

Product Name:

MPLS VPN

Availability:

PAETEC's MPLS VPN is now available in 151 markets including the US, US territories, and Canada

Ideal Customer Profile:

Primary customers included corporations that currently use frame relay, ATM, or leased lines to link remote branches, telecommuters, and/or mobile workers to their corporate network.

CPE Requirements:

The customer should consult an authorized PAETEC representative to ensure 100% compliance and operability. Customers must maintain a PAETEC-approved CPE device (i.e. ADTRAN or Cisco CPE)

MPLS VPN | In Brief

Product Description

PAETEC provides your company with a fully meshed, secure, and reliable network through Multi-Protocol Label Switching (MPLS). Your company's data information travels through PAETEC's private, national IP network, enhancing connections among your internal and external customers. MPLS VPN with QoS provides the ability to prioritize data and delivery to maximize available bandwidth with limited expenditures. In addition, MPLS VPN is available anywhere in the United States and across more than 50 countries internationally.

Product Capabilities

Private, virtual paths – PAETEC's private IP network ensures privacy and security as your data travels on virtual paths separate from other customers' applications.

Fully meshed network – All locations are automatically interconnected, allowing site-to-site communications without built-in network connections.

Quality of Service (QoS) – Time sensitive applications are granted precedence over less time sensitive applications.

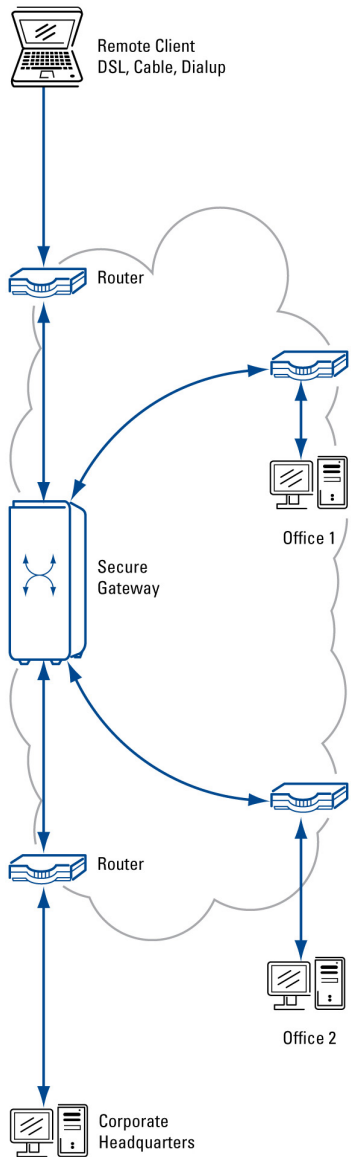
Self-healing network – In the event of an outage, data is automatically rerouted to another path to prevent delays and congestion.

Remote access – Employees are able to securely access the corporate network anywhere, anytime.

Product Requirements

PAETEC requires that 60% of the customer's locations must be directly connected to PAETEC's network (on-net).

PAETEC requires that the customer's hub must be directly connected to PAETEC's network (on-net).



Application One

The United Bank of Rochester, which supports nine local offices, currently routes their data transmissions through a local carrier's frame relay network. The company would like to expand by opening three more locations in the Rochester area. They have decided to implement PAETEC's innovative approach to business infrastructure and use MPLS VPN. Instead of physically connecting the new site to each of the existing nine locations, PAETEC can enable site-to-site connections using MPLS VPN. Each site's data applications are routed through PAETEC's private network, and then distributed to the appropriate destinations. By virtually linking all locations, future IP driven applications, such as Voice over IP (VoIP), can travel over the company's existing MPLS network.

Application Two

Sales executives, employed at Thomas Telecom Corporation, rely heavily on communication between their twelve national, off-site locations to the corporate headquarters. In order to keep sensitive data secure from competitors and network hackers, PAETEC's MPLS VPN was implemented. Between Thomas Telecom Corporation's business sites, data travels across PAETEC's private network. IP addresses are not visible or recognized on the public Internet, allowing a secure connection between multiple sites. From home or hotel locations, sales executives simply access the Thomas Telecom Corporation's network, using their secure ID. Data is then transferred to its final destination, within their private network, through a secure, encrypted tunnel on the public Internet. Regardless of physical location, employees are continuously conducting secure and private business communications.

Application Three

At Fairport Financials, a sizable corporation with five regional business offices, data applications were previously routed on a frame relay network. Time-sensitive applications were not delivered efficiently, and their network was congested due to bandwidth constraints. Since then, they have implemented PAETEC's MPLS VPN. Data applications are prioritized according to time-sensitivity, utilizing PAETEC's Quality of Service (QoS) control. Time-sensitive applications, which require all components of the application to be delivered simultaneously (i.e. presentations utilizing audio and visual elements), take precedence over other, less critical applications. QoS labels and filters mission critical applications according to their elements, granting precedence to time-sensitive transfers. The data applications are streamlined through the network facilitating full port speed for each application and limiting bandwidth constraints.