

Deploying CMA Desktop clients in Disparate Networks



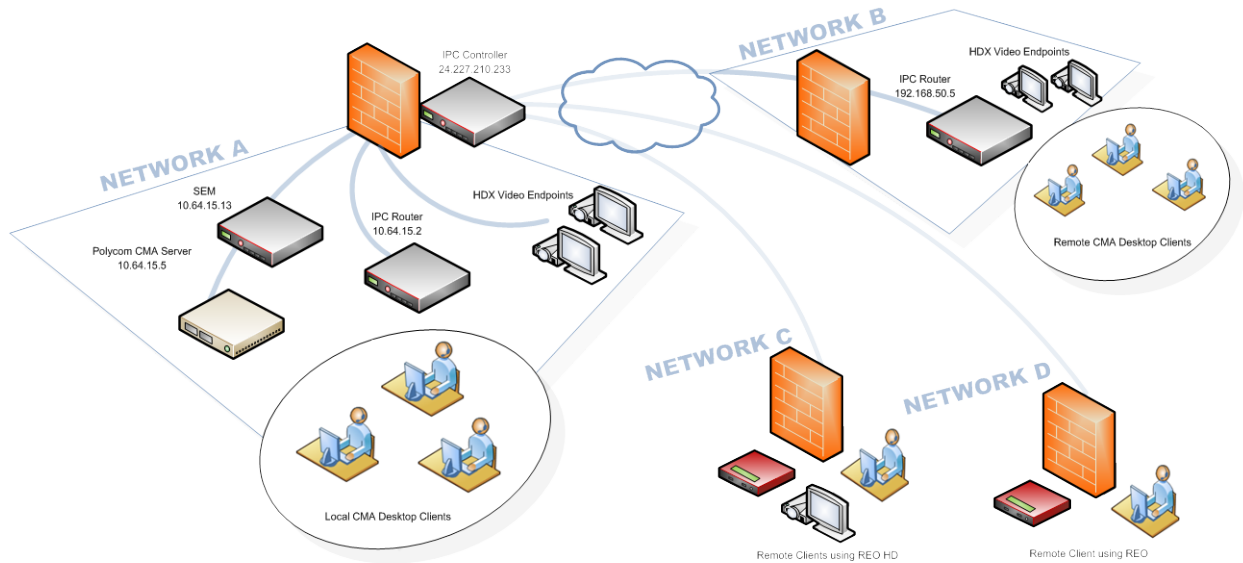
directPacket Product Supplement

About this Supplement

Polycom and Polycom CMA are trademarks of Polycom, Inc.

Intro

This document describes how to configure a directPacket IPC community and Polycom CMA Server to facilitate seamless communication and integration of remote Polycom CMA Desktop clients and provisioned Polycom HDX endpoints.

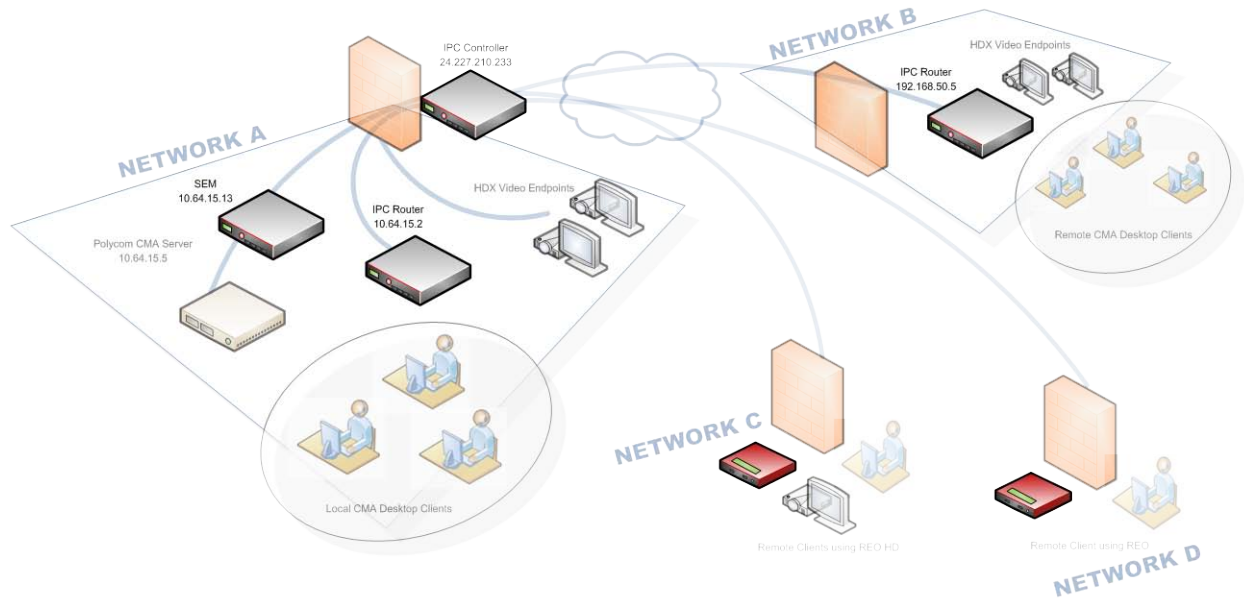


This scenario utilizes the directPacket IPC-R unit as the H.323 gatekeeper. Other scenarios utilizing the CMA server H.323 gatekeeper may be used, but are not covered in this document.

The H.323 dial plan should be defined prior to proceeding. In this example, each network or site with more than one endpoint will have a prefix. Networks with only one endpoint will use a specific E.164 number and/or H.323 ID.

In this example, the Secure Endpoint Manager located in Network A will handle all provisioning data from remote CMA Desktop clients. The H.323 signaling and media for all CMA Desktop clients will be handled by the directPacket IPC community devices.

1 The IPC Community



The IPC Community is made up of a single IPC-Controller (IPC-C), a Secure Endpoint Manager (SEM), one or more IPC-Routers (IPC-R), and/or one or more Remote Executive Office (REO) units. The IPC-C is placed on the external internet cloud while the IPC-R(s) and REO(s) units are placed on internal networks.

Network A is the main network consisting of the following:

- An IPC-Controller on the public internet with a public IP address
- An IPC-Router inside the network acting as a gatekeeper for local H.323 traffic.
- CMA Server.
- Various CMA Desktop clients, and various H.323 Endpoints.

Network B – this is a remote location consisting of the following:

- An IPC-Router communicating with Network A's IPC-Controller, which acts as a gatekeeper for H.323 traffic and as a provisioning server for CMA Desktop clients.
- Various CMA Desktop clients, and various H.323 Endpoints.

Network C – This is a remote client in a hotel, in a home or remote office.

This network consists of a REO HD unit, connecting a CMA Desktop client and a video endpoint.

Network D – This is a remote client in a hotel, in a home or a remote office.

This network consists of a REO unit, connecting either a single CMA Desktop client or a single video endpoint.

2 Establish the STNS Stream

Summary: This section will outline how to establish the STNS stream between directPacket devices.

Checklist:

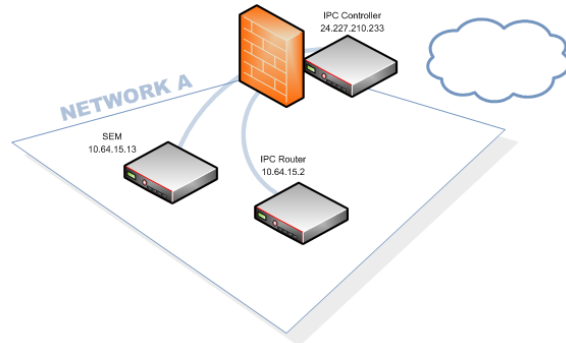
- You need the following directPacket devices:
 - IPC-Controller
 - Secure Endpoint Manager
 - IPC-Router and/or REO units.

Skip this section if you:

Already have an established STNS Community.

What is not covered in this section:

- Network Configuration of the directPacket IPC devices.
- Connecting REO Units to the IPC-Controller.



2.1

Log on to the IPC-Controller.

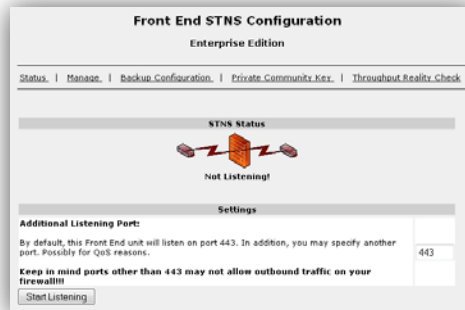
Using the left hand navigation pane, navigate to **Networking - Enterprise Front End**.



2.2

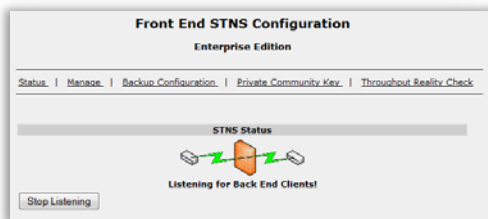
Using the default port **443**, press the **Start Listening** button. The IPC-Controller startup process can take up to two minutes to complete. Watch the browser's progress indicator and do not navigate away from this page.

Once the process is complete, the page will redirect to the status page.



2.3

At this time, the IPC-Controller is listening for IPC-Routers and REO units to connect.



2.4

Next, we will configure the IPC-Router to connect to the IPC-Controller using an STNS stream.

Log into the IPC-Router.

Navigate to **Networking and Enterprise Back End STNS**.

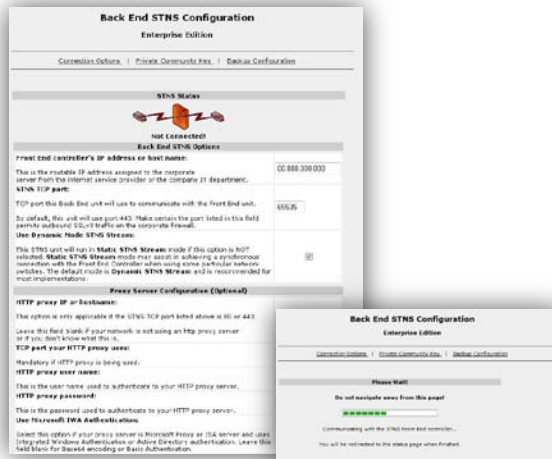


2.5

Enter the IP Address or host name of the IPC Controller.

If you are using a proxy server, enter the address and TCP port of the HTTP proxy server and authentication information if necessary. Otherwise, leave them blank.

Scroll to the bottom of the page and click **Connect**. Watch your browser, and do not navigate away from this page. This process can take up to 120 seconds.



2.6

Once completed, the IPC-Router and IPC-Controller are communicating through the STNS stream.

These steps will need to be performed for any additional IPC-Routers in the local or disparate networks.



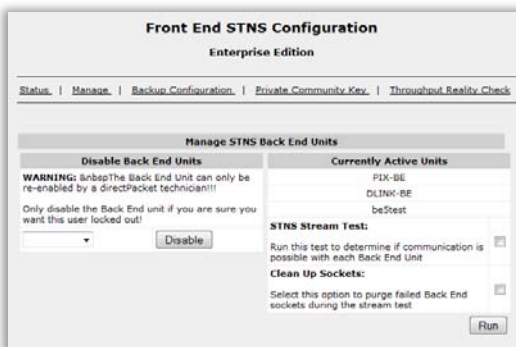
2.7

Next, log into the SEM server and perform the same steps as the IPC-Router to establish the STNS stream to the IPC-controller.

2.8

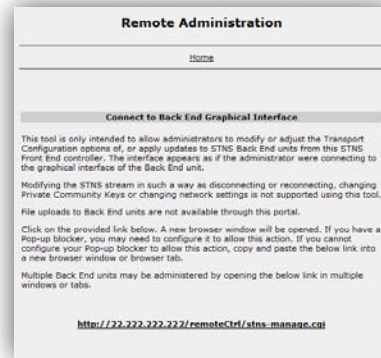
To verify the connections from the IPC-Router and SEM server, log into the IPC-Controller.

Navigate to **Networking – Enterprise Front End STNS and Manage**. Under the Manage section, there will be **Currently Active Units** listed. The IPC-R and SEM units, along with any other REOs or IPC-Rs will be listed here.



2.9

Once the STNS stream is established between the IPC-C and the IPC-R(s) and/or REO unit(s), you can access the **Remote Administration** module under **Networking**. This allows Remote Administration of IPC devices.



3 Configure H.323 Community

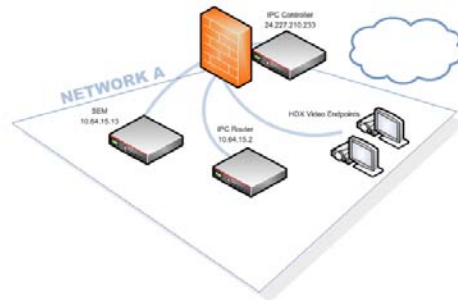
Summary: This section will outline how to establish the H.323 transport between video endpoints and IPC devices.

Checklist:

STNS Stream established between IPC-C and IPC-R or REO Units.
Secure Endpoint Manager
IPC-Router and/or REO units.

Skip this section if you:

Already have an established STNS Community.
Already using the IPC-Routers as a gatekeeper for H.323 registrations.
Already have a dial plan configured in the STNS community.



3.1

Log into the IPC-Controller.

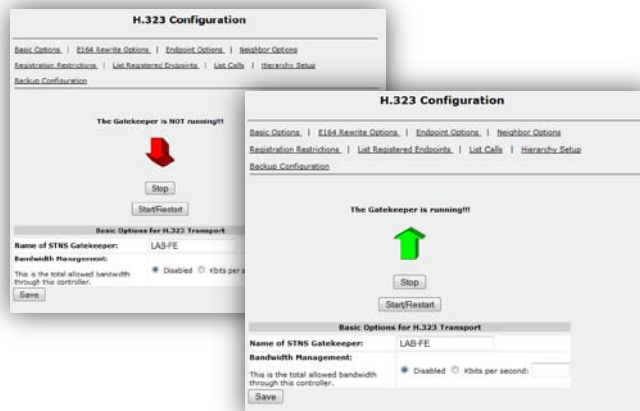
In the left hand navigation pane, choose: **Transport Configuration** and then **H.323 Configuration**.



3.2

Change the Gatekeeper to a unique name. For example: FEGate1, FrontEndGK1, FEK1

Click **Start/Restart**.



3.3

Next, log into the IPC-Router.

In the left hand navigation pane, choose: **Transport Configuration** and then **H.323 Configuration**.

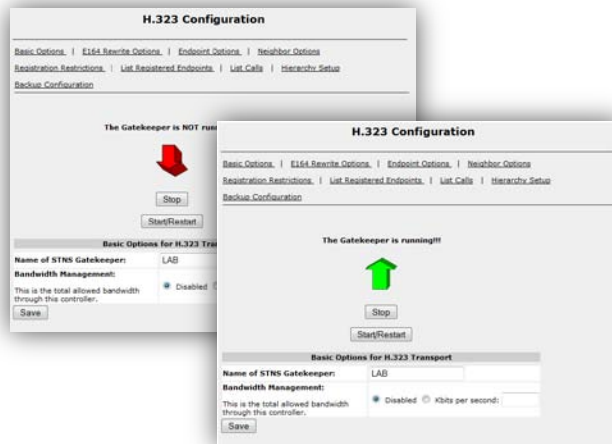
Change the Gatekeeper to a unique name. For example: FEGate1, FrontEndGK1, FEGK1

Click **Start/Restart**.



3.4

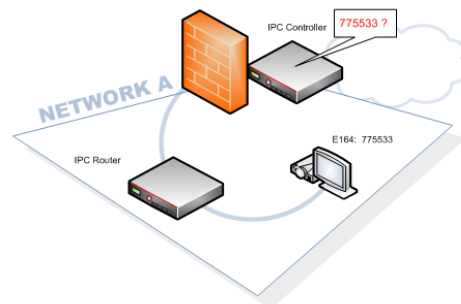
Navigate to **Transport Configuration, H.323 Configuration**. Click on **Save**, then **Start/Restart Gatekeeper**. At this point, the gatekeeper will restart and the endpoints will register to the IPC-Router.



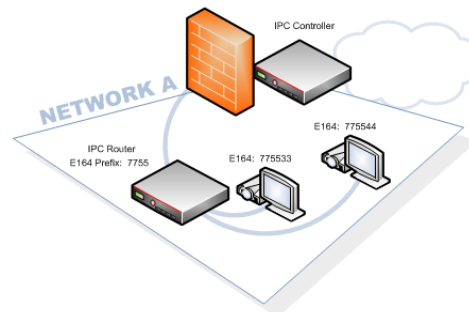
3.5

The gatekeepers are now running on the directPacket IPC-C and the IPC-R(s). The IPC-Controller needs to know how to route calls to the appropriate network by means of the IPC-Router. This is performed through hierarchy.

In hierarchy, the IPC-R will tell the IPC-C which endpoints or prefix it manages.



When an IPC-R has a prefix, the IPC-C will send any calls beginning with that prefix to the corresponding IPC-R.

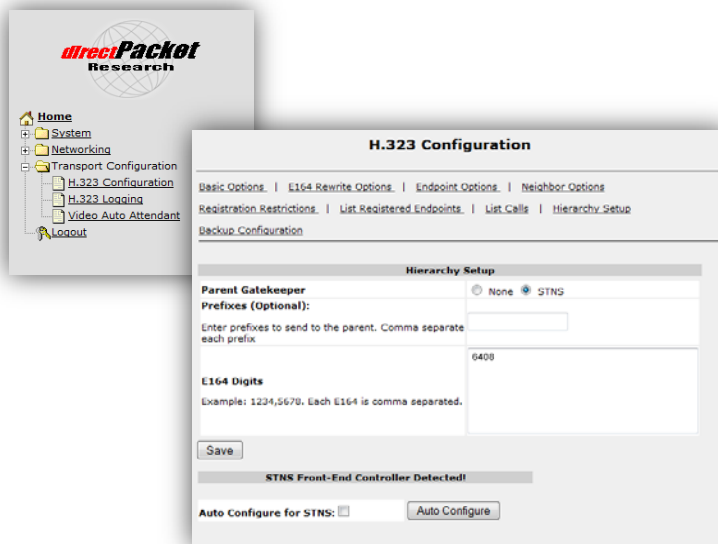


To configure hierarchy and add prefixes, log into the IPC-R. Navigate to **Transport Configuration – H.323 Configuration** and then **Hierarchy Setup**.

Place a checkmark in the **Auto Configure for STNS** and click **Auto Configure**. The E164's for all registered endpoints will show up in the E164 digits field. Remove any E164 which you do NOT wish to traverse the firewall.

You will also want to add any prefixes for endpoints and CMA Desktop clients connecting through this IPC-Router.

Prefixes can be added at this time if desired. Click **Save** and then **Start/Restart Gatekeeper**.



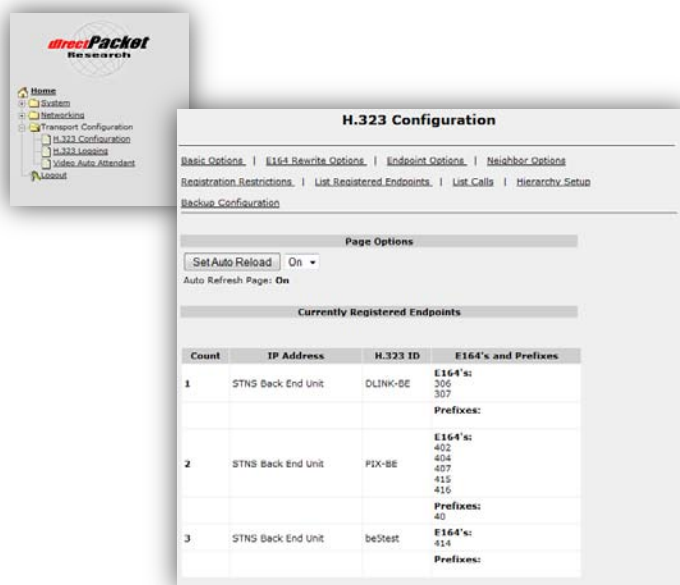
3.6

Next, perform the same steps with each IPC-Router in local and disparate networks.

3.7

Next, verify your endpoints by navigating to **Transport Configuration, H.323 Configuration, and List Endpoints**.

Verify the endpoints on the IPC-Controller. Each endpoint will be registered under the associated IPC-Router.



4 Configure Endpoint Management

Summary: Configure master SEM unit and Endpoint Management modules.

Checklist:

You need the following directPacket devices:

- IPC-Controller
- Secure Endpoint Manager
- IPC-Router and/or REO units.

Skip this section if you:

Already have an established STNS Community with a fully configured SEM

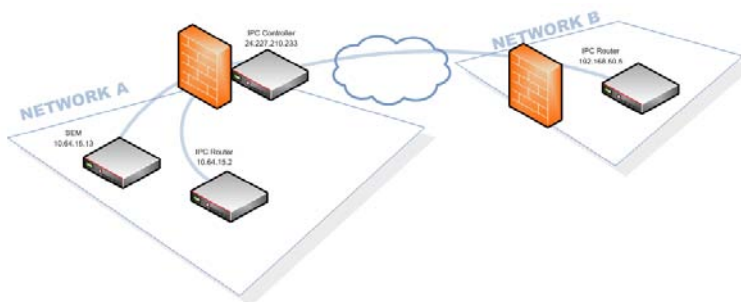
What this section does not cover:

This section does not cover IP configuration of SEM, nor any remote administration functions of SEM.

4.1

First, we will configure the remote IPC-Routers. In the given example, this will be Network B.

Perform the following steps for each of the IPC-Routers and REO units in your STNS community.

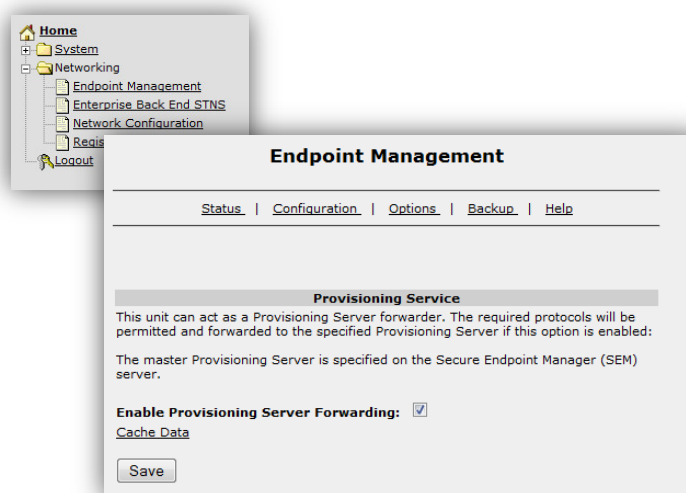


4.2

Log into the remote IPC-Router.

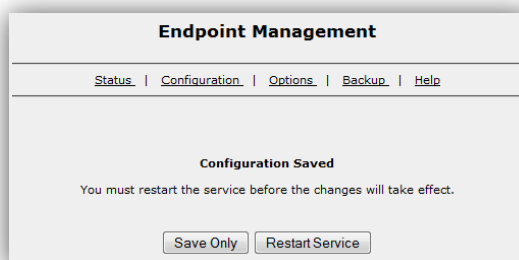
Navigate to Networking – Endpoint Management. Select Options. Place a checkmark in **enable Provisioning Server Forwarding**, and click **Save**.

Configure Endpoint Management on Each respective unit- order Start with remote IPC-R's/REOs Enable provisioning forwarding. Perform inventory on IPC-C



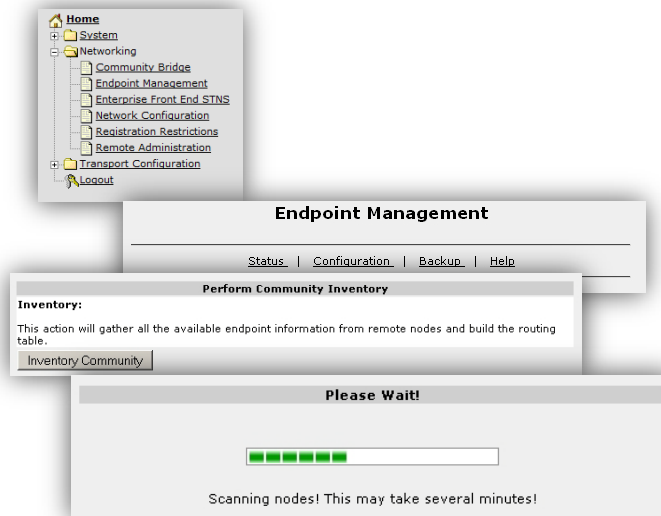
4.3

Next, you will be prompted to Save or Restart the Service. Click **Restart the Service**.



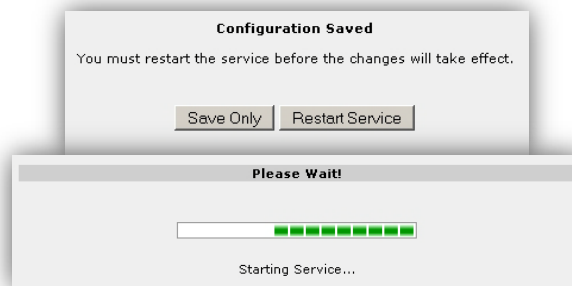
4.4

Log onto the IPC-Controller, under **Networking, Endpoint Management, and Configuration**, click **Inventory Community**. Once completed, the endpoints will need to be allocated in SEM, and the service will need to be restarted.



4.5

Once scanning is completed. You will be prompted to restart the service. Click **Restart Service**. Only the endpoint management service will be restarted.



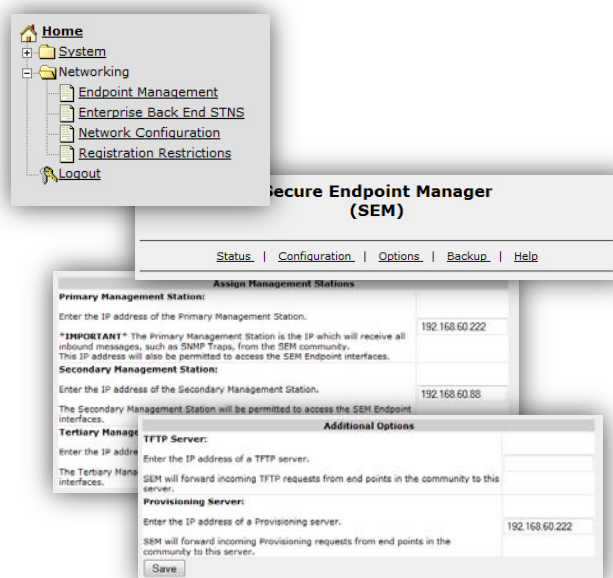
4.6

Next, log into the SEM server. Navigate to **Networking - Endpoint Management - Options**.

Enter the IP Address of the CMA Server under the **Primary Management Station**.

At the bottom of the page, add in the CMA Server's IP address as the **Provisioning Server**.

Click **Save**. Click **Restart Service**.

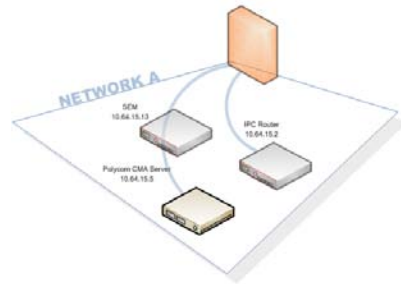


5 Configure CMA Server

Summary: Configuring the CMA Server

Checklist:

- Established STNS Stream
- H.323 gatekeeper running on IPC-Router(s) and/or REO unit(s).
- Secure Endpoint Manager configured.



5.1

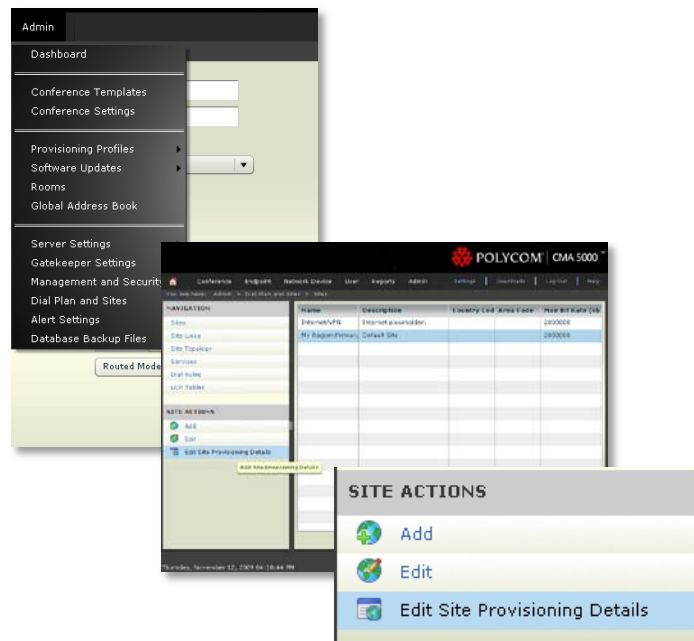
Each of the following steps must be done in the order specified in this manual.

Log into the CMA Server. Under **Admin – Gatekeeper Settings – Primary Gatekeeper**, uncheck **default Gatekeeper**.



5.2

Under **Admin – Dial Plan and Sites – Sites**, highlight **My Region:Primary Site**. In the left menu, click **Edit Site Provisioning Details**.



5.3

Under the **Site Provisioning Details**, the **H.323** settings needs to be changed to use gatekeepers **specify** Gatekeeper IP address which is the nearest directPacket IPC-R's IP.

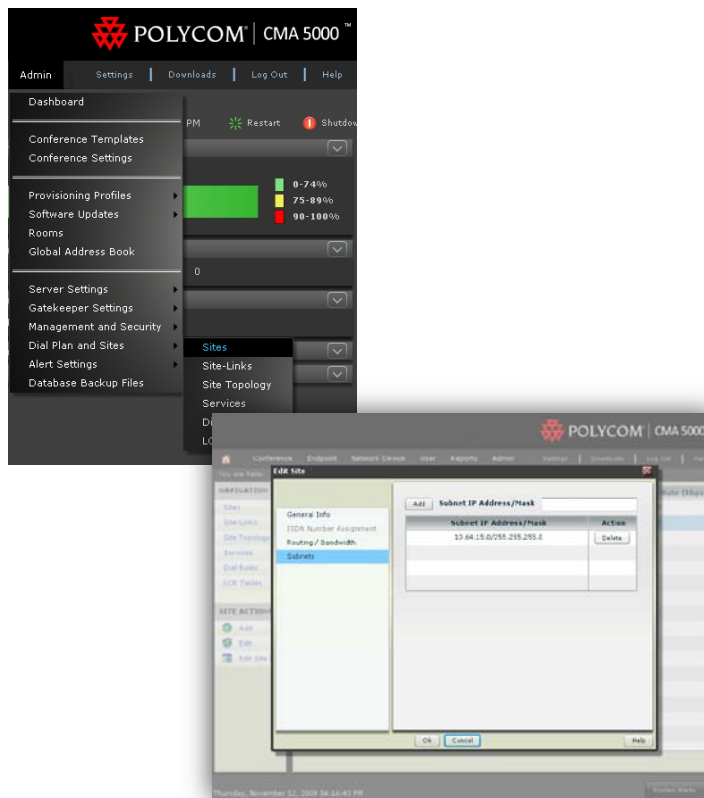


5.4

Next, under **Admin – Dial Plan and Sites – Sites**, highlight **My Region:Primary Site**.

Select **Subnets** and add a Subnet for the LAN.

For example: 192.168.5.0/26



6 Configure CMA Desktop

Summary:

Connecting CMA desktop clients to the CMA server in local and disparate networks.

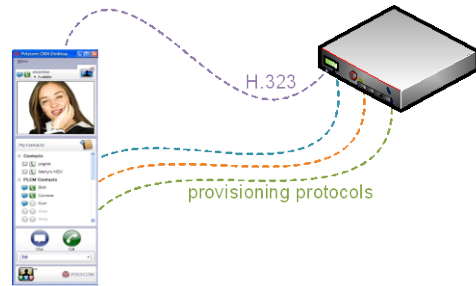
Checklist:

Established STNS Stream

H.323 Gatekeeper running on IPC-Router(s) and/or REO units.

Secure Endpoint Manager configured.

CMA Server configured for STNS community



In remote locations, each CMA Desktop client will use the IPC-R as a provisioning server to communicate with the CMA Server.

On the workstation, open up the CMA desktop and click on **Menu** and **Sign In**. There are provisioning server options for Automatic or Specify.

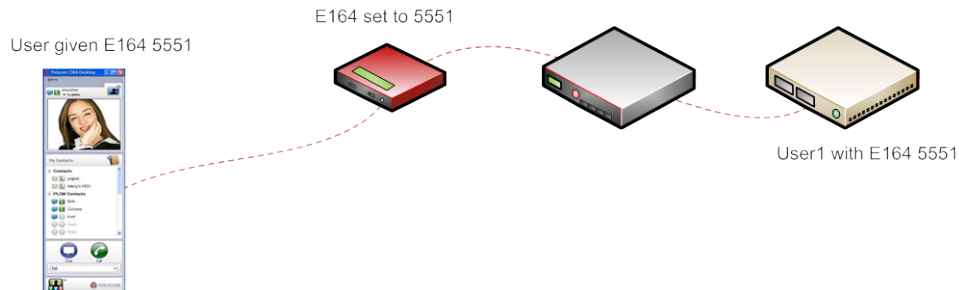
CMA Desktop on same subnet: automatic or manual configuration can be performed to specify the CMA server as the provisioning server.

CMA Desktop on disparate network: If a CMA desktop client is not in the same subnet, or in a disparate network, the provisioning server will need to be specified to use the directPacket IPC-R or REO unit.



7 REO & IPC-R Configurations

REO: When setting up the REO unit through the REO Wizard, verify the E164 is the same as the number provided through CMA Administration.



IPC-R: The E164 must be provided in CMA Server, and prefixes must be specified in the dial plan. Hierarchy must be run to be properly routed from the IPC-Controller. See the IPC Platform Setup & Reference manual for more information on community setup.

8 Endpoint Configuration with CMA

Each endpoint will need to be connected to a gatekeeper. In remote locations, endpoints will use the gatekeeper within a directPacket IPC-R which will also facilitate communications to the CMA server.

9 Troubleshooting

Message: “Checking connection to server.”

Message: “Unable to connect to server. Retrying...”

These messages illustrate the inability for the provisioning protocols to reach the CMA server. On the IPC-Router or REO unit, verify provisioning server is enabled under Endpoint Management and restart the Endpoint Management service. On the IPC-Controller, run inventory under Endpoint Management and restart the Endpoint Management service

If you are still unable to log in, contact a Direct Packet technician.

Not able to receive video calls.

Verify the E164 is set correctly in the CMA server.

Run hierarchy on the IPC-Router. This will tell the IPC-Controller where the endpoints or CMA Desktop is and how to route calls appropriately.

If you are connected through a REO, re-run the setup wizard.