AN XO™ WHITE PAPER

XO™ MultiTransport Networking Service Layer 2 VPN Solutions

Table of Contents

Introduction

Historically, a corporation which needed to provide Internet, intranet, extranet or other wide-area data connectivity between its locations has been required to buy multiple networking services from service providers. Even worse, not all service providers may have offered all the services needed by company, so the company was forced to buy a single service from multiple service providers and keep those services “glued together to meet the company’s data networking needs. There is no “economy of scale” (that’s to say, no savings) in having multiple network services provided by many vendors using multiple access circuits to each corporate site. Additionally, an IT organization’s operating expense for these multiple connections is substantial. Each vendor adds incremental operational expenses to the company’s IT group because there are multiple vendors to deal with, multiple vendors to open trouble tickets with, and multiple vendors whose performance needs to be monitored. Finally, the IT organization has to take all these different parts and ensure that the end-to-end service to the company’s users is easy to utilize.

XO™ MultiTransport Networking Service (MTNS) simplifies this complicated operational and expensive headache by offering multiple services across a single access circuit to each of the company’s sites. This allows economies of scale by reducing direct costs to the company (both in telephony expense and internal operating expense) and indirect costs by simplifying the job of the IT group. Additionally, XO MTNS service provides future growth and compatibility with applications needing private IP connectivity, IP Class-of-Service (CoS), and interworking between different types of Layer-2 connections (such as ATM and Ethernet, for example).

XO MTNS product is provided across the XO Multiprotocol Label Switching (MPLS)-enabled OC-192 IP network which uses clear-channel 10Gb circuits, dual OC-3c to OC-48c SONET uplinks from each market, and state- of-the-art IP / MPLS routers in redundant configurations to ensure the highest levels of availability and throughput while minimizing latency and jitter.

This white paper gives an overview of XO MTNS product and shows examples of typical applications for customers.

MTNS Product Overview

XO MTNS will be fully implemented in several phases. Phase 1 (now available) provides Layer-2 VPN connectivity over Frame Relay and Ethernet. Future phases will provide Layer-3 private IP connectivity, full interoperability between different Layer-2 transport types (such as ATM and Ethernet), and both Layer-2 and Layer-3 Quality of Service capabilities. As those future enhancements are introduced, each additional capability will be immediately available to all existing MTNS customers.

The following port speeds are supported for MTNS Layer-2 VPNs:

- Frame Relay:
  - fractional DS-1 (64Kb, 128Kb, 256Kb, 384Kb, 512Kb, 768Kb)
  - full DS-1 (1.536Mb)
  - fractional DS-3 (6Mb, 9Mb, 12Mb, 18Mb)
  - full DS-3 (45Mb)
  - full OC-3c (155Mb)
  - full OC-12c (622Mb)
- Ethernet:
  - full Ethernet (10Mb)
  - full Fast Ethernet (100Gb)
  - full Gigabit Ethernet (1000Mb)

A variety of Frame Relay connectivity options are supported, depending on the customer's requirements, including:

- hub-and-spoke connectivity to support data flows from remote sites to a central location
- partial-mesh connectivity to allow some direct site-to-site connectivity as well as connectivity to a central hub (note: the customer can choose the level of "meshiness" desired)
- full-mesh connectivity for direct any-site to any-site connectivity.

Two Ethernet connectivity options are supported:

- direct port-to-port connections between two sites
- use of VLANs (802.1Q) to provide direct Ethernet connectivity between multiple locations

On any number of a customer's MTNS connections, Dedicated Internet Access (DIA) can be provided simultaneously[1] with private data connectivity. Most customers prefer to only have one or two MTNS connections configured with DIA because they use firewall or other filtering software and wish to limit expenses associated with firewalls, but there is no technical limitation to providing DIA on all of a customer's MTNS connections.

A map of the XO MPLS-enabled IP Network is shown in Figure 1.

[1] As detailed later, this capability is supported for all Frame and Ethernet VLAN customers. Simultaneous Internet access is not supported for Ethernet Port customers.

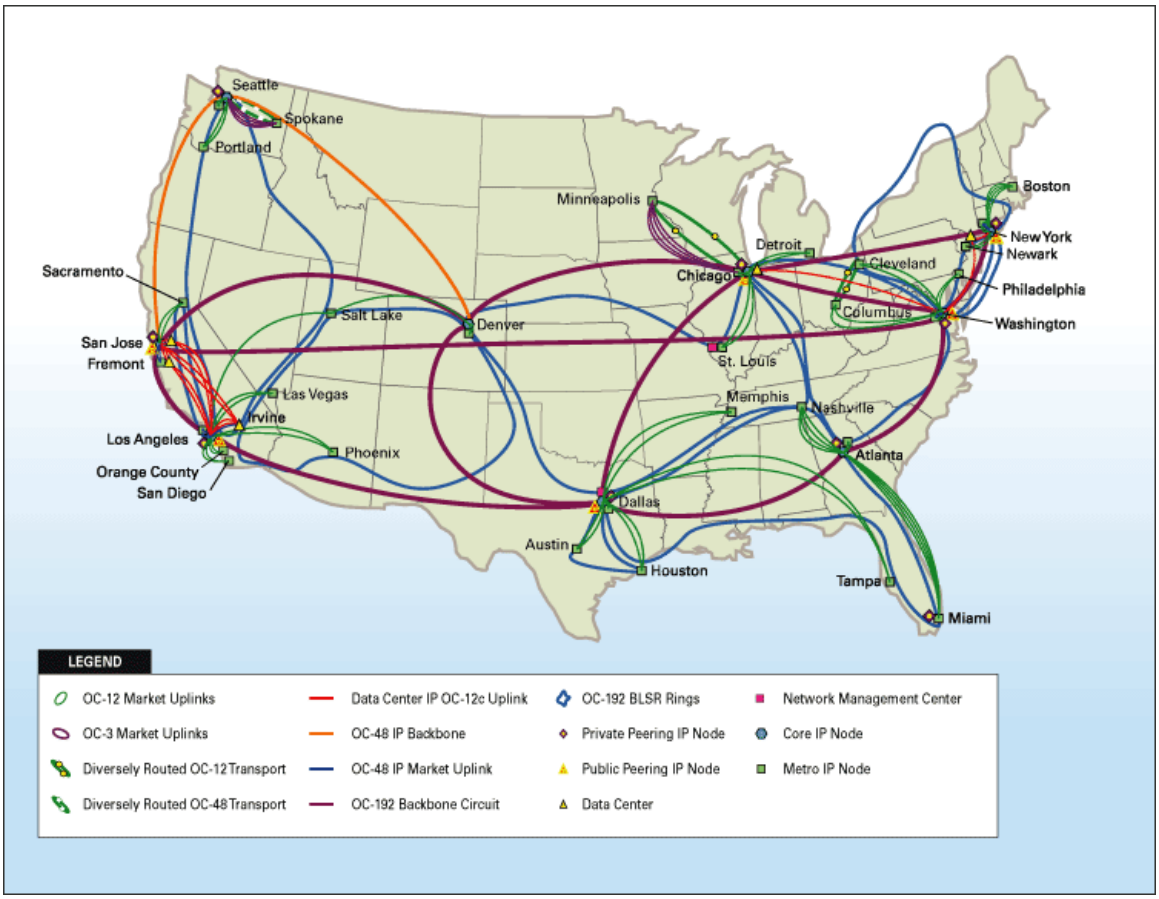

Figure 1: XO MPLS-enabled OC-192 IP Network

Layer 2 connectivity within MTNS is based on technology from the *Martini* IETF draft standard. Simply put the *Martini* draft standard details how customer traffic received across Frame Relay or Ethernet interfaces is transported using MPLS across an IP network. Transport of customer traffic using the *Martini* draft standard is a well-known trouble-free method of providing secure Layer-2 connectivity across a MPLS network.

MPLS Overview

Multiprotocol Label Switching (MPLS) is a technology whose functionality includes Traffic Engineering, VPNs, and Layer-2 transport across a Layer-3 network. Originally MPLS was developed to accelerate packet forwarding within Layer-3 networks; this initial justification has been negated through use of hardware-based packet forwarding in IP routers. Today, MPLS is primarily used to add enhanced functionality to IP networks.

In an MPLS network, a Label Edge Router (LER) assigns labels to incoming data packets. Label Switching Routers (LSRs) are used within the MPLS network to forward packets along Label Switched Paths (LSPs). At each hop, the LSR examines the label and determines where to forward the packet next. Each LSR also strips the label and replaces it to tell the next hop how to forward that packet. A simplified diagram of this is shown in Figure 2.

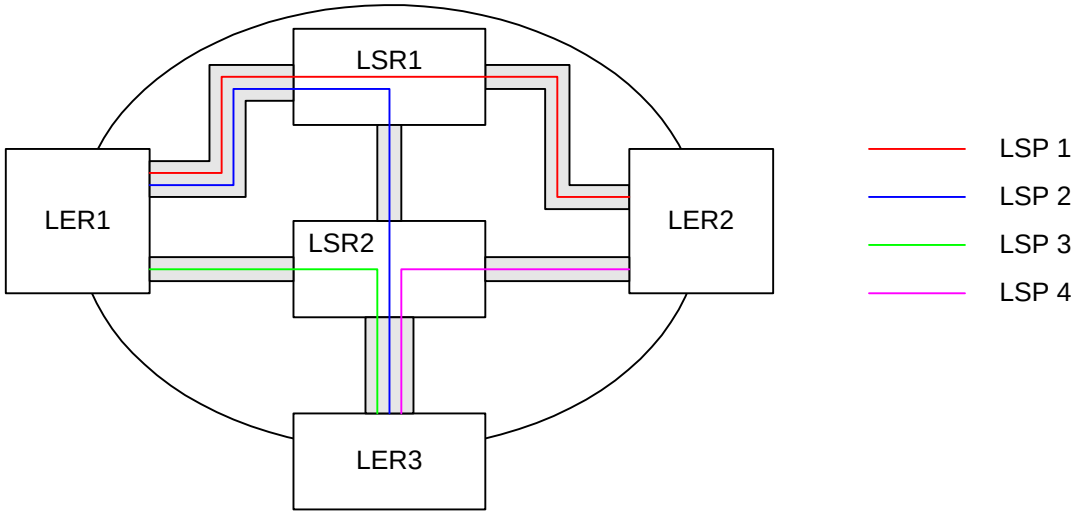

Figure 2: Simple diagram of a MPLS Network

As a simple example of MPLS forwarding, suppose a packet needed to transit the MPLS network from LER1 to LER2. When the packet arrives at LER1, a label is attached and the packet forwarded along LSP1 to LSR1. When the packet arrives at LSR1, a lookup is done on the label to determine its next hop in the MPLS network (LER2). A new label is attached to the packet and it continues its path along LSP1 from LSR1 to LER2. The packet finally arrives at LER2, the label is stripped, and the packet forwarded to its ultimate destination.

Label Switched Paths (LSPs) within a MPLS network can be configured in a variety of ways such as to guarantee a certain level of performance, route around network congestion, or to create tunnels for Layer 2 virtual private networks. In many ways, LSPs are no different than circuit-switched paths in ATM or Frame Relay networks, except that they are not dependent on a particular Layer 2 technology. LSPs are end-to-end tunnels in a MPLS network and can cross multiple types of Layer 2 transport types such as ATM, Frame Relay, Ethernet, or even traditional private line circuits at DS-0, DS-1, DS-3 or OC-X. The end-to-end capability of LSPs eliminates the significant operational complexities of legacy ATM and Frame networks in MPLS networks.

XO MTNS Frame Relay Service

Figure 3 illustrates a typical Frame customer network provided via XO MTNS service.

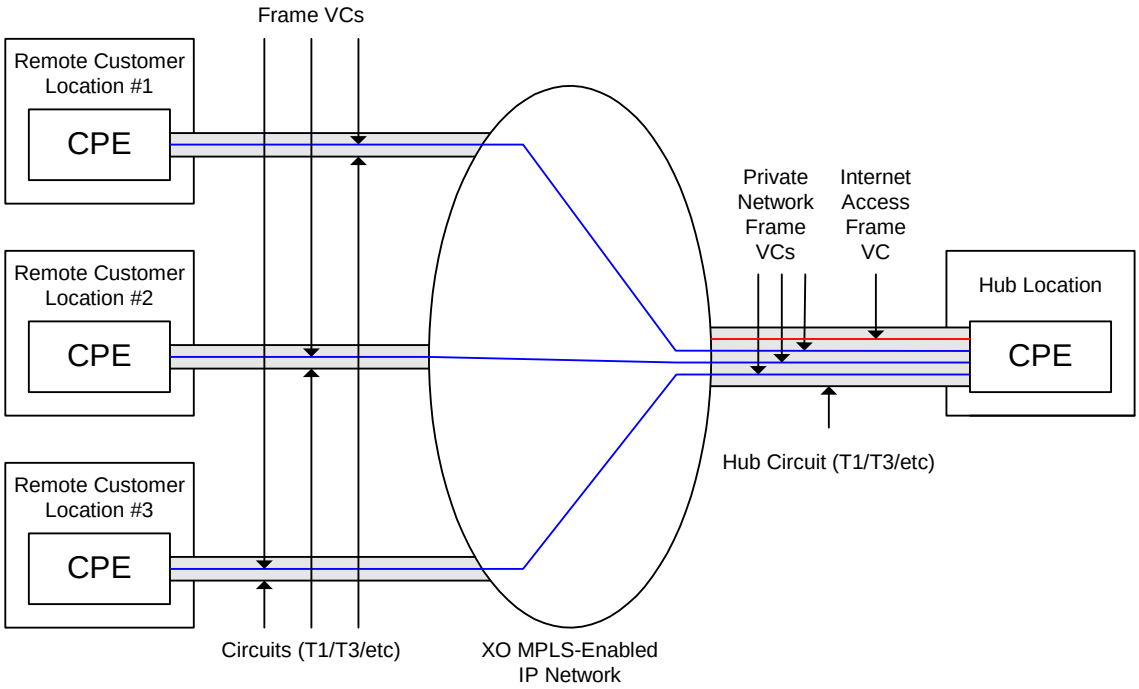

Figure 3: Example of Customer Network configuration

XO MTNS Frame Relay Service is designed to provide private data connectivity over the XO MPLS-enabled IP network. Figure 3 shows a typical hub and spoke configuration with three spokes and one hub.

On each CPE, Frame Relay Virtual Circuits (VCs) are configured as “traditional” Frame VCs would be on the CPE device. At the edge of XO MPLS network, traffic from each Frame VC is configured to use a separate label for transport within the MPLS network. No other XO customer traffic uses that specific label within the MPLS network to ensure privacy and security of the customer’s data. Traffic from the VC (using that separate label) is then transported using a LSP between the ingress and egress points of the MPLS network. While the transport within the MPLS network differs from a legacy Frame Relay service, there is no difference in functionality at each endpoint between that same legacy Frame Relay service and XO MTNS product.

A unique feature of XO MTNS service is shown with the presence of both private data VCs and an Internet access VC on the same physical access circuit. On the XO customer aggregation router, data is sent either to the public Internet or onto one of the customer’s other MTNS-connected sites via the XO MPLS-enabled IP network. XO customer aggregation router(s) ensures that data sent through a private data VC will not be routed to the public Internet or that data from the Internet will not enter a private data VC.

Existing Frame Relay CPE that a customer may have is compatible with XO MTNS service. There should be no reason for a customer to invest significant money in CPE upgrades to utilize XO MTNS Frame Relay.

XO MTNS Frame Relay service does not, at present, support Multilink Frame Relay (MFR) connectivity (FRF.16). MFR provides functionality equivalent to Multilink PPP (MLPPP) allowing for load sharing across multiple physical connections but at Layer-2 rather than Layer-3. Note that an MTNS Frame Relay customer may still purchase multiple physical circuits with a VC on each circuit and have their CPE load-share across each VC.

Note that, at present, MTNS Frame Relay and Ethernet services may not be interconnected. “Any-to-any” connectivity between disparate physical media will be supported in a future MTNS product release.

XO MTNS Ethernet Service

XO offers traditional Transparent LAN services today with both metropolitan and intercity Ethernet services over its fiber network. The introduction of MTNS Ethernet Service complements the existing intercity Ethernet products by addressing the demand for richer connectivity and lower entry costs.

Two types of connectivity are offered via XO MTNS Ethernet Service: Port and VLAN. The port service, as shown in Figure 4, offers direct connectivity between two Ethernet ports; the VLAN service, as shown in Figure 5, allows the customer to connect multiple sites together, utilizing 802.1Q VLAN tagging.

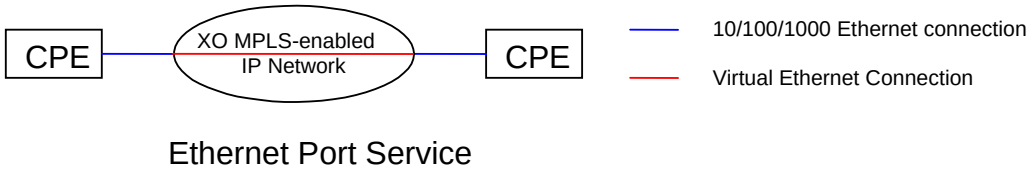

Figure 4: MTNS Ethernet Port Service example

MTNS Ethernet Port Service allows the customer to connect two sites directly via Ethernet, Fast Ethernet, or Gigabit Ethernet using the XO MPLS-enabled IP network for transport. The physical speed of the circuit on each end of an Ethernet port connection must be the same (e.g., Fast Ethernet to Fast Ethernet; not Ethernet to Fast Ethernet). Since Ethernet port service ties two Ethernet Ports together, Internet and private data access are not available on the same port (VLAN service is required for shared private and public Internet access). No special CPE is required to utilize MTNS Ethernet port Service; any existing CPE that can interoperate with a standard Ethernet, Fast Ethernet, or Gigabit Ethernet port will interoperate correctly with the MTNS service.

At the edge of XO MPLS network, traffic from each Ethernet port is configured to use a separate label for transport within the network. No other XO customer traffic uses that specific label within the MPLS network to ensure the privacy and security of the customer’s data. Traffic from that Ethernet port (using the separate label) is sent across a LSP between the ingress and egress points of the MPLS network. While the transport within the MPLS network differs from a legacy private-line Ethernet service, there is no difference in functionality at each endpoint between that same legacy private-line Ethernet service and XO MTNS product.

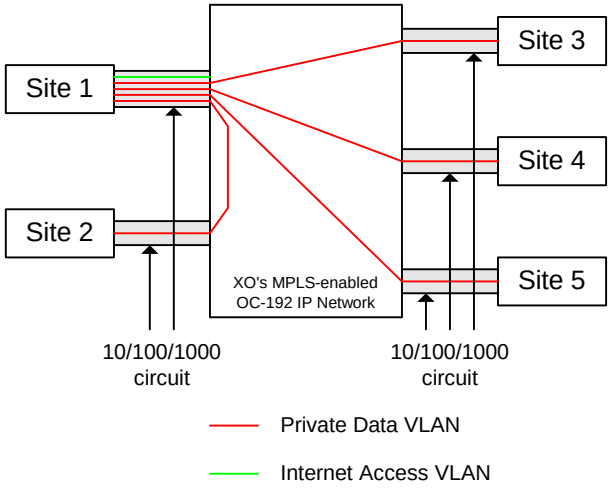

Figure 5: MTNS Ethernet VLAN Service example

MTNS Ethernet VLAN Service allows the customer to provide Ethernet connectivity between multiple sites across a single connection from each site.

A customer may configure up to 1024 802.1Q VLANs per physical Ethernet, Fast Ethernet or Gigabit Ethernet port to provide connectivity between sites as requirements dictate. In Figure 5, a hub-and-spoke configuration is shown with all remote Sites (2-5) having to first send data to the hub (Site 1) to get connectivity to another site or to the Internet. Additional VLANs could be added directly between sites building the equivalent of partial- or full-mesh connectivity between all the sites in the Private Data Network. For example, if Sites 3 and 4 had significant volumes of traffic directly between them, then a VLAN could be created between the two sites to transport that traffic. This additional VLAN has the benefit of removing traffic from the hub connection, allowing a more cost-effective sizing of the hub's circuit.

At the edge of XO MPLS network, traffic from each Ethernet VLAN is configured to use a separate label for transport within the MPLS network. No other XO customer traffic uses that specific label within the MPLS network to ensure the privacy and security of the customer's data. Traffic from that Ethernet VLAN is sent across a LSP between the ingress and egress points of the MPLS network. While the transport within the MPLS network differs from a legacy private-line Ethernet service, there is no difference in functionality at each endpoint between that same legacy private-line Ethernet VLAN service and XO MTNS product.

With Ethernet VLAN service, the restriction between having the same port speed on each end of the virtual connection is removed. A logical configuration for VLAN service might be similar to a Frame Relay hub-and-spoke configuration. A customer could choose Fast Ethernet or Gigabit Ethernet as a hub and then use Ethernet or Fast Ethernet at each remote site to provide high-speed connectivity between the hub and the spoke sites. Additionally, use of VLANs allows both Internet access and private data access on each physical circuit, similar to Frame Relay.

The choice between Ethernet port and VLAN service is typically driven by factors such as:

- Is Internet and private data access simultaneously required across the same 10 / 100 / 1000 access circuit? If both are required, then VLAN would be the correct choice.

- Are there a small number of sites with high bandwidth requirements between them that would benefit from having direct connectivity? If so, then port service might be preferable.

- Is connectivity required between all of the sites using MTNS across a single access circuit at each site? If yes, then VLAN service is required.

- Do sites with different access speeds (10, 100, or 1000) need connectivity between each other? Since port service only allows connections between ports of the same speed, VLAN service is required.

- Does the customer's CPE support 802.1Q VLAN tagging or is an upgrade required? If an upgrade is required, then the cost of port service may be lower than the total cost of VLAN service plus CPE upgrade(s).

Note that, at present, MTNS Ethernet and Frame Relay services may not be interconnected. "Any-to-any" connectivity between disparate physical media will be supported in a future MTNS product release.

Committed Bandwidth, Committed Rate and Bursting

XO MTNS allows customers significant flexibility in selecting port speeds and committed bandwidth levels on each port. As described earlier, a wide variety of port speeds ranging from 64Kb to OC-12c for Frame Relay connections and 10Mb, 100Mb, and 1000Mb for Ethernet connections are available, depending on a customer's needs.

On each Frame or Ethernet port, the customer selects a level of "committed bandwidth"; that means the level of usage that the customer commits to on that port and for which the customer will be billed each month, regardless of actual usage. The level of committed bandwidth chosen therefore should represent the typical monthly utilization on the port. Any usage above the committed bandwidth level on a per-port basis will be charged per-Kb/Mb as measured using a 95^{th} percentile algorithm at five-minute intervals.

Additionally, the customer selects a "committed rate" (CR) for each VC defined in the customer's private data network. The committed rate ensures that each VC will receive its share of capacity across a port as utilization on the port increases. The CR has no billing effect; it is only used by XO customer aggregation equipment to allocate bandwidth on a per-VC basis when congestion exists on that port. If a customer makes no CR choices, then XO equipment divides the available bandwidth evenly between the VCs configured on a physical port. However, if – in times of congestion – certain VC(s) need additional bandwidth (as compared to other VCs on that port), then the capability of setting that policy via CR exists for MTNS customers.

However, as capacity is available, any single VC or combination of VCs can burst to full port speed; there is no restriction on the bursting capability of MTNS connections. This bursting capability ensures that MTNS customers can fully utilize each MTNS port when required. This is a significant different between legacy Frame and Ethernet services and MTNS: there is no limitation on per-port bursting in MTNS. Traditionally, legacy services have required purchasing a full-port speed Committed Information Rate (CIR) between customer locations to ensure that bursting between those locations could occur. This sometimes meant that customers would have CIR which, in aggregate on a single physical port, added up to many times the physical port's speed. XO does not require that because XO does not want customers to pay for the same port multiple times so that they can burst to full port speed. With XO MTNS, the customer purchases committed bandwidth and can burst above that to full port speed when and if needed. There is no requirement to pay for or configure the same port repeatedly through oversubscription of CIR. The customer purchases a port, specifies a committed bandwidth rate, and then configures CR, which tells XO how to allocate the bandwidth on each port when we detect congestion. XO "capacity plans" our network to carry customer bursts; unlike some legacy carriers, XO doesn't require customers to pay repeatedly to manage XO capacity.

Security Concerns

Many customers have concerns about taking data off traditional Frame Relay (as well as other private data networks) and placing that data on MPLS transport. Typically, those concerns are, "My sensitive corporate data is traveling over the public Internet!" or "Can attacks on your IP infrastructure affect my private data in any way?" This section addresses those concerns.

The XO MPLS-enabled IP network is used by many services, including both MTNS and those customers who merely want public Internet access. Those different services are kept separated from each other via basic MPLS mechanisms.

At the edge of XO MPLS network, all MTNS packets are assigned a label. Any packets with labels that might be received from other customer connections are dropped (therefore no "spoofing" of labels and misdirection of traffic or injection of traffic into a MTNS connection is possible). Each label is unique to that customer's connection within XO MPLS network; therefore, this label ensures that no external traffic can be injected or misdirected into a customer's private data network. Once a label is assigned, the packet is forwarded across the appropriate LSP by XO MPLS network. Within the core of XO MPLS network, forwarding for MTNS traffic is only done via label lookups, and not via any IP information in the packet; there is no level of "IP address spoofing" that can cause traffic to be misdirected.

Thus, for MTNS traffic, customer data security is maintained through use of separate per-VC, per-VLAN, and per-port labeling in the XO MPLS-enabled IP network. The base design of MPLS, using label tagging, means that cross-connection of data between customer interfaces with different labels is not possible. That means there is no risk to MTNS customer traffic from XO Dedicated Internet Access customer traffic, other MTNS customers or even the public Internet. Note that if a MTNS customer chooses to terminate both private data connections and an Internet connection on the same access circuit, then the Internet access connection (VLAN or VC) is a direct public Internet access connection, and may need additional protections (e.g., a firewall).

The XO infrastructure is protected from public traffic threats, including the use of encrypted management access, secure user authentication, separate management networks, configuration control techniques, software version controls and denial-of-service protections. Periodic security audits are performed on the XO MPLS-enabled IP network to ensure the infrastructure is secure.

MTNS customers, therefore, should have no security concerns about their internal private data traffic traversing XO MTNS service. The security offered by the MTNS service is equivalent to traditional Frame Relay, Ethernet and ATM public network services. However, XO recommends that highly sensitive data (such as credit card numbers or social security numbers) be encrypted during transport across any shared data network, even including the customer's internal LAN.

MTNS Service Level Agreement

XO MTNS offers the following Service Level Agreement (SLA):

- 100% availability metric
- 65ms average latency metric
- 99.8% packet throughput objective
- Four-hour Mean Time to Repair (MTTR) objective

These metrics are measured across XO MPLS-enabled IP backbone network and do not include the customer's local loop, CPE device, any disruptions caused by the customer's local-area network (LAN), any scheduled maintenance or other *force majeure* events (as defined in the relevant service contract). SLA metrics are backed by credits from XO Customer Care and may be viewed by customers via XOStats, the XO Web-based reporting and monitoring tool. More detail on the MTNS SLA may be found at http://www.xo.com/legal/sla/mtns.html?f=mtns.

MTNS Reporting and Monitoring Tools

XOStats, the XO Web-based reporting and monitoring tool, is available for all XO data customers, including MTNS customers. XOStats can display a variety of statistics, including utilization, errors and discards about each of a customer's MTNS connections as well as MTNS SLA statistics. An example showing the utilization of a MTNS circuit is shown in Figure 6.

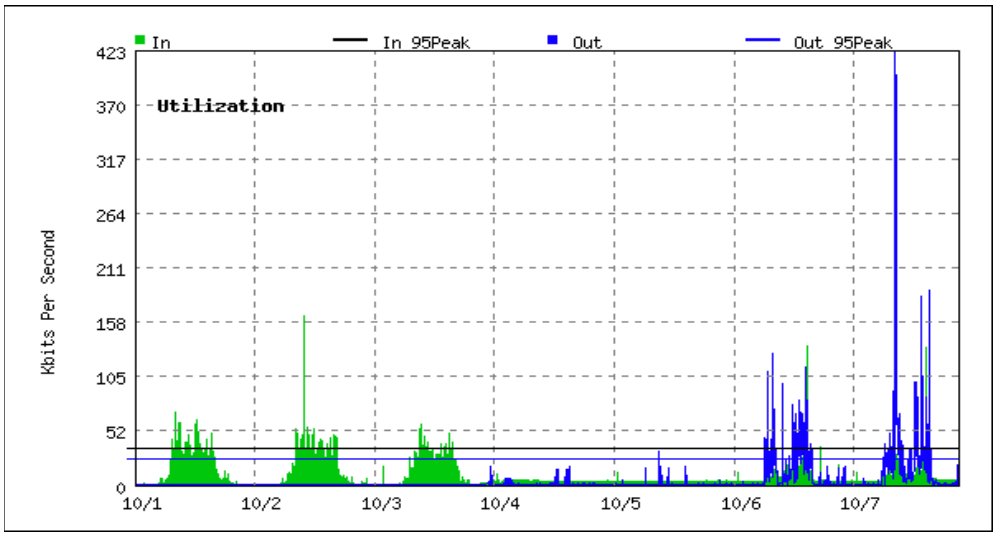

Figure 6: XOStats Utilization Example

MTNS Product Features

Billing Flexibility

MTNS usage-based billing offers customers extraordinary flexibility in service configuration. Customers can select from a variety of port speeds, different committed bandwidth for each port, and a variety of committed rate configurations for each VC. Usage above the committed bandwidth on each port is billed based on the actual measured usage. This flexibility allows customers to optimize their expenditure based on current and future bandwidth demands.

Committed Rate

MTNS allows traffic bursting up to full port speed; there are no preset burst limits per port. In event of congestion, all VCs within a port will receive equal proportion of the available bandwidth if the customer does not configure any committed rates. If a customer sets the committed rate for any or all VCs on a physical port, then that committed rate will be enforced during times of congestion on the port.

Bundled Services

MTNS allows simultaneous Internet access and private data access across the same access loop, saving the customer from paying for multiple access loops to provide the same services. Within a MTNS network, customers can decide on a per-port basis whether Internet access should be included. XO also offers a comprehensive list of voice and data services including TDM Voice, VoIP, DSL and many others that provide customers with a strong choice in service expansion or future migration paths.

Services Footprint

XO is one of the few nationwide providers that has both a strong metropolitan and intercity footprint. The award-winning OC-192c IP network, combined with extensive metropolitan fiber network footprints in 63 markets throughout the continental United States, provides customers with a fast and successful service delivery experience.

Seamless Migration Path to Network-based IP VPN

MTNS Layer 2 VPNs can be a stepping stone for customers who have a definite but non-immediate need for network-based IP VPN migration. The migration requires no physical change in the customer network such as access loop and Customer Premises Equipment; this means a customer's investment remains safe.

Seamless Migration Path to IP Class of Service

Future enhancements to XO MTNS will add IP Class of Service for network-based IP VPNs (L3VPN) and for existing Layer 2 VPNs (L2VPN). The migration requires no physical change in the customer network such as access loop and Customer Premises Equipment; this means a customer's investment remains safe.

Summary

XO MultiTransport Networking Service provides customers with a migration path from expensive, separate legacy transport services to a more economical integrated service from a single provider.

XO MTNS was designed to address both Layer 2 and future network-based IP (Layer 3) VPN demands. XO MTNS includes a broad range of features to provide service flexibility and investment protection for both Layer 2 and Layer 3 customers. Future MTNS enhancements (in addition to network-based IP VPNs) include Class-of-Service functionality (at both Layer-2 and Layer-3) and "any-to-any" connectivity between different physical media types.

The award-winning XO MPLS-enabled OC-192c IP network along with the experience XO has in versatile service delivery ensures a swift implementation and high-functionality solution for customers. Use of MPLS for MTNS offers customers a secure, highly available solution for private data and Internet access needs while realizing cost savings through reduced transport and internal support requirements.

XO MTNS is well suited for customers interested in:

- Migration from TDM private network
- Migration from traditional Frame Relay network
- Migration to Transparent LAN network
- Point-to-point Layer 2 transport
- Bundled Internet services
- Easy migration to network-based IP VPN

In summary, XO MTNS product allows customers to replace multiple legacy networks with a single private data network solution, saving the customer significant operational expense and simplifying the customer's private data network design and operation.