Q&A

Cisco IOS® MPLS Bandwidth-Assured Layer 2 Services

What is Cisco IOS® MPLS Bandwidth-Assured Layer 2 Services?

Cisco IOS® MPLS Bandwidth-Assured Layer 2 Services is a solution that enables service providers to offer premium Layer 2 services over an MPLS network. Service providers can offer Frame Relay, ATM, Ethernet, Point-to-Point Protocol (PPP), and High-Level Data Link Control (HDLC) services to their customers with tight QoS guarantees, extremely high levels of availability, and a great deal of flexibility. These Layer 2 services can be offered with proper internetworking functionality to satisfy varied customer requirements or overcome geographical or technological limitations of a specific Layer 2 service. MPLS Bandwidth-Assured Layer 2 Services ease the implementation of protected services, along with tight guarantees for packet latency, jitter, or loss to meet different customer needs. Cisco IP Solution Center (ISC) 3.1 allows service providers to easily deploy and manage the different components of this solution.

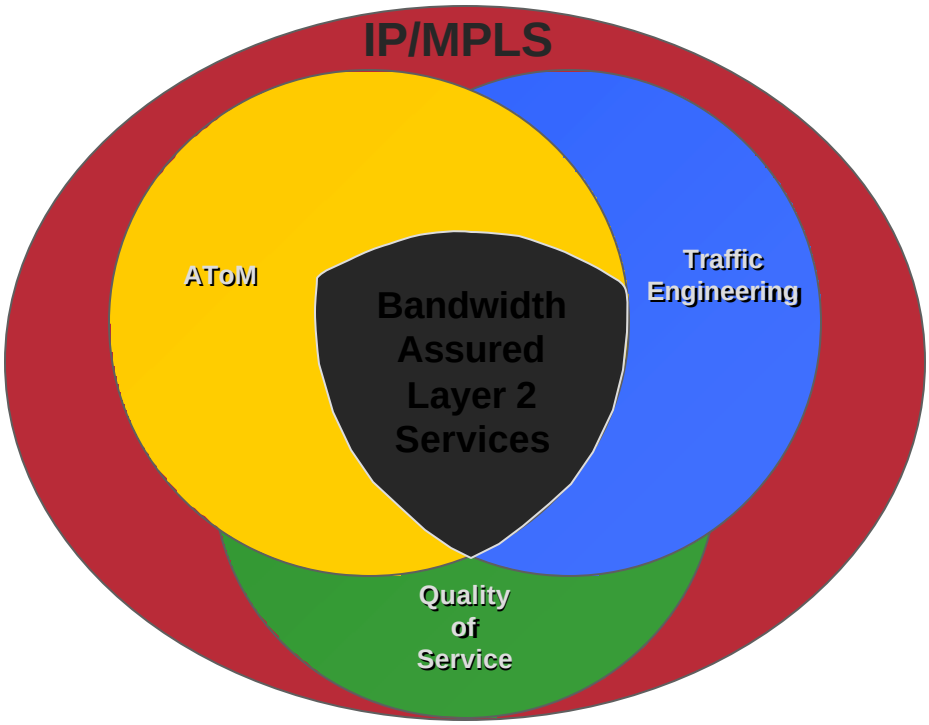
Why is Cisco IOS MPLS Bandwidth-Assured Layer 2 Services important for service providers?

Cisco IOS MPLS Bandwidth-Assured Layer 2 Services help service providers migrate to a truly converged network infrastructure in a cost-effective manner. Using MPLS as their core network, service providers can use the same network infrastructure to offer Frame Relay, ATM, Ethernet, PPP, HDLC, IP VPN, and Internet services, among others, in a scalable and very flexible solution. The consolidation of all these services on a common network brings economies of scale that can result in very significant capital expenditure (CapEx) and operating expenses (OpEx) savings. This convergence also brings new revenue opportunities to many service providers by enabling a greater number of Layer 2 and Layer 3 services that can be offered either directly by them or by extending existing services. The future success of many service providers will certainly be influenced by their ability to provide a diverse portfolio of network services to their customers in a very flexible and cost-effective way.

What technologies enable Cisco IOS MPLS Bandwidth-Assured Layer 2 Services?

Cisco IOS MPLS Bandwidth-Assured Layer 2 Services are enabled by a combination of multiple MPLS applications (Figure 1). The key components of this solution are Cisco Any Transport over MPLS (AToM), Cisco MPLS Traffic Engineering (TE), and Cisco MPLS Quality of Service (QoS). Cisco AToM provides the emulation and service interworking between different Layer 2 services. Cisco MPLS TE enables protected services, enhances point-to-point service-level agreements (SLAs), and provides greater routing control of Layer 2 traffic through the MPLS network. Cisco MPLS QoS supports traditional Layer 2 SLAs, such as those offered by ATM and Frame Relay, and helps to generate new revenue opportunities by making possible newer and more elaborate offerings for technologies, such as Ethernet. In addition to these components, Cisco ISC 3.1 facilitates the provisioning and management of each of these technologies to provide an end-to-end management solution.

Figure 1. Components of Bandwidth-Assured Layer 2 Services



Layer 2 Services Using Cisco Any Transport over MPLS (AToM)

What is Cisco AToM?

Cisco AToM provides the emulation of a Layer 2 service, such as Frame Relay, ATM, Ethernet, PPP, or HDLC across an MPLS network. This emulation provides behavior and characteristics that faithfully resemble the original service. Using Cisco AToM, a service provider can offer multiple Layer 2 services without building multiple networks or can easily extend the geographical span of its existing services. Cisco AToM is built around the work of the Pseudo Wire Emulation Edge to Edge (PWE3) working group at the IETF to provide a standards-based solution.

What Layer 2 services can be implemented with Cisco AToM?

Cisco AToM supports the emulation of Frame Relay, ATM, Ethernet, PPP, and HDLC services in operation modes relevant to the service. For Frame Relay, a service provider can emulate individual permanent virtual connections (PVCs) or can trunk a number of PVCs in a port-mode configuration. ATM traffic can be transported as ATM Adaptation Layer 5 (AAL5) for services based on this frame format. Alternatively, ATM traffic can be transported as cells carried individually or packed according to application requirements. These encapsulations can be implemented at a port, PVC, or permanent virtual path (PVP) level. In the case of an Ethernet service, a service provider can emulate individual virtual LANs (VLANs) or can transport traffic with an 802.1q or standard Ethernet encapsulations in a port-mode configuration. PPP and HLDC services are emulated with a port-mode configuration.

What is Layer 2 Interworking?

Layer 2 Interworking provides the translation mechanisms necessary to offer Layer 2 services with disparate termination circuits. Currently, a service provider customer can purchase a Layer 2 service (Frame Relay, ATM, Ethernet, PPP, or HDLC) and may be able to get some service interworking capabilities, such as ATM to Frame Relay service. With Layer 2 interworking using Cisco AToM, the same customer can have the Layer 2 service terminated with the technology most appropriate for a particular site according to the service geographical coverage and the customer requirements, including CPE functionality, service SLA, or circuit speed. The technology used to terminate the Layer 2 service on one end does not preclude the use of other technologies for the remote end. A service provider can easily offer a more flexible Layer 2 service with greater interworking capabilities, such as Ethernet to ATM, Frame Relay to Ethernet, and PPP to Frame Relay. In particular, the ability of providing Layer 2 service interworking between multiple technologies plays an important role for the introduction of high-speed services based on Ethernet.

How is Layer 2 Interworking implemented?

Cisco AToM currently provides two solutions: Ethernet Interworking and IP Interworking. Ethernet Interworking (also called bridged interworking) transports Ethernet frames across the Layer 2 service. It is especially appropriate for interworking between Ethernet and other Layer 2 services. Non-Ethernet circuit require support for bridged encapsulation. IP Interworking (also called routed interworking) transports IP packets across the Layer 2 service. This approach does not have special encapsulation requirements, but can only carry IP traffic end to end. The Layer 2 interworking approach used in a particular scenario depends on specific customer requirements and the functionality that the service provider can provide. In some scenarios, Ethernet Interworking may be more appropriate, while in others, IP Interworking may be preferred.

How does Ethernet Interworking operate?

Ethernet Interworking (also called bridged interworking) relies on the transport of Ethernet frames across the Layer 2 service. For non-Ethernet circuits, the customer-edge (CE) device needs to natively bridge Ethernet traffic onto the circuit or route traffic using a bridge encapsulation model, such as integrated routing and bridging (IRB) or routed bridged encapsulation (RBE). The PE device uses an emulated Ethernet virtual circuit across the MPLS network to achieve service interworking. CE devices are ultimately exchanging Ethernet frames. This Layer 2 service interworking approach does not impose any restriction on the upper layer protocols that use the Layer 2 service.

How does IP Interworking operate?

IP Interworking (also called routed interworking) transports IP packets across the Layer 2 service. The CE device can route IP packets onto the circuit without any special encapsulation requirement. The PE device uses an emulated IP virtual circuit across the MPLS network. With IP Interworking, the CE devices are ultimately exchanging IP packets. This Layer 2 interworking approach does, however, impose a restriction on the type of traffic that can be carried by the Layer 2 service. CE devices can only route IP traffic. On the other hand, IP Interworking does not impose any special encapsulation requirement on CEs as is the case with Ethernet interworking.

What Layer 2 Interworking combinations are currently supported by Cisco IOS Software?

Table 1 illustrates Layer 2 interworking support as introduced in Cisco IOS Software Release 12.0(26)S. Additional interworking combinations may be supported in the future based on customer demand.

Table 1. Layer 2 Interworking support in Cisco IOS Software Release 12.0(26)S

	Frame Relay	ATM AAL5	Ethernet	Ethernet VLAN	PPP	HDLC
Frame Relay	-	IP	IP Ethernet	IP Ethernet	IP	-
ATM AAL5	IP	-	IP Ethernet	IP Ethernet	-	-
Ethernet	IP Ethernet	IP Ethernet	-	IP Ethernet	-	-
Ethernet VLAN	IP Ethernet	IP Ethernet	IP Ethernet	-	-	-
PPP	IP	-	-	-	-	-
HDLC	-	-	-	-	-	-

Can Cisco IP Solution Center (ISC) be used to provision and manage Cisco AToM?

Yes. Cisco IP Solution Center (ISC) can be used to provision and manage Layer 2 services that use Cisco AToM. This Cisco product can provision Frame Relay, ATM, and Metro Ethernet services. Service providers can take advantage of the provisioning functionality in ISC for the deployment of Layer 2 services. This functionality includes auto discovery, provisioning based on current network, policy-based provisioning, managed services, role-based access control, user access control and a template manager, among other features.

What Cisco IOS Software release is required for Cisco AToM?

Cisco AToM functionality has been introduced gradually starting with Release 12.0(22)S. Layer 2 Interworking was first introduced in Release 12.0(26)S. Documentation can be found at http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/index.html.

Cisco MPLS Traffic Engineering (TE) and Cisco AToM

Why is Cisco MPLS TE important for Cisco IOS MPLS Bandwidth-Assured Layer 2 Services?

Cisco MPLS TE enhances the transport of Layer 2 service across an MPLS network. The Fast Reroute (FRR) functionality in MPLS TE allows a service provider to offer protected Layer 2 services in a very cost-effective manner. In addition, the combination of quality of service (QoS) and MPLS TE can be used to deploy a scalable implementation of the tight point-to-point SLAs that customers have come to expect from traditional Layer 2 services, such us ATM and Frame Relay. Similarly, QoS and MPLS TE can be used to enhance the SLAs that have been traditionally offered for Ethernet services. Last, MPLS TE enables the service provider to optimize bandwidth utilization in the MPLS backbone which can directly or indirectly benefit Layer 2 services.

How can you select the TE Label Switching Path (LSP) that will carry AToM traffic?

Cisco IOS Software introduced the AToM Tunnel Selection feature in Release 12.0(25)S to provide fine-grain control for the mapping of Layer 2 traffic to TE LSPs. With AToM Tunnel Selection, the PE device can map an individual Layer 2 circuit to a TE LSP for which the PE is a head end. For this mapping to occur, the TE LSP has to be locally defined as the preferred path to the egress PE across the MPLS network for that particular Layer 2 circuit. Additionally, the ingress PE can implement a fall-back mechanism where traffic is routed through an alternate default LSP in case the TE LSP fails. Given that a TE LSP can serve different purposes, the service provider could, for instance, configure a PE device to route a Layer 2 circuit highly sensitive to packet delay and loss through a protected TE LSP that has been engineered for low delay guarantees. At the same time, Layer 2 circuits carrying bulk traffic that require best-effort service could be mapped to a TE LSP that uses spare bandwidth capacity along a route that does not follow the shortest path to the egress PE. In addition to Cisco AToM Tunnel Selection, Cisco MPLS TE Auto-Route and static IP routes can be used to direct Layer 2 traffic into TE LSPs as previously available in Cisco IOS Software. These two mechanisms, however, provide less flexibility than Cisco AToM Tunnel Selection.

Does Cisco MPLS TE affect how Layer 2 circuits are signaled and encapsulated across an MPLS network?

No. The signaling of virtual circuits across the MPLS network and the encapsulation of the Layer 2 traffic that Cisco AToM provides is independent of the characteristics of the LSP carrying the traffic. Both the signaling and the encapsulation remain the same for RSVP LSPs and label distribution protocol (LDP) LSPs.

Can Cisco MPLS TE be used to offer protected Layer 2 services?

Yes. Layer 2 services can benefit from the cost-effective protection solution offered by Cisco MPLS TE FRR. Those Layer 2 circuits carried by protected TE LSPs will experience short restoration times. Those Layer 2 circuits carried by unprotected TE LSP or by regular LDP LSPs will experience longer restoration times depending on the convergence time of the Interior Gateway Protocol (IGP) used in the MPLS backbone. Cisco MPLS TE FRR appropriately reroutes Layer 2 traffic whether the failure is detected by the ingress PE or an intermediate node. In addition, the bandwidth protection enhancements to Cisco MPLS TE FRR can be used to provide greater protection. This gives the service provider a wide range of alternatives from using unprotected TE LSPs, to using connectivity-protected TE LSPs, to using full-bandwidth-protected TE LSPs. The decision of what level of protection to use for Layer 2 traffic can be made for each individual Layer 2 circuit by making use of AToM Tunnel Selection.

Can Cisco MPLS TE be used to switch AToM traffic according to its packet delay, jitter, and loss requirements?

Yes. Cisco MPLS TE can be combined with Cisco QoS to define multiple paths between PEs that satisfy different SLAs. Cisco MPLS TE features such us DiffServ-Aware Traffic Engineering (DS-TE), FRR, and bandwidth protection can be used for this purpose. Along with these

Cisco MPLS TE features, Cisco MPLS QoS provides traffic differentiation in the backbone based on experimental (EXP) bits. A service provider may choose to build multiple TE LSPs using DS-TE, protecting TE LSPs intended for the traffic that is most sensitive to packet loss, and supporting multiple classes of service on the MPLS network. There are multiple design alternatives that give the service provider a wide range of design options, from simple to elaborate.

Does all Layer 2 traffic have to be carried by a TE LSP?

No. The service provider can make that decision when a new Layer 2 circuit is being provisioned. The Layer 2 traffic can be carried entirely by TE LSPs, entirely by LDP LSPs, or by a combination of both according to the service requirements.

How can you use Cisco AToM Tunnel Selection if the PE devices are not part of the MPLS TE network?

Cisco AToM Tunnel Selection requires at least one TE LSP between the Cisco AToM PEs. Network designs where TE LSPs are defined between provider-core (P) devices have less control of what Layer 2 circuits are carried by TE LSPs. For those scenarios, Layer 2 services still benefit from the deployment of Cisco MPLS TE, but provider devices typically route aggregate traffic into TE LSPs, and traffic differentiation per circuit or per service is usually more complex, and sometimes not possible.

Is there any restriction on MPLS TE features that can be used with AToM?

No. The emulation of Layer 2 services using Cisco AToM is independent of the LSP that finally carries the traffic and the mechanisms used to build that LSP. This separation allows Cisco AToM to potentially benefit from any enhancements made to Cisco MPLS TE.

Does MPLS TE have any scalability effects on the implementation of Layer 2 services?

No. There is no special scalability effects when Cisco MPLS TE is used to carry Layer 2 services. The scalability of such solution is dictated by the scalability of each of its individual components: Cisco MPLS TE and Cisco AToM. Neither suffers a scalability impact due to the other.

Which Cisco IOS Software release is required for using Cisco MPLS TE and AToM?

In general, Cisco AToM features can make use of any existing Cisco MPLS TE features. One special case was the support for fast rerouting Layer 2 traffic when the ingress PE acts as a point of local repair (PLR). Support for this functionality was introduced in Cisco IOS Software Release 12.0(24)S. In addition, the Cisco AToM Tunnel Selection feature requires Cisco IOS Software Release 12.0(25)S.

Enhanced Quality of Service (QoS) for Layer 2 Services

Why is Cisco QoS important for Cisco IOS MPLS Bandwidth-Assured Layer 2 Services?

Cisco QoS is an important requirement for implementing traditional and new Layer 2 services. Frame Relay and ATM are widely deployed Layer 2 services that have well-defined SLAs. The transport of those services over an MPLS network requires no loss of functionality. For Layer 2 services that are becoming more popular, such as Ethernet, QoS plays a critical role in offering sophisticated SLAs that allow service providers to differentiate their offerings. Even though TE contributes to the implementation of tight SLAs, it is not a QoS mechanism by itself. A Layer 2 service requires the QoS mechanisms that can prioritize traffic in the MPLS network.

Are new QoS functions required to offer Layer 2 services with MPLS?

Yes. The PE device is required to enforce a Layer 2 SLA. This usually implies classifying, policing, re-marking, and differentiating traffic based on Layer 2 packet markings. Additionally, the PE device needs to mark MPLS-encapsulated Layer 2 traffic with the appropriate value in the EXP bits so that the core of the network can provide this traffic with the appropriate QoS treatment. The PE device needs to classify inbound Layer 2 traffic based on ATM cell loss priority (CLP) bit, Frame Relay discard eligibility (DE) bit, or 802.1p bits according to the technology. That same device needs to be able to queue outbound Layer 2 traffic based on EXP marking and implement a queuing policy that penalizes out-of-profile traffic over in-profile traffic in case of network congestion. The PE device also needs to be able to re-mark the outbound Layer 2 traffic based on ATM CLP bit, Frame Relay DE bit, or 802.1p bits according to the technology. For Frame Relay and ATM, the PE device may also need to mark the Layer 2 traffic to notify congestion conditions to the Layer 2 service endpoints.

Does Cisco AToM impose any special QoS requirements for the MPLS backbone?

No. The MPLS backbone usually differentiates traffic in terms of classes according to the packet EXP value, regardless of the application that generated the MPLS packet. This approach results in a very scalable and efficient solution to QoS in the backbone, where provider devices only deal with classes and do not need to keep track of individual service or customer details. The specifics of the QoS design in the backbone depend on business and technical considerations. For many service providers, a simple and scalable QoS design guarantees a wide spectrum of SLAs with a high level of certainty, even in the presence of transient congestion, failure conditions, planning mistakes, or denial-of-service (DoS) attacks.

Can Cisco IP Solution Center (ISC) be used to provision QoS?

Yes. Cisco ISC can be used to provision and manage Cisco QoS features. Service providers can take advantage of all the provisioning functions in Cisco ISC for the deployment of QoS-enabled Layer 2 services. These functions include auto discovery, provisioning based on current network, policy based provisioning, managed services, role-based access control, user access control, and a template manager, among other features.

What Cisco IOS Software release is required for QoS support for Layer 2 services?

Cisco IOS Software Release 12.0(25)S introduced the first group of QoS features required to support Layer 2 services using MPLS. Additional functions were introduced in Release 12.0(26)S. Documentation can be found at http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/index.html.

Building Cisco IOS MPLS Bandwidth-Assured Layer 2 Services

Are there any architectural restrictions on how AToM, QoS and MPLS TE can be combined to offer Layer 2 services?

No. Cisco MPLS provides a layered and modular architecture where MPLS TE and QoS mechanisms can be used as the base to implement and enhance other applications. Future enhancements to Cisco MPLS TE and Cisco MPLS QoS can be expected to enhance the transport of Layer 2 services over an MPLS network.

Are all components of Cisco IOS MPLS Bandwidth-Assured Layer 2 Services required to offer a Layer 2 service?

Most service providers will find Cisco IOS MPLS Bandwidth-Assured Layer 2 Services a necessary instrument to successfully offer Layer 2 services over an MPLS infrastructure. Cisco IOS MPLS Bandwidth-Assured Layer 2 Services are enabled by the combination of Cisco AToM, Cisco MPLS TE, and Cisco QoS. Cisco AToM is a definitive component of any solution because it provides the basic encapsulation and signaling mechanisms needed to emulate Layer 2 service over an MPLS network. While not every Layer 2 service will make use of Cisco MPLS TE and Cisco QoS, the service provider will certainly use different combinations of these technologies to satisfy service requirements and offer a comprehensive portfolio of services.

Does Cisco IOS MPLS Bandwidth-Assured Layer 2 Services preclude the implementation of Layer 3 VPN services over the same network infrastructure?

No. One of the benefits that service providers seek when deploying MPLS is the ability to provide multiple services over a single network infrastructure. Due to the inherent nature of MPLS, the core devices do not need to be aware of the service associated with packets that travel through an LSP. In this way, those core devices switch traffic in a service agnostic manner. Only PE devices have to implement the signaling and encapsulation specifics of Layer 3 and Layer 2 services. PE devices do not have to be dedicated to one service or another.

Does MPLS Bandwidth-Assured Layer 2 Services preclude the use of the same network infrastructure for other services, such as Internet connectivity?

No. MPLS allows service providers to deploy a converged network infrastructure that supports multiple services. Internet service can still be provided using the same network infrastructures. MPLS provides complete traffic isolation between Layer 3 VPN service, Internet service, and any other service deployed over the same infrastructure.

Where can additional sources of information about Cisco IOS MPLS Bandwidth-Assured Layer 2 Services and its components be found?

The following links provide additional information about Cisco IOS MPLS Bandwidth-Assured Layer 2 Services and its components:

Cisco IOS Software Release 12.0S Documentation

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/index.html

Cisco Technical Assistance Center (TAC) MPLS Page

http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Internetworking:MPLS

Cisco IOS MPLS Page (external)

http://www.cisco.com/go/mpls

Cisco IP Solution Center

http://www.cisco.com/en/US/partner/products/sw/netmgtsw/ps4748/index.html

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico• The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe