Release Notes for Cisco Internet Streamer CDS 2.3

These release notes cover Cisco Internet Streamer CDS Release 2.3.1-b7.

Revised: October 3, 2008, OL-17355-01

Contents

The following information is included in these release notes:

New Features

Release 2.3 of the Cisco Internet Streamer CDS introduces the following new features:

- Flash Media Streaming—Interactive applications
- Service Router—IP-based redirection

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

For more information, see the "Product Overview" chapter in the *Cisco Internet Streamer CDS Software Configuration Guide*.

Flash Media Streaming

In Cisco Internet Streamer CDS Release 2.3, Flash Media Streaming supports pass-through (proxy) support for interactive applications (non-VOD or non-live). The interactive applications are hosted on a Flash Media Interactive Server that is external to the CDS.

Direct routing from the Service Engine, acting as the Flash Media Streaming edge server proxy, to the Content Origin server (the Flash Media Interactive Server) is supported. Using the delivery service framework, the Content Origin server is abstracted from the client request by using the Service Router Domain Name (SRDN), which resolves to the Service Engine that accepts the user connection and forwards the request to the Content Origin server. In Release 2.3, Flash Media Streaming includes the edge server (proxy) mode, and by default, all non-live and non-VOD applications are proxied by using the edge server. Flash Media Streaming selectively picks connections for processing in edge server mode and aggregates connections to the Content Origin servers.

Service Router

When IP-based redirection is enabled, the Service Router uses the IP address of the Service Engine in the URL instead of the hostname. The redirected URL is http://<se ip addr>/ipfwd/<rfqdn>/<path>. The IP-based redirection method avoids the extra DNS lookup that was required in the RFQDN redirection.

Enhancements

Table 1 describes the enhancements to Internet Streamer CDS 2.3.

Table 1 New Features in Internet Streamer CDS 2.3

New Feature	Description
Flash Media Streaming supports port 80	Supports RTMPT and RTMPTE on port 80.
Flash Media Streaming Service Monitor	Added information on memory usage of Flash Media Streaming processes to the service monitoring information.
Flash Media Streaming supports referer header field in service rules	Supports allowing or blocking client requests based on where the request is being played from.
Flash Media Streaming supports FMRMS	Supports Adobe's Flash Media Rights Management Server (FMRMS) for VOD content; it is not supported for live streaming. FMRMS is also available for proxied content, if Adobe supports the content type. For more information about the Adobe Flash Media Rights Management Server, see www.adobe.com.
Device group assignment in delivery service	Supports assigning device groups to a delivery service.
Delivery service-based QoS	Per-delivery service support for QoS for Windows Media Streaming and Web protocol engines.

Table 1 New Features in Internet Streamer CDS 2.3 (continued)

New Feature	Description
Delivery service WMT/HTTP switch policy	Per-delivery service support for selecting progressive download or streaming of certain media file types.
Server offload before upgrade	Ability to offload a Service Engine in order to perform maintenance or software upgrades.
Movie Streamer statistics	Movie Streamer statistics have been enhanced for the show command.

System Requirements

The CDS Internet Streaming runs on the CDE100 and CDE200 hardware models. The CDE100 may run as the CDSM, while the CDE200 may run as the Service Router or the Service Engine. See the *Cisco Content Delivery Engine CDE100/200/300/400 Hardware Installation Guide* for set up and installation procedures.

Limitations and Restrictions

This release contains the following limitations and restrictions:

- There is no network address translation (NAT) device separating the CDEs from one another.
- Do not run the CDE with the cover off. This disrupts the fan air flow and causes overheating.

Note The CDS does not support network address translation (NAT) configuration, where one or more CDEs are behind the NAT device or firewall. The workaround for this, if your CDS network is behind a firewall, is to configure each internal and external IP address pair with the same IP address.

The CDS does support clients that are behind a NAT device or firewall that have shared external IP addresses. In other words, there could be a firewall between the CDS network and the client device. However, the NAT device or firewall must support RTP/RTSP.

Important Notes

To maximize the content delivery performance of a CDE200, we recommend you do the following:

1. Use port channel for all client-facing traffic.

   Configure interfaces number 3, 4, 5, and 6 (those on the quad-port Gigabit Ethernet Card) into a single port-bonding interface. Use this bonding channel, which provides instantaneous failover between ports, for all client-facing traffic. Use interfaces number 1 and 2 (the two on-board Ethernet ports) for intra-CDS traffic, such as management traffic, and configure these two interfaces either as standby or port-channel mode. Refer to the *Cisco Internet Streamer CDS 2.0-2.1 Software Configuration Guide* for detailed instruction.

2. Use the client IP address as the load balancing algorithm.

Assuming ether-channel (also known as port-channel) is used between the upstream router/switch and the SE for streaming real-time data, the ether-channel load balance algorithms on the upstream switch/router and the SE should be configured as "Src-ip" and "Destination IP" respectively. Using this configuration ensures session stickiness and general balanced load distribution based on clients' IP addresses. Also, distribute your client IP address space across multiple subnets so that the load balancing algorithm is effective in spreading the traffic among multiple ports.

3. Tune the TCP parameter.

   On the CDE200, execute the following commands once (This tunes the internal TCP configuration for better content delivery performance over HTTP.):

   ```
   Config# tcp server-satellite
   Config# tcp client-satellite
   Config# write memory
   ```

4. For high-volume traffic, separate HTTP and WMT.

   The CDE200 performance has been optimized for HTTP and WMT bulk traffic, individually. While it is entirely workable to have mixed HTTP and WMT traffic flowing through a single CDE200 simultaneously, the aggregate performance may not be as optimal as the case where the two traffic types are separate, especially when the traffic volume is high. So, if you have enough client WMT traffic to saturate a full CDE200 capacity, we recommend that you provision a dedicated CDE200 to handle WMT; and likewise for HTTP. In such cases, we do *not* recommended that you mix the two traffic types on all CDE servers which could result in suboptimal aggregate performance and require more CDE200 servers than usual.

5. For mixed traffic, turn on the HTTP bitrate pacing feature.

   If your deployment must have Streamers handle HTTP and WMT traffic simultaneously, it is best that you configure the Streamer to limit each of its HTTP sessions below a certain bitrate (for example, 1Mbps, 5Mbps, or the typical speed of your client population). This prevents HTTP sessions from running at higher throughput than necessary, and disrupting the concurrent WMT streaming sessions on that Streamer. To turn on this pacing feature, use the HTTP bitrate field in the CDSM Delivery Service GUI page.

   Please be aware of the side effects of using the following commands for Movie Streamer:

   ```
   Config# movie-streamer advanced client idle-timeout <30-1800>
   Config# movie-streamer advanced client rtp-timeout <30-1800>
   ```

   These commands are only intended for performance testing when using certain testing tools that do not have full support of the RTCP receiver report. Setting these timeouts to high values causes inefficient tear down of client connections when the streaming sessions have ended.

   For typical deployments, it is preferable to leave these parameters set to their defaults.

6. For ASX requests, when the Service Router redirects the request to an alternate domain or to the origin server, the Service Router does not strip the .asx extension, this is because the .asx extension is part of the original request. If an alternate domain or origin server does not have the requested file, the request fails. To ensure requests for asx files do not fail, make sure the .asx files are stored on the alternate domain and origin server.

Open Caveats

This release contains the following open caveats:

Flash Media Streaming

- CSCso78725

  Symptom:

  A low-rate memory leak exists for Flash Media Streaming live streaming when clients connect and disconnect. It is currently under investigation by both Adobe and Cisco. The memory leak eventually results in a process restart.

  Workaround:

  Flash Media Streaming live streaming can be recovered using next-click failover or simply retry from the client player.

- CSCsr29544

  Symptom:

  Due to the memory leak issue, which is under investigation by Adobe and Cisco, the FMS core process will fail over to a new FMS core process after 24 hours. All new request will go to a new FMS core process. The old FMS core process will continue to serve the existing clients until all clients have disconnected, at which point the process will end releasing all memory.

  This FMS core process failover feature disables an SE being used as a Flash Media Server Content Origin server.

  Workaround:

  Republish the stream from the Flash Media Encoder.

- CSCsq35801

  Symptom:

  The statistics displaying current live and VOD connections may fluctuate during stress testing. It does not have any adverse effect on the stream quality or transaction logs. These are just informational statistics and their inaccuracies have no operational or performance impact.

  Workaround:

  Retry the show command after a short interval of time.

- CSCsr66224

  Symptom:

  The Flash Media Streaming statistics that display the current live connections do not get updated after the statistics have been cleared. More detailed information and statistics on active live streams are not affected by this issue. The current live connections counters show a value of zero until the Flash Media Server statistics fluctuation subsides.

  Adobe TAM reference number for this issue is Cisco 180197164

  Workaround:

  Retry displaying the Flash Media Streaming statistics after a short interval of time.

- CSCsr78404

  Symptom:

Flash Media Streaming edge process memory in the Flash Media Server grows unbounded when a significant load of RTMPT video traffic is used. This occurs because the Flash Media Server requires additional internal buffers for HTTP tunneling.

Adobe TAM reference number for this issue is Cisco Adobe 180369081

Workaround:

In order to prevent an ungraceful disruption of RTMPT streams, new RTMPT requests are rejected after the process memory reaches the 2.5 GB limit. In addition, if the memory does not decrease after an hour, the Flash Media Streaming edge process is restarted. This may result in disruption of any RTMPT session that is longer than an hour of duration. No user intervention is required, and appropriate CDSM alarms and logs are updated to reflect this activity.

- CSCsu32956

  Symptom:

  For Flash Media Streaming live streams, the origin server or upstream connection is not released when the client stops playback but does not issue a disconnect. This is the case when playback has completed but the .swf file did not issue a disconnect. The Flash Media Server disconnects clients when they have been idle for more than three minutes.

  Workaround:

  When the client closes the browser, the Flash Media player is unloaded. Another workaround is to include timeout thresholds in the .swf file to disconnect connection after playback is complete.

Web Engine

- CSCsu51910

  Symptom:

  Files get partially cached on the Service Engine and are not cache filled. However, the client is served by using progressive download.

  Condition:

  Request for a .wmv file is sent from a browser and Windows Media Streaming is disabled on the Service Engine.

  Workaround:

  a. Windows Media Streaming is enabled on the Service Engine and the request is sent from a browser or player.
  b. Windows Media Streaming is disabled on the Service Engine, and the request is sent through an embedded player.
  c. The file is downloaded using other players like VLC and so on, which results in complete caching of the file.

Movie Streamer

- CSCsr96419

  Symptom:

  When a live program name is changed for an existing program, the CDS may fail to modify the program parameters and a client may fail to request this program using the correct Unicast Reference URL. Clients attempting to open a unicast SDP URL for a live program that has had a name change, receive the RTSP 415 error code, "Unsupported Media Type."

  Workaround:

  Using the CDSM, go to **Services > Live Video > Live Programs** and edit the live program that has the program name change. From the left-panel menu, choose **Live Streaming**, and when the Live Streaming page is displayed, click **Submit**. This will updated the Unicast Reference URL with the new program name.

- CSCsq72735

  Symptom:

  Adding or deleting Service Engines to or from a live delivery service while a live program is ongoing, causes system resource leaks and may cause system instability over time.

  Workaround:

  Stop the live program before changing the program itself or changing any Service Engine assignments for the live delivery service.

Windows Media Streaming

- CSCsq46063

  Symptom:

  Multiple stale outgoing sessions are displayed for the **show statistics wmt streamstat** command.

  Conditions:

  When an SSPL broadcast publishing point is stopped and a managed live Windows Media Streaming program is scheduled.

  Workaround:

  Stale sessions are removed periodically and do not impact streaming. Alternatively, you can enable the SSPL broadcast publishing point source.

CDSM

- CSCso75186

  Symptom:

  In some rare instances, when the system is in a stress test, a java core file is generated. The CDSM GUI restarts in less than 30 seconds and alarm is generated stating a core file is generated.

  Workaround:

  None. The issue does not impact the functionality of the CDSM GUI.

Caveats Not Caused by CDS Software

This release contains the following open caveats that are not cause by the CDS software:

Windows Media Streaming

- CSCsr58043

  Symptom:

  When using a file as the type of source for a live publishing point in Windows Media Server 2008 Standard, after starting multiple streaming requests from that publishing point, when the first stream reaches the end of the source file the second and subsequent streams fail with an error message at the same time. If Windows Media Server 2008 Standard is used as the origin server for a delivery service in CDS-IS, the second and subsequent streams will not fail, but will repeatedly loop the last segment of the stream.

  Workaround:

  Publishing points can be created using other source types (for example, playlists) rather than a file as the source type with the Windows Media Server 2008 Standard. The symptom described above is not seen with windows Media Server 2008 Enterprise used as the origin server.

Resolved Caveats

The following caveats have been resolved since Cisco Internet Streamer CDS Release 2.2 Not all the resolved issues are mentioned here. The following list highlights associated with customer deployment scenarios.

Movie Streamer

- CSCsq11663

  Movie Streamer VOD performance is currently not optimized for all unique file cases. Depending on the client request pattern for the VOD files, fragmentation in the storage may form that affects the throughput. Additionally, disk I/O prefetch support is not present for the Movie Streamer VOD case, which would limit the throughput when all streams are unique and are served from disk.

  Workaround:

  None.

Note All unique file cases refer to an access pattern from the client players when all the requests are towards different content items (for example, one user requests a movie, while another user requests a different movie and yet another user requests a different movie, and so on.)

CDSM

- CSCsq84208

  Symptom:

When a user clicks the View Detail of Bytes Served chart at the home page and then clicks Update in the detailed system-wide Bytes Served chart, the system throws a java exception.

Conditions:

This exception only happens in the system-wide Bytes Served chart.

Workaround:

Try to avoid submitting the system-wide Bytes Served chart. Using an SE-specific chart does not cause an exception.

- CSCsq84279

  Symptom:

  When a non-administrator user tries to create a delivery service, the system throws a java null pointer exception.

  Conditions:

  If a delivery service is created and granted access to a non-administrator user and then deleted, the exception occurs.

  Workaround:

  Remove the entity from the domain before deleting the delivery service.

Upgrading to Release 2.3

In order to upgrade to Release 2.3 from Release 2.2, the following changes between Release 2.2 and Release 2.3 need to be considered:

- If IP-based redirection is configured on the Service Router, the Coverage Zone file needs to be modified to reflect this change.
- In Release 2.3, SSH is enabled by default and Telnet is disabled by default. If a device is upgraded from Release 2.2 or an earlier release to Release 2.3, Telnet will not be enabled. If required, Telnet can be re-enabled by using SSH or console access.

Note The supported upgrade path is from Release 2.2 to Release 2.3 only. If you are running a release prior to Release 2.2, you must upgrade to Release 2.2 before upgrading to Release 2.3.

Documentation Updates

The following documents have been updated for this release:

- *Cisco Internet Streamer CDS 2.0-2.3 Software Configuration Guide*
- *Cisco Internet Streamer 2.0-2.3 API Guide*
- *Cisco Internet Streamer 2.0-2.3 Quick Start Guide*

The following documents have been added for this release:

- *Release Notes for Cisco Internet Streamer CDS 2.3*

Related Documentation

Refer to the following documents for additional information about the Cisco Internet Streamer CDS 2.0-2.2:

- *Cisco Content Delivery Engine 100/200/300/400 Hardware Installation Guide* (OL-13478-02)

  http://www.cisco.com/en/US/docs/video/cds/cde/installation/guide/CDE_Install_Book.html
- *Cisco Internet Streamer CDS 2.0-2.3 Software Configuration Guide* (OL-13493-04)

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_0/configuration/guide/is_cds20_22-cfguide.html
- *Cisco Internet Streamer CDS 2.0-2.3 Quick Start Guide* (OL-15479-03)

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_0/quick/guide/ISCDSQuickStart.html
- *Cisco Internet Streamer CDS 2.0-2.3 API Guide* (OL-14319-04)

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_0/developer/guide/cds20_22apiguide.html
- *Release Notes for Cisco Internet Streamer CDS 2.0* (OL-13494-02)

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_0/release_notes/CDS_RelNotes2_0.html
- *Release Notes for the Cisco Internet Streamer CDS 2.1* (OL-15751-01)

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_0/release_notes/CDS_RelNotes2_1.html
- *Release Notes for the Cisco Internet Streamer CDS 2.2* (OL-16951-02)

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_0/release_notes/CDS_RelNotes2_2.html
- *Cisco Content Delivery System 2.x Documentation Roadmap* (OL-13495-06)

  http://www.cisco.com/en/US/products/ps7127/products_documentation_roadmaps_list.html
- *Regulatory Compliance and Safety Information for Cisco Content Delivery Engine 100/200/300/400* (78-18229-02)

  http://www.cisco.com/en/US/docs/video/cds/cde/regulatory/compliance/CDE_RCSI.html

The entire CDS software documentation suite is available on Cisco.com at:

http://www.cisco.com/en/US/products/ps7127/tsd_products_support_series_home.html

The entire CDS hardware documentation suite is available on Cisco.com at:

http://www.cisco.com/en/US/products/ps7126/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.