OPTICAL VIRTUAL PRIVATE NETWORKS
Overview, Service Definition, and Key Applications

The current business environment puts a significant amount of pressure on service providers to increase the top line and reduce capital and operational expenses to achieve and maintain a profitable, ongoing business model. Fierce competition from existing and emerging players is shaping service providers’ strategies in their quest for new ways to increase customer loyalty, tap into new revenue streams, and optimize day-to-day operations. This paper describes Optical Virtual Private Network (O-VPN) technologies and how they allow service providers to offer high-performance service and enhanced service flexibility while leveraging their existing infrastructures.

Features and Benefits
- Secure, independent virtual networks within a shared switched infrastructure
- Segmentation without overlay
- Faster service turn-up/network expansion
- Service activation and restoration constrained to assigned OVPN
- Privacy and performance of private network with new economics
- Shared bandwidth potential for dynamic Bandwidth on Demand services

Business Challenge
Recent analyst reports highlight that high-end customers (Fortune 50, 100, and 500) significantly contribute to the service providers’ top line. Along with the large contribution to revenue, high-end customers bring very stringent requirements that span over many service aspects, such as enforced security to separate their traffic from others’, sophisticated Service Level Agreements (SLAs) to ensure their services are not impacted by any external disruptions, such as fiber cuts and traffic hits caused by other users in the service provider’s network, etc.) in addition to requirements for end-user manageability to establish connections and increase bandwidth without the service provider’s intervention.

Given the strategic importance of this type of customer, service providers tend to invest massively in the infrastructure to meet such requirements by building customer-dedicated private networks. However, this deprives the providers of potential service revenue and limits their service offering to just pipes or fiber links and, possibly, network management of these private builds. Such a solution proves extremely costly to implement and maintain, unscalable, and operationally challenging (such as the addition of other sites hardware and software upgrades, etc.). Consequently, the large contribution from these high-end customers is reduced or offset quickly by the high cost
of the private builds. Some other alternatives, such as Layer 3 (IP-VPN) or Layer 2 (Ethernet Local Area Network [E-LAN]) VPNs fall short of meeting the customers’ expectations for cost, network availability, end-user manageability, security, and performance.

**Solution: O-VPN**

The latest technology breakthroughs in software and hardware can turn the network into an intelligent, flexible, and highly secure infrastructure capable of meeting high-end customers’ most stringent requirements through the use of O-VPNs. Now, service providers can “virtually” partition their networks by allowing specific links, wavelengths, sub-wavelengths, or even nodes to be dedicated for use by a single customer (such as enterprise), while providing all the bandwidth, manageability, and security required without the extraordinary expense and inflexibility of building a completely dedicated service infrastructure.

O-VPNs provide a secure, high-bandwidth private network that connects end-user sites with a flexible, managed virtual infrastructure over fractional, single, or multiple transparent optical wavelength connections with a wide variety of client interfaces (including Ethernet, Optical Transport Network [OTN], SONET, SDH, Storage Area Network [SAN], and video). Moreover, O-VPNs provide a virtual infrastructure for end-users to manage their own site-to-site connections, bandwidth allocation, and circuit protection options within the O-VPN domain—or, optionally, have the service provider (carrier) manage this process.

Despite the fact that O-VPNs are offered across the service provider’s network, they provide dedicated bandwidth to connect multiple end-user sites in a mesh configuration with multiple parallel line rates available, and still maintain full separation in user traffic and restoration bandwidth. Full visibility of the network and optional control over provisioning, protection, and bandwidth on demand can be provided over a secure, Web-based customer portal.

**O-VPN Key Service Features and Controls**

O-VPNs provide numerous key service features and controls that allow end-users to get better flexibility and manageability than private networks. Some of these features are described below:

- **Circuit Creation:** Controlled by the end-user through a secure, Web-based interface, with visibility and path creation restricted to their respective O-VPN. Many path computation
options exist—including hop count, admin weight, and/or latency—as well as protection options including unprotected, 1+1 protection, shared mesh protection, and 1+1 mesh-restorable Sub-Network Connection Protection (SNCP). The O-VPN is offered as a SONET/SDH, transparent OTN, or any other service such as Ethernet, storage, or video. Planning of the O-VPN can be outsourced to the carrier or owned by the end-customer. An O-VPN planning tool is optionally provided.

- **Circuit Maintenance:** End-users can monitor the status and performance of their assigned O-VPN, including the creation and maintenance of their own SLAs and the ability to resize their circuits without traffic hits, through a secure, Web-based customer interface. End-users have visibility to only their own O-VPNs, and are ensured protection and isolation from other customers or services within the overall shared network.

- **Restoration and Protection:** The O-VPN offers the added advantage of protected shared restoration. Traditional services are based on either an unprotected or 1+1 protected service, which typically fails during cases of more than two simultaneous failures. In comparison, an optical mesh can survive multiple failures, offering increased service availability, and allow for a wider range of protection options. O-VPNs offer the option to provide privately shared bandwidth for protection and restoration for ultimate control by the end-user. Alternatively, end-users can opt for a service on working circuits only, while the carrier provides the restoration bandwidth for the O-VPN, in line with the agreed SLA.

- **Service Option – Circuit Resizing:** In the future, with the Circuit Resizing Service Option, end-users will be provided the capability for hitless resizing of the client bandwidth rates within the O-VPN, with granularity of 1G for OTN O-VPN or STS-1/VC-4 for SONET/SDH O-VPN.

**Benefits of using O-VPN**

O-VPNs set a new economic benchmark for both service providers and end customers by reducing the cost of delivering high performance and highly customized services. The benefits of O-VPNs can be summarized in the following bullets:

**For Service Providers**
- Lowers Capital Expenditure (CAPEX) by providing customers with private networks while maintaining a common physical infrastructure as a result of economies of network scale
- Increases revenue streams and accelerates time to revenue by expanding the addressable market for private networks
- Simplifies core infrastructure and reduces time to deliver private networks
- Offers a common management solution across core network and O-VPN services
- Simplifies service provisioning by leveraging the control plane to identify and manage dedicated bandwidth
- Maximizes network bandwidth utilization by sharing a common network infrastructure
- Reduces equipment count for operational savings in required power and physical footprint

**For End-Customers**
- Lowers cost and offers more visibility and control via optical private line services
- Eliminates infrastructure contention issues common with other VPN types
- Provides secure facilities that are isolated from other network disruptions caused by other customers
- Offers a network that may be engineered, managed, and operated as easily as a private network
- Leverages service provider infrastructure to reduce time to build out and turn up new sites
- Enables flexible bandwidth-on-demand services for increased bandwidth only when it is required

**O-VPN Targeted Applications**

O-VPN applications are numerous and span across many industries. A sample of these applications is described below:

**A. Enterprise O-VPNs:** Service providers now can offer customers such as enterprise, cloud providers, and intermediaries (social networks, search, Content Delivery Networks [CDNs]) virtual networks that can be dimensioned to achieve their own performance and resilience targets as business needs dictate, while realizing the benefits of a “private” network at a lower cost. The enterprise-dedicated O-VPN provides secure, highly customized network resources, full network visibility and control, and managed, portal-driven, end-to-end connection for all business needs (Ethernet, storage, and video service circuits).
B. Geo-Partitioning of International Networks: Given the large geographical distances covered by international networks and the various sources of potential failures (such as submarine cables or terrestrial links in harsh environments), the network has to be highly resilient and capable of surviving multiple simultaneous failures without impacting the traffic (self-healing), because even few seconds of network failure can cost millions of dollars. International network operators can now logically partition their physical networks to better control connection setup and traffic restoration within a required geographical area. This capability allows local operators to administer and control their local traffic while providing global access for traffic that may need to go between regions (cross-VPN traffic).
C. Line-of-Business Dedicated O-VPNs: Most service providers offer triple- or quadruple-play services (voice, video, Internet, wireless) to residential and business customers. While these services might be carried on the same service provider’s infrastructure, practically, each line of business (e.g. wireless, etc.) controls its own sub-network and has unique operational processes and service requirements. For example, business customers require higher resiliency, traffic collected from wireless towers must have low latency and jitter, and video networks must maintain a certain quality. O-VPNs allow service providers to partition their infrastructure based on the specific needs of each line of business, enabling better service management, higher service quality (e.g. prevent failures from propagating to or impacting other lines of business), and lower operating costs.

D. Tiered Service Offering through O-VPNs: Service providers now can establish their service offerings based on O-VPNs that have distinct levels of service quality and resiliency. While specific service layer offerings can certainly be made without the introduction of Optical VPxNs as well as within individual VPxNs, the introduction of an O-VPN concept allows the operator to create partitions which have a higher degree of shared bandwidth and, thus, a higher overall degree of service. For example, a pure mesh circuit’s overall resiliency metric is defined in part by the number of failures it can ultimately survive—the more shared protection in the network, the more failures it can survive. By using an O-VPN, some VPxNs can be created with more shared protection, and thus higher resiliency, than others.

E. Bandwidth Pools/Wholesale to Retail Carriers: Often, service providers sell or lease bandwidth to other carriers (across a region, across a country, or internationally) as part of their business model. O-VPNs allow service providers to create “bandwidth pools” in which they can tailor their leased services based on various market requirements and prevent these “leased” services from impacting the service provider’s network. This feature allows service providers to benefit from the revenue generated by these bandwidth pools without being impacted by potential disruptions on the infrastructure, such as fiber cuts or scheduled maintenance.
F. Video as a Service: O-VPNs allow service providers to offer secure, high-bandwidth private networks that connect end-user sites with a flexible virtual infrastructure, as depicted in Figure 5. Video services can be delivered over fractional, single, or multiple transparent optical wavelength connections with a wide variety of client video, Ethernet, and TDM interfaces. End-users can control their own site-to-site connections, bandwidth allocation, and circuit protection options within the O-VPN domain, or opt to have the carrier manage this process.

G. Research and Education Networks: Government-funded research and education networks rely on global networks for interchange of bandwidth-intensive experiment data between scientists in their day-to-day pursuit of technological breakthroughs. The research and education community can leverage O-VPNs to create a dedicated partition of the network for each type of application. For example, an O-VPN can be created for high-performance applications such as medical/astronomy imaging or ultra-fast computing, while other O-VPNs can be used for site interconnection with less stringent requirements.

H. Cloud Networks (Data Center Interconnect): Cloud-based services enable convenient, secure, and on-demand network access to a shared pool of configurable resources—such as networks, servers, storage, applications, and services—that can be provisioned rapidly and released with minimal management effort or service provider interaction. O-VPNs play a key part in the creation of intelligent and dynamic cloud networks. They allow network operators to define virtual and dedicated networks for data center interconnect, with specific requirements for latency, bandwidth, and resiliency. Other virtual networks can be created for user access or other applications.
O-VPN Service Pricing Options

Service providers can offer O-VPN-based services using different pricing structures or a mix of the following parameters:

→ Number of ports
→ Bandwidth size
→ Distance (coverage)
→ Shared restoration or dedicated restoration path
→ Carrier management

Ciena’s O-VPN Solution

Ciena’s O-VPN services are implemented in the 5410 and 5430 Reconfigurable Switching Systems. Both products provide the flexibility, capacity, and end-user integration required to deliver carrier-grade O-VPN solutions. The intelligent Layer 1 control plane in the 5400 family allows links or wavelengths to be identified automatically as part of an O-VPN group and ensures they are fully manageable as part of an O-VPN service offering. The integration of Ciena’s OneControl Unified Management System for infrastructure management allows a unified view for the service provider across the infrastructure while providing a Web-based portal for the enterprise customer to manage their facilities within the core. Offering the service at Layer 1 ensures dedicated, contentionless facilities are always available for the enterprise customer, and reliability and fault tolerance can be engineered with certainty.

Conclusion

O-VPN is a service that enables customers such as carriers, enterprises, cloud providers, and intermediaries such as social networks, search, and CDNs to dimension their networks to achieve their own performance and resilience targets as their business needs dictate, at a lower cost. Ciena’s market-leading optical switching portfolio and control plane allow O-VPNs to play an instrumental role in providing customers the benefits of private networks while maintaining a common physical infrastructure and reducing capital and operational expenditures. Furthermore, O-VPNs help service providers increase revenue streams by expanding their addressable market. O-VPNs offer tremendous value for end-customers, as they can benefit from secure, highly customized optical private line services at a lower cost.