Trademark Information

Polycom®, the Polycom logo design, [and others that appear in your document] are registered trademarks of Polycom, Inc. [List other trademarks]™ are trademarks of Polycom, Inc. in the United States and various other countries. All other trademarks are the property of their respective owners.
Contents

Introduction ................................................................. 1–1
   The V2iU 5300-E Series Converged Network Appliance .......... 1–1
   Features ................................................................. 1–1
   Front Panel ............................................................. 1–2
      LAN Ethernet port .................................................. 1–2
      WAN Ethernet port ............................................... 1–2
      Out of Band management port .................................. 1–2
      Console port ......................................................... 1–3

Getting Started ............................................................ 2–1
   Physical Installation ................................................... 2–1
   Connecting to the 5300-E ........................................... 2–1

Configuring the 5300-E .................................................... 3–1
   Configuration Guide For IP Centrex Applications ................. 3–1
      Configuration ......................................................... 3–3
   Configuration Guide For Station Side IP PBX Applications .... 3–4
      Configuration Outline ............................................. 3–5
   Configuration Guide For Trunk Side IP PBX Applications ....... 3–6
      Configuration Outline ............................................. 3–7
   Configuration Guide For Hosted Video Applications .............. 3–8
   Configuration Guide For Enterprise Video Applications ......... 3–10
   System Configuration .................................................. 3–12
      Configure the WAN Interface ...................................... 3–12
      Configure the LAN Interface ...................................... 3–13
         Set Ethernet Link Rate .......................................... 3–13
         Set WAN MTU size ............................................... 3–14
      Configure the DHCP Server ....................................... 3–15
      Delete a DHCP IP Address ........................................ 3–16
      Disable the DHCP Server ......................................... 3–17
      Configure SNMP .................................................... 3–17
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Static NAT</td>
<td>3–57</td>
</tr>
<tr>
<td>Delete a Static NAT entry</td>
<td>3–57</td>
</tr>
<tr>
<td>Static IP routing</td>
<td>3–58</td>
</tr>
<tr>
<td>Configure the static route</td>
<td>3–58</td>
</tr>
<tr>
<td>Delete the static route</td>
<td>3–58</td>
</tr>
<tr>
<td>Firewall Configuration</td>
<td>3–59</td>
</tr>
<tr>
<td>Enable or disable the firewall</td>
<td>3–59</td>
</tr>
<tr>
<td>Configure Basic Settings</td>
<td>3–60</td>
</tr>
<tr>
<td>Configure Advanced Settings</td>
<td>3–60</td>
</tr>
<tr>
<td>Remove Advanced Setting Entries</td>
<td>3–62</td>
</tr>
<tr>
<td>Traffic Management Configuration</td>
<td>3–62</td>
</tr>
<tr>
<td>Enable Traffic Shaping</td>
<td>3–63</td>
</tr>
<tr>
<td>A Closer Look at Traffic Management in the 5300-E</td>
<td>3–66</td>
</tr>
<tr>
<td>Classifying</td>
<td>3–66</td>
</tr>
<tr>
<td>Upstream Traffic Management</td>
<td>3–66</td>
</tr>
<tr>
<td>Downstream Traffic Management</td>
<td>3–66</td>
</tr>
<tr>
<td>System Diagnostics</td>
<td>4–1</td>
</tr>
<tr>
<td>Viewing Software Version, Hardware Platform and the LAN MAC Address</td>
<td>4–1</td>
</tr>
<tr>
<td>Viewing the ALG registration code</td>
<td>4–1</td>
</tr>
<tr>
<td>Enter the Registration Code</td>
<td>4–2</td>
</tr>
<tr>
<td>Viewing Networking Information</td>
<td>4–2</td>
</tr>
<tr>
<td>Routing Information</td>
<td>4–3</td>
</tr>
<tr>
<td>Link Status</td>
<td>4–3</td>
</tr>
<tr>
<td>Interface Information</td>
<td>4–3</td>
</tr>
<tr>
<td>Viewing Advanced System Information</td>
<td>4–4</td>
</tr>
<tr>
<td>System Uptime</td>
<td>4–4</td>
</tr>
<tr>
<td>Process Information</td>
<td>4–4</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>4–4</td>
</tr>
<tr>
<td>System Logging Messages</td>
<td>4–5</td>
</tr>
<tr>
<td>Passive Voice Call Monitoring</td>
<td>4–5</td>
</tr>
<tr>
<td>Accessing Troubleshooting Tools</td>
<td>4–5</td>
</tr>
<tr>
<td>Verify Registered Voice Devices</td>
<td>4–6</td>
</tr>
<tr>
<td>Performing a Ping Test</td>
<td>4–7</td>
</tr>
<tr>
<td>Performing a Traceroute Test</td>
<td>4–7</td>
</tr>
<tr>
<td>Performing a VoIP Traffic Test</td>
<td>4–8</td>
</tr>
<tr>
<td>Restarting Networking Processes</td>
<td>4–9</td>
</tr>
<tr>
<td>Rebooting the 5300-E</td>
<td>4–9</td>
</tr>
</tbody>
</table>
Saving and Restoring the 5300-E Configuration . . . . . . . . . . 5–1
  The ewn Command ...................................................... 5–1
  Create a Backup File and Save in Local Flash .................. 5–2
  Copy a Backup File to a Remote TFTP Server ................... 5–2
  Download a Backup File from a Remote TFTP Server .......... 5–2
  List the Available Backup Files ..................................... 5–2
  Delete a Backup File .................................................. 5–3
  Load a Backup File so that it Becomes the Running Configuration . 5–3

Upgrading the 5300-E .................................................. 6–1
  Upgrade Procedure for Software Revision 1.3.11 or Later .......... 6–1

Appendix ............................................................... Appendix–1
  Troubleshooting Tips ................................................ Appendix–1
  Specifications ......................................................... Appendix–2

Regulatory Notices .................................................... Regulatory Notices–1
  END-USER LICENSE AGREEMENT FOR POLYCOM® SOFTWARE . Regulatory Notices–1
  FCC PART 15 NOTICE ........................................... Regulatory Notices–11
  Industry Canada NOTICE ........................................... Regulatory Notices–11
Introduction

The V2IU 5300-E Series Converged Network Appliance

The V2IU 5300-E Series is a new generation of edge device providing the demarcation point for real-time, interactive IP services. It is the ideal solution for connecting enterprise PCs and IP Phones to a private or public IP network. It replaces multiple standalone systems by integrating voice-over-IP (VoIP), network security, traffic management and voice call monitoring into a low-cost, easily managed device.

Use the 5300-E to ensure high quality voice and video calls, maximize WAN link utilization for data traffic and protect the enterprise LAN from network based attacks.

Features

- Resolves NAT/firewall traversal problems for VoIP by providing a VoIP application layer gateway (ALG) that supports SIP, MGCP and H.323
- Supports up to 300 concurrent VoIP calls or up to 25 Mbps of any combination of voice, video, or data traffic
- Protects the enterprise LAN using a stateful packet inspection (SPI) firewall
- Provides NAT and PAT for voice and data
- Performs static IP routing
- Performs traffic management including prioritization, classification, queuing, TOS bit setting and call admission control for voice
- Provides voice call quality monitoring and testing
- Provides integrated test tools to facilitate problem isolation
- Provides a DHCP server for enterprise PCs and IP phones
- Performs TFTP relay for IP phone images
Uses a simple web based GUI for configuration and management

- Supports logging to external syslog servers and interfaces to network management systems using SNMP

Front Panel

The front panel of the 5300-E contains the following:

- Power switch
- LAN Ethernet ports (labeled “Port 1”)
- WAN Ethernet port (labeled “Port 2”)
- Optional out of band management Ethernet port (labeled “Port 3”)
- Console port
- Green power LED (illuminated when power is applied to the system)
- Red flash LED (Indicates compact flash read or write activity)
- Video port (not used)

LAN Ethernet port

The LAN Ethernet port (labeled “Port 1”) is a 10/100 auto sensing port that should be connected via an ethernet switch to IP phones, IADs or PCs installed on the local area network (also known as the private network).

WAN Ethernet port

The WAN Ethernet port (labeled “Port 2”) is a 10/100 auto sensing port that should be connected to the wide area network (also known as the public network) through a WAN termination device such as an xDSL modem or router.

Out of Band management port

This port can be configured to allow out of band management sessions with the 5300-E series. It is typically connected to a private management network.
Console port

This port is used to establish a local console session with the 5300-E using a VT100 terminal or emulation program. The baud rate is 9600. It is used for debug or local diagnostic purposes only. Primary configuration of the 5300-E is performed from a web browser as covered in “Chapter 3: Configuring the 5300-E”. 

1 - 3
Getting Started

Physical Installation

The 5300-E is designed for 19” rack mount installation. Please observe the following guidelines when installing the system:

• Never assume that the AC cord is disconnected from a power source. Always check first.

• Never place objects greater than 5 lbs on top of the 5300-E as damage to the chassis may result.

• Always connect the AC power cord to a properly grounded AC outlet to avoid damage to the system or injury.

• Ensure that the physical location of the installation has adequate air circulation and meets the minimum operating conditions as provided in the environmental specifications for the system.

Connecting to the 5300-E

The 5300-E is configured using a web browser such as Internet Explorer or Netscape Navigator. The 5300-E is shipped with a pre-configured IP address for its LAN port of 192.168.1.1. To connect to the 5300-E, do the following:

1. Connect a PC using an IP address of 192.168.1.2 and subnet mask of 255.255.255.0 to the 5300-E LAN port or the LAN switch associated with the 5300-E LAN port.
2. Launch a web browser on the PC and enter the URL string: 192.168.1.1. Press Return. The initial 5300-E main configuration menu appears.

3. Select the Network link - enter the username root and the password default to log into the system.

4. Continue to configure the system using the information provided in “Chapter 3: Configuring the 5300-E”.
Configuring the 5300-E

The 5300-E is a flexible, easy to use converged network appliance that provides many critical networking functions for IP based voice and data. It can be installed in several different topologies:

- At the customer premise for IP Centrex applications
- At the station side of enterprise IP PBXs
- At the trunk side of enterprise IP PBXs

Most users will follow the steps provided in the System Configuration section of this manual to initially connect the 5300-E into their IP network. The remainder of the configuration can be different based on the application, VoIP topology and presence of other networking equipment such as firewalls or DHCP servers. In general, however, the steps used to configure the 5300-E are:

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>System configuration</td>
</tr>
<tr>
<td>2</td>
<td>VoIP configuration</td>
</tr>
<tr>
<td>3</td>
<td>Data networking configuration</td>
</tr>
<tr>
<td>4</td>
<td>Firewall configuration</td>
</tr>
<tr>
<td>5</td>
<td>Traffic management configuration</td>
</tr>
</tbody>
</table>

Some of the steps are optional depending on your particular application. We have provided configuration guidelines below for each of the application types supported by the 5300-E.

Configuration Guide For IP Centrex Applications

A typical 5300-E installation for an IP Centrex application uses an external router to terminate or the 5300T or 300T2 with an integrated CSU/DSU to terminate the WAN link from the service provider. VoIP signaling is
performed in the service provider network via a softswitch and the 5300-E acts as a proxy for the voice devices installed in the enterprise LAN. In this configuration a single public IP address is used to proxy for all of the IP phones and to route to multiple PC’s installed on the LAN. This particular example also uses static NAT entries to route to the publicly addressable servers. The 5300-E performs the following functions in this application:

- WAN/LAN IP routing.
- Traffic shaping and priority queuing to guarantee high quality voice traffic. These mechanisms protect voice and data traffic from contending for the same network resources to guarantee low latency and the highest call quality possible for VoIP traffic. At the same time they ensure the best utilization of WAN bandwidth by enabling data traffic to burst up to full line rate in the absence of voice calls. Precedence is given to traffic for the range of addresses reserved for the IP phones.
- NAT/PAT translation for IP phones and PC’s. This allows a single public IP address to be used on the WAN link to represent all of the private IP addresses assigned to the LAN IP phones and PC’s.
- Static NAT entries. This enables the customer to use a WAN public IP address for data servers (web, mail, ftp, etc.) connected behind the 5300-E. These servers can then be configured with private IP addresses for additional security.
- A “VoIP” aware firewall. A full layer 7 gateway for voice traffic and a stateful packet inspection firewall for data traffic.
- Call Admission Control (CAC). CAC uses a deterministic algorithm to decide when there are insufficient network resources available to adequately support new calls and then return the equivalent of a “fast busy” to new call requests.
- DHCP server and TFTP relay. These features are used to simplify and expedite the IP configuration of phones and PC’s. This also includes VoIP signaling gateway information (MGCP, SIP, and H.323).
• Call quality monitoring and test tools.

**Configuration Outline**

<table>
<thead>
<tr>
<th>Task</th>
<th>Subtask</th>
<th>Configure For IP Centrex Application?</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Configuration</td>
<td>configure LAN/WAN interface</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>set Ethernet link rate</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>enable the DHCP server</td>
<td>Optional but recommended</td>
</tr>
<tr>
<td></td>
<td>configure SNMP</td>
<td>Optional</td>
</tr>
<tr>
<td>VoIP Configuration</td>
<td>enable the VoIP ALG</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>configure a VoIP subnet route</td>
<td>Optional</td>
</tr>
<tr>
<td>Data Networking Configuration</td>
<td>dynamic NAT</td>
<td>Optional but recommended</td>
</tr>
<tr>
<td></td>
<td>static NAT</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>static IP routing</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Most private enterprise VoIP networks use an IP PBX at the corporate headquarters location to provide voice switching between headquarters, branch offices and the PSTN. The 5300-E is used in these environments to securely connect branch office employees to the IP PBX installed in the corporate headquarters location.
The installation of an 5300-E on the station side of an enterprise IP PBX is very similar to the IP Centrex application above. The branch office is connected to the corporate network using VPNs or private T1 links terminated by a WAN router. The 5300-E is then connected directly to the WAN router and the LAN port of the 5300-E is connected to the enterprise ethernet local area network (typically a layer 2 switch). The IP PBX in the corporate headquarters location performs VoIP signaling and the 5300-E acts as a proxy for the voice devices installed at the branch office. The 5300-E can perform the following functions in this application:

- WAN/LAN IP routing.
- Traffic shaping and priority queuing to guarantee high quality voice traffic. These mechanisms protect voice and data traffic from contending for the same network resources to guarantee low latency and the highest call quality possible for VoIP traffic. At the same time they ensure the best utilization of WAN bandwidth by enabling data traffic to burst up to full line rate in the absence of voice calls. Precedence is given to traffic for the range of addresses reserved for the IP phones.
- NAT/PAT translation for IP phones and PC’s. This allows a single IP address to be used on the WAN link to represent all of the private IP addresses assigned to the LAN IP phones and PC’s.
- A “VoIP” aware firewall. A full layer 7 gateway for voice traffic and a stateful packet inspection firewall for data traffic.
- Call Admission Control (CAC). CAC uses a deterministic algorithm to decide when there are insufficient network resources available to adequately support new calls and then return the equivalent of a “fast busy” to new call requests.
- DHCP server and TFTP relay. These features are used to simplify and expedite the IP configuration of phones and PC’s. This also includes VoIP signaling gateway information (MGCP, SIP, and H.323).
- Call quality monitoring and test tools.

### Configuration Outline

<table>
<thead>
<tr>
<th>Task</th>
<th>Subtask</th>
<th>Configure For Station Side IP PBX Application?</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Configuration</td>
<td>configure LAN/WAN interface</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>set Ethernet link rate</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>enable the DHCP server</td>
<td>Optional but recommended</td>
</tr>
<tr>
<td></td>
<td>configure SNMP</td>
<td>Optional</td>
</tr>
<tr>
<td>VoIP Configuration</td>
<td>enable the VoIP ALG</td>
<td>Yes</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------</td>
<td>-----</td>
</tr>
<tr>
<td></td>
<td>configure a VoIP subnet route</td>
<td>Optional</td>
</tr>
<tr>
<td>Data Networking Configuration</td>
<td>dynamic NAT</td>
<td>Optional but recommended</td>
</tr>
<tr>
<td></td>
<td>static NAT</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>static IP routing</td>
<td>Optional</td>
</tr>
<tr>
<td>Firewall Configuration</td>
<td>enable the data firewall</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>configure basic settings</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>configure advanced settings</td>
<td>Optional</td>
</tr>
<tr>
<td>Traffic Management Configuration</td>
<td>enable traffic shaping</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>enable Call Admission Control</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**Configuration Guide For Trunk Side IP PBX Applications**

Companies using shared WAN links for inter-office IP voice communications can use the 5300-E as a traffic shaper to meet the stringent jitter, latency and packet loss requirements for toll quality voice. The 5300-E is deployed in the network between WAN and LAN connections in headquarters and branch office locations. One appliance is required for each end of a WAN link and they are installed logically between IP PBX trunk interfaces.

The 5300-E performs WAN/LAN IP routing and traffic management functions in this application.
## Configuration Outline

<table>
<thead>
<tr>
<th>Task</th>
<th>Subtask</th>
<th>Configure For Trunk Side IP PBX Application?</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Configuration</td>
<td>configure LAN/WAN interface</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>set Ethernet link rate</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>enable the DHCP server</td>
<td>Not required</td>
</tr>
<tr>
<td></td>
<td>configure SNMP</td>
<td>Optional</td>
</tr>
<tr>
<td>VoIP Configuration</td>
<td>enable the VoIP ALG</td>
<td>Not required</td>
</tr>
<tr>
<td></td>
<td>configure a VoIP subnet route</td>
<td>Not required</td>
</tr>
<tr>
<td>Data Networking Configuration</td>
<td>dynamic NAT</td>
<td>Not required</td>
</tr>
<tr>
<td></td>
<td>static NAT</td>
<td>Not required</td>
</tr>
<tr>
<td></td>
<td>static IP routing</td>
<td>Not required</td>
</tr>
<tr>
<td>Firewall Configuration</td>
<td>enable the data firewall</td>
<td>Not required</td>
</tr>
<tr>
<td></td>
<td>configure basic settings</td>
<td>Not required</td>
</tr>
<tr>
<td></td>
<td>configure advanced settings</td>
<td>Not required</td>
</tr>
<tr>
<td>Traffic Management</td>
<td>enable traffic shaping</td>
<td>Yes</td>
</tr>
<tr>
<td>Configuration</td>
<td>enable Call Admission Control</td>
<td>Not required</td>
</tr>
</tbody>
</table>
Configuration Guide For Hosted Video Applications

A typical 5300-E installation for hosted video applications is depicted in the diagram below. In this scenario, the 5300-Es are used to connect all of the video endpoints to the Gatekeeper. The video endpoints should be configured to point to the LAN address of the 5300-E as the Gatekeeper and the 5300-E will proxy RAS and call setup messages to the Gatekeeper.

The 5300-E is installed at the customer premises and is used as a demarcation point for the video service by providing the following functions:

- WAN/LAN IP routing.
• Traffic shaping and priority queuing to guarantee high quality video traffic. These mechanisms protect video and data traffic from contending for the same network resources to guarantee low latency and the highest call quality possible for voice and video traffic. At the same time they ensure the best utilization of WAN bandwidth by enabling data traffic to burst up to full line rate in the absence of video calls. Precedence is automatically given to traffic coming from video endpoints and other devices using the 5300-E’s Application Layer Gateway function.

• Video NAT/PAT translation for video endpoints and PC’s. This allows a single IP address to be used on the WAN link to represent all of the private IP addresses assigned to the LAN video endpoints and PC’s.

• A video aware firewall. A full layer 7 gateway for video traffic and a stateful packet inspection firewall for data traffic

• Call Admission Control (CAC). CAC uses a deterministic algorithm to decide when there are insufficient network resources available to adequately support new video calls and then return the equivalent of a “fast busy” to new call requests.

<table>
<thead>
<tr>
<th>Task</th>
<th>Subtask</th>
<th>Configure For Hosted Video Applications?</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Configuration</td>
<td>configure LAN/WAN interface</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>set ethernet link rate</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>enable the DHCP server</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>configure SNMP</td>
<td>Optional</td>
</tr>
<tr>
<td>VoIP Configuration</td>
<td>enable the VoIP ALG</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>configure a VoIP subnet route</td>
<td>Optional</td>
</tr>
<tr>
<td>Data Networking Configuration</td>
<td>dynamic NAT</td>
<td>Optional but recommended</td>
</tr>
<tr>
<td></td>
<td>static NAT</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>static IP routing</td>
<td>Optional</td>
</tr>
<tr>
<td>Firewall Configuration</td>
<td>enable the data firewall</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>configure basic settings</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>configure advanced settings</td>
<td>Optional</td>
</tr>
<tr>
<td>Traffic Management Configuration</td>
<td>enable traffic shaping</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>enable Call Admission Control</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Configuration Guide For Enterprise Video Applications

A typical 5300-E installation for enterprise video applications is depicted in the diagram below. In this scenario, the 5300-Es are used to connect all of the video endpoints to the Gatekeeper. The video endpoints should be configured to point to the LAN address of the 5300-E as the Gatekeeper and the 5300-E will proxy RAS and call setup messages to the Gatekeeper.

The 5300-E is installed at the private/public IP address boundary and provides the following functions:

- WAN/LAN IP routing.
- Traffic shaping and priority queuing to guarantee high quality video traffic. These mechanisms protect video and data traffic from contending for the same network resources to guarantee low latency and the highest
Configuring the 5300-E

call quality possible for voice and video traffic. At the same time they ensure the best utilization of WAN bandwidth by enabling data traffic to burst up to full line rate in the absence of video calls. Precedence is automatically given to traffic coming from video endpoints and other devices using the 5300-E’s Application Layer Gateway function.

- Video NAT/PAT translation for video endpoints and PC’s. This allows a single IP address to be used on the WAN link to represent all of the private IP addresses assigned to the LAN video endpoints and PC’s.
- A video aware firewall. A full layer 7 gateway for video traffic and a stateful packet inspection firewall for data traffic
- Call Admission Control (CAC). CAC uses a deterministic algorithm to decide when there are insufficient network resources available to adequately support new video calls and then return the equivalent of a “fast busy” to new call requests.

<table>
<thead>
<tr>
<th>Task</th>
<th>Subtask</th>
<th>Configure For Hosted Video Applications?</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Configuration</td>
<td>configure LAN/WAN interface</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>set ethernet link rate</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>enable the DHCP server</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>configure SNMP</td>
<td>Optional</td>
</tr>
<tr>
<td>VoIP Configuration</td>
<td>enable the VoIP ALG</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>configure a VoIP subnet route</td>
<td>Optional</td>
</tr>
<tr>
<td>Data Networking Configuration</td>
<td>dynamic NAT</td>
<td>Optional but recommended</td>
</tr>
<tr>
<td></td>
<td>static NAT</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>static IP routing</td>
<td>Optional</td>
</tr>
<tr>
<td>Firewall Configuration</td>
<td>enable the data firewall</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>configure basic settings</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>configure advanced settings</td>
<td>Optional</td>
</tr>
<tr>
<td>Traffic Management Configuration</td>
<td>enable traffic shaping</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>enable Call Admission Control</td>
<td>Optional</td>
</tr>
</tbody>
</table>
System Configuration

This section explains how to configure the 5300-E to function in your IP network. You will configure the Ethernet interfaces, network addresses, DNS settings, default gateway, SNMP settings and change the administrative password.

Configure the WAN Interface

1. Select the Network link.
2. Select Static IP address if you want to manually assign the IP address configuration to the WAN interface.

   a. Enter the IP Address.
   b. Enter the Subnet Mask (e.g., 255.255.255.0).
   c. Enter the Default Gateway. Packets destined for IP networks not known to the 5300-E are forwarded to the default gateway for handling.
   d. Enter the Primary DNS Server. The DNS server is used by the 5300-E to resolve domain names to IP addresses. The value entered into this field is provided to IP devices that use the 5300-E as a DHCP server. The 5300-E VoIP ALG also uses it if domain names are used instead of IP addresses to identify signaling and/or TFTP servers (see the section entitled Configure the VoIP ALG for more details).
   e. Enter the Secondary DNS Server. This server will be used in the event that the primary DNS server is not reachable.
   f. Press Submit.

3. Select ADSL-PPPoE if you are connecting to the Internet using an ADSL link. The WAN IP address for the 5300-E is provided by your service provider as a part of the PPPoE protocol automatically and does not have
to be manually configured. Please contact your service provider for the PPPoE username and password as this will be required for link authentication.

**Note**
The 5300-E uses PAP authentication and you should inform your provider that this is required to ensure compatibility.

- Press Submit.
- Enter the User Name and Password.
- Press Submit. The service provider will automatically assign your WAN IP address.

4. Select DHCP if you want to receive your WAN IP address from a DHCP server located in the WAN.
5. Press Submit.

### Configure the LAN Interface

1. Select the Network link.
2. Enter the IP Address.
3. Enter the Subnet Mask (e.g. 255.255.255.0).
4. Press Submit.

**Warning**
After pressing submit the 5300-E will become unreachable until you use a PC with an address on the same subnet as entered in steps B and C above.

### Set Ethernet Link Rate

**Warning**
The vast majority of Ethernet networking devices including the 5300-E use “autonegotiate” as a default setting. Chances are that you will not have to set the ethernet link rate as described below. Please use caution if manually configuring the link rate as a speed or duplex mismatch will result in a loss of connectivity.

If needed configure the rate of the physical ethernet port on the 5300-E. The default setting for the Ethernet port is to “autonegotiate” both the link speed and duplex with locally attached devices.

1. Select System.
2. Select System Overview.
3. Select Set Link Rate.
4. Select LAN and/or WAN.
5. Select the appropriate link rate for your Ethernet network:

- 10baseT-HD = 10Mbits per second using half duplex transmission
- 10baseT-FD = 10Mbits per second using full duplex transmission
- 100baseT-HD = 100Mbits per second using half duplex transmission
- 100baseT-FD = 100Mbits per second using full duplex transmission
- Autonegotiate = The 5300-E will autonegotiate link rate and duplex with the directly attached device.

6. Press Submit.

**Set WAN MTU size**

The WAN MTU size may be set to reduce the latency that is introduced when large data packets are sent over a slow link. The default setting is 1500 bytes for static IP addresses. PPPoE links negotiate the value automatically although the value can be overridden using this field. If the WAN Upstream Bandwidth is less than 256 Kbit/s, the MTU size is automatically reduced to 800 bytes.

**Warning**

When manually configuring the MTU size we recommend that you use a setting of 800 bytes or greater. You may experience problems with certain types of VoIP traffic if the MTU size is set below 800 bytes.

1. Select System.
2. Select System Overview.
3. Enter the WAN MTU size
4. Press Submit.
Configure the DHCP Server

The 5300-E can act as a DHCP server granting IP addresses to PCs, workstations, servers or voice devices (IP phones, IADs or softphones). DHCP is a protocol that enables IP devices to obtain temporary or permanent IP addresses (out of a pool) from centrally administered servers. The user can configure blocks of IP addresses, a default gateway, DNS servers, NTP server address, Time offset from NTP value, WINS address and TFTP/FTP server name that can be served to the requesting IP devices. In addition the 5300-E will provide its LAN IP address in DHCP user options 150 and 151 for use by IP phones. Some IP phones use these values for configuration of their TFTP server and MGCP control server addresses.

1. Select DHCP Server.
2. The default value for the DHCP server is enabled.
3. Enter the Lease Duration.

   The lease duration is the amount of time in days that an IP device may use an assigned IP address before requesting that it be renewed. The default value is 7 days and the valid range of input is 1 to 300 days.
4. Enter the Subnet Mask.

   This is the subnet mask that will be sent via DHCP to the requesting IP devices.

Note

The DHCP server in the 5300-E should not be used if a DHCP server already exists in the same subnet as the 5300-E. Also, it is recommended that you assign static IP addresses for common-access devices such as network printers or fax machines.
5. Enter the DHCP IP Addresses.
   This is the pool of IP addresses that will be provided to the requesting IP devices. You can enter both individual IP addresses or a range of addresses using the following format:

   192.168.1.3-5

   where 192.168.1.3 is the starting address and 192.168.1.5 is the ending address.

   **Note** The range format can only be used for class C addresses.

6. Enter the Time Offset (DHCP user option 2).
   Set the time offset in hours from UTC for your local location.

7. Enter the NTP Server Address (DHCP user option 42).
   This is the IP address of your NTP server.

8. Enter the WINS Address.

   **Note** If you are not using WINS this field may be left blank.

   The Windows Internal Naming Service (WINS) is a service that keeps a database of computer name-to-IP address mappings so that computer names used in Windows environments can be mapped to IP addresses. The WINS Address is the IP address of the WINS server in your network.

9. Enter the TFTP/FTP Server Name (DHCP user option 66).
   Some IP phones use this setting to locate the TFTP or FTP servers which contain the phone software image used during boot. By default this option is the same as the TFTP server on the VoIP ALG page.

10. Press Submit.

## Delete a DHCP IP Address

1. Select DHCP Server.

2. To delete an IP address or a range of IP addresses highlight the entry in the DHCP IP Addresses list and press the Delete key on your keyboard.
3. Press Submit.

Disable the DHCP Server

1. Select DHCP Server.
2. Uncheck the Enable DHCP Server checkbox.
3. Press Submit.

Configure SNMP

The 5300-E can be managed remotely by an SNMP network management system such as HP Openview. The 5300-E supports SNMPv1 and MIB-II (RFC1213). All MIB-II variables are read only. The MIB variables sysContact and sysLocation are set by the web GUI.

1. Select System.
2. Select System Overview.
3. Select Services Configuration.
4. Select the Enable SNMP checkbox.
5. Enter the Read-Only Community.
   This is the community string that the management station uses when accessing read-only objects from the 5300-E. The default is 'public'.
6. Enter the System Location.
   This is a comment string that can be used to indicate the location of the 5300-E. By default, no value is set.
7. Enter the System Contact.
   This is the administrative contact information for the 5300-E. By default, no value is set.
8. Enter the SNMP Port.
   This is the port that the 5300-E uses for SNMP communications with the network management system. The default is 161.
9. Press Submit.

**Disable SNMP**

1. Select System.
2. Select System Overview.
3. Select Services Configuration.
4. Uncheck the Enable SNMP checkbox.
5. Press Submit.

**Enable Remote System Logging**

The 5300-E can be configured to log system messages to an external syslog server.

1. Select System.
2. Select System Overview.
3. Select Services Configuration.
5. Enter the IP address of the Remote Syslog Host.
6. Press Submit.

**Disable Remote System Logging**

1. Select System.
2. Select System Overview.
3. Select Services Configuration.
5. Press Submit.
Change the Administration Password

We strongly recommend that you change the default password for the “root” administrative account using the following steps:

1. Select System.
2. Select changed in the Change Password section of the GUI.
3. Enter the New Password.
4. Enter the password you chose in step C again in the Confirm Password to ensure that there were no mistakes in the initial entry.
5. Press Submit.

Note: The new password must be between 6 and 20 characters in length. Any combination of alpha and numeric characters is accepted.

Read-only User

This feature works by creating a new user with read-only access to the system. All information is displayed in a non-changeable form. Information changed in entry boxes cannot be submitted. In fact, most Submit and OK buttons are not visible.

Note: You must have administrator privileges and log in as an administrator to change read-only user.

Enabling a Read-only User

To enable a read-only user, use the following steps:

1. Using the configuration graphical user interface, from the Configuration Menu on the left-hand side, click Network.

   Note: You must have administrator access and log in as an administrator to change read-only user.
2. Scroll down to the area of the screen shown below.

3. Click changed. The following window screen appears:

![Set Read-Only User Password]

**Note:** All open web browsers must be closed when you change between administrative user “root” and read-only “rouser.”

4. Enter a new password. The password must be a minimum of six characters long.

4. Re-enter the new password to confirm it.

5. Click **Submit**.

Now when you access the system using this user name (rouser) and password, all fields are read-only.

## Subinterfaces

The Subinterfaces feature allows a system administrator to assign additional IP addresses to interfaces. These are sometimes referred to as aliases or loopback interfaces. An additional address may be assigned to the system’s WAN interface to support, for example, another management IP address.

### How Subinterfaces Works

A common use for subinterfaces is forwarding a public subnet. A subinterface may be created to support a subnet forwarded through the Polycom V²IU 5300-E. When forwarding a subnet through the Polycom V²IU 5300-E, it is
necessary to assign an address for this subnet to the system to act as the subnet's gateway. To configure forwarding rules, use the **Forwarding Rules** submenu under the **Firewall** configuration link.

When applied to the WAN/Provider interface, these addresses are protected by the same firewall policy that is applied to the WAN/Provider address. Several other features in the system automatically create Subinterfaces. VRRP (if supported) and Static NAT automatically create Subinterfaces.

When viewing the Network Information page, Subinterfaces are designated in the Interface Information section with the device name and number, separated by a colon (for example, eth0:100).

### Configuring Subinterfaces

To configure subinterfaces, use the following steps:

1. Using the configuration graphical user interface, from the Configuration Menu on the left-hand side, click **Network**.

2. Click **Subinterfaces**. The window shown below opens.

   ![Subinterfaces Window](image)

3. On this screen, complete the following information:
   - **IP Address** is the address to be assigned to the subinterface.
   - **Netmask** is the network mask to use for the address. If several addresses are applied to an interface and these addresses are in a common network, they must use a common subnet. The system does not support supernetting.
   - **Interface** is the port where the subinterfaces will be configured.
4. When you have finished entering this information, click **Add**. The following popup appears:

5. Click **OK**. The new subinterfaces entry appears on the Subinterfaces window in the list area.

---

**ToS Byte Setting**

Since the Internet itself has no direct knowledge of how to optimize the path for a particular application or user, the IP protocol provides a limited facility for upper layer protocols to convey hints to the Internet Layer about how the trade-offs should be made for the particular packet. This facility is the “Type of Service” or ToS facility.

ToS settings allow the service provider to prioritize time sensitive traffic, such as voice plus video to ensure minimized packet loss and delay through their network. When providing end-to-end QoS, it is important that the voice plus video traffic be placed in the correct queues to deliver a higher QoS than regular traffic. Regular traffic, that is not time sensitive, can be delayed with little or no indication to the user, while the slightest delay in voice plus video can cause auditable differences. The ToS byte setting helps prioritize traffic going to the WAN so a provider can prioritize the traffic correctly in its network.

Although the ToS facility has been a part of the IP specification since the beginning, it has been little used in the past. However, the Internet host specification now mandates that hosts use the ToS facility. Additionally, routing protocols (including OSPF and Integrated IS-IS) have been developed which can compute routes separately for each type of service. These new routing protocols make it practical for routers to consider the requested type of service when making routing decisions.

---

**How the ToS Byte Setting Works**

For all RTP traffic (voice and video), the Polycom V^2^IU 5300-E marks the ToS byte in the IP header as “High Priority,” and strips (set to 0) the ToS byte for all other traffic. Unchecking the “Enable ToS Byte Stripping” option means that the ToS byte will not be stripped from non-RTP traffic, but will remain unchanged.

**Note:** For most situations, you should leave this setting as it is. Only change it if your provider indicates that you should do so.

---

**Viewing or Changing the ToS Byte Setting**

To view or change the ToS byte setting, use the following steps:
1. Using the configuration graphical user interface, from the Configuration Menu on the left-hand side, click **Traffic Shaper**.

2. Scroll down the area of the screen shown below.

3. For most situations, you should leave this setting as it is. Only change it if your provider indicates that you should do so. If your provider indicates that you need to change the ToS byte setting, that provider should also provide the other parameters required on this screen.

4. If you have changed the values, click **Submit** to activate the new settings.
H.323 Configuration

To access the H.323 Settings page, select VoIP ALG > H.323 in the Configuration Menu.

H.323 Settings

H.323 protocol settings.

Gatekeeper mode
The gatekeeper mode configuration specifies whether the system should work in WAN/Provider-side gatekeeper mode, Peering-Proxy mode, or embedded gatekeeper mode.
- None (H.323 is disabled)
- WAN/Provider-side gatekeeper mode
- LAN/Subscriber-side gatekeeper mode
- Peering-Proxy mode (configure prefixes)
- Embedded gatekeeper mode

WAN/Provider-side gatekeeper mode settings
The H.323 gatekeeper that all client traffic shall be forwarded to.

WAN/Provider-side GK address: 192.168.1.25
Modify Time-To-Live: [ ]
New Time-To-Live (s): 300
Gatekeeper reachability: N/A (Not in WAN GK mode)

LAN/Subscriber-side gatekeeper mode settings
The H.323 gatekeeper that all incoming calls should be forwarded to. It is possible to have a LAN side gatekeeper configured for peering-proxy mode as well.

LAN/Subscriber-side GK address: [ ]

By allowing public IP addresses to be returned in an LCF, the gatekeeper may be able to do more complex policy decisions. This field should usually not be enabled.

Allow public IP in LCF: [ ]

Embedded gatekeeper mode settings
These settings control the embedded gatekeeper behavior.

Time-To-Live (s): 300
GK routed mode: [ ]
Prevent calls from unregistered endpoints: [ ]
The H.323 Settings page has the following areas:

- Gatekeeper Mode
- WAN/Provider-side gatekeeper mode settings
- LAN/Subscriber-side gatekeeper mode settings
- Embedded gatekeeper mode settings
- LRQ Size
- Default Alias
- Stale Time
- Multicast Messages
• H.460.18 Support
• Alias Restrictions

In the Gatekeeper mode area, select one of the following modes:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>H.323 is disabled.</td>
</tr>
<tr>
<td>WAN/Provider-side gatekeeper mode</td>
<td>Specifies that the system will forward all client RAS messages to the gatekeeper. If this is selected, you must configure the settings in the WAN/Provider-side gatekeeper mode settings area.</td>
</tr>
<tr>
<td>LAN/Subscriber-side gatekeeper mode</td>
<td>Specifies that the system will act as a gatekeeper. If this option is selected, you must configure the settings in the LAN/Subscriber-side gatekeeper mode settings area.</td>
</tr>
<tr>
<td>Peering-Proxy mode</td>
<td>Allows calls to be forwarded to other endpoints based on the information sent from the endpoints. All the information about routing the call must be sent as part of the request or prefixes must be configured.</td>
</tr>
<tr>
<td>Embedded gatekeeper mode</td>
<td>Provides gatekeeper functions and accepts endpoint registrations. If this option is selected, you must configure the settings in the Embedded gatekeeper mode settings area. This mode supports a maximum of 50 registered endpoints for the E10 V²IU and 100 registered endpoints for the E25 V²IU.</td>
</tr>
</tbody>
</table>

If WAN/Provider-Side Gatekeeper mode is selected, you must configure the following parameters:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN/Provider-side GK address</td>
<td>Specifies the IP address of the gatekeeper</td>
</tr>
<tr>
<td>Modify Time-To-Live</td>
<td>Allows you to override the value for time-to-live returned by the gatekeeper before forwarding the response to the endpoint.</td>
</tr>
<tr>
<td>New Time-To-Live</td>
<td>Specifies how long an endpoint's registration should be valid.</td>
</tr>
</tbody>
</table>
If LAN/Subscriber-Side Gatekeeper mode is selected, you must configure the following parameters:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN/Subscriber-side GK address</td>
<td>Enter the IP address of the gatekeeper.</td>
</tr>
<tr>
<td>Allow public IP in LCF</td>
<td>Select the checkbox if the gatekeeper has been deployed with multiple outbound proxies and must decide which proxy to use based on the IP address returned in the LCF. This is an advanced configuration option and should usually not be selected.</td>
</tr>
</tbody>
</table>

If Embedded Gatekeeper is selected, you must configure the following parameters:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time-to-Live(s)</td>
<td>Enter a time in seconds. This setting controls how long an endpoint’s registration should be valid. At the end of this period the endpoint sends another registration request.</td>
</tr>
<tr>
<td>GK routed mode</td>
<td>Specifies whether the system should allow signaling to go directly between endpoints when possible (disabled) or always route signaling between endpoints (enabled).</td>
</tr>
<tr>
<td>Prevent calls from unregistered endpoints:</td>
<td>Blocks unregistered LAN-side endpoints from making calls through the device.</td>
</tr>
</tbody>
</table>

In the LRQ Size area, you can limit the number of source aliases in a forwarded LRQ message to a maximum of two to allow interoperability with gatekeepers that cannot handle more than two source aliases.

In the Default Alias area, you can specify a default alias to be added to incoming calls without a destination message in the Q.931 Setup message. This alias allows the embedded gatekeeper or a LAN/Subscriber-side gatekeeper to route the call to a default endpoint. Enter a default alias and select one of the following types:

- E.164
- H.323
In the Stale Time area, you can arrange to delete clients that have not sent any registration requests for the specified interval. This area includes the following configurable parameters:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete stale clients</td>
<td>Select this checkbox to enable the stale timer feature.</td>
</tr>
<tr>
<td>Stale time (m)</td>
<td>Specify the length of the interval in minutes.</td>
</tr>
</tbody>
</table>

Some RAS messages can be multicast in order to automatically detect gatekeepers. In the Multicast Messages area, you can enable listening to multicast messages. This area includes the following configurable parameter:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listen to multicast messages</td>
<td>Select this checkbox to enable listening to multicast messages.</td>
</tr>
</tbody>
</table>

In the H.460.18 Support area, you can configure H.460.18 support. This allows the system to do NAT/Firewall traversal for clients behind NAT or firewall devices. This area includes the following configurable parameters:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Disables H.460.18 support.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enables H.460.18 support.</td>
</tr>
<tr>
<td>Keep-alive time(s)</td>
<td>Specifies the keep-alive time if H.460.18 support is enabled.</td>
</tr>
</tbody>
</table>

In the Alias Restrictions area, you can set a limit on the number of aliases that are allowed to register with the system. If this number is exceeded when a client tries to register, the registration is rejected. This area includes the following parameter:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Aliases</td>
<td>Enter the maximum number of allowed aliases. If the value is set to 0, the maximum is not enforced.</td>
</tr>
</tbody>
</table>

The H.323 Settings page includes the following two buttons:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submit</td>
<td>Applies the settings configured on this page.</td>
</tr>
<tr>
<td>Reset</td>
<td>Clears all fields and selections and allows you to enter new information.</td>
</tr>
</tbody>
</table>
H.323 Activity

To access the H.323 Activity page, select **VoIP ALG > H.323 Activity** in the Configuration Menu.

The H.323 Activity page is a read-only page that shows the following information:

- Current time
- WAN Gatekeeper status
- Current payload bandwidth
- Estimated total bandwidth
- Activity log of recent H.323 events

H.323 Alias Manipulation

Alias manipulation is performed immediately when a message (such as an ARQ, LRQ or a Setup) is received. Any matching pattern is replaced with the specified string, allowing you to replace characters or strings that are hard or impossible to dial on certain endpoints. Normal call look-up is performed following alias manipulation.
To access the H.323 Alias Manipulation page, select **VoIP ALG > H.323 > Alias Manipulation** in the Configuration Menu.

**H.323 Alias Manipulation**

**Destination H323-ID or E.164 Alias Modification**

The alias modification table can be used to modify aliases before they are acted on.

<table>
<thead>
<tr>
<th>Index</th>
<th>Pattern</th>
<th>Replace</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>#</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>*</td>
<td></td>
</tr>
</tbody>
</table>

**Add a rule**

- **Action:**
- **Pattern:**
- **Index:**
- **Replace:**

This page includes the following areas:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination H323-ID or E.164 Alias Modification table</td>
<td>Lists alias manipulation rules. Rules are executed in the order in which they are listed. Use the arrows to move entries up and down, or use the Index field to specify where a new or edited rule falls in the list.</td>
</tr>
<tr>
<td>Add a rule</td>
<td>Allows you to add new prefixes to the Prefix Routing and Gatekeeping Neighboring table.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Indicates whether the rule is to be added or edited.</td>
</tr>
<tr>
<td>Pattern</td>
<td>Specifies the pattern to be matched. See &lt;l_link&gt;“Regular Expressions” on page 33 for details on valid patterns.</td>
</tr>
<tr>
<td>Index</td>
<td>Determines the order in which the rule is scanned in the Destination H323-ID or E.164 Alias Modification table. To add a rule between two rules with consecutive indexes (n and m), use the higher index (m).</td>
</tr>
<tr>
<td>Replace</td>
<td>Specifies the string that will replace the matched pattern.</td>
</tr>
</tbody>
</table>
The H.323 Alias Manipulation page includes the following buttons:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commit</td>
<td>Applies the settings configured on this page.</td>
</tr>
<tr>
<td>Reset</td>
<td>Clears all fields and selections and allows you to enter new information.</td>
</tr>
</tbody>
</table>

**H.323 Neighboring**

Neighboring and prefix routing can be used to route calls based on a matching prefix in the destination alias of the call. The call decision is made following alias manipulation and acts on the modified string, similar to other call lookup processes such as registered client look-up. Each prefix is associated with a domain name or IP address that is used in the event that the prefix matches.

To access the H.323 Neighboring page (formerly the Prefix Routing page), select *VoIP ALG > H.323 > Neighboring* in the Configuration Menu.
This page includes the following areas:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prefix Routing and Gatekeeper Neighboring table</strong></td>
<td>Lists rules for forwarding incoming calls based on their dialed alias. Rules are executed in the order in which they are listed. Use the arrows to move entries up and down, or use the Index field to specify where a new or edited rule falls in the list.</td>
</tr>
<tr>
<td>Add a prefix</td>
<td>Allows you to add new prefixes to the Prefix Routing and Gatekeeper Neighboring table.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Indicates whether the rule is to be added or edited.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Specifies the prefix pattern to be matched against the dialing string. See &quot;Regular Expressions&quot; on page 33 for details on valid patterns.</td>
</tr>
<tr>
<td>Index</td>
<td>Determines the order in which the rule is scanned in the Prefix and Gatekeeper Neighboring table. To add a rule between two rules with consecutive indexes (n and m), use the higher index (m).</td>
</tr>
<tr>
<td>Strip</td>
<td>Indicates whether the matching prefix is stripped from the dialing string.</td>
</tr>
<tr>
<td>Add</td>
<td>Specifies a string to be prepended to the dialing string.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>Determines whether a location request (LRQ) is sent when this prefix matches.</td>
</tr>
<tr>
<td>• If enabled, the prefix becomes a neighboring statement.</td>
<td></td>
</tr>
<tr>
<td>• If disabled, the incoming Q.931 Setup is forwarded to the given address without a preceding LRQ.</td>
<td></td>
</tr>
<tr>
<td>This field is used for interoperability with other gatekeepers that may not accept a Setup without a preceding LRQ.</td>
<td></td>
</tr>
<tr>
<td>Local Zone</td>
<td>Provides compatibility with remote gatekeepers that are configured to accept LRQs only from sources that match its configured remote zone. If a gatekeeper is configured to accept requests only from a known source, enter the zone in this field.</td>
</tr>
<tr>
<td>Address</td>
<td>Specifies the IP address or domain name of the device to which the call is to be forwarded.</td>
</tr>
</tbody>
</table>

The H.323 Neighboring page includes the following buttons:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commit</td>
<td>Applies the settings configured on this page.</td>
</tr>
<tr>
<td>Reset</td>
<td>Clears all fields and selections and allows you to enter new information.</td>
</tr>
</tbody>
</table>
Regular Expressions

Alias manipulation patterns and prefixes use regular expressions to match a string in the destination alias. A regular expression can be a string of literal characters to match or a set of special expressions.

Alias manipulation patterns can match a sub-string at any location and number of times within the alias. Prefixes are always searched from the left of the alias and cannot match a middle part or the end of the alias.

Regular expressions are listed in Table 1 and Table 2 lists some example expressions.

Table 1  Regular Expressions

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>Matches any single character.</td>
</tr>
<tr>
<td>[]</td>
<td>Matches any single character listed between the []. For example, [abc], [123]. If the characters are separated by a -, all characters between the two are matching, e.g. [a-z], [0-9]</td>
</tr>
<tr>
<td>()</td>
<td>Matches the literal string given, e.g. (abc)</td>
</tr>
<tr>
<td></td>
<td>Matches the block on either side of the [], e.g. a</td>
</tr>
<tr>
<td>?</td>
<td>Matches 0 or 1 of the preceding block.</td>
</tr>
<tr>
<td>*</td>
<td>Matches 0 or more of the preceding block.</td>
</tr>
<tr>
<td>+</td>
<td>Matches 1 or more of the preceding block.</td>
</tr>
<tr>
<td>\</td>
<td>Escapes the special meaning of the next character.</td>
</tr>
<tr>
<td>{a}</td>
<td>Matches exactly 'a' numbers of the preceding block.</td>
</tr>
<tr>
<td>{a,}</td>
<td>Matches 'a' or more of the preceding block.</td>
</tr>
<tr>
<td>(a,b)</td>
<td>Matches between 'a' and 'b' (inclusive) of the preceding block.</td>
</tr>
</tbody>
</table>

Table 2  Example Regular Expressions

<table>
<thead>
<tr>
<th>Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Matches the string 100.</td>
</tr>
<tr>
<td>(555)?123</td>
<td>Matches 555123 or 123.</td>
</tr>
<tr>
<td>(408</td>
<td>555)</td>
</tr>
<tr>
<td>555[0-9]{3}</td>
<td>Matches 555 followed by exactly 3 digits.</td>
</tr>
<tr>
<td>#</td>
<td>Matches the character '#'.</td>
</tr>
<tr>
<td>*</td>
<td>Matches the character '&quot;'. Note that &quot;&quot; by itself is a regular expression and must therefore be escaped with a '&quot;' to match the character itself.</td>
</tr>
</tbody>
</table>
Forwarding Rules

Forwarding Rules allows a system administrator to forward data traffic for a subnet from one interface to another, overriding the firewall’s default drop rules.
Allowing a subnet to be forwarded is commonly used when servers with public addresses are placed behind the system. Configuring the network in this way allows the system to manage and prioritize bandwidth, sharing it between the VoIP services and the servers.

How Forwarding Rules Works

When forwarding, one address from the forwarded range of addresses must be assigned to the rule’s output interface. The Polycom V²IU 5300-E uses this address to act as a gateway router for the subnet. The address may be assigned using the Subinterfaces page.

Note: The subnet and forwarded addresses are not protected by the firewall. A similar method for forwarding traffic is provided by Proxy ARP. Proxy ARP is used to “bridge” addresses within a single subnet range from one interface to another. Often this is used to bridge and forward a public address to the protected side of the system without having to subnet the public address range. Proxy ARP does not require an additional gateway address on the system for the subnet, but does not allow port and protocol filtering for forwarded data.

Example

In this example:

- The ISP has supplied two separate subnets to the customer:
  - A small one (2 hosts) for the WAN link
  - A large one (254 hosts) for a bank of servers
- 67.40.41.2 is the WAN IP address for the Polycom V²IU 5300-E
- NAT is a private IP range of 192.168.1.xxx using the WAN address for PCs and Phones
- On the LAN side of the Polycom V²IU 5300-E are the following:
  - Private IP subnet (192.168.1.xxx)
  - Public IP subnet (67.40.40.xxx)

This is shown below.
Configuring Forwarding Rules

To configure address forwarding rules, use the following steps:

1. Using the configuration graphical user interface, from the Configuration Menu on the left-hand side, click Firewall.
2. Click Forwarding Rules. The window shown below opens.
3. On this screen, complete the following information:

- **IP Subnet**: The subnet to be forward through the firewall from the Input Interface to the Output Interface.
- **Netmask**: The network mask to apply to the IP Subnet to create the range of IP addresses that are forwarded through the firewall.
- **Input Interface**: The interface where data is received that is destined for the forwarded subnet (destination address(es)).
- **Output Interface**: The interface where data is received that is sent from the forwarded subnet (source address(es)).
- **Protocol**: The following protocols are used:
  - **UDP**: for the specified network, allows the specified UDP port or port range to pass through the system
  - **TCP**: for the specified network, allows the specified TCP port or port range to pass through the system
— Any: for the specified network, allows all ports and protocols through the system. No ports are required because not all protocols support the concept of ports.

- Port or Port Range: The port number or port range allowed through the system when UDP or TCP are selected. A port range is specified by separating the starting and ending ports with a colon ':' (for example, 22:80). The ports parameter is not supported when you select **Any** protocol because not all protocols support the concept of ports.

4. When you have finished entering this information, click **Add**.

5. Click **OK**. The new forwarding entry appears on the Forwarding Rules window in the list area.

### Peering Proxy

H.323 prefixes can be used to route calls based on a matching prefix in the destination alias of the call. Each prefix is associated with a domain name or IP address to send the call to in case the prefix matches.

The prefixes are searched in order, that is, the first prefix is tried first, and then the next one on the list until the system finds a matching prefix. This means that if there are multiple matching prefixes, the first one is used.

### How Peering Proxy Works

The Polycom V^2^IU 5300-E supports the concept of an H.323 Peering Proxy. This function provides advanced security layers or peering points within the network where a security layer is needed. Peering Proxy allows network providers to add internetworking connections between their “trusted” network and an unknown network. This topology hides their trusted network and the Stateful packet inspection Firewall provides the policies to ensure security. You can add Peering Proxies in series with one another to push the core H.323 networking infrastructure to meet individual security requirements.

The illustration below shows a sample diagram with dial plan and call flow examples. It is a snapshot of how the Peering Proxy can be deployed. Peering Proxy however, is not limited to this specific scenario, so contact your Polycom representative to discuss specific network requirements for full Peering Proxy support.
Note: A minimum configuration for Peering Proxy would be for inbound only prefixes, since there may be many endpoints to statically route calls to. There might also be a master gatekeeper to which all endpoints are registered. In this case, you would only need 1 prefix pointing to the master gatekeeper and let that gatekeeper signal the other endpoints directly.

In the example above, the Polycom V2IU 5300-E Peering Proxy is installed in “Private Video Network A and B,” a peering point into this network. This network could have additional peering points to allow topology spreading of network resources. However, this example shows only a single point. Peering
Proxy provides an access point into this network and is responsible for the E.164 dial plan using NANP (North American Numbering Plans or NPA’s). The NPA’s in this case are 831 and 408.

Dial plan integrity is required to insure proper routing of prefix’s. This means that if users are to dial into your network, they could be required to enter a “Prefix” on their V2IU with a corresponding destination IP. If the user was to dial another user NOT destined to your network with the same beginning prefix, the prefix configured on this V2IU would create a prefix match and the call would route incorrectly. The call routes to the destination defined in the prefix and not to the intended endpoint. The example shows “Private Video Network A’s Peering Proxy” with an inbound prefix defined as 8315……. Any inbound call that matches 8315 with any 6 digits creates a prefix match and sends the call to 10.10.11.1. Refer to “Regular Expressions” in the Info button on the GUI interface for information on all the methods for defining prefixes.

Private Video Network A is one example of a V2IU configured in “LAN Side Gatekeeper” mode with an ANNEX O dial method to dial “Off Net.” Internal “On Net” endpoints registered to the LAN Side Gatekeeper will dial E.164 only. This allows any location to place calls to any location with an ANNEX O dial plan, that is, E.164@WAN_IP or other V2IU’s deployed on the network. In this example a Peering Proxy has been deployed to allow dialing ingress and egress to the Public Internet. At each V2IU location required to egress, the Public Internet requires a “Prefix” to be configured. This allows that location’s endpoint to dial “Off Net” to the Public Internet. This prefix can be configured to any digit and may be part of the externally dialed E.164 in the E.164@WAN_IP, that is, to reach site A by dialing 4155551000@66.20.20.4 where the prefix is defined as 415* or 415……. In this example, a “9” was chosen. The prefix is then mapped to the LAN interface of the Peering Proxy 10.10.11.1. The dial string is now 94155551000@66.20.20.4 and a strip rule for the prefix is applied. This is needed to route the call at the destination correctly. If the Site C V2IU does not strip the “9”, the destination V2IU fails the call with a “No Registered Client” message (call failures can be viewed under the “H323 Activity” page in the GUI), since the “9” becomes part of the E.164. If you choose a prefix that matches the destination E.164, set Site C’s V2IU to NOT strip matching prefixes.

**NOTE:** In this illustration E.164@WAN_IP was used as an example. Peering Proxy and all V2IU’s support user@host ANNEX O dialing methods, for example 123@1.1.1.1 or abc@1.1.1.1 or abc@abc.com with a DNS SRV record configured to point to an A record for the WAN IP of the V2IU.

The following sections demonstrate the Dial Plan for ingress and egress calls to Private Video Network A as shown in the illustration.

**Outbound from Site C to Site A**

Site C dials an endpoint located at Site A: 94155551000@66.20.20.4. The PathNavigator receives the call and generates a Q.931setup to the V2IU for that subnet. The V2IU processes the Q.931 setup from the calling endpoint. The V2IU looks for a prefix match. In this case, the “9” creates a match. The “Strip Matching Prefix” rule is applied, the “9” is stripped, and the call is routed to
the Peering Proxy IP 10.10.10.1. The Peering Proxy applies the same rule set, in this case, NO matching prefix is found and ANNEX O dialing is applied. The call is now routed to Site A's V2IU. The call is forwarded to the LAN Side PathNavigator where the registered client with the E.164 of 4155551000 is located and the call is gatekeeper routed to the called endpoint.

Inbound from Site A to Site C

Site A dials: 8315551000@67.40.40.4. (The destination IP is the Peering Proxy WAN IP address.) The Peering Proxy is configured with prefix 8315… and is mapped to the WAN IP of the V2IU 10.10.11.1. As explained earlier, the prefix could be 831* or 83…… and so on, depending upon dial plan requirements. The PathNavigator receives the Q.931 setup from the endpoint and forwards the call to the V2IU for that subnet. The V2IU receives the Q.931 setup from the calling endpoint. The V2IU looks for a prefix match, finds NO matching prefix, and ANNEX O dialing is applied. The call is now routed to the Peering Proxy IP 67.40.40.4. The Peering Proxy receives the Q.931 setup and looks for a prefix match, in this case “8315” creates a match. The Peering Proxy now changes the destination IP to 10.10.11.1 and routes the call to Site C's V2IU. The Q.931 setup is forwarded to the LAN Side PathNavigator where the registered client with the E.164 of 8315551000 is located, and the call is gatekeeper routed to the called endpoint.

Outbound from Site C to Site D

Site C dials an endpoint located at Site D: 95105551000@65.10.10.4. The PathNavigator receives the call and generates a Q.931 setup to the V2IU for that subnet. The V2IU processes the Q.931 setup from the calling endpoint. The V2IU looks for a prefix match, in this case the “9” creates a match. The “Strip Matching Prefix” rule is applied, the “9” is striped, and the call is routed to the Peering Proxy IP 10.10.10.1. The Peering Proxy applies the same rule set, in this case NO matching prefix is found, and ANNEX O dialing is applied. The call is now routed to the Peering Proxy for “Private Video Network B” IP 68.30.30.4. The Peering Proxy receives the Q.931 and looks for a prefix match. In this case, “5125” creates a match. The Peering Proxy now changes the destination IP to 172.16.2.1 and routes the call to Site D's V2IU. The V2IU is configured for Embedded Gatekeeper Mode. In this mode, the endpoint is directly registered and an E.164 registered client match is made. The call is then routed to the called endpoint.

Outbound from Site D to Site B

Site D dials an endpoint located at Site B: 95105551000@65.10.10.4. The V2IU Embedded Gatekeeper is configured with a prefix of “9” to point to Peering Proxy 172.16.1.1. The V2IU looks for a prefix match. In this case, the “9” creates a match. The “Strip Matching Prefix” rule is applied, the “9” is striped, and the call is routed to Peering Proxy IP 172.16.1.1. The Peering Proxy applies the same rule set. In this case NO matching prefix is found and ANNEX O dialing is applied. The call is now routed to Site B. The V2IU is configured for
Embedded Gatekeeper Mode. In this mode, the endpoint is directly registered, an E.164 registered client match is made, and the call is routed to the called endpoint.

**Outbound from Site C to Public IP Endpoint**

Site C dials the public endpoint: 9@61.10.10.4. The PathNavigator receives the call and generates a Q.931 setup to the V2IU for that subnet. The V2IU receives the Call setup from the calling endpoint, and the V2IU looks for a prefix match. In this case, the “9” creates a match. The “Strip Matching Prefix” rule is applied, the “9” is striped, and the call is routed to the Peering Proxy IP 10.10.10.1. The Peering Proxy applies the same rule set, in this case NO matching prefix is found, and direct IP dialing is applied.

**Inbound from Public IP Endpoint to Site C**

Public IP endpoint is NOT registered to a gatekeeper and must dial an IP+EXT to reach Site C's endpoint. In this case, the IP address is 67.40.40.4 and EXT 8315551000. The Peering Proxy receives the call and looks for a prefix match. In this case “8315” creates a match. The Peering Proxy now changes the destination IP to 10.10.11.1 and routes the call to Site C's V2IU. The Q.931 setup is forwarded to the LAN Side PathNavigator where the registered client with the E.164 of 8315551000 is located, and the call is gatekeeper routed to the called endpoint.

**Configuring Peering Proxy**

To configure peering proxy, use the following steps:

1. Using the configuration graphical user interface, from the Configuration Menu on the left-hand side, click **VoIP ALG**.
2. Click **H.323**. The window shown below opens.
3. On this screen, check “Peering-Proxy mode”.

4. Scroll to the bottom of the window and click Submit.

Adding an H.323 Prefix Entry

You can add prefixes by entering the prefix string and the target address.

To add an H.323 prefix entry, use the following steps:

1. Using the configuration graphical user interface, from the Configuration Menu on the right-hand side, click VoIP ALG.

2. Click H.323 Prefixes. The window shown below opens.
The prefix routing table shows all currently configured prefixes. The prefixes are searched in the order they are entered. Each prefix can be moved up or down in the list. You can select and delete prefixes.

3. To strip a matching prefix, select the checkbox and click **Submit**. If you enable this, all matching prefixes are stripped from the destination alias before the call is forwarded.

4. To add an entry, enter the prefix and the address. The prefix string can be a regular expression as described above. The target address can be a domain name or an IP address.

5. Click **Add**. The new entry appears in the table.

### Clients List Lock

Client List lockdown allows you to prevent new clients from registering. This is done as follows:

- Creating a client, as follows:
— Manually entering all clients that are allowed to use the system
— Running the system without the Client List lockdown feature until all desired clients have registered
• Enabling this feature.
  This feature is useful for lists involved with 911 usage.
  When this feature is in effect, any message from an unauthorized SIP client will be rejected with a “403 Forbidden” response. MGCP messages will be discarded.

**Enabling the Clients List Lock**

To configure clients list lock, use the following steps:

6. Using the configuration graphical user interface, from the Configuration Menu on the left-hand side, click **VoIP ALG**. The following window appears.

![VoIP ALG Configuration Window](image)

3. On this screen, check “Enable Client List lockdown”.
4. Scroll to the bottom of the window and click **Submit**.
H.323 Activity Monitor

The H.323 Activity Monitor shows any recent H.323 events that may be of interest to the administrator of the system. The information appears in three columns:

- Event/Time
- Source
- Destination

Following this information are a number of lines with event specific information such as call-id, duration, call-status, and so on. Abnormal events have their event specific information listed in red.
Type of Events

The events that may currently be listed in the activity monitor are as follows:

- **Bandwidth change** - the endpoint requested a change of the bandwidth used for its call, only sent if the bandwidth management is enabled.

- **Call Setup** – Only sent if the call was ‘successfully’ established. A call is successfully established if the H.245 media negotiation connection was established.

- **Call Termination** – Sent when a call terminates. You can have a call termination event without a call setup event, for example, a failed call that doesn’t reach the H.245 established state will not cause a call setup event, but only a call termination event.

- **Registration Reject** – Sent when a registration was rejected. This includes the authority that rejected the registration (our side or the gatekeeper (only in WAN GK mode) as well as a text reason for the rejection.

- **Gatekeeper reachability changed** (only in WAN GK mode). Gatekeeper status toggled from reachable to unreachable or vice versa.

- **Location Request** – Received a location request from a neighboring gatekeeper.

- **Location Confirm** – Sent, or forwarded, a location confirm to a previous request.

- **Location Reject** - Sent, or forwarded, a location reject to a previous request.

Call Status

The call status shows the last state of the call at the time of the event. Each call progresses through a number of states when being established. If a call fails, the call-status in the call termination event can help trouble-shoot the cause of the call failure. For example, if the call fails at the “Caller/Callee admission request received” state, there may be a problem communicating with the gatekeeper, whereas if the call fails at the “Attempting to establish outgoing Q.931 TCP connection” state, the remote endpoint may not be reachable. The following are call status messages:

- **“Caller admission request received”**
  Received an admission request from the source endpoint and forwarded it to the gatekeeper.

- **“Caller admission response received”**
  Received an admission response (either confirm or reject) from the gatekeeper and forwarded it to the source endpoint.

- **“Incoming Q.931 TCP connection established”**
  Received an incoming Q.931 TCP connection from the source.
• “Attempting to establish outgoing Q.931 TCP connection”
Successfully resolved the destination of the call and attempting to establish an outgoing Q.931 TCP connection to the destination.

• “Q.931 signaling received and forwarded”
Both Q.931 TCP connections have been successfully established and Q.931 signaling has been received and forwarded.

• “Callee admission request received”
Received an admission request from the destination endpoint and forwarded it to the gatekeeper.

• “Callee admission response received”
Received an admission response (either confirm or reject) from the gatekeeper and forwarded it to the destination endpoint.

• “Incoming H.245 TCP connection established”
Received an incoming H.245 TCP connection from the source.

• “Attempting to establish outgoing H.245 TCP connection”
Attempting to establish an outgoing H.245 TCP connection to the destination.

• “H.245 signaling received and forwarded”
Both H.245 TCP connections have been successfully established and H.245 signaling has been received and forwarded. At this point, the call is considered established, even though no media channels have been opened up yet.

• “Outgoing media channel established”
An outgoing media channel (from the LAN/subscriber side to the WAN/provider side) has been opened.

• “Incoming media channel established”
An incoming media channel (from the WAN/provider side to the LAN/subscriber side) has been opened.

• “Bidirectional media channels established”
Media channels have been opened in both directions. This is a normal call where media is being sent in both directions.
Call Termination

The call termination cause may also give some information about why the call terminated or failed to be established.

- "Out of system resources"
The call could not be completed because the system was out of system resources.

- "Client owning the call has been deleted"
The call could not be completed because the client that made this call was deleted during the call setup.

- "Connection to destination could not be established"
A TCP connection to the destination could not be established.

- "Connection refused by destination"
The call could not be completed because the destination refused the incoming TCP connection.

- "No route to destination"
A TCP connection to the destination could not be established because the destination could not be reached. This could happen if there is no route to the destination or, if the destination is on the same subnet, the destination does not answer to ARP requests.

- "Connection to destination timed out"
The TCP connection attempt to the destination timed out before it could be established.

- "Call ended by source"
The call was gracefully terminated by H.323 signaling from the source. This usually indicates that the endpoint intended to terminate the call.

- "Call ended by destination"
The call was gracefully terminated by H.323 signaling from the destination. This usually indicates that the endpoint intended to terminate the call.

- "Connection terminated by source"
The call was terminated because the source terminated the TCP connection without prior call termination signaling.

- "Connection terminated by destination"
The call was terminated because the destination terminated the TCP connection without prior call termination signaling.

- "No admission confirm received"
The call could not be established because the admission response was not received from the gatekeeper.

- "Cannot resolve destination"
The call could not be established because the destination could not be resolved.

- "At maximum bandwidth usage"
The call could not be established because the system already is at the maximum allowed bandwidth.

- “Received admission reject”
The call was terminated because an admission reject was received from the gatekeeper.

- “Received disengage request”
The call was terminated because the endpoint requested to tear down the call.

- “Received invalid data”
The call could not be established because the system received invalid data on the signaling channel.

- “Cannot find client”
The call could not be established because the called client could not be found.

**Viewing the H.323 Activity Monitor**

To configure the H.323 Activity Monitor, use the following steps:

5. Using the configuration graphical user interface, from the Configuration Menu on the left-hand side, click **VoIP**.

6. Click **H.323 Activity**. The window shown below opens.

![Recent H.323 activity logs](image)

The H.323 activity logs shows recent H.323 events such as call terminations and registration rejects.

2. On this screen, the event list contains three columns:
   - The Event/Time field - shows the type of event and the time that it occurred.
   - The Source field - shows the source of the event as an IP address and an alias (when available).
   - The Destination field - shows the destination of the event as an IP address and an alias (when available).
VoIP Configuration

The 5300-E provides a VoIP application layer gateway (ALG) for the SIP, MGCP, and H.323 protocols. The ALG proxies the connection between the VoIP softswitch, IP PBX or gatekeeper and voice and video devices such as IP phones, IADs or softphones. By acting as a proxy the 5300-E is able to provide several important functions for IP based voice and video:

- Provide NAT/PAT services for voice and video traffic. NAT/PAT for VoIP enables you to use a single public IP address on the WAN interface of the 5300-E to represent multiple private IP addresses assigned to voice or video devices on the LAN. The NAT function maps both IP address and IP port number between the public and private addresses so that all signaling and VoIP media packets are translated. A single public IP address can support up to 253 voice and video devices.

- Provide security services for voice and video traffic.
  - NAT/PAT services hide enterprise LAN topology from hackers.
  - The ALG acts as a “voice and video aware” firewall and ensures only authenticated voice traffic enters the enterprise LAN. This is accomplished by the dynamic provisioning of signaling and media ports for authenticated voice devices. The implementation is stateful and open ports are closed automatically when no longer required to support the voice or video call.

- Enable mobility in the enterprise LAN for voice devices. This is useful, for example, when using WiFi or moving office locations. In these instances the IP address of the voice and video device may be changed.
Configure the VoIP ALG

In order to configure the VoIP ALG the 5300-E must be told where to reach the signaling servers and TFTP server on behalf of the voice devices.

1. Select VoIP ALG.
2. If using VLANs assign the ALG to a specific VLAN id using the drop down menu.
3. If you are using MGCP enter the MGCP Server IP Address, MGCP Media Gateway Port and MGCP Notified Entity Port.
4. If you are using SIP enter the SIP Server IP Address and SIP server port. The SIP server port is the port used by the SIP registrar. The default value is port 5060.
5. If you are using H.323 enter the H.323 Gatekeeper IP Address.
6. Enter the TFTP Server Address. This address is used to identify the TFTP server that contains the images used by IP phones at boot up. The 5300-E performs a TFTP server relay function.
7. Automatic MGCP Re-registration is used to re-register MGCP endpoints every time the network or system restarts. Enable this feature to automatically synchronize the softswitch and phones immediately after a restart. The default is Enabled.

8. The MGCP Re-registration Rate is used to set the number of MGCP RSIP messages to send per second to the Media Gateway Controller when re-registration is needed. If the MGCP Re-registration Rate needs to be changed, enter a value between 1 and 5. Generally, this value does not need to be modified. The default value is 5 msg/second.

9. The system re-registers clients when it starts up. If any of these re-registration requests fail, the system will wait for the configured number of seconds and then retry the re-registration for the clients that failed. The system will make at most 10 re-registration requests for failed attempts. If the MGCP Re-registration Retry Delay needs to be changed, enter a value between 30 and 60 seconds. Generally, this value does not need to be modified. The default value is 30 seconds.

10. The H.323 TerminalType is used to specify the type of terminal that the Voice Appliance should use. It can be either endpoint or gateway. The Maximum Bandwidth specifies the bandwidth to allow for H.323 calls. The bandwidth is specified in kbps and if it is set to 0, bandwidth management is not enforced. Only calls with media traversing the 5300-E is counted towards the bandwidth maximum.

**Note**

It is not necessary to program in an FTP server address if your IP phones use the FTP protocol instead of TFTP to retrieve their images. A relay function is not needed for FTP as the 5300-E will forward FTP traffic to the destination server as programmed in your IP phone.
11. The Current payload bandwidth calculates the current video traffic, without IP overhead, traversing the Appliance. The Estimated total bandwidth calculates the total video traffic, plus IP overhead, traversing the Appliance.

12. The H.323 Max Aliases limits the number of aliases that are allowed to register with the Voice Appliance. If this number is exceeded when a client tries to register, the registration will be rejected. If the value is set to 0, the maximum is not enforced.

13. The SIP LAN Side Gateway is used to configure a LAN side SIP gateway to which calls that are not for a registered phone can be sent. The name of the gateway is the name that is configured for the gateway in the soft-switch and the IP address is the address where the gateway can be reached.

14. Press Submit.

**Configure VoIP Subnet Routing**

It is not necessary to configure VoIP subnet routing if all of your voice devices are installed on the same IP subnet as the 5300-E. In some installations the voice devices are located in different subnets than the 5300-E and connected via intermediate routers. In these instances it is necessary to configure a return path in the 5300-E by specifying the intermediate router who knows how to reach the voice devices. This router must be reachable by the 5300-E.
Enter a VoIP Subnet Route

1. Select System.
2. Select System Overview.
4. Enter the IP Network (e.g., 10.10.12.0).
   This is the IP address of the remote subnet containing the voice devices.
5. Enter the Netmask (e.g., 255.255.255.0).
   This is the mask of the IP address of the subnet containing the voice devices.
6. Enter the Gateway (e.g., 10.10.10.2).
   This is the IP address of the intermediate router that knows the return path to the remote subnet from the 5300-E.
   Press Submit.
Perform steps A through G for each remote subnet containing the voice devices.

**Note**
The 5300-E is limited to a total of 20 different VoIP subnets.
Delete a VoIP Subnet Route

1. Select System.
2. Select System Overview.
4. Enter the IP Network (e.g., 10.10.12.0) .
   This is the IP address of the remote subnet containing the voice devices.
5. Enter the Netmask (e.g., 255.255.255.0).
   This is the mask of the IP address of the subnet containing the voice devices.
6. Enter the Gateway (e.g., 10.10.10.2).
   This is the IP address of the intermediate router that knows the return path to the remote subnet from the 5300-E.
7. Select the Delete Subnet checkbox.
8. Press Submit.
Perform steps A through H for each remote subnet that you wish to delete.

Configure IP Phones, IADs or Softphones

After configuring the 5300-E VoIP ALG the voice devices must be configured to point to the LAN interface of the 5300-E as their signaling gateway and optionally as their TFTP server (if they use the TFTP protocol to retrieve their software images). The steps required to setup these devices differ from vendor to vendor. Using the DHCP server included in the 5300-E will significantly simplify the setup of these devices if they are able to obtain their IP configuration via DHCP. Please consult the applicable users guide of each device for detailed instructions.
Data Networking Configuration

The 5300-E provides static IP routing and two types of Network Address Translation (NAT) functions for data traffic. This chapter explains the use and configuration of these features.

NAT for Data Traffic

NAT allows hosts on a private internal network (the LAN side of the 5300-E) to anonymously communicate with devices on an external network (the WAN side of the 5300-E). The 5300-E with NAT enabled will re-write outbound packet headers using public IP addresses in place of private IP addresses so that the private IP addresses are not exposed to the external network. Additionally, the ports used by the IP addresses are also changed as they traverse the 5300-E. This is known as Port Address Translation (PAT) and provides an additional security measure. The 5300-E maintains a table of these mappings so that return packets can be forwarded to the correct host on the private network.

The 5300-E provides two types of NAT functions: dynamic NAT and static NAT. Dynamic NAT allows many private IP addresses to be mapped to a single public IP address (using different port numbers of the public IP address). Static NAT maps private IP addresses and port numbers to public IP addresses and port numbers on a one-to-one basis.

Note

The 5300-E ALG automatically handles NAT for voice devices as described in Chapter 3 “VoIP Configuration”.

The 5300-E provides static IP routing and two types of Network Address Translation (NAT) functions for data traffic. This chapter explains the use and configuration of these features.
Configure Dynamic NAT

Use Dynamic NAT when you have multiple PCs installed on the LAN side of the 5300-E that require Internet or WAN access. Once Dynamic NAT is enabled the 5300-E will automatically perform an address translation for all packets to/from the LAN side PCs.

1. Select NAT.
   The default value for dynamic NAT is enabled.
2. Use the Enable Lan NAT checkbox to enable or disable dynamic NAT.
3. Press Submit.

Configure Static NAT

Use Static NAT when a server or PC located in the private network needs to be accessible from the external network. Some examples include a corporate web server, a mail server or an FTP server. In these instances, the 5300-E statically maps the public IP address of each server to the actual private IP address of the server.

In order for Static NAT to function dynamic NAT must be enabled.

1. Select NAT.
2. Enter the public and private IP addresses and ports to be mapped in Static NAT Client Entries using the following format:
   Protocol;PublicIPAddress/netmask-port>PrivateIPAddress-port
   For example the entry “tcp;198.66.203.19-80>192.168.1.3-8080” will map all web traffic destined to public IP address 198.66.203.19 to the private webservice 192.168.1.3 port 8080. The public IP address of 198.66.203.19 is automatically created as a “subinterface” or “secondary address” on the WAN interface of the 5300-E so that external hosts can reach the web server.
   Each entry should be placed on a new line.
3. Press Submit.

Delete a Static NAT entry

1. Select NAT.
2. To delete an IP address or a range of IP addresses highlight the entry in the Static NAT Client Entries list and press the Delete key on your keyboard.
3. Press Submit.

Static IP routing

In addition to locally connected IP networks the 5300-E can forward traffic for one remote data network by configuring a static route entry. Any packets destined for the remote data network will be forwarded to the specified gateway address in the entry.

Configure the static route

1. Select System.
2. Select System Overview.
3. Select Route.
4. Select the Apply Route checkbox.
5. Enter the IP Network address. This address is the remote data network you would like the 5300-E to forward to the gateway. The hosts portion of the IP address should be set to “0”. For example, 10.10.20.0
6. Enter the Netmask of the remote data network. For example, 255.255.255.0
7. Enter the Gateway IP address of the interface that will receive all packets destined for the remote data network.
8. Press Submit.

Delete the static route
1. Select System.
2. Select System Overview.
3. Select Route.
4. Remove the check in the Apply Route checkbox.
5. Press Submit.

**Firewall Configuration**

The 5300-E uses a Stateful Packet Inspection (SPI) firewall to protect data devices installed behind the LAN interface. The 5300-E ALG as described in the “Configure the VoIP ALG” section of this manual protects voice devices. The firewall is enabled by default. The default behavior of the firewall is to:

- deny all traffic originating from the WAN
- allow all traffic originating from the LAN
- allow only return traffic for connections that originated from the LAN
- deny all traffic originating from the WAN to the 5300-E itself except for http and SSH connections
- allow all traffic originating from the LAN to the 5300-E

The default behavior can be modified using the basic and advanced settings fields on the firewall configuration page. We recommend that you use the 5300-E firewall however it can be disabled if the 5300-E is installed behind an existing legacy firewall.

**Enable or disable the firewall**

1. Select Firewall.
2. Use the Enable Firewall checkbox to either enable or disable the firewall.
3. Select Submit.

**Configure Basic Settings**

To allow or deny http and SSH traffic originating from the WAN to the 5300-E simply use the checkboxes provided in the basic settings area of the firewall configuration page.

**Warning**

Denying http or SSH traffic from the WAN may result in losing management connectivity to the 5300-E if you are configuring the system remotely using the WAN link.

1. Select Firewall.
2. Use the Allow HTTP access from WAN side and Allow SSH access from the WAN side checkboxes to either enable or disable the http or ssh access.
3. Select Submit.

**Configure Advanced Settings**

A comprehensive security policy can be created using the advanced settings of the 5300-E firewall. The policy actions that can be taken on any packet processed by the 5300-E are summarized in the following table:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Input format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow TCP Port</td>
<td>Allows traffic with the specified TCP port to terminate on the 5300-E.</td>
<td>*Valid values range from 1 through 65535. *Multiple entries are separated by a space *Range value specified by : character. For example, 25:50 means perform the action on ports 25 through 50</td>
</tr>
<tr>
<td>Allow UDP Port</td>
<td>Allows traffic with the specified UDP port to terminate on the 5300-E.</td>
<td>• Valid values range from 1 through 65535. • Multiple entries are separated by a space • Range value specified by : character. For example: 25:50 means perform the action on ports 25 through 50</td>
</tr>
<tr>
<td>Deny Hosts (IP)</td>
<td>Denies all traffic with the source IP address matching the specified hosts</td>
<td>• Multiple entries are separated by a space • Classful IP addresses are assumed by default. For example: 192.168.3.1 uses a class c mask. Subnets can be specified using the / notation. Egg. 192.168.3.1/24</td>
</tr>
</tbody>
</table>
1. Select Firewall.
2. Enter the desired Advanced Settings using the table above as a guide.
3. Select Submit.
Remove Advanced Setting Entries

To remove an advanced firewall setting simply highlight the value in the entry box and delete it using the keyboard.

1. Select Firewall.
2. Highlight the entry to be deleted in the Advanced Settings list and press the Delete key on your keyboard.
3. Press Submit.

Traffic Management Configuration

Traffic management is required to ensure high quality voice and video calls when voice, video and data traffic share the same WAN link. Voice and video traffic must be prioritized for transmission over data traffic to meet the stringent jitter, latency and packet loss requirements for high quality voice and video. The 5300-E:

- Automatically prioritizes voice and video traffic over data traffic to ensure high quality voice and video calls.
- Manages bandwidth using different upstream and downstream link speeds (e.g. ADSL).
- Maximizes WAN link utilization by allowing data traffic to burst up to full line rate in the absence of voice and video calls.
- Controls the data transfer rate of upstream TCP devices to limit WAN link congestion.
- Optimizes throughput for low-bandwidth WAN links (e.g. ADSL) by automatically adjusting the Maximum Transmission Unit (MTU) and Maximum Segment Size of IP datagrams during periods of WAN congestion.
- Supports network-based QoS applications by setting the TOS bits for all VoIP packets sent to the WAN and the LAN. TOS bits are used so that VoIP packets can be prioritized in the network by DiffServ enabled routers. The TOS bit value used for voice and video traffic is set to 0xb8. For other priority devices the TOS bit is set to 0x10. All other data will have the TOS bit cleared if set by the endpoints. This value is set for all VoIP packets processed by the 5300-E and overwrites any specific TOS bit configuration set by VoIP endpoints.
• Ensures that bandwidth allocated to new voice and video calls does not adversely affect the quality of existing active calls (Call Admission Control or CAC).

The 5300-E combines sophisticated traffic management mechanisms including classification, prioritization, queuing, rate limiting and CAC to ensure high quality voice and video calls. Fortunately the system manages this complexity for you and configuring traffic management is very straightforward:

• Enable traffic shaping.
• Specify the upstream and downstream bandwidth of your WAN link.
• Enable CAC.

Follow the steps below to configure and enable traffic management.

**Enable Traffic Shaping**

2. Select the Enable traffic shaper checkbox.

3. Specify the upstream and downstream bandwidth of your WAN link
   a. Enter the WAN Downstream Bandwidth in Kbps.
   b. Enter the WAN Upstream Bandwidth in Kbps.

   If you are unsure of the WAN link bandwidth available your IT administrator or service provider can usually provide these values. Some typical examples are as follows:

<table>
<thead>
<tr>
<th>WAN Link</th>
<th>WAN Downstream Bandwidth</th>
<th>WAN Upstream Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>1.544Kbps</td>
<td>1.544Kbps</td>
</tr>
</tbody>
</table>
4. Optionally enable priority IP addresses

VoIP traffic from devices that use the VoIP ALG function (phones, video stations, softphones on PCs, etc.) are already marked as high priority and do not need to be manually configured in this list. This list is used to prioritize voice traffic from trunk interfaces of IP PBXs or other high priority devices that do not use the VoIP ALG function of the 5300-E.

α Enter the IP address of other high priority devices in the priority IP Addresses box.

You can enter individual IP addresses or a range using by appending a “-” character to the last octet. For example, 10.10.10.2-5 would specify 10.10.10.2, 10.10.10.3, 10.10.10.4 and 10.10.10.5 as voice devices.

5. Enable CAC

The 5300-E uses CAC to limit the number of active voice calls over the WAN link. This is necessary because a typical installation uses a ratio of 1:2 or 1:4 active voice calls to voice devices on the assumption that 50% or 25% of all users are on the phone at the same time. These ratios are guidelines only and at times the number of concurrent calls may exceed the amount of WAN bandwidth available to process the calls. In this instance existing phone calls will experience poor quality or be dropped all together. To prevent this from occurring a typical voice installation will set a threshold for the maximum number of concurrent voice calls supported by the WAN access link. New call requests in excess of this threshold will receive the equivalent of a “fast busy” and the WAN link will not become oversubscribed.

For IP Centrex installations the maximum number of concurrent voice calls is usually configured in the 5300-E by enabling CAC. When the 5300-E is deployed in IP PBX applications the maximum number of concurrent calls could be configured in the IP PBX. If the PBX is responsible for this setting you do not need to configure CAC in the 5300-E. Please check with your IT administrator to determine if this is the case.
6. Determine the maximum number of concurrent calls

The maximum number of concurrent calls that can be supported by the WAN access link is calculated using the following formula:

\[
\text{Max calls} = \frac{\text{Maximum WAN upstream bandwidth} \times .85}{\text{VoIP codec rate}}
\]

where,

- Maximum WAN upstream bandwidth = value entered in step D above (in Kbps)
- VoIP codec rate = 85.6Kbps for G.711 voice devices or 29.6Kbps for G.729 voice devices.

The maximum WAN upstream bandwidth is multiplied by .85 in the formula above to reduce the total bandwidth available for voice calls by 15%. This reduction is necessary because the 5300-E automatically reserves 15% of the total WAN bandwidth for low priority data traffic so that it is not starved completely. Starving data traffic completely would increase the number of retry attempts and exacerbate congestion on the link during periods of peak usage.

**Examples**

The maximum number of G.711 voice calls supported by a T1 (1.544 Kbps) WAN is calculated as follows:

\[
\frac{1544 \times .85}{85.6} = 15.3 \text{ or 15 total voice calls.}
\]

The maximum number of G.711 voice calls supported by a 768Kbps SDSL WAN is calculated as follows:

\[
\frac{768 \times .85}{85.6} = 7.6 \text{ or 7 total voice calls}
\]

The maximum number of G.711 voice calls supported by an ADSL WAN with 768Kbps downstream WAN bandwidth and 256Kbps upstream WAN bandwidth is calculated as follows:

\[
\frac{256 \times .85}{85.6} = 2.5 \text{ or 2 total voice calls}
\]

The maximum number of G.729 voice calls supported by an ADSL WAN with 768Kbps downstream WAN bandwidth and 256Kbps upstream WAN bandwidth is calculated as follows:

\[
\frac{256 \times .85}{29.6} = 7.4 \text{ or 7 total voice calls}
\]

7. After determining the maximum number of voice calls CAC is enabled as follows:

a. Select the Enable Call Admission Control checkbox.

b. Enter Maximum number of calls allowed as calculated above.

c. Press Submit.
A Closer Look at Traffic Management in the 5300-E

The traffic management mechanisms provided by the 5300-E are designed to ensure high priority real time voice and video traffic is processed before lower priority data traffic. At the same time, bandwidth not in use by voice and video traffic is made available so that data traffic can burst up to full line rate making efficient use of WAN bandwidth. Traffic management mechanisms are applied to traffic in both the upstream (LAN to WAN) and downstream (WAN to LAN) direction. Each direction is independent of the other and can support different size priority queues. This is particularly useful in the case of ADSL where the downstream bandwidth is greater than the upstream bandwidth and it would be undesirable to limit downstream data traffic to the rate of the slower upstream link.

Classifying

High priority voice and video traffic generated by endpoint devices is automatically identified by the V2IU’s VoIP Application Layer Gateway.

Upstream Traffic Management

The 5300-E appliance uses a combination of Class Based Queuing and simple classless queuing to send data in the upstream direction. The Class Based Queue (CBQ) consists of two priority classes (high and low), a scheduler to decide when packets need to be sent earlier than others and a traffic shaper to rate limit by delaying packets before they are sent. Voice and video traffic is placed in the high priority class and data traffic is placed in the low priority class. High priority data is sent out at up to the configured priority data rate and this class is polled before lower priority data to reduce overall latency for voice and video traffic. Although preferential treatment is given to priority data, it is bounded so that low priority data is not starved. To smooth bursts from high speed data links (typically from the LAN Ethernet segment to the WAN) the 5300-E appliance uses a buffer that clocks data out at a rate not exceeding the maximum amount for the slowest link. Any lasting burst condition will cause packets to be delayed and then dropped.

Downstream Traffic Management

In the upstream direction (LAN to WAN) it is easy to see how QoS mechanisms can be applied to traffic being sent by the 5300-E to guarantee sufficient bandwidth for voice traffic. We have control over how packets are handed to the WAN interface. In the downstream direction (WAN to LAN) we are installed at the CPE end of a service provider link and have no control over the amount of voice or data traffic being sent to the WAN interface. How then can we still guarantee the quality of voice traffic when it is entirely possible for an FTP session, for example, to consume the vast majority of downstream bandwidth?
Fortunately this is possible by shaping on both the egress LAN and egress WAN ports of the 5300-E appliance and leveraging the congestion avoidance mechanisms built into TCP to reduce the amount of data traffic on the link. Essentially, data packets received at a rate that exceeds the configured maximum are delayed (then dropped if necessary) when sent to the LAN interface by the 5300-E appliance. Similarly data traffic sent back to the 5300-E for transmission to the WAN are also delayed. This results in the end stations slowing down their transmit rate. This technique is quite effective in practice as end stations usually reduce their transmit rate before VoIP signaling has completed for new call setup.

For example consider the scenario where there are no voice calls over a SDSL WAN link and multiple FTP sessions are consuming all available bandwidth:

1. A new call request is received by the 5300-E from the WAN.
2. All signaling messages for the call are classified as voice traffic and prioritized for transmission over the LAN before servicing FTP data.
3. RTP traffic is similarly classified as voice traffic and treated with priority.
4. FTP data is buffered (or dropped) on the egress LAN port and ACKs are also delayed on the egress WAN port. This throttles the transmit rate of the FTP hosts to reduce overall WAN bandwidth consumption.

Excessive UDP traffic must be shaped in the service provider network, as UDP does not provide congestion avoidance mechanisms. The exception to this is in the case of RTP messages for voice traffic. Although RTP is based on UDP, the 5300-E appliance provides its own congestion avoidance mechanism for voice traffic using Call Admission Control (CAC).
System Diagnostics

The 5300-E provides a powerful set of diagnostic information, troubleshooting tools and utilities for system maintenance to network operators.

Viewing Software Version, Hardware Platform and the LAN MAC Address

The software version, hardware platform, and LAN MAC address are common pieces of information requested by technical support and are accessed directly through the System page of the 5300-E web GUI.

Viewing the ALG registration code

You will also find a link to the ALG registration code on the System page. The registration code enables the ALG and is pre-installed at the factory. If the registration code is inadvertently deleted you can re-enter the code using the following steps:
Enter the Registration Code

1. Select System.
2. Select registration code.
4. Enter the Registration Code.

The registration code can be found on the sticker located on the bottom of the 5300-E.
5. Press Submit.

Viewing Networking Information

To view the networking configuration and status of the 5300-E proceed to the Network Information page as follows:

1. Select System.
2. Select System Overview.
3. Select Network Information.

The following networking information is displayed:
**Routing Information**

The system routing table contains the static routes for hosts and networks that are configured on the 5300-E. If just the LAN and WAN IP addresses have been configured there will be four lines displayed:

- The private subnet will be associated with the LAN interface.
- A public subnet present for the WAN interface.
- An entry for the 5300-E loopback interface
- The 5300-E’s default gateway forwarding to the WAN interface

Additional lines may be displayed depending on the contents of the Route and VoIP Subnet Routing pages. Each of the entries on these pages will cause an additional entry in the routing table.

**Link Status**

Link Status displays the status of the Ethernet interfaces. Ethernet autonegotiation is often unreliable, especially between different vendors or old and new networking equipment. Failure of autonegotiation is generally not a cause for concern. However, if the negotiated rates change intermittently or the link is reported as down or no link, the link rate may need to be set manually on the Set Link Rate page. Intermittent data and voice outages may be caused by link flapping when the two endpoints of the Ethernet cable cannot reach agreement using autonegotiation". If the link rate is set manually, ensure that the device at the far end of the connection can communicate at the desired rate. Incompatible rates can cause a loss of communication with the 5300-E.

Link status for the Ethernet ports is displayed via the LEDs adjacent to each physical port.

**Interface Information**

The specific status and configuration information for the system interfaces is displayed in the Interface Information section. HDLC0 shows the interface statistics for the T1/E1 WAN link. ETH0 shows the interface statistics for the internal LAN interface between the 5300-E processor and the built-in LAN switch. Interface statistics for the external LAN ports are not displayed.

The interface statistics can point to areas of congestion in the network. If the errors statistic is a few percent or more of the total packets sent it may be an indication of excessive congestion on the network interface. If the congestion is not corrected the quality of voice calls will be affected. The topology of the network attached to the network interface with the errors should be examined and modified to better segment and isolate network traffic.
Viewing Advanced System Information

To view advanced system information for the 5300-E proceed to the System Information page as follows:

1. Select System.
2. Select System Overview.
3. Select System Information.

The following system information is displayed:

**System Uptime**

System Uptime displays the current time, the amount of time elapsed since the last system reboot, and the system load averages for the past 1, 5, and 15 minutes. Uptime can help trace when a power outage may have interrupted service. Load averages that remain greater than 2 indicate excessive system loading. Partitioning voice traffic using a second system may be required.

**Process Information**

Displays the active processes in the 5300-E.

**Memory Usage**

Displays detailed memory allocation information that may be of use to technical support.
System Logging Messages

Displays information logged during system boot and normal operation. Logging messages may indicate unauthorized attempts to access the 5300-E, process restart messages, and excessive resource utilization messages.

Passive Voice Call Monitoring

The 5300-E monitors live voice calls and performs objective speech quality assessment. This information enables the network operator to assess voice quality for the purposes of SLA tracking or problem isolation. Mean Opinion Score (MOS) results for RTP streams in both directions of a VoIP call are calculated at call completion. This information along with the IP addresses of the VoIP endpoints supporting the call are logged locally and optionally sent to an external syslog server (see Enable Remote System Logging for instructions on enabling logging to a remote syslog server). Additionally the 5300-E will generate a real-time message for any MOS values calculated less than 2.5 (considered poor quality) during an active call.

Voice call quality information is found locally in the System Logging Messages section of the System Information page and a sample output is provided below.

Accessing Troubleshooting Tools

The 5300-E provides convenient test tools to facilitate problem isolation and resolution. A network operator can use these tools to verify connectivity to/from the 5300-E as well as trace datapaths to endpoints throughout the network.
Verify Registered Voice Devices

The 5300-E maintains a list of all registered voice and video devices called a “clients list” so that it can properly route voice and video calls. At startup, voice and video devices register their IP addresses with the 5300-E. The 5300-E then registers on behalf of the voice and video devices by providing its own WAN IP address to the softswitch, gatekeeper, or IP PBX. If a user or network operator reconfigures the IP address of the voice and video device, it will re-register the new address with the 5300-E. In this instance voice and video calls may be routed improperly because the 5300-E clients list contains out of date information.

To update the clients list simply highlight and delete the stale entry using the following steps:

1. Select System.
2. Select System Overview.
3. Select Clients List.
4. Proceed to the appropriate signaling section, highlight the duplicate entry or entries and press the delete key on the keyboard.
5. Press Submit.
6. Restart the VoIP ALG by following the instructions found in Restarting Networking Processes.
Performing a Ping Test

A ping test is the most common test used to verify basic connectivity to a networking device. Successful ping test results indicate that both physical and virtual path connections exist between the 5300-E and the test IP address. Successful ping tests do not guarantee that all data traffic is allowed between the 5300-E and the test IP address but is useful to verify basic reachability.

The following steps are used to perform a ping test:
1. Select System.
2. Select System Overview.
4. Enter the IP Address to Ping.
5. Press Ping.

The Network Test Tools page will be refreshed and the results of the ping test are displayed (this may take several seconds). The Reset button is used to clear the IP address entry used in step D above.

Performing a Traceroute Test

A traceroute test is used to track the progress of a packet through the network. The test can be used to verify that data destined for a WAN device reaches the remote IP address via the desired path. Similarly, internal network paths can be traced over the LAN to verify the local network topology. The following steps are used to perform a traceroute test:
1. Select System.
2. Select System Overview.
4. Enter the IP address to Trace.
5. Select either the WAN or the LAN radio button
6. Press Traceroute.

The Network Test Tools page will be refreshed and the results of the traceroute test are displayed (this may take several seconds). The Reset button is used to clear the IP address entry used in step D above.

Performing a VoIP Traffic Test

The 5300-E includes the VoIP Test Module traffic simulation client manufactured by NetIQ. The client allows remote monitoring of the quality of service that can be delivered to the 5300-E.

The simulation client can be activated on the 5300-E and then controlled remotely by a NetIQ console test application (sold separately). The test application can initiate VoIP tests as well as other data sessions between the test client in the 5300-E and test clients placed in other parts of the network to simulate different traffic patterns. Latency, jitter, MOS scores, and other QoS or data measurements can be reported by the console test application. The following steps configure the traffic simulation client:

1. Select System.
2. Select System Overview.
4. Select the Enable Endpoint checkbox.
5. Enter the Endpoint IP Address.
6. This is IP address of the remote test client.
7. Enter the Console IP Address.
8. This is the IP address of the workstation running the netIQ console.
9. Press Submit.

The following steps are used to disable the traffic simulator:

1. Select System.
2. Select System Overview.
4. Uncheck the Enable Endpoint checkbox.
5. Press Submit.

Warning

The traffic simulator should be used for testing purposes only. Do not leave the traffic simulator enabled for extended periods of time as it generates simulated traffic that may interrupt and negatively impact the quality of voice calls.
Restarting Networking Processes

In extreme circumstances while troubleshooting you may be asked to restart the networking processes including the VoIP ALG in the 5300 by technical support. Use the following steps to restart the networking processes:

1. Select System.
2. Select System Overview.
4. Press restart.

**Warning**

Restarting network services will interrupt the system for up to a minute. All voice and data sessions currently in progress will be interrupted.

Rebooting the 5300-E

In extreme circumstances while troubleshooting you may be asked to reboot the 5300-E by technical support. Please use the following steps to reboot the system:

1. Select System.
2. Select System Overview.
3. Select Rebooting System.
4. Press reboot.

Alternatively a reset can be performed locally by temporarily disconnecting the power cable from the 5300-E.

**Warning**

Rebooting the system will interrupt services for a few minutes. All voice and data sessions currently in progress will be interrupted.
Saving and Restoring the 5300-E Configuration

The 5300-E stores all configuration information for the system in a series of individual files that reside in local flash memory. These files are read at boot time to determine the configuration identity of the 5300-E and then stored in RAM as “running” state. As you configure the 5300-E the submit command writes the configuration changes to both RAM and flash so that the files stored in flash are always up to date with the running state of the system.

The 5300-E provides a utility that enables you to copy the individual configuration files stored in flash to a single, consolidated backup file. This single file can then be used as a backup for the entire system and restored at a later date if necessary. Multiple backup files with different system configurations can also be created and stored locally in the 5300-E or on remote TFTP servers.

### Note

No more than 2 backup files can be stored in the 5300-E flash due to size constraints. Also, it is recommended that you create a backup file after any configuration changes are made to the 5300-E. This is to prevent the loss of any configuration changes made since your last backup in the event that you must restore the system configuration.

Backup file operations are performed in the 5300-E CLI using the ewn command.

### The ewn Command

The syntax for the ewn command is as follows:

**USAGE:**

- `ewn help|list`
- `ewn save|load|delete [file name]`
- `ewn upload|download [file name] [ip address]`

where file name must use extension .conf1 or .conf2
The `ewn` command can be used with a local terminal connection or remotely using SSH.

1. Use a NULL modem cable to connect to serial port 1 of the 5300-E
2. Use a terminal emulator such as Hyperterminal set to a baud rate of 115200, 8, 1 and none (databits, stop bits and parity)

Alternatively you can connect to the 5300-E remotely using SSH:

1. Logon as root
2. Enter the password

Once you are at the command prompt (bash#) you can create the backup file, store it to local flash, copy it to a remote TFTP server, copy it from a remote TFTP server, delete it, load it or list all available backup files.

---

### Create a Backup File and Save in Local Flash

bash# `ewn save <filename>`

Saves the current running configuration.

Filename format (must use extension .conf1 or .conf2):
- `<filename1>.conf1`
- `<filename2>.conf2`
- `<filenameX>` can be a combination of both letters and characters. For example, EWN300_041503.conf1 or location1_E300.conf2. Trying to use any other filename format will result in the error message: “EWN_ERROR_BAD_FILE_NAME”.

**Warning**
The `.conf` extensions have special significance. If you save a configuration with `<filename-new>.conf1`, then any existing `<filename-old>.conf1` will be overwritten with the new one.

### Copy a Backup File to a Remote TFTP Server

bash# `ewn upload <filename> <tftp server IP Address>`

Copy a backup file from the 5300-E to a TFTP server.

### Download a Backup File from a Remote TFTP Server

bash# `ewn download <filename> <tftp server IP Address>`

Download a backup file from a TFTP server to the 5300-E.

### List the Available Backup Files

bash# `ewn list`
List all backup files stored in FLASH. If no file has been saved, the command will only return the # prompt.

**Delete a Backup File**

```
bash# ewn delete <filename>
```

Delete the backup file specified in the filename.

**Load a Backup File so that it Becomes the Running Configuration**

```
bash# ewn load <filename>
```

Loads the specified backup file into RAM and makes it the active running configuration.

**Warning**

Issuing this command will automatically restart the 5300-E and therefore interrupt any active voice calls and data sessions.
Upgrading the 5300-E

This chapter describes how to upgrade your 5300-E to the latest software release available from Polycom.

Upgrade Procedure for Software Revision 1.3.11 or Later

Use this procedure if your 5300-E is running software revision 1.3.11 or later. The software version can be found on the System page of the web GUI.

1. Select System.
2. Select System Overview.
3. Select Upgrade firmware.

Warning
When you update your software telephone services will be unavailable for several minutes. It is therefore advised that upgrades be performed during a maintenance window when telephone traffic can be interrupted.
4. Enter the Download Server address of ftp.support.polycom.com
5. Enter the Filename: flash.bin
6. Press Submit.
   You can follow the progress of the upgrade by selecting the refresh the upgrade status link.

**Warning**

Do not change the configuration or power off the device until the write is 100 percent complete. The 5300-E may become unusable if the write is interrupted. The flash write can take up to 5 minutes depending on the speed of the download server.

The system will automatically restart after the new image has been loaded.

7. Verify that the upgrade was successful by checking the software revision number found on the System page.
Appendix

Troubleshooting Tips

This section contains possible solutions to problems regarding the installation of the 5300-E.

I am having trouble reaching the Internet through the 5300-E.

We recommend connecting a PC directly (or via a switch) to the LAN port of the 5300-E. The default LAN IP address of the 5300-E is 192.168.1.1 so please be sure that the IP address of the PC is on the same network (e.g., 192.168.1.2). Once you have connected please verify that the IP configuration information in the Network page is correct. Some other items to try:

- Ping the WAN interface of the 5300-E from the attached PC
- Ping the DNS server for your network. Sometimes connectivity problems occur when the domain name being used cannot be mapped to the proper IP address.
- Ping a well known address on the Internet.
- Ping the IP address of the remote softswitch or IP PBX.

I do not receive dial tone when going “off hook” or my phone will not register with the softswitch/IP PBX.

- Verify the configurations on the VoIP ALG page.
- Check that the ALG registration code is configured
  - Select System.
  - Select registration code.
- Attempt to ping the softswitch using the ping tool in the web gui
  - Select System.
  - Select System Overview.
Select Network Test Tools.

Enter the softswitch address in the IP Address to Ping field.

Press Ping.

### Specifications

<table>
<thead>
<tr>
<th></th>
<th>5300-E:</th>
<th>5300T:</th>
<th>5300T2:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WAN Port</strong></td>
<td>1x10/100 Ethernet</td>
<td>1xT1 CSU/DSU</td>
<td>2xT1 CSU/DSU</td>
</tr>
<tr>
<td><strong>LAN Port</strong></td>
<td></td>
<td>1x10/100 Ethernet</td>
<td></td>
</tr>
<tr>
<td><strong>T1 WAN</strong></td>
<td>T1/E1—RJ 45 Connector, Integrated CSU/DSU</td>
<td>Full T1/E1</td>
<td></td>
</tr>
<tr>
<td><strong>Management Ports</strong></td>
<td>1xRS-232 Serial, 1x10/100 Ethernet</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Dimensions</strong></td>
<td>19” Rack Mount, 1RU</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Weight</strong></td>
<td>11.5 lbs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Power</strong></td>
<td>100/240v VAC, manual selecting, 47 to 63 Hz</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Warranty</strong></td>
<td>1 Year</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Regulatory Notices

**Important Safeguards**

Read and understand the following instructions before using the system:

- Close supervision is necessary when the system is used by or near children. Do not leave unattended while in use.
- Only use electrical extension cords with a current rating at least equal to that of the system.
- Always disconnect the system from power before cleaning and servicing and when not in use.
- Do not spray liquids directly onto the system when cleaning. Always apply the liquid first to a static free cloth.
- Do not immerse the system in any liquid or place any liquids on it.
- Do not disassemble this system. To reduce the risk of shock and to maintain the warranty on the system, a qualified technician must perform service or repair work.
- Connect this appliance to a grounded outlet.
- Only connect the system to surge protected power outlets.
- Keep ventilation openings free of any obstructions.

SAVE THESE INSTRUCTIONS.

**END-USER LICENSE AGREEMENT FOR POLYCOM® SOFTWARE**

**IMPORTANT-READ CAREFULLY BEFORE USING THE SOFTWARE PRODUCT:**

This End-User License Agreement ("Agreement") is a legal agreement between you (and/or any company you represent) and either Polycom (Netherlands) B.V. (in Europe, Middle East, and Africa), Polycom Hong Kong, Ltd. (in Asia Pacific) or Polycom, Inc. (in the rest of the world) (each referred to individually and collectively herein as “POLYCOM”), for the SOFTWARE PRODUCT licensed by POLYCOM. The SOFTWARE PRODUCT includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By clicking "I AGREE" or by installing, copying, or otherwise using the SOFTWARE PRODUCT, you...
agree to be and will be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, your use is prohibited and you may not install or use the SOFTWARE PRODUCT.

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed (not sold) to you, and its use is subject to the terms of this Agreement. This is NOT a sale contract.

1. **GRANT OF LICENSE.** Subject to the terms of this Agreement, POLYCOM grants to you a non-exclusive, non-transferable, revocable license to install and use the SOFTWARE PRODUCT solely on the POLYCOM product with which this SOFTWARE PRODUCT is supplied (the "PRODUCT"). You may use the SOFTWARE PRODUCT only in connection with the use of the PRODUCT subject to the following terms and the proprietary notices, labels or marks on the SOFTWARE PRODUCT or media upon which the SOFTWARE PRODUCT is provided. You are not permitted to lease, rent, distribute or sublicense the SOFTWARE PRODUCT, in whole or in part, or to use the SOFTWARE PRODUCT in a time-sharing arrangement or in any other unauthorized manner. Further, no license is granted to you in the human readable code of the SOFTWARE PRODUCT (source code). Except as expressly provided below, this License Agreement does not grant you any rights to patents, copyrights, trade secrets, trademarks, or any other rights in respect to the SOFTWARE PRODUCT.

2. **OTHER RIGHTS AND LIMITATIONS.**
   
   2.1 **Limitations on Reverse Engineering, Decompilation, and Disassembly.** You may not reverse engineer, decompile, modify or disassemble the SOFTWARE PRODUCT or otherwise reduce the SOFTWARE PRODUCT to human-perceivable form in whole or in part, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one PRODUCT. You may not use the SOFTWARE PRODUCT for any illegal purpose or conduct.

   2.2 **Back-up.** Except as expressly provided for under this Agreement you may not copy the SOFTWARE PRODUCT; except, however, you may keep one copy of the SOFTWARE PRODUCT and, if applicable, one copy of any previous version, for back-up purposes, only to be used in the event of failure of the original. All copies of the SOFTWARE PRODUCT must be marked with the proprietary notices provided on the original SOFTWARE PRODUCT. You may not reproduce the supporting documentation accompanying the SOFTWARE PRODUCT.

   2.3 **No Modifications.** You may not modify, translate or create derivative works of the SOFTWARE PRODUCT.

   2.4 **Proprietary Notices.** You may not remove or obscure any proprietary notices, identification, label or trademarks on or in the SOFTWARE PRODUCT or the supporting documentation.
2.5 Software Transfer. You may permanently transfer all of your rights under this Agreement in connection with transfer of the PRODUCT, provided you retain no copies, you transfer all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades, this Agreement, and, if applicable, the Certificate of Authenticity), and the recipient agrees to the terms of this Agreement. If the SOFTWARE PRODUCT is an upgrade, any transfer must include all prior versions of the SOFTWARE PRODUCT. However, if the SOFTWARE PRODUCT is marked "Not for Resale" or "NFR", you may not resell it or otherwise transfer it for value.

2.6 Copyright. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by POLYCOM or its suppliers. Title, ownership rights, and intellectual property rights in the SOFTWARE PRODUCT shall remain in POLYCOM or its suppliers. Title and related rights in the content accessed through the SOFTWARE PRODUCT is the property of such content owner and may be protected by applicable law. This Agreement gives you no rights in such content.

2.7 Confidentiality. The SOFTWARE PRODUCT contains valuable proprietary information and trade secrets of POLYCOM and its suppliers that remains the property of POLYCOM. You shall protect the confidentiality of, and avoid disclosure and unauthorized use of, the SOFTWARE PRODUCT.

2.8 Dual-Media Software. You may receive the SOFTWARE PRODUCT in more than one medium. Regardless of the type or size of medium you receive, you may use only one medium that is appropriate for your single PRODUCT. You may not use or install the other medium on another PRODUCT.

2.9 Reservation of Rights. POLYCOM reserves all rights in the SOFTWARE PRODUCT not expressly granted to you in this Agreement.

2.10 Additional Obligations. You are responsible for all equipment and any third party fees (such as carrier charges, internet fees, or provider or airtime charges) necessary to access the SOFTWARE PRODUCT.

3. SUPPORT SERVICES. POLYCOM may provide you with support services related to the SOFTWARE PRODUCT ("SUPPORT SERVICES"). Use of SUPPORT SERVICES is governed by the POLYCOM policies and programs described in the POLYCOM-provided materials. Any supplemental software code provided to you as part of the SUPPORT SERVICES is considered part of the SOFTWARE PRODUCT and is subject to the terms and conditions of this Agreement. With respect to technical information you provide to POLYCOM as part of the SUPPORT SERVICES, POLYCOM may use such information for its business purposes, including for product support and development. POLYCOM will not utilize such technical information in a form that personally identifies you.
4. TERMINATION. Without prejudice to any other rights, POLYCOM may terminate this Agreement if you fail to comply with any of the terms and conditions of this Agreement. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts. You may terminate this Agreement at any time by destroying the SOFTWARE PRODUCT and all of its component parts. Termination of this Agreement shall not prevent POLYCOM from claiming any further damages. If you do not comply with any of the above restrictions, this license will terminate and you will be liable to POLYCOM for damages or losses caused by your non-compliance. The waiver by POLYCOM of a specific breach or default shall not constitute the waiver of any subsequent breach or default.

5. UPGRADES. If the SOFTWARE PRODUCT is labeled as an upgrade, you must be properly licensed to use the software identified by POLYCOM as being eligible for the upgrade in order to use the SOFTWARE PRODUCT. A SOFTWARE PRODUCT labeled as an upgrade replaces and/or supplements the software that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded SOFTWARE PRODUCT only in accordance with the terms of this Agreement. If the SOFTWARE PRODUCT is an upgrade of a component of a package of software programs that you licensed as a single product, the SOFTWARE PRODUCT may be used and transferred only as part of that single SOFTWARE PRODUCT package and may not be separated for use on more than one PRODUCT.

6. WARRANTY AND WARRANTY EXCLUSIONS.

6.1 Limited Warranty. POLYCOM warrants that (a) the SOFTWARE PRODUCT will perform substantially in accordance with the accompanying documentation for a period of ninety (90) days from the date of receipt by you, and (b) any SUPPORT SERVICES provided by POLYCOM shall be substantially as described in applicable written materials provided to you by POLYCOM. POLYCOM does not warrant that your use of the SOFTWARE PRODUCT will be uninterrupted or error free, or that all defects in the SOFTWARE PRODUCT will be corrected. You assume full responsibility for the selection of the SOFTWARE PRODUCT to achieve your intended results and for the installation, use and results obtained from the SOFTWARE PRODUCT. POLYCOM’s sole obligation under this express warranty shall be, at POLYCOM’s option and expense, to refund the purchase price paid by you for any defective software product which is returned to POLYCOM with a copy of your receipt, or to replace any defective media with software which substantially conforms to applicable POLYCOM published specifications. Any replacement SOFTWARE PRODUCT will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

6.2 Warranties Exclusive. IF THE SOFTWARE PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, YOUR SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT POLYCOM’S SOLE OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR
IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. POLYCOM NEITHER Assumes NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF THE SOFTWARE PRODUCT. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM POLYCOM OR THROUGH OR FROM THE SOFTWARE PRODUCT SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS AGREEMENT.

POLYCOM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE SOFTWARE PRODUCT DOES NOT EXIST OR WAS CAUSED BY YOUR OR ANY THIRD PARTY’S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, POWER CUTS OR OUTAGES, OTHER HAZARDS, OR ACTS OF GOD.

7. LIMITATION OF LIABILITY. YOUR USE OF THE SOFTWARE PRODUCT IS AT YOUR SOLE RISK. YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OR USE OF THE SOFTWARE PRODUCT. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL POLYCOM OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF POLYCOM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, POLYCOM’S ENTIRE LIABILITY SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE PRODUCT OR U.S. $5.00. PROVIDED, HOWEVER, IF YOU HAVE ENTERED INTO A POLYCOM SUPPORT SERVICES AGREEMENT, POLYCOM’S ENTIRE LIABILITY REGARDING SUPPORT SERVICES SHALL BE GOVERNED BY THE TERMS OF THAT AGREEMENT.

8. INDEMNITY. You agree to indemnify and hold harmless POLYCOM and its subsidiaries, affiliates, officers, agents, co-branders, customers or other partners, and employees, from any loss, claim or demand, including reasonable attorneys’ fees, made by any third party due to or arising out of your use of the SOFTWARE PRODUCT, your connection to the SOFTWARE PRODUCT, or your violation of the Terms.
9. DISCLAIMER. Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety due to local law, they will be limited to the duration of the applicable warranty.

10. EXPORT CONTROLS. The SOFTWARE PRODUCT may not be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iraq, Libya, North Korea, Yugoslavia, Iran, Syria, Republic of Serbia, or any other country to which the U.S. has embargoed goods; or (ii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. By downloading or using the SOFTWARE PRODUCT, you are agreeing to the foregoing and you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list. If you obtained this SOFTWARE PRODUCT outside of the United States, you are also agreeing that you will not export or re-export it in violation of the laws of the country in which it was obtained.

11. MISCELLANEOUS.


11.2 Entire Agreement. This Agreement represents the complete agreement concerning the SOFTWARE PRODUCT and may be amended only by a writing executed by both parties. If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

11.3 Contact. If you have any questions concerning this Agreement, or if you desire to contact POLYCOM for any reason, please contact the POLYCOM office serving your country.

11.4 U.S. Government Restricted Rights. The SOFTWARE PRODUCT and documentation are provided with RESTRICTED RIGHTS. The SOFTWARE PRODUCT programs and documentation are deemed to be "commercial computer software" and "commercial computer software documentation", respectively, pursuant to DFAR Section 227.7202 and FAR 12.212(b), as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the SOFTWARE PRODUCT programs and/or documentation by the U.S. Government or any of its agencies shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Any technical data provided that is not covered by the above provisions is deemed to be "technical data-commercial items" pursuant to DFAR Section 227.7015(a).
Any use, modification, reproduction, release, performance, display or disclosure of such technical data shall be governed by the terms of DFAR Section 227.7015(b).

BY INSTALLING, COPYING, OR OTHERWISE USING THIS SOFTWARE PRODUCT YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTAND AND AGREE TO BE BOUND BY THE TERMS AND CONDITIONS INDICATED ABOVE.

Polycom, Inc. © 2007. ALL RIGHTS RESERVED.

4750 Willow Road
Pleasanton, CA 94588
U.S.A.

Software included in this product contains a module called PsyVoIP which is protected by copyright and by European, US and other patents and is provided under licence from Psytechnics Limited.

Portions of this product also include software sponsored by the Free Software Foundation and are covered by the GNU GENERAL PUBLIC LICENSE:

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).

Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of
the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the
conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation. each version.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make
exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

FCC PART 15 NOTICE

This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Industry Canada NOTICE

This Class (A) digital apparatus complies with Canadian ICES-003.