Packeteer® Deployment Guide

DEPLOYING PACKETSHAPER® IN A VIDEO OVER IP ENVIRONMENT

Deploying PacketShaper® solutions to ensure efficient, reliable performance of video over IP in shared networks

July 2002

Packeteer, Inc.
10495 N. De Anza Blvd.
Cupertino, CA 95014
408.873.4400
info@packeteer.com
www.packeteer.com

This paper examines best practices for configuring Packeteer's PacketShaper® to protect H.323 video over IP traffic.

IP Convergence & the Need to Manage Video over IP Traffic

IP convergence, long the holy grail of the Internet revolution, is finally starting to become a reality in the enterprise. Video over IP for videoconferencing is one of the key applications driving this revolution. While single-service IP networks are relatively manageable, multi-service networks present a greater challenge. The convergence of voice, video, and data traffic over a shared network introduces heightened concern over ensuring efficient, reliable application performance, particularly latency-sensitive traffic like video over IP.

Compared to aggressive, bandwidth-intensive applications, many of which are unsanctioned for business purposes, video over IP uses an invariable amount of bandwidth. It is not bursty. However, it is highly susceptible to interference from other applications.

Therefore, the primary objective for network administrators is to control the performance of unpredictable and less-urgent applications that share the same link as video over IP traffic. This traffic may include web surfing, FTP, email, and print jobs. It may also include managing mission-critical traffic like ERP, CRM, messaging, and other business applications, because despite their importance, network managers ultimately need to ensure that all applications perform efficiently without disrupting the delivery of other important traffic.

Deploying PacketShaper®

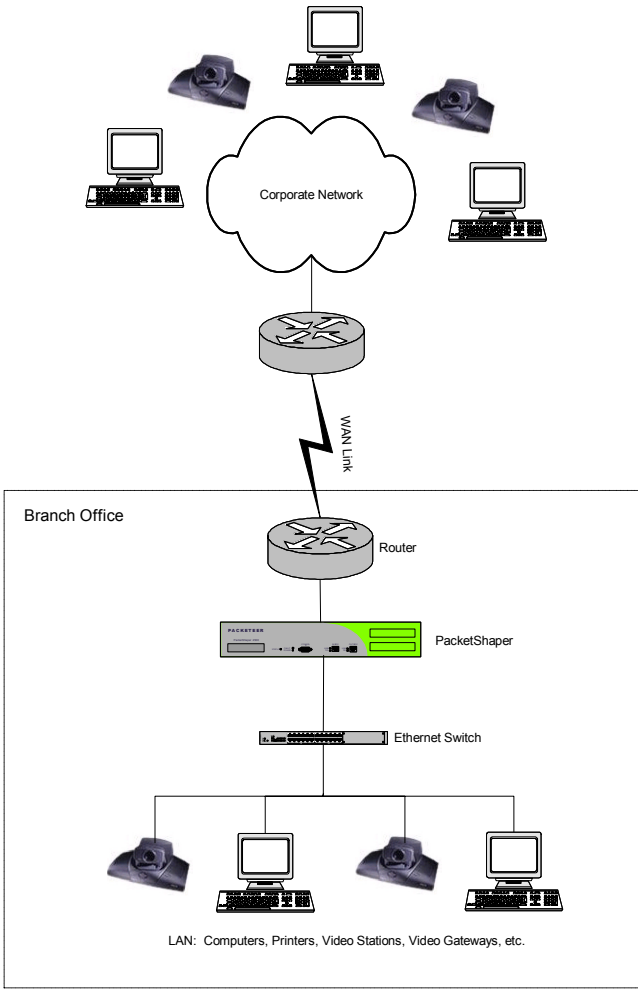
The proliferation of IP convergence and the need to manage it has prompted the need for Packeteer's PacketShaper, an application performance solution that ensures the efficient, reliable performance of business-critical applications over the WAN and Internet.

PacketShaper is deployed at branch offices, next to WAN-link routers on the Ethernet side. From this vantage point, its Layer 7 visibility provides organizations with thorough visibility into traffic heading to and from the central site and between other branch sites. This visibility provides the intelligence needed to utilize PacketShaper's policy control features for managing bandwidth allocation, latency, and the efficiency of each application based on its relative business importance. Like a switch, PacketShaper fits transparently in the traffic path and does not add a hop or alter routing configurations. Because it resides on the Ethernet side of the router, PacketShaper is transport-agnostic. In other words, it integrates seamlessly with frame-relay, point-to-point, ATM, DSL, wireless, and most other WAN transport mechanisms.

QoS Methodology

Implementing PacketShaper to enhance a video environment involves three steps:

1. Assess network requirements through traffic classification and performance analysis
2. Implement policies
3. Monitor results



Assess Network Requirements

The first step in deploying a QoS strategy is to assess the true bandwidth requirements of video over IP traffic. This involves identifying its presence on the network and analyzing its performance to determine its bandwidth needs.

It also entails classifying all traffic running on the network. Overall visibility into the types of traffic running on the network provides a comprehensive view of traffic patterns and each application's impact on other traffic. An H.323 session alone includes numerous traffic components that have their own policy and performance requirements.

Classification

To classify traffic, create a class named *Video over IP* and identify the video over IP endpoints or gateways at this branch. This needs to be done for both inbound and outbound directions, because video over IP is typically bi-directional. The endpoints can be identified either by IP address or by dynamic name if you are using a DHCP environment (i.e. conference-room-3.packeteer.com). If you have multiple endpoints at a location, you may enter them in a Host List. If you have a Packeteer PolicyCenter™ Central Management server, you may create one list of all approved videoconference stations for the whole organization and store it on a central LDAP server.

H.323 Elements	Protocol
Call Setup Protocols	Q.931, H.323 Gatekeeper, etc
Video & Voice Channels	RTP
Control Channels	RTCP
Collaboration Channels	T.120
System Control	RSVP, Proprietary Management

Creating a list of approved stations assures that non-approved H.323 equipment will not sneak onto the network. If this is not a concern, disregard the option of entering IP addresses. PacketShaper will discover all H.323 traffic on the network.

Next, enable traffic discovery for that traffic class. This will automatically identify all of the different types of traffic generated by the endpoint and will begin collecting data about them. To facilitate this process, start and then stop a few videoconferences to generate some traffic. Leave one of the conferences running at least 10 minutes to collect a substantial amount of measurement data. You should see most of the individual H.323 sub-protocols, such as RTP and RTCP, discovered as classes (not every call uses every protocol, so some may not appear immediately). Because PacketShaper discovers H.323 traffic regardless of what port number it is using, you do not need to define a specific port range.

Measurement
Now use PacketShaper's Report tab to view the data collected. You should see how much bandwidth was consumed by video traffic.

Implement Policy
From the report, you should be able to see how much actual bandwidth a call requires using your chosen codecs. PacketShaper measures both data payload and header overhead, so requirements will be slightly higher than the nominal bandwidth rate of the codec. In general, you should expect to see an increase ranging from 10 to 20 percent. Thus, a nominal 768k stream might take 820k when headers are accounted for.

Keeping in mind how much bandwidth a single call requires, determine how much bandwidth you want to allocate to video traffic. Create a partition on the video over IP parent class that you created earlier that reflects your decision, both in inbound and outbound directions. Partitions are defined with a CIR (minimum) and EIR (maximum). Because PacketShaper's unique dynamic partitioning reallocates unused bandwidth to other applications so that it is not wasted, it is advised to provide a little extra bandwidth for video. For instance, in our example above, you might select a CIR of 850k to allow the protocol extra headroom.

Example
A common partition setting for a T1 link and video using 384k encoding is:

Partition: Minimum 500k Burstable to 1,000k
Policy: 420k Burstable at Priority 5

A 384k codec will probably use about 420k with headers and overhead. So, if one video flow is present, it will receive 420k (or whatever it needs up to 500k) and the rest of the bandwidth will be available to data track. If two flows exist, each will receive 420k (840k total), and the remaining bandwidth will be given to data traffic.

Monitor Results
Once policies have been implemented, monitor the network to validate their success. PacketShaper's extensive reporting capabilities provide comprehensive details to ensure service-level agreements are being met.

Summary
Implementing PacketShaper to ensure efficient, predictable performance of video over IP requires:

1) Installing the unit and turn on Traffic Discovery and Auto Policy provisioning.
2) Generating video over IP traffic over the link so that PacketShaper can discover the H.323 traffic.
3) Applying a partition to set minimum and maximum bandwidth allocations for the H.323 traffic. Additional tuning can be applied to achieve a more complex and specific network policy.

For implementation details, visit:
http://support.packeteer.com/documentation/packetguide/current/solutions/app-control/manage-voip.htm