NN10367-111

Carrier Voice over IP

Communication Server 2000

RTP Media Portal Basics

(I)SN08 Preliminary 03.01 March 2005

NORTEL

Overview

How this chapter is organized

This chapter is organized as follows:

Functional description

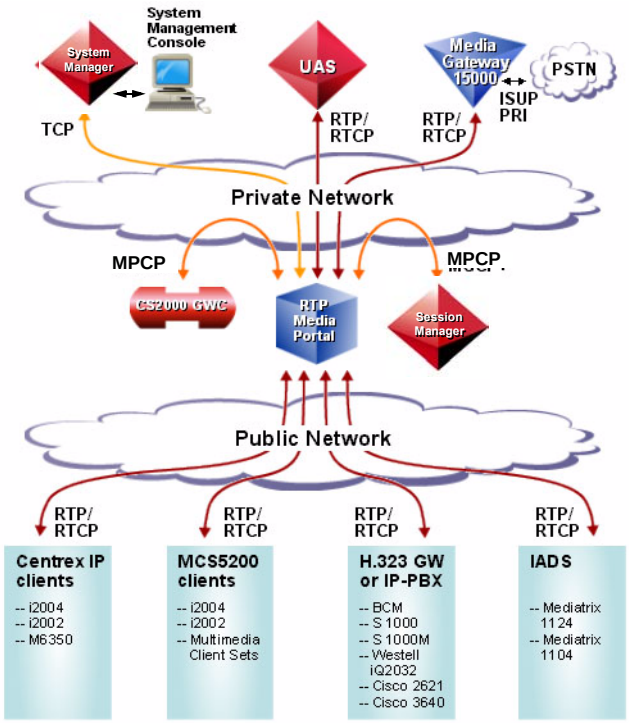
The Real-time Transport Protocol (RTP) Media Portal is an optional component that addresses media plane specific issues with advanced service delivery, Internet addressing efficiencies, and system security.

The primary function of the RTP Media Portal is to extend the reach of multimedia services so that they are accessible to obscured endpoints, devices residing behind a firewall, or a Network Address Translation (NAT) and/or Network Address Port Translation (NAPT) device.

The RTP Media Portal provides IP address/port pair mapping between internal and external network components, and media anchoring and media pivot abilities for terminals. For NAPT functionality, the Media Portal relays packets between two end points located in different networks using the same or different IP address spaces. The RTP Media Portal can perform NAPT on both the source and destination IP addresses for every media packet authorized to traverse.

Figure 1, Network Component Interoperability, on page 4 is a graphical depiction of the RTP Media Portal's position in a CS 2000 solution.

Figure 1 Network Component Interoperability



In this figure, the clouds represent two distinct networks. The private network cloud interacts with the public network cloud through the different edge components. The RTP Media Portal provides media-layer functionality for Real Time Transport Control Protocol (RTCP), and User Datagram Protocol (UDP) transmissions.

A call control signaling channel is established between the H.323 gateway and the CS 2000. If the GW and the CS 2000 reside in separate IP-VPNs (different IP address domains that cannot route directly to one another) dynamic discovery and keep alive are supported on the gateways and GWCs to provide another mechanism for GW->CS2K communication. Discovery provides another mechanize for GW->CS2K communication.

Hardware

The RTP Media Portal resides on a Motorola* CPX8216T platform, a 16-slot CompactPCI (cPCI) chassis design.

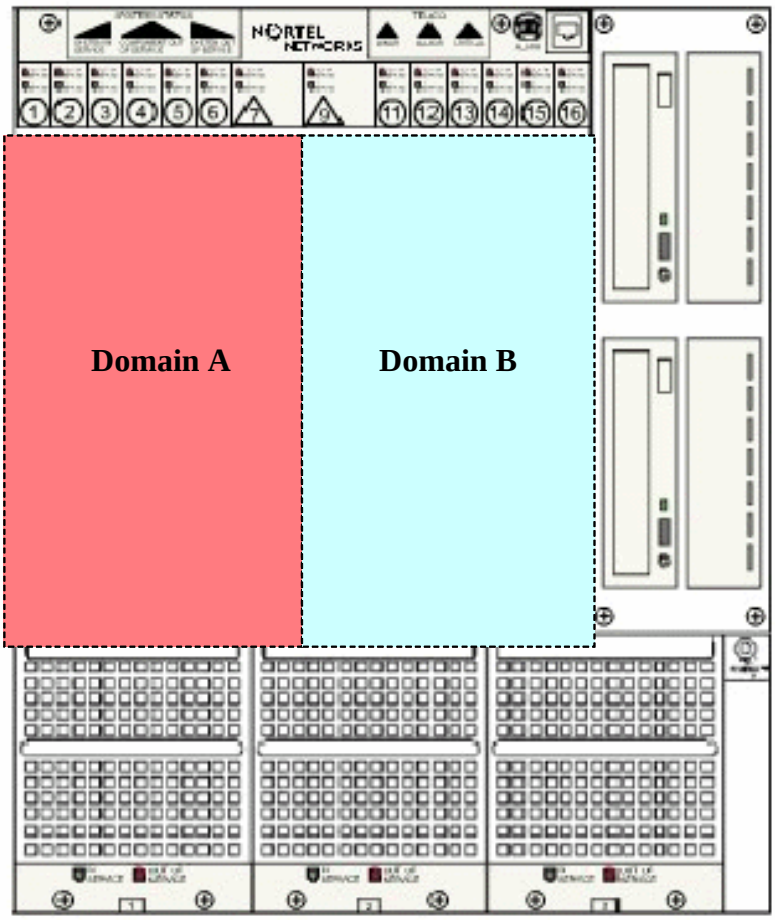
The chassis offers a High Availability platform that provides the basic operating environment (such as power, backplane, cooling, and mounting slots) required to sustain the resident subcomponent single-board computers. The CPX8216T hardware architecture

partitions the chassis into separate logical operational Domains, dividing the chassis shelf into two half-shelves consisting of 8-slots each.

Note: The chassis logical Domains are not internet Domains. Rather, the term is used to identify Side A and Side B of the chassis. Other terms used interchangeably include: Domain A and Domain B, Left Domain and Right Domain, and half-shelf.

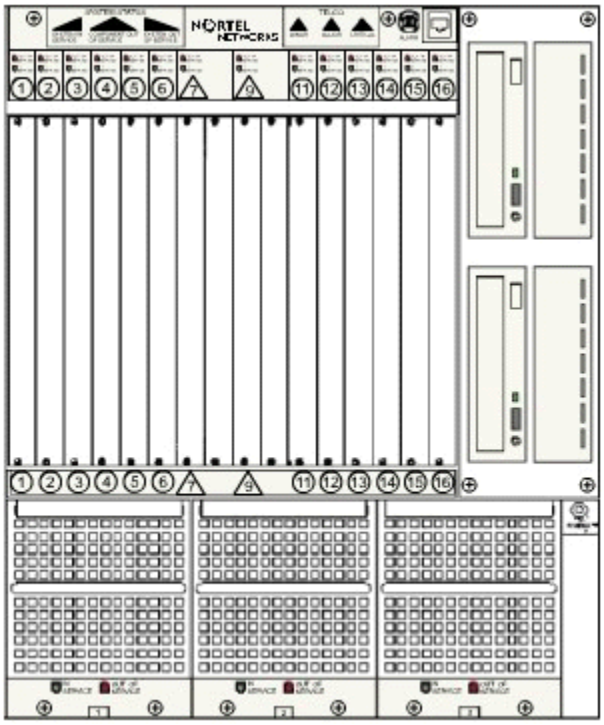
An RTP Media Portal occupies a single logical operational Domain in the CPX8216T. A single CPX8216T chassis can host two RTP Media Portal components (one in chassis Domain A, the other in chassis Domain B) as shown in Figure 2, Card slot associations for the two logical Domains in a single chassis, on page 5.

Figure 2 Card slot associations for the two logical Domains in a single chassis



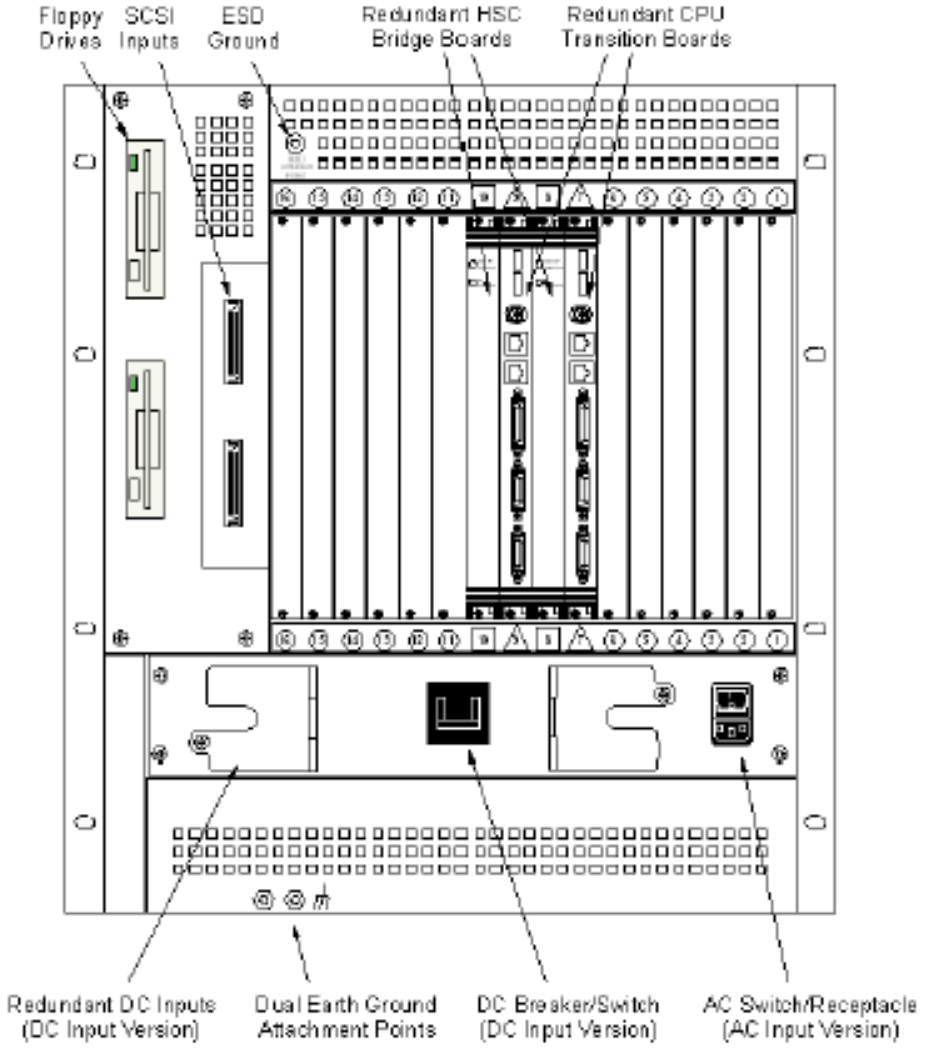
If the chassis is viewed from the front, the slots are numbered from left to right (1-16). If viewed from the rear, the slots are numbered from right to left (1-16). A front view of the CPX8216T is shown in Figure 3, Motorola chassis CPX8216T - front view, on page 6.

Figure 3 Motorola chassis CPX8216T - front view



A rear view of the CPX8216T is shown in Figure 4, Motorola chassis CPX8216T - back view, on page 7.

Figure 4 Motorola chassis CPX8216T - back view



Within the CPX8216T dual 8-slot architecture, each logical Domain in the chassis contains a dedicated host card (with an associated transition module in the rear), a slot dedicated to the Motorola Hot Swap Controller (HSC), and the remaining six slots which may be populated with Media Blades (media input/output cards with an associated transition module in the rear).

The Hot Swap Controller in the Left Domain controls the Right Domain. The Hot Swap Controller in the Right Domain controls the Left Domain.

Each logical Domain, and therefore each RTP Media Portal, consists of the following hardware components:

- a single CPV5370 Intel processor board (the host card) with 1 GB memory, a SCSI input/output (I/O) daughter board, and rear Transition Module.
- Hot Swap Controller and Bridge (HSC) module
- SCSI CD-ROM drive
- SCSI hard drive
- Floppy drive
- One (or more) Motorola MCPN765 Power PC processor board (the Media Blade), with 64 MB RAM and associated Rear Transition Module.
- Available AC or DC power options

Customer provided requirements include:

- Mouse
- Keyboard
- Monitor

Software

The RTP Media Portal is primarily a software entity that is comprised of subcomponents distributed across the hardware platform.

The RTP Media Portal, servers and components must be configured and provisioned under the same site as the management server, even if deployed from a remote location. Failure to deploy the RTP Media Portal under the same site as the management server will prevent OMs, logs, and alarms form being managed from the System Management Console.

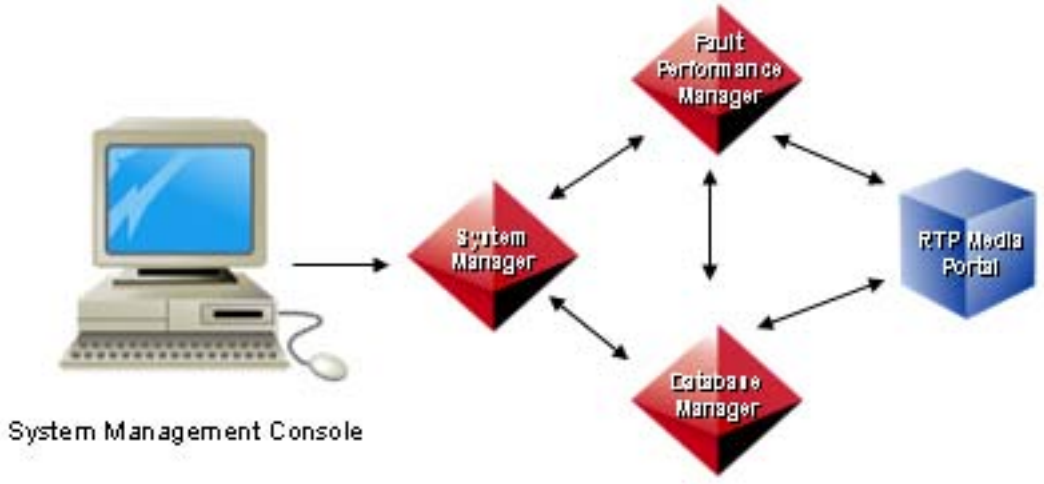
For information regarding maintenance updates, refer to Maintenance updates on page 17. For information regarding the upgrading of RTP Media Portal software releases, refer to SN07 to SN08 RTP Media Portal upgrade procedures on page 64.

Operations, administration, and management

Operations, administration, and management (OAM) access to the RTP Media Portal is available through the System Management Console. This console provides an overall view into the status of the various components in the system, and administrative access to OAM functions (including fault and configuration management).

RTP Media Portal OAM data is stored on the System Manager, Fault Performance Manager, and the Database Manager. The System Manager stores alarm and log data. Configuration data is stored locally on the RTP Media Portal as well as persistently in the database. For a graphical view of these relationships, please refer to Figure 5, OAM interoperability, on page 9.

Figure 5 OAM interoperability



For additional information, please refer to *Carrier Voice over IP System Management Console User Guide*.

Interfaces

Protocols

While in service, the RTP Media Portal interfaces with other components in the system using the following protocols:

- **MPCP,** Media Portal Control Protocol, controls messages between the Session Manager and the RTP Media Portal. MPCP messages control the making, modification, and breaking of media session

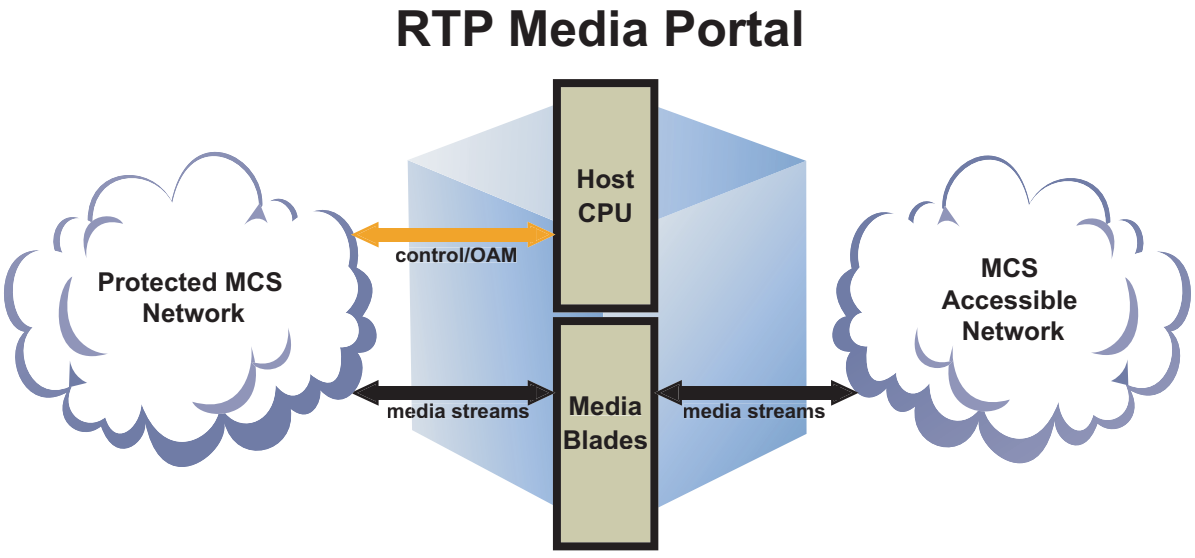
connections. Refer to Carrier Hosted Services Basics (NN10234-100) for call flow information.

- **RTP**, Real-time Transport Protocol, transports real-time media streams (for example, audio and video) across a packet network.
- **RTCP**, -time Transport Control Protocol (RTCP) that provides an exchange of information pertaining to the quality of an associated media session (e.g. packet counts, packets lost, latency, jitter).
- **UDP**, User Datagram Protocol, transports data-based media streams (for example, file transfer).
- **TCP**, Transmission Control Protocol, communicates configuration, performance data, logs, and alarms (OAM data) between the RTP Media Portal and the Management System.

Network interfaces

The RTP Media Portal is comprised of two physical hardware subcomponents: a single Host CPU, and up to six (6) Media Blades.

Figure 6 RTP Media Portal operational interface - dual-network deployment



The Host CPU interacts with the management infrastructure to provide OAM capabilities. The Host CPU also provides the control capabilities (MPCP) through which a call controller Session Manager can access, manipulate, and apply advanced functions to media streams.

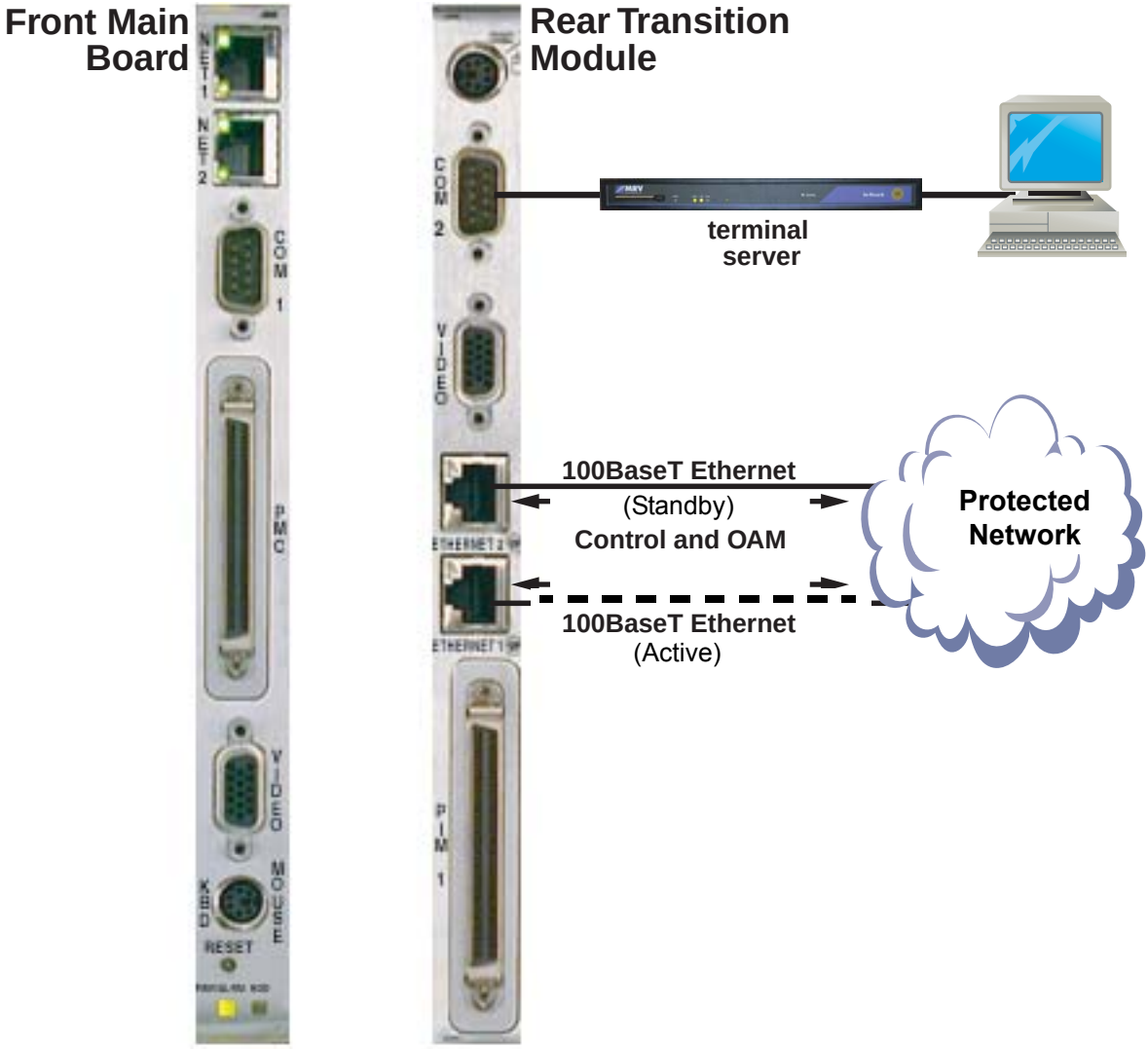
The Media Blades provide the Media Packet Engine for processing media streams.

Host CPU

The Host CPU in the RTP Media Portal consists of the CPV5370 (Front Main Board) and the CPTM-04 Transition Module. There is a 1:1 relationship between the Front Card and the Rear Transition Module. As shown in Figure 7, Control and OAM interface - CPV5370 Host card and RTP Media Portal, on page 12, the Rear Transition Module for the host card (CPV5370) provides the following:

- COM2 port for connection to a terminal server and local monitor.
- Two Ethernet ports which provide connectivity to the Protected Network. The connection carries control and OAM data.
  - The Ethernet 1 port is used to provide an active connection.
  - The Ethernet 2 port provides a standby connection. The standby ethernet function is enabled at installation.

Figure 7 Control and OAM interface - CPV5370 Host card and RTP Media Portal



These Ethernet connections carry the following:

- MPCP control messages to communicate with the Communication Server 2000.
- Operations, administration, and maintenance (OAM) data to the System Manager.
- Internal communications between Host and Media Blades.

Media blades

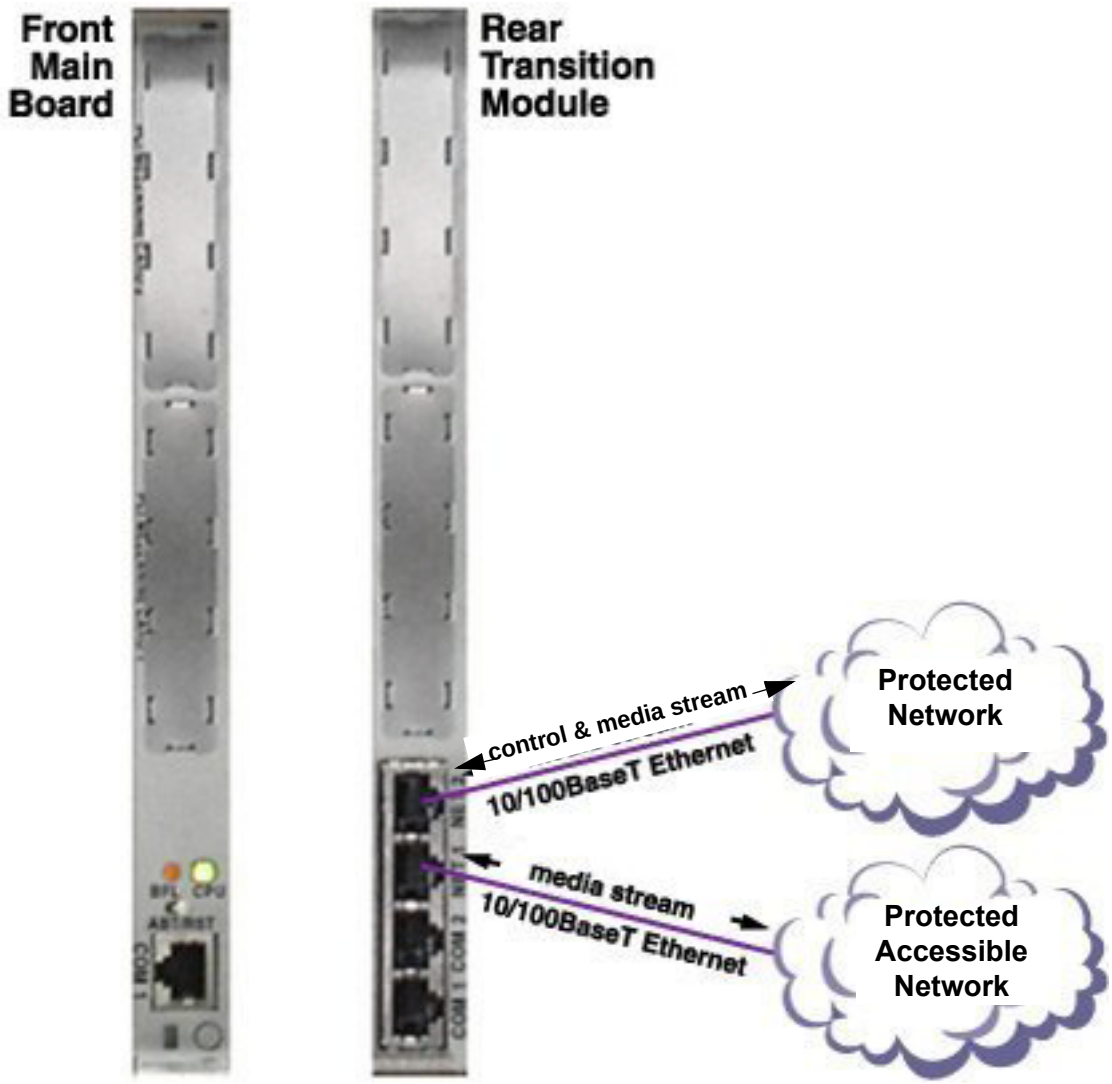
A Media Blade in the RTP Media Portal consists of the following input/output cards:

- MCPN765 Front Main Board
- TM-PIMC-0101 Rear Transition Module

There is a 1:1 relationship between the Front Card and Rear Transition Module.

Network interfaces on each of the Media Blade Transition Modules in the RTP Media Portal provide a path for media streams. Figure 8, Media stream interface - MCPN765 Media Blade to RTP Media Portal, on page 14 illustrates media stream interfaces in a dual-network deployment between a Protected Network and MCS Accessible Network.

Figure 8 Media stream interface - MCPN765 Media Blade to RTP Media Portal



The Rear Transition Module contains two, 10/100 BaseT Ethernet connections for RTP/RTCP/UDP media streams. Each Media Blade (pair of MCPN765 and TM-PIMC-0101 cards) performs the following functions:

- Connectivity for RTP/RTCP/UDP media streams.
- Address and Port Discovery (APD) for obscured media endpoints.

- Relay of media packets between end points.
- An array of NAT and/or NAPT functions.
- Internal communications between Host and Media Blades.

The NET ports are used as following:

- In a single-network deployment, only the NET2 port is used.
- In dual-network deployment, NET2 is used for connectivity to the Protected Network and NET1 for the other network.

Maintenance updates

How this chapter is organized

This chapter is organized as follows:

Functional description

This chapter documents upgrade tasks to be performed when updating a maintenance release.

Tools and utilities

Updates to the RTP Media Portal are performed through the System Management Console. Please refer to *Carrier Voice over IP System Management Console User Guide* for more information.

Operations, administration, and management

The Communication Server 2000 may try to contact the RTP Media Portal while the update is in progress, potentially generating error logs. To eliminate this potential and minimize impact to service, the RTP Media Portal should first be shut down so that it does not accept new service requests. While shutting down, the RTP Media Portal will continue to process established media sessions. These pre-existing media sessions are cleared as the associated calls end. The RTP Media Portal will automatically transition from the active into the inactive state when there are no longer any active media sessions

present. When this state transition occurs, it is safe to proceed with the update without affecting service.

CAUTION

It is possible to update and reboot one RTP Media Portal in a chassis, while the RTP Media Portal in the other half of the chassis continues to run the previous software. Once one RTP Media Portal is updated, the other RTP Media Portal in the chassis can be shut down, updated, and rebooted. This rolling update will only impact available capacity and will not cause a service outage.

Updating all RTP Media Portals concurrently will cause a service outage.

If an update fails during the initial stages, an automatic rollback to the previous load is performed. A notification of the failure appears within the System Management Console.

If a component update fails after the initial stages of the update, it does not rollback automatically. A dialog box appears in the Management Console stating that the update failed and prompts the administrator to determine whether a rollback should be performed. When the update passes, the RTP Media Portal can be started again by the administrator.

Maintenance update tasks

Update operations are issued to the RTP Media Portal from the System Management Console. The final stage of update causes a reboot of all Media Blades. When the update operation is complete on the RTP Media Portal, it can be brought back in service (active) with the updated software by the administrator.

To avoid any conflicts with service requests from the Communication Server 2000, the following procedure describes the steps that must be followed when updating a software load for the RTP Media Portal component.

From the System Management Console

1 Shut down the RTP Media Portal component. For details, please refer to Shutting down the RTP Media Portal component on page 19.

2 Update the software load for the RTP Media Portal component. For details, please refer to Deploying the RTP Media Portal component on page 21.

3 Start the new load. For more information, refer to Starting the RTP Media Portal on page 22.

Shutting down the RTP Media Portal component

The following procedure describes how to shut down the RTP Media Portal component. To perform this procedure, the administrator must login to the System Management Console. For detailed procedures on logging into the System Management Console, please refer to *Carrier Voice over IP System Management Console User Guide*.

From the System Management Console

1 From the System tree, click on the plus sign next to **Network Elements** to expand the view of the folder.

Figure 1 Expanding RTP Portal windows

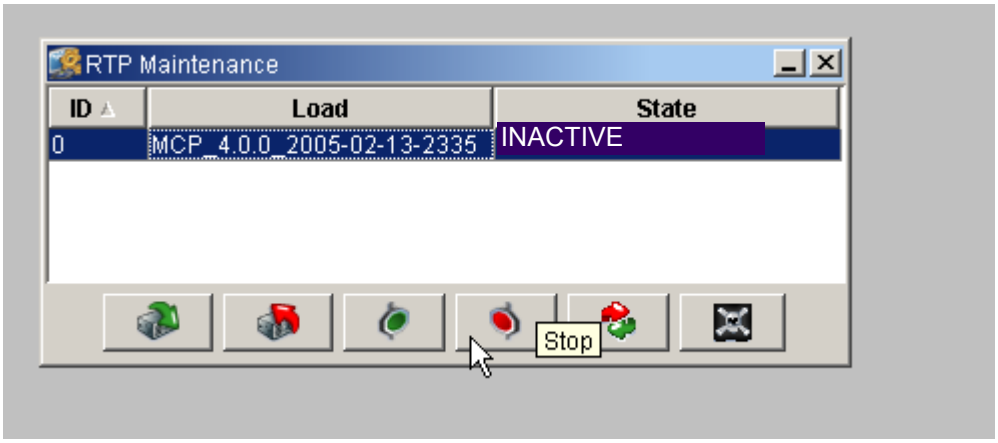
2 Next, click on the plus sign next to **RTP Portals** to expand the view of the folder. The contents of this folder lists all RTP Media Portals configured for the site.

3 Continue to expand the view of folders until the target Portal is selected.

4 Click on the **NE Maintenance** option**.** A new window opens.

5 Select the load to update, and click on the **Stop** button to initiate shut down.

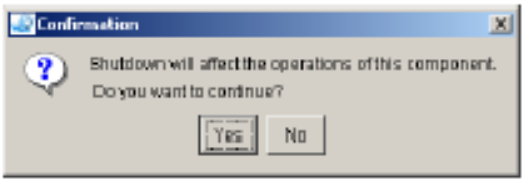
Figure 2 RTP Portal Shut down



Note: The Stop button shuts down the system. The Kill button locks the RTP Media Portal, and the Restart button stops and starts the system.

6 A confirmation window appears. Click on the **Yes** button to continue.

Figure 3 RTP Portal Shut down confirmation



7 The RTP Media Portal component shuts down gracefully and eventually goes into an inactive state when the last active media session ends (as seen in the General Information Area of the System Management Console).

Deploying the RTP Media Portal component

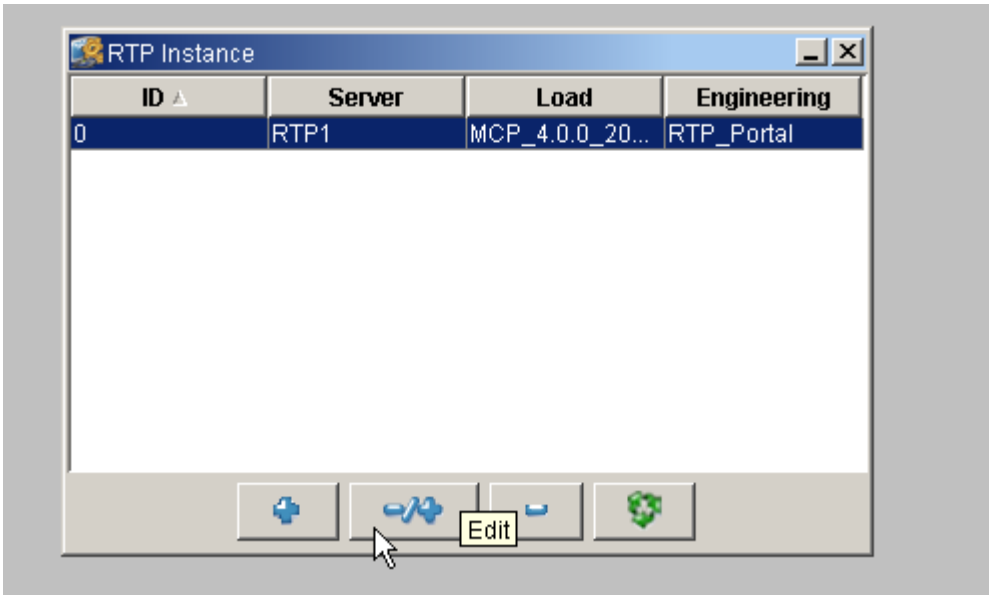
The following procedure describes how to update a load for the RTP Media Portal component.

From the System Management Console

1 From the System tree, click on the **Instance** option. A new window opens.

2 Select the Server, and click on the **Edit** button. You may update the ID, server, load and engineering fields.

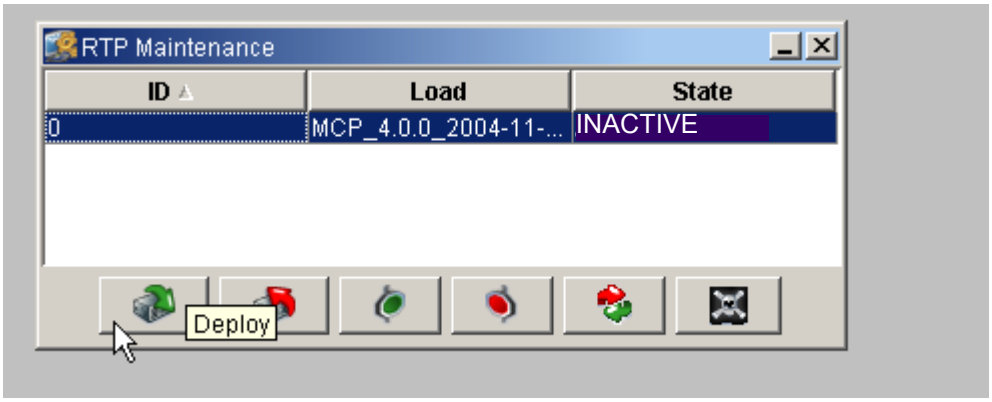
Figure 4 Edit Instance variables



3 Click on the **NE Maintenance** option.

4 Highlight the Portal and click on the **Deploy** button.

Figure 5 Deploying the RTP Portal



5 A window showing the progress of the update appears.

Starting the RTP Media Portal

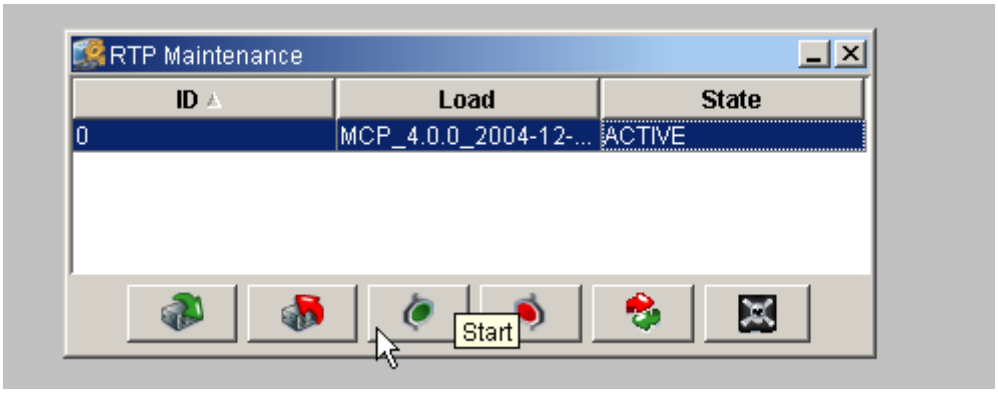
The following procedure lists the steps necessary to start the RTP Media Portal.

From the System Management Console

1 Once the update has completed, the state changes to active.

2 Click on the **Start** button to cause the RPT Media Portal to run the new load.

Figure 6 Start the Portal



Fault management

How this chapter is organized

This chapter is organized as follows:

Network fault management

The system handles network fault management through the reporting of alarms and logs to the Fault Performance Manager. RTP Media Portal alarms and logs are viewed from the System Management Console. For further details related to alarms, please refer to *Carrier Voice over IP Fault Management*: *Alarm and Log Reference*.

Fault tolerance

The RTP Media Portal provides base capabilities that significantly improve the performance and reliability of the system in the event of a fault. These capabilities include:

- Dynamic Pool Registration
  - provides a basic mechanism that ensures resource availability and utilization in the event of a loss of communications with a call server. This is accomplished through the generation of periodic registration messages (over the control channel) to each of the call servers configured for the RTP Media Portal.
- Idle Session Detection
  - enables the RTP Media Portal to detect and recover media resources associated with idle media sessions. This basic

capability enables the system to recover resources as well as maintain capacity and performance.

- Media Survivability
  - enables the RTP Media Portal to allow media sessions to survive (through to session completion) in the absence of control signaling from the call server. This capability enables the system to permit media sessions to continue through to completion in the wake of loss of communications with the call server.
- Host IP Failover
  - provides redundant (active/standby) network connectivity for the RTP Media Portal host card so that if there is a network issue that affects one of the connections then the other connection will assume activity. This functionality enables the RTP Media Portal to maintain control and OAM connectivity in the event of a network failure.
- Shared Resource
  - enables the distribution of RTP Media Portal resources through association with multiple call servers. The strategy of distributing media sessions over multiple RTP Media Portals strengthens the network's ability to continue processing sessions in the event of a failure condition. Failures would result in diminished capacity, but not necessarily a service outage since many other RTP Media Portals remain available for the call server to utilize.
- Host CPU Recovery
  - provides for media stream survival through a Host CPU failure and subsequent recovery. Upon Host CPU failure, media streams on subtending Media Blades continue to flow undisturbed. During the subsequent Host CPU recovery process, communications are re-established with the Media Blades and available capacity information is retrieved from each of the Media Blades. When the RTP Media Portal resumes service, it offers the remaining available capacity on the Media Blades for the processing of new sessions.

Fault management procedures

Alarm surveillance

The following procedure lists steps to obtain information regarding alarms.

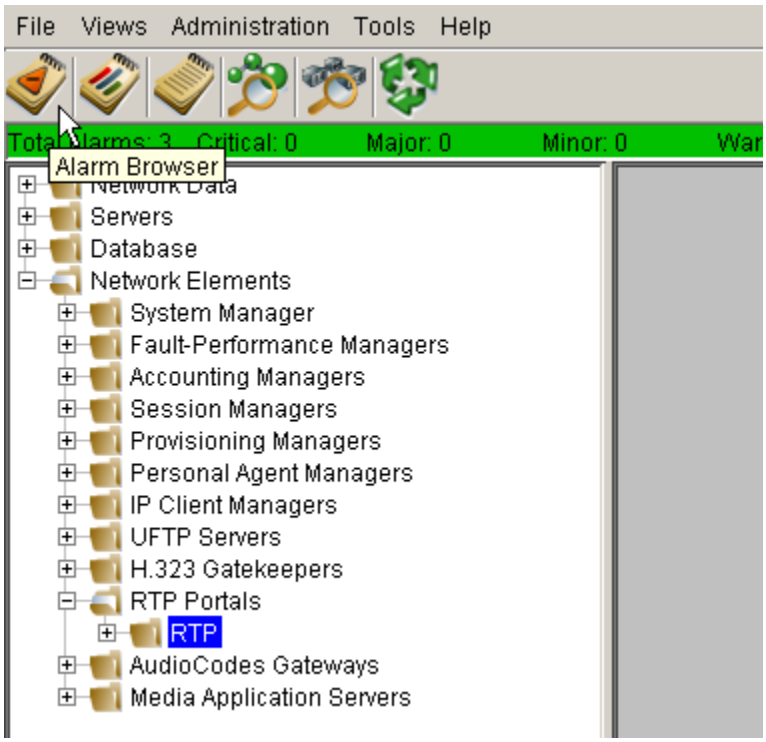
From the System Management Console

1 On the Alarm Bar, right-click and select **Logical View**. A new window opens.

2 Open the RTP Portal folder by clicking on the plus. Highlight the target RTP Portal.

3 At the bottom of the Logical Views screen, click on the **Alarm Browser** button.

Figure 1 Alarm Browser



Select an alarm to view alarm details. For alarm severity classification, refer to *Carrier Voice over IP Fault Management*: *Alarm and Log Reference.*

Clearing an alarm

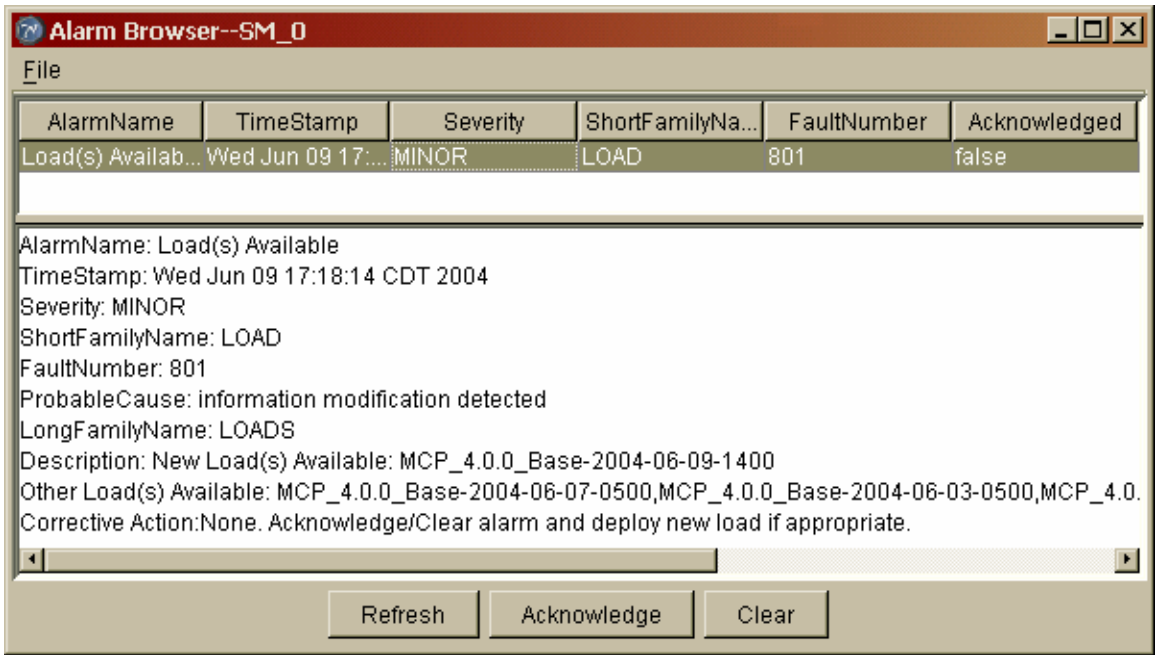
The following procedure lists steps to clear an alarm.

From the System Management Console

1 From the Alarm Browser window, click on the alarm row. Information regarding the alarm appears in the information screen at the bottom of the window.

2 Click on the **Clear** button.

Figure 2 Clearing alarms



RTP Media Portal alarms

The following section details how to clear certain alarms that affect the RTP Media Portal. RTP Media Portal alarms are discussed in further detail in *Carrier Voice over IP Fault Management*: *Alarm and Log Reference*.

Clearing the RTP101 Alarm (Blade out of service on initialization)

1. Ensure network connectivity between the host and blade, or network connectivity on its other interfaces (link LED is lit on the blade card). Verify that the Media Blade is running (Telnet to the suspect Media Blade).
2. Contact your next level of support with the results of these tests.

Clearing the RTP102 Alarm (RTP Media Portal Out of Service)

1. Ensure network connectivity between the host and blade, or network connectivity on its other interfaces (link LED is lit on the blade card).
2. Contact your next level of support.

Clearing the RTP103 Alarm (Portal Port Usage)

1. Ensure the configured capacity limits (the “ports” configuration parameter) provide adequate capacity to handles session load.

This alarm is cleared once occupancy falls below the configured onset threshold.

2 Contact your next level of support.

Clearing the RTP104 Alarm (Host Interface Failure)

1 Ensure network connectivity. Verify interfaces have a good connection to the network (link LED is lit on the host card).

2 Ensure that IP failover functionality is enabled on the RTP Media Portal. Verify the host IP failover setters were properly configured during installation and commissioning. Verification and configuration of settings is performed using the **PortalConf.pl** script on the Host. This alarm is cleared once both host Network Interfaces exhibit no communications problems.

3 If the alarm persists, contact your next level of support.

Additionally, alarms are generated whenever the Session Manager does not receive responses to requests to the RTP Media Portal. RTP108 and RTP 109 are generated by the Session Manager to indicate the connection with the Media Portal is lost. For information regarding these alarms, refer to *MCS 5200 Fault Management: Alarm and Log Reference.*

Informational and communication logs

Logs assist with the maintenance and operation of the RTP Media Portal. Information logs begin with the number nine (RTP**9**06), where communication logs begin with one (RTP**1**08). Administrative logs begin with the number eight (RTP**8**01).

- **Host Recovery-Mode Initiated**, RTP906. Produced upon recovery of the RTP Media Portal Host application upon discovery of pre-existing media sessions. No action is required.
- **Host Recovery- Mode Completed**, RTP907. Produced during the Host CPU recovery process to report the number of connections recovered on a Media Blade. No action is required.
- **Lost connection with Media Portal**, RTP108. Ensure the referenced Media Portal is accessible over the network, and functional. If not functional, restart the Media Portal.
- **Blade Recovery-Mode Initiated**, RTP909. Indicates that the Host CPU was able to re-establish communication with a subtending Media Blade and that the Media Blade is supporting connections. No action is required.
- **Blade Recovery-Mode Completed**, RTP910. Indicates the Host CPU was able to re-establish communication with a subtending

Media Blade and reports the number of connections the Host CPU was able to restore control over. No action is required.

- **Connection Map Increase Capacity**, RTP911. Generated whenever it is necessary for an increase in the size of the Hash Map used to store connection information. This may indicate a need for additional RTP Media Portal resources.
- **Connection Map Increase Capacity Denied**, RTP912. Generated whenever a request for an increase in the size of the Hash Map is denied. This indicates the Hash Map has already doubled in size, and prevents unbounded increases in the size of the Connection Map. Report this log to your next level of support.
- **Connection Map Increase Capacity Failed**, RTP913. Generated whenever a request for an increase in the size of the Hash Map fails due to some unforeseen software issue. Report this log to your next level of support.
- **Connection Not Found**, RTP914. Generated whenever an audit is performed over the Connection Map and a particular connection is not found on the corresponding Media Blade to match the entry in the Connection Map. No action is required.
- **Connection Idle**, RTP915. Generated whenever an audit is performed over the Connection Map and a particular connection is found idle on the corresponding Media Blade. No action is required.
- **Connection Exceeds Long Idle Duration**, RTP916. Generated whenever an audit is performed over the Connection Map and a particular connection is found on the corresponding Media Blade which exceeds the Long Idle Duration threshold. No action is required.
- **Connection Exceeds Long Call Duration**, RTP917. Generated whenever an audit is performed over the Connection Map and a particular connection is found on the corresponding Media Blade which exceeds the Long Call Duration threshold. No action is required.
- **Failed to Send Signal**, RTP118. Generated whenever an attempt to dispatch an outgoing signal fails. No action is required.
- **Failed to Reboot IO Exception**, RTP919. Generated whenever a request for reboot of the system fails due to a software request for said reboot. Report this log to your next level of support.
- **No Blades Configured**, RTP920. Generated whenever the Media Portal initiates in a state in which no Media Blade information has been configured from the System Management Console. Install the Media Blade in order to activate the RTP Media Portal.

- **Unknown Proxy**, RTP921. Generated whenever a request for service is made from an unknown proxy, one which is not datafilled for this Media Portal. Investigate the source proxy to ensure it is a valid network node, and if it should be part of the RTP Media Portal datafill.
- **Unable to Register with Proxy**, RTP922. Generated whenever an attempt to send a registration message to a proxy fails.
- **Host Interface Status File Problem**, RTP923. Generated during a failed attempt to establish a file handle for the interface status file, read from it, or it does not exist. Verify the host IP failover setting is properly set from the System Management Console. Report this log to your next level of support.
- **Lost connection with Last Media Portal**, RTP105. Ensure the referenced Media Portal is functional. If not, user may be required to restart the Media Portal.
- **Blade out of Service for Network Difficulty**, RTP106. Ensure network connectivity between the host and blade, or network connectivity on its other interfaces (link LED is lit on the blade card).
- **Blade out of Service for Public Network Difficulty**, RTP107. Ensure network connectivity between the host and blade, or network connectivity on its other interfaces (link LED is lit on Media Blade, ping the Media Blade).
- **Lost connection with Media Portal**, RTP109. Ensure the referenced Media Portal is accessible over the network, and functional. If not functional, restart the Media Portal.
- **RTP Media Portal does not support live configuration update**, RTP801. Configuration data change does not take effect until the RTP Media Portal is re-initialized using the Stop/Start, Restart, or Kill/Start maintenance commands.
- **System Property Portal.Config.BRHOME is not defined**, RTP802. The Portal.Config.BRHOME is not defined. Contact your next level of support.
- **Host Recovery-Mode Initiated**, RTP110. Produced during recovery of the RTP Media Portal Host application upon discovery of pre-existing media sessions on a Media Blade. No action is required.
- **Blade Recovery-Mode Completed**, RTP111. Indicates that the Host is able to establish communication with a subtending Media Blade. This log also reports the number of connections over which the Host was able to restore control. No action is required.
- **Host Recovery-Mode Initiated**, RTP 112. Produced at the start of the RTP Media Portal Host application recovery process. This

process attempts to reconstitute control overall pre-existing media sessions. No action is required.

- **Host Recovery - Mode Completed**, RTP 113. Produced during the Host recovery process to report the number of connections recovered on a specific Media Blade. No action is required.
- **Host Recovery - Mode Blade Communication Failure**, RTP114. Produced during the Host recovery process to report the number of Media Blades with which the Host failed to establish communications. No action is required.
- **No Blades Configured**, FTP200. Generated whenever the RTP Media Portal initializes in a state in which no Media Blade information has been configured. The RTP Media Portal requires at least one Media Blade in order to provide service. Install a Media Blade, and configure it from the System Management Console in order to successfully activate the RTP Media Portal.
- **Failed to Reboot IO Exception**, RTP201. Generated whenever a request for reboot of the RTP Media Portal fails due to a software exception. Report this log to your next level of support.
- **Unknown Proxy,** RTP202. Generated whenever a request for service is made from an unknown proxy, one which is not configured for the RTP Media Portal. Investigate the source proxy to ensure it is a valid network node. Then either update the configuration to include the node, or secure the control plane.
- **Unable to Register**, RTP203. Generated whenever an attempt to send a registration message to one of the configured proxies fails. Verify the configuration data represents an existing proxy. Verify the affected proxy exists and is reachable in the network.
- **Connection Not Found**, RTP204. Generated whenever an audit is performed over the Connection Map, and a particular connection is not found on the corresponding Media Blade. Report this log to your next level of support.
- **Connection Idle**, RTP 205. Generated whenever an audit is performed over the Connection Map, and a particular connection is unexpectedly found to be idle on the corresponding Media Blade. The invalid idle connection is identified in this log. No action is required.
- **Connection Exceeds Long Idle Duration**, RTP206. Generated whenever an audit is performed over the Connection Map, and a particular connection is found on the corresponding Media Blade which exceeds the Long Idle Duration threshold. No action is required, unless this log is generated excessively in which case the Long Idle Duration period may be configured for a longer interval.

- **Connection Exceeds Long Call Duration**, RTP207. Generated whenever an audit is performed over the Connection Map, and a particular connection is found on the corresponding Media Blade which exceeds the Long Call Duration threshold. No action is required.
- **Host Interface Status File Problem**, RTP208. Generated during a failed attempt to access the interface status file. Verify the host IP failover settings are properly configured using the **PortalConfig.pl** script on the Host. Report this log to your next level of support.
- **Connection May Increase Capacity**, RTP300. Generated whenever it is necessary for the RTP Media Portal to autonomously increase in the size of the Hash May used to store connection information. This may indicate a need for additional RTP Media Portal resources. Report this log to your next level of support.
- **Connection Map Increase Capacity Denied**, RTP301. Generated whenever a request for an increase in the size of the Hash Map is denied. This log indicates the Hash Map has already increased in size, and prevents unbounded increases in the size of the Connection Map. Report this log to your next level of support.
- **Connection May Increase Capacity Failed**, RTP302. Generated whenever a request for an increase in the size of the Hash Map fails due to some unforeseen software issue. Report this log to your next level of support.

System logs

System logs are discussed in detail in *Carrier Voice over IP Fault Management*: *Alarm and Log Reference*.

Configuration management

How this chapter is organized

This chapter includes information regarding the reconfiguration and maintenance of the RTP Media Portal. It assumes the RTP Media Portal has been installed and properly deployed. For more information regarding installation, refer to MCS 3.0 to MCS 4.0SN07 to SN08 RTP Media Portal upgrade on page 81.

The chapter is organized as follows:

For information about configuring the RTP Media Portal on the CS 2000, refer to *GWC Configuration Management*.

Tools and utilities

Deployment and configuration of the RTP Media Portal is performed by the System Management Console and the Provisioning Client. Please refer to *Carrier Voice over IP System Management Console User Guide* and *Provisioning Client User Guide* for more information.

The add operation on the System Management Console allows administrators to initially deploy and configure the RTP Media Portal component. The query operation is used for viewing configuration property values. The modify operation is used for changing the values of configuration properties any time after initial deployment.

Configuration changes do not occur in real-time. Rather, they are persistently stored in the Management Database Server until the RTP Media Portal is re-started.

Configuring and managing the RTP Media Portal component

This section provides procedures relevant to configuring the RTP Media Portal component.

Deploying the RTP Media Portal server

For information regarding how to deploy and configure an RTP Media Portal server, please refer to *Carrier Voice over IP System Management Console User Guide*.

For detailed instructions to deploy the RTP Media Portal, refer to Deploying the RTP Media Portal on page 83.

RTP Media Portal configuration

Physical data

Users may edit physical properties of the configuration including the IP addresses, default gateway, and server.

To edit the IP addresses, select **Network Data > Addresses** from the configuration view of the System Management Console. **Blade1Net1Address** is the address of the Net1 interface on the Media Blade in slot 1, and **RTPServer1Addr** is the host IP address.

To change the default gateway, select **Network Data > Gateways**. Use the **Add** button to add a gateway and the **Edit** button to change the default gateway. Gateways are specified by name and IP address.

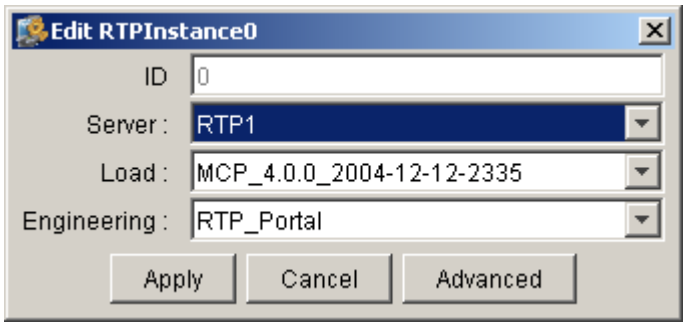
Servers may also be added or reconfigured. From the configuration view, select **Servers**. Enter Interface addresses, SNMP profile, and host name. Specify Linux as the operating system.

Logical data

To add system-level service information, select **Network Elements > RTP Portals** from the configuration view of the System Management Console. Users may add or edit Portal configuration properties to specify the base port, FPM, and default gateway.

To associate logical data with physical data, select the **Network Elements > Instance** of the target Portal. Use the **Add** or **Edit** buttons to specify the server. Click on the Advanced button to access specific parameter groupings.

Figure 1 Editing advanced properties

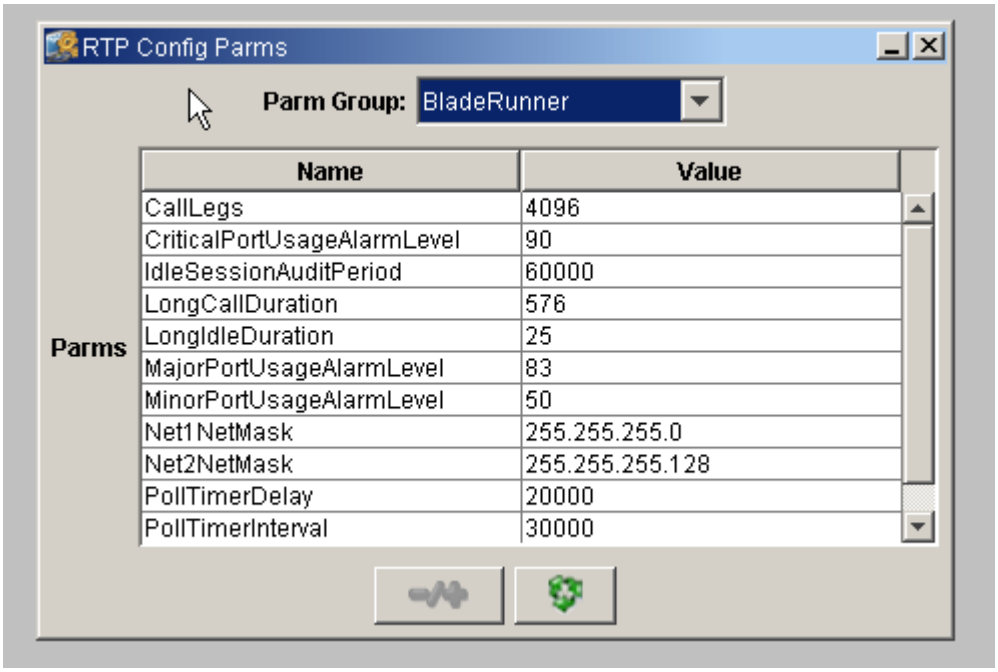


The following Parameter Groupings are accessible:

- OAMCom
- BladeBase
- TaskFW
- SystemTimers
- SubrCache
- ITaskFW
- RSIP
- Accounting
- OM
- DB
- Log
- Telnet
- SipBase
- Fault Tolerance

Users select the **Network Elements > Configuration Parameters** of a target RTP Media Portal, to edit BladeRunner and OAM Parameter Groups. Click on the **Edit** button to change the properties.

Figure 2 Blade Runner configuration parameters



The following table details the BladeRunner configurable properties.

Table 1 RTP Media Portal BladeRunner configurable properties

Configuration property	Format	Description
CallLegs	Type: String Range: 4096-MaxInt Default: 4096	Defines the bounds for internal data structures. This value is not normally changed. Default recommended.
PollTimerDelay	Type: String Range: 0-65535 Default: 20000 milliseconds	Time span (in milliseconds) required for startup and initialization of the Media Blades. The Host waits this period of time before attempting to contact the Media Blades. **Note:** The use of the default value for this property is highly recommended.

(Sheet 1 of 3)

Table 1 RTP Media Portal BladeRunner configurable properties (Continued)

Configuration property	Format	Description
PollTimerInterval	Type: String Range: 0-65535 Default: 30000 milliseconds	Interval (in milliseconds) at which the Host periodically polls the Media Blades to ensure they are still available. (Periodic checks that make sure the media blade is still up.) **Note:** The use of the default value for this property is highly recommended.
MinorPortUsageAlarmLevel	Type: Percent Range: 0-100 Default: 50	The percent usage at which the number of ports used on an RTP Media Portal (over all Media Blades) causes a minor RTP104/RTP105 alarm.
MajorPortUsageAlarmLevel	Type: Percent Range: 0-100 Default: 83	The percent usage at which the number of ports used on an RTP Media Portal (over all Media Blades) causes a major RTP104/RTP105 alarm.
CriticalPortUsageAlarm Level	Type: Percent Range: 0-100 Default: 90	The percent usage at which the number of ports used on the an RTP Media Portal (over all Media Blades) causes a critical RTP104/RTP105 alarm.
Net1NetMask	Type: IP address Range: N/A Default: 255.255.255.0 **(Used for the Media Blades, not for the host card.)**	The Net1NetMask is the netmask used for routing on the network that is reachable by the NET1 interface on the Media Blade. This is only used in dual-network configurations.

(Sheet 2 of 3)

Table 1 RTP Media Portal BladeRunner configurable properties (Continued)

Configuration property	Format	Description
Net2NetMask	Type: IP address Range: N/A Default: 255.255.255.0 **(Used for the Media Blades, not for the host card.)**	The Net2NetMask is the netmask used for routing on the network that is reachable by the NET2 interface on the Media Blade.
LongIdleDuration	Type: String Range: 0-65535 Default: 25	This represents the maximum amount of time that a RTP Media Portal resource may remain validly idle.
LongCallDuration	Type: String Range: 0-65535 Default: 576	This represents the maximum amount of time that an RTP Media Portal resource may remain active in a media session. This has units of number of Idle Session Audit Periods.
StaticRTPPorts	Type: Boolean Range: true/false Default: false	Boolean indicating whether the RTP Media Portal should perform static fixed port allocation/management, or dynamic randomized port allocation/management. **Note:** When this parameter is selected, the Media Blade's configuration parameter "Number Ports" is disregarded and all ports in the range from “Min Port Value” to “Max Port Value” are allocated for usage. All even-numbered ports in the specified range are used for RTP and UDP streams and the odd-numbered ports are used for RTCP streams (if required).

(Sheet 3 of 3)

From the configuration view, select the **Network Elements > Blade** of the target RTP Media Portal to add or change Media Blade information.

Select **Network Elements > Session Manager** of the target Portal to add or change Controller/Session Manager information.

RTP Media Portal maintenance

From the configuration view of the System Management Console, select **Network Elements > NE Maintenance** of the target Portal. Here the user may deploy, undeploy, start, stop, restart, or kill a Portal.

Accounting management

Functional description

The RTP Media Portal does not perform accounting management.

.

Performance management

Functional description

RTP Media Portal performance is monitored through the System Management Console by viewing Operational Measurements (OMs). For more information on RTP Media Portal OMs and the viewing of these OMs, please refer to *Carrier Voice over IP System Management Console User Guide*.

- OMs generated by the Session Manager for the RTP Media Portal are listed below.

Security and administration

How this chapter is organized

This chapter is organized as follows:

Security overview

One function of the RTP Media Portal is to secure the media interface to the MCP Services Network. Securing the media layer is achieved through a combination of methods at the network level and the component (RTP Media Portal) level.

Network level security functions

At the network level, media layer security is achieved by the randomization of the IP addresses/ports used for multimedia sessions and utilization of NAPT (Network Address Port Translation) technology to obscure the network topology of the MCP Services Network.

Media Blade (IP address) randomization

When a multimedia session requests resources, the RTP Media Portal selects an appropriate Media Blade to host the session. Media Blade selection determines the specific IP address that will be made available to the media streams for the session.

During the selection of a Media Blade, the port usage of each available Media Blade is queried to determine the number of available ports for each. The Media Blade which has the most available ports is selected. This method of selection provides randomization and helps distribute the session load across the Media Blades.

Port randomization

When the RTP Media Portal is deployed, each Media Blade is configured with a pool of ports containing a specific number of ports in a specific range based on configuration data (“Number Ports”, “Min Port Value”, “Max Port Value”, respectively). For more information on these configuration properties, refer to Table 1, RTP Media Portal BladeRunner configurable properties, on page 36.

As multimedia sessions are initiated, a port is chosen from the port pool associated with the selected Media Blade. For non-static port configurations (i.e. “Static RTP Ports” is configured to be “false”), when a multimedia session completes, their associated ports are deallocated from the pool and new replacement ports are allocated to the pool. The deallocation of used ports and allocation of replacement ports provides randomization in the port pools for the Media Blades.

NAPT function

In order to obscure the MCP Services Network topology, the RTP Media Portal uses the NAPT functionality to secure the multimedia sessions so that there is no leakage of topology information.

This is achieved by maintaining a list of media ports (NAPT table) which are being used within active multimedia sessions. Only packets which arrive on these active ports are processed. Packets which arrive on non-active ports are rejected.

RTP Media Portal component level security functions

The RTP Media Portal component also contributes to system security by opening and closing media ports only in response to requests from the Communication Server 2000 (which has pre-authenticated such requests) and by rejecting any unauthorized packets arriving on an active connection.

Authenticated requests

All requests to manipulate the media resources on the RTP Media Portal originate from the Communication Server 2000. The Communication Server 2000 ensures that all requests are made by, or made to, a valid service subscriber. In this way, the Communication Server 2000 effectively authenticates all requests.

In addition, the portion of the RTP Media Portal which processes these requests to manipulate the media resources resides safely within the MCP Services Network.

Packet filter/firewall

As packets are received, the RTP Media Portal analyzes each packet to ensure the following:

- The data format is RTP/RTCP/UDP, as indicated by the session description. All other packet types are discarded.
- The source/destination addresses match the expected source/destination addresses indicated in the session description. Packets that do not have a matching source/destination address are discarded.
- The source/destination ports match the expected source/destination ports indicated in the session description. Packets that do not have a matching source/destination port are discarded.

User administration

Basic administrative tasks for the RTP Media Portal are covered in the Upgrade, Configuration, and Fault sections of this document. Other basic administrative tasks related to the System Management Console are covered in *Carrier Voice over IP System Management Console User Guide.*

Backup and recovery

How this chapter is organized

This chapter is organized as follows:

Backup and restore

Prerequisites

The following prerequisites are required for a RTP Media Portal backup or restore.

- Remote DDS4 or Universal Serial Bus (USB) tape drive. The tape drive does not need to be within the MCP Service Network, but it must be attached to a Solaris* machine that is visible to the server conducting the backup.
- Tape in the remote tape drive. For USB drives, use a 20 GB tape. For SCSI drives, use a 12 GB tape.
- Live 100Mbps Ethernet connection.
- IP address of the tape server.
- Full duplex mode. Ensure all nodes involved have their network interface set to full duplex mode. This includes the server being backed up or restored, the tape server, and any intermediate node in the network being traversed. All MCP Servers should be set to Auto Negotiate so that they too will respond in full duplex mode.

Failure to set the mode to full duplex will result in restore times that are ten times normal.

- For restore operation, server address information is required.
- For restore operation, the Portal Installation CD is required.

When connecting a USB tape drive to the server, perform the following:

- Log in as **root** to the server where the tape drive is being connected or disconnected.
- Type the command **/etc/init.d/volmgt stop** and press **Enter**.
- Connect or remove the USB tape drive. When connecting the tape drive, use port 0.
- If connecting the tape drive, type the command **/etc/init.d/volmgt start** and press **Enter**.
- If connecting the tape drive, turn it on.

If there is an error installing a USB tape drive, refer to Error installing USB tape drive on page 61 for instructions to correct the problem.

System access

Backup

To establish connection to the RTP Media Portal, access is obtained through a Secured Shell (SSH). Note, if this connection is used and the SSH session dies, the backup operation will die as well.

Restore

During a system restore, the server's operating system is executing in a limited capacity. Therefore, access must be through the server's console port (via the serial port).

Remote tape drive set up

A remote tape drive is required. The following procedure outlines the steps necessary to properly set up the remote tape drive if it is on an MCP Server.

If the remote tape drive is NOT on a MCP Server, you may skip this procedure. However, the user must ensure the remote shell operations from the server to be backed up are enabled on the remote tape drive server.

From the terminal server

1 As the MCP Server has to access the tape drive on the remote host, make sure it has the proper access to that host.

2 Log in as **sysadmin** to the server with the tape drive.

3 Enable the execution of remote shell commands.

sudo /usr/local/bin/mcp_enable_remote_sh.pl <MCP_Server_IP> <Enter>

where **<MCP_Server_IP>** is the Portal Host IP address.

4 From the Portal, log in as **root**.

5 Verify access to the remote host has been set correctly.

rsh -l sysadmin <Tape_Server_IP> df -k <Enter>

where **<Tape_Server_IP>** is the IP address of the remote host with the tape drive.

6 Output appears on screen, indicating the target system is correctly set for the restore operation. In not, contact your next line of support before continuing.

Backup to remote tape drive

The following procedure lists steps to backup the RTP Media Portal to tape.

Ensure the remote tape drive has been set up correctly before proceeding with the backup. For more information, refer to Remote tape drive set up on page 50.

From a terminal server

1 Label the DDS4 tape with the RTP Media Portal name and the date of backup. Insert the tape into the tape drive of the server acting as backup host.

2 Log in as **sysadmin** to the RTP Media Portal.

3 Initiate the backup.

sudo /usr/local/bin/mcp_backup.pl <Enter>

4 The user is prompted for the type of backup. Enter a selection to continue.

```
Select a backup operation from the following
list:
[1] Backup to remote Tape Drive
[2] Backup to remote Disk
[3] Backup to local Disk
[4] Exit/Abort backup
```

To backup to a remote tape, continue with the next step. For remote tape backup, proceed to step 8. For backup to a local disk, proceed to step 9.

5 Next the user is asked for the IP address of the host where the tape drive resides. Type the IP address and press **Enter** to continue. Note the logical IP address, not the physical address, should be used.

```
Enter the IP address of the remote device (in
dot notation):
```

6 Information regarding the remote tape drive is displayed, and the user is prompted to verify tape insertion. Verify the information and press **Enter** to continue.

```
<timestamp> Backup to remote tape drive
/dev/rmt/0cn on host <Remote_Host_IP.
<Remote_Host_IP> is alive.

Please verify a tape has been freshly inserted
into the tape drive.
Any pre-existing data on the tape will be
overwritten.
Press Enter when you are ready.....
```

7 If the tape needs to be rewound, the user is prompted to rewind the tape as shown in the example below. Press **Enter** to accept the Default (Y) and continue.

```
The tape needs to be rewound, current tape
fileNo = 1, Rewind Tape? [Y]:
```

To backup to a remote tape, proceed to step 9.

8 For Remote Disk backup, the user is prompted for the IP address of the remote host.

```
Enter the IP address of the remote device (in
dot notation):
```

9 For Remote and Local Disk backups, the user is prompted for the full path and filename of the backup file.

```
Please enter the path/filename to write the
backup file to:
```

10 The backup operation may require several minutes to complete. If the backup requires more than one tape, the system will prompt the user to insert additional tapes as needed.

When the backup is complete, remove the tape from the tape drive. Store the tape in a safe, dry location.

11 Review the backup log **mcp_backup.pl** to ensure the backup was successful. The log file is stored in the directory **/home/sysadmin/bkup_restore**, and the filename is

mcp_backup.pl.log.<dayTimeStamp>. Where **<dayTimeStamp>** is YYYY_MM_DD_HH:MM:SS.

12 Log off the machine.

13 From the remote host, disable remote access.

sudo /usr/local/bin/mcp_disable_remote_sh.pl <Enter>

14 Store the tape in a safe, dry location.

Restore

The following procedure lists steps to restore the RTP Media Portal from tape. Ensure the remote tape drive has been set up correctly before proceeding with the restore. For more information, refer to Remote tape drive set up on page 50.

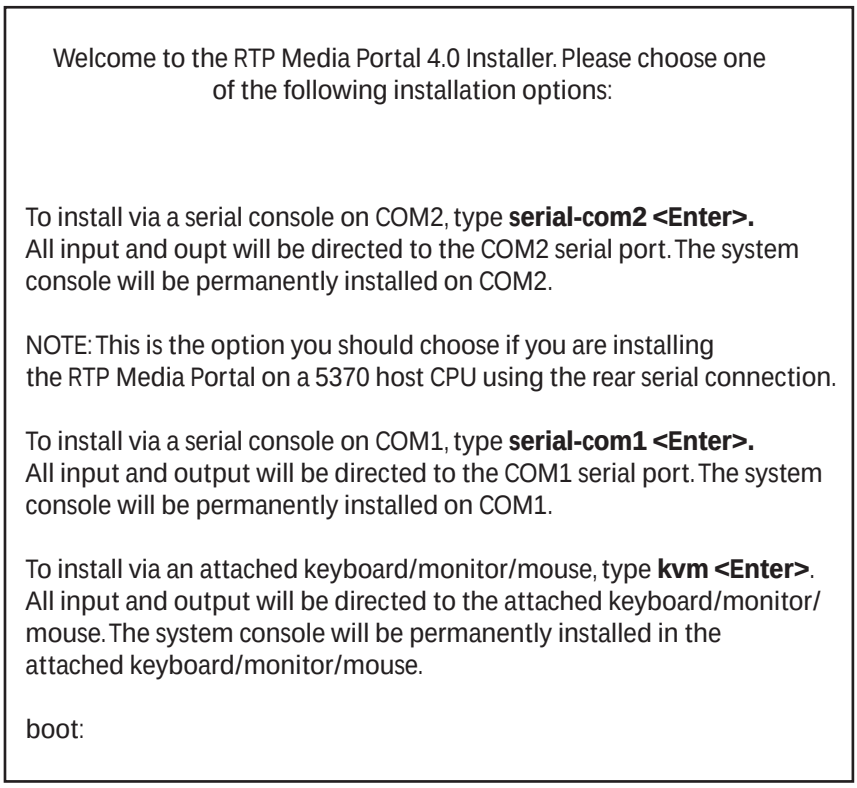
From the terminal server

1 Establish a terminal session to the Host CPU through the terminal server.

2 Insert the installation CD, and reboot the system.

3 After the system boots from the installation CD, the initial welcome screen appears.

Figure 1 Welcome screen



4 Enter one of the following at the “boot:” prompt.

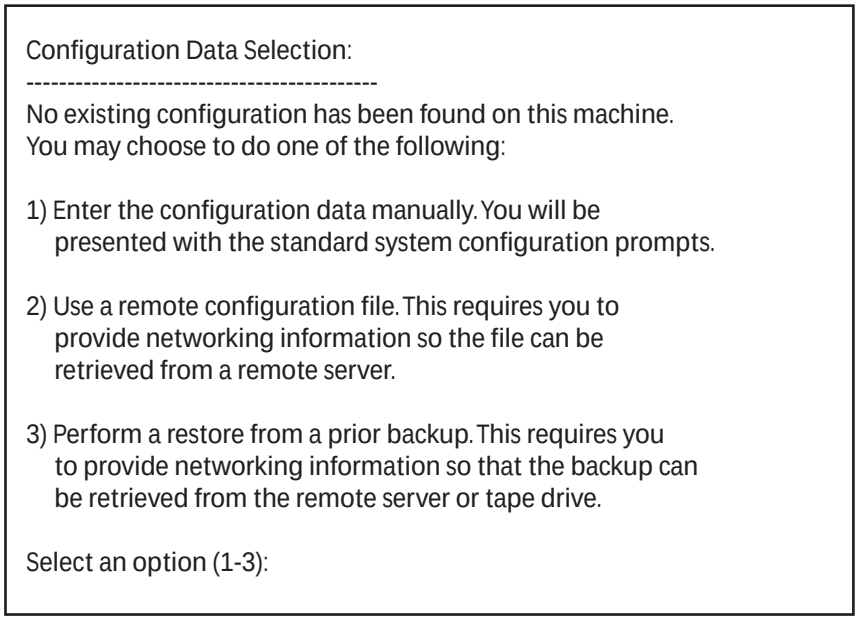
- **serial-com1** — installation will require the COM1 serial port.
- **serial-com2** — installation will require the COM2 serial port. This is the required setting for a CPV5370 host CPU.
- **kvm** — installation will require attached keyboard, monitor, and mouse.

Note the selection will determine the permanent location of the system console.

5 The software loads and checks for existing disk partitions. The system will output results of the check and whether any partitions are created and formatted. Press **<Enter>** to proceed.

6 The script presents the Configuration Data Selection screen. Select the third option.

Figure 2 Configuration selection

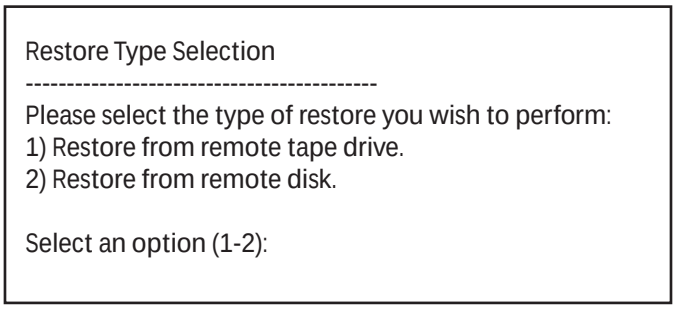


7 The restore assumes the default backup settings are used. By default, the backup procedure backs up the /admin partition. This partition contains the configuration files. If some other partition is backed up, the backup cannot be used to perform a restore.

8 The user is prompted for the restore type. Make the appropriate selection.

If restoring from tape, the script contacts the remote tape server. If the tape is not rewound, the user is given the option to do so. When the tape is ready, the script continues.

Figure 3



9 The script prompts the user for the IP address of the remote machine. If restoring from a remote file, the filename must also

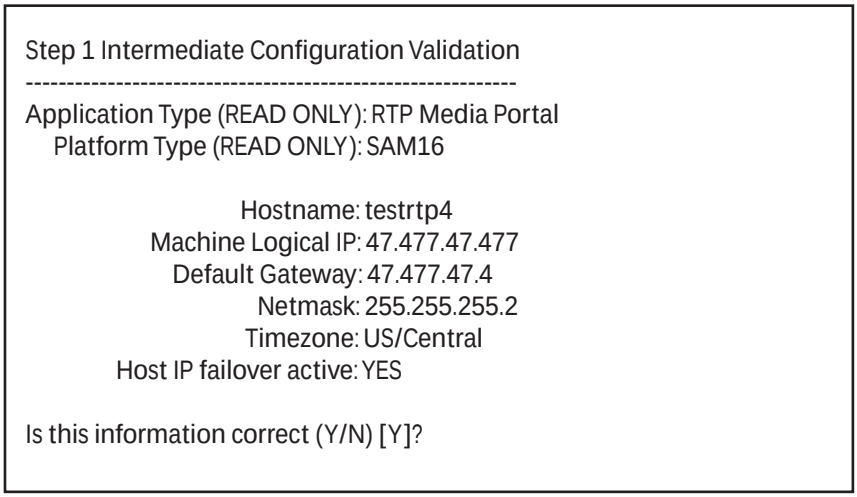
be entered. As the system restore overwrites any existing data, the script prompts for verification before beginning the operation.

10 The first phase of data configuration involves network-based items.

- **Application type**. This is a read-only value that is set automatically by the installer and cannot be changed. It describes the type of application being installed.
- **Platform type**. This is a read-only value that is set automatically by the installer and cannot be changed. This value is set according to the hardware platform being configured.
- **Hostname**. The name given to the RTP Media Portal.
- **Machine Logical IP**. The IP address assigned to the RTP Media Portal.
- **Default Gateway**. The default gateway router assigned to the RTP Media Portal host card.
- **Netmask**. The network mask for the RTP Media Portal host card.
- **Timezone**. The timezone in which the RTP Media Portal is physically located.
- **Host IP failover active**. True/false value that controls the host IP failover service. If the service is active, the host card uses its network interfaces in an active/standby configuration.

11 The user is prompted with a validation screen.

Figure 4 Step 1 Intermediate Configuration Validation



12 The second phase of data configuration involves items related to the media cards.

- **Chassis Identifier**. This is a number that uniquely identifies the RTP Media Portal chassis. As a chassis can contain two independent Media Ports, this value is specific to the chassis. The number must be between 0 and 255 inclusive. Do not assign the same chassis identifier to multiple chassis on the same local network.
- **Host card slot number**. The slot number in which this host card is located. It must be either 7, for side A of the chassis, or 9, for side B of the chassis.
- **Media Blade Default Gateway**. This is the gateway router that is assigned to each media card in the system. This IP address may be different than the gateway IP assigned to the host card.
- **Blade MAC Addresses**. These are the MAC addresses for each media card in the system. There are two MAC addresses for each card (NET1 and NET2).
- **NTP Clock Source**. This is the IP address of an NTP server from which the RTP Media Portal obtains clock synchronization. There may be zero or more configured NTP clock sources.

13 The user is prompted with a validation screen.

Figure 5 Step 2 Intermediate Configuration Validation

```
Step 2 Intermediate Configuration Validation
---------------------------------------------------------------
                  Chassis identifier: 100
                Host card is in slot: 9
Media blade default gateway: 47.477.47.4

            Blade 11 NET1 MAC: 112233445566
            Blade 11 NET2 MAC: 665544332211
            Blade 12 NET1 MAC:
            Blade 12 NET1 MAC:
            Blade 13 NET1 MAC:
            Blade 13 NET1 MAC:
            Blade 14 NET1 MAC:
            Blade 14 NET1 MAC:
            Blade 15 NET1 MAC:
            Blade 15 NET1 MAC:
            Blade 16 NET1 MAC:
            Blade 16 NET1 MAC:
              NTP Clock Source: 47.477.47.477
              CS2K Portal (Y/N): N

Is this information correct (Y/N) [Y]?
```

14 Next, the Date and Time Configuration screen appears. If the time is correct, press **<Enter>**. Otherwise, press **N** to make corrections using the local time.

15 The user is then prompted for passwords for “root”, “nortel”, and “sysadmin”. Passwords must be at least eight characters in length. The installer performs a basic validation of passwords.

16 The script begins the restore. A progress indicator displays on screen.

17 Next, the system is configured for specific Media Portal requirements. This step in the process takes approximately 5-10 minutes to complete.

18 The system reboots. Remove the CD-ROM from the drive when it is ejected.

19 As the system is powering on, hold down the **F2** key to enter BIOS set up. For security purposes, remove everything from the boot device list *except* the hard drive. Save and exit BIOS set up. The system will reboot.

20 When the system completes the reboot process, press **<Enter>** to boot the default image. After rebooting, the login prompt appears and the Media Portal is ready for software deployment.

Error scenarios

This section provides information regarding error scenarios that could occur when a backup or restore operation is in progress. For RTP Media Portal, log files are located in the directory **/home/sysadmin/bkup_restore/**

Invalid IP address

If an invalid IP address is entered, an information message is displayed. Example output:

```
/usr/local/bin/mcp_backup.pl 47.47.47.46
 no answer from 47.47.47.46
 10:22:27 ERROR: System, 47.47.47.46, could not be
pinged
 10:22:27 Remote Backup verification failed, aborting
backup process
 Logs are written to
/export/home/sysadmin/bkup_restore/mcp_backup...
```

For restore operations, if an invalid IP address is entered after the **ufsrestore** command has been executed, an information message is displayed. Example output:

```
ufsrestore rfsv sysadmin@47.47.47.47:/dev/rmt/Ocn 1
Fri Feb 6 17:06:14 CST 2004

48.48.48.48: Connection timed out
before Fri Feb 6 17:11:03 CST 2004
```

Connection to remote tape server is lost

If a RTP Portal loses connection to the tape drive during a backup, the system will display error messages on screen.

Example output:

```
<47.47.47.48:20976,47.104.157.20:16001,108076965965
5,3,1080343335125,54>:
Established ---> Destroying
<47.47.47.48:20976,47.104.157.20:16001,108076965965
5,3,1080343335125,54>:
Destroying ---> Destroyed
<47.47.47.48:20976,47.104.157.20:16001,108076965965
5,4,null,null>:
Inactive ---> Reset
<47.47.47.48:20976,47.104.157.20:7001,1080769659655
,2,1080343397775,63>:
Established ---> Destroying
```

```
<47.47.47.48:20976,47.104.157.20:7001,1080769659655
,2,1080343397775,63>:
Destroying ---> Destroyed
<47.47.47.48:20976,47.104.157.20:7001,1080769659655
,5,null,null>:
Inactive ---> Reset

DUMP: Lost connection to remote host.
```

As the **mcp_backup** script “hangs”, type **Ctrl-C** to abort. (To kill the process from another session type **=> kill -9 <pid>**.)

Tape drive failure

If something happens to the tape drive during a backup, an information message is displayed. Example output:

```
DUMP: write: I/O error
DUMP: write error 8320 blocks into volume 1
DUMP: Do you want to restart?: (“yes” or “no”)
```

Answer **no** to this prompt. The script will terminate, and another backup can be started. An information message is displayed on screen:

```
DUMP: The ENTIRE dump is aborted.
19:29:15
************************************************
19:29:15 An error occurred during one (or more) dump
commands=>

19:29:15 DUMP: Do you want to restart? (“yes” or
“no”) DUMP: the ENTIRE dump is aborted.

19:29:15 DO NOT USE THIS BACKUP - a RESTORE USING THIS
BACKUP WILL FAIL
19:29:15 Fix the associated problem, and perform
another backup
19:29:15
************************************************
19:29:15 Dump command(s) failed. Aborting backup.
Logs are written to
/home/sysadmin/bkup_restore/mcp_backup.pl.log
```

Restoring from multiple tapes

When restoring from multiple tapes, if a user presses **Enter** before inserting the next tape into the tape drive, the restore process must be restarted.

To recover, continue to press **Enter** until a “Read error” is displayed. For example, the following shows output generated when a user incorrectly presses **Enter** before tape 2 is inserted, then presses **Enter** again to obtain the “Read error” message:

```
Mount volume 2
then enter volume name (default: /dev/rmt/0cn)

Mount volume 3
then enter volume name (default: /dev/rmt/0cn)

Read error while restoring
./me/loads/pool9/Files/B/UAS06.zip.bLfCbwYvd5YvveYt
continue? [y n] n
Verify volume and initialize maps
Media read error: I/O error
rest*: No such file or directory
12:49:35 Failed to Restore /IMS/imssipdb directory,
aborting restore process
Logs are written to
/export/home/sysadmin/bkup_restore/mcp_recover.pl.
log.2004_03_24.12:49:35
```

Error installing USB tape drive

If there is an error installing a USB tape drive, reboot the server and log in as **root**. Then type the command **shutdown -y -g0 -i6** and press **Enter**.

Recovery

The following procedures include instructions to replace the CPU host card and task processor.

Replacement of CPU host card

If a CPV5370 fails, calls in progress stay up but call control is lost. Calls cannot be controlled again, nor can any new calls be set up on that Portal until the CPV5370 has been replaced and the new CPV5370 is in service.

If a CPU host card fails, replace the bad card with a new one. Follow steps in BIOS configuration of the CPV5370 Host Card on page 70 to make the appropriate BIOS changes to the new card.

Replacement of task processor

If the RTP Media Portal MCPN765 fails, all calls set up on that blade are lost at the time of the failure and cannot be recovered. Replace the bad card, and perform the following initialization procedures. This

procedure requires a special cable to configure the BIOS of the card. For more information regarding the installation of MCPN765 cards, refer to Installing MCPN765 cards on page 80.

SN07 to SN08 RTP Media Portal upgrade

This section includes instruction for upgrading the RTP Media Portal from SN07 to SN08.

As the physical partitioning and file system types on the hard drive have been changed, it is not possible to perform an **upgrade** from a SN07 Portal to a SN08 Portal. Rather, the SN08 Portal must be **installed**. Before proceeding, secure a backup of the Portal and database file.

How this chapter is organized

This chapter is organized as follows:

SN07 to SN08 RTP Media Portal upgrade procedures

Prerequisites

This chapter provides instruction for installing a new RTP Media Portal. A RTP Media Portal occupies a single chassis domain. It is assumed that hardware is already assembled as follows:

- MCPN765 I/O blades are installed (in front slots 1-6 for Domain A, and slots 11-16 for Domain B).
- TM-PIMC-0101 765 transition modules are installed (in rear slots 1-6 for Domain A, and slots 11-16 for Domain B).
- CPV5370 host blades are installed (in front slot 7 for Domain A, and slot 9 for Domain B).
- CPTM-04 transition modules are installed (in rear slot 7 for Domain A, and slot 9 for Domain B).
- CPX8216T HSC/BR hot swap controllers are always installed in rear slot 8 for Domain B, and slot 10 for Domain A.
- Hard drives and CD-ROM drives are installed in the front peripheral bay.
- Floppy drives are installed in rear peripheral bays.

Installing the RTP Media Portal software consists of placing the required packages on the hard drive of the Host Card. As the Host Card is the only component in the system that has a hard drive, it is also configured to allowMedia Blades to boot and mount their file systems over the network.

Installing the RTP Media Portal software requires a single CD-ROM. The complete base system can be installed in approximately 15 minutes.

IMPORTANT: The installation procedures must be followed separately for each side of the chassis if two Portals are installed in the same chassis.

The following is required for an installation:

- Chassis and peripherals
  - — One Motorola CPX8216T high availability compact PCI which is divided into two domains (A and B), each running independent media portals.
  - — One SCSI hard drive per domain, minimum 40Gb.
  - — One SCSI CD-ROM per domain.
  - — One 3.5” floppy drive per domain.
  - — One Motorola CPX8216T HSC/BR hot swap controller per domain.
- Host Card
  - — One Motorola CPV5370 per domain.
  - — One Motorola CPTM-04 transition module per domain.
- Media Blades
  - — Up to six MCPN765 per domain.
  - — One PIMC-0101 transition module for each MCPN 765.
- Other hardware
  - — VT100-compatible terminal device for console access to the host and I/O blades.
- Base software
  - — RTP Media Portal installation CD
- Passwords
  - — Root password for host(s)
  - — Password for “nortel” user
  - — Password for “sysadmin” user
- Required configuration information. Collect and record the following information prior to proceeding with the installation. Successful

configuration of the RTP Media Portal depends on the accurate capture of this information.

Table 1 Configuration Information

Slot	Attribute	Value
1	NET1 MAC address for I/O card	
	NET2 MAC address for I/O card	
2	NET1 MAC address for I/O card	
	NET2 MAC address for I/O card	
3	NET1 MAC address for I/O card	
	NET2 MAC address for I/O card	
4	NET1 MAC address for I/O card	
	NET2 MAC address for I/O card	
5	NET1 MAC address for I/O card	
	NET2 MAC address for I/O card	
6	NET1 MAC address for I/O card	
	NET2 MAC address for I/O card	
(Sheet 1 of 3)		

Table 1 Configuration Information (Continued)

Slot	Attribute	Value
7	Host card network address (Portal address)	
	Host card netmask	
	Host card default gateway	
	Host card IP failover active	
	Hostname	
	Timezone	
	Chassis identifier	
	I/O card default gateway	
	Timeserver IP address(es)	
11	NET1 MAC address for I/O card	
	NET2 MAC address for I/O card	
12	NET1 MAC address for I/O card	
	NET2 MAC address for I/O card	
13	NET1 MAC address for I/O card	
	NET2 MAC address for I/O card	
14	NET1 MAC address for I/O card	
	NET2 MAC address for I/O card	
15	NET1 MAC address for I/O card	
	NET2 MAC address for I/O card	
16	NET1 MAC address for I/O card	
	NET2 MAC address for I/O card	
(Sheet 2 of 3)		

Table 1 Configuration Information (Continued)

Slot	Attribute	Value
9	Host card network address (Portal address)	
	Host card netmask	
	Host card default gateway	
	Host card IP failover active	
	Hostname	
	Timezone	
	Chassis identifier	
	I/O card default gateway	
	Timeserver IP address(es)	
(Sheet 3 of 3)		

MAC addresses may be obtained several ways:

- MAC addresses for I/O cards are located on the actual cards.
- MAC addresses may be obtained by following Installing MCPN765 cards on page 80.
-

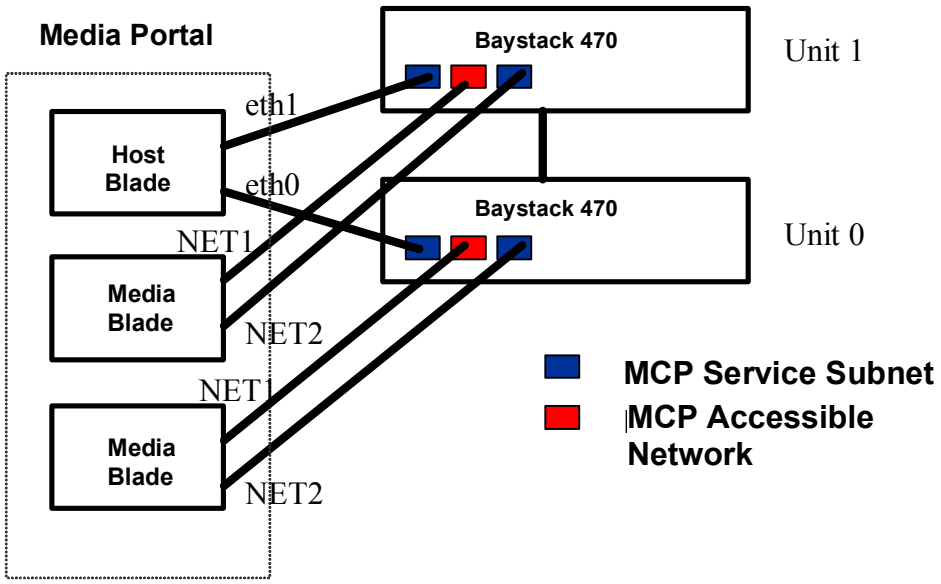
Network deployment

It is recommended to deploy the RTP Medial Portal in a dual-network configuration.

Dual-network deployment

For the dual-network configurations, the Host Card is connected to the MCP Service Network. The Media Blades have one interface connected to the MCP Service Network (NET2) and one to the MCP Accessible Network. The two interfaces on the Host Card are used in an active, standby mode and there is no interface redundancy on the Media Blades as each connects to a separate network. This configuration is depicted in Figure 1 on page 69.

Figure 1 Dual-network deployment



The below table details the usage of the physical port for dual-network deployment.

Label	BIOS device number	Linux interface name	Usage
MCPN 765 I/O Card Ethernet port usage			
NET1	CLUN 0/DLUN 0	eth0	Public
NET2	CLUN 13/DLUN 0	eth1	CS 2000 Service
CPV5370 Host Card Ethernet port usage			
1	N/A	eth0	CS 2000 Service
2	N/A	eth1	CS 2000 Service

Failure to use the ports as described will result in a non-operational RTP Media Portal.

Installing RTP Media Portal

This section outlines steps to install the RTP Media Portal.

From the terminal console

1 Establish BIOS settings for the CPV5370 Host Card. For details, refer to BIOS configuration of the CPV5370 Host Card on page 70.

2 Install the RTP Media Portal. For details, refer to Installing the RTP Media Portal on page 73.

BIOS configuration of the CPV5370 Host Card

This procedure provides instruction for BIOS settings. While many of the factory default settings are acceptable, a few require changes. If you are not certain the factory settings are in effect, reset all values to default from within the BIOS set up under the **Exit** menu.

From the terminal console

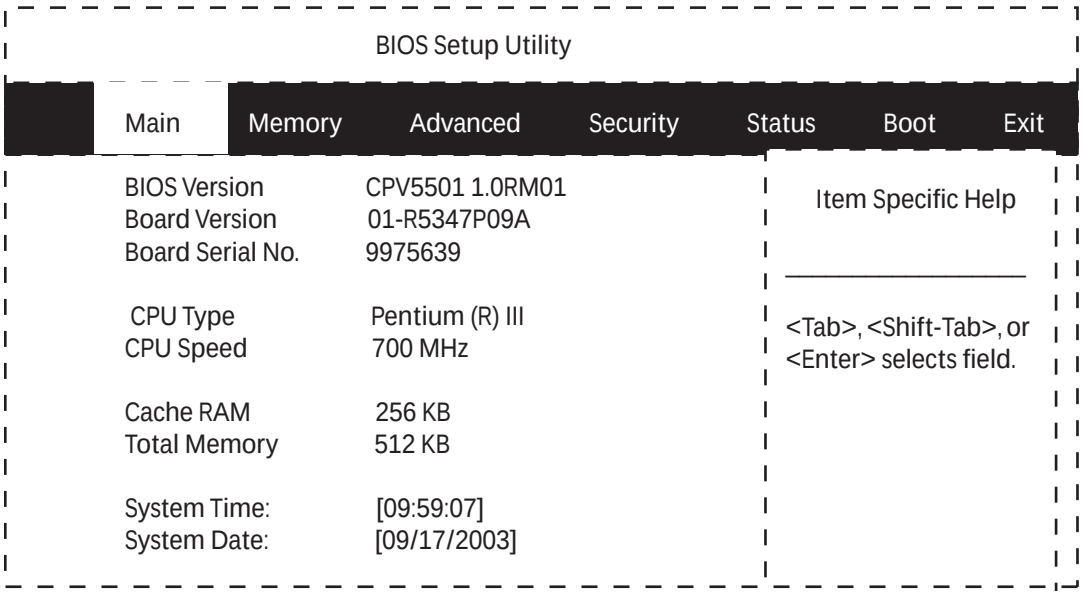
1 Create a console connection to COM1 (A) on the front panel of the host CPU card.

A connection to COM1 is only used during the initial power up procedures. Once the BIOS configuration is set, the user must remove the serial cable from COM1 and connect the Terminal Server to cable COM2 on the transition module.

2 As the system is powering on, hold down the **F2** key to enter BIOS set up. The CPV5370 Card ships from the factory with serial port settings 19,200 baud, 8/n/1.

If you do not see output on screen, it may be necessary to reseat the CPV5370 card and press the Reset button on the front panel.

Figure 2 BIOS Setup Utility screen



3 From the **Advanced** menu, move to **IDE Configuration** and press **Enter**.

4 Verify, or change, the values on screen to match the values listed below. Leave all other values as default.

```
Local Bus IDE adapter: [Disabled]
Large Disk Access Mode: [DOS]
SMART Device Monitoring: [Disabled]
Primary Master: [NONE]
Primary Slave: [NONE]
Secondary Master: [NONE]
Secondary Slave: [NONE]
```

5 Press **Esc** twice to return to the **Advanced** menu.

6 Move to **PCI Configuration** and press **Enter**.

7 Verify, or change, the values on screen to match the values listed below.

```
Default Primary Video Adapter: [AGP]
On-Card Ethernet 1: [Enabled]
Ethernet 1 Connection: [Rear]
Ethernet 1 Option ROM: [Disabled]
On-Card Ethernet 2: [Enabled]
Ethernet 2 Connection: [Rear]
Ethernet 2 Option ROM: [Disabled]
```

8 Move to the **HA configuration** sub-menu and press **Enter**.

9 Set the **HA Config** value to **Enabled**. Also, set the Domain that is being configured to **Enable**, and **Disable** for the other domain. CPU in slot 7 is Domain A, and CPU in slot 9 is Domain B.

Example for Domain A, the Host Card in slot 7:

```
HA Config [Enabled]
Domain A [Enabled]
Domain B [Disabled]
```

10 Press **Esc** twice to return to the **Advanced** menu.

11 Move to **Remote Console** and press **Enter**.

12 Verify, or change, the values on screen to match the values listed below. Leave all other values as default.

```
COM Port: [COM B]
Serial port B: [Enabled]
Base I/O address: [2F8]
Interrupt: [IRQ 3]
Baud Rate: [9600]
Console Type: [VT100]
Flow Control: [None]
Screen Lines: [25]
Active After Post: [On]
```

13 Press **Esc** twice to return to the **Advanced** menu.

14 From the **Boot** menu, move the cursor to **Boot Device Priority** and press **Enter**.

15 Ensure the system boots in the following order:

```
8XX SCSI CD-ROM LSI Logic
+Hard Drive
! +Removable Devices
! ATAPI CD-ROM Drive
! Legacy Network Boot
```

Place an exclamation mark (!) beside the appropriate devices to disable them.

16 Press the **Esc** key to return to the main menu.

17 Move to the **Security** menu to set control access to the BIOS settings. Unauthorized BIOS access enables any Linux security to be circumvented.

18 Set up the BIOS supervisor password. Ensure the password on Boot option is disabled.

19 Move to the **Exit** menu to save changes and exit the BIOS set up. The system will reboot.

20 While the system is rebooting, quickly change the console connection from COM1 to COM2. Use the escape sequence **<Esc><Shift>OQ** to enter the BIOS set up screen again.

If you do not see output on the terminal, make sure the terminal is set to **9600/8/n/1** and reset the CPV5370 card to try again.

21 When prompted, enter the supervisor password to ensure the password was correctly set and is using COM2 as the console port.

22 Insert the RTP Media Portal installation CD in the CD-ROM drive for the domain (the top CD-ROM drive is Domain A).

23 Press the **Esc** key to exit BIOS without making any changes. The system will reboot.

24 Remove the serial cable from COM2, and connect the serial cable from the Terminal Server to that port.

Installing the RTP Media Portal

The installation script provides a text-based user interface. The script includes the installation of RedHat, HA-specific packages, and RTP Portal-specific packages.

If it is necessary to re-enter the BIOS from the Terminal Server, use the Escape key sequence **<Esc><Shift>OQ** .

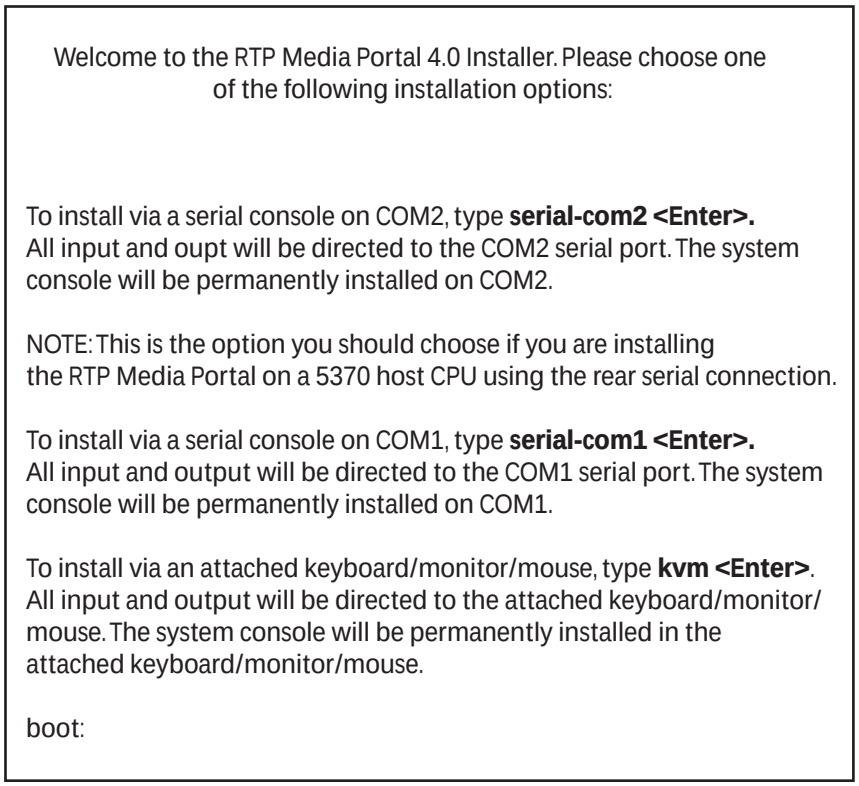
From the terminal server

1 Establish a terminal session to the Host CPU through the terminal server.

2 Insert the installation CD, and reboot the system.

3 After the system boots from the installation CD, the initial welcome screen appears.

Figure 3 Installation welcome screen



4 Enter one of the following at the “boot:” prompt.

- **serial-com1** — installation will require the COM1 serial port.
- **serial-com2** — installation will require the COM2 serial port. This is the required setting for a CPV5370 host CPU.
- **kvm** — installation will require attached keyboard, monitor, and mouse.

  Note the selection will determine the permanent location of the system console.

5 The installation software loads and checks for existing disk partitions. The system will output results of the check and whether any partitions are created and formatted. Press **<Enter>** to proceed.

6 Next, the script begins data configuration. If you are installing the RTP Media Portal for the first time on this hardware, you must enter all the required data. If this is a re-install, the existing data is preserved and may be reused. If you are performing a restore from a prior backup, the configuration data backed up is restored and may be reused or changed.

When entering configuration data, note that mistakes can be corrected. At each major step of data entry, the user is prompted to verify the information is correct. If not, answer **N** and re-enter the information.

Default values are shown to the right of the prompt and enclosed in brackets. To accept the default, press **<Enter>**.

7 For first-time installations, skip to step 8. For re-installation instructions, skip to step 9.

8 If this is a first-time installation, the system will note there is no existing configuration data and prompt the user with the following options:

- Enter the configuration data manually. Use the information recorded in Configuration Information on page 66.
- Use a remote configuration file. This is helpful when installing several Portals. Create a basic configuration file and store it on a remote server. The file can then be used as a starting point for subsequent installations, changing only the machine-specific settings.

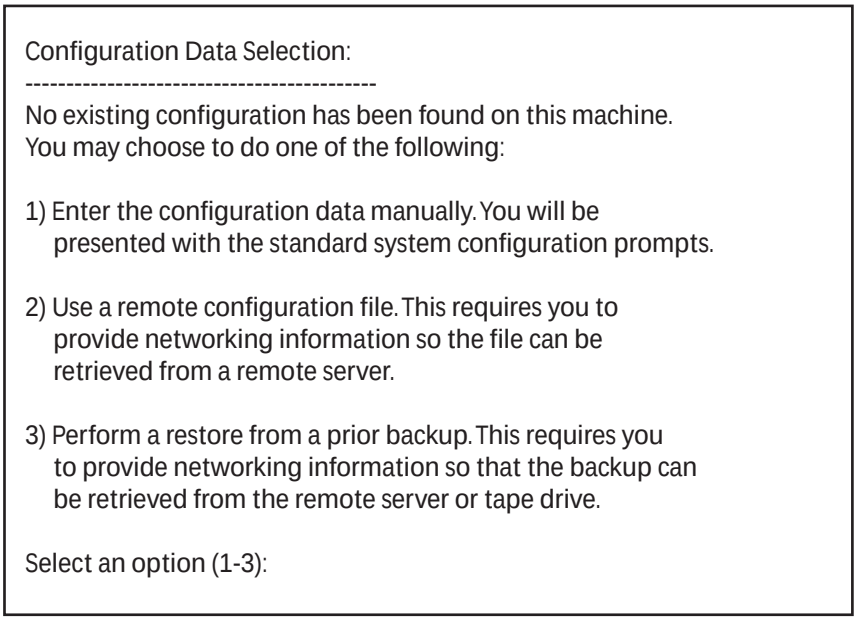
  If this option is selected, the user is prompted to enter the IP address, gateway, and netmask for the Portal being installed. Next, enter the remote FTP server IP address, and userid/login information. The pathname of the directory containing the configuration file is also required. Note the pathname is relative to the home directory of the userid specified for the FTP login.

  The installer script contacts the FTP server and obtains a directory listing, which is displayed on screen. Each file is numbered. Enter the number of the filename and press **<Enter>**.
- Perform a restore from a prior backup. If this option is selected, the user is prompted to enter the IP address, gateway, and netmask for the Portal being installed. You will then be prompted to select the restore type, either remote

tape drive or remote disk. In either case, the system prompts the user for the IP address of the remote machine.

Continue with the installation by skipping to step 10.

Figure 4 Configuration selection



9 When re-installing an existing RTP Media Portal, the installation script detects the existing configuration data and existing partitions. Press **<Enter>** to continue.

The installer next presents several options including:

- Use existing configuration values. In most re-installation scenarios, this option would be chosen unless a significant number of configuration values change.
- Use a configuration file from a remote server.

  If this option is selected, the user is prompted to enter the IP address, gateway, and netmask for the Portal being installed. Next, enter the remote FTP server IP address, and userid/login information. The pathname of the directory containing the configuration file is also required. Note the pathname is relative to the home directory of the userid specified for the FTP login.

  The installer script contacts the FTP server and obtains a directory listing, which is displayed on screen. Each file is

numbered. Enter the number of the filename and press **<Enter>**.

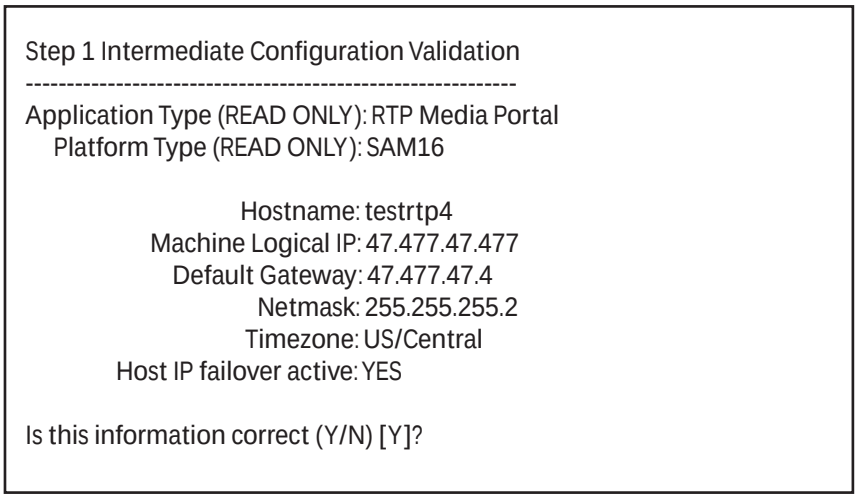
- Use configuration data from a prior backup. If this option is selected, the user is prompted to enter the IP address, gateway, and netmask for the Portal being installed. You will then be prompted to select the restore type, either remote tape drive or remote disk. In either case, the system prompts the user for the IP address of the remote machine.
- Manually enter configuration data. You will be prompted for configuration values.

10 The first phase of data configuration involves network-based items.

- **Application type**. This is a read-only value that is set automatically by the installer and cannot be changed. It describes the type of application being installed.
- **Platform type**. This is a read-only value that is set automatically by the installer and cannot be changed. This value is set according to the hardware platform being configured.
- **Hostname**. The name given to the RTP Media Portal.
- **Machine Logical IP**. The IP address assigned to the RTP Media Portal.
- **Default Gateway**. The default gateway router assigned to the RTP Media Portal host card.
- **Netmask**. The network mask for the RTP Media Portal host card.
- **Timezone**. The timezone in which the RTP Media Portal is physically located.
- **Host IP failover active**. True/false value that controls the host IP failover service. If the service is active, the host card uses its network interfaces in an active/standby configuration.

11 The user is prompted with a validation screen.

Figure 5 Step 1 Intermediate Configuration Validation

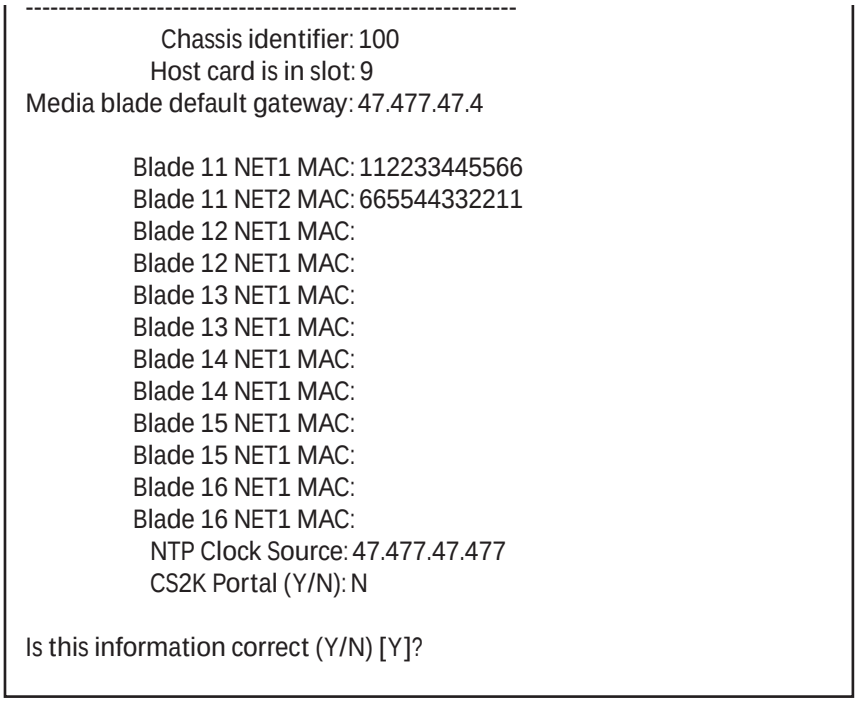


12 The second phase of data configuration involves items related to the media cards.

- **Chassis Identifier**. This is a number that uniquely identifies the RTP Media Portal chassis. As a chassis can contain two independent Media Ports, this value is specific to the chassis. The number must be between 0 and 255 inclusive. Do not assign the same chassis identifier to multiple chassis on the same local network.
- **Host card slot number**. The slot number in which this host card is located. It must be either 7, for side A of the chassis, or 9, for side B of the chassis.
- **Media Blade Default Gateway**. This is the gateway router that is assigned to each media card in the system. This IP address may be different than the gateway IP assigned to the host card.
- **Blade MAC Addresses**. These are the MAC addresses for each media card in the system. There are two MAC addresses for each card (NET1 and NET2).
- **NTP Clock Source**. This is the IP address of an NTP server from which the RTP Media Portal obtains clock synchronization. There may be zero or more configured NTP clock sources.

13 The user is prompted with a validation screen.

Figure 6 Step 2 Intermediate Configuration Validation



14 Next, the Date and Time Configuration screen appears. If the time is correct, press **<Enter>**. Otherwise, press **N** to make corrections using the local time.

15 The user is then prompted for passwords for “root”, “nortel”, and “sysadmin”. Passwords must be at least eight characters in length. The installer performs a basic validation of passwords.

16 The script begins the installation of the individual software packages. A progress indicator displays on screen. This part of the installation takes approximately 10 minutes to complete.

17 Next, the system is configured for specific Media Portal requirements. This step in the process takes approximately 5-10 minutes to complete.

18 The system reboots. Remove the CD-ROM from the drive when it is ejected.

19 As the system is powering on, hold down the **F2** key to enter BIOS set up. For security purposes, remove everything from the boot device list *except* the hard drive. Save and exit BIOS set up. The system will reboot.

20 When the system completes the reboot process, press **<Enter>** to boot the default image. After rebooting, the login prompt appears and the Media Portal is ready for software deployment.

Installing MCPN765 cards

The following procedure outlines instructions for adding MCPN765 I/O Cards in RTP Portal (Domain A). To add new I/O cards to Domain B, repeat this procedure.

A terminal device (such as a dumb terminal, or PC COM port plus terminal software) is required to change the NVRAM settings on the MCPN765 I/O blade. The 765 serial port uses 9600/8/N/1 settings. Use the port labeled **COM1** on the rear transition module.

From a terminal device

1 Once the blade and transition module has been physically installed in the chassis, connect the specialized serial cable to the COM1 port at the bottom of the transition module.

2 Press the reset button on the front of the MCPN765 card to reboot the card.

3 Press the **Esc** key to abort the re-boot process.

4 Set and enable the real time clock on the blade.

set <MMDDYYHHMM> <Enter>

5 At the Bug prompt, display the MAC address for the card.

niot ;h <Enter>

6 Record the MAC address for CLUN 0/DLUN 0 (NET1), and CLUN13/DLUN 0 (NET2).

CLUN 0/DLUM 0 (NET1): _____

CLUN 13/DLUN 0 (NET2): _____

7 Type **env** to verify, and change as necessary, BIOS settings on the I/O Card. Ensure they match the settings shown below.

Note the entries may appear differently depending on the version of BIOS loaded on each card. If an entry appears that is not described below, accept the default.

```
PPC6-Bug>env
Bug, AST or System environment [B/A/S] = B?
Maximum Memory Usage (Mb, 0=AUTO) = 0?
Field Service Menu Enable [Y/N] = N?
Probe System for Supported I/O Controllers [Y/N] =
Y?
Auto-Initialize of NVRAM Header Enable [Y/N] = Y?
```

```
Network PReP-Boot Mode Enable [Y/N] = Y?
SCSI Bus Reset on Debugger Startup [Y/N] = N?
Primary SCSI Bus Negotiations Type [A/S/N] = A?
Primary SCSI Data Bus Width [W/N] = N?
Secondary SCSI Identifier = “07”?
NVRAM Boot List (GEV.fw-boot-path) Boot Enable [Y/N]
= N?
NVRAM Boot List (GEV.fw-boot-path) Boot at power-up
only [Y/N] = N?
NVRAM Boot List (GEV.fw-boot-path) Boot Abort Delay
= 5?
Auto Boot Enable [Y/N] = N?
Auto Boot at power-up only [Y/N] = N?
Auto Boot Scan Enable [Y/N] = Y?
Auto Boot Scan Device Type List =
FDISK/CDROM/TAPE/HDISK/?
Auto Boot Controller LUN = 00?
Auto Boot Device LUN = 00?
Auto Boot Partition Number = 00?
Auto Boot Abort Delay = 7?
Auto Boot Default String [NULL for an empty string]
= ?
ROM Boot Enable [Y/N] = N?
ROM Boot at power-up only [Y/N] = Y?
ROM Boot Abort Delay = 5?
ROM Boot Direct Starting Address = FFF00000?
ROM Boot Direct Ending Address = FFFFFFFC?
Network Auto Boot Enable [Y/N] = Y?
Network Auto Boot at power-up only [Y/N] = N?
Network Auto Boot Controller LUN = 13?
Network Auto Boot Failover Controller LUN = 00?
Network Auto Boot Device LUN = 00?
Network Auto Boot Abort Delay = 5?
Network Auto Boot Configuration Parameters Offset
(NVRAM) = 00001000?
Watchdog prior status ignored at autoboot [Y/N] = Y?
Watchdog shutdown at board reset [Y/N] = N?
Reset Ethernet chip after file transfer [Y/N] = N?
Stop Auto Boot after selftest failure [Y/N] = N?
Memory Size Enable [Y/N] = Y?
Memory Size Starting Address = 00000000?
Memory Size Ending Address = 04000000?
DRAM Speed in NANO Seconds = 8?
ROM Bank A Access Speed (ns) = 90?
ROM Bank B Access Speed (ns) = 120?
DRAM Parity Enable [On-Detection/Always/Never -
O/A/N] = O?
```

```
L2Cache Parity Enable [On-Detection/Always/Never -
O/A/N] = O?
PCI Interrupts Route Control Registers (PIRQ0/1/2/3)
= 0A0B0E0F?
Serial Startup Code Master Enable [Y/N] = N?
Serial Startup Code LF Enable [Y/N] = N?
Firmware Command Buffer Enable [Y/N] = N?
Firmware Command Buffer Delay = 5?
Firmware Command Buffer : <Enter>
['NULL' terminates entry]?
Update Non-Volatile RAM (Y/N)? y
Reset Local System (CPU) (Y/N)? n
```

8 At the prompt, type **niot** to access the Network boot settings.

```
PPC6-Bug>niot
Controller LUN =00? 13
Device LUN =00?
Node Control Memory Address =03E1D8A0?
Client IP Address =0.0.0.0? 192.168.<chassis #>.<slot #>
Server IP Address =0.0.0.0? 192.168.<chassis #>.<hostcard #>
Subnet IP Address Mask =255.255.255.0?
Broadcast IP Address=255.255.255.255? 192.168.<cage
#>.255
Gateway IP Address =0.0.0.0?
Boot File Name ("NULL" for None) =?
/tftpboot/bladeRunner
Argument File Name ("NULL" for None) =?
Boot File Load Address =001F0000?
Boot File Execution Address =001F0000?
Boot File Execution Delay =00000000? 00000005
Boot File Length =00000000?
Boot File Byte Offset =00000000?
BOOTP/RARP Request Retry =00? 50
TFTP/ARP Request Retry =00? 50
Hardware error retry attempts =00?
Trace Character Buffer Address =00000000?
BOOTP/RARP Request Control: Always/When-Needed
(A/W)=W?
BOOTP/RARP Reply Update Control: Yes/No (Y/N) =Y?
Update Non-Volatile RAM (Y/N)? y
```

9 At the prompt, type **reset** to reboot the network once it completes the necessary self-tests.

```
PPC6-Bug>reset
Cold/Warm Reset [C,W] = C?
Execute Local SCSI Bus Reset [Y,N] = N?
Execute Local (CPU) Reset [Y,N] = N? y
```

10 Repeat this procedure for all I/O cards in the Domain. The Host Card IP address and the Broadcast IP address should be the same between all I/O Cards.

11 Unplug the console connection from the last I/O card.

12 Log in to the system as **root**.

13 Run PortalConfig.PL to change the MAC addresses.

```
/opt/mcp/mediaportal/bin/PortalConfig.pl
```

Deploying the RTP Media Portal

The RTP Media Portal is deployed from the System Management Console. For more information regarding the deployment of VoIP components, refer to *System Management Console User Guide.*

Network configuration

Each media card has two network interfaces, NET1 and NET2. Enter the netmask for the network connected to the media card's NET2 interface.

If the media card uses NET1 to connect to a different network, enter the netmask for that network in the NET1 netmask field. Otherwise leave it set to 0.0.0.0.

Usage of "NET1 Media IP" and "NET2 Media IP" fields for each media card depends on the network configuration.

Dual-network deployment

If the Media Portal is used in a dual-network configuration, both the NET1 and NET2 IP fields must be used.

- Enter both the NET1 and NET2 netmasks in the appropriate fields.
- Enter the media card's IP address on the NET1 network in the NET1 Media IP field.
- Enter the media card's IP address on the NET2 network in the NET2 Media IP field.

Deployment procedures

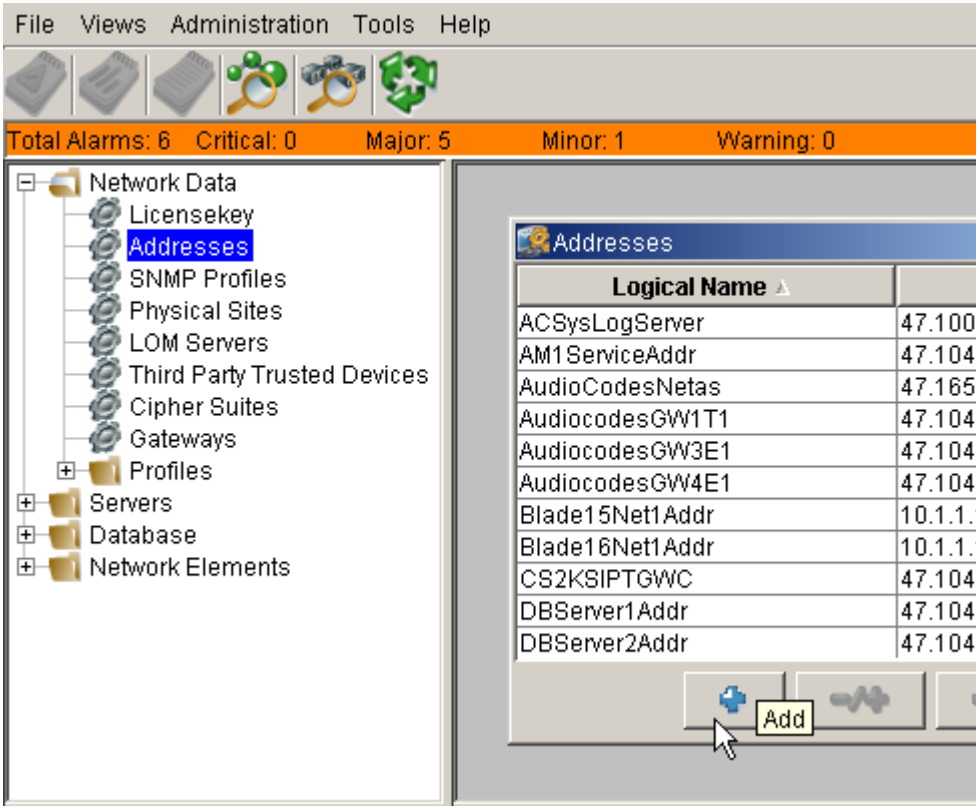
Follow steps in the following procedure to deploy the Portal.

From the System Management Console

1 Create network addresses for the RTP Media Portal Blade(s). From the configuration view, click on the plus sign next to the **Network Data** folder to expand the view.

2 Select the **Addresses** option. A new dialog box opens.

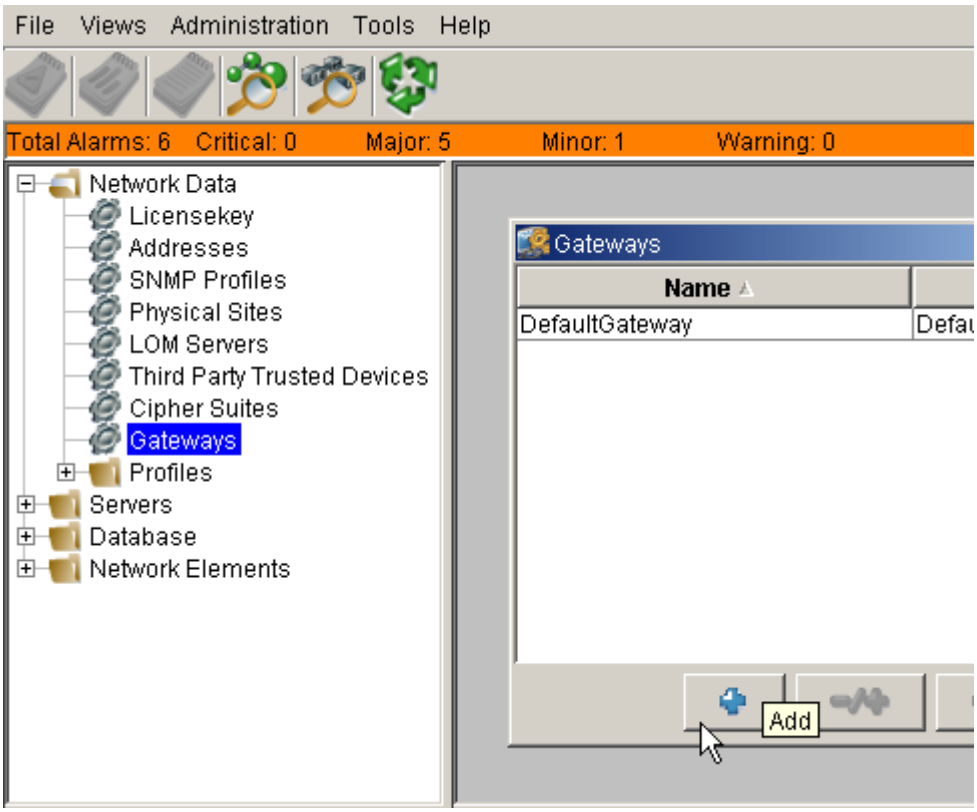
Figure 7 Adding network addresses



3 Click on the **Add** button, and enter the logical name and IP address.

4 If deploying a Portal in a new gateway, create a gateway address. Select the **Gateway** option. A new window opens. Click on the **Add** button. Enter a name and address for the gateway.

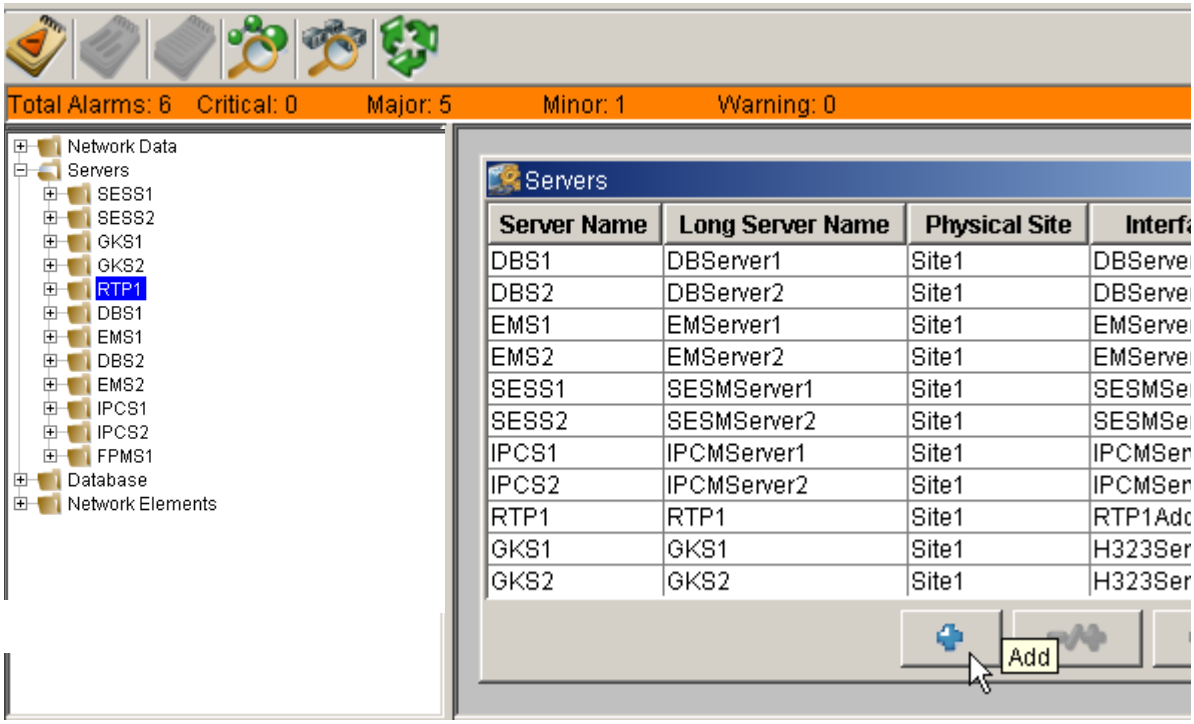
Figure 8 Adding a gateway



5 Add interface addresses for the RTP Server. From the configuration view, click on the plus sign next to the **Servers** folder to expand the view.

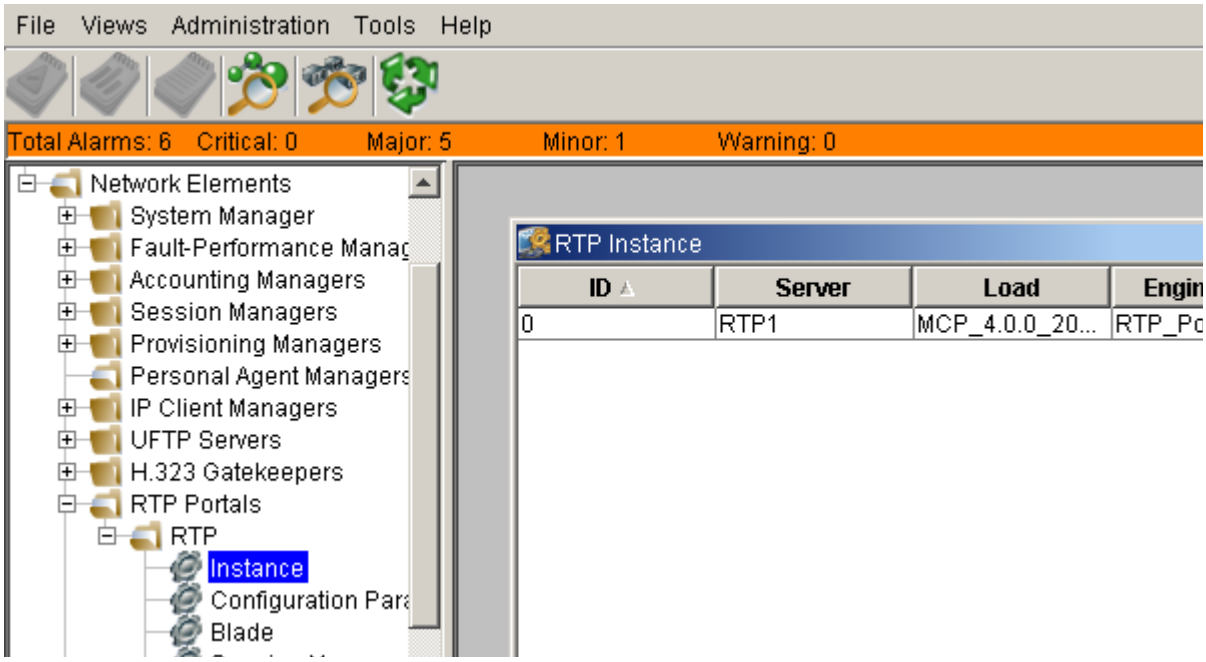
6 Click on the Portal folder. A new window opens. Click on the **Add** button, and enter Interfaces addresses and host name. Select the SNMP profile from the pull-down menu. Specify Linux as the operating system.

Figure 9 Add Portal server



7 Click on the plus sign next to **Network Elements** to expand the view. Click on the plus sign next to the **RTP Portals** folder. Click on the plus sign next to the Portal folder you wish to deploy.

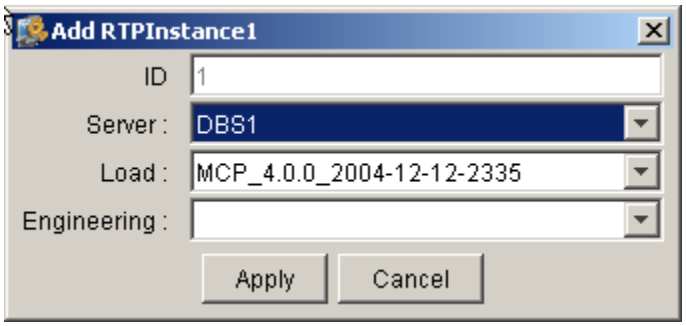
Figure 10 Add Portal Instance



8 Select the **Instance** option. A new window opens.

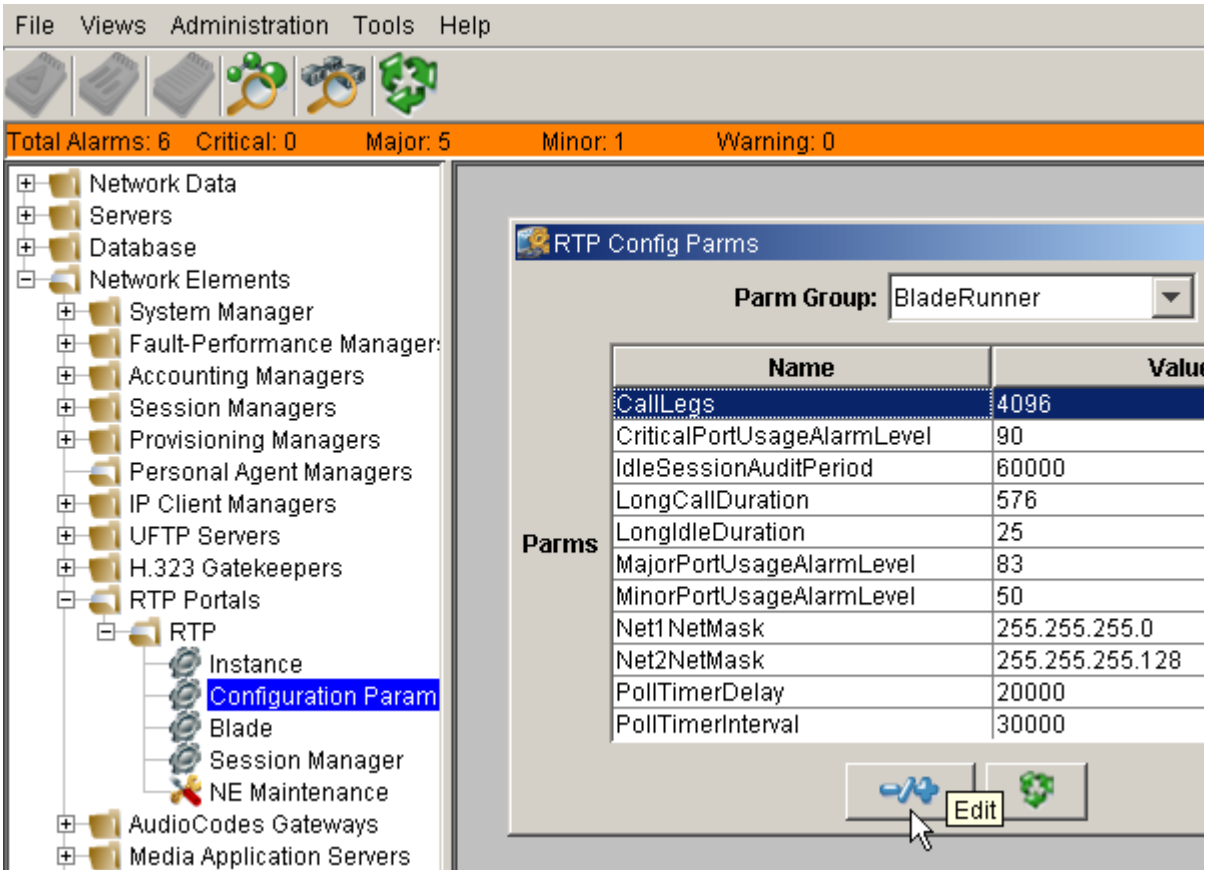
9 Select the Portal, and click on the **Add** button. Enter information as requested.

Figure 11 Define Portal Instance



10 Click on the **Configuration Parameters** option. A new window opens.

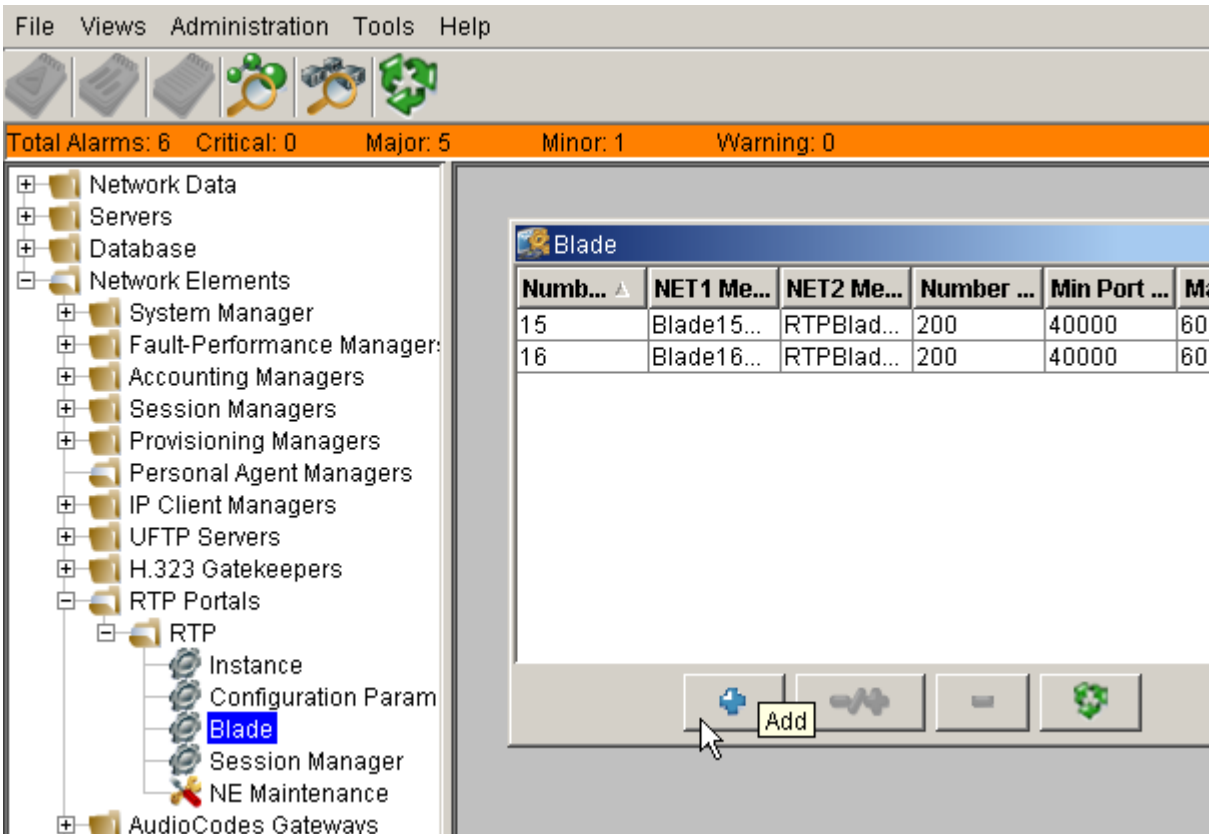
Figure 12 Edit Configuration Parameters



11 Select a variable and click on the **Edit** button to change properties. For more information regarding variables, refer to Configuring and managing the RTP Media component" in CVoIP RTP Media Portal Basics, NN10367-111.

12 Click on the **Blade** option. A new window appears.

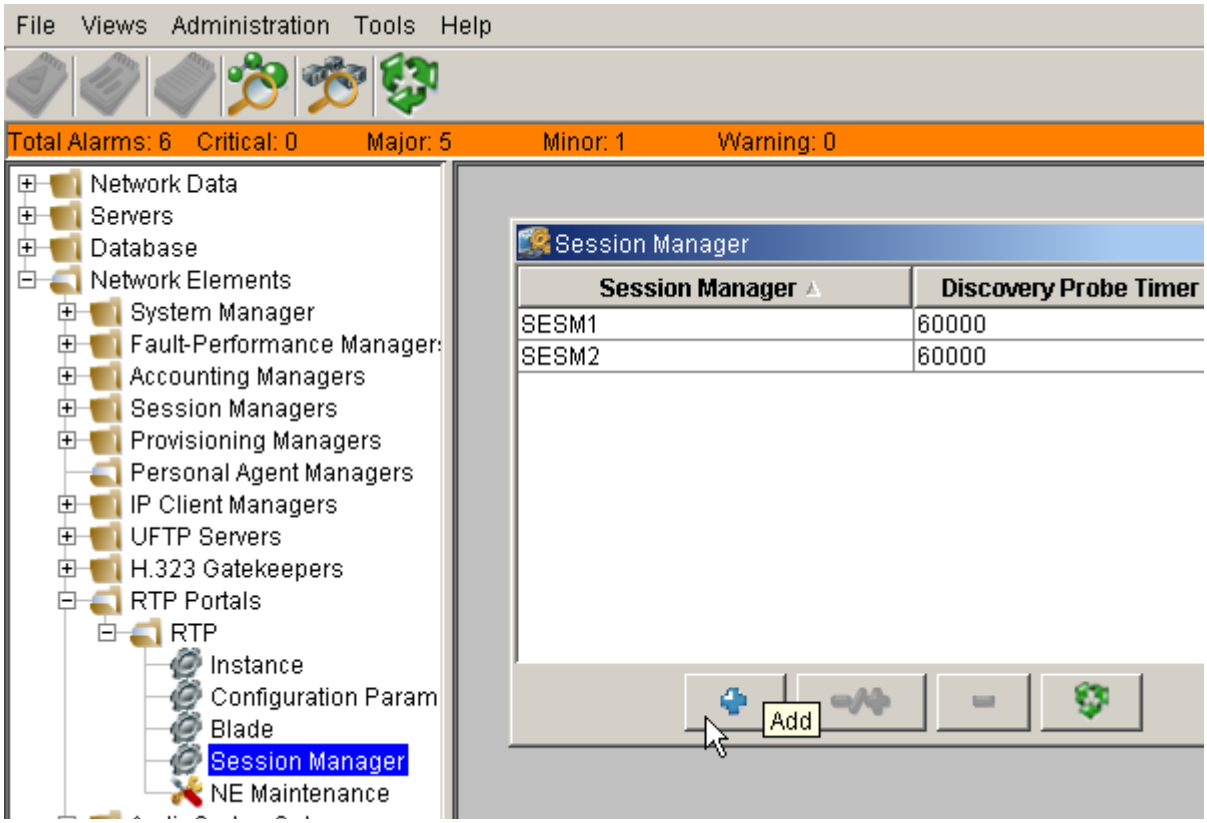
Figure 13 Add Blade



13 Click on the **Add** button, and enter the required information. For single-network configurations, Net1 Media IP is “none”.

14 Select the **Session Manager** option. A new window opens.

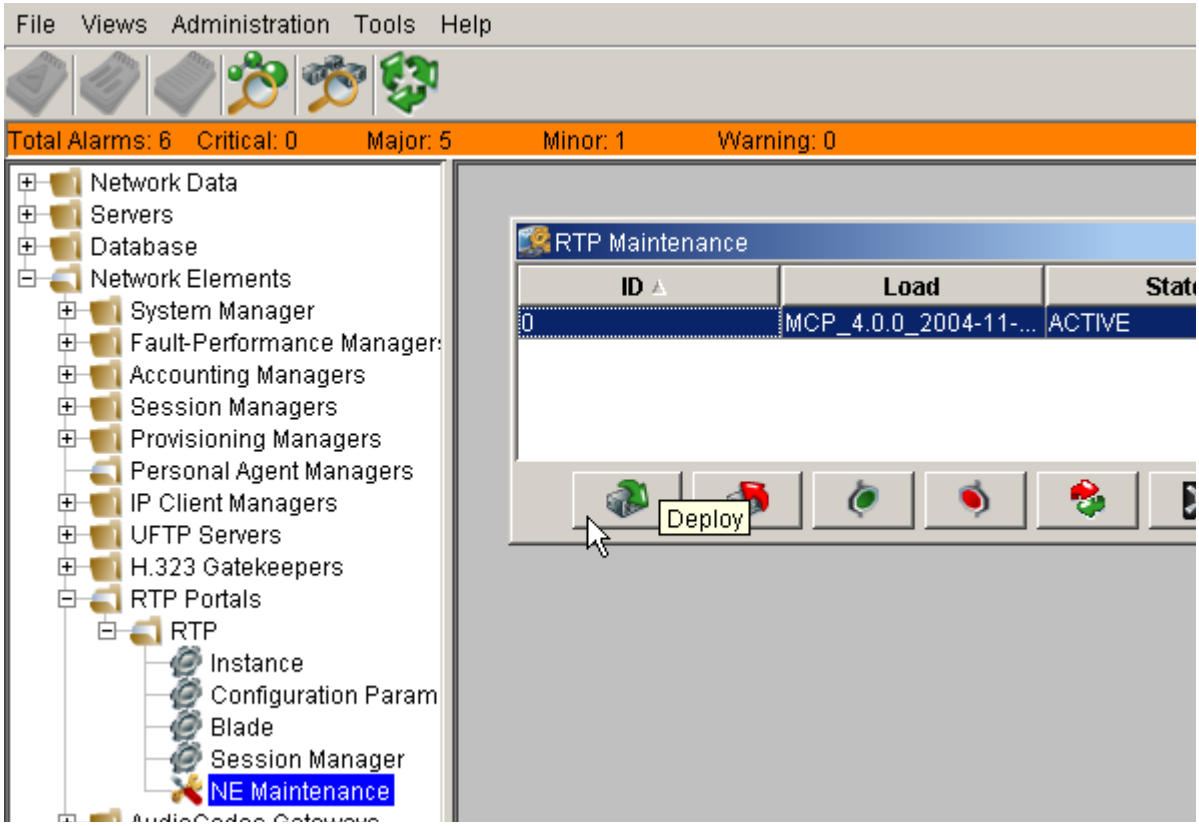
Figure 14 Add Session Manager



15 Click on the **Add** button, and enter the required information. For CS2K deployments a Session Manager presented here equates to a single CS2K Gateway Controller (GWC). Each Gateway Controller in the system that requires an RTP Portal must be configured as a separate Session Manager in the MCS 4.0 GUI. The Session Manager IP address should be that of the active Gateway Controller Unit. Set Discovery Probe Time at 15,000.

16 Select the **NE Maintenance** option. A new window opens.

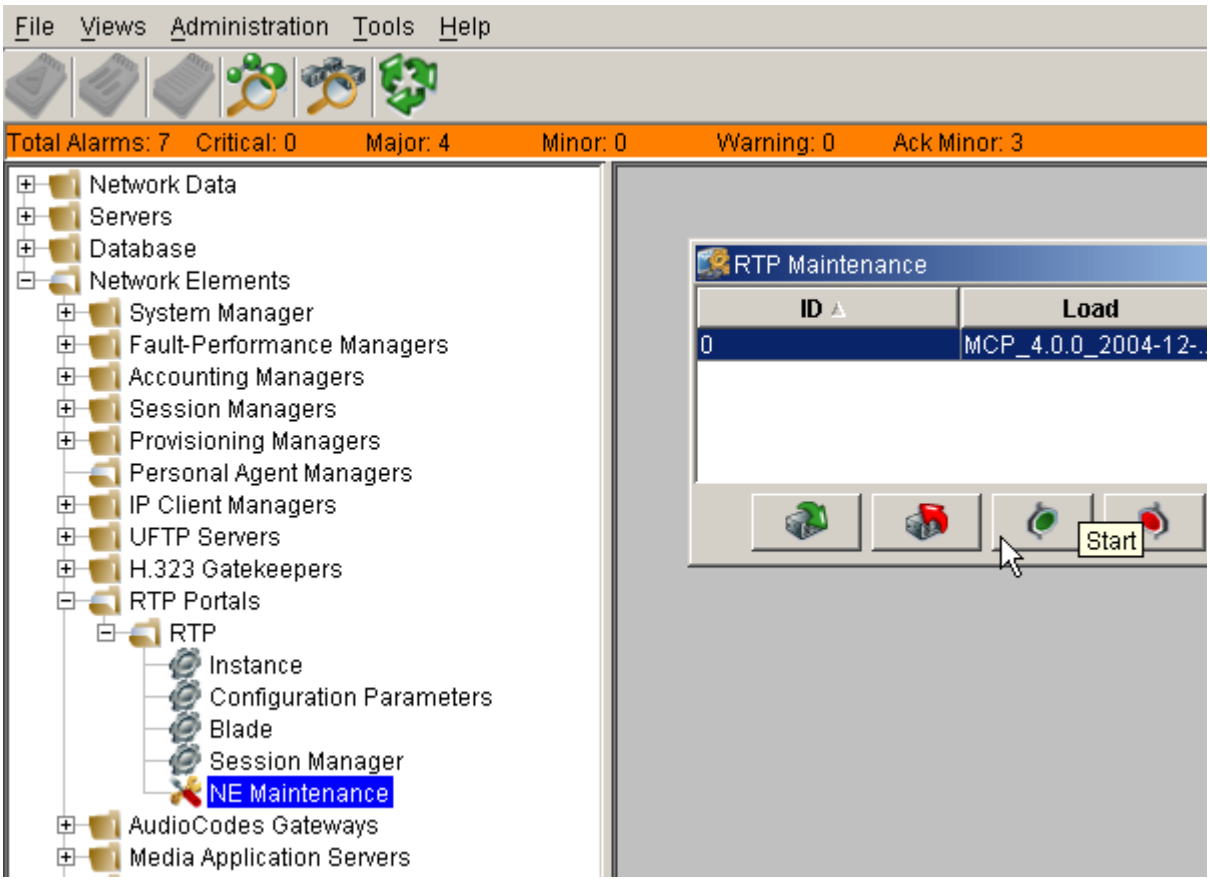
Figure 15 Deploy Portal



17 Select the Portal from the listing, and click on the **Deploy** button.

18 Click on the **Start** button to complete deployment.

Figure 16 Start the Portal



SN06.2 to SN07 RTP Media Portal upgrade

How this chapter is organized

This chapter is organized as follows:

Functional description

This chapter documents upgrade tasks to be performed when upgrading to a full release.

Tools and utilities

Upgrades to the RTP Media Portal are partially performed through the System Management Console. Please refer to *Carrier Voice over IP System Management Console User Guide* for more information.

SN06.2 to SN07 RTP Media Portal upgrade procedures

Operations, administration, and management

The Communication Server 2000 may try to contact the RTP Media Portal while the update is in progress, potentially generating error logs. To minimize impact to service, the RTP Media Portal should first be SHUTDOWN so that it does not accept new service requests. While shutting down, the RTP Media Portal will continue to process established media sessions. These pre-existing media sessions are cleared as the associated calls end. The RTP Media Portal automatically transitions into the LOCKED state when there are no active media sessions present. When this occurs, it is safe to proceed with the upgrade without affecting service.

CAUTION

It is possible to update and reboot one RTP Media Portal in a chassis, while the RTP Media Portal in the other half of the chassis continues to run the previous software. Once one RTP Media Portal is updated, the other RTP Media Portal in the chassis can be shutdown, locked, updated, and rebooted. This rolling upgrade will only impact available capacity and will not cause a service outage.

Upgrading all RTP Media Portals concurrently will cause a service outage.

If an upgrade fails during the initial stages, a rollback to the previous load is performed. A notification of the failure appears within the System Management Console.

If a component upgrade fails after the initial stages of the upgrade, it does not rollback automatically. A dialog box appears in the Management Console stating that the upgrade failed and prompts the administrator to determine whether a rollback should be performed.

The length of time required to complete an upgrade is approximately 30 minutes. While there is no impact to call-processing services, perform updates during low traffic periods to minimize reduced capacity.

The upgrade can be performed at any time following upgrade of the Gateway Controller. Steps include:

- Upgrade Communication Server
  - — Install and commission N240 servers as either non-redundant or redundant.
  - — Install MCP02 and MCP03 software on the N240 Management Server.
  - — Deploy MCP03 Management Server and database on N240 servers.
  - — Freeze configuration changes for the site.
  - — Move system data (backup and restore) from T1400 server to N240 server.
  - — Update the MCP03 database.
  - — Run MCS Conversion Script to configure site as either non-redundant or redundant.
- Upgrade RTP Media Portal as specified in Upgrade tasks on page 95.
- Decommission T1400 system
  - — Unfreeze configuration changes for the MCP03 N240 system.
  - — Shutdown and disassemble the MCP02 T1400 MCS Manager system.

Upgrade tasks

This section provides instruction for a full release RTP Media Portal upgrade.

From the System Management Console and terminal window

1. Shutdown the targeted RTP Media Portal component. For details, please refer to Shutdown the target RTP Media Portal component on page 95.
2. Perform the upgrade. For details, refer to Upgrade the RTP Media Portal component on page 97.
3. Deploy the upgraded RTP Media Portal. For details, refer to Deploy the RTP Media Portal component on page 97.

Shutdown the target RTP Media Portal component

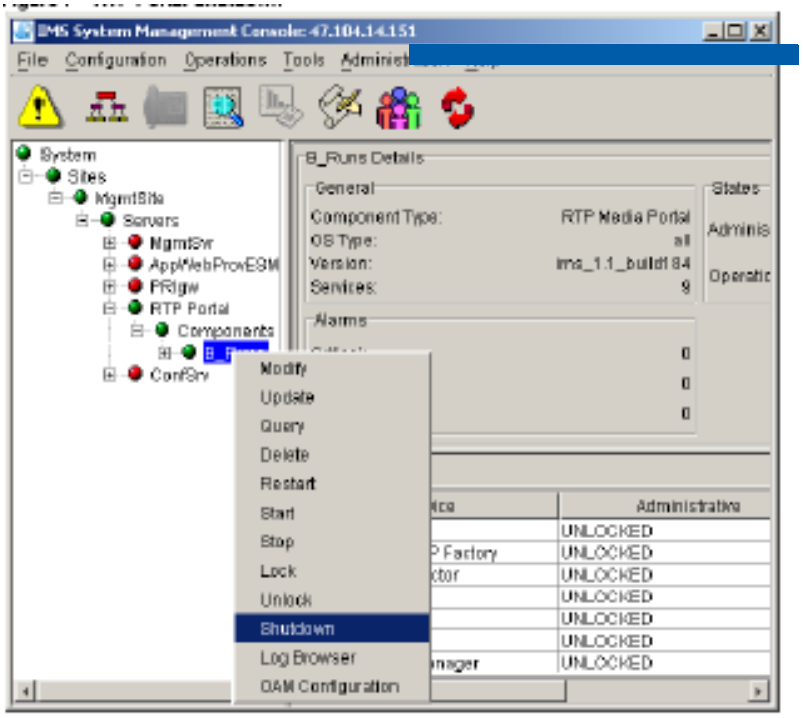
The following procedure describes how to shutdown the target RTP Media Portal component.

From the System Management Console

1 In the System tree, right-click on the target RTP Media Portal component.

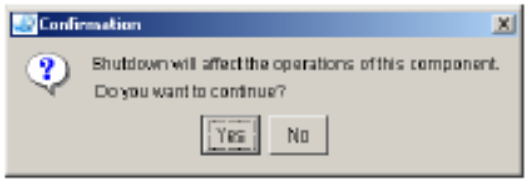
2 From the pop-up menu, select the **Shutdown** command. Users may also choose the shutdown command from the pull-down **Operations** menu.

Figure 1 RTP Portal Shutdown



3 A confirmation window appears. Click on the **Yes** button to continue.

Figure 2 RTP Portal Shutdown confirmation



4 The RTP Media Portal component shuts down gracefully and eventually goes into a LOCKED state when the last active media session ends (as seen in the General Information Area of the System Management Console).

Upgrade the RTP Media Portal component

The following procedure describes how to upgrade the RTP Media Portal load. Use Terminal Server access, or the main console with keyboard and monitor attached.

From a terminal window

1. Log in as **root** on the target RTP Media Portal.
2. Insert the upgrade CD into the associated CD-ROM.
3. Mount the CD.

   mount /dev/cdrom <Enter>
   mnt/cdrom <Enter>
4. Change directory to the top-level directory on the CD.

   cd /mnt/cdrom <Enter>
5. Run the install script.

   ./install <Enter>
6. Change directory.

   cd <Enter>
7. Dismount the CD.

   umount /mnt/cdrom <Enter>
8. Eject the upgrade CD from the CD-ROM.

   eject <Enter>
9. Remove the upgrade CD from the CD-ROM.
10. Repeat step 2 through step 9 for each upgrade CD.
11. Reboot the RTP Media Portal.

    reboot <Enter>

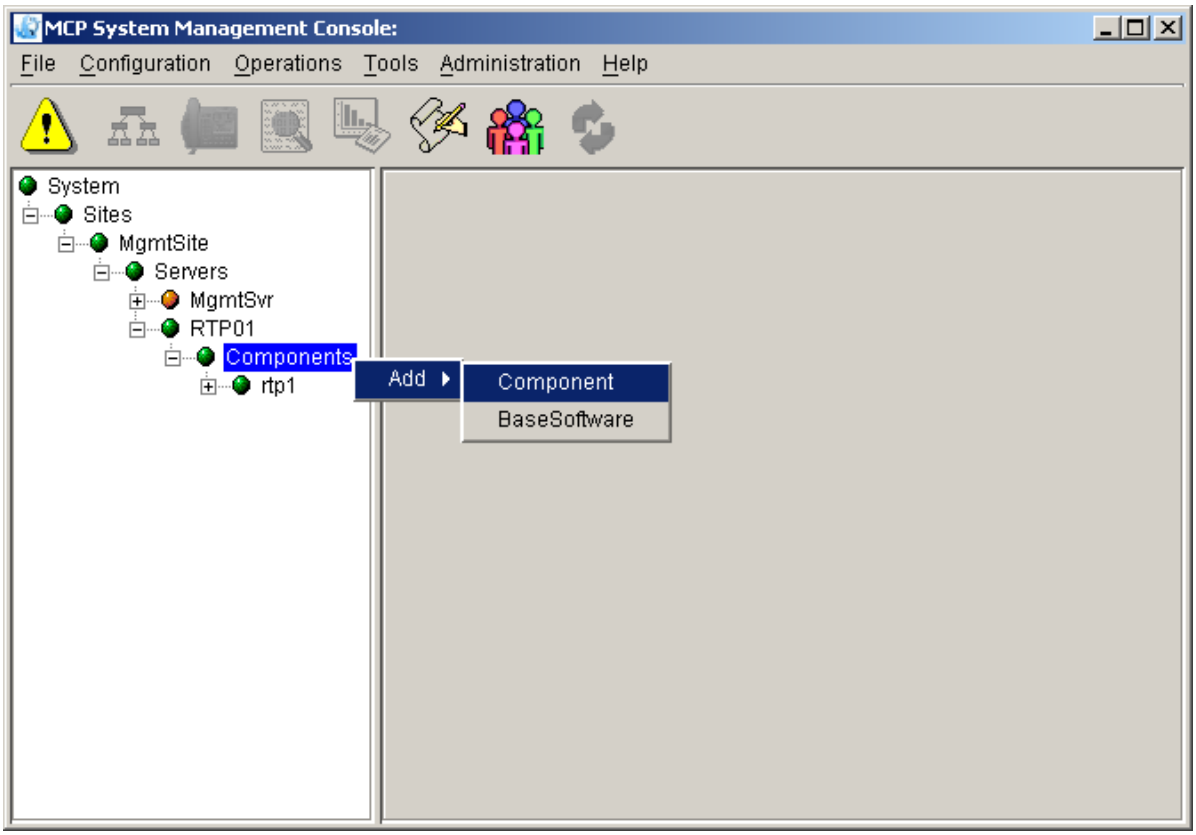
Deploy the RTP Media Portal component

This section provides instruction to deploy the upgraded RTP Media Portal component.

From the System Management Console

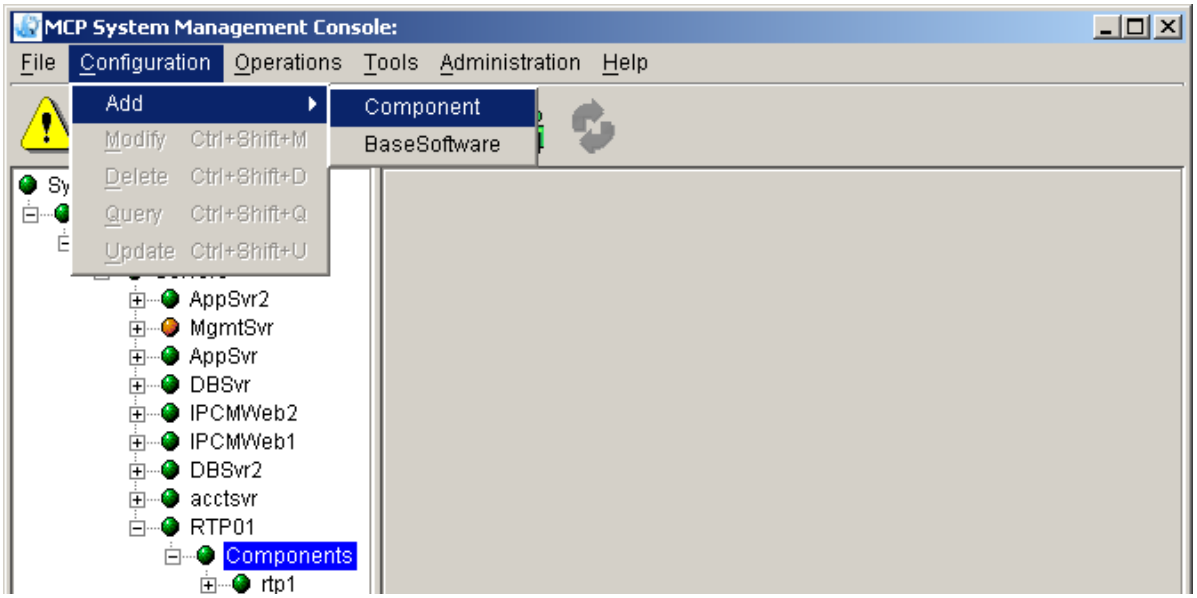
1. In the System tree, right-click **Components** under the appropriate RTP Media Portal server.
2. From the pop-up menu, select the **Add > Component** command.

Figure 3 Add from the pop-up menu



Note, you may also launch the add command from the pull-down Configuration menu.

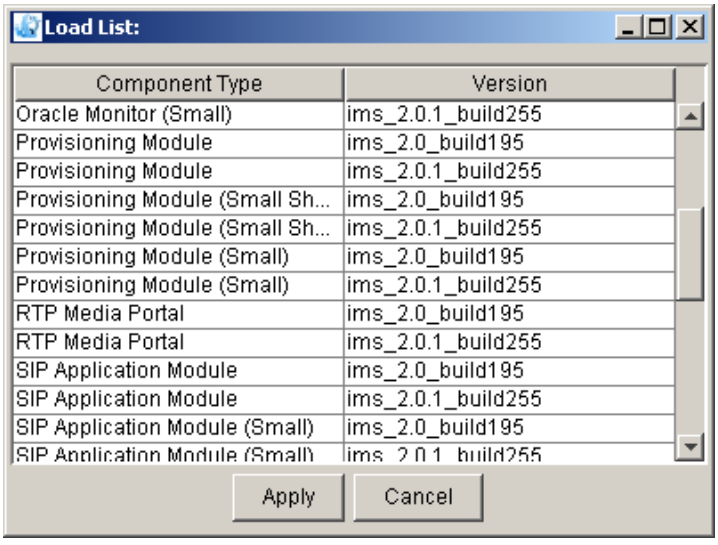
Figure 4 Add from the Configuration menu



After **Add > Component** is selected, you must wait for the load list to retrieve.

3 The Load List window appears with all available component loads (except for those components already deployed to the server).

Figure 5 Load list for adding



4 Select the desired software load version for the RTP Media Portal. Click on the **Apply** button.

5 Enter a label (six characters or less) in the Service Component Name field. This label is the component name that appears in the System tree after deployment. Click on the **Apply** button. A progress screen appears while it deploys

6 When deployment completes, and information dialog message appears to indicate that the action was successful.

SN06.2 to SN08 RPT Media Portal upgrade

To upgrade the RTP Media Portal from SN06.2 to SN08, you must complete the following:

- Upgrade from SN06.2 to SN07. Follow instructions in section *SN06.2 to SN07 RTP Media Portal Upgrade*.
- Upgrade from SN07 to SN08. Follow instructions in section *SN07 to SN08 RTP Media Portal Upgrade*.

RTP Media Portal rollback

In the event there is a problem with the 4.0 upgrade, complete the following steps in order to rollback the system:

- Re-install the previous version of the Portal. For more information refer to the previous version of *RTP Media Portal Basics.*
- Restore the backed up database file. For more information, refer to *Upgrading the CS 2000 T1400/T1405 Servers*.

SN08 to SN07 RTP Media Portal rollback

Prerequisites

This chapter provides instruction for installing a SN07 RTP Media Portal. It is assumed that hardware is already assembled as follows:

- MCPN765 I/O blades are installed in front slots 1-6 for Domain A, and slots 11-16 for Domain B.
- PIMC-0101 765 transition modules are installed in rear slots 1-6 for Domain A, and slots 11-16 for Domain B.
- CPV5370 host blades are installed in front slot 7 for Domain A, and slot 9 for Domain B.
- 5370 transition modules are installed in rear slot 7 for Domain A, and slot 9 for Domain B.
- CPX8216T HSC/BR hot swap controllers are installed in front slot 8 for Domain B, and slot 10 for Domain A.
- Hard drives and CD-ROM drives are installed in the front peripheral bay.
- Floppy drives are installed in rear peripheral bay.

Installing the RTP Media Portal software consists of placing the required packages on the hard drive of the host blade. As the host blade is the only blade in the system that has a hard drive, it is also configured to allow I/O blades to boot and mount their file systems over the network.

The complete base system can be installed in approximately 30 minutes.

IMPORTANT: The installation procedures must be followed separately for each side if two Portals are installed in the same chassis.

The following is required for an installation:

- Chassis and peripherals
  - One Motorola CPX8216T high availability compact PCI which is divided into two domains (A and B), each running independent media portals.
  - One SCSI hard drive per domain, minimum 40Gb.
  - One SCSI CD-ROM per domain.
  - One 3.5” floppy drive per domain.
  - One Motorola CPX8216T HSC/BR hot swap controller per domain.
- Host Blade
  - One Motorola CPV5370 per domain.
  - One Motorola 5370 transition module per domain.
- I/O Blades
  - Up to six MCPN765 per domain.
  - One PIMC-0101 transition module for each MCPN 765.
- Other hardware
  - VT100-compatible terminal device for console access to the host and I/O blades.
- Base software
  - Red Hat 6.2 installation CD (disc 1)
  - RTP Media Portal installation CD
- Required information
  - IP address information: one address per host blade and one or two media addresses per I/O blade.
  - IP address(es) of timeservers.
  - MAC (ethernet) addresses of all I/O blades (two addresses per blade). Addresses can be found on labels affixed to the blade or

from blade NVRAM (use the **niot ;h** command to get the blade Ethernet addresses from the bug prompt).

- RTP Portal chassis number
- Gateway router address, may be different between host(s) and media card(s).
- Netmasks for all assigned IP addresses
- Root password for host(s)
- Password for user “nortel”
- Time zone

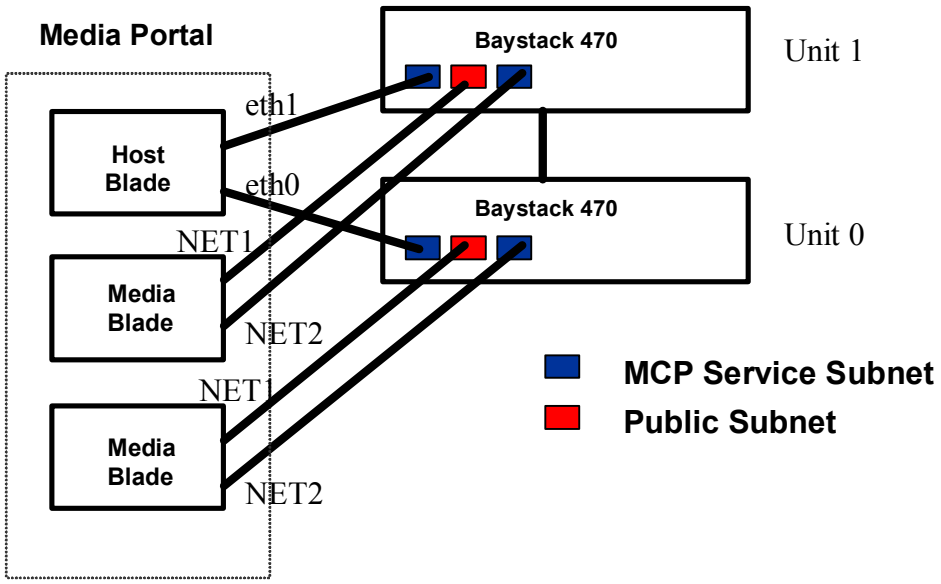
Network deployment

It is recommended to deploy the RTP Medial Portal in a dual-network configuration.

Dual-network deployment

For the dual-network configurations, the host is connected to the MCP Service Network. The Media Card has one interface connected to the MCP Service Network (NET2) and one to the other network (NET1), either a public network or a subnet of the MCP Service Network. The two interfaces on the host are used in an active, standby mode and there is no interface redundancy on the media cards as each connects to a separate network. This configuration is depicted in Figure 1 on page 107.

Figure 1 Dual-network deployment



The below table details the usage of the physical port for dual-network deployment.

Label	BIOS device number	Linux interface name	Usage
MCPN 765 I/O Card Ethernet port usage			
NET1	CLUN 0/DLUN 0	eth0	Public
NET2	CLUN 13/DLUN 0	eth1	MCS Service
CPV5370 Host Card Ethernet port usage			
1	N/A	eth0	MCS Service
2	N/A	eth1	MCS Service

Failure to use the ports as described will result in a non-operational RTP Media Portal.

Installing RTP Media Portal

This section outlines steps to install the RTP Media Portal.

From the terminal console

1. Establish BIOS settings for the CPV5370 Host Card. For details, refer to BIOS configuration of the CPV5370 Host Card on page 108.
2. Install the base operating system, Red Hat 6.2. For details, refer to Installing the base Red Hat system on page 111 and Partitioning the hard drive on page 112
3. Complete the installation. For details, refer to Completing the installation on page 114.
4. Install the RTP Media Portal packages. For details refer to Installing the RTP Media Portal packages on page 119.
5. Configure the Network Time Protocol. For details, refer to Configuring Network Time Protocol on page 121.

BIOS configuration of the CPV5370 Host Card

This procedure provides instruction for BIOS settings. While many of the factory default settings are acceptable, a few require changes. If you are not certain the factory settings are in effect, reset all values to default from within the BIOS set up under the **Exit** menu.

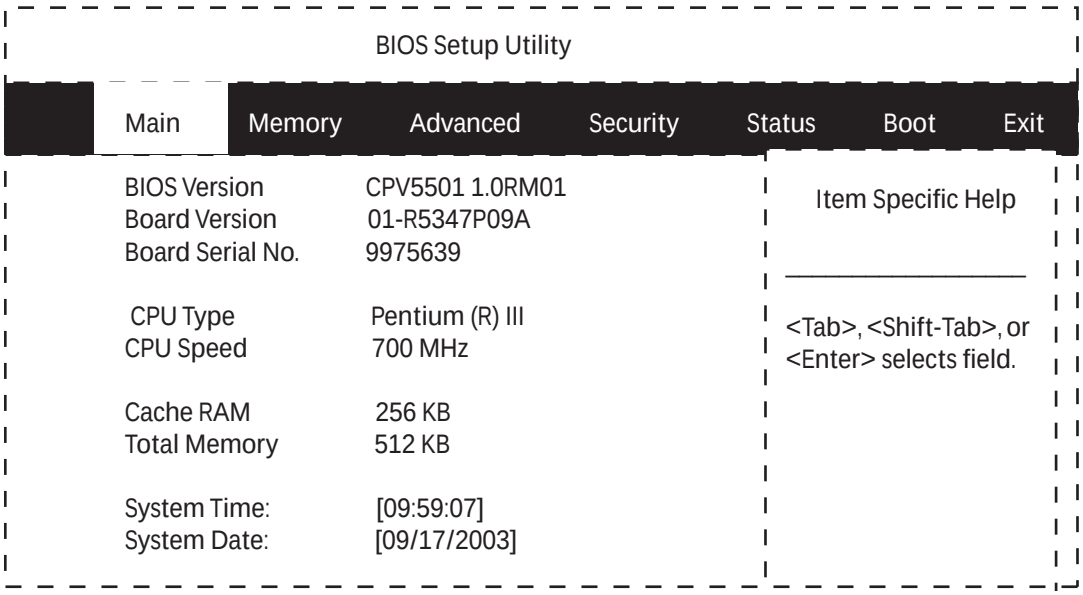
From the terminal console

1. Create a console connection to COM1 (A) on the front panel of the host CPU card.

   A connection to COM1 is only used during the initial power up procedures. Once the BIOS configuration is set, the user must remove the serial cable from COM1 and connect the Terminal Server to cable COM2 on the transition module.
2. As the system is powering on, hold down the **F2** key to enter BIOS set up. The CPV5370 Card ships from the factory with serial port settings 19,200 baud, 8/n/1.

   If you do not see output on screen, it may be necessary to reseat the CPV5370 card and press the Reset button on the front panel.

Figure 2 BIOS Setup Utility screen



3 From the **Advanced** menu, move to **IDE Configuration** and press **Enter**.

4 Verify, or change, the values on screen to match the values listed below. Leave all other values as default.

```
Local Bus IDE adapter: [Disabled]
Large Disk Access Mode: [DOS]
SMART Device Monitoring: [Disabled]
Primary Master: [NONE]
Primary Slave: [NONE]
Secondary Master: [NONE]
Secondary Slave: [NONE]
```

5 Press **Esc** twice to return to the **Advanced** menu.

6 Move to **PCI Configuration** and press **Enter**.

7 Verify, or change, the values on screen to match the values listed below.

```
Default Primary Video Adapter: [AGP]
On-Card Ethernet 1: [Enabled]
Ethernet 1 Connection: [Rear]
Ethernet 1 Option ROM: [Disabled]
On-Card Ethernet 2: [Enabled]
Ethernet 2 Connection: [Rear]
Ethernet 2 Option ROM: [Disabled]
```

8 Move to the **HA configuration** sub-menu and press **Enter**.

9 Set the **HA Config** value to **Enabled**. Also, set the Domain that is being configured to **Enable**, and **Disable** for the other domain. CPU in slot 7 is Domain A, and CPU in slot 9 is Domain B.

Example for Domain A, the Host Card in slot 7:

```
HA Config [Enabled]
Domain A [Enabled]
Domain B [Disabled]
```

10 Press **Esc** twice to return to the **Advanced** menu.

11 Move to **Remote Console** and press **Enter**.

12 Verify, or change, the values on screen to match the values listed below. Leave all other values as default.

```
COM Port: [COM B]
Serial port B: [Enabled]
Base I/O address: [2F8]
Interrupt: [IRQ 3]
Baud Rate: [9600]
Console Type: [VT100]
Flow Control: [None]
Screen Lines: [25]
Active After Post: [On]
```

13 Press **Esc** twice to return to the **Advanced** menu.

14 From the **Boot** menu, move the cursor to **Boot Device Priority** and press **Enter**.

15 Ensure the system boots in the following order:

```
8XX SCSI CD-ROM LSI Logic
+Hard Drive
! +Removable Devices
! ATAPI CD-ROM Drive
! Legacy Network Boot
```

Place an exclamation mark (!) beside the appropriate devices to disable them.

16 Press the **Esc** key to return to the main menu.

17 Move to the **Security** menu to set control access to the BIOS settings. Unauthorized BIOS access enables any Linux security to be circumvented.

18 Set up the BIOS supervisor password. Ensure the password on Boot option is disabled.

19 Move to the **Exit** menu to save changes and exit the BIOS set up. The system will reboot.

20 While the system is rebooting, quickly change the console connection from COM1 to COM2. Use the escape sequence **<Esc><Shift>OQ** to enter the BIOS set up screen again.

If you do not see output on the terminal, make sure the terminal is set to **9600/8/n/1** and reset the CPV5370 card to try again.

21 When prompted, enter the supervisor password to ensure the password was correctly set and is using COM2 as the console port.

22 Insert the Red Hat 6.2 installation CD in the CD-ROM drive for the domain (the top CD-ROM drive is Domain A).

23 Press the **Esc** key to exit BIOS without making any changes. The system will reboot.

24 Remove the serial cable from COM2, and connect the serial cable from the Terminal Server to that port.

Installing the base Red Hat system

The RTP Media Portal uses the operating system Red Hat 6.2.

The installation script provides a graphic user interface (GUI). Use the **Next** or **Done** keys to move to the next screen, the **Tab** key to move between items/buttons, the **Space** key to select and deselect items, the **Enter** key to expand items for editing, and **arrow keys** for moving between items in a list.

If it is necessary to re-enter the BIOS from the Terminal Server, use the Escape key sequence **<Esc><Shift>OQ** .

From the terminal server

1 Establish a terminal session to the Host CPU through the terminal server.

2 After the system boots from the Red Hat CD, the Red Hat installation menu appears. Type the following:
text console=ttyS1,9600n8 <Enter>

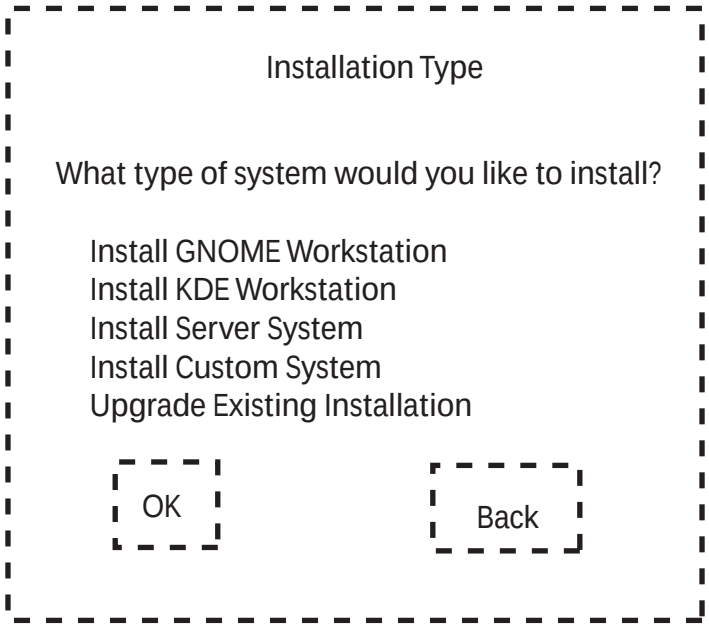
IMPORTANT: If the first character is not quickly typed, the Red Hat installation script will use the default automatic option and begin installation.

If entry is not typed correctly, reset the card using the reset button in the front of the 5370 card.

3 Select **English** for the Language Selection, then select **OK**.

4 In the Red Hat welcome screen, Choose the **Install Custom System** installation.

Figure 3 Red Hat: Installation Type screen



5 For **Bad Partition Table**, select **Initialize**.

Partitioning the hard drive

The following includes instruction to partition the hard drive.

From the terminal server

1 Press **w** and press **Enter** to save changes and exit.

2 Select **Done** and press **Enter** to continue.

3 At the **Disk Setup** screen, select the individual partitions and press **Tab** to move to the **Edit** button. Press **Enter**.

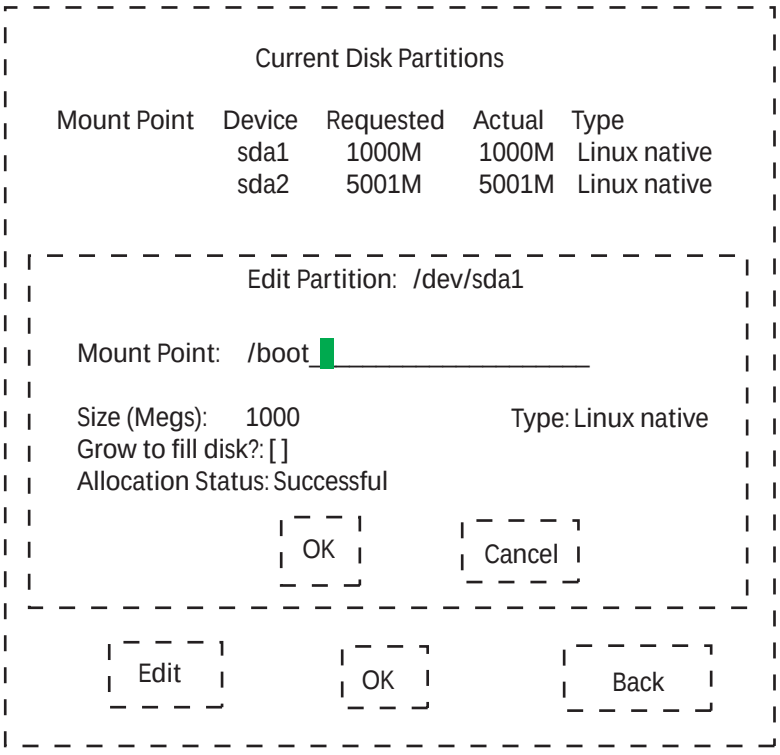
4 Type in the mountpoints. The highlighted line indicates the current cursor position. Press **Enter**, input the mountpoint in the text box, and press **Enter** again.

```
Partition 1: mountpoint = /boot <Enter>
Partition 2: mountpoint = / <Enter>
Partition 3: /swap <Enter>
Partition 5: mountpoint = /var <Enter>
Partition 6: mountpoint = /usr <Enter>
Partition 7: mountpoint = /IMS <Enter>
```

It is not necessary to enter the mountpoint for the swap partition, as this occurs automatically when this partition is designated as a swap partition.

Repeat for all partitions as necessary. Select **OK** when finished.

Figure 4 Red Hat: Mountpoints

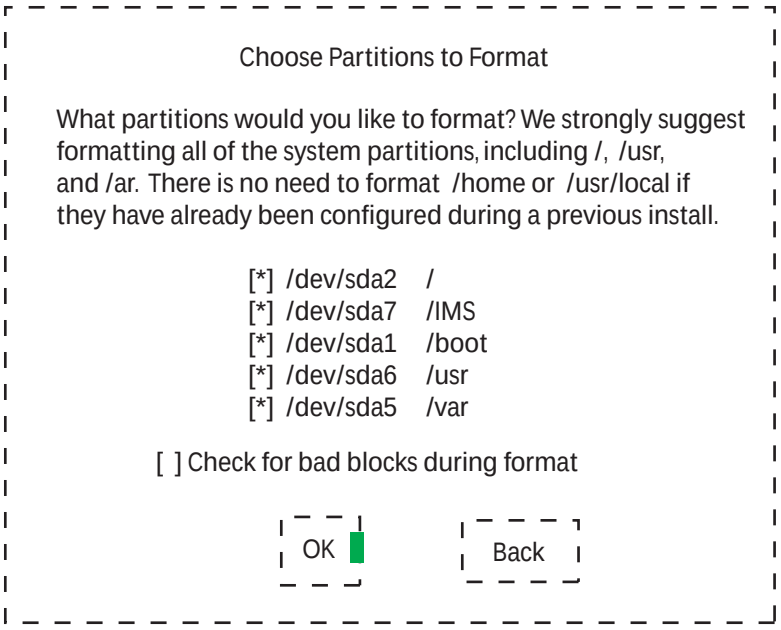


5 In the **Choose Partitions to be Formatted** screen, ensure all partitions are selected and the **Check for bad blocks** option is NOT selected.

```
[*] /dev/sda2   /
[*] /dev/sda7   /IMS
[*] /dev/sda1   /boot
[*] /dev/sda6   /usr
[*] /dev/sda5    /var
```

Press the **Tab** key twice to position the cursor on the **OK** button, and press the **Enter** key.

Figure 5 Red Hat: Formatting partitions



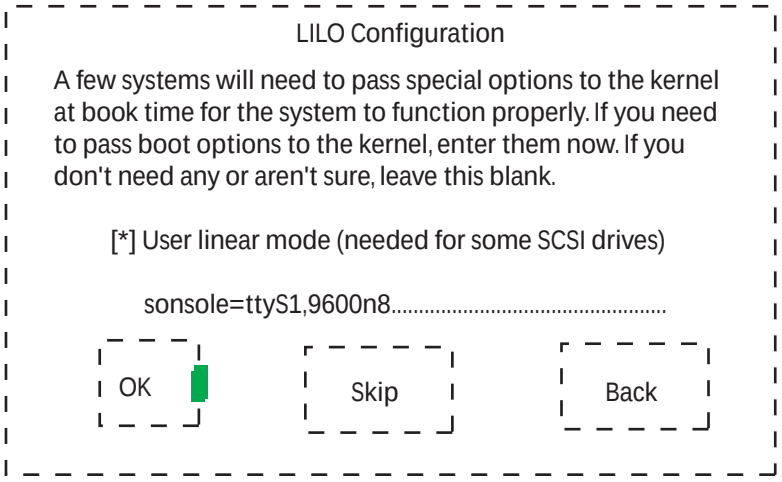
Completing the installation

The following procedure includes instructions for completing the installation.

From the terminal server

1. The LILO Configuration screen appears. Ensure the **User linear mode (needed for some SCSI drives)** is selected.
2. Type the boot arguments for LILO as follows:
   console=ttyS1,9600n8 <Enter>

Figure 6 Red Hat: LILO Configuration



Select **OK** when finished.

3 Ensure **/dev/sda** for the location to install LILO is selected, and select **OK** to continue.

4 Select **OK** to accept the default selection for the partition to boot the Linux OS.

5 The Host Configuration screen will appear. Type in the host name of the RTP Media Portal. Select **OK** when finished.

6 In the Network Configuration screen, de-select the **bootp/DHCP** check box.

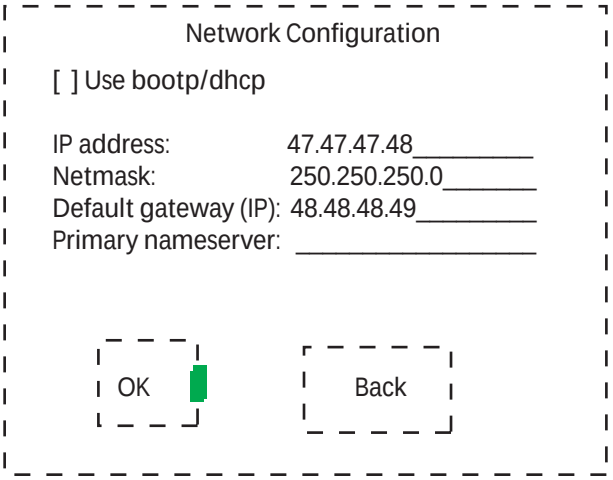
Enter nameserver IP addresses if they are available. If you enter nameserver addresses, ENSURE THEY ARE CORRECT. The RTP Media Portal will not function correctly if unreachable or otherwise incorrect nameserver IP addresses are used. If you do not have nameserver IP addresses, leave this field empty.

```
[ ] Use bootp/dhcp

IP address:             <eth0 IP of Host Card>
Netmask:                <Host Card Netmask>
Default gateway (IP):   <Default Gateway>
Primary nameserver:
```

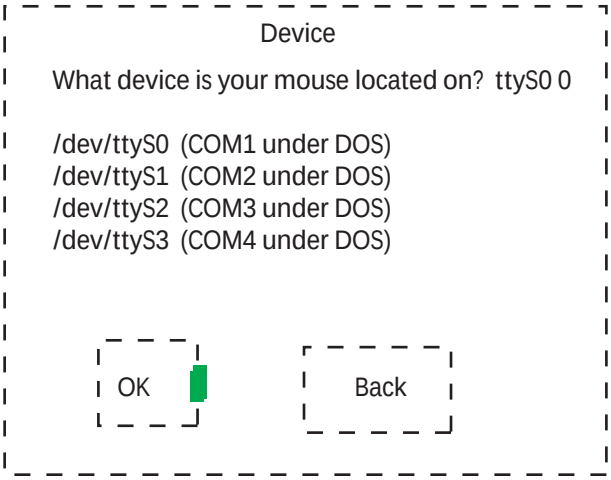
Select **OK** to continue.

Figure 7 Red Hat: Network Configuration screen



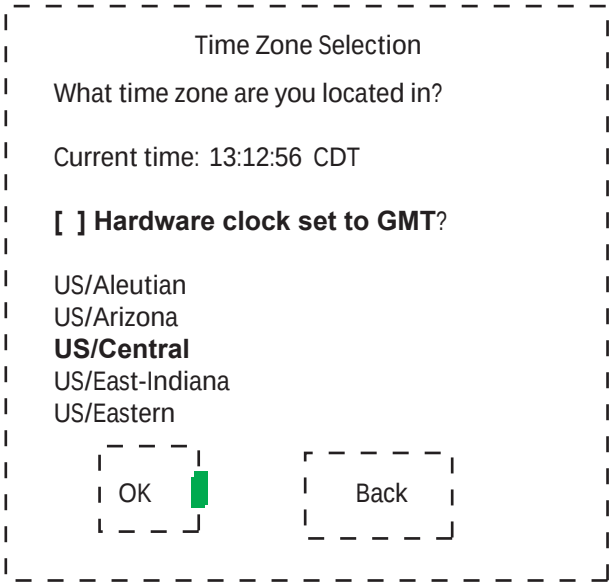
7 In the Device settings screen, accept the default setting and select **OK** to continue.

Figure 8 Red Hat: Device settings screen



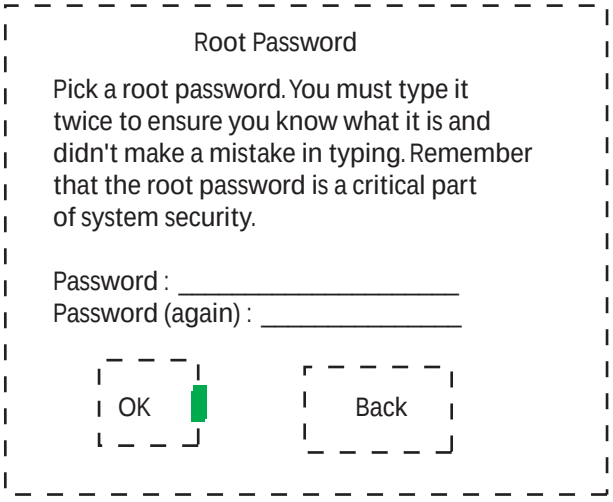
8 In the Time Zone Selection screen, select the appropriate local time zone and select **OK**.

Figure 9 Red Hat: Time Zone Selection screen



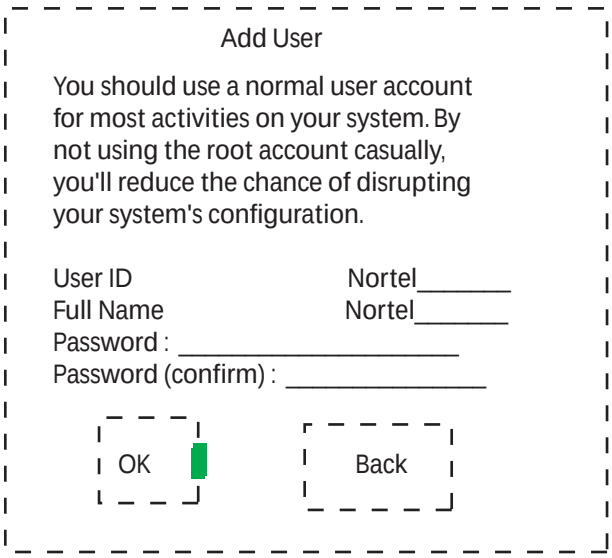
9 The next screen sets the root password. When prompted, enter the appropriate root password. Retype the password for confirmation and select **OK** to continue.

Figure 10 Red Hat: Root Password screen



10 The Add User screen appears. Create a “nortel” user account with password. Retype the password for confirmation and select **OK** to continue.

Figure 11 Red Hat: Add User screen



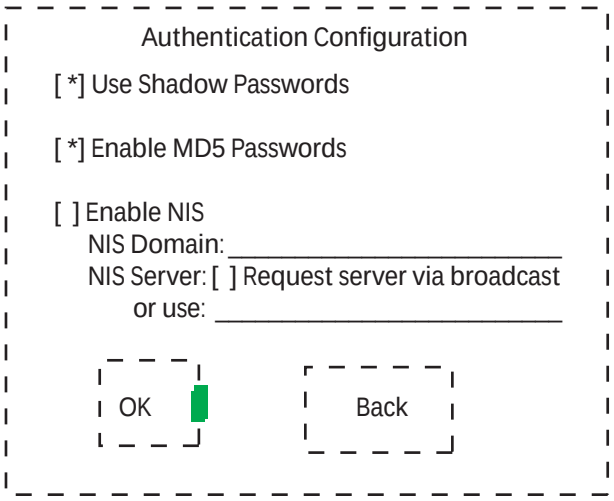
11 In the Authentication Configuration screen, verify the **Use Shadow Password** and **Enable MD5 password** check boxes are selected. Select **OK** to continue.

```
[*] Use Shadow Password

[*] Enable MD5 Password

[ ] Enable NIM
  NIS Domain:
  NIS Server: [ ] Request server via broadcast
       or use:
```

Figure 12 Red Hat: Authentication Configuration screen



12 Select the software packages to install the following.

- Networked Workstation
- NFS Server
- Anonymous FTP Server
- Utilities

De-select packages not included in this list. Select **OK** to continue.

13 Select **No** when asked if a boot disk is to be created.

14 Select **OK** to begin the installation. Installation will require approximately 10 minutes to complete.

Once completed, the system will prompt you to reboot and remove the installation CD from the CD-ROM.

IMPORTANT: Remove the CD before the POST boot sequence is complete, otherwise the base installation script will begin again. If this happens, press the reset button on the front panel of the Host CPU Card to reboot the system again.

Installing the RTP Media Portal packages

Once the Red Hat installation is complete, the RTP Media Portal and HA packages can be installed from the second CD.

From the terminal server

1 After the system reboots, the LILO prompt is displayed. Press **Tab** to halt the LILO boot process.

2 Insert the RTP Portal Install CD into the CD-ROM, and reboot the system by pressing the Reset button on the front of the Host CPU Card.

3 The system will reboot from the CD and begin executing the installation scripts.

4 Press **Tab** when the LILO prompt appears. Type **install-serial** at the prompt to begin the installation.

5 The system prompts for the following information.

```
Host CPU slot number: [7 or 9]
RTP Portal chassis number: [1, 2, 3,...]
Timeserver IP address:
Permanent system console type: s
Blade MAC addresses:
```

The chassis number is used to configure both the host and the Media Blades. They must be consistent. Also, the chassis number is used to construct a virtual address of the form 192.168.<chassis>.<slot>. This address MUST be unique on the MCP Service Network, so it is necessary for the chassis number to be selected based on its use to create this address.

Timeserver IP address(es) is generally the service logical IP of the Management Server.

If there is an error in the input, type **n** in the confirmation screen to re-enter the values. Otherwise, type **y** to continue.

6 When prompted, provide the MAC addresses for each of the I/O cards in the Domain. If there is no I/O card present in a slot, press **Enter** to skip to the next slot entry. Select **OK** to continue.

7 Installation will begin, requiring approximately 5-10 minutes. Do not touch the keyboard of the system until installation is complete.

8 Press **Enter** to continue. The system will reboot.

9 When the LILO prompt appears, press the **Tab** key to halt the process.

10 Remove the RTP Portal install CD from the CD-ROM, and reboot the system by pressing the Reset button on the front panel of the Host CPU card.

11 After the system reboots, use the escape sequence **<Esc><Shift>OQ** to return to BIOS set up. Remove everything from the boot device list except the hard drive (for security reasons).

12 Move to the **Exit** menu to save changes and exit the BIOS set up. The system will reboot.

13 After the system reboots, press the **Enter** key to boot the default image.

14 After booting, the login prompt will appear on screen.

Configuring Network Time Protocol

This section includes instruction for synchronizing the RTP Portal clock to the master clocks. This is performed automatically during installation if the user entered a Timeserver IP address in Installing the RTP Media Portal packages on page 119. Only modify the **ntp.conf** file if the timeserver address(es) change or if they were not entered at install time for some reason.

From the terminal server

1 Establish a serial terminal connection to the Host CPU card, and log in the system as **root**.

2 Create a new **ntp.conf** file in the **/etc** directory.

vi /etc/ntp.cont <Enter>

3 Add the following lines in the text.

<Enter><Enter>server <Machine Logical IP RTP EM (Mgmt/Db Combo) Server>
driftfile /etc/ntp/ntp.drift <Enter>

4 Save and exit the editor.

5 Verify the file was correctly saved.

more /etc/ntp.conf <Enter>

The display should match the contents entered in the previous step. Note the clock on the RTP Portal must be set to within one hour of the time set on the management servers, or Network Time Protocol will not be able to adjust the time. If the clocks differ by more than one hour, set the time manually.

date <MMDDHHMM> <Enter>

6 Exit **root**.

exit <Enter>

Installing MCPN765 cards

The following procedures outline instructions for adding MCPN765 I/O Cards in RTP Portal (Domain A). To add new I/O cards to Domain B, repeat these procedures.

From a terminal device and the System Management Console

1 Set the MCPN765 I/O card. For more information, refer to Setting up the MCPN765 I/O Card on page 122.

2 Configure the MCPN765 card. For more information, refer to Configuring the MCPN765 I/O Card on page 125.

Setting up the MCPN765 I/O Card

A terminal device (such as a dumb terminal, or PC COM port plus terminal software) is required to change the NVRAM settings on the MCPN765 I/O blade. The 765 serial port uses 9600/8/N/1 settings. Use the port labeled **COM1** on the rear transition module. A serial cable is required to connect to the I/O blade, as a specialized serial cable will not work.

From a terminal device

1 Once the blade and transition module has been physically installed in the chassis, connect the specialized serial cable to the COM1 port at the bottom of the transition module.

2 Press the reset button on the front of the MCPN765 card to reboot the card.

3 Press the **Esc** key to abort the re-boot process.

4 Set and enable the real time clock on the blade.

set <MMDDYYHHMM> <Enter>

5 At the Bug prompt, display the MAC address for the card.

niot ;h <Enter>

6 Record the MAC address for CLUN 0/DLUN 0 (NET1), and CLUN13/DLUN 0 (NET2).

CLUN 0/DLUM 0 (NET1): _____

CLUN 13/DLUN 0 (NET2): _____

7 Type **env** to verify, and change as necessary, BIOS settings on the I/O Card. Ensure they match the settings shown below.

Note the entries may appear differently depending on the version of BIOS loaded on each card. If an entry appears that is not described below, accept the default.

```
PPC6-Bug>env
Bug, AST or System environment [B/A/S] = B?
Maximum Memory Usage (Mb, 0=AUTO) = 0?
Field Service Menu Enable [Y/N] = N?
Probe System for Supported I/O Controllers [Y/N] =
Y?
```

```
Auto-Initialize of NVRAM Header Enable [Y/N] = Y?
Network PReP-Boot Mode Enable [Y/N] = Y?
SCSI Bus Reset on Debugger Startup [Y/N] = N?
Primary SCSI Bus Negotiations Type [A/S/N] = A?
Primary SCSI Data Bus Width [W/N] = N?
Secondary SCSI Identifier = "07"?
NVRAM Boot List (GEV.fw-boot-path) Boot Enable [Y/N]
= N?
NVRAM Boot List (GEV.fw-boot-path) Boot at power-up
only [Y/N] = N?
NVRAM Boot List (GEV.fw-boot-path) Boot Abort Delay
= 5?
Auto Boot Enable [Y/N] = N?
Auto Boot at power-up only [Y/N] = N?
Auto Boot Scan Enable [Y/N] = Y?
Auto Boot Scan Device Type List =
FDISK/CDROM/TAPE/HDISK/?
Auto Boot Controller LUN = 00?
Auto Boot Device LUN = 00?
Auto Boot Partition Number = 00?
Auto Boot Abort Delay = 7?
Auto Boot Default String [NULL for an empty string]
= ?
ROM Boot Enable [Y/N] = N?
ROM Boot at power-up only [Y/N] = Y?
ROM Boot Abort Delay = 5?
ROM Boot Direct Starting Address = FFF00000?
ROM Boot Direct Ending Address = FFFFFFFC?
Network Auto Boot Enable [Y/N] = Y?
Network Auto Boot at power-up only [Y/N] = N?
Network Auto Boot Controller LUN = 13?
Network Auto Boot Failover Controller LUN = 00?
Network Auto Boot Device LUN = 00?
Network Auto Boot Abort Delay = 5?
Network Auto Boot Configuration Parameters Offset
(NVRAM) = 00001000?
Watchdog prior status ignored at autoboot [Y/N] = Y?
Watchdog shutdown at board reset [Y/N] = N?
Reset Ethernet chip after file transfer [Y/N] = N?
Stop Auto Boot after selftest failure [Y/N] = N?
Memory Size Enable [Y/N] = Y?
Memory Size Starting Address = 00000000?
Memory Size Ending Address = 04000000?
DRAM Speed in NANO Seconds = 8?
ROM Bank A Access Speed (ns) = 90?
ROM Bank B Access Speed (ns) = 120?
DRAM Parity Enable [On-Detection/Always/Never -
```

```
O/A/N] = O?
L2Cache Parity Enable [On-Detection/Always/Never -
O/A/N] = O?
PCI Interrupts Route Control Registers (PIRQ0/1/2/3)
= 0A0B0E0F?
Serial Startup Code Master Enable [Y/N] = N?
Serial Startup Code LF Enable [Y/N] = N?
Firmware Command Buffer Enable [Y/N] = N?
Firmware Command Buffer Delay = 5?
Firmware Command Buffer : <Enter>
['NULL' terminates entry]?
Update Non-Volatile RAM (Y/N)? y
Reset Local System (CPU) (Y/N)? n
```

8 At the prompt, type **niot** to access the Network boot settings.

```
PPC6-Bug>niot
Controller LUN =00? 13
Device LUN =00?
Node Control Memory Address =03E1D8A0?
Client IP Address =0.0.0.0? 192.168.<chassis #>.<slot #>
Server IP Address =0.0.0.0? 192.168.<chassis #>.<hostcard #>
Subnet IP Address Mask =255.255.255.0?
Broadcast IP Address=255.255.255.255? 192.168.<cage
#>.255
Gateway IP Address =0.0.0.0?
Boot File Name ("NULL" for None) =?
/tftpboot/bladeRunner
Argument File Name ("NULL" for None) =?
Boot File Load Address =001F0000?
Boot File Execution Address =001F0000?
Boot File Execution Delay =00000000? 00000005
Boot File Length =00000000?
Boot File Byte Offset =00000000?
BOOTP/RARP Request Retry =00? 50
TFTP/ARP Request Retry =00? 50
Hardware error retry attempts =00?
Trace Character Buffer Address =00000000?
BOOTP/RARP Request Control: Always/When-Needed
(A/W)=W?
BOOTP/RARP Reply Update Control: Yes/No (Y/N) =Y?
Update Non-Volatile RAM (Y/N)? y
```

9 At the prompt, type **reset** to reboot the network once it completes the necessary self-tests.

```
PPC6-Bug>reset
Cold/Warm Reset [C,W] = C?
```

```
Execute Local SCSI Bus Reset [Y,N] = N?
Execute Local (CPU) Reset [Y,N] = N? y
```

10 Repeat this procedure for all I/O cards in the Domain. The Host Card IP address and the Broadcast IP address should be the same between all I/O Cards.

11 Unplug the console connection from the last I/O card.

12 Log in to the system as **root**.

13 Edit the **/etc/bladeEtherAddrs** file to change the MAC addresses for each of the new I/O cards in the system. It is only necessary to change the entries for slots that contain a card. If a slot is empty, or contains something other than a card, leave the corresponding entry as is.

vi /etc/bladeEtherAddrs <Enter>

For example, if the I/O card was added in slot 3, enter the new MAC addresses on the appropriate line as shown below.

```
##############################################
#MAC addresses for all blades in the system
#
#Format: <slot>: <private NET2 MAC>: <public NET1
MAC>
##############################################
1:FF00FF00FF00:FF00FF00FF00
2:FF00FF00FF00:FF00FF00FF00
3:<New NET2 MAC Addr.>:<New NET1 MAC Addr.>
4:FF00FF00FF00:FF00FF00FF00
5:FF00FF00FF00:FF00FF00FF00
6:FF00FF00FF00:FF00FF00FF00
11:0001af04666a:0001af04666b
12:0001af04a022:0001af04a023
13:0001af000709:0001af00070a
14:0001af040390:0001af040391
15::
16::
```

14 Save the file and exit the editor.

15 Exit root.

exit <Enter>

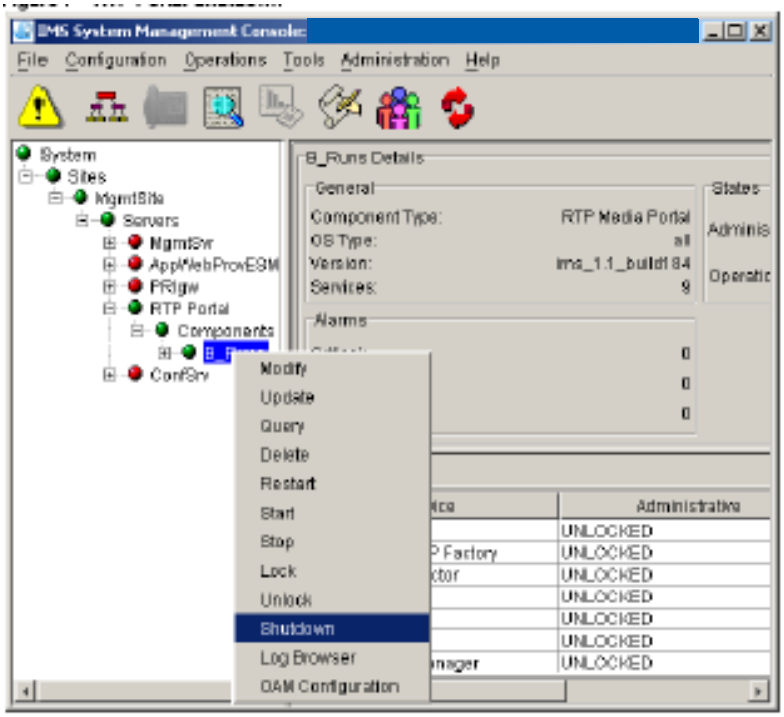
Configuring the MCPN765 I/O Card

It is recommended the following procedure be completed during maintenance hours as it will require the RTP Media Portal to reboot, and be out of service for approximately 15-20 minutes.

From the System Management Console

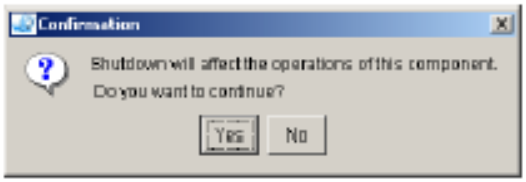
1 Expand the RTP Portal options, right-click on RTP Portal to select **Shutdown**.

Figure 13 RTP Portal Shutdown



2 A confirmation window appears. Click on the **Yes** button to continue.

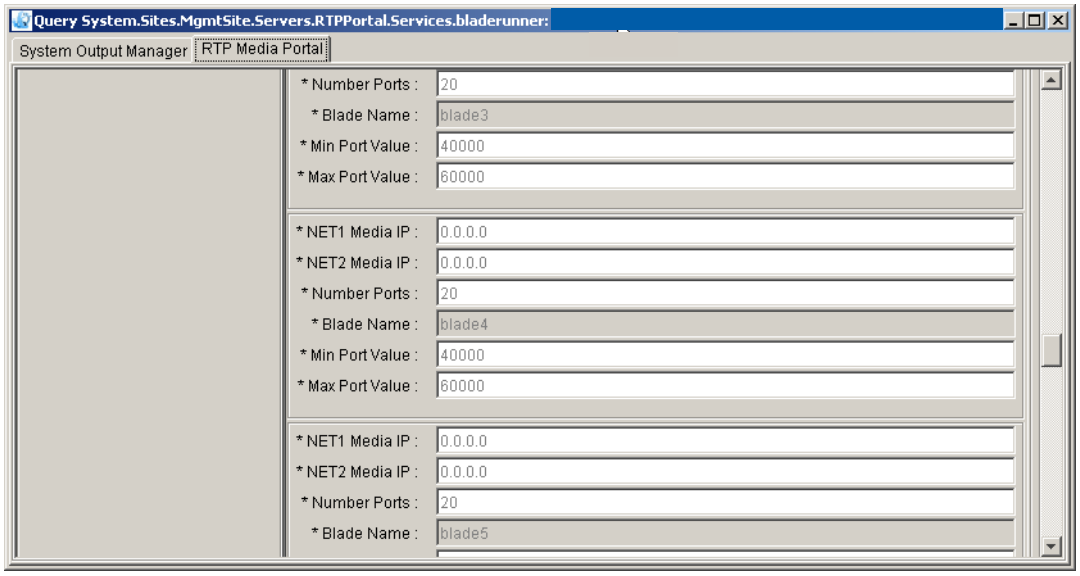
Figure 14 RTP Portal Shutdown confirmation



3 If it is NOT necessary to change the IP address of the MCPN765 card, skip to step 4.

If it is necessary to change the IP address, expand the RTP Portal options and right-click on RTP Portal to select **Modify.** From the **RTP Media Portal** tab to make the appropriate changes.

Figure 15 RTP Media Portal tab



No further action is required, and the final step in this procedure may be skipped.

4 Expand the RTP Portal options and right-click on RTP Portal to select **Restart**. The system will reboot.

Restoring the Management Server database

For more information refer to *Upgrading the CS 2000 T1400/T1405 Servers.*

SN08 to SN06.2 RTP Media Portal rollback

This section documents instructions for installing the base operating system (Red Hat Linux 6.2) and the RTP Media Portal application software.

Pre-requisites

Prior to installation, secure the following information in order to fully configure a new RTP Media Portal. Depending on hardware configuration, not all I/O cards may be present.

Slot	Component	Address
Domain A (left side, front)		
1	Private IP address for I/O card Private MAC address for I/O card Public IP address for I/O card Public MAC address for I/O card	
2	Private IP address for I/O card Private MAC address for I/O card Public IP address for I/O card Public MAC address for I/O card	

(Sheet 1 of 6)

Slot	Component	Address
3	Private IP address for I/O card Private MAC address for I/O card Public IP address for I/O card Public MAC address for I/O card	
4	Private IP address for I/O card Private MAC address for I/O card Public IP address for I/O card Public MAC address for I/O card	
5	Private IP address for I/O card Private MAC address for I/O card Public IP address for I/O card Public MAC address for I/O card	

(Sheet 2 of 6)

Slot	Component	Address
6	Private IP address for I/O card Private MAC address for I/O card Public IP address for I/O card Public MAC address for I/O card	
7	eth0 Private IP of Host Card eth1Private IP of Host Card Hostname Sub Netmask Address Gateway Address (Default Router)	

(Sheet 3 of 6)

Slot	Component	Address
Domain B (right side, front)		
9	eth0 Private IP of Host Card eth1 Private IP of Host Card Hostname Sub Netmask Address Gateway Address (Default Router)	
11	Private IP address for I/O card Private MAC address for I/O card Public IP address for I/O card Public MAC address for I/O card	
12	Private IP address for I/O card Private MAC address for I/O card Public IP address for I/O card Public MAC address for I/O card	
(Sheet 4 of 6)		

Slot	Component	Address
13	Private IP address for I/O card Private MAC address for I/O card Public IP address for I/O card Public MAC address for I/O card	
14	Private IP address for I/O card Private MAC address for I/O card Public IP address for I/O card Public MAC address for I/O card	
15	Private IP address for I/O card Private MAC address for I/O card Public IP address for I/O card Public MAC address for I/O card	

(Sheet 5 of 6)

Slot	Component	Address
16	Private IP address for I/O card Private MAC address for I/O card Public IP address for I/O card Public MAC address for I/O card	
General		
	Management Server Machine Logical IP Management Server Logical IP Accounting Manager Machine Logical IP BIOS Supervisor password (for A and B) RTP OS root user password (for A and B) RTP OS nortel user password (for A and B)	
(Sheet 6 of 6)		

Before commencing with software installation, ensure the RTP Media Portal physical installation is complete. The unit should be able to power on without hardware faults or errors.

Additionally, ensure no I/O devices are connected to Host Cards. These include keyboards, mouse, and monitors (i.e., KVM devices). Only the serial connection to a PC workstation/Laptop should be connected.

The network to which the Host Card is connected is the CS2K Management Network (private network). Only one of the network connections on the I/O cards is connected to the private network.

Network connectivity is accomplished through the rear Ethernet port (transition modules).

Label	BIOS Device Number	Linux Interface Name	Network
MCPN 765 I/0 Card Ethernet port usage			
NET1	CLUN 0/CLUN 0	eth0	public
NET2	CLUN 13/DLUN 0	eth1	private
CPV5370 Host Card Ethernet port usage			
1	N/A	eth0	private
2	N/A	eth1	private

BIOS configuration of CPV5270 Host Card

This section provides instruction to configure BIOS on the Host Card. Estimated time of completion is 12 minutes.

Create a console connection to COM1 (A) on the front panel of the Host CPU Card using a null modem serial cable. A connection to COM1 is only used during the initial power up. Once the BIOS is saved, the user must remove the serial cable and connect the Terminal Server cable to COM2 (on the transition module). COM1 is then available for future mouse connection.

From the console connection to COM1

1 As the machine is powering on, hold down the **F2** key to enter BIOS setup.

2 Once in BIOS mode, go to the **Advanced** menu, move to **IDE Configuration** and press the **Enter** key. Verify or change the values on the screen to match the values below. Leave all other values as default.

Local Bus IDE adapter: [Disabled]
Large Disk Access Mode: [DOS]
SMART Device Monitoring: [Disabled]

Primary Master: [NONE]
Primary Slave: [NONE]
Secondary Master: [NONE]
Secondary Slave: [NONE]

Press the **Esc** key twice to return to the **Advanced** menu.

3 Move to the **PCI Configuration** option and press the **Enter** key. Verify or change the values on the screen match the values below. Leave all other values as default.

Default Primary Video Adapter: [AGP]

On-Card Ethernet 1: [Enabled]
Ethernet 1 Connection: [Rear]
Ethernet 1 Option ROM: [Disabled]

On-Card Ethernet 1: [Enabled]
Ethernet 1 Connection: [Rear]
Ethernet 1 Option ROM: [Disabled]

Press the **Esc** key twice to return to the **Advanced** menu.

4 Move to the **HA Configuration** sub-menu and press the **Enter** key. Set the **HA Config** value to **Enabled**. Also set the Domain that is being configured to **Enable,** and **Disable** for the other domain. CPU in slot 7 is Domain A, and CPU in slot 9 is Domain B.

For example, for Domain A (for Host Card in Slot 7):
HA Config [Enabled]
Domain A [Enabled]
Domain B [Disabled]

Press the **Esc** key twice to return to the **Advanced** menu.

5 Move to the **Remote Console** option and press the **Enter** key. Verify or change the values on the screen match the values below. Leave all other values as default.

COM Port: [COM B]
Serial port B: [Enabled]
Base I/O address: [2F8]
Interrupt: [IRQ 3]

Baud Rate: [9600]
Console Type: [VT100]
Flow Control: [None]
Screen Lines: [25]
Active After POST: [On]

Press the **Esc** key twice to return to the **Advanced** menu.

6 Move to the **Boot** menu, then move to **Boot Device Priority** and press the **Enter** key. Make sure it boots in the following order:

```
  8XX SCSI CD-ROM LSI Logic
 +Hard Drive
!+Removable Devices
! ATAPI CD-ROM Drive
! Legacy Network Boot
```

Ensure the appropriate devices are disabled by placing an exclamation mark (!) beside them.

Press the **Esc** key twice to return to the **Advanced** menu.

7 Move to the **Security** menu to set the control access to the BIOS settings. Unauthorized BIOS access enables any Linux security to be circumvented (e.g. by booting into single-user mode from the floppy drive, etc.)

8 Setup the BIOS supervisor password. Ensure that the **Password on Boot option** is **Disabled**.

9 Press the **F10** key to save changes and exit the BIOS setup. The unit will reboot.

10 Quickly change the console connection from COM1 to COM2 as the unit is booting. Hold down the **F2** key to enter the BIOS setup screen again.

11 When prompted, enter the supervisor password. This step is to verify the supervisor password was correctly setup and using COM2 as the console port.

12 Insert the Red Hat 6.2 installation CD is in the correct CDROM drive for the domain (top CDROM is domain A).

13 Press the **Esc** key to exit the BIOS without any changes.

14 The unit will reboot. This completes the Host Card configuration. Remove the serial cable from COM2 and connect the serial cable from the Terminal Server to that port. At this point, all installation procedures should be performed from the Terminal Server.

Base operating system installation

The RTP Media Portal uses Red Hat Linux 6.2 as the underlying operating system. Estimated time for installation is approximately 75 minutes.

If it is necessary to re-enter the BIOS from the Terminal Server, the **F2** key will not work. It is necessary to use the escape key sequence **ESC+SHIFT+OQ**.

Once a selection has been made, select **Next** or **Done** to move to the next screen. The install process uses the **TAB** key to move between items/buttons on a screen, **SPACE BAR** to select/deselect items, **ENTER** key to expand items for editing, and **ARROW KEYS** for moving between items in a list.

From a terminal session

1 After the system boots from the Red Hat CD, the installation menu appears. Type the following: **text console=ttyS1,9600n8**

   If mistyped, reset the card using the reset button on the front of the 5370 card.

2 Select **English** for the Language Selection, then select **OK** to continue when the Red Hat welcome screen appears.

3 Several installation options are available: workstation, server, and custom. Choose **Install Custom System** installation. For **Bad Partition Table**, select **Initialize**.

4 Select the **fdisk** option under Disk Setup to partition the hard drive.

5 Select the only highlighted hard disk present and select **Edit**.

Hard drive partitioning

Disk partitioning on the RTP Media Portal is accomplished with the Linux **fdisk** commands including:

- **m** - displays a list of available commands.
- **n** - adds a new partition.
- **p** - prints the current partition table.
- **d** - deletes a partition.
- **t** - changes the partition type.
- **w** - writes the partition table and exits **fdisk**.

Partition recommendations (assuming a 36 GB hard drive) are listed below. Sizes are given in megabytes and also include an approximate percentage of the entire disk.

Before continuing, type **p** to display any existing partitions. If these exist, delete them by using the **d** command.

From a terminal server

1 Type **n**, then **p**, then **1**. Press the **Enter** key to accept the default beginning block, then type **+1000M** for the size as shown below:

```
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-35242, default 1): <Enter>
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-32542, default
35242): +1000M
```

2 Enter **n**, then **p**, then **2**. Press the **Enter** key to accept the default beginning block, then type +5000M for the size as shown below:

```
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 2
First cylinder (1002-35242, default 1002): <Enter>
Using default value 1002
Last cylinder or +size or +sizeM or +sizeK (1002-32542, default
35242): +5000M
```

3 Enter **n**, then **p**, then **3**. Press the Enter key to accept the default beginning block, then type **+1000M** for the size as shown below:

```
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-1)
p
Partition number (1-4): 3
First cylinder (6003-35242, default 1): <Enter>
Using default value 6003
Last cylinder or +size or +sizeM or +sizeK (6003-32542, default
35242): +1000M
```

4 Change the partition type by entering **t**, then **3**, then type **82**.

```
Command (m for help): t
Partition number (1-7): 3
Hex code (type L to list codes): 82

Changed system type of partition 3 to 82 (Linux swap)
```

5 Enter **n**, then **e**, then **4**. Press the **Enter** key to accept the default beginning block, then press the **Enter** key again to accept the default for the last block.

```
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-1)
e
Partition number (1-4): 4
First cylinder (7004-35242, default 7004): <Enter>
Using default value 7004
Last cylinder or +size or +sizeM or +sizeK (7004-32542, default
35242): <Enter>

Using default value 35242
```

6 The drive can have only 4 main partitions. The last main partition holds partitions 5 through 7.

Enter **n**, then press the **Enter** key to accept the default beginning block, then type **+10000M** for the size as shown below:

```
Command (m for help): n
First cylinder (7004-35242, default 7004): <Enter>
Using default value 7004
Last cylinder or +size or +sizeM or +sizeK (7004-32542, default
35242): +10000M
```

7 Enter **n**, then press the Enter key to accept the default beginning block, then type **+10000M** for the size as shown below:

```
Command (m for help): n
First cylinder (17005-35242, default 17005): <Enter>
Using default value 17005
Last cylinder or +size or +sizeM or +sizeK (17005-32542, default
35242): +10000M
```

8 Enter **n**, then press the **Enter** key to accept the default beginning block, then type press the **Enter** key again to accept the default value for the last block:

```
Command (m for help): n
First cylinder (27006-35242, default 27006): <Enter>
Using default value 27006
Last cylinder or +size or +sizeM or +sizeK (17005-32542, default
35242): <Enter>
```

Using default value 35242

9 Enter **p** to view the final partition table:

Command (m for help): **p**

Disk /tmp/sda: 64 heads, 32 sectors, 35242 cylinders
Units = cylinders of 2048 * 512 bytes

Device Boot	Start	End	Blocks	Id	System
/tmp/sda1	1	1001	1025008	83	Linux
/tmp/sda2	1002	6002	5121024	83	Linux
/tmp/sda3	6003	7003	1025024	82	Linux swap
/tmp/sda4	7004	35242	28916736	5	Extended
/tmp/sda5	7004	17004	10241008	83	Linux
/tmp/sda6	17005	27005	10241008	83	Linux
/tmp/sda7	27006	35242	8434672	83	Linux

10 Press w when complete to save and exit **fdisk**.

11 Select **Done** and press the **Enter** key to continue.

12 Back at the Disk Setup screen, select the individual partitions, then press **TAB** to select **Edit** and press the **Enter** key. Type in the mount points and select **OK**. Repeat for all the other partitions as necessary.

Partition 1: mountpoint = /boot
Partition 2: mountpoint = /
Partition 3: (should already be set to swap)
Partition 4 (is an extended partition and is not listed)
Partition 5: mountpoint = /var
Partition 6: mountpoint = /usr
Partition 7: mountpoint = /IMS

(mountpoints must be typed in the text box)

13 Select the **OK** option to exit the Disk Setup screen.

14 In the **Choose Partitions to be Formatted** screen, ensure all partitions are selected and the **Check for bad blocks** option is NOT selected.

[*] /dev/sda2 /
[*] /dev/sda7 /IMS
[*] /dev/sda1 /boot
[*] /dev/sda6 /usr
[*] /dev/sda5 /var

These are usually default options. Press the **Tab** key twice to position the cursor on the **OK** button and press the **Enter** key.

Completing the installation

This section lists steps to complete the installation.

From a terminal server

1 The LILO Configuration screen will appear. Ensure the **User linear mode (needed for some SCSI drives)** is selected (default). In this window type in the boot arguments for LILO exactly as follows: **console=ttyS1,9600n8**

Select OK when finished.

2 Ensure **/dev/sda** for the location to install LILO is selected, and select **OK** to continue. It should be selected by default.

3 Select **OK** to accept the default selection for the partition to boot the Linux OS.

4 The Host Configuration screen will appear. Type in the hostname of the RTP Media Portal. Select **OK** when finished.

5 On the Network Configuration screen, de-select the **bootp/DHCP** checkbox. Then move the cursor to the individual fields and type in the appropriate information. Delete the entry for the **Primary Name Server**.

[ ] Use bootp/dhcp

IP address: <eth0 Private IP of Host Card>
Netmask: <Private Host Card Netmask>
Default gateway (IP): <Default Gateway>
Primary nameserver:

Then select **OK** to continue.

6 On the Device settings screen. Accept the default setting and select **OK** to continue. No mouse will be used on this system.

7 On the Time Zone Selection screen, select the appropriate local time zone and select **OK**.

8 The next screen will setup the root password for the “root” user. This user is automatically created during the Linux OS installation. When prompted, enter the appropriate root password. Retype the password for confirmation and select **OK** to continue. Do not forget the password.

9 The Authentication Configuration screen will appear. Accept the default values and select **OK** to continue.

[*] Use Shadow Passwords

[*] Enable MD5 Passwords

[ ] Enable NIS
NIS Domain:
NIS Server: [ ] Request server via broadcast
or use:

10 An Add User screen will appear. Create a normal user account with username “nortel” and the appropriate password. Do not forget the password. Retype the password for confirmation and select **OK** to continue.

11 In the Authentication Configuration screen, verify the **Use Shadow Password** and **Enable MD5 password** check boxes are checked and select **OK**.

12 Select the software packages to install. Some packages are selected by default; others are unselected by default. Select/deselect packages as required in order to obtain the following list, then select **OK** to continue:

[*] Xwindows
[*] GNOME
[*] Networked Workstation
[*] NFS Server
[*] Anonymous FTP Server
[*] Development
[*] Kernel Development
[*] Utilities

13 Select **No** when ask if a boot disk is to be created.

14 Select **OK** to begin the installation. The Operating System packages will begin to install. It will take approximately 20-30 minutes to complete. Once completed, the system will prompt the user to reboot and remove the installation CD from the drive.

Boot disk creation is optional, and can safely be skipped.

Remove the CD before the POST boot sequence is complete. If the user does not do this, the base installation scripts will begin again. If this happens, press the Reset button on the front panel of the Host CPU Card to reboot the machine again.

RTP Media Portal installation

This section lists steps to install the RTP Media Portal Application software from the CD. It requires approximately 20 minutes.

From the terminal server

1 After the system reboots and the LILO prompt is displayed, press the **TAB** key to halt the LILO boot process.

2 Insert the RTP Media Portal Install CD into the CD-ROM and reboot the system by pressing the Reset button on the front panel of the Host CPU Card.

3 The system will reboot from the RTP Media Portal Install CD and begin executing the installation scripts. Read and follow the instructions on the console in order to boot the correct installer for your console type. Choose the **Serial** console, for console type.

4 Press the **TAB** key when the LILO prompt appears. Then type **install-serial** at the prompt to being the installation process.

5 The following information is requested before the installation begins:

Host CPU Slot number: **[7 or 9]**
RTP Media Portal cage number **[1, 2, 3,...]**
Host CPU Type: **[5370]**
Time Zone and Format: [Local Values]
Time Server IP address: [See Below*]
Permanent system console type: **[s]**

*This is the service logical IP address of the Management Server. Do not use any default address.

Use cage number 1 for the first RTP shelf, and 2 if installing on another shelf. Increment accordingly to the number of RTP shelves present. Keep the same cage number for both Domain A and B.

If there is an error during the input, enter **n** on the confirmation screen to re-enter the values. Otherwise, enter **y** to continue.

6 When prompted, provide the MAC addresses for each of the I/O cards in the Domain. If there is no I/O card present in the slot, press the **Enter** key to skip to the next slot entry. Select **OK** when completed.

7 At this point, the RTP Media Portal packages will be installed. It will take approximately 40-50 minutes to complete the

installation. Do not touch the keyboard or the system until completion.

If for some reason the installation scripts does not finish or is aborted, the entire procedure must be repeated. Likewise, the RTP Media Portal install CD should never be used on a system that already has the RTP Media Portal software installed on it.

8 Once this process is complete, the program will display information concerning configuration that may have to be done manually. The system will display **Press <ENTER> to continue** prompt. Press the **ENTER** key. The system will reboot.

9 As the system reboots and when LILO prompt appears, press the **TAB** key to halt the process.

10 Remove the RTP Media Portal Install CD, and reboot the system by pressing the Reset button on the front panel of the Host CPU Card.

11 When the system reboots, go back into BIOS setup and remove everything from the boot device list except the hard drive for security reasons. Once this is complete, save and exit the BIOS. The system will reboot again.

12 When the system completes the reboot process, press the **ENTER** key. The login prompt will appear.

Configuring the MCPN765 I/o cards

This section describes the procedures to properly configure each I/O Card on the RTP Media Portal. It requires changes to settings in the BIOS, using a terminal/console connection. Estimated time to complete the configuration is approximately 10 minutes.

From a terminal server

1 Beginning with the first I/O Card (i.e. card in slot 1), establish a terminal connection to the Card using a PC/Laptop. Use the port labeled “COM1” on the rear transition module of the card.

2 Reset the Card via the RST button on the front panel. The RST button must be held for a few seconds until the activity light turns amber.

3 The boot process will begin; on the terminal, press the **ESC** key when prompted to halt the boot-up sequence.

4 When the command prompt appears, set the real-time clock on the Card by entering the following command at the prompt:

PPC6-Bug>set <MMDDYYHHMM>

where MM = month, DD = day, YY = year, HH = hour (24 hour clock), MM = minutes

5 Enter the following line to display MAC address for the card:
PPC6-Bug>niot ;h
Record the MAC address for CLUN 0/DLUN 0 (NET1) and for CLUN 13/DLUN 0 (NET2) fields.

6 Enter the **env** command at the prompt to verify the BIOS on the I/O Card. Ensure they match the settings shown below. If not, make the appropriate adjustments.

Note the questions listed below may appear differently depending on when the cards were ordered. This is due to the different BIOS versions that may be loaded on each card. If a question appears that is not described below, accept the default value and move on.

```
PPC6-Bug>env
Bug, AST or System environment [B/A/S] = B?
Maximum Memory Usage (Mb, 0=AUTO) =   0?
Field Service Menu Enable [Y/N] = N?
Probe System for Supported I/O Controllers [Y/N] = Y?
Auto-Initialize of NVRAM Header Enable [Y/N] = Y?
Network PReP-Boot Mode Enable [Y/N] = Y?
SCSI Bus Reset on Debugger Startup [Y/N]   = N?
Primary SCSI Bus Negotiations Type [A/S/N] = A?
Primary SCSI Data Bus Width [W/N]          = N?
Secondary SCSI Identifier                  = "07"?
NVRAM Boot List (GEV.fw-boot-path) Boot Enable [Y/N]
= N?
NVRAM Boot List (GEV.fw-boot-path) Boot at power-up only
[Y/N] = N?
NVRAM Boot List (GEV.fw-boot-path) Boot Abort Delay
= 5?
Auto Boot Enable [Y/N]           = N?
Auto Boot at power-up only [Y/N] = N?
Auto Boot Scan Enable [Y/N]      = Y?
Auto Boot Scan Device Type List  =
FDISK/CDROM/TAPE/HDISK/?
Auto Boot Controller LUN   = 00?
Auto Boot Device LUN       = 00?
Auto Boot Partition Number = 00?
Auto Boot Abort Delay      = 7?
Auto Boot Default String [NULL for an empty string] = ?
ROM Boot Enable [Y/N]            = N?
ROM Boot at power-up only [Y/N]  = Y?
```

```
ROM Boot Abort Delay              = 5?
ROM Boot Direct Starting Address = FFF00000?
ROM Boot Direct Ending Address    = FFFFFFFC?
Network Auto Boot Enable [Y/N]           = Y?
Network Auto Boot at power-up only [Y/N] = N?
Network Auto Boot Controller LUN = 13?
Network Auto Boot Failover Controller LUN = 00?
Network Auto Boot Device LUN      = 00?
Network Auto Boot Abort Delay     = 5?
Network Auto Boot Configuration Parameters Offset (NVRAM)
= 00001000?
Watchdog prior status ignored at autoboot [Y/N] = Y?
Watchdog shutdown at board reset          [Y/N] = N?
Reset Ethernet chip after file transfer   [Y/N] = N?
Stop Auto Boot after selftest failure     [Y/N] = N?
Memory Size Enable [Y/N]          = Y?
Memory Size Starting Address      = 00000000?
Memory Size Ending Address        = 40000000?
DRAM Speed in NANO Seconds        = 8?
ROM Bank A Access Speed (ns) = 90?
ROM Bank B Access Speed (ns) = 120?
DRAM Parity Enable [On-Detection/Always/Never - O/A/N]
= O?
L2Cache Parity Enable [On-Detection/Always/Never - O/A/N]
= O?
PCI Interrupts Route Control Registers (PIRQ0/1/2/3) =
0A0B0E0F?
Serial Startup Code Master Enable [Y/N] = N?
Serial Startup Code LF Enable [Y/N] =     N?
Firmware Command Buffer Enable [Y/N] = N?
Firmware Command Buffer Delay  = 5?
Firmware Command Buffer : <Enter>
['NULL' terminates entry]?

Update Non-Volatile RAM (Y/N)? y

Reset Local System (CPU) (Y/N)? n
```

7 Next, to access the Network boot settings enter **niot** command at the prompt.

Do not change the IP addressing format in this section. Follow exactly what is documented above. These IP addresses are internal addresses between the I/O and Host cards which are different than the customer provided IP address schemes.

```
PPC6-Bug>niot
```

```
Controller LUN =00? 13
Device LUN     =00?
Node Control Memory Address =03E1D8A0?
Client IP Address   =0.0.0.0? 192.168.<cage #>.<i/o card
#>
Server IP Address   =0.0.0.0? 192.168.<cage #>.<hostcard
#>
Subnet IP Address Mask =255.255.255.0?
Broadcast IP Address=255.255.255.255? 192.168.<cage
#>.255
Gateway IP Address     =0.0.0.0?
Boot File Name ("NULL" for None)   =?
/tftpboot/bladeRunner
Argument File Name ("NULL" for None) =?
Boot File Load Address          =001F0000?
Boot File Execution Address     =001F0000?
Boot File Execution Delay       =00000000? 00000005
Boot File Length                =00000000?
Boot File Byte Offset           =00000000?
BOOTP/RARP Request Retry        =00? 50
TFTP/ARP Request Retry          =00? 50
Hardware error retry attempts   =00?
Trace Character Buffer Address =00000000?
BOOTP/RARP Request Control: Always/When-Needed (A/W)=W?
BOOTP/RARP Reply Update Control: Yes/No (Y/N)       =Y?
```

8 Reset the Card with the **reset** command at the prompt. The Card should begin trying to network boot once it completes the necessary self-tests.

```
PC6-Bug>reset
Cold/Warm Reset [C,W] = C?
Execute Local SCSI Bus Reset [Y,N]       = N?
Execute Local (CPU) Reset [Y,N]          = N? y
```

9 Repeat these steps for ALL I/O Cards in this Domain.

The Host Card IP address and Broadcast IP address should be the same between all I/O Cards.

Network Time Protocol configuration

This section describes the procedures to synchronize the RTP Media Portal clock to the “master” clocks on the MCS 5200 / CS2K Management Servers. Estimated time required to complete the procedure is 5 minutes.

From a terminal server

1 Establish a serial/terminal connection to the Host CPU card and login into the system as **root** user.

2 Create a new **ntp.conf** file in the /etc directory by entering the following command:

bash# vi /etc/ntp.conf

3 Add the following three lines in the file:

server <Machine Logical IP RTP EM (Mgmt/Db Combo) Server>
driftfile **/etc/ntp/ntp.drift**

4 Save and exit the editor. Verify the file was correctly save by entering the following command:

bash# more /etc/ntp.conf

5 Exit the system by entering **exit** at the prompt. This completes the installation.

6 Repeat this procedure for Domain B of the RTP Media Portal, if applicable.

IP Security support

How this chapter is organized

This chapter is organized as follows:

Functional description

IP Security (IPSec) functionality for MCS components is enabled through the CS2K Gateway Controller and RTP Media Portal. Support for IPSec is also provided between the RTP Media Portal, the System Management Server (SM), and the Database Server (DB).

The following IPSec functionalities are supported:

- Internet Key Exchange (IKE) with pre-shared key.
- Automatic trigger of IKE when no outgoing Security Association (SA) is available.
- Support “Main Mode” exchange for IKE and Encapsulating Security Payload (ESP) Transport Mode for IPSec.
- Support time-based and provisionable IPSec SA lifetime.

Configuration and provisioning

This section provides instruction to configure and provision IPSec. The basic steps to enable IPSec include:

- Set pre-shared key.
- Set security policy.
- Configure IKE and IPSec SAs.

Setting pre-shared key

A hard-coded text or hex string that must be manually configured on the nodes being secured. The pre-shared key must match exactly on both ends of the negotiation, otherwise the key exchange will fail.

Setting security policy

The IPSec Security Policy Database (SPD) specifies which services are offered to which IP datagrams and in what fashion. The SPD must be consulted during the processing of all traffic both inbound and outbound (including non-IPSec traffic).

The SPD specifies the security processing to be applied to any packet entering or exiting the IPSec system on a per-packet basis. An SPD must discriminate between traffic that is afforded IPSec protection, and traffic that is allowed to bypass IPSec. Three options are possible: none, discard and ipsec.

The IPSec policy can enable/disable secure traffic on a per link basis or within a subnet range. The source and destination of the secure communication can be specified as IPv4 address or address range.

The security policy supports:

- IPSec ESP in Transport Mode
- IPSec anti-replay protection on its incoming SA.
- Non-configurable SA renew threshold when the existing SA reaches 80 percent of the SA hard limit.

Configuring IKE and IPSec SAs

The IKE and IPsec configuration parameters include:

- pre_shared_key: pre-shared text key specified in psk.txt
- exchange_mode: main
- encryption_algorithm: 3des, des, null_enc
- hash_ algorithm: md5, sha
- authentication_algorithm: hmac_md5, hmac-sha1
- dh_group 1
- time-based SA lifetime

The Media Portal IPSec configuration process is automated with MPIPSec perl script (**/opt/mcp/mediaportal/bin**) on the Linux machine. The MPIPSec script inputs and outputs, and operation menus are described below.

Before displaying the main menu, the following prompt is displayed to ask if the user wants to save the script process in a log file. If the user answers “y”, the script process is saved in a log file with a time stamp.

```
Do you want to save log for this script process ?
[Y,N]
```

Main menu

Upon initial startup, the MPIPSec script displays the Main Menu.

Figure 1 Main menu

```
Select an option from the MAIN menu:
[1] PSK Preshared Key
[2] SPD Security Policy
[3] SAD Security Associations
[4] RAC Racoon Configuration
[5] Restart IPSec
[6] Disable IPSec
[7] Quit

Please enter the number [1 to 7] of the MAIN menu: 1
```

PSK Preshared Key menu

Select an option from the PSK Preshared Key menu.

Figure 2 PSK Preshared Key menu

```
Select an option from the PSK menu:
[1] List all PSK
[2] Add PSK
[3] Delete PSK
[4] Flush all PSK
[5] Return to main menu
[6] Quit

Please enter the number [1 to 6] of the PSK menu:
```

Add PSK

PSK are created for each peer machine by identifying the remote IPaddress and the associated PSK (the PSK can be specified in ASCII or in hex). Note the remote host IP address is the active IP address of the CS2K GWC.

Example input:
Please enter remote host IP : 47.477.47.477

Please enter pre-shared key: TESTKEY
Pre-shared key in hex? [Y/N]: n

Example output:

```
*****************Add PSK***************
The following PSK entry was successfully added.
47.477.47.477      TESTKEY
```

Delete PSK

Use this option to remove a pre-shared key from the system associated with a remote peer. Each remote IPaddress can only map to one pre-shared key.

Example input:
Please enter remote host IP: 47.477.47.477

Example output

```
*****************Delete PSK***************
The following PSK entry was successfully deleted.
47.477.47.477      TESTKEY
```

Flush all PSK

Use this option to remove all pre-shared keys from the system. No other input is required.

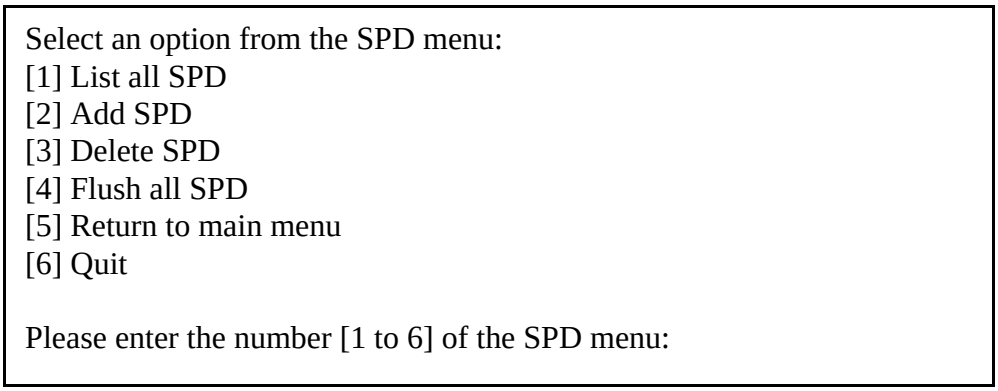
Example output

```
*****************Flush all PSK***************
PSK entries flushed.
```

SPD Security Policy menu

The SPD menu provides utilities required to manage the security policy database.

Figure 3 SPD Security Policy menu



List all SPD

Use this command to list all Security Policy Database entries. No input is required.

Example output:

```
*****************List all SPD***************
47.477.47.477 [any] 48.488.48.488 [any] any
   in ipsec
    esp/transport//require
   created: Jul 14 10:12:29 2004  lastused: Jul 14
            10:57:03 2004
   lifetime: 0(s) validtime: 0(s)
   spid=8 seq=1 pid=3223
   refcnt=1
48.488.48.488 [any] 47.477.47.477 [any] any
   out ipsec
   esp/transport//require
   created: Jul 14 10:12:29 2004  lastused: Jul 14
            10:57:03 2004
   lifetime: 0(s) validtime: 0(s)
   spid=9 seq=0 pid=3223
   refcnt=1
```

Add SPD

Use this command to add a SPD entry into the system for a remote peer, as identified by IPaddress.

Example input:
Please enter remote host IP: 47.477.47.477

Example output:

```
*********** Add SPD ******************
The SPD entry was successfully added.
```

Delete SPD

Use this command to remove a SPD entry from the system for a remote peer, as identified by IPaddress.

Example input:
Please enter remote host IP: 47.477.47.477

Example output:

```
*********** Delete SPD ******************
The SPD entry was successfully deleted.
```

Flush all SPD

Use this command to remove all SPD entries from the system. No other input is required.

Example output:

```
*********** Flush all SPD ***************
SPD entries flushed.
```

SAD Security Associations menu

The SAD Security Associations menu provides utilities to view and delete the phase-2 IPSec SAD entries The “Add SAD” operation is not provided because the SAD may only be added and negotiated by racoon. Manual addition of the SAD is not supported.

Figure 4 SAD Security Associations menu

```
Select an option from the SAD menu:
[1] List all SAD
[2] Delete SAD
[3] Flush all SAD
[4] Return to main menu
[5] Quit

Please enter the number [1 to 5] of the SAD menu:
```

List all SAD

Use this command to list all SAD entries in the system. No other input is required.

Example output:

```
********** List all SAD ****************
47.477.47.477 47.488.47.488
   esp mode=transport spi=161723184(0x09a3b330)
         reqid=0(0x00000000)
   A: hmac-md5  afd04584 d5b60f76 fd6cc195 8b3c09dc
   seq=0x00000000 replay=4 flags=0x00000000
         state=mature
   created: Jul 14 10:56:01 2004   current: Jul 14
         10:56:16 2004
   diff: 15(s)     hard: 100(s)    soft: 80(s)
   last:          hard: 0(s)      soft: 0(s)
   current: 0(bytes)  hard: 0(bytes)  soft: 0(bytes)
   allocated: 0    hard: 0 soft: 0
   sadb_seq=1 pid=3205 refcnt=0
47.488.47.488 47.477.47.477
    esp mode=transport spi=10873237(0x00a5e995)
        reqid=0(0x00000000)
    A: hmac-md5  2db95fe1 cd764aab feaa4ba5 eab34075
    seq=0x00000000 replay=4 flags=0x00000000
        state=mature
     created: Jul 14 10:56:01 2004   current: Jul 14
        10:56:16 2004
     diff: 15(s)     hard: 100(s)    soft: 80(s)
      last:            hard: 0(s)      soft: 0(s)
      current:0(bytes) hard: 0(bytes) soft: 0(bytes)
      allocated: 0    hard: 0 soft: 0
      sadb_seq=0 pid=3205 refcnt=0
```

Delete SAD

Use this command to remove a SAD entry from the system. The remote peer IPaddress and the Security Parameters Index (SPI) must be provided to find the specific SAD entry to be deleted.

Example input:

Please enter remote host IP: 47.477.47.477
Please enter SPI of the SAD: 123456789

Example output:

```
*********** Delete SAD ******************
The SAD entry was successfully deleted.
```

Flush all SAD

Use this command to remove all SAD entries from the system. No other input is required.

Example output:

```
********** Flush all SAD ******************
SAD entries flushed.
```

RAC Racoon configuration menu

The RAC sub menu provides utilities to view/add/delete configuration aspects with the **racoon.conf** file.

Figure 5 RAC Racoon configuration menu

```
Select an option from the RAC menu:
[1] List all racoon SA configurations
[2] Add a racoon SA configuration
[3] Delete a racoon SA configuration
[4] Return to main menu
[5] Quit

Please enter the number [1 to 5] of the RAC menu:
```

List all racoon SA configurations

Use this command to list all racoon SA configurations specified in the racoon. No other input is required.

Example output:

```
****** List all racoon SA configurations **********

path pre_shared_key "/admin/psk.txt";

remote 47.477.47.477 {
        exchange_mode main;

        proposal {
                encryption_algorithm des;
                hash_algorithm md5;
               authentication_method pre_shared_key;
                dh_group 1;
                lifetime time 60 sec;
        }
}
```

```
sainfo address 47.488.47.488 any address
47.477.47.477 any {
        encryption_algorithm null_enc;
        authentication_algorithm hmac_md5;
        compression_algorithm deflate;
        lifetime time 3600 sec;
}
```

Add a racoon SA configuration

Use this command to add racoon SA configuration (aspects) for a remote peer. The configure aspects include phase-1 and phase-2 SA lifetime, DH (Diffie-Hellman) group, authentication and encryption algorithms.

Example input:
Please enter remote host IP: 47.477.47.477
****** Add Phase 1 and Phase 2 SA Configuration Input ********
Enter lifetime time : value in seconds
IKE sa >> 60
Enter encryption_algorithm : [des,3des]
IKE sa >> 3des
Enter hash_algorithm : [md5,sha1]
IKE sa >> sha1
Enter dh_group : [1,2,3,4]
IKE sa >> 1
Enter authentication_alogrithm : [hmac_md5,hmac_sha1]
IPSEC sa >> hmac_sha1
Enter lifetime time : value in seconds
IPSEC sa >> 86400

Example output:

```
********** Add a racoon SA configuration *********
The racoon configuration has been successfully added
to racoon.conf.
```

Delete a racoon SA configuration

Use this command to remove racoon SA configuration (aspects) associated with a remote peer. No other input is required.

Example output:

```
********* Delete a racoon SA configuration **********
```

```
The racoon configuration has been successfully
deleted.
```

Restart IPSec

When any change (adding or deleting a racoon SA configuration) is made to the **racoon.conf** file, the IPSec racoon daemon needs to be restarted.

Example input:

```
This operation will disrupt all MPCP traffic, it is
recommended to shutdown Media Portal before restart
IPSec.

Restart IPSec will flush all existing SAD and SPD, do
you really want to restart ? [Y,N]  Y
```

To restart, first shutdown the old racoon IKE daemon and then restart a new racoon process. If the IKE racoon process was not running previously, the status for Shutting down IKE daemon would be “FAILED” which indicates that the IKE racoon daemon was not active before restart.

Example output:

```
************ Service restart IPSec *****************
Shutting down IKE daemon:          [FAILED]
Flushing security associations:      [OK]
Flushing security policies:              [OK]
Installing IPSec security policies:   [OK]

Starting IKE daemon:                        [OK]
```

If the IKE racoon process was running previously before restart, the status for Shutting down IKE daemon will be “OK”.

Example output:

```
************ Service restart IPSec *****************
Shutting down IKE daemon:           [OK]
Flushing security associations:     [OK]
Flushing security policies:         [OK]
Installing IPSec security policies: [OK]
Starting IKE daemon:                    [OK]
```

Disable IPSec

The IPSec service can be shutdown and disabled when the system is in maintenance state. Or for some reason, if IPSec needs to be

completely disabled or removed from the system, this function should be used to shutdown all the IPSec processes and remove all the IPSec configuration files (i.e. psk.txt, ipsec.conf and racoon.conf).

Example input:

```
This operation will disrupt all MPCP traffic, it is
recommended to shutdown Media Portal before disable
IPSec.

Disable IPSec will flush all existing SAD and SPD, do
you really want to disable IPSec ? [Y,N]  Y
```

Example output:

```
************ Disable IPSec *****************
Shutting down IKE daemon:          [OK]
Flushing security associations:    [OK]
Flushing security policies:        [OK]

Do you also want to REMOVE conf files ? [Y,N]

Remove  /admin/psk.txt ? [Y,N]

********** /admin/psk.txt has been removed *********

Remove  /admin/ipsec.conf ? [Y,N]

******** /admin/ipsec.conf has been removed ********

Remove  /admin/racoon.conf ? [Y,N]

******** /admin/racoon.conf has been removed *******
```

For normal shutdown and maintenance mode, users should answer “Y” to shutdown the IKE racoon process, but NOT to REMOVE the conf files. Users should only answer “Y” to REMOVE all conf files when the IPSec service is going to be completely removed from the system.

Quit

The Quit option is provided in all menus, allowing the user to quit running of the script. Whenever the script is completed, the following information is displayed. If the user answers “y” to save the script process in a log file, the log file name is displayed when the user completes the script process.

Example output:

```
MPIPSec perl script is successfully terminated from
```

```
the MAIN menu.
Logs have been written to
/tmp/logs/MPIPSec.log.2004_7_14.18:43:11.
```

Error Handling

All input data is validated. The user has two chances to input or correct information. If invalid data is entered once, the user gets a warning message to “try again”. If the second data is accepted, the operation proceeds as normal. If the second data is also invalid, the operation is aborted with error message.

For example, failure to provide a valid “remote host IP” would result in the following error messages:

```
Please enter remote host IP: abcd
Invalid data entered, please try again.
Please enter remote host IP: 123
Invalid data entered twice, aborting operation.
```

In order to support IPSec on RTP Media Portal, it is necessary for the base to be upgraded to Motorola’s AHA 4.0 software. Similarly, the System Management Server and Database Server require Solaris 9 in order to provide support for IPSec.

Restoring IPSec communications in the event of failure

The SA lifetime differential, short phase-1 (IKE) SA lifetimes and long phase-2 (IPSec) SA lifetimes, are used to recover failed IPSec communications sessions. The differential SA lifetime solution works by configuring the phase-1 IKE SA lifetime shorter than phase-2 IPSec SA lifetime. The short phase-1 IKE SA lifetime enables IKE to exist long enough for the IPSec session to establish, after which time the phase-1 IKE SA is no longer required. The longer phase-2 IPSec SA lifetime causes the IPSec session to refresh itself at regular intervals, long after the phase-1 IKE SA is gone. For this differential lifetime recovery strategy, the recommended phase-1 IKE SA lifetime is one minute which is based on the consideration that in the event of system outage, the estimated system down time is approximately one to two minutes. The recommended phase-2 IPSec SA lifetime is 24-hours.

Carrier Voice over IP

Communication Server 2000

RTP Media Portal Basics

Publication number: NN10367-111
Product release: (I)SN08
Document version:Preliminary (03.01)

NORTEL