

A Study on Any Transport over MPLS (AToM)

Tran Cong Hung, Ph.D. (*Posts & Telecommunications Institute of Technology, Viet Nam*)

E-mail: conghung@ptithcm.edu.vn

Le Quoc Cuong, Ph.D. (*Posts & Telecommunications Institute of Technology, Viet Nam*)

E-mail: lequoccuong@ptithcm.edu.vn

Tran Thi Thuy Mai, Eng. (*Posts & Telecommunications Institute of Technology, Viet Nam*)

E-mail: ttymai@gmail.com

Abstract - Recently there has been an increasing market demand to provide metropolitan and longer-reach Ethernet connectivity. According to a Yankee Group estimate, in 2001 the market for virtual private network (VPN) services over traditional (ATM and Frame Relay) transports was three times larger than IP VPN services in 2000, although the IP (including Multiprotocol Label Switching [MPLS]) segment is growing much faster and could eclipse traditional services before 2005.

This growth, combined with the increasing need to protect existing infrastructure and provide traditional point-to-point connections of different types, has pushed service providers to look for solutions that allow them to carry Layer 2 and Layer 3 traffic across a common, converged, single infrastructure without changing the existing service models.

Thus Cisco has an opportunity to deliver its Layer 2 tunneling solutions to address this market requirement. Cisco Any Transport over MPLS (AToM) is one such solution that addresses the needs of providers who would like to deploy MPLS and offer services such as Layer 2 aggregation and virtual leased lines using MPLS traffic engineering and quality of service (QoS) along with Cisco AToM.

Our paper “A study on Any transport over MPLS” is divided into the following main parts: *The first part* present “Introduction”. *The second part* present “AToM pseudowire operation”. *The third part* present “AToM and QoS support”. *The fourth part* present “DiffServ and AToM”. *The fifth part* present “Configuration Examples for AToM by NS2”. *The sixth part* present “Conclusion”.

I. INTRODUCTION

Any Transport over MPLS (AToM) was developed years after the huge success of MPLS VPN.

MPLS VPN is the virtual private network (VPN) solution to carry customer IP traffic over a shared MPLS service provider backbone. However, the leased lines, ATM links, and Frame Relay links still generate a lot of money for service providers. Many customers lease ATM or Frame Relay virtual circuits from a service provider and use them to carry their traffic

between their sites, across the infrastructure provided by the service provider. The customer has routers or other networking devices in each site, and the devices are interconnected via the leased lines, ATM virtual circuits (VCs), or Frame Relay VCs.

The service provider has a specific network built to carry the Layer 2 traffic from the customers. The routers from the customer are interconnected at Layer 3, but they do not interact with the equipment of the service provider at Layer 3. With the success of MPLS VPN, the service provider has an MPLS backbone set up, but the service provider still has the legacy network to carry the Layer 2 traffic from the customers. AToM provides a solution whereby the MPLS backbone also carries the Layer 2 traffic from the customers, thereby eliminating the need to run two separate networks side by side. Thus, the service provider can provide an existing service (ATM, Frame Relay, and so on) over the MPLS backbone. Using only one network infrastructure to provide both MPLS VPN and AToM services enables the service provider to save money. Customers are unwilling to migrate to the MPLS VPN solution for two reasons. The first reason is that they want to retain complete control over their network and the way it is built. The second reason is that they have legacy equipment (for example, IBM FEP) running protocols that cannot be carried over IP.

Whereas MPLS VPN provides a service of creating VPNs at Layer 3, AToM creates VPNs at Layer 2 and is sometimes referred to as L2VPN. The AToM intelligence is limited to the provider edge (PE) routers. Therefore, AToM is an edge technology—like MPLS VPN—that uses an MPLS backbone. However, AToM is limited to creating a Layer 2 point-to-point service, which is referred to as virtual private wire service (VPWS). You can also use MPLS to create a Layer 2 point-to-multipoint service. This service is referred to as Virtual Private LAN Service (VPLS), “Virtual Private LAN Service.” This chapter covers only AToM, the Layer 2 point-to-point service.

Any Transport over MPLS (AToM) is Cisco's solution for transporting Layer 2 packets over an IP/MPLS backbone. AToM is provided as part of the Unified VPN portfolio of leading-edge VPN technologies available over the widest breadth of Cisco routers. Cisco support for AToM enables service providers to provide connectivity between customer sites with existing data link layer (Layer 2) networks, by using a single, integrated, packet-based network infrastructure—a Cisco MPLS network. Instead of separate networks with network management environments, service providers can deliver both traditional ATM and Frame Relay connections and Ethernet connections over an IP/MPLS backbone.

The AToM product set accommodates many types of Layer 2 packets, including ATM, Ethernet, Frame Relay, PPP, or High-Level Data Link Control (HDLC)- based networks across multiple Cisco router platforms. With Cisco AToM technology, provisioning and connecting is straightforward. A customer using Ethernet within a building or campus in one location can connect via a service provider offering Ethernet over MPLS to the customer's Ethernet networks in distant locations. A service provider offering Cisco AToM-based services enables Layer 2 networks such as ATM or Frame Relay networks to make new point-to-point connections much more easily.

With point-to-point virtual circuits built with Cisco AToM, the Layer 2 connections retain their character as VPNs. The customer controls traffic routing within the network, and the routing information resides on the customer's routing equipment. The service provider's packet network equipment supplies point-to-point connections or an emulated pseudowire required by the customer.

Cisco AToM provides a common framework to encapsulate and transparently transport any traffic type over an MPLS network core. Service providers can use a single IP/MPLS network infrastructure and network management environment to offer customers connectivity for ATM, Frame Relay, Ethernet, PPP, and High-Level Data Link Control (HDLC) traffic, as well as carry customers' IP traffic in Layer 3 VPNs. Importantly, service providers can use Cisco superior capabilities in QoS to assure appropriate levels of service for different types of traffic. Cisco AToM saves money for service providers, and Cisco QoS provides ways to gain incremental

revenue for premium classes of service.

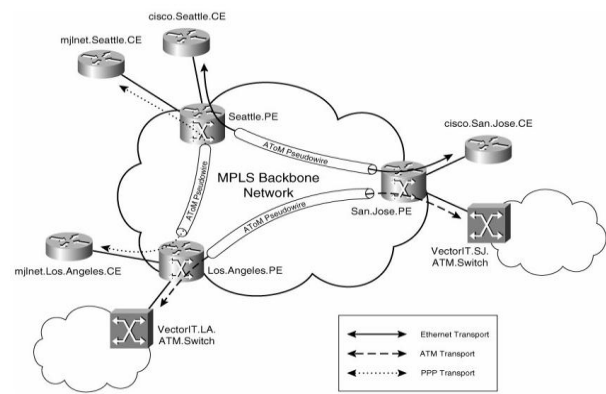


Figure 1-1. Transport of Layer 2 Protocols and Connections over AToM Pseudowires

In figure 1-1, ATM traffic is transported over an AToM pseudowire between VectorIT.LA.ATM.Switch and VectorIT.SJ.ATM.Switch; PPP traffic is transported over an AToM pseudowire between mjlnet.Los Angeles.CE and mjlnet.Seattle.CE; and Ethernet traffic is transported over an AToM pseudowire between cisco.Seattle.CE and cisco.San Jose.CE.

II. ATOMPSEUDOWIRE OPERATION

Figure 2-1 shows how a Layer 2 packet travels from Site 1 to Site 2 in VPN A, using the IP/MPLS backbone.

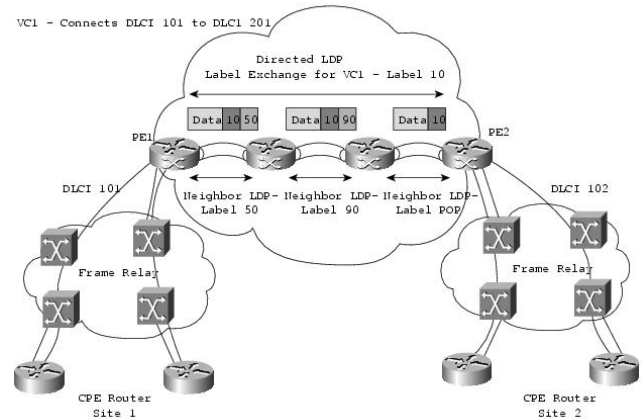


Figure 2-1 Layer 2 packet travels from Site 1 to Site 2

- The following process shows a Layer 2 packet traveling from Customer Edge 1 (CE1) on VPN A (Site 1) across the service-provider network, to CE 2 on VPN A (Site 2). CE1 connects to the Provider Edge 1 (PE1) on the service-provider network through a traditional Layer 2 virtual circuit, such as a Frame Relay, data link connection identifier (DLCI 101), virtual circuit. The packet travels from CE1 to PE1 through that circuit.

- In the service provider network, an operator configures a label switched path (LSP) from PE1 to PE2
- For AToM, the operator configures
 - (At PE1, a cross-connect between Attachment VC 101 and Emulated VC1, and the destination PE to be PE2
 - (b) At PE2, a cross-connect between Emulated VC1 and Attachment VC 201, and the source PE to be PE1
 - Note: No AToM configuration is required on the P routers.
- At PE1, the following events take place on the ingress interface of the router:
 - An incoming packet on the ingress line card of the provider-edge router is stripped of the Layer 2 header.
 - A control word and virtual-circuit label [10] are pushed on the packet.
 - An appropriate network-facing interface is selected.
 - A tunnel label is pushed (for normal MPLS routing through the cloud).

The control word and the virtual-circuit label are pertinent only to the ingress and egress provider-edge routers. The routers within the MPLS backbone (the P routers) do not use the control word or the virtual-circuit label. Instead, the P routers use the tunnel label [50 & 90] to move the packet through the MPLS backbone. A P router does not distinguish AToM traffic from other types of traffic. The packet is handled just like other packets in the MPLS backbone.

- The packet is sent through the service-provider network to PE2.
- The following events take place on the egress router PE2:
 - The virtual-circuit label [10] is stripped.
 - The control word is processed and stripped.
 - The header is reconstructed.
 - The packet is sent out the appropriate customer-facing interface.

No tunnel label is present in the network-facing side of the router because that label was popped by the penultimate router.
- PE2 connects to CE2 through a traditional Layer 2 virtual circuit, such as Frame Relay (DLCI 102) virtual circuit.

III. ATOM AND QOS SUPPORT

QoS sorts and classifies packet requests into different traffic classes and allocates the proper resources to direct traffic based on various criteria, including application type, user or

application ID, source or destination IP address, and other variables.

The bits in the packet translate to the priority of the packet. For MPLS packets, the MPLS experimental bits, also known as the EXP bits, allow you to specify the QoS for an MPLS packet. For an IP packet, the IP Precedence/differentiated services code point (DSCP) bits allow you to specify the QoS for an IP packet.

When an IP packet travels from one site to another, the IP Precedence field (the first three bits of the DSCP field in the header of an IP packet) specifies the QoS. Based on the IP Precedence marking, the packet is given the desired treatment such as the latency or the percent of bandwidth allowed for that class of service. If the service-provider network is an MPLS network, then the IP Precedence bits are copied into the MPLS EXP field at the edge of the network. When an Ethernet frame travels from one site to another, the 802.1P field (three bits in the Ethernet header) specifies the QoS. Similarly for Frame Relay, the discard-eligible bit specifies the discard eligibility of the Frame Relay frame and for ATM, the cell loss priority (CLP) field specifies the cell loss priority of the cell being carried. This marking can be translated to the MPLS EXP field for preservation and transportation of QoS across the provider network.

If the service provider wants to set the QoS of an MPLS packet to a different value than that of the IP Precedence bits or the Layer 2 frame bits, the service provider can set the MPLS EXP field instead of overwriting the value in the customer's IP Precedence field or the Layer 2 header. The IP header or the Layer 2 frame remains available for the customer's use and is not changed as the packet travels through the MPLS network.

Service providers can classify MPLS packets according to their type, input interface, and other factors by setting (marking) each packet within the MPLS EXP field without changing the IP Precedence/DSCP/Layer 2 field. For example, service providers can classify packets with or without considering the rate of the packets that PE1 receives. If the rate is a consideration, the service provider marks in-rate packets differently from out-of-rate packets.

This setup allows service providers to offer different grades of service for the same transport type to different customers. You can use QoS in MPLS networks to prioritize certain packets, just as you would prioritize IP packets. In the case of IP, you set the precedence or DiffServ Codepoint (DSCP) bits in the IP header to prioritize the IP packet. In the case of

MPLS, you prioritize the packet by setting the Experimental (EXP) bits to a value between 0 and 7. The MPLS payload is a frame instead of an IP packet in the case of AToM. Three possibilities exist for marking the EXP bits:

- Statically configuring the setting of the EXP bits
- Marking the EXP bits according to the IP precedence bits
- Using information from the frame header to set the EXP bits

You can statically configure the EXP bits by using Modular QoS Command Line Interface (MQC) on the router. You must configure a policy on the ingress interface (customer CE-facing interface) that sets the MPLS EXP bits. It is important to note that the EXP bits are set in both the tunnel and the VC label. This is important in the (default) case of PHP where, at the last P router, the tunnel label is removed, and the packet arrives at the egress PE with only the VC label in the label stack. Therefore, you must also set the EXP bits in the VC label if you want to preserve the QoS information that is encoded in MPLS all the way to the egress PE router.

IV. DIFFSERV AND ATOM

The motivations for DiffServ and AToM include user demands for consistent QoS guarantees, efficient network resource requirements by network providers, and reliability and adaptation of node and link failures. DiffServ provides scalable edge-to-edge QoS, while AToM performs traffic engineering to evenly distribute traffic load on available links and fast rerouting to route around node and link failures. Moreover, AToM can be deployed over a wide variety of link layer technologies such as IP, ATM, and Frame Relay. This paper first explains the combination between AToM and DiffServ. It then presents results from an event-driven simulation using Network Simulator (NS-2) to show how it works.

DiffServ provides scalable and “better than best-effort” QoS. DiffServ routers is stateless and do not keep track of individual microflows, making it scalable to be deployed in the Internet. The DiffServ Code Point (DSCP) in the Differentiated Services (DS) field of the IP header identifies the Per Hop Behavior (PHB) associated with the packet, which is used to specify queuing, scheduling, and drop precedence. There are three defined PHBs: Best effort, Assured Forwarding (AF), and Expedited Forwarding (EF). A PHB group is a set of PHBs that must maintain the order of packets in microflows. A behavior Aggregate (BA) is an aggregate of microflows with the same DSCP.

At the ingress node in a DiffServ domain, the DSCP value is determined based on multifold classification of the incoming packet. At the interior nodes, the PHB is determined from the DSCP and appropriate QoS treatment is applied to the packet. At the egress node, the packet is routed to the next hop in the next domain. Traffic conditioning is performed at the boundary nodes to ensure the traffic streams conform to the traffic conditioning agreement (TCA) between two domains. There are two basic problems for MPLS support of DiffServ. First, the DSCP is carried in the IP header, but the LSRs only examine the label header. Second, the DSCP has 6 bits but the EXP field has only 3 bits. There are two solutions defined to remedy these two problems: EXP-Inferred-PSC LSP (E-LSP), and Label-Only-Inferred-PSC LSP (L-LSP).

A. Advantages of DiffServ

Scalability:

Scalability is very important concern as a network core can have large number of flows and any protocol which requires to maintain per flow state or computational complexity does not scale well. DiffServ aggregates flows and hence can handle large number of flows. Also since PHBs are essentially kept simple, DiffServ lends itself well to use at high speeds making it scalable in terms of speed.

Ease of administering

In a Differentiated Services framework, different DiffServ domains can implement PHBs as they see fit as long as the bilateral agreements that it makes with the other domain are met. This gives the service providers a freedom to choose their implementation as a consequence they can provide Differentiated Services with minimal change in their infrastructure.

Simplicity

The DiffServ implementation does not diverge a lot from the basic IP. Hence it maintains simplicity and ease of implementation /upgradation at the cost of granularity.

Measurable

Since at each hop in a DiffServ domain, the traffic conditioners and shapers are constantly measuring arrival data and the link schedulers are monitoring packets to be sent, not much effort is required to procure vital information about the behavior of the network. The service providers can use the information to best allocate bandwidths and make service level agreements with the user.

B. AToM and DiffServ

1. Motivation

AToM and DiffServ share some common points. Both models do aggregation of traffic at the edge and processing of the traffic only at the core. Both models are scalable. AToM offers many advantages to service providers. However, it is incapable of providing differentiated service levels in a single flow. Hence AToM and DiffServ seem to be a perfect match and if they can be combined in such way to utilize each technology's strong points and counter the other's weaknesses, it can lead to a symbiotic association that can make the goal of end to end QoS feasible.

Note that either DiffServ or AToM can be used to offer some services with differing QoS. Any routing scheme can be used in a DiffServ network and some level of service differentiation will be perceived by the users due to the way packets with different codepoints are treated at DiffServ nodes. AToM networks can be configured to offer different QoSs to different paths through the network. If the two technologies are combined, then standardized DiffServ service offerings can be made and AToM can facilitate great control over the way these services are implemented. Such control means that it is more likely the operator will be able to offer services within well-defined QoS parameters.

2. DiffServ aids AToM in following ways

AToM only aids layer3 QoS and does not introduce a new QoS architecture. So DiffServ can help AToM by providing the QoS architecture to AToM networks.

AToM being a path-oriented mechanism, when used in backbone networks can give rise to scalability problems especially with RSVP-TE. AToM and DiffServ combination gives rise to networks where there is no per-flow state to be maintained in core routers. Only per-LSP state is to be maintained. If DiffServ is not used, and IntServ is used with AToM (as is proposed in a new draft), There will be the overhead of maintaining both per-flow state and per-LSP state. With LSP aggregation, one can reduce the number of LSPs.

DiffServ can provide differentiation of service within each flow.

The aggregated flow scheme of DiffServ not only reduces the flow state overhead, but also enhances the performance of AToM by reducing the number of labels to be managed.

3. AToM aids DiffServ in many ways

When link failures happen, AToM-based fast rerouting aids DiffServ in guaranteeing much stricter QoS. Of

course, link failures are not day-to-day occurrence in backbone networks. Traffic Engineering is provided by AToM to DiffServ. You can visualize different paths for different PHB groups, resource-preemption, different protection levels for different PHBs etc.

When you want to use DiffServ in heterogeneous link-layer environments, for example, in ATM networks, AToM is pretty much the best option to go for. Of course this may not be a great need, given the excellent QoS guarantees supported by ATM.

V. CONFIGURATION EXAMPLES FOR ATOMBY NS2

A. Simulation Aims and Environment

The aim of this simulation is to underline the need of integration of AToM with DiffServ. AToM rerouting is shown in this simulation as the motivating reason behind the AToM and DiffServ integration. AToM traffic engineering is an other important reason for AToM and DiffServ integration, but will not be dealt with here. The environment consists of ns-2 network simulation software in Linux operating system. Two ns-2 patches, the DiffServ patch and the MPLS patch were applied to execute the simulations.

B. Simulation Setup and Details

Figure 5-1 below shows the topology that was used in the simulation.

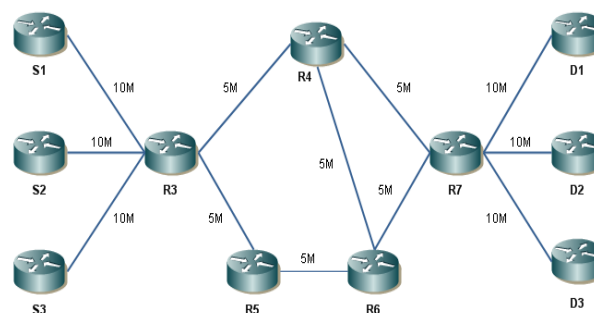


Figure 5-1 Simulation Topology

C. Simulation Results

1. AToM with no DiffServ

AToM can calculate and set up LSPs to make Quality of Service. The result followed:

	UDP 1	UDP 2	UDP 3
Packet size (bytes)	1000	1000	1000
Rate (Mbps)	2.5	2	1.5

LSP	3-4-7	3-5-6-7	3-5-6-7
Packet forward	7158	5753	4311
Packet lose	0	0	0
Packet lose percent (%)	0.0	0.0	0.0

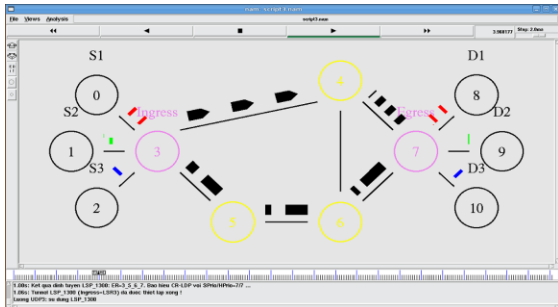
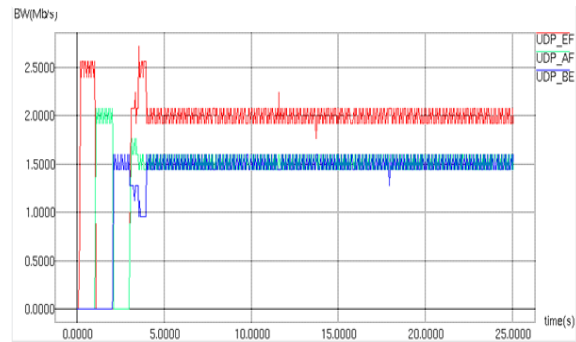


Figure 5-2 Simulation AtoM with no DiffServ

	UDP_EF	UDP_AF	UDP_BE
Packet size (bytes)	1000	1000	1000
Rate (Mbps)	2.5	2	1.5
LSP	3-4-7	3-4-7	3-4-7
Packet forward	7154	5750	4309
Packet lose	1324	1345	32
Packet lose percent (%)	18.5	23.3	0.74

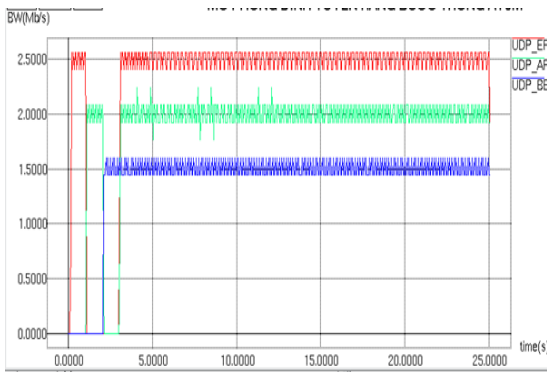


Figure 5-3 The flow rate

2. AtoM with DiffServ

	UDP_EF	UDP_AF	UDP_B E
Packet size (bytes)	1000	1000	1000
Rate (Mbps)	2.5	2	1.5
Mark Code	10	20	30
Packet lose priority	Low	Normal	High
Bandwidth (Mbps)	2.5	2	0.5

When the flow increase highly and fast, LSPs can not satisfy, so Packet lose percent increase.

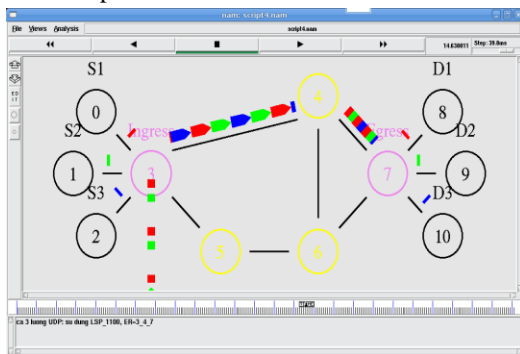


Figure 5-4 Simulation AtoM with no DiffServ and high flow

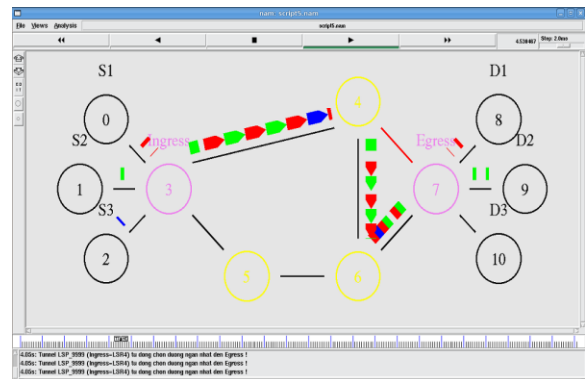
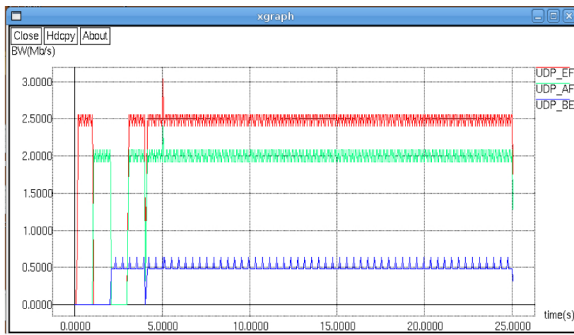


Figure 5-5 Simulation AtoM combine DiffServ



VI CONCLUSION

Concepts of DiffServ and AToM was presented, focusing on the operational procedures of E-LSP and L-LSP. This was followed by some simulation results to underline the need of DiffServ and AToM based on AToM-based rerouting. Currently, while multicast communication requires further study. Use of the EXP field to support Explicit Congestion Notification (ECN) together with DiffServ is also under development. Finally, there is not a cookbook approach as to how to combine both E-LSP and L-LSP efficiently, leaving open the research opportunities on the topic of DiffServ and AToM.

Future work should concentrate on simulations with more realistic topologies and different TCP sources like HTTP web traffic as observed. AToM-based traffic engineering is another important advantage to DiffServ. Similar experiments can be done to highlight these advantages.

Reference

- [1] Wei Luo, Carlos Pignataro, Dmitry Bokotey, Anthony Chan, “**Layer 2 VPN Architectures**”, Cisco Press 2005
- [2] Luc De Ghein, “**MPLS Fundamentals**”, Cisco Press 2007.
- [3] Mark Lewis, “**Comparing, Designing, and Deploying VPNs**”, Cisco Press 2006.
- [4] Lancy Lobo, Umesh Lakshman, “**MPLS Configuration on Cisco IOS Software**”, Cisco Press 2005.
- [5] RFC 4385, “**Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN**”
- [6] RFC 3985, “**Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture**”
- [7] Website: <http://pwp.net.cabo.pt/amsoares/dynamips/dynamips.htm>
- [8] Website: <http://dynagen.org/tutorial.htm>
- [9] Forum: <http://vnpro.org/forum/index.php>