Optional VBP-E at the Headquarters Location

As shown in the diagram above, you can choose to install a VBP-E to allow your enterprise users to call or be called by any “publicly” reachable H.323 system. This VBP-E system can also be secured to allow only certain endpoints to call your enterprise by deploying a “whitelist/blacklist” (see the VBP configuration guide on the Polycom Support web site for details).

This VBP-E can also provide a secure SIP trunking service from your SIP provider for local and long distance calling. Some Internal SIP servers or IP-PBX systems installed on the enterprise LAN can accept direct ISDN or POTS service for offnet dialing, or you can use a separate ISDN gateway for local and long distance calling. For this example, the internal SIP server uses a SIP trunking service for local and long distance calling.

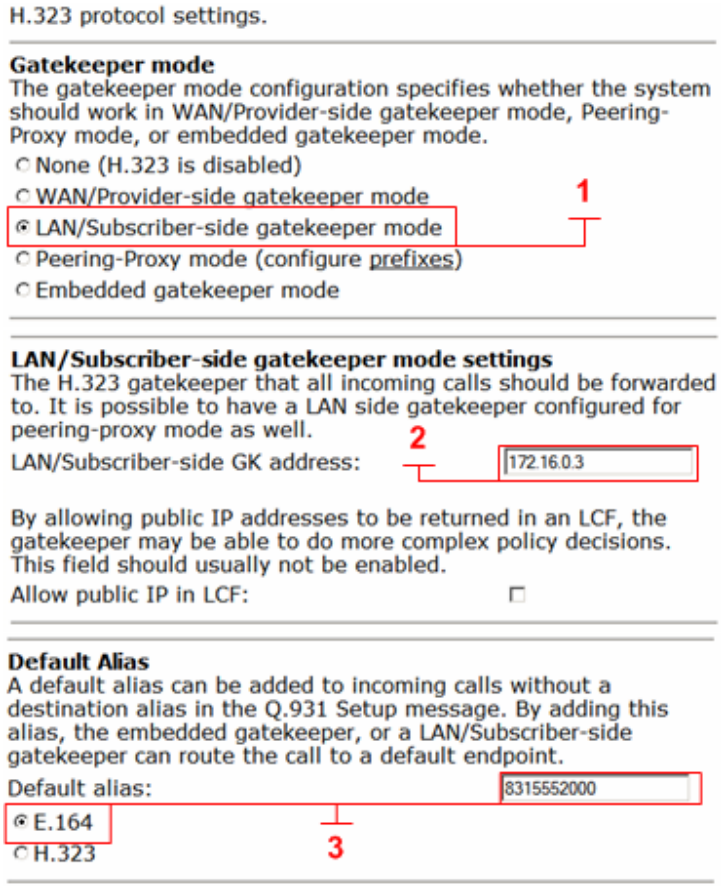
Configuring the VBP H.323 Video Settings

On the LAN-side computer, open a web browser and enter http://172.16.0.5 (this IP address implies the IP address shown in the diagram for the optional VBP-E LAN IP address). Use the following login information: Login: root / Password: default

Select “VoIP ALG” -> H.323

1. Enable “LAN/Subscriber-side gatekeeper mode.” **(1)**
2. Enter the “LAN/Subscriber-side GK address.” This will be the IP address of the CMA server. **(2)**
3. Select “Submit” to save changes.

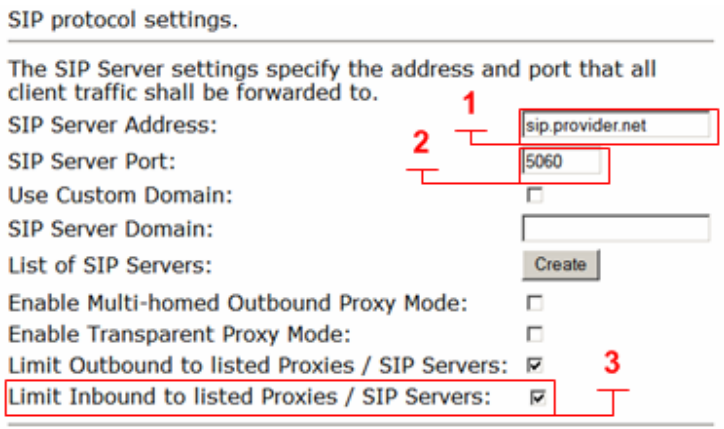
(Optional) **(3)** Set the “Default alias” to be a single endpoint or an IVR entry queue on the RMX. This feature allows a public IP endpoint to dial the IP address of the VBP-E (e.g., 12.48.260.5). When the call is received, the system will forward the call to this alias. The RMX IVR method is used by enterprise networks that do not allow direct dialing to users. This is called a “Meet in the Bridge” method.



Configuring the VBP SIP Voice Settings

Select “VoIP ALG” -> SIP

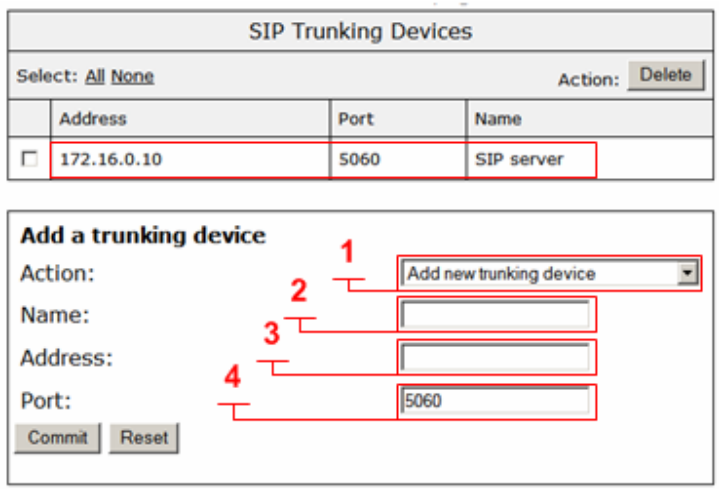
1. Set the “SIP Server Address” to your SIP provider’s IP address or FQDN. **(1)**
2. Enter the “SIP Server Port.” The default port is UDP 5060. **(2)**
3. (Recommended setting) Select the “Limit Inbound to listed Proxies / SIP Servers” setting. By limiting inbound SIP requests from the defined SIP server, you limit your chances of rogue users trying to send INVITES to your SIP server to make international long distance calls on your system. **(3)**
4. Select “Submit” to save changes.



The above settings are for outbound SIP requests. You will need to configure your internal SIP server with a SIP trunk to the LAN-side IP address of the VBP-E (e.g., 172.16.0.5). The VBP-E will then proxy SIP requests from your internal SIP server to your provider.

Select “VoIP ALG” -> SIP -> Trunking Device

1. From the “Action” list, select Add new trunking device. **(1)**
2. Enter the SIP device “Name.” This setting can be anything you want to call it. When you configure the SIP dial rules, you will apply the rules you want to the trunking device name. You can have more than one trunking device for routing different dial patterns. **(2)**
3. Enter the IP “Address” for this trunking device. This will be the IP address of the internal SIP server (e.g., 172.16.0.10). **(3)**
4. Enter the SIP signaling “Port.” By default, most SIP servers will use UDP 5060. (4)
5. Select “Commit” to save changes.



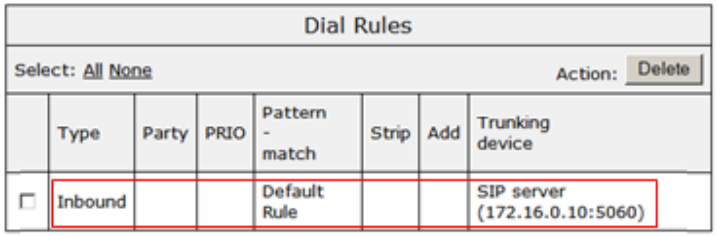
The above Trunking settings are for inbound SIP requests. When an inbound SIP message is received by the system and it matches the “Dial Rules” for this device, the SIP message will be forwarded to the defined IP address.

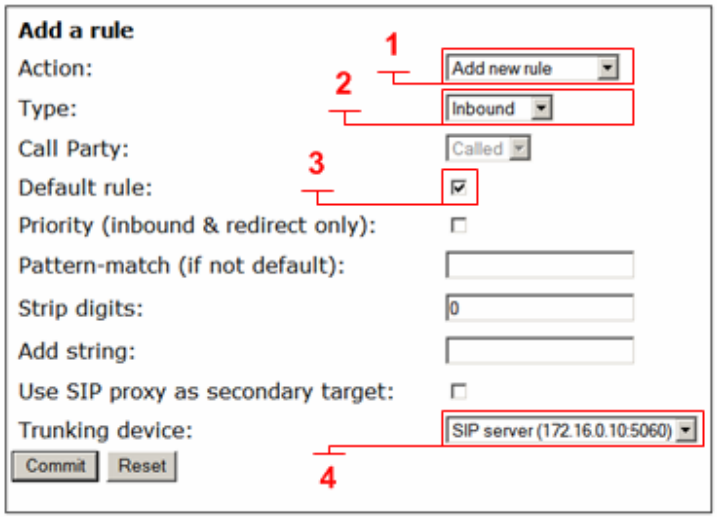
Select “VoIP ALG” -> SIP -> Trunking Dial Rule

1. From the “Action” list, select Add new rule. **(1)**
2. From the “Type” list, select Inbound. **(2)**
3. Select the “Default rule” setting. By selecting the default rule, all calls will be forwarded to the defined trunking device. **(3)**
4. From the “Trunking device” list, select the defined SIP server entry (e.g., SIP server 172.16.0.10:5060). **(4)**
5. Select “Commit” to save changes.

Note: By default, you should select the default rule unless you want to limit the inbound “TO URI’s” that are able to reach your internal SIP server.

TO URI manipulation can also be performed in these rules. These rules are not only for inbound messages. You can also manipulate outbound and/or redirect SIP messages. It’s possible to have a different SIP provider handling your E911 service (e.g., you can add a trunking device and a dial rule for 911).





Optional VBP-E at the Headquarters Location - CMA Settings

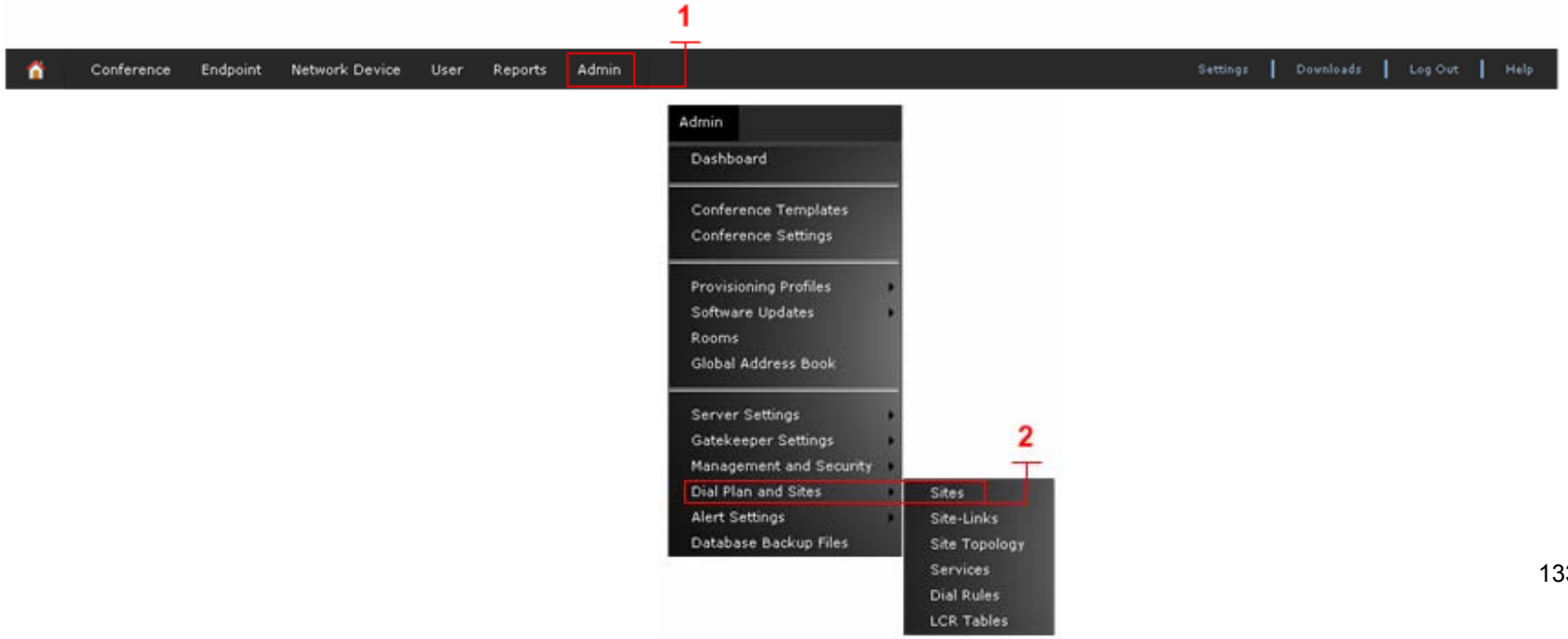
The optional VBP-E configuration requires a CMA task to be completed for internal users to call from the Headquarters location to any publicly reachable H.323 endpoint. When installing the CMA server onto the network, you may have configured more than one site or you may only have one site for your network. CMA site features can be used to manage your network's bandwidth usage which controls the amount of traffic allowed to and from each site location. The sites feature also allows you to configure a default location to send H.323 calls when the destination the user dialed is not on the network. Sites are controlled by source subnets. To define which endpoint belongs to which site, you can create a site that has a single subnet, or you can add multiple subnets to the site.

When installing a VBP-E to provide "offnet" dialing, the CMA needs to have the LAN IP address of the VBP-E configured to send offnet calls to. When configuring your CMA server for sites, you can define one VBP-E per site as the video gateway. This feature allows the admin to control which subnets use a VBP-E to send offnet calls to.

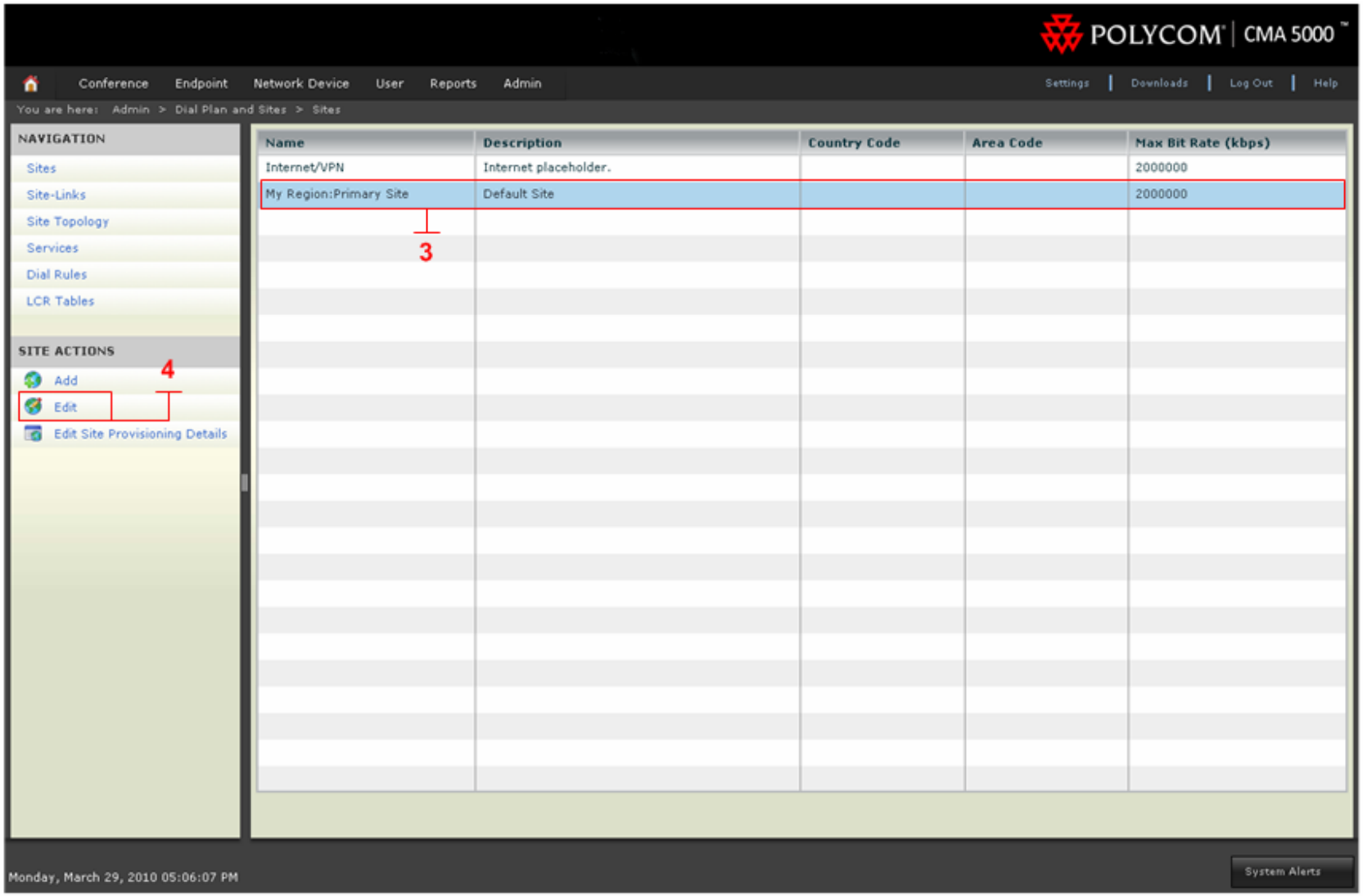
In the following example, one flat subnet (e.g., 172.16.0.0/24) will be used. The following configuration will explain how to define the VBP-E in the CMA server's configuration to provide users with offnet dialing.

Log in to your CMA server as the "admin."

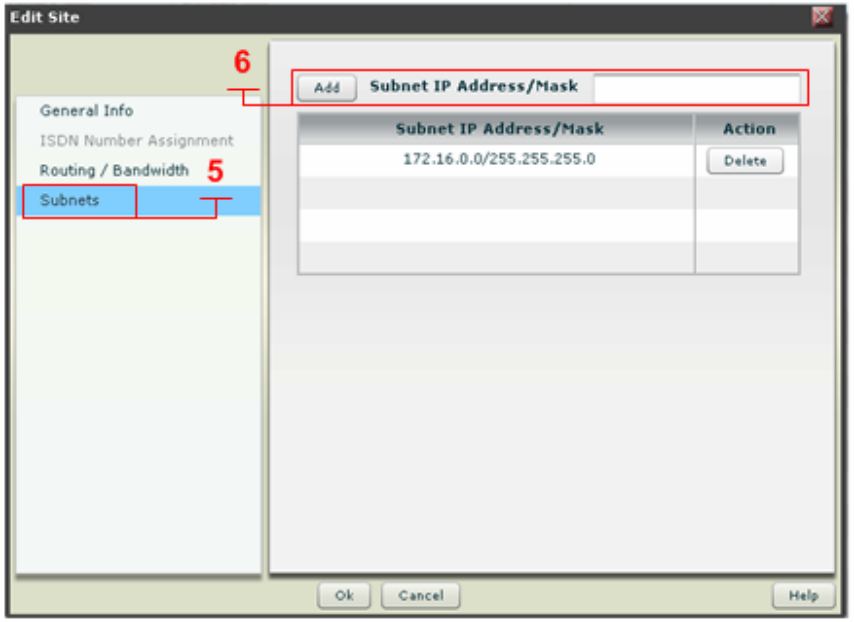
1. On the "Admin" menu **(1)**, point to "Dial Plan and Sites," and then click "Sites." **(2)**

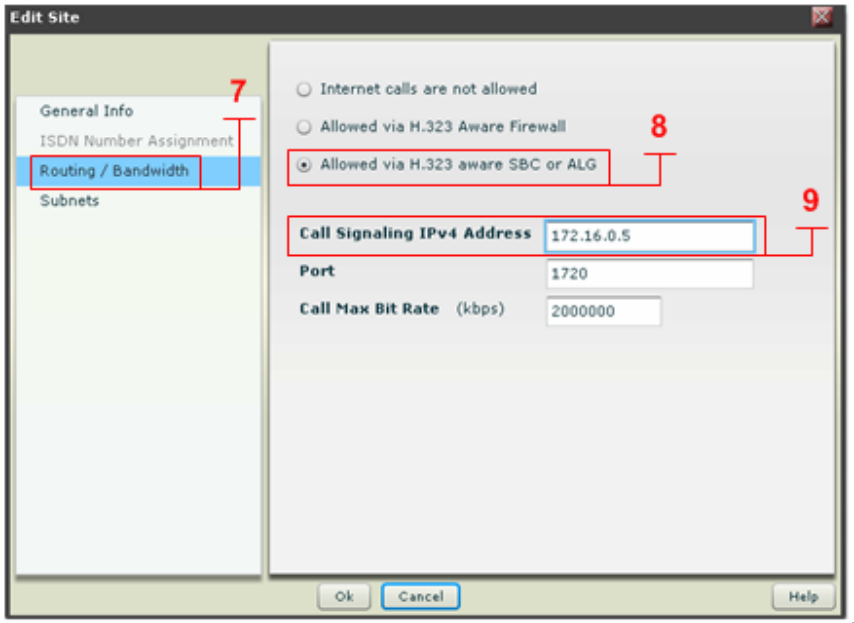


2. Select “My Region:Primary Site.” **(3)**
3. Select “Edit.” **(4)**



4. Select “Subnets.” **(5)**
5. Enter the “Subnet IP Address/Mask” (e.g., 172.16.0.0/255.255.255.0), and then click “Add.” **(6)**
6. Select “Routing/Bandwidth.” **(7)**
7. Enable the “Allowed via H.323 aware SBC or ALG” setting. **(8)**
8. Enter the “Call Signaling IPv4 Address.” This is the LAN IP address of the VBP-E (e.g., 172.16.0.5 is used). **(9)**
9. Verify the “Port” is set to 1720.
10. Select “Ok” to save changes.





You are now ready to start making offnet H.323 calls. There are many management and control features supported by the CMA system. However, this setup is the minimum requirement for configuring the CMA to use the VBP-E to dial public offnet IP endpoints.

From a CMA registered endpoint, you can dial just the IP address of the public IP endpoint, or you can dial an ANNEX O address of another location which has a deployed VBP-E as the perimeter security device. This is known as “user@host or email address URI dialing.”

Using that example, a remote user that is not part of your enterprise who wishes to call the Headquarter’s VVX 1500 D system would dial 8315551501@12.48.260.5

If you follow an email style H.323-ID (e.g., john.smith.work) for the VVX 1500 D system, the remote user would dial john.smith.work@12.48.260.5

You can apply a DNS name to the VBP-E public IP address. The following is a DNS A record example:

A record IN video.yourvbpip.net 12.48.260.5

The remote user would dial john.smith.work@video.yourvbpip.net to reach the VVX 1500 D system.