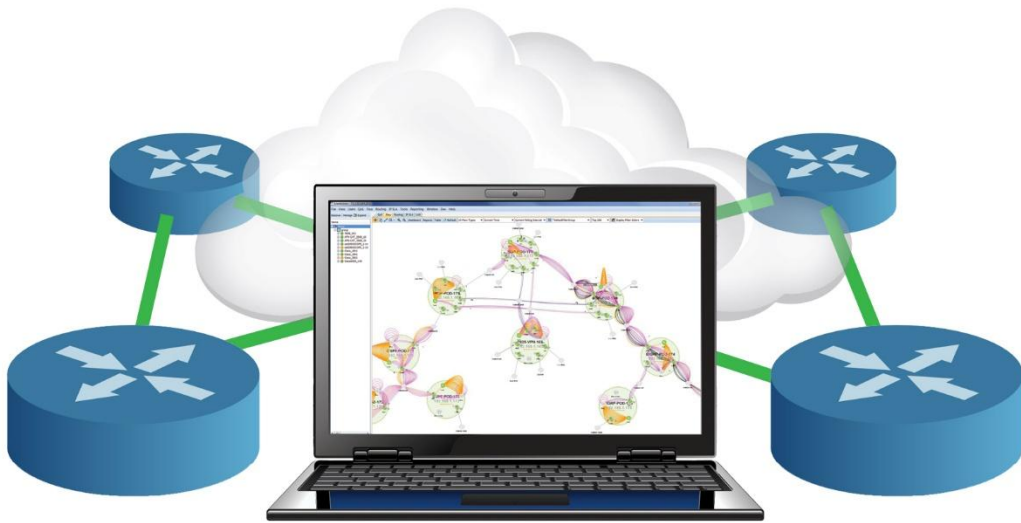


Managing DMVPN QoS with LiveAction



LiveAction™

Table of Contents

DMVPN QoS Overview.....	3
Network QoS Configuration	4
How Does QoS Work?.....	4
DMVPN QoS Design.....	5
Protecting Priority Data Within DMVPN Tunnels	5
Protecting Tunnels From Casual Internet Traffic.....	7
Understanding End-to-End Logical Throughput.....	9
DMVPN QoS Configuration.....	9
QoS Pre-Classify.....	10
Per-Tunnel QoS.....	11
LiveAction Overview	13
LiveAction DMVPN QoS Configuration	15
Remote Site DMVPN QoS Configuration.....	15
Remote Site DMVPN QoS Validation.....	23
Data Center DMVPN Per-Tunnel QoS Configuration.....	26
Data Center DMVPN QoS Validation	30
Remote Ingress Shaping QoS Configuration.....	35
Validating DMVPN QoS with LiveAction.....	38
Reports	38
Alerts.....	39
Medianet.....	39
Medianet Flow Path Analysis.....	41
Appendix A. – DMVPN Putting It All Together.....	44
Appendix B. – Sample DMVPN Branch Office QoS Configuration with RIS.....	53
Appendix C. – Sample DMVPN Data Center Per-Tunnel QoS Configuration.....	54

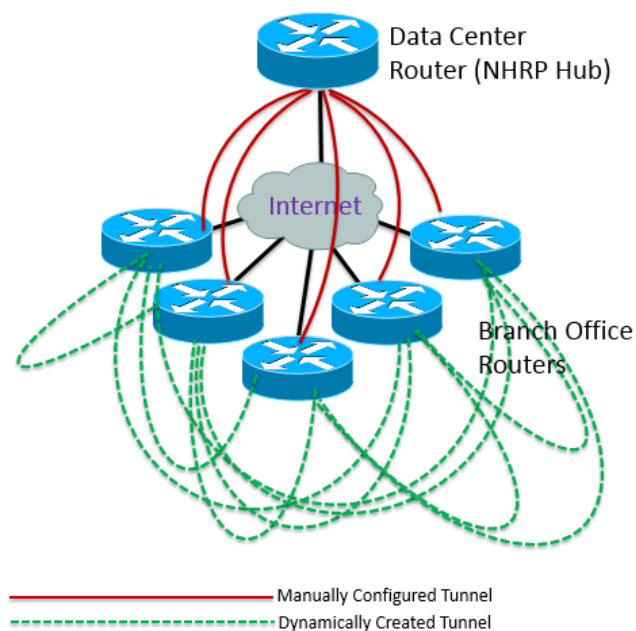
DMVPN QoS Overview

Cisco's Dynamic Multipoint Virtual Private Network (DMVPN) is a VPN deployment strategy for building a secure and scalable connectivity platform for large wide area networks (WANs). DMVPN technologies are most often used for enabling any-to-any, full-meshed communication for mobile workers, telecommuters, and extranet users over the public Internet. For example, two branch locations requiring a direct communication path, such as when using Voice-over-IP (VoIP) between the two offices, but don't require a permanent VPN connection between sites, can benefit from DMVPN. It enables zero-touch deployment of dynamic IPsec VPNs and improves network performance by reducing latency and jitter, while optimizing head office bandwidth utilization.

Many organizations are migrating part or all of their WAN environments to Internet based VPN strategies to gain the benefit of low cost, high bandwidth connectivity. With the proliferation of this deployment model DMVPN has become an attractive solution for the following benefits:

- Lowering the cost for implementing large, redundant WAN network environments
- Simplified and direct branch-to-branch connectivity for business applications like Voice- and Video-over-IP
- Dramatically reducing the deployment complexity in VPNs with zero touch configuration

IP quality-of-service (QoS) is a core component for successful deployments of VoIP, Video-over-IP and virtual desktop infrastructure (VDI) applications. Traditional WAN technologies, like MPLS, provide any-to-any dedicated bandwidth with the additional benefit of QoS-aware service providers that protect business-critical applications. Internet VPN connectivity solutions such as DMVPN do not have this QoS protection as the Internet is not QoS aware. However, due to the cost savings and higher bandwidth of Internet-based VPNs, business are still transitioning to these types of networks. As a result, there is still the need for QoS protection in such VPN environments; yet these configurations must be implemented correctly for a business to gain the full benefit of the VPN solution. The following diagram depicts a typical DMVPN configuration:



This document will outline the design framework for successful QoS deployment in DMVPN environments. It will also detail the required steps of implementing QoS in a DMVPN network infrastructure. Finally, this document will highlight how a network infrastructure's QoS can be configured, monitored and validated using LiveAction software.

Network QoS Configuration

How Does QoS Work?

VoIP, video and other critical data applications rely on the network infrastructure to honor and queue their traffic for call quality and application performance protection. This need for QoS is a requirement in WAN environments, regardless of the underlying transport mechanism (DMVPN vs. traditional WANs), if business-critical applications are to receive their required level of service.

QoS is a suite of technologies used to manage bandwidth usage as data crosses computer networks. Its most common use is for the protection of real-time voice or video communications and high-priority data applications. QoS technologies, or tools, each have specific roles that are used in conjunction with one another to build end-to-end network QoS policies.

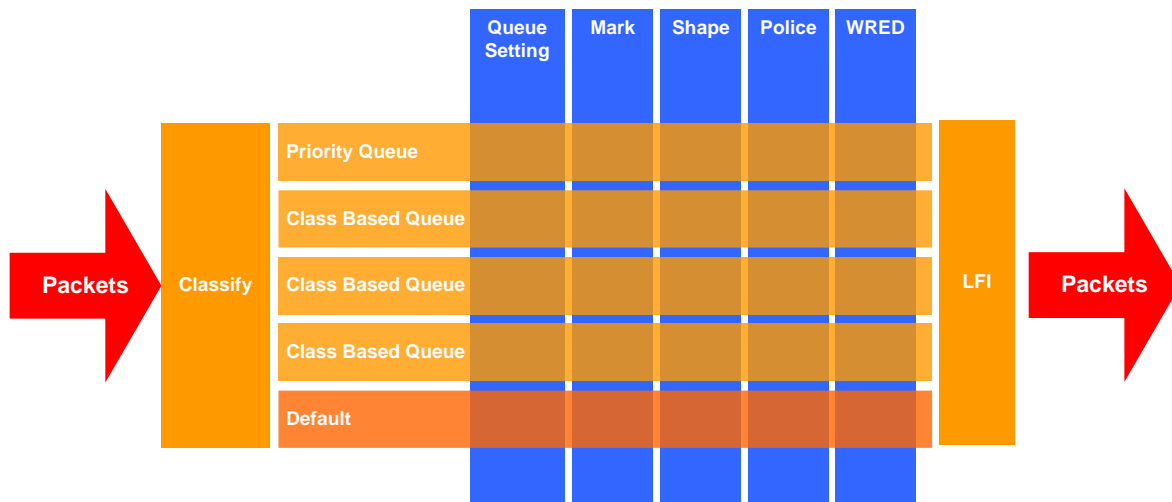
The two most common QoS tools used to handle traffic are classification and queuing. Classification identifies and marks traffic to ensure network devices know how to distinguish and prioritize data as it traverses a network. Queues are buffers in devices that hold data to be processed. Queues provide bandwidth reservation and prioritization of traffic as it enters or leaves a network device. If the queues are not emptied (due to higher priority traffic going first), they overflow and drop traffic.

Policing and shaping are also commonly used QoS technologies that limit the bandwidth utilized by administratively defined traffic types. Policing enforces bandwidth to a specified limit. If applications try to use more bandwidth than they are allocated, their traffic will be remarked or dropped. Shaping defines a software-set limit on the transmission bandwidth rate of a data class. If more traffic needs to be sent than the shaped limit allows, the excess will be buffered. This buffer can then utilize queuing to prioritize data as it leaves the buffer.

The WRED (Weighted Random Early Discard) technology provides a congestion avoidance mechanism that will drop lower priority TCP data to attempt to protect higher priority data from the adverse effects of congestion.

Finally, link-specific fragmentation and compression tools are used on lower bandwidth WANs to ensure real-time applications do not suffer from high jitter and delay.

Table 1: Packet flow through a typical QoS policy



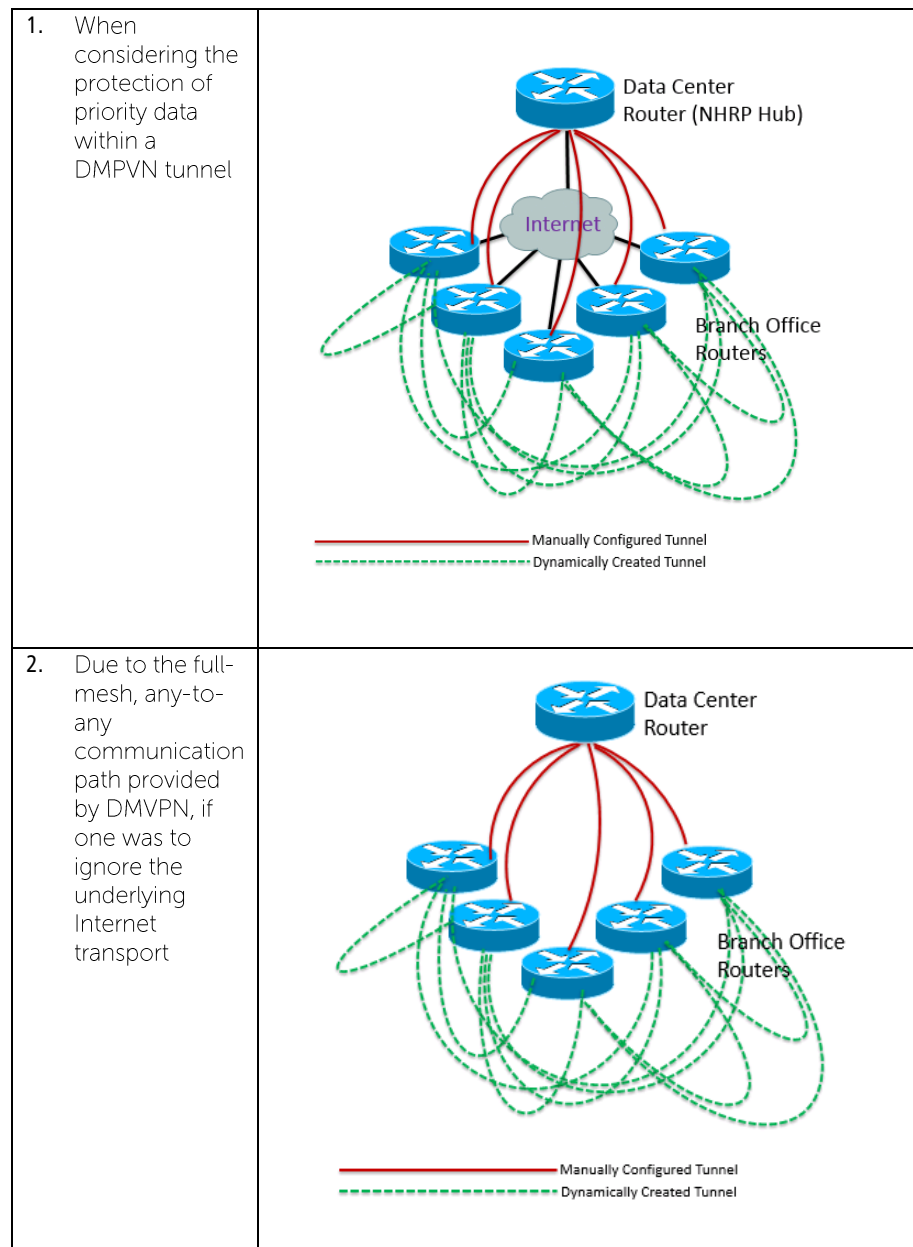
DMVPN QoS Design

There are three main components of a DMVPN QoS design that must be considered for successful protection of VoIP, video and high priority data. These are:

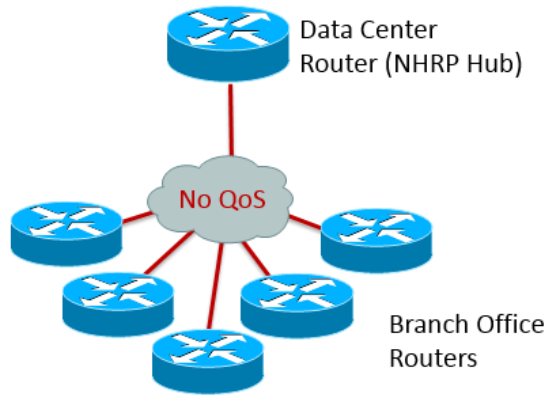
1. Protecting priority data within DMVPN tunnels
2. Protecting tunnels from casual Internet traffic
3. Understand end-to-end logical throughput

Protecting Priority Data Within DMVPN Tunnels

When designing QoS policies to protect priority data within a DMVPN tunnel, the concepts outlined in the diagrams below should be considered:



3. The design could be considered similar to a high bandwidth private WAN in which the service provider does not have QoS on their backbone. When considered in this manner, the DMVPN QoS design for protecting priority data in the tunnel becomes much simpler to understand.



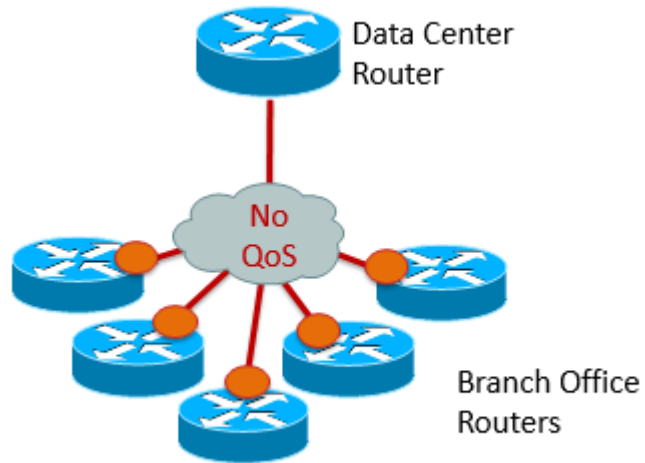
The following diagram shows an example of a typical branch office QoS configuration when no service provider QoS is available. This is the type of configuration that would also be used for a DMVPN remote branch/spoke. It is caricatured by a hierarchical QoS policy that contains a parent shaping policy and a child queuing policy.

Traditional Branch Office QoS Configuration When Service Provide Does Not Have QoS

```

policy-map QUEUING
class VOIP
priority percent 20
class VIDEO
bandwidth percent 30
class MGMT_DATA
bandwidth percent 5
class CALL_SIGNALING
bandwidth percent 5
class CRITICAL_DATA
bandwidth percent 10
class class-default
fair-queue
!
policy-map Shaping_2Mb
class class-default
shape average 2000000 20000 0
service-policy QUEUING
!
interface GigabitEthernet0/0
description WAN_INTERFACE
service-policy output Shaping_2Mb

```



The following diagram shows an example of a typical data center QoS configuration when no service provider QoS is available. This is similar to the traditional configuration used for a DMVPN design. This configuration is caricatured by a multi-class hierarchical QoS policy that contains a parent shaping policy for each remote site. Each site's parent policy will contain a child queuing policy. This will ensure the data center router never sends more traffic than any remote site can handle. But, if congestion does occur for traffic destined to a particular remote, priority applications (VoIP, video, etc.) will be scheduled first.

Traditional Data Center QoS Configuration When Service Provide Does Not Have QoS	
<pre> policy-map QUEUING class VOIP priority percent 20 class VIDEO bandwidth percent 30 class MGMT_DATA bandwidth percent 5 class CALL_SIGNALING bandwidth percent 5 class CRITICAL_DATA bandwidth percent 10 class class-default fair-queue ! policy-map Shaping class REMOTE_1 shape average 2000000 20000 0 service-policy QUEUING class REMOTE_2 shape average 1000000 10000 0 service-policy QUEUING class REMOTE_3 shape average 1500000 15000 0 service-policy QUEUING ...etc... ! interface GigabitEthernet0/0 description WAN_INTERFACE description service-policy output Shaping </pre>	<p>The diagram illustrates a network topology where a central Data Center Router is connected to four Branch Office Routers. A cloud labeled 'No QoS' is placed between the Data Center Router and the Branch Office Routers, signifying that there is no Quality of Service (QoS) protection on the links connecting them.</p>

Protecting Tunnels From Casual Internet Traffic

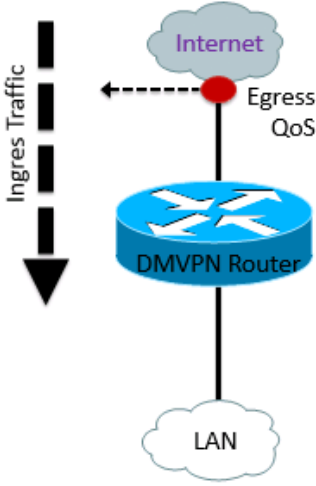
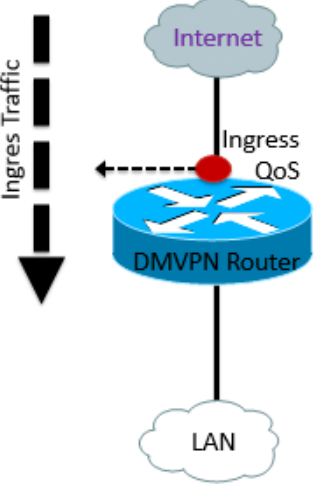
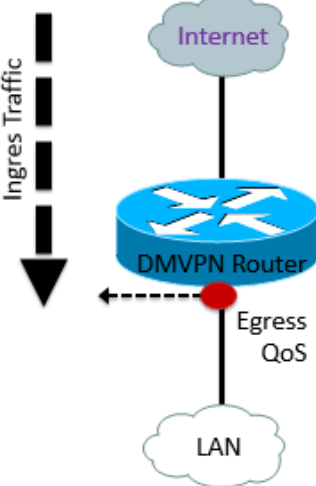
Once priority data is protected inside a DMVPN tunnel, the tunnel(s) itself needs to be protected from casual Internet traffic. Due to an engineer's ability to control egress traffic for both Internet and tunnel destinations via QoS, as outlined in this document, controlling ingress Internet traffic will be the focus of this section of the document.

There are three design options for controlling ingress Internet traffic for the protection of DMVPN tunnels. Each of these may be used as a stand-alone solution or could be combined for specific use cases.

These three options are:

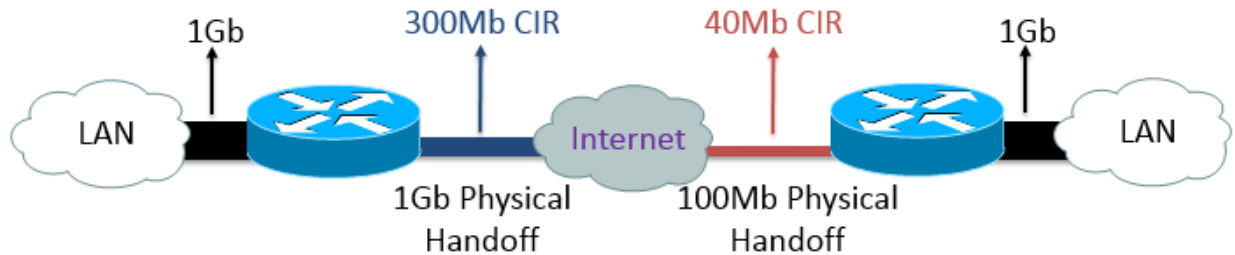
- Service Provider Last Mile QoS
- Ingress Policing
- Remote Ingress Shaping (RIS)

These design options will be presented in the table below:

<p style="text-align: center;">Service Provider Last Mile QoS</p> <p>Some Internet service providers now provide QoS on the last mile connection to the customer edge (CE) device. This is usually the DMVPN terminating router. This service provider egress queuing policy can be used for protecting tunnel traffic from casual Internet traffic.</p> <p>This service is not yet widely available and will most likely incur an additional cost.</p>	
<p style="text-align: center;">Ingress Policing</p> <p>An ingress policing QoS policy may be applied to the Internet interface of the DMVPN router. This will provide protection of DMVPN tunnel traffic by limiting the volume of casual ingress Internet traffic.</p> <p>This configuration is not very flexible as it does not allow casual Internet traffic to use any unallocated bandwidth if the tunnel is not fully utilized.</p>	
<p style="text-align: center;">Remote Ingress Shaping</p> <p>Remote Ingress Shaping (RIS) is an egress QoS policy applied to the LAN interface of a DMVPN router. This policy's configuration is very similar to that of the hierarchical configuration used at a remote branch office's WAN interface. The key to the RIS policy configuration is that the parent classes' shaper is set to only 95% of the target bandwidth rate. By creating this artificial congestion point, ingress traffic (VoIP, video, critical data and casual Internet) can be prioritized as it is delivered to the LAN.</p> <p>Since most casual Internet traffic is TCP and TCP will adapt to the underlying network's capacity, this RIS policy will effectively control the casual TCP based Internet traffic while protecting priority tunnel traffic.</p>	

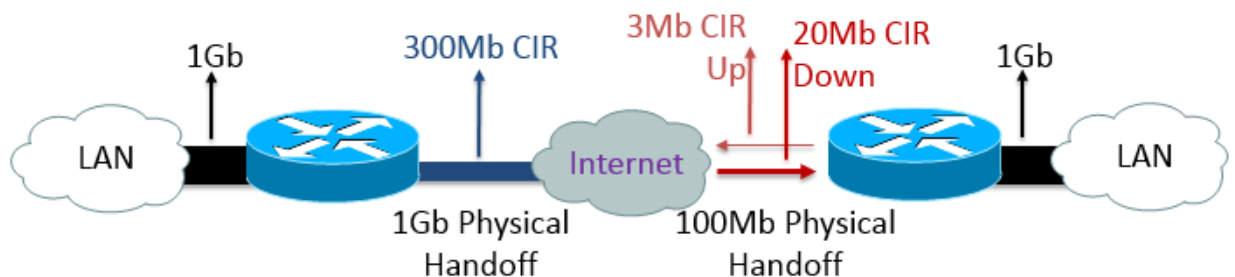
Understanding End-to-End Logical Throughput

Another key DMVPN QoS concept that must be understood for successful protection of VoIP, video and priority data is that of determining the end-to-end bi-directional logical bandwidth of the Internet connectivity between the data center and each DMVPN remote site. Consider the following diagram:



The data center device physically has a 1Gb connection to the service provider, but the provider has implemented a 300Mb CIR. This means the service provider will drop any data sent or received over 300Mb on the data center circuit. The remote site has a 100Mb connection, but the CIR is 40Mb. This means the service provider will drop any data sent or received over 40Mb. When considered end-to-end, the DMVPN QoS policies for this example need to be configured for 40Mb, the lowest end-to-end throughput.

Below is a second example:



The data center device physically has a 1Gb connection to the service provider, but the provider has implemented a 300Mb CIR. This means the service provider will drop any data sent or received over 300Mb on the data center circuit. The remote site is connected to the service provider using a 100Mb connection, but is using an asymmetric service in which the download rate is 20Mb, but the upload rate is 3Mb. Any data sent/received over these rates will be dropped. When considered end-to-end, this DMVPN QoS policy must be configured for 20Mb from the data center to the remote site and 3Mb from the remote site to the data center.

DMVPN QoS Configuration

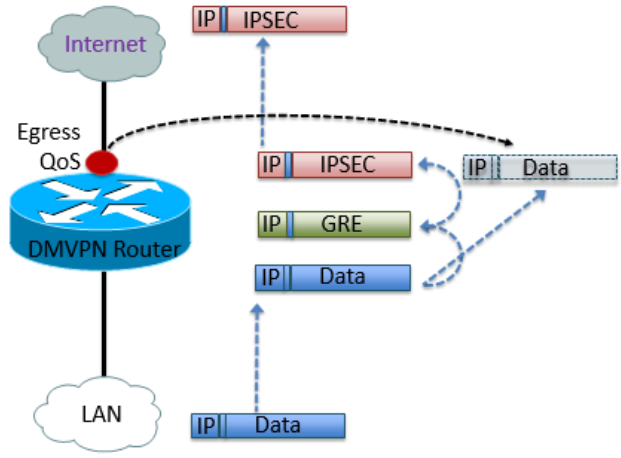
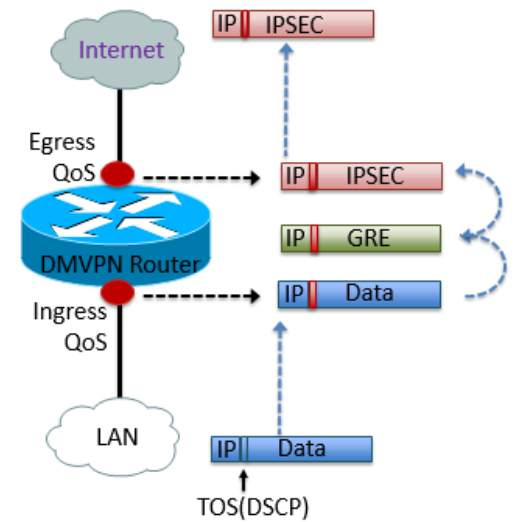
QoS configuration for DMVPN networks follow many of the same methodologies as traditional WAN technologies, but there are a few exceptions that should be understood. These will be highlighted below:

QoS policies cannot be applied directly to multipoint GRE tunnel interfaces	QoS policies can be applied to point-to-point GRE tunnel interfaces, but these are seldom used in DMVPN configurations	QoS policies can be applied to the physical interface that sources multipoint GRE tunnel interfaces. This is the most common configuration.
! interface Tunnel1 description MULTI-POINT GRE TUNNEL tunnel mode gre multipoint service-policy output My-QoS-Policy !	! interface Tunnel1 description POINT-to-POINT GRE TUNNEL tunnel mode gre point-to-point service-policy output My-QoS-Policy !	! interface Tunnel1 description MULTI-POINT GRE TUNNEL tunnel mode gre multipoint tunnel source GigabitEthernet0/0 ! interface GigabitEthernet0/0 description INTERNET CONNECTION service-policy output My-QoS-Policy !

QoS Pre-Classify

QoS Pre-Classify is a configuration option that is applied to tunnel interfaces. It can give an engineer more classification options for the matching of interesting traffic to the WAN egress QoS policy. The following table highlights this configuration in more detail:

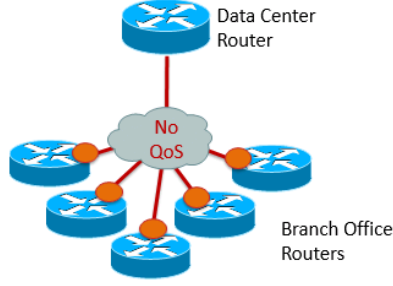
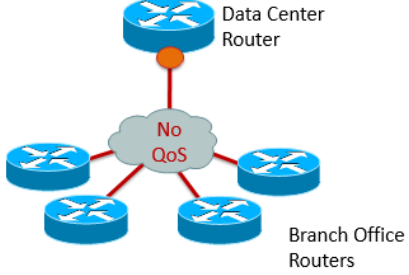
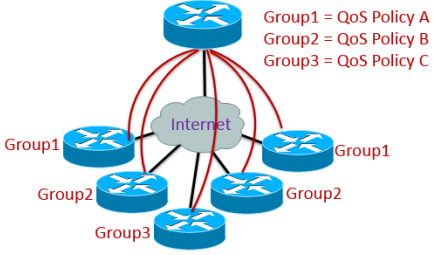
<p>When qos pre-classify is not used on a DMPN tunnel interface, as a packet is put inside the tunnel, destined to the Internet interface, the original packet is encapsulated inside a GRE and then IPSEC. The egress QoS policy on the Internet interface only sees the IPSEC packet and does not have any understanding of the original IP headed information but with one exception. The original DSCP value is kept intact as the encapsulation process transpires. This means that the egress QoS policy can use the priority marking of the original packet for traffic classification.</p>	<p style="text-align: center;">Without QoS Pre-Classify</p> <p>The diagram illustrates the traffic flow on a DMVPN Router. On the left, a LAN cloud is connected to the router. On the right, an Internet cloud is connected. Traffic enters from the LAN, passes through the router, and is classified by TOS(DSCP). The traffic then undergoes encapsulation: Data (blue box) is encapsulated into GRE (green box), which is then encapsulated into IPSEC (red box). The final IPSEC packet is sent to the Internet. A dashed arrow labeled 'Egress QoS' points to the IPSEC packet, indicating that the QoS policy is applied to this final packet. A curved dashed arrow indicates the encapsulation process from Data to GRE to IPSEC.</p>
---	---

<p>When the qos pre-classify command is applied to a tunnel interface, a shadow copy of the original packet is available for the egress QoS policy for reference. When used with DMVPN, this allows the QoS policy on the Internet interface to use the DSCP markings as well as the original source/destination IP addresses and layer 4 TCP/UDP port numbers for classification.</p>	<p style="text-align: center;">With QoS Pre-Classify</p> 
<p>Is qos pre-classify a requirement?</p> <p>In many organizations QoS classification will be performed at the LAN level. As a packet enters the WAN router, its DSCP will have already been pre-marked. In this scenario, there is no need for qos pre-classify.</p> <p>As well, if a LAN ingress QoS policy is used for classification, qos pre-classify is not a requirement, as any updated DSCP values will be kept during the encapsulation process.</p>	<p style="text-align: center;">Without QoS Pre-Classify</p> 

Per-Tunnel QoS

The traditional QoS configuration of a DMVPN data center router can become extremely large. Since the data center will use a multi-class hierarchical policy, with each remote site getting its own class and child queuing policy, if the DMVPN network consists of hundreds of remote sites, the QoS configuring can grow to thousands of lines of code. To eliminate this potential management nightmare, Cisco has implemented a solution named Per-Tunnel QoS. This allows engineers to configure and manage a simple, consolidated QoS configuration, but gain the benefit of dynamically created QoS policies for each DMVPN tunnel.

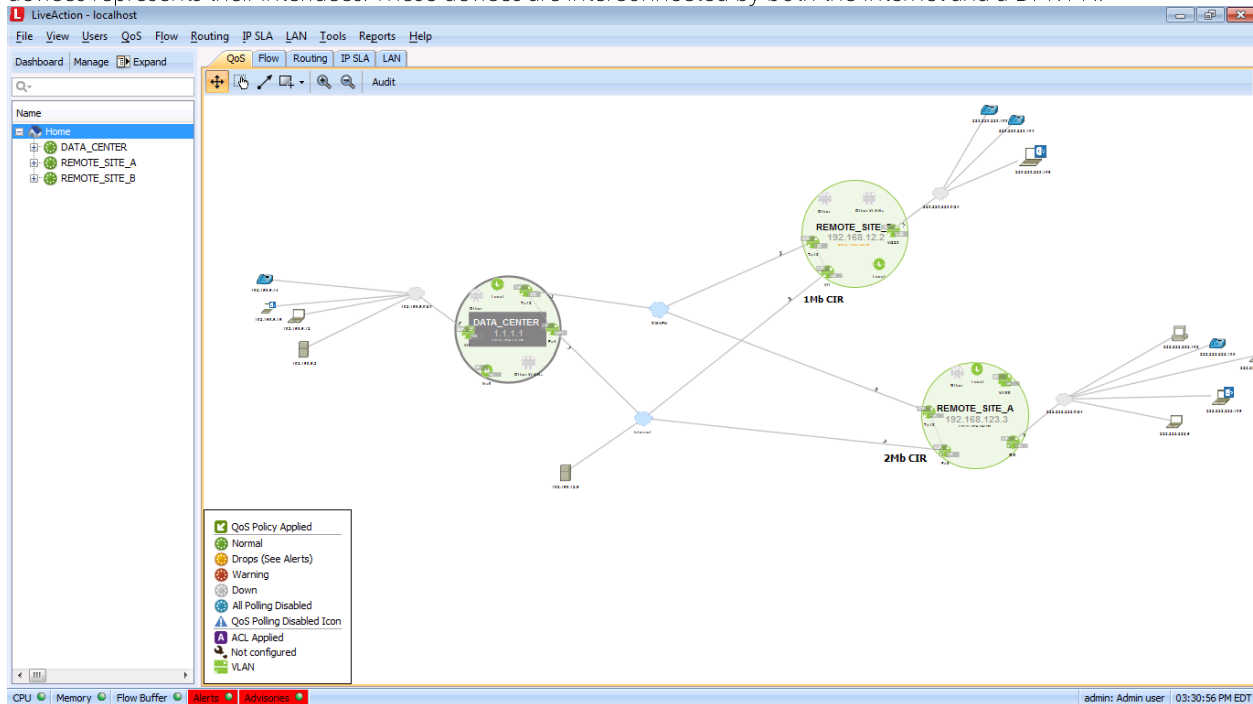
There are two steps for creating a Per-Tunnel QoS configuration. These are:

<p>Step 1 - Configuring all remote branch offices with a NHRP group.</p> <pre>! interface Tunnel1 ip nhrp group <GROUP_NAME> !</pre>	 <p>The diagram shows a central cloud labeled "No QoS" connected to a "Data Center Router" at the top and five "Branch Office Routers" arranged in a circle below it.</p>
<p>Step 2- Configuring the data center router's tunnel interface with a NHRP group(s) to QoS policy mapping(s)</p> <pre>! interface Tunnel1 ip nhrp map group <GROUP_NAME> service-policy output <QoS_POLICY> !</pre>	 <p>The diagram shows a central cloud labeled "No QoS" connected to a "Data Center Router" at the top and three "Branch Office Routers" below it.</p>
<p>NHRP group names are typically selected by using some form of bandwidth or QoS characteristic common with multiple remote devices. The fewer group names that are used in a network, the smaller the QoS configuration on the data center device.</p>	 <p>The diagram shows a central cloud labeled "Internet" connected to a "Data Center Router" at the top and six "Branch Office Routers" below it. The routers are grouped into three categories: Group1 (two routers), Group2 (two routers), and Group3 (two routers). A legend indicates: Group1 = QoS Policy A, Group2 = QoS Policy B, Group3 = QoS Policy C.</p>

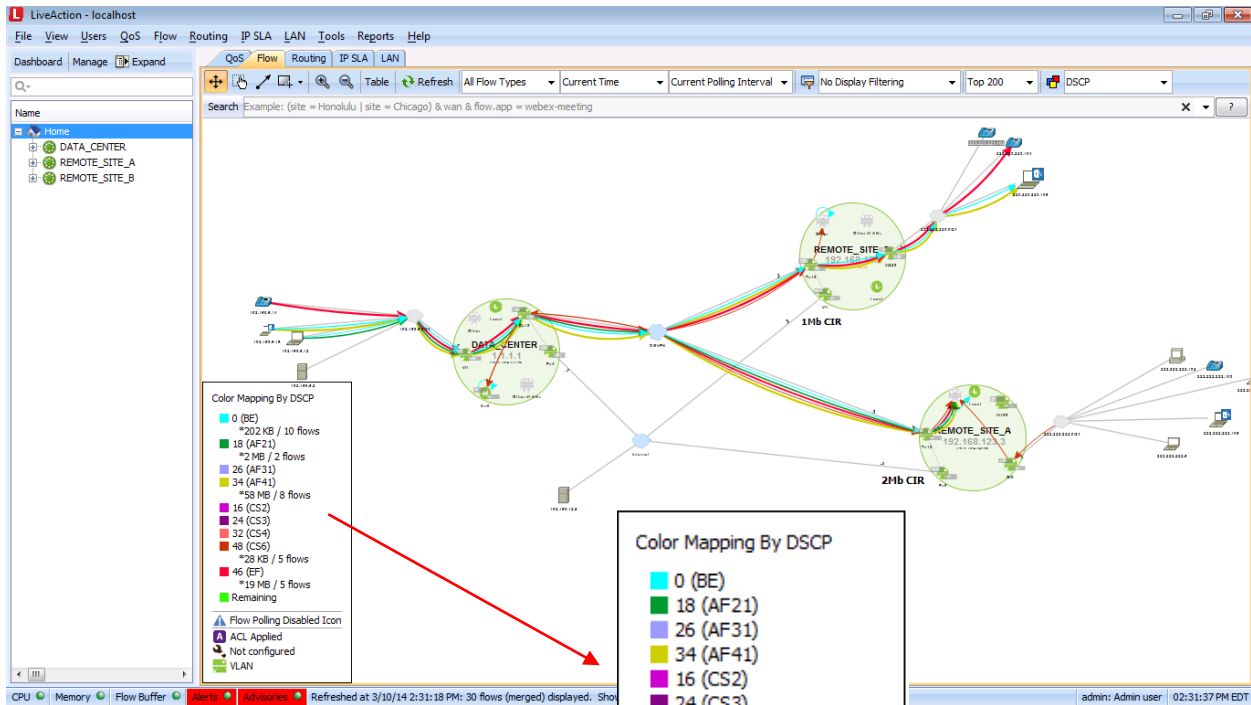
LiveAction Overview

LiveAction is an application-aware network performance management tool that will graphically display how networks and applications are performing using SNMP and the latest advanced NetFlow capabilities embedded in Cisco devices. In addition to showing application and network performance, LiveAction provides the ability to control application performance via its graphical QoS management capabilities. In the following pages, LiveAction will be used to highlight how easily QoS can be configured to manage and control DMVPN and Internet traffic. Moreover, this document will describe how LiveAction can be used to confirm the application performance of VoIP and video in DMVPN networks using the latest Medianet technology now available in some Cisco devices.

The image below is a view of the LiveAction console. It shows a network diagram consisting of three network devices. The three larger green circles represent routers and switches managed by LiveAction. The little green circles inside the devices represent their interfaces. These devices are interconnected by both the Internet and a DMVPN.



Since LiveAction is also a special NetFlow collector, it has the ability to graphically visualize the traffic that is flowing over the network. In the diagram below, the multi-colored arrows visualize the traffic traversing the network by DSCP value. In this example, the color legend below shows that red arrows represents EF traffic, green arrows represent AF21, light blue is Best-Effort traffic, etc. This is what one would expect to see if QoS matching and marking policies are configuration for VoIP, video and other high priority traffic. LiveAction allows one to visually understand the end-to-end QoS configurations and validate a traffic type's DSCP value is being honored throughout a network environment.



Double-clicking on any of the larger circles (routers/switches) in the LiveAction network diagram will show the real-time NetFlow data of traffic that is flowing through the device. In the example below, multiple DSCP values can be validated. This again confirms that VoIP and video's (RTP's) DSCP values are configured and being honored appropriately.

Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	In IF	Out IF	DSCP and IPv6
TCP	192.168.6.12	4,218	222.222.222.101	1,494	Vlan1	Tunnel13	18 (AF21)
TCP	192.168.6.12	1,494	222.222.222.101	4,218	Vlan1	Tunnel13	18 (AF21)
UDP	192.168.6.14	31,196	223.223.223.103	19,420	Vlan1	Tunnel13	46 (EF)
UDP	192.168.6.14	31,196	222.222.222.103	19,420	Vlan1	Tunnel13	46 (EF)
UDP	192.168.6.16	20,100	223.223.223.105	20,100	Vlan1	Tunnel13	34 (AF41)
UDP	192.168.6.16	20,100	222.222.222.105	20,100	Vlan1	Tunnel13	34 (AF41)
UDP	192.168.6.16	20,101	223.223.223.105	20,101	Vlan1	Tunnel13	0 (BE)
UDP	192.168.6.16	20,101	222.222.222.105	20,101	Vlan1	Tunnel13	0 (BE)
EIGRP	192.168.13.2	-	224.0.0.10	-	Tunnel13	Null0	48 (CS6)
ICMP	192.168.13.3	-	192.168.6.1	771	Tunnel13	Local	48 (CS6)
EIGRP	192.168.13.3	-	224.0.0.10	-	Tunnel13	Null0	48 (CS6)
OSPF	192.168.13.3	-	224.0.0.5	-	Tunnel13	Null0	48 (CS6)
ICMP	192.168.13.3	-	192.168.6.1	771	Tunnel13	Local	48 (CS6)

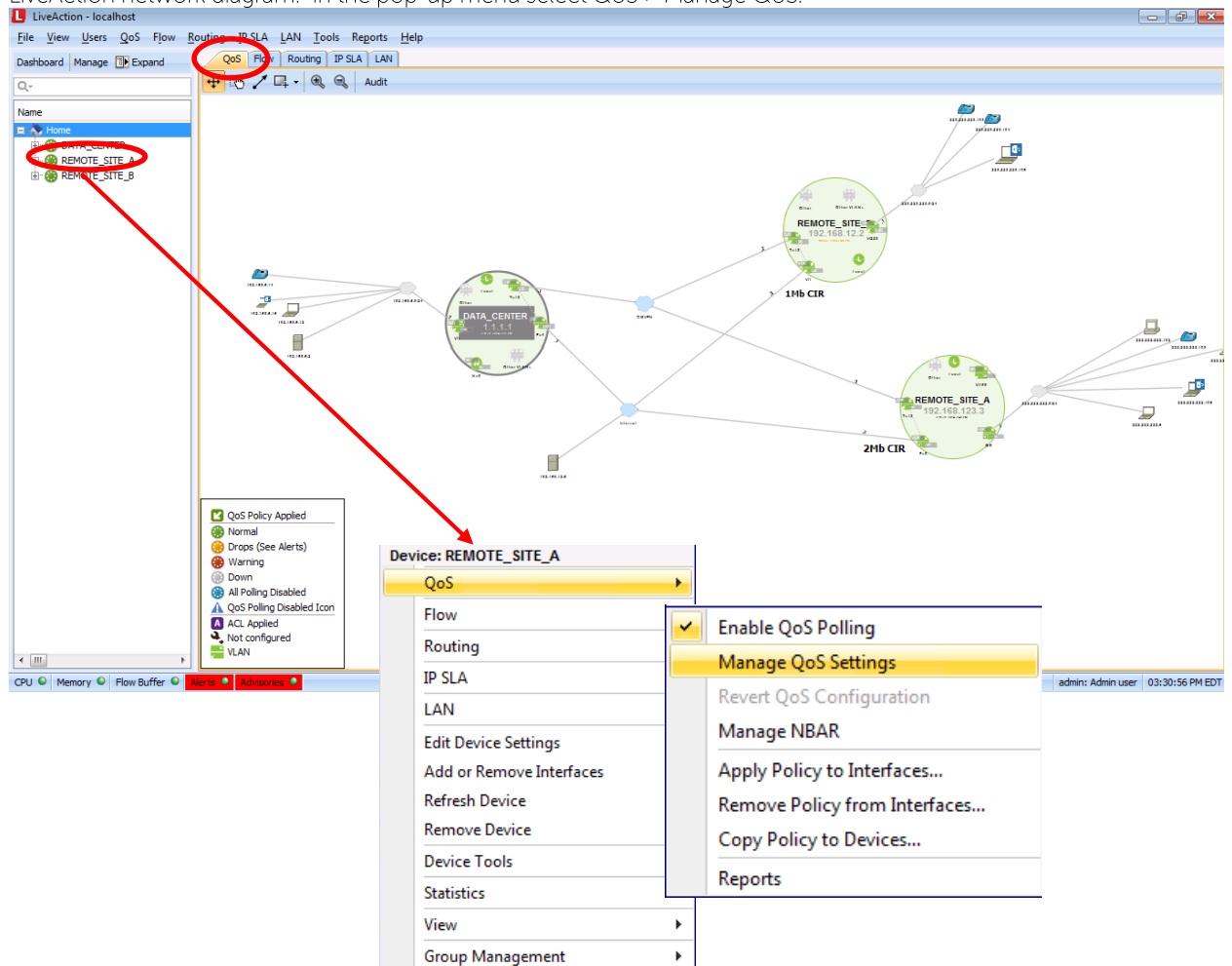
LiveAction DMVPN QoS Configuration

LiveAction provides engineers a graphical interface for simplifying the creation, modification and deployment of QoS policies. This GUI can be used for greatly simplifying DMVPN QoS. The following pages will show in detail how QoS can be configured, deployed, and validated for DMVPN using LiveAction.

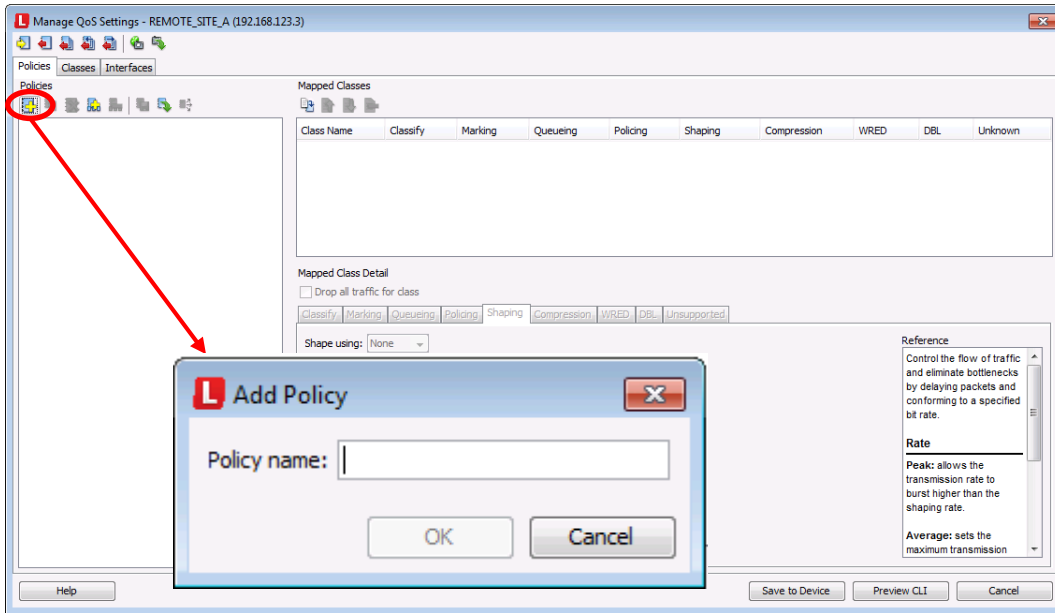
Remote Site DMVPN QoS Configuration

To configure the hierarchical shaping policy on the Internet interface for the prioritization of traffic inside the tunnel, perform the following:

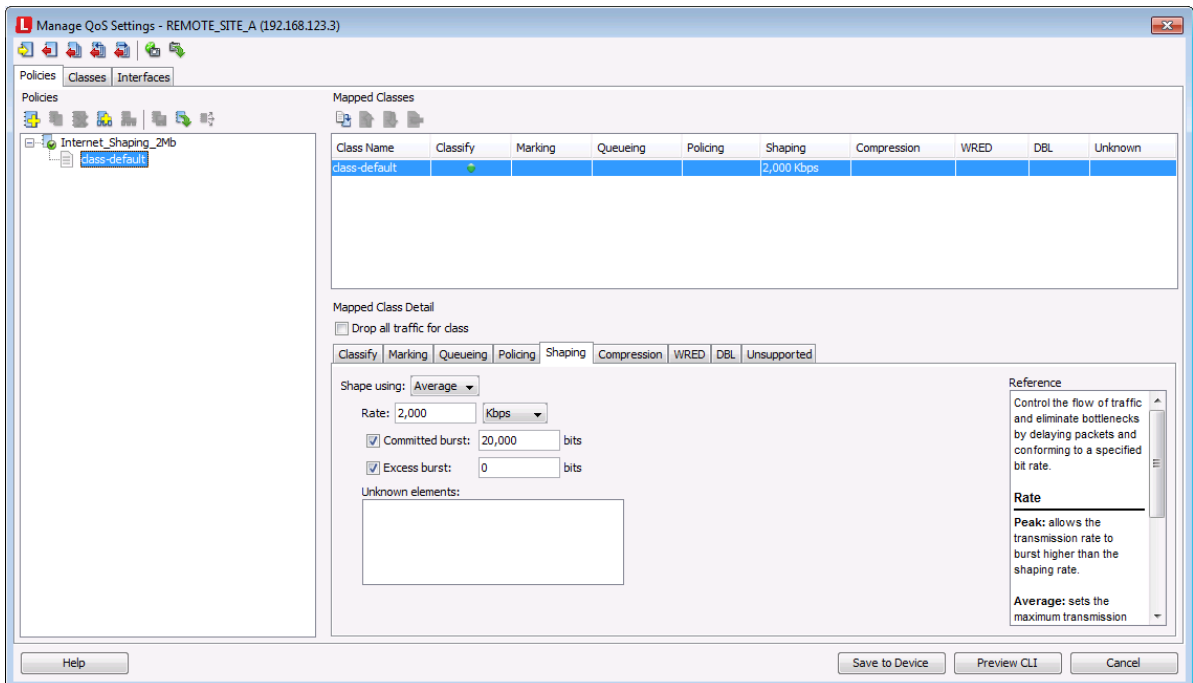
1. Select the QoS tab. Then right-click the on a remote site device object in the device list to the left of the LiveAction network diagram. In the pop-up menu select QoS > Manage QoS.



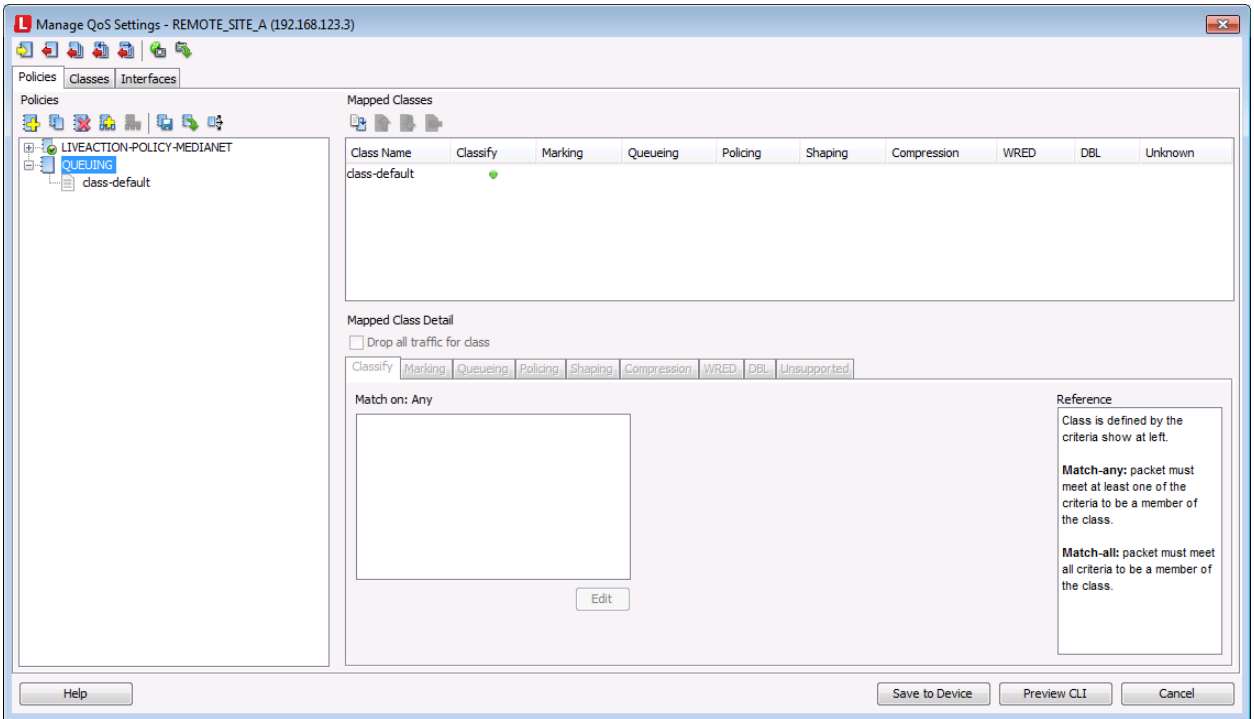
2. The Manage QoS dialog window appears. Click the Add Policy icon to the top left of the screen.



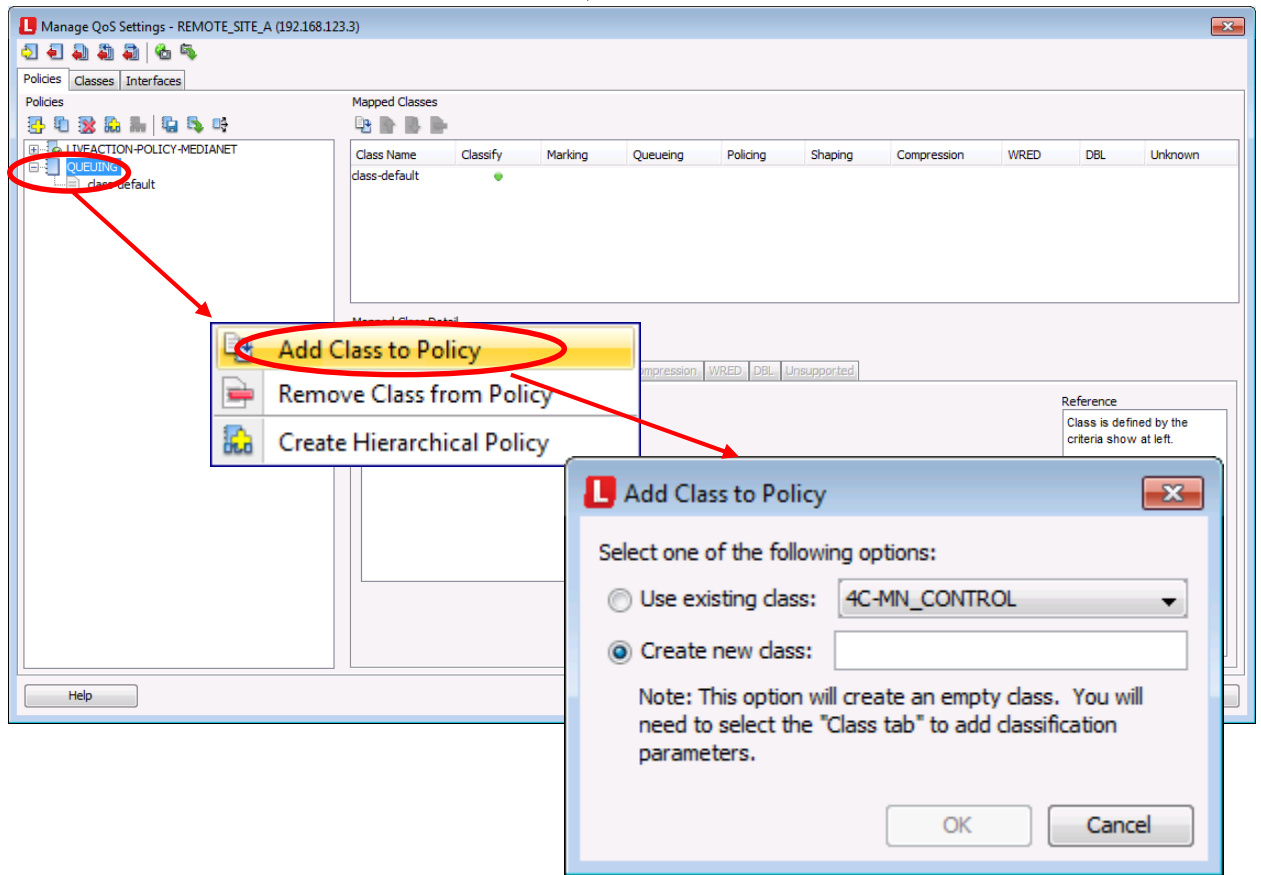
3. Give the policy a name and click OK. In this example, the policy will be named Internet_Shaping_2Mb.
4. Expand the new policy by clicking on it and click its class-default to highlight it.
5. Click the shaping tab in the middle of the window, and add a shaper. In this example, a shaper of 2Mb was created with the following parameters:
 - Rate: 2,000 Kbps
 - Committed burst: 20,000 bits
 - Excess burst: 0 bits



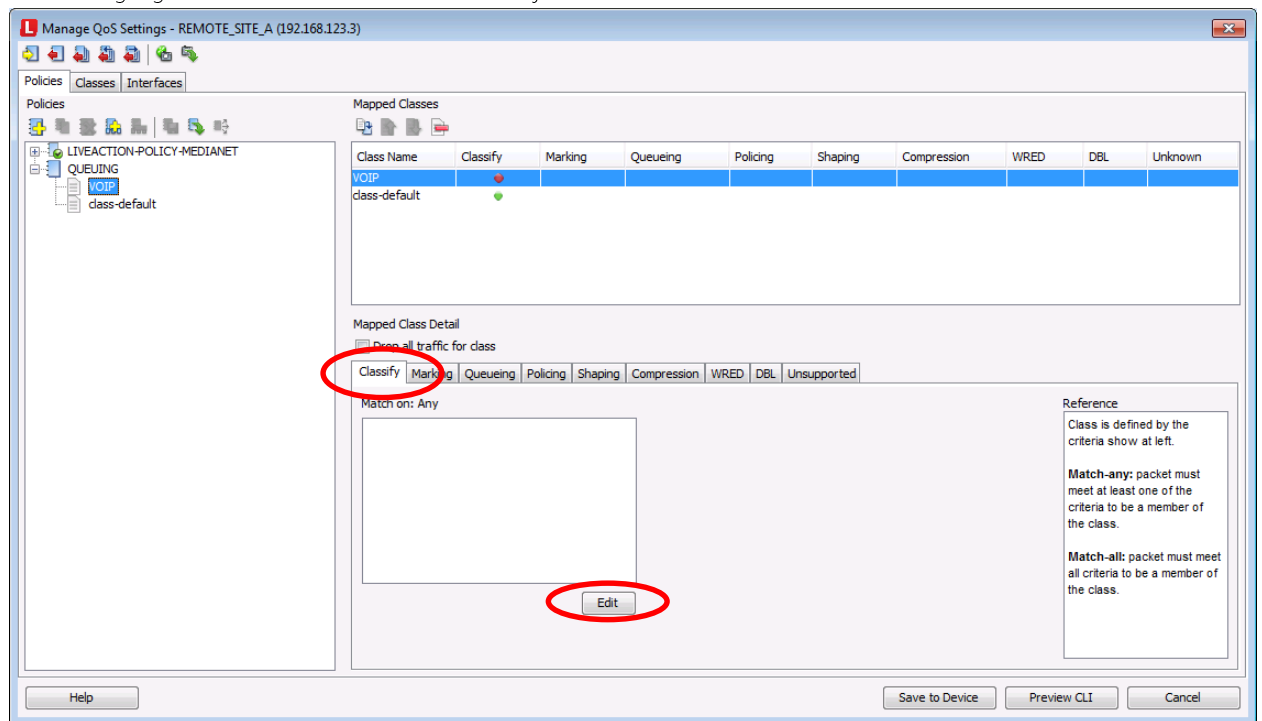
6. Click the Add Policy icon to the top left of the screen again, give the new policy a name, and click OK.
7. In this example the name of the second policy is QUEUING. This will become a child policy for the Internet_Shaping_2Mb policy.



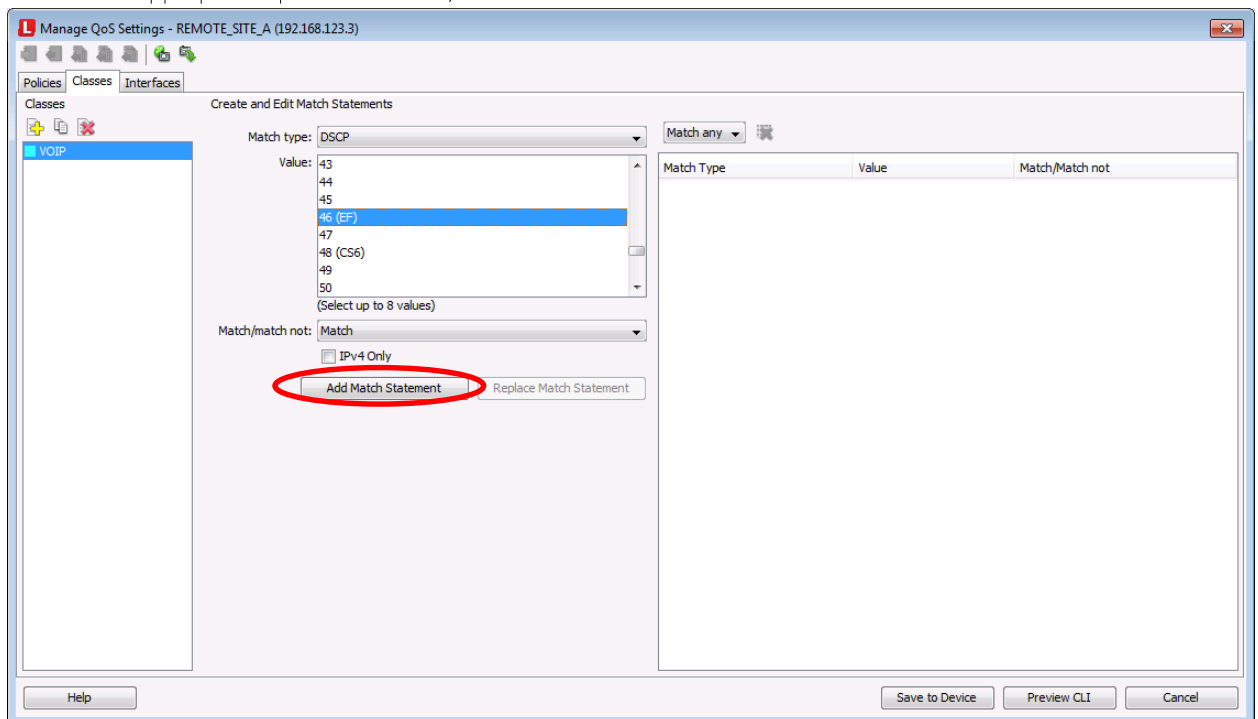
8. Right-click on the QUEUEING policy and select Add Class to Policy.
9. Select Create new class and enter a name. In this example, the first class created will be named VOIP.



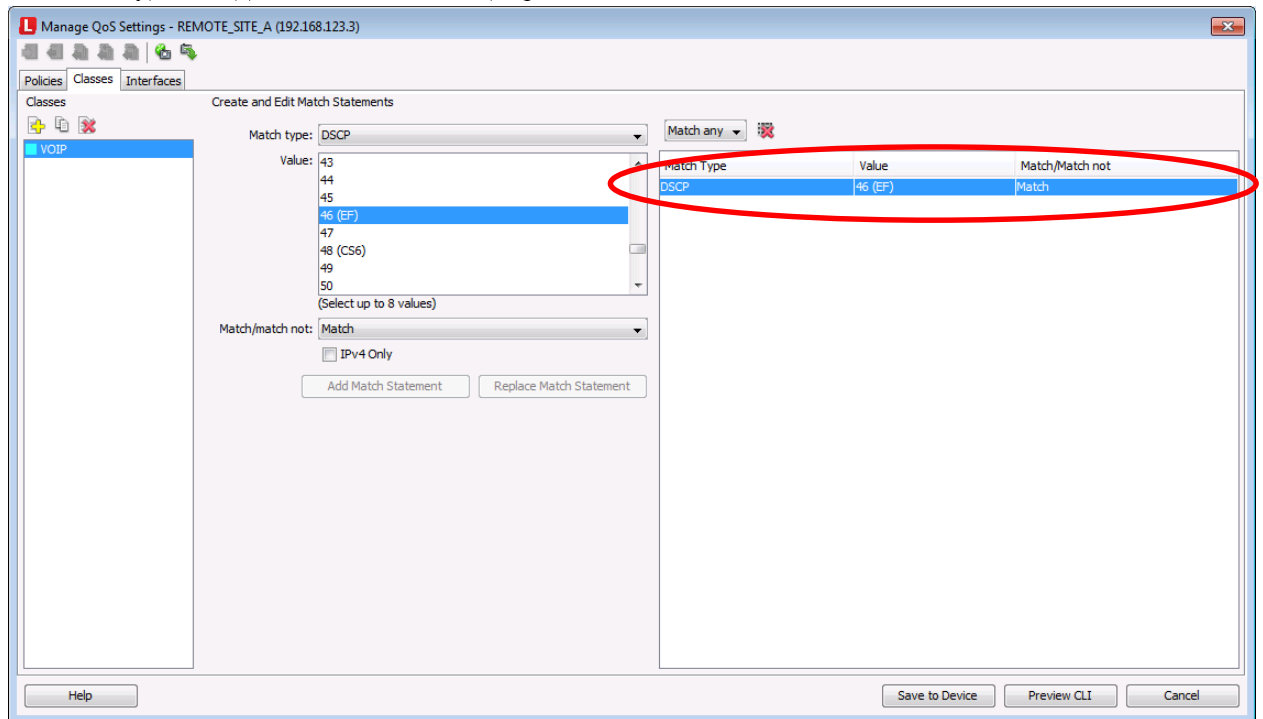
- Click to highlight the VOIP class. Select the Classify tab and click the Edit button.



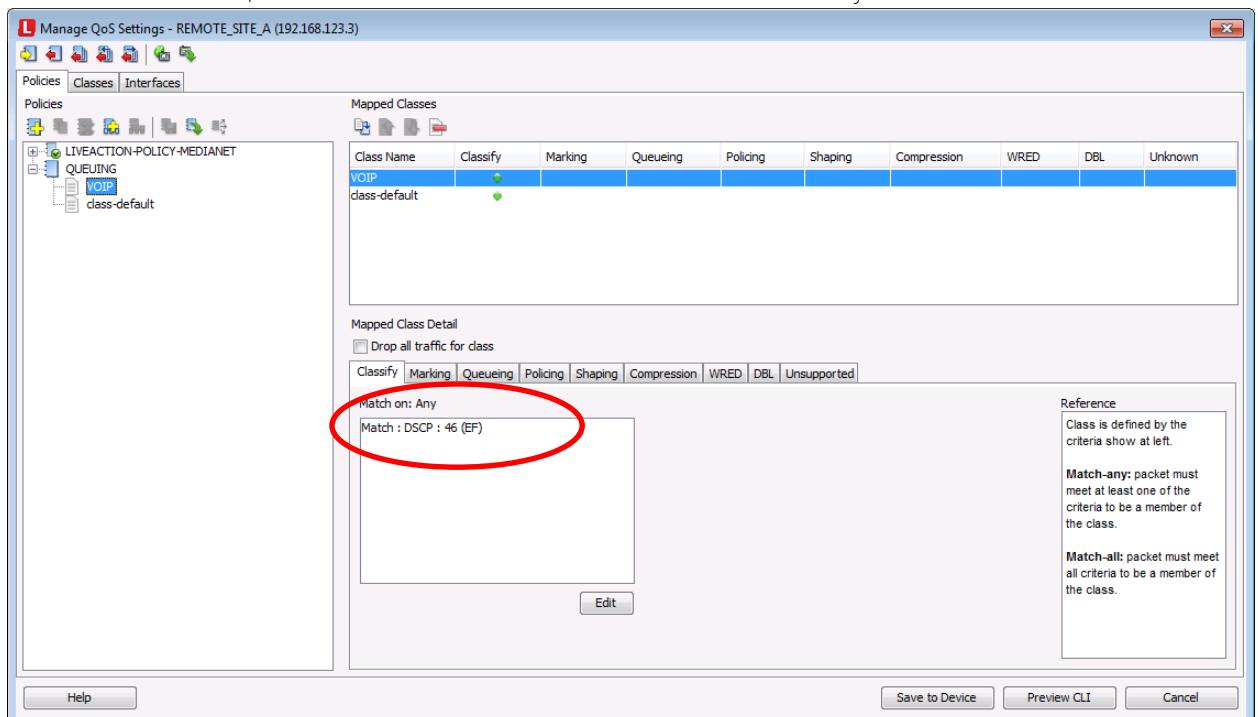
- This brings up the Classes tab. Select the Match type dropdown and select the appropriate match criteria for the VOIP class.
- In this example, the DSCP value of 46(EF) is selected.
- Once the appropriate option is selected, click Add Match Statement.



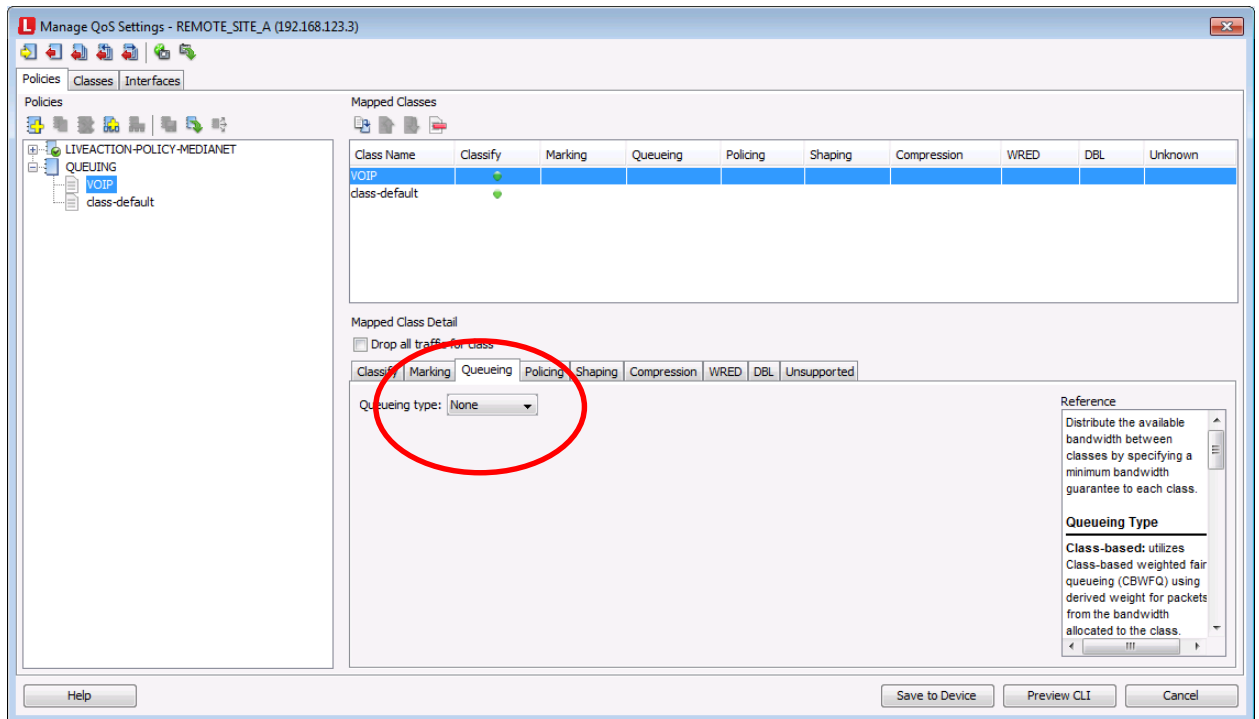
14. The match type will appear in the list to the top right of the window.



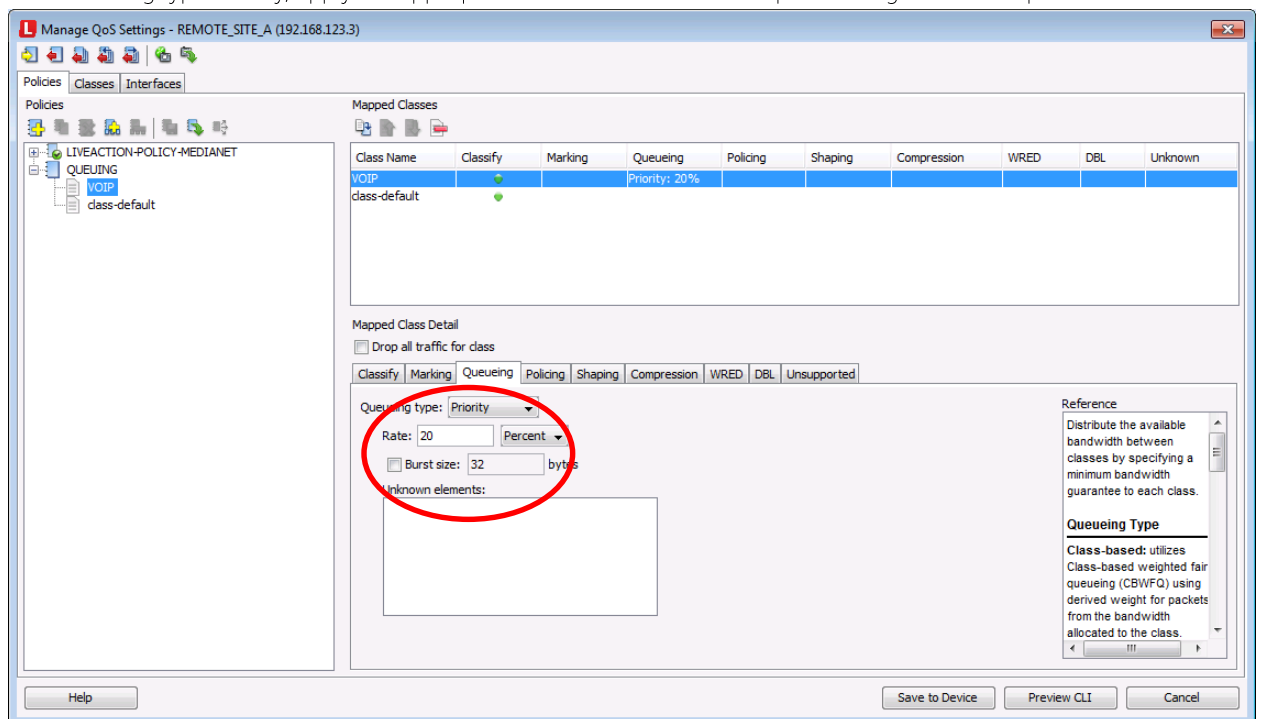
15. Click the Policies tab, notice how the match criteria is now visible in the Classify tab for the class.



16. Click the Queueing tab. Select the Queueing type of Priority.



17. With Queueing type Priority, apply the appropriate bandwidth. In this example 20% is given to this queue.

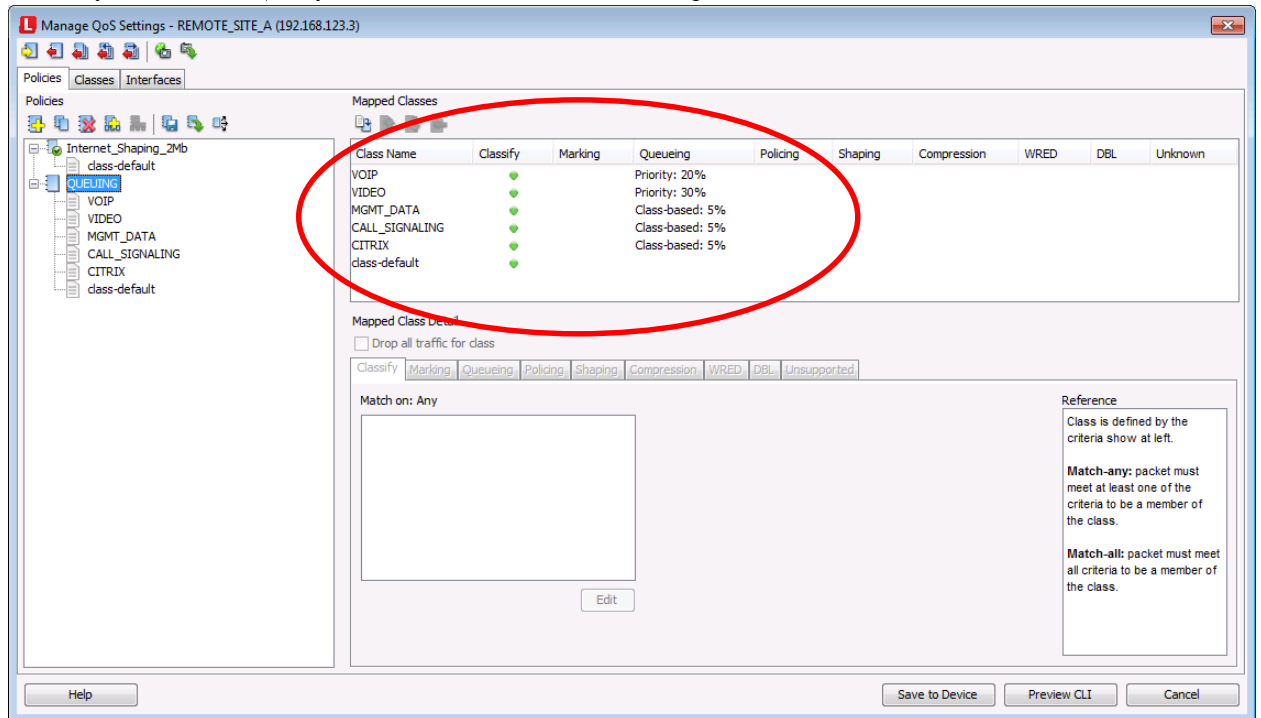


18. Repeat these same steps and create any additional queues required for protection of VoIP, video, and high priority data. In this example, the full QUEUING policy is utilizing the following data:

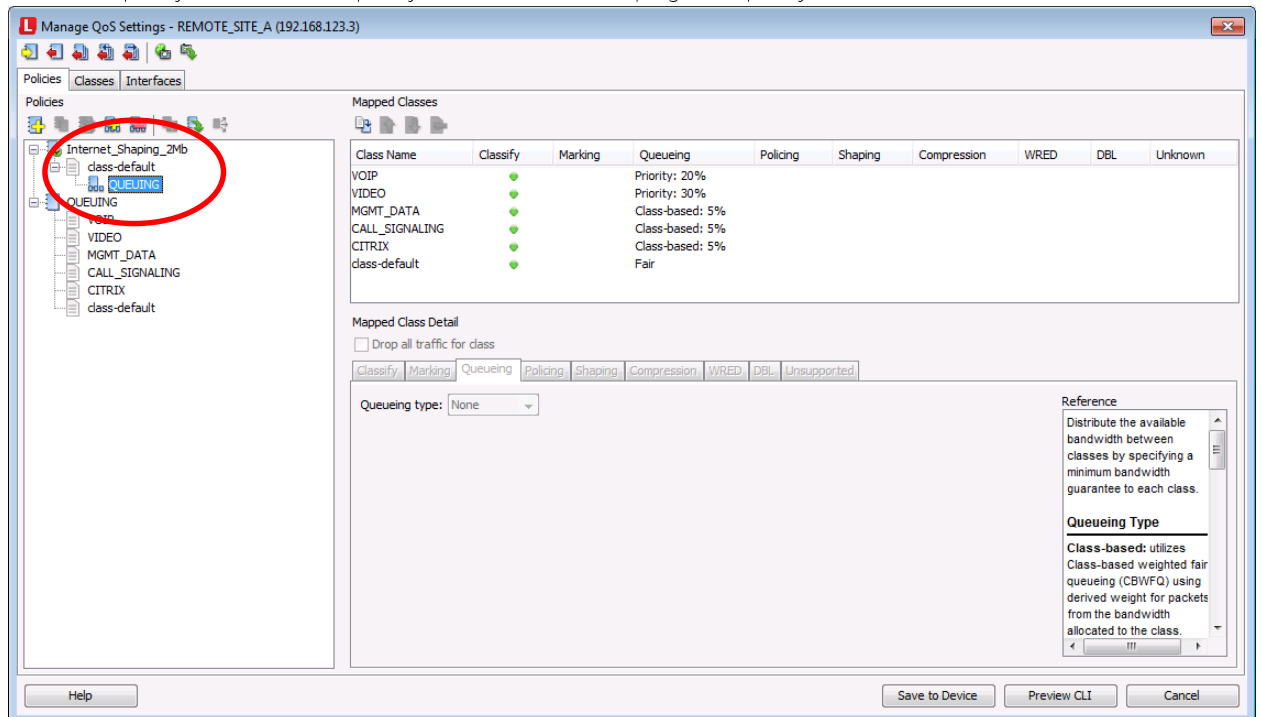
Queue Name	Match Type	Queueing
VOIP	DSCP = EF	Priority = 20%
VIDEO	DSCP = AF41	Priority = 30%, Burst = 128,000
MGMT_DATA	ACL = MGMT_ACL	Class-based = 5%
CALL_SIGNALING	DSCP = CS3	Class-based= 5%

CITRIX	DSCP = AF21	Class-based = 5%
Class-default		Fair-queue

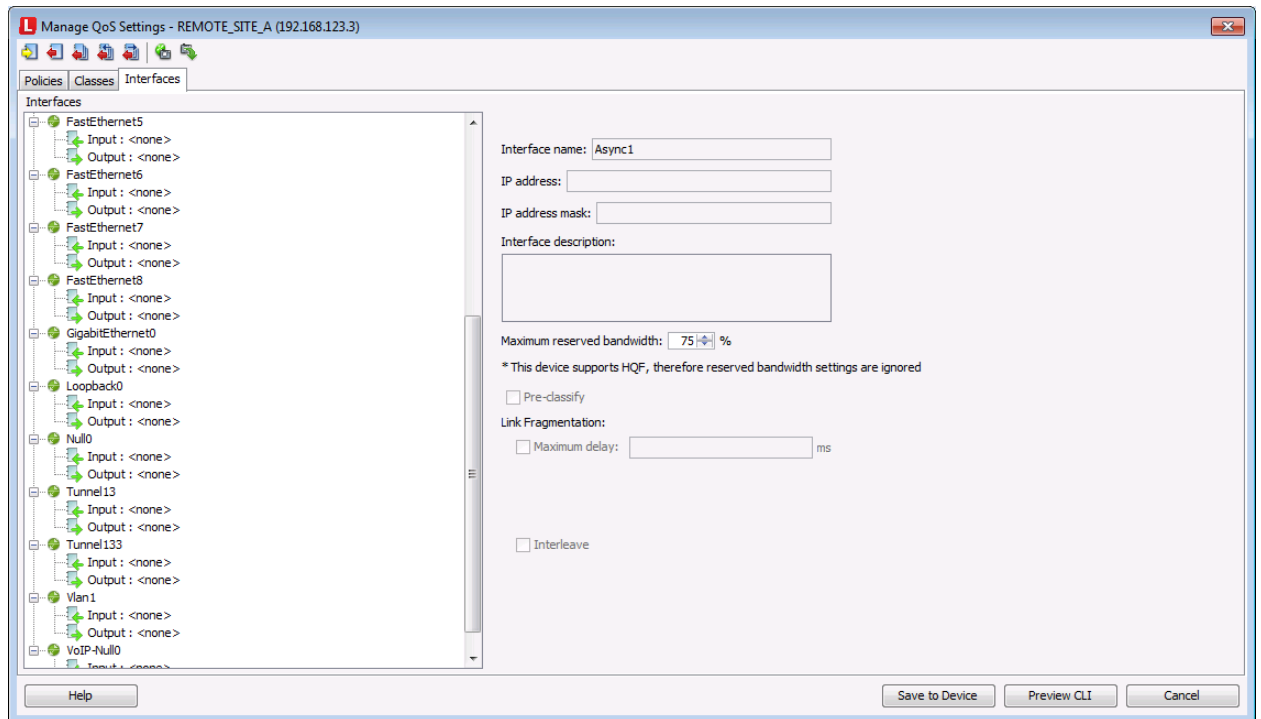
19. When finished, creating all class of the QUEUEING policy, click on the policy named QUEUEING. The summary section of the policy should look similar to the following:



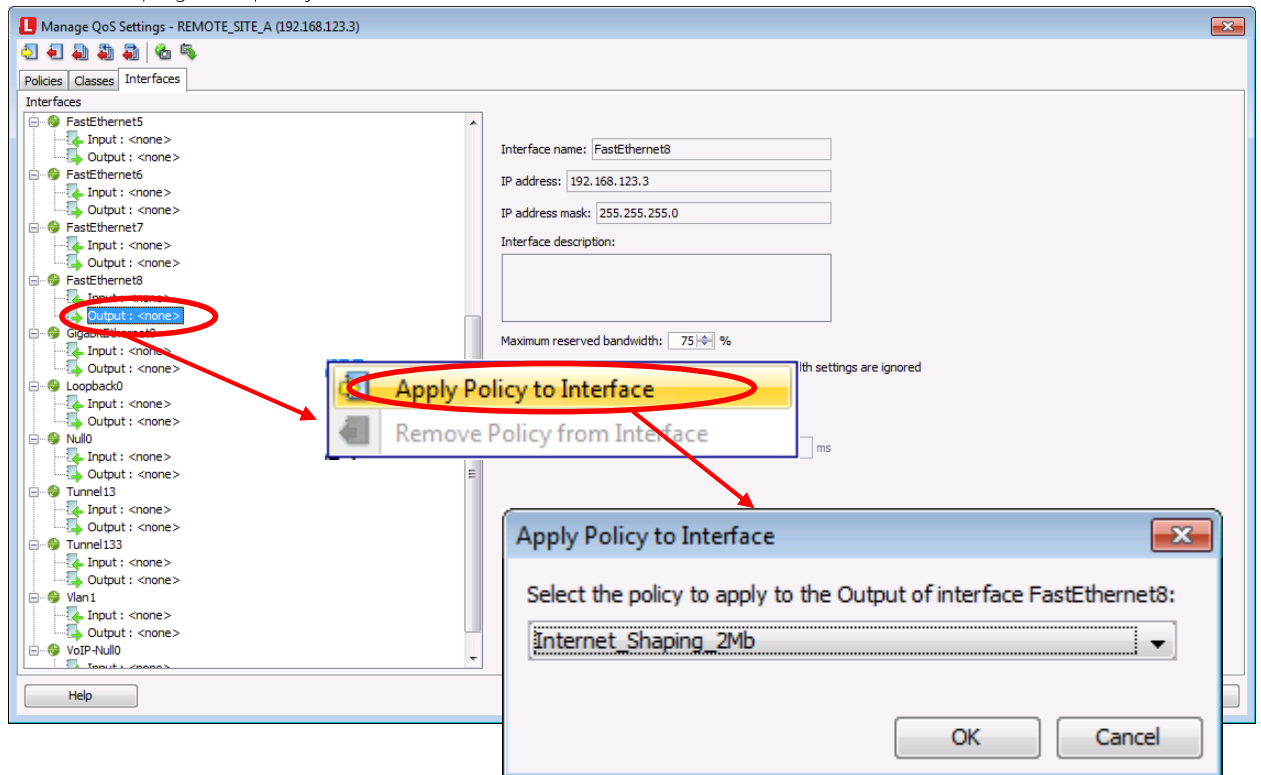
20. Click, drag and drop the QUEUEING policy onto the Internet_Shaping_2Mb policies class-default. The QUEUEING policy will act as child policy for the Internet_Shaping_2Mb policy.



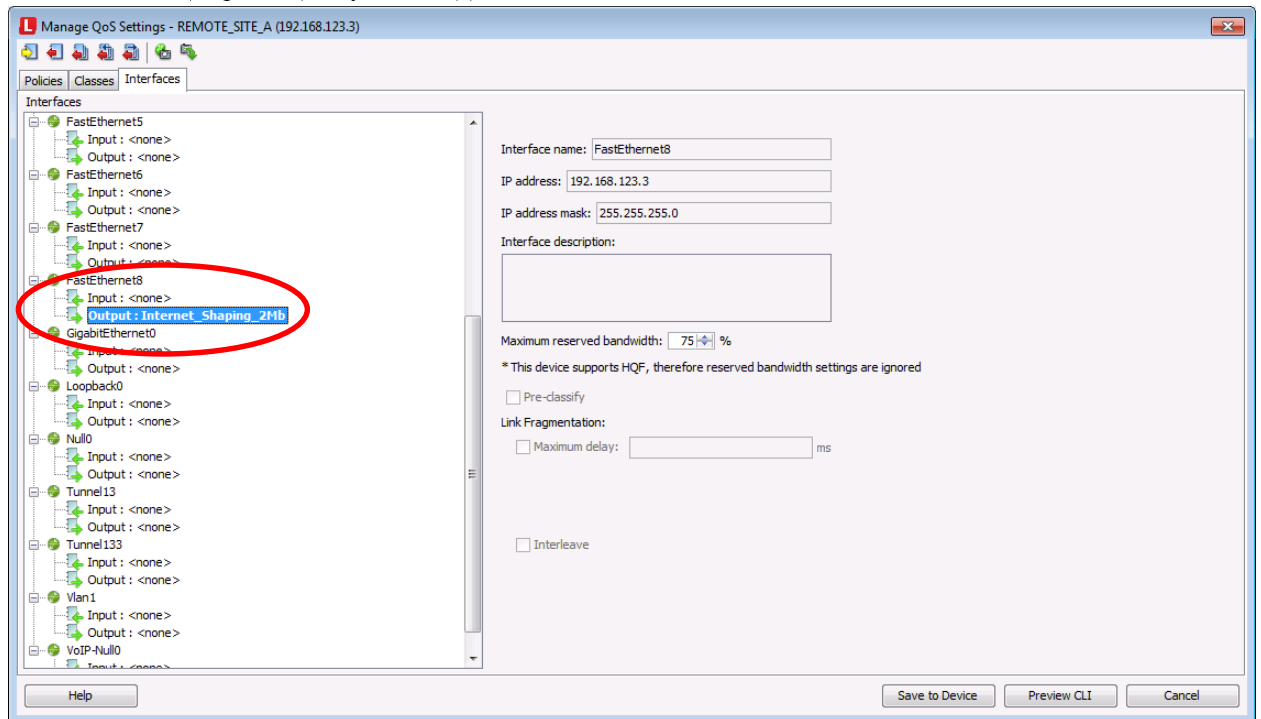
21. Click the Interfaces tab.



22. Right click on the Output of the applicable Internet interface and select Apply Policy to Interface. Select the Internet_Shaping_2Mb policy and Click OK.



23. The Internet_Shaping_2Mb policy will be applied to the Internet interface.

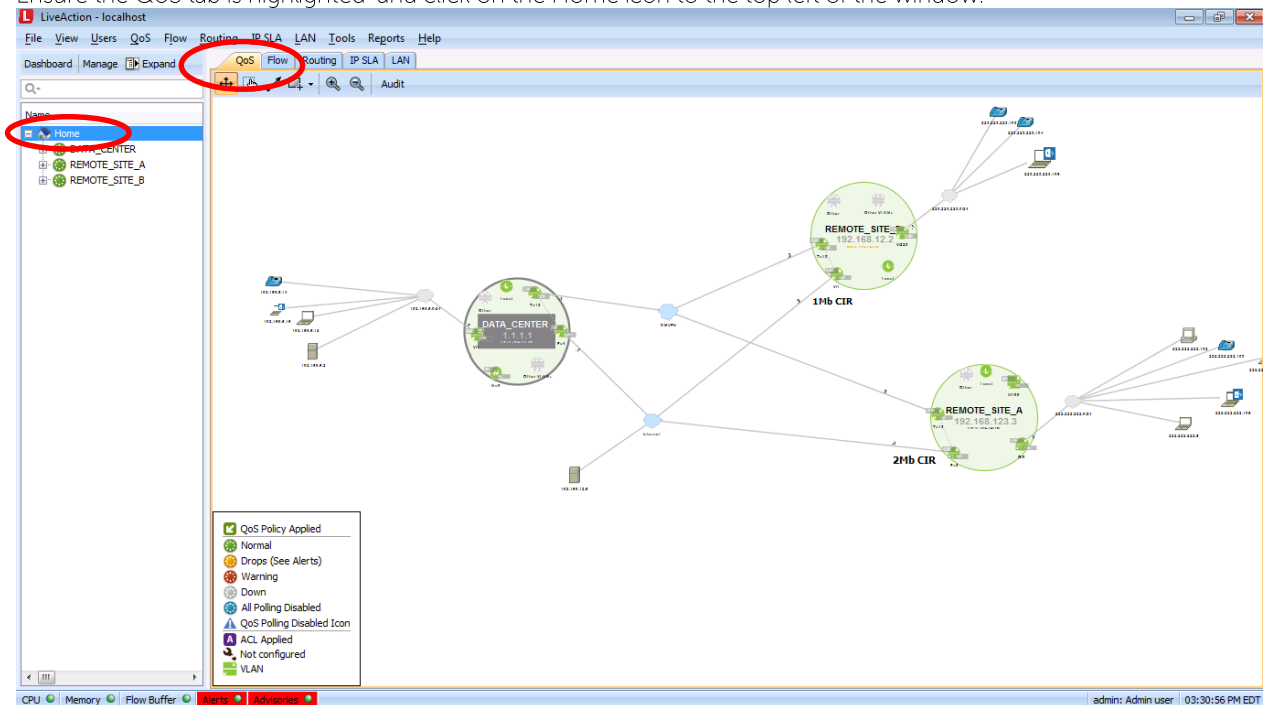


24. Click Save to Device.

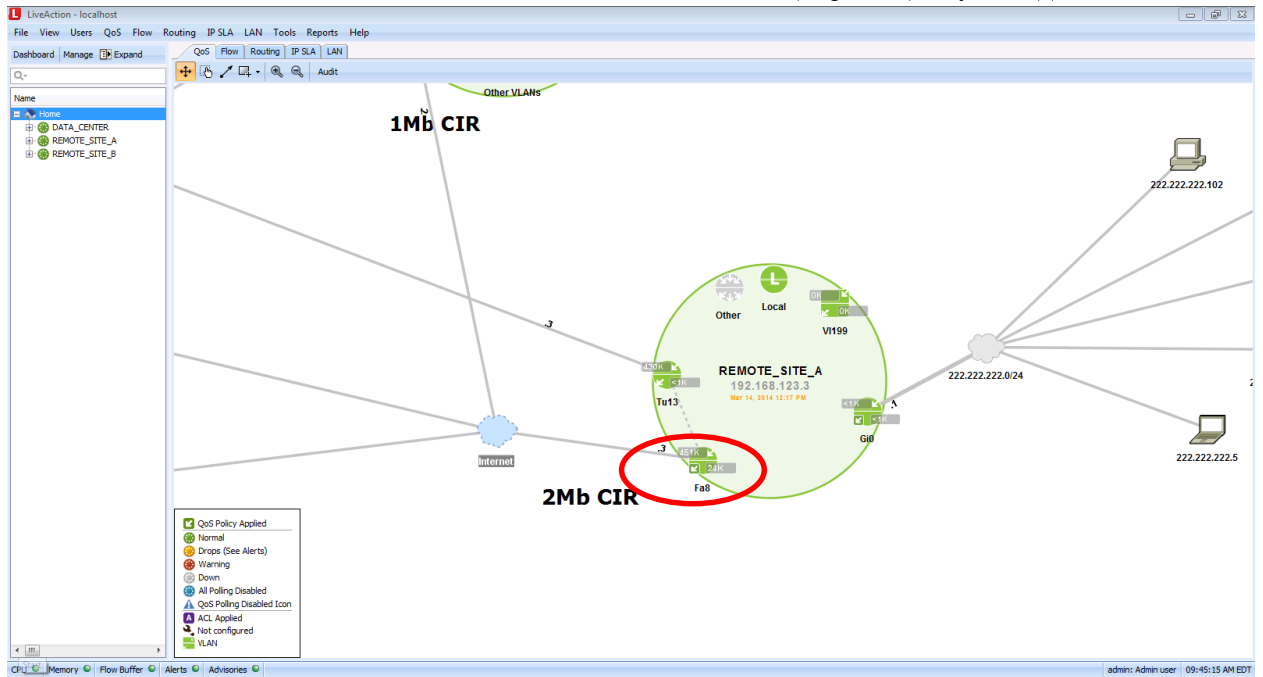
Remote Site DMVPN QoS Validation

To validate the hierarchical shaping policy on the Internet interface, perform the following:

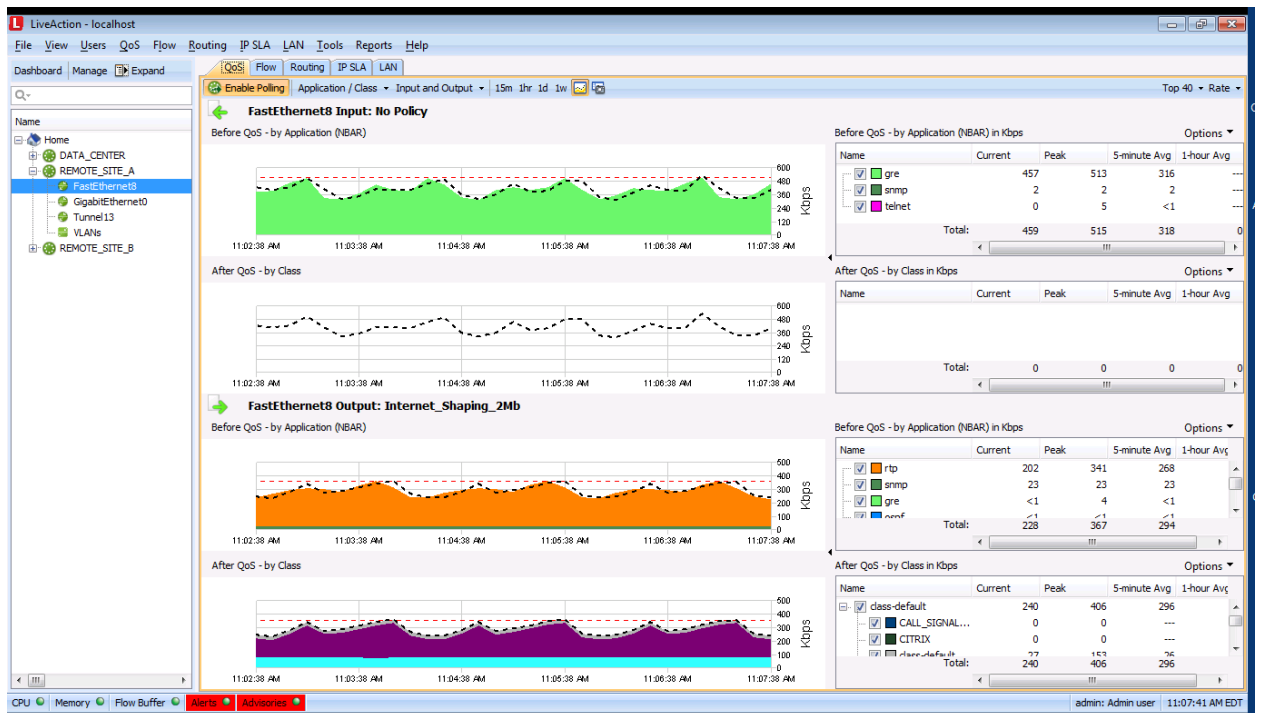
1. Ensure the QoS tab is highlighted and click on the Home icon to the top left of the window.



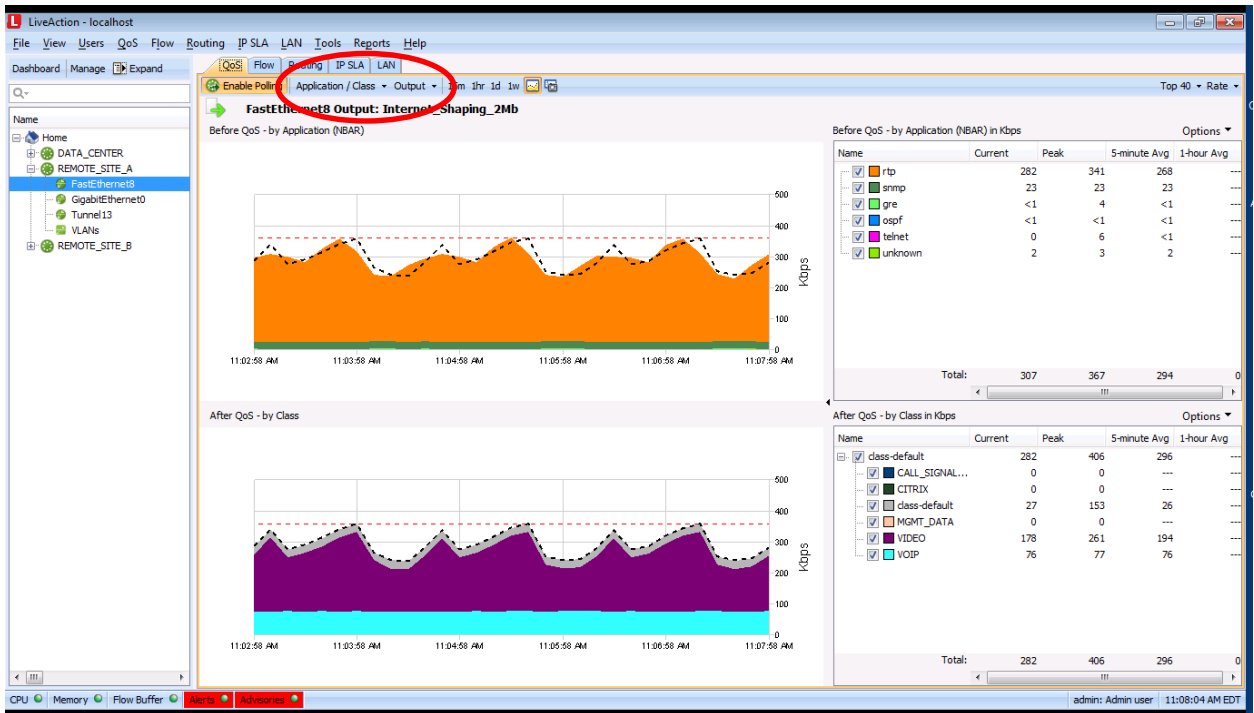
2. Double-click on the remote site's Internet interface where the Internet_Shaping_2Mb policy was applied.



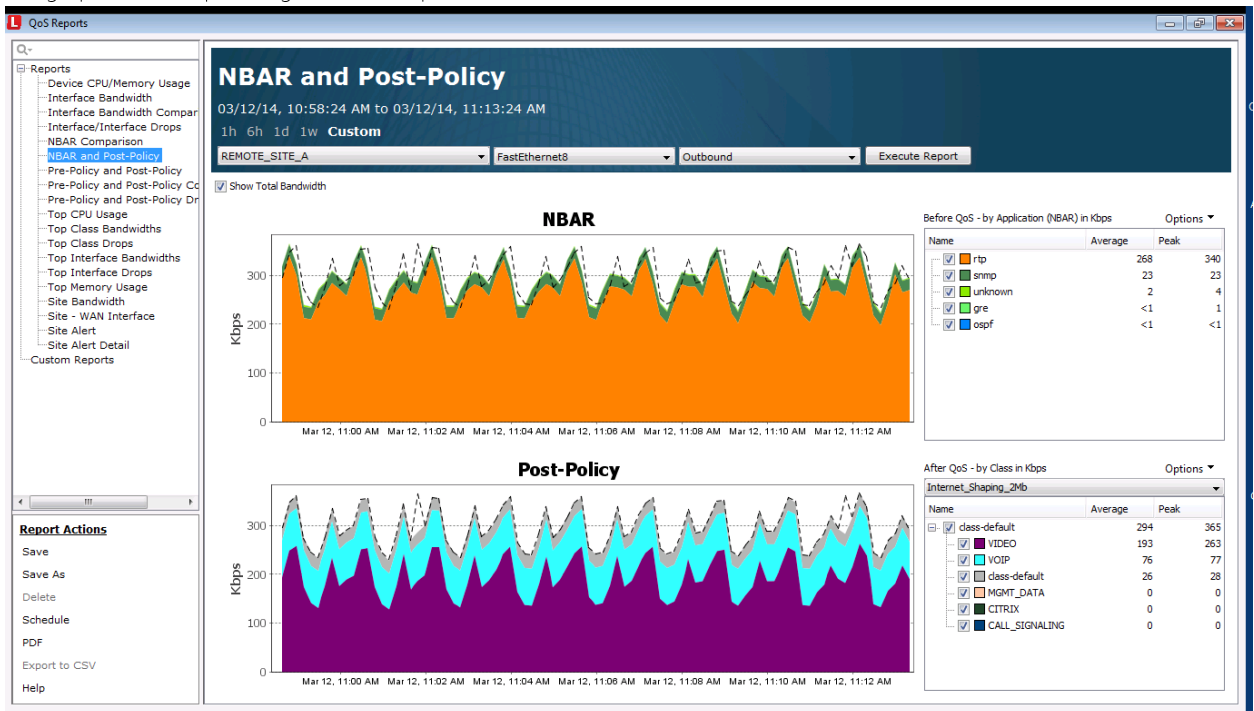
3. This will show the real-time statistics of this interface.



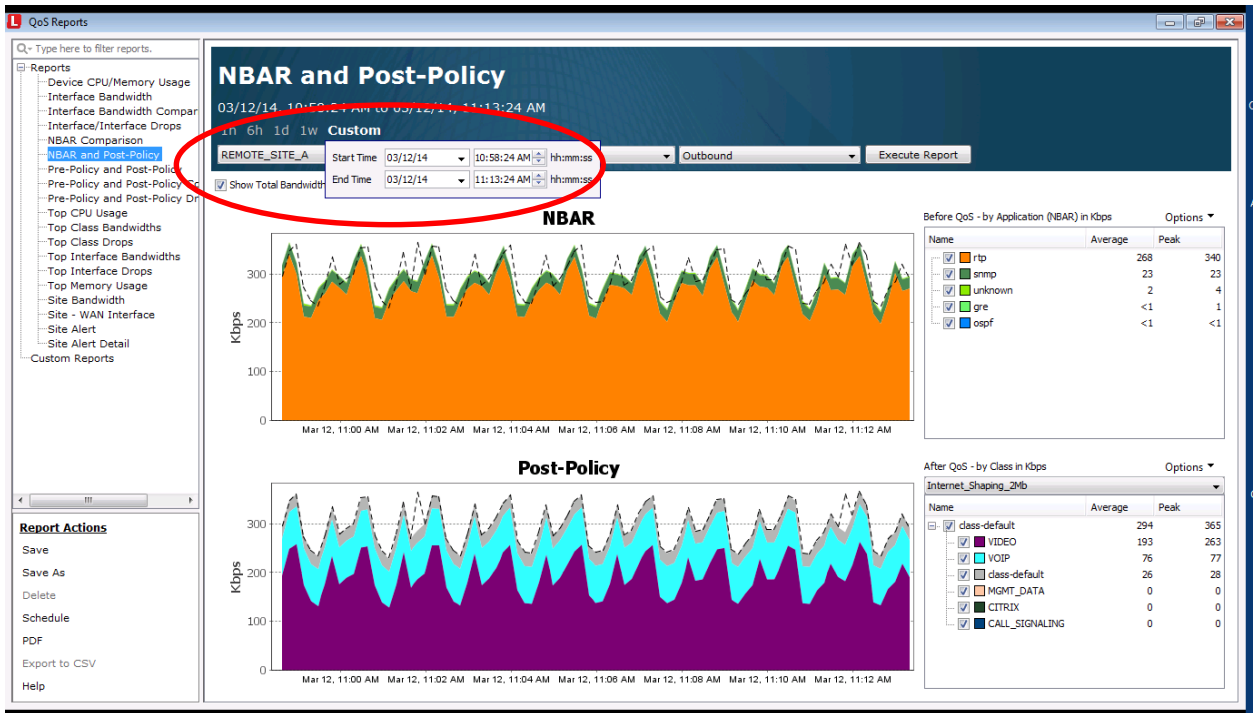
4. Ensure that the drop down menus at the top of this page show Application/Class and Output. This will ensure the graph is focusing on the interface's output statistics. In the example below, notice the bottom graph. This is a graphical view of the CBQoS MIB, the real-time QoS stats of the Internet_Shaping_2Mb policy. Note that the bandwidth graph is showing data in the VOIP and VIDEO queues.



- To view historical statistics for this interface, select the 15m, 1hr, 1d, 1w icons at the top of the page. This will bring up the corresponding historical reports.



- The time range of the historical statistics can be further customized by utilizing the time range options on the report.

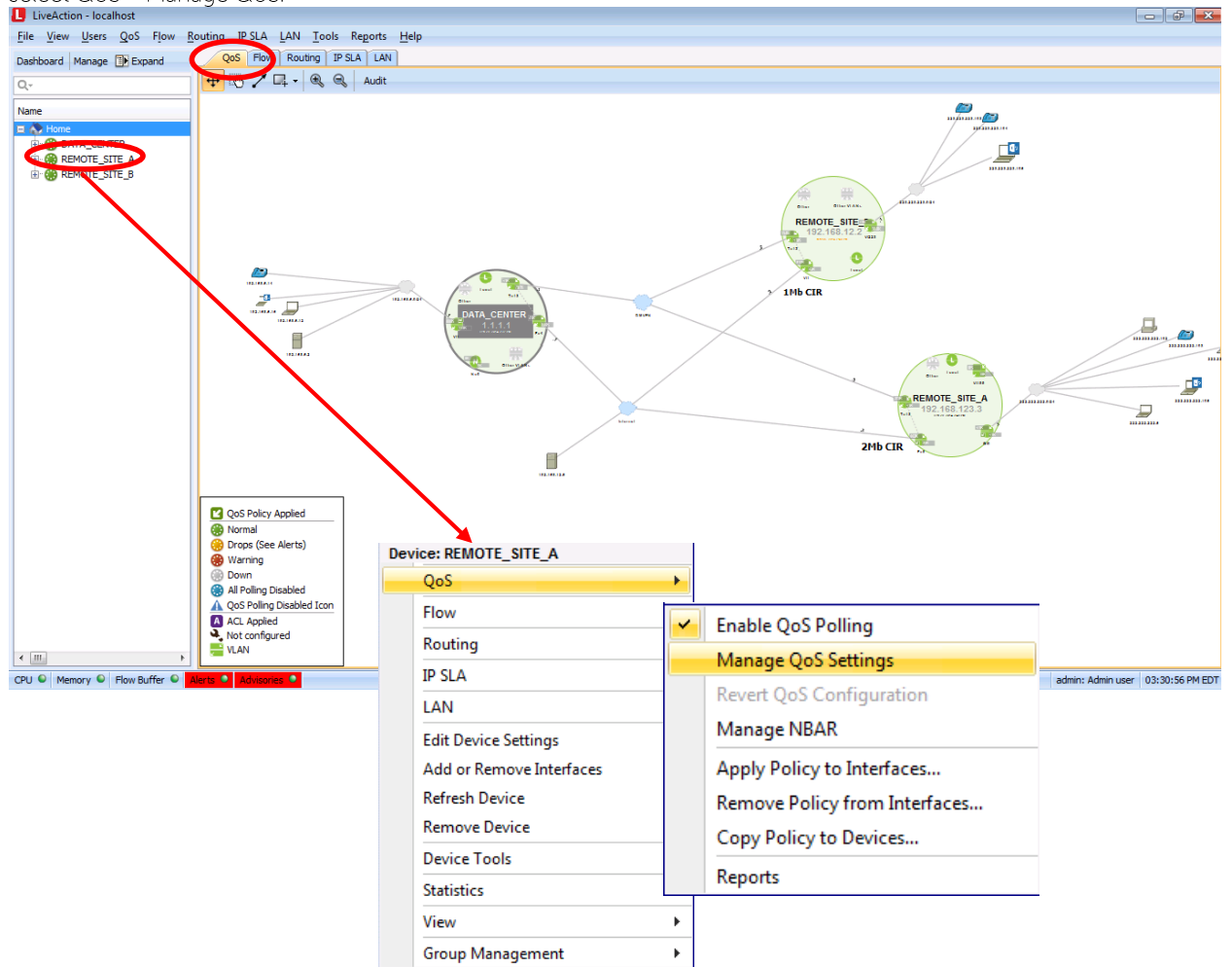


Data Center DMVPN Per-Tunnel QoS Configuration

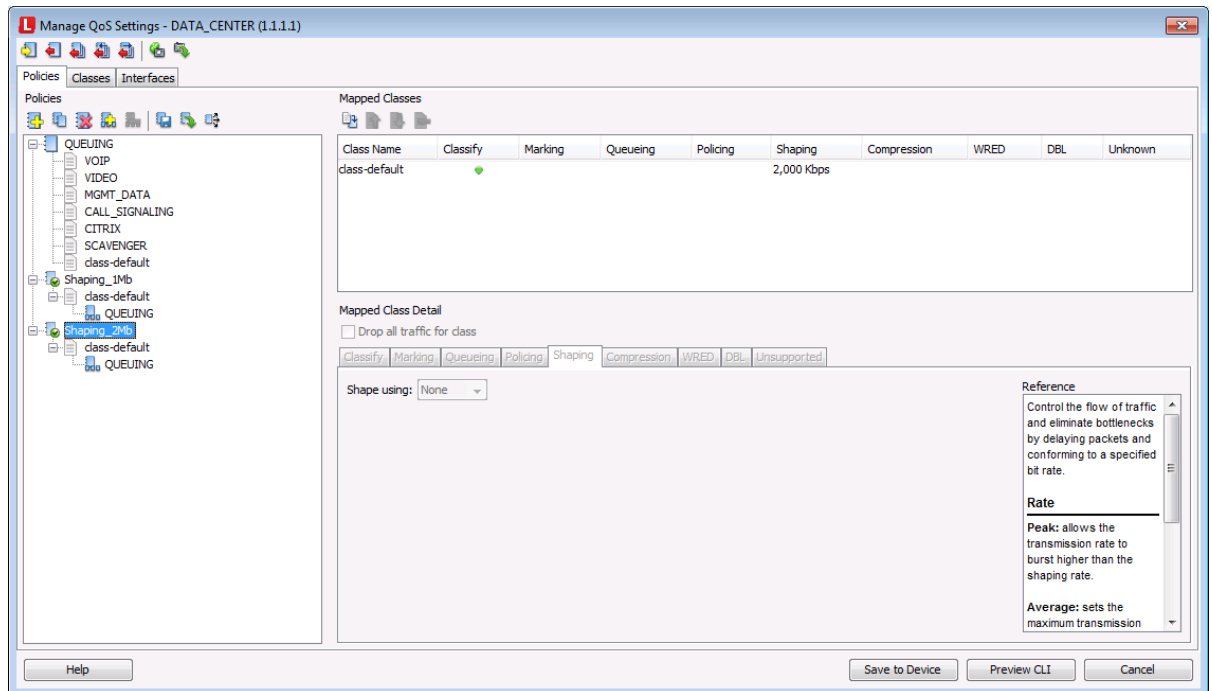
Configuring Per-Tunnel QoS at the data center will require all remote DMVPN devices to utilize the following command on their tunnel interfaces: `ip nhrp group <GROUP_NAME>`. The following example is assuming that each remote site already has this prerequisite command in place.

Each NHRP group will get its own unique hierarchical QoS policy on the data center router. The configuration steps to configure these hierarchical QoS policies are identical to those of the remote site DMVPN QoS configuration as outlined in this document. This section will only focus on concepts unique to Per-Tunnel QoS. To implement Per-Tunnel QoS, perform the following:

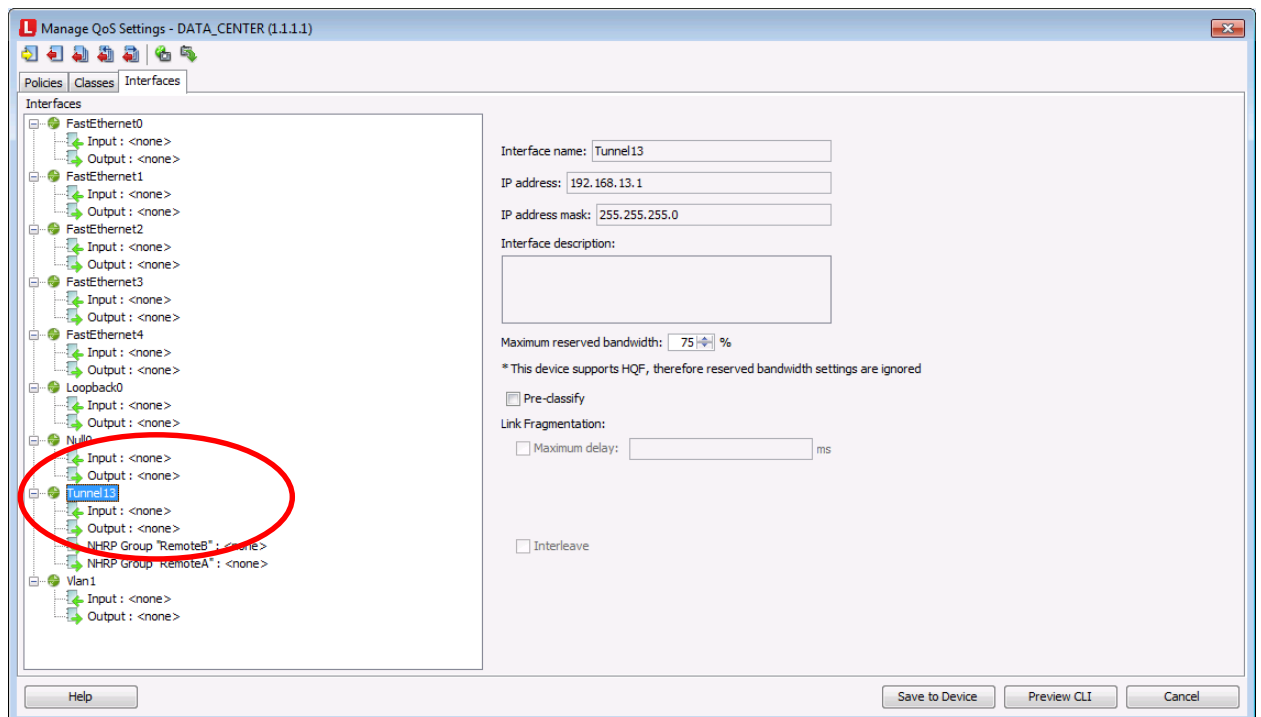
1. Select the QoS tab. Then, right-click the on the data center object in the device list. In the pop-up menu select QoS > Manage QoS.



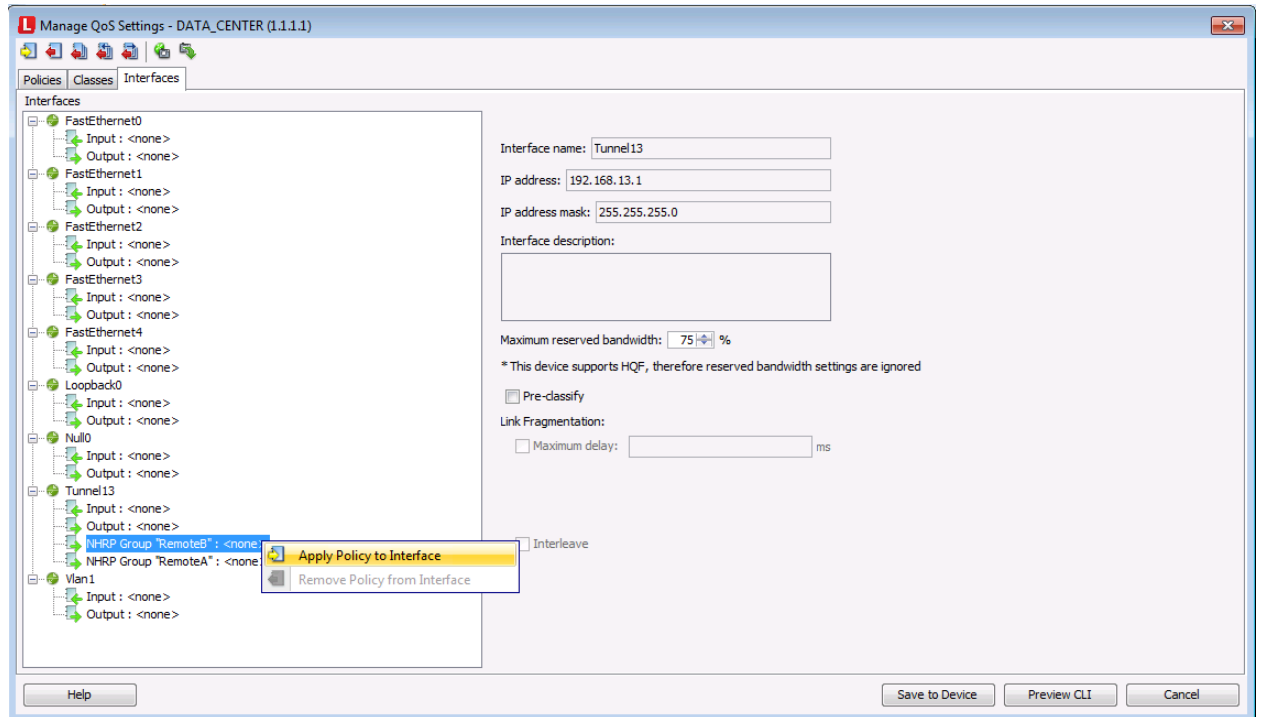
2. The Managed QoS dialog window appears. In the example below, a QUEUING and two hierarchical policies are already configured on the data center DMVPN device. These were created using the steps outlined in the remote site DMVPN QoS configuration of this document.



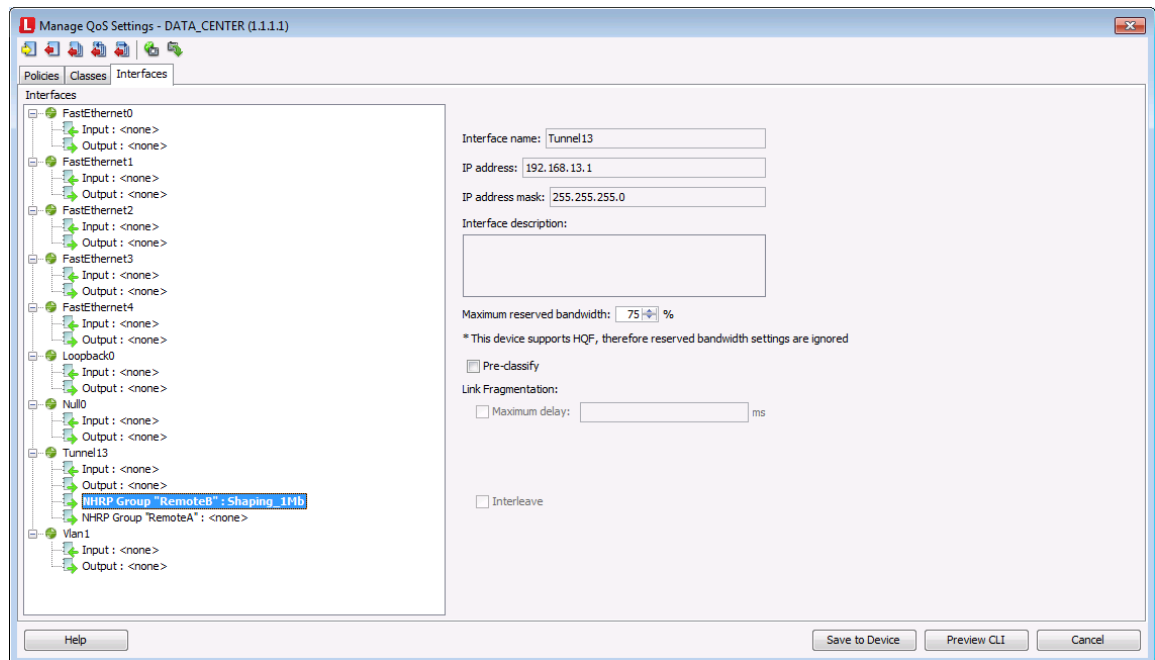
3. Select the Interfaces tab. Notice how the data center's DMVPN tunnel interface shows NHRP Group information. This is because LiveAction discovered the remote site's the group memberships on the data center router.



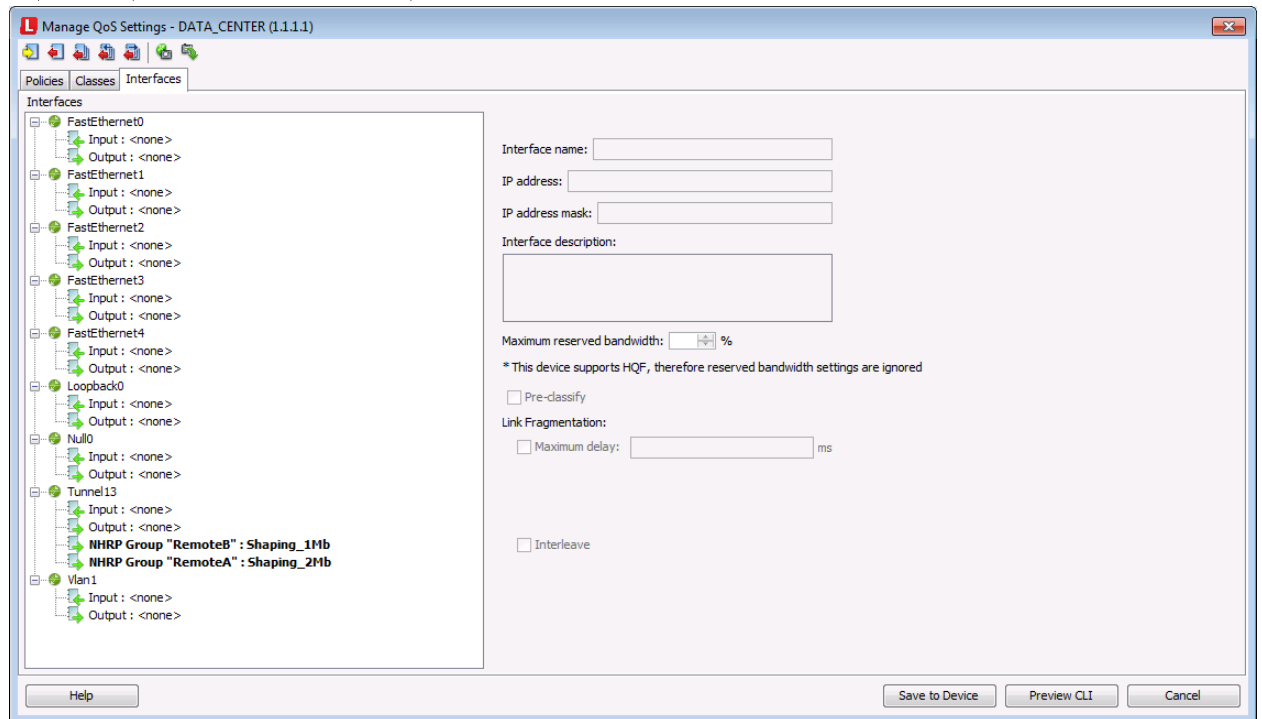
- Right click on one of the NHRP Groups and select Apply Policy to Interface.



- Select the appropriate hierarchical QoS policy for the NHRP Group.



- Repeat this process for all NHRP Groups.



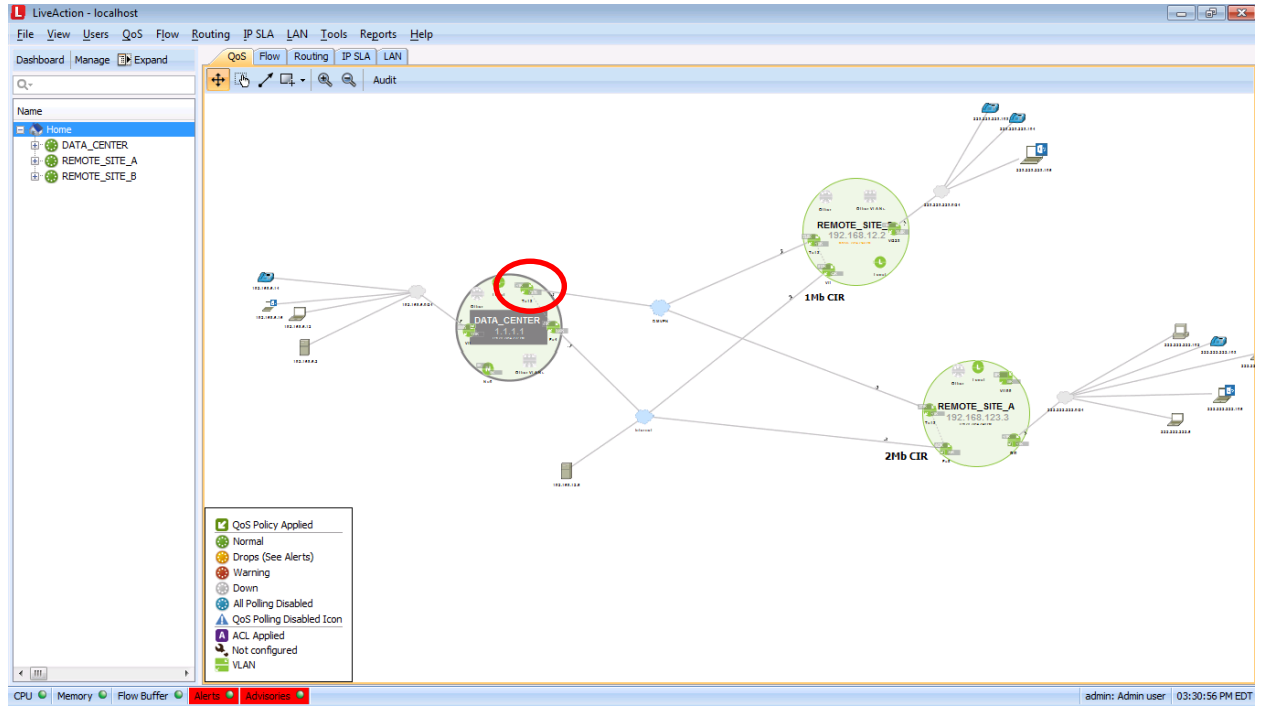
- Click Save to Device.

Data Center DMVPN QoS Validation

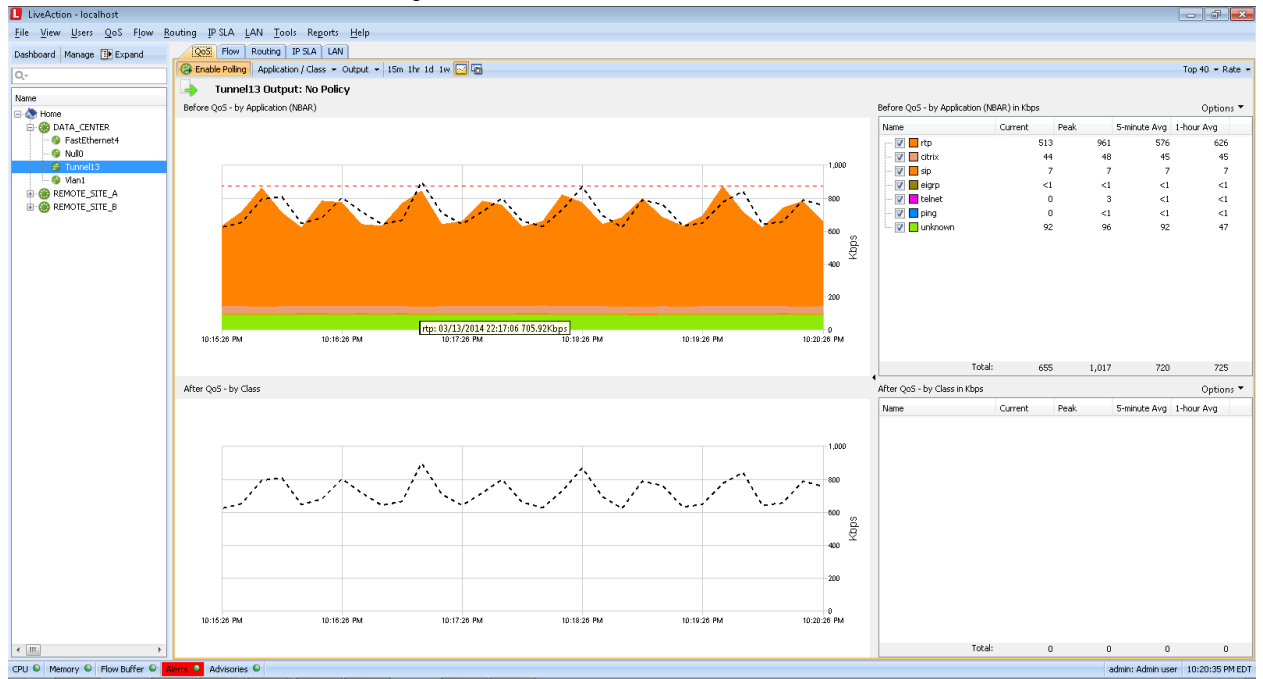
At the time of this document's creation, Cisco has not yet implemented the CBQoS MIB for Per-Tunnel QoS. Due to this limitation, it is not possible for LiveAction to monitor these QoS statistics directly because the MIB does not yet exist. But LiveAction can use its robust NetFlow reporting to provide similar data. To monitor Per-Tunnel QoS statistics using LiveAction's NetFlow reports, perform the following task:

- Click the Home icon to view the network diagram.
- Click the QoS tab.

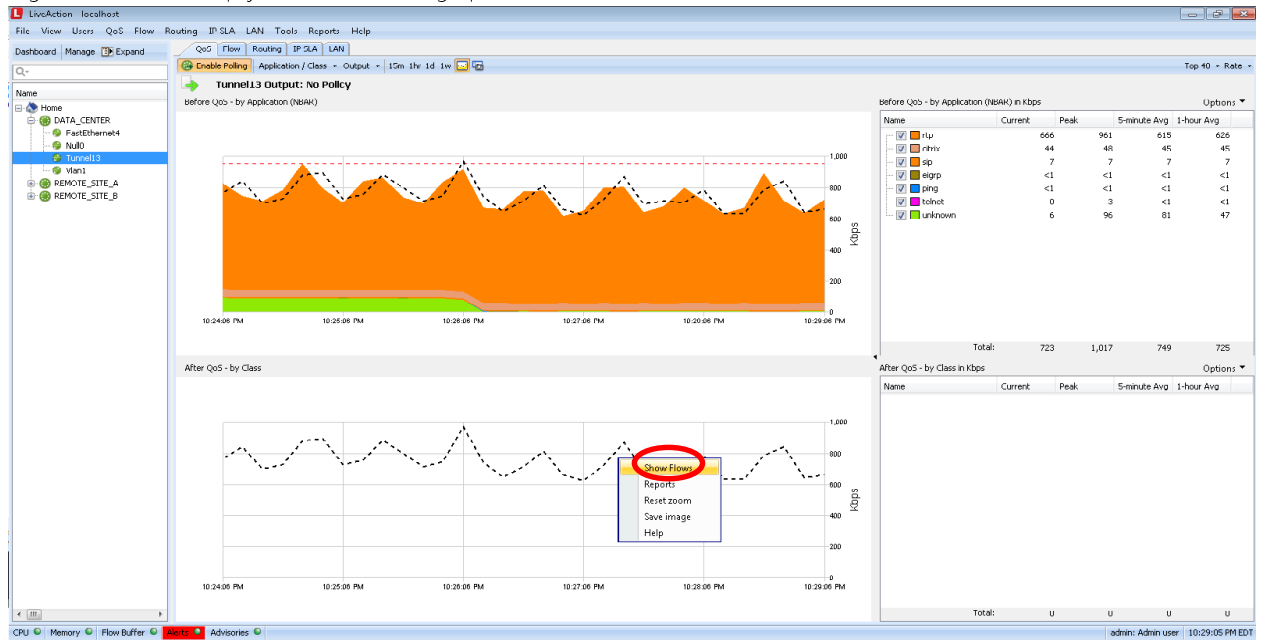
3. Double-click on the data center's DMVPN tunnel interface.



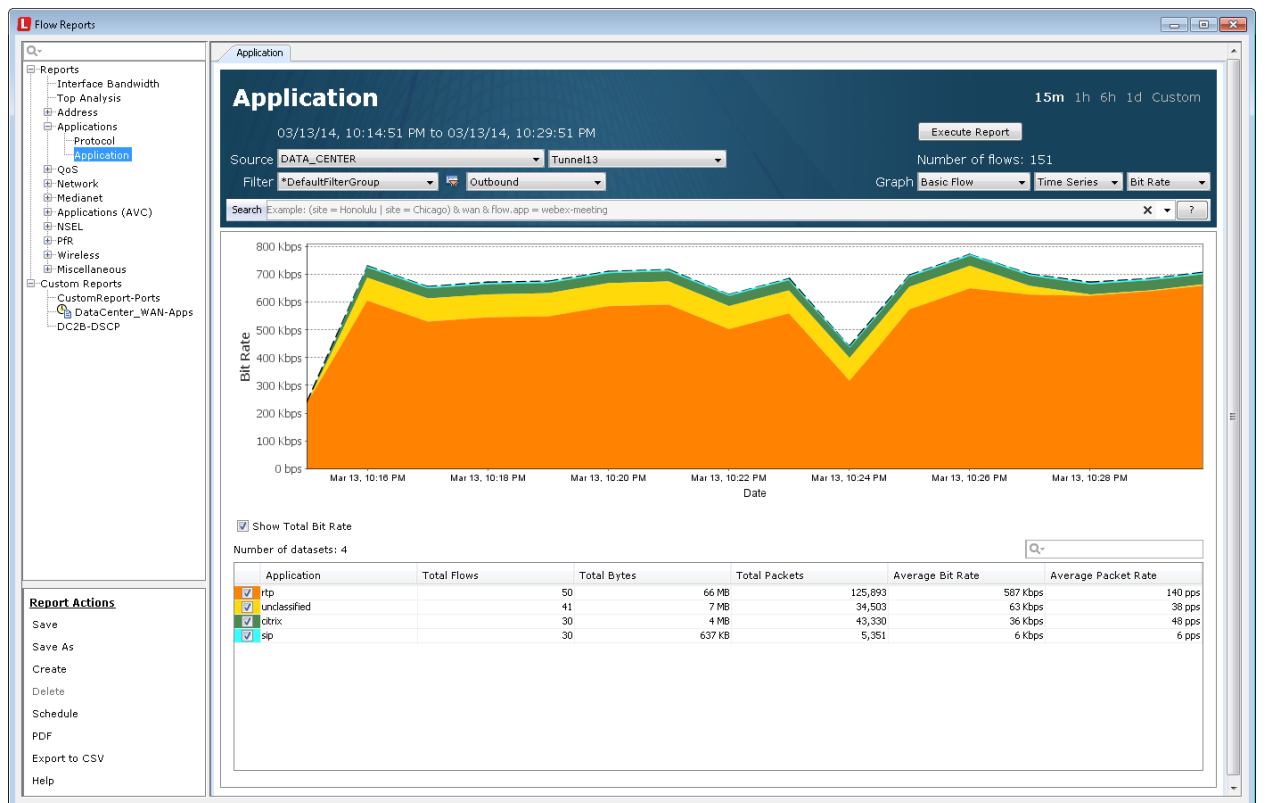
4. This will show the real-time interface statistics of the tunnel interface. Notice how there are now QoS statistics for this Per-Tunnel QoS configuration.



- Right-click in the empty QoS bandwidth graph and select Show Flows.



- This will run the corresponding NetFlow Applications > Application report for the data center's DMVPN tunnel interface.

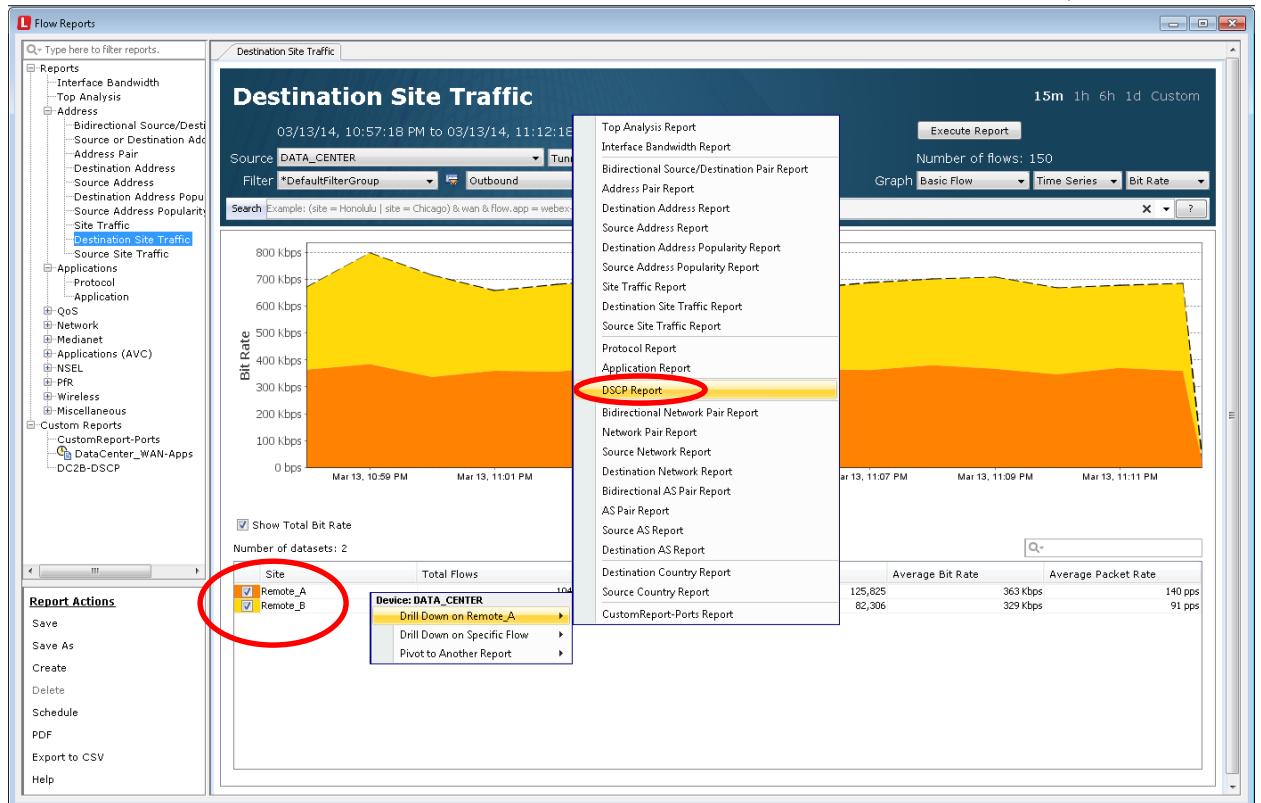


- From the report list, select the Address > Destination Site Traffic report and click the Execute Report button.

The screenshot displays the 'Flow Reports' application window. On the left, a navigation tree lists various report categories, with 'Destination Site Traffic' highlighted under the 'Address' section. The main panel shows the report configuration for 'Destination Site Traffic' on 03/13/14, from 10:57:18 PM to 11:12:18 PM. The source is set to 'DATA_CENTER' and the tunnel to 'Tunnel13'. The filter is 'DefaultFilterGroup' and 'Outbound'. The number of flows is 150. Below the configuration is a line graph showing 'Bit Rate' over time, with a peak around 700 kbps. At the bottom, a table shows the number of datasets (2) and a summary table for 'Remote_A' and 'Remote_B'.

Site	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate
Remote_A	104	41 MB	125,825	363 kbps	140 pps
Remote_B	46	37 MB	82,306	329 kbps	91 pps

- This report will show the data center's tunnel interface bandwidth utilization for each remote site. Right click on a remote site's name in the table, select Drill Down on <Site Name>, and select the DSCP Report.



- This will filter the previous report so only the bandwidth of the selected site will be visible. This bandwidth will be categorized by DSCP value. Since the Per-Tunnel QoS QUEUEING policy is referencing DSCP values for class selection, this report is the equivalent of a QoS bandwidth graph.



10. For easy access to see this report again, save the report. It can be viewed on demand at any time or scheduled at daily, weekly or monthly time periods.

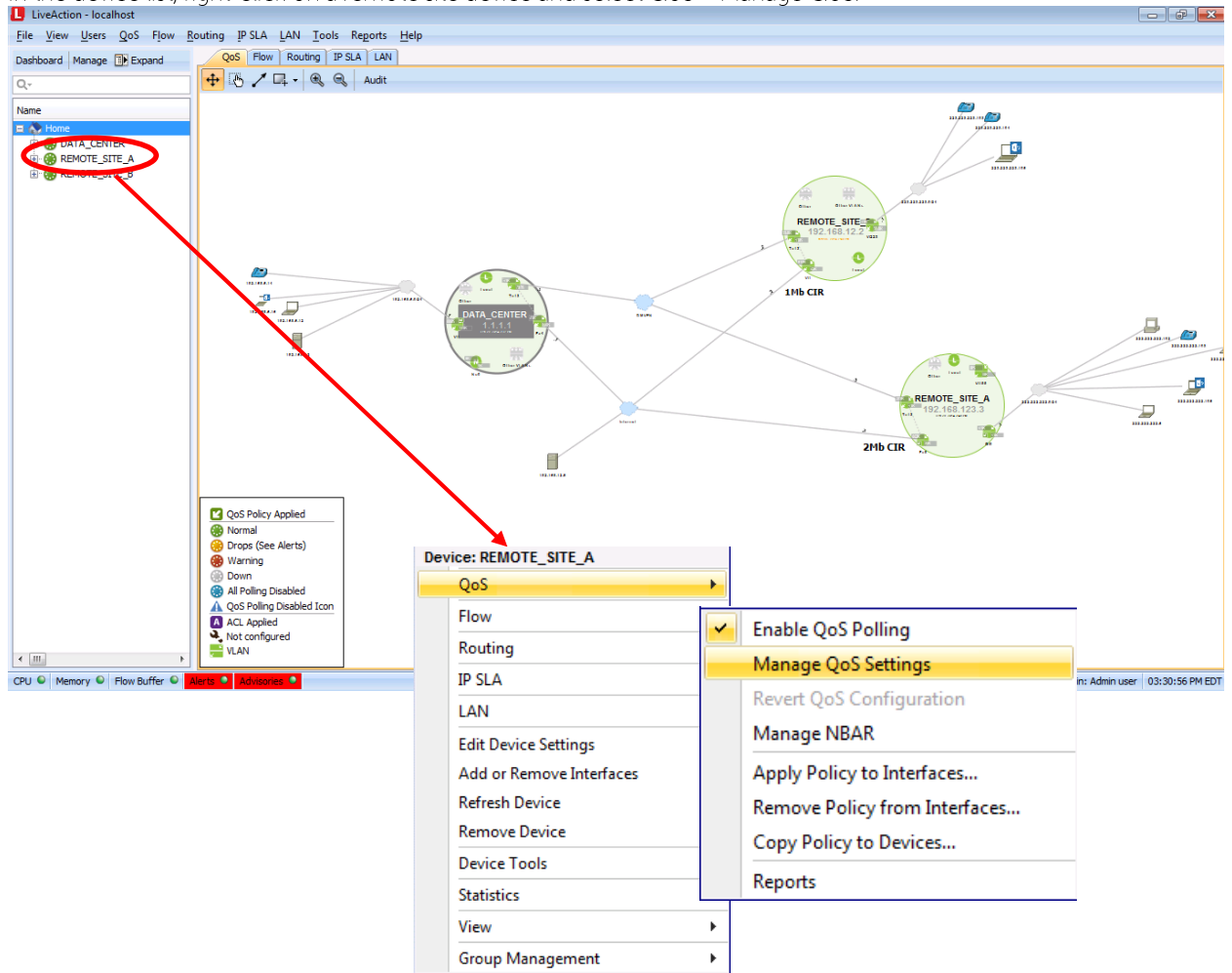
Remote Ingress Shaping QoS Configuration.

Remote Ingress Shaping (RIS) is a technique for protecting inbound tunnel traffic from casual Internet traffic. It can protect VoIP, video and priority tunnel data from Internet based TCP traffic. RIS is nothing more than a hierarchical QoS policy applied to a DMVPN router's LAN interface in the outbound direction. A key configuration component of RIS is that the parent shaping policy will only use 95% of the Internet circuit's logical bandwidth. Usually in DMVPN designs, Internet service providers will use an Ethernet broadband connection with a CIR or cap on the throughput. The RIS QoS policy will shape to 95% of the CIR.

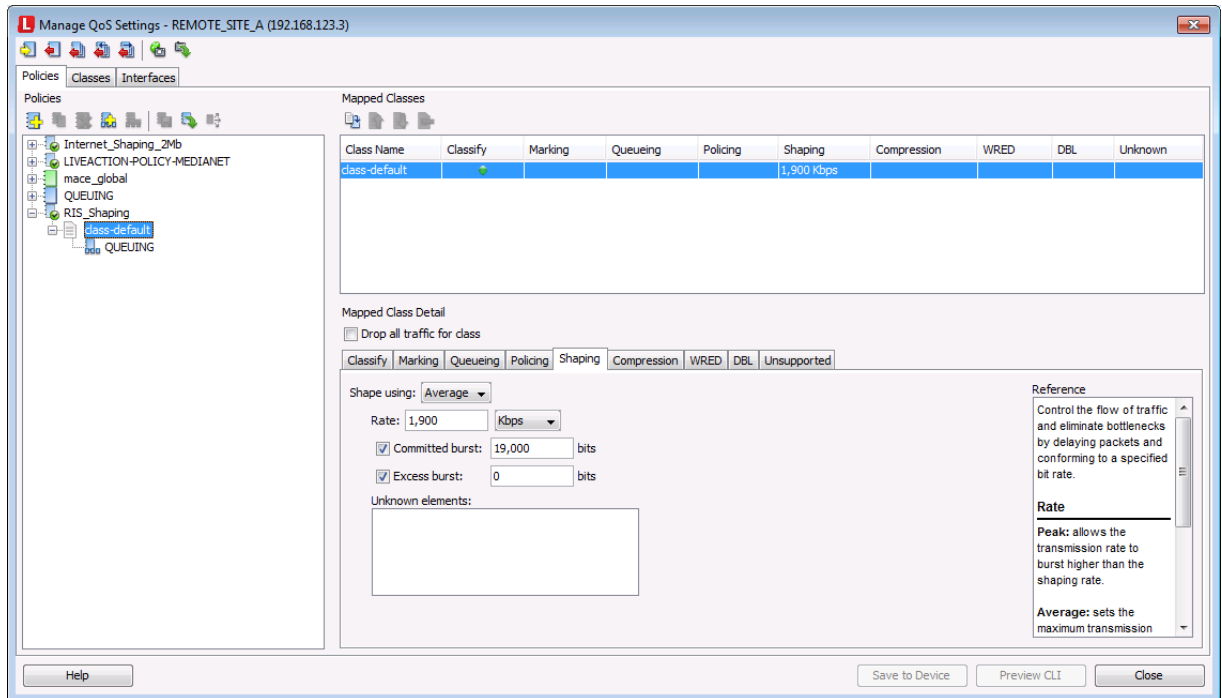
The configuration of a RIS hierarchical QoS policy as identical the other policies outlined in this document. Only the differences will be highlighted.

1. Click the Home icon to view the network diagram.
2. Click the QoS tab.

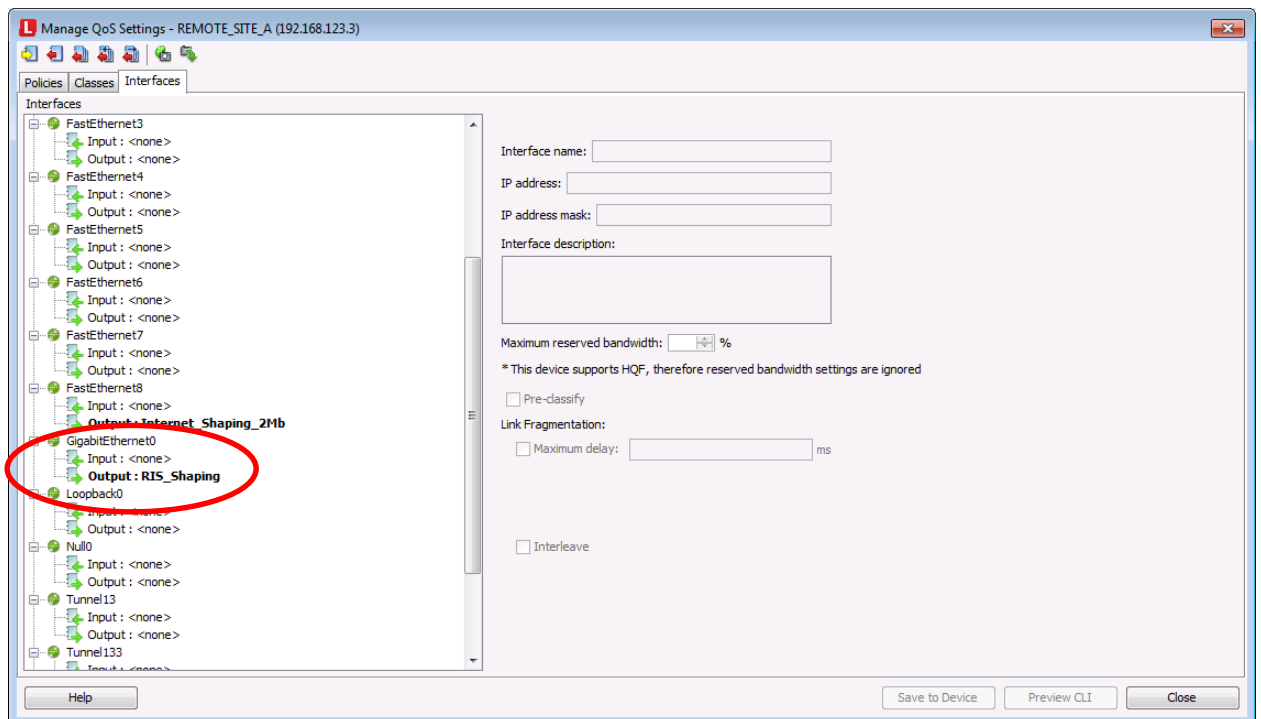
3. In the device list, right-click on a remote site device and select QoS > Manage QoS.



- In the Manage QoS dialog window example below, a hierarchical policy named RIS_Shaping has already been created following the steps outlined in this document. In this example the parent classes' shaper is set to 95% of the logical bandwidth of the Internet circuit.



- Once the RIS policy has been created, select the Interfaces tab and apply the RIS policy to the Output of the LAN interface.



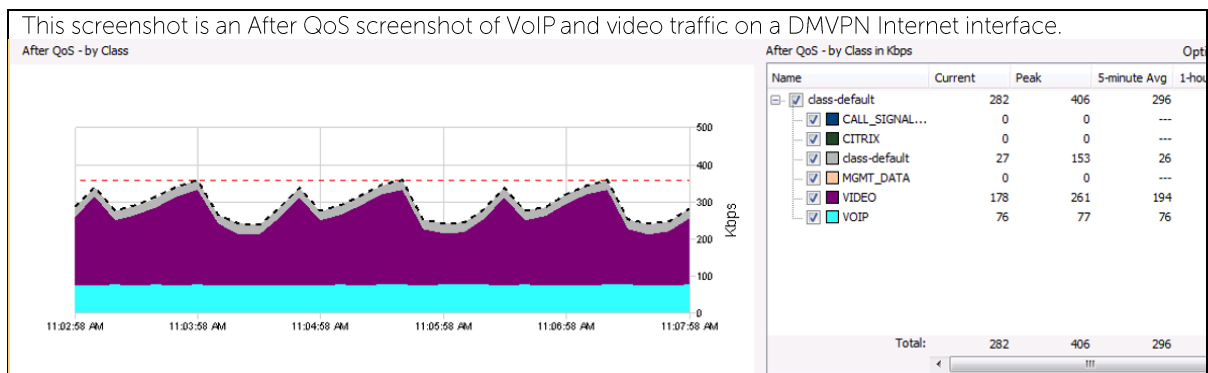
Validating DMVPN QoS with LiveAction

LiveAction can be used to validate DMVPN QoS performance in many ways. These are:

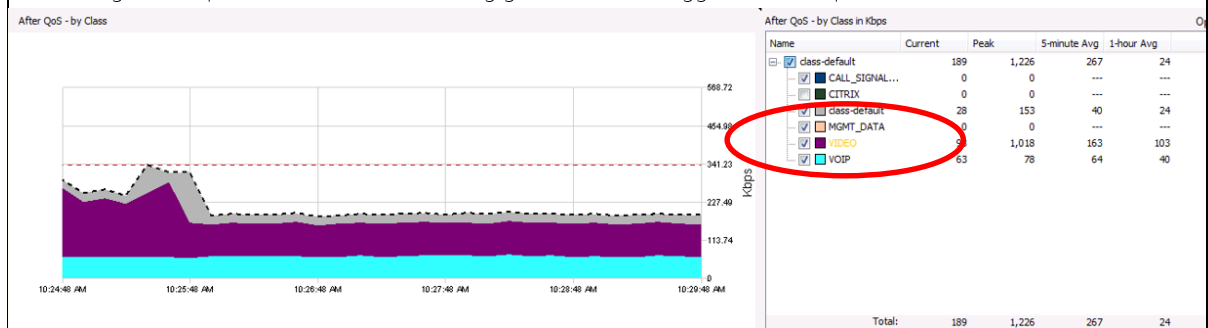
- Reports
- Alerts
- Medianet (Cisco's Medianet Performance Monitor)

Reports

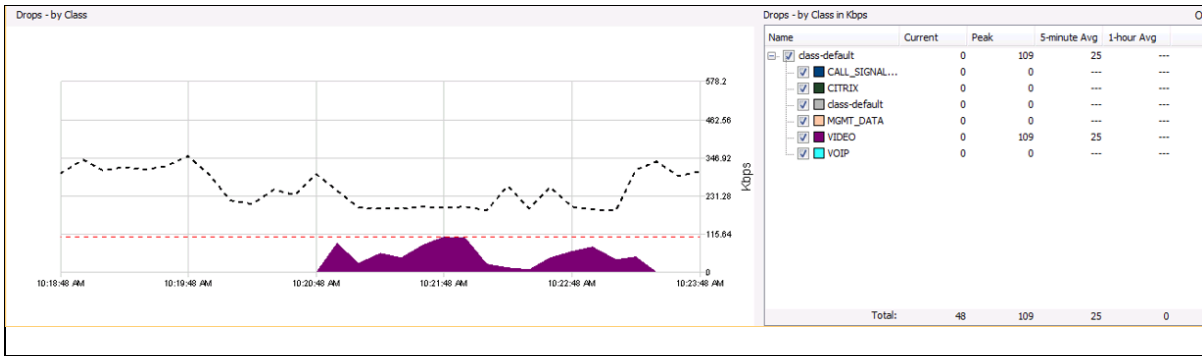
LiveAction's real-time and historic reporting provides a very granular view of how DMVPN QoS polices are performing. LiveAction stores QoS data in raw format, with no averaging. This gives engineers the ability to drill down into historic QoS events and view them as if they were occurring in real-time. LiveAction can also show QoS statistics from three angles: Before QoS, After QoS, and Drops. Below examples LiveAction real-time QoS screenshots.



This is a second After QoS screenshot. Notice how the VIDEO queue is amber. This indicates drops are actively occurring in this queue. QoS Alerts are being generated and logged when a queue is amber.



This is a screenshot of the QoS Drops view. The purple in the graph shows the drop rate of traffic in the VIDEO queue. The VIDEO queue is not amber indicating that the drops are not actively occurring.



Alerts

LiveAction will generate an alert whenever a configurable QoS threshold is crossed. These alerts will be saved and can be reviewed by doing a historical search. This makes pinpointing the exact times of past QoS issues easy to identify. LiveAction alerts can also be sent to an external Syslog or Email server. LiveAction's QoS alerts include:

- Interface Drop Rate
- QoS Class Drop Rate
- QoS Class-Default Rate
- Interface Bandwidth Utilization
- QoS Bandwidth Utilization

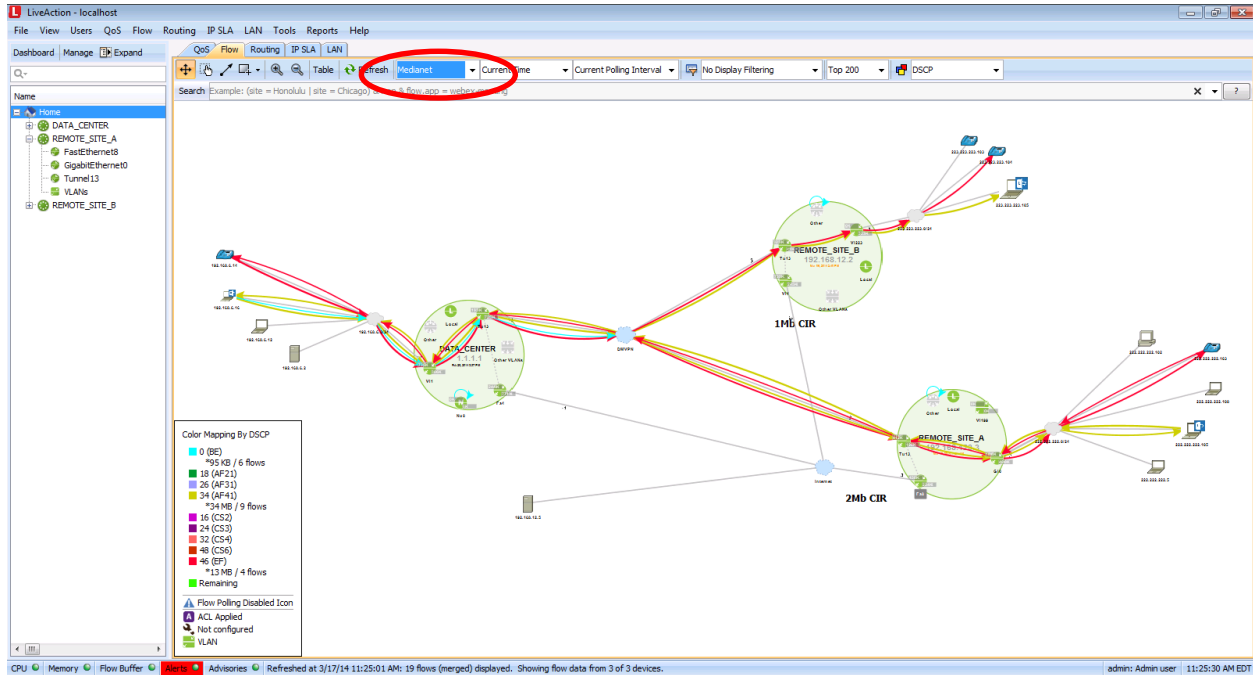
Time	Severity	Device	Group	Alert Type	Details
2014/03/17 10:08:35 AM	Warning	REMOTE_SITE_B	Device Conf...	Running config may have changed since startup confi...	
2014/03/17 10:10:48 AM	Warning	REMOTE_SITE_A	Device Conf...	Running config may have changed since startup confi...	
2014/03/17 10:13:35 AM	Warning	REMOTE_SITE_B	Device Conf...	Running config may have changed since startup confi...	
2014/03/17 10:15:48 AM	Warning	REMOTE_SITE_A	Device Conf...	Running config may have changed since startup confi...	
2014/03/17 10:18:35 AM	Warning	REMOTE_SITE_B	Device Conf...	Running config may have changed since startup confi...	
2014/03/17 10:19:21 AM	Warning	REMOTE_SITE_A	Device Conf...	Device configuration changed	Username - admin; Commands - config t; policy-map QUEUING; class VIDEO; no priority ...
2014/03/17 10:20:44 AM	Warning	REMOTE_SITE_A	Device Conf...	Device configuration changed	Username - admin; Commands - config t; policy-map QUEUING; class VIDEO; police 1100...
2014/03/17 10:20:48 AM	Warning	REMOTE_SITE_A	Device Conf...	Running config may have changed since startup confi...	
2014/03/17 10:20:48 AM	Warning	REMOTE_SITE_A	QoS	Class-default dropped rate	Interface name - FastEthernet0; Interface direction - OUTPUT; Policy name - Internet...
2014/03/17 10:20:58 AM	Warning	REMOTE_SITE_A	QoS	Class dropped rate	Interface name - GigabitEthernet0; Interface direction - OUTPUT; Policy name - RIS_Sh...
2014/03/17 10:21:02 AM	Warning	REMOTE_SITE_A	Flow	High media packet loss percentage	High media packet loss percentage - 33.01 %
2014/03/17 10:21:13 AM	Warning	DATA_CENTER	Flow	High media packet loss percentage	High media packet loss percentage - 36.16 %
2014/03/17 10:21:38 AM	Warning	REMOTE_SITE_A	QoS	Class dropped rate	Interface name - GigabitEthernet0; Interface direction - OUTPUT; Policy name - QUEUING...
2014/03/17 10:21:48 AM	Warning	REMOTE_SITE_A	QoS	Class dropped rate	CLEARED: Interface name - GigabitEthernet0; Interface direction - OUTPUT; Policy name - QUEUING...
2014/03/17 10:21:58 AM	Warning	REMOTE_SITE_A	QoS	Class dropped rate	Interface name - GigabitEthernet0; Interface direction - OUTPUT; Policy name - QUEUING...
2014/03/17 10:22:15 AM	Warning	REMOTE_SITE_A	QoS	Class-default dropped rate	CLEARED: Interface name - FastEthernet0; Interface direction - OUTPUT; Policy name - QUEUING...
2014/03/17 10:22:15 AM	Warning	REMOTE_SITE_A	QoS	Class-default dropped rate	CLEARED: Interface name - FastEthernet0; Interface direction - OUTPUT; Policy name - QUEUING...
2014/03/17 10:23:22 AM	Warning	REMOTE_SITE_A	Device Conf...	Device configuration changed	Username - admin; Commands - config t; policy-map QUEUING; class VIDEO; no police 11...
2014/03/17 10:23:28 AM	Warning	REMOTE_SITE_A	QoS	Class-default dropped rate	Interface name - FastEthernet0; Interface direction - OUTPUT; Policy name - Internet...
2014/03/17 10:23:35 AM	Warning	REMOTE_SITE_B	Device Conf...	Running config may have changed since startup confi...	
2014/03/17 10:23:38 AM	Warning	REMOTE_SITE_A	QoS	Class dropped rate	CLEARED: Interface name - GigabitEthernet0; Interface direction - OUTPUT; Policy nam...
2014/03/17 10:23:38 AM	Warning	REMOTE_SITE_A	QoS	Class-default dropped rate	CLEARED: Interface name - FastEthernet0; Interface direction - OUTPUT; Policy name ...
2014/03/17 10:23:38 AM	Warning	REMOTE_SITE_A	QoS	Class dropped rate	CLEARED: Interface name - FastEthernet0; Interface direction - OUTPUT; Policy name ...
2014/03/17 10:25:36 AM	Warning	REMOTE_SITE_A	Device Conf...	Device configuration changed	Username - admin; Commands - config t; policy-map QUEUING; class VIDEO; police 1000...
2014/03/17 10:25:48 AM	Warning	REMOTE_SITE_A	Device Conf...	Running config may have changed since startup confi...	
2014/03/17 10:25:58 AM	Warning	REMOTE_SITE_A	QoS	Class dropped rate	Interface name - GigabitEthernet0; Interface direction - OUTPUT; Policy name - QUEUING...
2014/03/17 10:25:58 AM	Warning	REMOTE_SITE_A	QoS	Class dropped rate	Interface name - FastEthernet0; Interface direction - OUTPUT; Policy name - QUEUING...
2014/03/17 10:26:14 AM	Warning	DATA_CENTER	Flow	High media packet loss percentage	High media packet loss percentage - 30.46 %
2014/03/17 10:26:32 AM	Warning	REMOTE_SITE_A	Flow	High media packet loss percentage	High media packet loss percentage - 56.62 %
2014/03/17 10:28:35 AM	Warning	REMOTE_SITE_B	Device Conf...	Running config may have changed since startup confi...	
2014/03/17 10:30:58 AM	Warning	REMOTE_SITE_A	Device Conf...	Running config may have changed since startup confi...	
2014/03/17 10:30:58 AM	Warning	REMOTE_SITE_A	QoS	Class dropped rate	Interface name - GigabitEthernet0; Interface direction - OUTPUT; Policy name - QUEUING...

Medianet

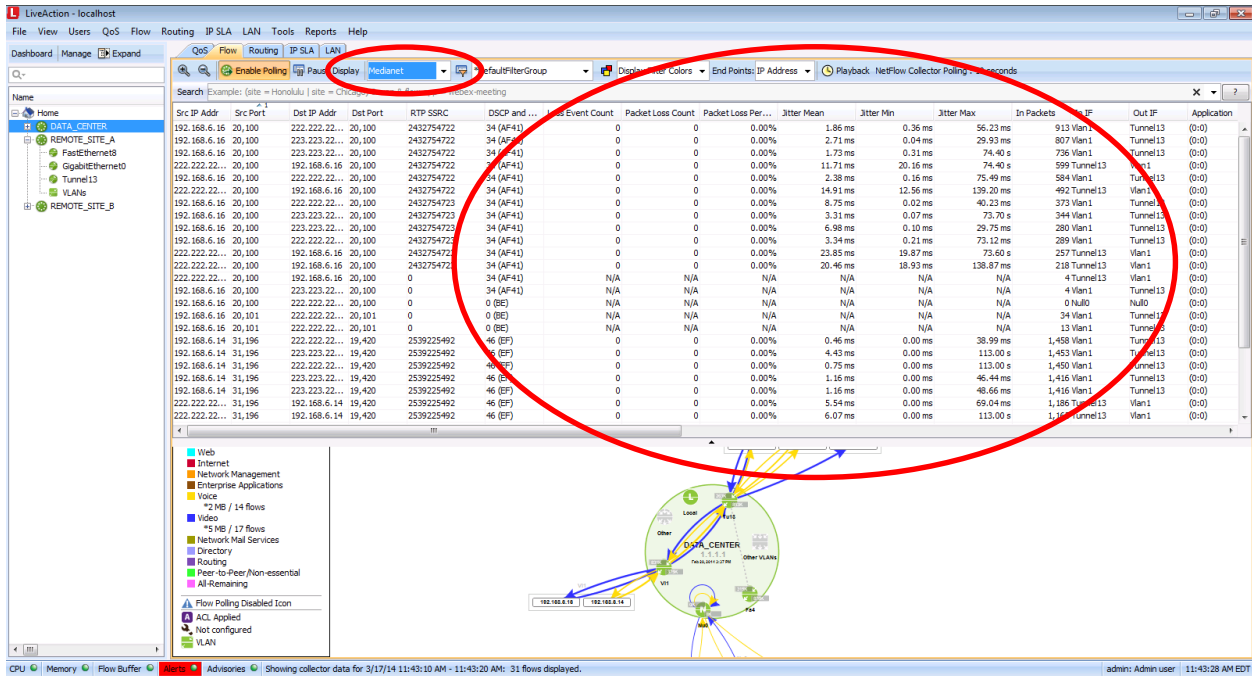
LiveAction is a NetFlow collector. It can collect the Cisco Medianet Performance Monitor flow type. This is a specific NetFlow version 9 flexible template that includes VoIP and video application performance metrics. LiveAction can also generate the appropriate Medianet NetFlow configuration for many device types. This allows for the easy enablement

of this advanced technology in a point-and-click fashion. This document will highlight how Medianet flows can be used to validate the application performance of VoIP and video in a DMVPN network environment.

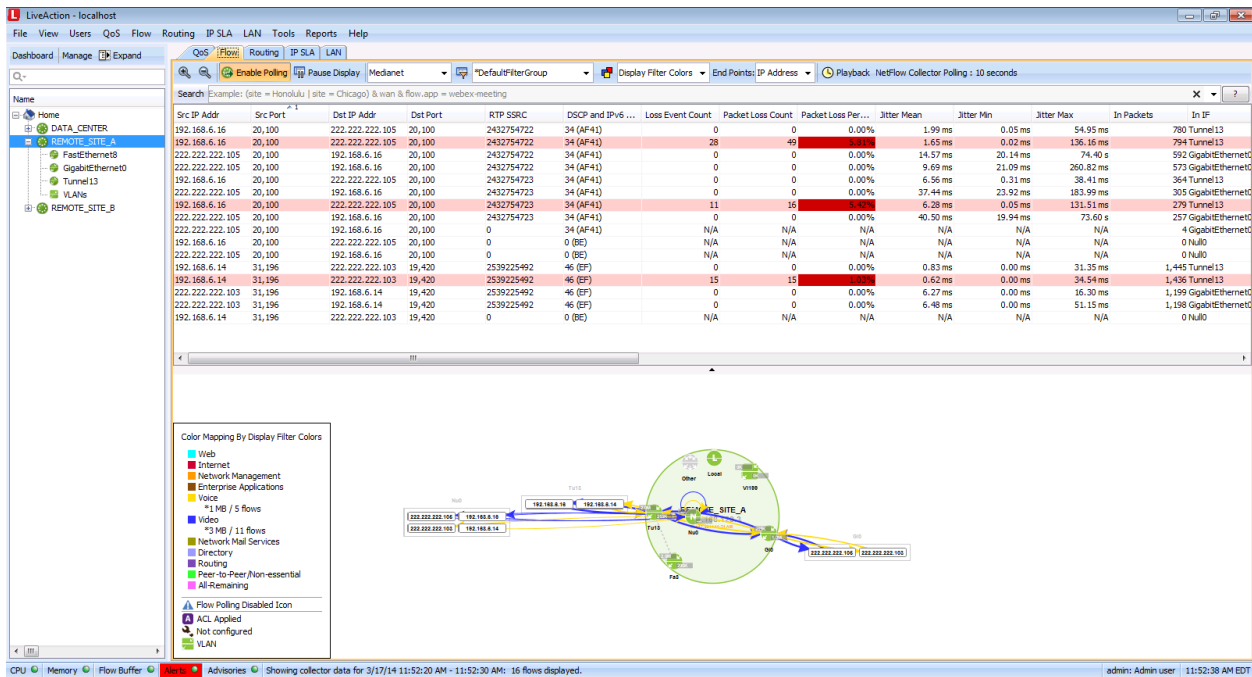
Below is a LiveAction topology diagram of a DMVPN network. This screenshot is showing Medianet flows (VoIP and video) across the DMVPN network. Notice the Flow Type pull-down is set to Medianet. In this example, all three monitored devices are exploring the Medianet flow type to LiveAction.



Real-time Medianet flows can be viewed in detail by double-clicking on a network device and selecting Medianet from the Flow Type pull-down. Both packet loss and jitter measurements of the RTP calls passing through this device will be shown. Below is a LiveAction screenshot of real-time Medianet flows:



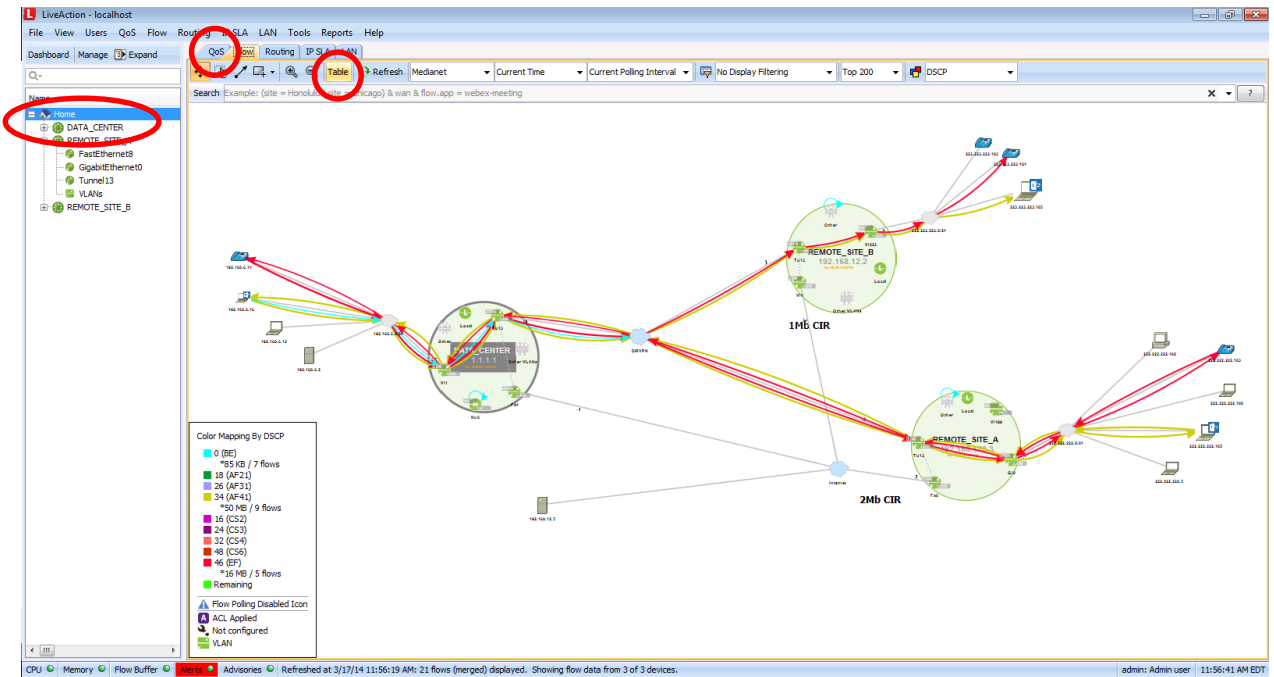
Below is a second real-time screenshot of Medianet flows. Notice the cells in red in the Packet Loss Percentage column. This indicates a configurable threshold was exceeded in LiveAction and the statistics received in the Medianet flow is triggering an alert for the bad performance of a VoIP/video call.



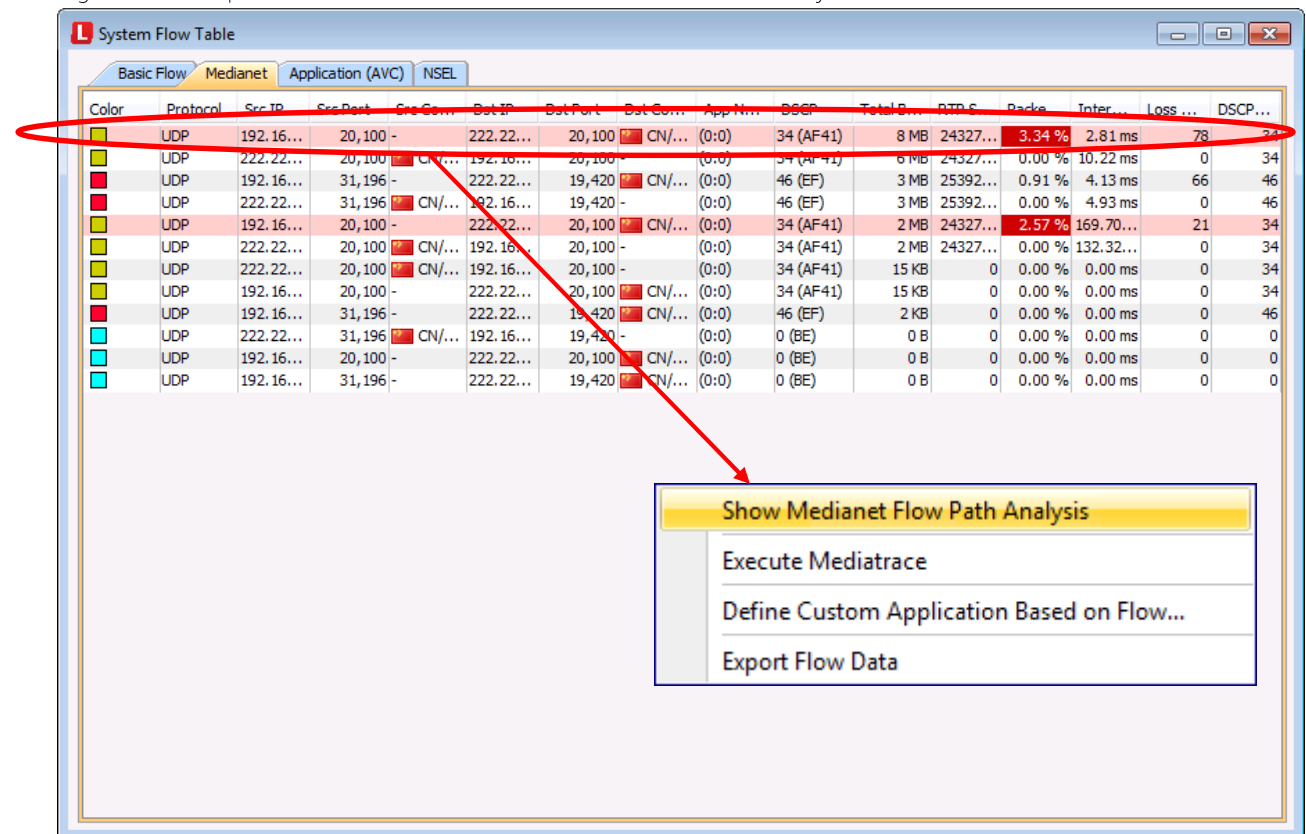
Medianet Flow Path Analysis

LiveAction can also visually paint an end-to-end picture of how VoIP/video call performance across a network. It will also correlate device, interface and QoS statistics with the performance of the VoIP/video call. To see this end-to-end flow performance, perform the following:

1. Click on the Home icon, Flow tab, and click the Table icon.



2. The System Flow Table window will appear. Select the Medianet tab. This will show a list of VoIP/video (RTP) calls being collected in the environment. The calls in red are highlighting problems.
3. Right-click on a problem flow and select Show Medianet Flow Path Analysis.



- This will execute a Medianet Flow Path Analysis. It will show the router or switches' performance that the call was passing through, the input and output interfaces at each hop, the input and output QoS policies at each hop, and the call's Medianet statistics. The example below is showing packet loss on the 2nd device in the calls path. Click on the Show Path button to visually see the performance of the call end-to-end.

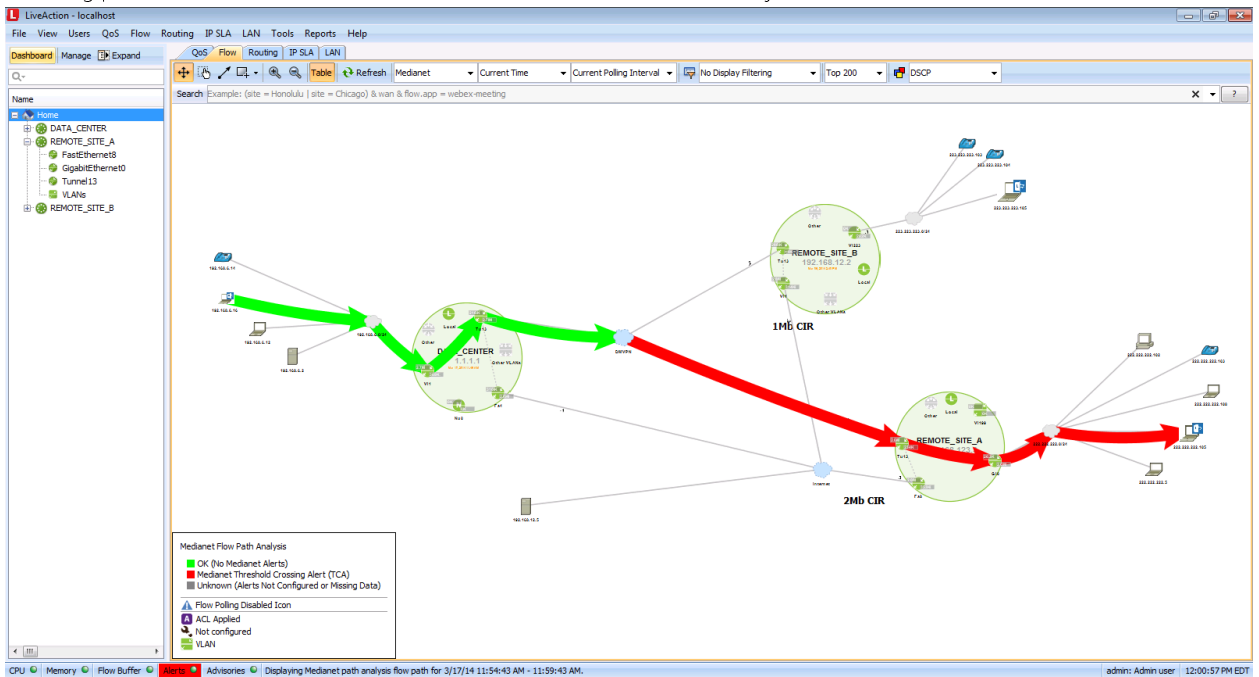
Medianet Flow Path Analysis

Flow: UDP 192.168.6.16:20100 -> 222.222.222.105:20100 SSRC: 2432754722 3/17/14 11:54:43 AM - 11:59:43 AM Refresh Show Path

	DATA_CENTER	REMOTE_SITE_A
Device Name	DATA_CENTER	REMOTE_SITE_A
CPU Usage +	24 - 25 %	13 %
In IF +	Vlan1	Tunnel13
Out IF +	Tunnel13	GigabitEthernet0
In QoS Policy +	SET_DSCP	No Policy
Out QoS Policy +	No Policy	No Policy
Jitter Mean	0.86 - 2.53 ms	1.03 - 2.59 ms
Packet Loss Count	0	28 - 101
Packet Expected Count	561 - 924	663 - 925
Packet Loss % *	0.00 %	4.03 - 10.91 %
Loss Event Count	0	15 - 47
Forwarding Status	Forwarded	Forwarded
Media Bit Rate	15 Kbps - 26 Kbps	16 Kbps - 23 Kbps
IP Bit Rate	16 Kbps - 27 Kbps	17 Kbps - 24 Kbps
DSCP and IPv6 Traffic Class	AF41 (34)	AF41 (34)
Last Media Event	Normal	Normal

+ QoS Alert Enabled Threshold Crossing Alert (TCA) Interface/QoS Policy Drops

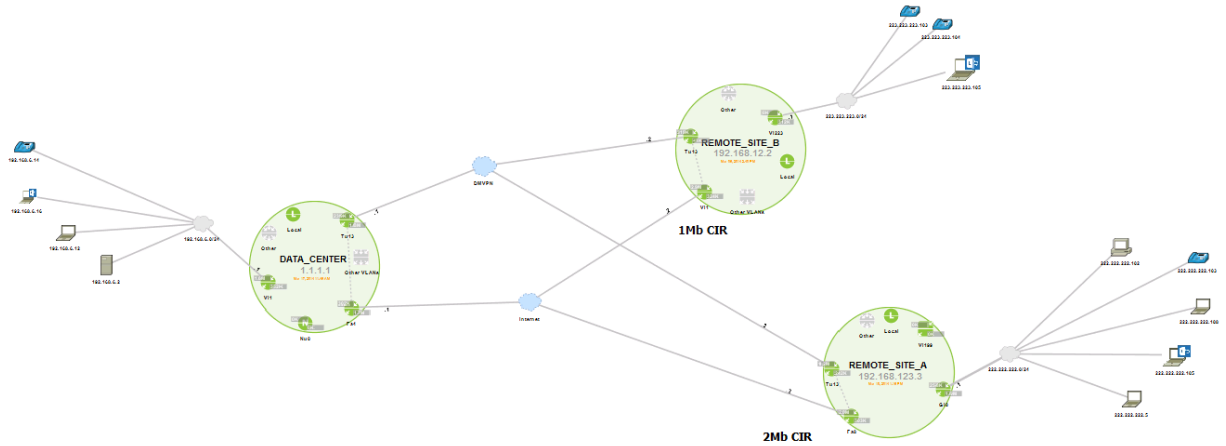
- Below is an end-to-end visual view of the Medianet Flow Path Analysis. The device on the right is visually showing problems with the VOIP or video call on the DMVPN network by its red color.



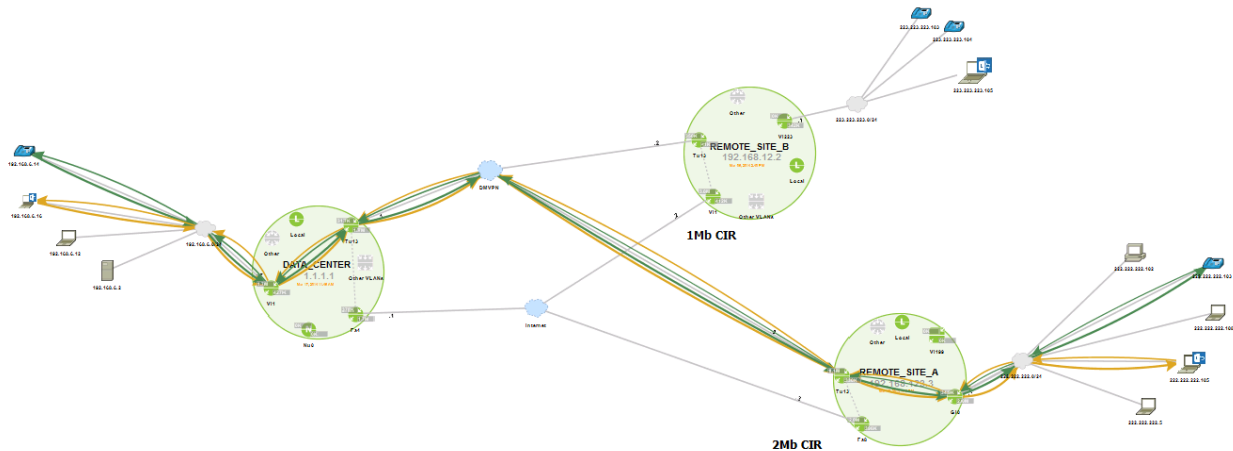
Appendix A. – DMVPN Putting It All Together.

In the following pages, the concepts outlined in this document will be combined to tell the complete DMVPN QoS story for a sample network. Consider the following network diagram.

- This shows a small DMVPN network comprised of three sites: DATA_CENTER, REMOTE_SITE_B, and REMOTE_SITE_A.
- Each site is connected to the Internet with a 100Mb hand-off.
- REMOTE_SITE_B's Internet circuit has a 1Mb CIR.
- REMOTE_SITE_A's Internet circuit has a 2Mb CIR.



Below is a second diagram of this network, but in this example, end-to-end flow visualization (based on NetFlow data) is shown across the network diagram representing VoIP and video applications on the DMVPN tunnel between the DATA_CENTER and REMOTE_SITE_A. Assume that no QoS is configured at any site and only this one VoIP/video call is traversing the network (no other data, VoIP, video or Internet traffic).



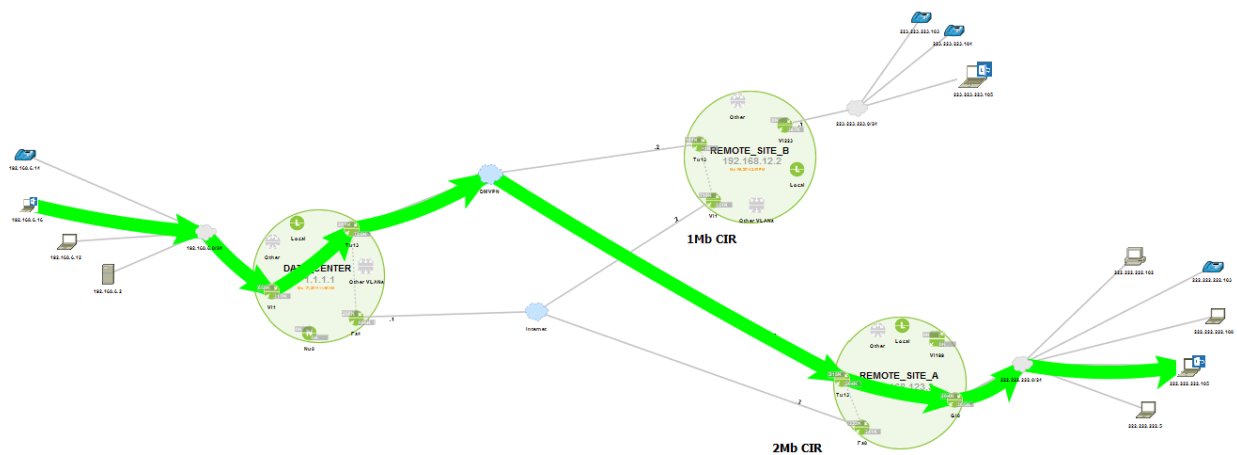
In this scenario, if a Medianet Flow Path Analysis was executed in LiveAction on VoIP call from the DATA_CENTER to REMOTE_SITE_A, the network would show the following hop-by-hop view for a VoIP or video call.

Medianet Flow Path Analysis

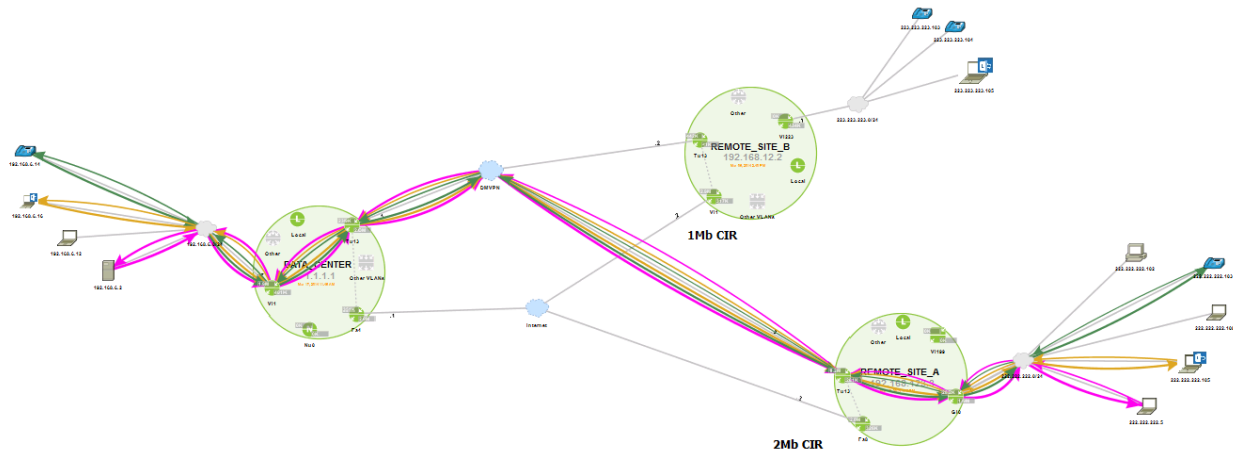
Flow: UDP 192.168.6.14:31196 -> 222.222.222.103:19420 SSRC: 2539225492 3/18/14 4:44:18 PM - 4:49:18 PM Refresh Show Path

	DATA_CENTER	REMOTE_SITE_A
Device Name	DATA_CENTER	REMOTE_SITE_A
CPU Usage +	20 %	9 %
In IF +	Vlan1	Tunnel13
Out IF +	Tunnel13	GigabitEthernet0
In QoS Policy +	No Policy	No Policy
Out QoS Policy +	No Policy	No Policy
Jitter Mean	0.67 - 3.59 ms	0.68 - 1.18 ms
Packet Loss Count	0	0
Packet Expected Count	1,438 - 1,450	1,432 - 1,453
Packet Loss % *	0.00 %	0.00 %
Loss Event Count	0	0
Forwarding Status	Forwarded	Forwarded
Media Bit Rate	8 Kbps - 8 Kbps	8 Kbps - 8 Kbps
IP Bit Rate	10 Kbps - 10 Kbps	10 Kbps - 10 Kbps
DSCP and IPv6 Traffic Class	EF (46)	EF (46)
Last Media Event	Normal	Normal

+ QoS Alert Enabled Threshold Crossing Alert (TCA) Interface/QoS Policy Drops



The quality of the VoIP call would be good; with no packet loss and very low jitter. But this is not how networks operate. VoIP and video must compete with data applications and Internet traffic for bandwidth. In this scenario, all applications are competing with the end-to-end logical throughput, the 2Mb CIR being enforced by the Internet Provider at REMOTE_SITE_A. Consider the next screenshot. This diagram shows VOIP, video and internal data passing between the DATA_CENTER and REMOTE_SITE_A inside the DMVPN tunnel. There is still no Internet traffic shown in this example. Assume that a lot of data is TCP and is being downloaded from the DATA_CENTER, by REMOTE_SITE_A. So much bandwidth is being consumed by the TCP data application in the DMVPN that the 2Mb CIR of the service provider becomes congested and the provider starts dropping data.



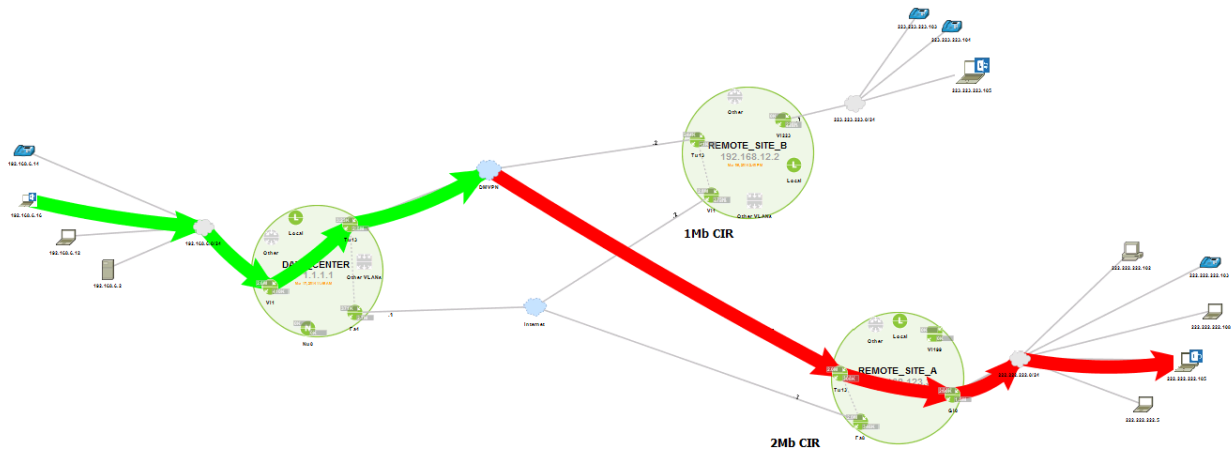
If QoS is not configured, Medianet Flow Path Analysis will show the following hop-by-hop analysis with packet loss marked in red in the table and visually across the topology:

Medianet Flow Path Analysis

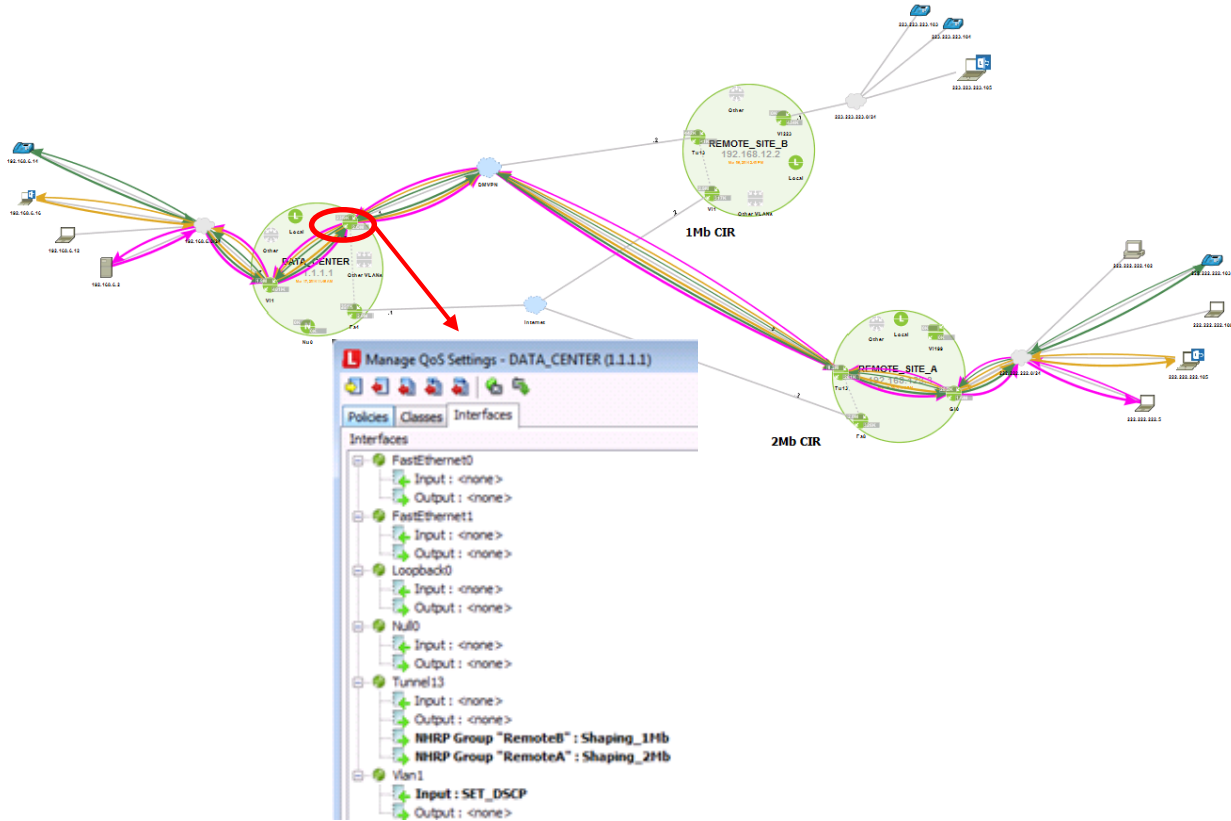
Flow: UDP 192.168.6.14:31196 -> 222.222.222.103:19420 SSRC: 2539225492 3/18/14 5:06:45 PM - 5:11:45 PM Refresh Show Path

	DATA_CENTER	REMOTE_SITE_A
Device Name	DATA_CENTER	REMOTE_SITE_A
CPU Usage +	25 - 27 %	13 - 14 %
In IF +	Vlan1	Tunnel13
Out IF +	Tunnel13	GigabitEthernet0
In QoS Policy +	No Policy	No Policy
Out QoS Policy +	No Policy	No Policy
Jitter Mean	0.55 - 88.69 ms	0.49 - 2.05 ms
Packet Loss Count	0	12 - 21
Packet Expected Count	1,413 - 1,458	1,403 - 1,458
Packet Loss % *	0.00 %	0.83 - 1.47 %
Loss Event Count	0	12 - 21
Forwarding Status	Forwarded	Forwarded
Media Bit Rate	8 Kbps - 8 Kbps	8 Kbps - 8 Kbps
IP Bit Rate	9 Kbps - 10 Kbps	9 Kbps - 10 Kbps
DSCP and IPv6 Traffic Class	EF (46)	EF (46)
Last Media Event	Normal	Normal

* Medianet Alert Enabled + QoS Alert Enabled ■ OK (No Medianet Alerts) ■ Threshold Crossing Alert (TCA) ■ Interface/QoS Policy Drops ■ Unknown



But, if the appropriate Per-Tunnel QoS policy was configured on the DATA_CENTER, this issue could be fixed. In this example this would be a hierarchical QoS policy with a 2Mb shaping parent policy and a child queuing policy. The traffic sent in the DMVPN tunnel to REMOTE_SITE_A would adhere to the remote device's service provider CIR, and VoIP and video would be protected inside the DMVPN tunnel.



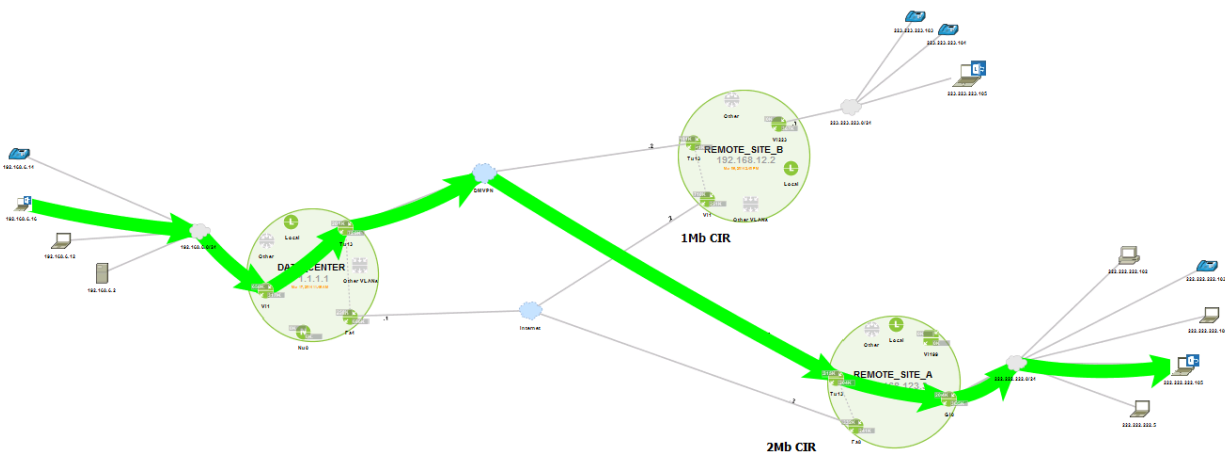
Medianet Flow Path Analysis visually confirms the Per-Tunnel QoS policy is working and that VoIP and video calls are performing well again.

Medianet Flow Path Analysis

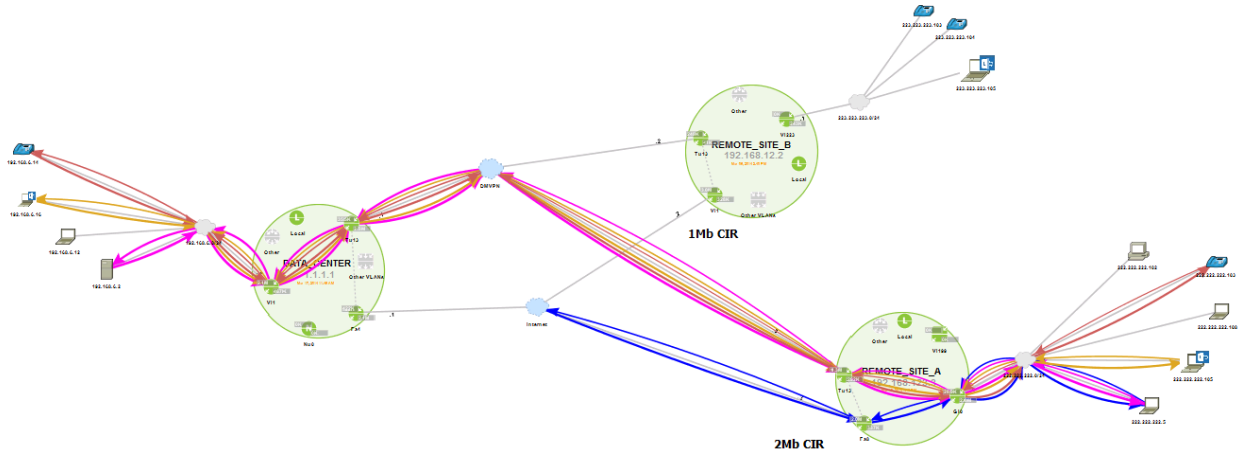
Flow: UDP 192.168.6.14:31196 -> 222.222.222.103:19420 SSRC: 2539225492 3/18/14 7:27:29 PM - 7:32:29 PM Refresh Show Path

	DATA_CENTER	REMOTE_SITE_A
Device Name	DATA_CENTER	REMOTE_SITE_A
CPU Usage +	20 - 24 %	9 - 10 %
In IF +	Vlan1	Tunnel13
Out IF +	Tunnel13	GigabitEthernet0
In QoS Policy +	SET_DSCP	No Policy
Out QoS Policy +	No Policy	No Policy
Jitter Mean	0.57 - 2.61 ms	0.62 - 1.05 ms
Packet Loss Count	0	0 - 9
Packet Expected Count	1,426 - 1,455	1,432 - 1,454
Packet Loss % *	0.00 %	0.00 - 0.62 %
Loss Event Count	0	0 - 9
Forwarding Status	Forwarded	Forwarded
Media Bit Rate	8 Kbps - 8 Kbps	8 Kbps - 8 Kbps
IP Bit Rate	10 Kbps - 10 Kbps	10 Kbps - 10 Kbps
DSCP and IPv6 Traffic Class	EF (46)	EF (46)
Last Media Event	Normal	Normal

+ QoS Alert Enabled ■ Threshold Crossing Alert (TCA) ■ Interface/QoS Policy Drops



The next screenshot shows an even more complete picture of what one would expect to see in a real network; VoIP, video and data going through the DMVPN tunnel and casual Internet traffic all competing for the same 2Mb CIR Internet circuit at REMOTE_SITE_A. Assume the casual Internet traffic is TCP and is consuming as much bandwidth as possible just like as the DMVPN data application.



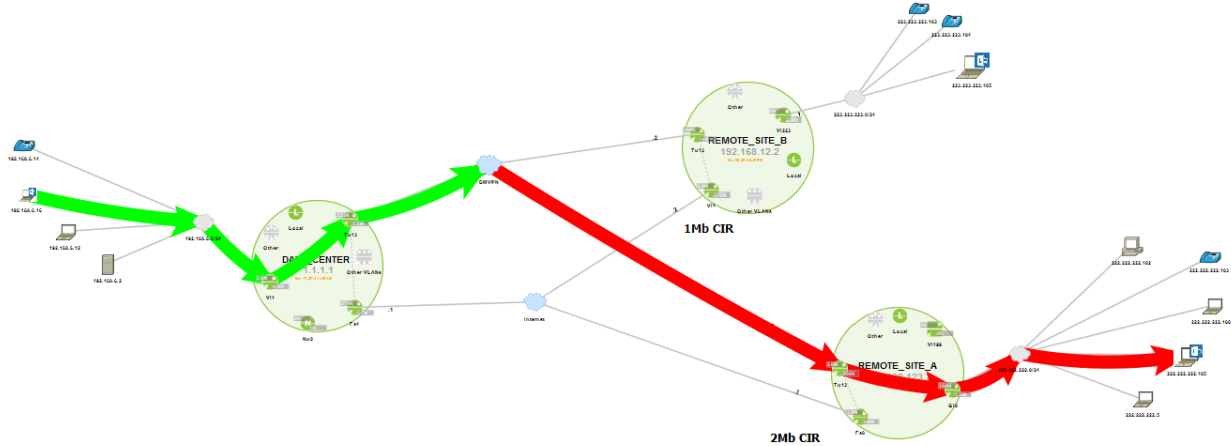
Again, Medianet Flow Path Analysis visually show the VoIP call performance issues at REMOTE_SITE_A via the red color below.

Medianet Flow Path Analysis

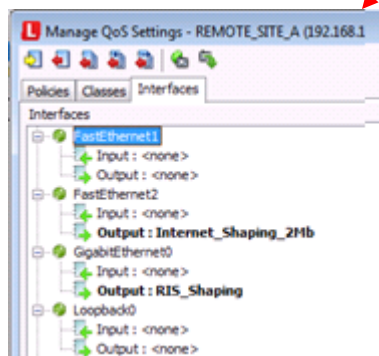
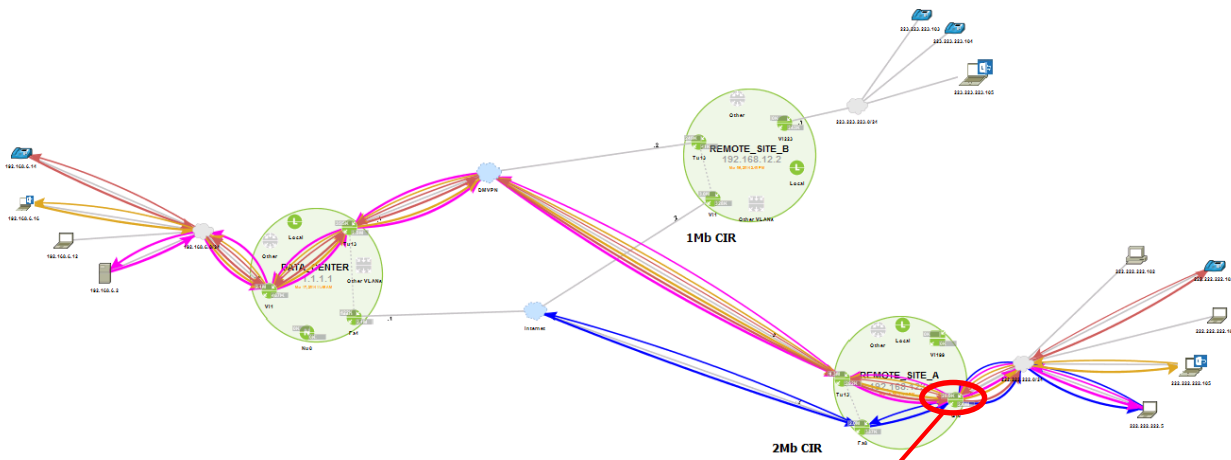
Flow: UDP 192.168.6.14:31196 -> 222.222.222.103:19420 SSRC: 2539225492 3/18/14 7:46:56 PM - 7:51:56 PM Refresh Show Path

	DATA_CENTER	REMOTE_SITE_A
Device Name	DATA_CENTER	REMOTE_SITE_A
CPU Usage +	25 - 29 %	12 - 15 %
In IF +	Vlan1	Tunnel13
Out IF +	Tunnel13	GigabitEthernet0
In QoS Policy +	SET_DSCP	No Policy
Out QoS Policy +	No Policy	No Policy
Jitter Mean	0.51 - 2.84 ms	0.52 - 4.28 ms
Packet Loss Count	0	0 - 24
Packet Expected Count	1,320 - 1,441	1,345 - 1,442
Packet Loss % *	0.00 %	0.00 - 1.76 %
Loss Event Count	0	0 - 24
Forwarding Status	Forwarded	Forwarded
Media Bit Rate	8 Kbps - 8 Kbps	8 Kbps - 8 Kbps
IP Bit Rate	9 Kbps - 10 Kbps	9 Kbps - 10 Kbps
DSCP and IPv6 Traffic Class	EF (46)	EF (46)
Last Media Event	Normal	Normal

+ QoS Alert Enabled ■ Threshold Crossing Alert (TCA) ■ Interface/QoS Policy Drops



But, if the appropriate RIS QoS policy was configured on the REMOTE_SITE_A, inbound TCP based Internet traffic could be throttled. In this example this would be a hierarchical QoS policy with a 1.9Mb shaping parent policy (95% of 2Mb CIR) and a child queuing policy. The traffic sent in the DMVPN tunnel to REMOTE_SITE_A would still be protected as it entered the tunnel and the tunnel would be protected from the casual inbound TCP Internet traffic.



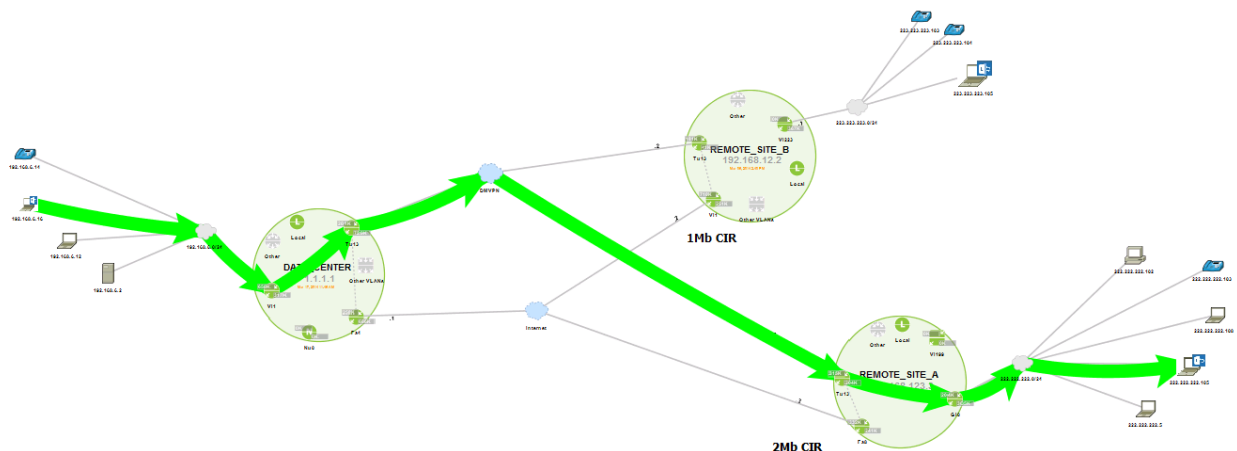
Medianet Flow Path Analysis visually confirms the RIS QoS policy applied to the egress of the LAN interface is working and that VoIP and Video calls are performing well again.

Medianet Flow Path Analysis

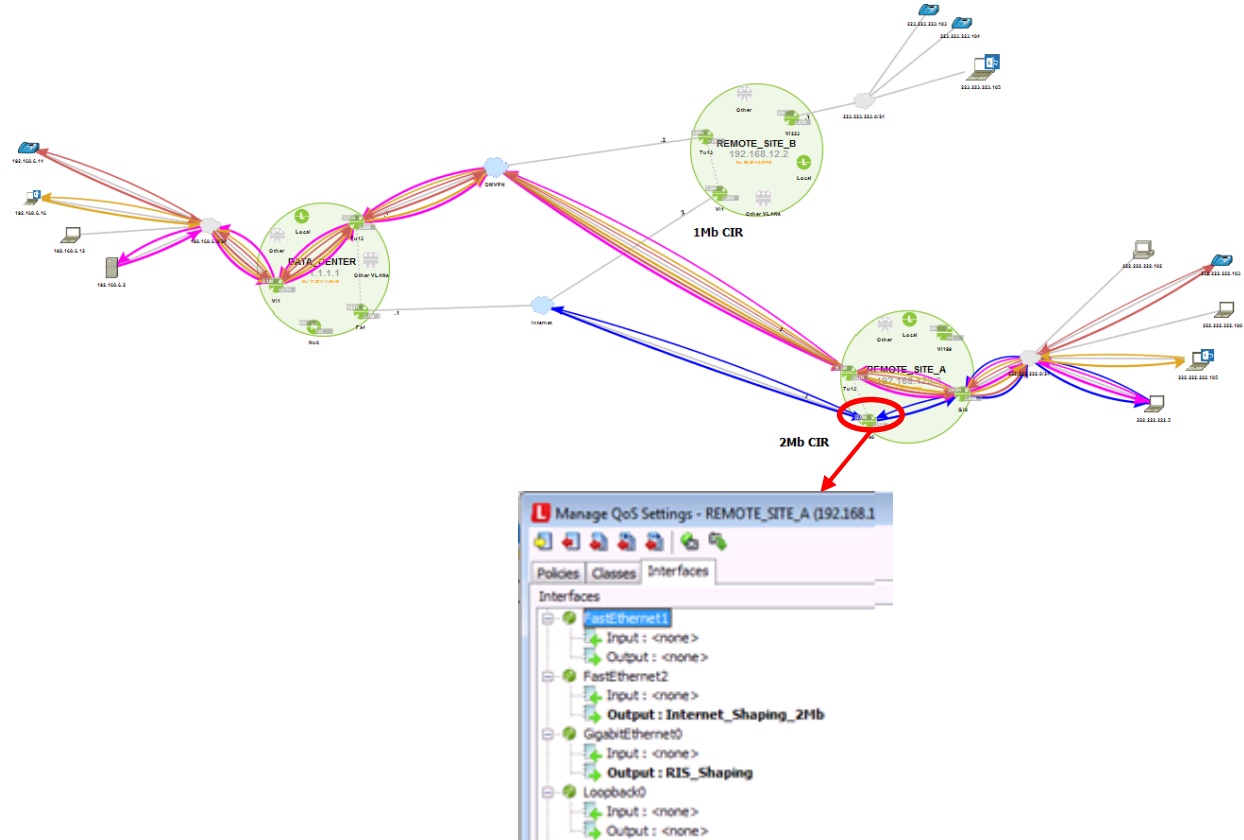
Flow: UDP 192.168.6.14:31196 -> 222.222.222.103:19420 SSRC: 2539225492 3/18/14 8:18:12 PM - 8:23:12 PM Refresh Show Path

	DATA_CENTER	REMOTE_SITE_A
Device Name	DATA_CENTER	REMOTE_SITE_A
CPU Usage +	23 - 24 %	13 - 19 %
In IF +	Vlan1	Tunnel13
Out IF +	Tunnel13	GigabitEthernet0
In QoS Policy +	SET_DSCP	No Policy
Out QoS Policy +	No Policy	RIS_Shaping
Jitter Mean	0.43 - 1.60 ms	0.44 - 1.13 ms
Packet Loss Count	0	0 - 14
Packet Expected Count	1,384 - 1,455	1,390 - 1,452
Packet Loss % *	0.00 %	0.00 - 0.97 %
Loss Event Count	0	0 - 14
Forwarding Status	Forwarded	Forwarded
Media Bit Rate	8 Kbps - 8 Kbps	8 Kbps - 8 Kbps
IP Bit Rate	9 Kbps - 10 Kbps	9 Kbps - 10 Kbps
DSCP and IPv6 Traffic Class	EF (46)	EF (46)
Last Media Event	Normal	Normal

* Medianet Alert Enabled + QoS Alert Enabled ■ OK (No Medianet Alerts) ■ Threshold Crossing Alert (TCA) ■ Interface/QoS Policy Drops ■ Unknown



What about WAN QoS for the REMOTE_SITE_A? Yes, it will need a hierarchical QoS policy. Its parent policy will shape at 2Mb and its child policy will queue VoIP, video and high priority DMVPN data.

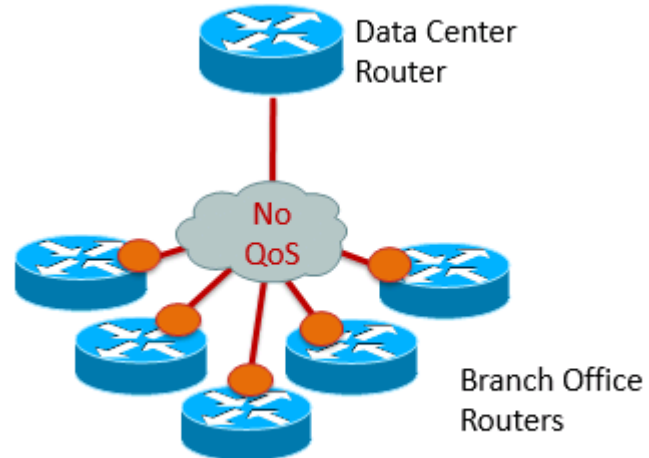


What about a RIS policy at the DATA_CENTER? Depending on the traffic patterns at the DATA_CENTER device, a RIS policy may also be needed. If required, the DATA_CENTER's RIS policy would have a parent policy shaper configured to 95Mb (95% of 100Mb) and a child queuing policy.

Appendix B. – Sample DMVPN Branch Office QoS Configuration with RIS

Branch Office Per-Tunnel QoS DMVPN Configuration

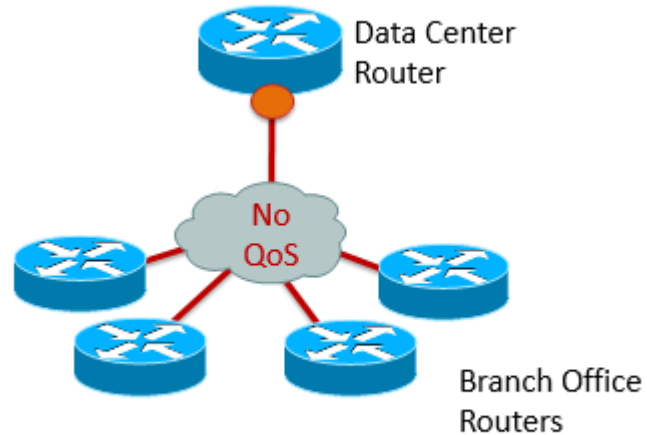
```
policy-map QUEUEING
class VOIP
  priority percent 20
class VIDEO
  bandwidth percent 30
class MGMT_DATA
  bandwidth percent 5
class CALL_SIGNALING
  bandwidth percent 5
class CRITICAL_DATA
  bandwidth percent 10
class class-default
  fair-queue
!
policy-map Internet_Shaping_2Mb
class class-default
  shape average 2000000 20000 0
  service-policy QUEUEING
!
policy-map RIS_2Mb
class class-default
  shape average 1900000 19000 0
  service-policy QUEUEING
!
interface Tunnel1
description MULTI-POINT GRE TUNNEL
ip nhrp group MY_REMOTE_GROUP_A
tunnel mode gre multipoint
tunnel source GigabitEthernet0/0
!
interface GigabitEthernet0
description INTERNET
service-policy output Internet_Shaping_2Mb
!
interface GigabitEthernet1
description LAN
service-policy output RIS_2Mb
```



Appendix C. – Sample DMVPN Data Center Per-Tunnel QoS Configuration

Data Center Per-Tunnel QoS DMVPN Configuration

```
policy-map QUEUING
class VOIP
  priority percent 20
class VIDEO
  bandwidth percent 30
class MGMT_DATA
  bandwidth percent 5
class CALL_SIGNALING
  bandwidth percent 5
class CRITICAL_DATA
  bandwidth percent 10
class class-default
  fair-queue
!
policy-map Internet_Shaping_2Mb
class class-default
  shape average 2000000 20000 0
  service-policy QUEUING
!
policy-map Internet_Shaping_1Mb
class class-default
  shape average 1000000 10000 0
  service-policy QUEUING
!
interface Tunnel13
description MULTI-POINT GRE TUNNEL
ip nhrp map group GroupA service-policy output Internet_Shaping_2Mb
ip nhrp map group GroupB service-policy output Internet_Shaping_1Mb
!
```



For More Information

On the Web—www.liveaction.com/QoS

Go to our web site to find out more about Cisco QoS including best practices, the latest tools for monitoring and creating new policies, and a schedule for QoS webinars.

How to get more copies of this and future "hand-books" —www.liveaction.com/hand-books

Go to our web site if you want additional copies or printable PDF versions of this document.

Software Tools for Cisco QoS—www.liveaction.com

Visit our web site for free trial downloads of our LiveAction software for monitoring and configuring Cisco QoS. Be sure to check for periodic specials including free licenses on selected items.

About LiveAction

LiveAction is an application-aware network performance management and QoS control software incorporating QoS, NetFlow, Routing, IP SLA, and LAN functionality. LiveAction enhances understanding and control of the network by combining rich visualizations, application-level analysis and optimization, and expert rules-based configuration and editing.

Copyright © 2014 LiveAction. All rights reserved.. LiveAction is a trademark and LiveAction logo is a registered trademark of ActionPacked Research, Inc. in the US. All other trademarks mentioned in this document are the property of their respective owners.

LiveAction dba ActionPacked Research, Inc.
825 San Antonio Road, Suite 209
Palo Alto, CA 94303