PAETEC

MPLS VIRTUAL PRIVATE NETWORK SERVICE

1. DESCRIPTION. This service description sets forth the entire Preferred Advantage[SM] Multiprotocol Label Switching Site to Site IP Virtual Private Network Service offering. PAETEC reserves the right to make enhancements to the Service and shall advise Customer of any additional features.

PAETEC's Preferred Advantage[SM] Multiprotocol Label Switching Site to Site IP Virtual Private Network ("MPLS VPN") Service is a network-based IP VPN available across PAETEC's IP/MPLS backbone. This solution provides Customer with a secure IP VPN solution with any-to-any intranet connectivity and a private means by which to connect its enterprise sites. In addition, Customer can purchase optional services, such as VPN Internet Access with Network-based Firewall, all on the same underlying network infrastructure.

A. Primary Service Components. The primary service components for the Services are as follows:

(i) MPLS VPN Port. A Port is the physical entrance to the PAETEC network. PAETEC will charge Customer a Non-Recurring Charge ("NRC") and a Monthly Recurring Charge (MRC) for each Services Port, including all sub elements or configurable attributes to the Port. The Network Design Document and Port Order will specify the sub-elements or configurable attributes to the Port (e.g. Port speed, routing protocol, IP Addressing). Port options available are:

a. Dedicated VPN. Dedicated VPN provides a physical port connected directly to the PAETEC VPN network, which allows connectivity to all other Customer sites on the VPN and the Internet/Managed Firewall service if purchased in addition.

b. Dynamic Integrated Access. VPN Access may be ordered as an option on Dynamic Integrated Access in place of Internet access.

(ii) Dedicated VPN Local Access. Dedicated local access is required for the Dedicated VPN ports. If Dedicated VPN Port is selected, Customer may purchase PAETEC-provided local access facilities or Customer may provide its own local access facilities. There will be a NRC and MRC for each local access loop provided by PAETEC. If Customer purchases VPN service as part of Dynamic Integrated Access, Local Access is included as part of the service and the monthly recurring charges are included in the charges for Dynamic Integrated Access.

(iii) IP Addresses. Customer may opt to use private IP space or PAETEC assigned public IP space. If selected, PAETEC grants Customer a license to use the public network IP addresses PAETEC provides Customer during the term of the Agreement. However, public network IP addresses provided by PAETEC shall remain at all times the property of PAETEC and shall be non-transferable. Customer has no right to such network IP addresses upon expiration or termination of the Agreement. Customer agrees that this license is revocable, and is for non-portable network address space. PAETEC may in its sole discretion renumber public network IP addresses as necessary after giving Customer notice.

B. Customer Premises Equipment ("CPE"). CPE is required for the Services. Customer may elect to purchase CPE from PAETEC as part of the optional Managed Services (described below) or provide its own CPE. CPE includes, but is not limited to the following:

(i) Routers. Unless Customer has separately contracted with PAETEC to provide Managed Services, Customer is fully responsible for the router, including configuration, maintenance, and management. In addition, if Customer elects not to obtain Managed Services, Customer must furnish the necessary ancillary equipment (cables, routing software, etc.) to ensure interoperability with the Services.

C. Optional Services. PAETEC provides optional services that Customer may purchase as part of its Site to Site VPN solution. Optional Services have both a monthly charge and a non-recurring charge. The following Optional Services are available:

(i) VPN Internet Access with Managed Firewall. Regional gateways provide secure access from the Customer's VPN network to the Internet. Each site in Customer's MPLS VPN will receive Internet access secured by a state-full inspection firewall located within PAETEC's network. VPN Internet Access may be purchased in bandwidth increments to meet Customer's requirements. Two Managed Firewall options are available:

a. **Standard.** This option provides a pre-configured policy rule set which trusts all internal traffic, but blocks all externally initiated traffic. This policy is known as "Trust Inside." In this scenario, it is assumed that the most significant threats will come from outside the Customer enterprise network, and the emphasis of the policy will be keeping outsiders from getting in. This type of stance is implemented by defining a firewall rule set that permits all connections, which are initiated from the inside, but blocks connections initiated from the outside. If any customized rules are required, the Customer must upgrade to the Enhanced option.

b. **Enhanced**. Provides a completely customizable policy rule set, which is defined by the Customer upon order initiation. Customer is responsible for defining all rules for their network and providing written documentation for initial configuration and any changes.

(ii) **Remote Access Service ("RAS").** RAS allows Customer's employees or users to obtain remote access to the Services through the use of a VPN client. This client is installed on an employee's or user's laptop. The client, when open, builds an IP Sec tunnel back to a Remote Access gateway to enable employees or users to run corporate applications while away from the office. A Web-based administration tool allows the Customer administrator to manage it's remote access user needs to easily add and delete users as required as well as creating user and usage reports. Two feature plans are available fore each remote user.

(a) **RAVPN.** Provides an IPSEC client that may be used with either Broadband or Dial-up access for individual remote users. Customer is required to purchase broadband Internet access, either from PAETEC or another provider separately and is not included in the monthly recurring charge. Broadband connectivity is provided on an unlimited basis. If Dial-up access is desired, the Single Click connect client is required and provided. All Dial-up charges, including domestic local, toll-free, and international roaming are charged at hourly rates.

(b) **RAVPN150.** Provides the same features and functionality as RAVPN described above except that 150 hours per month of local dial-up access is included in the monthly recurring charge for each remote user. If an individual user exceeds the 150 hours of dial-up connectivity, each hour over the limit will be charged an overage fee. International dial is not included in the 150 hours and is charged an hourly rate.

(iii) **Off-net Tunnel.** Off-net Internet Protocol Security ("IPSec") or GRE Tunnel is for customers who have sites outside PAETEC's footprint. The Off-net Tunnel provides connectivity from the Internet of an IPSec or GRE tunnel terminated to the Customer MPLS VPN on the PAETEC network. With this option, Customer is responsible for securing Internet access at the off-net location and configuring their hardware to terminate an IPSec or GRE tunnel to the PAETEC MPLS VPN network with configuration information provided by PAETEC.

(iv) **Managed Services.** PAETEC Managed Services provides a PAETEC-owned or leased and managed router to be used with the Dedicated VPN Access. The standard CPE option (Adtran) is the only option available for Dedicated VPN Access. Managed Service requires installation of certain equipment at your premises. Customer Premises Equipment ("CPE") provided by PAETEC remains the property of PAETEC. CPE may only be installed, opened and maintained by an authorized PAETEC representative. PAETEC will work with Customer to find a mutually agreeable time, but PAETEC has the right to take any action in connection with the equipment at any time for any reason. Customer must take precautions to protect such equipment and will be liable for any damage to the equipment subject to normal wear and tear. Customer may use PAETEC provided equipment only for PAETEC Managed Service. PAETEC has the unmitigated right to unrestricted access to recover any PAETEC-owned or leased CPE within ten (10) days of service termination. If Customer does not provide PAETEC unrestricted access to recover the equipment in a timely fashion, Customer agrees to immediately pay PAETEC the original cost of the CPE. If a PBX is involved, Customer must arrange to have its PBX vendor on-site during installation of service.

The PAETEC demarcation for Managed Services Internet is the 10/100 base T router port. Customer is responsible for providing a reasonably accessible grounded 90 to 130 VAC power outlet that will meet the power requirements of the PAETEC provider router and other CPE. Customer must promptly notify PAETEC of any problems with the router, and must not voluntarily power down the router. PAETEC may assess a service charge to restore service in the event the router is subject to a loss of power that Customer could have reasonably prevented. All PAETEC inside wiring work is guaranteed for 60 days from service installation. Customer is responsible for installation and maintenance of all LAN/data related wiring. Customer will be charged a dispatch cancellation fee unless it cancels its original order within four hours of placing the order.

(v) **Local Access.** If required, Customer appoints PAETEC as its agent for the purpose of arranging for interconnection from PAETEC Points-of-Presence to Customer's facilities ("Local Access") for a circuit-based product. Customer

understands that PAETEC may rely on a third party for installation of Local Access service. PAETEC is not responsible if Local Access service is not available on the requested Service Activation Date or for service issues on Customer's side of the demarcation point.

(vi) Demarc Extension. For specific voice and data services, upon Customer's request, PAETEC will extend the Local Access Loop for up to 25 feet by providing a cross-connect from the Demarc to a Customer-provided industry standard distribution panel or CSU/DSU located in the same room. Charges for this cross-connect will be on a time and material(s) basis. Final charges will not be determined until work is completed and will be billed to Customer within two billing cycles of the completed work.

2. CUSTOMER ROLES AND RESPONSIBILITIES.

A. Review and approve, by signature, Customer Network Design that provides to PAETEC with the Customer's desired network configuration and Managed Firewall policy (if ordered). Customer Network Design will be gathered after the Agreement has been signed by both parties and before the order is processed.

B. Provide reasonable physical access for PAETEC technicians to service the PAETEC-owned or leased equipment and infrastructure on each premise if provided.

C. Install and maintain LAN infrastructure at each Customer location.

D. Maintain servers and workstations for Customer purposes.

E. Inform PAETEC of any internal changes that may affect the Services PAETEC provides.

3. ACCEPTABLE USE.

A. Revocable, Non-portable License. PAETEC grants Customer a license to use the public network IP addresses PAETEC provides Customer during the term of the Agreement. However, public network IP addresses provided by PAETEC shall remain at all times the property of PAETEC and shall be non-transferable. Customer has no right to such network IP addresses upon expiration or termination of the Agreement. Customer agrees that this license is revocable, and is for non-portable network address space. PAETEC may in its sole discretion renumber public Network IP addresses as necessary after giving Customer notice.

B. Acceptable Use Policy. Internet access services are subject to the PAETEC Acceptable Use Policy ("AUP"), which is posted at www.mcleodusa.com/SiteInformation/AcceptableUse.do. Customer agrees that its failure to abide by the AUP can be a material breach of this Agreement. PAETEC may revise the AUP from time to time in its sole discretion without notice. PAETEC's AUP, including any amendments, will be effective upon posting.

4. SERVICE LEVEL AGREEMENTS. PAETEC MPLS VPN and Managed MPLS VPN are backed by the following service level agreement ("SLA") guarantees.

A. Service Delivery Interval for DS-1 Based Services. PAETEC will install service by the Firm Order Commitment date or within 90 calendar days as measured from the date on which Customer has signed an order and submitted all required information (including signed Customer Network Design described above) to PAETEC to provision services to complete the original order. Calculation of the service installation interval will exclude delays caused by Customer, including but not limited to, Customer Premises Equipment ("CPE") issues, order supplementation or modification and limitations on premises access. The Service Delivery Interval guarantee does not include orders delayed beyond the reasonable control of PAETEC such as, but not limited to, modification of the original order by Customer, a third-party act or omission; or the unavailability or failure of facilities or equipment available to serve Customer's location. If the Service Delivery Interval guarantee is not met, Customer will receive a credit of 1/30th of the impacted port and local loop's monthly recurring charge ("MRC") per day over the stated interval. Limits on the credit and the reporting procedures are detailed below.

B. Restore Time. PAETEC guarantees the following average service restoration intervals for each circuit measured on a per circuit, per outage occurrence:

MPLS VPN	
DS-1	**4 hours**
DS-3	**2 hours**

The restoration interval will begin when Customer provides notice to PAETEC of the outage in accordance with outage notification procedures and PAETEC opens a trouble ticket. Customer's wait time, including but not limited to waiting on Customer response,

facilities access restrictions, or response delays caused by inaccurate contact information will be subtracted from the restore time calculation. The PAETEC restore guarantee does not include outages found to the result of problems with CPE or LAN equipment owned by Customer, scheduled maintenance events, outages or disruptions caused by Customer, interconnections to or from and connectivity with other ISP networks, and force majeure events. For purposes of this SLA, scheduled maintenance events include any maintenance that supports Customer's network or services, for which (i) Customer is notified at least 48 hours in advance, or (ii) that is performed during a standard maintenance window Monday through Friday from 12:00 a.m. CST to 6:00 a.m. CST. If the restore time guarantee is not met on a per outage basis, Customer will receive a credit of 1/30th of the port and local loop monthly recurring charge ("MRC"). Limits on the credit and the reporting procedures are detailed below.

C. **Chronic Circuit Outages.** If Customer receives a credit under the Restore Time SLA three times in a 30-day period, PAETEC will have a 15-day repair period after the third incident to remedy the chronic problem. If there are any additional failures within a 15-day observation period after the 15-day repair period then Customer may terminate or disconnect the impacted circuit without incurring early termination fees. Customer must file a claim for early termination in writing within 14 calendar days after the failure in the 15-day observation period.

D. Network Availability Guarantee. The PAETEC MPLS VPN service is guaranteed to be available and capable of passing Customer's traffic 99.99% of the time, averaged over a calendar month. The PAETEC Network Availability guarantee does not include the outages found to be caused by CPE (router or switch) or Local Area Network ("LAN") owned by Customer, scheduled maintenance events, Customer-caused outages or disruptions, interconnections to or from and connectivity within other Internet Service Provider ("ISP") networks, and force majeure events. If the Network Availability guarantee is not met in a calendar month, Customer will receive a credit of 1/30th of the monthly recurring charges ("MRC") for that impacted port and local loop. Limits on the credit and the reporting procedures are detailed below.

E. Latency Guarantee. The PAETEC MPLS VPN service is guaranteed to have an average round trip transit time within the PAETEC IP backbone network of 55 Milliseconds (ms) or less as averaged over a calendar month, measured between PAETEC Core Network Nodes. PAETEC maintained and operated ICMP message generators and associated tools will be used to record Core-to-Core Network Latency. The PAETEC Latency Guarantee for MPLS VPN does not include the local access circuit (*e.g.*, local loop), CPE or LAN owned by Customer, scheduled maintenance events, outages or disruptions caused by the Customer, interconnections to or from and connectivity with other ISP networks, and force majeure events. PAETEC will total the results of each ICMP message response, excluding any failures due to Maintenance, and divide by the message count to produce an Average Core to Core Network Latency. If the Latency Guarantee is not met in a calendar month, Customer will receive a credit of 1/30th of the monthly recurring charges ("MRC") per impacted port and local loop for that month. Limits on the credit and the reporting procedures are detailed below.

F. Packet Delivery Guarantee. The PAETEC MPLS VPN Network, as defined in this section, is guaranteed to deliver 99.5% of IP packets averaged over a calendar month. The PAETEC IP Network includes Customer's access port (the port on the PAETEC router upon which the Customer's circuit terminates), and the PAETEC IP backbone network. The PAETEC IP backbone network includes PAETEC-owned or leased and controlled routers and circuits (including any transit connections). The PAETEC Packet Delivery Availability guarantee does not include outages found to be caused by the Local Access loop, Customer-owned CPE (router or PBX/Key System) or LAN, scheduled maintenance events, Customer-caused outages or disruptions, interconnections to or from and connectivity within other Internet Service Provider ("ISP") networks, and force majeure events. If the Packet Delivery Guarantee is not met in a calendar month, Customer will receive a credit of 1/30th of the monthly recurring charge ("MRC") including additional lines after all applicable discounts. Limits on the credit and the reporting procedures are detailed below.

G. Jitter Guarantee. The PAETEC MPLS VPN backbone network is guaranteed to have the deviation of packet transit time, within the PAETEC IP backbone network, of 2 Milliseconds (ms) or less as averaged over a calendar month, measured between PAETEC Core to Core Network Nodes for VPN traffic. For Internet traffic the guarantee is 3 ms. For Dynamic Integrated Access VOIP traffic, the guarantee is 1.5 ms. PAETEC maintained and operated ICMP message generators and associated tools will be used to record Core-to-Core Network Jitter. The PAETEC Jitter Guarantee does not include the Local Access loop, Customer-owned CPE or LAN, scheduled maintenance events, Customer-caused outages or disruptions, interconnections to or from and connectivity with other ISP networks, and force majeure events. If the Jitter Guarantee is not met in a calendar month, Customer will receive a credit of 1/30th of the monthly recurring charge (MRC) including additional lines after all applicable discounts. Limits on the credit and the reporting procedures are detailed below.

5. SLA CREDITS. Total credits under the Service Level Agreement ("SLA") are limited to, unless otherwise required by law, the monthly recurring charge for the affected service for the month in which the service does not meet the guarantees. The service credits provided under SLAs are Customer's sole remedy unless otherwise required by law when PAETEC fails to meet a SLA. Customer must make a Performance Claim in writing no more than 14 days after the end of the outage event for which Customer claims that PAETEC failed to meet an SLA, or Customer waives its right to make a Performance Claim for that period. For purpose

of the SLA, a "Performance Claim" is a written notice sent to the designated representative of PAETEC advising of the perceived violation of the SLA. Only one SLA parameter violation may be claimed per event. Customer must be in good standing with PAETEC with regard to account receivables in order to submit a performance claim.

6. SERVICES TERM. Customer desires to obtain VPN Service under the terms and conditions of the Agreement for a term as defined in the Agreement. Customer agrees that all terms and conditions of the Agreement and this service description shall remain effective until the expiration of the Customer's term. Termination charges shall be assessed according with the terms of the Agreement and may also include any Local Access charges assessed by the Local Access provider.

7. OTHER SERVICES/CUSTOMER SPECIFIC TERMS AND CONDITIONS.

A. Disclaimer of Warranties. The MPLS VPN service should be regarded as one tool that can be used as part of Customer's overall security strategy, but not as a total solution. As with all security systems, Customer's system may have potential security vulnerabilities, even with the IP VPN, including the vulnerability of the system to access by a person(s) which exceeds the authority granted to such person(s). PAETEC does not guarantee that the IP VPN will eliminate all risk or prevent damage from one or more network security breaches.

All services and equipment provided hereunder are on an "as is" basis. Notwithstanding anything stated herein or elsewhere, PAETEC makes no express or implied warranties of title, non-infringement, merchantability or fitness for a particular purpose. Under no circumstances and under no legal theory (tort, contract, statutory or otherwise) shall PAETEC its agents, affiliates, licensors, subcontractors or vendors be liable to Customer or any other person for any direct, indirect, incidental, special, punitive or consequential damages of any character that arise from Customer's or any users' use of or inability to use the IP VPN Service, including, but not limited to, an damages arising from or relating to loss or compromise of stored data or communications, unauthorized intrusion of Customer's computer network.

B. Firewall Disclaimer. The parties hereby further agree to the following terms if Managed Firewall Service is ordered. The PAETEC Managed Firewall solution is designed to prevent outsiders from gaining access to private corporate information and will provide an effective method of monitoring and limiting access. However, the service is characterized as "best effort" based on the Customer-defined policies. It may not prevent some instances of dedicated fraudsters from breaking their way in, or an employee from gaining unauthorized access to the Internet or to confidential information stored on the corporate network.

Customer should ensure that any confidential or valuable corporate data is not accessible via the Internet. PAETEC will not accept liability for any losses or damage to Customer's business or data that arise as a result of the Firewall not preventing unauthorized access. The PAETEC Managed Firewall service does provide a high standard of protection and service, but no system can claim to be completely secure.

8. SERVICE SUSPENSION AND MAINTENANCE. PAETEC may perform scheduled network maintenance as stated in Section 4(B). PAETEC may also perform unscheduled network maintenance that may result in a brief service interruption. PAETEC will give advance notification of unscheduled interruptions whenever reasonably possible. Any PAETEC liability resulting from an unscheduled Service interruption will be determined in accordance with the governing Agreement.