The Need for LAN Extensions
Businesses face the challenge of providing very high availability for applications while maximizing the use of their infrastructure and keeping operational expenses low.

The deployment of geographically disperse data centers allows IT designers to put in place effective disaster avoidance and disaster recovery mechanisms that increase the availability of applications. Geographic dispersion also enables the optimization of application response through improved facility placement and allows the flexible mobility of workloads across data centers to avoid demand hotspots and fully utilize available capacity.

To achieve all the benefits of geographically dispersed data centers, the network must extend Layer 2 connectivity across the diverse locations.

LAN Extensions Compared to Layer 2 Transport Services
Enterprises and service providers have different views on the use of Layer 2 virtual private networks (VPNs). Service providers have requirements that derive from their need to offer a very large number of Layer 2 VPNs as a transport service to a multitude of customers. The technical requirements of service providers are therefore very different from those of enterprises seeking LAN extensions between data centers. Cisco Overlay Transport Virtualization (OTV) was specifically designed to meet the challenges of LAN extensions between data centers. To meet the technical challenges of a provider network, Cisco continues to provide innovative and industry-leading technology, offering transport services for which Multiprotocol Label Switching (MPLS) technologies are optimized.

Just as service providers and enterprises face different challenges, they also require different solutions. In many situations, a combination of technologies may render the optimal solution. For example, an enterprise may have an MPLS backbone that provides Layer 3 VPNs and traffic engineering services, while leveraging OTV to provide inter-data center LAN extensions.

Challenges of LAN Extensions
Extending the LAN across multiple data centers creates a series of challenges that are different from the challenges faced by service providers providing transport services:

- **Maintaining site independence:** The extension of Layer 2 domains across multiple data centers can cause the data centers to share protocols and failures that would normally have been isolated when interconnecting data centers over an IP network. These failures propagate freely over the open Layer 2 flood domain.

A solution that provides Layer 2 connectivity yet restricts the reach of the flood domain is necessary to limit failure propagation.

- **Transport independence:** The nature of the transport between data centers varies depending on the location of the data centers and the availability and cost of services in the different areas. A cost-effective solution for the interconnection of data centers must be transport agnostic and give the network designer the flexibility to choose any transport between data centers based on business and operational preferences. A solution capable of using an IP transport is expected to provide the most flexibility.

- **Multihoming and end-to-end loop prevention:** LAN extension techniques should provide a high degree of resiliency, and therefore multihoming of the Layer 2 sites onto the VPN is required. Mechanisms must be provided to prevent loops that may be induced when connecting bridged networks that are multihomed.

- **Bandwidth utilization with replication, load balancing, and path diversity:** The use of available bandwidth between data centers must be optimized to obtain the best connectivity at the lowest cost. Balancing the load across all available paths while providing resilient connectivity between the data center and the transport network requires added intelligence above and beyond that available in traditional Layer 2 VPNs. Multicast and broadcast traffic should also be replicated optimally to reduce bandwidth consumption.

- **VLAN and MAC address scalability:** The extension of LANs between data centers requires the simultaneous extension of multiple VLANs. Furthermore, in some applications, duplicate VLAN IDs will be in use, and these must be carried independently of each other yet on a common LAN extension. As sites are interconnected, the number of MAC addresses involved will grow, since the MAC address space cannot be summarized; this can become a problem and limit the reach of the solution if not handled correctly.

- **Complex operations:** Layer 2 VPNs can provide extended Layer 2 connectivity across data centers, but will usually involve a mix of complex protocols, distributed provisioning, and an operationally intensive hierarchical scaling model. A simple overlay protocol with built-in capability and point-to-cloud provisioning is crucial to reducing the cost of providing this connectivity.

Table 1 summarizes the different ways that OTV and virtual private LAN service (VPLS) meet the challenges of LAN extensions.
# Cisco Overlay Transport Virtualization (OTV) and Virtual Private LAN Service (VPLS) as Enablers of LAN Extensions

## At-A-Glance

Table 1. Comparison of OTV and VPLS

<table>
<thead>
<tr>
<th>Requirement or Technology</th>
<th>OTV</th>
<th>VPLS</th>
<th>Cisco VPLS Enhancements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preservation of site independence</td>
<td>• Flood suppression and broadcast controls</td>
<td>• Spanning Tree Protocol and VTP filtering</td>
<td>• Layer 2 Protocol Filters</td>
</tr>
<tr>
<td></td>
<td>• Address Resolution Protocol (ARP) localization</td>
<td></td>
<td>• Broadcast-rate limiters</td>
</tr>
<tr>
<td></td>
<td>• Layer 2 protocol localization (Spanning Tree Protocol, Hot Standby Router Protocol [HSRP], etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport independence</td>
<td>• Transport agnostic (Ethernet over IP)</td>
<td>• Requires MPLS</td>
<td>• VPLS over Generic Router Encapsulation (GRE)</td>
</tr>
<tr>
<td></td>
<td>• Use of MPLS or IP transport services</td>
<td>• Integrated with MPLS transport services</td>
<td></td>
</tr>
<tr>
<td>Multithoming with loop prevention</td>
<td>• Autodetection</td>
<td>• Configured</td>
<td>• Virtual switching system (VSS) for dual homing</td>
</tr>
<tr>
<td></td>
<td>• All active with virtual PortChannel (vPC) technology</td>
<td>• Single active provider edge per VLAN</td>
<td>• All active</td>
</tr>
<tr>
<td></td>
<td>• Built-in capability</td>
<td>• No per-flow load balancing</td>
<td></td>
</tr>
<tr>
<td>Traffic replication</td>
<td>• Native multicast</td>
<td>• Label switch multicast (LSM) with full mesh of point-to-multipoint (P2MP) tunnels</td>
<td>• Optimal multicast handling in hardware</td>
</tr>
<tr>
<td>Load balancing</td>
<td>• Equal-cost multipath (ECMP) across multiple edge devices</td>
<td>• Single active provider edge per VLAN</td>
<td>• Per-flow load balancing possible with VSS and vPC</td>
</tr>
<tr>
<td></td>
<td>• Per flow and per VLAN</td>
<td>• No per-flow load balancing</td>
<td></td>
</tr>
<tr>
<td>Path diversity</td>
<td>• 5-tuple hashing on User Datagram Protocol (UDP) headers</td>
<td>• Traffic engineering</td>
<td>• FAT pseudowire per-flow labels</td>
</tr>
<tr>
<td></td>
<td>• Core traffic engineering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scalability</td>
<td>• Hundreds of edge devices</td>
<td>• Hierarchical VPLS (H-VPLS)</td>
<td>• Hardware-accelerated learning</td>
</tr>
<tr>
<td></td>
<td>• Stateless</td>
<td>• Border Gateway Protocol (BGP) signaling</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Packet switched</td>
<td>• LSM</td>
<td></td>
</tr>
<tr>
<td>VLAN scalability</td>
<td>• Integrated service ID (SID) and VLAN ID</td>
<td>• Requires IEEE QinQ</td>
<td>• Integrated IEEE QinQ</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IEEE 802.1ah</td>
<td>• IEEE 802.1ah</td>
</tr>
<tr>
<td>MAC-address scalability</td>
<td>• VLAN scoping</td>
<td>• Linear: no VLAN scoping</td>
<td>• VLAN scoping possible</td>
</tr>
<tr>
<td>Protocol proliferation</td>
<td>• Conversational programming</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Effect on network design</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disruptive</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Why Cisco?

Cisco provides significant enhancements to VPLS and continues to invest in the development of innovative technologies for VPLS. Simultaneously, Cisco continues to achieve innovation with new technologies like OTV that are the product of years of experience. VPLS and OTV technologies both have strengths and weaknesses, but for the specific application of LAN extensions in the data center interconnect (DCI) space, OTV provides a much simpler approach.