Enterprise and government CIOs will testify that lowering information technology (IT) communication costs is of paramount importance for any organization. The challenge is how to save costs while offering the end user new services with better performance. This dilemma has prompted many large organizations to consider new technology options that satisfy current and future user and application requirements. Multiprotocol label switching (MPLS)-based technology (Layer 2 and Layer 3 virtual private networks [VPNs]) is gaining traction for enabling next generation campus networks, as well as for wide area connectivity. This whitepaper discusses the various options available to enterprise and government IT decision makers when considering selecting an MPLS-enabled network infrastructure for their organization.
# Table of Contents

1. **The CIO’s Challenge**

2. **MPLS for Enterprise and Government Infrastructures**
   1. Existing Campus Networks
   2. Existing Wide Area Network Connectivity
   2. Evolving Trends and the Role of MPLS
   3. The MPLS Value Proposition

3. **MPLS Layer 2 and Layer 3 VPNs**
   5. Virtual Leased Line (VLL)
   5. Virtual Private LAN Service
   6. IP-VPN

4. **MPLS-Based Enterprise WAN Connectivity**
   7. VPLS for WAN Connectivity
   9. Provider-Managed Versus Self-Managed Layer 3 MPLS VPN

5. **Service-Aware VPLS Infrastructure Campus Networks**

6. **Service-Aware Management**
   14. IP Routing Management Control

7. **Summary and Conclusions**
   15. VPLS versus IP-VPNs Positioning for Enterprises
   15. Conclusion

8. **Acronyms**
The CIO’s Challenge

The challenge for CIOs is how to save costs while increasing services and performance to the end user. Significant savings can be realized by converging multiple separate networks into a single, well-managed network; this requires next generation products and management tools. The resulting network has to be flexible enough to carry all traffic types and ensure the mission-critical traffic is carried without compromise.

Large organizations are having to look at new technology options to satisfy their current and future user and application requirements. MPLS-based technology (Layer 2 and Layer 3 VPNs) is gaining traction for enabling next generation campus networks as well as for wide area connectivity within enterprise and government.

MPLS for Enterprise and Government Infrastructures

Existing Campus Networks

Figure 1 depicts a typical existing campus deployment. The campus employs Ethernet Layer 2 switches in the access layer. Larger networks may also have a distribution layer consisting of Layer 2 switches (or Layer 3 routers). The access and distribution switches connect to backbone Layer 3 routers.

Enterprises configure groups of users within virtual local area networks (VLANs). These VLANs are bridged using Ethernet bridging technology. VLANs are terminated on the centrally located backbone Layer 3 routers. In this manner, routing decisions and policy are controlled in a centralized manner and restricted to a limited set of nodes. This approach simplifies the overall network architecture and helps the IT group manage the campus network in an efficient manner.

Figure 1. Existing Campus Network Design
Existing Wide Area Network Connectivity

Figure 2 depicts a typical enterprise wide area network (WAN) connectivity scenario.

The enterprise has a central campus which hosts the data center (could be multiple sites) and several smaller sites distributed within the city (metro), or in other cities (national and international). Today's connectivity within the WAN is primarily based on private line, frame relay or ATM WAN links.

Enterprises typically lease links from service providers and then interconnect wide area sites with routers. In this model the enterprise has full control over its routing domain and manages all routing policy changes independent of the service provider.

Evolving Trends and the Role of MPLS

As enterprises and governments evolve, so do their network service needs. Applications within their networks are evolving at a rapid pace.

Trends that are causing IT groups to evaluate their approaches for the evolution of their existing network infrastructures:

• Support for mainstream corporate applications – Applications like customer relationship management (CRM) and enterprise resource planning (ERP) have become commonplace in most enterprises today. Servers hosting these applications can now process and deliver data at Gigabit speeds. The network infrastructure must support these increased bandwidth and performance demands.

• An increase in power users – Power users are users who run special applications and have higher bandwidth processing needs. Within large enterprises, power users include graphic artists, design engineers, healthcare personnel and research personnel.
• Gigabit to the user – Bandwidth-hungry applications are driving the move towards Gigabit (10/100/1000) to the desktop.

• Remote connectivity demands the same level of performance as a local area network (LAN) – The notion of “remote site = slower speed links” is no longer acceptable. Users in remote sites expect any and all applications running at the central site to be accessible and to perform equally well from remote locations.

• Security is a paramount concern – The increase in mobile workers and remote site connectivity, as well as the move toward web-based services, has put a significant focus on ensuring that security holes do not compromise an enterprise's intellectual property.

• User experience guarantee – Voice and video applications are moving to IP technology. The end user is transparent to the network infrastructure and expects the service to work without problems. This imposes stringent requirements on how applications are prioritized within the network.

• Lower costs without compromising service quality – This is, by far, the most important aspect for all IT groups.

These trends are why IT groups are considering MPLS-based technology options for their enterprise infrastructures (campus and WAN connectivity); MPLS offers solutions that future-proof enterprise networks to meet the requirements of these trends. (Refer to Figure 10).

The MPLS Value Proposition
For an enterprise to achieve its business goals, an enterprise campus and WAN must be highly scalable. MPLS can integrate both Layer 2 switching and Layer 3 routing in a single node.

The following aspects of MPLS make it an enabling technology for implementing carrier-grade networks. Note that carrier grade refers to an enterprise network that offers its users a range of services with the same level of resiliency and flexibility as provided in a service provider grade network.

MPLS supports Layer 2 and Layer 3 VPNS
• Enterprises have the choice of deploying Layer 2 or Layer 3 VPNS based on MPLS
• VPNs allow an enterprise to implement virtualization within their networks; VPNs are provisioned between MPLS nodes
• VPNs are configured as an overlay over the MPLS network
• An MPLS network is capable of supporting thousands of VPNS on a single physical infrastructure

MPLS provides traffic engineering
• In an IP-only network, packets from source nodes to destination nodes travel along a path that is determined by routing information computed by IP routers
• An IP-only network offers little flexibility in providing alternate paths for traffic flow
• An MPLS-based network supports traffic engineering whereby, an MPLS path (logical connection) can be defined to use network links that are different from the normal path taken by IP packets; this helps to better use links within the enterprise network

MPLS provides deterministic re-route behavior
• In a typical Ethernet network based on Spanning tree, it is very difficult to predict the recovery times when links or switches fail; best case recovery times are in the order of seconds
• MPLS provides deterministic re-route times which match that of transport network (SONET/SDH) recovery times. MPLS supports a mechanism called fast re-route, which can deliver best re-route times of 50ms
**MPLS nodes offer superior QoS capabilities**

- Ethernet switches typically support port-based queuing
- MPLS nodes support service-based queuing (each logical port, VLAN or VC within a physical port has dedicated queues), and they support queues and quality of service (QoS) for traffic classes within the logical port (supporting thousands of end users and their corresponding services within the enterprise network)

**MPLS nodes offer superior OAM capabilities**

- An Ethernet bridging-based network supports limited tools, based on IEEE 802.3ah EFM (Ethernet in the First Mile) operations, administration and maintenance (OAM) and IEEE 802.1ag CFM (Connectivity Fault Management), to help install and debug the network
- MPLS nodes support OAM tools, such as LSP ping and trace route, Bi-directional Forwarding Detection (BFD) and Virtual Connectivity Check Verification (VCCC), plus VPLS-based OAM tools, such as MAC ping, MAC trace, MAC purge and CPE ping that help simplify the installation and day-to-day operation of an enterprise network

Most campus networks are based on Spanning Tree-based bridging. Table 1 compares a spanning tree based bridging network and an MPLS-based network.

### Table 1. Comparison of Spanning Tree-Based and MPLS-Based Networks

<table>
<thead>
<tr>
<th>SPANNING TREE BASED NETWORK</th>
<th>MPLS BASED NETWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Services</strong></td>
<td></td>
</tr>
<tr>
<td>Basic services only – data</td>
<td>Advanced Services – voice, video, data as well as other real time applications</td>
</tr>
<tr>
<td><strong>Traffic Engineering</strong></td>
<td></td>
</tr>
<tr>
<td>Not supported</td>
<td>Supports ability to define alternate paths for better link utilization</td>
</tr>
<tr>
<td><strong>Deterministic Route Times</strong></td>
<td></td>
</tr>
<tr>
<td>Spanning tree protocol, not carrier class convergence in seconds</td>
<td>MPLS supports fast re-route which converges in 50 milliseconds</td>
</tr>
<tr>
<td><strong>QoS</strong></td>
<td></td>
</tr>
<tr>
<td>Typically port-based QoS</td>
<td>Service-based QoS with support for thousands of queues</td>
</tr>
<tr>
<td><strong>OA&amp;M</strong></td>
<td></td>
</tr>
<tr>
<td>Limited standardization</td>
<td>Support for MPLS-based OA&amp;M tools which ease installation and day-to-day operations</td>
</tr>
<tr>
<td>Complex management based on vendor implementation</td>
<td></td>
</tr>
<tr>
<td><strong>High Availability</strong></td>
<td></td>
</tr>
<tr>
<td>Ethernet switches do not support high availability features like non-stop routing</td>
<td>MPLS nodes support non-stop routing. With non-stop routing control, card failovers do not impact the network</td>
</tr>
<tr>
<td><strong>Manageability</strong></td>
<td></td>
</tr>
<tr>
<td>No network and service management tools</td>
<td>Support network and service management tools for GUI-based point-and-click provisioning</td>
</tr>
</tbody>
</table>

Note: The high availability and manageability features are specific to some vendors like Alcatel-Lucent. These help to further enhance the overall MPLS value proposition.

**MPLS Layer 2 and Layer 3 VPNs**

The IT group can be viewed as the service provider for users within the enterprise. It is therefore essential that the deployed technology must support flexible choices to implement any applications being run within the network.

When deciding to implement an IP/MPLS-based VPN, the IT group has the flexibility of choosing either a Layer 2 approach or a Layer 3 approach, or more often, a combination of the two:

- **Layer 2 approach:**
  - Commonly referred to as Layer 2 VPN
  - Includes virtual leased lines (VLLs) and virtual private LAN services (VPLS)
- **Layer 3 approach:**
  - Commonly referred to as Layer 3 VPN
  - Includes IP-VPN
**Virtual Leased Line**

A VLL, also known as a pseudowire (PW) or virtual private wire service (VPWS) is an example of a Layer 2 VPN. An MPLS VLL is analogous to a private line within the MPLS enterprise infrastructure. It offers a point-to-point connection between any two end users or applications or devices.

Figure 3 depicts two MPLS VLL connections. The VLL can be used for applications that require dedicated point-to-point connectivity.

An MPLS VLL can be deployed within an enterprise network for:
- Point-to-point connectivity within a campus
- Point-to-point connectivity between WAN sites (i.e. applications/devices within WAN sites)

Key characteristics of an MPLS VLL:
- A VLL is the simplest type of VPN to deploy; it’s a preferred solution for any new point-to-point connectivity requirements
- The VLL is completely transparent to the end user data and application protocol
- The end points of the VLL can be configured with the desired traffic parameters, such as required bandwidth and priority of traffic relative to other traffic in the network
- MPLS provides a quick recovery time for the VLL in the event of a transit node or link failure within the network

**Figure 3. Layer 2 VPN – Virtual Leased Line (VLL)**

---

**Virtual Private LAN Service**

VPLS is an example of a Layer 2 VPN. VPLS enables multipoint connectivity at Layer 2 within the enterprise infrastructure.

Figure 4 depicts a VPLS instance within a network. It is composed of three virtual bridges (VBs) — one VB on each node. Each VB performs media access control (MAC) learning and constructs a table that maps MAC addresses and corresponding MPLS paths. The VPLS concept is similar to a logical LAN connection (i.e., all end devices connected to the VPLS appear as if they are within the same LAN segment).

An MPLS VPLS can be deployed within an enterprise network for:
- Multipoint connectivity within a campus
- Multipoint connectivity between WAN sites
Key characteristics of an MPLS-based VPLS:
- VPLS is a bridged Layer 2 multipoint MPLS VPN
- Each user group or department can be assigned its own dedicated VPLS or Layer 2 domain
- VPLS is transparent to routing protocols; it is an ideal solution for non-IP protocols (e.g., IPX/SNA) within the campus
- Addition of new users is simple
- VPLS does not rely on protocols like BGP; VPLS only requires protocols like open shortest path first (OSPF) for offering connectivity

**IP-VPN**

IP-VPN is a Layer 3 VPN. IP-VPNs enable multipoint connectivity at Layer 3 within the enterprise infrastructure.

Figure 5 depicts an IP-VPN.
With IP-VPNs, each MPLS node supports a virtual routing and forwarding instance (VRF). The IP-VPN is implemented specifically for IP traffic only.

An MPLS IP-VPN can be deployed within an enterprise network for multipoint connectivity between WAN sites.

IP-VPNs require BGP/internal border gateway protocol (iBGP) as the routing protocol that runs between the MPLS nodes.

Key characteristics of an MPLS-based IP-VPN:
- An IP-VPN is a routed service performed at Layer 3
- An IP-VPN supports only IP-based traffic
- IP-VPNs are suitable for IP connectivity applications that require support for overlapping IP address spaces; this may be necessary when an enterprise acquires a new company or if connectivity with a partner network is required
- IP-VPN deployment requires expertise in BGP; BGP is a prerequisite for IP-VPN deployment, resulting in additional complexity

**MPLS-Based Enterprise WAN Connectivity**

**VPLS for WAN Connectivity**

Enterprises that currently deploy leased lines or Frame Relay/ATM virtual circuits for WAN connectivity can evolve their enterprise WAN connectivity to an MPLS-based infrastructure. VPLS provides an efficient solution for WAN connectivity by offering all the benefits of MPLS while allowing an enterprise to retain control over their enterprise WAN infrastructures.

Benefits of a VPLS service for WAN connectivity:
- A VPLS is a Layer 2 service; VPLS forwards traffic based on MAC addresses
- VPLS allows enterprises to benefit from Ethernet simplicity and higher speeds for connectivity between sites
- The enterprise retains complete control of their WAN network
- All routing decisions are controlled by the enterprise and there is no co-ordination required with the service provider (if the VPLS service is purchased from a service provider)
- VPLS in the WAN simplifies addressing in the WAN; since the WAN connection is like a logical LAN there is no need to plan/configure a subnet for each physical or logical WAN link (this simplifies routing connectivity)

The two options for implementing WAN connectivity using VPLS are discussed in the following sections.
**Self-deployed VPLS connectivity**

Figure 6 depicts how an enterprise can implement VPLS for connectivity of their wide area sites.

As shown in Figure 6, the head office and regional sites are connected via point-to-point Ethernet private lines or virtual leased lines which can be purchased from a service provider.

The WAN sites require a WAN router that can support Layer 2 and Layer 3 VPNs. For this scenario, VPLS support is mandatory in the WAN router.

The WAN router is configured with VPLS. Each router has a VB instance which performs MAC learning functions and maps traffic to corresponding MPLS label switched paths (LSPs) between the sites.

All WAN routers are connected to the same LAN segment.

VPLS allows connectivity of different applications within the enterprise. Data, voice and video can be assigned their dedicated VPLS instances across the wide area.

*Figure 6. Self-Deployed VPLS Connectivity*
**VPLS service from service providers**

An enterprise can subscribe to a VPLS service from a service provider that offers VPLS. As depicted in Figure 7, the routers in the service provider network support VPLS capability. Each connected enterprise site is assigned a dedicated VB (within the service provider’s network) that performs MAC learning. Each enterprise connected to the service provider network is configured with a unique set of VBs; this offers full separation and isolation for individual enterprises.

**Figure 7. VPLS Service from Service Provider**

---

**Provider-Managed Versus Self-Managed Layer 3 MPLS VPN**

**Provider-managed IP-VPN**

Provider managed IP-VPNs are one option for enterprises to connect wide area sites.

As depicted in Figure 8, an enterprise subscribes to an IP-VPN service from a service provider. The WAN router at the enterprise site is referred to as the customer edge (CE) router. The CE router connects to a service provider router referred to as the provider edge (PE) router. The CE router is typically managed by the service provider. The CE-to-PE connection may use static, routing information protocol (RIP), OSPF or BGP routing protocols. The PE router runs the IP-VPN functions as well as MPLS/BGP protocols.
The service provider manages the complexity of provisioning the PE nodes. The enterprise IP routes are redistributed into the service providers routing domain. The IP-VPN protocol offers unique and independent VRF instances which provide complete separation for the customers routing space, offering full security to each enterprise’s WAN connections.

Service provider managed IP-VPN service:
- The service provider acts as a partner to the enterprise for all aspects related to their IP-VPN-based WAN connectivity
- All IP addressing decisions require co-ordination with the service provider
- The enterprise must involve the service provider for any additions/changes to enterprise routing and policy
- The enterprise may lose control over their wide area network; sharing router table information could be perceived by some enterprises as a security risk
- Decision making cycles may take longer since it requires co-ordination with the service provider
- The benefits of reduction in cost and complexity must be weighed in relation to the extent of control that an enterprise may have to give away; this may not be a major issue for many enterprises, but some may prefer more control for their WAN connectivity
**Self-managed IP-VPN**

Figure 9 depicts a self-managed IP-VPN for the WAN. In this case, the enterprise WAN routers run the IP-VPN functions as well as MPLS/BGP protocols.

Typically, enterprises are less familiar with BGP implementations. Managing IP-VPNs adds complexity to the enterprise’s IT operations; options like VPLS can be a better choice for WAN connectivity.

The IP-VPN approach requires that an enterprise take on the complexity of deployment and management of the IP-VPN; it may be preferred by enterprise IT groups for some specific connectivity requirements like connectivity to extranets or to remove many of the constraints when subscribing to a service provider managed IP-VPN.

**Figure 9. Self-Managed Layer 3 VPN (BGP/MPLS IP-VPN)**
Service-Aware VPLS Infrastructure Campus Networks

Enterprises that have made the decision to implement MPLS within the campus network have the choice of deploying VPLS and/or IP-VPNs.

VPLS offers several advantages over IP-VPNs for MPLS-based campus deployments:

- VPLS offers the easiest and simplest way to migrate an existing campus infrastructure to an MPLS-based infrastructure
- Since VPLS is a Layer 2 VPN, no routing information has to be learned at each distribution node within the network
- Unlike an IP-VPN, which needs BGP to be configured on the distribution nodes, VPLS nodes do not need BGP

Figure 10 depicts a VPLS enabled campus network.

Access switches have the ability to support 10/100/1000 Mb/s access ports for bandwidth-hungry applications. A 1 Gigabit Ethernet (GigE) link can be used to interconnect access switches to the distribution MPLS nodes. Distribution-to-core MPLS node connectivity can use n* GigE or 10 GigE links. Core nodes interconnect to each other with 10 GigE links.

As depicted in Figure 10, the service-aware VPLS infrastructure provides support for all existing and new end-user applications/devices such as PC’s, IP telephones, wireless access points, CCTV cameras, etc.

End users and groups of user VLANs in the access switches are interconnected to VPLS instances in the distribution MPLS nodes. Research and development, marketing, and finance departments have separate dedicated VPLSs that terminate on a service routing MPLS node in the core layer.

Figure 10. VPLS and Centralized Service Routing
The core MPLS service node is the point where all Layer 3 (IP) routing decisions and policies are configured. The service nodes enable Layer 3 communications between the users and the application servers via the core layer. Typically a pair of service nodes is required for redundancy reasons. With this centralized approach to routing, the burden of setting up complex routing decisions and defining which user group has access to which set of applications, is contained in two centralized devices within the whole network.

A centralized approach to routing decisions is consistent with the way many existing enterprise networks are deployed today and is why the VPLS-based approach is preferable over the IP-VPN approach.

The service-aware VPLS infrastructure enables rollout of new services like video and voice, along with data services over IP. One approach is to deploy dedicated VPLS instances within the network for these applications; this simplifies the overall design for deployed new video and voice services.

Figure 11 depicts how a service aware VPLS infrastructure with multiple VPLS instances can be implemented.

Besides the VPLS instances for each division within the campus, separate VPLSs may be provisioned for voice and video services.

In this manner VPLS allows an enterprise to migrate to an MPLS-based infrastructure (and take advantage of all MPLS benefits) without taking on the added complexity of making drastic changes to the operational model and application connectivity within the campus.

Figure 11. Service-Aware VPLS Infrastructure for Campus Networks
A key element of reliable and flexible MPLS-based infrastructures is effective, simplified management tools that provide easy configuration and control of the network, fast, effective problem isolation and resolution, and support of new management applications.

The Alcatel-Lucent 5620 Service Aware Manager (SAM) is an integrated application that covers all aspects of element, network and service management on one platform. It automates and simplifies operations management for IP- and Ethernet-based services on a converged MPLS network. The Alcatel-Lucent 5620 SAM product suite supports element management, network mediation, network commissioning, service provisioning and service assurance for the Alcatel-Lucent 7750 Service Router (SR1, SR7, SR12), the Alcatel-Lucent 7710 Service Router (c4, c12), the Alcatel-Lucent 7450 Ethernet Service Switch (ESS-1, ESS-6, ESS-7, ESS-12), the Alcatel-Lucent 7250 Service Access Switch (SAS), Telco Systems T5C CLE (T5C-24G, 24GT, 24T, 48F, 48T), and third-party network elements.

The Alcatel-Lucent 5620 SAM also offers multivendor configuration and provisioning functionality that supports other Alcatel-Lucent network element types such as the Alcatel-Lucent OmniStack 6200, the Alcatel-Lucent OmniSwitch 6850 and Alcatel-Lucent OmniSwitch 9000 as well as any third-party CPE.

The Alcatel-Lucent 5620 SAM delivers the features that enterprise customers require to drive their operations to a new level of efficiency. It offers a carrier-grade application suite that consists of four functional domains covering element management (SAM-E), provisioning (SAM-P), Assurance (SAM-A) and OSS Interface (SAM-O).

**IP Routing Management Control**

The Alcatel-Lucent 5650 Control Plane Assurance Manager (CPAM) offers real-time control plane visualization, proactive control plane surveillance, configuration, validation and control plane diagnosis. In addition, by seamlessly integrating with the Alcatel-Lucent 5620 SAM, the Alcatel-Lucent 5650 CPAM provides simplified diagnosis and intuitive visualization of the relationship between services, the MPLS infrastructure and the routing plane.

The Alcatel-Lucent 5650 CPAM delivers this functionality based on real-time control plane information provided by the Alcatel-Lucent 7701 Control Plane Assurance Appliance (CPAA). The Alcatel-Lucent 7701 CPAA is a route listening and route processing hardware device that non-intrusively participates in routing plane signaling. It is based on Alcatel-Lucent's proven and evolving service router operating system (SR-OS) and it provides the Alcatel-Lucent 5650 CPAM with multi-vendor control plane topology visualization, including non-MPLS-based routers.

Integrated control plane and service management is an industry-first for service routing. It enables network managers to overlay Layer 2 and Layer 3 services, MPLS tunnels and various OAM traces on the control plane map to simplify problem resolution involving the need to correlate information between layers.

The Alcatel-Lucent 5650 CPAM allows network operators and routing architects to:

- Reduce control plane configuration errors due to manual command line interface (CLI) configuration validation
- Reduce troubleshooting time for control plane configuration, service/tunnel provisioning fall-outs and end-user service problem reports
- Proactively investigate control plane or service alerts to determine the control plane's impact on services
- Provide IP topology information to traffic engineering and operation support systems (OSS)
Summary and Conclusions

VPLS versus IP-VPNs Positioning for Enterprises

Table 2 summarizes the key differences between the possible roles of VPLS and IP-VPNs within an enterprise network.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>VPLS</th>
<th>IP-VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campus and WAN applicability</td>
<td>• Campus network</td>
<td>• WAN – Service-provider managed IP-VPN</td>
</tr>
<tr>
<td></td>
<td>• WAN – VPLS service from service provider</td>
<td>• WAN – Self-managed IP-VPN</td>
</tr>
<tr>
<td></td>
<td>• Metro – If fiber build-out is available, implement self deployed VPLS service</td>
<td></td>
</tr>
<tr>
<td>Connectivity</td>
<td>• Layer 2 multi-point</td>
<td>• Layer 3 multi-point</td>
</tr>
<tr>
<td>WAN control</td>
<td>• Full control of WAN</td>
<td>• Limited if service-provider managed IP-VPN</td>
</tr>
<tr>
<td>Routing management</td>
<td>• Less complex; no need for BGP expertise</td>
<td>• Not complex if purchased from service provider</td>
</tr>
<tr>
<td></td>
<td>• Independent of Layer 3 protocol; good for IPX/SNA-type protocols</td>
<td>• Requires co-ordination with service provider</td>
</tr>
<tr>
<td>Routed traffic</td>
<td>• Any Layer 3 protocol since VPLS is a bridged service</td>
<td>• IP only</td>
</tr>
<tr>
<td>Routing policy changes</td>
<td>• Totally transparent</td>
<td>• Requires co-ordination with service provider</td>
</tr>
<tr>
<td>WAN router configuration</td>
<td>• Simple, VPLS is analogous to a logical LAN; all WAN interfaces can be in the same subnet</td>
<td>• Each WAN link requires special address planning/IP subnet configuration</td>
</tr>
</tbody>
</table>

Conclusion

The enterprise and government IT group now have different choices of MPLS VPN technologies. Each organization is unique and the technology selection must be based on the connectivity and application requirements specific to the enterprise or government network.

MPLS is a very suitable technology for next-generation enterprise infrastructures. MPLS offers Layer 2 and Layer 3 VPNs that enable WAN connectivity between enterprise sites, as well as enabling implementation of next-generation campus networks.

VPLS introduces a very viable alternative approach for implementing WAN connectivity, as well as campus infrastructures. VPLS provides all the benefits of MPLS without adding the complexity of IP-VPNs. Since VPLS is a Layer 2 VPN, it is simpler to implement than alternative Layer 3 approaches like IP-VPNs.

All MPLS implementations are not equal. Today, campus networks rely predominantly on Ethernet switches. Most Ethernet switches offer very poor or limited scale/features for MPLS implementations. It is important to select products that are optimized for MPLS-based services.

Alcatel-Lucent – is a leader of MPLS-based implementations

Alcatel-Lucent has years of experience in developing MPLS-based technology. Alcatel-Lucent supports a complete MPLS offering (support for both Layer 2 and Layer 3 VPNs. Alcatel-Lucent’s IP/MPLS-based service routing and switching products offer enterprises the flexibility, scalability and feature sets required for next-generation enterprise and Government networks.
### Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>asynchronous transfer mode</td>
</tr>
<tr>
<td>BGP</td>
<td>border gateway protocol</td>
</tr>
<tr>
<td>CE</td>
<td>customer edge</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CRM</td>
<td>customer relationship management</td>
</tr>
<tr>
<td>ERP</td>
<td>enterprise resource planning</td>
</tr>
<tr>
<td>IP-VPN</td>
<td>IP virtual private network (a multipoint Layer 3 VPN based on MPLS, which is also referred to as 2547 VPN)</td>
</tr>
<tr>
<td>iBGP</td>
<td>internal border gateway protocol</td>
</tr>
<tr>
<td>IP</td>
<td>Internet protocol</td>
</tr>
<tr>
<td>IT</td>
<td>information technology</td>
</tr>
<tr>
<td>LAN</td>
<td>local area network</td>
</tr>
<tr>
<td>LSP</td>
<td>label switched path (an MPLS Layer 2 connection; this is a logical connection similar to a frame relay or ATM virtual circuit)</td>
</tr>
<tr>
<td>MAC</td>
<td>media access control</td>
</tr>
<tr>
<td>MPLS</td>
<td>multiprotocol label switching</td>
</tr>
<tr>
<td>OAM</td>
<td>operations, administration and maintenance</td>
</tr>
<tr>
<td>OSPF</td>
<td>open shortest path first</td>
</tr>
<tr>
<td>PE</td>
<td>provider edge</td>
</tr>
<tr>
<td>QoS</td>
<td>quality of service</td>
</tr>
<tr>
<td>RIP</td>
<td>routing information protocol</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>synchronous optical network/synchronous digital hierarchy</td>
</tr>
<tr>
<td>VB</td>
<td>virtual bridge</td>
</tr>
<tr>
<td>VLAN</td>
<td>virtual LAN</td>
</tr>
<tr>
<td>VLL</td>
<td>virtual leased line (a point-to-point Layer 2 VPN based on MPLS)</td>
</tr>
<tr>
<td>VPLS</td>
<td>virtual private LAN service (a multipoint Layer 2 VPN based on MPLS)</td>
</tr>
<tr>
<td>VPN</td>
<td>virtual private network</td>
</tr>
<tr>
<td>VRF</td>
<td>virtual routing forwarding</td>
</tr>
<tr>
<td>WAN</td>
<td>wide area network</td>
</tr>
</tbody>
</table>