

A managed MPLS VPN offers businesses the most flexible and scalable of network infrastructures. Suitable for those requiring a robust network, MPLS is also inherently secure.

Widely adopted by medium and large organisations MPLS is the accepted communications technology to deliver convergence across shared network infrastructures - including multisite, remote working environment and where extranet access is required.

MPLS provides a network independent of access technologies and enables organisations to incorporate existing and legacy infrastructure into their solution. For many organisations looking to consolidate their infrastructure, a wide area network based on MPLS offers the ability to consolidate network suppliers whilst benefiting from a more advanced infrastructure.

Business Flexibility

Businesses require a network that enables them to change as their business changes and IT requirements evolve. With an MPLS VPN it is relatively simple to add new sites and change the business access bandwidth making it easier to adapt the network when adding new offices or in the event of merger and acquisition activity.

Consolidation

Because integration of legacy infrastructure is a common requirement a managed MPLS solution is easier to manage. It allows for standardisation of the support infrastructure into one network, reducing the number of network suppliers required as well as allowing for consolidation of applications into one location.



Cost Efficiency

Compared to traditional ATM, Frame Relay and pure Leased Line networks, MPLS offers a highly cost-effective wide area network. As a managed network administration is simplified further enhancing operational efficiency.

“We wanted one network covering all of our branches that would encompass all of our communications requirements”.

Christopher Fullalove, IT Director, Caffyns.

Service Topologies

Any to Any

By default MPLS provides any-to-any connectivity where all locations can communicate with one another. This is useful when an organisation's IT infrastructure is not centralised in any one particular location and data needs to be communicated across different sites.

Hub and Spoke

Classic MPLS-VPN solutions mirror the structure of many company's IT architectures where applications have been centralised - often at the headquarters.

At the primary site the access circuit is likely to have greater bandwidth demands than the remote sites as more bandwidth will be aggregated across it.

NetServices manage all network connectivity and circuit-terminating CPE (Customer Premises Equipment) hardware located at all client sites.

Remote user sites are mapped within the NetServices core network, facilitating connectivity within the same virtual private network.

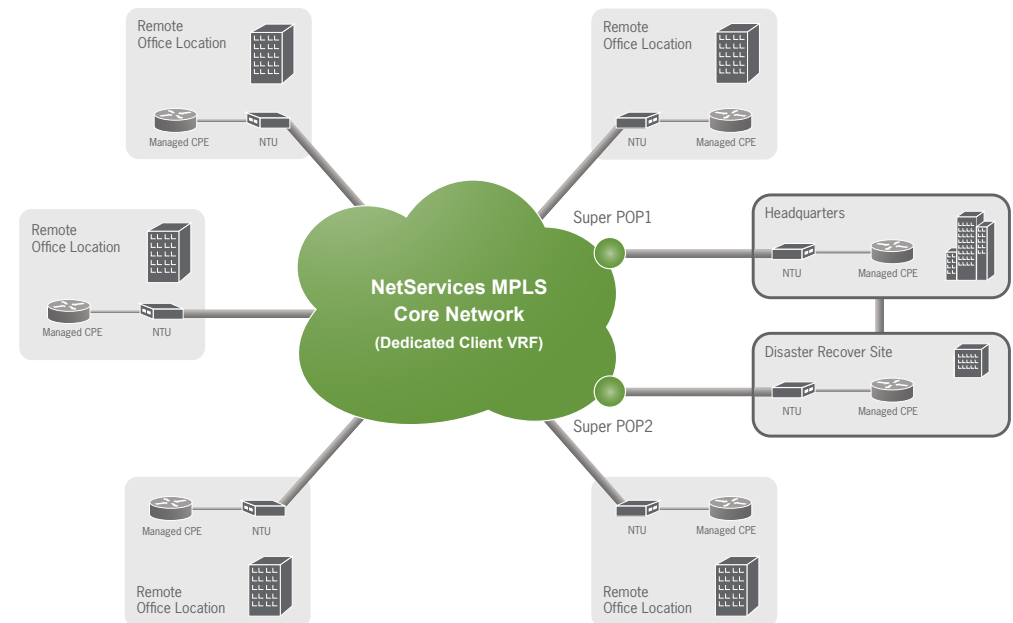
Disaster Recovery and Hub Resilience

For all IT-centric organisations with a large reliance on the WAN it is imperative that mission critical sites have a second diverse connection. This can terminate into the NetServices core network at a different access point, at a different Super POP to that of the primary access circuit. This also protects customers against outage of any single Super POP.

Should greater resilience be required into a headquarters site, the infrastructure can be designed to enable business continuity in the event of a disaster at their main site.

Many organisations create a disaster recovery (DR) site where IT applications are duplicated and data is mirrored either synchronously or asynchronously between the main and DR sites. This requirement can be supported within MPLS-VPN solutions.

A typical example is detailed below where a DR site has been configured with direct connectivity between the DR and HQ site to enable data replication to occur in the background to the everyday data traffic across the WAN. Should the primary site become unavailable for any reason, VPN traffic is routed directly to the DR site.



Convergence

Converged networks are being implemented at an unrelenting pace for businesses of all sizes and in all economic sectors so that organisations can realise the efficiencies of having a single networking infrastructure.

A converged network is a pre-requisite for voice traffic, however it may be equally important for other core business applications; implementation of new applications is becoming a core reason for the growth in converged networks.

Quality of Service

Quality of Service (QoS) is an essential ingredient of a converged network as this is what determines the networks' ability to deliver mission-critical or delay sensitive applications, during periods of congestion.

QoS addresses the two fundamental requirements for applications that run on a network: predictable performance and policy implementation. QoS capabilities allow users to prioritise service classes, manage bandwidth and avoid congestion.

The classes of service that are deployed are as follows:

IP Precedence	Class of Service	Typical use
5	Platinum	Multi-media applications such as Voice and Video only.
3	Gold	Real-time and mission critical data applications such as Voice, Video, SAP and Peoplesoft etc.
1	Silver	Mission critical data applications such as Citrix, Peoplesoft, Oracle and Telnet.
0	Bronze	Best effort data applications such as Internet, Email and FTP.

The NetServices network consists of a QoS enabled core MPLS network that is designed to optimise the bandwidth, delay, jitter and packet loss metrics ensuring end-to-end Quality of Service is delivered - from the remote customer LAN to the hub site.

Class of Service Deployments

With a fully managed solution NetServices has total control of end-to-end connectivity in order to guarantee quality of service. The network partitions traffic into four unique classes and then applies QoS accordingly.

Access Technologies

QoS can be applied to the following tail access circuit types:

- National Ethernet
- Local Ethernet
- Leased Lines
- QoS DSL

Traffic Prioritisation

NetServices deploy low latency queuing (LLQ) in the outbound direction of network interfaces. This ensures that a fixed portion of bandwidth is reserved for prioritised traffic at all times, in effect

providing a 'bus lane' for prioritised traffic; all non-priority services are given weightings for separate queues. The managed solution enables clients to choose a queue size per required class of service.

What you get with an MPLS VPN

Security

A private MPLS network fully segments the customer traffic across the core network. The network is completely isolated with no component being accessible by, or visible to, unauthorised parties or to the public internet (unless this is a requirement). This negates the need for firewall hardware at each site.

Resilience

The service to remote sites can be maintained even when the primary circuit has failed. Resilience levels can be selected on a per site basis as the client chooses from a low cost ISDN or ADSL back-up service through to higher bandwidth connections based on Ethernet or Leased Lines.

Performance

Increased performance in comparison to VPNs that utilise the public internet, supported by end to end QoS service level agreements (SLAs). MPLS VPN offers a range of optional value-add services including secure centralised internet access, remote end user access and extranet connectivity via IPsec.

Solution Delivery and Support

Pre-Sales Consultation

- Understand related business objectives
- Assess legacy technology and current and future application requirements
- Qualify technical requirements and pre-requisites

Network Design

- Assess technologies, core network and carrier options available for suitability to identified requirements
- Propose network utilising on best bit carrier and technology options
- Design a commercially practical network to meet agreed requirements

Implementation

- Implementation is co-ordinated through our Project Office, managed with PRINCE II qualified project managers
- Manage all carrier and suppliers involved in the solution

Support

- 24 x 7 Service Desk manage all customer queries, whether commercial or technical, until satisfactory resolution of the issue
- Issues allocated within NetServices to ensure correct ownership and managed by Service Desk
- Client Support Plans (CSPs) supplement contractual agreements providing customers with clear operational service management documentation

Options

Many organisations create a Disaster Recovery (DR) site where IT applications are duplicated and data is mirrored either synchronously or asynchronously between the main and DR sites.

Internet breakout from the VPN is available from the hub or centrally from the 'cloud' enabling the centralisation of internet connectivity and security policy.

Managed Firewall services for Managed MPLS VPN solutions can be hosted either within NetServices core or at the client primary site.

Load sharing options are available to sites where resilience has been provisioned.

NetServices can configure High Availability Resilient Circuits to mitigate risk of the failure of the primary access circuit using local access diversity if at all possible.

Hot Standby Routing Protocol can be used to offer sites both hardware and circuit resilience in the event of a circuit or hardware failure.

ISDN Backup provides a cost effective backup service utilising the legacy network with a dial up circuit charge. Site access resilience is provided by ISDN terminating into the client's VRF within the NetServices core network.

Load Sharing options are available to utilise all of the resiliently provided bandwidth connectivity to sites. Geographical and Host load sharing options are available.