




MPLS Networking

**Create a Secure Private Network
for Cloud Computing**

 **Learn More:** Call us at **877.634.2728.**

www.megapath.com

MegaPath's Secure Private Cloud for Networking

Your business may be considering a move to the “cloud” for some applications and communications services. Interest in cloud computing is driven by increasing expectations for always-on, geographically dispersed businesses—accompanied by decreasing budgets and staff availability to manage an in-house network.

But what does the cloud really mean to your network design and how you deliver voice and data services to users? What factors should you consider when evaluating how to use cloud-based applications with public and private network services? How do you create the best deployment of a private or hybrid public/private network for secure cloud computing?

Before moving to a cloud, it is important to identify the activities and applications that the cloud network will need to support. For example, do you want to:

- Access external storage and computing resources or cloud-based applications?
- Perform transactions—such as working with financial databases or verifying identities?
- Support real-time monitoring, collaboration, and instant communication?

The Drawbacks of a Public (Internet-Only) Network

After identifying your cloud computing goals, consider the type of network you want. Although a public network that uses the Internet to transport all traffic may seem like an attractive choice, it involves significant trade-offs for performance and security. Applications may not perform properly and/or bandwidth may not be available for mission-critical applications. Your network may suffer latency, jitter, and packet loss.

For performance, a public network provider using the Internet can only deliver a “best effort” priority level that applies to all traffic. This limitation exists because all Internet traffic is vulnerable to moment-by-moment congestion levels and routing path availability, which can render your applications unusable. Applications on a public network may create user frustration if the network delivers a slow response or when access is blocked because of Internet problems.

Security is another critical concern in using public networks. Private Networks, MPLS in particular, are less susceptible to Denial of Service (DOS) and other attacks than networks that utilize the public network for site-to-site communications. Additionally, although anti-virus, intrusion detection, and intrusion prevention services may be available, these services are usually applied only at the customer premises, which may be too late for protecting data and applications from unauthorized access, data theft, and disruption.

Together, the risk of network latency and security threats in a public network may outweigh the advantages of moving to a cloud environment in order to reduce computing costs and IT staff levels.

The Advantages of MegaPath’s Private MPLS-based Network for Cloud Computing

In contrast to the limitations of a public network, MegaPath’s private MPLS-based network offers many advantages for cloud computing. MPLS (Multi-Protocol Label Switching) has been the foundation technology for communications and creating private networks consisting of two or more locations. By design, MPLS creates a fully meshed network topology with multiple paths between any two or more sites. It automatically forwards your traffic via the optimal path, ensuring that packets—which carry data, voice calls, or video streams—are delivered quickly without bottlenecks or single points of failure. This efficiency makes MPLS ideal for supporting performance-sensitive applications such as Voice over Internet Protocol (VoIP) and videoconferencing, as well as financial and enterprise resource planning (ERP) transactions. Many large enterprises, healthcare organizations, government agencies, and other companies choose MPLS because of the advantages it offers for the safety and security of their networks and data.

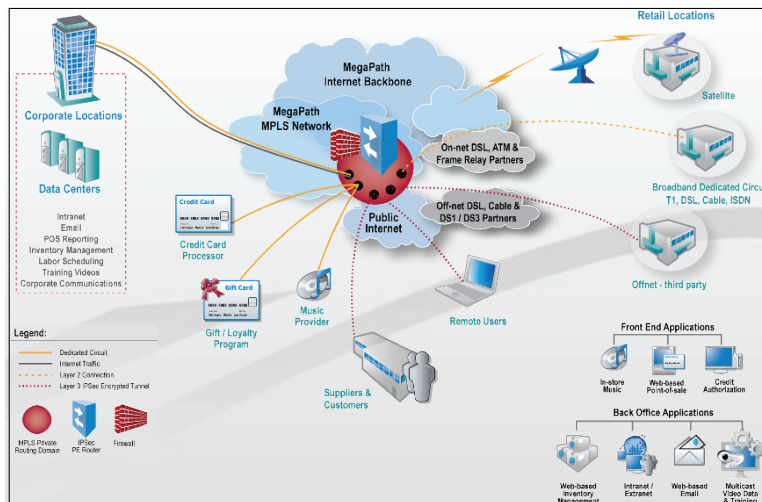


Figure 1. Private cloud design using a service provider’s MPLS network

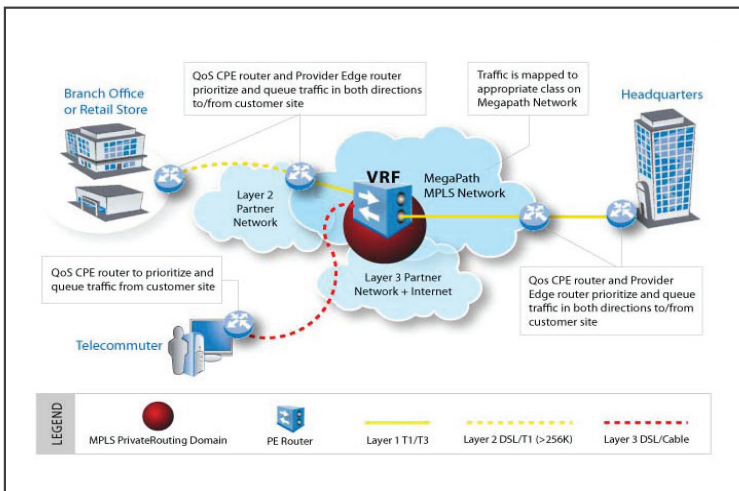
MPLS is both a secure and “self-healing” network that maintains multiple routes to cloud-based applications. If a private network becomes congested, the network can automatically reroute packets using another available path. In addition, Class of Service (CoS) definitions can prescribe the priority levels for certain types of packets (e.g., voice, video, and point-of-sale) throughout a private network to ensure your applications have the network resources available to function properly.

Additional security measures from MegaPath can protect your data if you include Internet access in your private network design. A gateway security service will check the data packets before they enter your private network looking for intrusions, viruses, and related threats. A MegaPath firewall can allow certain types of network traffic to access cloud-based applications, or it can deny external access.

MegaPath’s network plays a role your business’ cloud computing by connecting your business locations to each other and the Internet. This role means the capabilities of MegaPath’s network can greatly impact the performance, reliability, and security of your cloud-based applications.

MegaPath has an all-optical MPLS core network that offers a strong foundation for a private network because the MPLS network is engineered to maximize application performance. (Figure 1) Redundant OCx links and a fault-tolerant point-of-presence (POP) architecture maximize network uptime and reliability. In addition, MegaPath uses state-of-the-art MPLS routing technology to deliver your data with exceptionally low latency and packet loss.

High Performance from MegaPath with Traffic Shaping and Class of Service



A critical factor for the success of cloud computing is delivering high performance levels for each traffic type and application carried on the network. MPLS networks use Class of Service (CoS) tagging or labeling to shape voice, video, and data traffic, then maintain that priority across the network. This prioritization delivers the quality of service that is an important requirement for a provider's network. (Figure 2)

CoS rules ensure that voice calls and videos have optimal sound and playback quality. Additionally, IT managers can control bandwidth costs and network performance by using CoS to prioritize voice traffic ahead of data applications and real-time video conference streams ahead of stored video downloads.

Figure 2. How CoS prioritizes traffic on a MPLS network

As shown in Figure 2, a provider extends service classes to your sites using CoS-capable equipment to mark, queue, and prioritize traffic as it travels from the site to the MPLS network. This traffic marking and prioritization ensures consistent circuit performance for important applications. The provider-edge routers also prioritize and queue these traffic flows across the MegaPath MPLS network and in the return direction from the network to the site.

It is important to note that any traffic destined for the Internet cannot be prioritized once it leaves MegaPath's network because MegaPath has no control over the Internet routers. (A carrier may have its own Internet routers but cannot not control the Internet routers owned or managed by other carriers.) However, critical applications that access the Internet can still benefit from priority handling within MegaPath's network while en route to the Internet.

Although most service providers support some form of CoS prioritization in their MPLS networks, not all of these offerings are alike. Some service providers support only a few options for traffic prioritization CoS definitions, covering the broad categories of voice, video, and data. The most common definitions are:

- **Real-time:** Voice services and customer VoIP and video traffic
- **Critical:** Mission-critical data—such as financial transactions and credit card data transmission
- **Business:** Enterprise applications—such as SAP, Oracle, or video surveillance traffic
- **Data:** Low-priority traffic—such as Internet browsing, file transfers, and stored video downloads

The ability to create multiple CoS definitions helps you better manage traffic in a private cloud by:

- Prioritizing business-critical applications
- Controlling bandwidth allocations and avoiding the need to over-provision or dedicate circuits
- Promoting consistent, interruption-free network performance
- Preventing critical applications from failing or impacting the user experience due to network congestion

Protect Your Network with MegaPath’s Managed Security Services

To protect your cloud-computing solution, MegaPath offers powerful, cost-effective, and fully managed security solutions that are compliant with key industry standards, such as PCI and HIPAA. These services deliver a multilayer security approach that provides holistic protection from individual and blended threats, as well as coordinated security alerting, blogging, and reporting.

MegaPath offers cloud-based network edge protection, as well as site-level solutions to protect your assets from external and internal threats. Security solution components—which are managed and maintained by the provider—typically include managed firewalls; intrusion prevention systems; antivirus, anti-spyware, and anti-spam software; and Web and content/URL filtering tools. When delivered via a single platform, these components are classified as Unified Threat Management (UTM). When selecting a security solution, it is important to understand where the protection is being applied. In all scenarios, defense-in-depth is a best security practice.

MegaPath’s Connectivity Options for a Private Network

Multiple options for network connectivity are essential to meet the different needs of your sites and users. MegaPath offers connectivity to your MPLS network via DSL, T1, Bonded T1, high-speed Ethernet, Ethernet over Copper (EoC), wireless, and cable. (Figure 3)

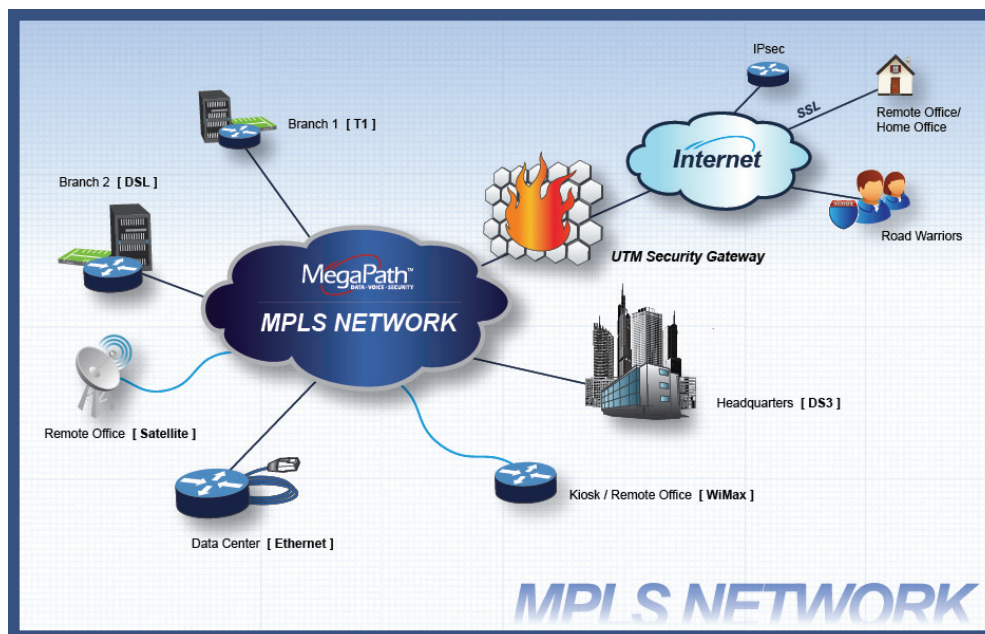


Figure 3. MPLS connectivity choices for remote sites and users.

MegaPath Managed VPN Services

MegaPath managed VPN services are another access option to consider. VPN services provide remote sites and users with secure, cost-effective connectivity over a service provider network or the Internet for remote sites and users. VPN services that are tailored for your business can deliver even more cost savings and performance benefits.

Most business needs can be met with one of the following VPN service types:

- **MPLS Site-to-Site VPN:** The service should consolidate business applications onto a private network with CoS rules, built-in security, and a choice of hosting and access options. The ability to integrate an IPsec VPN private network is important to cost-effectively reach remote sites. This integration results in a hybrid MPLS/IPsec VPN.
- **SSL VPN:** Especially for providing secure mobile access, this service should offer clientless, integrated network access based on secure sockets layer (SSL) technology. This service can be a cloud-based solution that enables secure remote access or it can use dedicated platforms to provide more granular access controls. Another use for SSL VPN is accessing in-store retail applications, such as point-of-sale systems and business reports, from any device virtually anywhere in the world.

MegaPath Network Services That Enhance Your Private Cloud

The MegaPath network alone can't help your business fully realize the benefits of cloud computing. Value-added services for voice and application server hosting are also important to consider in your private cloud design.

Voice Services

VoIP has become the technology of choice for businesses that want to replace an aging PBX or key system, or that are opening or moving an office. MegaPath's business-class voice services use advanced VoIP technology to reduce costs and offer advanced calling features, crystal-clear sound quality, and guaranteed QoS. MegaPath's voice services include:

- Hosted Voice replaces an on-site PBX with complete VoIP services from MegaPath's network cloud. At each site, phone calls are made over the same broadband connection used for internal network connections and Internet services.
- Integrated Voice combines voice and data over a single dynamic DSL, T1, or Ethernet connection to deliver concurrent call capacity to an existing PBX or IP PBX.

Hosted Collaboration Services from MegaPath

MegaPath also offers cloud-based collaboration tools—such as Hosted Exchange and Hosted SharePoint®—that enable businesses to improve communication, efficiency, and revenue by helping ensure that their employees, clients, and vendors can work smarter, more efficiently, and as a team, while avoiding the costs associated with administering an in-house system.

Hosted Microsoft Exchange features corporate-class email, shared calendaring, tasks, and contacts capabilities. Cloud-based hosted email services are a cost-effective and time-efficient alternative to purchasing and maintaining in-house email systems.

Hosted SharePoint® provides businesses with powerful tools that help employees maximize productivity, adapt quickly to changing business needs, and easily access vital information. It provides a flexible, customizable business collaboration platform that conforms to unique business needs, without the cost of in-house administration.

MegaPath’s Round-the-Clock Network Monitoring

MegaPath supports and proactively monitors our Data, Voice, and Security services on a 24 / 7 / 365 basis from multiple, redundant network and security operations centers. In order to prevent network outages, MegaPath’s engineers use carrier-class network management systems to continually groom the network, quickly diagnose and solve problems, and automatically reroute traffic and activate failover systems in the event of a network issue.

As part of MegaPath’s monitoring service, our customer portal provides complete visibility into your network connections and services. For example, use the portal to monitor availability, latency, jitter, packet delivery, bandwidth utilization, and mean opinion score (MOS) for voice traffic, as well as to review the results of circuit performance monitoring.

Evaluating Service Providers for Accessing a Private Cloud

Use this worksheet as a reference for evaluating the offerings and capabilities of potential network service providers for your private cloud.

Evaluation Factors	MegaPath MPLS Network	Alternate Provider #1	Alternate Provider #2
MPLS across the entire service provider network	X		
Class of Service definitions	4		
Strong service-level agreements	X		
Multiple connectivity options for each local site including a large EoC footprint	X		
SSL VPN options	X		
High-quality VoIP services	X		
Hosted Exchange and Hosted SharePoint services	X		
Managed security solutions with no need for special equipment at each site	X		
Security compliance with PCI and HIPAA	X		
Customer portal for network services management	X		
24 / 7 / 365 network and CPE monitoring and management	X		

Why MegaPath?

MegaPath is one of the largest facilities-based providers of managed network services in the United States, offering voice, data, and security services to enterprise and SMB customers. The MegaPath network is a nationwide, MPLS-enabled, all-optical, secure to the core IP network that provides quality of service through four CoS definitions for prioritizing critical voice and data traffic. For cloud computing, MegaPath can transport traffic among connected sites on its own network, avoiding the quality-impacting delays that can occur with providers who use the Internet for transport.

MegaPath security solutions deliver a comprehensive set of unified threat management (UTM) services that can be fully implemented in the cloud, at the customer's premises, or in a hybrid configuration to deliver unprecedented security. The MegaPath security solutions are compliant with stringent PCI and HIPAA security requirements.

Serving over 235 metro markets throughout the United States, MegaPath can combine the right access technologies, VPN and direct network connectivity, as well as security options to deliver a customized private or hybrid networks. MegaPath provides complete business solutions with its IP voice services that include hosted and premises-based solutions, data connections—including DSL, T1 and, high-speed Business Ethernet, and hosted collaboration solutions—Hosted Exchange and Hosted SharePoint®. MegaPath's security services are customized for private networking and provide complete data protection.

With one of the largest Ethernet footprints in the U.S., MegaPath offers economical Ethernet over Copper (EoC) services with speeds up to 45 Mbps in select major metropolitan areas. In other areas, choose from access options that meet your business needs—including T1 and DS3, DSL, cable, wireless, and satellite. All MegaPath network services are backed by comprehensive service-level agreements (SLAs).

When it comes to customer support, MegaPath is distinct from other providers in its offerings for project management, around-the-clock security and network monitoring, continuous device management, and comprehensive reporting.

For More Information

Learn more about MegaPath solutions for your business: www.megapath.com