Avaya Solution & Interoperability Test Lab

Application Notes for the Packeteer PacketShaper with Avaya SIP IP Telephony – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the Packeteer PacketShaper to guarantee WAN link bandwidth to SIP Voice over IP (VoIP) RTP traffic generated by Avaya SIP Telephones and Softphones, and give high priority to SIP VoIP signaling traffic generated by Avaya SIP Enablement Services (SES) servers, and Avaya SIP Telephones and Softphones. During compliance testing, SIP phone calls traversing the WAN link were successfully established and maintained while non-VoIP traffic such as HTTP and FTP traffic was sharing the WAN link. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a compliance-tested configuration comprised of Avaya SIP Enablement Services (SES), Avaya Communication Manager, Avaya SIP Telephones, Avaya SIP Softphones, and the Packeteer PacketShaper. PacketShaper is a traffic management appliance that monitors and controls IP network traffic going over WAN links. Typically placed between a site's WAN router and LAN, PacketShaper identifies and analyzes inbound and outbound WAN traffic up to and including the OSI Application Layer (Layer 7). In addition, PacketShaper manages WAN link utilization and throughput based on the bandwidth reservations and policies applied to the identified traffic classes. PacketShaper can thus ensure that SIP Voice over IP (VoIP) packets receive their guaranteed share of the WAN link capacity and do not encroach upon the guarantees provided to other traffic classes and applications sharing the WAN link.

Figure 1 illustrates a sample configuration consisting of an Avaya S8710 Media Server, an Avaya G650 Media Gateway, an Avaya SIP Enablement Services (SES) Server, Avaya SIP and H.323 IP Telephones, an Avaya SIP Softphone, and a Packeteer PacketShaper 6500 appliance. Avaya Communication Manager runs on the S8710 Media Server, though the solution described herein is also extensible to other Avaya Media Servers and Media Gateways. The Avaya C364T-PWR Converged Stackable Switch and Avaya P333T-PWR Stackable Switch perform Layer 2 switching within the enterprise site VLANs, and the Avaya C364T-PWR also routes packets between the enterprise site VLANs. The Cisco 2900 and 1841 routers route packets between the enterprise site and the simulated WAN.

In **Figure 1**, the SES server is configured as a combined home/edge SIP proxy and registrar server. The Avaya 4620SW SIP Telephone within the enterprise, as well as the 4610SW SIP Telephone and Avaya SIP Softphone in the WAN, register with the SES server. A T1 PPP link connects the enterprise site to a simulated WAN. The WAN SIP phones (4610SW SIP Telephone and Avaya SIP Softphone) exchange SIP signaling messages with the SES server over the T1 link. RTP packets between the WAN SIP phones and the enterprise also traverse the T1 link.

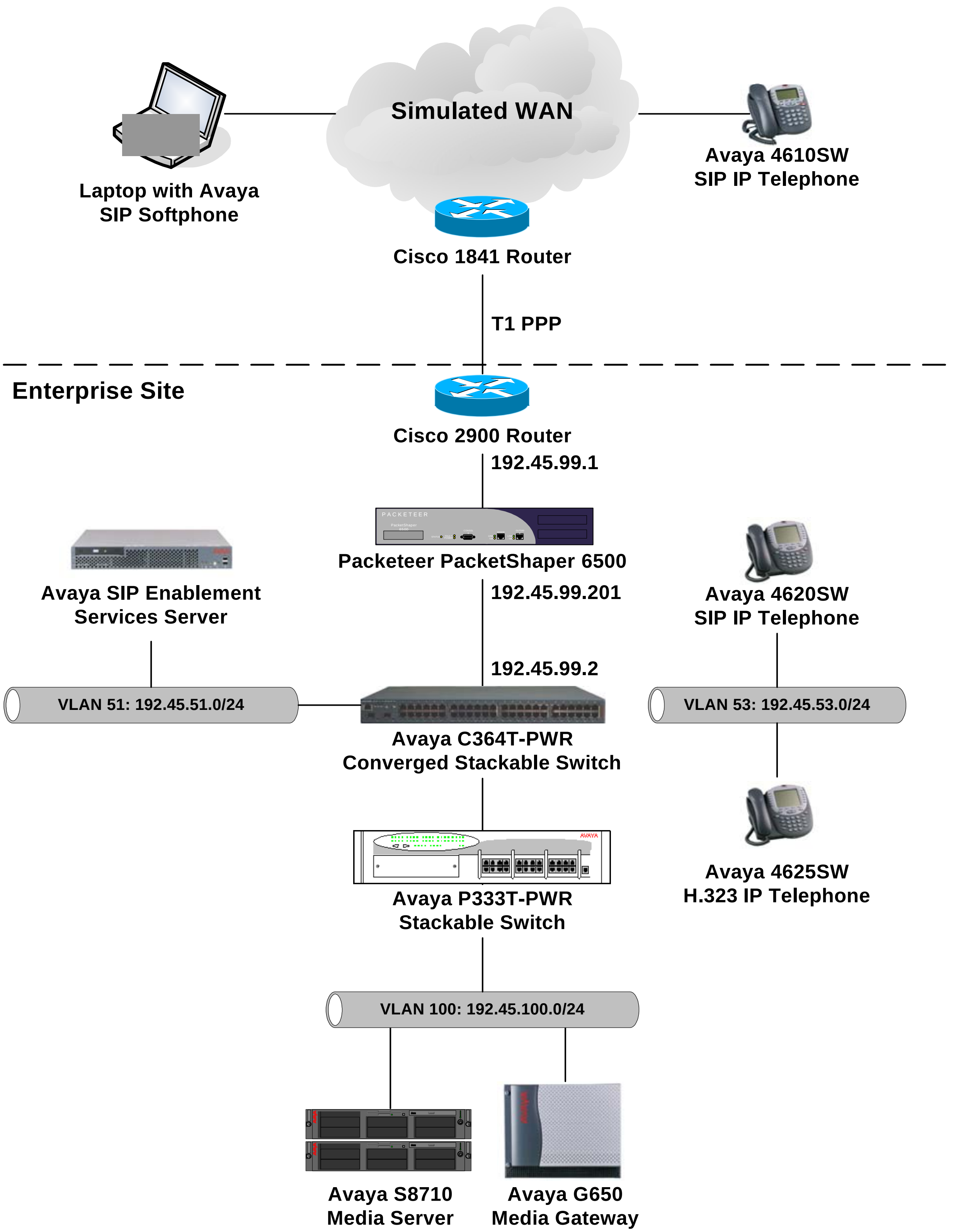


Figure 1: Sample configuration.

2. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

Equipment	Software/Firmware
Avaya S8710 Media Server	Avaya Communication Manager 3.0 (340.3)
Avaya G650 Media Gateway	-
TN2312BP IP Server Interface	21
TN799DP C-LAN Interface	15
TN2302AP IP Media Processor	104
Avaya SIP Enablement Services Server	SIP Enablement Services 3.0.0.0-031.0
Avaya 4600 Series IP Telephones	2.2 (4610SW SIP) 2.2 (4620SW SIP) 2.5 (4625SW H.323)
Avaya SIP Softphone	2.0 Build 43
Avaya C364T-PWR Converged Stackable Switch	4.5.14
Avaya P333T-PWR Stackable Switch	4.0.17
Packeteer PacketShaper 6500	7.2.1g1
Cisco 2900 Router	IOS 12.3
Cisco 1841 Router	IOS 12.3
Laptop	Windows XP Professional SP2

3. Configure Packeteer PacketShaper

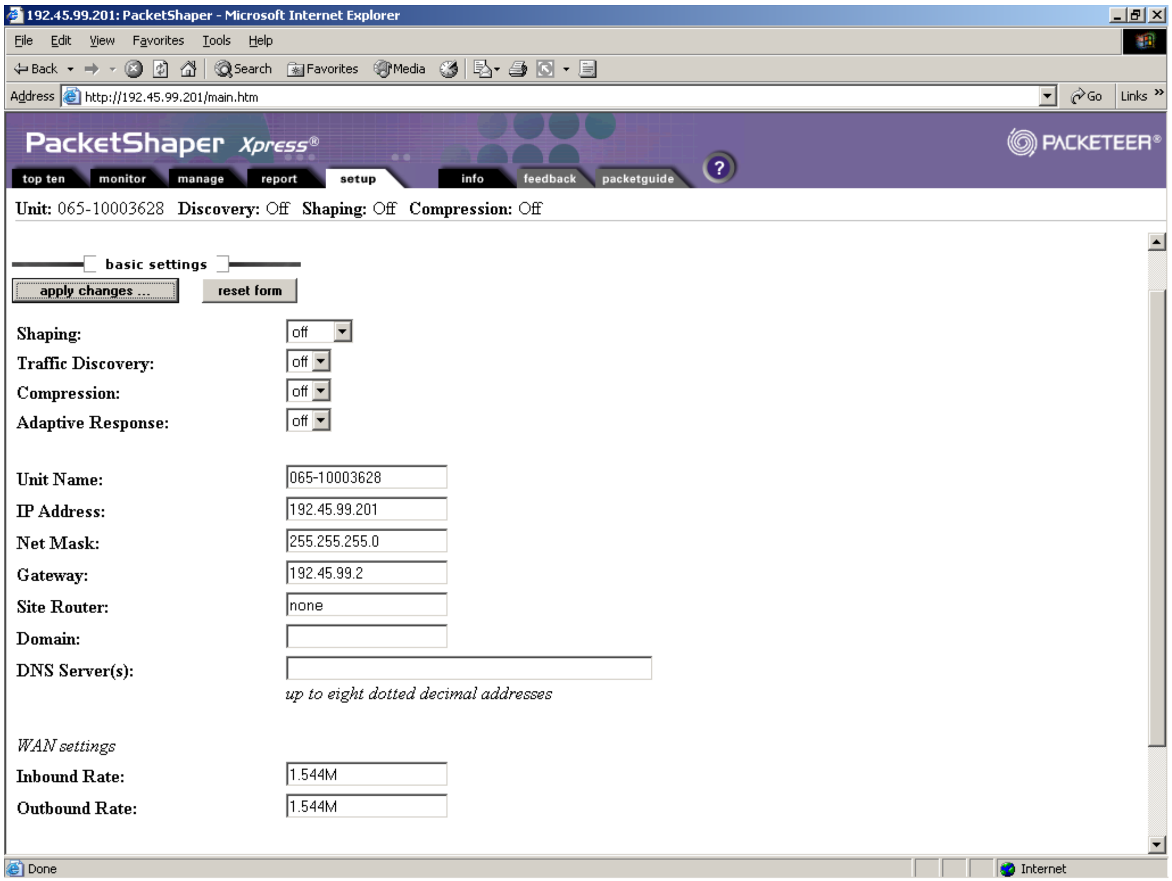
This section describes the steps for creating traffic classes for SIP VoIP protocols such as SIP, RTP, and RTCP, and configuring partitions and policies for those traffic classes on PacketShaper. The configuration is described in terms of inbound traffic, but is equally valid for outbound traffic. In fact, for the configuration of **Figure 1**, where the WAN link capacity (1.544 Mbps) is lower than the LAN capacity (10/100 Mbps), bandwidth management in the outbound direction towards the WAN is more critical than in the inbound direction towards the LAN.

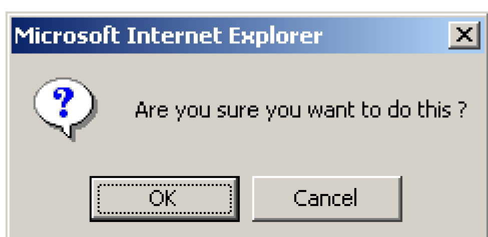
3.1. Create Inbound Traffic Classes

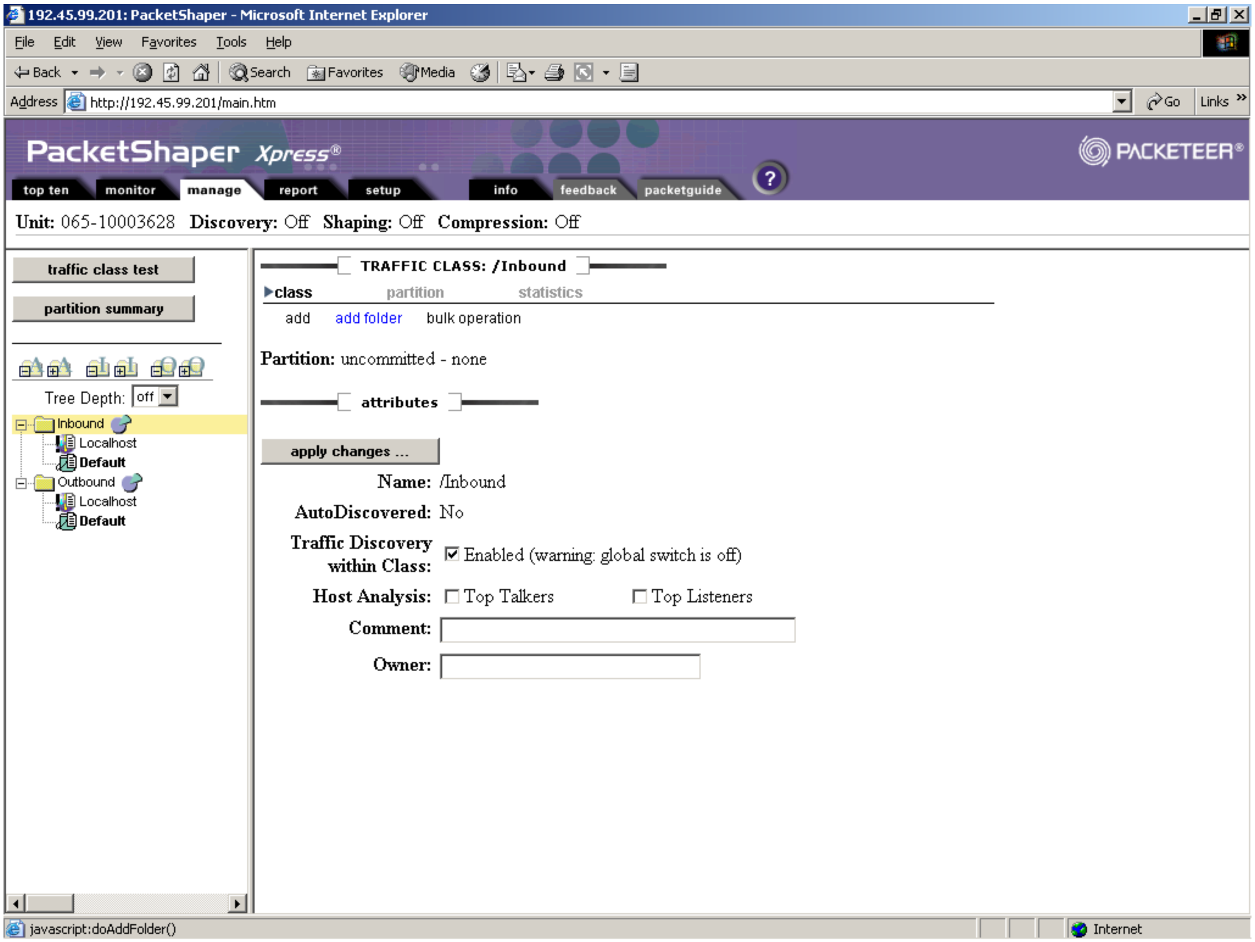
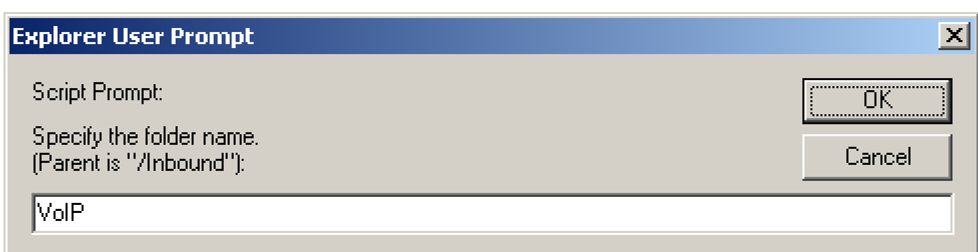
A traffic class identifies the traffic flows of specific IP addresses, protocols, or applications. Traffic classes may be either discovered or created. This section discusses the creation of traffic classes relevant to SIP VoIP.

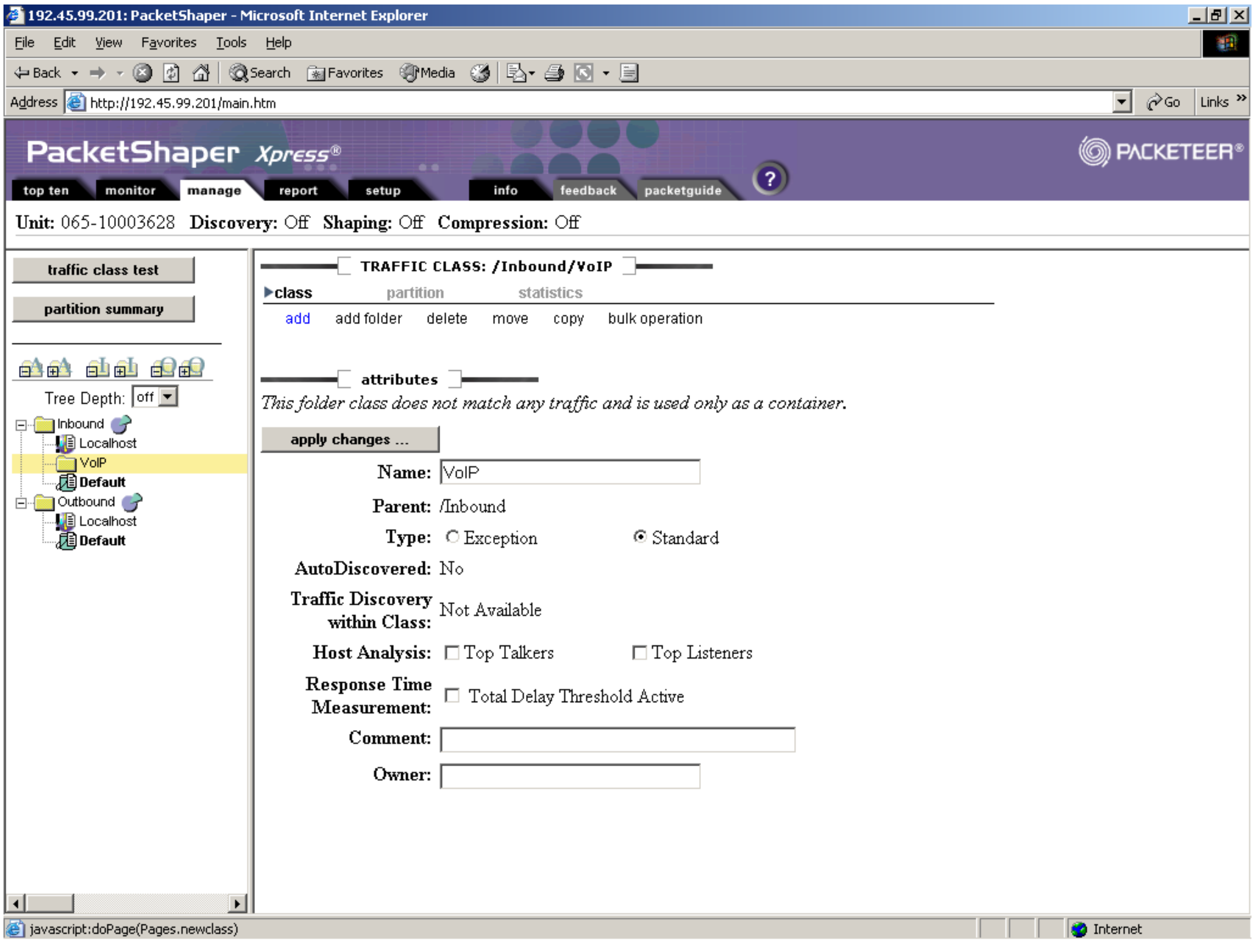
Step	Description
1.	Open a browser and enter http://<hostname or IP address of PacketShaper as the URL. Log in with the appropriate credentials.

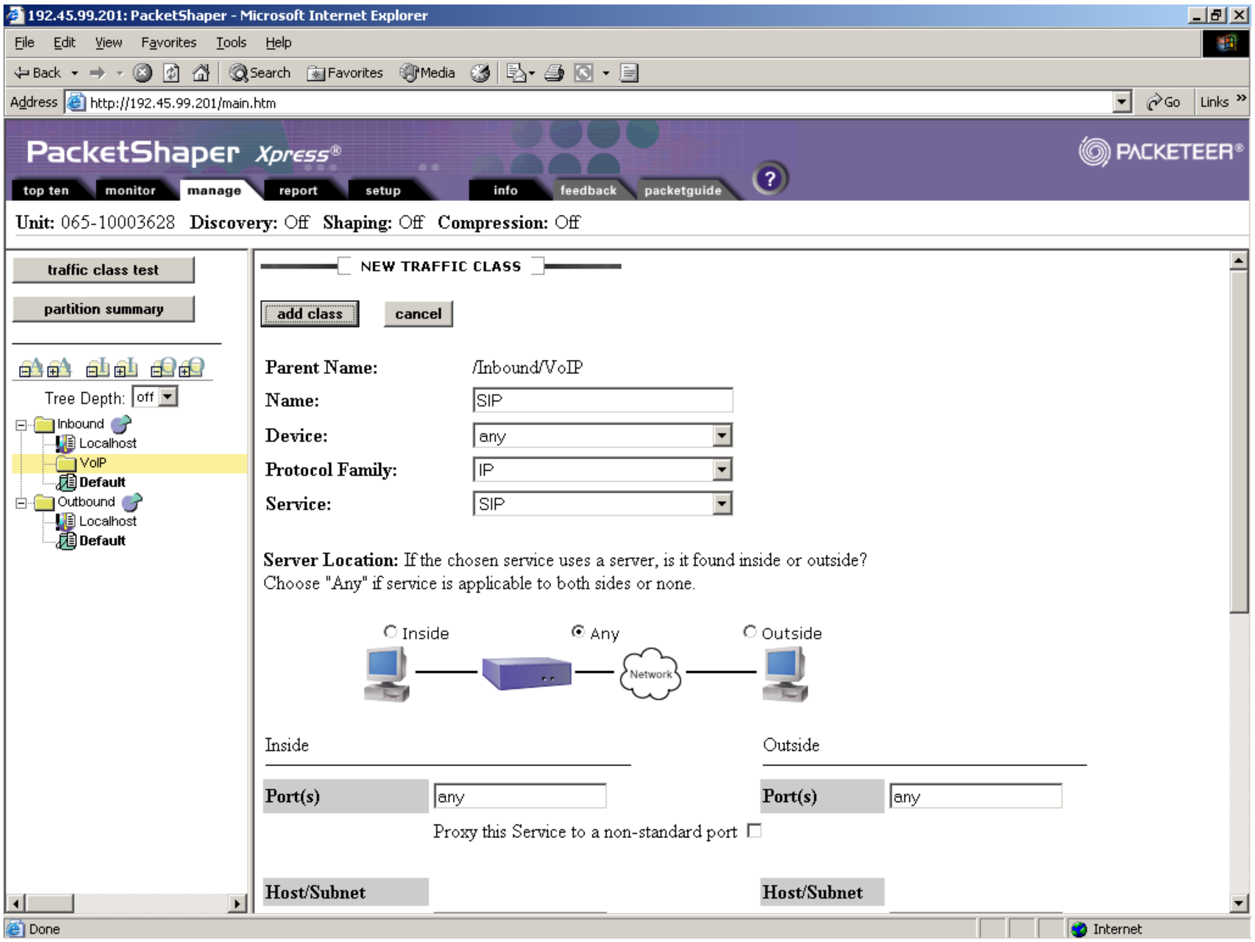
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>Click on the setup tab. Enter the capacity of the WAN link in the Inbound Rate and Outbound Rate textboxes and click on “apply changes …”. In the example below, a rate of 1.544M is used to approximate the T1 link rate.


</td></tr>
<tr><td>3.</td><td>Click on “OK” to confirm the changes.

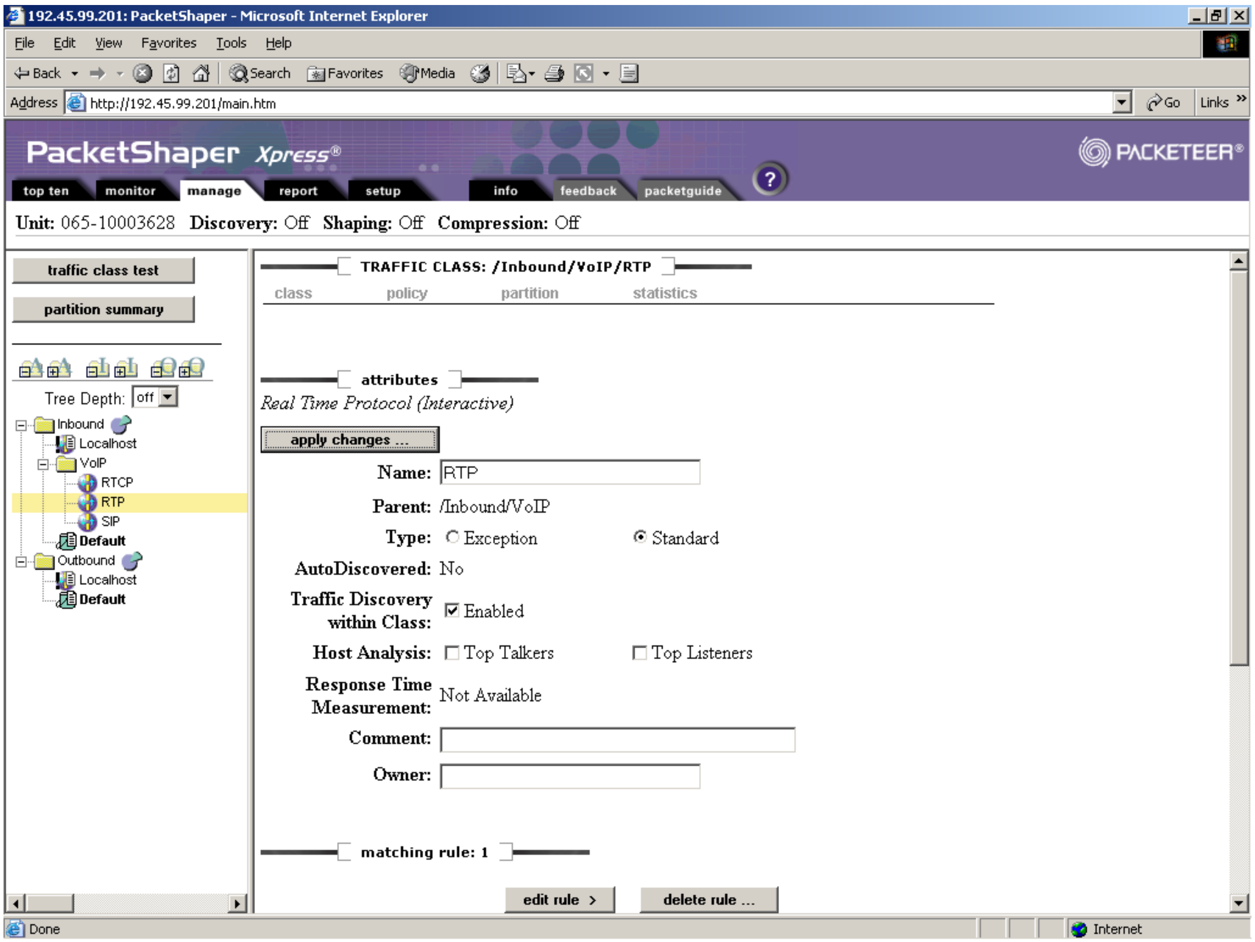

</td></tr>
<tr><td>4.</td><td>Click on the manage tab and then the Inbound folder in the left panel.</td></tr>
</table>

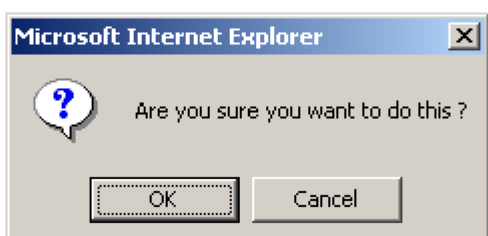
Step	Description
5.	Select **class->add folder** to create a folder for inbound VoIP traffic classes. 
6.	Enter a descriptive name for the folder and click on "**OK**". 

Step	Description
7.	Click on the newly created folder in the left panel. Select **class->add** to create an inbound traffic class. 

Step	Description
8.	Enter a descriptive **Name** for the traffic class and select the **Service** corresponding to the traffic class. The example below shows the creation of a SIP traffic class. Click on "**add class**". 
9.	Repeat Steps 7-8 for the following traffic classes: • RTP: Select **RTP-I** from the **Service** drop-down menu box. • RTCP: Select **RTCP-I** from the **Service** drop-down menu box.

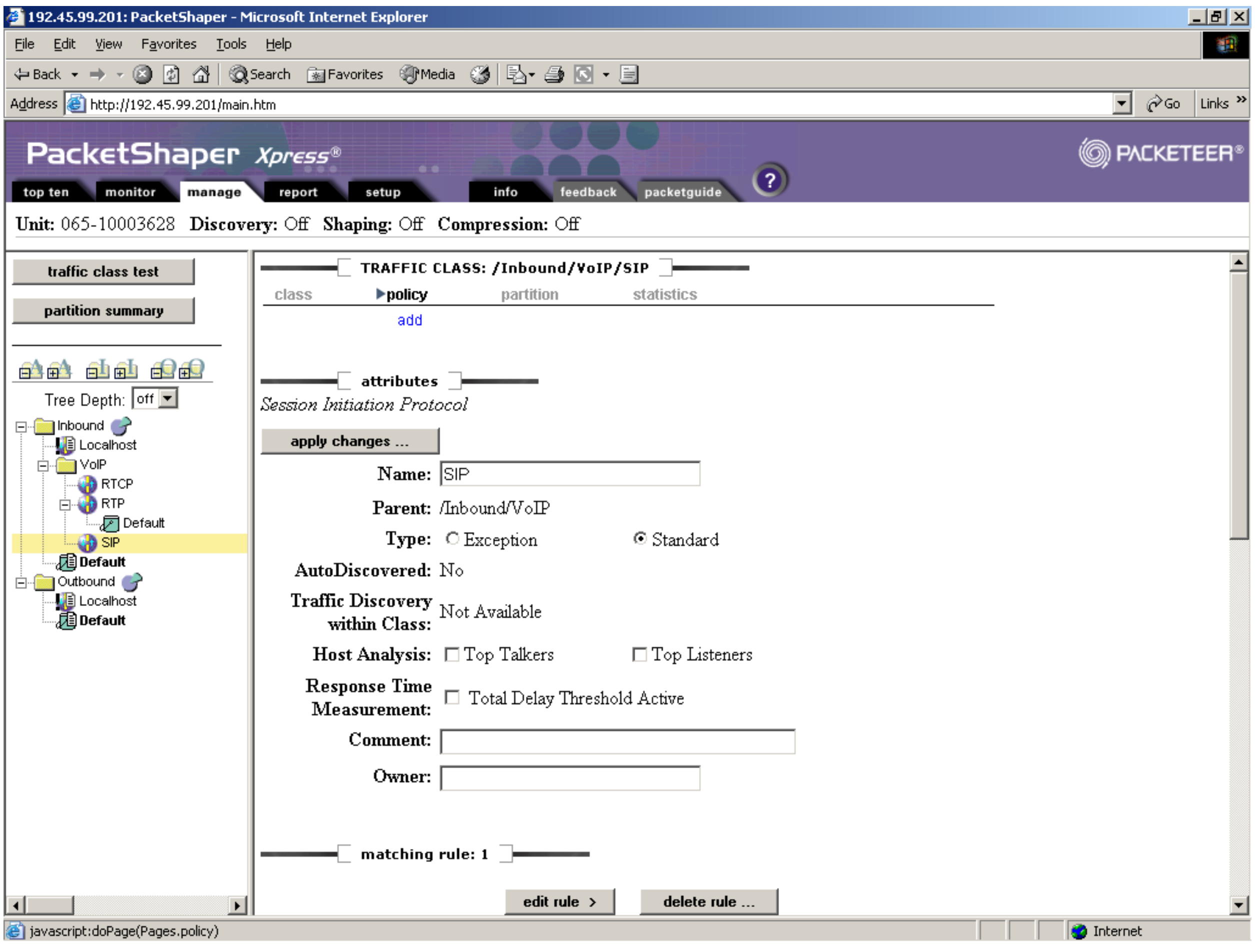
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>10.</td><td>Click on the RTP traffic class in the left panel. Enable Traffic Discovery within Class to allow PacketShaper to automatically create sub-classes for discovered codecs. Click on “apply changes …”.

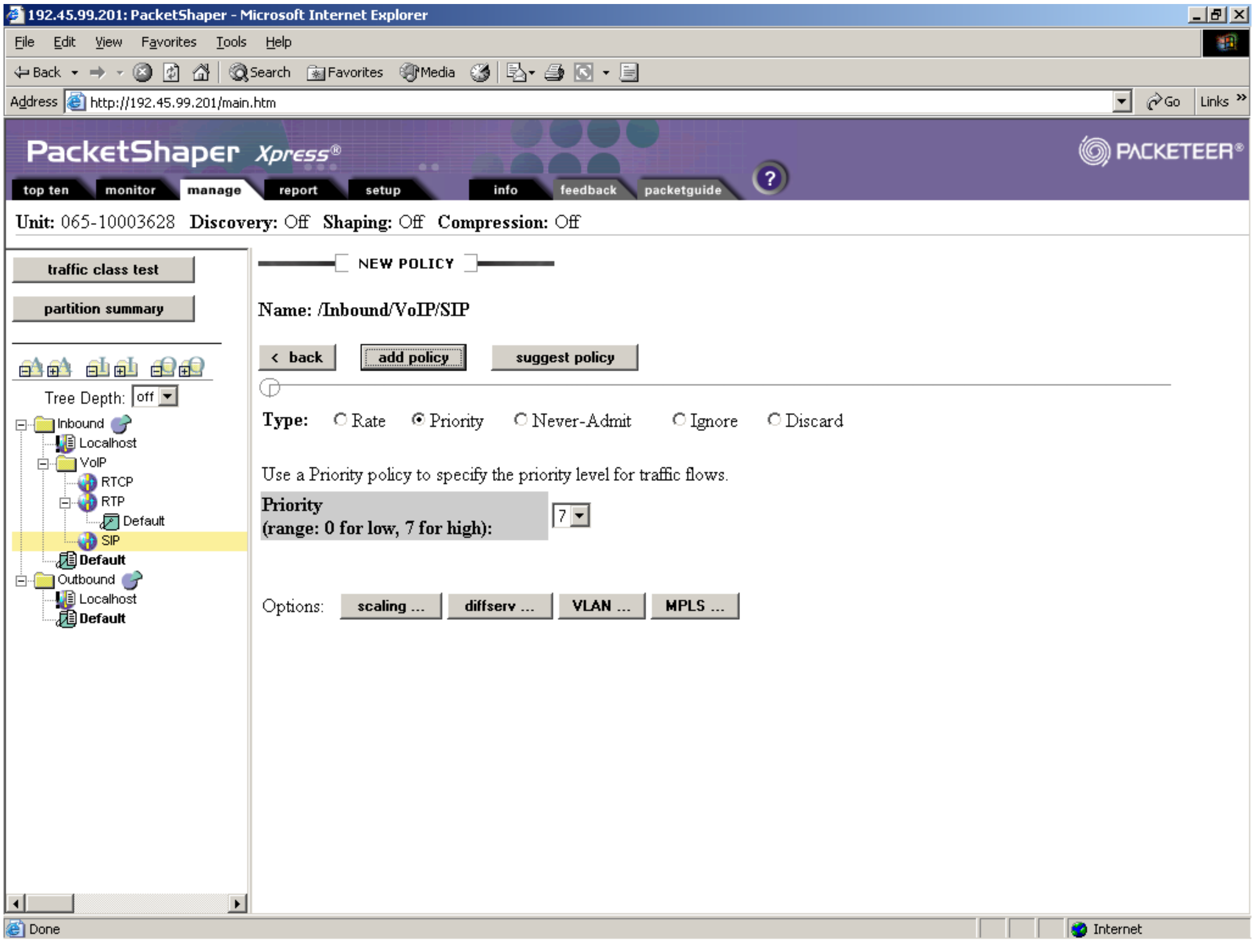

</td></tr>
<tr><td>11.</td><td>Click on “OK” to confirm the change.


</td></tr>
</table>

3.2. Assign Priority Policies to Inbound Call Control Traffic Classes

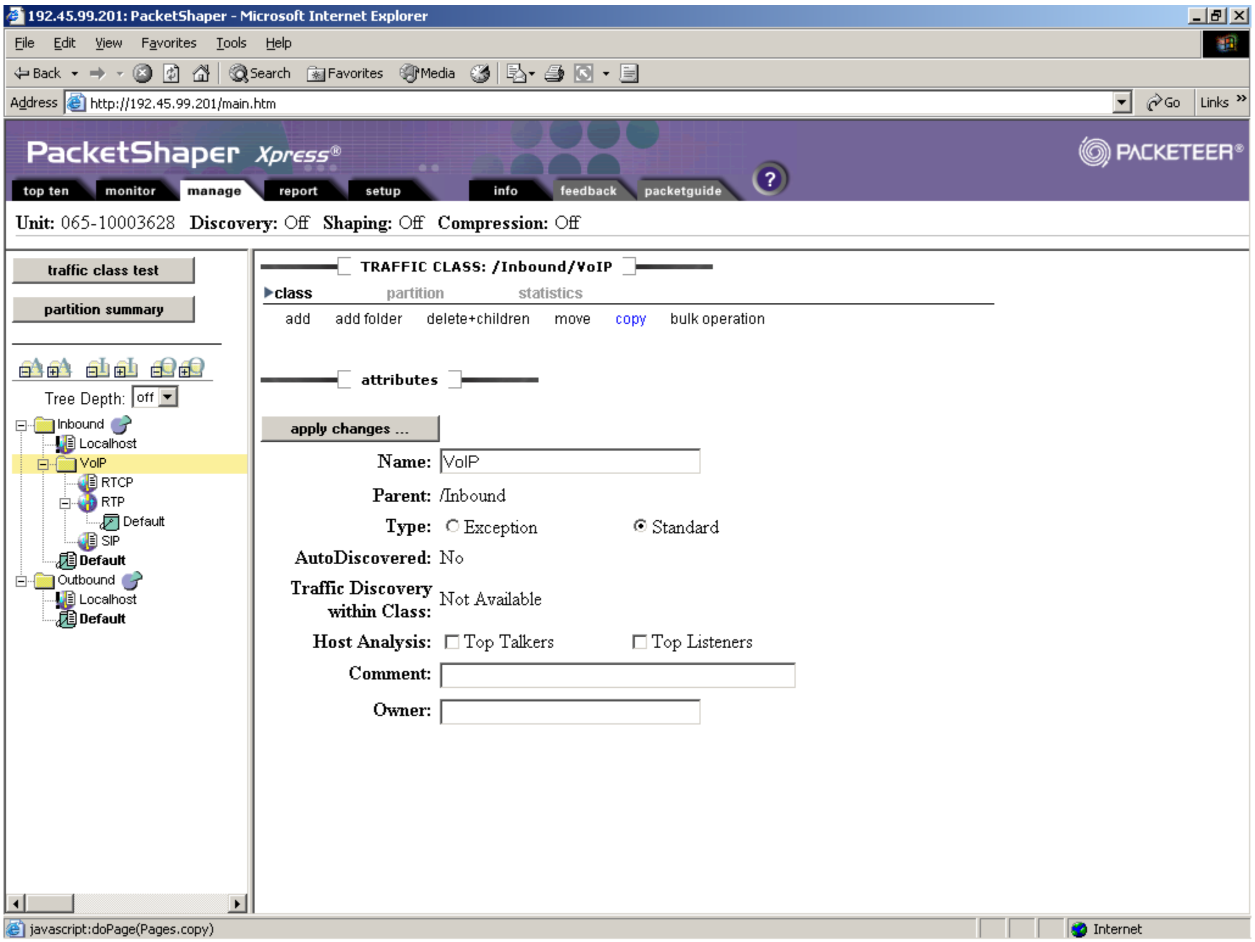
A priority policy applied to a traffic class specifies the precedence that packets within the traffic class should have relative to packets within other traffic classes. For example, a priority policy may be applied to each SIP call control traffic class so that SIP call control traffic takes precedence over less real-time sensitive data traffic.

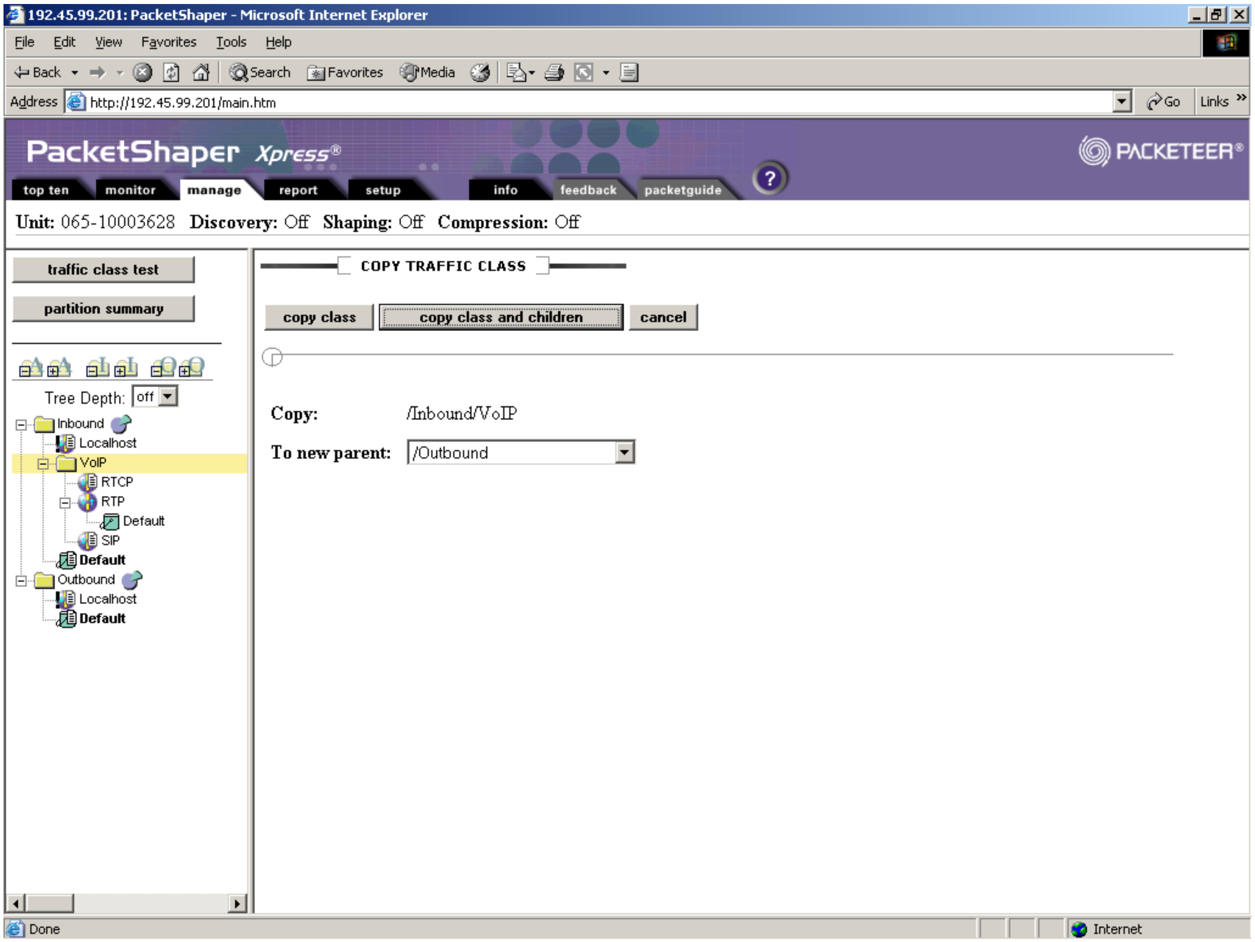
Step	Description
1.	In the **manage** tab, click on the inbound SIP traffic class in the left panel and select **policy->add**. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>Set Type to "Priority" and specify "7" for the Priority value. Click on "add policy".

</td></tr>
<tr><td>3.</td><td>Repeat Steps 1-2 for the inbound RTCP traffic class.</td></tr>
</table>

3.3. Configure Outbound Traffic Classes

Traffic classes may be configured for outbound traffic in the same manner as described in Sections 3.1 – 3.2 for inbound traffic. If the outbound configuration is to be the same as the inbound configuration, then perform the steps below.

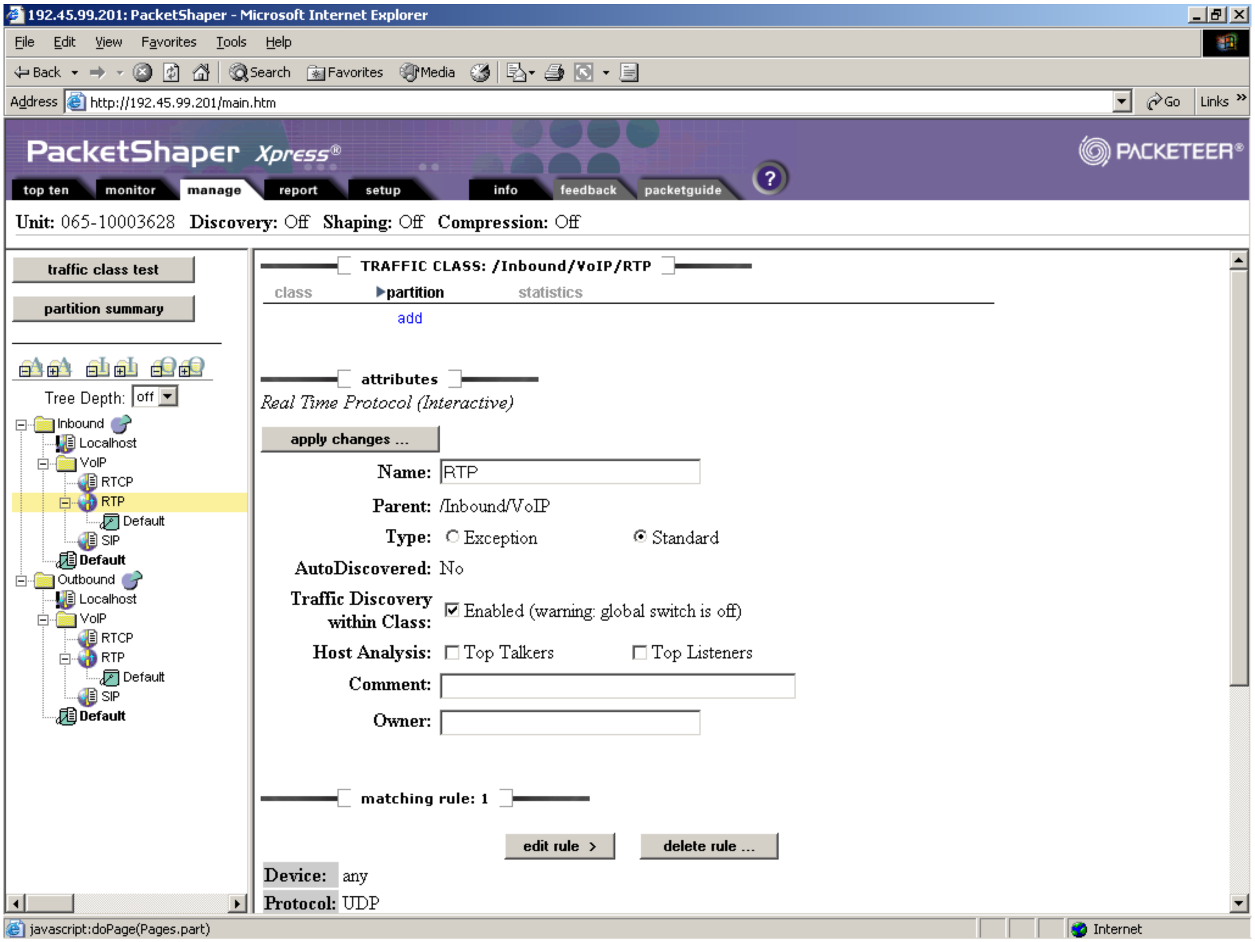
Step	Description
1.	In the **manage** tab, click on the inbound VoIP folder in the left panel and select **class->copy**. 

Step	Description
2.	Set **To new parent** to "**/Outbound**" and click on "**copy class and children**". 

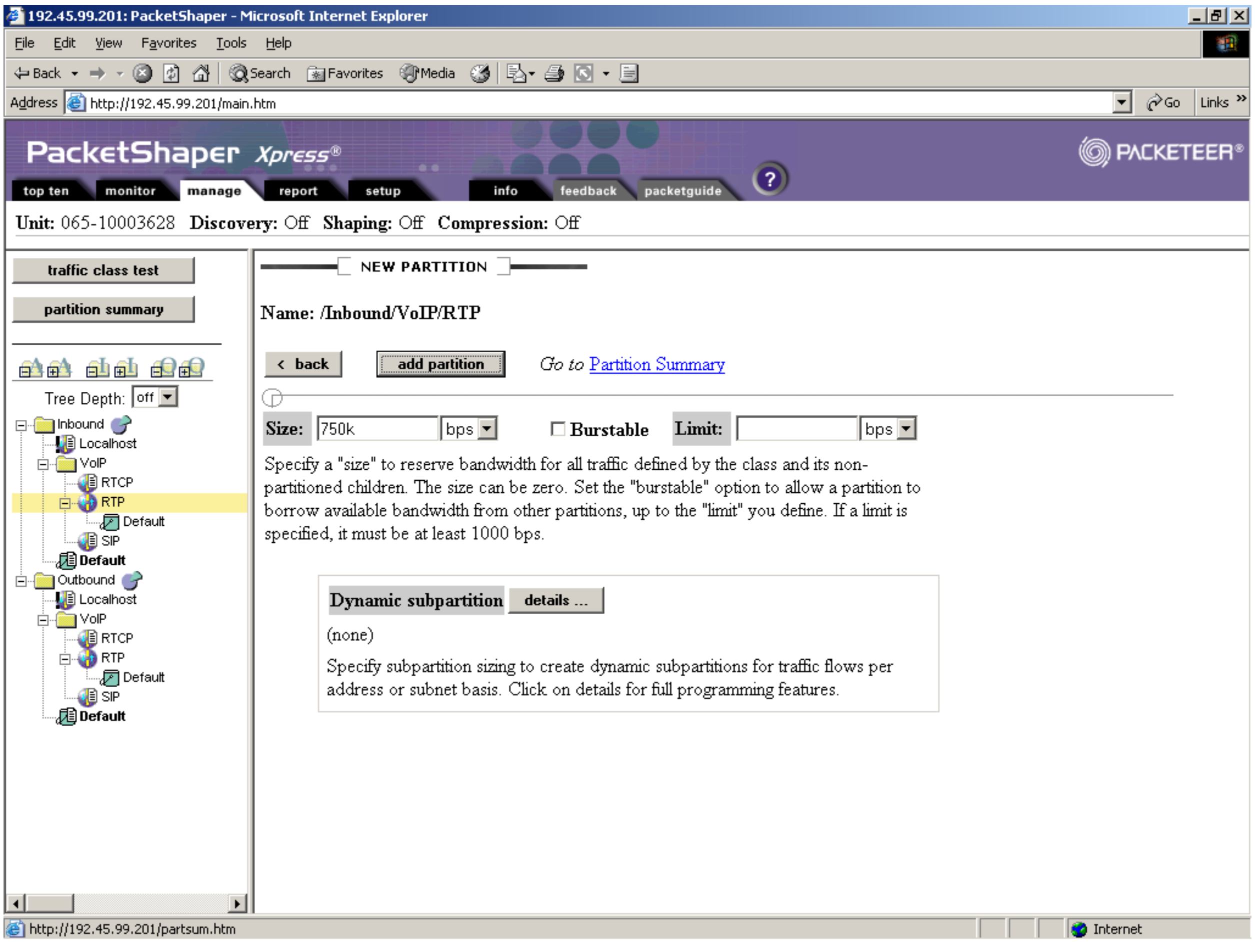
3.4. Bandwidth Partition for the RTP Traffic Class and Rate Policy for Individual RTP Flows

A partition specifies the total bandwidth reserved for all traffic within a traffic class. A partition applied to the RTP traffic class thus reserves a portion of the WAN link capacity for all RTP traffic. When combined with a rate policy (described below) on individual RTP flows, the partition effectively sets a maximum on the number of concurrent RTP flows going across the WAN link. Bandwidth above the reserved partition amount cannot be guaranteed, even with burstable limits defined.

Since the audio (RTP) portion of a VoIP connection typically requires a constant bit rate, a rate policy should be applied to individual RTP flows within the RTP traffic class. A rate policy specifies the amount of bandwidth reserved for each RTP flow, and when properly defined, ensures that each RTP flow going to the WAN router receives enough bandwidth.

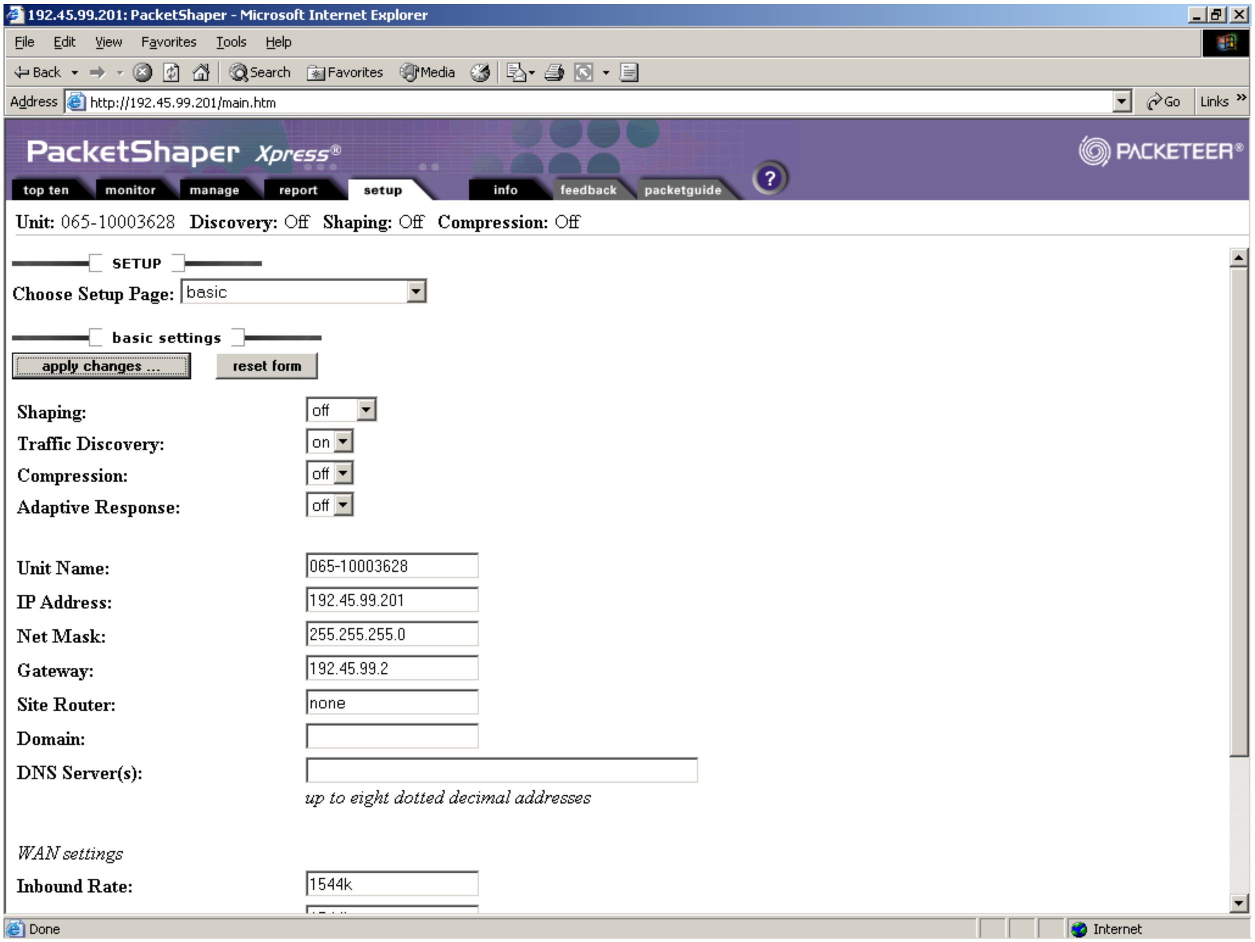
Step	Description
1.	In the **manage** tab, click on the inbound RTP traffic class in the left panel and select **partition->add**. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>Enter the Size (in bit rate or percentage) of the bandwidth partition for inbound RTP traffic and click on “add partition”. In the example below, approximately half of the inbound T1 link is reserved for RTP traffic.

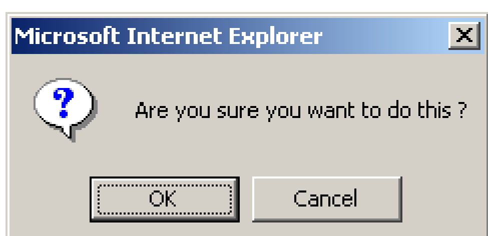


</td></tr>
<tr><td>3.</td><td>Repeat Steps 1 – 2 for the outbound RTP traffic class.</td></tr>
</table>

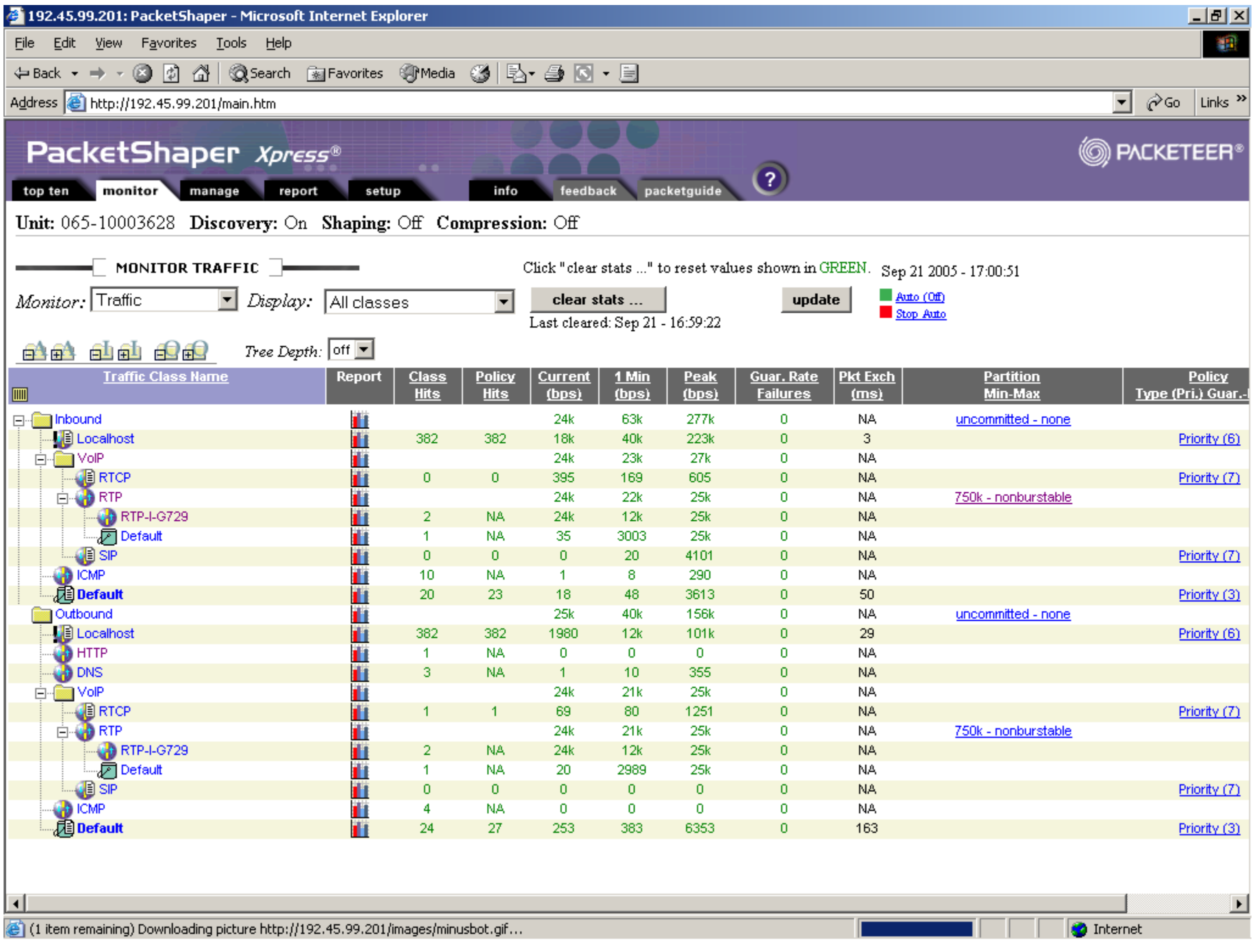
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.</td><td>Click on the setup tab. Set Traffic Discovery to “on” and click on “apply changes …”.



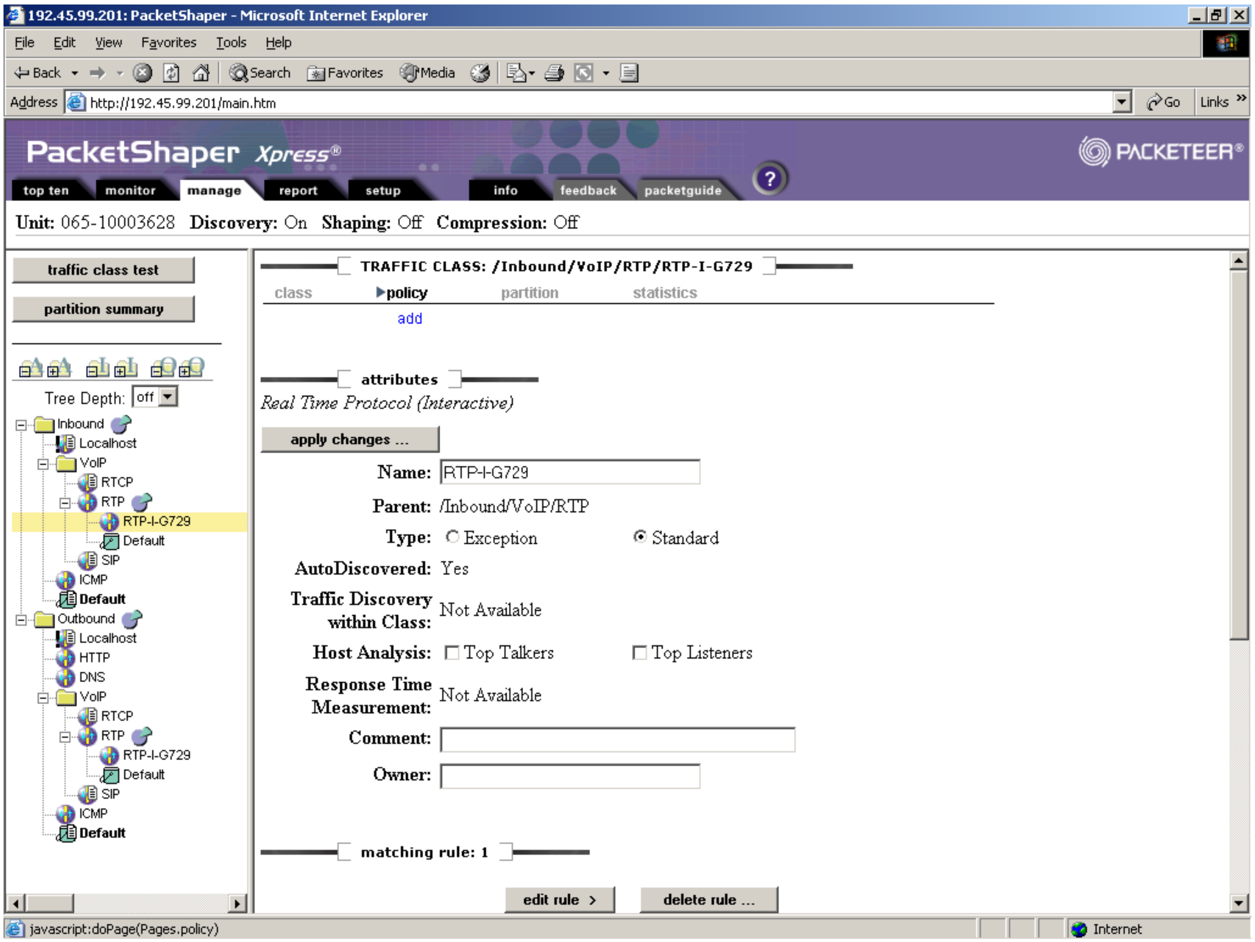
</td></tr>
<tr><td>5.</td><td>Click on “OK” to confirm the change.



</td></tr>
</table>

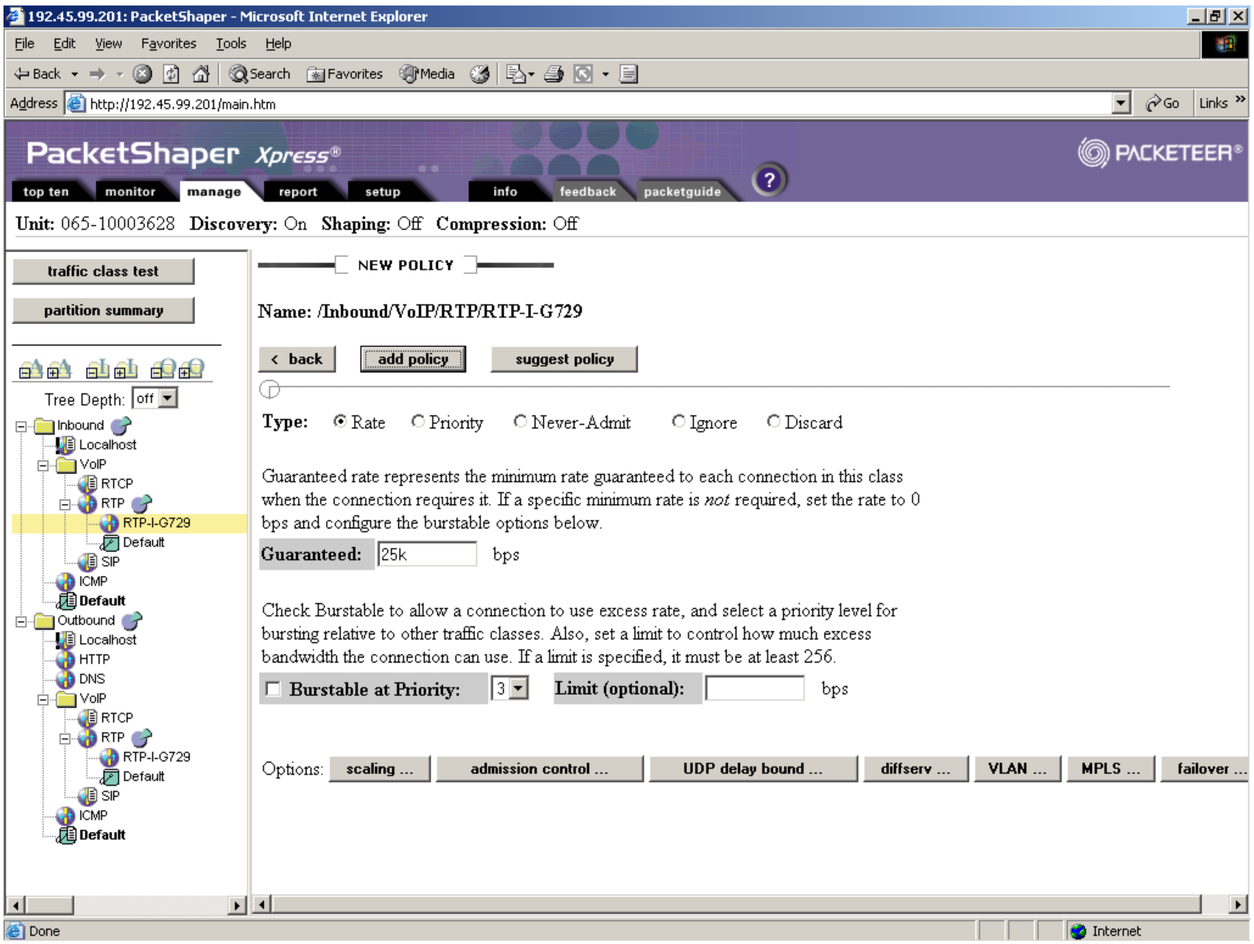
Step	Description
6.	Click on the **monitor** tab. Place several SIP phone calls across the WAN link until the codec(s) is (are) discovered and displayed on the traffic monitor. Click on the **update** button as necessary. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>7.</td><td>
Click on the manage tab and then the Inbound folder in the left panel. Click on the discovered codec and select policy->add.



</td></tr>
</table>

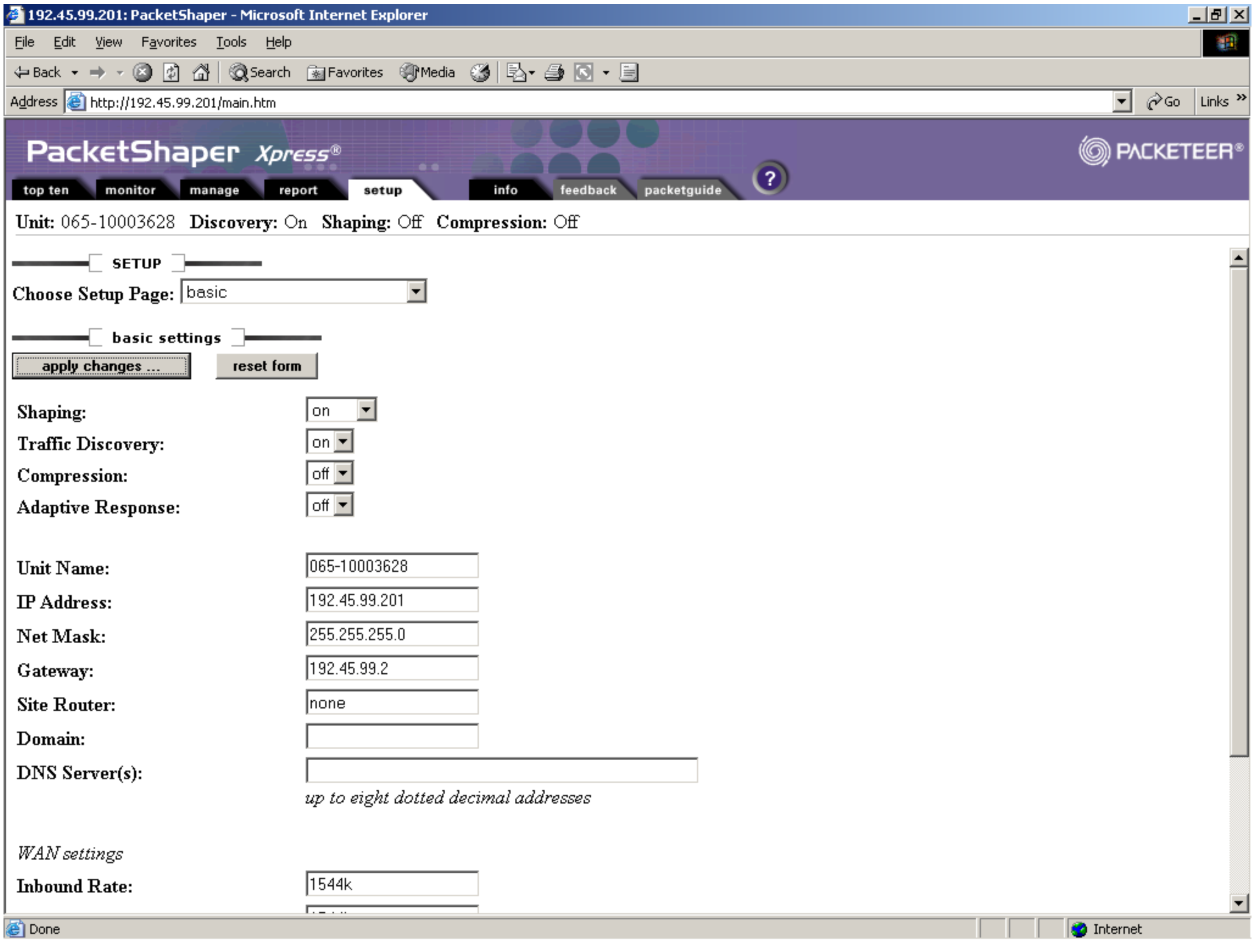
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>8.</td><td>Set Type to “Rate” and enter the Guaranteed bandwidth for each inbound RTP flow (for example, each phone call). The per-call bandwidth depends on the codec, packet size, and number of frames per packet. For example, for G.729 codec packets with 20 ms packet size and 2 frames per packet, the calculated per-call bandwidth including overhead is approximately 25kbps. Click on “add policy”.



</td></tr>
<tr><td>9.</td><td>Repeat Steps 7 – 8 for the discovered outbound traffic codec.</td></tr>
</table>

3.5. Enable Traffic Shaping

To turn on traffic shaping, click on the **setup** tab, set **Shaping** to "**On**", and click on "**apply changes …**".



4. Avaya Communication Manager and Avaya SIP Enablement Services

Basic administration of SIP stations, SIP trunking support, and SIP call routing in Avaya Communication Manager and Avaya SIP Enablement Services (SES) is assumed. In **Figure 1**, the Avaya SES Server routes calls originated by the registered SIP phones (IP telephones and softphones) in the enterprise and simulated WAN of **Figure 1**, to Avaya Communication Manager. Conversely, Avaya Communication Manager routes calls destined for the registered SIP phones to the Avaya SES server via SIP trunks. Note that for calls between the registered SIP phones, the call is routed from the Avaya SES server to Avaya Communication Manager and back to the Avaya SES server before terminating on the destination SIP phone.

5. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the impact that PacketShaper has on Avaya SIP VoIP traffic traversing a T1 link connecting an enterprise site to a simulated WAN. On PacketShaper, rate policies were applied for each RTP flow and bandwidth reservations were configured for the total RTP traffic. For SIP call control and RTCP traffic, bandwidth reservations were not made, but high priority policies were applied.

5.1. General Test Approach

The general approach was to attempt SIP phone calls between the enterprise and the simulated WAN with and without competing HTTP and FTP traffic. The competing FTP traffic traversed the WAN link and simulated an enterprise user performing an FTP download from a WAN host. An HTTP traffic generator was connected to the enterprise router (the Cisco 2900 router in **Figure 1**) and although the HTTP traffic did not traverse the WAN link, it did traverse the link between the enterprise router and the LAN. This arrangement allowed for more than 1.544 Mbps of HTTP traffic (in both directions) to go through the PacketShaper.

The main objectives were to verify that:

- Calls between SIP phones in the enterprise and in the WAN are successfully completed and maintained with good voice quality.
- Calls between an H.323 phone in the enterprise and a SIP phone in the WAN are successfully completed and maintained with good voice quality.
- Multiple SIP phone calls between the enterprise and the WAN up to the reserved amount are successfully completed and maintained with good voice quality.
- Non-VoIP traffic (HTTP and FTP) does not encroach upon the bandwidth reserved for SIP RTP traffic.
- SIP RTP traffic does not encroach upon the bandwidth reserved for other traffic.
- The solution is valid for G.711 and G.729 codecs.

5.2. Test Results

The test objectives of Section 5.1 were verified. With the appropriate bandwidth reservations and rate policies, PacketShaper was able to guarantee bandwidth for all calls up to the reservation amount during varying levels of competing HTTP and FTP traffic on the WAN link.

Calls above the expected number of calls allowed by the bandwidth reservation were established, but without audio. Since SIP call control traffic was assigned a high priority policy in PacketShaper, SIP signaling packets were able to traverse the WAN link unimpaired, and thus successfully establish the additional calls. However, the total bandwidth reservation for RTP traffic combined with the per-flow rate policy for RTP traffic limited the number of RTP flows, and thus the RTP (audio) streams of the additional calls were denied.

6. Verification Steps

The following steps may be used to verify the configuration:

- On PacketShaper, verify that the partitions, rate policies, and priority policies are configured correctly.
- From each side of the WAN link, ping SIP endpoints (Avaya SES server, Avaya SIP Telephones, and Avaya SIP Softphones) on the other side of the link.
- Place SIP phone calls across the WAN link and verify good voice quality when the WAN link is unsaturated and saturated with competing traffic.

7. Support

For technical support on the Packeteer PacketShaper, consult the support pages at http://www.packeteer.com/support or contact Packeteer Technical Support at 408-873-4550.

8. Conclusion

These Application Notes described the procedures for configuring the Packeteer PacketShaper to guarantee WAN link bandwidth to SIP Voice over IP (VoIP) RTP traffic generated by Avaya SIP Telephones and Softphones, and give high priority to SIP VoIP signaling traffic generated by Avaya SIP Enablement Services (SES) servers, and Avaya SIP Telephones and Softphones. During compliance testing, SIP phone calls traversing the WAN link were successfully established and maintained while non-VoIP traffic such as HTTP and FTP traffic was sharing the WAN link.

9. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com.

Product documentation for Packeteer products may be found at http://www.packeteer.com/support.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.