Application Note: MPLS Networking with the EdgeMarc Network Services Gateway

Summary

This application note provides a description of how to deploy EdgeMarc Network Services Gateways in DiffServ aware MPLS Networks. DiffServ enabled EdgeMarcs combine multiple priority queues with traffic shaping to accommodate multiple applications with different needs for bandwidth and priority. The EdgeMarc is used to provide a consistent level of service to the enterprise in MPLS based virtual private networks.

Introduction

In the early days of IP networking, traffic on IP networks was delivered on a best effort basis. The best effort delivery method was sufficient at that time for the available applications which did not require any guarantees on packet loss, delay or jitter in the network. As time progressed, newer technologies gave birth to applications that required considerably less latency, jitter, and packet loss. The best effort delivery method could not always meet these more stringent requirements. In addition, Service Providers (SPs) could not reliably offer any Service Level Agreements (SLAs) to their customers.

Multi Protocol Label Switching (MPLS) presented the SPs with the opportunity to provide SLAs to their customers as it not only carves out a predetermined path in the network for connection oriented application packets (such as voice), but also provides guarantees on bandwidth, latency, jitter, and packet loss among other parameters. In addition, the Fast Reroute (FRR) link protection feature of MPLS made it possible to restore connectivity in milliseconds in the case of a link or node failure. Without FRR, the network re-convergence used to take a few seconds in the best case. FRR provides link protection to Label Switched Paths (LSP) by setting up a backup tunnel around the failed link.

Even though MPLS is deployed to prevent congestion, it is possible for congestion to occur during FRR. Therefore, it is imperative that critical services, such as voice, receive the necessary Quality of Service (QoS) even during FRR, if SPs were to maintain their SLAs with their customers. Differentiated Services (DiffServ) provides the solution to this problem by enabling priority queues for each Class of Service (CoS) in the PE routers of the MPLS network as well as the customer premise equipment (CPE) installed at the enterprise location. This allows SPs to provide end to end class of services between applications. In short DiffServ together with MPLS resolves the congestion problem completely which enables SPs to price their value added services differently resulting in increased revenues and margins.

EDGEWATER NETWORKS, INC.
Converged Networking. Simplified.

Class of Service information is stored in the three most significant bits of the Type of Service (TOS) byte of the IP header for each IP packet. DiffServ uses the DiffServ Code Point (DSCP) to distinguish between different classes of traffic while some SPs use the IP Precedence portion of the TOS byte. The DSCP is stored in the first six most significant bits in the TOS byte of the IP header. Based on the DSCP, each router in the path decides how to route the packet. The table below shows all possible DSCPs and IP Precedence values.

Associated Priority Queue	First 6 most significant bits of TOS byte from left to right					
	3 Bits			2 Bits		1 Bit
	IP Precedence	DSCP				
		Per Hop Behavior	Binary Value	Drop Probability	Binary Value	Unused
1	Routine	Best Effort (BE)	000		00	0
2	Priority	Assured Forwarding (AF11)	001	Low	01	0
		Assured Forwarding (AF12)	001	Medium	10	0
		Assured Forwarding (AF13)	001	High	11	0
3	Immediate	Assured Forwarding (AF21)	010	Low	01	0
		Assured Forwarding (AF22)	010	Medium	10	0
		Assured Forwarding (AF23)	010	High	11	0
4	Flash	Assured Forwarding (AF31)	011	Low	01	0
		Assured Forwarding (AF32)	011	Medium	10	0
		Assured Forwarding (AF33)	011	High	11	0
5	Flash Override	Assured Forwarding (AF41)	100	Low	01	0
		Assured Forwarding (AF42)	100	Medium	10	0
		Assured Forwarding (AF43)	100	High	11	0
6	Critical	Expedited Forwarding (EF)	101	N/A	11	0
7	Internetwork Control	N/A	110	N/A	N/A	N/A
8	Network Control	N/A	111	N/A	N/A	N/A

Table 1: TOS byte values

EDGEWATER NETWORKS, INC.
Converged Networking. Simplified.

DiffServ and IP Precedence in EdgeMarc Network Services Gateways

The EdgeMarc honors both DiffServ and IP Precedence, which share the first 3 bits of the TOS byte in the IP header. IP Precedence can be from 0 to 7 since it is 3 bit. The EdgeMarc provides a total of 8 priority queues, one per IP Precedence. The first 6 queues are also used for each DiffServ class. The default configuration for EdgeMarc is one high priority queue with 90% WAN bandwidth and one low priority queue with 10% of the WAN bandwidth. This means that during light use the low priority queue is allowed to use all the available bandwidth, but under heavy load it is only allowed to use 10% of the WAN bandwidth.

The priority queues work with the WAN Link Redundancy (WLR) feature and adjust their bandwidth upon a switchover from Primary to Secondary link.
The figure below shows a typical DiffServ/MPLS deployment scenario with the following priority queue usage:

- SIP based voice and video streams traffic marked with DSCP EF on priority queue 6.
- SIP based voice and video signaling traffic marked with DSCP AF41 on priority queue 5.
- BGP routing protocol traffic marked with DSCP AF41 on priority queue 5.
- SSH, Telnet, and HTTP traffic marked with DSCP AF42 on priority queue 5.
- Real-time terminal services traffic to devices on the LAN marked with DSCP AF31 on priority queue 4.
- All other data traffic marked with DSCP BE on priority queue 1.

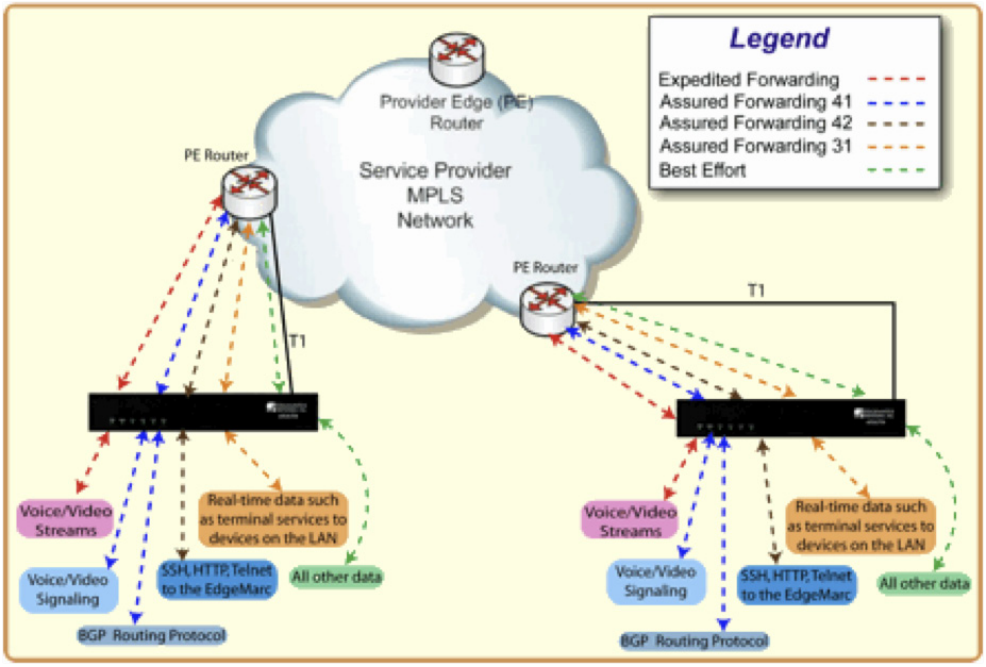


Figure 1: Sample DiffServ / MPLS network

EDGEWATER NETWORKS, INC.
Converged Networking. Simplified.

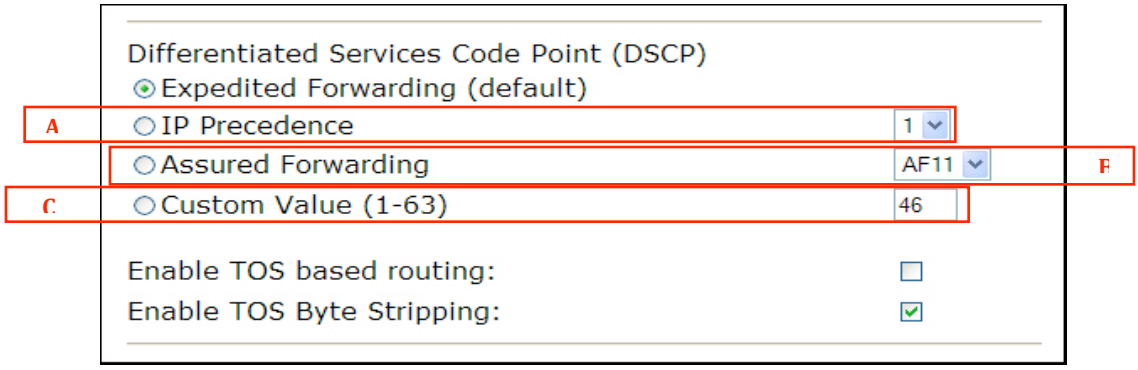
Configuring EdgeMarc for the above scenario

Marking voice traffic as a priority: setting TOS bits for the outbound packets

This operation is performed by going to the Traffic Shaper page under the main configuration menu. The default setting is set to EF. Since in the above figure voice and video traffic is going over the EF Class, there is no need to change this setting. If a change was required, then any of the four (4) classes under Assured Forwarding or a custom value could be chosen from areas B and C respectively, as shown in the figure below. In addition, any IP Precedence level from one to seven could also be chosen from area A. Keep in mind that at this point all voice and video streams and signaling will be marked with the DSCP value specified here. A rule will be defined later to route the SIP based voice and video signaling to priority queue 5.

"Enable TOS byte Stripping" should be checked, since the EdgeMarc will populate the TOS byte based on the specified rules as explained below.

Note: Traffic shaping to enforce the configured prioritization is performed on the outbound direction of each interface.



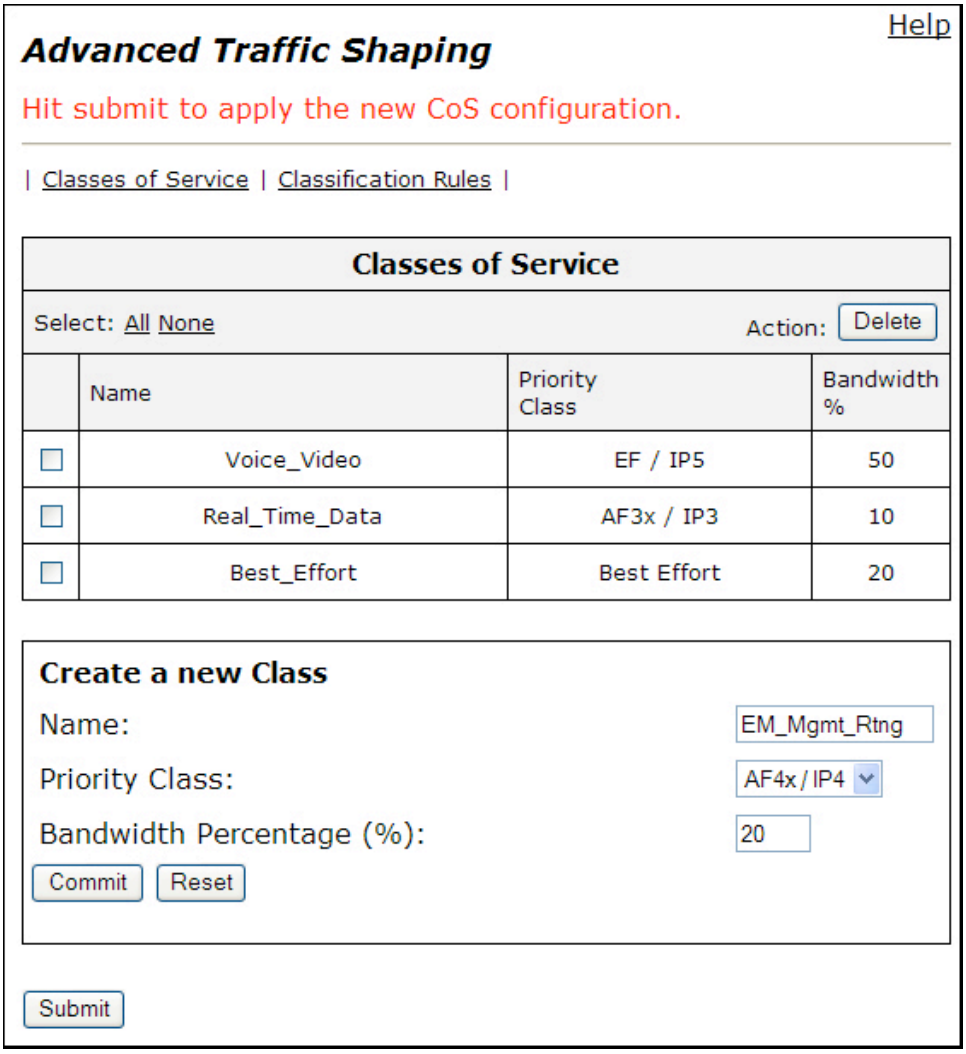
Creating Queues with Bandwidth Specifications

This is done by going to Configuration ***Menu - Traffic Shaper - Advanced*** menu and creating the required classes with their associated bandwidth requirements. From the picture above, we will need one FE, one AF4, one AF3, and one best effort queue. In the screen shot below four classes have been created with the following specifications:

- FE with 50% of the WAN bandwidth
- AF3 with 10% of the WAN bandwidth
- AF4 with 20% of the WAN bandwidth
- Best Effort with 20% of the WAN bandwidth

EDGEWATER NETWORKS, INC.
Converged Networking. Simplified.

Note: *If a queue is not created for a DSCP value in use, all packets with that DSCP value will be sent to the Best Effort queue. Furthermore, CAC values for Primary and Secondary links specified on the Traffic Shaper page must not exceed the specified bandwidth of the priority queue associated with the voice and video traffic.*



To create the class, simply enter the information as shown above and click **Commit**. Once all the classes have been created then click **Submit**.

Note: *All classes can exceed their specified bandwidth if bandwidth is available, otherwise they will be restricted to the bandwidth values assigned to them. In the case where multiple classes are exceeding the bandwidth values assigned to them but the WAN link is not yet saturated each queue will be allocated the remaining unused bandwidth equally. This will continue until the WAN link becomes congested or saturated at which point the throughput for any queue falls back to its configured bandwidth.*

Assigning Traffic Flows to Priority Queues

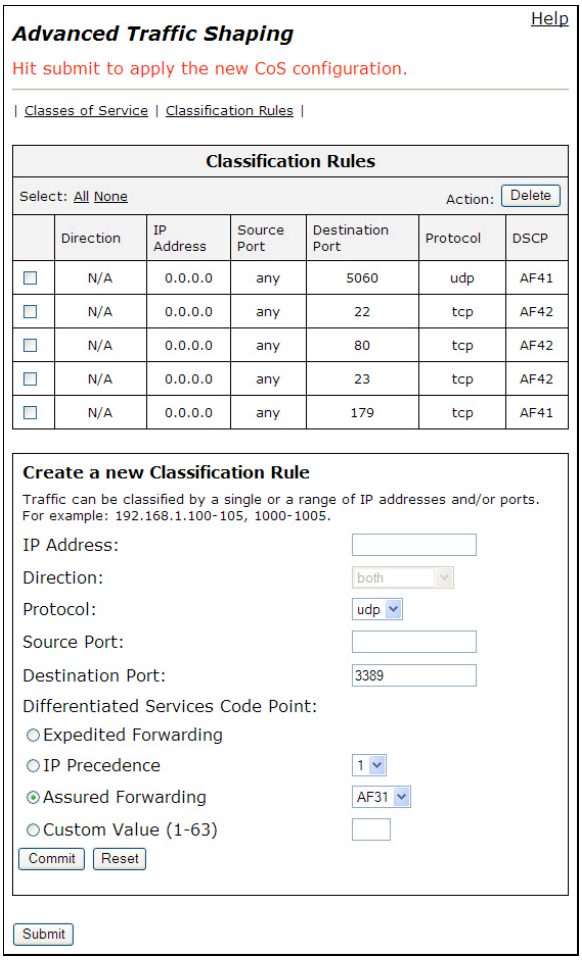
By clicking the **Classification Rules** link from the **Advanced Traffic Shaping** page specific rules for the traffic flows can be entered. The following figure shows the entries which will make the necessary association of traffic flows with the priority queues.

As can be seen from the figure below, a total of 6 flow associations have been created to achieve the objectives in the example network of Figure 1.

Following mappings explain the entries made in the figure below:

1. Any UDP packet with 5060 as the destination port (voice and video SIP signaling) - priority queue 5
2. Any TCP packet with 22 as the destination port (SSH traffic) - priority queue 5
3. Any TCP packet with 80 as the destination port (HTTP traffic) - priority queue 5
4. Any TCP packet with 23 as the destination port (Telnet traffic) - priority queue 5
5. Any TCP packet with 179 as the destination port (BGP routing protocol traffic) - priority queue 5
6. Any UDP packet with 3389 as the destination port (terminal services) - priority queue

Note: *Any traffic flow that is not specified in the list and is not a voice or video stream will be put in priority queue 1. Furthermore, all voice and video stream traffic flows will be automatically put into priority queue 6.*



Help

Advanced Traffic Shaping

Hit submit to apply the new CoS configuration.

| Classes of Service | Classification Rules |

Classification Rules

Select: All None Action: Delete

	Direction	IP Address	Source Port	Destination Port	Protocol	DSCP
☐	N/A	0.0.0.0	any	5060	udp	AF41
☐	N/A	0.0.0.0	any	22	tcp	AF42
☐	N/A	0.0.0.0	any	80	tcp	AF42
☐	N/A	0.0.0.0	any	23	tcp	AF42
☐	N/A	0.0.0.0	any	179	tcp	AF41

Create a new Classification Rule

Traffic can be classified by a single or a range of IP addresses and/or ports.
For example: 192.168.1.100-105, 1000-1005.

IP Address:
Direction: both
Protocol: udp
Source Port:
Destination Port: 3389
Differentiated Services Code Point:
○ Expedited Forwarding
○ IP Precedence 1
◉ Assured Forwarding AF31
○ Custom Value (1-63)

Commit Reset

Submit

EDGEWATER NETWORKS, INC.
Converged Networking. Simplified.