NN10035-111

Succession Multimedia Communications Portfolio

MCP RTP Media Portal

Basics

Standard MCP 1.1 FP1 (02.02) April 2003

NORTEL NETWORKS™

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

Overview

How this chapter is organized

This chapter is organized as follows:

Functional description

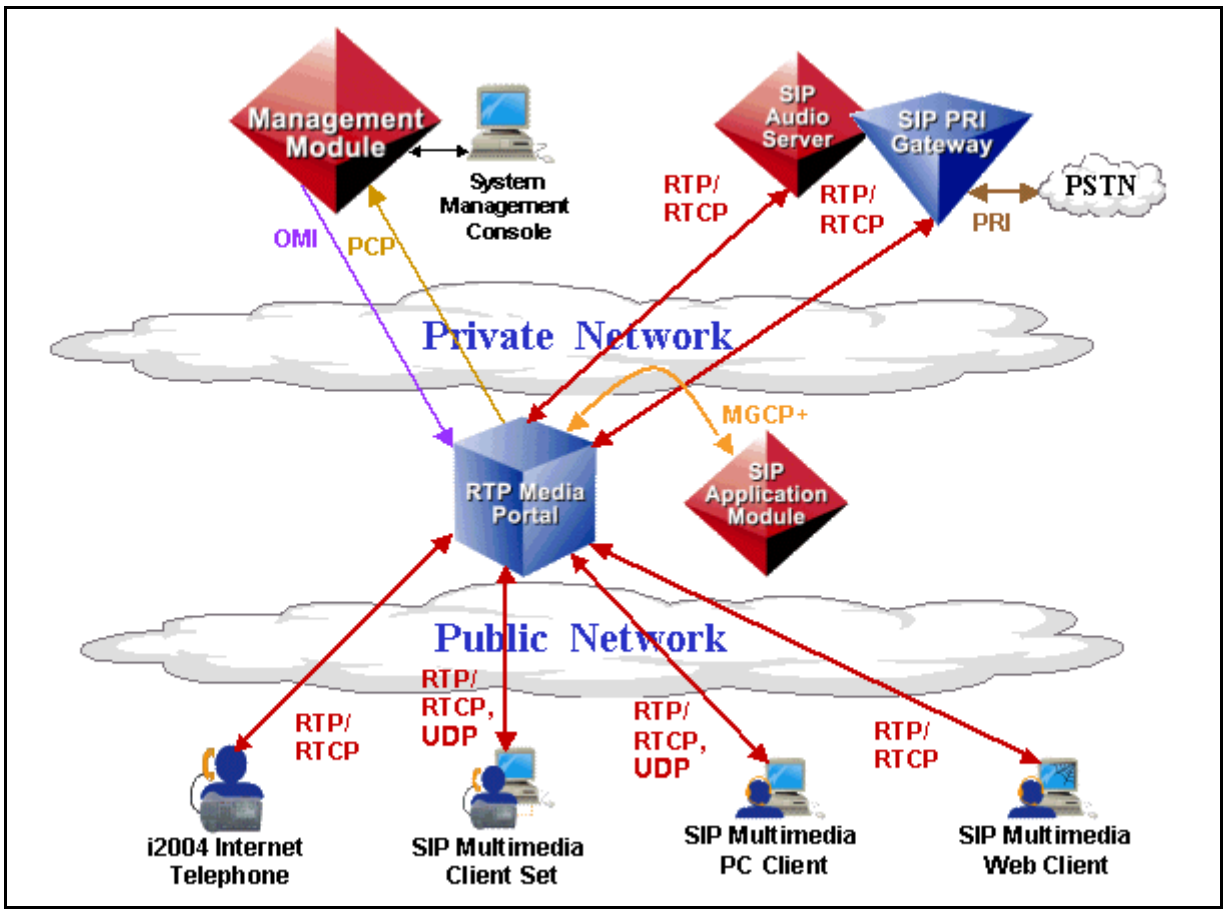
The Real-time Transport Protocol (RTP) Media Portal is an optional component of the network that performs many media-layer functions. The RTP Media Portal addresses media specific issues with advanced service delivery, Internet addressing efficiencies, and system security. It functions as a media Network Address and Port Translation (NAPT) point that shields private network components from external exposure through leaks in the media streams. The RTP Media Portal also enables elements in the private network to safely communicate with elements in the public network. The RTP Media Portal provides IP address/port pair mapping between internal and external network components, as well as media anchoring and media pivot abilities for terminals.

Figure 1, “Network Component Interoperability,” on page 4 is a graphical representation of the RTP Media Portal interworking among other components in the Multimedia Communications Portfolio.

Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

Figure 1 Network Component Interoperability



The clouds in the diagram 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 Protocol (RTP), Real-time Transport Control Protocol (RTCP), and User Datagram Protocol (UDP) transmissions.

Hardware

Description

The RTP Media Portal resides on a Motorola CPX8216T platform which is a CompactPCI (cPCI) chassis design.

The chassis provides the basic operating environment (such as power, backplane, cooling, and mounting slots) required to house cPCI-based single-board computers. The CPX8216T partitions the chassis into two separate logical operational domains (dividing the chassis shelf into two half-shelves consisting of 8-slots each).

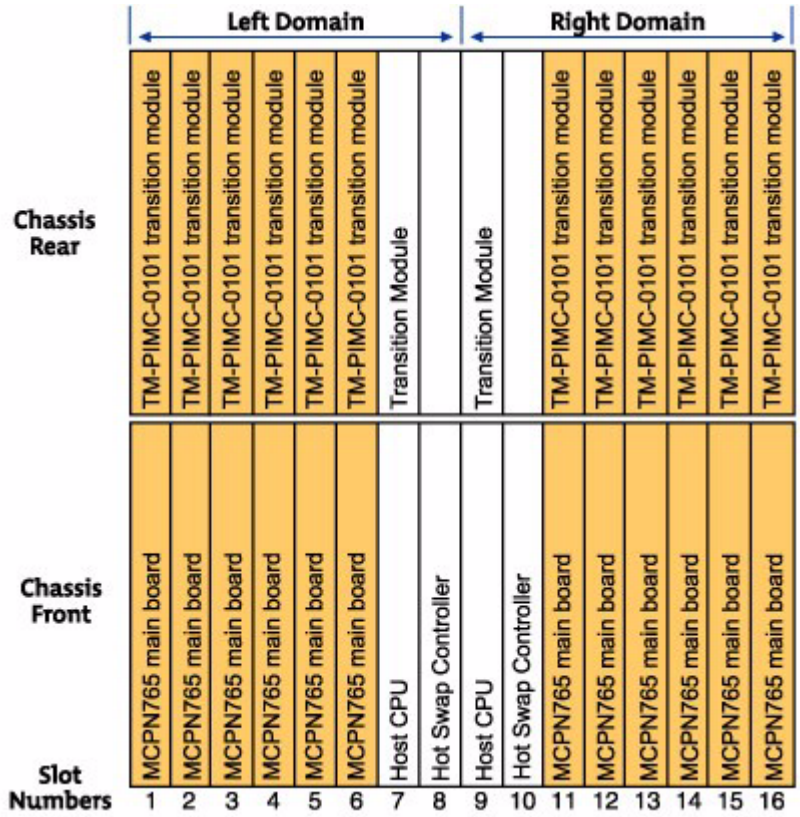
 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

An RTP Media Portal occupies a single chassis domain (side) on a CPX8216T. Therefore, a single CPX8216T can host two RTP Media Portal components (one in chassis Domain A, the other in chassis Domain B).

Note: Chassis domains are not internet domains. This is just another terminology intended to identify Side A and Side B of the chassis. Other terms often used interchangeably are: Domain A and Domain B, as well as Left Domain and Right Domain.

Figure 2 Card slots for the two different domains



Note 1: The Hot Swap Controller in the Left Domain (Domain A) controls the Right Domain (Domain B). The Hot Swap Controller in the Right Domain (Domain B) controls the Left Domain (Domain A).

Note 2: If the chassis is viewed from the front, the slots are numbered from left to right (1-16), and if viewed from the rear, the slots are numbered from right to left (1-16).

The CPX8216T dual 8-slot architecture further refines the domain definition so that each chassis domain is dedicated to a Host CPU board (with an associated transition module in the rear), another slot is

Download from Www.Somanuals.com. All Manuals Search And Download.

dedicated to the Motorola Hot Swap Controller (HSC), and the remaining six slots can be populated with peripheral resource cards (Input/Output cards with an associated transition module in the rear)).

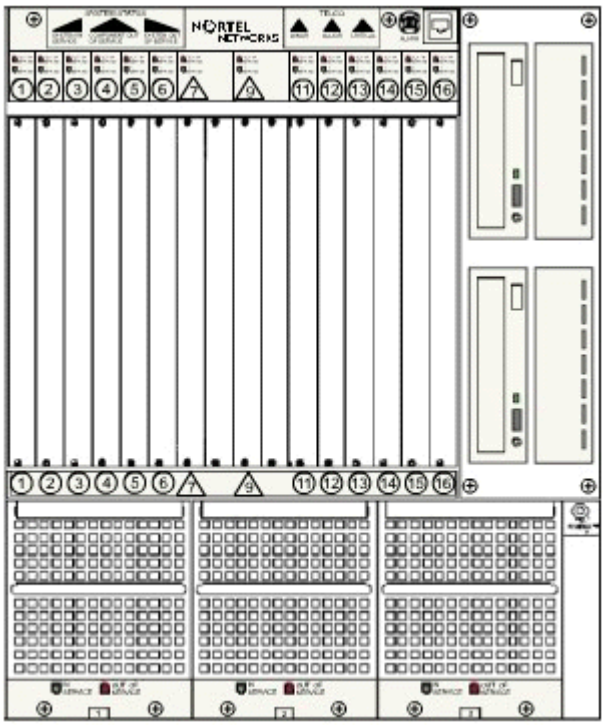
Each chassis half shelf consists of the following hardware components:

- Intel processor board with 1 GB memory and a SCSI Input/Output (I/O) daughter board (CPV5370 host card)
- Hot Swap Controller and Bridge (HSC) module
- SCSI CD-ROM drive
- SCSI hard drive
- Floppy drive
- Motorola MCPN765 card(s) with 64 MB RAM
- Available ac or dc power options

Additional hardware (non-Motorola):

- Mouse, keyboard, monitor

Figure 3 Motorola chassis CPX8216T



 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

Software update maintenance loads

Information on updating software loads for the RTP Media Portal are covered in “Upgrades” on page 13.

OAM&P strategy

The OAM&P strategy for the system is to manage operations from a central location. The central location for OAM&P management is in the System Management Console. From the System Management Console, you can view and perform operations on the various components in the system.

Interfaces

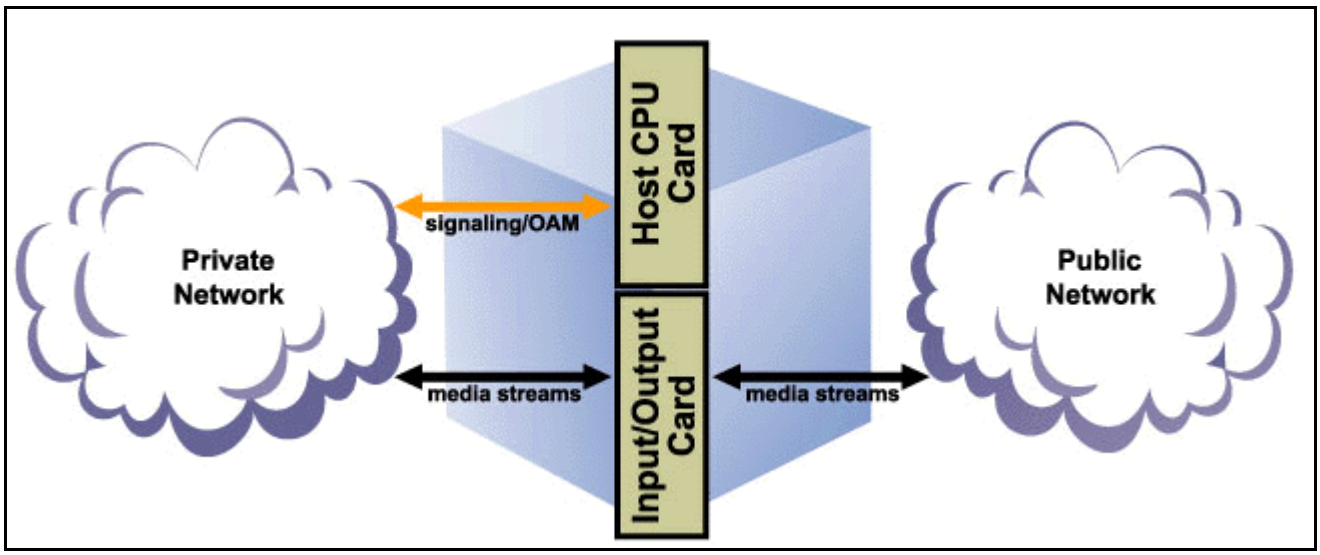
Protocols

While in service, the RTP Media Portal interfaces with the network through the following protocols:

- **MGCP+** is the Enhanced Media Gateway Control Protocol that is used for messaging between the RTP Media Portal and the SIP Application Module, and controls the making, modification and breaking of media session connections.
- **RTP** is the Real-time Transport Protocol for transport of real-time media streams (for example, audio and video) across a packet network.
- **RTCP** is the Real-time Transport Control Protocol that provides a means of sharing session data (for example, performance data) between endpoints.
- **UDP** is the User Datagram Protocol that provides data-based media streams (for example, file transfer).

Download from Www.Somanuals.com. All Manuals Search And Download.

Figure 4 RTP Media Portal interfaces



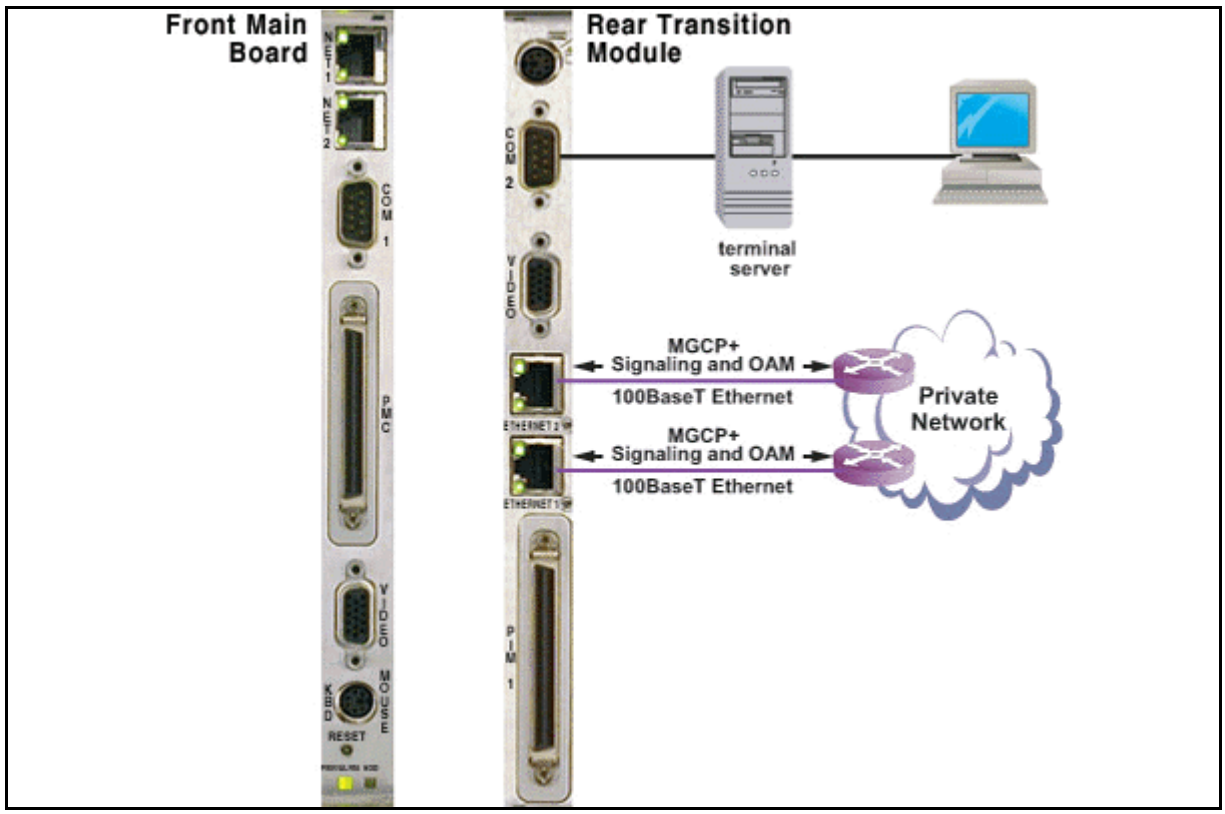
Network Interfaces

The Host CPU card provides the signaling and OAM data interface to/from the Private Network. Each I/O card (commonly referred to as a blade) provides a media stream interface to the Private Network and a media stream interface to the Public Network.

 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

Figure 5 Signaling and OAM interface - CPV5370 Host CPU



The rear transition module for the CP5370 Host Central Processing Unit (CPU) card contains the following:

- COM2 port for connection to a terminal server and local monitor.
- Two Ethernet ports which provide connectivity to the Private Network. The connection carries signaling and OAM data.
  - The Ethernet 1 port is always used to provide an active connection.
  - The Ethernet 2 port provides a standby connection. The standby ethernet function is enabled by default through the “Activate IP Failover” property when configuring the RTP Media Portal. (See Table 2, “RTP Media Portal tab configurable properties,” on page 33.)

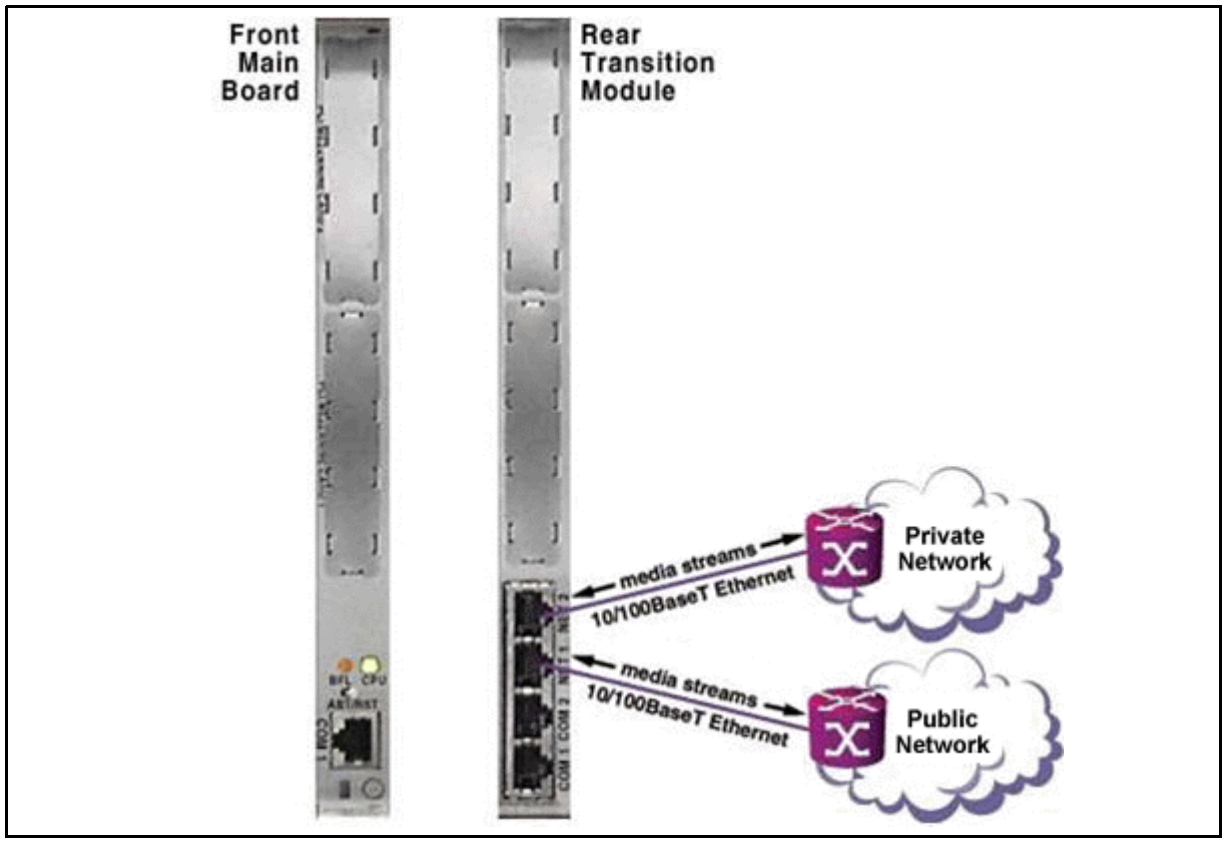
These Ethernet connections carry the following:

- MGCP+ signaling to communicate with the SIP Application Module.
- operations, administration and maintenance (OAM) data to the Management Module.

Download from Www.Somanuals.com. All Manuals Search And Download.

Network interfaces on each of the Input/Output cards (MCPN765) in the RTP Media Portal provide a path for media streams to/from the Private Network and Public Network.

Figure 6 MCPN765 Media stream interface



 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

The RTP Media Portal uses the following input/output (I/O) cards:

- MCPN765 front card
- TM-PIMC-0101 rear transition module

The transition module contains two, 10/100 BaseT Ethernet connections for RTP/RTCP/UDP media streams. Each pair of MCPN765 and TM-PIMC-0101 cards perform the following functions:

- Provides connectivity for RTP/RTCP/UDP media streams to pass between the Private Network and the Public Network, as well as the public to public network.
- Relays media packets between end points.
- Performs Network Address and Port Translation (NAPT) functions.

NET ports

- NET1 port = IP address of Public Network
- NET2 port = IP address of Private Network

The RTP Media Portal Host CPU is only connected to the private network. The RTP Media Portal is an edge component that is dual-homed on the public network and the Private Network. It is the Peripheral I/O cards that span these two distinct networks.

User interfaces

The System Management Console is used for fault and configuration management of the RTP Media Portal. RTP Media Portal management data is stored on both the Management Module and the Database Module. The Management Module stores alarm, log, and OM data. The Database Module stores configuration data.

Download from Www.Somanuals.com. All Manuals Search And Download.

 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

Upgrades

How this chapter is organized

This chapter is organized as follows:

OAM&P strategy

RTP Media Portal software upgrade

This section describes the update strategy for the RTP Media Portal. The RTP Media Portal run-time sub-component can be upgraded by deploying the new software to the target node from the System Management Console.

Note: The SIP Application Module may try to contact the RTP Media Portal while the upgrade is in progress, thus 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 is still processing established media sessions. These pre-existing media sessions will slowly become inactive as the calls end. The RTP Media Portal will automatically transition 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.

Updating the software of the new run-time sub-component(s) from the System Management Console can commence.

A reset is then issued to the RTP Media Portal from the System Management Console. This reboots the host CPU, which in turn

Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

reboots the Peripheral CPUs. When the RTP Media Portal recovers from the reset, it is running (UNLOCKED) with the upgraded software.

Note: It is possible to update one RTP Media Portal and reboot it while the other half shelf is running the load that has not been updated. Once one half shelf is updated, the other half shelf can be locked, updated, and rebooted. **Upgrading all RTP Media Portals concurrently will cause a service outage.**

The length of outage due to the reboot is approximately 3-5 minutes.

Note 1: Software loads are encrypted for security reasons.

Note 2: If a component upgrade fails, it does not roll back automatically. A roll back prompt appears. If the upgrade is not successful, note as much of the event as possible and contact your next level of support.

Task flows

To avoid any problems with the SIP Application Module, 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. Shutdown the RTP Media Portal component. See “Shutdown the RTP Media Portal component” on page 14.
2. Update the software load for the RTP Media Portal component. See “Update a software load” on page 15.

Shutdown the RTP Media Portal component

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

From the System Management Console

1. Select the RTP Media Portal Server, select Components and then select the appropriate RTP Media Portal component.
2. To Shutdown the component, either right-click and select **Shutdown** or select **Shutdown** from the Operations menu.
3. The RTP Media Portal component will shutdown gracefully and go into a LOCKED state, as seen in the General Information Area of the System Management Console.

 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

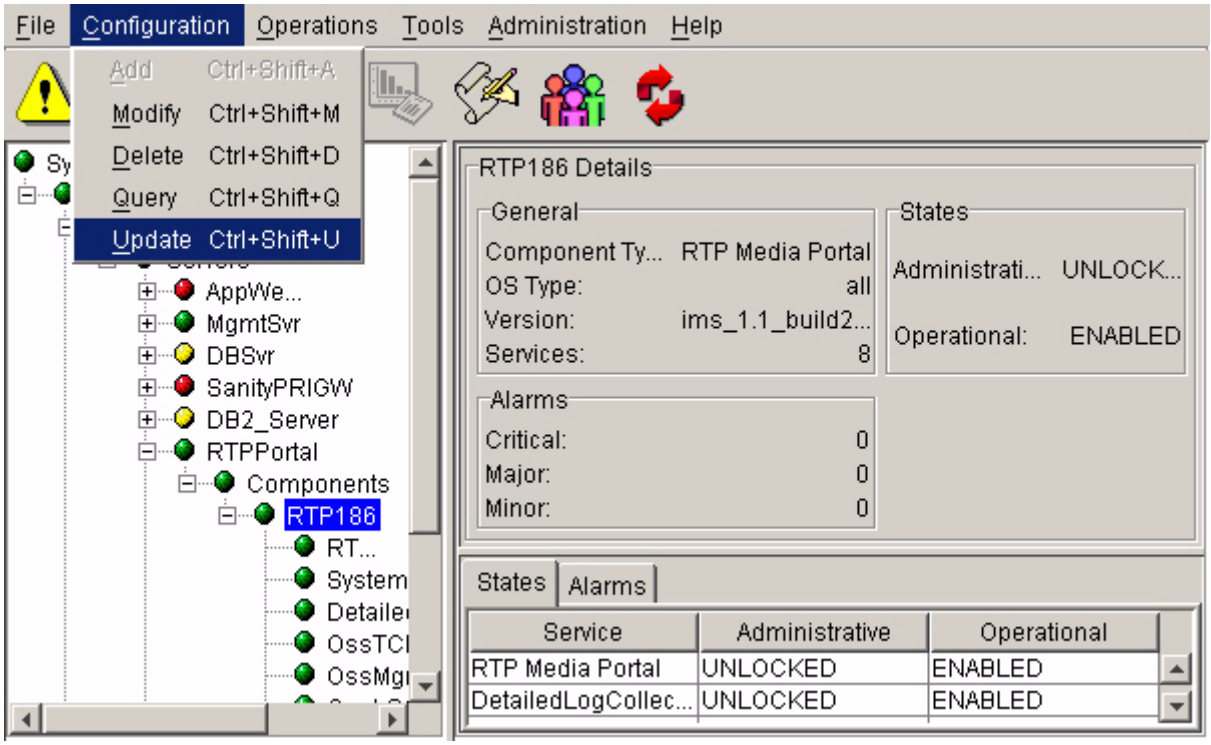
Update a software load

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

From the System Management Console

1 Select the RTP Media Portal Server, select Components, right-click the desired component and select **Update**.

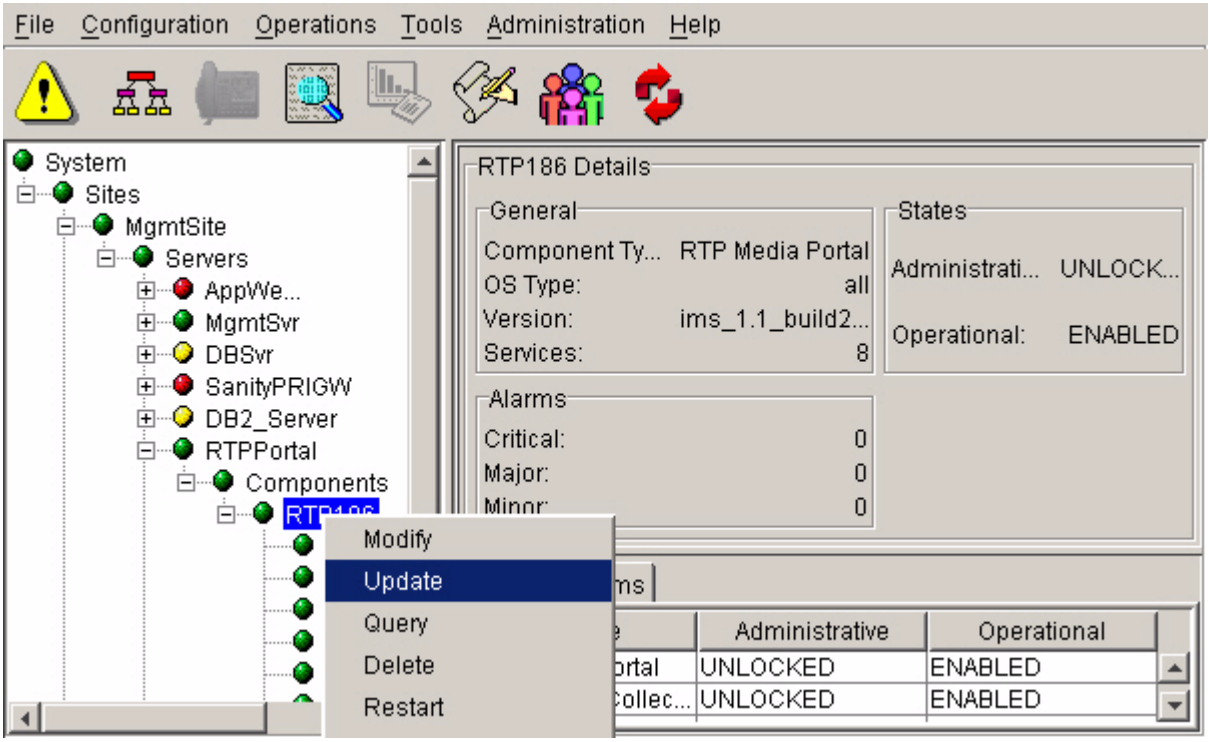
Figure 7 Updating the RTP Media Portal from the menu tree



You can also launch the update from the pull-down Configuration menu, as shown:

Download from Www.Somanuals.com. All Manuals Search And Download.

Figure 8 Updating the RTP Media Portal from the pull-down menu



After selecting **Update**, the following window appears:

Figure 9 The update window, retrieving the load list

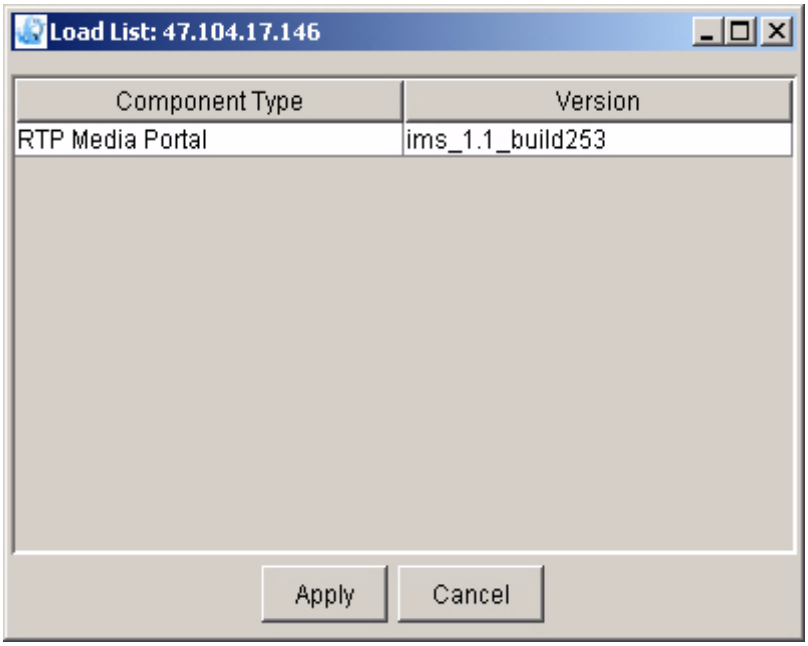
 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

2 You can only do an update from one version to another.

Note: The currently deployed software load will not appear in the load list.

Figure 10 Load list for updating



3 Select the load version that should be used to update the RTP Media Portal. Click on the **Apply** button.

4 The System Management Console displays the four tabs that can be reconfigured. Modify any configuration values you need.

Note 1: Configuration fields ranges are detailed in the Configuration section of this document.

Note 2: If an older version of the RTP Media Portal software is deployed, it may not work with a newer version of the components already installed. Administrators should upgrade as per the release notes provided with each release.

5 Click on the **Apply** button.

6 Once the update is complete, the following window appears:

Download from Www.Somanuals.com. All Manuals Search And Download.

Figure 11 Successful update dialog box

 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

Fault management

How this chapter is organized

This chapter is organized as follows:

Network fault management strategy

The system handles network fault management through the reporting of alarms and logs. RTP Media Portal alarms and logs are viewed from the System Management Console. (See the *MCP System Management Console Basics* for further details related to alarms and logs.)

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 the basic mechanism that ensures resource availability and utilization in the event of a SIP Application Module failure. This function works in tandem with SIP Application Module redundancy to ensure that RTP Media Portal resources continue to be used in the event of a SIP Application Module failure. The RTP Media Portal is configured to "pre-register" its availability with the Standby SIP Application Module. This configuration enables the Standby SIP Application Module to immediately begin utilization of the RTP Media Portal for session requests

Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

whenever a failure condition occurs on the Active SIP Application Module.

- 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 maintain capacity and performance in the wake of a SIP Application Module failure that causes the isolation of active media sessions.
- 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 SIP Application Module. This capability enables the system to permit media sessions to continue through to completion in the wake of SIP Application Module failure.
- Shared Resource
  - enables the distribution of RTP Media Portal resources to multiple SIP Application Modules. 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 across the entire network, but not necessarily a service outage, since there are many other RTP Media Portals available to many SIP Application Modules.

Fault management procedures

Alarm surveillance

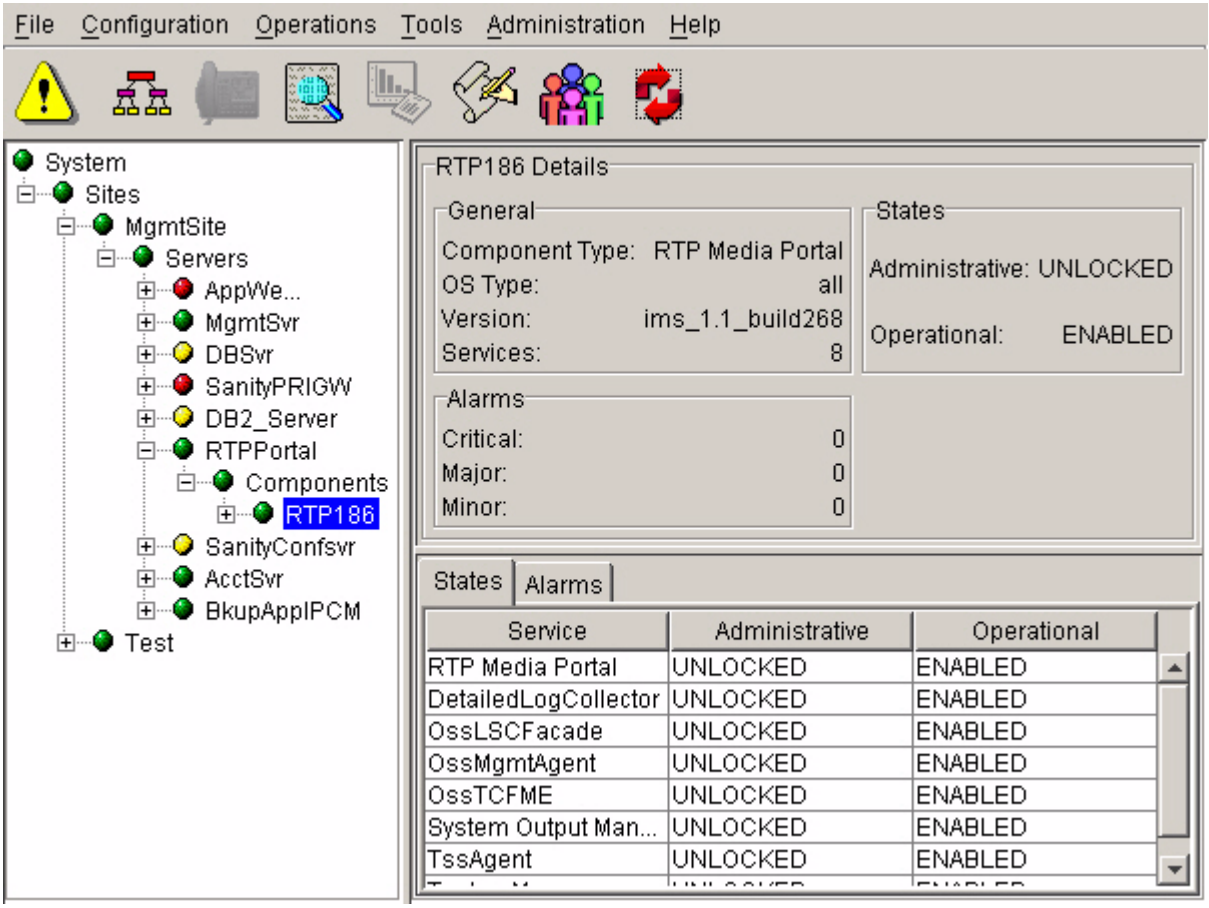
From the System Management Console

1. From the System Management Console, under the RTP Portal Components folder, highlight the appropriate RTP Media Portal.
2. The main screen appears to the right and describes RTP Media Portal component details such as general details, CPU usage, Disk Usage, I/O Usage, and Alarms.
3. Below the status details, click the alarm tab to view the service component and what severity of an alarm is raised against it. For alarm severity classification, refer to the *MCP System Management Console Basics.*

 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

Figure 12 Example of viewing alarm information



Clearing an alarm

From the System Management Console

1 From the System Management Console, under the RTP Portal Components folder, highlight the appropriate RTP Media Portal.

2 From the toolbar, select Tools, alarm browser.

3 An alarm table appears displaying the alarms.

4 Double click the alarm row. Information regarding the alarm and necessary steps to clear the alarm appear in the information screen at the bottom of the alarm window.

5 Follow the steps to clear the alarm.

Note: These steps are defined in “RTP Media Portal Alarms” on page 22.

Download from Www.Somanuals.com. All Manuals Search And Download.

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 the *MCP System Management Console Basics*.

Clearing the RTP101 Alarm (Blade out of service)

1. Verify that you can log in to the blade (card) from the host. If successful, the private network connection is OK.
2. Once you are logged in to the blade, verify the blade can reach the default gateway: Ping the gateway IP address from the blade. If successful, the public network connection is OK.
3. Contact your next level of support with the results of these tests.

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

1. Verify that you can log in to the host. If successful, the private network connection to the host is OK.
2. Once you are logged in to the host, verify that each of the available blades is reachable (ping each blade).
3. Log in to a blade. Verify the blade can reach the default gateway: Ping the gateway IP address from the blade. If successful, the public network connection is OK.
4. Repeat for each blade.
5. Contact your next level of support with the results of these tests.

Clearing the RTP103 Alarm (Best Blade Selection)

1. Verify that you can log in to the blade (card) from the host. If successful, the private network connection is OK.
2. Once you are logged in to the blade, verify the blade can reach the default gateway: ping the gateway IP address from the blade. If successful, the public network connection is OK.
3. Repeat for each blade.
4. Verify that the correct number of public/private ports have been configured. Use the query tool in the System Management Console.
5. Contact your next level of support with the result of these tests.

Clearing the RTP104 Alarm (Public Port Usage)

1. Wait for at least two audit cycles to see if the alarm is cleared automatically. An audit cycle has a duration defined by the “Idle Session Audit Period” property.

 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

2 If the alarm persists, the number of available ports per blade (card) and/or the number of blades (cards) in the system must be increased. To increase the number of ports or the number of blades, contact your next level of support.

Clearing the RTP105 Alarm (Private Port Usage)

1 Wait for at least two audit cycles to see if the alarm is cleared automatically. An audit cycle has a duration defined by the “Idle Session Audit Period” property.

2 If the alarm persists, the number of available ports per blade (card) and/or the number of blades (cards) in the system must be increased. The recommended maximum ports per blade is 300.

3 If it is not possible to increase the number of ports or the number of blades, contact your next level of support.

Logs

System logs are discussed in detail in the *MCP Management Module Basics*.

Download from Www.Somanuals.com. All Manuals Search And Download.

 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

Configuration management

How this chapter is organized

This chapter is organized as follows:

Network strategy

The network strategy is to configure all of the components in a central location. The central location for configuration is the System Management Console.

The following sections provide information on configuring the RTP Media Portal.

Configuration procedures

Login to the System Management Console. For detailed procedures on logging into the System Management Console, refer to the *MCP System Management Console Basics*.

Adding the RTP Media Portal component

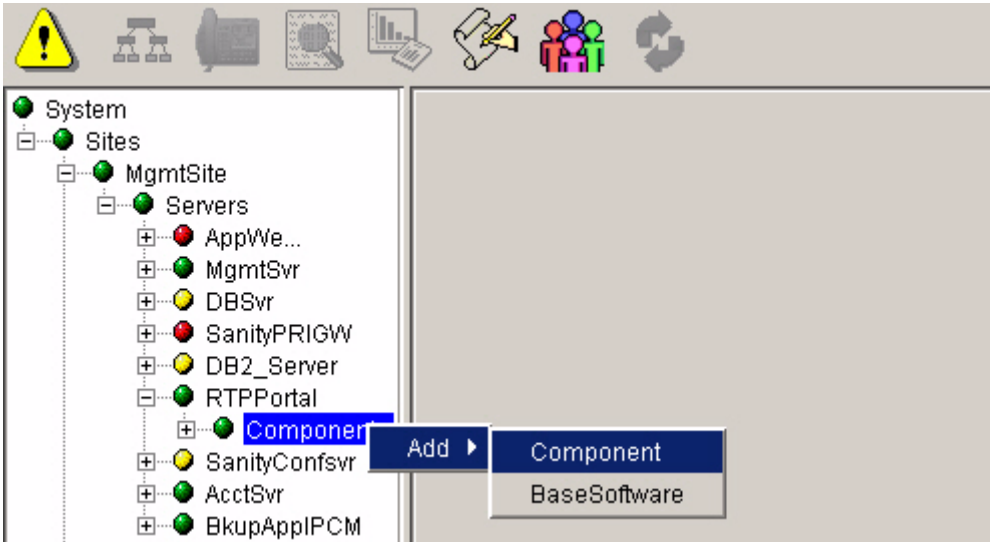
This procedure assumes that the server on which the RTP Media Portal will be deployed, has already been configured. For example, Figure 13, "Adding the RTP Media Portal component" on page 26 shows the RTP Media Portal component being deployed onto the previously configured server, "RTP Portal".

From the System Management Console

1 To add the RTP Media Portal component, right-click on Component under the Server definition and select Add > Component as shown in Figure 13, "Adding the RTP Media Portal component" on page 26.

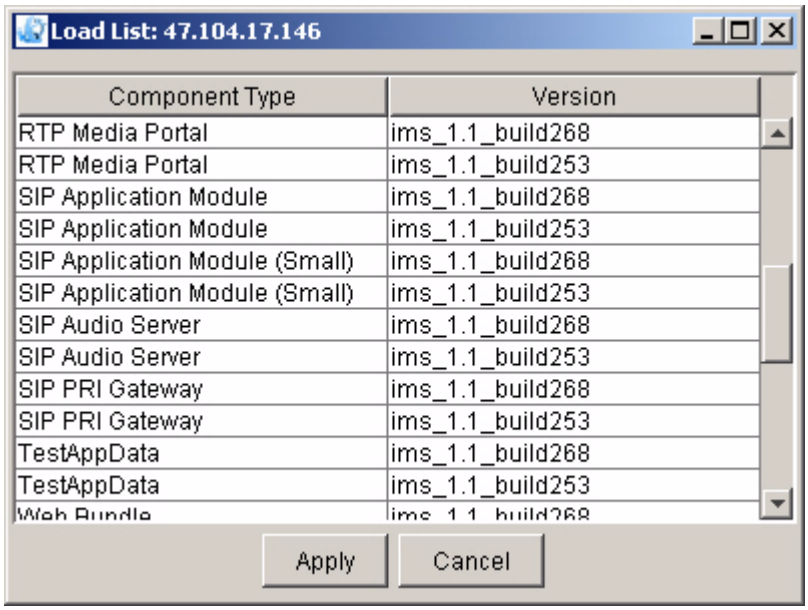
Download from Www.Somanuals.com. All Manuals Search And Download.

Figure 13 Adding the RTP Media Portal component



2 You will be prompted to choose a software load.

Figure 14 Software load list



3 Select the desired software load version for the RTP Media Portal and click **Apply**.

4 You will be prompted to configure the RTP Media Portal.

5 Configure the RTP Media Portal properties as described in “Configuration tabs and properties” on page 27. (For configuration property details, place your cursor over the property and a definition help box will pop up.)

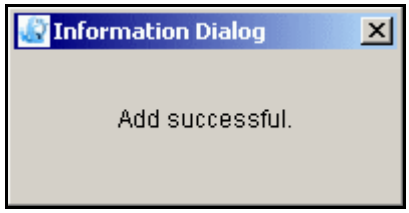
 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

6 Enter a label in the Service Component Name field at the bottom of the window and click **Apply**.

7 When deployment completes, there is a screen showing that the component was added successfully.

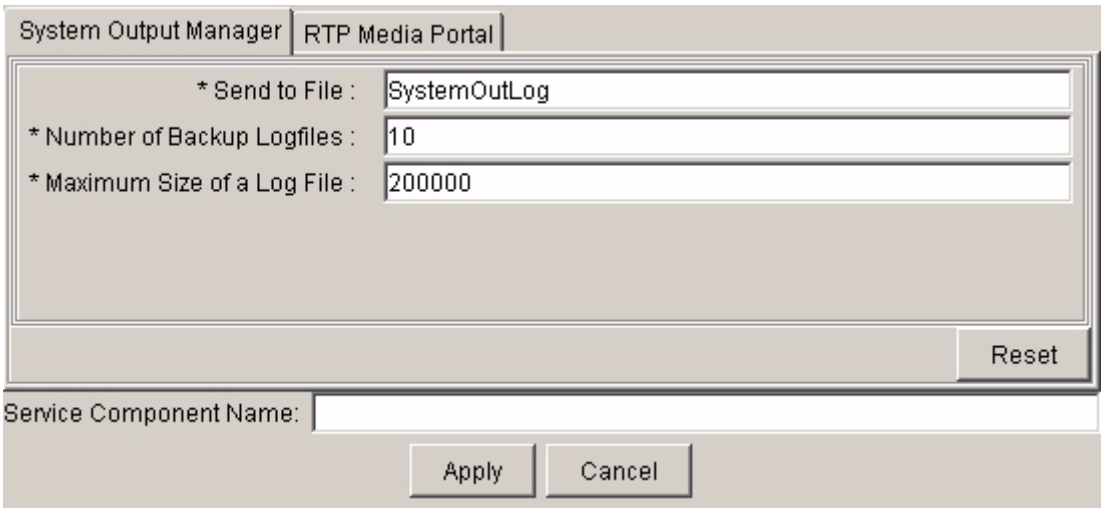
Figure 15 Add successful dialog box



Configuration tabs and properties

The following figure shows the configurable properties of the System Output Manager tab:

Figure 16 System Output Manager tab



Download from Www.Somanuals.com. All Manuals Search And Download.

The following table details the configurable properties of the System Output Manager tab:

Table 1 System Output Manager tab configurable properties

Configuration Property	Format	Description
Send to File	Type: String Range: Null, 1-500 characters Default: SystemOutLog	Name of file that additional detailed logs should be sent to.
Number of Backup Logfiles	Type: Integer Range: N/A Default: 10	Number of logfiles that should be kept.
Maximum Size of a Log File	Type: Integer (bytes) Range: 200000-2147483647 Default: 200000	Maximum size of the log file in bytes. When this size is reached, the log file is rotated.

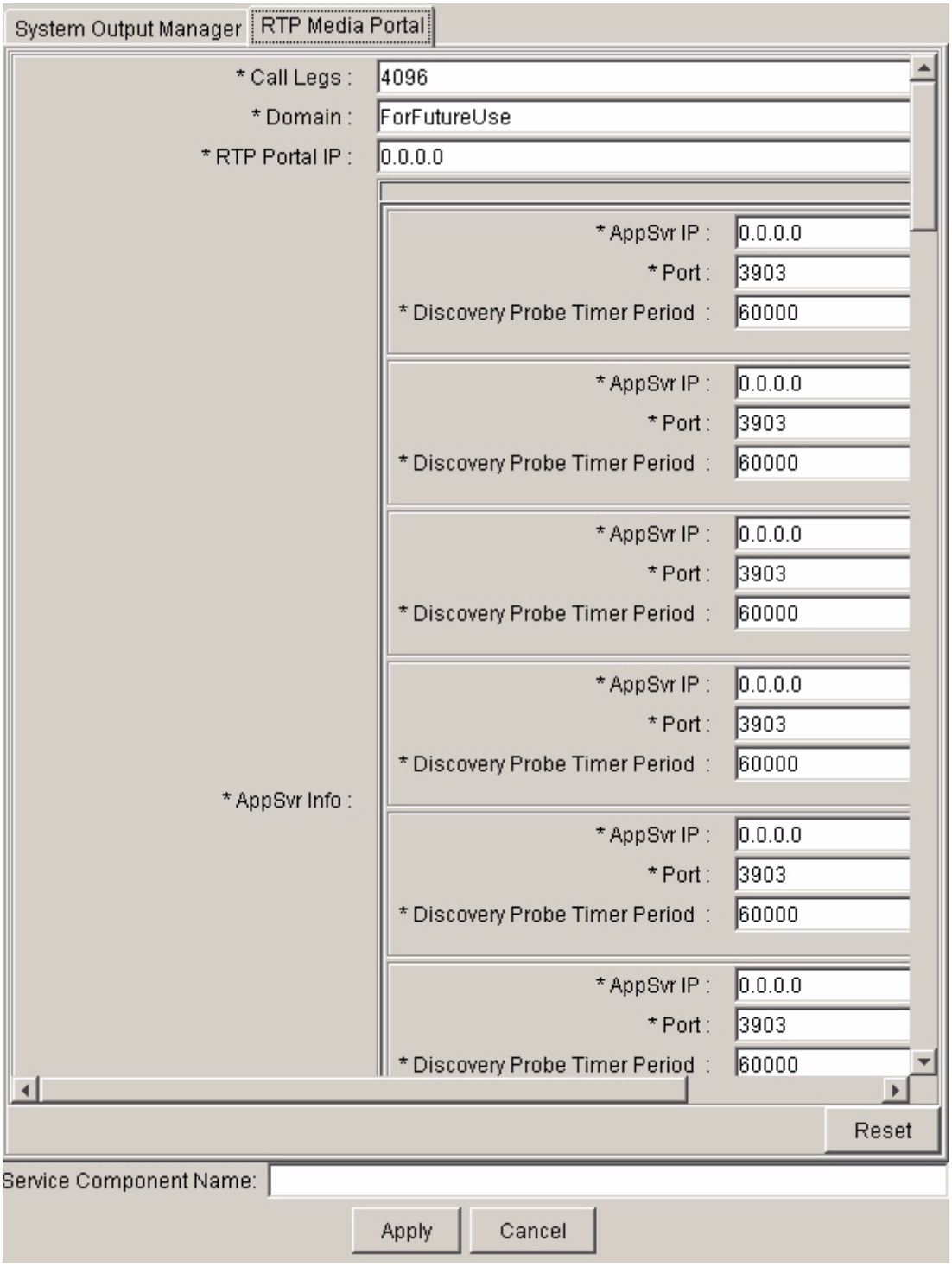
The following figures show the configurable properties of the RTP Media Portal tab:

Note: The configurable properties of the RTP Media Portal tab span more than one page and so, are shown in the next four figures.

 Copyright © 2003, Nortel Networks

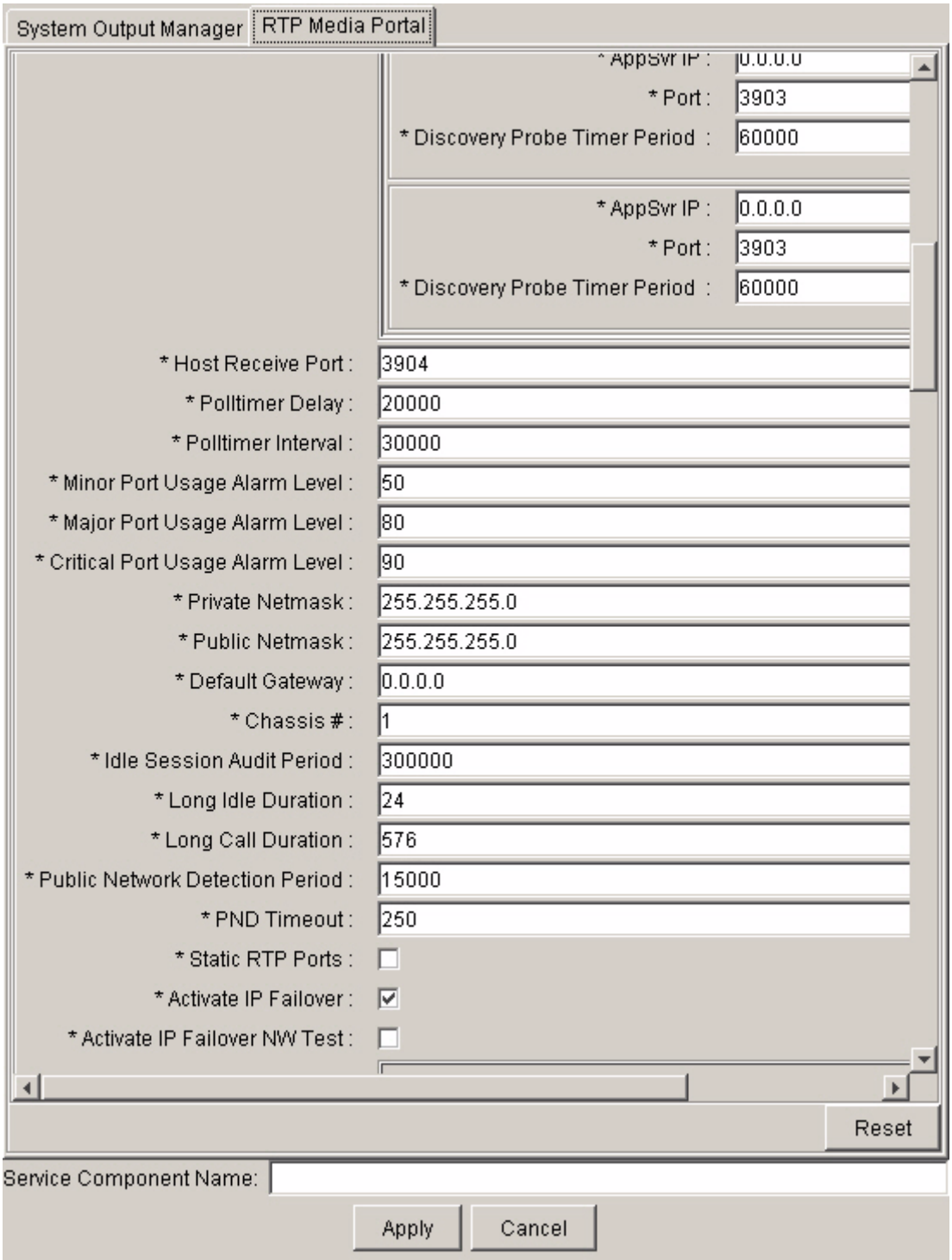
Download from Www.Somanuals.com. All Manuals Search And Download.

Figure 17 RTP Media Portal tab (1 of 4)



Download from Www.Somanuals.com. All Manuals Search And Download.

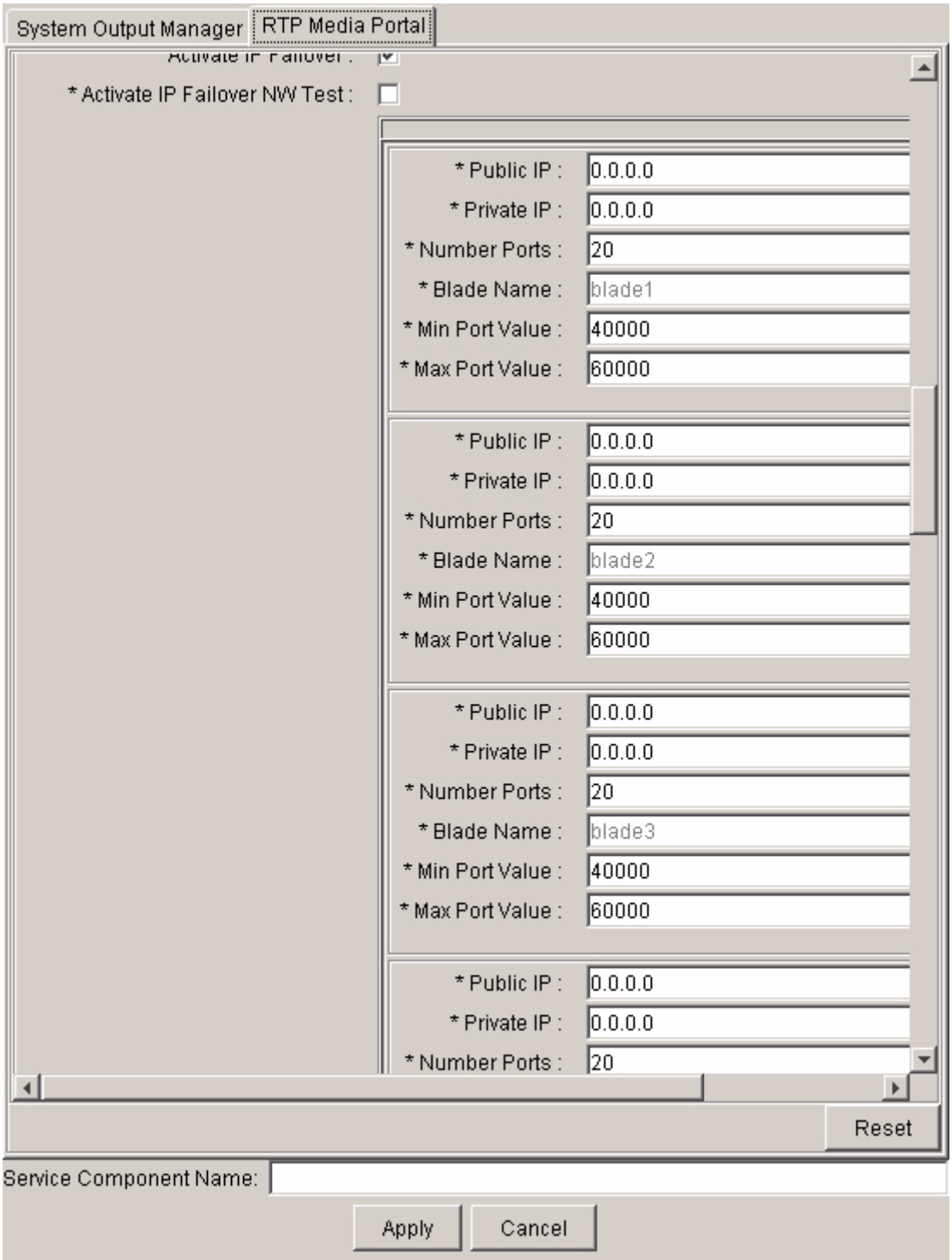
Figure 18 RTP Media Portal tab (2 of 4)



 Copyright © 2003, Nortel Networks

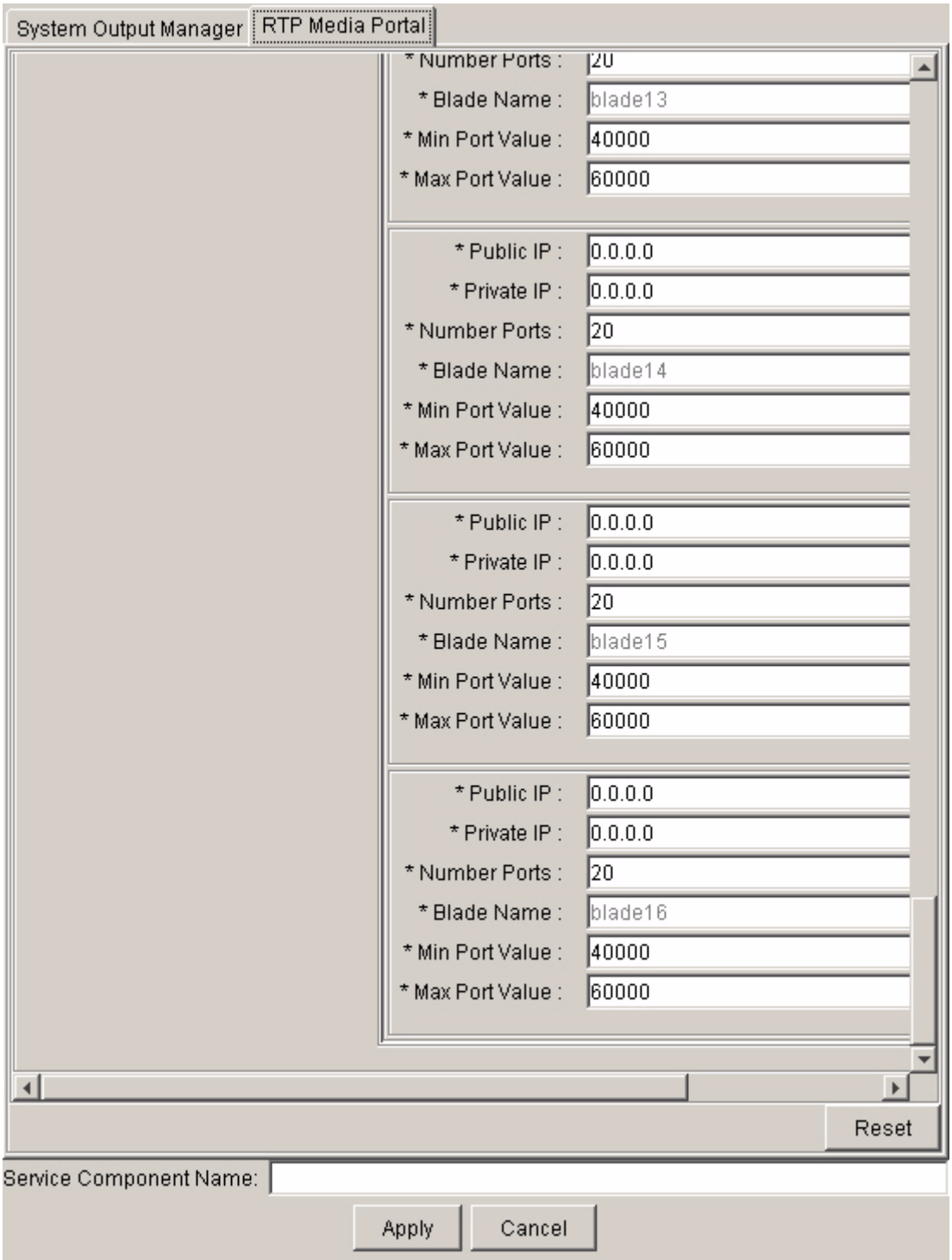
Download from Www.Somanuals.com. All Manuals Search And Download.

Figure 19 RTP Media Portal tab (3 of 4)



Download from Www.Somanuals.com. All Manuals Search And Download.

Figure 20 RTP Media Portal tab (4 of 4)



 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

The following table details the configurable properties of the RTP Media Portal tab:

Table 2 RTP Media Portal tab configurable properties

Configuration Property	Format	Description
Call Legs	Type: String Range: 4096-MaxInt Default: 4096	Controls the number of simultaneous transactions.
Domain	Type: String Range: 1-20 characters Default: For future use	Domain in which the RTP Portal will operate. For future use.
RTP Portal IP	Type: String Range: 7-15 characters Default: 0.0.0.0	Private IP Address of the RTP Media Portal host. Identifies a specific host. **Note:** This value must be unique.
AppSvr IP	Type: String Range: 7-15 characters Default: 0.0.0.0	Private IP Address of SIP Application Module to which this portal is assigned. **Note:** In a redundant configuration, the value for this property must be set to the private static address of each SIP Application Module in the network.
Port	Type: String Range: 1025-65535 Default: 3903	Port on which the SIP Application Module is listening for MGCP+ messaging from the media portal. It must match the associated setting on the SIP Application Module. **Note:** The use of the default value for this property is highly recommended.

Download from Www.Somanuals.com. All Manuals Search And Download.

Table 2 RTP Media Portal tab configurable properties

Discovery Probe Time Period	Type: String Range: 0-3600000 Default: 60000	Controls the frequency (in milliseconds) of registration messages (RSIPs) sent from the RTP Media Portal to the SIP Application Module in the absence of MGCP+ messaging from the SIP Application Module.
Host Receive Port	Type: String Range: 1025-65535 Default: 3904	Port on which the RTP Media Portal listens for MGCP+ messaging from the SIP Application Module. **Note:** The use of the default value for this property is highly recommended.
Polltimer Delay	Type: String Range: 0-65535 Default: 20000 milliseconds	Time span (in milliseconds) required for startup and initialization of the cards. The host CPU waits this period of time before attempting to contact the cards. (This is how long the host waits to talk to the cards to ask if they are up yet.) **Note:** The use of the default value for this property is highly recommended.
Polltimer Interval	Type: String Range: 0-65535 Default: 65000 milliseconds	Interval (in milliseconds) at which the host polls the blades to ensure they are still available. (Intermediate checks just to make sure the blade is still up.) **Note:** The use of the default value for this property is highly recommended.
Minor Port Usage Alarm Level	Type: Percent Range: 0-100 Default: 50	The percent usage at which the number of ports used on the public or private side of an RTP Media Portal (over all blades) causes a minor alarm.

 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

Table 2 RTP Media Portal tab configurable properties

Major Port Usage Alarm Level	Type: Percent Range: 0-100 Default: 80	The percent usage at which the number of ports used on the public or private side of an RTP Media Portal (over all blades) causes a major alarm.
Critical Port Usage Alarm Level	Type: Percent Range: 0-100 Default: 90	The percent usage at which the number of ports used on the public or private side of an RTP Media Portal (over all blades) causes a critical alarm.
Private Netmask	Type: IP address Range: N/A Default: 255.255.255.0 **(Default gateways are for the cards, not for the host.)**	The Private Network Mask is used for routing on the Private network.
Public Netmask	Type: IP address Range: N/A Default: 255.255.255.0 **(Default gateways are for the cards, not for the host.)**	The Public Network Mask is used for routing on the Public network.
Default Gateway	Type: IP Address Range: N/A Default: 0.0.0.0	The Default Gateway is the gateway router to the rest of the world (the default route). **Note:** If this value is not filled in, the RTP Media Portal will fail to provide service. The RTP Media Portal will not provide service unless the blades can communicate with the specified Default Gateway.

Download from Www.Somanuals.com. All Manuals Search And Download.

Table 2 RTP Media Portal tab configurable properties

Chassis #	Type: String Range: 0-255 Default: 1	Chassis identifier used to identify a specific CPX8216T chassis. This information is used by configuration scripts to synchronize RTP Media Portal configuration across multiple CX8216T chassis. Must be unique per chassis. Must match the Chassis # assigned to the blades during the staging of the portal.
Idle Session Audit Period	Type: String Range: 0-3600000 Default: 300000 (ms)	The period of the audit that runs to detect idle media sessions on the Peripheral CPU (Blade).
Long Idle Duration	Type: String Range: 0-65535 Default: 24	This represents the maximum amount of time that a RTP Media Portal resource may remain validly idle. This has units of number of IdleSessionAuditPeriods.
Long Call Duration	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.
Public Network Detection Period	Type: String Range: 0-3600000 Default: 15000	The period of the audit that runs to detect the Public network interface on the Peripheral CPU (Blade). This has units of milliseconds. If the value is set to zero, then the audit is disabled.
PND Timeout	Type: String Range: 0-10000 Default: 250	The amount of time that the Public Network Detection algorithm will wait for a response to a query sent to the default gateway. This has units of milliseconds. If the value is zero, no query will be made to the default gateway.

 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

Table 2 RTP Media Portal tab configurable properties

Static RTP Ports	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 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 streams and the odd-numbered ports are used for RTCP streams.
Activate IP Failover	Type: Boolean Range: true/false Default: true	Enables the RTP Media Portal Host CPU to monitor the status of the Private network Interface and react accordingly. This basic capability enables the system to maintain service availability in the wake of Private network failures. Whenever an RTP Media Portal Host CPU detects that it is having problems with its Private network interface, the Host switches to another available Private network interface. **Note:** There are two tests associated with the activation of Host IP Failover: a carrier sense test and an optional network (ping) test. Upon activation of Host IP failover, the carrier sense test is automatically provided. Enabling of the optional network test is controlled by the “Activate IP Failover NW Test” configuration parameter. Enabling the optional network test will generate a periodic ping to the default gateway on the private network which was configured during installation and commissioning.

Download from Www.Somanuals.com. All Manuals Search And Download.

Table 2 RTP Media Portal tab configurable properties

Activate IP Failover NW Test	Type: Boolean Range: true/false Default: false	This configuration parameter is associated with the “Activate IP Failover” configuration parameter. Please refer to **Note** in description of the “Activate IP Failover” configuration parameter for details.
Public IP	Type: IP Address Range: 7-15 characters Default: 0.0.0.0	The Public IP address of this particular blade. Repeated for each blade.
Private IP	Type: IP Address Range: 7-15 characters Default: 0.0.0.0	The Private IP address for this particular Blade. Repeated for each Blade.
Number Ports	Type: Positive Integer Range: 0-65535 Default: 20	Number of ports (this many private and this many public) configured on this blade. Controls maximum allowable simultaneous media streams permitted on this particular Blade. Repeated for each Blade.
Blade Name	Type: Text Range: blade1-blade16 Default: blade1, blade 2, etc.	String describing this particular Blade. Repeated for each Blade. **Note:** This field is not configurable.
Min Port Value	Type: Positive Integer Range: 0-65535 Default: 40000	Minimum port range value.
Max Port Value	Type: Positive Integer Range: 0-65535 Default: 60000	Maximum port value.

 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

Accounting management

Strategy

The RTP Media Portal does not perform any accounting management. For more information on accounting, see the *MCP Accounting Module Basics.*

Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

Performance management

Strategy

RTP Media Portal performance is monitored through the System Management Console GUI by viewing Operational Measurements. Refer to the *MCP System Management Console Basics* for information on OMs and viewing OMs.

Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

Security and Administration

How this chapter is organized

This chapter is organized as follows:

Security strategy overview

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

Blade (IP address) randomization

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

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

Port randomization

When the RTP Media Portal is deployed, each blade is assigned a pool of ports with 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,

Download from Www.Somanuals.com. All Manuals Search And Download.

refer to Table 2, “RTP Media Portal tab configurable properties” on page 33.

As multimedia sessions are initiated, a port is chosen from the port pool associated with the selected blade. 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 blades.

NAPT function

In order to obscure the private 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 and logged as potential problems.

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 SIP Application Module (which has pre-authenticated such requests) and by rejecting any unauthorized packets on an active connection.

Authenticated requests

All requests to manipulate the media resources on the RTP Media Portal originate from the SIP Application Module. The SIP Application Module ensures that all requests are made by, or made to, a valid service subscriber. In this way, the SIP Application Module 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 private network.

Packet filter/firewall

As packets are received from the public network, 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 and logged as problems.
- the source/destination addresses match the expected source/destination addresses indicated in the session description.

 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

Packets that do not have a matching source/destination address are discarded and logged as potential problems.

- 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 and logged as potential problems.

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 the *MCP System Management Console Basics.*

Download from Www.Somanuals.com. All Manuals Search And Download.

 Copyright © 2003, Nortel Networks

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

Succession Multimedia Communications Portfolio

MCP RTP Media Portal

Basics

Copyright © 2003 Nortel Networks,
All Rights Reserved

NORTEL NETWORKS CONFIDENTIAL: The information contained in this document is the property of Nortel Networks. Except as specifically authorized in writing by Nortel Networks, the holder of this document shall keep the information contained herein confidential and shall protect same in whole or in part from disclosure and dissemination to third parties and use same for evaluation, operation, and maintenance purposes only. Changes or modifications to the MCP RTP Media Portal without the express consent of Nortel Networks may void its warranty and void the user's authority to operate the equipment.

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

*Nortel Networks, the Nortel Networks logo, the Globemark, UNIStim, MCP, Nortel, Northern Telecom, and NT, are trademarks of Nortel Networks.

Publication number: NN10035-111
Product release: MCP 1.1 FP1 Standard
Document release: Standard MCP 1.1 FP1 (02.02)
Date: April 2003
Printed in the United States of America.

Download from Www.Somanuals.com. All Manuals Search And Download.

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com