bandwidth for IP VPN traffic. In this way, Internet traffic and IP VPN traffic are kept logically separate. If a CoS is selected, it is only available on the IP VPN service bandwidth. IIA CPE-based is not supported at sites connected by DSL circuits (Colt DSL and wDSL).

There are two Ethernet interface options:

- [Single Ethernet interface](#)
- [Dual Ethernet interface](#)

4.4.1 Single Ethernet interface

IIA is provided from the on-site Colt managed CPE router. A single public Internet address is provided with port address translation (PAT) to allow multiple internal hosts to access the Internet from this one public address. Access lists bar from the Internet any inbound traffic other than traffic that is destined for specified public addresses within the customer's network. Routing is based on destination address with the assumption that private addressees are used within the customer's IP VPN.

4.4.2 Dual Ethernet interface

With the dual Ethernet interface option, two Ethernet interfaces are deployed on the Colt managed CPE router: one for connection to the customer's own firewall for data packets bound for the Internet and one for general IP VPN traffic. The two ports on the router are thus used respectively for Internet access and for the IP VPN. These interfaces and ports enable customers to integrate the IP VPN solution with their existing firewall configuration. A firewall is necessary to provide security and address translation between the internal VPN and public Internet network. The Internet access port and its corresponding WAN sub interface are configured in the global routing tables.

The following table describes dual Ethernet interface options.

Table 7: Dual Ethernet interface options

Option	Comments
PA address space	Default is eight
Primary DNS, Secondary DNS	N/A

Option	Comments
Reverse DNS	Available to customers who have their domain names hosted by Colt
Customer self-care on domain zone file	Available to customers who have their domain names hosted by Colt
SMTP backup, SMTP relay	N/A

4.5 Integrated Internet Access network-based

Internet Access could also be provided to customer sites via a network-based gateway to the public Internet. If customers take this option, all sites get a centralized access to the public Internet from a central point in the Colt MPLS network.

The aggregated service bandwidth for the Internet Access is defined centrally at the gateway. If CoS is selected, it is only available on the IP VPN service bandwidth. IIA Network-based is supported at all sites, including sites connected by DSL circuits (Colt DSL and wDSL).

Since the Internet Access is delivered from within the network, a firewalling function also has to be provided in the network. The firewalling function can be provided in two ways:

- A Colt managed hosted dedicated or Virtual firewall; Colt provides the firewall and manages it according to desired specifications
- A firewall provided and managed by the customer, housed in a Colt rack in the Colt Data Centre where the gateway to the Internet is located (Brussels, Belgium)

4.6 Hybrid MPLS and Ethernet networking

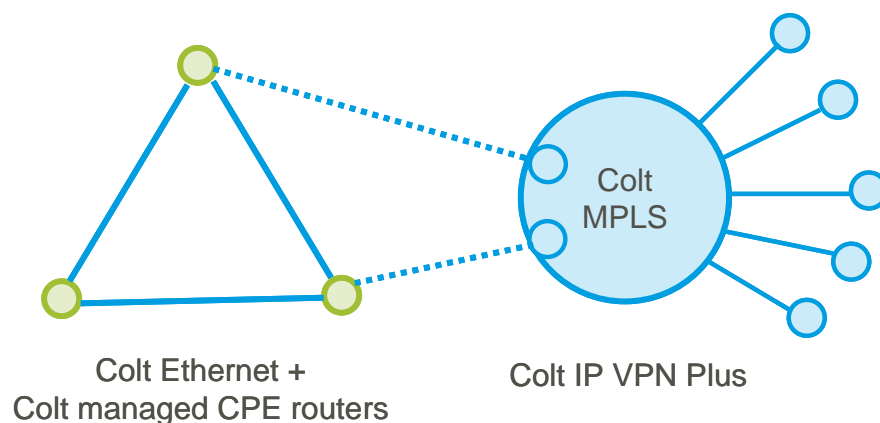
In the past a hard choice was imposed on the networking technology used in a WAN network service from a network provider:

Ethernet services,

or MPLS-based IP VPN services,

Colt provides you with the capability to mix the above technologies into one WAN networking service. For illustration purposes, assume a WAN network consisting of one HQ, two datacentres and 15 branch sites. The hybrid networking capability

would mix the strengths of every networking technology, for example this could mean that your HQ and 2 data centres are connected by Colt Ethernet services at 1G speed (or higher) and terminated on Colt managed layer 3 CPE router service. This is then fully interconnect to the IP VPN solution consisting of an MPLS network with 15 branch sites. The interconnect can be a single one, a resilient one or even a multiple resilient one.



Additionally, Colt can also integrate secure tunnels (like IPsec) over the public Internet into this WAN solution, to connect sites where no good fixed access exist from Colt or its suppliers, or where connectivity is expensive.

4.7 CoS

CoS enables customers to prioritise different traffic streams so that their most important data takes precedence over less time-critical traffic. Colt offers five different CoS classes. The Premium class is used specifically for voice and video applications, which are particularly delay-sensitive. Up to 50% of the service bandwidth can be assigned to carry Premium traffic. There are three Business CoS (1, 2 and 3) that enable customers to prioritise other business-critical or delay-sensitive traffic such as SAP and Citrix. The Standard CoS carries all other traffic that is not specifically assigned to a higher class and therefore designated as non-critical such as web browsing or email. Management traffic may use a small amount of the available bandwidth.

Bandwidth reservation takes affect at the network ingress when the customer is sending more traffic than the subscribed service bandwidth. If this is the case, traffic is randomly discarded before the queue is full. The Premium queue is policed at the assigned bandwidth level for that queue.

For IP VPN Access services, CoS will be available on the Colt backbone MPLS router in the direction towards the customer LAN. The customer must agree to use

the Colt packet markings in order to benefit from this feature.

CoS is not available on DSL circuits in which the contention ration is greater than two. Instead, Colt will implement ingress prioritisation that will enable traffic to be prioritised but cannot guarantee that Premium traffic will not be dropped in favour of other traffic.

4.8 SNMP read-only access

SNMP read-only access is available for IP VPN Plus. It is not available for IP VPN Access because there is no Colt managed CPE included with the latter.

SNMP read-only access to the Colt managed CPE provides access to parts of the Management Information Base (MIB)-II system: MIB-II interfaces and Environmental Monitoring MIBs.

4.9 IP Sec over IP VPN Plus

IP VPN Plus offers IP Sec encryption on top of the private Colt IP VPN backbone. Note that this should not be confused with IP Sec-based VPN on the public Internet. IP Sec encryption is not available with IP VPN Access.

IP Sec over IP VPN Plus satisfies customers who must encrypt all data network traffic. Each crypto map lists the valid peers and dynamically discovers peers and tunnels using End Point Discovery (EPD). Preshared keys are used to authenticate between IP Sec peers.

During the qualification phase protocol overhead, CPE router capabilities and fragmentation need to be reviewed.

4.10 Dynamic Host Configuration Protocol (DHCP)

DHCP allows the Colt managed CPE to lease IP addresses to local clients that have not been explicitly configured with the IP addressing details for a network. This enables users with interchangeable desktop PCs as well as laptop users who roam between sites to connect into the network.

Two options exist:

- **DHCP Server** - Enabled on the Colt managed CPE at each site, configured with a pool of addresses taken from the customer's LAN range. The server issues address details when a request is made by a user. When the address details are not renewed, they return to the pool of addresses for use by another user

- **DHCP Relay** - A central server owned and operated by the customer receives a request for addressing information by a user. The Colt managed CPE adds its own information to the request so the server knows from which site the request has come. Addressing information is relayed back to the user via the Colt managed CPE

DHCP is only available with IP VPN Plus services.

4.11 Multi VPN

Multi VPN enables customers to manage multiple extranets or internal sub VPNs over a single Colt IP VPN Plus network while ensuring that each extranet is entirely separate and unable to communicate with any other.

On the LAN side, multiple sub VPNs can be delivered on either separate physical Ethernet interfaces (there is a maximum of two per site) or up to 10 logical VLANs (802.1q). On the WAN interface, multiple logical circuits are presented on a single physical WAN access circuit.

Bandwidth is defined on a per **logical** circuit basis (that is, per sub VPN), so it is not possible for one sub VPN to burst into the bandwidth on another on the shared physical access circuit. The sum of the sub VPNs on one access circuit must be smaller than the service bandwidth of that site. The maximum number of sub VPNs is 10 per site.

Multi VPN cannot be configured on DSL sites. The following figure shows Multi VPN.

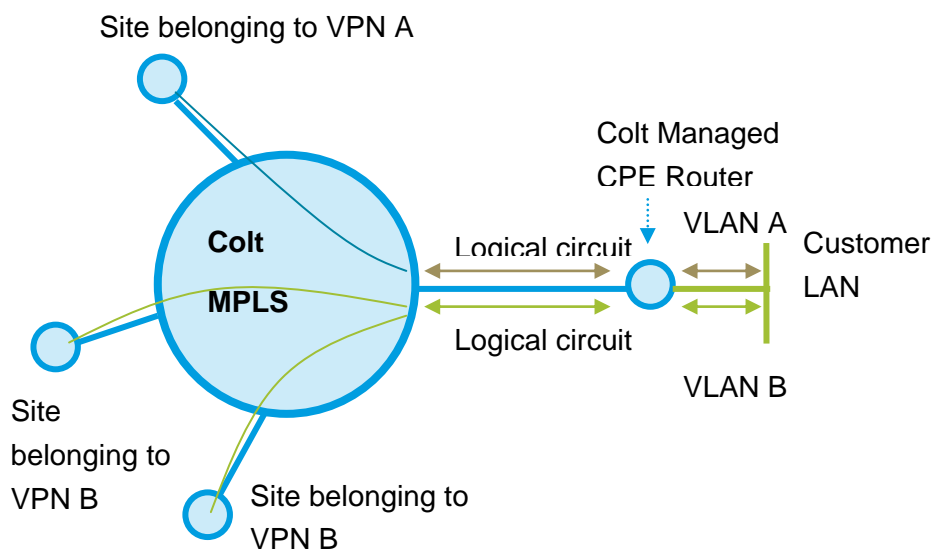


Figure 8: Multi VPN

4.12 Hybrid Networking

Business Critical Applications, such as ERP, Virtual Desktop and Collaboration, are increasingly Centralised and Virtualised in Data Centres.

Strong availability requirements drive the need for data replication and migration of Virtual Machines. At the network level, a few high-speed low-latency point-to-point interconnections are needed for traffic predictability and low-latency to allow Data Centres to operate as a single, low-latency LAN, support virtual machine portability, and make the backup and restore process simple and automatic.

Business Critical users (users whose productivity is critical for the business) require strong performance to support the business; this allows the business to prevent any customer discomfort about the quality of service and reduce complaints to the IT department. At the network level, a high number of low-speed any-to-any interconnections are needed, with control and commitment over traffic and application performance.

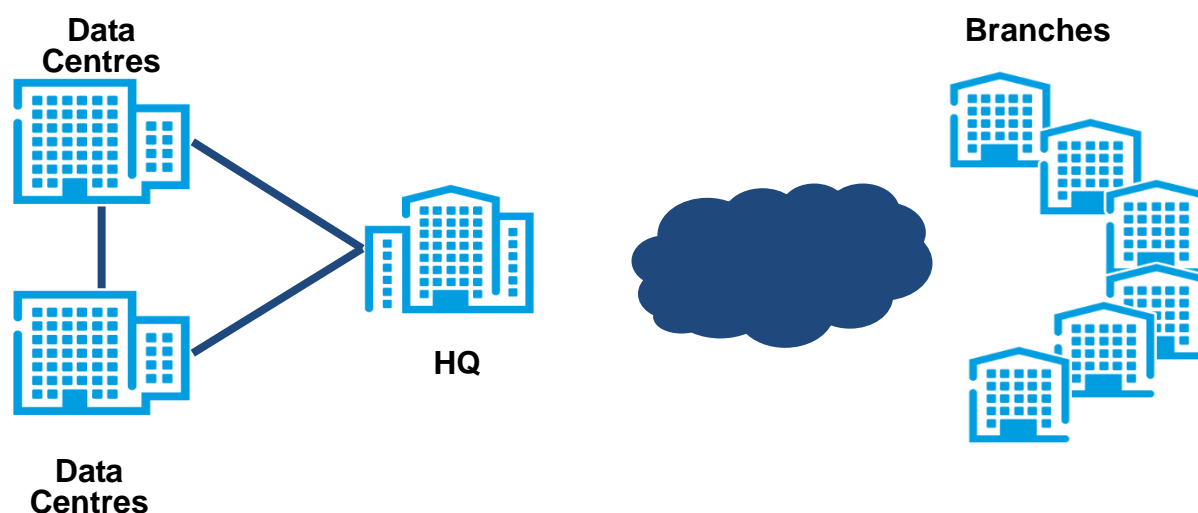


Figure 9: Hybrid Networking

Colt can implement the right technology to support the right application and make them interoperate, for example, Ethernet to interconnect Data Centres and headquarters, with a managed IP layer on top; IP MPLS VPN, with added Application Awareness, to make the different branches access and utilise the applications.

This provides visibility, in real time, of network and application performance; gives precedence and reduced response time to those applications that matter most to the success of your business, for example discriminating ERP and recreational peer-to-peer that use the same protocol/port (HTTP/80); and allows the definition of clear and measurable performance targets at the application level.

4.13 Performance Reporting

Online service performance and service management reports are available as part of the IP VPN service. Customers can access these reports at any time for up-to-the-minute indicative information on how their network is performing.

Customers can view performance reports of their IP VPN network online by selecting Colt's Silver or Gold packages.

The following figure shows the Colt Portal.

The screenshot shows the Colt Portal interface. At the top left is the Colt logo with the tagline "smarter / faster / further". On the top right, there is a user profile section for "ipvpngold@golddemo.net" with "Edit Profile" and "Logout" buttons, and a dropdown menu for "Choose Country & Language" set to "Pan-European Group". Below the header is a navigation menu with "Portal" selected. The main content area is titled "Current Services" and contains a table with the following data:

Contract	Service	Type	Details
080403205	IPC030600219	IP VPN	View Events Router Config View Service Status View Performance Reporting

Below the table is the "Service Tools" section, which includes a "Cisco VPN Client Download" link and a checkbox for "I accept the Licensing terms". Below this are links for downloading the client on Windows, Linux, and Solaris. At the bottom of the page, there is a copyright notice: "©2010 Colt Technology Services Group Limited. The Colt name and logos are trade marks. All rights reserved." and links for "Accessibility", "Terms of Use", and "Privacy Statement".

Figure 10: Performance Reporting

4.13.1 Silver

Customers can see throughput statistics on the physical interface in the network including any ISDN circuits as well as network performance information including availability, packet loss and round trip delay.

The following figure shows a report available with the Silver package.

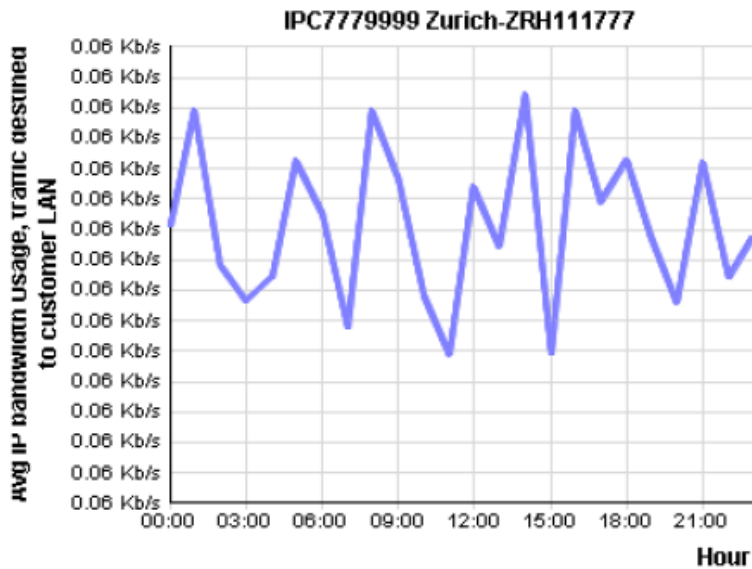


Figure 11: Silver report

4.13.2 Gold

As well as the reports available with the Silver package, customers can also see reports relating to router configuration, gain access to the logs for the devices installed by Colt and view graphical views of the real-time service status shown as red, amber or green.

Gold reporting is only available with IP VPN Plus.

4.13.2.1 Router Configuration View

The Router Configuration View provides customers with the following:

- Device identification and IP address
- Configuration of interfaces
- Ping, traceroute, routes
- BGP, CEF, RIP, OSPF, DHCP, policy maps
- Access lists
- Clear functions for counters, access lists and BGP configurations

The following figure shows the Router Configuration View.

[Home](#) > Router Tools

Router Tools

Service >> Site Order Number >> Device *

Command*

Command Response

```

show arp
Protocol Address      Age (min) Hardware Addr  Type   Interface
Internet 10.125.111.1      -          001f.9e65.76c8 ARPA   Vlan1
Internet 10.125.111.10    5          0014.389c.2b7e ARPA   Vlan1
Internet 10.125.111.11    250       001b.781a.94dd ARPA   Vlan1
Internet 10.125.111.15    0          0050.fc9. b1bf ARPA   Vlan1
Internet 10.125.111.25    9          001f.2951.1dbf ARPA   Vlan1
Internet 10.125.111.26    44        0022.64a6.d55a ARPA   Vlan1
Internet 10.125.111.50    1          0022.64a6.d55a ARPA   Vlan1
Internet 10.125.111.51    0          0008.190a.35c3 ARPA   Vlan1
Internet 10.225.111.1     -          001f.9e65.76c8 ARPA   Vlan2
Internet 10.225.111.100  1          001b.4f4d.7cb2 ARPA   Vlan2
Internet 10.225.111.101  6          001b.4f4d.7c9a ARPA   Vlan2
Internet 172.21.39.41    3          0023.abb0.f06a ARPA   FastEthernet4
Internet 172.21.39.42    -          001f.9e65.76d2 ARPA   FastEthernet4
BRU028744#
BRU028744#
BRU028744#

```

Figure 12: Router Configuration View

4.13.2.2 Event Log Viewer

The Event Log Viewer provides customers with access to the logs for the devices installed by Colt on the customer premises. This capability provides customers with:

- Device identification and IP address
- Ability to search for a given device or series of devices over the last 12 hours
- Ability to file based on severity

Note that one month of log data is kept available in the system and can be consulted. The following figure shows the Event Log Viewer.

[Home](#) > Event Audit

Event Audit

[Help](#)

Event Time* From: To:

Device

Available	Selected:
001554-IPC03060219.AMS.ipc.colt.net (IPC030600219)	
005497-IPC03060219.STO.ipc.colt.net (IPC030600219)	
021079-IPC03060219.ESS.ipc.colt.net (IPC030600219)	
025309-IPC03060219.HAG.ipc.colt.net (IPC030600219)	
026395-IPC03060219.LON.ipc.colt.net (IPC030600219)	

Message Require All Words

Severity Emergency Critical Error Alert Warning Notice Info Debug

[Search](#)

©2010 Colt Technology Services Group Limited. The Colt name and logos are trade marks. All rights reserved.

[Accessibility](#) | [Terms of Use](#) & [Privacy Statement](#)

Figure 13: Event Log Viewer

4.13.2.3 Service Status View

The Service Status View provides customers with graphical views of the real-time service status shown as red (critical), amber (minor) or green (no issue). The status is shown in real-time on the secured portal.

4.14 Application Aware VPN

Colt provides an Application Aware VPN (AAV) service as customers are citing that slower or unacceptable application response time and performance is among the main challenges currently being experienced by their business. This is primarily because of the following:

- Up to 60% of employees work in branch offices, many of which do not have local servers to host enterprise applications
- The number of servers are decreasing and data centres are being consolidated to reduce costs and increase security
- Many employees are therefore accessing critical data through a WAN – the performance of which has become a crucial element in overall application performance

- Many application protocols have been developed for the LAN where bandwidths are high and latencies are low. Now that these protocols are deployed over the WAN, the combination of lower bandwidth and much higher delays can lead to low performance

The Application Aware VPN service is specifically of interest:

- If customers manage a multinational IP VPN customers where traffic goes via multiple hops and where latency is a prohibitive factor
- If customers are looking for more application performance reporting – current reporting is mostly focused on the IP layer. Specifically, for customers who need to be able to see the activity of each of key applications to understand where the issues and bottlenecks may lie
- If customers have users who connect to their VPN remotely, either remote workers, mobile workers or third-party business partners

The AAV service consists of three parts:

- Application Visualisation
- Application Optimisation
- Application Acceleration

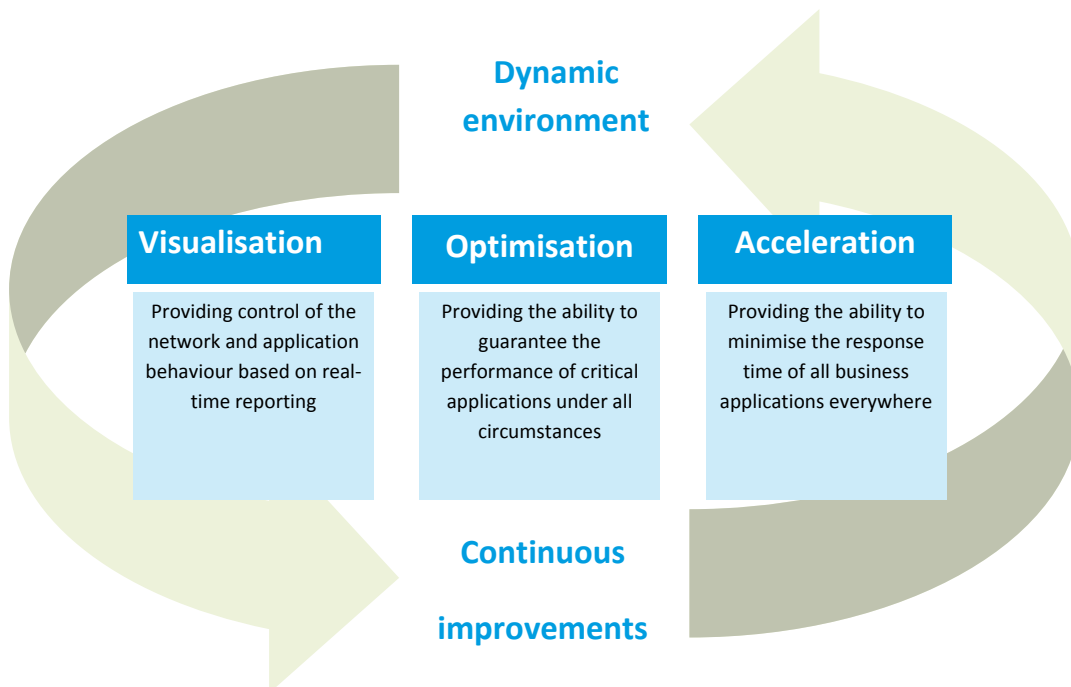


Figure 14: Application Aware VPN

A separate, more detailed description is available from Colt. Please ask an Account Executive for the *Application Aware VPN Service Guide*.

5 Coverage

Colt has also built up a capability to deliver IP VPN services to Western Europe, Eastern Europe, US, Asia and the rest of the world via a mix of Colt-owned infrastructure and third-party interconnects. Note that availability of services and features varies by geography.

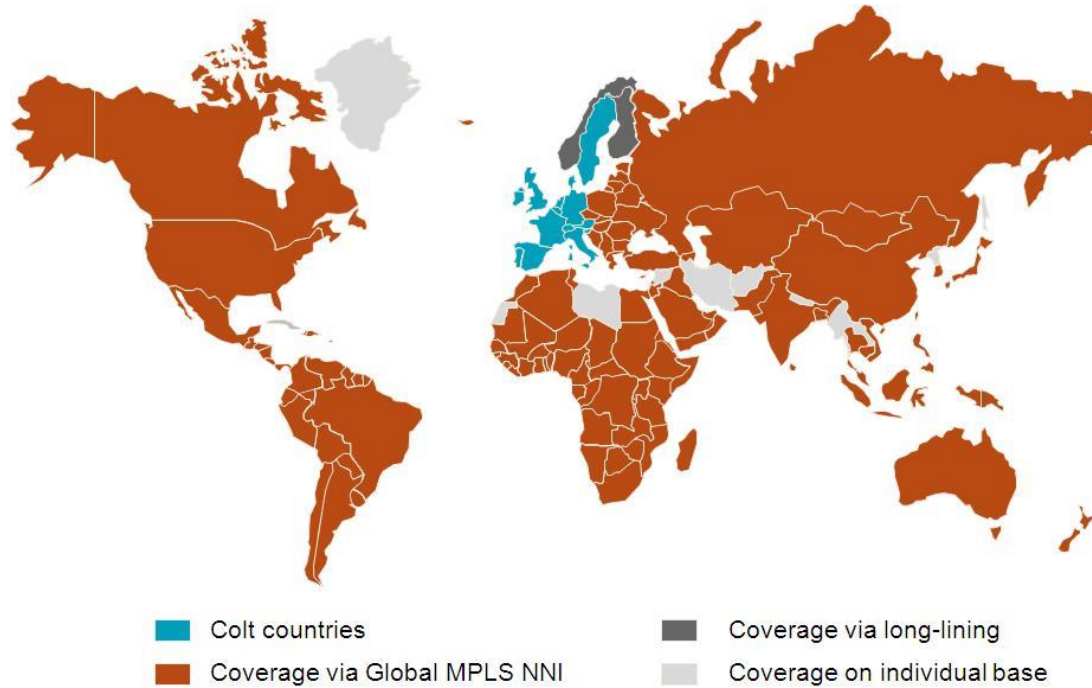


Figure 15: Coverage

6 Security

When the IP VPN service uses MPLS labels (for IP VPN Plus and IP VPN Access), it is impossible for another Colt customer to use their own access to intercept or send data to or from another customer's site. This is because logical channels are configured and routed by Colt from its management centre. So if a malicious user attempts to send data to an unauthorised site (assuming they knew a valid MPLS label or virtual path identifier [VPI] or virtual circuit identifier [VCI]), the traffic is discarded at the ingress node because no connection is established to support this traffic.

The physical security of our buildings is tightly controlled and access is strictly limited to authorised personnel only. All areas within Colt buildings are secured by means of an electronic access control system to ensure that access is controlled. All people must hold an appropriate pass card while on Colt premises. Non-Colt personnel are not allowed on Colt premises without specific authorisation and prior arrangement. Guests must be vouched for by a Colt host or verified by security in buildings.

7 Service delivery

Service delivery consists of the following:

- [New service order](#)
- [Modifying an existing service](#)
- [Out-of-hours changes](#)
- [Cessation or cancellation of service](#)
- [Demarcation point](#)

7.1 New service order

A new service order is the initial provision of the service to the customer premises including initial configuration of the network to the specification provided in the order form.

7.2 Modifying an existing service

Modifying an existing service consists of the subsequent enabling or disabling of service features, functions and interfaces as well as service changes following initial installation, which are chargeable items.

The implementation of most changes is chargeable, and some changes may mean that revised rental charges apply. Changes fall into the following categories: A, B and C.

- **Category A modifications** - Modifications that fall into this category require physical changes to the equipment delivering service. Examples include increasing the size of the access line to accommodate bandwidth increase outside of the existing access line. This is regarded as a new provision in terms of lead times. Category A changes can be scheduled out-of-hours subject to local approval. The local Colt Account Executive can provide customers with more information on any out-of-hours change requests
- **Category B modifications** – Configuration changes include modifications that can be done remotely. This category has been divided into two options:
 - **Option 1 (B1)** refers to service requests that can be completed within 12 working hours. The service request form identifies configurations that are typically able to be handled as B1. If a request cannot be handled within 12 working hours, then the delivery time is five working days
 - **Option 2 (B2)** refers to service requests that can be completed within five or 10 working days. These changes usually require the product order form to be completed

A committed lead time can only be given for ≤ 25 sites. Please contact a Colt Account Executive if there is a requirement involving > 25 sites because a specific lead time will have to be agreed with our IP Delivery Centre

- **Category C modifications** - Emergency configuration changes can be requested at any time and have a target implementation time of one hour from acceptance of order

7.3 Out-of-hours changes

Category B changes can also be requested out-of-hours. Out-of-hours changes must be scheduled and approved in advance, and there is a lead time of 10 working days. There is a charge of €200/hour per scheduled session with a minimum charge of €500 per session.

7.4 Cessation or cancellation of service

Request for cessation of service may be subject to a charge in accordance with Colt standard terms and conditions. Should the customer cancel their order during installation, Colt reserves the right to raise a charge.

7.5 Demarcation point

The demarcation point for Colt IP VPN services is:

- **IP VPN Plus** - Ethernet LAN port on the Colt managed CPE router
- **IP VPN Access** - Customer interface of the access circuit delivered

In-house cabling from the Colt cabinet to customer equipment is a chargeable service. If Colt installs cabling on the customer's behalf, the demarcation point remains the same: the base of the Colt cabinet. Colt is not responsible for fault-finding on the in-house cabling.

8 Service assurance

Colt provides a high level of service assurance:

- The core network is proactively monitored
- A local language help desk is available 24 hours a day, seven days a week
- Colt Online provides a web-based portal that enables customers to view bills and trouble tickets

Service assurance includes:

- [Customer service](#)
- [Service Level Agreement](#)
- [Colt Online](#)
- [Service monitoring](#)
- [Planned maintenance](#)

8.1 Customer service

Colt has a high quality European fibre network that enables the provision of an annual target service availability. The target availability depends on the service taken and the location of customer sites. The fault help desk is available 24 hours a day, seven days a week. Customers can report a fault at any time by contacting the Customer Service Centre and speaking to a representative in their local language.

When the service is provisioned, customers are issued with a unique service reference for each circuit that should always be used when reporting faults. The contact number for fault reporting is specified in the handover pack.

8.2 Service Level Agreement

Colt offers a comprehensive service level agreement with the IP VPN service, which pays compensation if agreed targets are not met. Our high quality European fibre network enables us to provide customers with an annual service availability of up to 99.99%. Ask a Colt Account Executive for more information about our SLA.

8.3 Colt Online

Colt Online is an intuitive, user-friendly application enabling new and existing Colt customers to interact with Colt via a secure Internet connection without the need to speak to a Customer Service Agent or Account Executive.

Every Colt Online customer is provided with an administrator account for a defined user within their organisation. This administrator has full access to the available features for all their customer accounts and sub accounts, including:

- Search and view any bill from the previous six months in .pdf format*
* Not available in Switzerland due to data protection legislation
- View the status of any order in the delivery process
- View the status of any ticket (covering faults, enquiries, service requests) in real-time
- Search and view all live services
- View an account dashboard, summarising the four features above

See [Colt Online](#) for images of Colt Online's features.

8.4 Service monitoring

The Colt IP VPN backbone network is proactively monitored and maintained by Colt. For IPVPN Plus, the IP VPN service is proactively monitored and maintained by Colt on an end-to-end basis, including the access circuit and the CPE router. This means that Colt proactively instigates remedial action when a fault is detected by the Colt monitoring.

Proactive notification is an optional service. In case this service is taken, customers are proactively informed of Colt opening a ticket. In case this service is not taken, Colt proactively instigates remedial action when a fault is detected but customers are not proactively informed of this action.

8.5 Planned maintenance

When planned works are required, customers will normally be notified in advance as per the following timelines:

- **Five working days** - Non-Service-Affecting planned works and standard planned work (routine maintenance)
- **15 to 17 days** - Service-Affecting planned works

Typically, planned works occur after 20:00 GMT on weekdays. For emergency changes, Colt endeavours to give four working days' notice; however, on some occasions, this is not viable and the work will be done in much shorter timescales with supporting justification and reasons.

9 Commercials

9.1 Contract period

The standard contract term is between one year and five years.

9.2 Billing

Colt offers a range of billing options including monthly billing for the IP VPN service. Bills are available on paper or on CD-ROM. Each bill contains summary sheet and further reports detailing the following charge types:

- Site installation and rental charges
- Any other charges and credits
- Discounts by service, if applicable

Charges will be billed on a per site basis as each site is provisioned. Bills are calculated on a pro rata daily basis. Bills will be raised for the entire network in the country in which the service was contracted.

9.3 Installation charges

Installation charges are billed after the service has been installed at a site.

9.4 Rental charges

Rental charges are billed in advance.

10 Colt Professional Services

Colt Professional Services is a team of highly focused experts dedicated to designing and managing solutions which support business transformation for our customers. Our consultants are available to:

- Conduct thorough reviews of current and future communications requirements
- Design complex projects to exacting standards
- Manage project implementations
- Ensure the service is being delivered to customer expectations

Colt has expertise in four areas: Project Management, Service Delivery, Consulting Services and Design Services. For full details of the services available, please contact a Colt Account Executive.

11 Glossary

MPLS - Multi Protocol Label Switching

IP VPN - Internet Protocol Virtual Private Network

IP Sec - IP Security protocol

NAT - Network Address Translation

PAT - Port Address Translation

NTP - Network Termination Point

ULL - Unbundled Local Loop DSL (DSL infrastructure owned and controlled by Colt except for the copper pair)

DSL - Digital Subscriber Loop

EFM - Ethernet First Mile DSL (high bandwidth, symmetric)

wDSL - wholesale DSL (DSL services bought by Colt from third-parties)

Contention ratio – Ratio of the bandwidth that is guaranteed, specified as X:1. If the contention ratio is not specified, the minimum bandwidth is not guaranteed (aka ‘best effort’)

12 Certifications and industry standards

Colt is dedicated to ensuring that our management systems adhere to the widely accepted International Standards Organisation (ISO) and British Standards Institute (BSI) standards. Colt holds the following certifications:

- **ISO 14001** - Internationally accepted standard that sets out a framework of essential elements for putting an effective Environmental Management System (EMS) in place. The standard is designed to address the delicate

balance between maintaining profitability and reducing environmental impact. This certificate is held for all Colt countries and helps us to identify the impacts that our operations have on the environment and then plan how we will reduce our most significant ones. It also ensures that we comply with all environmental regulations in each country we operate

- **ISO 9001** - The world's most established quality framework that sets the standard not only for quality management systems, but management systems in general. Colt holds this certification for the provision of service management for all Colt Data, Voice and Network Services, plus management of the Colt core network, backbone, switches, routers, infrastructure and associated systems
- **ISO/IEC 27001** - The only auditable international standard which defines the requirements for an Information Security Management System (ISMS). The standard is designed to ensure the selection of adequate and proportionate security controls have been established and also formally specifies a management system Information Security Management System (ISMS) that is intended to bring information security under explicit management control. Colt holds this certification for our Customer Managed Service (CMS) Solutions from European Data Centres. This includes customer European network monitoring, management and support services. In Colt India, this includes billing, revenue services and the Financial Shared Service Centre (FSSC). In Colt Spain, this includes Colocation Services in non-Data Centre locations

Appendix A Colt Online

Search and view any bill from the previous six months in .pdf format*

* Not available in Switzerland due to data protection legislation

Find Bill

Find a specific bill using the invoice number.

Invoice Number:

OR

Search Bills

To search for bills, use any combination of the following criteria

Billing Month:

Nov 2009 Dec 2009
 Jan 2010 Feb 2010
 Mar 2010 Apr 2010

Billing Contract Number:

Colt Customer Number:

Results Per Page:

[RESET](#) [SEARCH](#)

Bills

From here you can view, download and print bills from the past 6 months. Online billing is only an additional service feature. You will still receive a paper invoice for all services.

Bills are in PDF format. [Download Acrobat Reader](#) to view bills.

Figure 16: View Bills

View the status of any order in the delivery process

Order Details

[Print Order](#)

[Back to Search Results](#) << FIRST < BACK 2 / 2

This is a main order.

Overview

1. Raised	Order Validation	3. Implementation	Completed
<p>✓</p> <p>Order Received Date 25/03/2010</p>	<p>Order Entry</p> <p>Validation Completed 26/03/2010</p> <p>Order Entry</p>		

Please note that the additional Order Details will be displayed after order validation has been completed

Figure 17: Order Details

View the status of any ticket (covering faults, enquiries, service requests) in real-time

 [Print Ticket](#)




Overview	Details				
1. Raised		2. Diagnosing & Solving		3. Closure	
					
✓		✓		Closed	
Date & time (GMT) 29/03/2010 17:52		Diagnosed date & time (GMT) 29/03/2010 17:53		Restored date & time (GMT) 29/03/2010 17:53	

Figure 18: Ticket Details

Search and view all live services

Service Details ⓘ

[< Return to Search Results](#) | Service / 19 | [NEXT >](#) | [LAST >>](#)

Customer Details | **Service Details** | **Service Details - Billing**

Service Details - Billing

The amount shown on the invoices may include other services in addition to the one you are viewing on this page. Please view the invoice to check which orders are included.

Total Monthly Rental	0.0
Billing Start Date	Mon Mar 22 00:00:00 GMT 2010
Billing Expiry Date	

Invoice No.	Amount	Issue Date
20092010	78366.56	02-11-2009
20102010	77141.92	02-01-2010
20092010	75097.17	01-12-2009
20102010	75146.02	02-02-2010
20102010	75071.51	02-03-2010

Figure 19: Service Details

View an account dashboard, summarising the four features above

Appendix B Service delivery timeframes

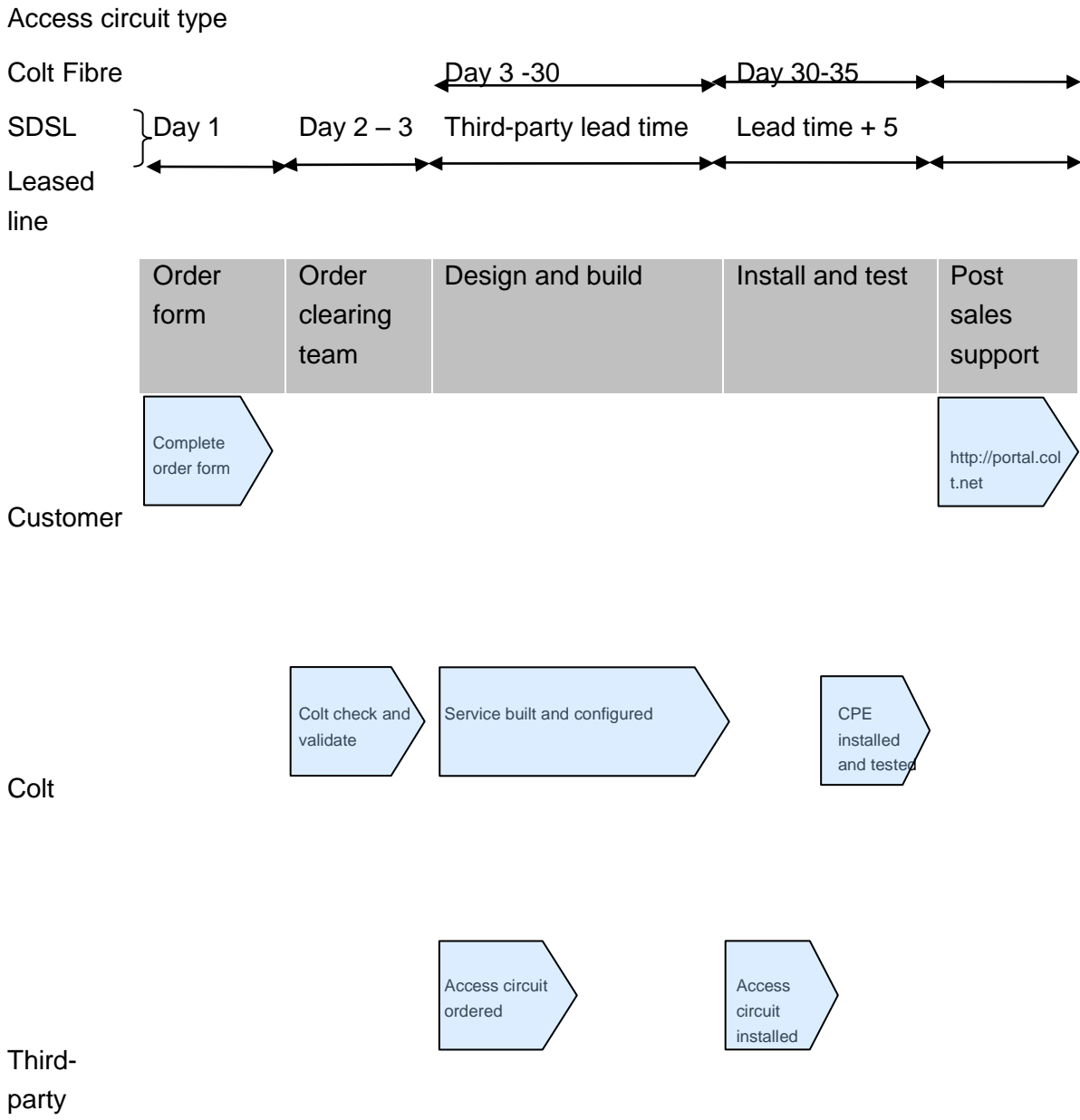


Figure 20: Timelines

Appendix C Order to delivery overview

Colt contact

Timeline of activities

Step 1 Order form completed

Working with the Colt sales contact, an order is raised for the Colt IP

VPN service.

Step 2 Order validated

The IP VPN service order is now validated by Colt and any outstanding issues or questions dealt with. Customers will be sent a letter confirming receipt and acceptance of their order.

Step 3 Design and build

The service is configured along with any optional features may have been requested. The access circuit will be ordered and customers will be sent a letter confirming the Colt installation date.

Step 4 (a) Access circuit installed

A technician is at the customer site to complete installation of the access circuit. Please ensure that they are given access to customer premises.

Step 4 (b) CPE equipment installed

Equipment is installed by Colt; the access circuit and IP VPN services are tested.

Step 5 Activation

Service is ready for activation. Customers will be given a handover pack that provides details of their service.
