Release Notes for *Cisco Videoscape Distribution Suite Transparent Caching* Release 5.0.2

First Published: May 2013
OL-28014-02

These release notes describe the new features and caveats of the Cisco Videoscape Distribution Suite Transparent Caching Release 5.0.2.

For a list of open caveats that are pertinent to this release, see the "Caveats" section.

Contents

Introduction

The Cisco Videoscape Distribution Suite Transparent Caching (VDS TC) solution is focused on reducing costs and improving quality of user experience in delivering unmanaged Internet-based content, including Internet video, file sharing, software distribution, mobile application downloads, and web browsing. VDS TC integrates highly scalable caching software with high-performance Cisco Unified Computing System™ (UCS) servers and blades, Cisco® switches, and SAN storage. The VDS TC solution, combined with other Videoscape products like Cisco Videoscape Distribution Suite for Internet Streaming (VDS IS), provides a complete platform for optimizing managed and unmanaged content delivery.

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

For unmanaged content, Cisco VDS TC empowers service providers to alleviate network congestion due to Internet video and other high-bandwidth applications in their networks, while meeting subscribers' demand for the content and improved quality of experience. VDS TC is typically deployed in conjunction with a network element, such as a router or Deep Packet Inspection (DPI) element, which is responsible for classification and redirection of traffic to the cache, based on Layer 4 and Layer 7 criteria.

New Features

Release 5.0.2 of Cisco Videoscape Distribution Suite Transparent Caching (VDS TC) introduced the following new features:

- New configuration models:
  - VDS TC Integrated Appliance (VDS-TC-1S), using the Cisco UCS C240 Rack Mount Server
  - VDS TC Blade Server installations, using the Cisco UCS B200 Series Blade Servers:
    - VDS-TC-4B, redundant and non-redundant configurations
    - VDS-TC-8B, redundant and non-redundant configurations
    - VDS-TC-16B, redundant and non-redundant configurations
- Support for using the Cisco UCS C240 with DC power supply as the VDS TC management server
- Support for the Cisco Nexus 7004 Switch as the VDS TC data switch and support for the Cisco C2248TP fabric extender
- IPv6 support for the entire VDS TC solution, including subscriber facing interfaces, VDS TC data switches, and Cisco UCS servers

Product Overview

Cisco VDS TC is multi-protocol, supporting HTTP for download, progressive download, and adaptive bit rate (ABR) streaming, as well as multiple peer-to-peer (P2P) protocols. The solution automatically adapts to content popularity once installed, and is access-network-agnostic. The system automatically adjusts to traffic mix changes during the day and week.

One of the benefits of Cisco VDS TC is that it can enable service providers to offload a significant amount of content traffic by serving the popular content from a locally cached copy, within the access network. As a result, service providers can experience a rapid return on investment (ROI) by reducing their operational network costs, and defer capital investments into their network infrastructures.

The other main benefit of Cisco VDS TC is the improvement of the quality of experience (QoE) for the subscribers of the service providers. By serving popular content from locally deployed cache, the content is better positioned to provide a better user experience than if the content were served from the original content server.

The Cisco VDS TC solution can enable service providers to:

- Lower core and edge network bandwidth
- Manage infrastructure costs for over-the-top (OTT) content in a cost-efficient manner
- Improve subscriber QoE for popular content
- Deploy OTT caching without impacting the client or origin CDN, or application behavior

System Requirements

Cisco VDS TC is optimized for use on the Cisco Unified Computing Systems (Cisco UCS), such as the Cisco UCS C220 Rack Server or the Cisco UCS B200 Blade Server.

Product	Hardware
VDS TC Cache Server	Cisco UCS B200 Blade Server or Cisco C220 Rack Mount Server with the following: • 2 x 2.40 GHz E5-2665, 115W 8C, 20 MB Cache, DDR3 1600 MHz • 32 GB DDR3-1333-MHz RDIMM, PC3-10600, 2R, 1.35v • 2 x 300 GB 6 Gb SAS 10K RPM SFF HDD, hot plug, drive sled mounted
VDS TC Cache Manager	Cisco C220 Rack Mount Server or the Cisco C240 Rack Mount Server with the following: • 2 x 2.4 GHz E5-2609/80W 4C, 10 MB Cache, DDR3 1066 MHz • 16 GB DDR3-1333-MHz RDIMM/PC3-10600, 2R, 1.35v • 2 x 300 GB 6 Gb SAS 10K RPM SFF HDD, hot plug, drive sled mounted
VDS TC SAN Storage	Dual controller, 24 x 600G SAS 10K RPM, 2.5 in. small form factor (SFF)
VDS TC Integrated Cache Server, Manager, and storage for a VDS-TC-1S installation	Cisco UCS C240 Rack Mount Server with the following: • 2 x 2.40 GHz E5-2665, 115W 8C, 20 MB Cache, DDR3 1600 MHz • 32 GB DDR3-1333-MHz RDIMM, PC3-10600, 2R, 1.35v • 2 x 300 GB 6 Gb SAS 10K RPM SFF HDD, hot plug, drive sled mounted • 12 x 1T B 6 Gb SATA 7.2K RPM SFF HDD, hot plug, drive sled mounted
VDS TC Analytics Server	Cisco UCS C240 Rack Mount Server with the following: • 2 x 2.40 GHz E5-2665, 115W 8C, 20 MB Cache, DDR3 1600 MHz • 48 GB DDR3-1333-MHz RDIMM, PC3-10600, 2R, 1.35v • 2 x 300 GB 6 Gb SAS 10K RPM SFF HDD, hot plug, drive sled mounted • 10 or 22 x 900 GB 6 Gb SAS 10K RPM SFF HDD, hot plug, drive sled mounted

Caveats

Open Caveats in Cisco Videoscape Distribution Suite Transparent Caching Release 5.0.2

- **CSCud85704**
  - **Symptom:** The previous license data remains in the existing CLI login session after an upgrade or a new license has been applied.
  - **Workaround:** To see the content of the latest license, log off of the CLI and log in again. This will sync the license content with the one seen in the UI. When applying a new license, the license is applied as shown in the UI. The CLI shows the old license information until you log off and log back in again, but the system *does* use the new license.
- **CSCud65345**
  - **Symptom:** Cluster is degraded for 15 minutes after disconnecting storage controller 1.
  - **Workaround:** The system recovers from degradation after 15 minutes.
- **CSCud43741**
  - **Symptom:** Incorrect reporting of some HTTP traffic as P2P traffic.
  - **Explanation:** Due to the way traffic is classified and the nature of HTTP requests, it is possible that some HTTP traffic may be classified as P2P. This behavior will not affect system functionality.
- **CSCug09063**
  - **Symptom:** For a VDS TC 1S system, when you execute the **oper service stop** command, it can take up to 20 seconds to stop the caching service. If you execute the **show status** command immediately after entering the **oper service stop** command, you may see a status of “enable started”, even though the stopping process has already been initiated.
  - **Workaround:** Continue to enter the **show status** command until you see a status of “oper service stop”. It may take up to 20 seconds to see this status depending on how busy the VDS TC 1S system is.
- **CSCug27744**
  - **Symptom:** When you enter the command **./cmdbutils -s** from the /opt/pang/bin folder, the following two lines of erroneous messages are returned at the beginning of the output. However, the correct output appears below these lines.

    ```
    sh: -c: line 0: unexpected EOF while looking for matching `"'
    sh: -c: line 41: syntax error: unexpected end of file
    ```

  - **Workaround:** Ignore the two lines of erroneous messages that appear at the beginning of the output.
- **CSCug46383**
  - **Symptom:** When you choose **Policies and Config > License Manager > Generate License Request** from Cisco VDS TC Manager, not all of the system ids are included in the license request that is generated.

  - **Workaround:** This problem occurs because not all cache engines are online when the license request is generated. Please ensure that all cache engines are online by issuing the **show status** command from the VDS TC CLI. To start a cache engine that is not online, from the VDS TC CLI Enable mode, enter the command **oper server** *x* **start** command, where *x* is the number of the cache engine that you want to start.

- **CSCug32380**
  - **Symptom:** Occasionally, incorrect messages are logged into /opt/pang/cdrs while unplugging and plugging back in the Ethernet1 and Ethernet2 cables of a cache engine.

    For example:

    stats: iff_4 (eth9) to classifier 0

    10-04-13 13:32:09.080, 7189[common:Statistics]void statistics_c::dump_packets_queues() ### Classifier Interface queues stats: iff_5 (eth10) to classifier 0

    10-04-13 13:32:09.080, 7189[common:Statistics]void statistics_c::dump_packets_queues() ### Classifier Interface queues stats: iff_6 (eth11) to classifier 0

    10-04-13 13:32:09.080, 7189[common:Statistics]void statistics_c::dump_packets_queues() ### Classifier Interface queues stats: iff_7 (eth12) to classifier 0
  - **Workaround:** The messages should be ignored, they do not belong in /opt/pang/cdrs.
- **CSCug77748**
  - **Symptom:** If all of the connections between the cache engines and the entire storage array are lost, all traffic is forwarded directly to the Internet (bypassed by the system). Once connection between the cache engines and the storage array is restored, it may take up to one hour before user requests will be handled by the cache engine.
  - **Workaround:** There is no work around. It will take one hour before the cluster returns to normal.
- **CSCud47393**
  - **Symptom:** VDS TC Manager shows an inactive volume on the cluster. However, when checking the volumes from the IBM storage manager, no bad sectors or errors can be found. This can occur if the volume had a corrupted file system when the VDS TC disk format script was executed. The disk format script will skip the re-format on that volume and leave it in an inactivate state.
  - **Workaround:** Perform the following steps if you know there are no bad sectors on the inactive volume:

Procedure

Step 1 Use SSH software to connect to the VDS TC management server. Log into the system using the username **padmin** and the password that was provided by Cisco.

Step 2 Enter the command **su root** to log in as the root user. When prompted, enter the password for the root user that was provided by Cisco.

Step 3 Enter the command **su admin** to log into the VDS TC CLI as admin.

Step 4 Enter the command **enable** and when prompted enter the Enable mode password.

Step 5 Enter the command **oper service stop** to stop the VDS TC caching service.

Step 6 Enter the command **exit** to logout of Enable mode.

Step 7 Enter the command **exit** to logout of the VDS TC CLI.

Step 8 Enter the command **ssh root@ce-1** to log into the cache engine.

Step 9 Enter the command **dd if=/dev/zero of=/dev/***drive_to_zero* **oflag=direct bs=4k**, replacing *drive_to_zero* with the id of the volume to zero out. For example, dd if=/dev/zero of=/dev/sdd oflag=direct bs=4k.

Note This step can take a long time (hours) depending on the size of the disk.

Step 10 Enter the command **/opt/pang/useful/format_disks_256k.sh** to format the disk.

Step 11 After the formatting of the disk is complete, enter the command **exit** to return to the management server.

Step 12 Enter the command **su admin** to log into the VDS TC CLI as admin.

Step 13 Enter the command **enable** and when prompted enter the Enable mode password.

Step 14 Enter the command **oper service start** to start the VDS TC caching service.

Step 15 Logout of the VDS TC CLI.

Step 16 In a web browser, enter the management IP address of the VDS TC management server to log into VDS TC Manager. Use the username **padmin** and the password that was provided by Cisco.

Step 17 Choose **Monitor** > **Storage** and click the **Volume Usage** tab. Verify that the volume that you reformatted shows a state of “active”.

- **CSCug22967**
  - **Symptom:** After entering a management IPv6 address on the VDS TC management server using either the GA_installer.sh script or the CLI commands, **network ip6** and **network default6_gw**, the IPv6 address information does not appear in the configuration of the VDS TC management server.
  - **Workaround:** This problem occurs because IPv6 is not enabled in the operating system. Use the following steps to enable IPv6 on the VDS TC management server and then configure a management IPv6 address and IPv6 gateway:

Note It is best to perform these steps during a maintenance window because these steps may cause a temporary service disruption.

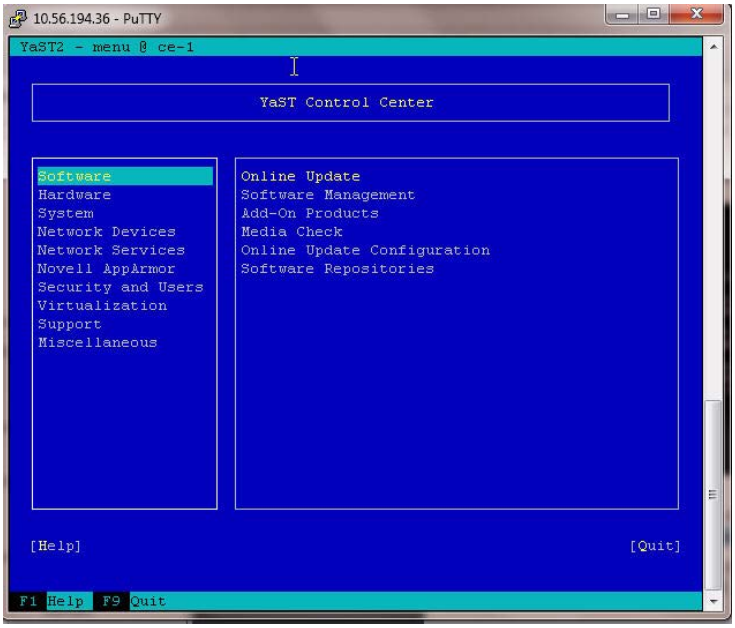
Enable IPv6

Step 1 Use SSH software to connect to the VDS TC management server. Log into the system using the username **padmin** and the password that was provided by Cisco.

Step 2 Enter the command **su root** to log in as the root user. When prompted, enter the password for the root user that was provided by Cisco.

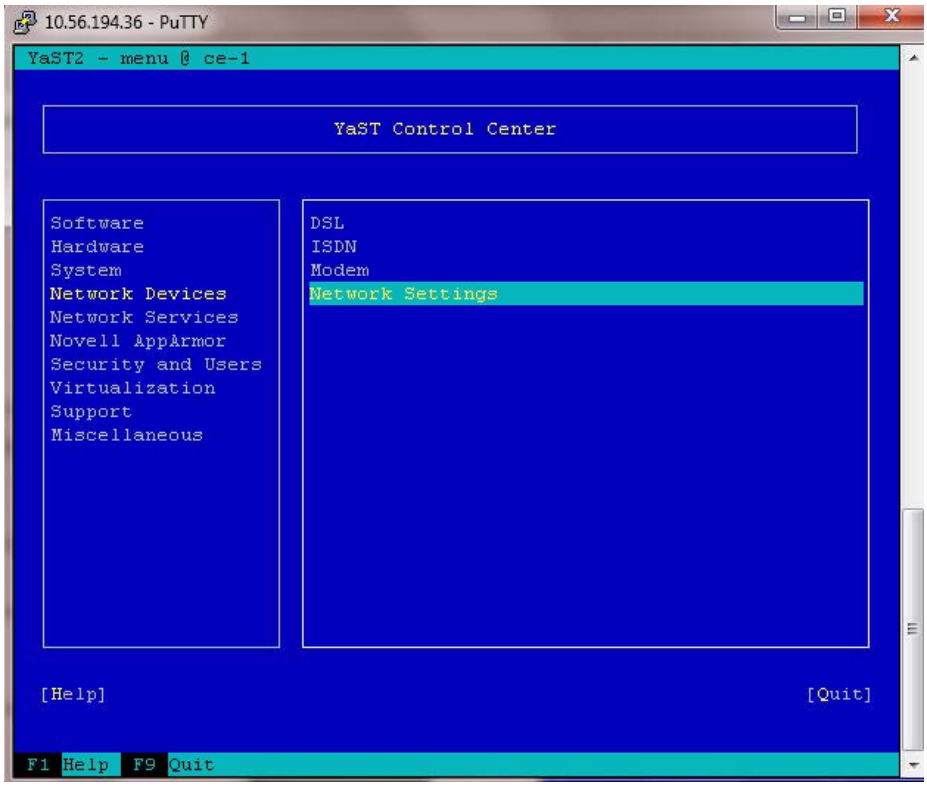
Step 3 Enter the command **yast** to enter the YaST environment. The YaST Control Center window appears.

Figure 1 YaST Control Center



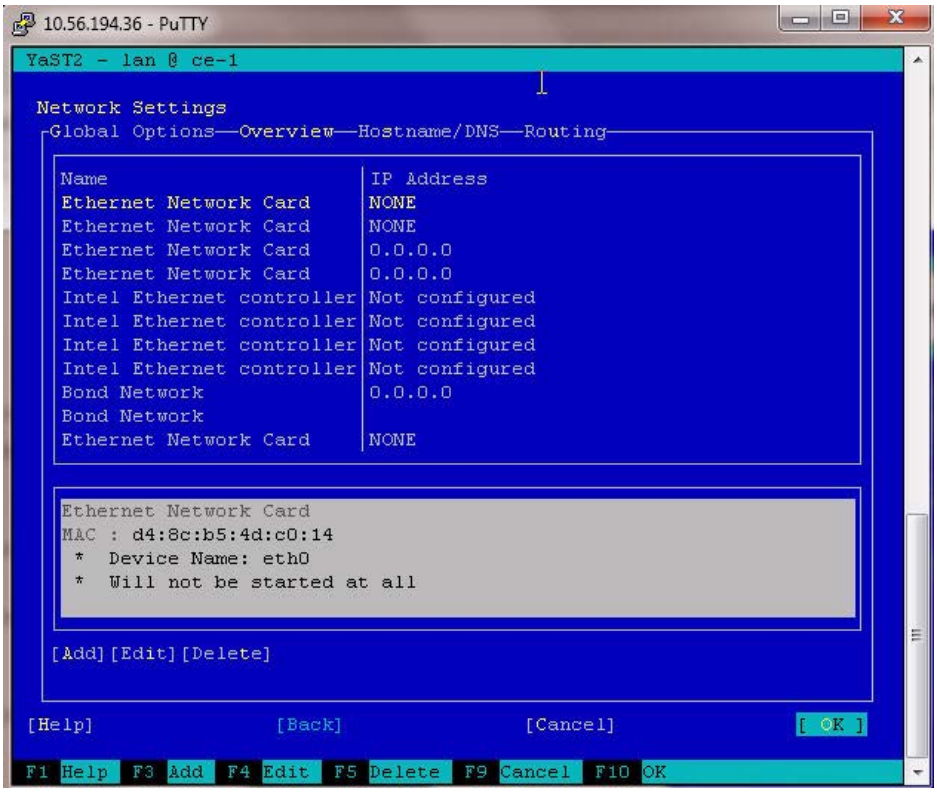
Step 4 From the YaST Control Center window choose **Network Devices** from the left pane and then choose **Network Settings** from the right pane. Press **Enter**.

Figure 2 Network Devices > Network Settings



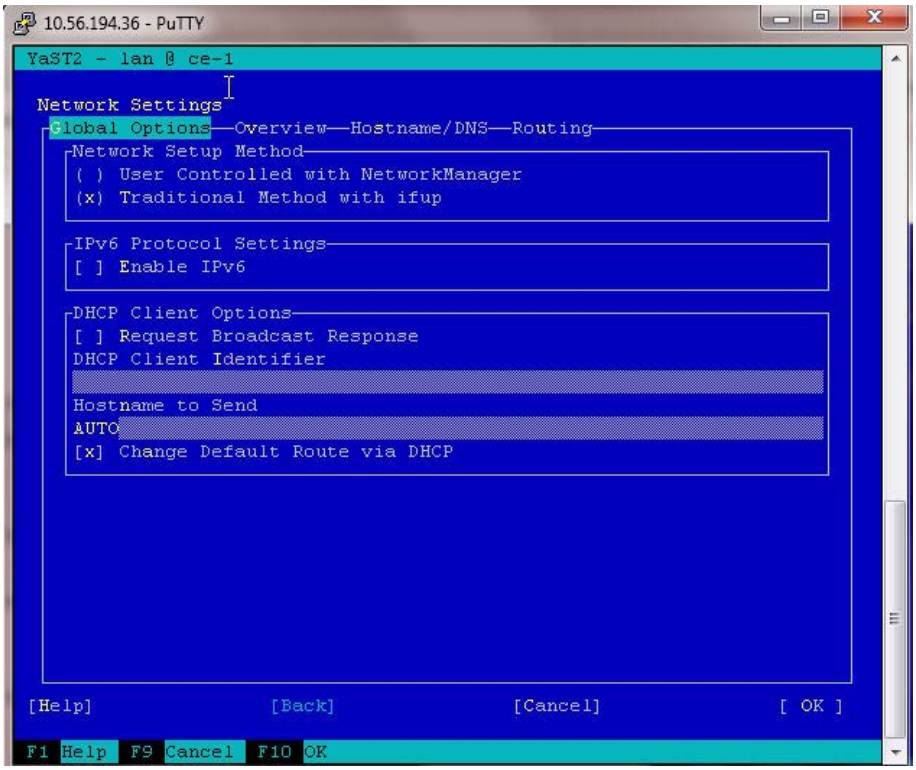
Step 5 From the Network Settings window, press **Alt-G** to choose Global Options.

Figure 3 Network Settings Window



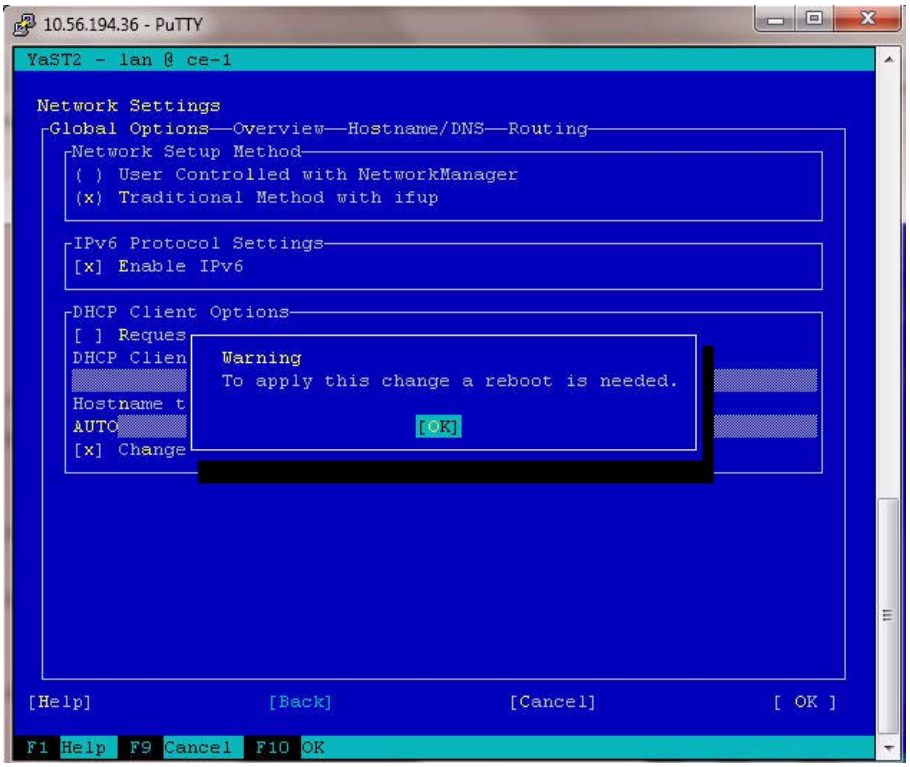
Step 6 Press **Alt-E** to choose Enable IPv6. A popup message appears telling you to reboot.

Figure 4 Global Options Window



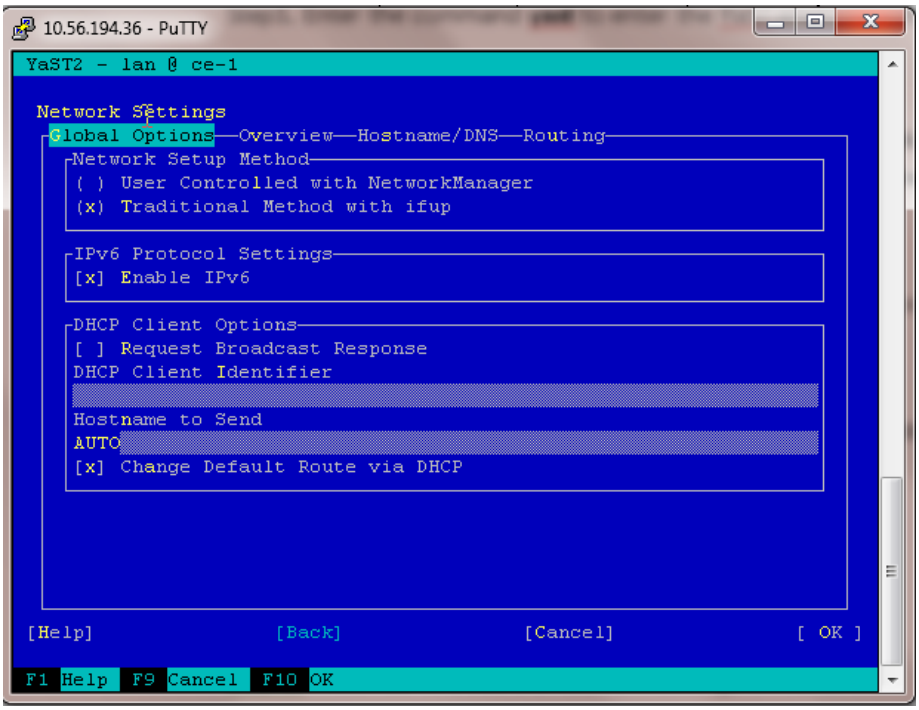
Step 7 Press **Enter** to close the warning window.

Figure 5 Enable IPv6 Warning Window



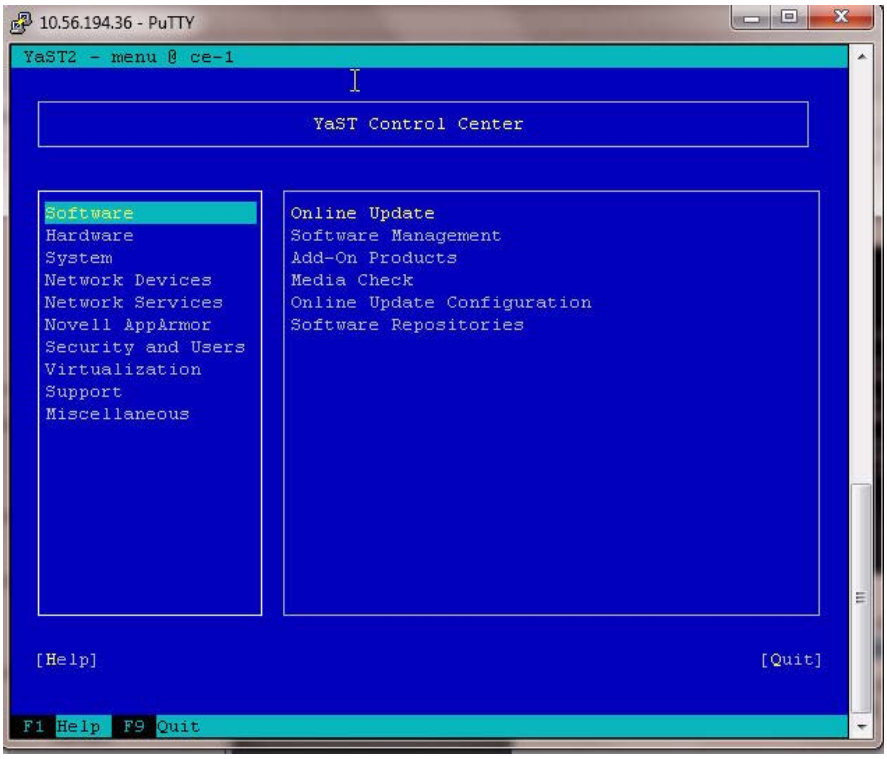
Step 8 Press **F10** to close the Network Settings window.

Figure 6 Network Settings Window



Step 9 Press **F9** to quit YaST.

Figure 7 YaST Control Center



Step 10 Reboot the VDS TC management server. This will disconnect you SSH session.

Configure Management IPv6 Address on VDS TC Management Server Using Network Commands

Note You must enable IPv6 in the operating system as described above in the Enable IPv6 procedure before performing these steps.

Note Performing these steps will cause your SSH session to the VDS TC management server to be closed and will cause a temporary service disruption. It is best to perform these steps during a maintenance window.

Step 1 After the VDS TC management server reboots, use SSH software to connect to the management IPv4 address that you assigned to the VDS TC management server. Use the username **admin** and the password provided by Cisco.

Step 2 Enter the command **enable** to switch to Enable mode. When prompted enter the enable password.

Note By default the enable password is the system ID, but this password may have been changed.

Step 3 Enter the command **config** to switch to Configuration mode.

Step 4 Enter the command **network ip6** *ipv6/prefix*, where *ipv6/prefix* is the management IPv6 address and prefix length that you want to configure. For example, **network ip6 2001::22/64**.

Step 5 Enter the command **network default6_gw** *dg_ipv6_address*, where *dg_ipv6_address* is the address of the IPv6 gateway. For example **network default6_gw 2001::1**.

Step 6 Enter the command **diff** to confirm the pending changes.

Step 7 If the IPv6 address and IPv6 default gateway information is correct, enter the command **apply** to apply the changes. If the IPv6 address or IPv6 default gateway information is not correct, repeat Step 5 through and Step 7.

Caution Applying this change will cause your SSH session to the VDS TC management server to be closed and will cause a temporary service disruption. It is best to perform these steps during a maintenance window.

Alternately to configure a management IPv6 address on the VDS TC management server, you can edit and import the cluster_conf.xml file. Follow these steps to configure a management IPv6 address by importing a cluster_conf file.

Note You must enable IPv6 in the operating system as described above in the Enable IPv6 procedure before performing these steps.

Note Performing these steps will cause your SSH session to the VDS TC management server to be closed and will cause a temporary service disruption. It is best to perform these steps during a maintenance window.

Configure Management IPv6 Address on VDS TC Management Server Using the Cluster_Conf File

Step 1 Using SSH software connect to the management IPv4 address that you assigned to the VDS TC management server. Use the username **admin** and the password provided by Cisco.

Step 2 Enter the command **enable** to switch to Enable mode. When prompted enter the enable password.

Note By default the enable password is the system ID, but this password may have been changed.

Step 3 Enter the command **config** to switch to Configuration mode.

Step 4 Enter the command **export localhost** *filename*, where *filename* is the name of the file to which you want to save the current configuration. The common filename to use is cluster_conf.xml.

Step 5 Using SFTP software, such as WinSCP, connect to the management IPv4 address that you assigned to the VDS TC management server. Log in using the user name **padmin** and the password that was provided by Cisco.

Step 6 Change to the /tftpboot folder and copy the file that you exported in Step 4 to your computer.

Step 7 Using a text editor, edit the file that you copied to your computer in Step 6 and add the following parameters in the <mgmt-config> section of the file:

```
<ip6addr>ipv6_address/prefix_length</ip6addr>
```

Note You must place this parameter immediately after the <netmask> parameter.

<default6-gw>*ipv6_default_gateway*</default6-gw>**

Note You must place this parameter immediately after the <default-gw> parameter.

For example:

```
<mgmt-config>
    <ipaddr>10.56.194.65</ipaddr>c
    <netmask>255.255.254.0</netmask>
    <ip6addr>2001:db8:8:4::2/64</ip6addr>
    <default-gw>10.56.194.1</default-gw>
    <default6-gw>2001:db8:8:4::1</default6-gw>
```

Note This is just a portion of the <mgmt-config> section that shows the newly added parameters. This example does *not* show the entire <mgmt-config> section in the configuration file.

Step 8 Save the file that you edited in Step 7, and using the SFTP software, copy the edited file to the /tftpboot folder on the VDS TC management server.

Step 9 From the VDS TC management server CLI, ensure that you are still in Configuration mode (the prompt will be configuration#.)

Step 10 Enter the command **import localhost** *filename*, where *filename* is the name of the file that you edited and copied to the /tftpboot folder in Step 8.

Step 11 Enter the command **diff** to confirm the pending changes.

Step 12 If the IPv6 address and IPv6 default gateway information is correct, enter the command **apply** to apply the changes. If the IPv6 address or IPv6 default gateway information is not correct, repeat Step 7 through Step 12.

Note Applying this change will cause your SSH session to the VDS TC management server to be closed and will cause a temporary service disruption. It is best to perform these steps during a maintenance window.

Caution If you have configured the timezone of the VDS TC management server or cache engines, or if you have configured the VDS TC management server to use an external NTP time server, you must repeat the NTP configuration after importing a cluster_conf file. See “Appendix D” of the *Cisco Videoscape Distribution Suite Transparent Caching Software Installation Guide* (OL-28015-02) for directions on how to do this.

Resolved Caveats

This section contains the resolved caveats in Cisco VDS TC Release 5.0.2. Not all resolved issues are mentioned here. The following list highlights resolved caveats associated with customer deployment scenarios:

- **CSCud86102:** Management server does not re-establish spread connection if it gets disconnected.

Related Documentation

Software Documents

Refer to the following documents for additional information about VDS TC 5.0.2.

Document	URL
Cisco Videoscape Distribution Suite Transparent Caching Software Installation Guide	http://www.cisco.com/en/US/docs/video/videoscape/distribution_suite/vds/v5_0_2/OL-28015-02_VDS-TC_5.0.2_sw_install_guide.pdf
Cisco Videoscape Distribution Suite Transparent Caching Software Configuration Guide	http://www.cisco.com/en/US/docs/video/videoscape/distribution_suite/vds/v5_0_2/OL-28016-02_VDS-TC_5.0.2_sw_config_guide.pdf
Cisco Videoscape Distribution Suite Transparent Caching Manager User Guide	http://www.cisco.com/en/US/docs/video/videoscape/distribution_suite/vds/v5_0_2/OL-28017-02_VDS-TC_5.0.2_manager_user_guide.pdf
Cisco UCS C-Series Rack Servers Install and Upgrade Guides web page	http://www.cisco.com/en/US/products/ps10493/products_installation_and_configuration_guides_list.html
Cisco UCS B200 Blade Server Installation and Service Note	http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/blade.html
Cisco UCS B-Series Blade Servers Configuration Guides web page	http://www.cisco.com/en/US/products/ps10280/products_installation_and_configuration_guides_list.html
Cisco UCS 5108 Server Chassis Installation Guide	http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/ucs5108_install.html

The entire VDS TC software documentation suite is available on Cisco.com at:
http://www.cisco.com/en/US/products/ps12654/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:

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

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