

Polycom® VBP™ System Configuration Guide

Trademark Information

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

© 2009 Polycom, Inc. All rights reserved.

Polycom Inc.
4750 Willow Road
Pleasanton, CA 94588-2708
USA

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Polycom, Inc. retains title to, and ownership of, all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g. a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc. is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

Export Notice

This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or re-export may be required by the U.S. Department of Commerce.

Regulatory Compliance

This product was tested to comply with FCC standards for home and office use. It also meets the applicable Industry Canada Terminal Equipment Technical Specifications and VCCI standards.

Licensing

Use of this product is subject to Edgewater Networks Software License Agreement. Portions of this product include software sponsored by the Free Software Foundation and are covered by the GNU GENERAL PUBLIC LICENSE.

Release Date:

October 7, 2009

Feature Summary	6
System Configuration.....	8
Configuring VBP-E Network Settings	9
Configure WAN settings	9
Configure WAN ADSL-PPPoE	9
Configure WAN DHCP	10
Configure WAN Static IP Address.....	11
Configuring VBP-ST Network Settings	12
Configure Subscriber and Provider settings.....	12
Subscriber Interface Settings	12
Provider Interface Settings	13
Configuring LAN Settings	14
Configure LAN network settings without VLANs	14
Configure LAN network settings with VLANs	14
Configuring VLANs	14
Set up VLANs on the 4350.....	15
Set up VLANs on the 5300-E and 6400-E series.....	15
Delete a VLAN.....	15
Configuring Ethernet Interface Link Settings.....	15
SNMP Overview.....	16
Configure SNMP.....	17
Disable SNMP	18
Delete an SNMP trap.....	18
Configuring DHCP Services	18
DHCP Relay	18
DHCP Server.....	19
Configuring DHCP Server	20
Configuring DHCP With VLANs	21
DHCP Leases.....	22
Firewall rules for securing the network	23
VBP Firewall Basics.....	23
VBP-E Whitelist/Blacklist rules	23
Whitelist	24
Blacklist	24
VBP-E or VBP-S and ST blocking management ports.....	26
VBP-E management ports.....	26
Trusted Management Addresses	27
VBP-S or ST management ports.....	28
CERT Advisory CA-2004-01.....	30
DMZ installation of the VBP – Required Ports.....	31
VBP Topologies	36

Overview	36
Centralized Gatekeeper Diagram	37
Distributed Gatekeeper Diagram - 1.....	38
Distributed Gatekeeper Diagram - 2.....	39
Configuring the VBP E-Series Appliance for LAN-side Gatekeeper Mode	40
Alias Manipulation	43
Configuring the VBP E-Series Appliance for Embedded Gatekeeper Mode.....	44
Example for prefix routing to simplify dialing using the DST E.164 as a prefix.....	47
Peering Proxy Overview	49
How Peering Proxy Works	49
Configuring the VBP E-Series Appliance for Peering-Proxy Mode.....	52
Regular Expressions	54
Centralized Gatekeeper Configuration.....	56
Centralized Gatekeeper DiagramConfiguring the VBP S and ST-Series Appliance for Provider-side gatekeeper mode.....	57
Configuring the VBP S and ST-Series Appliance for Provider-side gatekeeper mode.....	58
Configuring the VBP E-Series Appliance for WAN-side Gatekeeper Mode.....	60
Access Proxy Summary and Configuration	61
Access Proxy Diagram	62
NAT routers tested	63
Software requirements for Interoperability	63
Prerequisites.....	64
Configuration steps for the CMA server	65
Screen shots for CMA “sites”	68
Configuration steps for the VBP-ST	69
Configure the VBP-ST VoIP ALG H.323 settings.....	70
CMA Desktop Configuration.....	73
HDX Configuration.....	75
Troubleshooting Access Proxy.....	77
Traffic Shaper Configuration	85
Configuring the Traffic Shaper	85
Diagnostics and Troubleshooting.....	87
Viewing Version, Hardware Platform and LAN MAC Address	87
Viewing the ALG Registration Code.....	87
Entering the Registration Code	87
Viewing Networking Information.....	88
Link Status.....	88
Interface Information	88
Using Troubleshooting Tools.....	89
Ping and Traceroute Tests	89
Networking Restart.....	90
Rebooting the System	90
Reboot the system.....	90

Using T1 Diagnostics	91
Perform T1 diagnostics	91
View T1 Statistics	91
View advanced T1 diagnostics.....	91
Device Configuration Management.....	92
Overview	92
Using the configuration backup command	92
Creating a backup file and save to local flash.....	93
Copy a backup file to a remote TFTP server	93
Download a backup file from a remote TFTP server.....	93
List available backup files.....	93
Delete a backup file.....	93
Loading a backup file to become the running configuration.....	94
Regulatory Notices.....	95
END-USER LICENSE AGREEMENT FOR POLYCOM® SOFTWARE.....	95
Appendix A. Compliance and Compatibility for the VBP 200EW Converged Network Appliance.....	103
WIRELESS	103
INDUSTRY CANADA (IC) NOTICE.....	103
Appendix B. Compliance and Compatibility for the VBP 4350 Converged Network Appliance	105
JAPAN EMC COMPATIBILITY.....	105
FCC PART 68 NOTICE TO USERS OF DIGITAL SERVICE.....	105
Appendix C. Compliance and Compatibility for the VBP 4350W Converged Network Appliance.....	107
WIRELESS	107
INDUSTRY CANADA (IC) NOTICE.....	107
Appendix D. Compliance and Compatibility for the VBP 5300S Converged Network Appliance.....	109
FCC PART 15 NOTICE	109
Industry Canada NOTICE.....	109
Appendix E. Compliance and Compatibility for the VBP 5300E Converged Network Appliance.....	110
FCC PART 15 NOTICE	110
Industry Canada NOTICE.....	110
Appendix F. Compliance and Compatibility for the VBP 6400S Converged Network Appliance	111
Appendix G. Compliance and Compatibility for the VBP 6400E Converged Network Appliance.....	114

Feature Summary

The Video Border Proxy (VBP) Series features intelligent, all-in-one networking solutions for enterprises and service providers. These solutions reduce costs by simplifying the deployment, management and security of converged voice, video and data networks. The following table lists the important functions provided by each model of the VBP Series:

Function	200 EW	4350 and 4350EW	5300-E	5300-S & ST	6400-E	6400-S & ST
Resolves NAT/firewall traversal problems by providing an application layer gateway (ALG) that supports voice and H.323 protocols	X	X	X	X	X	X
Protects the enterprise LAN using a stateful packet inspection (SPI) firewall for both H.323 and data traffic	X	X	X		X	
Protects the enterprise LAN using a stateful packet inspection (SPI) firewall for H.323 traffic				X		X
Application aware firewall dynamically provisions and closes UDP ports used for H.323 calls	X	X	X	X	X	X
Provides NAT and PAT for data that hides enterprise LAN topology	X	X	X		X	
Provides NAT and PAT for H323 that hides enterprise LAN topology	X	X	X	X	X	X
Provides integrated tools to facilitate problem isolation	X	X	X	X	X	X
Uses a simple web based GUI for configuration	X	X	X	X	X	X
Site-to-site networking using IPSec: 3DES, SHA-1	X	X				
Performs static IP routing	X	X	X	X	X	X
Supports logging to external syslog servers	X	X	X	X	X	X

Function	200 EW	4350 and 4350EW	5300-E	5300-S & ST	6400-E	6400-S & ST
Provides a DHCP server for enterprise PCs and video devices	X	X	X		X	
Supports Access Proxy – requires H.460 traversal “ST” - S systems will need to be upgraded				X		X
Provides H.460-based traversal support (1)				X		X
Supports up to 1 Mbps of H.323 traffic - or up to 35 Mbps data traffic	X					
Supports up to 3 Mbps of H.323 traffic - or up to line rate for data traffic		X				
Supports up to 10 Mbps of H.323 traffic - or up to line rate for data traffic			X			
Supports up to 25 Mbps of H.323 traffic - or up to line rate for data traffic			X			
Supports up to 25 Mbps of H.323 traffic (2)				X		
Supports up to 85 Mbps of H.323 traffic - or up to line rate for data traffic					X	
Supports up to 85 Mbps of H.323 traffic (2)						X
Supports T1 and Ethernet WAN types		X				
Supports Ethernet WAN types	X	X	X	X	X	X
Supports WAN protocols, DHCP, ADSL-PPPoE, Static IP	X	X				
Supports WAN protocols, DHCP, Static IP			X	X	X	X
Supports up to 16 VLAN's	X	X	X		X	

(1) ST models only

(2) ST models do not support data NAT related features

System Configuration

You can configure the Video Border Proxy (VBP) series appliance to support a wide range of network services and enable or disable specific services based on the requirements of your network.

This chapter explains how to configure the VBP series appliance to function in your IP network. You will configure the Ethernet interfaces, network addresses, DNS settings, default gateway, SNMP settings, DHCP services, firewall settings, and change the administrative password.

Configuring VBP-E Network Settings

Note: Ask your ISP to assign an IP address for the VBP series appliance, an IP address for the gateway, and a preferred and secondary IP address for the DNS server.

Configure WAN settings

1. Choose **Network** from the Configuration Menu.
 2. Select the method to use to obtain an Internet connection.
 3. When you select a connection method, the page displays the appropriate settings in the WAN Interface Settings area.
 - a. ADSL-PPPoE—Enter the user name and password assigned by the network provider, and indicate whether to monitor the connection using keepalive ping messages.
 - b. DHCP—No additional configuration required.
 - c. Static IP Address—Enter the IP address and subnet mask.
 - d. T1—Enter the IP address and subnet mask. Click the underlined T1 link to open the T1 Configuration page and set additional T1 parameters.
 4. Click **Submit**.
- A message indicates that service will be temporarily interrupted.
5. Click **OK** to confirm.

Configure WAN ADSL-PPPoE

ADSL-PPPoE (1)

Select to display these options. When selected the WAN Ethernet port will perform a PPP negotiation to obtain and IP address, this IP will be assigned to the ppp0 interface viewable in the “Network Information page” a link to this page is provided. The default gateway and DNS servers are also sent to the system in the DHCP reply.

User Name (2)

Enter user name your ISP has assigned to your DSL account.

Password (3)

Enter password for your user name your ISP has assigned to your DSL account

WAN Interface Settings: 1

ADSL-PPPoE
 DHCP
 Static IP Address
 T1/E1

Enter the username and password given to you by your network provider.

User Name: 2

Password: 3

Keepalive Ping: 4

PPP Link Status: down

To see the IP address given to the WAN port, check the [Network Information page](#).

Note: In case of dynamic links, this DNS server address will override the DNS server address obtained from the Servers. Default value for dynamic links is obtained from the server, if left blank .

Primary DNS Server: 5

Secondary DNS Server: 6

Keepalive Ping (4)

Selected by default to send an LCP-echo request, this is called a link control protocol “ping” not to be confused with ICMP based ping. The PPP LCP “ping” interval is every 60 seconds; if 3 request are not responded to (180 seconds) the system will re-establish the PPP connection. When this happens you may receive a different IP address. For this reason it is recommended to setup a “Dynamic DNS” account, this allows remote locations to enter a DNS name to dial your location. (see the Dynamic DNS page under “System”) see RFC 1661 for PPP related information.

Primary DNS Server (5)

Entering static DNS information for a dynamic WAN type will override what is received during PPP negotiation

Secondary DNS Server (6)

Entering static DNS information for a dynamic WAN type will override what is received during PPP negotiation

Configure WAN DHCP

DHCP (1)

Select to choose this option. When selected the WAN Ethernet port will perform a DHCP negotiation to obtain and IP address, this IP will be assigned to the eth1 interface viewable in the “Network Information page” a link to this page is provided. The default gateway and DNS servers are also sent to the system in the DHCP reply.

Primary DNS Server (2)

Entering static DNS information for a dynamic WAN type will override what is received during DHCP negotiation

Secondary DNS Server (3)

Entering static DNS information for a dynamic WAN type will override what is received during DHCP negotiation

WAN Interface Settings:

1 ADSL-PPPoE
 DHCP
 Static IP Address
 T1/E1

To see the IP address given to the WAN port, check the [Network Information page](#).

Note: In case of dynamic links, this DNS server address will override the DNS server address obtained from the Servers. Default value for dynamic links is obtained from the server, if left blank .

Primary DNS Server: 2

Secondary DNS Server: 3

Configure WAN Static IP Address

Static IP Address (1)

Select to display these options

IP Address (2)

Enter IPv4 IP address

Subnet Mask (3)

Enter subnet mask as appropriate, default gateway must be in this subnet

Default Gateway (4)

Enter IP address of the upstream (WAN) router

Primary DNS Server (5)

Enter primary DNS server IP

Secondary DNS Server (6)

Enter Secondary DNS server IP

WAN Interface Settings:

ADSL-PPPoE
 DHCP
 Static IP Address
 T1/E1

IP Address:

Subnet Mask:

Network Settings:
 Default Gateway:

Note: In case of dynamic links, this DNS server address will override the DNS server address obtained from the Servers. Default value for dynamic links is obtained from the server, if left blank.

Primary DNS Server:

Secondary DNS Server:

Note: The VBP WAN interface must be assigned a publicly routable IP address. Assigning a RFC1918 address to the WAN interface is not supported

Configuring VBP-ST Network Settings

Configure Subscriber and Provider settings

1. Choose **Network** from the Configuration Menu.
2. Configure all parameters indicated, double check that you have the correct IP's for the interfaces as defined
3. Click **Submit**.

A message indicates that service will be temporarily interrupted.

4. Click **OK** to confirm.

Subscriber Interface Settings

IP Address (1)

Enter the IPv4 IP address, while this interface is call "Subscriber" its commonly placed on the Internet or WAN side of the network. The default IP address is 192.168.1.1 while this IP is associated to the LAN, it is used by default on the Subscriber interface. The reason for this is for configuring the system for the first time for documentation procedures of attaching your PC to "port 1" to reach 192.168.1.1, when you reconfigure the Public IP on the Subscriber interface, and the firewall is enabled, you will place this interface on the public network

Note: The firewall is disabled on ST platforms by default, go to the "Firewall" page and enable it before placing the system on the network.

Subnet Mask (2)

Enter subnet mask as appropriate, default gateway must be in this subnet

Default Gateway (6)

Enter IP address of the upstream (WAN) router

Primary DNS Server (7)

Enter primary DNS server IP

Secondary DNS Server (8)

Enter Secondary DNS server IP

[Help](#)

Network

Networking configuration information for the public and private networks.

Subscriber Interface Settings:

IP Address: 1

Subnet Mask: 2

Provider Interface Settings:

DHCP 3

Static IP Address

IP Address: 4

Subnet Mask: 5

Network Settings:

Default Gateway: 6

Note: In case of dynamic links, this DNS server address will override the DNS server address obtained from the Servers. Default value for dynamic links is obtained from the server ,if left blank . 7

Primary DNS Server: 8

Secondary DNS Server:

Provider Interface Settings

Static IP Address (3)

Select to display these options, while DHCP is an option on the Provider interface, it is not commonly used due to the nature of H.323, and the dependencies that other H.323 network equipment have on the Provider or LAN network. There are typically multiple devices that require entering this IP statically as part of installing and configuring these other H.323 devices, i.e. gatekeeper, MCU, other routers that provide route entries to the VBP-ST. It is highly recommended that you do not use DHCP on the Provider interface.

IP Address (4)

Enter IPv4 IP address, while this interface is called “Provider” In most deployments this interface will be placed in the private or LAN side of the network

Subnet Mask (5)

Enter subnet mask as appropriate, when creating “Route” entries the gateways for the route entry must be within this subnet.

Network

[Help](#)

Networking configuration information for the public and private networks.

Subscriber Interface Settings:

IP Address: **1**
 Subnet Mask: **2**

Provider Interface Settings:

DHCP **3**
 Static IP Address **4**
 IP Address: **5**
 Subnet Mask:

Network Settings:

Default Gateway: **6**

Note: In case of dynamic links, this DNS server address will override the DNS server address obtained from the Servers. Default value for dynamic links is obtained from the server ,if left blank . **7**

Primary DNS Server: **8**
 Secondary DNS Server:

Configuring LAN Settings

This section describes how to set up LAN parameters with and without VLANs. The VLAN configuration feature allows you to connect the appliance to an Ethernet switch that has been configured to use VLANs. VBP-S and ST platforms do not support VLAN's

Note: The VBP appliance is shipped with LAN IP address 192.168.1.1 and subnet mask 255.255.255.0

Configure LAN network settings without VLANs

1. Choose **Network** from the Configuration Menu.
2. The LAN Interface Settings area of the Network page shows the LAN IP address (192.168.1.1) and subnet mask (255.255.255.0).
3. Clear the Enable VLANs checkbox.
4. Click **Submit**.

A message indicates that service will be interrupted while the new interface is added.

5. Click **OK** to confirm.

Configure LAN network settings with VLANs

1. Choose **Network** from the Configuration Menu.
2. Select Enable VLANs.
3. Click **Submit**.

A message indicates that service will be interrupted while the new interface is added.

4. Click **OK** to confirm.
5. Click **VLAN Settings** to open the VLAN page.
6. Configure settings as appropriate for your VBP model.

Configuring VLANs

The VBP series appliance supports tagged and untagged VLANs. As specified in the IEEE 802.1q standard, tagged VLANs incorporate the VLAN ID and priority in the packet header. Untagged VLAN packets do not include the VLAN ID or priority.

Most VBP series appliances (200EW, 4300T, 4350, 4350EW and the 5300/6400 series) provide support for multiple tagged VLANs. The 5300-E and 6400-E series each support a single untagged VLAN; while the 200EW, 4300T, 4350, 4350EW support up to four untagged VLANs. VBP-S and ST platforms do not support VLAN's

All VBP-E series appliances support up to 16 VLANs.

Set up VLANs on the 4350

1. Choose **System > VLAN Configuration** from the Configuration Menu.
2. Choose 802.1 or 802.1q from the LAN Port Membership pull-down list. Click **Modify**. If 802.1 is selected, radio buttons are presented to permit selection of a single VLAN. If 802.1q is selected, checkboxes are presented to permit selection of multiple tagged VLANs.
3. To add and configure a new VLAN, enter the new VLAN ID, IP address, and network mask. Click **Add**. A new VLAN entry is added to the VLAN configuration. The mode of the physical port determines the rules for VLAN assignment:
 - a. 802.1 mode: Assign the port to a single VLAN.
 - b. 802.1q mode: Assign the port to multiple VLANs
4. Repeat steps 3 for each VLAN you wish to create.

Set up VLANs on the 5300-E and 6400-E series

1. Choose **System > VLAN Configuration**.
2. The screen displays the IP address and subnet mask of the default untagged VLAN. The LAN Ethernet port on the 5300 and 6400 can have both a single untagged and multiple tagged VLANs. Each new VLAN that you add will be tagged only, the untagged VLAN is represented as "eth0", if changes to this VLAN are necessary go to the "**Network**" page and modify the "**LAN Interface Settings**".
3. To add a tagged VLAN, enter the VLAN ID, IP address, and network mask, and click Submit.

A message indicates that service will be interrupted while the new interface is added.

4. Click **OK** to confirm.
5. Repeat steps 3 for each VLAN you want to create.

Delete a VLAN

1. Choose **System > VLAN Configuration** from the Configuration Menu.
2. Click the "trash can" icon to the right of the VLAN entry. It is not necessary to click Submit after deleting a VLAN.

Configuring Ethernet Interface Link Settings

You can modify the Ethernet interface link settings for the appliance, since "Auto-negotiate" interoperability can be problematic for real time protocols, it is recommended to statically configure both VBP Ethernet ports and the switch ports the VBP's interfaces are connected to.

Depending on the WAN link it may be necessary to adjust the WAN MTU size, this issue is typically seen on connections under T1 rates or, DSL links and that depends on the DSL devices ability to set the MTU or MSS size.

Note: Take care when adjusting the Ethernet link rate. The device may become unreachable if an incompatible rate is set.

1. Choose System > Set Link.
2. Select a rate for each Ethernet link, or choose **Auto-negotiate**.
3. Click **Submit**.

A message indicates that service will be interrupted while the new interface is added.

4. Click **OK** to confirm.

SNMP Overview

The VBP series appliance can be managed remotely by an SNMP network management system such as HP Openview. SNMPv1, v2, and v3 and the following MIBS are supported:

- MIB-II (RFC 1213)
- IF-MIB (RFC 2863)
- SNMP MIB-V2 (RFC 3418)
- TCP-MIB (RFC 4022)
- IP-MIB (RFC 2011)
- UDP-MIB (RFC 4113)
- SNMP-VIEW-BASED-ACM-MIB (RFC 3415)
- SNMP-MPD-MIB (RFC 3412)
- SNMP-USER-BASED-SM-MIB (RFC 3414)
- SNMP-FRAMEWORK-MIB (RFC 3411)

All MIB variables are read only. The SNMP MIB-V2 variables sysContact, sysLocation and sysName can be set through the web GUI.

The web GUI supports the configuration of multiple SNMP v1 and SNMP v2 trap destinations. The traps are sent to each of the configured destination using the appropriate protocol version and community string. SNMPv3 supports only one trap destination.

The VBP series appliance sends the following traps:

- coldStart
- authenticationFailure
- linkup
- linkDown

Configure SNMP

1. Choose **System > Services Configuration**.
2. To use SNMPv1 or SNMPv2, select the Enable SNMPv1 checkbox. By default, the agent-address field in SNMPv1 traps is set to the address of the interface that is used to send the trap. You can assign a custom IP address by entering a value in the SNMPv1 Trap Agent IP Address field.
3. To use SNMPv3, check the Enable SNMPv3 checkbox. Enter the user name, passphrase, security method, trap context, and destination trap IP address. The following security methods are supported:
4. None: No authentication and no Privacy
5. Auth(MD5): Authentication using MD5
6. AuthPriv(MD5/DES): Authentication using MD5 and Privacy using DES protocol
7. Click **Submit**.

A message indicates that service will be temporarily interrupted.

8. Click **OK** to confirm.

The figure below displays the VBP configuration for the SNMP Network setup:

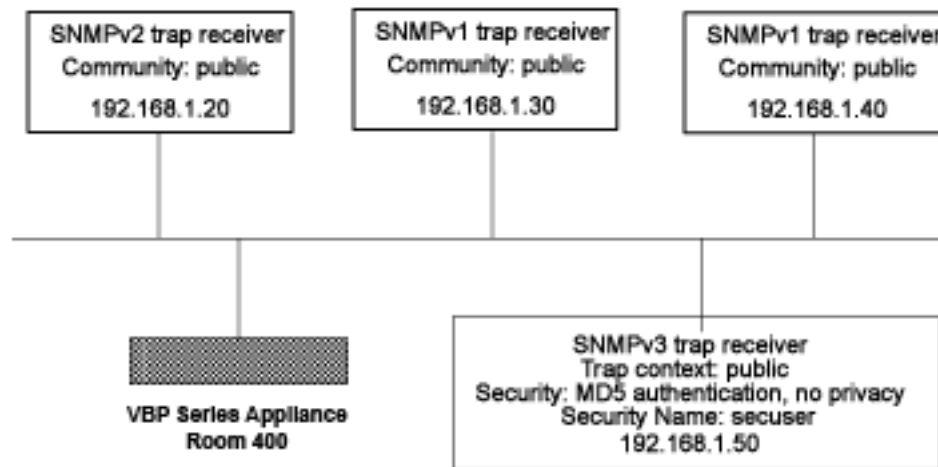


Figure 1. SNMP Configuration Example

Services Configuration

[Help](#)

Customize the configuration of the services accessible on the System.

Enable SNMPv1:

SNMPv1 Read-Only Community:

SNMPv1 Trap Agent IP Address:

Trap Destinations:

IP Address	Version	Community	Delete
192.168.1.20	2	public	<input type="button" value="Delete"/>
192.168.1.30	1	public	<input type="button" value="Delete"/>
192.168.1.40	1	local	<input type="button" value="Delete"/>

Enable SNMPv3:

SNMPv3 User Name:

SNMPv3 Passphrase:

SNMPv3 Security:

SNMPv3 Trap Context:

SNMPv3 Trap Destination IP Address:

Disable SNMP

1. Choose **System** > Services Configuration.
2. Clear the Enable SNMPv1 or Enable SNMPv3 checkbox.

A message indicates that service will be temporarily interrupted.

3. Click **OK** to confirm.

Delete an SNMP trap

1. Choose **System** > Services Configuration.
2. Click the “trash can” icon for the trap.
3. Click **Delete**.

Configuring DHCP Services

You can configure DHCP services with and without VLANs on all E series appliances. You can also relay DHCP requests to an external DHCP server or use the DHCP server included in the VBP series appliance.

DHCP Relay

When you enable DHCP relay and point to a valid DHCP server, you determine that all DHCP requests will be forwarded to that server. Local DHCP and DHCP Relay are mutually exclusive. That is, turning on DHCP Relay automatically turns off local DHCP, and turning on DHCP automatically turns off DHCP Relay.

As you configure the functions featured on the page, review the following list:

Enable DHCP Relay

Select this checkbox to enable DHCP Relay.

DHCP Relay IP Address

Enter the IP address of the DHCP server where the system will forward traffic.

1. Choose **DHCP Relay** from the Configuration Menu.
2. Check Enable DHCP Relay
3. Enter the DHCP Relay IPv4 IP Address
4. Click **Submit**.

A message indicates that service will be temporarily interrupted.

5. Click **OK** to confirm.

DHCP Server

DHCP is a protocol that enables PCs and workstations to get temporary or permanent IP addresses (out of a pool) from centrally administered servers. All VBP E series appliances can act as a DHCP server, assigning IP addresses to devices in the network. You can configure blocks of IP addresses, default gateway, DNS servers, and other parameters that can be served to requesting devices.

Table 1 lists the DHCP options supported by the systems DHCP Server.

DHCP on your system does not have to be enabled if a DHCP server exists elsewhere in your company network. It can be disabled. When you have enabled the DHCP server, you can turn it on or off using the **Enable DHCP Server** box without having to change other settings.

The DHCP IP Address Ranges table shows the dynamic addresses to use for the LAN devices. Enter individual DHCP IP addresses or a range. Assign static IP addresses for any common-access devices, such as printers or fax machines.

Table 1 DHCP Server Options	
Option	Description
1	Subnet Mask - LAN Netmask of the VBP Network page
2	Time Offset
3	Router - LAN IP of the VBP Network page
6	DNS Server - DNS IP, Network page
42	NTP Servers
51	IP address lease time - Lease duration in seconds, DHCP page
53	DHCP Message Type - Set by DHCP server
54	Server Identifier - LAN IP of the VBP
66	FTP Server name
67	Boot file name
129	Call Server IP Address - VLAN ID Discovery
150	Phone Image TFTP Server IP - LAN IP of the VBP, Network Page
151	MGCP Control Server IP - LAN IP of the VBP, Network Page
159	Allows the user to enter a text string in the form of a FQDN. It can be used to point phones to the domain name of a TFTP server using HTTP.
160	Allows the user to enter a text string in the form of a FQDN. It can be used to point phones to the domain name of a TFTP server using HTTPS.

Configuring DHCP Server

Configuring DHCP Server on the VBP appliance includes enabling the server and configuring the DHCP IP Address range to be used by LAN devices. Use the following procedure to configure DHCP.

Configure DHCP

Choose **DHCP Server** to open the DHCP Server page.

As you configure the functions featured on the page, review the following list:

DHCP IP Address Ranges Table (1)

Shows the dynamic addresses to use for the LAN devices. Enter individual DHCP IP addresses or a range. To configure an address range, select the appropriate values and click Add. To delete an address, Click the trash can icon. When adding a new range you must click submit to apply the new range to the DHCP server.

VLAN (9) see next page for reference

Select the VLAN served by the DHCP server.

Enable DHCP Server (2)

Select this checkbox to enable the DHCP server.

Subnet Mask (3)

Subnet Mask address for the DHCP pool. This mask is configured from the LAN subnet mask in the Network page

Lease Duration (Days) (4)

Enter the number of days you want to lease the DHCP service. This is the amount of time a DHCP service will remain connected without lapse. The value can be 1 day minimum and 30 days maximum. Note: when the DHCP lease has expired and the client requests a new IP, it is common for the system to assign the same IP to that system MAC address, if 2 clients make a DHCP request at the same time the lease expires, it is "possible" the system will not assign the same IP.

Time Offset, +/- hours (option 2) (5) (optional)

Set the time offset in hours from UTC (Universal time Code) for your local location.

The screenshot shows the DHCP Server configuration interface. At the top right is a 'Help' link. The main section is titled 'DHCP Server' and contains a table for 'DHCP IP Address Ranges'. The table has three columns: 'Start Address', 'End Address', and 'Action'. The first row shows '192.168.1.60' and '192.168.1.70' with a trash icon. The second row shows '192.168.1.21' and '192.168.1.21' with an 'Add' button. Below the table is a checkbox for 'Enable DHCP Server' which is checked. Below that are several input fields: 'Subnet Mask' (255.255.255.0), 'Lease Duration (Days)' (7), 'Time Offset, +/- hours (option 2)', 'NTP Server Address (option 42)' (IP or DNS can be entered), 'WINS Address (option 44)', 'TFTP/FTP Server Name (option 66)' (00.0.0), 'Boot File Name (option 67)', 'VLAN ID Discovery (option 129)', 'Option 150' (192.168.1.20), 'Option 159', and 'Option 160'. At the bottom, there are 'From Network page:' fields for 'Primary DNS' (4.2.2.2), 'Secondary DNS' (4.2.2.1), and 'Default Gateway' (192.168.1.20). At the very bottom are 'Submit' and 'Reset' buttons. Red callout numbers 1 through 8 point to these various elements.

Start Address	End Address	Action
192.168.1.60	192.168.1.70	
192.168.1.21	192.168.1.21	Add

Enable DHCP Server:

Subnet Mask: 255.255.255.0

Lease Duration (Days): 7

Time Offset, +/- hours (option 2):

NTP Server Address (option 42): IP or DNS can be entered

WINS Address (option 44):

TFTP/FTP Server Name (option 66): 00.0.0

Boot File Name (option 67):

VLAN ID Discovery (option 129):

Option 150: 192.168.1.20

Option 159:

Option 160:

From Network page:

Primary DNS: 4.2.2.2

Secondary DNS: 4.2.2.1

Default Gateway: 192.168.1.20

Submit Reset

NTP Server Address (option 42) (6) (optional)

Set the Network Time Protocol (NTP) address that is served out by DHCP. This field can have a IP address or DNS name of a valid NTP server. Note: if a DNS name is entered in this field the system will perform a DNS A record lookup and use the IP address returned from this lookup to respond to the DNS request from the client as option 42, if the systems DNS server's configured on the Network page are unresponsive, the DHCP response will be delayed.

WINS Address (option 44) (7) (optional)

Enter the IPv4 IP address of your WINS server. 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.

TFTP/FTP Server Name (option 66) (optional)

Set the TFTP/FTP server name that is served out by DHCP. By default, this option is the same as the TFTP server on the ALG page.

VLAN ID Discovery (option 129) (optional)

Set the VLAN ID that devices will acquire after rebooting.

From the Network page (8)

This area is for information only, the DNS IP's shown and the Default Gateway shown will be sent to the client in the DHCP reply

Configuring DHCP With VLANs

This section describes using the DHCP Server capability on the VBP series appliance with configured VLANs. The VBP series appliance supports a maximum of 16 VLANs, all of which could be associated with the DHCP Server. The following are default VLAN IDs used on the VBP appliance:

- VLAN ID 1 (formerly 2730)-- used for management interface (VBP 5300 and 6400 appliances only)
- VLAN ID 500 -- used for video
- VLAN ID 600 -- used for data

Note: To use DHCP with VLANs, the VLAN capability must be enabled and VLANs configured.

Once VLAN capability is enabled and VLANs configured, use the following procedure.

1. Select the VLAN to be used from the drop down list.
2. Check Enable DHCP Server.
3. Add DHCP IP Address Ranges (Scope). In the DHCP IP Address Range table input the starting and ending IP address, then click **Add**.
4. Click Submit, when adding an extra IP Address Range to this server you must click submit to apply the new range.

[Help](#)

DHCP Server

DHCP IP Address Ranges		
Start Address	End Address	Action
No IP Address Ranges Configured		
192.168.1.6	192.168.1.6	<input type="button" value="Add"/>

VLAN: 9
 192.168.1.5 (Id=1)
 192.168.1.5 (Id=1)
 192.168.5.1 (Id=500)
 192.168.6.1 (Id=600)

Enable DHCP Server:

Subnet Mask: 255.255.255.0

Lease Duration (Days):

Time Offset, +/- hours (option 2):

NTP Server Address (option 42):

WINS Address (option 44):

TFTP/FTP Server Name (option 66):

Boot File Name (option 67):

VLAN ID Discovery (option 129):

Option 150:

Option 159:

Option 160:

DHCP Leases

The DHCP Leases page displays view-only information about clients that are currently leasing a DHCP address.

View DHCP lease information

Choose DHCP Server > DHCP Leases.

Hostname

Name of the client that is currently using this DHCP address.

IP Address

IP address of the client.

MAC Address

MAC address of the client.

Expires

Date and time that the DHCP address expires.

Delete

Select the client you wish to delete and click "Delete"

[Help](#)

DHCP Leases

DHCP Leases displays information about hosts who are currently leasing a DHCP address.

DHCP Leases Table				
Select: All None			Action: <input type="button" value="Delete"/>	
	Hostname	IP Address	Mac Address	Expires
<input type="checkbox"/>	hdx8207470891DFP1	192.168.1.62	00:e0:db:08:91:df	2009/10/02 19:56:30
<input type="checkbox"/>	SIP000BBEE3950D	192.168.1.69	00:0b:be:e3:95:0d	2009/10/01 21:42:52
<input type="checkbox"/>	MikeRDelllaptop	192.168.1.61	00:15:c5:6a:03:0e	2009/09/15 22:06:00
<input type="checkbox"/>	SIP000BBEE3950D	192.168.1.69	00:0b:be:e3:95:0d	2009/10/07 16:49:42
<input type="checkbox"/>	SIP000BBEE3950D	192.168.1.69	00:0b:be:e3:95:0d	2009/10/07 16:50:41

Firewall rules for securing the network

VBP Firewall Basics

The VBP system deploys a Linux iptables firewall, and as a converged system, this firewall is controlled by internal applications dynamically. The H.323 ALG application uses iptables dynamically; as H.323 calls are being proxied and modified at Layer 5, the firewall ports for TCP H.245 messages are dynamically opened. This H.245 TCP connection is used by the endpoints to send media related parameters, what codecs can be used for audio and video, how many channels will be used, what ports both endpoints intend to send/receive RTP on, etc. During this negotiation the VBP NAT/PAT's this information as messages pass through the system, since the VBP provides the NAT (network address translation) PAT (port address translation) function, the VBP will know what UDP ports and IP's to allow to incoming connections.

This process happens dynamically, there is nothing to configure on the Firewall page to setup the system. The below methods are mainly for call control, as soon as the call control is allowed the system will allow the RTP media ports dynamically. TCP Port 1720 is used by H.323 devices as the call control port and more important is the presence of the TCP port 1720 connection; if this connection is closed by any device in the path, the endpoints will disconnect the session and the VBP will shut down access to the UDP media ports dynamically. During normal call control when a user hangs up the system, there are normal disconnect messages that happen at Layer 5 when a system wishes to disconnect, the end result after these Layer 5 messages have terminated normally is both endpoints will close the TCP port 1720 connection causing all devices between the endpoints to remove there NAT/PAT contracts.

VBP-E Whitelist/Blacklist rules

Securing the Enterprise network from unwanted "rogue" calls can be done with "User Commands" iptables Firewall rules. By default the system allows anyone to call into the network to establish 2 way video communications. For most companies this is the desired function by installing the VBP. A remote user would have to know the destination E.164 of the registered device and the IP address of the VBP-E series to be able to call in. If you wish to limit who can call into the system, you can configured a Whitelist/Blacklist function by using the below rules. These rules will be placed into the "User Commands" section in the GUI. These rules drop requests from un-desired Layer 3 IP addresses. Blocking inbound calls by destination E.164 is not supported.

The system by default is listening on TCP port 1720, when a calling endpoint sends a Call SETUP it will be sent to the VBP system on TCP port 1720. These blocking methods will not allow the TCP port 1720 connection to be created, the firewall will DROP the request to this port as defined in the methods below.

Whitelist - allows all and block the defined source IP's – If you wanted to block IP 12.48.260.1, you would enter the below command

```
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+ -s 12.48.260.1 -j DROP
```

If you have more than on IP you wish to block, repeat this command and change the source IP you wish to block.

Example:

```
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+ -s 12.48.260.1 -j DROP
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+ -s 1.1.1.1 -j DROP
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+ -s 2.2.2.2 -j DROP
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+ -s 3.3.3.3 -j DROP
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+ -s 4.4.4.4 -j DROP
```

Blacklist – blocks all and only allows the defined source IP's – if you only wanted to allow 12.48.260.1 to call into the system

```
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+ -s 12.48.260.1 -j ACCEPT
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+ -j DROP
```

If you have more than on IP's you wish to allow, repeat this ACCEPT line command and change the source IP you wish to allow. Since iptables uses a top down approach, the DROP rule needs to be at the bottom, the `-A` also mean's to append i.e. insert at the bottom on the chain.

Example:

```
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+ -s 12.48.260.1 -j ACCEPT
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+ -s 1.1.1.1 -j ACCEPT
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+ -s 2.2.2.2 -j ACCEPT
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+ -s 3.3.3.3 -j ACCEPT
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+ -j DROP
```


Example of the Blacklist commands, as you will see below in the next section, you can add more user commands to provide different security functions, while you should keep one function separate for viewing reasons, it is not necessary. It is important to note the dependencies of the Blacklist example, while the Whitelist does not require a specific rule to be in order, the Blacklist does i.e. the DROP rule needs to be at the bottom. The single line block rules could be placed anywhere in the user commands, top or bottom.

User Commands

The User Commands page is used to enter specialized commands or enable features that are not available through other GUI pages. User commands are stored in the file `/etc/config/user_defs.conf`, as described in a number of Edgewater Knowledgebase articles. They are automatically executed whenever the box starts or a Network Restart is performed. User commands are commonly used to create user specific firewall and routing rules.

The user should use caution when adding user commands. The system may become unreachable if an incorrect command is entered.

Once user commands have been entered, if changes are later made on other GUI pages, it is recommended that a [Network Restart](#) be performed.

User Commands:

```
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+
iptables -A PREROUTING -t mangle -p tcp --dport 1720 -i eth1+
```

VBP-E or VBP-S and ST blocking management ports

It may be necessary to block un-encrypted methods of managing the VBP for security reasons. By default the VBP-E system accepts the management port connections on the LAN interface.

VBP-E management ports

- Port 80 – HTTP
- Port 443 – HTTPS
- Port 22 – SSH
- Port 23 – Telnet
- Port 161 – SNMP

You can define rules to block LAN side access to these ports.

CAUTION: If you plan to manage the system with HTTPS, you must configure a certificate in the “HTTPS Certificate” page before the system will accept HTTPS requests. You should test an HTTPS connection to the system before you enter the rule that will DROP port 80 HTTP requests.

To block HTTP

```
iptables -I INPUT -i eth0+ -p tcp --dport 80 -j DROP
```

To block Telnet

```
iptables -I INPUT -i eth0+ -p tcp --dport 23 -j DROP
```

To block SNMP

```
iptables -I INPUT -i eth0+ -p tcp --dport 161 -j DROP
```

Most security teams will allow HTTPS and SSH as both protocols are SSL encoded

By default the system allows ICMP ping to the WAN/LAN interfaces

To block ICMP on the LAN interface

```
iptables -I INPUT 1 -i eth0+ -p icmp -j DROP
```

To block ICMP on the WAN interface

```
iptables -I INPUT 1 -i eth1+ -p icmp -j DROP
```

To block ICMP on both interfaces

```
iptables -I INPUT 1 -p icmp -j DROP
```

Trusted Management Addresses

Trusted Management Addresses are configured to control access to management functions on a VBP-E to a given IP address or subnet, simply enter the appropriate information in Trusted Management Addresses. The logic for Trusted Management Addresses is easy to follow: By entering one or more IP addresses or subnets into this field, the E Series will create ACCEPT rules for the Management protocol defined in the Basic WAN Firewall Settings area (HTTP/HTTPS/Telnet/etc.) for the IP addresses entered, and drop rules for any other IP address.

1. Decide which IP/subnets will be allowed access
2. Decide which management type will be allowed
3. Select the Management type in Basic Firewall Settings area
4. Enter the relevant IP address information in Trusted Management Addresses section
5. Click - >**Submit**

Trusted Management Addresses:

Apply basic settings configuration only to the following addresses:

Address can be host IP or network/mask, e.g. 10.10.10.1 or 10.10.10.0/24. To delete an entry, highlight and delete it.

VBP-S or ST management ports

- Port 80 – HTTP
- Port 443 – HTTPS
- Port 22 – SSH
- Port 23 – Telnet
- Port 161 – SNMP

VBP-S or ST systems have a different firewall concept, the VBP-S or ST is traditionally placed on the Enterprise security boundary. The VBP-S or ST could be placed in a Service Provider model which would have public IP's on both interfaces, this is the reason the system uses the term Provider/Subscriber instead of WAN/LAN. With this in mind, unlike the Firewall page in the VBP-E, which only blocks management port access from the WAN side, the VBP-S or ST applies the allow/deny rules by checking or un-checking the desired management access to both Provider/Subscriber interfaces. By un-checking HTTP access, the system will create rules to block port 80 request on both interfaces.

The below rules are provided for both interfaces, as you may want to allow HTTP on the Provider side and block HTTP on the Subscriber side, in this case you will have HTTP checked on the Firewall page and then insert the rule to block port 80 HTTP on the Subscriber interface.

CAUTION: If you plan to manage the system with HTTPS, you must configure a certificate in the "HTTPS Certificate" page before the system will accept HTTPS requests. If you are enabling the Access Proxy, you will need to re-map HTTPS to an alternate ports, Access Proxy requires the use of port 443

To block HTTP on the Subscriber Interface

```
iptables -I INPUT -i eth0+ -p tcp --dport 80 -j DROP
```

To block Telnet on the Subscriber Interface

```
iptables -I INPUT -i eth0+ -p tcp --dport 23 -j DROP
```

To block SNMP on the Subscriber Interface

```
iptables -I INPUT -i eth0+ -p tcp --dport 161 -j DROP
```

To block HTTP on the Provider Interface

```
iptables -I INPUT -i eth1+ -p tcp --dport 80 -j DROP
```

To block Telnet on the Provider Interface

```
iptables -I INPUT -i eth0+ -p tcp --dport 23 -j DROP
```

To block SNMP on the Provider Interface

```
iptables -I INPUT -i eth0+ -p tcp --dport 161 -j DROP
```

Most security teams will allow HTTPS and SSH as both protocols are SSL encoded

By default the system allows ICMP ping to the WAN/LAN interfaces

To block ICMP on the Subscriber interface

```
iptables -I INPUT 1 -i eth0+ -p icmp -j DROP
```

To block ICMP on the Provider interface

```
iptables -I INPUT 1 -i eth1+ -p icmp -j DROP
```

To block ICMP on both interfaces

```
iptables -I INPUT 1 -p icmp -j DROP
```

CERT Advisory CA-2004-01

When performing a security scan of the VBP system, the scan results may indicate a vulnerability for this CERT advisory. Most port scanning application detect the presence of the well known H.323 ports, UDP 1719 and TCP 1720 and flag this as a concern to be addressed. Below are the details of the CERT advisory and the version of the H.323 stack the VBP uses.

The VBP uses a Linux kernel "Linux 2.4.24-uc0"

The following link provides the concerns for the CERT advisory CA-2004-01

<http://www.cert.org/advisories/CA-2004-01.html>

At the following link, you will see:

http://www.voxgratia.org/docs/faq.html#1_10

"The [NISCC](#) announced on 13 January 2004 that they had [discovered vulnerabilities in several implementations](#) of the H.323 protocol. This announcement was also released by [CERT](#) as [Advisory CA-2004-01](#).

All releases of PWLib after v1.6.0 contain fixes for the vulnerabilities demonstrated by the NISCC test suite. This includes the Janus and Pandora baseline releases and all subsequent stable and development code releases."

In the release notes for version 5.1.0 you will find the following statement

"Updated the H.323 stack to the Pandora release (version numbers: pwlib 1.7.5,openh323 1.14.4). This version of the stack has numerous fixes, most importantly the security issues discovered in the ASN.1 encoder/decoder have been fixed."

The key to these statements is "All releases of PWLib after v1.6.0 contain the fixes" for this advisory the current Polycom version is "Pandora release (version numbers: pwlib 1.7.5,openh323 1.14.4)"

The above concerns were addressed in VBP version 5.1.0

The current firmware version of VBP is 9.1.5.1

DMZ installation of the VBP – Required Ports

If your security configuration includes a DMZ, the firewall used to create the DMZ must forward and receive data using the ports that are listed in the following table.

Note: For public Internet connectivity, the VBP-E or ST series must have a publicly routable non-NATed IP address assigned to the WAN or Subscriber-side interface

A firewall must be configured to allow inbound and outbound H.323 protocols to the VBP, as well as other protocols used by the H.323 devices (such as SNTP) and used to manage the VBP (such as SSH, HTTP, HTTPS, Telnet). Since the VBP is a Firewall proxy, all H.323 packets will have a source or destination IP address of the VBP's Subscriber (VBP-S or ST) or WAN (VBP-E) interface. This can be used to help set up the appropriate rules on the Firewall.

VBP RTP media ports will always be even numbered e.g. 16386, 16388, the port ranges will be used in a circular hunt from lowest to highest per the platform, the odd numbered ports are used for RTCP e.g. 16387, 16389. The VBP 5300-E/S 10 and 25 does not have a reduced port number that equals the bandwidth model; a single port range is used for both the 5300-E10 and 5300-E25 models. Using the VBP in a Firewall DMZ configuration, the following protocols are required, RAS, Q.931 (H.225), H.245, RTP as specified per platform.

For H.323 specific ports see Table 2, Table 3 and Table 4

Table 2 will explain the H.323 ports inbound and outbound from the WAN interface.

Table 3 will explain the H.323 and Access Proxy ports inbound and outbound from the WAN interface.

Table 4 will explain the H.323 ports inbound and outbound from the LAN interface.
The Firewall in front of the VBP must allow the following ports inbound to the VBP:

Table 1

In all cases		
FTP	TCP	21 (optional)
HTTP	TCP	80 (optional for management)
HTTPS	TCP	445 (optional for management, this port is adjustable in the "HTTPS Certificate" page)
HTTPS	TCP	443 (Access Proxy)
XMPP	TCP	5222 (Access Proxy)
LDAP	TCP	389 (Access Proxy)
RTP	UDP	16386 - 17286 (200EW,4300T,4350,4350EW) 16386 - 25386 (5300-E10 and E25) 16386 - 34386 (6400-E and S85)
SNMP	UDP	161 (optional for management)
SSH	TCP	22 (optional for management)
Telnet	TCP	23 (optional for management)
TFTP	UDP	69 (optional)
SNTP	TCP	123 (optional)
H.323 Endpoints		
Q.931 (H.225)	TCP	1720
RAS	UDP	1719
H.245	TCP	14085 -15084

Table 2

In the case where you have an H.460-capable endpoint at a location that is registering to the Subscriber interface of an ST Series, the H.460-capable endpoint must be able to communicate to the Subscriber interface over the defined destination (DST) ports in table 2:

Please ensure that if there is a firewall between the H.460-capable endpoint and the Subscriber interface, the endpoint can communicate over these ports and protocols. Also, note that H.460 as a standard assumes that there is not an “H.323-helper” style service running on the firewall protecting the H.460 endpoint; if there is such a service running on the firewall, please disable it.

H.323 Endpoints Specific				
Inbound from the Internet to VBP WAN/Subscriber Interface IP				
Internet SRC IP	Internet SRC Port	VBP DST IP	Proto	VBP DST port
Any	1024 - 65535	VBP WAN IP	UDP	1719
Any	1024 - 65535	VBP WAN IP	TCP	1720
Any	1024 - 65535	VBP WAN IP	TCP	14085 - 15084 (contiguous range)
Any	1024 - 65535	VBP WAN IP	UDP	16386 - 17286 (200EW,4300,4350,4350EW) (contiguous range)
				16386 - 25386 (5300-E/S10 and E/S25) (contiguous range)
				16386 - 34386 (6400-E and S85) (contiguous range)
Outbound to the Internet from VBP WAN/Subscriber Interface IP				
VBP SRC IP	VBP SRC Port	Internet DST IP	Proto	Internet DST port
VBP WAN IP	1024 - 65535	Any	TCP	1024 - 65535
VBP WAN IP	1024 - 65535	Any	UDP	1024 - 65535

Table 3

H.323 Endpoints Specific and Access Proxy services				
Inbound from the Internet to VBP WAN/Subscriber Interface IP				
Internet SRC IP	Internet SRC Port	VBP DST IP	Proto	VBP DST port
Any	1024 – 65535	VBP WAN IP	UDP	1719
Any	1024 – 65535	VBP WAN IP	TCP	1720
Any	1024 – 65535	VBP WAN IP	TCP	443
Any	1024 – 65535	VBP WAN IP	TCP	5222
Any	1024 – 65535	VBP WAN IP	TCP	389
Any	1024 - 65535	VBP WAN IP	TCP	14085 - 15084 (contiguous range)
Any	1024 - 65535	VBP WAN IP	UDP	Access Proxy in version 9.1.5.1 is only supported on the ST platforms
				16386 - 25386 (5300-E/S10 and E/S25) (contiguous range)
				16386 - 34386 (6400-E and S85) (contiguous range)
Outbound to the Internet from VBP WAN/Subscriber Interface IP				
VBP SRC IP	VBP SRC Port	Internet DST IP	Proto	Internet DST port
VBP WAN IP	1024 - 65535	Any	TCP	1024 - 65535
VBP WAN IP	1024 - 65535	Any	UDP	1024 - 65535

Use the below chart to configure the VBP in a DMZ/port filtering on the LAN side; this is sometimes required for IT departments that want to monitor traffic going to/from the LAN interface of the VBP.

Table 4

(Note: The Layer 3 traffic to and from the LAN interface of the VBP can NOT be NATed by the firewall, the VBP MUST see the real LAN IP of the H.323 endpoint)

H.323 Endpoints Specific				
Inbound from the H.323 endpoint to VBP LAN/Provider Interface IP				
LAN SRC IP	LAN SRC Port	VBP DST IP	Proto	VBP DST port
Any	1024 - 65535	VBP LAN IP	UDP	1719
Any	1024 - 65535	VBP LAN IP	TCP	1720
Any	1024 - 65535	VBP LAN IP	TCP	14085 - 15084 (contiguous range)
Any	1024 - 65535	VBP LAN IP	UDP	16386 - 17286 (200EW,4300,4350,4350EW) (contiguous range)
				16386 - 25386 (5300-E/S10 and E/S25) (contiguous range)
				16386 - 34386 (6400-E and S85) (contiguous range)
Outbound from the LAN/Provider interface IP to LAN H.323 endpoint				
VBP SRC IP	VBP SRC Port	LAN DST IP	Proto	LAN DST port
VBP LAN IP	1024 - 65535	Any	TCP	1024 - 65535
VBP LAN IP	1024 - 65535	Any	UDP	1024 - 65535

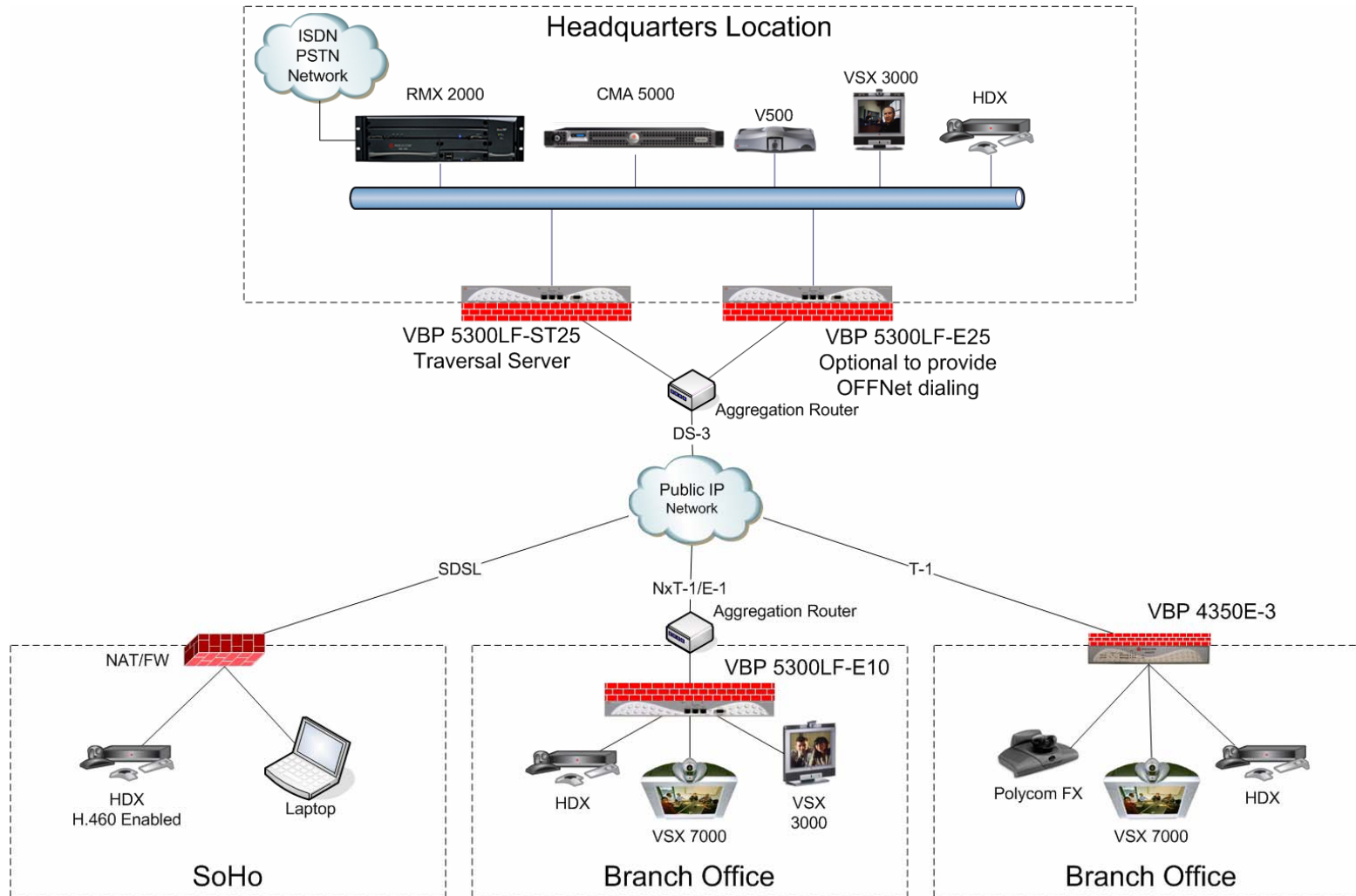
VBP Topologies

Overview

The VBP-series appliance communicates with other sites that use multiple topologies and administrative policies. The VBP appliance can work with a centralized gatekeeper or one or more distributed gatekeepers. It may also act as an embedded gatekeeper in a distributed model.

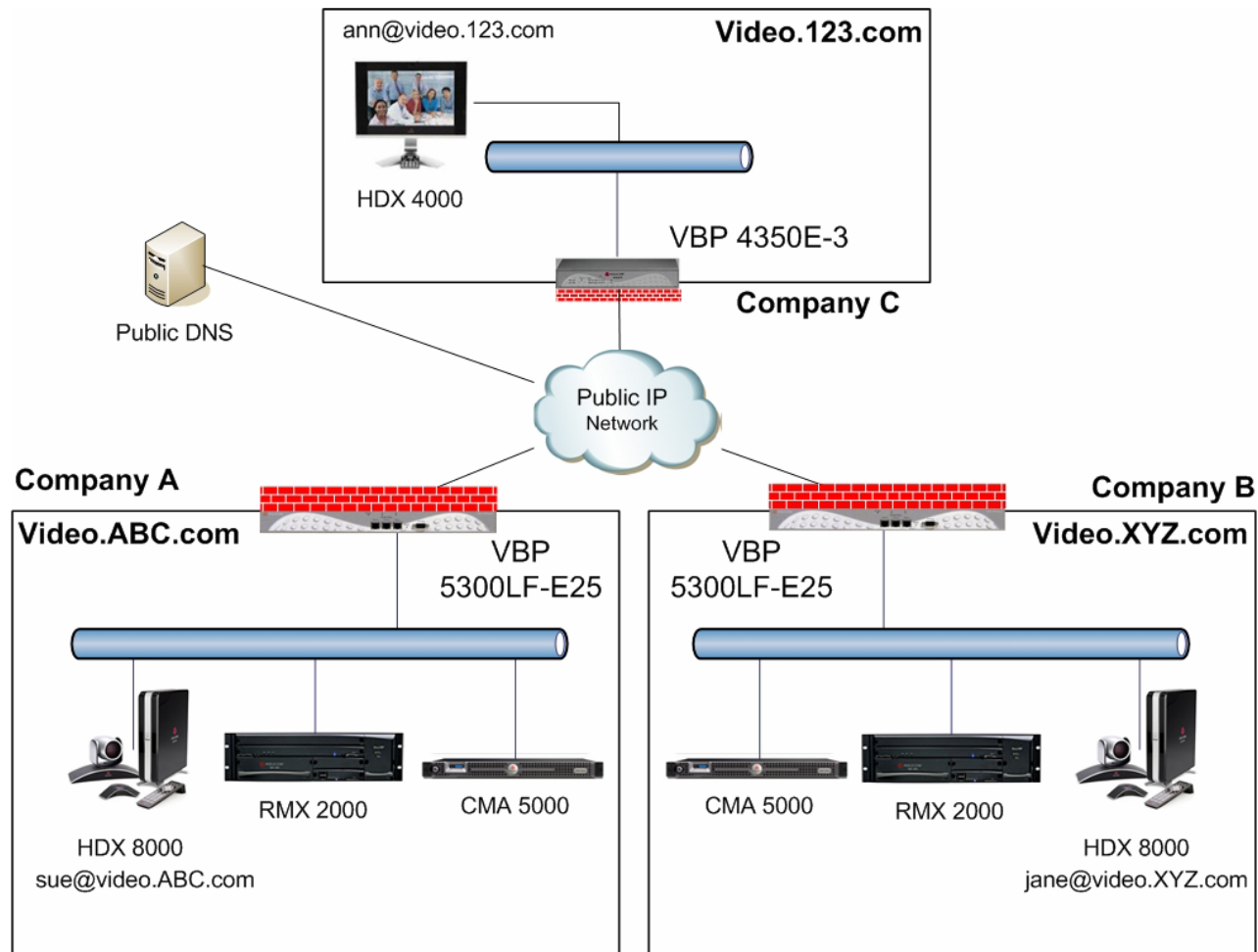
Centralized Gatekeeper Diagram

In this diagram, the headquarters location 5300LF-ST25 is configured for a LAN/Subscriber-side gatekeeper mode with the CMA 5000's IP configured; the VBP's in the branch offices are VBP-E series and are configured in WAN/Provider-side gatekeeper mode with the 5300LF-ST25's Subscriber (or public IP) configured. This configuration allows the remote endpoints to be centrally registered to the CMA server for call control. This configuration allows the CMA server's services to extend past the enterprise network. (CMA is a gatekeeper reference only, this could be most H.323 gatekeepers in the industry that support "routed mode")



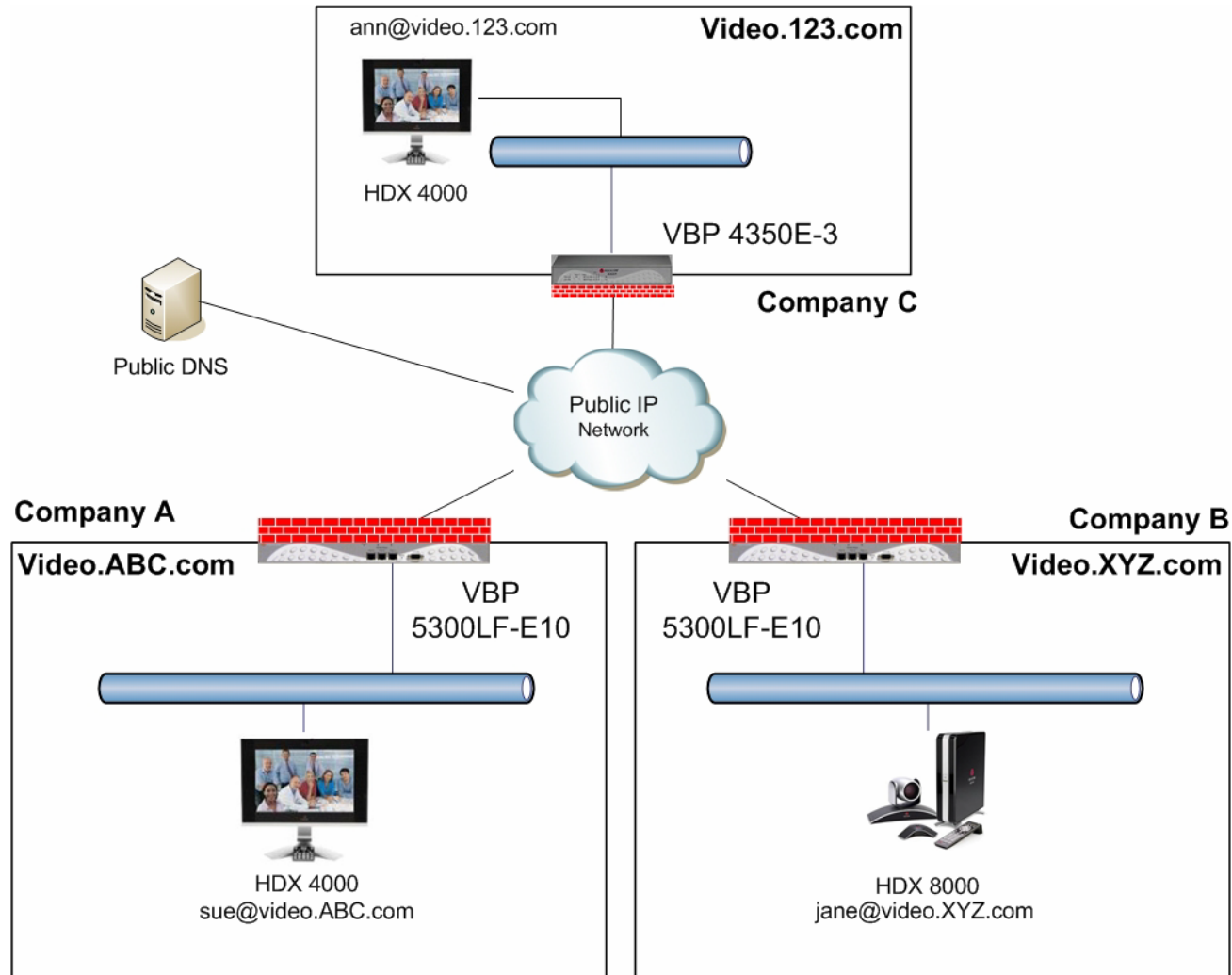
Distributed Gatekeeper Diagram - 1

In this diagram the example is 3 different companies using a mix of “Embedded Gatekeeper” and “LAN/Subscriber-side gatekeeper” modes. Company A and B have the LAN/Subscriber-side gatekeeper technology deployed and Company C did not have any H.323 info-structure, Company C chose to use the Embedded gatekeeper on the VBP-E series. All 3 companies had requirements to communicate with one another over H.323 video technology. Each deployed the VBP as a security border device to allow secure traversal from their internal network to the external “un-trusted” network; in this case the Internet was the transport of choice. This diagram also shows the use of DNS based ANNEX O dialing; while possible, most deployments to date use ANNEX O dialing [E.164@VBP-WAN-IP](#) methods. Direct gatekeeper neighboring is also possible by configuring prefix based gatekeeper neighboring.



Distributed Gatekeeper Diagram - 2

In this diagram the example is be 3 different companies using the “Embedded Gatekeeper” mode on the VBP-E series platform. This diagram could also be the same company that only had a single endpoint requirement and had no existing H.323 info-structure. This diagram also shows the use of DNS based ANNEX O dialing, while possible, most deployments to date use ANNEX O dialing [E.164@VBP-WAN-IP](#) methods. Direct gatekeeper neighboring is also possible by configuring prefix based gatekeeper neighboring.



Configuring the VBP E-Series Appliance for LAN-side Gatekeeper Mode

Configure the VBP E-series appliance by specifying parameters on the following two pages in the Configuration Menu:

The H.323 Settings page

The H.323 Neighboring page (optional)

Aliases Manipulation (optional)

1. To access the H.323 Settings page, select **VoIP ALG > H.323** in the Configuration Menu. The following screen appears.
2. In the Gatekeeper mode area, select the **LAN/Subscriber-side Gatekeeper Mode**. (2)
3. In the LAN/Subscriber-Side Gatekeeper mode settings area, enter the IP address of the gatekeeper in the **LAN/Subscriber-side GK address** field. (3)
4. Click **Submit** to save the changes.

You can also optionally complete the following fields.

Allow public IP in LCF

Select this checkbox if the gatekeeper has been deployed with multiple outbound proxies and you must decide which proxy to use based on the IP address returned in the LCF.

Note: This is an advanced configuration option and should usually not be selected.

Default Alias

The default alias can be added to incoming calls without a destination message in the Q.931 Setup message. This field is typically set to static MCU meeting room, or an IVR entry queue, this can also be a defined conference room system for adhoc meetings

Specify one of the following two types of default aliases:
 E.164
 H.323

H.323 Settings [Help](#)

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

2

WAN/Provider-side gatekeeper mode settings

The H.323 gatekeeper that all client traffic shall be forwarded to.

WAN/Provider-side GK address:

Modify Time-To-Live:

New Time-To-Live (s):

Gatekeeper reachability:

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:

3

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:

Max aliases

Enter the maximum number of allowed aliases. If the value is set to 0, the maximum is not enforced.

You can also optionally enable the LAN-side gatekeeper to provide prefix routing functionality by specifying values on the H.323 Neighboring page.

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

To enable prefix routing functionality, review the following list when completing the featured fields on the H.323 Neighboring page:

Action

Indicates whether a prefix routing rule is to be added or edited.

Prefix

Specifies the prefix pattern to be matched against the dialing string.

Index

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).

Strip

Indicates whether the matching prefix is stripped from the dialing string.

Add

Specifies a string to be pre-pended to the dialing string.

Neighbor

Determines whether a location request (LRQ) is sent when this prefix matches. If enabled, the prefix becomes a neighboring statement. If disabled, the incoming Q.931 Setup is forwarded to the given address without a preceding LRQ. When the incoming Q.931 Setup is forwarded without a preceding LRQ, this is sometimes referred to as “prefix-routing”.

This field is used for interoperability with other gatekeepers that may not accept a Setup without a preceding LRQ.

H.323 Neighboring

[Help](#)

Prefix Routing and Gatekeeper Neighboring

The prefix routing table can be used to forward incoming calls based on their dialed alias.

Prefix and Gatekeeper Neighboring table							
Select: All None						Action: Delete	
Index	Prefix	Strip	Add	Neighbor	Local Zone	Address	
The list is currently empty							

Add a prefix

Action: Add new prefix ▾

Prefix:

Index:

Strip:

Add:

Neighbor:

Local Zone:

Address:

[Commit](#) [Reset](#)

Local Zone

Provides compatibility with remote Cisco IOS 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.

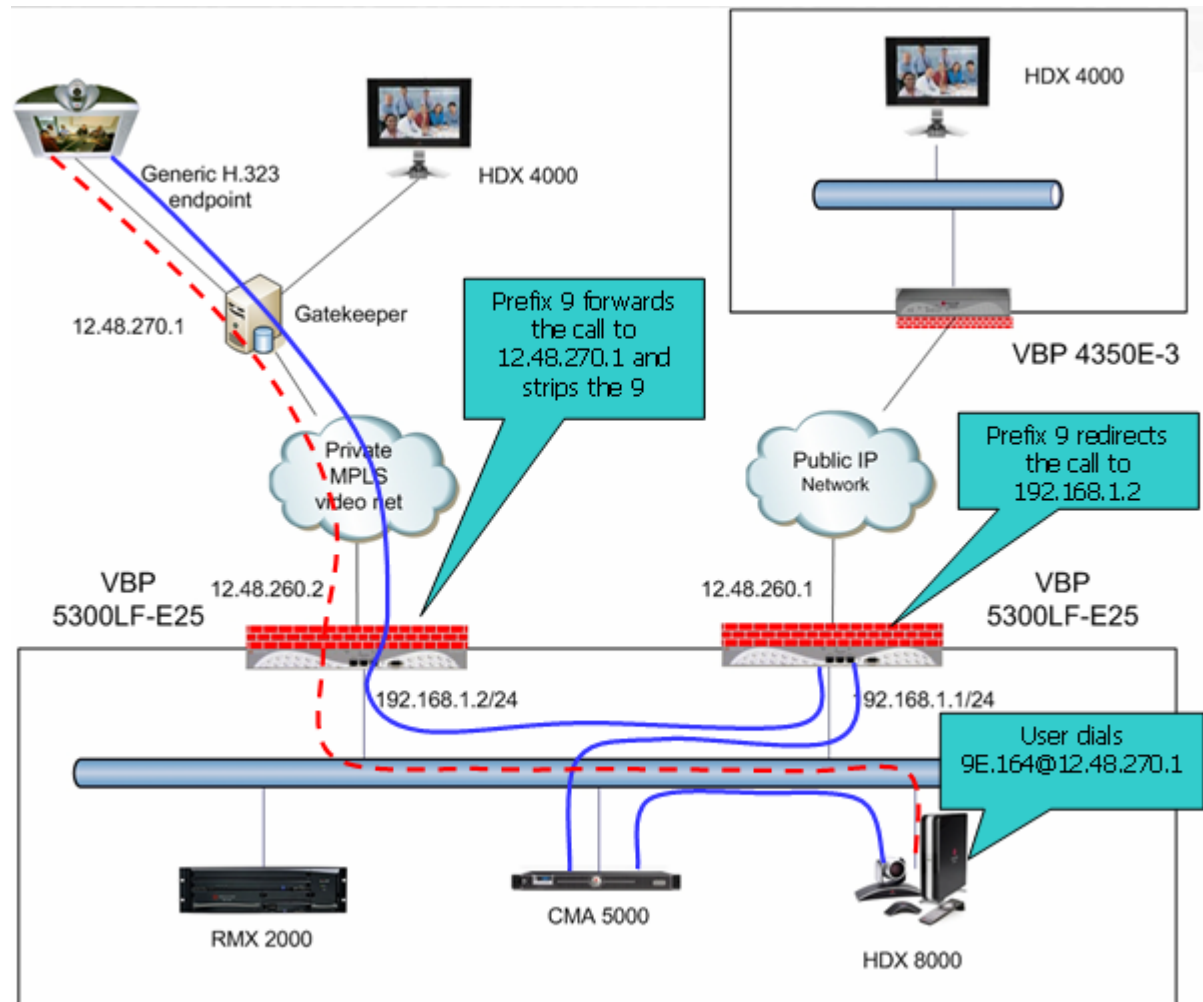
Address

Specifies the IP address or domain name of the device to which the call is to be forwarded.

This example shows the use of prefix routing and prefix based gatekeeper neighboring. The CMA gatekeeper on the LAN is provisioned to use the Internet VBP as its SBL/ALG, in this VBP there is a prefix route for digit 9 to the LAN address of the MPLS egress VBP, the call is redirected to the MPLS VBP. The MPLS VBP receives the call see the 9 prefix, strips the 9 and forwards the call to the gatekeeper for the remote endpoints E.164.

There are many methods for using prefix or LRQ based routing, you could simplify your frequently dialed locations by adding a prefix i.e if you dial [5551000@12.48.270.1](tel:5551000@12.48.270.1) on a daily basis you could enter a prefix of "09" to address 12.48.270.1 and strip "09" then you could simply dial 095551000 to reach this destination.

This method can also be used in "Embedded gatekeeper" mode



Alias Manipulation

You can optionally replace characters or strings that are hard or impossible to dial on certain endpoints before they are associated with IP addresses that are specified on the **H.323 Neighboring** page by completing fields on the **H.323 Alias Manipulation** page.

This feature is useful for endpoints that cannot easily dial ANNEX O user@host methods, most H.323 system remotes have the * and # symbols on the key pad, and not to many have the @ symbol, for this reason default patterns have been set on the VBP. If a user wishes to dial [1234@1.1.1.1](#) they can enter the string as 1234#1*1*1*1 and the VBP by default will translate this string as an ANNEX O method.

This feature is commonly used in VBP-E series in Embedded gatekeeper mode

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

Action

Indicates whether the rule is to be added or edited.

Pattern

Specifies the pattern to be matched.

Index

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).

Replace

Specifies the string that will replace the matched pattern.

H.323 Alias Manipulation [Help](#)

Destination H323-ID or E.164 Alias Modification

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

Destination H323-ID or E.164 Alias Modification			
Select: All None			Action: <input type="button" value="Delete"/>
	Index	Pattern	Replace
<input type="checkbox"/> <input type="button" value="▲"/> <input type="button" value="▼"/>	1	#	@
<input type="checkbox"/> <input type="button" value="▲"/> <input type="button" value="▼"/>	2	*	.

Add a rule

Action:

Pattern:

Index:

Replace:

Configuring the VBP E-Series Appliance for Embedded Gatekeeper Mode

Configure the VBP E-series appliance by specifying parameters on the following two pages in the Configuration Menu:

- The H.323 Settings page
- The H.323 Neighboring page (optional)
- Aliases Manipulation (optional)

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

1. In the Gatekeeper mode area, select **Embedded Gatekeeper Mode**. (2)
2. In the Embedded Gatekeeper mode settings area, confirm the value of the **Time-To-Live (s)**. The time is entered in seconds. The entered time determines how long an endpoint's registration should be valid. At the end of this period the endpoint will send another registration request.
3. Confirm that **Prevent calls from unregistered endpoints** is checked. By default this option is not enabled to allow for multiple ingress/egress scenario's (5)
4. Click **Submit** to save the changes.

You can also optionally complete the following fields.

GK routed mode (4)

Specifies whether the system should allow signaling to go directly between endpoints when possible (unchecked) or always route signaling between endpoints (checked). This option is useful when you have multiple gatekeepers on the LAN, or you wish to use the Embedded gatekeeper in combination with a VBP-ST as the ST's gatekeeper, when using the system in this manner gatekeeper route mode must be enabled. If you are deploying the Embedded gatekeeper as a stand alone system, you can leave this option unchecked.

Default Alias (6)

The default alias can be added to incoming calls without a destination message in the Q.931 Setup message. Specify one of the following two types of default aliases: E.164 and H.323. As noted previously the default alias can be set for different reasons, a common configuration for a SoHo can be to deploy the Embedded gatekeeper and a single video system, you can set the default

[Help](#)

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 2

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

Time-To-Live (s): 4

GK routed mode: 5

Prevent calls from unregistered endpoints: 5

alias to this single system to allow users to call you by just dialing the WAN IP of the VBP, the VBP will receive the call without a DST E.164 and then forward the call to the defined default alias.

Delete stale clients (optional)

Select this checkbox to enable the stale timer feature.

Stale time (m) (optional)

Specify the length of the interval in minutes.

Listen to multicast messages (7)

Select this checkbox to enable listening to multicast messages. This option enables automatic “Gatekeeper Discovery” if enabled on the endpoints, the Embedded gatekeeper will reply and the endpoint will automatically register to this gatekeeper. Caution: having 2 gatekeepers with this enabled will cause unpredictable endpoint registration and calling behavior.

Max Aliases (optional)

Enter the maximum number of allowed aliases. If the value is set to 0, the maximum is not enforced.

Default Alias

A default alias can be added to incoming calls without a destination alias in the Q.931 Setup message. By adding this alias, the embedded gatekeeper, or a LAN/Subscriber-side gatekeeper can route the call to a default endpoint.

Default alias:

E.164 H.323

6

Stale Time

The system can automatically delete clients when they have not sent any registration requests for a given period of time.

Delete stale clients:

Stale time (m):

Multicast Messages

Some RAS messages can be multicast in order to automatically detect gatekeepers.

Listen to multicast messages: 7

Alias Restrictions

The maximum number of aliases to be allowed to register

Max Aliases:

You can also optionally enable the Embedded gatekeeper to provide prefix routing functionality by specifying values on the H.323 Neighboring page. To access the H.323 Neighboring page, select **VoIP ALG > H.323 > Neighboring** in the Configuration Menu. To enable prefix routing functionality, review the following list when completing the featured fields on the H.323 Neighboring page:

Action

Indicates whether a prefix routing rule is to be added or edited.

Prefix

Specifies the prefix pattern to be matched against the dialing string.

Index

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).

Strip

Indicates whether the matching prefix is stripped from the dialing string.

Add

Specifies a string to be pre-pended to the dialing string.

Neighbor

Determines whether a location request (LRQ) is sent when this prefix matches. If enabled, the prefix becomes a neighboring statement. If disabled, the incoming Q.931 Setup is forwarded to the given address without a preceding LRQ. When the incoming Q.931 Setup is forwarded without a preceding LRQ, this is sometimes referred to as “prefix-routing”. This field is used for interoperability with other gatekeepers that may not accept a Setup without a preceding LRQ.

Local Zone

Provides compatibility with remote Cisco IOS 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.

Address

Specifies the IP address or domain name of the device to which the call is to be forwarded.

H.323 Neighboring

[Help](#)

Prefix Routing and Gatekeeper Neighboring

The prefix routing table can be used to forward incoming calls based on their dialed alias.

Prefix and Gatekeeper Neighboring table							
Select: All None						Action: Delete	
Index	Prefix	Strip	Add	Neighbor	Local Zone	Address	
The list is currently empty							

Add a prefix

Action: Add new prefix ▾

Prefix:

Index:

Strip:

Add:

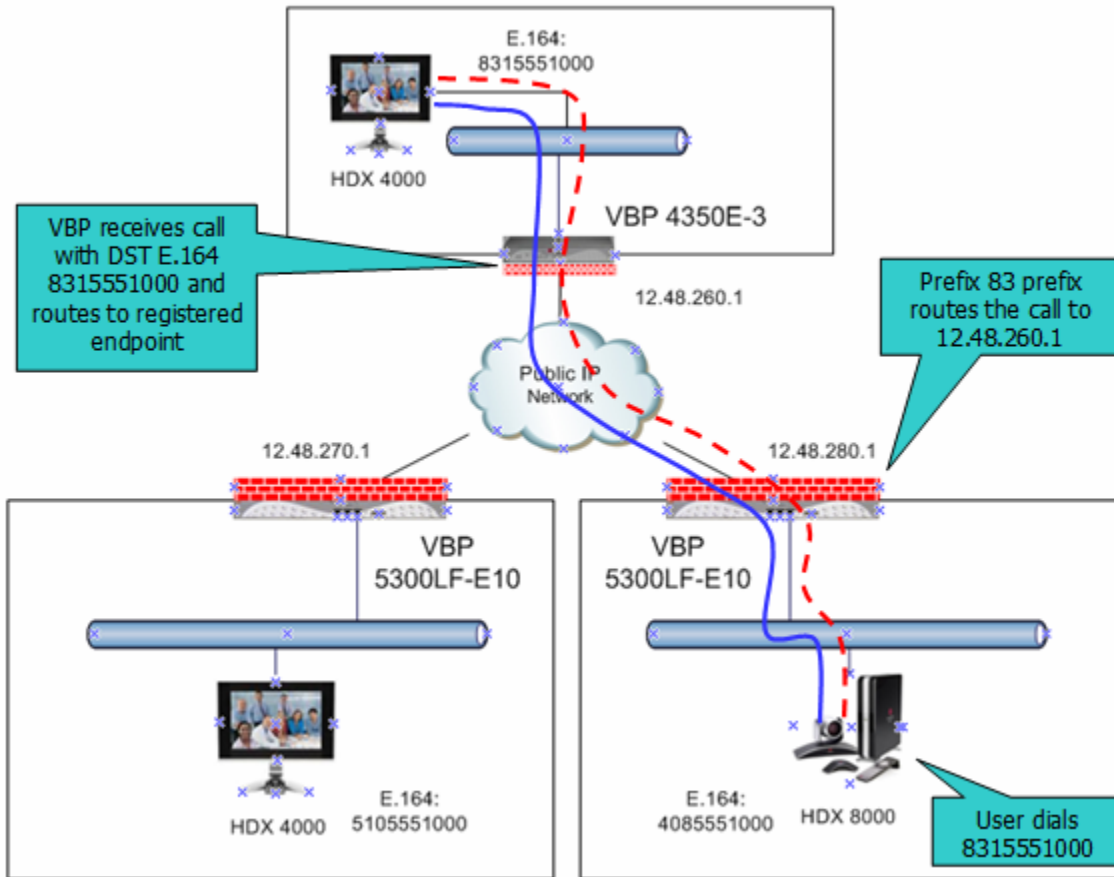
Neighbor:

Local Zone:

Address:

[Commit](#) [Reset](#)

Example for prefix routing to simplify dialing using the DST E.164 as a prefix



H.323 Neighboring [Help](#)

Prefix Routing and Gatekeeper Neighboring

The prefix routing table can be used to forward incoming calls based on their dialed alias.

Prefix and Gatekeeper Neighboring table							
Select: All None							Action: Delete
	Index	Prefix	Strip	Add	Neighbor	Local Zone	Address
<input type="checkbox"/>	1	83					12.48.260.1

Add a prefix

Action: [Add new prefix](#)

Prefix:

Index:

Strip:

Add:

Neighbor:

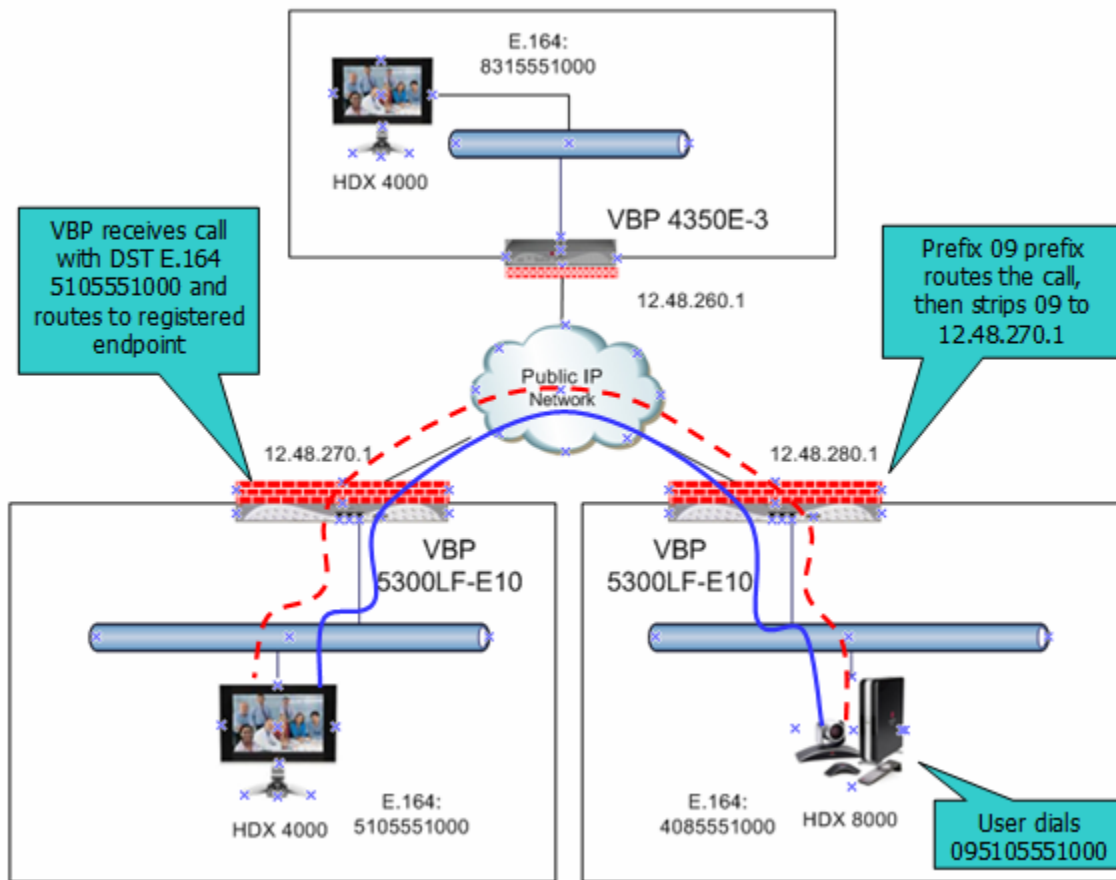
Local Zone:

Address:

[Commit](#) [Reset](#)

In this case "Neighbor" could be set

Example of Prefix routing to simplify the dial plan and use extra routing digits



H.323 Neighboring [Help](#)

Prefix Routing and Gatekeeper Neighboring

The prefix routing table can be used to forward incoming calls based on their dialed alias.

Prefix and Gatekeeper Neighboring table							
Select: All None							Action: Delete
	Index	Prefix	Strip	Add	Neighbor	Local Zone	Address
<input type="checkbox"/>	1	83					12.48.260.1
<input type="checkbox"/>	2	09	Yes				12.48.270.1

Add a prefix

Action: [Add new prefix](#)

Prefix:

Index:

Strip:

Add:

Neighbor:

Local Zone:

Address:

In this case "Neighbor" could be set

[Commit](#) [Reset](#)

Peering Proxy Overview

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

VBP 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 illustrations 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, 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 below, the VBP 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 NAP’s). The NAP’s in this case are 831 and 408.

Dial plan integrity is required to insure proper routing of prefixes. This means that if users are to dial into your network, they could be required to enter a “Prefix” on their VBP 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 VBP 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 VBP 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 VBP’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 VBP 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 9415551000@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 VBP does not strip the “9”, the destination VBP 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 A’s VBP to NOT strip matching prefixes.

NOTE: In this illustration E.164@WAN_IP was used as an example. Peering Proxy and all VBP’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 VBP.

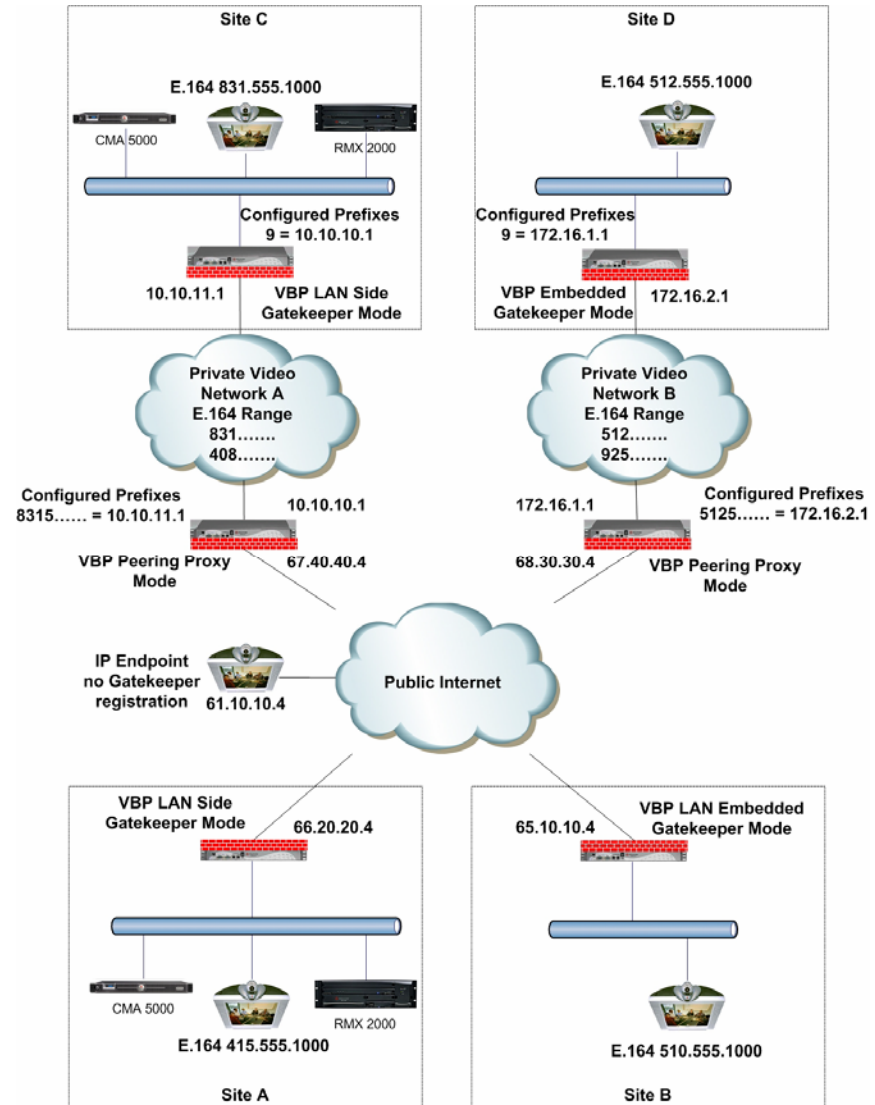
The following sections demonstrate the Dial Plan for ingress and egress calls to Private Video Network A as shown in the illustration.

Outbound from Site C to Site A

Site C dials an endpoint located at Site A: 9415551000@66.20.20.4. The CMA receives the call and generates a Q.931setup to the VBP for that subnet. The VBP processes the Q.931 setup from the calling endpoint. The VBP 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 VBP. The call is forwarded to the LAN Side CMA where the registered client with the E.164 of 415551000 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 VBP 10.10.11.1. As explained earlier, the prefix could be 831* or 83..... and so on, depending upon dial plan requirements. The CMA receives the Q.931setup from the endpoint and forwards the call to the VBP for that subnet. The VBP receives the Q.931 setup from the calling endpoint. The VBP 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 A’s VBP. The Q.931 setup is forwarded to the LAN Side CMA where the registered client with the E.164 of 8315551000 is located, and the call is gatekeeper routed to the called endpoint.

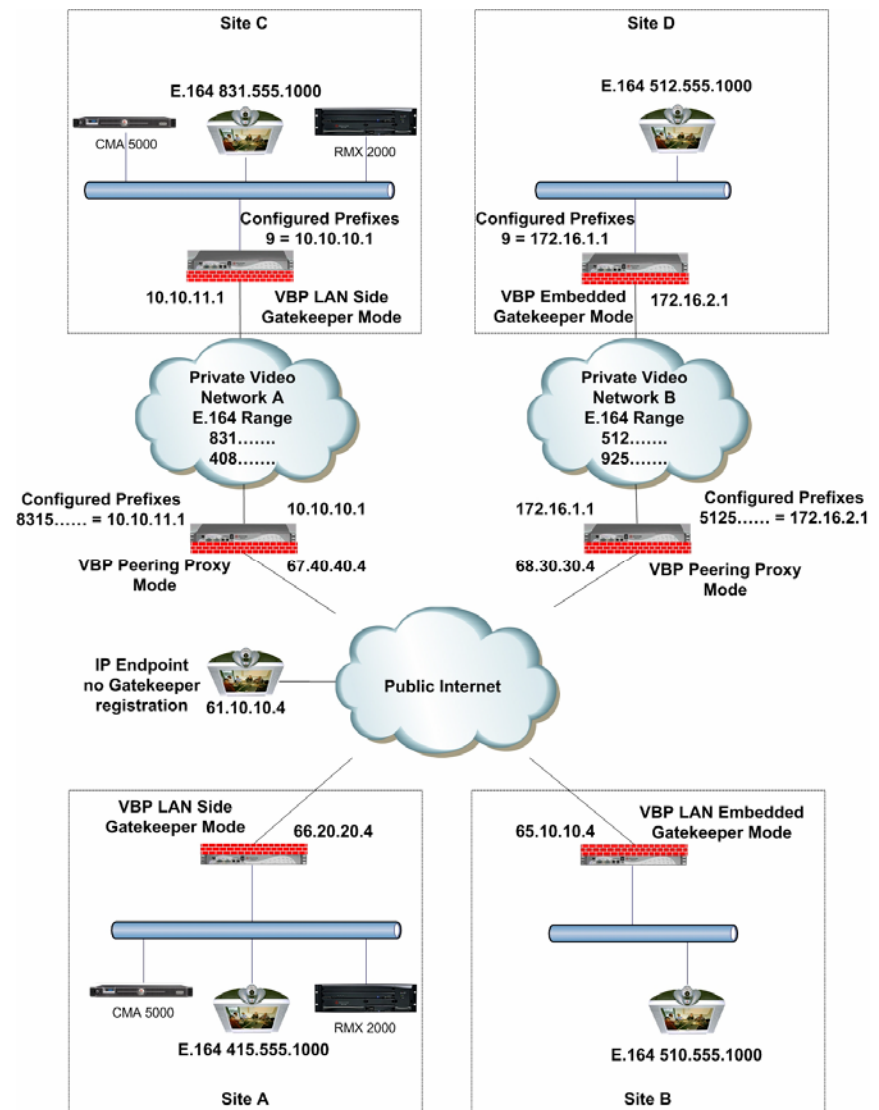


Outbound from Site C to Site D

Site C dials an endpoint located at Site D: 95125551000@68.30.30.4. The CMA receives the call and generates a Q.931 setup to the VBP for that subnet. The VBP processes the Q.931 setup from the calling endpoint. The VBP 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 VBP. The VBP 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 VBP Embedded Gatekeeper is configured with a prefix of “9” to point to Peering Proxy 172.16.1.1. The VBP 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 VBP 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 CMA receives the call and generates a Q.931 setup to the VBP for that subnet. The VBP receives the Call setup from the calling endpoint, and the VBP 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 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 A’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 A’s VBP. The Q.931 setup is forwarded to the LAN Side CMA where the registered client with the E.164 of 8315551000 is located, and the call is gatekeeper routed to the called endpoint.

Configuring the VBP E-Series Appliance for Peering-Proxy Mode

Configure the VBP E-series appliance by specifying parameters on the following two pages in the Configuration Menu:

The H.323 Settings page
The H.323 Neighboring page

1. To access the H.323 Settings page, select **VoIP ALG > H.323** in the Configuration Menu.
2. In the Gatekeeper mode area, select **Peering-Proxy Mode. (1)**
3. Click **Submit** to save the changes.
4. (configure [prefixes](#)) will link you to the “Neighboring”, this page is also available in the H.323 menu.

[Help](#)

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

As an advanced function of Peering-Proxy, you can set a default IP address that you want to forward inbound call setup's that have no prefix match. By default the Peering-Proxy system is a prefix routing engine, and therefore you may not wish to terminate undefined destinations, however; you can set a default IP address to forward inbound calls from the WAN to a LAN side IP that has no prefix match by setting the IP in the LAN/Subscriber-side GK address. **(2)**

Adding an H.323 Prefix Entry

To access the H.323 Neighboring page, select **VoIP ALG > H.323 > Neighboring** in the Configuration Menu. The following screen appears.

Note: in Peering-Proxy mode LRQ Neighboring is not possible since the system in this mode is not a gatekeeper

To enable prefix routing functionality, review the following list when completing the featured fields on the H.323 Neighboring page:

- Action**
Indicates whether a prefix routing rule is to be added or edited.
- Prefix**
Specifies the prefix pattern to be matched against the dialing string.
- Index**
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).
- Strip**
Indicates whether the matching prefix is stripped from the dialing string.
- Add**
Specifies a string to be pre-pended to the dialing string.

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:

2

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:

H.323 Neighboring [Help](#)

Prefix Routing and Gatekeeper Neighboring

The prefix routing table can be used to forward incoming calls based on their dialed alias.

Prefix and Gatekeeper Neighboring table							
Select: All None						Action: Delete	
Index	Prefix	Strip	Add	Neighbor	Local Zone	Address	
The list is currently empty							

Add a prefix

Action:

Prefix:

Index:

Strip:

Add:

Neighbor:

Local Zone:

Address:

Neighbor (Do not set this, in Peering Proxy mode, the system does not support LRQ's)

Determines whether a location request (LRQ) is sent when this prefix matches. If enabled, the prefix becomes a neighboring statement. If disabled, the incoming Q.931 Setup is forwarded to the given address without a preceding LRQ. When the incoming Q.931 Setup is forwarded without a preceding LRQ, this is sometimes referred to as "prefix-routing".

This field is used for interoperability with other gatekeepers that may not accept a Setup without a preceding LRQ.

Local Zone (Do not set this, in Peering Proxy mode, the system does not support LRQ's, i.e. no Cisco gatekeeper support)

Provides compatibility with remote Cisco IOS 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.

Address

Specifies the IP address or domain name of the device to which the call is to be forwarded.

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 number of special expressions.

Alias manipulation patterns can match a sub-string anywhere and multiple 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

.	Matches any single character.
[]	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]
()	Matches the literal string given, e.g. (abc)
	Matches the block on either side of the , e.g. a b.
?	Matches 0 or 1 of the preceding block.
*	Matches 0 or more of the preceding block.
+	Matches 1 or more of the preceding block.
\	Escapes the special meaning of the next character.
{a}	Matches exactly 'a' numbers of the preceding block.
{a,}	Matches 'a' or more of the preceding block.
{a,b}	Matches between 'a' and 'b' (inclusive) of the preceding block.

Some examples of prefixes:

100	Matches the string 100.
(555)?123	Matches 555123 or 123.
(408 555)	Matches 408 or 555.
555[0-9]{3}	Matches 555 followed by exactly 3 digits.

Centralized Gatekeeper Configuration

In the centralized gatekeeper model, the Main Headquarters gatekeeper is the only gatekeeper installed in the Enterprise network; while it is possible to have more than one gatekeeper in large Enterprises, this configuration exercise will reference a single gatekeeper. You can apply what this sections explains to deploy more than one gatekeeper and VBP-ST platform to provide geographically localized ingress points throughout your Enterprise.

As shown in the below diagram the VBP 5300LF-ST25 will extend the reach of the enterprise gatekeeper by allowing remote branch offices with VBP-E series or non-VBP SoHo offices using H.460 traversal methods to register back to the core gatekeeper. This could be viewed as a reverse firewall proxy for H.323/H.460 devices to reach the Enterprise gatekeeper for service.

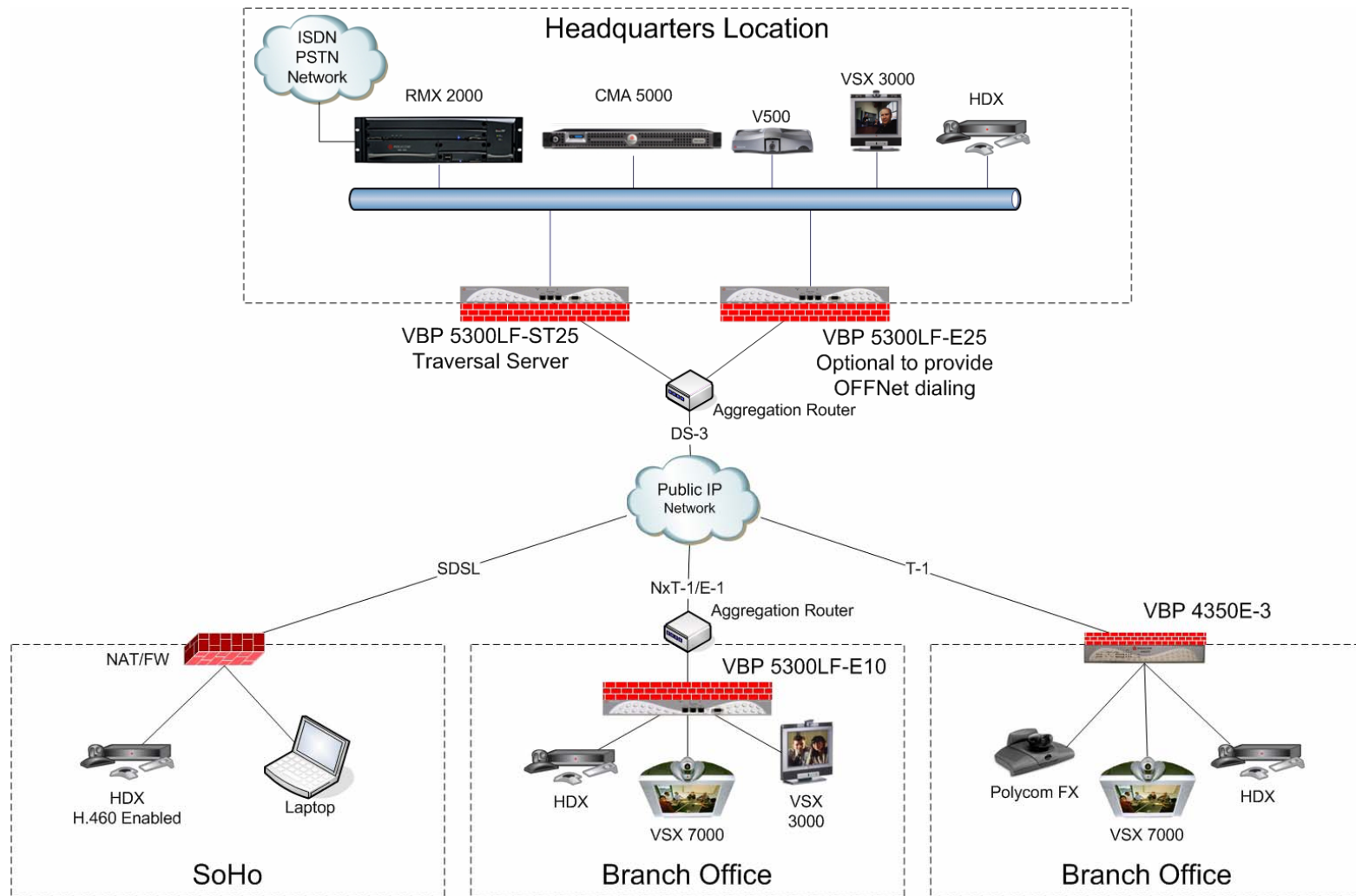
The VBP-ST platform can also support stand alone H.323 endpoints on the Internet that wish to register into the Enterprise gatekeeper. Some companies have deploy this for security reason to not allow any non-registered device outside of the Enterprise to communicate with internal or external registered users.

By default, the VBP-ST will allow any IP to send a registration request to the system, however, the gatekeeper can control which aliases are allowed to register to the gatekeeper.

Further security can be provided by the VBP-ST to only allow defined source IP's to create connections to the system, examples will be provided later in this document.

H.323 endpoints on the Internet/Subscriber side of the VBP-ST must register with this gatekeeper. These endpoints set there gatekeeper IP to the VBP E-Series LAN IP, the VBP E-Series then forwards the registration messages to the Subscriber IP of the VBP-ST, the VBP-ST then forwards the request to the actual gatekeeper.

Centralized Gatekeeper Diagram



Configuring the VBP S and ST-Series Appliance for Provider-side gatekeeper mode

Configure the VBP ST-series appliance by specifying parameters on the following pages in the Configuration Menu:

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

In the Gatekeeper mode area, select **WAN/Provider-side Gatekeeper Mode**. (1)
 In the WAN/Provider-side gatekeeper mode settings area,

WAN/Provide-side GK address, enter the IP of the gatekeeper, in this example the CMA 5000's IP (2)

Modify Time-to-Live, this is typically unchecked for most installation. (3)

Time-To-Live (s). The time is entered in seconds. The entered time determines how long an endpoint's registration should be valid. At the end of this period the endpoint will send another registration request. This option is typically not set, the TTL is being assigned by the gatekeeper and works for most installation, if this field is modified, it is typically a shorter period than what the gatekeeper is using, if the value is longer than the gatekeepers, the endpoint may become un-registered by the gatekeeper before the endpoints next registration interval. (3)

H.460.18 Support, in this case, the remote SoHo office is using a H.460 capable endpoint, confirm this is set to enable (5)

Keep-alive time, this value defaults to 45 seconds and is used by the H.460 endpoint to set the time between registration messages, the H.460 endpoint will typically cut this time in half and then send a registration message at that interval. The keep-alive and registration message provides the following H.460 functions, the UDP registration message is how the traversal server sends the H.460 endpoint an indication message that an incoming call is being requested, this allows the H.460 endpoint to setup an outbound TCP DST port 1720 connection to the traversal server to forward the incoming call to this endpoint, with this UDP registration message the traversal server now understands what the NAT/FW IP address is and what SRC port the message is coming from, in order to forward the registration response and H.460 related message back to the H.460 endpoint. The default value has been found in the field to be a common working interval to keep the NAT contract alive in most NAT/FW devices. (6)

Click **Submit** to save the changes.

You can also optionally complete the following fields.

[Help](#)

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. 1

None (H.323 is disabled)
 WAN/Provider-side gatekeeper mode
 Peering-Proxy mode (configure prefixes)

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

WAN/Provider-side GK address: 3 2 1

Modify Time-To-Live: 3

New Time-To-Live (s): 4

Gatekeeper reachability: N/A

H.460.18 Support

H.460.18 allows the system to do NAT/Firewall traversal for clients behind NAT and/or firewall devices.

Disabled 5
 Enabled 6

Keep-alive time (s):

LRQ size (optional)

Limits 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.

Default Alias (typically not set in this mode)

The default alias can be added to incoming calls without a destination message in the Q.931 Setup message. Specify one of the following two types of default aliases E.164 and H.323

Delete stale clients (optional)

Select this checkbox to enable the stale timer feature.

Stale time (m) (optional)

Specify the length of the interval in minutes.

Listen to multicast messages (typically not set in this mode)

Select this checkbox to enable listening to multicast messages.

Note: RTP traffic cannot be routed directly between two remote endpoints that have H.460 enabled; H.460 traversal requires the RTP media to be relayed by the VBP-ST system

LRQ size

Some gatekeepers do not accept more than 2 source aliases in the LRQ message.

Limit LRQ size:

Default Alias

A default alias can be added to incoming calls without a destination alias in the Q.931 Setup message. By adding this alias, the embedded gatekeeper, or a LAN/Subscriber-side gatekeeper can route the call to a default endpoint.

Default alias:

E.164

H.323

Stale Time

The system can automatically delete clients when they have not sent any registration requests for a given period of time.

Delete stale clients:

Stale time (m):

Multicast Messages

Some RAS messages can be multicast in order to automatically detect gatekeepers.

Listen to multicast messages:

H.460.18 Support

H.460.18 allows the system to do NAT/Firewall traversal for clients behind NAT and/or firewall devices.

Disabled

Enabled

Keep-alive time (s):

Alias Restrictions

The maximum number of aliases to be allowed to register

Max Aliases:

Configuring the VBP E-Series Appliance for WAN-side Gatekeeper Mode

Configure the VBP E-series appliance by specifying parameters on the H.323 Settings page in the Configuration Menu.

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

1. In the Gatekeeper mode area, select the **WAN/Provider-side Gatekeeper Mode**. (1)
2. In the WAN Provider-Side Gatekeeper mode settings area, enter the IP address of the VBP-ST subscriber interface in the **WAN/Provider-side GK address** field. (2)
3. **Modify Time-to-Live**, this is typically unchecked for most installation. (3)
4. **Time-To-Live (s)**. The time is entered in seconds. The entered time determines how long an endpoint's registration should be valid. At the end of this period the endpoint will send another registration request. This option is typically not set, the TTL is being assigned by the gatekeeper and works for most installation, if this field is modified, it is typically a shorter period than what the gatekeeper is using, if the value is longer than the gatekeepers, the endpoint may become un-registered by the gatekeeper before the endpoints next registration interval. (4)
5. Click **Submit** to save the changes.

You can also optionally complete the following fields:

Stale time (m)

Specify the length of the interval in minutes. Caution should be used when setting this, if this value is set below the gatekeepers TTL value, the VBP-E will remove the client, this causes the VBP-ST to remove the client, and then the gatekeeper will remove the client, which leave the endpoint un-reachable, until its TTL value expires and re-registers

Listen to multicast messages (typically not set in this mode)

Select this checkbox to enable listening to multicast messages.

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:
- Modify Time-To-Live:
- New Time-To-Live (s):
- Gatekeeper reachability: N/A (Not in WAN GK mode)

Stale Time

The system can automatically delete clients when they have not sent any registration requests for a given period of time.

- Delete stale clients:
- Stale time (m):

Multicast Messages

Some RAS messages can be multicast in order to automatically detect gatekeepers.

- Listen to multicast messages:

Alias Restrictions

The maximum number of aliases to be allowed to register

- Max Aliases:

Max Aliases

Enter the maximum number of allowed aliases. If the value is set to 0, the maximum is not enforced. This option can be set to control how many aliases are allow to register through to the gatekeeper, while this is typically a gatekeeper related task the VBP can control how many aliases can be proxied. When setting this value keep in mind that each endpoint typically has 2 aliases i.e. E.164 and H323ID, if you want to restrict 10 endpoints, you would enter a value of 20 in this field

Access Proxy Summary and Configuration

Access Proxy is a feature added to the VBP-ST that “allows” authorized outside endpoints access to the CMA server for VC2 services; this feature is the next step in video unified communications. Access Proxy provides connectivity to the Enterprise directory server and provides the external clients with IM style “point and click” to initiate text chat, and launch video calls from a centralized directory of all users on the system. Access Proxy provides secure TLS (transport layer security) encrypted sessions for authentication, directory searches and real time “buddy” status, also known as VC2 services.

Access proxy secure reverse proxy for VC2 services, these services use the following protocols.

- HTTPS – for authentication and configuration management
- XMPP – “Jabber” or presence information to/from the remote clients
- LDAP - Directory searching for users that you want to add as buddies
- H.323/H.460 – For video and audio traversal

All protocols except H.323/H.460 use TLS to encapsulate the data in secure encrypted packets – H.323/H.460 does not use TLS encapsulation.

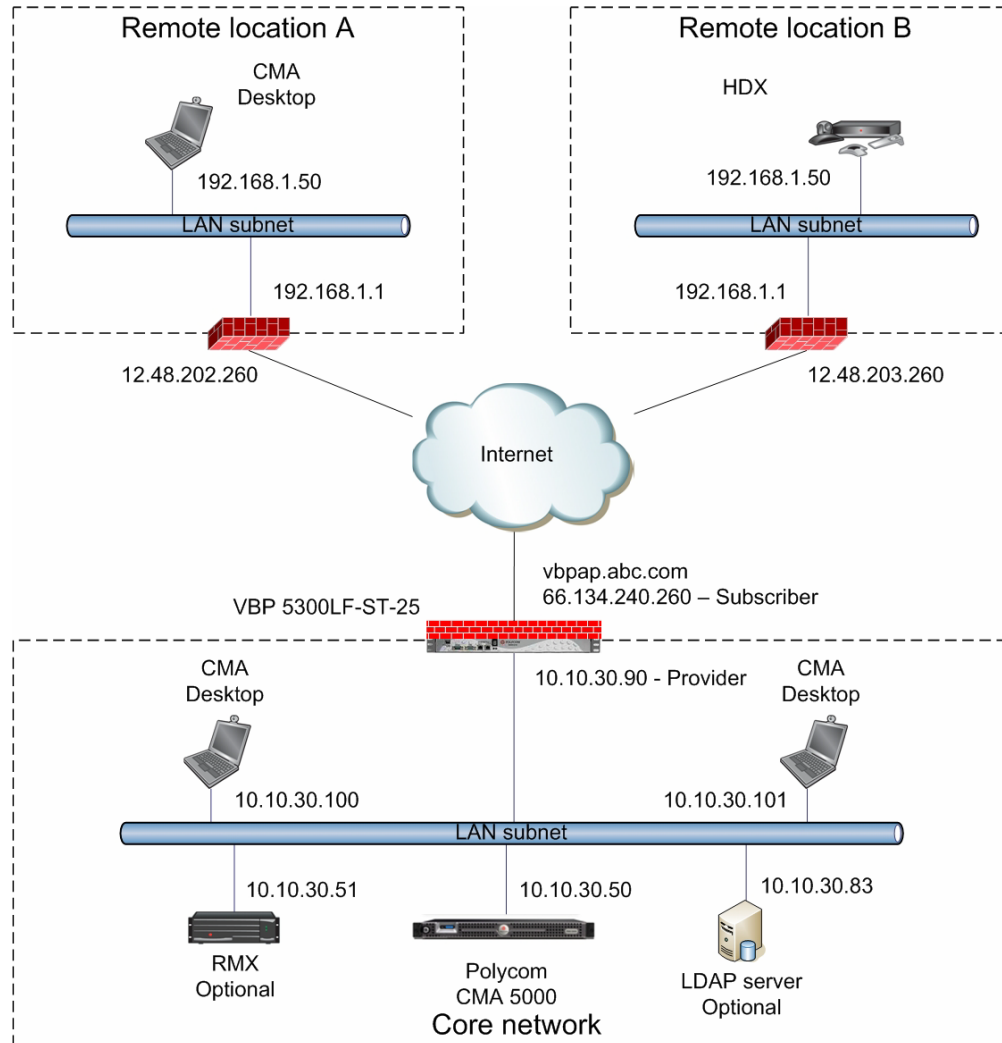
Access Proxy uses SSL based certificates to encrypt the session, Each SSL Certificate consists of a **public key and a private key**. The public key is used to encrypt information and the private key is used to decipher it. When a CMA desktop clients points to the Access Proxy, a Secure Sockets Layer handshake authenticates the server (Access Proxy) and the client (CMAD). An encryption method is established with a unique session key and secure transmission can begin.

Theory - Imagine sending mail through the postal system in a clear envelope. Anyone with access to it can see the data. If it looks valuable, they might take it or change it. An SSL Certificate establishes a private communication channel enabling encryption of the data during transmission. Encryption scrambles the data, essentially creating an envelope for message privacy.

The VBP is pre-installed with self signed certificates to configure the Access Proxy. These certificates can be changed with Signed certificates, from a CA (certificate authority) if you choose to. Access Proxy can have different certificates for each protocol making the SSL encryption different for each service

Access Proxy Diagram

This diagram shows the supported network methods for deploying remote VC2 based clients. The Access Proxy enabled VBP-ST is installed at the core location with the CMA server. The remote locations have standard NAT/FW devices, the list of tested and known working devices will be listed later in this document.



NAT routers tested

Manufacture	Model –HW version	SW version	Multiple H.460 endpoints	Issues noticed
Netgear	WGR614-v9	1.2.2NA	Yes	none
Linksys	WRT54GL-v1.1	4.30.11	Yes	none
Dlink	WBR-1310-B1	2.00	No *	Router tends to reboot occasionally
Linksys	WRT54G2-v1	1.0.01	Yes	none
Belkin	F5D9231-4-v1	1.00.01	Yes	none

* Dlink WBR-1310 can support only 1 H.460 endpoint, the first endpoint that registers is the only endpoint that will work, even if this 1st endpoint has been powered down. This router creates “H.323” connection tracking at the MAC layer, the only way to clear this is to reboot the router. After a reboot you can now register a new H.460 device.

Software requirements for Interoperability

- CMA 4000/5000 server – 4.01.02 or higher (see note)
- CMA Desktop – 4.1.1 or higher
- HDX – 2.5.0.5 or higher

Note: The following issues, which may impact VBP functionality, exist in CMA 4.01.02. These issues are addressed in CMA version 4.01.04

- Duplicate Aliases – When a CMAD or HDX in VC2 mode moves from an internal CMA connection to an external VBP Access Proxy connection you might experience a scenario where the endpoint cannot connect to the CMA Server. An HDX endpoint is likely in this state if it displays an indicator stating that the gatekeeper service is down. A CMAD client is likely in this state if cannot progress beyond the “signing into the media server” message. In some cases, gracefully logging out of the internal location and waiting at least 10 minutes before an external login can reduce the chances of experiencing this issue.
- Dual Redundancy – When deploying 2 VBP’s and 2 CMA server’s for what is called “Dual Redundancy” if the MASTER CMA server fails, this forces the BACKUP CMA server to have control of all services, it is possible when this CMA failover happens, this CMA server may NOT send responses from the VIP (virtual IP) causing messages to be sent from the physical IP, the VBP is expecting messages to come from the VIP and will not be forwarded to the remote client. When deploying “Single Redundancy” 2 VBP’s and 1 CMA server, If the MASTER VBP fails, the BACKUP VBP will take over and function as expected.

Prerequisites

CMA server installed on the LAN subnet, this subnet can be on the same broadcast domain as the VBP, however it is not required. If the CMA is on a remote LAN subnet from the VBP's providers interface, there can be NO NAT devices between these subnet's, traffic to and from the CMA and to and from the VBP need's to be on routed subnets – "routes" will need to be added to the VBP for all subnet's to contact the CMA and all video endpoint's.

- Configure CMA network IP's and related network parameters
- From the VBP you should be able to send an ICMP ping to the CMA LAN IP and receive a response
- From the VBP you should be able to send an ICMP ping to a few LAN endpoints and receive a response
- Configure "users" on the CMA
- Configure the VBP as a "Network Device"

VBP-ST installed on the Public internet with NO NAT between the "Subscriber" interface and the public FW/NAT devices or public IP video endpoints. The VBP-ST system's "Provider" interface also cannot have a NAT device between this interface and the LAN side CMA server or LAN side endpoints. Installing a VBP-ST on a DMZ port for port monitoring is supported; please reference the "VBP required Ports_V8_11.16.2007.pdf" document for installing the system on a DMZ port. Ask your Polycom Account team for this document.

- Configure VBP-ST network IP's and related parameters
- From the VBP you should be able to send an ICMP ping to a public IP and get a response
- Configure the VBP-ST in WAN/**Provider** side gatekeeper mode
- Configure the WAN/**Provider** side gatekeeper address as the CMA server IP
- Enable H.460-18 support – keep-alive time = 45 (secs)
- Install your certificate – default certificate provided
- Configure Access Proxy protocols
- Configure "Route" in the GUI as necessary to support other subnet's behind the WAN/Provider-side interface. In the diagram below a single subnet example was used.

DNS A Record entry for the VBP-ST Subscriber interface IP. This DNS name needs to be resolvable by the HDX's configured DNS server to create VC2 based TCP SSL connections request to the VBP-ST system for secure proxy services to the CMA server.

Address (A) Records

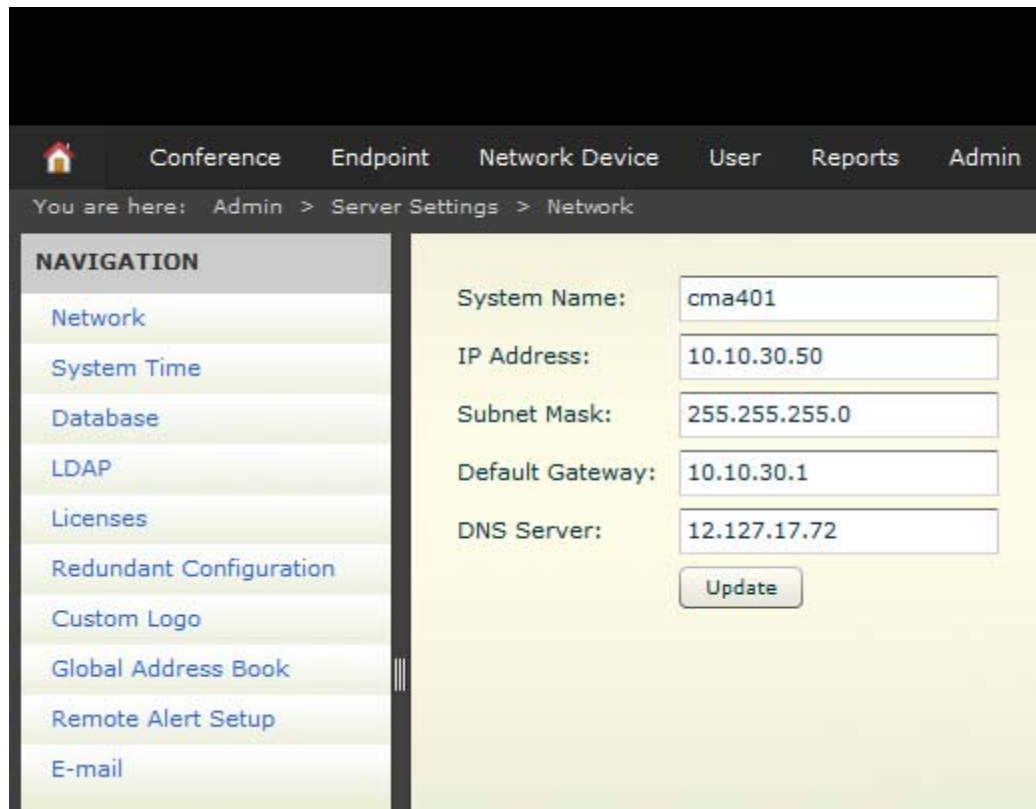
The address record allows you to map a name to an internet address. Every domain name has a primary address record which associates the domain name with an IP address. Consider the following example:

```
vbpap.abc.com.      IN A    66.134.240.260
```

HDX Installed in the remote location and able to "ping" the DNS name of the VBP-ST interface

Configuration steps for the CMA server

1. Configure the CMA servers IP and related network parameters – note: the default gateway is set for the network IP of the corporate data firewall/NAT device – it is recommended for remote configuration tasks to manage the CMA server through the corporate data firewall.



The screenshot displays the configuration interface for the CMA server. At the top, there is a navigation bar with a home icon and menu items: Conference, Endpoint, Network Device, User, Reports, and Admin. Below this, a breadcrumb trail reads: You are here: Admin > Server Settings > Network.

On the left side, there is a 'NAVIGATION' menu with the following items: Network (highlighted), System Time, Database, LDAP, Licenses, Redundant Configuration, Custom Logo, Global Address Book, Remote Alert Setup, and E-mail.

The main configuration area on the right contains the following fields:

- System Name:
- IP Address:
- Subnet Mask:
- Default Gateway:
- DNS Server:

Below these fields is an 'Update' button.

2. Configure CMA users – in this example we will use the local CMA database for CMA users – LDAP server is optional
 - Click -- > Users
 - Select “Add user”
 - Enter data
 - Select “ok”

Add New User

General Info
Associated Endpoints
Associated Roles
Associated Alert Profile

First Name

Last Name

User ID

Password

Confirm Password

Email Address

Ok Cancel Help

3. Configure the VBP as a Network Device
 - Click -- > Network Device -- > VBPs
 - Select “Add” under “Actions”
 - Enter data for the VBP
 - Select “Ok”

Add VBP

Model: ST-Series

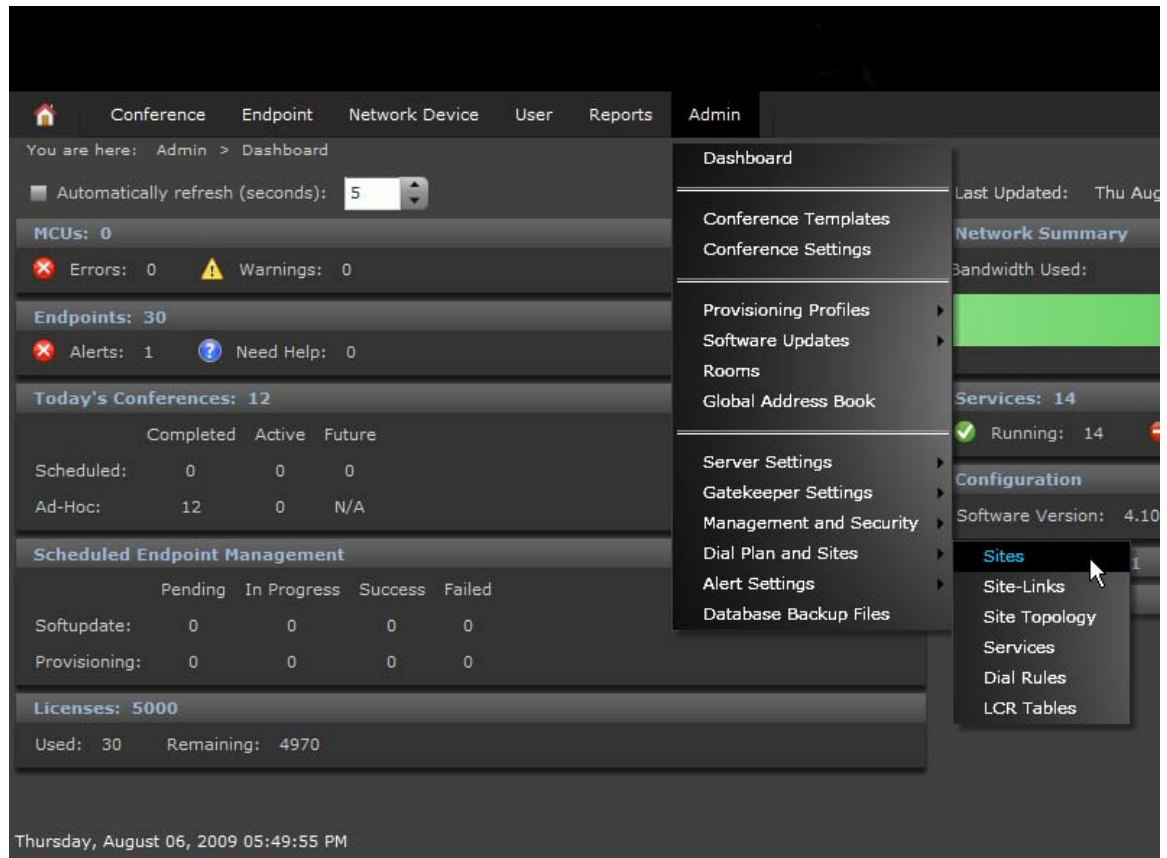
Name:
Unique name to identify this VBP.

Provider-side IP:
Provider interface IP address.

Subscriber-side IP:
Subscriber interface IP address.

Ok Cancel

4. This step is required for HDX support only, setting this parameter will not affect the functionality of “remote” CMA Desktop users.
 - Click -- > Admin
 - Dial Plan and Sites -- > Sites
 - Select and highlight the “Default site”
 - Click -- > Edit Site Provisioning details
 - Select -- > Firewall Settings
 - i. De-select “Use Fixed Ports”
 - ii. Select “Enable H.460 Firewall Traversal”
 - Select -- > ok



Screen shots for CMA “sites”

NAVIGATION

- Sites
- Site-Links
- Site Topology
- Services
- Dial Rules
- LCR Tables

SITE ACTIONS

- Add
- Edit
- Edit Site Provisioning Details

Name	Description	Country Code	Area Code	Max Bit Rate (kbps)
Internet/VPN	Internet placeholder.			2000000
EW:Primary Site	Default Site			2000000
Demo	Demo only			2000000

Thursday, August 06, 2009 05:48:00 PM

Edit Site Provisioning Details

- Date and Time Settings
- Firewall Settings**
- H.323 Settings
- Provisioning Settings
- Quality of Service Settings
- Security Settings
- CMA Desktop Settings

Use Fixed Ports

Start TCP Port

Start UDP Port

Enable H.460 Firewall Traversal

NAT Configuration

- Off
- Auto
- Manual

NAT Public (WAN) Address

NAT is H.323 Compatible

Address Displayed in Global Directory

Ok Cancel Help

Configuration steps for the VBP-ST

Configure the VBP-ST network parameters

1. Select - > Network
2. Configure the Network parameters – Note: on the 5300LF chassis “Provider Ethernet port is Port 2 and the Subscriber is Port 1 on the front panel” See the hardware guides to reference which interface port is used for the VBP platform you are using.
3. Select - > Submit

Terminology clarification – the VBP-ST uses the terms “Subscriber and Provider” the VBP-E uses the term’s WAN/LAN – this is why both terms are in the GUI; when working with the VBP-ST think Subscriber = WAN and Provider = LAN.

- LAN/**Subscriber**-side interface is installed on the WAN/Internet
- WAN/**Provider**-side interface is installed on the LAN

[Help](#)

Network

Networking configuration information for the public and private networks.

Subscriber Interface Settings:

IP Address:

Subnet Mask:

Provider Interface Settings:

DHCP
 Static IP Address

IP Address:

Subnet Mask:

Network Settings:

Default Gateway:

Note: In case of dynamic links, this DNS server address will override the DNS server address obtained from the Servers. Default value for dynamic links is obtained from the server ,if left blank .

Primary DNS Server:

Secondary DNS Server:

Configure the VBP-ST VoIP ALG H.323 settings

1. Select - > VoIP ALG
2. Select - > H.323
3. Select - > WAN/Provider-side gatekeeper mode
4. Enter data - > WAN/Provider-side GK address = 10.10.30.50
5. Enable H.460.18 Support
6. Keep-alive time = 45 seconds (default)
7. All other parameters are default settings
8. Click - > submit

Specify the **Gatekeeper mode** by selecting the desired mode. If "None" is selected, H.323 processing will be disabled. "WAN/**Provider**-side gatekeeper" mode will cause the system to forward all client RAS messages on port 1719 and 1720 to the gatekeeper.

H.460.18 Support allows the system to do H.460.18 NAT traversal for endpoints that support it. The endpoint will have to have H.460.18 enabled as well for NAT traversal to work. The **Keep-alive time** is the time given to the endpoint, CMA desktop clients and other compatible H.460 endpoint's will use this interval for sending keep-alive packets. These packets keep the NAT/Firewall port bindings open and allows NAT traversal to work. A lower time will increase bandwidth usage but the time must be lower than the NAT/Firewalls port binding expiration time. The **Stale Time** settings allows for automatic deletion of stale endpoints if the **Delete stale clients** checkbox is enabled. An endpoint is considered stale if more than **Stale time** minutes have passed since the last registration from that client this will assist when using the CMA desktop in a mobile environment, i.e. moving from a home office to the corporate data network – the registration from one location needs to time out and be removed from the system in order for the same client to register in from a different location. The automatic deletion can be prevented by locking the client in the client list.

H.323 Settings [Help](#)

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
- Peering-Proxy mode (configure [prefixes](#))

WAN/Provider-side gatekeeper mode settings

The H.323 gatekeeper that all client traffic shall be forwarded to.

WAN/Provider-side GK address:

Modify Time-To-Live:

New Time-To-Live (s):

Gatekeeper reachability:

Select Certificate Repository to install your own cert

Certificates are maintained here in the Certificate Repository (CR). An entry represents either a client or a server. A client entry in the CR has only a Certificate Authority certificate; a server entry has a certificate, the certificate's private key, and an optional password that protects the key. An entry is referenced by the name of the certificate, such as cacert.pem, which was also the name of the file when it was uploaded. An entry can be added, deleted, and viewed but not edited. Since certificate, private key, and password are so highly interdependent, there would little reason to edit an entry. To do so, such as to change the name of an entry, you must delete the entry and add it anew. An entry can only be deleted if it is not being referenced elsewhere; you must remove those references before deleting the entry. When an entry is viewed, the PEM-encoded file contents are displayed, not the file names. VBP certificate repository allows you to browse your hard drive to upload you generated certificate and private key combinations. A file must be in Base64, PEM-encoded format and have the file extension, ".pem". A file name can be up to twenty characters long and contain any character except forward slash. The password is never displayed, can be from one to twenty characters long, and contain any character except space, single quote, and double quote.

The VBP has a default certificate and private key installed that can be used to configure all the access proxy protocols, or you can install separate certificates and key's for each protocol.

This document was created using a certificate "vbpcert.pem" and private key "vbpkey.pem" this certificate combination did not use a "password" during the generation process;

- vbpcert.pem
- vbpkey.pem

Shown below is "stunnel.pem" certificate, this certificate is by default installed on the system and is used for another application. This certificate will not work correctly for access proxy configurations, in other words, do not use it to configure the access proxy. At the time of this document "stunnel" support is not enabled for the VBP – this feature is for SSL TLS connections and tested only in a specific environments, if you have interest in this feature ask your Polycom account team for details on how this feature can be deployed.

The Access Proxy accepts incoming "public" connections from clients on the LAN/Subscriber-side interface and propagates those connections to the configured CMA server on the WAN/Provider-side. It is a secure reverse proxy, not a forward proxy like most other proxies with which you may be familiar, such as an HTTP or SIP proxy. Access Proxy is also not an ALG because it in no way modifies the tunneled data.

Certificate Repository [Help](#)

Certificates and their associated private keys and passwords are stored in this repository and referenced elsewhere by Certificate file name.

Certificate			
Select: All None		Action: Delete	
	Certificate	Private Key	Password
<input type="checkbox"/>	ssl_cert.pem		
<input type="checkbox"/>	stunnel.pem		
<input type="checkbox"/>	vbpcrt.pem	vbpkey.pem	

Add a certificate

Action: Add new certificate ▾

Certificate: Browse_

Private Key: Browse_

Password:

Commit Reset

- LAN/Subscriber-side interface is installed on the WAN/Internet
- WAN/Provider-side interface is installed on the LAN

[Help](#)

Configure the Access Proxy protocols

1. Select -> System
2. Select -> Access Proxy
3. Configure your proxy ports as shown below
 - a. 443
 - b. 389
 - c. 5222
4. Enable Access Proxy -> click Commit

In the below example the same certificate was used “vbpcert.pem” you could use a different certificate for each entry if desired.

Note: the “Provider Address” is the IP address of your CMA server.

Access Proxy

HTTPS Provisioning for VBP is enabled on port= 445.

An access proxy can provide a secure connection between Subscriber clients and Provider servers.

Settings

Enable Access Proxy:

Access Proxy							
Select: All None						Action: <input type="button" value="Delete"/>	
	Name	Type	Subscriber Port	Subscriber Certificate	Provider Address	Provider Port	Provider Certificate
<input type="checkbox"/>	HTTPS	HTTPS	443	vbpcrt.pem	10.10.30.50	443	vbpcrt.pem
<input type="checkbox"/>	LDAP	LDAP	389	vbpcrt.pem	10.10.30.50	389	vbpcrt.pem
<input type="checkbox"/>	XMPP	XMPP	5222	vbpcrt.pem	10.10.30.50	5222	vbpcrt.pem

Add an access proxy

Action:

Name:

Type:

Subscriber Port:

Subscriber Certificate:

Provider Address:

Provider Port:

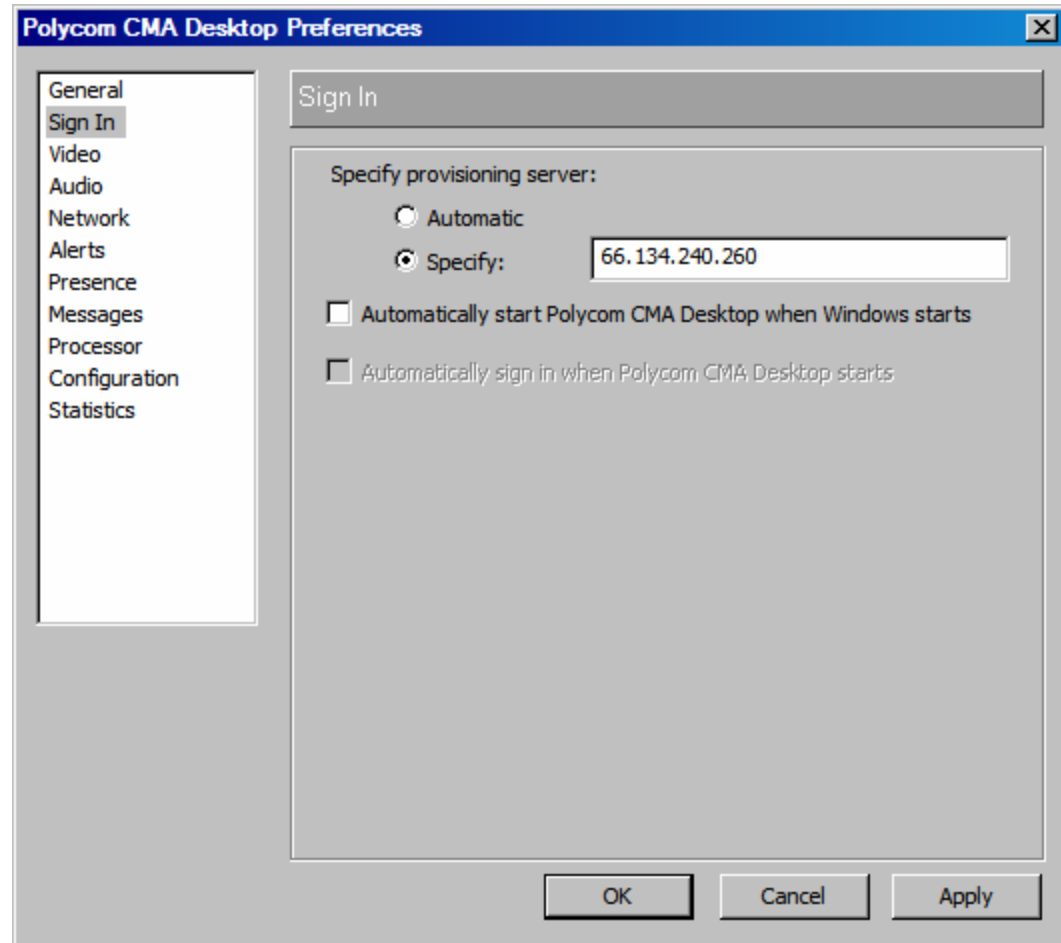
Provider Certificate:

CMA Desktop Configuration

You will need to define the “Provisioning Server” (VBP-ST Subscriber IP) you want to connect to.

Open the CMA desktop application

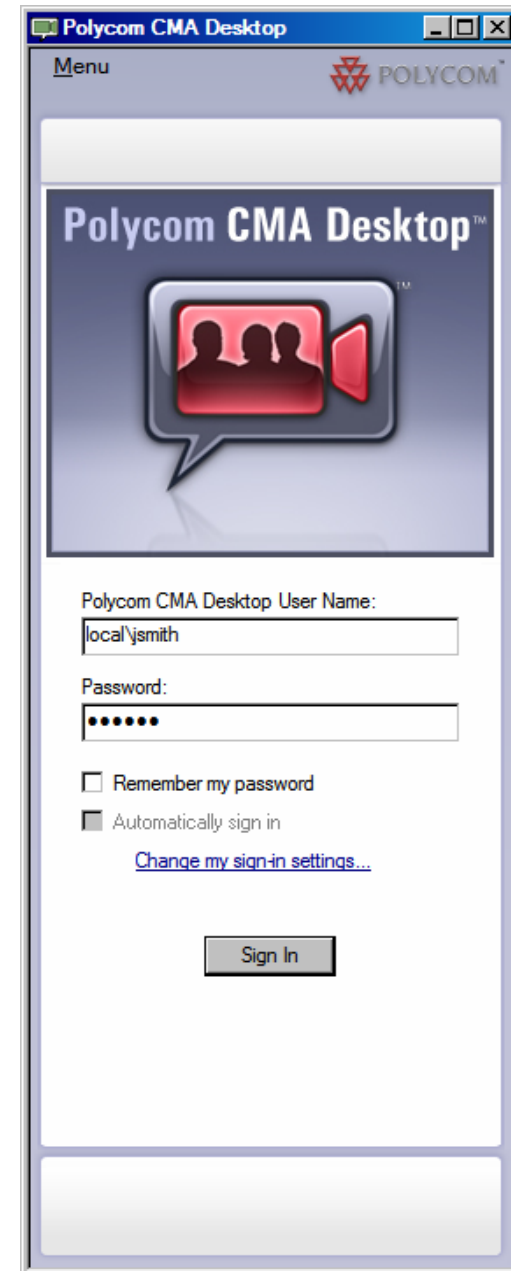
1. Select - > Menu
2. Select - > Preferences
3. Click on the “Sign In” tab
4. Specify provisioning server - > 66.134.240.260
5. Select - > Apply then Ok



Sign into the CMA server

1. Polycom CMA Desktop User Name - > local\jsmith
2. Password - > the password you created for this user on the CMA "User" setup
3. Click - > Sign in

The CMA desktop client will now create and HTTPS, LDAP, XMPP and H.323/H.460 connections to the Access Proxy for CMA access.



HDX Configuration

For systems prior to having 2.5.0.5 firmware installed it may be necessary to “factory restore” the system before configuring the system for VC2 services. The VC2 configuration parameters automatically configure certain system parameters i.e. H.323, LDAP settings, when this “automated” configuration happens as part of the new “Access Proxy” installation you can no longer change these parameters on the “GUI”. Changes to these fields will be controlled from the CMA interface.

Since systems prior to 2.5.0.5 “may” have H.323 and LDAP existing configurations, this “may” cause the system to have issues accepting the VC2 automatic configuration details. If you are having issues getting the system to connect, perform a factory reset on the HDX using the “Tech Bulletin - HDX Flash Memory Erase Procedure.pdf” procedure.

Note: for reverting a HDX out of VC2 mode a “factory reset” is “required” in the version Below are the minimal settings for configuring a HDX for VC2 mode using the HDX GUI

Configure the LAN Properties

1. Click --> Admin Settings (you will be re-directed to the HTTPS interface and if security is enabled, the system will prompt you for a “Login and Password”)
2. Click --> LAN Properties
3. Enter a “Domain Name” – this parameter needs to be set, in the below screen shot the CMA’s “local” domain was defined, however you could enter “abc.com”. For future reasons this should be set to a valid DNS resolvable domain.
4. Click --> Update (the system will now restart)

LAN Properties

IP Address:
 Link-Local:
 Site-Local:
 Global Address:
 Default Gateway:
 Host Name:
 Domain Name:
 DNS Servers:
 LAN Speed:

Update


Obtain IP address automatically ▾

fe80::2e0:dbff:fe08:91df/64

Cam1BeachHDX

local

Auto ▾ 100 Mbps



Configure the Provisioning Service

1. Click -- > Admin Settings (you will be re-directed to the HTTPS interface and if security is enabled, the system will prompt you for a “Login and Password”)
2. Click -- > Global Services
3. Click -- > Provisioning Service
4. Domain Name: Enter the CMA domain, in the screen shot “local” was the default CMA domain when the CMA was configured.
5. User Name: Enter the CMA configured user “jsmith”
6. Change Password: Select this to show the password options and enter the password for user “jsmith” note: after the system configures this user it will NOT show any password characters when re-visiting this page.
7. Server Address: Enter the VBP-ST DNS name

This field requires a DNS A record name for the VBP-ST Subscriber IP address. This DNS name needs to be resolvable by the HDX’s configured DNS server to create VC2 based TCP SSL connections request to the VBP-ST system for secure proxy services to the CMA server.

8. Click -- > Update

Note: Adding or changing a DNS A record on the public Internet DNS server’s can take 24 hours to propagate, try pinging the DNS name from a PC using the same DNS server IP’s before entering the DNS name in the HDX.

Provisioning Service

Domain:	<input type="text" value="local"/>
User Name:	<input type="text" value="jsmith"/>
Change Password	<input checked="" type="checkbox"/>
New Password:	<input type="password" value="•••••"/>
Confirm Password:	<input type="password" value="•••••"/>
Server Address:	<input type="text" value="vbpap.abc.com"/>

Troubleshooting Access Proxy

Using the VBP-ST for connection related troubleshooting will be the method discussed. The CMA server can give you some immediate information using the logs; however, if there is no connection to the CMA server, the VBP's CLI interface will be the best place to start when diagnosing a connection related issue.

The best method to connect to the VBP for troubleshooting is the CLI interface. The VBP supports SSH and telnet to give you CLI access; SSH is the recommended method to connect to the CLI.

When troubleshooting you will need the CLI login/password, this login/password is not documented for security reason's, please call Polycom Support 800.POLYCOM – 800.765.9266

If you are not familiar with SSH, you can do an Internet search for "putty" and download this freeware client. Putty is a "secure shell" client and encrypts the session to ensure no-one listening on port 22 can intercept your session and see clear text commands.

1. Check to see if the Access Proxy service is bound to the ports you've defined.
 - a. Login with SSH
 - b. Type - > netstat -ap

Example IP's only, the IP's were changed to protect the innocent

```
# netstat -ap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State                   PID/Program name
tcp      0      0 10.10.30.90:5060        *:*                     LISTEN                  30356/mand
tcp      0      0 12.48.203.90:5060        *:*                     LISTEN                  30356/mand
tcp      0      0 66.134.240.260:389      *:*                     LISTEN                  11134/accessproxyd
tcp      0      0 66.134.240.260:5222     *:*                     LISTEN                  11134/accessproxyd
tcp      0      0 *:80                    *:*                     LISTEN                  605/boa
tcp      0      0 *:21                    *:*                     LISTEN                  602/inetd
tcp      0      0 *:22                    *:*                     LISTEN                  620/sshd
tcp      0      0 *:23                    *:*                     LISTEN                  602/inetd
tcp      0      0 10.10.30.90:1720        *:*                     LISTEN                  30356/mand
tcp      0      0 66.134.240.260:1720     *:*                     LISTEN                  30356/mand
tcp      0      0 66.134.240.260:443      *:*                     LISTEN                  11134/accessproxyd
tcp      0      300 66.134.240.260:22       198.144.260.20:2245    ESTABLISHED            24321/sshd: root@tt
udp      0      0 *:514                   *:*                     625/syslogd
udp      0      0 66.134.240.260:161      *:*                     30145/snmpd
udp      0      0 10.10.30.90:161         *:*                     30145/snmpd
udp      0      0 10.10.30.90:1719        *:*                     30356/mand
udp      0      0 66.134.240.260:1719     *:*                     30356/mand
udp      0      0 *:69                    *:*                     602/inetd
raw      0      0 *:255                   *:*                     7                       30356/mand

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State      I-Node PID/Program name  Path
unix   2      [ ]         DGRAM     LISTENING  883383 30356/mand        /tmp/.mandctl_socket
unix   2      [ ACC ]     STREAM    LISTENING  883419 30380/asterisk    /var/run/asteriskctl
unix   2      [ ]         DGRAM     LISTENING  883385 30356/mand        /tmp/.mandctl_dbg_socket
unix   5      [ ]         DGRAM     LISTENING  2452   625/syslogd       /var/tmp/log
unix   2      [ ]         DGRAM     LISTENING  2103293 605/boa
unix   2      [ ]         DGRAM     LISTENING  883391 30356/mand
unix   2      [ ]         DGRAM     LISTENING  2488   606/cron
```

You will see the “accessproxyd” process bound to port 443,389 and 5222, this verifies the access proxy is running and listening to the correct ports.

You can also run a “ps” and see all processes running, however, if you run a “ps | grep access” you will get a more specific output that shows only the access proxy processes.

```
# ps | grep access
11134      root      11556    S    /usr/local/bin/accessproxyd
11140      root      11556    S    /usr/local/bin/accessproxyd
11141      root      11556    S    /usr/local/bin/accessproxyd
11143      root      11556    S    /usr/local/bin/accessproxyd
11146      root      11556    S    /usr/local/bin/accessproxyd
```

Since we are in this section to verify the access proxy process, if your CMAD client cannot initialize the media service you want to look at the “mand” process, as shown in the output of netstat –ap; you’ll see mand listening on port 1720 and 1719. Port 1719 is listening on both the Subscriber and Provider IP’s for RAS registration messages, port 1720 is also listening on both interface’s for call setup.

The output of “ps | grep mand” should show multiple instances of mand, note the “state” column, “S” is what you should expect, if you see a “Z” for either the accessproxy or mand process, this mean’s the process is in a “zombie” state, meaning a portion of the process is dead, but still existing. If you find this, collect the following and contact Polycom support with the output.

Note: collect the data required, if this was a previously working solution and you are troubleshooting a connection related problem and you find a zombie, entering “reboot” on the CLI may temporarily get you back and running, however collecting the data and getting to the root cause will solve the issue permanently, please collect the data below before rebooting and then contact Polycom Support.

- cat /var/log/messages
- cat /var/log/messages.old
- mandctl dbg replay
- cat /var/replay.cfg
- cat /var/mand/tinfo
- ps
- vmstat 3 (leave this run for a few lines, then ctrl c to stop)

The above will give the development team some historical date of the system state when the zombie accrued and possibly why it happened –
Note: it is likely that more debug will be requested by support if the above is inconclusive.

2. Check that your Access Proxy port connections are being received and forwarded.

For this process support will need traces, to setup a trace follow the below instructions. The VBP uses a linux kernel and supports the “tcpdump” command, this command tells the sub-system to capture a full decode of the packets that are coming in on the wire on the interface defined. This capture is then FTP-ed off the VBP system to a FTP server and then opened with the “WireShark” application to assist in troubleshooting many issues associated with connection problems.

For the first step we need to create a temporary space on the VBP's flash drive to capture these packets – note: this temporary space will not survive a reboot and should be un-mounted after the traces are taken, as this space is taking available memory the system “could” need at a later date, so its very important to un-mount the space.

On the CLI type

Type - > `mount -t tmpfs tmpfs /etc/images -o size=8m`

Note: you can cut&paste the above command, however the “-t” maybe converted to “.t” make sure you correct the syntax if it does not paste correctly.

Now type “df” and you will see file system /etc/images/ mounted with 8megs of space

```
# df
Filesystem          1k-blocks    Used Available Use% Mounted on
rootfs              23208       23208         0 100% /
/dev/ram0           23208       23208         0 100% /
/dev/hdc5           4939         85      4599   2% /etc/config
/dev/ram1          15856       1636     14220  10% /var
tmpfs               128000         0     128000   0% /var/spool/asterisk/voicemail/default
tmpfs                8192         0       8192   0% /etc/images
```

You are now ready to start the trace. The most common method support uses is to trace on the “any” interface, this allows for a single trace to capture both the provider and subscriber related traffic

`tcpdump -s 0 -ni any not port 22 -w /etc/images/ANYap.pcap`

The filename “ANYap.pcap” can be anything, if your troubleshooting a H.323 related connection issue, its handy to have different names for your traces (i.e. ANYh323.pcap etc.)

What is also handy is to filter out unwanted traffic. Above the “not port 22” qualifier filters out the SSH session traffic. Remember, there is only 8 megs of space to work with, and if there is RTP video traversing the VBP at the same time, the temporary space can fill up very fast, perhaps in a matter of seconds.

If the temporary disk fills up too fast, your trace will be useless because you may have missed the packets you're trying to capture versus the normal working traffic, this really depends on what you're troubleshooting, let me give you an example.

If support was trying to figure out why "Remote location A" couldn't connect to the access proxy, support would filter on that location's source IP

```
tcpdump -s 0 -ni any host 12.48.202.260 or host 10.10.30.50 -w /etc/images/ANYremoteA.pcap
```

This allows the trace to only capture packets to/from 12.48.202.260 and packets going to to/from the CMA. Unfortunately as all connection request packets go through the access proxy, they will all be destined for 10.10.30.50; however it will limit the Subscriber traffic quite a bit and allow support to look through the trace and find the packets going out to the CMA more easily. This will limit the size of the trace and allow you more time to capture data before the temporary /etc/images 8MB space fills up – this is our mission, capture the relevant data while the problem is happening, and have that data be as specific as we can.

Other filters can make capturing the data more specific, if you're already comfortable with the tcpdump command you can set the filter as needed for what you're trying to capture.

If you do an Internet search for tcpdump, there are many filters, however the above should get support what they need for problem isolation.

To stop the trace enter "ctrl c" that's hold the "ctrl" key on your keyboard and depress the letter "c"

Now that you have created the trace, you need to upload this to a FTP server, or if you are familiar with the SCP (secure copy) application you can attach directly to the VBP and copy the file to your hard drive. Note: SCP also uses SSH methods to connect to the VBP, so the session is secure/encrypted. WinSCP is also a free ware application that can be downloaded.

To FTP the file to a FTP server;

```
cd /etc/images
type "pwd" print working directory – this will show you where you are on the system
type "ls" this stand for "list the files" similar to a windows "dir"
```

```
# cd /etc/images
# pwd
/etc/images
# ls
ANYremoteA.pcap
#
```

Below is a sample FTP connection, the commands in blue is what was typed.

```
# ftp 204.202.2.260
Connected to 204.202.2.260.
220-
```

```
220-#####  
220-Welcome to ABC Networks FTP server!  
220-  
220-Please send any questions or reports about this server to  
220-support@abc.com  
220-#####  
220 204.202.2.260 FTP server ready  
Name (204.202.2.260:root): jsmith  
331 Password required for jsmith.  
Password:*****  
230 User jsmith logged in.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> lcd /etc/images  
Local directory now /etc/images  
ftp> put *.pcap  
local: ANYremoteA.pcap remote: ANYremoteA.pcap  
200 PORT command successful  
150 Opening BINARY mode data connection for ANYremoteA.pcap  
226 Transfer complete.  
ftp> bye  
221 Goodbye.
```

You can now login to the FTP server you put the file on and retrieve it to view the packets in WireShark. Note: this is also a free ware application that can be downloaded.

Always remember to “rm” remove and unwanted traces and remove traces between captures to ensure you get the full use of the 8MB temporary disk space.

Note: Make sure you have FTP-ed the traces you want off the system before removing them, once removed you cannot recover the file.

```
# pwd
/etc/images
# ls
ANYh323.pcap      ANYremoteA.pcap
# rm *.pcap
# ls
#
```

When you are done capturing its very important to “umount” /etc/images Note: You cannot umount /etc/images/ if you in this directory.

After the umount command type “df” and you should not see /etc/images mounted.

Type - > umount /etc/images

See below example

```
# umount /etc/images
umount: /etc/images: Device or resource busy
# pwd
/etc/images
# cd /
# pwd
/
# umount /etc/images
# df
Filesystem          1k-blocks    Used Available Use% Mounted on
rootfs              23208       23208         0 100% /
/dev/ram0           23208       23208         0 100% /
/dev/hdc5            4939         85     4599    2% /etc/config
/dev/ram1           15856       1640    14216   10% /var
tmpfs               128000         0    128000    0% /var/spool/asterisk/voicemail/default
```

Data collection

Now that we've covered some troubleshooting techniques for the VBP-ST running the Access Proxy, the more data you can capture previous to contacting support the greater chance support has of solving the issue quickly.

If, with the above steps, you cannot uncover the issue, then capture the data discussed and contact Polycom support, and we can assist you in isolating the issue.

- `Tcpdump` of the problem happening
- `cat /var/log/messages`
- `cat /var/log/messages.old`
- `mandctl dbg replay`
- `cat /var/replay.cfg`
- `ps`
- `netstat -ap`
- `vmstat 3`

Traffic Shaper Configuration

The traffic shaper page allows you to ensure that high priority real-time data is processed before lower priority non-real-time data. Use the following procedure to configure the traffic shaper.

Configuring the Traffic Shaper

Choose **Traffic Shaper** from the primary web configuration menu.

As you configure the functions featured on the page, review the following list:

Enable Traffic Shaping

Select this checkbox to enable traffic shaping.

Note: With traffic shaping disabled, the endpoints that are registered to the system's ALG will still have their layer 3 packets marked as TOS 0xb8 or DIFFServ AF46. Data traffic by default will be re-written to 0x00 (See Enable TOS Byte Stripping.)

Primary and Secondary WAN Downstream Bandwidth

Enter the total actual downstream bandwidth that applies to your Primary and Secondary WAN connection. This value is entered in Kbps; for example, 1024 = 1 Mbps.

Primary and Secondary WAN Upstream Bandwidth

Enter the total actual upstream bandwidth that applies to your Primary and Secondary WAN connection. This value is entered in Kbps; for example 1024 = 1 Mbps.

Enable Priority IP Address

To specify a device in the network as high priority, you can manually add its IP address to the list of high priority devices. Use care when entering IP addresses in this list. Devices that consume all the bandwidth may cause media quality problems. Enter an individual IP or range, for example 192.168.1.10-150. To delete an entry, highlight it and press the Delete key on your keyboard.

Enable TOS based routing

By default, this option is not selected. When enabled, this causes all H.323 packets to be forcefully routed through the main WAN interface. This is used in rare configurations where you want the default route to be other than the WAN interface (for example, VPN) and you want VoIP traffic to still be routed through the WAN. This option should NOT be enabled for most configurations.

Enable TOS Byte Stripping

By default, this option is selected. For all RTP traffic (voice and video) the system marks the TOS byte as High Priority, and strips (set to 0) the TOS byte for all other traffic. When this option is not selected, the TOS byte will not be stripped from non-RTP traffic, but will remain unchanged.

Note: Devices that use the ALG function (i.e. H.323 endpoints) are already marked as high priority and do not need to be in this list. All data from IP addresses in this list has the same priority as voice data. Poorly behaved data may cause voice quality problems. Use with caution!

Expedited Forwarding (Default)

This setting uses expedited forwarding as the forwarding rule.

IP Precedence

This setting uses classification of IP layer packets to determine priority.

Assured Forwarding

This setting assures that the packets will be forwarded.

Custom Value

For non-standard per-hop behavior, this field permits the use of a custom rule.

Enable Call Admission Control

Select this checkbox to enable the Call Admission Control.

Maximum Number of Calls Allowed

Determine and enter the number of calls that can be supported. If CAC is enabled and H.323 is used, then you must account for the total number of RTP streams that will be created. H.323 calls use multiple RTP streams for each video call, typically around 6-12 streams. For example, if your endpoints typically use 8 streams/call, then to allow 3 H.323 calls the CAC must be set to at least 24.

Note: It is not recommended to enable CAC when using H.323; instead, the "H.323 Maximum Bandwidth" setting is the recommended method to limit video calls.

Click Submit.

A message indicates that service will be temporarily interrupted.

Click OK to confirm.

Diagnostics and Troubleshooting

This chapter describes how to use the diagnostic information, troubleshooting tools, and system maintenance utilities on the VBP series appliance.

Viewing Version, Hardware Platform and LAN MAC Address

The software version, hardware platform, and LAN MAC address are common pieces of information requested by technical support. You can obtain this information from the **System** page.

To ensure that you are running the latest software version, visit our support website for a complete listing of software releases at:

http://www.polycom.com/support/network/security_firewall_traversal/

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.

Entering the Registration Code

If the registration code is inadvertently deleted you can re-enter the code.

1. Choose **System** from the Configuration Menu.
2. Click License Key.
3. Click Edit License Key.
4. Enter the **License Key** (registration code).
5. The registration code is printed on the sticker located on the bottom of the VBP series appliance.
6. Click **Submit**.

A message indicates that service will be temporarily interrupted.

7. Click **OK** to confirm.

Viewing Networking Information

To view the networking configuration and status of the VBP series appliance, open the **Network Information** page.

Choose **System > Network Information** from the Configuration Menu.

The Network Information page includes the following information:

Routing Information

The system routing table contains the static routes for hosts and networks that are configured on the VBP series appliance. If only the LAN and WAN IP addresses have been configured multiple lines are displayed:

- The private subnet associated with the LAN interface
- A public subnet present for the WAN interface
- An entry for the VBP series appliance loopback interface
- An entry for each IPSec tunnel
- The VBP series appliance's default gateway forwarding to the WAN interface

Additional lines may be displayed depending on the contents of the **Route** pages. Each entry on one of these pages causes an additional entry in the routing table.

Link Status

Link Status shows 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 if the link is reported as down, the link rate may need to be set manually on the Set Link page. Incompatible rates can cause a loss of communication with the VBP series appliance. 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, make sure that the device at the far end of the connection can communicate at the desired rate.

Interface Information

The specific status and configuration information for the system interfaces is displayed in the Interface Information section.

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 this 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.

Using Troubleshooting Tools

The VBP series appliance provides convenient test tools to facilitate problem isolation and resolution. A network operator can use these tools to verify connectivity to and from the VBP series appliance and to trace data paths to endpoints throughout the network.

Ping and Traceroute Tests

The **Network Test Tools** page provides an easy way to perform a ping test or traceroute test. To access the Network Test Tools page, select **System > Network Test Tools** in the Configuration Menu.

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 VBP series appliance and the test IP address. A successful ping test does not guarantee that all data traffic is allowed between the VBP series appliance and the test IP address, but it is useful to verify basic reachability.

1. Choose **System > Network Test Tools** from the Configuration Menu.
2. Enter an address in the IP Address to Ping field.
3. Click **Ping**.

The Network Test Tools page reopens to display results of the ping test. (This may take several seconds.)

4. Click **Reset** to clear the data.

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.

1. Choose **System > Network Test Tools** from the Configuration Menu.
2. Enter an address in the IP address to Trace field.
3. Select **WAN** or **LAN**.
4. Click Traceroute.

The Network Test Tools page reopens to display results of the test. (This may take several seconds.)

5. Click **Reset** to clear the data.

Networking Restart

Technical support may request that networking services be restarted during a troubleshooting session. In this case, you can use the **Network Restart** page to stop and restart all the networking services that are running on the system.

Restart networking services

1. Choose **System > Restart** to open the Networking Restart page.
2. Click **Submit**.
3. A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

Note: Restarting network services will interrupt the system for up to a minute. All voice, video and data sessions currently in progress will be interrupted. Proceed with caution.

Rebooting the System

Rebooting the system stops all networking services and reboots the system. The operating system and networking services will be loaded from scratch. Reboot is functionally equivalent to power cycling the system. Technical support may request that the system be rebooted during a troubleshooting session.

Note: As an alternative to rebooting, you can perform a reset locally by temporarily disconnecting the power cable from the VBP series appliance.

Reboot the system

1. Choose **System > Reboot System** from the Configuration Menu.
2. Click **Reboot**.
3. Click **Submit**.

A message indicates warns that rebooting the system will interrupt services for a few minutes.

4. Click **OK** to confirm.

Note: Rebooting the system will interrupt services for a few minutes. All voice, video and data sessions currently in progress will be interrupted. Proceed with caution.

Using T1 Diagnostics

Open the T1 Diagnostics page to display T1 diagnostic information and statistics and run diagnostic commands.

Perform T1 diagnostics

1. Choose **System > T1 Diagnostics** from the Configuration Menu.
2. Select the loopback test you want to run from a pull-down list, and click **Submit** for the desired interface.
3. Select the BERT test type from the BERT menu and click **Submit**.

The BERT test sends a framed Quasi Random Bit Sequence (QRBS) on the T1 link and monitors the receive path for bit errors. A BERT test is usually run in conjunction with a network loopback at the remote end so that the test pattern sent by the VBP appliance can be compared to the pattern received on the same interface. The VBP can send a QRBS 2¹⁵-1 and a QRBS 2²⁰-1 pattern.

Note: The VBP series appliance also responds to network generated, AT&T formatted loop up/down codes. Loopback codes sent from far end equipment will loop the T1 interfaces back towards the network.

The T1 Status shows the current alarm state and indicates if there is a loopback or BERT test in progress.

The T1 Diagnostics page displays the current 15-minute (CUR) and 24-hour total (SUM) statistics for the T1 interfaces. This information allows you to compare performance from different time intervals.

View T1 Statistics

1. Choose **System > T1 Diagnostics** from the Configuration Menu.
2. Click **Reset** to clear the statistics for the current interval.
3. A message indicates that service will be temporarily interrupted.
4. Click **OK** to confirm.

View advanced T1 diagnostics

1. Choose **System > T1 Diagnostics** from the Configuration Menu.
2. Click T1 advanced diagnostics page
3. The page displays data for each 15-minute interval over the last 24 hours.

Note: The oldest-15 minute interval is removed from the 24-hour total as each new 15-minute interval is added.

Device Configuration Management

This chapter describes the tools available to manage the VBP series appliance configuration. It contains the following sections:

Overview

The VBP appliance 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 VBP appliance and then stored in RAM as “running” state.

The VBP appliance 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 VBP appliance or on remote TFTP servers.

The Command Line Interface (CLI) provides access to these files and the utility that enables you to copy them. The CLI can be accessed with a local terminal connection or remotely using SSH.

Follow these guidelines when connecting to the CLI:

Use a straight-through or null modem cable to connect to the console port of the VBP series appliance (Note: 5300 appliances use a null modem cable).

Use a terminal emulator such as HyperTerminal set to a baud rate of 9600, 8 data bits, 1 stop bit, and no and parity. Alternatively, you can connect to the VBP series appliance remotely using SSH. Log on as root and enter the password provided by Edgewater.

Note: No more than two backup files can be stored in the VBP series appliance’s flash memory because of size constraints. Also, it is recommended that you create a backup file after any configuration changes are made to the VBP series appliance. 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.

Using the configuration backup command

The **ewn** command is used to perform backup file operations with the Command Line Interface (CLI).

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

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.

Creating a backup file and save to local flash

The following command creates a backup file of the current running configuration and saves it to local flash memory:

```
bash# ewn save <filename>
```

Filename format (must use extension .conf1 or .conf2):

```
<filename1>.conf1
```

```
<filename2>.conf2
```

<filenameX> can be a combination of both letters and characters. For example, EWNxx_041503.conf1 or location1_Exx00.conf2. Trying to use any other filename format will result in the error message: "EWN_ERROR_BAD_FILE_NAME".

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

Copy a backup file to a remote TFTP server

The following commands copies a backup file from the VBP series appliance to a TFTP server.

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

Download a backup file from a remote TFTP server

The following command downloads a backup file from a TFTP server to the VBP series appliance.

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

List available backup files

The following command lists all backup files stored in flash memory. If no file has been saved, the command will only return the bash# prompt.

```
bash# ewn list
```

Delete a backup file

The following command deletes the specified the backup file:

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

Loading a backup file to become the running configuration

The following command loads the specified backup file into RAM and makes it the active running configuration.

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

Note: Issuing this command will automatically restart the VBP series appliance and therefore interrupt any active H.323 calls and data sessions.

Regulatory Notices

Important Safeguards
<p>Read and understand the following instructions before using the system:</p> <ul style="list-style-type: none">• 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. <p>SAVE THESE INSTRUCTIONS.</p>

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, NEGLIGENCE, 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.**

11.1 **Governing Law.** THIS AGREEMENT SHALL BE GOVERNED BY THE LAWS OF THE STATE OF CALIFORNIA AS SUCH LAWS ARE APPLIED TO AGREEMENTS ENTERED INTO AND TO BE PERFORMED ENTIRELY WITHIN CALIFORNIA BETWEEN CALIFORNIA RESIDENTS, AND BY THE LAWS OF THE UNITED STATES. The United Nations Convention on Contracts for the International Sale of Goods (1980) is hereby excluded in its entirety from application to this Agreement.

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. © 2008. 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.

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

Appendix A. Compliance and Compatibility for the VBP 200EW Converged Network Appliance

WIRELESS

- IEEE 802.11d - Worldwide roaming
- IEEE 802.11h
- European 5GHz regulatory
- Japan 5GHz DFS
- IEEE 802.11j
- Japan Regulatory
- Korean 5GHz updates
- US Public Safety 4.9 GHz band

INDUSTRY CANADA (IC) NOTICE

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by a user to this equipment, or equipment malfunctions, may give the telephone communications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection, that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas”.

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.”

WARRANTY AND REPAIR SERVICE CENTER:

The RAM Group

Kent McDonald

kent.macdonald@theramgroup.com

(403) 266-5840 x 100

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

Appendix B. Compliance and Compatibility for the VBP 4350 Converged Network Appliance

JAPAN EMC COMPATIBILITY

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要請される場合があります。

This is a class A product based on the standard of the Voluntary Control Council for Interference (VCCI) by Information Technology Equipment. If this equipment is used in a domestic

environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

FCC PART 68 NOTICE TO USERS OF DIGITAL SERVICE

This equipment complies with Part 68 of the FCC Rules and the requirements adopted by ACTA. On the bottom surface of this equipment is a label that contains, among other information, a product identifier in the format US: EWRDENAN4300T. If requested, this number must be provided to the telephone company.

The following instructions are provided to ensure compliance with the Federal Communications Commission (FCC) Rules, Part 68.

- (1) This device must only be connected to the T1 WAN network.
- (2) Before connecting your unit, you must inform the telephone company of the following information:

Port ID	REN/SOC	FIC	USOC	
T1 WAN	04DU9-DN, 04DU9-BN	6.0N	RJ48C	
- (3) If the unit appears to be malfunctioning, it should be disconnected from the telephone lines until you learn if your equipment or the telephone line is the source of the trouble. If your equipment needs repair, it should not be reconnected until it is repaired.
- (4) If the telephone company finds that this equipment is exceeding tolerable parameters, the telephone company can temporarily disconnect service, although they will attempt to give you advance notice if possible.
- (5) Under the FCC Rules, no customer is authorized to repair this equipment. This restriction applies regardless of whether the equipment is in or out of warranty.

(6) If the telephone company alters their equipment in a manner that will affect use of this device, they must give you advance warning so as to give you the opportunity for uninterrupted service. You will be advised of your right to file a complaint with the FCC.

(7) In the event of equipment malfunction, all repairs should be performed by our Company or an authorized agent. It is the responsibility of users requiring service to report the need for service to our Company or to one of our authorized agents.

INDUSTRY CANADA (IC) NOTICE

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by a user to this equipment, or equipment malfunctions, may give the telephone communications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection, that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas”.

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.”

WARRANTY AND REPAIR SERVICE CENTER:

The RAM Group

Kent McDonald

kent.macdonald@theramgroup.com

(403) 266-5840 x 100

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

Appendix C. Compliance and Compatibility for the VBP 4350W Converged Network Appliance

WIRELESS

- IEEE 802.11d - Worldwide roaming
- IEEE 802.11h
- European 5GHz regulatory
- Japan 5GHz DFS
- IEEE 802.11j
- Japan Regulatory
- Korean 5GHz updates
- US Public Safety 4.9 GHz band

INDUSTRY CANADA (IC) NOTICE

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by a user to this equipment, or equipment malfunctions, may give the telephone communications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection, that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas”.

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.”

WARRANTY AND REPAIR SERVICE CENTER:

The RAM Group

Kent McDonald

kent.macdonald@theramgroup.com

(403) 266-5840 x 100

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

Appendix D. Compliance and Compatibility for the VBP 5300S Converged Network Appliance

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.

Appendix E. Compliance and Compatibility for the VBP 5300E Converged Network Appliance

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.

Appendix F. Compliance and Compatibility for the VBP 6400S Converged Network Appliance

This product is in compliance with European Union EMC Directive 89/336/EEC, using standards EN55022 (Class A) and EN55024 and Low Voltage Directive 73/23/EEC, Standard EN60950.

Safety Compliance

USA:	UL 60950 – 3rd Edition/CSA 22.2. No. 950-M93
Canada:	cUL Certified – CAN/CSA 22.2. No. 60950-00 for Canada (product bears the single UL mark for U.S. and Canada)
Europe:	Low Voltage Directive, 73/23/EEC/UV/GS to EN60950 2 nd Edition with Amendments, A1 = A2 + A3 + A4
International:	TUV/CB to IEC 60950 3 rd Edition, EN60950 2 nd Edition + Amd 1-4, EMKO-TSE (74-SEC) 207/94 plus International deviations
Australian / New Zealand:	CB Report to IEC 60950, 3 rd Edition plus International deviations

Electromagnetic Compatibility (EMC)

USA:	FCC CFR 47 Part 2 and 15, Verified Class A Limit
Canada:	IC ICES-003 Class A Limit
Europe:	EMC Directive, 89/336/EEC <ul style="list-style-type: none"> • EN55022, Class A Limit, Radiated & Conducted Emissions • EN55024, ITE Specific Immunity Standard • EN61000-4-2, ESD Immunity (Level 2 Contact Discharge, Level 3 Air Discharge) • EN61000-4-3, Radiated Immunity (Level 2) • EN61000-4-4, Electrical Fast Transient (Level 2) • EN61000-4-5, AC Surge • EN61000-4-6, Conducted RF • EN61000-4-8, Power Frequency Magnetic Fields • EN61000-4-11, Voltage Dips and Interrupts • EN61000-3-2, Limit for Harmonic Current Emissions • EN61000-3-3, Voltage Flicker
Japan:	VCCI Class A ITE (CISPR 22, Class A Limit) IEC 1000-3-2 Limit for Harmonic Current Emissions
Australia/New Zealand:	AS/NZS 3548, Class A
Taiwan:	BSMI Approval, Class A
Korea:	RRL Approval, Class A
China:	CCC Approval, Class A
Russia:	GOST Approved
International:	CISPR 22, Class A Limit

FCC Electromagnetic Compatibility Notice (USA)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operating in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference. In this case, the user is required to correct the interference at his or her expense. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment. The customer is responsible for ensuring compliance of the modified product.

FCC Declaration of Conformity

Product Type: TIGPR2U

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.

For questions related to the EMC performance of this product, contact:

Intel Corporation
250 Berry Hill Rd., Suite 100
Columbia, SC 29210

Electromagnetic Compatibility Notices (International)

Europe (CE Declaration of Conformity)

This product has been tested in accordance to, and complies with the Low Voltage Directive (73/23/EEC) and EMC Directive (89/336/EEC). The product has been marked with the CE Mark to illustrate its compliance.

Appendix G. Compliance and Compatibility for the VBP 6400E Converged Network Appliance

This product is in compliance with European Union EMC Directive 89/336/EEC, using standards EN55022 (Class A) and EN55024 and Low Voltage Directive 73/23/EEC, Standard EN60950.

Safety Compliance

USA:	UL 60950 – 3rd Edition/CSA 22.2. No. 950-M93
Canada:	cUL Certified – CAN/CSA 22.2. No. 60950-00 for Canada (product bears the single UL mark for U.S. and Canada)
Europe:	Low Voltage Directive, 73/23/EEC/TUV/GS to EN60950 2 nd Edition with Amendments, A1 = A2 + A3 + A4
International:	TUV/CB to IEC 60950 3 rd Edition, EN60950 2 nd Edition + Amd 1-4, EMKO-TSE (74-SEC) 20794 plus International deviations
Australian / New Zealand:	CB Report to IEC 60950, 3 rd Edition plus International deviations

Electromagnetic Compatibility (EMC)

USA:	FCC CFR 47 Part 2 and 15, Verified Class A Limit
Canada:	IC ICES-003 Class A Limit
Europe:	EMC Directive, 89/336/EEC <ul style="list-style-type: none"> • EN55022, Class A Limit, Radiated & Conducted Emissions • EN55024, ITE Specific Immunity Standard • EN61000-4-2, ESD Immunity (Level 2 Contact Discharge, Level 3 Air Discharge) • EN61000-4-3, Radiated Immunity (Level 2) • EN61000-4-4, Electrical Fast Transient (Level 2) • EN61000-4-5, AC Surge • EN61000-4-6, Conducted RF • EN61000-4-8, Power Frequency Magnetic Fields • EN61000-4-11, Voltage Dips and Intermitts • EN61000-3-2, Limit for Harmonic Current Emissions • EN61000-3-3, Voltage Flicker
Japan:	VCCI Class A ITE (CISPR 22, Class A Limit) IEC 1000-3-2 Limit for Harmonic Current Emissions
Australia/New Zealand:	AS/NZS 3548, Class A
Taiwan:	BSMI Approval, Class A
Korea:	RRL Approval, Class A
China:	CCC Approval, Class A
Russia:	GDST Approved
International:	CISPR 22, Class A Limit

FCC Electromagnetic Compatibility Notice (USA)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operating in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference. In this case, the user is required to correct the interference at his or her expense. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment. The customer is responsible for ensuring compliance of the modified product.

FCC Declaration of Conformity

Product Type: TIGPR2U

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.

For questions related to the EMC performance of this product, contact:

Intel Corporation
250 Berry Hill Rd., Suite 100
Columbia, SC 29210

Electromagnetic Compatibility Notices (International)

Europe (CE Declaration of Conformity)

This product has been tested in accordance to, and complies with the Low Voltage Directive (73/23/EEC) and EMC Directive (89/336/EEC). The product has been marked with the CE Mark to illustrate its compliance.

Japan EMC Compatibility

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

English translation of the notice above:

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) by Information Technology Equipment. If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

ICES-003 (Canada)

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques", NMB-003 édictée par le Ministre Canadien des Communications.

English translation of the above notice:

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Canadian Department of Communications.

BSMI (Taiwan)

The BSMI Certification number and the following warning are located on the product safety label that is located visibly on the external chassis.

警告使用者:
這是甲類的資訊產品，在居住的環境中使用時，
可能會造成射頻干擾，在這種情況下，使用者會
被要求採取某些適當的對策。