

Multiprotocol Label Switching (MPLS) is a technology used by many telcos and ISPs to deliver services including VoIP. Many service providers are positioning this as a security technology, and are claiming that there is no need for additional security measures. This application note reviews the technology, use and limitations of MPLS from the stand-point of delivering comprehensive security in VoIP networks.

MPLS Technology

In order to deliver improved reliability and quality of service, telcos and service providers have long recognized the need for additional tools to make service improvements a reality in multi-purpose IP networks.

MPLS has evolved from earlier technologies developed by a number of networking vendors including Cisco Systems, IBM and Toshiba. Today's implementations provide powerful switching capabilities, used to route packets across WANs with previously unavailable control mechanisms. MPLS is used in conjunction with IP to deliver a number of services including VPNs and to deliver VoIP services.

MPLS can provide virtual IP network connections between an end-user and a service provider. The traffic on this virtual IP network need not be routable to the rest of the Internet and the result may be thought of as being similar to a VPN without encryption.

MPLS is also able to prioritise traffic depending on QoS (Quality of Service) flags. This provides an obvious benefit to real-time applications such as VoIP, with priority and improved voice quality over less time-critical applications such as email.

The same traffic prioritisation is used by some ISPs to delivery different levels of service. If you pay more, your traffic gets delivered at a higher priority, but you still share the same infrastructure with everyone else. This enables ISPs to offer a range of service levels as well as providing service level guarantees.

Although MPLS is widely deployed by service providers, it should be noted that there is no single MPLS standard. MPLS facilities are implemented in a variety of ways and there are numerous proposed standards documents currently under review.

Use and Deployment

MPLS is used by many service providers to deliver VoIP. This is done over a MPLS virtual link between the service provider and the customer. MPLS is terminated on a router which supports label switching at the customer site and standard IP directed either through a firewall or more likely directly into an IP PBX. MPLS is in many ways similar to VLANs, except that it works on WANs.

With this deployment model, MPLS is used only between the customer's network and the VoIP Service provider. The MPLS link may carry only VoIP traffic or may carry other traffic as well.

MPLS can also be used to provide virtual links between different office locations. For example a company in New York could use MPLS to route "private" traffic to London. MPLS labels data packets and forwards them over a public network but provides no additional security such as encryption. Security of the data is the customer's responsibility. MPLS provides optimized routing and faster switching, but does not explicitly provide any security measures such as encryption, and all data flows over public networks.

VoIP Security Issues

The key to understanding security issues is to remember that MPLS is not a security technology, it is a switching and routing technology. It is designed to operate at layer 2/3 and has no knowledge of any application security requirements. MPLS routes traffic between two or more points, for example between an IP PBX and a VoIP service provider. It does not examine the traffic at an application level and so has no way to detect or block threats such as flooding attacks or call disruption attacks. Customers are forced to rely on the integrity of their service providers.

If MPLS is used to route traffic between two office locations and if that traffic includes VoIP there is no protection for that VoIP stream unless it is provided by some other mechanism. The VoIP stream flows through the service provider's infrastructure where it can be monitored. Unless you absolutely trust the service provider, this is an issue.

A major weakness is that MPLS only works between the service provider and the terminating equipment in the customer's premises. If VoIP connections to other locations, e.g. roaming users and home workers, are used then these connections will run over a standard IP network. MPLS does absolutely nothing for this type of link, falling short when security is needed most.

Since the MPLS link terminates at the customer's external router the problem of firewall configuration still exists. Customers must still make the decision about routing SIP traffic through the firewall or directly to the IP PBX. Both solutions are extremely risky; the first can severely impact the security provided by the firewall when necessary configuration changes are made, and in either case the IP PBX is vulnerable to SIP application attacks.

Using MPLS to handle VoIP from a service provider does block other connections. However, attacks from the internal network are still possible and depending on the network topology attacks from outside may also be possible.

The use of MPLS for VPNs simply provides traffic isolation, much like an ATM or Frame Relay service. MPLS currently has no mechanism for packet encryption, so if customer requirements included encryption, some other method, such as IPsec, would have to be employed. The best way to think of MPLS VPNs is to consider them the equivalent of a Frame Relay or ATM virtual circuit.

Configuration complexity can also be a major vulnerability and since configuration is typically outside the control of the customer, the customer's network may operate with unknown and undetectable vulnerabilities.

MPLS and UM Lab's SIP Security Controllers

The range of SIP Security Controllers from UM Labs is fully compatible with MPLS. A SIP Security controller can be used as a perimeter security gateway and can secure VoIP and related services delivered over a MPLS link. The same Security Controller can also secure links to other remote locations that do not have the benefit of an MPLS service.

A SIP Security Controller can add a number of significant benefits when used in this way. These benefits are summarised in the following table which shows how the SIP Security Controller and an MPLS link can work together to provide an enhanced VoIP service.

Security Requirement	SIP Security Controller	MPLS
IP Level Security Controls	The SIP Security Controller includes a robust IP Security module optimised for handling VoIP traffic.	<p>MPLS does not directly provide IP Level Security controls. Most organisations would choose to deploy a dedicated IP Security gateway (Firewall) at the network perimeter.</p> <p>If a SIP Security Controller is used in conjunction with an MPLS circuit, then the necessary IP Level security at the corporate network perimeter is optimised for VoIP applications.</p>
VoIP Protocol and Application Security	<p>The SIP Security Controller protects against malformed SIP requests, flooding attacks, call disruption threats, call hijacking and other related threats.</p> <p>A locally administered SIP Security Controller can be configured with knowledge of the local domain and network work configuration and so is in the optimum position to block this class of threat.</p>	<p>MPLS cannot protect against any of these threats. With MPLS alone the only defence is assumption that all of the service provider's systems are completely reliable and the provider implements their own robust security controls preventing any accidental or malicious threat from reaching your corporate VoIP system.</p> <p>If the service provider relays calls from other providers then many of those threats are outside of the provider's direct control.</p>
Content Security	The SIP Security Controller protects against content threats which include call monitoring, and RTP injection attacks. Also, if you are running related services such as presence or SIP based IM, malicious content threats.	MPLS cannot protect against any of these threats.
SIP Signalling Encryption	The SIP Security Controller runs SIP over TLS, the standard for SIP signalling encryption providing direct interoperability with an increasing number of soft-phones and hardware phones and some PBXs.	MPLS does not directly provide any encryption services. In some cases encryption services may be provided over an MPLS connection. However as these services are unlikely to follow the documented standard for SIP signalling encryption, interoperability is limited.
RTP Media Encryption	The SIP Security Controller uses SRTP, the standard for media encryption. The Security controller also offers two standard key exchange protocols, SDES and ZRTP each of which are suited to different application areas. These media encryption standards are supported by a growing number of soft-phones, hardware phones and some PBXs.	MPLS does not directly provide any encryption services. In some cases VPN services may be provided over an MPLS connection. However as these services are unlikely to follow the documented standard for media encryption, interoperability is limited.

Security Requirement	SIP Security Controller	MPLS
Securing Connections from SIP Trunk providers	The SIP Security Controller is designed to provide security for any remote SIP connection, including a SIP trunk connection.	MPLS provides traffic separation and prioritisation on SIP trunk connections, both of which are valuable services, but MPLS does not directly offer any security controls.
Secure Connections from remote users	The SIP Security Controller is designed to provide security for any remote SIP connection, including connections to remote users.	MPLS is a switching protocol that routes traffic over a service provider's network. It has no role to play in providing VoIP services to home workers and roaming users.
Secure Internet Calling	The SIP Security Controller is designed to provide security for any remote SIP connection, including securing calls to other users over the Internet.	MPLS is a switching protocol that routes traffic over a service provider's network. It cannot provide these services when calls are made to or accepted from other Internet connected users.
Local NAT and far-end NAT traversal	<p>When VoIP services are provided to remote users, the VoIP data stream must navigate both local and far-end NAT gateways. This is a significant challenge to all VoIP deployments.</p> <p>The SIP Security Controller automatically handles local NAT and all far-end NAT traversal challenges.</p>	MPLS avoids the NAT problem but this solution works only on the link to and from the service provider. MPLS does not provide a solution for other remote links.

SIP Security Controllers from UM Labs have been designed to provide comprehensive security for all SIP based VoIP and Unified Messaging applications. The focus on providing perimeter security means that customers are provided with true application-level security, the ability to manage their own security policies and avoid the possible vulnerabilities introduced by dependence on complex configuration management in service provider data centers.

About UM Labs UM Labs Ltd. was founded in 2008 by security software pioneers dedicated to the promotion of secure global standards for unified communications. The company has an extensive support organization and partner network, with offices in the following locations:

United Kingdom

Heathrow Blvd 4
280 Bath Road
West Drayton
UB7 0DQ
UK
Phone: +44 20 3021 3200

Website: um-labs.com

USA

5586 Main St, Suite 206
Williamsville
NY 14221
USA
Phone: 716 568-4931

Email: info@um-labs.com

Canada

366 Adelaide St, Suite 301
Toronto, ON
M5V 1R9
Canada
Phone: 416 598-7537

VoIP: sip:info@um-labs.com