



Release Notes:

Helix Server 11.1.4

Helix Proxy 11.1.4

June 19, 2007

©RealNetworks, Inc. All rights reserved.

RealAudio and RealVideo are registered trademarks of RealNetworks, Inc. in the United States of America and other countries.

Basic Server, Basic Server Plus, Real Broadcast Network, RBN, RealDeveloper, RealProducer, RealMedia, RealNetworks, RealPix, RealPlayer, RealPlayer Plus, RealPublisher, RealServer, RealSystem, RealText, the Real Bubble and the RealNetworks Media Type logotypes are trademarks of RealNetworks, Inc. in the United States of America and other countries.

RealFlash is a trademark of Macromedia, Inc. and RealNetworks, Inc. in the United States of America and other countries.

Macromedia, the Macromedia logo, and Flash are registered trademarks of Macromedia, Inc. in the United States of America and other countries.

All other trade names, trademarks or registered trademarks are trade names, trademarks or registered trademarks of their respective companies.

RealNetworks

2601 Elliott Avenue
Seattle, Washington 98121
Phone: (206) 674.2700
Fax: (206) 674.2699
www.real.com

Table of Contents

1.	VERSION INFORMATION.....	2
2.	HARDWARE/SOFTWARE REQUIREMENTS.....	3
3.	WHAT'S NEW	3
4.	NEW SINCE 11.1.2 GA RELEASE	3
4.1	<i>Alternate Mount Point</i>	3
5.	DOCUMENTATION ADDITIONS	9
5.1	<i>Security Updates</i>	9
5.2	<i>Operating System Configuration Changes</i>	9
5.3	<i>Memory Allocation</i>	9
5.4	<i>File Descriptor Settings</i>	9
5.5	<i>RHEL4</i>	9
5.6	<i>Solaris 8 and Solaris 9</i>	10
5.7	<i>Solaris 8 and Solaris 9 Patch Recommendations</i>	10
5.8	<i>RHEL4 Kernel Configuration Recommendations</i>	10
5.9	<i>PSTACK Installation</i>	11
5.10	<i>Windows Registry Update</i>	11
5.11	<i>Cross Version Plug-in Compatibility</i>	11
5.12	<i>RTPLive Legacy Mode Support</i>	11
6.	FIXES SUPPLIED IN THIS RELEASE.....	12
6.1	<i>Listed Issues Fixed as part of v11.1.4</i>	12
7.	FIXES SUPPLIED IN PREVIOUS RELEASES	12
7.1	<i>Listed Issues Fixed as part of v11.1.3</i>	12
7.2	<i>Listed Issues Fixed as part of v11.1.2</i>	13
7.3	<i>Listed Issues Fixed as part of v11.1.1</i>	15
8.	KNOWN ISSUES.....	16
8.1	<i>Windows Media Player 11 With Helix Server</i>	16
8.2	<i>Alternate Mount Point</i>	18
8.3	<i>Broadcast Redundancy</i>	18
8.4	<i>Content Distribution</i>	18
8.5	<i>3GP Compliance</i>	18
8.6	<i>Admin System</i>	18
8.7	<i>Content Browser</i>	19
8.8	<i>Delayed Shutdown</i>	19
8.9	<i>General</i>	19
8.10	<i>Java Monitor</i>	19
8.11	<i>Live</i>	19
8.12	<i>Logging</i>	19
8.13	<i>Multicast</i>	19
8.14	<i>Proxy</i>	19
8.15	<i>Rate Adaptation</i>	19
8.16	<i>Reduced Startup Delay</i>	19
8.17	<i>SNMP</i>	20
8.18	<i>Windows Media Support (non-WMP 11 related)</i>	20
8.19	<i>Crash Avoidance Issues (CAs)</i>	20
9.	CHECKSUM	21

1. Version Information

Release: Helix Server 11.1.4 and Helix Proxy 11.1.4

Version: 11.1.4.2194

Build: servproxyall-050307-8752

Release Status: General Availability

Products: Helix Server, Helix Proxy

Files:

Windows Server and Proxy Software:

rs1114-ga-win32.zip

px1114-ga-win32.zip

Linux Server and Proxy Software:

rs1114-ga-linux-rhel4.tar.gz

px1114-ga-linux-rhel4.tar.gz

Solaris 8, 9 and Solaris 10 Software:

rs1114-ga-solaris-8.tar.gz

px1114-ga-solaris-8.tar.gz

Documentation:

HelixServerAdmin.pdf

HelixServerConfig.pdf

HelixProxyAdmin.pdf

HelixProxyConfig.pdf

Note: not all files are distributed with all distributions.

2. Hardware/Software Requirements

Supported Platforms:

Redhat Enterprise Linux 4

Solaris 8

Solaris 9

Solaris 10

Windows 2003 Server

Additional information about platform configuration recommendations for operating systems and hardware available at:

http://www.realnetworks.com/resources/contentdelivery/server/recommended_platforms.html

3. What's New

No new features have been included in this release.

4. New Since 11.1.2 GA Release

4.1 Alternate Mount Point

Feature Overview

The Alternate Mount Point feature will provide an alternate (or backup) path to the Real System Content directory as existing currently in the Server.

4.1.1 Use Cases

4.1.2 Performance enhancement

Performance of the server could be enhanced by allowing high demand content to reside locally, whilst lower demand content can reside on a file server, configured as the alternate (backup) content directory.

4.1.3 Content fail-over

In a scenario where the user configures both main and alternate Content directories as a network device, the alternate can be used as a back-up if the main directory is unavailable.

4.1.4 Content authoring

Having a backup Content Mount Point will allow the user to author content URLs without having to change the URL when content is moved to alternate location.

4.1.5 Theory of Operation

The ability to search an alternate (or backup directory) is achieved by allowing additional Mount Points to be created with the same name, but different base paths. Additionally, each of the file systems sharing the same Mount Point will be assigned a Mount Point search order. This search order will determine the sequence in which the server will look for content in the additionally configured file systems.

4.1.6 Interoperability

- **Network and Network Technologies Compatibility**

This feature may be configured to use a Local or Network file system. A choice of Networked File System will invoke the Asynchronous File System features, which are platform specific to each of the supported server platforms.

- **Component/Feature interoperability**

This section refers to areas where this feature will or not be interoperable. In addition, areas in which the feature is interoperable, but specific behavior needs to be called out will be noted as well.

- Content Browsing – Supported for both main and alternate Mount Points
- View Source – Supported for both main and alternate Mount Points, See *Section 3.16*
- Data types – All currently supported data types will be supported.
- Aliasing – Supported.
- Live Archiving – Not supported, see *Section 3.17*
- Cdist – Supported, see *Section 3.15*
- Logging – Standard and custom, will not be affected.
- SDPGen – This Mount Point will not be affected. SDPGen needs to follow the same login as for file system Mount Points when finding a file.
- ASXgen – This Mount Point will not be affected
- Ramgen – This Mount Point will not be affected
- Smilgen - This Mount Point will not be affected
- Live/On-demand switching, this feature will continue to work as previously designed

4.1.7 Functional Behavior

4.1.7.1 Alternate Mount Point(s)

With the implementation of this new feature, the server allows for one or more Mount Points to have the same MountPoint Attribute, but different base paths. The creation of Alternate Mount Points will be supported for all Mount Points listed under FSMount in the rmserver.cfg file. It is recommended that only Mount Points that contain a base path have an Alternate Mount Point configured for them.

4.1.7.1.1 Configuration

Alternate Mount Points will be configured via direct edit of the configuration file.

4.1.8 Mount Point Search Order

To determine the order in which the server will search through the alternate Mount Points, a configuration file variable `<Var MountPointSearchOrder="VAL"/>` will need to be added by the end-user to all additional Mount Points.

4.1.8.1.1 Configuration file editing

The default value for MountPointSearchOrder is 1. If MountPointSearchOrder is omitted, the default value is assumed.

Additional Mount Points will need to have the variable `<Var MountPointSearchOrder="n"/>` added to them in the configuration file see *Section 3.18*.

The end-user will be required to enter a search order (n = search order). The user does not have to number additional file systems sequentially (1,2,3, etc), but may assign higher values to allow for additional file systems to be added later (i.e. 1, 10, 100, etc.).

The end-user may also add this variable to a default Mount Point, and change its search order.

4.1.8.1.1.1 Duplicate Mount Point Search Order

If the end-user has one or more alternate file systems for the same Mount Point and two or more are configured with the same value for the variable *MountPointSearchOrder* the server will only execute a search on the first file system in the list, and ignore the others. This can occur if the end-user creates an alternate file system, and does not include a value (manual edit of the configuration file), the server will assign a default of 1. On server startup if a duplicate Mount Point with the same search order, the server will continue to startup, log an error message, and will ignore the duplicate

4.1.9 Process Flow

This section defines the flow of the new feature, as integrated with the legacy functionality.

4.1.9.1 Mount Point Hierarchy

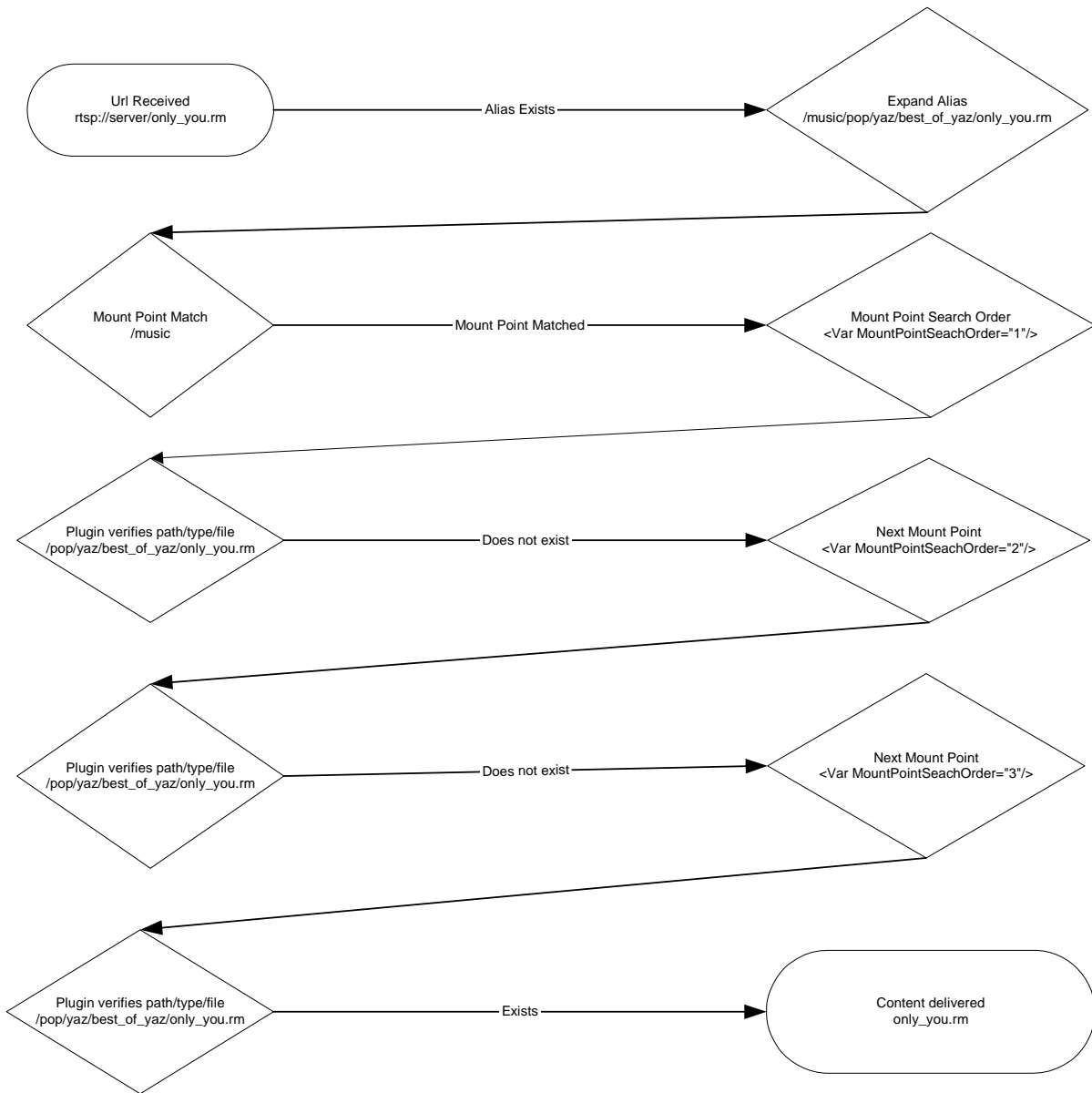
- When the Mount Points are loaded into the system on server startup, they are arranged into a tree, this is for search optimization. When a URL is received, the system will step down the tree and look for the most specific match, if that is not found, the next most specific Mount Point is tested, and this is repeated until “/”.

4.1.9.2 Content Search

- Once the mount point is matched, the path will be verified for the content
- If the content exists, the plug-in associated with the Mount Point will take over verification and delivery.
- If the content does not exist, the next Mount Point in order (if configured) will be searched
- If the content exists, the plug-in associated with the Mount Point will take over verification and delivery.
- If the content does not exist, the next Mount Point in order (if configured) will be searched. This continues for the number of Alternate Mount Points configured for that Mount Point.
- If the content exists, the plug-in associated with the Mount Point will take over verification and delivery.
- When the search through all Alternate Mount Points is exhausted, and the content is not found, the system will then attempt to find the content on the next step up the tree see *Section 3.12 Mount Point Hierarchy*, above.

4.1.10 Example

- The following example (flowchart on the next page) uses the configuration file variables shown in *Section 3.19*, below.
url: rtsp://server/onlyyou.rm



4.1.11 Content Caching

Content Caching (CDist) will be supported by this feature.

Currently, we have a configuration variable "UseContentDistribution" for each Mount Point which can be set by selecting "Cacheable by Content Subscribers" checkbox on Server Setup > Mount Points page.

- **Publisher**

When a server is acting as a Content Publisher, for each CDist rule it will receive a request for content from Content Caching Subscriber. The "UseContentDistribution" values of Mount Point on Publisher don't have any affect with respect to AMP. If the Mount Point on Publisher is having AMPs, the content will be searched on each AMP until content is found or the AMP list exhausts. If content is not found on any of the Publisher's AMPs, then it will fallback to Publisher's root mount point and check the subdirectory structure. If found, stream the content to Subscriber; otherwise, give an error.

- **Subscriber**

Currently, the "UseContentDistribution" flag is used by a Content Caching Subscriber to make a decision on whether or not to go to publisher if the content is not found locally. And this behavior would be changed as follows with respect to AMP. When a server is configured as a Content Caching Subscriber, and there are multiple Mount Points with the same name, they will be searched for content first. If content is not found on any of the Subscriber's Mount Points, then it should fallback to root and search subdirectory structure for the content. If still content is not found then we will check "UseContentDistribution" flag of the Mount Point having Highest Priority Search Order. If this flag is set, then we will be fetching the content from Publisher when content is not found in local cache. For example, if we have following mount point configuration:

```
MountPoint: "/music/"
BasePath: C:\Program Files\Real\Helix Server\Content\audio
MountPointSearchOrder=1
UseContentDistribution=1
```

```
MountPoint: "/music/"
BasePath: C:\Program Files\Real\Helix Server\Content\audiovideo
MountPointSearchOrder=2
UseContentDistribution=0
```

Here Highest Priority Search Order is "1". So, the first Mount Point's "UseContentDistribution" value will be used to decide whether or not go to Publisher to fetch the content. In above case, it will go to Publisher. "UseContentDistribution" value of other mount points will not matter.

4.1.12 View Source

When there are multiple Mount Points with the same name, *View Source* and *Hide Paths* will be applied as a group, to all Mount Points with the same name.

4.1.13 Live Archiving

When Live Archiving is enabled, the Server will attempt to save the broadcast to a file on the default path associated with the Mount Point selected. If that Mount Point is not available, the system will not attempt to write to the Alternate Mount Point associated for that Mount Point, and the attempt will fail.

4.1.14 Configuration File

The following configuration variable is added to the rmserver.cfg (default.cfg) file on system install.

```
<!-- Local File System; Media -->
  <List Name="RealSystem Content">
    <Var ShortName="pn-local"/>
    <Var MountPoint="/Music"/>
    <Var BasePath="/home/server11/Content"/>
    <Var MountPointSearchOrder="1"/>
    <Var UseContentDistribution="0"/>
  </List>
<!-- Local File System; Media -->
  <List Name="RealSystem Content Alternatel">
    <Var ShortName="pn-network"/>
    <Var MountPoint="/Music"/>
    <Var BasePath="/mnt/filesserver1/Content"/>
    <Var MountPointSearchOrder="2"/>
    <Var UseContentDistribution="0"/>
  </List>
<!-- Local File System; Media -->
  <List Name="RealSystem Content Alternate2">
    <Var ShortName="pn-network"/>
    <Var MountPoint="/Music"/>
    <Var BasePath="/mnt/filesserver2/Content"/>
    <Var MountPointSearchOrder="3"/>
    <Var UseContentDistribution="0"/>
  </List>
...
</List>
```

4.1.15 Variable Name

Name	Type	Range	Default	Description
MountPointSearchOrder	string	1 to 256 bytes	1	Must be a positive integer, greater than 0

- **Duplicate List Name**

The List Name of the Mount Point is the only means by which the server can differentiate between Mount Points. Upon startup, the server will parse the rmserver.cfg file if more than one Mount Point shares the same List Name, the server will continue to startup, log an error message, and will ignore the original, using the last one in the list.

4.1.16 Default Configuration Files

The following Mount Points located within the 'FSMount' section of the default "rmserver.cfg" and "default.cfg" files will be modified to include `<Var MountPointSearchOrder="1"/>`.

- Name="RealSystem Content"
- Name="RealSystem Secure Content"
- Name="CapExProfiles"

4.1.17 Notes

- Upon making manual changes to the configuration file, a server restart is required for these changes to take effect.
- Whenever the Mount Points are re-parsed the sever will validate that both the Mount Point Search Order and Mount Point Descriptions are unique for a group of Mount Points and log an error to the error log.
- When this feature is used to back up static content, the back up must mirror the original content. Different content with the same filename can cause errors, and should be avoided.

5. Documentation Additions

5.1 Security Updates

Please review the recent Security Update and Incident Report. The most recent posting can be reviewed by visiting <http://www.service.real.com/help/faq/security>

5.2 Operating System Configuration Changes

5.3 Memory Allocation

The Helix Server and Proxy consume memory on a per-client basis. The amount of memory consumed will vary, according to the nature of the presentation streamed to each. Memory is allocated by using the `-m #` command line flag at startup, where `#` is the amount of memory to allocate, in megabytes.

For example, starting the server with the command `Bin/rmsrver rmserver.cfg -m 512` would allocate 512 megabytes of memory to the server process.

Memory allocation limits of Helix Server and Proxy:

- Solaris: 4GB
- Linux/i386: ~2.8GB
- Windows: 2 GB (the OS is limited to 2 GB also)

About Memory-Mapped I/O

Since the server uses memory-mapped I/O that is not counted as part of this `-m` shared memory segment, additional memory should be reserved for mapped I/O. Not doing so may result in a significant performance penalty. The amount of memory needed for memory-mapped I/O varies with the number of clips being played and the bit rate of those clips. Generally reserving about 30% of the system memory for memory-mapped I/O is a good rule of thumb, but when setting this variable, one should monitor the system performance and watch for sudden changes in performance such as page faults.

5.4 File Descriptor Settings

RealNetworks recommends increasing the default file descriptor setting for your Solaris and Linux servers. File descriptors are heavily used by the server, for each file read, each open socket, etc. The recommended number of file descriptors to set is 65536 for each CPU. So on a dual processor machine you would set the value to 131072, and on a quad processor machine you would set it to 262144.

5.5 RHEL4

1. Examine system fd limit and ensure it meets or exceeds the recommended minimum:

```
$ cat /proc/sys/fs/file-max
```

If it doesn't, increase it by editing the file `/etc/sysctl.conf` (all file edits will require root access) and adding:

fs.file-max = number_of_desired_file_descriptors

2. Edit as root `/etc/security/limits.conf` and add the lines:

```
*      soft      nofile      number_of_desired_file_descriptors
*      hard      nofile      number_of_desired_file_descriptors
```

3. Edit `/etc/pam.d/login` and add the following line:

```
session required pam_limits.so
```

4. Edit `/etc/pam.d/sshd` and add the following line:

```
session required pam_limits.so
```

5.6 Solaris 8 and Solaris 9

1. examine system fd limit and ensure it exceeds the recommended minimum:

```
$ ulimit -Hn
```

If it doesn't, increase it by editing the file `/etc/system` (all file edits will require root access) and adding:

```
set rlim_fd_max=number_of_desired_file_descriptors
```

5.7 Solaris 8 and Solaris 9 Patch Recommendations

Testing at RealNetworks has shown some instability of Solaris 8 and 9 operating systems related to high levels of UDP usage. Sun has provided and recommends the following patch in order to address this situation.

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57728-1>

This patch is not necessary unless the operating systems experience kernel panic messages related to the UDP module.

5.8 RHEL4 Kernel Configuration Recommendations

Testing at RealNetworks has shown some instability on Red Hat Enterprise Linux 4. This instability is manifested as "kernel panics" related to "out of memory and no killable processes". This is partially because the 11.0.1 release of the Helix Server and Helix Proxy has a larger memory footprint than previous releases. Because of the 1 gigabyte (default) kernel virtual memory limitation on 32-bit systems with less than 4G RAM, we are recommending application of the 4G/4G patch set:

```
linux-2.6.0-4g4g.patch
linux-2.6.8-4g4g-backout.patch
linux-2.6.9-4g4g-hugemem-warning.patch
linux-2.6.9-net-b44-4g4g.patch
linux-2.6.9-4g4g-noncacheable.patch
```

Note: This should only be necessary in cases where there will likely be enough player load on the server that memory usage would exceed 1 gigabyte. If the server is started with a memory flag setting of less than 1 gigabyte (-m 1024), this patch solution will not be required.

To install the Linux kernel patches, do the following steps:

Download the kernel-2.6.9-5.0.5.EL.i686 kernel from <http://rhn.redhat.com>; you can find it by searching for "kernel" under "Packages"

Please refer to your Linux documentation regarding updating your Linux kernel

During the configuration step of your kernel update, make the following changes:

Under "Processor type and features" change the following:

Select "4 GB kernel-space and 4 GB user-space virtual memory support"

Select "Symmetric multi-processing support"

Deselect "Virtual Kernel Preemption"

Under "High Memory Support (65GB)", select "4GB"

Save the configuration, and compile and install the kernel

5.9 PSTACK Installation

There are known stability issues on Solaris and Linux systems running Helix Server and Helix Proxy which don't have pstack installed. Pstack is installed and configured on Solaris by default, however if you are running RHEL4, you will need to install and configure pstack for reliable Helix Server and Helix Proxy operation. You find the pstack package by searching for "pstack" under Packages at <http://rhn.redhat.com>. Please refer to your Linux documentation for instructions on installing or updating package files.

5.10 Windows Registry Update

When running the Helix Server and Helix Proxy on Windows, it will be necessary to increase the Default Send Buffer size in the operating system. To do this you will need to add a value to your Windows Registry.

Launch the Registry Editor from the Start→Run... option by typing the `regedt32.exe` command

Traverse through the tree to the following branch:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters

Add a new DWORD Value to the key called `DefaultSendWindow` and set that value to 32767 (decimal).

Restart your Windows 2003 Server machine.

This change will prevent poor QOS for clients connecting to live broadcasts over TCP.

5.11 Cross Version Plug-in Compatibility

Plug-ins are not binary-compatible between v9/v10 and v11 on Linux due to changes in compiler versions. The plugins need to be recompiled with the updated build environment to be useful.

5.12 RTPLive Legacy Mode Support

A new configuration variable has been added to fix an issue with live streams using RTP which caused sync, and other QOS issues. The variable is `<Var RTPLiveLegacyMode="1"/>`. When this flag is set to 1, RTP transport forces initial RTPtime and sequence to be 0. After a PAUSE, sequence will be the last sequence number of RTP packet plus 1 and RTPtime will reflect the elapsed time between the PAUSE and PLAY request (i.e. RTPtime is offset only at the initial PLAY request). This is in accordance with 3GPP specifications.

6. Fixes Supplied in this Release

6.1 Listed Issues Fixed as part of v11.1.4

- **157648 Proxy fails to timeout and terminate invalid connection attempts**
Under certain conditions Helix Proxy would not correctly terminate invalid connection attempts. Resulting in what is commonly referred to as lingering connections. Helix Proxy now correctly terminates invalid connection attempts.
- **183554 SMIL File with RealText and RealPix causes CA when using UDP**
Smil files that contained both RealText and RealPix elements would not stream correctly from Helix Server via UDP. Smil files that contain RealText and RealPix elements will now correctly stream from Helix Server via UDP.
- **184342 Helix Server could potentially run out of memory under heavy loads**
Under a specific set of load circumstances Helix Server would run out of memory and restart. Corrective measures have been included in Helix Server 11.1.4. It is now possible to support varying load scenarios with Helix Server.
- **188627 HTTP Delivery of MP3 content to Windows Media client fails**
Helix Server would fail to stream MP3 content to Windows Media clients when the content was located in an HTTP deliverable directory.
Helix Server will now correctly stream MP3 content stored in an HTTP deliverable directory.
- **191820 Stopping Helix Server with CTRL+C from a command prompt on Windows systems generates an error message.**
Helix Server 11.x will generate the following message when closed with CTRL+C on Windows systems: "KillSelect: -- send() failed - error(10093)". The appearance of this message is not indicative of an abnormal condition within the server. Using CTRL+C to terminate Helix Server from a command prompt on Windows systems will no longer generate that error message.

7. Fixes Supplied in Previous Releases

7.1 Listed Issues Fixed as part of v11.1.3

- **178520 Backchannel Multicast does not fail over**
In a situation where a client connects to Helix Server for Backchannel multicast, the server is not sending PLAY response. As a result the player is not failing over to next selected transport and times out. The above-described condition has been corrected. The server now sends the PLAY response at the appropriate time so that the failover is successful. This fix is applicable to backchannel multicast only.
- **181297 Watch Log Transmitting via TCP Breaks when Receiving Service Temporarily Down**
When Helix Server 11 is configured to regularly send a Watch log via TCP to a remote Log Processing service, it works fine. However, if the remote server becomes unavailable then even after it is restored, log transmitting is not restored and Helix Server must be restarted in order to resume log transmitting. The above-described condition has been corrected. Connection sockets between the server and the remote service are now properly maintained and transmitting of the logs resumes as expected.

- **184340 Invalid RTSP clients in registry cause incorrect real-time statistics reporting**
And when a player connects to a redundant live stream via a receiver, and if the encoder suddenly becomes unavailable, the player's registry entry is not cleared and the player count is not getting decremented on the receiver. Specifically, what happens is that during this particular time the receiver server is sending a REDIRECT request to the connected client and the client is tearing down the existing connection and sending a new OPTIONS request followed by the DESCRIBE. The receiver is not responding to this DESCRIBE request and it is this second client connection attempt that is causing hung registry entry. The initial connection however is getting cleaned up as expected.
The above-described condition has been corrected.
- **185748 Server exhibits Heartbeat Failure; fails to restart**
During a heartbeat failure, the server uses "pstack" (on a Linux Red Hat Enterprise 4 platform) on the controller Process ID to receive stack traces of all the pthreads. The pstack invokes gdb, attaches a binary to the controller Process ID and runs the gdb command to print the stack traces of all the threads. However, the particular gdb version would hang during the process, resulting in eventual 100% usage of the CPU. A manual kill of the gdb and the server processes is required in order to recover from this state. The above-described condition has been corrected. Solution includes avoidance of the condition under which the server process is trapped when gdb process is rendered unresponsive.
- **187510 Server stops sending post-seek packets of sparse data streams (timestamp delivery ones)**
After a seek operation, the event which start time is before the seek point, and end time is after the seek point, does not launch.
The above-described condition has been corrected. The events are launching as expected.
- **187816 Live streams drop at the edge servers**
Under certain conditions in encoder -> transmitter --(multicast)-> edge server setup, the live stream would suddenly become unavailable. A restart is necessary in order to correct the issue. However, this results in dropping all of the client connections.
The above-described behavior in the specific scenario as outlined has been corrected. The end result was caused by a Crash Avoidance instance. Addressing the condition leading to the CA has resulted in streams no longer being dropped at the edge servers.

7.2 Listed Issues Fixed as part of v11.1.2

- **121899 RBS encodes do not show source IP address.**
Unavailability of the source IP address prevents identification of (remote) host encoders. This becomes critical in managing significant number of concurrent encoders and in case of troubleshooting problems with the encoded streams.
The above-described condition has been corrected. The server now properly displays source IP address of RBS encoders.
- **132494 Misleading error messages logged for ANY LatencyMode (True Live) streams**
The error message: "Low latency streaming is not licensed in this server. Stream being reverted to normal latency mode" is seen in all latency configurations (low, moderate & normal) with and without servers which have the LowLatencyLive (True Live) feature enabled. Expected results:

Expected Results:
When the server has the license with LLL enabled, no errors are written to the rmerror log file when the encoder uses Normal, Moderate or Low settings

When the server has the license with LLL disabled, no errors are written to the rmerror log file when the encoder uses Normal settings

When the server has the license with LLL disabled, an error message is written to the rmerror log file when the encoder uses Moderate or Low settings

The above-described condition has been corrected. The log entries are being made as expected.

- **143204 Windows Media Client requests are logged incorrectly**
The server incorrectly reports a status code of 0 rather than the expected 200
The above-described condition has been corrected. The server properly logs the expected status code.
- **166738 Status 404 (file not found) errors not logged in access log from QuickTime player**
The server's rmerror log file reports "Error retrieving URL" message. The log should include proper status code, which in this case is 404.
The above-described condition has been corrected. The server properly logs the expected status code.
- **170865 Unexpected 408 errors - Connection refused, too many connections**
Under certain load conditions the proxy would enter an erroneous condition causing it to report client connections count exceeding that of the license file.
The above-described condition has been corrected. The proxy no longer enters a state causing it to report an invalid client count.
- **175954 Helix Server Configuration Guide error**
The example of a variable setting on page 156 is incorrect:

Shows:	<Var Disable3GPPKeyframeDetection="1">
Should be:	<Var Disable3GPPKeyframeDetection="1"/>

The Server Configuration Guide has been updated with the appropriate correction.

- **175190 Incorrect SNMP MIB values returned**
The incorrect values are returned with the following variables:
hsUDPTransports (.1.1.5 & .1.1.6)
hsPercentCPUUsage
clientRequests
clientRequestsSuccessCount
clientsLeaving.

The above-described condition has been corrected.

- **176500 Server does not release connections, triggers Crash Avoidance and restarts**
A race condition with the Administration UI Server Monitor was causing the server not to release connections.
This issue has been fixed.
- **177358 Cannot redirect output of the master command to a log file**
Commands such as `./Bin/master master.cfg > master.log` would not capture output as expected. The resulted files contained no data.
This issue has been fixed. The output redirection now functions as expected.

- **177553 Server statistics for Free Pages Outstanding & Overhead becomes inaccurate under certain conditions**
Negative values for Memory Allocation Overhead appear in the rss logs. In the case of allocation of big pages of size more than 1 MB, free page outstanding was not getting decremented and hence the observed behavior.
The fix corrects the above mentioned counter and all related calculations are now correct.
- **177728 Server leaves RTSP session open, and unresponsive after issuing Server Alert in response to bad DESCRIBE request**
Under certain conditions the TCP connection is still active, but the server is non-responsive to further RTSP requests.
The above-described condition has been corrected.
- **180912 RMERROR.LOG shows UNKNOWN instead of milliseconds for each entry**
The date timestamp is missing the milliseconds and puts UNKNOWN instead. This should be filled in with the number of milliseconds or nothing if not supported.
This issue has been fixed. The server now logs expected values.
- **182056 HTTP Content-length of ZERO causes client connection failure**
Server is treating Content-Length Zero in HTTP header as an invalid value. The result is a client connection failure and a Crash Avoidance on the server.
The above-described condition has been corrected.

7.3 Listed Issues Fixed as part of v11.1.1

- 154092 Windows Media client connections show multiple "New players" in server's log file
This is by design. Windows Media Players establish and then tear down two RTST connections to the same server on port 554 before attempting MMS connection on port 1755.
- 155842 Startup.log doesn't contain date/time when server was started
Issue has been resolved. The logs now contain startup time and date.
- 159274 Content accessed from Helix or Windows Server using MMS protocol fails to stream via Helix Proxy
Problem has been caused by truncation of MMS response from the Player on the proxy. Issue is fixed.
- 165119 Windows Media content streams audio only when accessed via HTTP
Problem was caused by the server reading stream number in decimal rather than in hex. This has been fixed.
- 166361 Proxy keeps connection open to Helix Server for Windows Media content
Playing windows media content resulted in a leak, which then caused the connections to remain in an open state. This has been resolved.
- 166673 Unable to play from Windows Media server WM content via Helix Proxy using RTSP
Problem was related to proxy's failure to parse control lines inside an SDP file. This has been fixed.
- 166694 MMS server response forwarded to client through proxy is truncated – client disconnects
This has been corrected. Truncation no longer occurs and therefore the clients do not get disconnected.
- 167421 Missing date and time from the startup.log
Problem with missing time and date stamp have been corrected.
- 167761 Authentication failure when using NTLM features of the Server
Problem was due to a broken functionality. Issue has been resolved.

- 170686 Windows Media video playback from Helix Server 11.1 fails on certain SunOS 5.8 machines
Problem caused by outdated patch level. To correct the problem ensure that the latest patches are applied to the Solaris 5.8 operating system.

8. Known Issues

Below is a summary of known issues in functional and stability areas of the Helix Server 11.1.4 and Helix Proxy 11.1.4.

8.1 Windows Media Player 11 With Helix Server

Windows Media Player 11 no longer requests media using the MMS protocol. When it encounters an MMS URL for on-demand or live content on Helix Server, the player attempts to access the clip in the following order:

1. The player first requests the stream over HTTP, issuing an HTTP request in one of two possible ways:
 - If the MMS URL explicitly contains an MMS port number, the player directs the HTTP request toward that port on Helix Server. In this case, the request fails because Helix Server does not listen for HTTP requests on its MMS port. The standard port used for MMS on Helix Server is 1755.
 - If the MMS URL does not provide a port number, the player directs the HTTP request toward Helix Server port 80. If Helix Server uses port 80 for HTTP, the request succeeds and the server delivers the stream as cloaked MMS. If the server does not use port 80 for HTTP, however, the request fails.
2. If the HTTP request fails, the player sends an RTSP request to Helix Server port 554, the standard RTSP port. This request always fails regardless of the RTSP port that Helix Server uses. This is because Helix Server does not support the streaming of Windows Media content over RTSP.

Supporting Windows Media Player 11

You can update your streaming media system to provide Windows Media Player 11 with an alternate HTTP URL whenever it requests an MMS URL. The HTTP URL will contain the appropriate Helix Server port number for the player's HTTP request. Once the player makes the HTTP connection, Helix Server delivers the stream as HTTP-cloaked MMS.

Note that the HTTP connection used to deliver cloaked streams to Windows Media Player 11 is **not** managed the same as HTTP requests from browsers. You therefore do **not** need to add the mount points under which the Windows Media content resides to the HTTPDeliverable list in the Helix Server configuration file. The content is delivered only to the media player, and is protected against browser caching and user download.

Updating your system requires the following actions:

- Modify an existing Helix Server configuration value for the ASXgen utility. This causes Helix Server to provide an alternate HTTP URL to any Windows Media Player that requests an MMS URL.
- Update any .asx files linked to Web pages to include an alternate HTTP URL.

Modifying ASXgen

ASXgen is a Helix Server utility for launching Windows Media Player from a Web page link. Helix Server is configured with a mount point named /asxgen/, which you add to a Web page link for Windows Media content. For example:

```
<a href="http://helixserver.example.com:8080/asxgen/video.wmv">Play Windows Media</a>
```

When Helix Server receives an HTTP request that contains the /asxgen/ mount point, it sends a MIME stream that causes the browser to launch Windows Media Player. This MIME stream instructs the player to contact Helix Server on its MMS port, and explicitly provides the MMS port number (typically 1755). To support Windows Media Player 11 for on-demand and live streams, you configure ASXgen to provide an alternate HTTP URL along with each MMS request. This alternate URL includes the actual HTTP port number used by Helix Server. After the initial MMS URL returned by ASXgen fails, Windows Media Player 11 requests the stream using the alternate HTTP URL.

- o To configure ASXgen to Support Windows Media Player 11:
 1. Using any text editor, open the Helix Server configuration file (rmserver.cfg). This file resides in the Helix Server main installation directory.

2. Find the ASXgen configuration list and variables:

```
<List Name="ASX File Generator">  
<Var ShortName="pn-asxgen"/>  
<Var MountPoint="/asxgen"/>  
<Var HaveAltHTTPURL="0"/>  
</List>
```

3. Enable the HaveAltHTTPURL variable by setting its value to 1:
<Var HaveAltHTTPURL="1"/>

Note: Beginning with Helix Server maintenance release 11.1.2, the HaveAltHTTPURL variable is enabled by default.

4. Save and close the configuration file. A Helix Server restart or a "kill -HUP `cat ./Logs/rmserver.pid`" command is required unless the modification is done through the Admin page (see below).

- o To make the change from "HaveAltHTTPURL=0" to "HaveAltHTTPURL=1" without any restart can be done through the Helix Administrator page. The setting can be found in "Server Setup/Ports" as "Enable HTTP Fail Over URL for ASXGen" – where it can be changed from "No" to "Yes." Finally clicking on "Apply" enables the new setting.

Updating ASX Files

If you direct Windows Media Player to MMS streams using ASX files, you can update the files to include an alternate HTTP URL. Simply add a second REF entry to the same content, using an HTTP URL that indicates the Helix Server HTTP port number. For example:

```
<ASX Version = "3.0">  
<ENTRY>  
<Ref href = "mms://helixserver.example.com:1755/wmvideo.wmv"/>  
<Ref href = "http://helixserver.example.com:8080/wmvideo.wmv"/>  
</ENTRY>  
</ASX>
```

Note: Updating ASX files is not required only if the MMS URL in each file does **not** contain an explicit MMS port number and your Helix Server uses port 80 for HTTP connections.

Using a Proxy

Windows Media Player 11 does not provide an option to use an MMS proxy. Instead, its player preferences contain options to use an HTTP proxy and an RTSP proxy:

- For the HTTP proxy, you can select any HTTP proxy available to you. You cannot use Helix Proxy, however, because Helix Proxy does not proxy any media using HTTP.
- For the RTSP proxy option, you can specify Helix Proxy. Note the following, however:
 - Because Helix Server does not support Windows Media over RTSP, Helix Proxy cannot proxy any Windows Media content residing on Helix Server for Windows Media Player 11. Streams originating from Helix Server can be delivered only by an HTTP proxy as HTTP-cloaked MMS.
 - Helix Proxy can proxy on-demand and live, RTSP-based Windows Media streams originating from a Windows Media Server. However, all streams are delivered in pass-through mode only. Helix Proxy does not cache on-demand clips or split live streams.

8.2 Alternate Mount Point

Alternate Mount with same (duplicate) List Name does not log an error in Error.log

Alternate Mount Point feature can be configured via the configuration file only. Currently there's no GUI interface for this function.

8.3 Broadcast Redundancy

When sending a live feed to the Helix Server, if the filename has multiple dots in it then broadcast redundancy generates multiple alternative files available. This means that one live feed being sent in is duplicated hundreds of times (depending on the number of dots in the original filename).

8.4 Content Distribution

If no default "/" Mount exists, Cdist still looks in "/" for files

If no "/" mount point exists in the rmserver.cfg and Cdist is configured, the Content subscriber sends the wrong URL to the Content publisher when looking for content and therefore returns a "404 - File Not Found."

Explanation: The default mount point must always exist in order for the feature to work as designed.

8.5 3GP Compliance

Bandwidth of RTCP RR/SR exceeded XXbps limit

Under certain conditions the RTCP sender and receiver reports indicate that the bandwidth limit setting of 5000bps has been significantly exceeded.

Explanation: This would degrade the quality of the stream if there was insufficient capacity in the channel to handle the extra 2 kbps but otherwise would not have any negative impact. The most likely result would be for the rate manager to lower the bit rate if the stream was multi-rate and the player supported rate adaptation. Otherwise, end-users may experience rebuffering. This issue is to be addressed in the next major release.

8.6 Admin System

Clicking on some pages of the Helix Admin System will cause extraneous 404 errors in the server's logs

Changing the Transmitter Source name in the Admin System requires a server restart for the change to take effect, however the Admin System will not notify the user that this is required

The Quicktime sample clip will not play if the link is clicked in the Admin System

8.7 Content Browser

Content browsing feature doesn't work through admin UI in version 11.1.2.
Restricting Content Browsing to specific extensions does not function
Directories in the Content Browser windows are improperly displayed as files

8.8 Delayed Shutdown

Disabling "Allow New Client Connections" will not keep new clients from connecting when a Delayed Shutdown of the server is in progress

8.9 General

System time changes of more than a few seconds while the server is running, and particularly while the server is under load can cause severe memory leaks and potentially restarts. This sort of system time change may be triggered by NTP services, daylight savings changes, or simply by manual date/time changes. We recommend disabling these sorts of services on systems running Helix Server and Helix Proxy, and that time adjustments be made during server down times, or times of low load.

8.10 Java Monitor

Bandwidth Usage is not recorded for 3GP Live streams being played

8.11 Live

Live RTP: Server sends duplicate RTP packets causing reported packet loss of 16777215 (0xfffff)
The Standby message does not work with RTP based broadcasts

8.12 Logging

Superfluous error message: "couldn't lookup session for channel <0x1>" is getting written to the error log

8.13 Multicast

When configuring Scalable Multicast, "VirtualPath" values cannot be numeric only; "2" won't work, but "2a" will

8.14 Proxy

Proxy does not support Caching or Splitting for scenarios where Proxy Routing is used

8.15 Rate Adaptation

When MDP is enabled, and you are using TCP Limirate, the server has a tendency to over send data. The higher the bitrate, the more it will over send. You can compensate for this by increasing the MaxBurst size variable on the server when streaming at higher bitrates until the margin of error is within acceptable limits

8.16 Reduced Startup Delay

Setting the variable "CPUThresholdToDisableRSD" to 100 will roll the value back to the default of 65; 99 is the highest value the system will recognize

8.17 SNMP

The SNMP v1 user name must be set to "public" for traps to function properly

The Trap Interval value has no effect

The Master Agent doesn't return an error message if it is started with an invalid configuration

The Master Agent doesn't return an error message if authentication information is invalid

The Master Agent prints an error when starting without a community string being configured; this error message should be ignored

Setting the trap values for CPU or MaxConnections to zero doesn't disable these traps; you must set them to a value which is high enough that it won't be reached

ServerStart trap is never sent

8.18 Windows Media Support (non-WMP 11 related)

Windows Media 9 live streams won't work if hosted from SLTA

Windows Media Player will sometime give an error when attempting to connect to the server using ASXGen

Windows Media Push Splitting fails if setup to use TCP on an IPv6 network

Windows Media streams fail to connect to the Helix Proxy via an IPv6 network

Windows Media clips will not play properly if clicked on in the Content Browsing window

There are various logging errors, which occur when playing MMS through the Helix Proxy

8.19 Crash Avoidance Issues (CAs)

When using a Parent and Child Proxy routing setup, the Parent proxy CAs on RTSP request.

Adding a Scalable Multicast channel through the Admin System will cause a CA

Requesting a MMS stream through the proxy will cause the proxy to CA

9. Checksum

File Name	MD5 Checksum
px1114-ga-linux-rhel4.tar.gz	8b27291177427c98abf3845e1db83f08
px1114-ga-solaris-8.tar.gz	84ffbbba4e32d759c3e3a9d8abc1a0b30
px1114-ga-win32.zip	d8c1afb61d0093114a1dc04ae8e3944e
rs1114-ga-linux-rhel4.tar.gz	d742c2bfc2d1ba0b5e4bbf385e028f9a
rs1114-ga-solaris-8.tar.gz	31b05ed47d7317692ed693b298018ee2
rs1114-ga-win32.zip	011e91498426ec79dbf460787fbde7ab