Solutions Guide

Visual Communication Services Using Polycom® VVX 1500 Phones on the BroadSoft® BroadWorks™ Call Server

This solutions guide provides detailed information for system administrators on using the Polycom VVX 1500 phones with the BroadSoft BroadWorks call server, the Acme Packet Net-Net 4250 Session Border Controller (SBC), and the Edgewater 200/4500T and U4EA Fusion 200/500 enterprise edge devices.

This information applies to Polycom VVX 1500 phones running SIP application version 3.1.2RevB or later. This information applies to BroadSoft BroadWorks R14 SP7 or later and BroadWorks Media Server (MS) R15 or later. Polycom does not support the use of earlier versions of BroadWorks with the Polycom VVX 1500 phone.

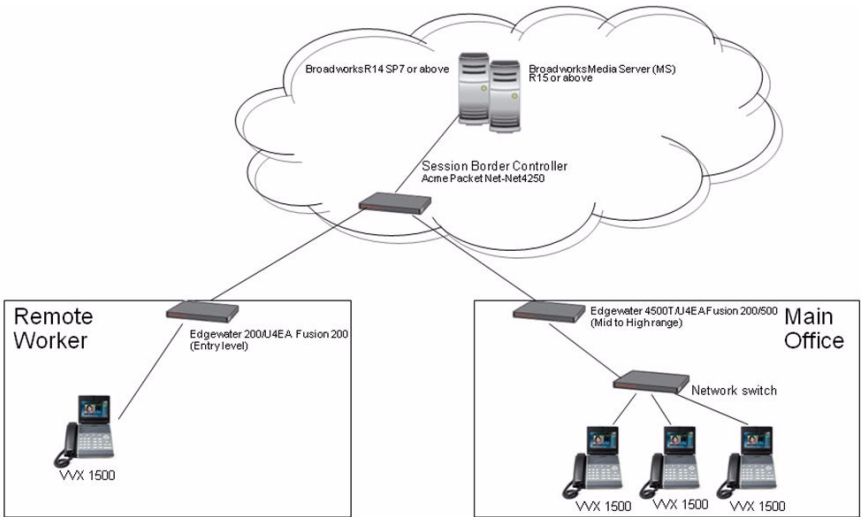
Overview

In today's competitive hosted ITSP market, there is increasing pressure on the ITSPs to reap new revenues and customer loyalty through differentiated service innovations. The question most service provider is asking is "How do I differentiate myself, other than pricing?"

Polycom's approach is designed to address the complex challenges faced by hosted service providers in today's VoIP market by enabling voice and video solutions which offer *easy integration*, provide *proven value*, and are *quick to deploy*.

As shown below, the solution consist of several different access components. These access components include:

- Session Border Controller
- Enterprise Edge Device
- Polycom VVX 1500 Business Media Phone



<June 2009>
1725-47075-001/B1

This solutions guide provides the administrator, using Polycom VVX 1500 phones with the BroadSoft BroadWorks call server, information on how to configure each of the components:

- Configuring the BroadWorks Call Server
- Configuring Session Border Controllers
- Configuring Enterprise Edge Devices
- Configuring the Polycom VVX 1500 Phone

Configuring the BroadWorks Call Server

Every registration in BroadWorks is associated with a device profile that determines the broad capabilities for that device. One of the capabilities listed in this profile is support for Video, otherwise the BroadWorks Application Server (AS) will strip out all Video m-lines from the SDP.

By default, none of the Polycom device profiles shipped with the current BroadWorks release have Video support enabled, so to correctly deploy the Polycom VVX 1500 phones, you have three options:

- You can modify one of the existing Polycom device profiles to support video. Refer to Edit an Existing Device Type Profile on page 3.
- You can create an entirely new device profile for the Polycom VVX 1500. Refer to Create a New Device Type Profile on page 5.
- You can select the **Generic SIP Phone** device type for the Polycom VVX 1500 registrations.

Note Future releases of BroadWorks will include an existing device profile for the Polycom VVX 1500.

The Polycom VVX 1500 phone has been certified for use with BroadWorks AS R14sp7 and BroadWorks Media Server (MS) R15.

Before you read this section of the document, become familiar with your BroadWorks call server capabilities. Documentation should be obtained from BroadSoft.

Changing the BroadWorks Call Server

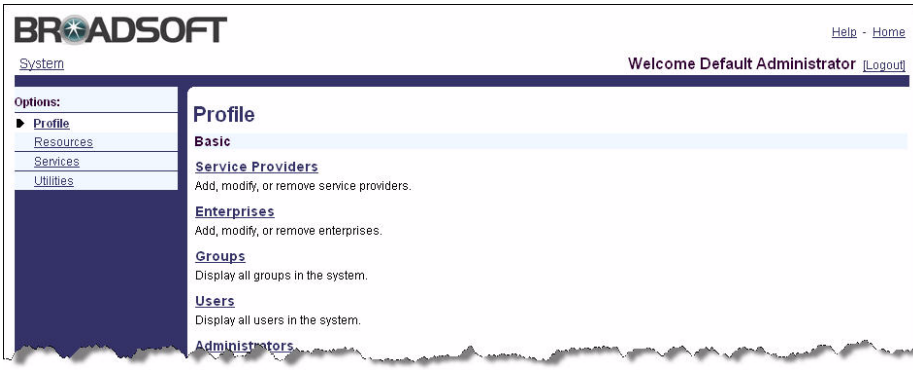
The options for phone profiles are:

- Edit an Existing Device Type Profile
- Create a New Device Type Profile

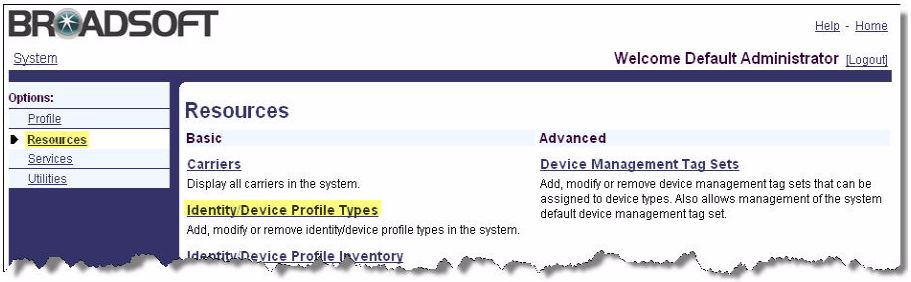
Edit an Existing Device Type Profile

To edit an existing device profile:

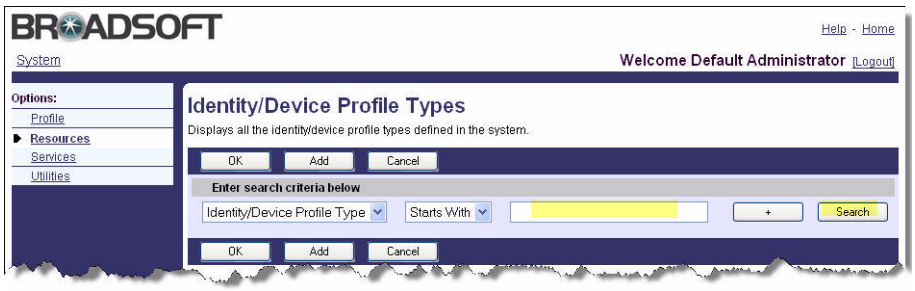
1. Login to the AS web user interface as the System Administrator.



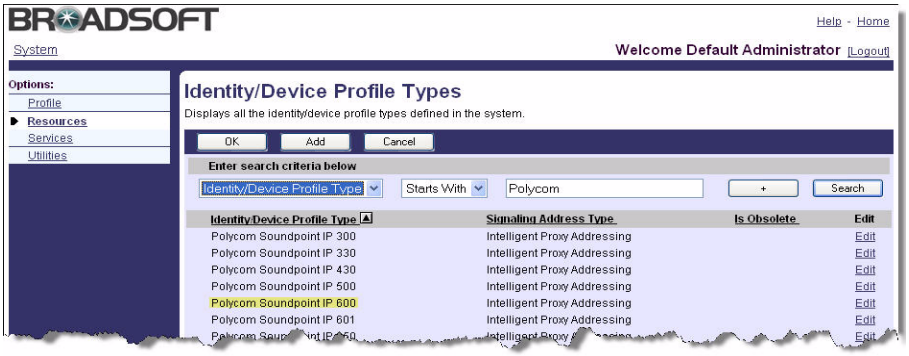
2. From the System Administrator's default screen, select the **Resources** option from the left hand menu.



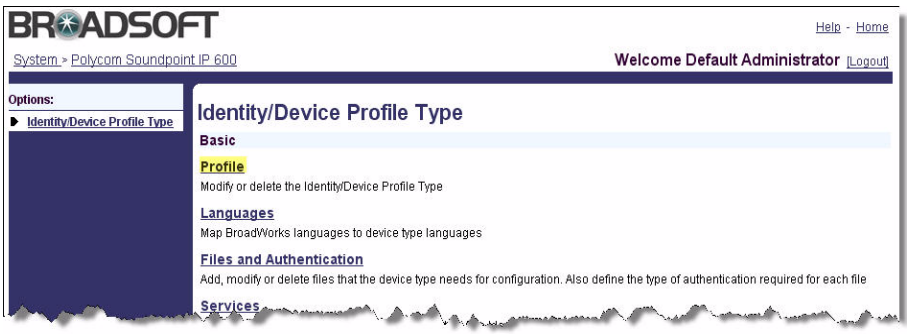
3. From the Resources menu, select **Identity/Device Profile Types**.



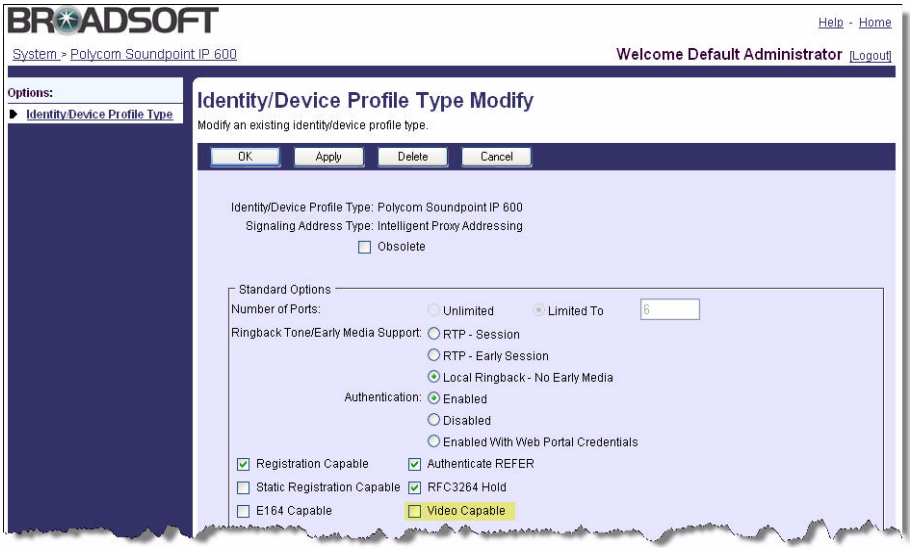
4. Enter **Polycom** in the text box and click **Search**.



5. Select the profile type that you want to modify (for example, “Polycom SoundPoint IP 600”).



6. Select **Profile**.



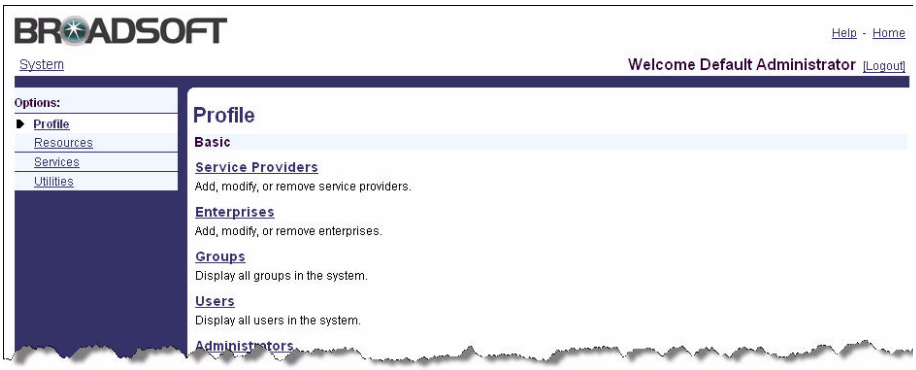
7. In the Standard Options section, select the **Video Capable** option.
8. Click **Apply**.

At this point, any device profile using the selected Device Profile Type (either "Polycom Soundpoint IP 600" or whatever you chose in step 5 above) will be able to make video calls. Some of the features require additional services assigned to the users to take advantage of the video portions of those features. For example, you have to add the specific "Music on Hold - Video" service to a group before video devices will start getting video when on hold.

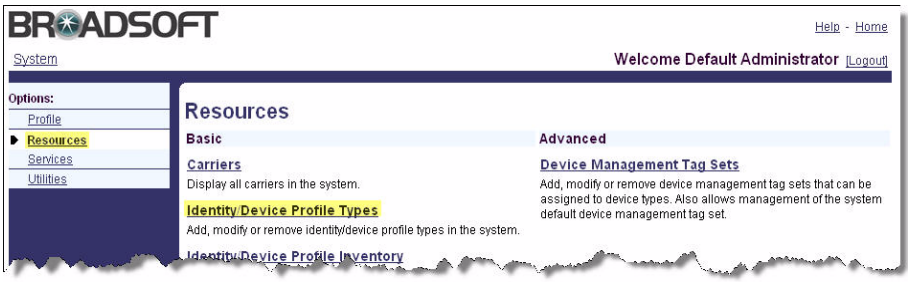
Create a New Device Type Profile

To create a new device type profile:

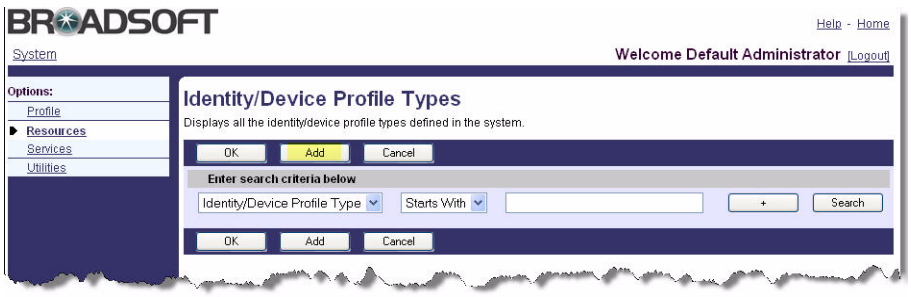
1. Login to the AS web user interface as the System Administrator.



2. From the System Administrator's default screen, select the **Resources** option from the left hand menu.



3. From the Resources menu, select **Identity/Device Profile Types**.



4. Click **Add**.
5. Fill in the form as follows:

Field Name	Value
Identity/Device Profile Type	Polycom VVX 1500
Signalling Address Type	Intelligent Proxy Addressing
Options	
Number of Ports	Limited to 6
Ringback Tone/Early Media Support	Local Ringback - No Early Media
Authentication	Enabled
Registration Capable	Yes
Static Registration Capable	No
E164 Capable	No
Trusted	No
Authenticate REFER	Yes
RFC 3264 Hold	Yes
Video Capable	Yes
Advance Options	
Route Advance	No
Wireless Integration	No
PBX Integration	No
Use Business Trunking Contact	No
Auto Configuration Soft Client	No
Supports BroadWorks INFO for Call Waiting	Yes
Forwarding Override	No
Conference Device	No
Mobility Manager Device	No
Music On Hold Device	No
TDM Overlay	No
Auto Configuration Options	
Web Base Configuration URL	<blank>

Field Name	Value
Auto Configuration Type	3 Config File
Reset Event	checkSync
Enable Monitoring	No
CPE System File Name	PolyComVVXSystem.cfg
Device File Format	%BWMACADDRESS%.cfg

6. Click **OK**.

Note For additional steps to correctly configure Auto-Configuration, refer to the BroadSoft Enhanced IP Phone Configuration Guide.

Any registration using a device of this Device Type will be able to support video calls.

Configuring Session Border Controllers

A session border controller provide critical control functions to enable high quality interactive communication—voice, video and multimedia sessions—across IP network borders.

Before you read this section of the document, become familiar with your Acme Packet's Net-Net family of products. Documentation should be obtained from Acme Packet.

Changing the Acme Packet Net-Net SBC

Acme Packet's Net-Net product family enables the secure delivery of a broad range of interactive communications services and applications ranging from basic VoIP to Service Oriented Architecture (SOA) enabled unified communications. It secures the borders to the service provider IP network, the private VPN connecting major enterprise or contact center sites, and the Internet for connecting remote offices, teleworkers and callers to the contact center. It ensures interoperability of both legacy IP-PBX equipment and next-generation unified communications platforms such as Microsoft Office Communications Server and manages their traffic load and resource availability.

The topics in this section include:

- Video Enabling the SBC
- Bandwidth Management

- Call Admission Control
- Bandwidth-Based Call Admission Control
- Multi-level Admission Control and Bandwidth Policy Enforcement for Oversubscribed Broadband Access Networks
- Session Capacity and Session Rate
- Signaling Quality
- SIP Server Failure Detection
- External Policy Decision Function

Video Enabling the SBC

The Acme Packet Net-Net Session Director (SD) architecture supports any signaled service including voice and video applications. Codec Media Profiles in the SD are used to determine the proper amount of bandwidth allocated for a given session, distinguishing between G.711 or G729 voice and H.263/264 video requirements, for example. By supporting video transmission as well as voice over the IP MPLS core, the SD allows Service Providers to roll out new services to their enterprise customer such as video/audio conferencing.

To alleviate the bandwidth demands of high-definition video streams the Acme Packet Net-Net SD should be ordered with the 2 or 4 Gigabit PHY card option.

Bandwidth Management

Embarking on a migration to multi-media over IP requires the adoption of a management strategy that spans the end-to-end service delivery system—including not only the service infrastructure and its components, but also overall network management and Quality of Service (QoS) policy management. Service assurance is the ability to monitor and manage the network to ensure a defined service level, regardless of the technology, service, protocol, or vendor. Employing the appropriate service assurance tools enables high quality multi-media IP services.

Acme Packet's Net-Net family of products enables service providers to address critical requirements in the following areas:

- Resource and admission control
- Traffic and capacity management
- Quality-of-Service
- Service availability
- Network monitoring and reporting

Call Admission Control

End-to-end call admission control and bandwidth management can sometimes become very challenging for network and service providers, due to the complicated nature of today's networking environment. Bandwidth bottlenecks are usually located at network borders where various types of network traffic aggregated. Acme Packet's ability to foresee this bandwidth management demand allowed it to design its session border controller products to carry the mission of achieving maximum flexibility. With Acme Packet's highly configurable QoS and protocol interworking features, network and service providers will be able to perfect their network traffic planning, whether QoS decisions are to be performed at borders, or by core-network application servers.

The Acme Packet Net-Net SD currently provides call admission control capabilities based on a several different policies including:

- Bandwidth (single and multi-level policies)
- Session capacity
- Session rate (sustained and burst)

Bandwidth-Based Call Admission Control

Whether in a carrier interconnect model or a hosted IP services model, bandwidth consumption must be managed in accordance with capacity engineered in the network. The Acme Packet Net-Net SD allows for aggregate bandwidth policies to be configured for each realm. A realm is a logical distinction that represents a route (or group of routes) reachable by the Acme Packet Net-Net SD. As the SD processes call requests (to and from) a particular realm, the bandwidth consumed for the call is decremented from the bandwidth pool for that realm. The SD determines the required bandwidth from the SDP/H.245 information. Any request that would cause the bandwidth constraint to be exceeded is rejected with a SIP 503 Service Unavailable or an H.323 Release Complete.

Multi-level Admission Control and Bandwidth Policy Enforcement for Oversubscribed Broadband Access Networks

Multi-level nesting of bandwidth policy enforcement addresses the following service provider challenges:

- Bandwidth over-subscription: Access or transit transport networks are aggregated and/or oversubscribed. (i.e., DSL, FR, ATM). Admission control policies must reflect access network topology.
- Bandwidth partitioning for multiple services: Access or transit bandwidth is to be partitioned between multiple service profiles (i.e. SIP & MGCP) in the same customer network).
- Multi-site VPN environments where admission control must be applied at the site level as well as the VPN level.

Session Capacity and Session Rate

Session capacity and rate limits are also configured for each destination. The SD will deny any call request to a destination that has exceeded it's configured policies for session capacity and session rate. The SD may reject the call request back to the originator. If multiple destinations are available, the SD will check current capacity and rate for each destination and attempt to route the call only to destinations whose policy limits have not been reached.

Acme Packet's Net-Net SD also addresses these QOS requirements for VoIP-based networks by providing several key functions:

- **Classification**—The Acme Packet Net-Net SD acts as a media and signaling proxy (also described as a QoS anchor point), aggregating all signaled high quality sessions to a fixed set of IP addresses and/or interfaces on the edge router. This provides the missing granularity, needed in existing edge routing QoS solutions. For more fine-grained control, classification rules can be established by customer(department), service and media type (for example, voice or video).
- **Packet Marking**—The Acme Packet Net-Net SD provides per-session DiffServ or ToS marking. Media flows destined for the routed core network can be explicitly marked using ToS or DiffServ. Media packets can be marked by VPN, by codec (voice or video) or by E.164 phone number prefix. Alternatively, edge routers can implicitly classify and mark and queue all flows arriving from the Media Manger interface. 802.1p VLAN termination and origination is also supported on the Net-Net SD, allowing you to utilize VLANs with your Ethernet infrastructure to specify internal QoS priorities and integrate with MPLS based QoS schemes.
- **QoS Reporting**—The Acme Packet Net-Net SD provides QoS statistics that may be used for SLA customer reporting, fault isolation, SLA verification and traffic analysis. The Net-Net SD employs specialized hardware to inspect RTP and RTCP flows while maintaining wire-speed packet forwarding. QoS metrics including jitter, latency and packet loss are collected and reported on a per-session basis, per call-leg basis. These metrics are reported through real-time RADIUS records along with call accounting data. The source of poor quality can be isolated in terms of the source, service provider and the destination network. Acme Packet plans to release this functionality for general availability in Release 2.0.

  Reported QoS data includes the following per-flow metrics:

  - RTP Lost Packets
  - RTP Jitter
  - RTP Maximum Jitter
  - RTCP Lost Packets
  - RTCP Jitter
  - RTCP Latency

- RTCP Maximum Jitter
- RTCP Maximum Latency
- Total packets sent and received
- Total octets sent and received

Signaling Quality

Signaling quality refers to the time it takes to setup a call and the overall call completion rate for traffic to a particular destination.

- **Post-Dial Delay**—Measured as the time it takes from initiating a call and receiving acknowledgment that the far-end device ringing.
- **Call Setup Delay**—Measured as the time it takes to setup a call and receive acknowledgment that the far end has accepted the call (e.g., answer)
- **Answer-seizure ratio (ASR)**—Measured as the ration of calls answered proportional to the total number of calls attempted for a given traffic flow.

The Acme Packet Net-Net SD's call accounting (RADIUS) and network management (SNMP) functions provide the performance data needed for service providers to monitor these signaling quality metrics.

SIP Server Failure Detection

The Acme Packet Net-Net SD provides additional service availability benefits by monitoring the availability of IP network based elements such as IP-PBX's and/or application servers. The SD regularly polls each SIP server using SIP OPTIONS (or other user defined method) to determine its availability. In the event of a SIP server failure, the SD routes all traffic to alternate server(s).

External Policy Decision Function

Standards bodies and forums defining the architecture for policy control and end-to-end QoS in the carrier world that are also followed in the enterprise may include 3GPP, PacketCable, ETSI TISPAN, ITU-T and the MSF. Each standards body uses slightly different terminology, interface definitions and physical realizations; however the fundamental principles and architecture are very similar.

All architectures share the same fundamental principles and goals:

- A Uniform end-to-end network resource control plane to provide admission control, QoS guarantees and control access to network resources.
- A new function, let's call it PDF to be generic, to separate network resource control from application specific vertical interfaces

- Provide applications with a common resource allocation interface, abstracting the network complexities from higher level applications.
- Develop standardized interfaces.

A key function in each architecture is know as Bandwidth Manager, Bandwidth Broker, QoS Manager, QoS controller, Resource Manager, Resource Admission Controller, Policy Server, Policy Decision function (PDF), etc. For the sake of this discussion, we refer to this function as the PDF.

The Acme Packet Net-Net SD logically incorporates session control functions (B2BUA, IMS P-CSCF and IWF), the SPDF (Service Policy Decision Function) and the bearer control or Border Gateway Function (BGF). As the first signaling entity in the service delivery network, the Net-Net SD performs admission control in conjunction with the external PDF. Upon receiving a session requests (for example, SIP INVITE) , the Net-Net SD formulates and sends a bandwidth request with a QoS flow-spec to the PDF to request network and QoS resources. Based on the response from the PDF, the SD either forwards the request or rejects the request with the appropriate status code (for example, "503 Service Unavailable").

Details on the configuration parameters associated with these techniques can be found in any *Acme Packet Net-Net ACLI Configuration Guide*, which is available from Acme Packet, http://www.acmepacket.com/default.asp.

Configuring Enterprise Edge Devices

It is recommended that all your customers' premise site use a traffic shaping/ QOS management gateway. This is to guarantee that the video traffic is well managed within your network. Polycom has tested two gateways:

- U4EA Fusion 200/500
- Edgewater 200/4500T

The topics in this section include:

- Configuring the U4EA Fusion 200/500
- Configuring the Edgewater EdgeMarc 200/4500T

Note

The configuration information in the following pages is based upon a simple setup with most of the default settings unchanged. Advanced settings can be found in at the U4EA support site at http://www.u4eatech.com/downloads and at the Edgewater knowledgebase site at http://portal.knowledgebase.net/?cid=4739&c=4601&cpc=5GRJ7U2h1JFMjxc4w263d7PPk3g4QY1m respectively.

Configuring the U4EA Fusion 200/500

The U4EA Fusion 200/500 enterprise edge device is a multi-service business gateways (MSBGs) that delivers voice, video, data, and security services. Fusion Business Gateways provide firewall, NAT, VPN support, multiple WAN interface types, and emergency connections to the PSTN.

The topics in this section include:

- Network Layout
- Fusion MSBG Configuration
- Connecting Polycom VVX 1500 Phones to the Network

Network Layout

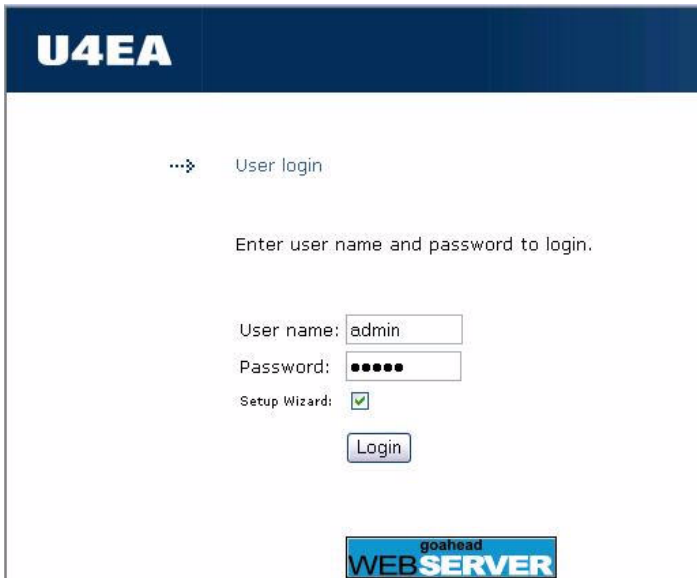
Connect the LAN port on your computer to a switch port on the Fusion MSBG. The computer will automatically receive an IP in the range 192.168.1.50 - 192.168.1.250 .

Fusion MSBG Configuration

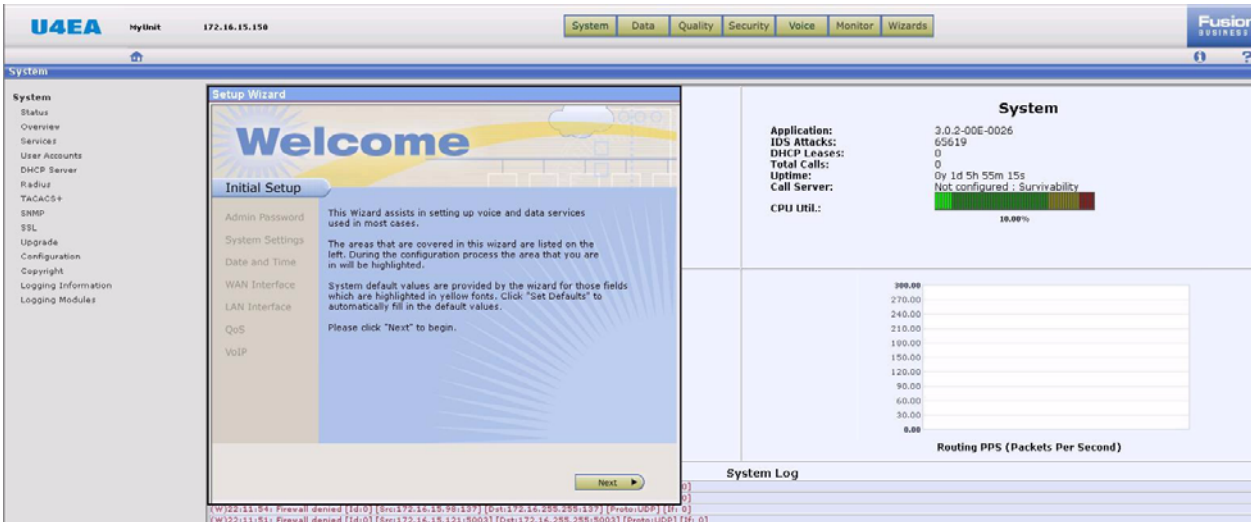
To configure the Fusion MSBG, use the built-in Web UI. Supported web browsers are Microsoft Internet Explorer 7.0 or higher and Mozilla Firefox 1.5 or higher.

To log in to the Fusion MSBG Web UI and launch the Initial Setup Wizard:

1. In your computer's web browser, enter http://192.168.1.1 .
2. On the Login page, enter **admin** for both the Username and Password, select the **Setup Wizard** check box, and then click the **Login** button.

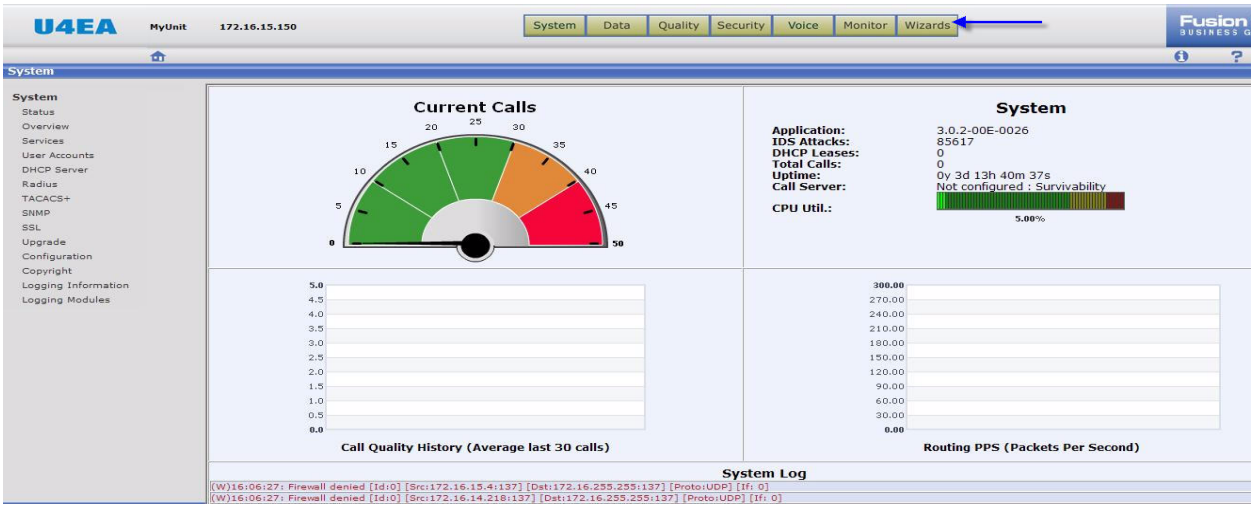


The Fusion Web UI home page opens and the Setup Wizard is launched automatically.



Note

Alternately, you can launch the Initial Setup Wizard after logging in by clicking on **Wizards > Initial Setup** as show below. This will start the Initial Setup Wizard in a new window. You may need to allow popups in your browser in case the new window does not open right away.

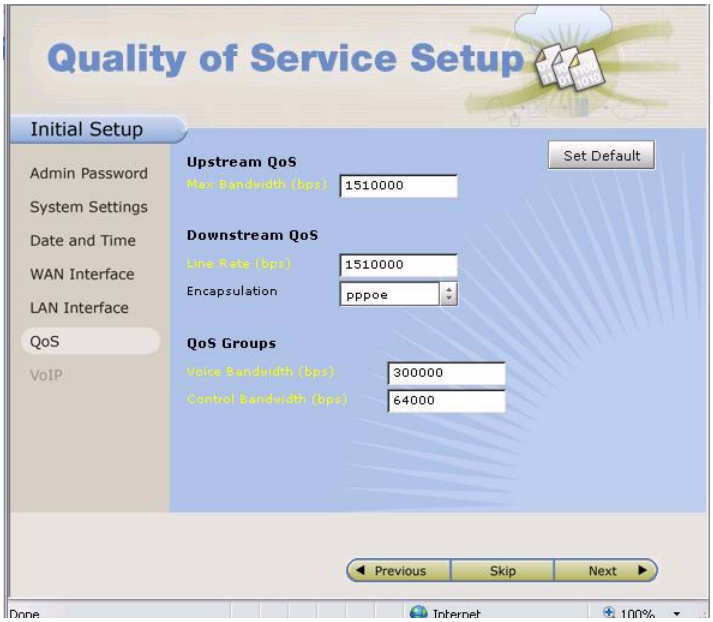


To configure QoS settings:

1. Click the **Next** button on the Wizard screen to advance to the next screen.

   You can change settings on the **Admin Password**, **System Settings**, **Date and Time**, **WAN Interface** and **LAN Interface** screens, and then click the

Next button or just click on **Skip** to advance to the next screen without making any changes.



2. On the **QoS** screen, do the following:

   a Enter the **Upstream** and **Downstream** bandwidth in bits per second (bps) if it is an Ethernet WAN interface (on Fusion 200 or 500).

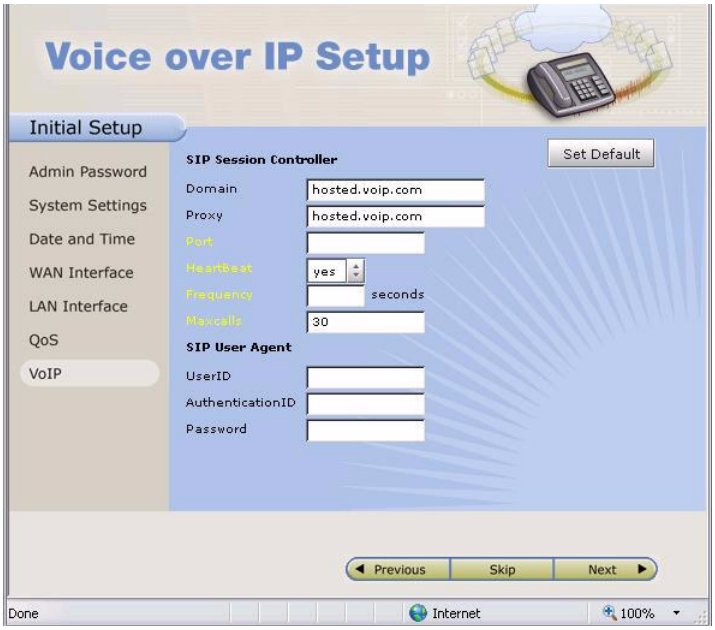
   b Select the type of **Encapsulation** used on the WAN link. If it is an ADSL or T1/E1 WAN interface (on Fusion 210, 420 or 500), Upstream/Downstream/Encapsulation information is populated automatically based on the WAN interface configuration.

   c Enter the amount of WAN bandwidth required for voice traffic in bps in the **Voice Bandwidth** field.

   d Enter the **Control Bandwidth** for traffic such as PPP, Frame Relay LMI, and ARP to at least 64000 bps.

To configure the SIP session controller:

1. Click the **Next** to advance to the VoIP screen.

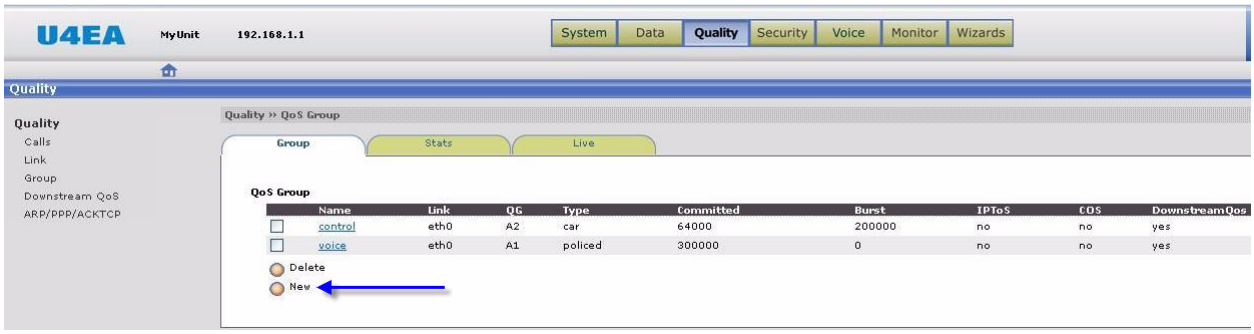


2. On the **Voice over IP Setup** screen, do the following:
   – Enter the Domain and Proxy addresses given by the Service Provider.
3. Click the **Next** to advance to the final screen, click the **save** button, and then click the **Finish** button to close the wizard.

This completes the basic configuration of the Fusion MSBG using the Initial setup Wizard.

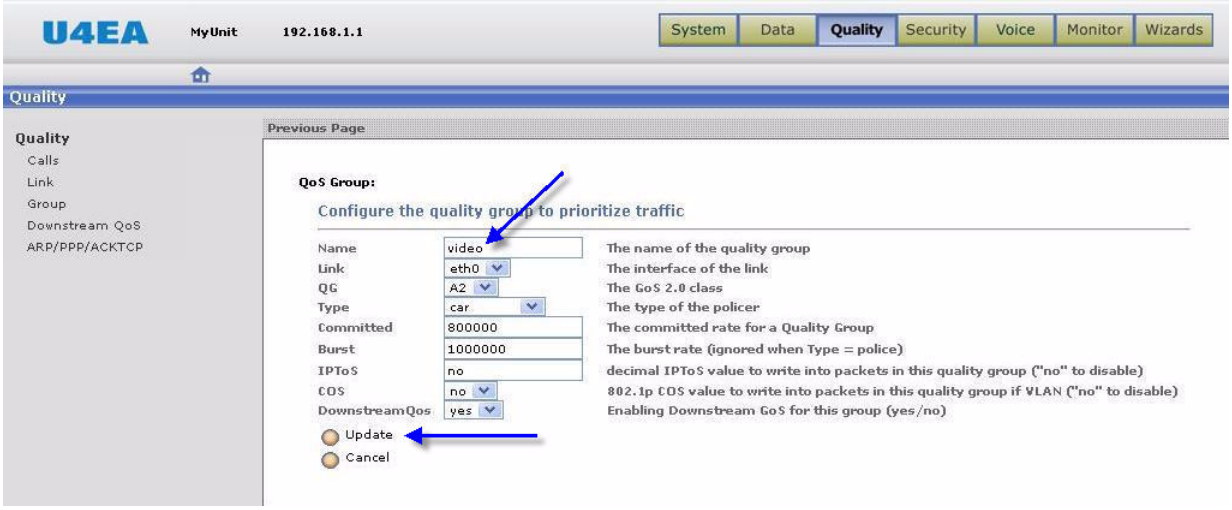
To configure a QoS group for video traffic:

1. Click on **Quality > Group > New**.



2. Enter **video** as the name of the group.

   You must use this exact name for this group; otherwise QoS for video will not work properly.



3. Do the following:

   a Select **A2** as the **QC** (Quality Group) type.

   b Select **car** as the policer **Type**.

   QG type A2 puts video at the same delay priority as the voice traffic in class A1, but at a lower loss priority.

   The Committed Access Rate (CAR) policer accommodates variable bit rate video codes by providing a combination of a committed rate i.e. guaranteed bandwidth and a burst rate.

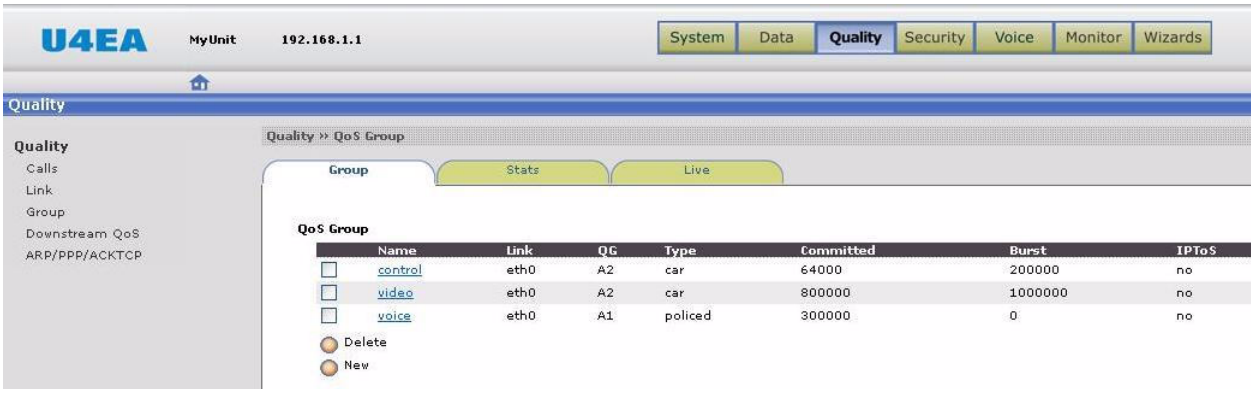
   c Enter values for the **Committed** Rate and **Burst** Rate in bits per second (bps).

   d Select **yes** to enable **Downstream QoS**.

   The Committed Rate should be set to the average bandwidth required for all video calls and the Burst Rate should be set to the maximum bandwidth required for all video calls.

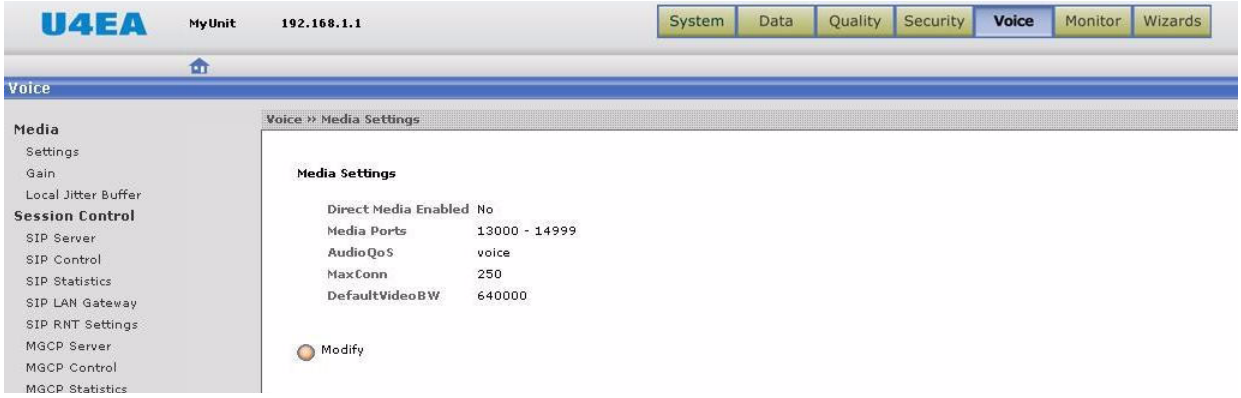
Note The voice streams accompanying the video calls are not included here, since those are handled in the **Voice** QoS group.

4. Click on **Update** to create the QG for video.



Note

The current Fusion MSBG software provides automatic QoS for VVX video calls. Voice and video traffic is prioritized separately through the respective A1 and A2 QGs. However, this software has only basic video Call Admission Control (CAC) based on the assumption of a fixed video bandwidth per call. This **default video bandwidth** is set to 640 kbps and it can be modified via **Voice > Media > Settings > Modify**. The video CAC mechanism will be improved in future software releases to take the actual video bandwidth per call into account.



5. Click the **Save Changes** button to save the configuration changes.

Connecting Polycom VVX 1500 Phones to the Network

Connect the Polycom VVX 1500 phones to the Fusion MSBG either directly or indirectly via an Ethernet switch and power them up.

Note It is assumed that the configuration files for all the phones are already available on the provisioning server (**configserver.voip.com**) in the Service Provider network.

The phones will discover the address of the server via DHCP option 66/160 and will download and get configured automatically. The list of registered phones can then be viewed on the Fusion MSBG under **Voice > SIP Control > Endpoints**. The phones should now be ready for use for calling internal (office) and external numbers.

To test the setup:

- Pick up one of the VVX phones and call the number of an external Polyom VVX 1500 or another video phone.
- Call one of the Polycom VVX 1500 phones from an external Polycom VVX 1500 or another video phone.

Configuring the Edgewater EdgeMarc 200/4500T

The EdgeMarc 200 or 4500 Series combines multiple voice and data features into a single, ease to use network services gateway. It includes choice of ADSL or single to 4 T1 Ethernet WAN interfaces. It also includes a 4 port managed VLAN switch and integrated analog phone and line ports. In addition, an optional Wireless Access Point (WAP) is available. Among other benefits, it provides cost savings through ease of deployment, management, and robust converged voice and data network security. It is an ideal platform for Service Providers offering hosted Voice over IP (VoIP), SIP Trunking, and other managed services for Small Office/Home Office (SOHO) and small to medium enterprise deployment environment. The 200 or 4500 Series contains models that support 2, 5, 10 or 30 concurrent WAN VoIP calls.

The topics in this section include:

- EdgeMarc 200/4500T Configuration
- Test the Setup

EdgeMarc 200/4500T Configuration

Refer to the Edgewater 200 and 4500 Series Converged Networking Router Quick Start Guides and become familar with your Edgewater device. The Edgewater Edgemarc 4500 Quick Start Guide is available from http://portal.knowledgebase.net/utility/getfile.asp?rid=37160 .

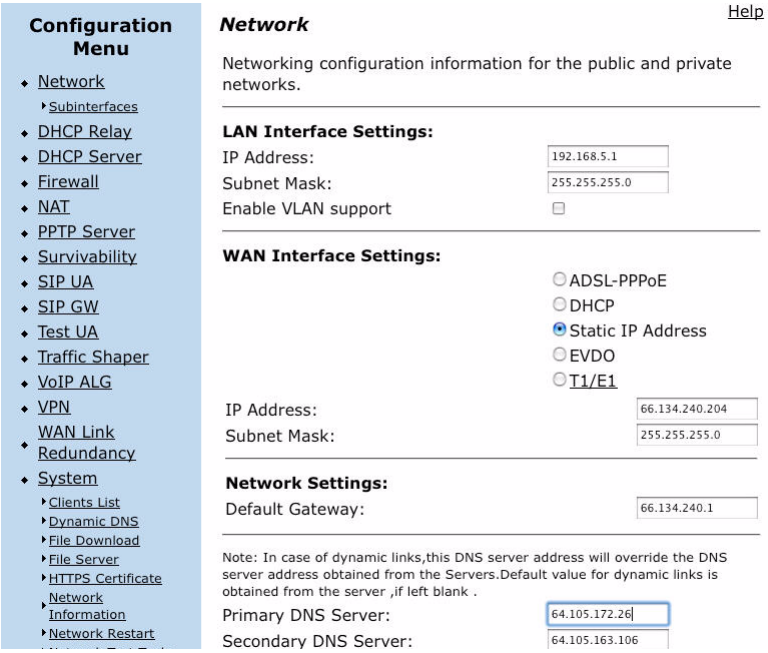
To configure the Edgewater 200/4500T, use the built-in Web UI. Supported web browsers are Microsoft Internet Explorer 7.0 or higher and Mozilla Firefox 1.5 or higher.

To log in to the Edgewater 200/4500T Web UI:

1. In your computer's web browser, enter http://192.168.1.1 .
2. On the Login page, enter **root** for the Username and **default** for the Password, and then click the **Login** button.

To configure the network settings:

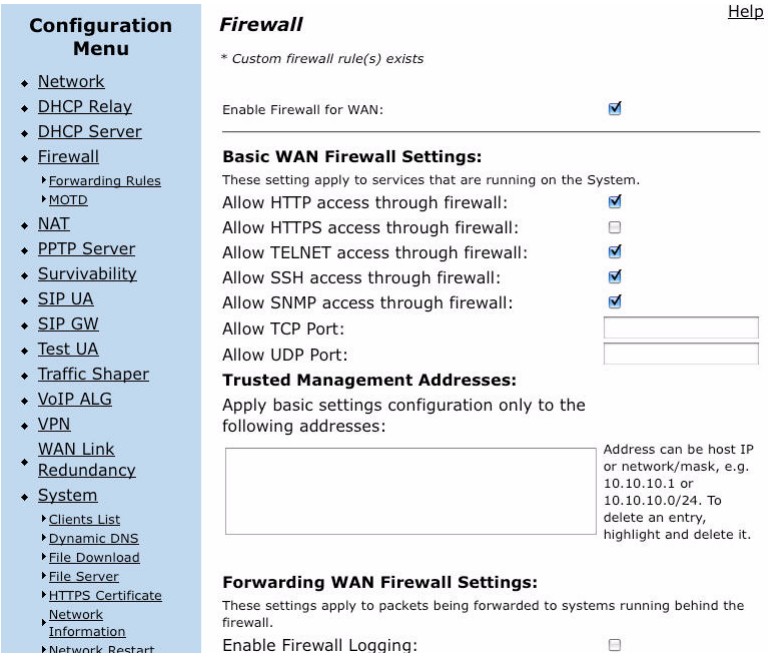
1. Click the **Network** link.



2. Enter values as directed by your ISP.

To configure the firewall settings:

1. Click the **Firewall** link.

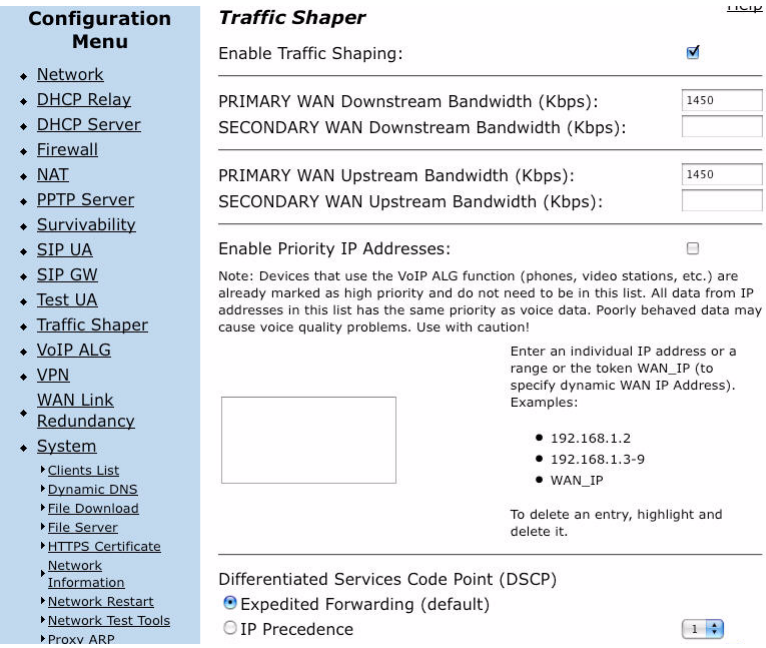


2. Enter appropriate values.

   Most users will turn on the Edgewater Edgemarc firewall. To access the Edgemarc remotely, select the protocols you want to allow.

To configure the traffic shaper:

1. Click the **Traffic Shaper** link.

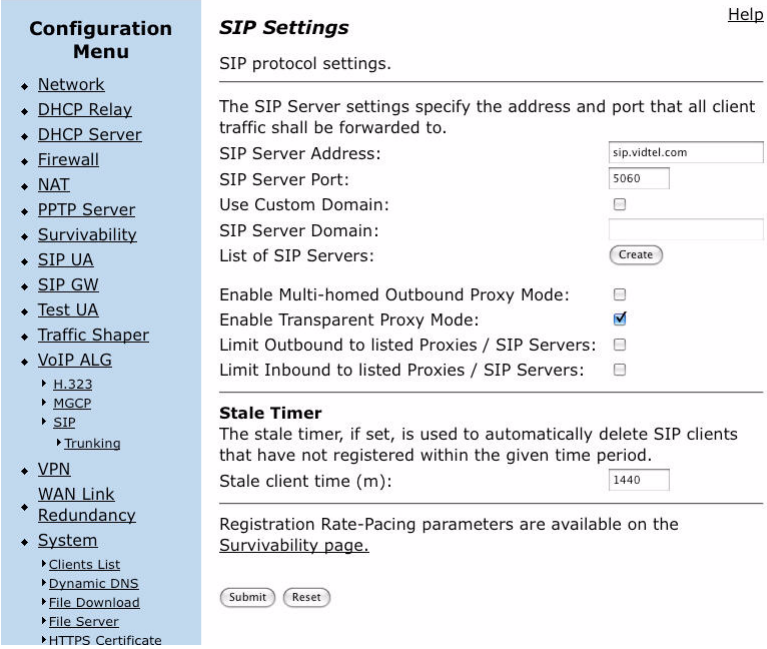


2. Enter values for **Primary WAN Downstream Bandwidth** and **Primary WAN Upstream Bandwidth** in Kbps.

   Refer to this Edgewater Knowledge Dbase article on tips on how to determine proper bandwidth settings: http://portal.knowledgebase.net/article.asp?article=105099&p=4739

To configure VoIP settings:

1. Click the **VoIP ALG** link, then click the **SIP** link.



2. Enter the ITSP SIP settings (**sip.xxxx.com** and port 5060).
3. Select the **Enable Transparent Proxy Mode** check box.
4. Click the **Submit** button.

   A message indictating that service will be temporarily interrupted appears.
5. Click the **OK** button to confirm.

Test the Setup

You should run a simple test for verify their IP network. The ITSP can license one or you can use http://www.testyourIPvideo.com as a free IP assessment tool.

Configuring the Polycom VVX 1500 Phone

Refer to the latest *SIP Administrator's Guide*, available at http://www.polycom.com/global/documents/support/setup_maintenance/products/voice/VVX1500_spip_ssip_SIP_3_1_2RevB_admin_guide.pdf to become familar with the Polycom VVX 1500 configuration parameters.

In particular, you should review the following parmeters if you are in a low bandwidth environment:

Attribute	Permitted Values	Default	Interpretation
video.maxCallRate	128 - 1024 kbps	Null	Limits the maximum network bandwidth used in a call. It is used in the SDP bandwidth signaling. If honored by the far end, both Rx and Tx network bandwidth used in a call will not exceed this value (in kbps). If set to Null, the value 448 is used.
video.camera.frameRate	5 to 30 frames per second	Null	Set target frame rate. Values indicate a fixed frame rate, from 5 (least smooth) to 30 (most smooth). If set to Null, the value 25 is used.

Trademark Information