

# Managed Metronet MPLS and Secure IP Virtual Private Network

Implementation of a MPLS network can benefit customers with multiple sites in their corporate network or customers who have or plan to have a business critical server located in a data centre. In a non-MPLS multi site corporate network, network management personnel need to administer and monitor very complex VPN setups and firewall rules at each site because sites are communicating across the internet. The more sites and security rules, the more complex and prone to error this infrastructure becomes. An MPLS infrastructure removes the requirement to have firewalls at each site. Instead, a single firewall device can be implemented and managed at the edge of the customer network. MPLS provides the following:

#### Improved Security.

There is only one firewall or pair of firewalls in HA configuration to manage and one point of the corporate network touching the INTERNET. All the other sites sit safely within the MPLS. Changing rules and monitoring traffic is much simpler and less prone to error on one firewall device.

#### Improved Performance.

Intersite data and/or voice traffic is not subject to the ever-present contention in the Internet. Also, bad traffic is blocked at the edge of the corporate network and does not use up precious bandwidth to and from company offices.

#### Reduced Administration burden.

Instead of spending time driving from site to site updating firewalls with VPN and security policies, IT staff can concentrate on strategic mission critical IT projects

#### Reduced cost.

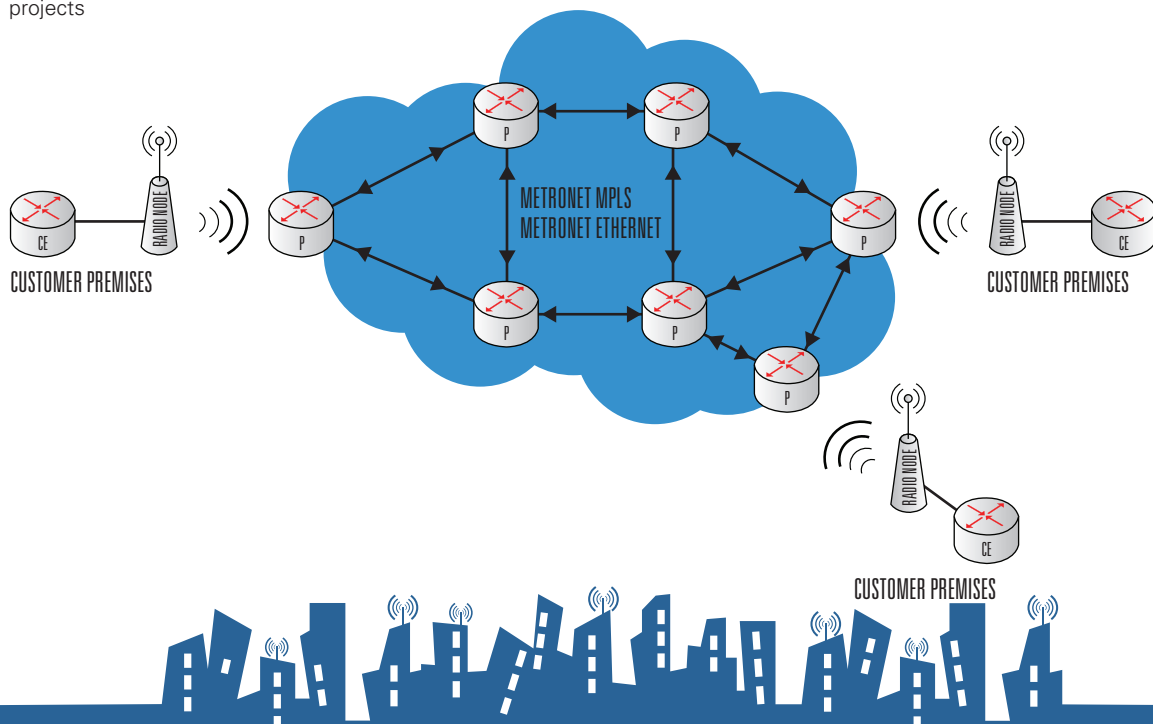
Cost can be reduced in many ways. First of all, only one firewall is required instead of one for each site Metronet's Virtual Firewall can significantly reduce costs compared to purchasing dedicated firewall appliances. Since communication is no longer across the latency laden internet, companies often use MPLS to provide the network infrastructure for Voice over IP and video conferencing, both of which can reduce monthly costs significantly.

#### Heads up on 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.

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*

