WHITE PAPER

METRONET DATA SERVICES

Adding Network Value

INTRODUCTION

Metronet was formed in 2003 acquiring the Manchester based assets of Atlantic Telecom; an investment of up to £15 million in a dark fibre optic ring encircling Manchester City Centre running through six high-rise Points of Presence (POP).

Since this time, Metronet has added further POPs in the Manchester area enabling it to provide comprehensive coverage for its last mile wireless IP services throughout Greater Manchester, Bolton, Stockport and Warrington.

MANCHESTER
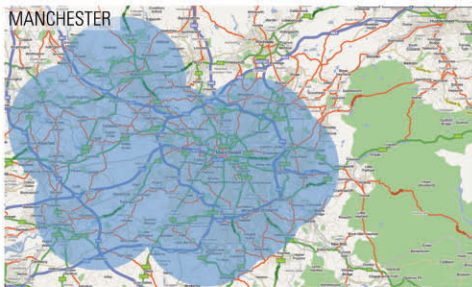
At the turn of 2009, Metronet announced that it had acquired more than 200 customers for its B2B Internet access services and Point-to-Point private IP circuits.

2008 marked the launch of services in Liverpool and Leeds with 2009 marking the launch of coverage across both Birmingham and Dublin.

With a 10Gb layoff via Telecity, IFL and Synergy House, Metronet offers its customers unparalleled connectivity to the world wide web by providing the most powerful and yet shortest route to the Internet of any carrier in the UK.

LEEDS

The establishment of an 'on net' data centre, coupled with a complete upgrade of its core network to a Cisco based MPLS (Multi Protocol Label Switching) infrastructure has enabled Metronet to launch a range of unique data services.

MPLS gives Metronet the opportunity to support a completely private network infrastructure (per customer) overlaid across its powerful fibre-optic based Metropolitan Area Network taking advantage of state-of-the-art Quality of Service techniques that ensure that bandwidth is allocated and used as though it were traversing a customer's own private network.

"Protocol agnostic", MPLS is ideally suited to networking converged voice and data traffic, with packets forwarded rapidly through the network without reference to data and specific protocols (network and transport protocols supporting the end-to-end control and data integrity). As such, MPLS accommodates legacy protocols (e.g. IP, ATM, SONET, etc.) whilst accommodating the variable packet lengths associated with different datagram types (e.g. short packets for voice, long packets for file transfer) and it is cited as the transport protocol of choice for the foreseeable future.

LIVERPOOL
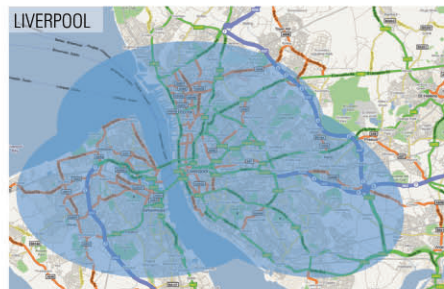
The need for MPLS has its origins in 21st Century fibre-optic technologies such as those employed in the Metronet core network, where the sheer data rates now achievable have largely eradicated concerns about variable length packets causing congestion for time sensitive applications such as video conferencing and voice.

BIRMINGHAM
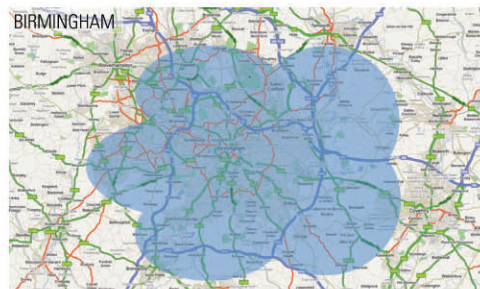
For existing customers, Metronet offers a single point of responsibility for both the network and data services under a single framework management facility that operates 24x7x365. No longer will customers face having to apportion responsibility for service performance between an ISP and data services providers, which is important given the history of finger pointing that has simply led to delays in problem resolution in the past.

For customers that are yet to migrate to Metronet last mile connectivity services and those that are beyond the Company's current coverage areas, Metronet data services offer unparalleled value for money from the UK's most progressive network operator.

This paper provides an overview of the range of services now available which include:

- IP VPN
- Managed Security
- Co-location
- QinQ
- IP Transit

MPLS IP-VPN

Heads up on the Technology

MPLS IP-VPN is a service provider layer 3 VPN (Virtual Private Network) technology that transports secure discreet overlay VPN solutions over a powerful shared backbone network, affording users an opportunity to take advantage of the service provider's economies of scale. Metronet's MPLS IP-VPN introduces optimum flexibility in ongoing network design and virtually unlimited scalability within a managed service package that provides assurance of Quality of Service and traffic engineering.

An MPLS IP-VPN comprises three classes of networking device:

Customer Edge Device (CE). A CE is a router located on a customer network with an appropriate number of local network interfaces that is connected to the Metronet MPLS network core via a PE device which serves as the MPLS gateway. Consequently, the CE requires no knowledge of VPN or MPLS technologies and is therefore easily managed locally.

Provider Edge Router (PE). A PE resides on Metronet's network connecting one or more CEs to the MPLS network and is responsible for all MPLS tagging and network processing.

Provider (P) Router. P routers make up the backbone network (not connected directly to CE equipment) and provide MPLS forwarding across the core.

With a Metronet MPLS service, the CE is a Cisco device that is installed and managed by Metronet, marking the boundary between Metronet and the customer. Connectivity across the Metronet is established either by the CE and PE exchanging routing information using the MP BGP (Multiprotocol Border Gateway Protocol) or by configuration of static routes by Metronet on the customer's behalf.

Once the PE has learnt the VPN routing information for specific CEs, it exchanges VPN routing information with those appropriate PEs specifically associated with an individual customer's CEs. It is not necessary for all VPN routing information to be understood by all PEs.

P Routers have no VPN knowledge as they simply serve to forward packets between PEs based upon MPLS labels. Consequently, an ingress PE is also referred to as a Label Switch Router (LSR), the egress PE is an Egress LSR and the P routers are referred to as Transit LSRs.
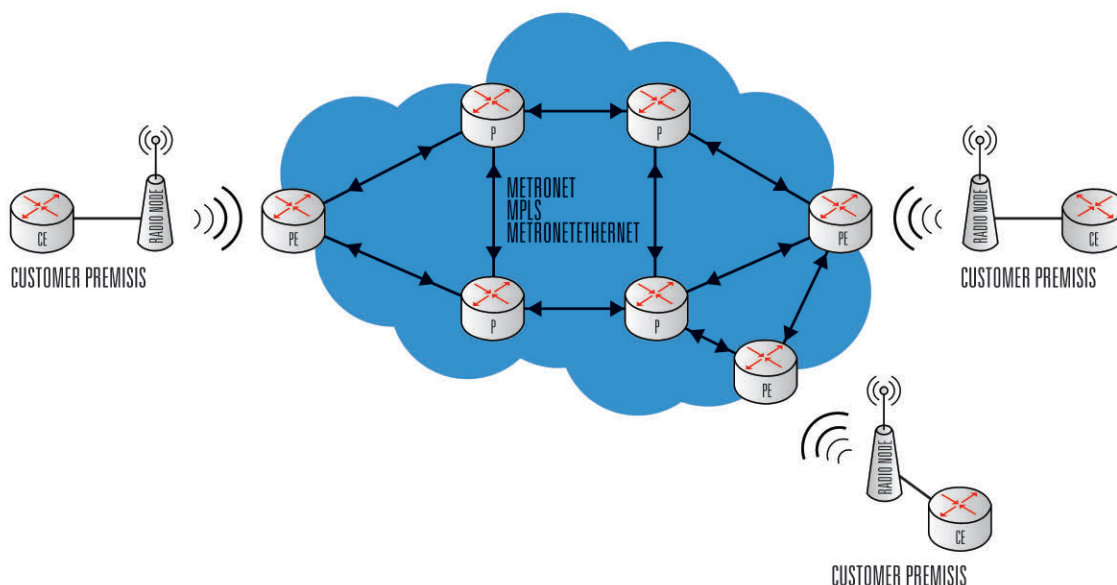
SECURE IP VIRTUAL PRIVATE NETWORK (VPN)

The strategic importance of inter-branch communications is now critical with increased dependency upon IP Telephony, virtualisation and web based services all of which combine to mean

"no network = no business"

Add increasing IT based interdependency between organisations and a case is made for ensuring that they have a secure network infrastructure capable of supporting mission critical applications as well as rudimentary everyday communications; both now and into an unpredictable future.

Metronet's managed VPN services provide a secure resilient platform for sharing applications and information, and for supporting IP telephony between branch offices and remote workers across its Cisco based MPLS network that offers prioritisation for mission critical and delay-sensitive applications.

Within Metronet's coverage areas, VPN access connections operate at data rates of up to 1Gbps with point-to-multi-point communication direct between locations without touching the public Internet, thereby ensuring the best possible performance.

For locations beyond Metronet's coverage area integration is possible by incorporating third party ADSL, SDSL and leased circuits within Metronet's central management framework. Having a single point of responsibility for multiple operators eradicates the possibility of finger pointing between suppliers should problems arise.

Metronet's management infrastructure and personnel monitor all VPNs 24x7 ensuring that potential network faults and issues are proactively addressed before User service is affected.

A single point of Internet access allows a single firewall to control all communications to and from the web for all sites within the VPN. The managed firewall can either be located 'onsite' at a customer's office or 'on net' as a fully managed service (see Managed Security).

Metronet IP VPNs are individually designed to meet the specific communications needs and priorities of each customer.

The business benefits of a Metronet IP VPN can be summarised as follows…

A single secure, managed, Wide Area Network for converged communications that is delivered to a committed Service Level Agreement allowing internal resources to be focused on core business ICT issues

Clear cost savings made by outsourcing network management & hardware resource and by consolidating firewall security at a single point in the network

24x7 single point Technical Account Management and support from Metronet's locally based Consultants giving assurance that any issues that arise are dealt with promptly

CUSTOMER PREMISIS   METRONET MPLS METRONETETHERNET   CUSTOMER PREMISIS
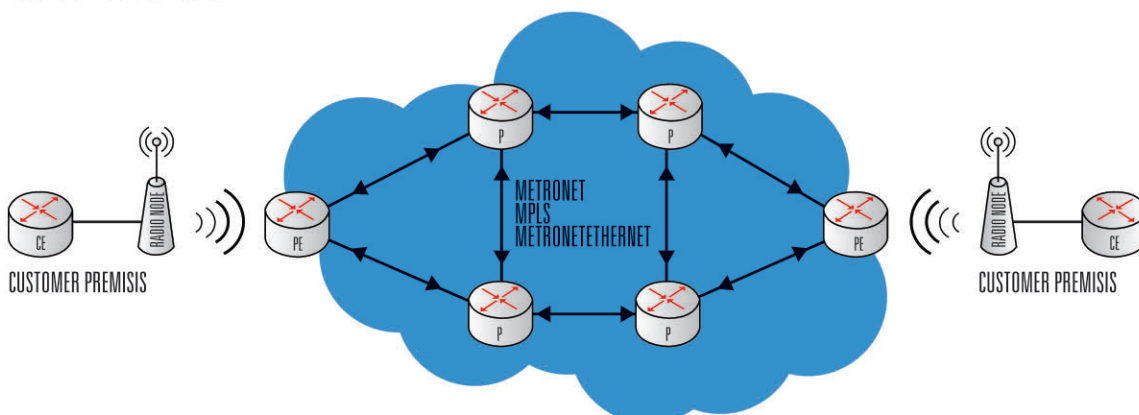
MANAGED SECURITY

All organisations now face a Blended Security Threat comprising potential attacks from network intrusion, viruses, worms, phishing, spyware, denial of service (DOS) attacks and spam. Management and administration of multiple point solutions that have traditionally been used to address the individual elements of the Blended Security Threat is now widely acknowledged as an enormous challenge. To address this challenge, Unified Threat Management (UTM) solutions have emerged as the only reliable means of protection against the multiplicity of threats now targeting corporate networks.

Metronet's Managed Security services that encompass systems administration and support, VPN configuration, policy management, hardware maintenance and support are delivered either 'On Net' or 'Onsite'.

Full Service 'On Net'

For organisations that seek to hand off day-to-day responsibility for Managed Security, this service is hosted 'on net' at Metronet's Data Centre and managed from Metronet's 24x7 Network Control Centre.

An ancillary benefit to this service is that the Data Centre is directly attached to Metronet's 10Gbps resilient fibre lay off to the Internet with the advantage that customers' last mile access circuits are not burdened with traffic blocked by the security process. Consequently, as well as safeguarding IT resources, the potential for malicious attacks to impact end user network performance is mitigated.

Full Service 'On Net' customers also benefit from the economies of scale presented by a shared resource. As a result, SMEs of any size can now benefit from 'blue chip' industrial strength security that would otherwise only be available to the largest organisations.

Co-Managed 'Onsite'

For IT and Network Managers that wish to retain control over security, this service comprises an onsite firewall with dual management responsibility. Working in partnership with Metronet Consultants, customers retain management control whilst taking advantage of Metronet's 24x7 service management that provides cover for:

- Out of hours support
- Holidays and sick leave
- Day-to-day distractions
- Specific systems expertise

In the unlikely event of hardware failure, Metronet guarantees next working day replacement; however, with its engineers based in the North West and having spares in-house, Metronet goes further with a best efforts promise to replace systems inside four hours.

A Comprehensive Package

Both Metronet Managed Security services comprise common elements that combine to provide a total solution.

Consulting

With in excess of 200 corporate customers and more than 500 network connections, Metronet Consultants have vast experience of network management and maintenance. The same Consultants that manage Metronet's Telco infrastructure provide direct support and consultancy for Metronet's Managed Security Solutions.

Pre and post sales support determines customer requirements both at the time of installation and as requirements evolve; with customers encouraged to develop working relationships with Metronet Consultants.

Ongoing support is available 24x7 with consultants available at any time day or night to assist with problems as they arise.

Real-time Protection – 24x7

As well as guaranteeing service availability in line with its 99.95% Service Level Agreement, Metronet also ensures real-time updates to guard against the changing Blended Security Threat.

Secure Roaming VPN Access

As well as configuring secure site-to-site communications, Metronet's Managed Security service also supports secure SSL VPN to accommodate the needs of roaming users that require web access via any machine, anytime, anywhere.

Management Reporting

Automatic periodic reports detail:

- Virus Activity
- Denial of Service Attacks
- Web Bandwidth Utilisation Statistics
- Spam Bandwidth Utilisation Statistics
- Website Activity Reports

Industry Leading Hardware

Metronet has selected Fortinet as its strategic hardware partner. With countless awards and more than 20,000 customers, Fortinet is the world's leading supplier of UTM security systems.
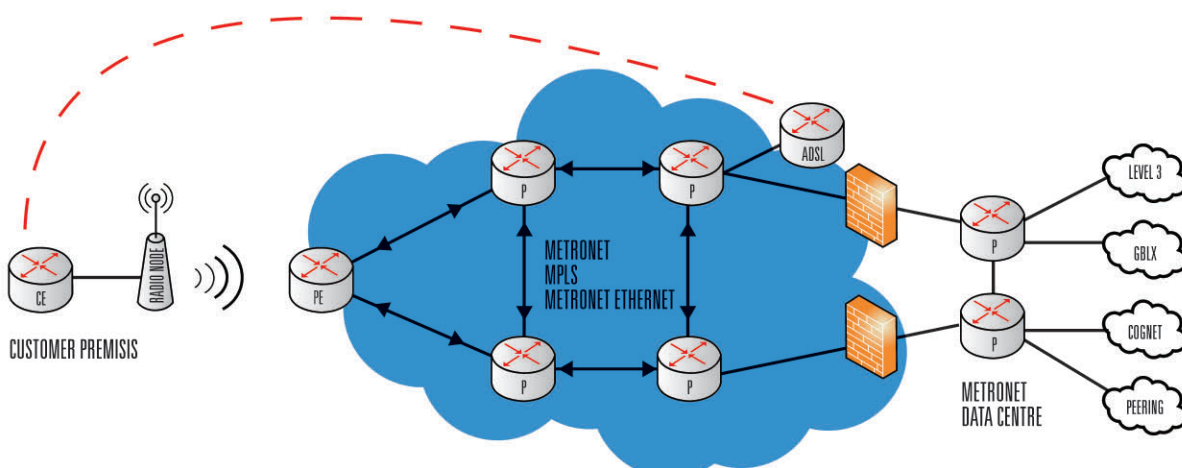
COLOCATION (COLO)

The costs of running an in-house computer centre can be eye watering, and for all but the largest organisations the challenge of professionally managing a controlled environment typically rests with ICT personnel as a secondary activity.

For many this is a time bomb ticking. Air conditioning failure, unauthorised computer room access, a worn out UPS and system malfunction leading to fire are but a few examples of unforeseen events that lead to corporate IT systems meltdown.

Every Organisation should at least evaluate shared facilities that allow even the smallest SME to take advantage of the economies of scale presented by a Data Centre.

With its newly commissioned Data Centre on the Manchester Science Park (serviced by a fully diverse fibre ring) Metronet now offers high-end high availability data space with fully redundant power and cooling.

For Metronet customers 'on-net', Metronet's Colo service represents a uniquely powerful proposition. Whereas customer access to collocated services is restricted to ordinary internet connections which limits upload and download data rates, Metronet customers are afforded access bandwidth at the full rate available through its last-mile circuits. As a result, server maintenance can be performed more efficiently than is otherwise normally the case.

Power

Supported by an independent High Voltage supply and substation, Metronet's Data Centre is able to sustain high powered racks that are required by today's power servers. In the event of primary power failure, N+1 Scania Generators will take the full loading of the entire Data Centre and chloride energy efficient UPS systems provide N+1 uninterruptable power to racks with a 10 minute autonomy providing power protection from spikes and mains failures.

Cooling

An N+1 Airdale HVAC system provides redundant under floor cooling with an ambient temperature kept at a constant 22°C to guard against any possibility of system failure due to overheating.

Fire Detection and Suppression

Equipped with both FM200 and VESDA systems above and below the raised floor, Metronet's Data Centre is protected by the most efficient non-water based data centre fire detection/suppression system available on the market today.

Physical Security

On site 24x7 security is supported by a swipe card operated secure door entry control system giving customer access only to appropriate areas of the Data Centre and internally/externally monitored IP based CCTV which is prevalent throughout the building.

Connectivity

Metronet's Data Centre is connected to a dark fibre ring with dual entry points to the building and interconnects with Metronet's backbone dark fibre ring at two of its Points of Presence. A carrier neutral facility provides a rich choice of connectivity with Tier1 and Tier2 bandwidth at the North of England's primary Internet Exchange.

Colo Racks

Each cabinet within the Data centre is 48RU and 600mm x 1000mm and can be subdivided to accommodate even relatively small servers. Private collocation cages are available for larger system requirements.

Technical Support

Colo N+1 support is integrated with Metronet's central Control Centre and network management facilities, giving reassurance that responsibility for both falls to a single point of accountability and authority. With Metronet, you will never be caught in a finger pointing exercise with separate suppliers seeking to pass the buck!

QinQ

IP Transit

Metronet's QinQ service provides an opportunity for organisations to use Metronet's powerful dark fibre Metropolitan Area Network as though it were simply another trunk in their own self managed VLAN infrastructure.

Metronet's separate 10Gbps internet layoff into the North West's leading Data Centres not only makes it the most cost effective QinQ infrastructure in the UK, but also makes the service viable for organisations that do not subscribe to Metronet's last mile circuits but wish to take advantage of its cost effective infrastructure to connect between Data Centres.

For organisations that depend upon high Internet availability and resilience such as, for example, regional ISPs and hosting companies, Metronet offers powerful, flexible and cost effective IP Transit services. As a tier 2 provider with its own fully resilient multi-homed network, Metronet has multiple connections to tier 1 providers and other tier 2 providers allowing it to deliver independent IP transit.

With ownership and responsibility for its own independent core network and last mile delivery circuits, Metronet is the only network operator capable of delivering tier 1 services at a price that is within reach of SMEs inside its areas of coverage.

Unlike other IP Transit providers, Metronet does not demand a contractual minimum commitment that is beyond the reach of SME Organisations, which makes it an ideal partner for those seeking to establish cost effective additional resilience and availability for IP services.

Metronet IP Transit services are covered by the Company's standard SLA commitment providing reassurance of service continuity. Add a completely independent 'last mile' access infrastructure and backbone network, and it becomes clear that Metronet is an obvious partner for anyone seeking maximum service resilience.

QinQ VLAN Tag

PANNONE
THE COMPLETE LAW FIRM

Pannone LLP is a full service law firm with clients split almost equally between businesses and private individuals. With roots that can be traced back as far as 1852, the firm now has 380 solicitors, 92 partners and a total staff of 780.

Pannone prides itself on providing a quality service to its clients; a commitment that it claims is illustrated through the following accreditations and awards.

ISO9001 – first law firm in the UK to achieve accreditation in 1991

Lexcel – the Law Society's Practice Management Standard

SQM – Specialist Quality Mark of the Legal Services Commission for specialist departments in respect of publicly funded work (legal aid)

Investor in People

Pannone Solicitors was voted 5th in the Sunday Times 100 Best Companies survey 2008 (the highest placed law firm in the history of the survey) and was most recently voted 'Enterprising Law Firm of the Year 2007'.

IT STRATEGY

The expression "Time is Money" is oft overused, but not in the case of a Law Firm, where IT failure can literally bring billing to a halt.

Pannone's server farm is based upon Microsoft 2003/2008. Recent implementation of VMware has greatly assisted with Data Centre administration and power conservation: an important consideration in a City Centre location dependent upon aging electrical infrastructure.

As you might expect with a leading Law Practice, efficient access to data is vitally important. To meet the demanding requirements of Users, Pannone invested in a NetApp Storage Area Network primarily because of the vendor's close association with VMware.

When it comes to its network, Pannone is not inclined to take risk. It does not wish to be an early adopter of technology and nor does it seek to integrate multi-vendor hardware in order to take advantage of specific niche functionality. Instead it has adopted a Cisco network strategy covering all elements of private network connectivity from Switches and Routers through to Firewalls, etc.

Microsoft dominates the desktop both in terms of operating system and generic office applications. Importantly, Pannone operates a sophisticated Case Management System, a strategic application that underpins the efficient management of a wide variety of legal cases ensuring that critical timescales are met: further accentuating the importance of IT and systems availability to the Practice.

As you might expect, Pannone is heavily dependent upon the Internet for email and online research. However, for Pannone the importance of the Internet is increased through support of its Client Portal that is hosted on-site: a tangible measure of the quality by which customers judge the "Pannone Difference".

Add remote 24/7 User access (enabled by 2008 Terminal Services) widely used to support home and out of hours working and the case for industrial strength Internet services is made.

THE CHALLENGE

During late 2008, Pannone's IT Manager, Chris Styles, identified the need to review the capacity and operation of the Law Firm's Internet access circuits; at the time comprising 2 x 2Mbps circuits from Verizon. In particular, he was very concerned about peak time Internet usage that was saturating the links; largely as a result of the extensive use of web casts.

"The Help Desk", according to Mr Styles, "was increasingly receiving calls from Users frustrated about Internet response times: a problem for which we had no 'flick of the switch' resolution. We simply lacked sufficient bandwidth."

Mr Styles' review also raised concern about business continuity for whilst he had implemented an off-site DR strategy, fall back would require IP reconfiguration, which was not ideal as such manual intervention would inevitably delay failover at a time of extreme pressure.

To counter the bandwidth challenge, Chris explored the possibility of new circuits and upgrades and was faced with a 90-day delivery time, which prompted evaluation of alternative suppliers and his approach to Metronet.

THE SOLUTION

"At first I was sceptical about relying upon wireless communications for last-mile delivery of such strategically important circuits; however, when I learnt that Local Authorities depend upon Metronet circuits for CCTV monitoring I was prepared to take a leap of faith despite not having legal reference sites that I would ordinarily wish to consult."

In terms of addressing business continuity concerns, Mr Styles recognised the value of having a diverse DR strategy comprising a triangulated network topology incorporating Metronet wireless circuits unequivocally independent of cable connections.

Initial consultation with Metronet's Network Support Manager, Craig Timmis, introduced a novel approach to resolving issues with dealing with separate IP address ranges (and the associated need for IP reconfiguration in the event of disaster) in that Timmis recommended Pannone adopt and own its own IP range. The result would a) unlock Pannone from its network service suppliers and b) remove the need for complex configuration and reconfiguration when using two separate suppliers.

Craig oversaw the acquisition of Pannone's IP range as part of the project management service.

By bringing Metronet together with Pannone's Firewall supplier, Chris Styles oversaw the implementation of an "Active/Active" network configuration that would combine seamless business continuity failover with continuous availability of all circuits for day-to-day operations.

Metronet delivered a 14Mbps circuit capable of bursting to 25Mbps to accommodate peak-time utilisation, which of course triggered the initial network review. Mr Styles also drew comfort from the seamless upgrade path offered by Metronet that gives him the opportunity to increase bandwidth should he need to do so in the future.

Given the unusual complexity of the network configuration and taking into account the need for multiple supplier coordination, Chris Styles was impressed that the network went live within one month of the initial consultation.

THE BENEFITS

Prior to commissioning the Metronet circuit, Pannone's Help Desk was regularly faced with calls from frustrated Users suffering poor Internet response times during peak times: calls that have now all but disappeared.

With a fully resilient diverse triangulated network topology, Pannone has reinforced its business continuity strategy with a multi-vendor network.

Above all, Chris Styles now values the direct relationship that he has with technical authorities inside a suppliers business with which he can work in partnership to address any issues and concerns that arise from time to time.