# Release Notes for Cisco Internet Streamer CDS 2.1

These release notes covers the 2.1.1-b14 release.

**Revised: April 4, 2008, OL-15751-01**

## Contents

This information is in the release notes:



## New Features

Release 2.1 of the Internet Streamer CDS introduces the Flash Media Streaming feature. The Flash Media Streaming feature offers the ability to stream and monitor flash media content using the Internet Streamer CDS.

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

# Enhancements

Table 1 describes the enhancements to Internet Streamer CDS 2.1.

*Table 1 New Features in Internet Streamer CDS 2.1.1*

| New Feature | Description |
|---|---|
| Movie Streamer–Live streaming | In Release 2.0, Movie Streamer was in a demonstration state for live streaming, prefetched, cached and dynamically cached content.<br>In Release 2.1, live streaming is in full production. Prefetched, cached, and dynamically cached content remain in a demonstration state.<br>For details of live streaming performance for Movie Streamer, please refer to the 2.1 performance bulletin. |
| Management IP address and port | Allows you to specify the management IP address and port for the device. |
| Disable HTTP download | Allows you to disable HTTP download for a delivery service. |
| Application Control on the Service Router | Enables incoming proxy for HTTP. |
| Service Engine Windows Media server-side playlist | The NSC URL Reference field allows you to enter the URL for a server-side playlist for a multicast station configured on a Service Engine. |
| Threshold Monitoring for disk, Kmemory, Movie Streamer, Flash Medias Streaming, and Web Engine. | In addition to existing threshold monitoring (CPU, memory, and Windows Media). you can now set thresholds for disk, Kmemory (kernel memory), Movie Streamer Engine, Flash Media Streaming, and Web Engine. |
| More control of content management. | Allows you to set the maximum number of cache entries for each Service Engine. |
| Refined communication with Service Router | Allows you to set the keep-alive interval the Service Router uses for messages to each Service Engine. |
| Access Control List (ACL) server setting | Allows you to specify the IP address and type of the ACL server. |
| Service Router Last-Resort domain name | Allows you to specify the last-resort domain name for the Service Router. |
| Various changes to configuring live programs | Removed auto deletion of live program. Removed auto select of IP address from multicast pool. Removed “Customized URL.” |

# System Requirements

The CDS Internet Streaming runs on the CDE-100 and CDE-200 hardware models. The CDE-100 may run as the CDSM, while the CDE-200 may run as the Service Router or the Service Engine. See the *Cisco Content Delivery Engine CDE-100 and CDE-200 Hardware Installation Guide* for set up and installation procedures.

# Limitations and Restrictions

This release contains the following limitations and restrictions:

- The Movie Streamer functionality is capable of MPEG1/2/4 and H.264 streaming over RTP/RTSP to a wide range of devices including PC, Mac, PDA, and cell phones, with 3GPP release 6 support for rate adaptation and capability exchange. However, this Movie Streamer functionality is available only on a demo and lab trial basis, and the software enforces a hard limit of 20 concurrent sessions. If you are interested in running the Movie Streamer in a field trial or production environment, please contact your Cisco account team.
- There is no NAT separating the CDEs from one another.
- Do not run the CDE with the cover off, this disrupts the fan air flow and causes overheating.

# Important Notes

To maximize the content-delivery performance of a CDE-200, 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 CDE-200, 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 CDE-200 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 CDE-200 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 CDE-200 capacity, you are recommended to provision a dedicated CDE-200 to handle WMT; and likewise for HTTP. In such cases, we do *not* recommended you mix the two traffic types on all CDE servers which could result in suboptimal aggregate performance and require more CDE-200 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.

# Open Caveats

This release contains the following open caveats:

## Cache Routing Module

- CSCso57696

  Symptom:

  The CacheRouter process gets restarted in rare longevity runs with mixed traffic. This may result in a core dump of the process. A core file is viewable in the cor_dir directory, by using the CLI.

  Conditions:

  This problem is likely to happen whenever there is a transition between active cache miss traffic and no traffic. A core dump and restart may not occur every time this situation is present.

  Workaround:

  No manual intervention is required. The CacheRouter process restarts instantly and is operational again. A few requests for cache miss traffic are redirected to the origin server. End clients should not be affected.

## Flash Media Streaming Engine

- CSCso15521

  Symptom:

  When Flash Media Streaming is enabled, the fmsadmin process may leak memory every time the **show statistics flash-media-streaming** command is run either through the CLI or the CDSM GUI.

  In order to minimize the memory leak, the periodic polling of Flash Media Streaming statistics has been disabled. Customers can still check statistics on Flash Media Streaming by issuing the **show statistics flash-media-streaming** command through the CLI or CDSM GUI.

  Recovery:

  Recovery of the memory leak can be accomplished by disabling and re-enabling the Flash Media Streaming engine.

## Windows Media Engine

- CSCso38319

  Symptom:

Playback of a VOD wsx playlist over HTTP fails when authentication is enabled on the Windows Media Server (origin server).

Conditions:

When NTLM or Negotiate authentication is enabled.

Workaround:

For VOD wsx playlists requiring authentication, use RTSP instead of HTTP.

## Web Engine

- CSCsi84922

  Symptom:

  For a cache miss scenario, the HTTP bitrate configured for the delivery service does not take effect. The client receives the content at the rate the Content Origin server sends the response.

  Workaround:

  Once the content is cached on the SE, for subsequent requests, which area cache hit, the bitrate takes effect. However, you may choose not to configure any bitrate for the delivery service, and let TCP congestion control determine the optimal rate of each HTTP progressive download session.

## Movie Streamer

- CSCsl80363

  Symptom:

  When running a Movie Streamer live program, Service Engines in the second level location may try to acquire the live stream directly from the Content Origin server.

  There is no service or functionality impact on the CDS network. However, the load on the Content Origin server or encoders for the live source is increased.

  Conditions:

  This only happens when the Service Engines associated with the delivery service for the live program have experienced a failure or have been manually forced to reboot.

  Workaround:

  From the CDSM, disable and enable the delivery service for the live program. This action returns the CDS live program delivery tree back to normal.

- CSCsl96464

  Symptom:

  In the CDSM, the Bytes Served graph for Movie Streamer shows "0" bytes.

  Condition:

  Movie Streamer is enabled in the SE, and Movie Streamer content is streaming to clients.

  Workaround:

  Start a Telnet session to each participating SE, and use the **show statistics rtsp server movie-streamer all** command to view the Movie Streamer statistics.

## Service Router

- CSCsi68373

  Symptom:

  When the Service Router is at peak load (approximately beyond 4000 to 8000 session set-ups a second), depending on the routing algorithms being used (consult the data sheet performance section), a few of the client requests may fail with 404 response. The maximum Service-Router performance as published in the data sheet is measured by ensuring that no more than 0.2% of the requests may result in 404 failure; and typically only 0.001% results in 404 failures.

  Workaround:

  If the client retries, it almost always gets successfully routed. The operator can further reduce the failure rate by adequately provisioning and deploying enough Service Router to absorb not only the average but also the peak workload. If the deployment is not provisioned properly, and the aggregate load on the Service Router goes beyond the published performance number (for example, 8000 HTTP or ASX redirections a second), then the number of 4xx failures may increase dramatically. However, if the load is at or below the published performance limit, then only a tiny faction fails.

## Storage

- CSCsi32228

Symptom:

After a reload, the CDNFS statistics are incorrect until the SE has synchronized all the content information in the system. The cached content database restoration can take a few hours if there are more than a million assets in the SE. During this time, content delivery, including cache hits, continues to work properly, buy the statistics are inaccurately displayed.

Workaround:

Allow the cache database to complete the restoration before checking the CDNFS statistics. Since database restoration can take even longer if there is constant and heavy traffic on the server, you are not recommended to direct too much traffic to a SE that has just reloaded.

## Acquisition and Distribution

- CSCsi48105

  Symptom:

  The error reported for manifest file parsing may not provide the exact location of the parsing error. It is usually off by a few lines.

  Workaround:

  There is no workaround. This is an inherited problem from the open-source XML parser and is a known problem of the parser.

- CSCsj26190

  Symptom:

  If content deletion of preposition contents is occurring at the same time as newer contents are getting acquired, the content deletion may be very slow. This is noticeable when the number of assets >20 K.

  Workaround:

  There is no workaround.

### SNMP

- CSCsk09674

  Symptom:

  When you execute the following config command in the SE to view the MIB, you receive an error.

  ```
  (config)#snmp-server view see ciscoServiceEngineMIB excluded
  ```

  Workaround:

  Use the object identifier (OID) instead of the symbolic name for the MIB subtree.

## Caveats Not Caused by CDS Software

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

### Network Configuration

- CSCsi29008

  Symptom:

  Traffic loss occurs for a few seconds when a failover from primary to standby is triggered. This is an intrinsic property of the standby network interface mode.

  Workaround:

  Configure the port channel on both CDE and the connected switch, instead of standby interface. Port channel can recover interface failures in sub-seconds.

### Windows Media Streaming

- CSCsi57903

  Symptom:

  Client cannot use RTSPU when it is behind a NAT. This is an expected behavior as the client IP address is translated and not visible to server.

  Workaround:

  Configure the client to use RTSPT instead of RTSPU in its network configurations.

- CSCsh91171

  Symptom:

  The Windows Media Player controls are enabled for live sessions. This is a Windows Media Player issue.

  Workaround:

  There is no workaround. This problem exists with or without CDS.

- CSCsh90306

  Symptom:

  During playback of high bit-rate files, server streams the data at five times the rate of the bit-rate. This issue is seen even when the CDS is not used. It is Windows Media Player issue.

Workaround:

Turn off the fast cache feature on the server (Windows Media Server or CDS WMT), when serving high bitrate content (more than 780Kbps).

### Web Engine

- CSCsi08778

  Symptom:

  Windows Media Player cannot play media files with a size greater than or equal to 4GBytes that are progressively downloaded. This is a Windows Media Player issue as it does not work whether the Content Origin server is IIS or Apache and whether CDS is used.

  Workaround:

  There is no workaround.

- CSCsi50430

  Symptom:

  When the origin server is Windows Media Server, and the client request causes a progressive download to occur, content playback fails in a hierarchical setup.

  Workaround:

  Make sure the file is streamed through WMT streaming.

- CSCsh85626

  Symptom:

  For contents in the Content Origin server which are authenticated using NTLM, the Web-Engine download fails for those contents. It is commonly believed in the Internet community that supporting this for a proxy is a security hole, because we have multiple clients sharing same back end connection to Content Origin server, since NTLM is a connection-based authentication scheme. For this same reason web proxies like Squid and Apache proxy module do not support this nor does the CDS.

  Workaround:

  Do not use NTLM authentication on the Content Origin server.

## Resolved Caveats

Release 2.1.1 consists of many resolved issues since 2.0.3. Not all the resolved issues are mentioned here. The following list highlights the associated with customer deployment scenarios.

### CDSM

- CSCsj30486

  Symptom:

  The CMS does not come up when the CDSM is reloaded and the CDSM GUI is not accessible (this happens extremely rarely). The following exception (or similar) is logged:

```
06/18/2007 06:19:25.189(Local) [W] cdm(Scheduler): java.sql.SQLException: ERROR: Index
sys_mess_time_idx is not a btree: java.sql.SQLException: ERROR: Index
sys_mess_time_idx is not a btree
```

Workaround:

Execute the following command to run database maintenance:

```
DT-612-10#cms database maintenance full ?
```

## Platform

- CSCsj87235

  Symptom:

  In performance tests, when 1000 concurrent HTTP sessions are ungracefully shutdown without sending the SE the normal TCP teardown messages, the SE takes up to 40 minutes to clean up all the zombie TCP sessions from its memory. The impact is that the memory resource and connections are temporarily held up by the zombie sessions in the period. If another 1000 to 2000 sessions are immediately sent to the SE before the previous 1000 sessions are cleaned up, it is possible that some of the new sessions are denied due to the 2000 concurrent sessions limit of web-engine.

  Workaround:

  There is no workaround. This is not a real deployment scenario because typical clients always tear down the session before exiting and the only time a client does not is when it is abruptly power-cycled. Therefore, it is extremely hard to have such an ungraceful tear-down happen in a synchronized fashion across thousands of sessions going to the same CDE. Considering that each session had been properly authorized by the operator's entitlement servers, it is also unlikely any malicious user can feasibly launch such an attack.

## Storage

- CSCsk82154

  Symptom:

  Under heavy stress, during mixed traffic of WMT and HTTP, the storage layer may report errors indicating corruption of storage metadata files. This is due to race conditions that occur when the content is being modified and looked at simultaneously.

  Workaround:

  These errors are transient and only result in a failure of a single request. New requests will not see this failure when the content is fully cached and the race condition does not exist.

## SNMP

- CSCsk11560

  Symptom:

  SNMP Server authentication does not work if the privacy password is using SHA.

  Workaround:

  Use an MD5 based privacy password instead.

# Documentation Updates

The following documents have been updated for this release:

- *Cisco Internet Streamer CDS 2.0-2.1 Software Configuration Guide*
- *Cisco Internet Streamer 2.0-2.1 API Guide*
- *Cisco Content Delivery Engine 100/200/300/400 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for Cisco Content Delivery Engine 100/200/300/400*

The following documents have been added for this release:

- *Release Notes for Cisco Internet Streamer CDS 2.1*
- *Cisco Internet Streamer CDS 2.0-2.1 Quick Start Guide*

# Related Documentation

Refer to the following documents for additional information about the Cisco Internet Streamer CDS 2.0-2.1:

- *Cisco Content Delivery Engine 100/200/300/400 Hardware Installation Guide* (OL-13478-03)

  http://www.cisco.com/en/US/docs/video/cds/cde/installation/guide/CDE_Install_Book.html
- *Cisco Internet Streamer CDS 2.0-2.1 Software Configuration Guide* (OL-13493-02)

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_0/configuration/guide/is_cds20_22-cfguide.html
- *Cisco Internet Streamer CDS 2.0-2.1 Quick Start Guide* (OL-15479-01)

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_0/quick/guide/ISCDSQuickStart.html
- *Cisco Internet Streamer CDS 2.0-2.1 API Guide* (OL-14319-02)

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_0/developer/guide/cds20_21apiguide.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
- *Cisco Content Delivery System 2.x Documentation Roadmap* (OL-13495-03)

  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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

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