What It Takes To Build MPLS+ Managed Services

Blue Coat works with service provider partners to implement the underlying infrastructure that delivers managed services for multi-protocol label switching (MPLS). With the increasing shift to Web-enabled applications and SaaS solutions hosted in the cloud, greater application awareness, intelligence and control are critical to maximize MPLS investments. Organizations continue the consolidation of the data center to contain costs and realize security, compliance and “green IT” benefits. The key is in combining MPLS investments with adjacent application visibility, acceleration and security technologies to more effectively enhance the prioritization of traffic. Only Blue Coat offers the breadth of technologies in a single platform that empowers service providers to differentiate their MPLS solution and enable the upsell to value-added managed services.

Introduction to next-generation MPLS networks

Throughout the telecom industry the shift to standardized, end-to-end IP-based networks has been underway for well over a decade. As part of this shift, MPLS has been adopted as a key protocol-agnostic, data-carrying technology to help service providers better scale their networks and offer traditional packet-level interconnections or virtual private networks at a much lower cost. Leveraging a common infrastructure, MPLS has also opened the door to a host of new revenue-generating opportunities.

Starting in 2000, many enterprises and public sector organizations started to adopt MPLS as a cost-cutting strategy to migrate off of legacy WAN technologies like international Frame Relay, leased lines and ATM. Equant (now Orange Business Services) and Infonet (now BT Global Services) were early in providing MPLS-based networks. At that time the shift was mostly driven by early adopters who found MPLS provided significant benefits around cost, but also greater flexibility in how they deployed a global WAN infrastructure. The adoption of MPLS today represents a key area of revenue growth and sales focus for most global service providers who provide enterprise WAN services.

According to a Forrester Research report published in 2009, 35% of global firms with more than 1,000 employees have already fully deployed MPLS and another 9% are rolling it out, while 32% are evaluating or piloting the technology. And Forrester says 37% of firms are using site-to-site MPLS delivered as a managed service. The combination of strong demand for MPLS combined with the preference to purchase and deploy MPLS as a managed service is clearly defining the opportunity. In fact, according to an Infonetics Research note published in 2008, the overall MPLS market is worth more than $13 billion with strong growth forecast through 2011.

In addition to providing managed network services based on MPLS, service providers are seeing an opportunity to layer on value-added services like ethernet over MPLS, WAN optimization and other application-oriented security and performance management services. Blue Coat is ideally suited to help service providers roll out MPLS and generate incremental revenues through MPLS+ managed services.

Class-of-service definition in an MPLS world

A key technical advantage of MPLS is the flexibility it provides around class-of-service (CoS) to manage application performance. For example, service providers will often pre-define bandwidth allocation for each CoS to prioritize VoIP, video and mission critical data over email or Web traffic. But as an increasing amount of traffic moves to the Web over HTTP and HTTPS protocols, service providers are unable to distinguish between business applications and personal Web transactions such as a Webmail session. As an example, it is impossible to give special priority treatment to prioritize SAP or Salesforce.com over generic Web traffic.

MPLS relies on the capabilities of existing routers to set CoS policies and their exceptions through custom Access Control Lists (ACL). Unfortunately, routers have limited intelligence beyond routing packets according to rudimentary CoS assigned, say, to all traffic over a given port. Attempting to control traffic for a distributed WAN comprising hundreds of routers can quickly become unmanageable this way. Custom ACLs would require complex configurations for each router to assure fail-over scenarios, affecting manageability and router performance.
Blue Coat adds value to network investments with MPLS+

Blue Coat dramatically simplifies the ability to set CoS and fully leverage the prioritization of traffic allowed by MPLS. Service providers are able to upgrade networks with MPLS services more quickly and profitably. Blue Coat decreases the management complexity of offering differentiated MPLS services by removing the need for special rules or ACLs at the router beyond their simply acknowledging assigned CoS tags.

The Blue Coat ProxySG appliance provides a simplified management interface that allows for Type of Service (ToS) bits to be set in the IP header, which are then used to define CoS for that traffic within the MPLS network. At the simplest level, Blue Coat supports the ability of CoS tagging based on user authentication and an understanding of who the user is. More interestingly, it also allows for CoS tagging to be set on more detailed information about the actual application traffic. An example of how the Blue Coat ProxySG setting of ToS bits might play out in an MPLS environment is how an enterprise employee interacts with three unique web applications:

- Business-critical enterprise application
- Personal online banking site
- Accessing Webmail account

In all three of these instances, this traffic would occur on a Web channel, such as Port 443. Where traditional methods would force brute CoS definition based on all traffic on this port, Blue Coat acts more intelligently on this traffic to set policy and associated priority.

**Business-critical enterprise application** – In the case of the business user accessing a Web application like SAP, a higher priority and CoS tagging may be desired across the MPLS cloud, giving it priority over recreational Web usage such as accessing an online video. With Blue Coat in place at the branch and data center, the secure SAP traffic could be identified as a business-critical Web application, decrypted, and then accelerated across the MPLS cloud with the appropriate, higher priority CoS tag set.

**Personal online banking site** – In comparison, the same user might go online to do personal banking again using the HTTPS protocol running over Port 443. In this situation, Blue Coat could add value by identifying the transaction as personal banking and not decrypting the traffic to protect privacy, preserve security of the session, and apply no acceleration or higher prioritization.

**Accessing Webmail account** – Lastly, this same user later in the day might access an online Webmail account like Gmail or Yahoo! Blue Coat would not boost the prioritization of this traffic or accelerate it, but at the outbound Internet gateway could decrypt traffic and scan to prevent leaked data or malware communications.

In all three of these examples, the old approach of using router-based ACLs for setting CoS would lead to the same MPLS priority being set for all three of these Web activities. In truth, a business that wants to fully leverage its MPLS infrastructure and prioritize the network to best align with business objectives, would want to accelerate and boost priority for only the traffic that matters.

With Blue Coat it is possible to understand the user and the application, and put these two attributes into context to derive a better alignment of infrastructure to business needs. This culminates in the same user, doing the same browser-based Web activity, but receiving a very different handling of this traffic behind the scenes based on a deeper awareness of what they are actually doing. This level of intelligence synergy allows service providers to dramatically differentiate their MPLS offerings and create upsell opportunities for MPLS value-added services around acceleration or security.

Other acceleration approaches force all traffic to be accelerated in the same fashion, regardless of whether recreational or business-critical applications. Without the ability to distinguish between applications, point acceleration solutions are unable to take advantage of MPLS prioritization. Unlike Blue Coat, they lack the technical ability to set ToS bits and take advantage of MPLS prioritization. Finally, they also lack the integrated security features necessary to secure SSL communications, prevent data leaks and compliance breaches, or prevent malware from accessing the network.

**The Blue Coat MPLS+ vision**

Blue Coat offers the breadth of managed services, available in a single platform – from application performance monitoring to WAN optimization and security – enabling service providers to further drive their MPLS selling efforts, and provide complementary technologies to enhance the upsell to value-added managed services. Blue Coat calls this our MPLS+ story and today works with leading global service providers like AT&T, BT, Orange, Verizon, Sprint, NTT, and others to deliver on this vision.