Release Notes for Cisco Internet Streamer CDS 2.4.5

These release notes cover Cisco Internet Streamer CDS Release 2.4.5-b3.

Revised: December 2009,OL-21469-01

Contents

The following information is included in these release notes:

Release 2.4.5 consists of resolved caveats. See the "Resolved Caveats" section on page 4 for more information.

Note The Flash Media Streamer DVR support are available as an early field trial release. For more information, contact your Cisco account representative.

Note The Session Shifting feature is not supported in Release 2.4. For 3-Screen Session Shifting, use the Cisco Internet Streamer CDS 2.3 software.

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

© 2009 Cisco Systems, Inc. All rights reserved.

System Requirements

The Internet Streamer CDS runs on the CDE100, CDE200, CDE205, and the CDE220 hardware models. Table 1 lists the different device modes for the Cisco Internet Streamer CDS software, and which CDEs support them.

Table 1 Supported CDEs

Device Mode	CDE100	CDE200	CDE205	CDE220
CDSM	Yes	No	Yes	No
SR	No	Yes	Yes	Yes
SE	No	Yes	Yes	Yes

Release 2.4.5 supports the CDE220 2G2 platform. There are a total of ten gigabit Ethernet ports in this CDE. The first two ports (1/0 and 2/0) are management ports. The remaining eight gigabit Ethernet ports can be configured as one port channel. See the *Cisco Content Delivery Engine CDE205/220/420 Hardware Installation Guide* for set up and installation procedures for the CDE220 2G2.

The CDE100 can run as the CDSM, while theCDE200 can 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 for the CDE100 and CDE200.

The CDE205 can run as the CDSM, Service Router, or Service Engine. See the *Cisco Content Delivery Engine CDE205/220/420 Hardware Installation Guide* for set up and installation procedures for the CDE205.

Note For performance information, see the release-specific performance bulletin.

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, CDE205, or CDE220, we recommend you do the following:

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

   Configure interfaces on the quad-port gigabit Ethernet cards 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 2.4 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.

   Note The optimal load-balance setting on the switch for traffic between the Content Acquirer and the edge Service Engine is dst-port, which is not available on the 3750, but is available on the Catalyst 6000 series.

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

   The CDE200, CDE205, or CDE220 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, CDE205, or CDE220 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, CDE205, or CDE220 servers than usual.

4. 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.

5. 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.

Resolved Caveats

The following caveats have been resolved since Cisco Internet Streamer CDS Release 2.4.3. Not all the resolved issues are mentioned here. The following list highlights the resolved caveats associated with customer deployment scenarios.

Windows Media Streaming

- CSCtd39651

  Symptom:

  Because the content is very specific (encrypted flag in ASF file is 1), client sends a request with stream-switch-entry=ffff:8001:0 ffff:8002:0. 8001&8002 are flags of ASF file only 0~6 bits are used as stream number. This case is not addressed.

- CSCtc63215

  Symptom:

  DSCP value not set for RTSP.

- CSCtc57849

  Symptom:

  SE marks fast-cache for RTSPT when fast-cache is disabled.

- CSCtc33684

  Symptom:

  Only audio is available when HTTP request is used to playback some of the media files. These media files have an audio track == 1 and a video track = 31.

- CSCtc21243

  Symptom:

  SE to send A-record instead of AAAA-record for DNS resolution.

- CSCsx58932

  Symptom:

  Windows Media Streaming core dumps during testing of live streaming.

  Conditions:

  This happens when a server-side playlist (SSPL) source is used and automation scripts are used as clients.

Flash Media Streaming

- CSCtd59141

  Symptom:

  Rule-enable configuration does not persist across a reboot. After a system reboot, the rule enable configuration is not being set in shared memory, which results in inconsistent rule allow/blocking behavior across reboot.

Kernel Streaming Engine

- CSCtc98738

  Symptom:

  Client disconnecting triggers internal error in Windows Media Streaming.

- CSCtc98733

  Symptom:

  Windows Media Streaming hand off causes KDB crash.

- CSCtc58223

  Symptom:

  Memory leak occurred when Windows Media Streaming delivery service is configured with Primed configuration for a live radio delivery service.

Acquisition and Distribution

- CSCtc83166

  Symptom:

  Virtual memory size exceeds limit causing acquisition and distribution processes to get disabled and exit.

- CSCtc07937

  Symptom:

  Disk quota exceeds limit causing Content Acquirer to restart loop.

URL Manager

- CSCtd48216

  Symptom:

  When a client sends a request for live Flash Media Streaming content with a signed URL using a private key and a .flv extension, a core dump occurs.

- CSCtd03738

  Symptom:

  The first request from client is SETUP not DESCRIBE. This is not handle this case properly.

Service Router

- CSCtd48118

  Symptom:

  The SR transactions per second (TPS) drops to 200 when proximity cache-hit case.

- CSCtd28648

  Symptom:

  The SR returns an empty DNS response for AAAA if IPv6 is not configured.

- CSCtc86425

  Symptom:

  When there are multiple cache entries for the same route, the one with longest match is used. However, once the matched one expires, the SR ignores the other valid one and sends a proximity request to the Proximity Engine for all future client requests from that subnet. This causes a performance issue since the cache-miss transactions per second (TPS) is a lot lower than the cache hit TPS.

- CSCsy98504

  Symptom:

  SR core dumps when Proximity Engine or location-based routing is under stress.

SNMP

- CSCtc63501

  Symptom:

  SNMP MIB incorrectly reports that CPU on SR and Content Acquirer is at 100 percent.

Platform

- CSCtc99024

  Symptom:

  Some hard disk drives are not recognized when the CDE200 gets a cold restart.

Service Monitor

- CSCtd30350

  Symptom:

  Alarm ID is wrong for CPU and memory thresholds. Alarm 560006 is for disk fail count, while 560001/560002 are for cpu/mem alarm.

Upgrading to Release 2.4.5

The only supported upgrade paths are Release 2.4.x to Release 2.4.5 and Release 2.3.x to Release 2.4.5. If you are running a release prior to Release 2.3.x, you must upgrade to Release 2.3.x before upgrading to Release 2.4.5.

Note An SR running the Release 2.4 software is not compatible with an SE running the Release 2.3.x software. We strongly recommend that you upgrade your CDS network devices in the following order:

1. Multicast sender Service Engines
2. Multicast receiver Service Engines
3. Non-Content Acquirer Service Engines
4. Content Acquirer Service Engines
5. Service Routers
6. Standby CDSMs (Upgrade before primary when using the GUI only.)
7. Primary CDSM

URL Public Key Signing

Table 2 describes the compatibility and results when using a prior CDS software release to perform URL signing and the current software release to perform URL validation.

Table 2 Release Compatibility of URL Signing and URL Validation

Release Used for URL Signing	Release Used for URL Validation	Results
2.3.x	2.4.3, 2.4.5, or 2.5.x	Does not work because the Release 2.3.x URL signing uses the port and schema for signing, but the port is stripped off during validation by the current software release.
2.4.1	2.4.3	Works for URL signing version 0, 1, or 2. URL signing version 3 is the new version introduced in Release 2.4.3 for the public/private key signing.
2.4.3	2.4.5	Works for URL signing version 0, 1, 2, or 3.

Documentation Updates

The following documents have been added for this release:

- *Release Notes for Cisco Internet Streamer CDS 2.4.5*

The following documents have no changes:

- *Cisco Internet Streamer CDS 2.4 Software Configuration Guide*
- *Cisco Internet Streamer CDS 2.4 API Guide*
- *Cisco Internet Streamer CDS 2.4 Quick Start Guide*
- *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide*
- *Cisco Internet Streamer CDS 2.4 Command Reference Guide*
- *Cisco Internet Streamer CDS 2.4 Alarms and Error Messages Guide*

Related Documentation

Refer to the following documents for additional information about the Cisco Internet Streamer CDS 2.4:

- *Cisco Internet Streamer CDS 2.4 Software Configuration Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_4/configuration_guide/is_cds24-cfguide.html
- *Cisco Internet Streamer CDS 2.4 Quick Start Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_4/quick_guide/ISCDSQuickStart.html
- *Cisco Internet Streamer CDS 2.4 API Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_4/developer_guide/is_cds_24_apiguide.html
- *Cisco Internet Streamer CDS 2.4 Command Reference Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_4/command_ref/Command_Ref.html
- *Cisco Internet Streamer CDS 2.4 Alarms and Error Messages Guide*
  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_4/message_guide/Messages.html
- *Cisco Content Delivery System 2.x Documentation Roadmap*
  http://www.cisco.com/en/US/docs/video/cds/overview/CDS_Roadmap.html
- *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide*
  http://www.cisco.com/en/US/docs/video/cds/cde/cde205_220_420/installation/guide/cde205_220_420_hig.html
- *Cisco Content Delivery Engine 100/200/300/400 Hardware Installation Guide*
  http://www.cisco.com/en/US/docs/video/cds/cde/installation/guide/CDE_Install_Book.html
- *Regulatory Compliance and Safety Information for Cisco Content Delivery Engines*
  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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.