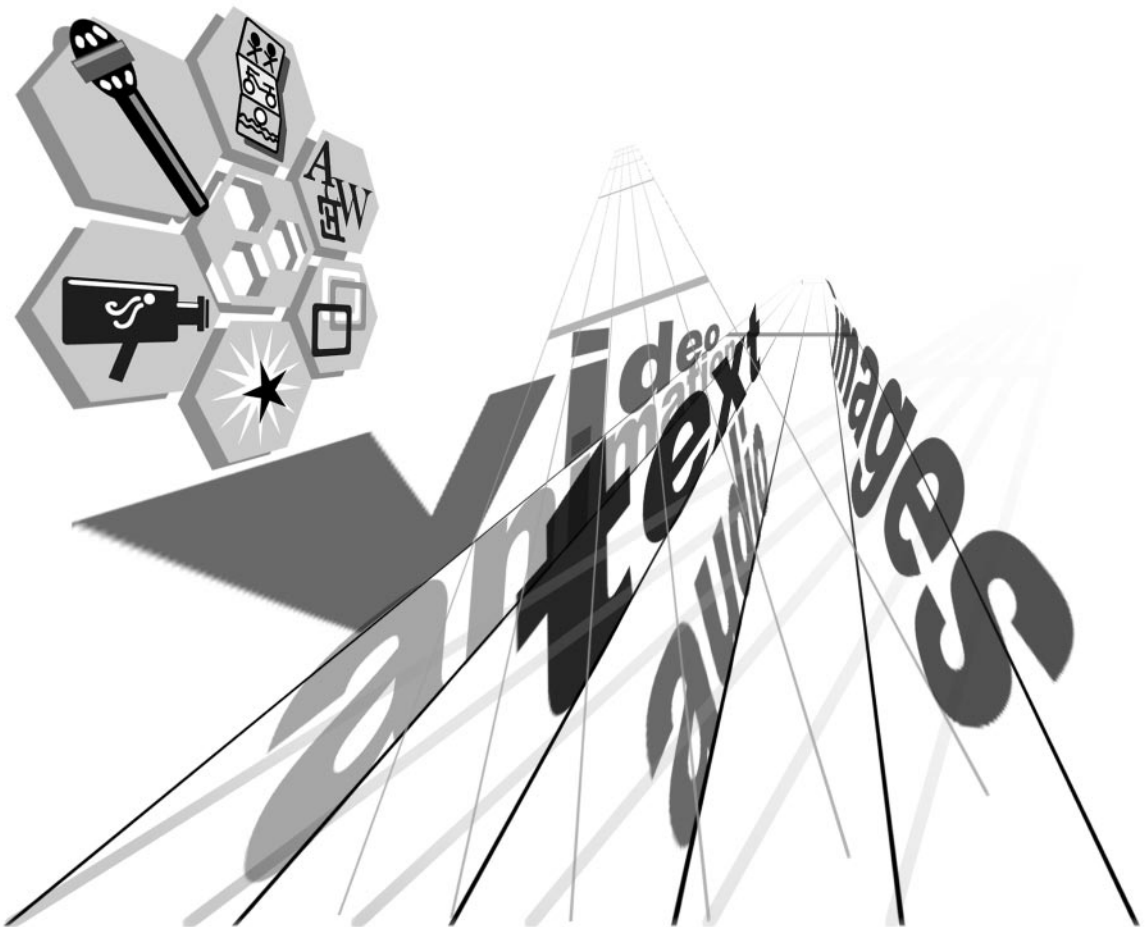




REALPROXY G2 ADMINISTRATION GUIDE

BETA ONE



Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of RealNetworks, Inc.

© 1999 RealNetworks, Inc.

RealAudio, RealVideo, and RealPlayer are registered trademarks of RealNetworks, Inc.

The Real logo, RealServer, RealPlayer Plus, RealText, RealPix, RealAudio Encoder, RealVideo Encoder, RealEncoder, RealPublisher, RealProducer, RealProducer Plus, RealProducer Pro, SureStream, RealBroadcast Network, and RealSystem are trademarks of RealNetworks, Inc.

RealFlash is a trademark of Macromedia, Inc. and RealNetworks, Inc.

Macromedia is a registered trademark and Flash and Shockwave are trademarks of Macromedia, Inc.

STiNG is a trademark of Iterated Systems, Inc.

ACELP-NET codec used under license from Université de Sherbrooke. Sipro Lab Télécom, Inc. Copyright ©1994-1997. All rights reserved.

DolbyNet is a trademark of Dolby Laboratories, Inc.

Dolby Digital AC-3 audio system manufactured under license from Dolby Laboratories.

Apple, Macintosh, and Power Macintosh are registered trademarks of Apple Computer, Inc.

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks and ActiveX is a trademark of Microsoft Corporation.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation.

Pentium is a registered trademark and MMX and the Intel Optimizer Logo are trademarks of Intel Corporation.

Sonic Foundry and Sound Forge are registered trademarks of Sonic Foundry, Inc.

Other product and corporate names may be trademarks or registered trademarks of other companies. They are used for explanation only, with no intent to infringe.

RealNetworks, Inc.
1111 Third Avenue, Suite 2900
Seattle, WA 98101 USA

<http://www.real.com>



CONTENTS

	Overview.....	9
	How This Manual Is Organized	9
	Conventions in This Manual	11
	Additional RealSystem Resources	12
	Technical Support.....	12
1	OVERVIEW	15
	How RealProxy Works	15
	Media Cache Software	17
	Modes of Operation.....	18
	Passthrough.....	18
	Cache Integration	19
	Bitsave.....	21
	Pull Splitting	22
	Requirements for Each RealProxy Mode	22
	Interaction with RealServer	22
	Controlling Client Access.....	23
	Denying Client Access.....	23
	Tracking Activity.....	23
	Cache Requests.....	23
	When RealProxy Will Not Conserve Bandwidth	24
	Additional Features	24
	Administration.....	24
	Setting Up Clients	25
	Limiting Network Traffic.....	25
	Chaining One RealProxy to Another	25
	Monitoring RealProxy in Real Time.....	26
	Tracking RealProxy Activity	26
	Protocols	26
2	STARTING AND STOPPING REALPROXY	29
	Windows	29
	Starting RealProxy Under Windows	29
	Stopping RealProxy Under Windows	32
	UNIX.....	32

	Starting RealProxy Under UNIX.....	33
	Stopping RealProxy Under UNIX.....	34
	Configuring MIME Types	34
	License Information	36
3	CONFIGURING REALPROXY FEATURES	39
	Configuring RealProxy Using RealSystem Administrator	39
	Starting RealSystem Administrator.....	39
	Using RealSystem Administrator	40
	Restricting Access to RealSystem Administrator.....	41
	Configuration File	41
	Editing the Configuration File with a Text Editor	42
	Common Settings	43
	Port Variables	43
	Configuring RealProxy Features.....	43
	Passthrough Mode.....	44
	Bitsave Mode.....	44
	Cache Mode.....	44
	Pull Splitting.....	44
	Multicasting	44
4	CONNECTING CLIENTS TO REALPROXY	45
	Overview	45
	Configuring Clients to Send Requests to RealProxy	45
	Using a Router to Send Client Requests to RealProxy	45
	Configuring RealPlayers to Contact RealProxy	46
	Configuring RealProxy to Listen for Re-Routed Client Messages	47
5	ADVANCED FEATURES	51
	Running Web Servers and RealProxy on the Same System	51
	Administering Both RealProxy and RealServer.....	52
	Reserving IP Addresses for RealProxy's Use	52
	Features Specific to the Operating System	53
	Windows NT	53
	UNIX.....	54
6	MANAGING BANDWIDTH	55
	Overview	55
	Maximum Clients.....	56
	Maximum Bandwidth.....	56
	Maximum Gateway Bandwidth	57
	Low Gateway Bandwidth.....	57
	Limiting Access to Multicast Reception	58

	Limiting Access by RealPlayer Version	59
7	LIMITING ACCESS TO REALPROXY	61
	Overview	61
	Deciding What Rules to Create	62
	Numbering the Rules.....	63
	Setting Up IP Access Control	64
8	CHAINING ONE REALPROXY TO ANOTHER	71
	Overview	71
	Setting Up Chaining.....	72
	Turning Off Chaining	73
9	MULTICASTING LIVE STREAMS	75
	Overview	75
	Multicast Methods.....	76
	Setting Up Multicasting.....	76
	Setting Up the Network for Multicasting	77
	Allocating Addresses and Port Numbers in RealProxy.....	77
	Determining Required Addresses and Port Numbers	78
	Setting Up Back-Channel Multicasting	78
10	MONITORING REALPROXY ACTIVITY	83
	Using RealSystem Administrator	83
11	TRACKING REALPROXY ACTIVITY	85
	Proxy Log.....	85
	Reading a Proxy Log.....	85
	Customizing Information Reported by the Proxy Log.....	91
	Log File Rolling	93
	Disabling Log File Rolling	94
	Error Log.....	94
A	CONFIGURATION FILE SYNTAX	97
	Configuration File Components	97
	XML Declaration Tag	97
	Comment Tags	97
	List Tags.....	98
	Variable Tags.....	98
B	CONFIGURATION FILE CONTENTS	101
	Editing the Configuration File	101
	Elements of the Configuration File	102
	Ports	102

Paths.....	102
RealProxy	103
RTSP Redirection	105
MIME Types	105
File Systems	106
IP Binding.....	108
Allowance.....	109
HTTP Support	110
Access Control.....	110
Splitting	111
Multicasting	112
Authentication.....	113
Passwords	114
Logging	114
C FILES INCLUDED WITH REALPROXY	117



INTRODUCTION

This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

Welcome to RealProxy™, a network server that works with RealServer™ to reduce streaming media bandwidth and improve the viewing experience on your intranet or Internet gateway. This manual will help you use and optimize RealProxy.

Overview

This manual is aimed at information services administrator who will be setting up RealProxy.

How This Manual Is Organized

This manual contains the following chapters:

Chapter 1: Overview

This chapter gives the “big picture” of how RealProxy streams media to a clients, while conserving bandwidth used.

Chapter 2: Starting and Stopping RealProxy

This is a guide to starting and stopping RealProxy. Depending on which platform your RealProxy runs on, different automatic starting options are available. The license structure and MIME types are also discussed.

Chapter 3: Configuring RealProxy Features

RealSystem Administrator is the web-based console for fine-tuning RealProxy features.

Chapter 4: Connecting Clients to RealProxy

There are just a few steps you need to take to set up clients to take full advantage of RealProxy. Or, you can set up RTSP redirection so that this happens automatically.

Chapter 5: Advanced Features

This chapter discusses differences between RealProxy on the different platforms, the assignment of IP addresses for RealProxy's use, and some differences between RealProxy and RealServer.

Chapter 6: Managing Bandwidth

RealProxy has several methods of managing the amount of bandwidth it uses. You can limit the amount of bandwidth in use at one time, and place a cap on the number of clients who can receive streaming media.

Chapter 7: Limiting Access to RealProxy

You can limit which clients use your RealProxy, based on their IP addresses.

Chapter 8: Chaining One RealProxy to Another

By employing several RealProxies at once, you can funnel all streaming media Internet traffic through a single point.

Chapter 9: Splitting Live Streams

Splitting can distribute load over your network.

Chapter 9: Multicasting Live Streams

Take advantage of multicasting when streaming from RealProxy.

Chapter 10: Monitoring RealProxy Activity

To provide highest quality service, you'll want to keep track of how many people are accessing your RealProxy.

Chapter 11: Tracking RealProxy Activity

You'll want to look at trends and see what content is most popular. RealProxy can report player behavior with a customizable degree of detail. Errors are reported in their own log, which can help you troubleshoot any problems that arise.

Appendixes

Appendix A: Configuration File Syntax

This appendix consists of a discussion of the XML syntax used by the configuration file.

Appendix B: Configuration File Contents

This is a guide to the configuration file, for those who prefer to edit it directly rather than using RealSystem Administrator.

Appendix C: Files Included with RealProxy

A list of the files installed by RealProxy.

Conventions in This Manual

Because this manual is aimed at the RealProxy administrator, the term “you” refers to the administrator.

RealSystem clients, such as RealPlayer, are referred to generically as “clients”. Where information applies specifically to the RealNetworks RealPlayer® or RealPlayer Plus™, this is spelled out. Although most clients in use are RealNetworks’ own RealPlayer, RealNetworks also makes a software development kit that enables other companies to develop their own players which can also receive streamed data types.

“Clips,” “content,” “media files,” and “files” are used interchangeably to indicate the material that RealProxy streams.

The following table explains the typographic conventions used in this manual:

Notational Conventions

Convention	Meaning
<code>syntax</code>	Syntax of configuration files, URLs, or command-line instructions are given in this typeface.
<i>value</i>	Placeholder words are given in an italic monospaced typeface. Substitute the appropriate value for your system.
...	Ellipses indicate nonessential information omitted from the example.
[]	Square brackets indicate optional material. If you choose to use the material within the brackets, do not type the brackets themselves.

Additional RealSystem Resources

In addition to this manual, you may be interested in the following RealNetworks resources, available at **<http://service.real.com/help/library/index.html>**.

- *RealServer Administration Guide*

The basic reference for the RealServer administrator, this manual explains how to set up, configure, and run RealServer to stream multimedia.

- RealSystem G2 Software Development Kit

RealNetworks has developed a Software Development Kit (SDK) that lets you integrate applications with RealSystem or create new plug-ins for RealServer or RealPlayer. Knowledge of programming is required to use the SDK. Register for and download the SDK from

<http://www.real.com/devzone/>.

Technical Support

For technical support with RealSystem G2, please fill out the form at:

- **<http://service.real.com/contact/email.htm>**

The information you provide in this form will help technical support personnel to give you a prompt response. For general information about RealNetworks' technical support, visit:

- **<http://service.real.com/help/call.html>**

Chapter 1

OVERVIEW

This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

RealProxy manages clients requests for RealServer content. RealProxy can also be integrated with third-party cache software, enabling RealProxy to stream stored media closer to clients and to conserve gateway bandwidth.

How RealProxy Works

RealProxy is software you install on a network or ISP gateway that aggregates and handles client requests for media streamed by RealServer. When installed with streaming media cache software, RealProxy reduces network traffic by eliminating redundant requests for streaming media.

RealProxy provides two main benefits:

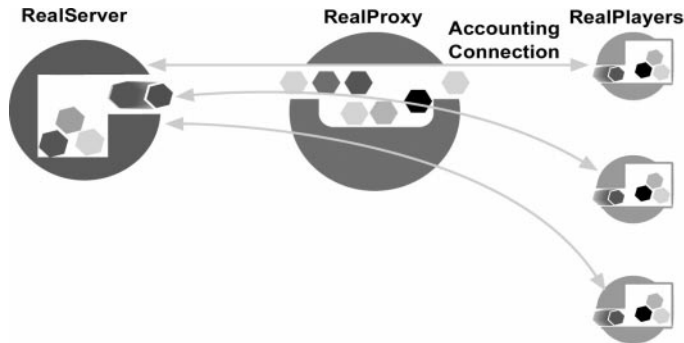
- Reducing bandwidth consumption by eliminating redundant data transmissions.
- Improving quality of service by distributing streaming media close to the user.

Overview of the RealProxy Process

1. Clients request streamed media files via RealProxy.
2. RealProxy forwards the requests to the RealServer where the requested streamed media files are stored (called the “origin RealServer”).
RealServer verifies the file’s existence, and that the clients are authorized through IP addresses or authentication. If RealServer denies the request, it does not stream the requested file, and neither does RealProxy. Clients receive an error message.

This initial transaction, in which RealServer examines and authorizes individual client requests, is called an “accounting connection.”

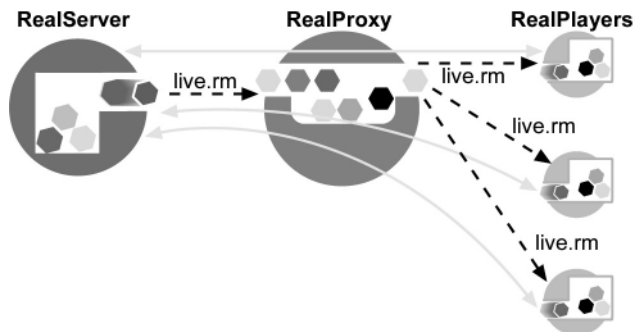
Steps in the RealProxy Process



3. If the stream is live, and served from a RealServer that supports splitting, RealProxy replicates the live stream for each client requesting the stream. The origin RealServer sends only a single stream to RealProxy.

If the live stream is not available via splitting, RealProxy delivers the data separately for each client.

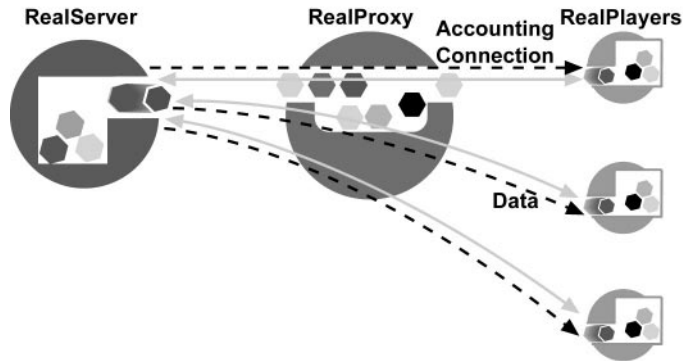
Live Content



4. If the stream is on-demand, and RealProxy is set up to use a media cache, it fills the request from the cache.

If the stream is on-demand, and a media cache is not available, RealProxy passes a data stream for each client that requested it.

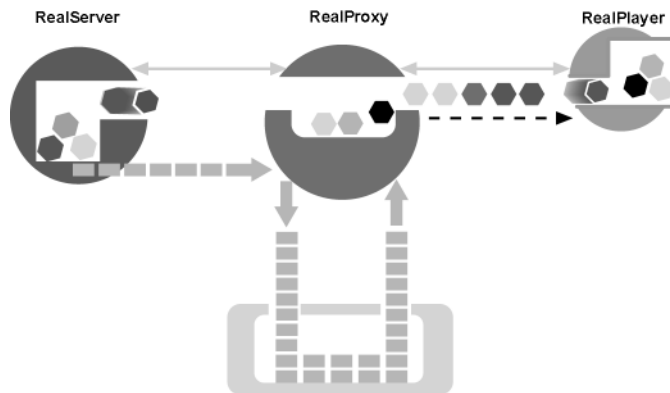
On-Demand Content (No Media Cache in Use)



Media Cache Software

RealProxy can be configured to work with a third-party media cache, which will store streamed data for clients requesting these streams later. A media cache file lowers network traffic by reducing the number of connections to the source of the requested material, and improves quality by distributing the streaming content closer to the user. Clients receive improved quality of service because media streams travel a shorter distance from the cache to clients, reducing the possibility of network congestion or packet loss.

RealProxy and Media Cache Software Delivering On-Demand Streams



Once configured to work with a media cache, RealProxy sends the client's request to the origin RealServer. After the request is approved and RealServer begins streaming, RealProxy looks at the incoming stream to determine

whether it is live or on-demand material. If the request is for on-demand material, RealProxy sends the request to the media cache software. The media cache software locates the data and streams it to the client.

Modes of Operation

RealProxy has four modes of operation:

- Passthrough
- Bitsave
- Caching
- Splitting

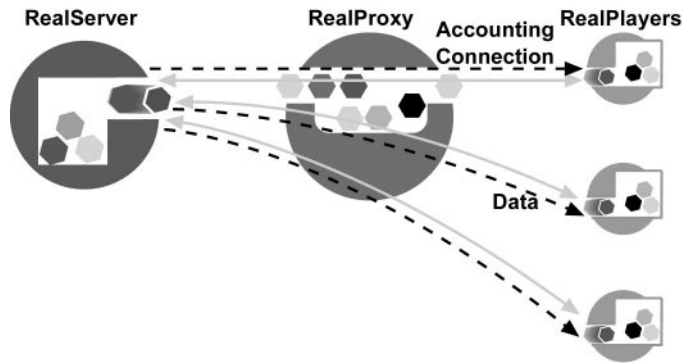
In addition, the methods that handle live broadcasts (passthrough, bitsave, and push splitting) can be configured to transmit via multicast.

RealProxy Modes				
Mode	Streams on-demand clips	Streams live clips	Can be configured to multicast	Conserves bandwidth
Passthrough	•	•	–	–
Caching	•	–	–	•
Bitsave	–	•	•	•
Splitting	–	•	•	•

In passthrough, caching, and bitsave modes, an accounting connection is opened between the client and the origin RealServer.

Passthrough

This is the RealProxy's simplest method of operation. In passthrough mode, no special features are activated, but all streaming media traffic passes through one point. In addition to the usual accounting connection opened between the client and the origin RealServer, RealProxy creates a data connection for each client. No bandwidth conservation is appreciated.

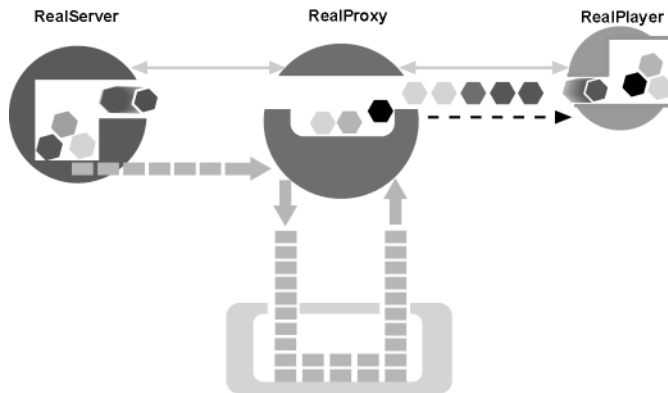
RealProxy in Passthrough Mode (Handling Live and On-Demand Streams)**Cache Integration**

Cache software stores on-demand streams from RealServer. Since cached files are stored in a proprietary format and cannot be accessed directly, RealProxy interfaces with the cache to redistribute the stored media to clients.

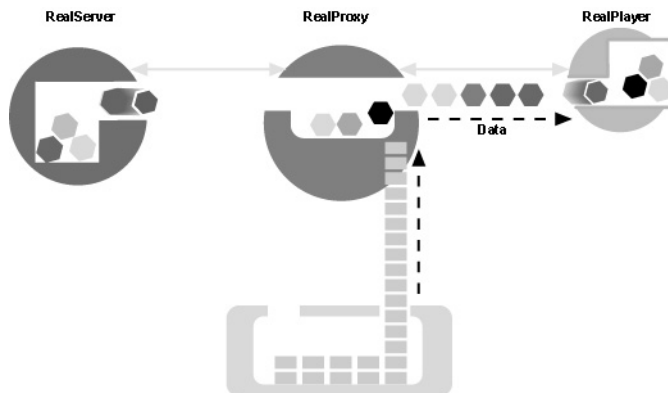
When caching is enabled, the media cache software stores streamed data when requested by the first client. When a second client makes a request for a stream, RealProxy checks with the cache to see if a stored version is already present. To ensure that the stored version is the most up-to-date version available, RealProxy checks with the origin RealServer to see if a newer version exists. After determining that the stored copy is the latest version, RealProxy streams the stored copy to the second client.

Only on-demand files streamed by RealServer G2 can be cached. Live material is handled as in the most efficient mode suitable—bitsave or passthrough (and sent via multicast, if available on the network).

RealProxy Filling the Media Cache (Handling On-Demand Streams)



RealProxy Serving On-Demand Media from the Cache



To ensure high-quality data at all times, RealProxy monitors the quality of both the cached data it is streaming and the connection between the origin RealServer and the client.

Should the data from the media cache become impaired in some way, the stream halts and clients receive an error message.

If the accounting connection between the client and the origin RealServer is interrupted, RealProxy terminates the stream, and the client receives an error message.

You won't be able to take advantage of your media cache if clients are requesting streams from an origin RealServer which has been configured to prevent caching. Clients will still receive the streams, but the media cache won't be permitted to store them. When RealServer is installed, all its streams are cacheable by default.

Even if a RealServer manager opts to prevent caching of some content (such as advertisements), he or she will probably permit it for most items. Since RealServers can reach more clients if caching is allowed, managers are encouraged to leave all content cacheable.

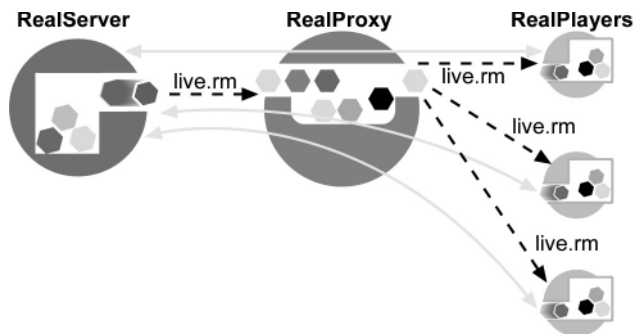
For specific instructions on configuring a third-party media cache, refer to the documentation included with that software.

Bitsave

Bitsave mode is for use with live material. The first time a client requests a particular stream, RealProxy contacts the origin RealServer on the client's behalf and then sends the stream to the client. The second client to request a live stream will receive it directly from RealProxy, and RealProxy will not have to obtain another stream from the origin RealServer. The origin RealServer has only to serve a single stream to every client that uses a particular RealProxy.

The advantage to the client is that the material is delivered from a local source. As long as the quality of reception between RealProxy and the origin RealServer remains good, the client will receive a high-quality live stream, as well.

RealProxy in Bitsave Mode (Handling Live Streams)



Pull Splitting

If you have your own RealServer that broadcasts within your network, you can configure RealProxy to act as a splitter. RealProxy can then share the streaming load with the source RealServer.

Requirements for Each RealProxy Mode

The following table outlines the configuration requirements for each aspect of RealProxy operation.

Requirements for Each Feature			
Mode	RealProxy Configuration	Your Network Requirements (assumes RealProxy is running)	Origin RealServer Requirements
Passthrough	None.	None.	Broadcasting live and/or on-demand content.
Caching	Cache is enabled; configuration file contains media cache settings (added by cache's setup program).	Media cache software installed. Refer to media cache documentation.	Has on-demand content, and is configured to accept requests from caches. (RealServers are configured this way by default.)
Bitsave	None. RealProxy is configured to do bitsave at installation.	Network allows UDP transport between RealProxy and RealServer.	Broadcasting live content. Configured for pull splitting (the pull splitting method allows other RealServers or RealProxy servers to "rebroadcast" live content.)
Pull splitting	None. RealProxy is configured to do bitsave at installation.	Network allows UDP transport between RealProxy and RealServer.	Configured to allow pull splitting, with default values.
Multicasting	Configured to use multicast address range.	Clients and routers are multicast-enabled.	Broadcasting live content.

Interaction with RealServer

This section describes what happens on the origin RealServer when RealProxy forwards a client request.

Controlling Client Access

Each time it receives a request, RealServer determines whether it can allow a particular client to receive streams, based on the number of available streams and bandwidth. In addition, RealServer may be configured to require a user name and password for certain material. If the requested material requires a password, the user will be prompted for the password. RealServer does not begin streaming until it receives the correct password.

Only after RealServer has authorized the client's request will RealServer begin streaming. Restrictions imposed by the origin RealServer's administrator on client access are always honored by RealProxy. The same is true when a cache is in use—RealProxy waits for RealServer approval of each request before streaming it from the cache.

Denying Client Access

An origin RealServer may deny a request for the following reasons:

- The requested material is secured, and the user does not have permission to access it
- RealServer can restrict access according to IP address, and the client's IP address is on the restricted access list
- No more connections are available on the origin RealServer. The number of connections is governed by the license, and can be further limited by the manager of the RealServer.

The client receives a message if it is denied access for any reason.

Tracking Activity

To the origin RealServer, requests made via RealProxy appear identical to requests made by any other client, and information about quality of service is logged in the log file, just as it is for any other type of connection. Information about quality of service comes from the accounting connection between the RealServer and the client.

Cache Requests

RealProxy only streams media from the cache after opening an accounting connection to the origin RealServer. If the accounting connection cannot be

established, or if it is disrupted, RealProxy will not stream from the cache to the client.

RealProxy cannot cache content which an origin RealServer administrator has configured as non-cacheable. Instead, it will use passthrough mode to deliver the material to the client.

When RealProxy Will Not Conserve Bandwidth

Under the following circumstances, RealProxy will be unable to conserve bandwidth:

- If the origin RealServer is configured to only allow caching on some files, or not at all. You have no control over this. (For example, a RealServer administrator might prevent frequently updated material, such as advertisements, from being cached.)
- If the origin RealServer is not configured for pull splitting. RealProxy's bitsave mode takes advantage of splitting on the origin RealServer, and if the RealServer is not set up to allow splitting, bitsave mode won't work.

In all cases, however, using RealProxy on your network serves to collect all streaming media traffic at a single point, so that you can better monitor activity and maintain security.

Additional Features

RealProxy contains additional features that make it easy to configure, administer, and maintain.

Administration

RealSystem Administrator is a web-based console for customizing RealProxy features. You can access via a browser anywhere on your network, using either Netscape Navigator version 4.06 or higher, or Internet Explorer version 4.0 or higher.

Changes you make using RealSystem Administrator are stored in the RealProxy configuration file. This text file is based on Extensible Markup Language (XML) and can be edited directly. Because the structure of this file is complex, RealSystem Administrator is the recommended tool for making changes.

See Chapter 3: Configuring RealProxy Features on page 39 for specific instructions on customizing RealProxy.

Setting Up Clients

Once you have configured RealProxy, you will need to arrange for clients (such as RealPlayer) to send their requests to RealProxy.

There are two ways you can do this:

- Configure clients to directly contact RealProxy with their streaming media requests. You can send instructions for doing this to users.
- Configure RealProxy to intercept client requests. This does not require any special client configuration, but it does require the use of software or hardware which routes TCP traffic by destination port (such as a layer-4 switch).

For information on setting up either method, see Chapter 4: Connecting Clients to RealProxy.

Limiting Network Traffic

To limit the amount of bandwidth used by RealProxy, several features allow you to restrict the number of requests or amount of bandwidth it uses. Clients that attempt to contact RealServers after RealProxy's limits have been reached receive an error message.

Additional Information

See Chapter 6: Managing Bandwidth.

Chaining One RealProxy to Another

To carefully direct the streaming media traffic on your network, you can configure RealProxy to direct its clients' requests to yet another RealProxy. A RealProxy that sends its requests to another RealProxy is called a child; the RealProxy that receives requests from other RealProxies is called the parent.

Additional Information

See Chapter 8: Chaining One RealProxy to Another.

Monitoring RealProxy in Real Time

RealSystem Administrator includes an HTML page which dynamically displays the status of your RealProxy.

Additional Information

Refer to Chapter 10: Monitoring RealProxy Activity.

Tracking RealProxy Activity

RealProxy records information in the access log about all clips it has served. Errors are noted in the error log.

RealProxy error logs use the same format as RealServer error logs. Access logs are similar to RealServer logs, but include additional information about the address of the origin RealServer and the RealProxy operational mode (bitsave, caching, and so on).

Log files on the origin RealServer do not show that a RealProxy is in use; only the client data is gathered.

Additional Information

Access and error log information is described in depth in Chapter 11: Tracking RealProxy Activity.

Protocols

RealProxy handles client requests and proxies RealServer streams by using the Real Time Streaming Protocol (RTSP), the Internet standard control protocol for streaming multimedia, and PNA, the RealNetworks legacy protocol. RealProxy does not handle HTTP requests made between clients and origin RealServer.

Supported Protocols and Data Packet Formats

Control Protocol	Control Transport	Data Packet Format	Data Packet Transport	Supported by RealProxy?
RTSP	TCP	RDT (RealNetworks)	IP multicast, UDP, TCP	Yes
RTSP	TCP	RTP	IP multicast, UDP, TCP	Yes
PNA (RealNetworks)	TCP	RDT (RealNetworks)	UDP, TCP	Yes

(Table Page 1 of 2)

Supported Protocols and Data Packet Formats (continued)

Control Protocol	Control Transport	Data Packet Format	Data Packet Transport	Supported by RealProxy?
PNA (RealNetworks)	TCP	RTP	UDP, TCP	Yes
HTTP (Streaming)	TCP	—	—	No
HTTP (Cloaking)	TCP	RDT (RealNetworks), RTP	TCP	No

(Table Page 2 of 2)

Chapter 2

STARTING AND STOPPING REALPROXY

This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

This chapter gives information on starting and stopping RealProxy on both Windows and UNIX platforms, setting up MIME types, and explains the RealProxy license method.

Windows

Instructions in this section describe how to start and stop RealProxy running under Windows.

Starting RealProxy Under Windows

RealProxy can be started manually or as a service. You can configure each service to use different configuration files.

Whether you start RealProxy manually or as a service, if you start it without including a configuration file, RealProxy uses the most recently used configuration settings.

Starting RealProxy Manually

You can start RealProxy from the **Start** menu or from a command line.

- To start RealProxy from the Start menu:

On the **Start** menu, click **Programs**, then click **RealProxy**, and finally click **RealProxy G2**. This starts the `rmserver.exe` program. If this is the first time you have run RealProxy, it loads the default configuration file.

Additional Information

The configuration file is described in Chapter 3: Configuring RealProxy Features.

- To start RealProxy from a command line:

Move to the RealProxy Bin directory and type the following at a command line:

```
rmserver ..\rmserver.cfg
```

To limit the amount of memory that RealServer G2 uses, start RealServer with the `-m` parameter:

```
rmserver ..\rmserver.cfg -m 32
```

where the number after `-m` can be any amount of memory in megabytes, 32 or greater. Each megabyte of RealServer memory accommodates 3 to 4 simultaneous connected users. To allow 200 users to connect, specify 50 megabytes of memory instead of 32. (This parameter is optional.)

Setting Up RealProxy as a Service

RealProxy on Windows NT can be run as a service. An option during setup configures this automatically. Instructions in this section describe how to add RealProxy to the services list if you did not instruct setup to do so.

You can load different configuration files into different Windows NT registry keys, and connect them to different instances of RealProxy running as separate services. Multiple services of RealProxy can be useful if you want to switch between a production and a test configuration file, for example.

- To install RealProxy as a service:

1. At a command prompt, move to the RealProxy Bin directory.
2. Import the configuration file you want to use into a specific key in the registry by typing the following:

```
rmserver.exe -import[:key] configuration_file
```

where:

key is the Registry key name you want to use. If you omit it, the default name `Config` is substituted.

configuration_file is the path and configuration file you want to import. For example, the following command:

```
rmserver.exe -import:Proxy1 ../rmserver.cfg
```

imports all the values in the `rmserver.cfg` file into the following key of the Windows registry:

```
HKEY_CLASSES_ROOT\Software\RealNetworks\RealMedia Proxy\6.0\Proxy1
```

Note

You must supply the path to the configuration file. If RealProxy cannot find the configuration file, it may not start.

Tip

You can now start RealProxy using this configuration by typing the following at a command line:

```
rmserver.exe registry:Proxy1
```

3. Install the service by typing the following command at a command prompt:

```
rmserver.exe -install[:ServiceName] "parameters"
```

where:

ServiceName is the name that will appear in the Services dialog box. If you omit *ServiceName*, RMPProxy is substituted.

parameters is either the name of the configuration file, or the registry and key name, as entered in Step 2. The format of the registry and key name is `registry:key`. Any command line parameters, such as the `-m` switch, can be used.

Note

The quotation marks surrounding *parameters* are required.

The next time you start RealProxy from the Services dialog box, it will use the settings specified in *parameters*, and will be configured to start automatically.

For example, the following command:

```
rmserver.exe -install:NewYorkProxy "Proxy1"
```

installs RealProxy with the service name “NewYorkProxy” and uses the settings in the Proxy1 key.

- To remove any RealProxy from the services list:

At a command prompt, type the following:

```
rmserver.exe -remove[:ServiceName]
```

where *ServiceName* is the optional name of the service. If you omitted a service name when you installed the service, you can omit it here, and RealProxy will use RMPProxy.

Running Multiple Servers on One Windows NT System

You can have configuration files with different names for different configurations of a single RealProxy, or use different names for different RealProxy installations.

You can load configuration files into separate registry keys. Then, run RealProxy as a service, one for each configuration file you loaded.

► To import a configuration file into a specific key in the registry:

1. Follow the instructions in Step 2 of “Setting Up RealProxy as a Service”.
2. Start RealProxy by typing the following:

```
rmserver.exe registry:key
```

where:

key is name you want to use for the configuration. RealProxy places the configuration information in

```
HKEY_CLASSES_ROOT\Software\RealNetworks\RealMedia Proxy\6.0\Key.
```

In the example from Step 2 of “Setting Up RealProxy as a Service”, in which the configuration settings are loaded into the “Proxy1” key, the full key name would be HKEY_CLASSES_ROOT\Software\RealNetworks\RealMedia Proxy\6.0\Proxy1.

Stopping RealProxy Under Windows

If RealProxy was started from the Start menu or the command prompt, switch to the command window and press **CTRL+C**.

If RealProxy was started as a service, stop RealProxy through the Services control panel.

UNIX

Instructions in this section describe how to start and stop RealProxy running under UNIX.

Starting RealProxy Under UNIX

Start RealProxy initially with the default configuration file; later, you can create other configuration files and start RealProxy using those.

► **To start RealProxy under UNIX:**

Run the `rmserver` program. It is located in the `bin` subdirectory of the RealProxy directory, and the configuration file (`rmserver.cfg`) is located in the main RealProxy directory.

Move to the `bin` directory and type the following:

```
rmserver ../rmserver.cfg
```

If you do not start from the `bin` directory, RealProxy cannot understand the relative paths in the configuration file.

You can run RealProxy in the background by typing the following from the `bin` directory:

```
rmserver ../rmserver.cfg &
```

If you have other configuration files, you can substitute their names for `rmserver.cfg` and RealProxy will use the settings in the file you name.

To limit the amount of memory that RealServer G2 uses, start RealServer with the `-m` parameter:

```
rmserver ../rmserver.cfg -m 32
```

where the number after `-m` can be any amount of memory in megabytes, 32 or greater. Each megabyte of RealServer memory accommodates 3 to 4 simultaneous connected users. To allow 200 users to connect, specify 50 megabytes of memory instead of 32. (This parameter is optional on FreeBSD and Linux.)

Stopping RealProxy Under UNIX

To stop RealProxy running under UNIX, first obtain the process identification number, and then issue the **kill** command with that process number. The process ID is stored in the `rmserver.pid` file, which is usually kept in the `Logs` directory. The `PIDPath` variable specifies this location.

You can perform both actions with one command. Move to the directory which contains the RealProxy PID file, and type the following:

```
kill `cat pidfile`
```

where *pidfile* is the name of the RealProxy PID file, as shown in the `PIDPath` variable. The usual name for this file is `rmserver.pid`.

Configuring MIME Types

RealProxy works with any Web server that supports configurable MIME types. Make sure that your Web server has the RealNetworks MIME types defined.

In addition, RealProxy serves its own HTML pages. To this end, be sure that RealProxy has the correct MIME type information.

- To set up MIME types on the Web server:

Refer to the instructions accompanying your Web server to define the following MIME types on your Web server:

- audio/x-pn-realaudio (files with a `.ra`, `.rm` or `.ram` file extension)
- audio/x-pn-realaudio-plugin (files with a `.rpm` file extension)
- application/smil (files with a `.smi` or `.smil` extension)
- application/sdp (files with a `.sdp` extension)
- application/x-pn-realmedia (files with `.rp`, extension)
- text/html (files with a `.html` or `.htm` extension)
- image/gif (files with a `.gif` extension)
- image/jpeg (files with a `.jpg` or `.jpeg` extension)

When you install RealProxy, the MIME Types section is present in the configuration file. You need only examine this list if something happened in the meantime and you think the list might be incomplete. You can examine the MIME types section using the following instructions.

Additional Information

See “Configuring RealProxy Features” for instructions on using RealSystem Administrator.

- To set up MIME types used by RealProxy:
1. In RealSystem Administrator, click **General Setup**. Click **MIME Types**.
 2. The list should match the table below:

Names	Extensions
audio/x-pn-realaudio	.ra .ram
application/smil	.smi .smil
application/sdp	.sdp
application/x-pn-realmedia	.rm .rp .rt
text/html	.html .htm
image/gif	.gif
image/jpg	.jpg .jpeg

You should only modify the list if you will be streaming a data type via HTTP that is not on the list.

- To add another MIME type, click **Add**. Type the name and extension in the respective boxes, and click **Submit**.
- To edit an existing MIME type, select it from the **Names** list, and click **Edit**. Change the name or extension and click **Add**.
- To remove a MIME type, select it from the **Names** list, and click **Remove**. Click **OK**.

License Information

Information about the license for your RealProxy is stored in a file in a license directory. License files are written in XML format.

You can read the file with RealSystem Administrator by clicking **About** in the left-hand frame. A second browser window appears, displaying the values for your license file. If you have multiple license files, RealProxy will show the values for all of them at once.

You can also read the file with any text editor.

If the license file is invalid, RealProxy will report an error message, add the error to the error log file, and will not start.

If your RealProxy suddenly allows fewer connections or otherwise appears to be using minimum settings, either your license has expired or RealProxy is unable to start using the settings you've selected.

The LicenseDirectory variable in the configuration file tells RealProxy where to look for license information.

Additional Information

To learn about the configuration file, see “Configuration File” on page 41.

CONFIGURING REALPROXY FEATURES

Chapter 3

This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

All RealProxy settings are customized through the RealSystem Administrator. This chapter describes how to use RealSystem Administrator as well as the basic settings used by all RealProxys.

Configuring RealProxy Using RealSystem Administrator

When the RealProxy installation program completes, it asks if you want to run RealSystem Administrator. If you choose yes, RealSystem Administrator displays. To make changes to any feature, click on the appropriate category listed under **Configure**. Make the changes and click **Apply**.

Starting RealSystem Administrator

You can view the configuration of your RealProxy from nearly any browser on your network. Compatible browsers are Netscape Navigator version 4.0 or higher and Microsoft Internet Explorer version 4.0 or higher.

► To start RealSystem Administrator:

1. Start RealProxy. (See Chapter 2: Starting and Stopping RealProxy for instructions).
2. In a browser, type the following address:

`http://realproxy.company.com:AdminPort/admin/index.html`

where:

realproxy is the name of the machine on which RealProxy is installed.

company.com is the name of the domain in which RealProxy exists.

Or, rather than typing the name and domain of the system on which RealProxy is installed, you can type the IP address.

AdminPort is the port which RealSystem Administrator uses to connect to RealProxy. You are asked for a port number during setup. Use that port number here.

The following URL will start RealSystem Administrator if it is typed in the browser on the same computer as RealProxy (be sure to substitute your port number for *AdminPort*):

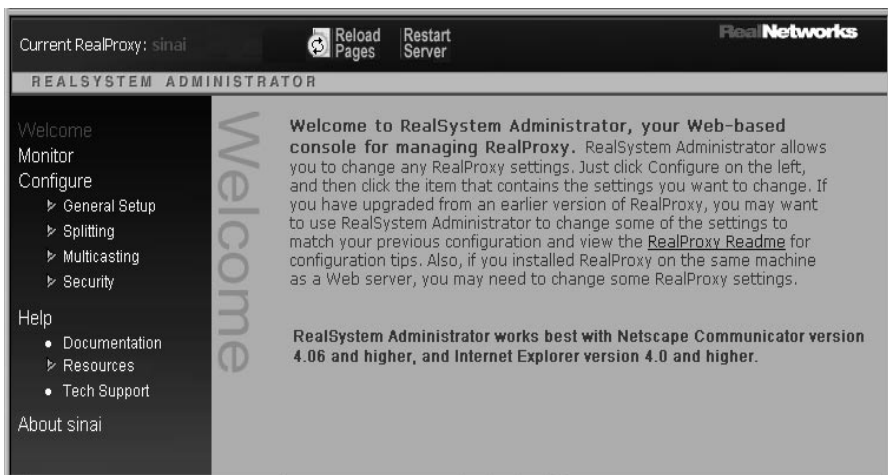
`http://127.0.0.1:AdminPort/admin/index.html`

The following command also works on the same computer:

`http://localhost:AdminPort/admin/index.html`

3. You are prompted for your user name and password; these will match the values you entered during setup. Click **OK**.

RealSystem Administrator appears.



Using RealSystem Administrator

Once you have started RealProxy and then RealSystem Administrator, you can change RealProxy features with the instructions below:

- To customize RealProxy settings:
 1. In RealSystem Administrator's left-hand frame, click the appropriate category below **Configure**.
 2. Change the values in the page on the right.

3. When you have finished changing values, click **Apply**.

RealSystem Administrator makes the changes to the configuration file.

Restricting Access to RealSystem Administrator

When you install RealProxy, RealSystem Administrator is configured to require user names and passwords for anyone who connects to RealSystem Administrator itself. You can add permission for additional users, so that other people in your organization can use RealSystem Administrator to customize RealProxy.

Additional Information

RealProxy uses a subset of the authentication features available to RealServer. For more information on authentication, refer to *RealServer Administration Guide*.

- To add access for additional RealSystem Administrator users:

1. In RealSystem Administrator, click **Security**. Click **Authentication**.
2. In the **Realms** list, select SecureAdmin.
3. Click **Add a User to Realm**. A new dialog box appears.
4. Type the new user name in the **Name** box.
5. In the **Password** box, assign a password.
6. Click **Add**. A message appears; click **OK**.

Repeat Step 2 through Step 6 for each person who will have administration privileges.

Configuration File

Changes made with RealSystem Administrator are stored in the configuration file. It is a text file formatted with tags which are based on XML (Extensible Markup Language). This language introduces great flexibility to the configuration file format and allows third-parties to use this file and add to its functionality. Syntax of this file is given in Appendix A: Configuration File Syntax.

Be sure that your configuration file is stored where only authorized users can make changes to it.

Tip

Keep a backup copy of the configuration file. You may need it if you make changes to this file that you later want to undo or if you accidentally delete the working copy.

Editing the Configuration File with a Text Editor

You can change the RealProxy settings by opening the configuration file with any text editor. You can also add variables that aren't included in the initial file, but are listed in this manual in Appendix B: Configuration File Contents. In addition, third-party plug-ins may require their own parameters and variables. Use a text editor to add them to the configuration file.

To make changes to existing settings in this file is simple; this manual provides guidance. If, however, you plan to add new sections, you will need to understand the syntax of the entire file. The file is organized into sections. This is not strictly necessary, but helps with clarity. The structure of the configuration file is described in detail in Appendix A: Configuration File Syntax.

The default name of the configuration file is `rmserver.cfg`, but if you have multiple servers you may want to rename the files so as to easily identify which server you're working with.

When you edit the configuration file manually, be sure to use correct syntax, because RealProxy looks for exact spellings and correct use of angle brackets. RealProxy does not display messages related to syntax errors; instead, it will ignore those settings it does not understand.

Note

Always restart RealProxy after changing any settings in the configuration file with a text editor.

RealSystem Administrator shows the configuration file settings of the RealProxy configuration file in use; use caution if you are switching between manually editing the file and using RealSystem Administrator to edit it.

Warning

Exit RealSystem Administrator before opening the configuration file with a text editor or unexpected changes may result.

Common Settings

Regardless of which features are in use, certain powerful settings apply to every RealProxy. They are described in this section.

Port Variables

Port settings tell RealProxy where to listen for requests.

If your RealProxy and Web server are on the same machine, you may need to modify the HTTP Port setting. See “Running Web Servers and RealProxy on the Same System” on page 51 for additional information.

► To add port settings:

1. In RealSystem Administrator, click **General Setup**. Click **Ports**.



Ports ?	
RTSP Proxy Port	1091
PNA Proxy Port	1090

2. Tell RealProxy where to listen for material requested via PNA (these begin with pnm://) by typing the correct value in the **PNA Port** box. The default value is 1090.
3. Tell RealProxy where to listen for RTSP requests (these begin with rtsp://) by typing the correct value in the **RTSP Port** box. At installation, the value is 1091.
4. Tell RealProxy where to listen for RealSystem Administrator connection requests by typing any unique port number in the **Admin Port** box.

Note

To use a port lower than 1024 on a UNIX system, you must be logged on as super-user.

5. When you have finished making changes, click **Apply**.

Configuring RealProxy Features

To customize RealProxy features, you'll need to modify settings with RealSystem Administrator or by editing the configuration file directly.

Passthrough Mode

Passthrough mode is always enabled. It can't be turned on or off.

Bitsave Mode

In bitsave mode, RealProxy redistributes the incoming live streams with all the clients who request it, rather than requesting additional streams on their behalf.

Currently, this can only be configured by editing the file directly.

- ▶ To set up bitsave mode by editing the configuration file:

Set `BitsaveEnable` to 1 (this is the default value).

Cache Mode

Refer to the documentation included with your caching software for instructions.

Pull Splitting

Pull splitting is enabled by default.

Multicasting

Instructions on configuring RealProxy to perform multicasting in Chapter 9: Multicasting Live Streams.

CONNECTING CLIENTS TO REALPROXY

Chapter 4

This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

This chapter describes how to make clients send their requests to RealProxy.

Overview

Even after RealProxy is installed, clients will not automatically contact it. So that clients (such as RealPlayer) route their requests to your RealProxy, you must either configure the clients individually, or configure a third-party router to automatically redirect streaming media requests to RealProxy.

Configuring Clients to Send Requests to RealProxy

Most clients contain an option to contact a proxy rather than sending requests directly to RealServers. In the client software, the user types the IP address (or host name) and port number of the proxy software to contact.

If you choose to connect clients to your RealProxy this way, you must either set up your users' client software yourself or send instructions to the users on how to set up the software themselves.

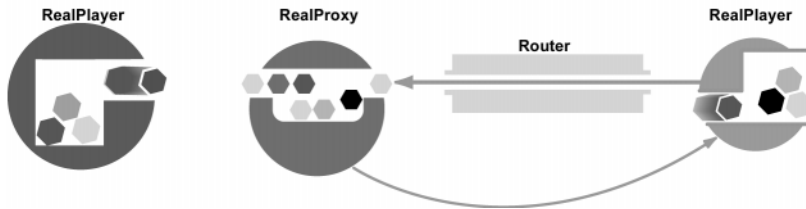
Choose this option if you have only a few clients or if you don't have a router.

Using a Router to Send Client Requests to RealProxy

Routers intercept all packets of network traffic. Routers examine each packet and decide where the packets should go next, according to an administrator-defined set of rules. If the packet contains a request that includes port 554 or 7070 (clues that the request is for streaming media), the router sends it to RealProxy.

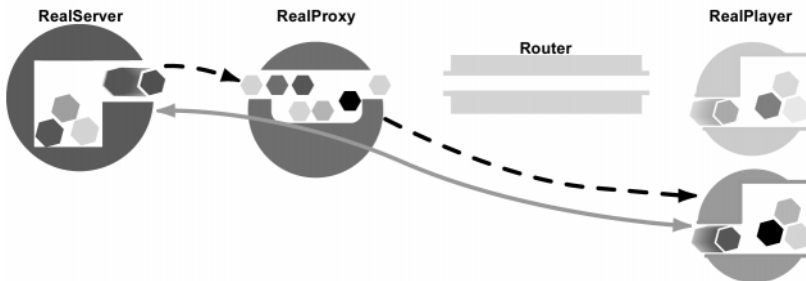
After it receives the redirected request, RealProxy contacts the client, and tells it to contact RealProxy directly.

RealProxy Contacting Client with New Connection Information



Now that the client knows the correct address and port number to use, it re-submits its streaming media request. Having received the request directly from the client, RealProxy now handles the requests in the usual manner.

Origin RealServer Connecting to New Instance of RealProxy



For each presentation that the client requests (whether an individual clip or a SMIL presentation), this process will be repeated.

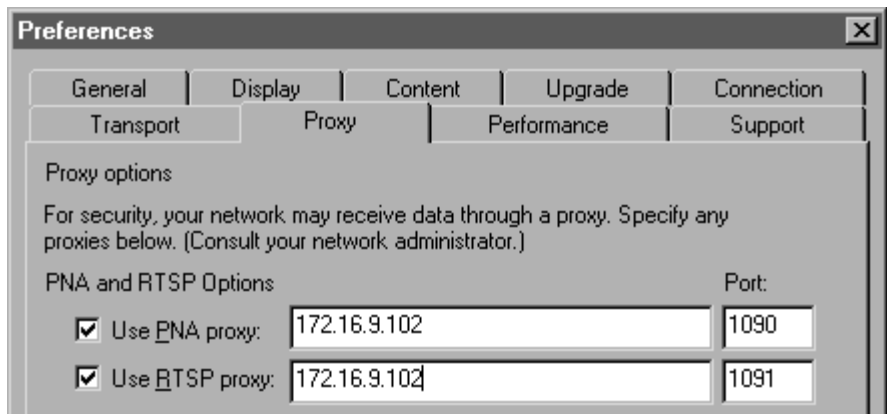
Configuring RealPlayers to Contact RealProxy

If you choose to configure RealPlayers to connect directly to RealProxy, use the instructions in this section.

- To configure RealPlayer:
 1. In RealPlayer, select **Options > Preferences**.
 2. Select the **Proxy** tab.
 3. Select the **Use PNA proxy** box.

4. In the box next to it, type the IP address or DNS of the RealProxy computer.
5. In the **Port** box, type the number of the RealProxy port number to which this client should send its PNA requests (usually 1090). The number you type here must match the number in the **PNA Port** box on the Ports page in RealSystem Administrator (or the Port variable in the Proxy list in the configuration file).
6. Select the **Use RTSP proxy** box.
7. In the box next to it, type the IP address or DNS of the RealProxy computer.
8. In the **Port** box, type the number of the RealProxy port number to which this client should send its RTSP requests (usually 1091). The number you type here must match the number in the **RTSP Port** box on the Ports page in RealSystem Administrator (or the Port variable in the Proxy list in the configuration file).
9. Click **OK**.

RealPlayer Proxy Tab



Configuring RealProxy to Listen for Re-Routed Client Messages

Configuring RealProxy to use this method consists of two steps:

1. Configuring the router to redirect streaming media requests to RealProxy.

2. Configuring RealProxy to listen for redirected requests and to give correct address information to the clients.

When you have finished with these steps, clients will know to contact the RealProxy directly.

Warning

If you are running RealProxy on a UNIX system, the RTSP redirection feature may not start correctly. It uses a port number lower than 1024—and on UNIX systems, you must be logged on as super-user for lower port numbers to be recognized.

If this is happening, you can either log on as super-user, or change the port number in the configuration file and restart RealProxy.

► **To configure your router:**

Consult your router's instructions and configure it to re-route streaming media requests to RealProxy. Typically, you would re-route TCP PNA or RTSP packets. Typically, any TCP packets which are bound for port 7070 or 554. (PNA traffic usually is associated with port 7070 on the origin RealServer, and RTSP traffic is associated with port 554.) The router must replace the address to which the client was sending its address with the address of RealProxy.

► **To configure RealProxy:**

1. In RealSystem Administrator, click **General Setup**. Click **Ports**.
2. Identify the port number on which RealProxy will receive the clients' RTSP requests as redirected by the router. This is usually 554. Type this number in the **RTSP Redirect Port** box.
3. Type the port number to which clients should send their RTSP requests (usually 1090) in the **RTSP Redirect Port** box.
4. Type the IP address of RealProxy to which clients should send their RTSP requests in the **RTSP Redirector Address** box.
5. Identify the port number on which RealProxy will receive the clients' RTSP requests as redirected by the router. This is usually 7070. Type this number in the **PNA Redirect Port** box.

6. Type the port number to which clients should send their PNA requests (usually 1091) in the **PNA Redirect Port** box.
7. Type the IP address of RealProxy to which clients should send their PNA requests in the **PNA Redirector Address** box.
8. Click **Apply**.

Chapter 5

ADVANCED FEATURES

This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

This chapter covers features which are specific to the operating system, as well as reserving IP addresses for RealProxy's use, and running RealProxy on the same system as a Web server.

Running Web Servers and RealProxy on the Same System

If you install RealProxy on the same system as your Web server, you may need to complete additional steps. Most Web servers use port 80 for HTTP requests. At installation, RealProxy's default HTTP Port is 8080, but if you configure RealProxy to use port 80 (the same port as the Web server), problems may ensue. You may have to perform the following steps:

- Choose a different port for RealProxy to use for HTTP requests and change links that point to HTTP pages
- Reserve an IP address for RealProxy

Change the HTTP Port Value

Because RealProxy can serve requests for HTML pages sent via HTTP (such as RealSystem Administrator), if RealProxy is on the same system as a Web server, requests that begin with `http://` may be misdirected. When a user clicks a link that begins with `http://` and does not contain a port number, the client supplies a port number—80. When the Web server and RealProxy are on the same machine, the Web server will attempt to serve the file. If the link points to what's meant to be a RealSystem presentation, the Web server will not find the file and will display the error message "File not found."

To prevent this problem from occurring, make sure the HTTP Port value is not the same as the port number your Web server is using. The default value is

8080. Most Web servers use port 80. Be sure that you include the port number in the URL.

Set IP Binding List

You may need to reserve at least one IP address for RealProxy's use. See "Reserving IP Addresses for RealProxy's Use" on page 52.

Administering Both RealProxy and RealServer

If you are the administrator of both RealProxy and RealServer (for example, if you administer a corporate Web presence for both internal (RealProxy) and external (RealServer) use, or if you are an ISP host and you offer RealServer streaming services to your clients), here are some things to keep in mind:

- **Configuration file**—the structure of the configuration file is the same; only certain sections are unique to RealProxy.
- **Access log**—RealProxy's access log uses the same structure as RealServer, with additional proxy-specific information appended to the end of each record.
- RealProxy's bitsave method is nearly identical to the RealServer method of pull splitting. The only difference is that RealProxy does not need to include the origin RealServer in the URL. The `Splitter_DoubleURL` section in the RealProxy's configuration file is the bitsave/pull splitting method.
- **Multicast**—RealProxy has only one method of multicast, which is the same as RealServer's back-channel multicast.

Reserving IP Addresses for RealProxy's Use

When RealProxy starts, it uses the first IP address of the first interface card it detects. If there is more than one IP address on the machine on which RealProxy is installed, the operating system assigns an address to RealProxy. Because the operating system's assignments may be random, clients attempting to connect to your RealProxy may not be able to receive streams.

You can configure RealProxy to always use the same IP addresses by setting up the IP Binding list. Within this list, you cite individual addresses to use, or you can reserve all the IP addresses available to the machine on which RealProxy is installed.

Additional Information

Instructions on customizing RealProxy can be found in Chapter 3: Configuring RealProxy Features on page 39.

► To reserve IP addresses for RealProxy:

1. In RealSystem Administrator, click **General Setup**. Click **IP Binding**.
2. Click the **Add** button.
3. In the **IP Address** box, type the address or DNS name that you want RealProxy to use. Typing an IP address here, rather than the DNS name, allows RealProxy to be more efficient.
RealProxy will bind to the specified addresses only; it will not bind to localhost.
4. To capture all addresses for RealProxy's use, add the IP address of 0.0.0.0, and delete any other addresses. RealProxy will automatically bind to all addresses and to localhost.

Warning

Use either 0.0.0.0 or other addresses, but not both. If you use both, RealProxy will not start.

5. Click **Add**.

If you leave the **IP Address** box blank, RealProxy binds to the host IP address and localhost. It does not bind to any others.

Features Specific to the Operating System

While RealProxy functions nearly identically on both Windows NT and UNIX platforms, there are a few differences that allow you to take advantage of unique characteristics of each operating system.

Windows NT

This section describes features unique to RealProxy running on a Windows NT system.

Windows NT Service

When you install RealProxy, you have the option to install it as a service. You can also configure this later. Several instances of RealProxy can be run from the same machine, with different configuration files.

Additional Information

See “Setting Up RealProxy as a Service” on page 30.

Windows NT Performance Monitor

RealProxy comes with a file to use with the Windows NT Performance Monitor, so that you can use the Windows NT method of monitoring RealProxy performance.

Additional Information

See Chapter 10: Monitoring RealProxy Activity on page 51.

UNIX

This section describes features unique to RealProxy running on a UNIX system.

Process ID (PID)

RealProxy creates a text file that stores the current value of the process ID of the main RealProxy file, `rmserver`. The file is stored in the directory indicated by the `PIDPath` variable, and is named `rmserver.pid` at installation. If `PIDPath` is omitted from the configuration file, RealProxy stores the information in the directory specified by the `LogPath` variable.

SIGHUP

When you make changes to RealProxy using RealSystem Administrator, those changes are saved and RealProxy is restarted immediately. If you make changes to the configuration file manually, you will need to restart RealProxy yourself. This is possible for RealProxy running on a UNIX platform with the **SIGHUP** command. Use the following command at a command prompt:

```
kill -HUP processID
```

where *processID* is the RealProxy process number, as shown in the `rmserver.pid` file.

Chapter 6

MANAGING BANDWIDTH

This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

RealProxy has several methods of managing the bandwidth that it uses. Whether you use just one method, or you use several in conjunction, you control the amount of traffic on your network.

Overview

When you install RealProxy, the values for each of these settings is configured to use the maximum available number.

Techniques for managing the bandwidth you use include:

- **Maximum Proxy Connections**— limit the number of clients that can connect at one time
- **Maximum Proxy Bandwidth**— limits the bandwidth in use between RealProxy and clients
- **Maximum Gateway Bandwidth**— limits the bandwidth in use between RealProxy and RealServers
- **Low Bit Rate Gateway**—deliver appropriate bit rate in SureStream file if connection between RealProxy and Internet is small
- **Require Multicast Delivery**— require clients to connect in Multicast mode

If you establish values for all these features, RealProxy will limit access when the lower threshold is reached. If a client tries to make a request after a limit has been reached, the client receives an error message.

In addition, you can require that the only certain client versions can connect to your RealProxy.

For information on restricting which clients can connect to RealProxy based on their IP addresses, see Chapter 7: Limiting Access to RealProxy.

Maximum Clients

By using the **Maximum Proxy Connections** setting (the `MaxProxyConnections` variable in the configuration file), you can limit the number of clients who connect simultaneously. Once this limit is reached, clients that attempt to connect receive an error message, and will not be able to connect until other clients disconnect.

► To limit access by limiting connections:

1. In RealSystem Administrator, click **General Setup**. Click **Bandwidth Management**. (Picture to be supplied later)

2. In the **Maximum Proxy Connections** box, type the number of client connections you want to allow simultaneously.

This number can be from 1 to 32767, as long as it is less than or equal to the number of streams permitted by your license. If it is 0 or blank, RealProxy uses the number of streams specified by your license. The default value is 0.

3. Click **Apply**.

Maximum Bandwidth

The **Maximum Proxy Bandwidth** setting (`MaxBandwidth` in the configuration file) limits the amount of bandwidth RealProxy can use to any number of kilobits per second (Kbps).

► To limit client bandwidth:

1. In RealSystem Administrator, click **General Setup**. Click **Bandwidth Management**.
2. In the **Maximum Proxy Bandwidth** box, type the maximum number of kilobits per second (Kbps) that should be in use at once.

For example, to limit the bandwidth to one megabyte, specify maximum bandwidth usage by setting **Maximum Proxy Bandwidth** to 1024.

3. When you have finished making changes, click **Apply**.

Maximum Gateway Bandwidth

You may want to limit the amount of bandwidth **RealProxy** uses to send its requests to its gateway, whether the gateway is another **RealProxy**, **RealServer**, or the Internet. Limiting gateway bandwidth limits the following **RealProxy** functions:

- passthrough data connections
- pull splitter data connections
- initial cache requests

► To limit **RealProxy**-to-gateway bandwidth:

1. In **RealSystem Administrator**, click **General Setup**. Click **Bandwidth Management**.
2. In the **Maximum Gateway Bandwidth** box, type the maximum number of kilobits per second (Kbps) that **RealProxy** should use when it connects to its gateway.

For example, to limit the bandwidth to two megabytes, specify maximum bandwidth usage by setting **Maximum Gateway Bandwidth** to 2048.

Maximum Gateway Bandwidth	<input type="text" value="2048"/> kilobits per second
----------------------------------	---

3. When you have finished making changes, click **Apply**.

Low Gateway Bandwidth

This feature allows you to take advantage of **RealNetworks'** **SureStream** technology if your **RealProxy** is connected to the Internet at a low bit rate. Use this feature if all the following are true:

- Clients are requesting **SureStream** files.
- A media cache is in use, and the stream is not yet stored in the media cache.

- The connection between RealProxy and the gateway is drastically smaller than the connection between clients and RealProxy.

SureStream files are streaming media files encoded at multiple bit rates; a client automatically chooses the highest bit rate available for the connection. Because clients connect to RealProxy through a high bandwidth connection, they select the best bit rate in the SureStream file for their connection speed. However, if the connection between RealProxy and the origin RealServer only permits low bit-rate connections, RealProxy will not be able to obtain the high bandwidth stream.

With the Low Gateway Bandwidth feature, RealProxy intercepts the client's request for a high bit-rate stream and requests only the low bit rate stream, storing it in the media cache.

Although the client receives the low bit-rate stream, the client receives a high-quality stream because it is arriving from a local source.

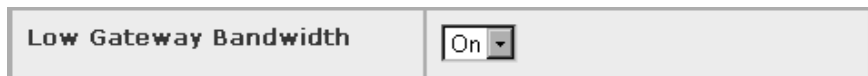
This setting has no effect on non-SureStream media.

Tip

Use this feature only if you have a small connection between RealProxy and the Internet. If you use it when a high-bandwidth connection is available, clients will only receive low bit rate streams.

► To use low bit rate connections:

1. In RealSystem Administrator, click **General Setup**. Click **Bandwidth Management**.
2. From the **Low Gateway Bandwidth** list, select **On**.



3. When you have finished making changes, click **Apply**.

Limiting Access to Multicast Reception

By setting **Delivery Only** to Yes in the multicast list, you can require that clients within a certain range of IP addresses connect only in multicast mode. When this option is set to Yes, clients that are not able to connect in multicast mode

receive an error message. If this option is **No**, clients that cannot connect in multicast mode can use unicast mode to receive the presentation.

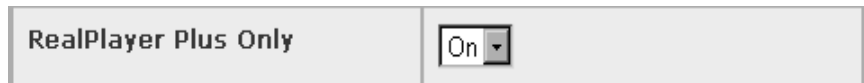
This feature is described in [Chapter 9: Multicasting Live Streams](#) on page 75.

Limiting Access by RealPlayer Version

Two settings restrict access to all RealProxy content, based on the client version. **RealPlayer Plus Only** means that only the RealNetworks RealPlayer Plus software can play presentations. And **Minimum Player Version** lets you limit your content to clients of a certain version. This can be helpful if you know that clients will be viewing complex material or if you want to record statistics in the access log that are only supplied by later versions.

► **To limit access to RealPlayer Plus:**

1. In RealSystem Administrator, click **General Setup**. Click **Bandwidth Management**.
2. In the **RealPlayer Plus Only** list, select **On**.



3. Click **Apply**.

► **To limit access by player protocol number:**

This variable was used in earlier versions of RealProxy and is included here for backwards compatibility. It must be added to the configuration file directly by using a text editor. It denies access to players whose version number is less than the number specified. Use one of the following values for Minimum Player Version:

- 0 All clients are permitted to connect to RealProxy
- 4 RealAudio Player 1.0 and later can connect
- 7 RealAudio Player 2.0 and later can connect
- 8 RealAudio Player 3.0 and later can connect
- 10 RealPlayer 4.0 and later can connect

Chapter 7

LIMITING ACCESS TO REALPROXY

This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

RealProxy allows you to restrict access to certain clients based on their IP addresses.

Overview

You can block or permit access to specific RealProxy ports based on the IP address of the client and the port to which they are sending their requests. Clients whose IP addresses are configured with “deny” receive an error message indicating that the URL is not valid or that the connection has timed out.

For example, you can restrict which clients can send requests to your RealProxy by restricting access to the RTSP Proxy port (usually 1091).

Information about each IP address or range of addresses you want to allow or restrict is stored in a rule. A rule is a set of instructions to RealServer about the address range and behavior to allow. Rules are identified by numbers which you assign.

Before using this feature, you must make decisions about the types of rules you will create.

Each rule contains the following information:

- **Access Rule Number**—Identification number for this rule.
- **Access**—Whether the client will be allowed or denied access.
- **To**—RealProxy’s address.
- **From**—Client’s address, or a range of addresses. This can also be an encoder’s IP address.

- **Restricted Ports**—Port numbers to which access is specified. For general content viewing, these numbers correspond to settings on the Ports page: RTSP Port, PNA Port, and HTTP Port. For encoders, these correspond to the port numbers in the Broadcasting pages.

When a client attempts to play a RealServer presentation, or an encoder attempts to send material, RealServer compares its address and the requested port to the addresses and ports listed in the rules. You can create as many rules as you like. If the client's IP and requested port number do not match any rules, RealServer denies access.

For example, to allow a content creator to encode live material and send it to your RealServer, you would create a rule that listed the client's address and the encoder port (4040).

Deciding What Rules to Create

There are two ways you can restrict access, and these determine how you set up the rules. Create the third rule first, so that you will be able to connect to RealSystem Administrator and create the rest.

- **Specific Address Denial:** Deny a specific group of IP addresses and ports, and allow access to everyone else.
- **Specific Address Permission:** Allow a specific group of IP addresses and ports, and deny access to everyone else.

Both methods require that you set up three sets of rules:

1. The first set of rules refers to specific client addresses you are denying or allowing. There can be several rules that refer to specific addresses or ranges of addresses.
2. All clients not noted specifically in the first set of rules are allowed access (in Specific Address Denial) or denied access (in Specific Address Permission). This second set usually consists of a single rule which uses the word "Any" in the **From** box.

Warning

If you are using Specific Address Denial and you omit this step, you will deny access for everyone except those clients mentioned in the first set of rules.

If you are using Specific Address Permission, this set of rules is optional.

3. Finally, the last rule allows you to access to the RealSystem Administrator port.

Note

Even if you are only interested in restricting access for a single client's requests, you must still create all the rules necessary for your method.

Numbering the Rules

Rule numbers can be any length, but a number of more than one digit is recommended in case more lists are added later; with multiple digits, the new lists can be inserted between existing lists. When you create a rule, you give it a number. RealServer uses these numbers to sort the rules before it looks at a client's request.

RealProxy compares the client's IP address and requested port to the sorted rules, beginning with the lowest-numbered rule. As soon as RealProxy finds a rule which matches the client's address, it allows or denies access, according to the rule's characteristics.

You do not have to create the rules in a certain order; RealProxy will perform the sorting automatically.

Getting the Expected Connections

Because RealProxy examines the rules in numeric order, you should make the lowest-numbered rules the most strict. Reserve high rule numbers for the most lenient rules. This is similar to the schema for firewall addresses.

Suggested Rule Schemes

Rule Set	Specific Address Denial	Specific Address Permission
Contents of Rules in Each Set		
1. Specific client addresses Suggested rule numbers: 100 - 490	Clients prevented from accessing RealServer. From setting: specific client addresses. Access setting: Deny Ports setting: <i>specific ports</i>	Clients permitted to connect to RealServer. From setting: specific client addresses. Access setting: Allow Ports setting: <i>specific ports</i>
2. All other addresses Suggested rule numbers: 500 - 990	Clients that can use your RealServer. From setting: Any Access setting: Allow Ports setting: <i>content ports</i> (Clients not permitted to use RealServer. From setting: Any Access setting: Deny Ports setting: <i>specific ports</i> This set of rules is optional.
3. Access to RealSystem Administrator Suggested rule number: 1000	All clients not listed in either of the rules above. From setting: Any Access setting: Allow Ports setting: <i>Admin Port</i>	All clients not listed in either of the rules above. From setting: Any Access setting: Allow Ports setting: <i>Admin Port</i>

Setting Up IP Access Control

There are two steps to setting up access control rules, regardless of which method you chose in “Deciding What Rules to Create”:

1. Set up general rules which allow you to remain connected to RealSystem Administrator. You need only perform this set of steps once.
2. Create rules for specific IP addresses and port numbers.

Creating General Access Rules

The steps in this section create a rule that allows you to connect to RealSystem Administrator, regardless of the restrictions you create in other rules.

Although it appears that you are allowing everyone to access RealSystem Administrator, the only people who will use it are other administrators who

know the Admin Port number (chosen randomly at installation) and who have a user name and password specifically for RealSystem Administrator.

Warning

If you omit this initial step, you will not be able to connect to RealSystem Administrator when you restart RealProxy, regardless of whether you have username-and-password permission.

Additional Information

To learn how to give access to RealSystem Administrator based on user name, see “RealSystem Administrator User Authentication” on page 129.

► To create the required access rule:

1. In RealSystem Administrator, click **General Setup**. Click **Ports**.
 2. Make a note of the **Admin Port** number. (This is the same number as the port number shown in your browser URL.)
 3. In RealSystem Administrator, click **Security**. Click **Access Control**.
 4. Click **Add an Access Rule**. A new browser window appears. (Picture to be supplied later)
-

5. In the **Access Rule Name** box, type 1000.
 6. From the Access list, select **Allow**.
 7. In the **To** box, type Any.
 8. In the **From** box, type Any.
-

9. In the **Restricted Ports** box, type the Admin Port number you noted in Step 2.
10. Click **OK**. You are returned to the Access Control page of RealSystem Administrator.
11. Click **Apply**.

You will now be able to access RealSystem Administrator, no matter what rules you create in the next section.

Creating Specific Access Rules

Use the steps in this section to allow or deny access to specific IP addresses or address ranges.

Warning

Be sure to first follow the steps in “Creating General Access Rules”, or you will not be able to access RealSystem Administrator after you restart RealProxy.

► To limit access according to IP number:

1. Determine the port numbers in use. You’ll use these in Step 8.
If this rule will refer to users who want to play streaming media, click **General Setup > Ports**. Make a note of the values for **PNA Port** (usually 7070), **HTTP Port** (usually 8080), and **RTSP Port** (usually 554).
If this rule will refer to G2 encoders that will be sending content to your RealProxy, click **Broadcasting > G2 Encoder**. Make a note of the value for **Port** (usually 4040).
If this rule will refer to pre-G2 encoders that will be sending content to your RealProxy, click **Broadcasting > Pre-G2 Encoder**. Make a note of the value for **Port** (usually 5050).
2. In RealSystem Administrator, click **Security**. Click **Access Control**. (Picture to be supplied later)

3. Click **Add an Access Rule**.
4. In the new window that appears, type a three-digit number for the new access rule in the **Access Rule Number** box. RealProxy uses the rule numbers in numeric order.

Warning

You must type a number in this box. RealProxy will ignore any rule that is not numbered.

Tip

Technically, you can type any number in this box. But because rules are sorted numerically, and because the rule that allows access to RealSystem Administrator must be the last rule on the list, use a three-digit number here so the RealSystem Administrator rule (given as rule 1000 in “Creating General Access Rules”) can be the last rule on the list.

5. Indicate whether permission is being granted or refused by selecting **Allow** or **Deny** from the **Access** list.
6. In the **To** box, type the IP address of the RealProxy machine.

Note

Avoid using 127.0.0.1 or localhost, unless you will only be using test links which use that exact text in their links.

Tip

To refer to any IP address on the RealProxy machine, type Any.

7. In the **From** box, type the IP address of the client machine, followed by the subnet mask. The subnet mask indicates whether the restriction refers to a single IP address an entire range of addresses.

There are two ways of showing the subnet mask:

- Place a slash mark after the IP address, and give the number of bits for the mask.
- Place a colon after the IP address, and give the full subnet mask.

For example, the following are equivalent and acceptable in the **From** box: 172.16.3.0:255.255.255.0 and 172.16.3.0/24. Both examples specify the range of addresses from 172.16.3.0 to 172.16.3.254.

To specify the netmask for single IP address, type either :255.255.255.255 or /32 after the IP address.

To specify the subnet for a range of IP addresses, type either a colon after the IP address followed by the full subnet mask, or type a slash mark after the IP address, and give the number of bits for the subnet mask (24, 16, or 8).

Tip

To refer to all clients, regardless of IP address, type the word Any in the **From** box, and omit the subnet mask.

8. Finally, list the RealProxy port numbers to which you want to restrict access. In the **Restricted Ports** box, type the port numbers, separated by commas.

You'll probably want to use the numbers for **RTSP Port** (1091) and **PNA Proxy Port** (1090).

To restrict access to all RealProxy content, the port numbers should match the other port numbers you've instructed RealProxy to listen to; look at the port numbers for RTSP port, PNA port, HTTP port, and the port value used by the encoder.

9. Click **OK**. You are returned to the Access Control page of RealSystem Administrator.

10. Click **Apply**.

Chapter 8

CHAINING ONE REALPROXY TO ANOTHER

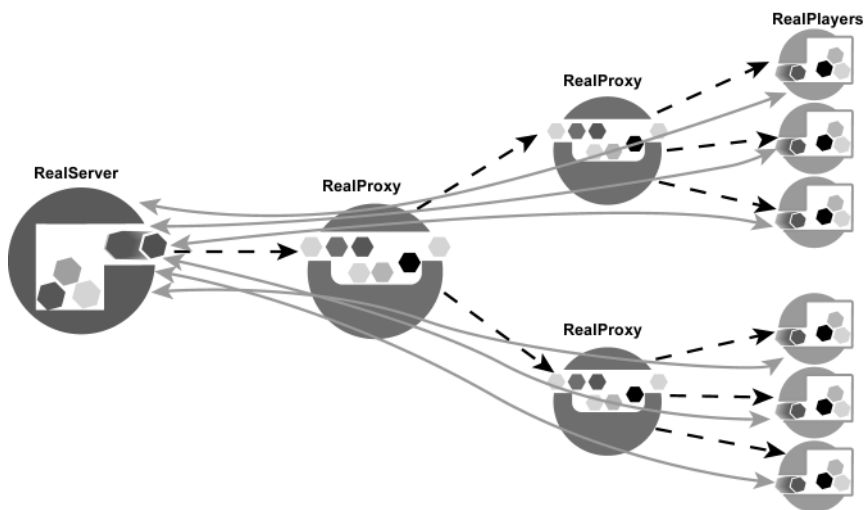
This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

Chaining is a way of connecting several RealProxies on a network so that all client requests for streamed media go through a single point.

Overview

By redirecting the requests handled by multiple RealProxies to a single RealProxy, you can funnel all client requests for streaming media to one point. A RealProxy that has been configured to send its requests to another RealProxy is called a “child” RealProxy; the RealProxy that receives the request is the “parent” RealProxy.

Chaining: Connecting RealProxies



In the example above, a client directs its request to a child RealProxy. That RealProxy, in turn, sends the request to the parent RealProxy. It is the parent RealProxy that sends the client's request to the origin RealServer. Once the RealServer has received the request, it establishes the accounting connection in the usual manner.

Setting Up Chaining

Configure a RealProxy to be a “child” RealProxy; you do not need to configure the parent RealProxy, since it will receive the connections automatically.

You can set up this feature for both RTSP client requests and PNA client requests.

► To set up chaining:

1. In RealSystem Administrator, click **Ports**. (Picture to be supplied later)



2. Indicate which the parent RealProxy to which this RealProxy should send requests by typing the parent RealProxy address in the **RTSP Parent Proxy Address** box.

If you want to forward PNA requests also, type the parent RealProxy address in the **PNA Parent Proxy Address** box.

3. Type the port number of the parent RealProxy in the **RTSP Parent Proxy Port** box.

Note

The port number you type needs to match the parent RealProxy's value for **RTSP Proxy Port**, usually 1091. (In

the configuration file, match the value for RTSPPort in the Proxy list.)

If you will be forwarding PNA requests, type the parent RealProxy port number in the **PNA Parent Proxy Port** box. This number needs to match the parent RealProxy's value for **PNA Proxy Port**, usually 1090. (In the configuration file, match the value for PNAPort in the Proxy list.)

4. Click **Add**.

Turning Off Chaining

Using RealSystem Administrator, delete the values you typed for the parent proxy addresses in “Setting Up Chaining”.

Chapter 9

MULTICASTING LIVE STREAMS

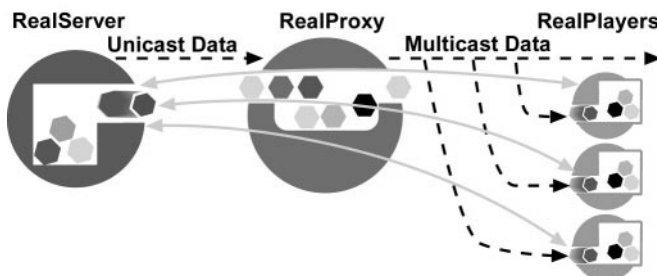
This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

Multicasting helps you conserve bandwidth. It requires a multicast-enabled network.

Overview

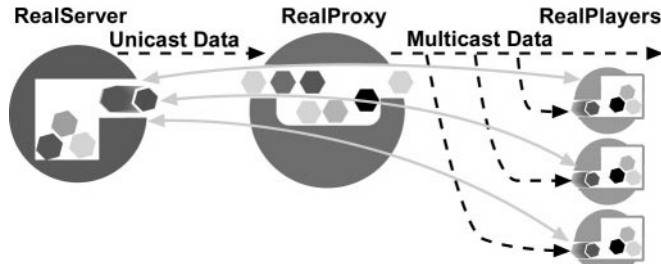
Multicasting is a way of sending a single live stream to multiple clients, rather than sending a stream to every single client.

Multicasting



In contrast, regular unicasting transmission sends a stream to each client that requests it.

Unicasting



To take advantage of multicasting, both RealProxy and clients, as well as the routers between them, must be multicast-enabled. For this reason, multicasting is mostly used with intranets where routers can be configured for multicasts. Multicast delivery can be done over the Internet where intermediary network devices have been multicast-enabled.

Multicast Methods

This method of multicasting uses the RTSP protocol to send control information over a TCP channel. RealProxy maintains a control connection for each client. The data channel is multicast to all clients.

RTSP multicast provides the following features:

- **Authentication**—user name and password for secure content is sent securely.
- **Connection statistics**—RealProxy can receive client connection information.
- **SureStream**—these multiply-encoded files are supported.

Note

RTSP multicasting works only with RealSystem G2 clients.

Setting Up Multicasting

Before you set up either type of multicasting, you need to do two things:

- Configure the network for multicasting.

- Select the addresses you'll use for your multicasts.

Setting Up the Network for Multicasting

Before setting up RealProxy, verify the following items with your network administrator:

- Routers in your network are multicast-enabled.
- The system running RealProxy is correctly configured for multicast support.

In addition to network settings, for clients to take full advantage of multicast transmissions, they must be configured to request multicast transmission of live material. Consult the client's user guide for information on configuring the client.

As noted earlier, both RealProxy and clients, as well as the routers between them, must be multicast-enabled in order for you to distribute presentations using the multicast features. This section describes only what is required to enable RealProxy for multicast broadcasting.

Allocating Addresses and Port Numbers in RealProxy

There are two factors to take into account when establishing the addresses and port numbers that RealProxy will use for multicasting:

- Select addresses from a legal range of available addresses. Valid ranges are between 224.0.0.0 and 239.255.255.255. The network administrator should know which multicast addresses are available on the intranet. On the Internet, certain ranges such as the addresses between 224.0.0.0 and 224.0.0.255 are reserved for other uses; see RFC 1700, "Assigned Numbers" for a complete list of restricted addresses.
- You must select enough addresses for the type of file you are multicasting. See "Determining Required Addresses and Port Numbers" for information on selecting the appropriate number. You'll need to know how many bit rates are included in each file that you are multicasting, and set aside the appropriate number.

Although the information in this document will help you calculate the number of addresses and port numbers you'll need for multicasting, you'll still need to consult with your network administrator regarding the actual addresses you'll use.

Determining Required Addresses and Port Numbers

For each file that you are transmitting via multicast, you must calculate the number of addresses you'll need. The number of addresses is based on the number of bit rates in the file. For simple RealVideo files, figuring the number of addresses and port numbers is relatively simple. SureStream files are more complex, as they can contain several bit rates, each with its own number of streams.

Unless you can find out the number of bit rates in the files that you are streaming, you'll have to guess. A safe number is six bit rates per file; the maximum number of bit rates that would be present in a single SureStream file is 14, yet files prepared for multicasts are likely to include only the higher encoding rates. A non-SureStream file would have at most one bit rate and two streams.

Addresses Needed for Back-Channel Multicasts

Bit Rates	Addresses
1	1
2	2
3	3
...	...
n bit rates	n

Setting Up Back-Channel Multicasting

Follow the instructions below to set up back-channel multicasting. After you set it up, you will need to create the links that point to your multicasted events.

► To set up back-channel multicasting:

1. In RealSystem Administrator, click **Multicasting**. Click **Back-Channel**.
(Picture to be supplied later)

2. In the **RTSP Port** box, type the port number to which RealProxy will direct its RTSP multicast streams. The value in this box refers to the client's port number. A typical value is 554.
3. Specify the range of addresses to which you want to multicast streams by filling in the **Address Range** box. RealProxy uses the first available address in this range. If your multicast streams are referenced in SMIL files, you will need one address for each stream.

Refer to "Determining Required Addresses and Port Numbers" on page 78 to calculate the exact number of addresses you'll need.
4. In the **IP Address** section, click **Add**.
5. In the new window that appears, type a description for this list in the **Rule Number** box.
6. In the **IP Address** box, type an address to the domain address of the client computer or network to which RealProxy will permit multicast transmissions.
7. In the **Netmask** box, type a netmask that limits the range to a particular subnet.
8. Click **Add**.

9. To require that the client addresses you just listed use multicast only, and not unicast, select Yes from the **Delivery Only** list. To remove this restriction and permit unicast for clients unable to connect via multicast, set it to No.
10. Indicate how far multicast packets can travel over a network by typing a value in the **Time to Live** box. Each time a multicast data packet passes through a multicast-enabled router, its Time to Live is decreased by 1. When the value is decremented to 0, the router discards the data packet. The value for **Time to Live** can range from 0 to 255. The larger the Time to Live, the greater the distance a data packet will travel.
The default value of 16 is enough to keep multicast packets within a typical internal network.

Time to Live (TTL) Values

TTL Value	Packet Range
0	Local host
1	Local network (subnet)
32	Site
64	Region
128	Continent
255	World

11. To allow missing packets to be resent to clients that request them, select True from the **Resend** list. This setting is optional. It adds some overhead to the traffic on your network; however, clients receive better quality multicasts.
12. Indicate which clients will be able to view your multicast presentations by configuring the **User List**.
To require that clients with IP addresses in the User List must connect in multicast mode, set **Deliver Only** to Yes. This setting means that clients that are not configured for multicast will not be able to receive the multicast, and will receive an error message instead. Use this feature when you want to restrict the multicast to a limited number of clients, or if you are multicasting a high-bandwidth presentation and do not want unicast to be an option.
 - a. In the **User List** area, select Yes from the **Delivery Only** list.

- b. Click **Add a User List**.
- c. In the **Rule Name** box that appears, type a rule number. The rule number is used by RealProxy for sorting the address rules.
- d. Type the IP Address of the client allowed to receive the multicast in the **IP Address** box. To allow any client to access the multicast, type 0.0.0.0.
- e. Type the subnet mask for the client IP in the **Netmask** box.
To indicate a single IP address, type 255.255.255.254 in the **Netmask** box. If you typed 0.0.0.0 in the **To** box, type the same thing in the **Netmask** box.
- f. Click **OK**.

Repeat Step b through Step f for each set of clients that will be accessing your multicast.

13. Click **Apply**.

Note

Access Control rules are enacted before User List rules. A client that is excluded by Access Control will not be able to connect to any multicasts, regardless of the rules you create here. (IP Access Control is described in “Limiting Access Via IP Address” on page 110.)

MONITORING REALPROXY ACTIVITY

This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

To manage current activity on your RealProxy, you'll want to track how many clients are being served. RealProxy includes a monitoring page within RealSystem Administrator. To generate reports of historical activity, see Chapter 11: Tracking RealProxy Activity.

Using RealSystem Administrator

RealSystem Administrator includes a section where you can view RealProxy activity.

- To view RealProxy activity via RealSystem Administrator:

In RealSystem Administrator, click **Monitor**. The monitor page appears in the right-hand frame. It dynamically updates to show information about the number of connections, and so on.

Additional information about the information shown is available on the monitor page itself.

Monitor in RealSystem Administrator

Session Type	Session Count	Client Traffic	Gateway Traffic
Passthrough	0	0	0
Cache	0	0	0
Splitter	0	0	0
Total	0	0	0

TRACKING REALPROXY ACTIVITY

This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

RealProxy can create reports of historical data that let you see trends and gather information. Track which visitors requested what data and how well the data was delivered. This information is stored in the proxy log. Any error messages are recorded in the error log.

Proxy Log

The RealProxy proxy log records the IP addresses of the clients that have connected, the clips they listened to, the times of day they connected, and much more. New information is always appended to the end of the proxy log.

Reading a Proxy Log

To read the contents of the proxy log, you must first look up the values of Logging Style in RealSystem Administrator, as this determines how much information is present in the proxy log. At installation, Logging Style is set to 3.

Logging Style provides information about RealProxy clip-serving activity.

Additional Information

Read about customizing RealProxy settings in “Configuring RealProxy Features”.

Once you know the values of Logging Style, view the proxy log by opening proxy.log (Windows) or proxy (UNIX) file in a word processor or text editor.

Proxy Log Format

RealProxy stores information about each clip it serves in a separate record. Each record is delimited by a new line. Fields within each record are separated by spaces.

One record is created for every clip served; if the client requests a presentation that includes several clips, one record is created for each clip in the presentation.

The fields that appear within each record depend on the settings for Logging Style. The complete syntax of each record, assuming Logging Style is gathering all possible information (Logging Style is 5) is shown:

```
client_IP_address - - [timestamp] "GET filename protocol/version" HTTP_error_code
bytes_sent [client_info] [client_id] file_size file_time sent_time resends failed_resends
[stream_components] start_time server_address average_bitrate packets_sent presentation_id
[proxy_info]
```

Note

Although in the rest of this manual, square brackets indicate optional material, the square brackets shown in the proxy log actually appear within proxy log records.

The following table lists the format for each proxy log record:

Proxy Log Format

Proxy Log Field	Description
<i>client_IP_address</i>	IP address of client, such as 123.45.123.45
- -	Two hyphens for compatibility with standard Web server log formats.
<i>timestamp</i>	Time that client accessed the file in the format: <i>dd/Mmm/yyyy:hh:mm:ss TZ</i> where <i>TZ</i> is the time zone expressed as the number of hours relative to the Coordinated Universal Time (Greenwich, England) and is relative to the server. For example: [31/Oct/1996:13:44:32 -0800]
" <i>GET filename</i>	File name (and path) requested by the client. If the client requests a file that doesn't exist, UNKNOWN appears in place of a file name.

(Table Page 1 of 5)

Proxy Log Format (continued)

Proxy Log Field	Description								
<i>protocol/version</i>	<p>Application-layer protocol used to send the clip to the client. Possible values are:</p> <p>RTSP PNA HTTP</p> <p>In addition, a letter at the end of the string indicates which transport type was used:</p> <table border="1"> <tr> <td>(blank)</td> <td>UDP connection</td> </tr> <tr> <td>T</td> <td>TCP connection</td> </tr> <tr> <td>H</td> <td>HTTP connection</td> </tr> <tr> <td>M</td> <td>Multicast</td> </tr> </table> <p>For example, PNAT means that the clip was sent using the PNA protocol over a TCP connection.</p> <p>The version number indicates the edition of the protocol.</p>	(blank)	UDP connection	T	TCP connection	H	HTTP connection	M	Multicast
(blank)	UDP connection								
T	TCP connection								
H	HTTP connection								
M	Multicast								
<i>HTTP_status_code</i>	Return code using HTTP standard error codes. Usually returns 200.								
<i>bytes_sent</i>	Number of bytes transferred to the client.								

(Table Page 2 of 5)

Proxy Log Format (continued)

Proxy Log Field	Description																
[<i>client_info</i>]	<p>Describes the version and type of client being used. Client information appears in the following format, [<i>platform version client type dist_code language CPU</i>]. If client information can't be gathered (the request came from a client that chose not to send statistics, or from a browser connecting to RealSystem Administrator pages), UNKNOWN appears within the brackets.</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>platform</i></td> <td>Operating system RealPlayer runs on-Win16, WinNT, Mac, and so on.</td> </tr> <tr> <td><i>version</i></td> <td>Operating system version number.</td> </tr> <tr> <td><i>client</i></td> <td>Version number of RealPlayer.</td> </tr> <tr> <td><i>type</i></td> <td>Type of RealPlayer.</td> </tr> <tr> <td><i>dist_code</i></td> <td>Distribution code of RealPlayer.</td> </tr> <tr> <td><i>language</i></td> <td>Language setting in RealPlayer.</td> </tr> <tr> <td><i>CPU</i></td> <td>Type of processor on which the client is running. If the processor does not have a hardware Floating Point Unit, the string "no-FPU" is appended to the end of the CPU field with no delimiter. For example: Win95_4.0_3.0.0.19_play32_PN01_EN_586</td> </tr> </tbody> </table> <p>RealAudio Player version 1.0 shows only two fields for [<i>client_info</i>]. They are <i>platform</i> and <i>client</i>.</p>	Field	Description	<i>platform</i>	Operating system RealPlayer runs on-Win16, WinNT, Mac, and so on.	<i>version</i>	Operating system version number.	<i>client</i>	Version number of RealPlayer.	<i>type</i>	Type of RealPlayer.	<i>dist_code</i>	Distribution code of RealPlayer.	<i>language</i>	Language setting in RealPlayer.	<i>CPU</i>	Type of processor on which the client is running. If the processor does not have a hardware Floating Point Unit, the string "no-FPU" is appended to the end of the CPU field with no delimiter. For example: Win95_4.0_3.0.0.19_play32_PN01_EN_586
Field	Description																
<i>platform</i>	Operating system RealPlayer runs on-Win16, WinNT, Mac, and so on.																
<i>version</i>	Operating system version number.																
<i>client</i>	Version number of RealPlayer.																
<i>type</i>	Type of RealPlayer.																
<i>dist_code</i>	Distribution code of RealPlayer.																
<i>language</i>	Language setting in RealPlayer.																
<i>CPU</i>	Type of processor on which the client is running. If the processor does not have a hardware Floating Point Unit, the string "no-FPU" is appended to the end of the CPU field with no delimiter. For example: Win95_4.0_3.0.0.19_play32_PN01_EN_586																
[<i>client_id</i>]	<p>Unique ID generated during RealPlayer installation that enables you to track details for individual clients. If client information can't be gathered (the request came from a client that chose not to send statistics, or from a browser connecting to RealSystem Administrator pages), UNKNOWN appears within the brackets. Included when Logging Style is set to 2 or higher.</p>																
<i>file_size</i>	<p>Total amount in bytes of media data in the media file. This number is less than the size of the media file because it does not include the file header and other non-media information stored in the file. For live broadcasts, <i>file_size</i> is always 0. Included when Logging Style is set to 1 or higher.</p>																
<i>file_time</i>	<p>Total length, in seconds, of media stored in the media file. For live broadcasts, <i>file_time</i> is always 0. Included when Logging Style is set to 1 or higher.</p>																

(Table Page 3 of 5)

Proxy Log Format (continued)

Proxy Log Field	Description
<i>sent_time</i>	Total length, in seconds, of the media sent to the client. Included when Logging Style is set to 1 or higher.
<i>resends</i>	Number of packets successfully resent because of transmission errors. Included when Logging Style is set to 1 or higher.
<i>failed_resends</i>	Number of packets not successfully resent in time to correct transmission errors. Included when Logging Style is set to 1 or higher.
[<i>stream_components</i>]	Type of material sent, indicated in the following pattern: RealAudio RealVideo Event RealImage 1 shows that the stream includes this type, 0 indicates that it does not. Thus, a stream that included RealVideo and RealAudio but no events or RealImages would appear in the proxy log as: 1 1 0 0. Included when Logging Style is set to 3 or higher.
<i>start_time</i>	Timestamp of start time. Included when Logging Style is set to 3 or higher.
<i>server_address</i>	IP address where clip came from. This may be the origin RealServer, a RealServer which is acting as a receive splitter, or another RealProxy which is acting as a receive splitter. Included when Logging Style is set to 3 or higher.
<i>average_bitrate</i>	Average bitrate of clip. Included when Logging Style is set to 4 or higher.
<i>packets_sent</i>	Number of packets sent. Included when Logging Style is set to 4 or higher.
<i>presentation_id</i>	Number used by other clips in a SMIL presentation. All elements from the same presentation use the same number. The SMIL file itself is also included in the log, and shares the number as well. The number is assigned by RealProxy at the time of transmission. Included when Logging Style is 5.

(Table Page 4 of 5)

Proxy Log Format (continued)

Proxy Log Field	Description	
[<i>proxy_info</i>]	Displays information about the type of proxied stream (always included):	
	Value	Meaning
	Demand Pass-Through	The proxied stream was an on-demand clip, and it was sent in passthrough mode.
	Live Pass-Through	The proxied stream was a live clip, and it was sent in passthrough mode.
	Live Split	The proxied stream was a live clip, and it was sent via push splitting.
	Demand Cache Hit	The proxied stream as an on-demand clip, and RealProxy served it from the media cache.
	Unknown	Clip type and delivery were of unknown type.

(Table Page 5 of 5)

LoggingStyle Results

The format of the proxy log under each of the different Logging Style values is shown in the table below:

Logging Style Effect on Proxy Log

Logging Style value	Individual record format
0	<i>client_IP_address</i> - - [<i>timestamp</i>] "GET <i>filename protocol/version</i> " <i>HTTP_status_code bytes_sent [client_info] [client_id]</i> <i>[proxy_info]</i>
1	<i>client_IP_address</i> - - [<i>timestamp</i>] "GET <i>filename protocol/version</i> " <i>HTTP_status_code bytes_sent [client_info] [client_id] file_size</i> <i>file_time sent_time resends failed_resends [proxy_info]</i>
2	<i>client_IP_address</i> - - [<i>timestamp</i>] "GET <i>filename protocol/version</i> " <i>HTTP_status_code bytes_sent [client_info] [client_id] file_size</i> <i>file_time sent_time resends failed_resends [proxy_info]</i>
3	<i>client_IP_address</i> - - [<i>timestamp</i>] "GET <i>filename protocol/version</i> " <i>HTTP_status_code bytes_sent [client_info] [client_id] file_size</i> <i>file_time sent_time resends failed_resends [stream_components]</i> <i>start_time server_address [proxy_info]</i>

(Table Page 1 of 2)

Logging Style Effect on Proxy Log (continued)

Logging Style value	Individual record format
4	<i>client_IP_address - - [timestamp] "GET filename protocol/version" HTTP_status_code bytes_sent [client_info] [client_id] file_size file_time sent_time resends failed_resends [stream_components] start_time server_address average_bitrate packets_sent [proxy_info] [proxy_info]</i>
5	<i>client_IP_address - - [timestamp] "GET filename protocol/version" HTTP_status_code bytes_sent [client_info] [client_id] file_size file_time sent_time resends failed_resends [stream_components] start_time server_address average_bitrate packets_sent presentation_id [proxy_info]</i>

(Table Page 2 of 2)

Customizing Information Reported by the Proxy Log

To gather information with the proxy log, you must first decide what types of information you want to gather. Then make the appropriate changes to Logging Style.

Placing the Proxy Log

At installation, RealProxy is configured to place log files in the Logs subdirectory of the main RealProxy directory and Logging Style is set to 3.

► To indicate where to store the proxy log file:

1. In RealSystem Administrator, click **General Setup**. Click **Logging**.
2. Type the name you want to use in the **Proxy Log Path** box. The default name of the proxy log file is proxy.log (Windows) or proxy (UNIX), and it is usually placed in the Logs subdirectory of the main RealProxy directory. The directory (if any) typed here can be absolute or relative to the base path of the main mount point.
The name of the access file will be different if Log File Rolling is enabled; see "Log File Rolling" on page 93.
3. When you are finished, click **Apply**.

If **Proxy Log Path** is blank, RealProxy records access information in the proxy.log or proxy file located in the same directory as the RealProxy executable file.

Gathering Information with Logging Style

To configure RealProxy to collect access information, configure Logging Style. There are six options, styles 0 through 5. Each logging style includes information of the logging styles with lower numbers. Thus, Logging Style 3 collects the information that's collected by styles 0, 1, and 2, as well as the material gathered by style 3. If you omit this variable, RealProxy uses the default style of 0.

A list of information gathered by each value is given below.

Logging Styles 0, 1, and 3 contain some additional information, as described in “Proxy Log Format” on page 86.

Information Collected by Logging Style

To gather this information...	...set LoggingStyle to this value
Bytes sent	0
Clip name including path	0
Client IP address and platform information	0
Timestamp	0
File size (in bytes)	1
File time (total file length in seconds)	1
Packets successfully and unsuccessfully resent	1

(Table Page 1 of 2)

Information Collected by Logging Style

To gather this information...	...set LoggingStyle to this value
Protocol (RTSP or PNA)	1
Send time (total media sent in seconds)	1
Transport method (TCP, UDP) and version	1
Client ID	2
Server IP Address	3
Stream components	3
Timestamp for start time	3
Average bitrate	4
Packets sent	4
Common presentation identifier	5

(Table Page 2 of 2)

Log File Rolling

Proxy log files can grow indefinitely as they accumulate data. To keep log files to a manageable size, you can limit the proxy log to a weeks's worth of information or a certain file size, and RealProxy will begin a new log file when the limit is reached.

Log file rolling applies only to proxy log files.

► To set up log file rolling:

1. In RealSystem Administrator, click **General Setup**. Click **Logging**.
2. Indicate where log files should be stored by giving the path and file name in the **Access Log Path** box. This is described in “Placing the Proxy Log” on page 91.
3. Decide whether to limit the log files by time period or by size.
 - To limit by time period, choose the period from the **Log Rolling Frequency** list. You can save by the hour, day, week, or month.
In the **Log Rolling Interval** box, type the number of time periods. For example, if you chose **Days** from the **Log Rolling Frequency** list and typed 4 in the Log Rolling Interval box, RealProxy will start a new proxy log every 4 days.
 - To limit by file size, type a number in the **Log Rolling Size** box. Specify the size in megabytes.

If you have values in all three boxes, RealProxy will use the size or time period that is reached first.

4. When you're done, click **Apply**.

Rolled log files are named with the following format:

name.log.datestamp

where:

<i>name</i>	Name of the regular log file. The name for proxy logs is taken from the LogPath setting (usually rmaxcess).
<i>log</i>	The log file extension.
<i>datestamp</i>	The date stamp, in the following format: <i>YYYYMMDDHHMMSS</i> where:
<i>YYYY</i>	Year.
<i>MM</i>	Two digits of the month.
<i>DD</i>	Date, in two digits. January would be 01.
<i>HH</i>	Hour
<i>MM</i>	Minutes
<i>SS</i>	Seconds

Disabling Log File Rolling

Choose **Never** from the **Log Rolling Time Period** list, and type 0 (zero) for the **Log Rolling size**.

Error Log

The error log contains both information and error messages about server operation. By looking for patterns of errors, you can troubleshoot and correct possible problems on your site.

View the text of the error log using a word processor or text editor.

The error log is an excellent tool for troubleshooting any problems that may arise with your RealProxy. An entry is made to the error log only when an error occurs. If no errors occur, this file will not exist.

Error messages relating to RealProxy activity appear in the error log. The error log is created when the first error occurs.

For a list of error messages that can appear in this file and what to do about them, visit the RealNetworks technical support page at <http://service.real.com>. If you have an entry that refers to a fatal error, contact the RealNetworks Technical Support Department for assistance.

- To customize where RealProxy creates the error log:
 1. In RealSystem Administrator, click **General Setup**. Click **Logging**.
 2. In the **Error Log Path** box, type the path and name you want to use for the error log. The default location is the Logs directory of the main RealProxy directory, and the default file name is `rmerror.log`.
 3. When you have finished making changes, click **Apply**.

Error Log Format

The error log records client connections and RealProxy errors. Each time an error is generated by RealProxy, a record is created in the error log. The error log path is stored in the same directory as the proxy log, indicated by the `LogPath` variable.

Syntax of the file is as follows:

```
***date time servername(process_ID): error_message
```

where entries are defined below:

Error Log Syntax	
Entry	Meaning
<code>***</code>	Three asterisks indicate an error. Informational messages are not preceded by asterisks.
<code>date</code>	Date on which the error occurred. Given in the form <code>d-Mmm-YY</code> .
<code>time</code>	Time the error occurred, according to RealProxy. Given in the form <code>HH:MM:SS:TT.hhh</code>
<code>servername(process_ID)</code>	The server name, followed by the process ID in parentheses.
<code>error_message</code>	Text of error message

Example Error Log

A sample error message looks like this:

```
***15-Nov-96 14:13:30.488 myserver(1556): 6220: No such user: joe
```




CONFIGURATION FILE SYNTAX

This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

This appendix describes the structure of the configuration file.

Configuration File Components

The configuration file is constructed entirely of tags. There are four types of tags in this file: the XML declaration tag, optional comment tags, list tags, and variable tags.

Of these four types, only two make up the instructions to RealServer: lists and variables. Lists are used for instructions that have several parts, such as the MIME types or the multicast instructions. A list tag is followed by one or more list tags or variable tags.

All values for lists and variables are enclosed in double quotation marks.

XML Declaration Tag

The XML declaration tag indicates which version of XML is in use. RealProxy uses XML version 1.0. The declaration tag looks like this:

```
<?XML Version="1.0" ?>
```

Comment Tags

Comment tags are used in the configuration file to identify the functions of tags, but the comments aren't required. XML comment tags are just like those in HTML: they begin with `<!--` and end with `-->`. RealProxy ignores these tags; they are for your benefit.

For example, this comment tag lets the administrator know that the parameters after it refer to the path settings:

```
<!-- P A T H S -->
```

Tip

To disable a feature, convert the feature's tag or tags to a comment. Rather than converting each tag to a comment, edit only the feature's first opening tag and last closing tag.

Do not nest comment tags within other comment tags.

List Tags

The list tag uses the following syntax:

```
<List Name="name">
```

```
...
```

```
</List>
```

where *name* is the list title. Using the correct capitalization for *name* is important.

Other lists or variables follow the list. The `</List>` tag signifies the end of the list. If other lists are inside the original list, they must also have closing `</List>` tags. The `MIMETypes` list is an example of a list that contains other lists.

Tip

Indenting list items is not required, but is recommended for clarity.

Variable Tags

Variable tags use the following syntax:

```
<Var name="value"/>
```

where *name* is the variable title, and *value* is a string or a number, depending on the variable. Capitalization for both *name* and *value* is important.

Unlike lists, variables do not have a closing tag; instead, a forward slash mark (/) appears before the closing angle bracket (>).

Tip

If you've restarted RealProxy and it's not responding to a change you've made to a variable, make sure the variable has a closing forward slash mark, and that there is no space between them.

Variables can be independent elements (such as `LogPath`) or they may appear inside a list. When variables appear within a list, their meaning is determined by the value of the list name, although they may be apparently identical in syntax to variables that are not inside lists. If there are multiple variables within a list that do similar things, their names must be unique. For example, the `Extension` variables within each `MIMETypes` list must have different names; this is accomplished by adding a number to the end of each (`Extension_01`, `Extension_02`, and so on).

CONFIGURATION FILE CONTENTS



This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

This appendix gives brief information about the contents of the configuration file for those administrators interested in editing it directly.

Editing the Configuration File

For those RealProxy administrators who prefer to modify features by editing the configuration file directly, this appendix shows sample configuration file contents with brief descriptions. Detailed descriptions can be found in the chapters that describe each subject.

If you are going to modify the configuration file directly, please read the following sections:

- **Appendix A: Configuration File Syntax**—explains the structure of this file
- **“Configuring RealProxy Features” in Chapter 3**—contains instructions on modifying the configuration file with a text editor

It is recommended that you first use RealSystem Administrator to make changes, and then examine the configuration file to learn how changes are made. Noticing how lists are created and changed will be especially instructive.

Warning

Exit RealSystem Administrator before opening the configuration file with a text editor or unexpected changes may result.

Elements of the Configuration File

Settings are grouped into like categories. Variables that are not part of lists can appear anywhere in the configuration file, but are grouped here for clarity.

Most configuration file variables closely match names in RealSystem Administrator. Differences are noted here.

Ports

Port settings are described in Chapter 3: Configuring RealProxy Features. MonitorPort is described in Chapter 10: Monitoring RealProxy Activity.

<code><Var MonitorPort="9090"/></code>	The port which monitors (such as G2 Java Monitor) connect to RealProxy.
<code><Var AdminPort="7845"/></code>	Port number for RealSystem Administrator connection.

Paths

LogPath and ErrorLogPath are described in Chapter 11: Tracking RealProxy Activity. PIDPath is described in Chapter 5: Advanced Features. PluginDirectory is described on Chapter 3: Configuring RealProxy Features. LicenseDirectory is given on Chapter 2: Starting and Stopping RealProxy.

Windows Variables

Path variables, along with typical paths used in Windows NT and Windows NT, are shown here.

<code><Var LogPath="C:\Program Files \Real\RealServer\Logs\proxy.log"/></code>	LogPath indicates where and with what name the proxy log will be stored. If omitted, RealProxy places proxy.log in the Logs directory.
<code><Var ErrorLogPath="C:\Program Files \Real\RealProxy\Logs\proxyerr.log"/></code>	ErrorLogPath gives the path and name of the error log file. If this setting is omitted, RealProxy places proxyerr.log in the Logs directory.
<code><Var PluginDirectory="C:\Program Files Real\RealProxy\Plugins"/></code>	Shows where the plug-in files are stored.

`<Var LicenseDirectory="C:\Program File
 \Real\RealProxy\License"/>` Gives the location of the license files.

`<Var SupportPluginDirectory=
 "C:\Program File\Real\RealProxy
 \Lib"/>` Shows location of the Lib directory

UNIX

One additional setting is found on RealProxy running on a UNIX system: PIDPath.

`<Var LogPath="/usr/bin/RealServer
 /Logs/proxy.log"/>` LogPath indicates where and with what name the proxy log will be stored. If omitted, RealProxy places proxy.log in the Logs directory.

`<Var ErrorLogPath="/usr/bin/
 RealProxy/Logs/proxyerr.log"/>` ErrorLogPath gives the path and name of the error log file. If this setting is omitted, RealProxy places proxyerr.log in the Logs directory.

`<Var PluginDirectory="/usr/bin
 /RealProxy/Plugins"/>` Shows where the plug-in files are stored.

`<Var LicenseDirectory="/usr/bin
 /RealProxy/License"/>` Gives the location of the license files.

`<Var PidPath="/usr/bin/RealProxy
 /Logs/rmsserver.pid"/>` In UNIX systems, the location of the process id file.

`<Var SupportPluginDirectory="/usr/bin
 /RealServer/Lib"/` Shows location of the Lib directory

RealProxy

Three sections refer specifically to RealProxy.

If you establish values for MaxProxyConnections, MaxProxyBandwidth, MaxGatewayBandwidth, and LowBitRateGateway, RealProxy will limit access when the lowest threshold is reached.

```
<!-- P R O X Y   S E R V E R-->
```

```
<List Name="Proxy">
```

```
<Var RTSPPort="1091"/>
```

Port number where RealProxy listens for RTSP requests.

```
<Var PNAPort="1090"/>
```

Port number where RealProxy listens for PNA requests.

<code><Var CacheEnable="0"/></code>	When value is 1, RealProxy looks for media cache information in the configuration file and forwards requests for on-demand material to the cache file system. (See the next section.)
<code><Var BitsaveEnable="1"/></code>	When value is 1, RealProxy streams all live requests, rather than opening separate data channels between the origin RealServer and the client. If you disable this setting, RealProxy will not be able to perform pull splitting.
<code><Var BitsaveMountPoint="/split"/></code>	Used for bitsave mode.
<code><Var BitsavePort="3030"/></code>	Used for bitsave mode.
<code><Var MaxProxyConnections="1000"/></code>	Limits the number of connections that RealProxy will proxy simultaneously. Must be less than or equal to the number of streams in your license. Range is 1 to 32767. If omitted or set to 0, RealProxy uses the number in your license.
<code><Var MaxProxyBandwidth="0"/></code>	Limits the amount of kilobits per second which RealProxy will use when clients connect
<code><Var MaxGatewayBandwidth="0"/></code>	Limits the bandwidth in kilobits per second that RealProxy will use when connecting to its gateway.
<code><Var LowBitRateGateway="0"/></code>	When set to "1", uses minimum bit rate for SureStream requests. Normally, clients can shift through available bit rates in a SureStream file. This feature automatically requests only the lowest bit rate available. In RealSystem Administrator, this is called Low Gateway Bandwidth .
<code><Var LoggingStyle="5"/></code>	Determines how much data about clips served is gathered in the access log. See Chapter 11: Tracking RealProxy Activity for a list of options.
<code><Var RTSPParentProxyAddress="RTSPProxyHostIP"/></code>	When a value is included, chains this RealProxy's RTSP requests to a parent RealProxy, as identified by the IP.
<code><Var RTSPParentProxyPort="1091"/></code>	Parent RealProxy's RTSP port number.

<code><Var PNAParentProxyAddress= "PNAProxyHostIP" /></code>	When a value is included, chains this RealProxy's PNA requests to a parent RealProxy, as identified by the IP.
<code><Var PNAParentProxyPort="1090" /></code>	Parent RealProxy's PNA port number.
<code></List></code>	

RTSP Redirection

The RTSPRedirector list is used to instruct clients to contact RealProxy directly. It requires that you use a third-party hardware or software router to redirect the client requests to RealProxy. See “Configuring RealProxy to Listen for Re-Routed Client Messages” on page 47 for more information.

<code><List Name="RTSPRedirector"></code>	
<code><Var Port="554" /></code>	Port number where the redirect plugin should listen for RTSP redirections from the router.
<code><Var RedirectToAddress= "RedirectIPGoesHere" /></code>	RealProxy address to which the clients should directly address their requests.
<code><Var RedirectToPort="1091" /></code>	RealProxy port number to which the clients should directly address their requests.
<code></List></code>	
<code><List Name="PNARedirector"></code>	
<code><Var Port="7070" /></code>	Port number where the redirect plugin should listen for PNA redirections from the router.
<code><Var RedirectToAddress= "RedirectIPGoesHere" /></code>	RealProxy address to which the clients should directly address their requests.
<code><Var RedirectToPort="1090" /></code>	RealProxy port number to which the clients should directly address their requests.
<code></List></code>	

MIME Types

Setting up RealProxy to send correct MIME type information with clips is described in Chapter 2: Starting and Stopping RealProxy.

<code><List Name="MimeTypes"></code>
<code><List Name="audio/x-pn-realaudio"></code>

```
<Var Extension_01="ra"/>
<Var Extension_02="ram"/>
</List>
<List Name="application/x-pn-realmedia">
  <Var Extension_01="rm"/>
</List>
<List Name="application/x-pn-realmedia">
  <Var Extension_01="rt"/>
</List>
<List Name="application/x-pn-realmedia">
  <Var Extension_01="rp"/>
</List>
<List Name="application/x-pn-realmedia">
  <Var Extension_01="smi"/>
</List>
<List Name="application/sdp">
  <Var Extension_01="smi"/>
</List>
<List Name="text/html">
  <Var Extension_01="html"/>
  <Var Extension_02="htm"/>
</List>
<List Name="image/gif">
  <Var Extension_01="gif"/>
</List>
<List Name="image/jpg">
  <Var Extension_01="jpg"/>
  <Var Extension_02="jpeg"/>
</List>
</List>
```

File Systems

The FSMount section of the configuration file gives the names of all the configurable file system plug-ins in use. The plug-ins themselves are stored in a directory indicated by the PluginDirectory variable.

All requests of the RealProxy are processed by plug-ins. Plug-ins control which features are available. The modular plug-in design means that new features can be programmed and easily substituted for the existing plug-ins. New plug-ins may require different list arrangements and variables; check with the developer of the plug-in for this information.

Additional Information

RealSystem G2 SDK Developer's Guide provides developers with the public interfaces used to extend and customize RealSystem G2 to stream new datatypes, create new clients, or to customize RealProxy by building a new plug-in.

ShortName Variable

Each list within `FSMount` gives a short name for the plug-in. The short name is also stored within the plug-in file itself, and RealProxy uses this to identify the correct file to use. To add a plug-in to your RealProxy, you must know the name to use in the `FSMount` section; this name is supplied by the developer of the plug-in. The short name is referenced with the `ShortName` variable in each file systems list.

RealNetworks Plug-in Names

ShortName	Windows Filename	UNIX Filename	Description
pn-local	smp13260.dll	smp1fsys.so.6.0	Local File System
pn-admin	admi3260.dll	adminfs.so.6.0	Admin File System
pn-splitter	pull3260.dll	pullplin.so.6.0	Pull Splitting File System

RealSystem Administrator

Two file systems work together to operate RealSystem Administrator: the local file system and the administration file system.

The administration file system accepts the initial URL for RealSystem Administrator. It requests the HTML files from the local file system. Once the local file system delivers the HTML files, the administration file system looks up your RealProxy's values and displays them at the appropriate points in RealSystem Administrator.

Three variables are used for the RealAdministrator list: `ShortName`, `MountPoint`, and `BasePath`.

Five variables are use in the RealAdministrator_Files list: ShortName, MountPoint, Authorized_User_Group, Authentication, and Realm.

This tool is described in Chapter 3: Configuring RealProxy Features.

```
<ListName="RealAdministrator_Files">
  <Var ShortName="pn-admin">      RealSystem Administrator uses the pn-
                                admin plugin.
  <Var MountPoint="/admin/">     The default value for MountPoint is
                                /admin/. If you change this, you will need to
                                type a new URL to connect to RealSystem
                                Administrator.

  <Var BaseMountPoint=
"/localadmin/">                This special form of mount point reflects
                                the mount point of the RealAdministrator
                                list.
  <Var Realm="AdminRealm"/>     The Realm variable identifies which
                                AuthenticationRealm settings will be used
                                with requests sent to the RealSystem
                                Administrator mount point.

  <Var Authentication="True"/>   Indicates that authentication is in use.
</List>

<List Name="RealAdministrator">
  <Var ShortName="pn-local"/>    RealSystem Administrator uses the local file
                                system.
  <Var MountPoint="/localadmin/"> Mount point, used when
                                RealAdministrator_Files list requests files
                                from this plugin. The default value is
                                /localadmin/. If you change this, be sure to
                                change the RealAdministrator_Files list's
                                BaseMountPoint to match.

  <Var BasePath="C:\Program Files
\Real\RealProxy
\RealAdministrator"/>         Location of the RealSystem Administrator
                                files.
</List>
```

IP Binding

The ability to reserve specific addresses for RealProxy's use is explained in Chapter 5: Advanced Features. This list uses variables numbered sequentially:

Address_01, Address_02, and so on. Use one for each IP address you want to set aside for RealProxy. Use the RealProxy's IP address or DNS name for each variable; however, the IP address allows RealProxy to be more efficient.

RealProxy will bind to the specified addresses only; it will not bind to localhost.

If you don't use any values for the variables in the IPBinding list, RealProxy binds to the host IP address and localhost. It does not bind to any others.

```
<List Name="IPBinding">
```

```
<Var Address_01="0.0.0.0"/>
```

Each variable gives an address to reserve for use by RealProxy. To reserve all addresses, set the address variable to 0.0.0.0 and remove all other address variables from the list.

```
</List>
```

Allowance

Settings in this section refer to the allowance plug-in. They are described in Chapter 7: Limiting Access to RealProxy.

When set to On, ValidPlayerOnly sends a message to any clients other than RealNetworks RealPlayer version 5.0 or RealNetworks RealPlayer G2 directing them to upgrade to the latest version of RealPlayer. If set to Off, all clients can receive all clips.

```
<Var ValidPlayersOnly="True"/>
```

Allows only RealPlayer version 5.0 and RealPlayer G2 to access content. Any other clients attempting to view or listen to content display a message directing them to upgrade to the latest version of RealPlayer. If ValidPlayerOnly is set to Off, all clients can receive all clips. In Basic Server and Basic Server Plus, this is set to On and cannot be changed.

```
<Var MinPlayerVersion="2"/>
```

Sets the minimum RealPlayer version that can access the content. To limit to version 2.0 and later, set MinPlayerVersion to 2, and so on. To allow only RealPlayer G2, set it to 6.

<code><Var MinPlayerProtocol="0"/></code>	Limits access by protocol number. Use one of the following values for MinPlayerVersion: 1 RealAudio Player version 1.0 2 RealAudio Player version 2.0 3 RealAudio Player version 3.0 4 RealPlayer version 4.0 5 RealPlayer version 5.0 6 RealPlayer G2
<code><Var PlusOnly="False"/></code>	When set to True, PlusOnly allows only RealPlayer Plus to play content.

HTTP Support

This feature, which indicates the virtual directories whose content can be streamed via HTTP, is explained in [Chapter 7: Limiting Access to RealProxy](#). Each Path variable gives the name of a virtual directory whose content can be streamed via HTTP.

Be sure that Admin is on this list; Admin refers to RealSystem Administrator, which is served via HTTP. And push splitting uses HTTP for the initial connection conversation; add the push splitting mount point to this list, usually farm.

<code><List Name="HTTPDeliverable"></code>	
<code><Var Path_01="/admin"/></code>	Each Path variable gives the name of a mount point, directory or virtual directory whose content can be streamed via HTTP.
<code><Var Path_02="/localadmins"/></code>	
<code><Var Path_03="/ramgen"/></code>	
<code></List></code>	

Access Control

Restricting access to RealProxy content via the requesting client's IP address is described in [Chapter 7: Limiting Access to RealProxy](#). For every address or address range to which you want to restrict access, create a list with a unique number. The number can be any length, but a number of more than one digit is recommended in case more lists are added later; with multiple digits, the new lists can be inserted between existing lists.

Each list is called a rule. Rules are processed in numerical order. RealProxy searches the list of rules to find the first rule that matches the address. Because RealProxy searches the list of rules in numerical order, make your broadest categories first.

Within each list, the following settings are used: Access, Transport, To, From, and a list named Ports.

<List Name="AccessControl">	
<List Name="100">	
<Var Access="Allow"/>	Whether access is allowed or denied: set to Allow or Deny.
<Var Transport="TCP"/>	Transmission method being accessed. TCP is the only option for this list.
<Var To="127.0.0.1"/>	Address of the host RealProxy or network card of hosting machine. Use specific address or Any.
<Var From="any"/>	Address of the client computer whose access you are limiting. Use specific address or Any. To specify a range of IP addresses, either place a colon after the IP address and give the full subnet mask, or place a slash mark after the IP address and give the number of bytes for the subnet mask. For example, the following are equivalent values to use in the From variable: 172.16.3.0:255.255.255.0 and 172.16.3.0/24. Both examples specify the range of addresses from 172.16.3.0 to 172.16.3.254.
<List Name="Ports">	List of ports to which access is restricted.
<Var Port_01="554"/>	The port number should match the port numbers which RealProxy is using for other features, such as RTSPPort.
<Var Port_02="4040"/>	
<Var Port_03="5050"/>	
<Var Port_04="7070"/>	
<Var Port_05="8080"/>	
<Var Port_06="9090"/>	
</List>	
</List>	
</List>	

Splitting

Only three variables appear in the pull splitting section: ShortName, MountPoint, and Port. The source RealProxy and the source splitter have the same information in their Splitter_DoubleURL sections, but each system is

interested in different information: the RealProxy looks at the Port value, and the splitter looks at the mount point.

Warning

If you change these settings, RealProxy will not be able to operate in bitsave mode.

```
<List Name="Splitter_DoubleURL">
  <Var ShortName="pn-splitter"/>
  <Var MountPoint="/split/">
  <Var Port="3030"/>
</List>
```

Short name of the pull splitting plugin. Default is pn-splitter.

Mount point. Used in URLs that reference pull splitting streams. Default is /split/.

Port number to which the source RealProxy will listen for pull splitting requests.

Multicasting

Back-channel multicasting is described in Chapter 9: Multicasting Live Streams.

Settings used with this list are AddressRange, DeliveryOnly, RTSPPort, Resend, and TTL.

```
<List Name="Multicast">
  <Var AddressRange="">
  <List Name="ControlList">
    <Var Allow=
      "164.16.2.24:255.0.0.0"/>
  </List>
```

Range of addresses to which you want to send streams, in the form of *address-address*. RealProxy uses the first available address in this range. If you are using other types of multicast, be sure that the address ranges are different and do not overlap. If your multicast streams are referenced in SMIL files, you will need one address for each stream.

The ControlList list gives the addresses of clients allowed to receive multicast transmissions.

Address and netmask, separated by a colon, of clients allowed to receive multicast transmissions. Uses same format as From variable in AccessControl list.

<code><Var DeliveryOnly="False"/></code>	Requires clients listed in <code>Controllist</code> to receive only multicast transmissions from RealProxy. When <code>DeliveryOnly</code> is <code>False</code> , clients on <code>Controllist</code> can receive both multicasts and unicasts.
<code><Var RTSPPort="554"/></code>	Port on client machines to which RealProxy sends RTSP streams. Default value is 554.
<code><Var TTL="16"/></code>	Time To Live for multicast packets travelling over the network.
<code><Var Resend="True"/></code>	Allows or denies requests from clients for resends of missing UDP packets.
<code></List></code>	

Authentication

Authentication is used to verify the identity of users who access RealSystem Administrator. It ensures that only the people you've authorized can make changes to RealProxy.

Additional Information

RealProxy uses a subset of the authentication features available to RealServer. For more information on authentication, refer to *RealServer Administration Guide*.

Authentication Realms

A realm is a way of associating a group of users and the protocol used to verify their credentials.

Each sublist of `AuthenticationRealms` gives properties for a different realm. Every realm has a name (identified by the `Realm` variable), and a list that identifies what type of authentication is used in that realm. Depending on which authentication type you choose, different variables are required within the sublist.

```
<List Name="AuthenticationRealms">
  <List Name="SecureAdmin">      A realm.
    <Var Realm="AdminRealm"/>   Name of this realm.
    <List Name="BasicAuthenticator"/>
      <Var PluginID="rn-auth-basic"/> Security type.
      <Var DatabaseID="Admin_Basic"/>
```

```

    </List>
  </List>
</List>

```

Databases List

The databases list stores usernames and passwords of authorized users.

Within the list, sublists associate database plugins with location information.

The options available to each sublist are PluginID, Path, DBName, DBLoginPassword, and DBLoginPassword. The last two are only required if the PathToDBPlugin is set to ppvm3260 or ppvo3260.

```

<List Name="Databases">
  <List Name="Admin_Basic">
    <Var PluginID="rn-db-flatfile"/>   Name of plugin that will interact with the
                                     database.
    <Var Path="C:\Program Files
              \Real\RealProxy\adm_b_db"/> Location where the database files are stored
                                     or will be stored.
  </List>

```

Passwords

MonitorPassword is described in Chapter 10: Monitoring RealProxy Activity.

```

<Var MonitorPassword="letmein"/>   Password used by G2 Java Monitor in
                                     connecting to RealProxy.

```

Logging

Logging and reporting features are described in Chapter 11: Tracking RealProxy Activity. Variables which control the locations of the access and error log files are described in “Paths” on page 102 of this chapter.

Disable log file rolling by changing the LogRollFrequency and LogRollSize variables to 0.

```
<Var LogRollFrequency="4W"/>
```

Creates a new access log for each period specified. The period is indicated in the format `xD`, `xW`, or `xM`, where `x` is a number. See also `LogRollSize`. For example, `4D` will keep 4 days of information in the log file.

```
<Var LogRollSize="50"/>
```

Creates a new access log when the indicated file size is reached. See also `LogRollFrequency`. If you include both `LogRollFrequency` and `LogRollSize`, RealProxy uses the variable it finds first.



FILES INCLUDED WITH REALPROXY

This manual describes a pre-release product. As such, some features may not be fully implemented; any information here is subject to change.

This appendix lists the files used by RealProxy.

RealProxy Directories	
Directory	Description
adm_b_db	For authenticating RealSystem Administrator users, this directory stores names of authenticated users.
Bin	Utility programs are stored here. (More information is shown below.)
Content	Sample media presentations are stored in this directory; you can view them from RealSystem Administrator by clicking Samples .
Lib	Support libraries.
License	Contains license file(s). (More information is shown below.)
Logs	Reports of RealProxy will go in this directory. (More information is shown below.)
Plugins	Plugins, which perform RealProxy functions, are stored here.
RealAdministrator	HTML and other files required by RealSystem Administrator.

The table below shows the files stored in the main RealProxy directory.

Main Directory		
Windows	UNIX	Description
rmserver.cfg	rmserver.cfg	The configuration settings for RealProxy.
readme.txt	readme.txt	Last minute updates and changes.

Bin Directory

Windows	UNIX	Description
mkpnpass.exe	mkpnpass	Password tool (used for changing passwords of RealSystem Administrator users)
rmserver.exe	rmserver	RealProxy executable

Lib Directory

Windows	UNIX	Description
proxylib.lib	proxylib.lib	RealProxy Support Library
encn3260.dll	encn.so.6.0	Broadcasting Support Library

License Directory

Windows	UNIX	Description
proxy.key	proxy.key	License file.

Logs Directory

Windows	UNIX	Description
proxy.log	proxy.log	Proxy access log
log.txt	log.txt	Log text file
proxyerr.log	proxyerr.log	Error Log

Plugins Directory

Windows	UNIX	Description
admi3260.dll	adminfs.so.6.0	RealNetworks Admin File System
allo3260.dll	allow.so.6.0	RealNetworks Basic Allowance Plugin
audp3260.dll	audplin.so.6.0	RealNetworks Renderer Plugin
auth3260.dll	authmgr.so.6.0	RealNetworks Authentication Manager

(Table Page 1 of 3)

Plugins Directory

Windows	UNIX	Description
bas3260.dll	bascauth.so.6.0	RealNetworks Basic Authenticator
dbmg3260.dll	dbmgr.so.6.0	RealNetworks Database Manager
dbwr3260.dll	dbwrap.so.6.0	RealNetworks 5.0 Database Wrapper
farm3260.dll	farmplin.so.6.0	RealNetworks Farm Split Broadcast Plugin
ntau3260.dll	ntau.so.6.0	RealNetworks NTLM Authenticator
ntlo3260.dll	ntlo.so.6.0	RealNetworks NT Logger
perf3260.dll	perf.so.6.0	RealNetworks RMA Performance Monitor
plog3260.dll	plog.so.6.0	RealNetworks Proxy Logging Plugin
plus3260.dll	plusplin.so.6.0	RealNetworks PlusURL File Format Plugin
ppv3260.dll	ppvbasic.so.6.0	RealNetworks FlatFile Database Plugin
—	ppvmsql.so.6.0	RealNetworks mSQL Database Plugin
pxcb3260.dll	pxcbmp.so.6.0	RealNetworks RealPix BMP Codec Plugin
pxcg3260.dll	pxcgif.so.6.0	RealNetworks RealPix GIF Codec Plugin
pxcj3260.dll	pxcjpeg.so.6.0	RealNetworks RealPix JPEG Codec Plugin
pxcs3260.dll	—	RealNetworks RealPix STNG Codec Plugin
pxff3260.dll	pxff.so.6.0	RealNetworks RealPix Format Plugin
pxfx3260.dll	pxefx.so.6.0	RealNetworks RealPix External Effect Sam
pxgf3260.dll	pxgf.so.6.0	RealNetworks GIF File Format Plugin
pxjf3260.dll	pxjf.so.6.0	RealNetworks JPEG File Format Plugin
redi3260.dll	redipln.so.6.0	Real Networks RTSP Redirector Plugin
rmff3260.dll	rmffplin.so.6.0	RealNetworks RealMedia File Format Plugi
rn5a3260.dll	rn5auth.so.6.0	RealNetworks RN5 Authenticator
rprx3260.dll	rprxypln.so.6.0	RealNetworks RTSP Proxy Plugin
rtff3260.dll	rtffplin.so.6.0	RealNetworks RealText File Format Plugin
sdpp3260.dll	sdpplin.so.6.0	RealNetworks SDP Stream Description Plug
smlf3260.dll	smlffpln.so.6.0	RealNetworks SMIL File Format Plugin
smon3260.dll	smonplin.so.6.0	RealNetworks System Monitor
smpl3260.dll	smplfsys.so.6.0	RealNetworks Local File System
splt3260.dll	spltplin.so.6.0	RealNetworks Splitter Broadcast Plugin
swff3260.dll	swff.so.6.0	Shockwave Flash Format Plugin
vidp3260.dll	vidplin.so.6.0	RealNetworks Renderer Plugin

(Table Page 2 of 3)

Plugins Directory

Windows	UNIX	Description
vivf3260.dll	vivff.so.6.0	VivoActive File Format Plugin
exca3260.dll	excache.so.6.0	Example cache plugin
miiip3260.dll	miiiplin.so.6.0	Media Import plugin
sbmo3260.dll	sbmonpln.so.6.0	Splitter Monitor plugin

(Table Page 3 of 3)



INDEX

- A**
 - Access
 - in RealSystem Administrator, 67
 - variable, 111
 - Access Control
 - in RealSystem Administrator, 65, 66
 - list, 110, 111
 - Access Rule Name
 - in RealSystem Administrator, 65, 67
 - Address
 - in RealSystem Administrator, 86
 - Address Range
 - in RealSystem Administrator, 79
 - variable, 112
 - Address_01 variable, 109
 - Admin Port
 - in RealSystem Administrator, 43
 - variable, 102
 - adminfs mount point, 107, 108
 - Allow variable, 112
 - allowance plugin, 109
 - Authentication
 - variable, 108
 - Authentication Realm
 - variable, 113
 - Authentication variable, 108
 - Authorized_User_Group variable, 108
 - B**
 - Base Path
 - variable, 107
 - in RealAdministrator list, 108
 - BaseMountPoint
 - variable, 108
 - BitsaveEnable variable, 44, 104
 - BitsaveMountPoint variable, 104
 - BitsavePort variable, 104
 - C**
 - CacheEnable variable, 104
 - comment tag, 97
 - configuration file
 - components, 97
 - editing with text editor, 42
 - starting with, 33
 - D**
 - daisy-chain *See chaining*, 71
 - DBLoginPassword
 - variable, 114
 - DBName
 - variable, 114
 - Delivery Only, 58
 - in RealSystem Administrator, 80
 - variable, 112, 113
 - disabling features
 - log file rolling, 94
 - E**
 - error log, 94, 103
 - format, 95
 - Error Log Path
 - in RealSystem Administrator, 95
 - variable, 102, 103
 - error messages
 - "File not found", 51
 - Extensible Markup Language (XML) *See XML*
 - Extension_01 variable, 99, 106
 - F**
 - "File not found" error message, 51
 - file systems, 106
 - From
 - in RealSystem Administrator, 65, 68
 - variable, 111
 - FSMount list, 106, 107
-

- G** G2 Java Monitor, 102
GET, appearance in proxy log, 86
- H** HTTP Deliverable
list, 110
HTTP Port, 43, 51
in Access Control list, 68
Web server and RealProxy on same system, 51
- I** IP Address
in RealSystem Administrator, 79
IP Binding
list, 52, 109
- L** License Directory
in RealSystem Administrator, 36
variable, 36, 102, 103
list tag, 98
localadminfs mount point, 108
log files
media cache log, 26
Log Path, 94
variable, 54, 95, 99, 102, 103
Log Roll Frequency
variable, 114, 115
Log Roll Size
variable, 114, 115
Log Rolling, 94
Log Rolling Frequency, 93
Log Rolling Interval, 93
Log Rolling Time Period, 94
Logging Style
default value, 85
format, 90
options, 92
LoggingStyle variable, 104
logs
error log, 94
proxy log, 85
customizing, 91
format, 86
rolling, 93
Low Bit Rate Gateway, 57, 58
LowBitRateGateway variable, 104
- M** MaxBandwidth variable, 56
MaxGatewayBandwidth variable, 104
Maximum Gateway Bandwidth, 57
Maximum Proxy Bandwidth, 56, 57
Maximum Proxy Connections, 56
MaxProxyBandwidth variable, 104
MaxProxyConnections
variable, 56
MaxProxyConnections variable, 104
MIME Types
configuring on Web server, 34
in RealSystem Administrator, 34, 35
list, 98, 99, 105
Min Player Version
variable, 109, 110
Minimum Player Version, 59
Minimum RealPlayer Version, 109
MinimumPlayerProtocol, 59
MinPlayerProtocol
variable, 110
MinPlayerVersion variable, 109
Monitor Password
variable, 114
Monitor Port
variable, 102
multicasting
requiring use of, 58
- P** password
for RealSystem Administrator users, 40
Path variable, 114
Path_01 variable, 110
PathToDBPlugin
variable, 114
Pid Path
variable, 34, 54, 102, 103
PidPath variable, 103
Plugin Directory
variable, 102, 103, 106
Plugin ID
in Databases list, 114

- Plus Only
 - in RealSystem Administrator, 110
 - variable, 110
 - PNA Port
 - in RealSystem Administrator, 43
 - pn-admin, 107, 108
 - PNAPort variable, 103, 112
 - pn-local, 107, 108
 - pn-splitter, 107, 112
 - Port
 - variable
 - in pull splitting list, 111, 112
 - in Splitter_DoubleURL list, 112
 - Port_01 variable, 111
 - Ports
 - list, 111
 - Ports variable, 111
 - Process ID, 54
 - proxy log, 85, 93
 - customizing, 91
 - displaying player statistics, 59
 - format, 86, 90
 - purpose, 85
 - reading, 86
 - rolling, 93
 - Proxy Log Path
 - in RealSystem Administrator, 91, 93
 - proxy.log file, 102
 - proxyerr.log file, 102
- R**
- RealAdministrator list, 108
 - RealAdministrator_Files list, 108
 - Realm
 - variable
 - in AuthenticationRealms list, 113
 - in RealAdministrator_Files list, 108
 - RealPlayer Plus, 59
 - RealPlayer version, 59
 - RealProxy, 15
 - RealSystem Administrator, 39, 107
 - starting, 39
 - reports
 - error log, 94
 - proxy log, 85
 - customizing, 91
 - rolling, 93
 - Resend
 - in RealSystem Administrator, 80
 - variable, 112, 113
 - Restricted Ports, 68
 - rmserver.pid, 54
 - RTSP Port
 - in Access Control list, 68
 - in RealSystem Administrator, 43, 79
 - variable, 111, 113
 - in Multicast list, 112, 113
 - RTSPPort variable, 103
 - Rule Number
 - in RealSystem Administrator, 79
- S**
- server.cfg, 117
 - shaining, 71
 - ShortName variable
 - described, 107
 - in RealAdministrator list, 108
 - in RealAdministrator_Files list, 107, 108
 - in Splitter_DoubleURL list, 111, 112
 - SIGHUP command, 54
 - SMIL file
 - in proxy log, 89
 - multicasting and, 79, 112
 - split mount point, 112
 - Splitter_DoubleURL list, 112
 - starting RealProxy, 29
 - statistics, collecting in proxy log, 85
 - stopping RealProxy
 - UNIX, 34
 - Windows NT, 32
 - SureStream
 - multicasting, 76
- T**
- To
 - in RealSystem Administrator, 65, 67
 - variable, 111
 - Transport
 - in RealSystem Administrator, 111
 - variable, 111
 - TTL variable, 80, 112, 113

- U** unicasting, 76
 - UNIX
 - PID, 54
 - SIGHUP, 54
 - special features, 54
 - starting RealProxy, 33
 - stopping RealProxy, 34

- V** Valid Player Only, 59
 - variable, 109ValidPlayerOnly variable, 109
 - variable tag, 98

- W** Web server
 - and RealProxy, 43, 51
 - log format, 86
 - MIME types on, 34Windows NT
 - Performance Monitor, 54
 - running multiple instances of RealProxy, 32
 - special features, 53
 - stopping RealProxy, 32

- X** XML
 - configuration file, 41, 97
 - license files, 36XML declaration tag, 97