Release Notes for Cisco Broadband Troubleshooter Release 3.3

Cisco Broadband Troubleshooter Release 3.3
OL-14014-01
June 28, 2007

Multiple Service Operators (MSOs) and Cable companies provide a variety of services such as TV, video on demand, data, and voice telephony to subscribers. Network Administrators and radio frequency (RF) technicians need specialized tools to monitor and resolve RF problems in the cable plant.

Cisco Broadband Troubleshooter 3.3 (CBT 3.3) is a simple, easy-to-use tool designed to recognize and resolve such issues with efficiency and accuracy.

This document describes the new features and configurations introduced in CBT release 3.3, with resolved caveats and additional references.

Contents

This document describes CBT enhancements and feature sets for multiple versions of CBT in the following sections:

New and Changed Information in CBT 3.3

Cisco Broadband Troubleshooter Release 3.3 introduces significant enhancements, while sustaining several additional features introduced in prior versions (CBT 3.2 and CBT 3.1).

New Features in CBT 3.3

Cisco Broadband Troubleshooter Release 3.3 introduces the following categories of enhancements and features:

CBT 3.3 Download File Sizes

Table 1 summarizes approximate download file sizes for CBT 3.3.

Table 1   CBT 3.3 File Sizes

Platform	Filename	File Size[1]
Solaris	CBT33-Solaris.tar.gz	209 MB
Linux	CBT33-Linux.tar.gz	268 MB
Windows	CBT33-Win.exe	155 MB

1. Approximate compressed download file size.

Administrative and Security Enhancements

- CBT 3.3 supports the display of Cisco CMTS headend systems by name.
- CBT 3.3 adds support for hostnames that use dotted notation, such as cmts.a and cmts.b. CBT 3.3 lists only the hostnames of the Cisco CMTS headends for which hostnames are configured.
- CBT 3.3 adds hostname mapping from applet to servlet.
- CBT 3.3 adds an administrative setting for collection of maximum spectrum analyzer points.
- CBT 3.3 removes zero-second polling for non-administrative users.
- CBT 3.3 supports instantaneous CPU usage monitoring on the Cisco CMTS during spectrum operations. The supporting and configurable SpecDataMaxCPU parameter is available in the CBT 3.3 configuration file.

- CBT 3.3 supports the import of the Cisco CMTS data file to the CBT 3.3 server, rather than having to enter CMTS data as with earlier versions of CBT.
- CBT 3.3 introduces support for password-level security.
- CBT 3.3 supports spectrum data playback, according to Cisco CMTS name or IP address.

Cisco CMTS Support and Licensing Enhancements

- With 500 Cisco CMTS licenses, CBT 3.3 supports 500 Cisco CMTS headends, with 40,000 cable modems per Cisco CMTS. CBT 3.3 supports 50 simultaneous client browser sessions or users.
- CBT 3.3 supports the new Cisco uBR10-MC5X20H broadband processing engine for the Cisco uBR10012 router.
- CBT 3.3 supports DOCSIS 3.0 Wideband Channel Bonding on the Cisco uBR10012 router.

Enhanced Hardware Server and Client Support

Windows Systems

Windows systems supported include Windows 2000, Windows XP, and Windows XP Workstation with Linux Enterprise Edition.

UNIX Server Systems with Solaris

The following environment supports 10 Cisco CMTS headend systems:

- UNIX Server Sun Fire Systems with Solaris 10
- Sun Fire V100 server: small
- UltraSPARC-IIi processor: one at 550 MHz
- Memory: 256 MB (one 256-MB DIMM)
- 7200 RPM IDE disk drive: one at 80 GB

The following environment supports 50 or 100 Cisco CMTS headend systems:

- Sun Fire V210 server: Medium
- UltraSPARC IIIi Cu processor: two at 1.34 GHz
- Layer 2 cache per processor: 1 MB
- Memory: 2 GB (four 512-MB DIMMS)
- 10000 RPM Ultra 3 SCSI LVD disk drive: two at 73 GB

The following environment supports 500 Cisco CMTS headend systems:

- Sun Fire V440 server: Small
- UltraSPARC IIIi Processor: two at 1.593 GHz
- Internal cache per processor: 1 MB
- Memory: 4 GB (eight 12-MB DIMMS)
- 10000 RPM Ultra320 SCSI disk drive: four at 73 GB

UNIX Server Systems with Linux

The following environment supports 10, 50, or 100 Cisco CMTS headend systems:

- Linux Red Hat Enterprise Edition workstation
- Pentium 4, 3.2 gigahertz (GHz) processor or higher
- 2-GB DRAM
- 20-GB disk space

PC Server Systems for Windows

The following environment supports 10, 50, or 100 Cisco CMTS headend systems:

- Windows 2000, or Windows XP workstation
- Pentium 4, 3.2 gigahertz (GHz) processor or higher
- 2-GB RAM
- 20-GB disk space

UNIX Client Machine with Solaris

The following client system supports CBT 3.3 on Solaris:

- Sun Fire V100 server: Small
- UltraSPARC-IIi processor: one at 550 MHz
- Memory: 256 MB (one 256-MB DIMM)

UNIX Client Machine with Linux

The following client system supports CBT 3.3 with Linux:

- Pentium 4, 3.2 gigahertz (GHz) processor or higher
- 1-GB RAM
- Red Hat 10 or 9

PC Client Machine with Windows

The following client system supports CBT 3.3 with Windows:

- Windows 2000, or Windows XP workstation
- 1-GB RAM
- Pentium 4, at 3.2 GHz or higher

Enhanced Support for Operating Systems and Web Server Applications

CBT 3.3 offers enhanced support for the following operating systems and web server software environments:

- DST patch
- Java Runtime Environment (JRE)
- Linux operating system

- Solaris operating system
- Tomcat application server
- Windows operating system

DST Patch for Operating Systems

CBT 3.3 introduces the operating system patch associated with recent Daylight Savings Time (DST) requirements.

Java Runtime Environment in CBT 3.3

CBT 3.2 supported the Java Runtime Environment (JRE) through JRE version 1.4.1. CBT 3.3 comes with Java J2SE Runtime Environment 5.0 embedded in it.

We recommend upgrading to JRE 5.0 on the client side to benefit from the latest enhancements, caveat resolutions, and security features, specifically for the Solaris platform.

Linux Operating System

CBT 3.3 introduces support for Red Hat Enterprise Linux products and the Red Hat Desktop operating system. We recommend upgrading from prior Linux versions, such as Linux Red Hat 7, 8, and 9, as these prior versions have reached the end of their support lifetimes.

Solaris Operating System

CBT 3.3 introduces support for the Solaris operating system through Solaris 10. CBT 3.2 supported Solaris through Solaris 8. We recommend upgrading to Solaris 10 for use with CBT 3.3 to gain support for high-performance server machines that require Solaris 10, and related CBT 3.3 enhancements.

Tomcat Application Server

CBT 3.3 introduces upgraded support for the Tomcat Application Server. With the prior CBT 3.2 version, support was limited to jakarta-tomcat-4.1. CBT 3.3 extends support to include apache-tomcat-5.5.15. The latest Tomcat version introduces scalability and reliability enhancements supported in CBT 3.3, performance optimizations, and reduced garbage collection.

CBT 3.3 implements the latest Tomcat application upgrade, and it is not necessary to download this application server separate from an upgrade to CBT 3.3.

Windows Operating System

CBT 3.3 supports the latest Windows operating systems from Microsoft, such as Windows 2000 or Windows XP. No additional Windows upgrades are required for CBT 3.3.

SNMP MIBs

CBT 3.3 introduces support for additional Management Information Bases (MIBs) and related network management enhancements.

- The following new MIB objects are not contained in the CISCO-PROCESS-MIB for CBT 3.2:
  - cpmCPUTotal5secRev Gauge32
  - cpmCPUTotal1minRev Gauge32
  - cpmCPUTotal5minRev Gauge32

- CBT 3.3 adds SNMP CPU control, with administrative privilege to configure the number of CBT spectrum users.

- CBT 3.3 supports security enhancement for the SNMP community string.

- CBT 3.3 is more robust in clearing the spectrum request entries in the ccsSpectrumRequestTable MIB, applicable upon improper CBT shutdown or the *remove* scheduled event option.

- CBT 3.3 resolves instances in which the ccsSNRRequestEntry MIB was not cleared properly when the CBT server was shut down in earlier versions of CBT.

- CBT 3.3 introduces a new and efficient method for the checkCMTSCPU() MIB to obtain CPU utilization of broadband processing engines.

- CBT 3.3 replaces the obsolete MIB object supporting Subscriber Traffic Management (STM) with the latest objects in the CISCO-CABLE-QOS-MONITOR-MIB, supporting the Cisco IOS STM feature after Cisco IOS Release 12.3(9a)BC.

  In CBT 3.2, the STM feature obtained Enforce Rules and Get All Violators with the following obsolete MIB objects:

  - ccqmCmtsEnfRuleByteCount

  - ccqmEnfRuleViolateByteCount

  These obsolete MIB objects are not used by CBT 3.3, in which STM tools are compatible with the latest MIB changes supported in Cisco IOS, through release 12.3(21)BC.

Refer to the following document on Cisco.com for detailed information about MIBs support in relation to CBT 3.3:

- *Cisco CMTS Universal Broadband Series Router MIB Specifications Guide*

  http://www.cisco.com/en/US/products/hw/cable/ps2209/products_technical_reference_book09186a00807d2941.html

Trace Window Enhancements

- CBT 3.3 adds Trace Window configuration parameters.

- CBT 3.3 supports additional sorting functions in the Trace Window, by multiple fields.

- CBT 3.3 supports the disabling of the auto-select feature in the Trace Window.

Refer to the *Cisco Broadband Troubleshooter Release 3.3 User Guide* for additional information about using the Trace Window.

Troubleshooting Enhancements

The Flap List Analyzer management functions are enhanced to support detection of flap lists that may comprise hundreds of cable modems. In cases in which the number of cable modems exceeds 2,000, CBT 3.3 prompts you of the quantity of cable modems, and provides you with the option to either continue or cancel the Flap List Analyzer functions. CBT 3.3 shows the number of cable modems within the Flap List Analyzer.

Resolved Caveats for CBT 3.3

Table 2 describes CBT 3.3 enhancements that resolve prior caveats in earlier CBT releases.

Table 2   Resolved Caveats in CBT 3.3

DDTS ID Number	Description
CSCsb95957	CBT 3.3 updates the MIBs by which the Subscriber Traffic Manager feature obtains Enforce Rules and Violator Status. CBT 3.3 replaces the obsolete MIB object supporting Subscriber Traffic Management (STM) with the latest objects in the related MIB. This enhancement is supported for the Cisco IOS STM feature after Cisco IOS Release 12.3(9a)BC.
	Refer to the following section or document on Cisco.com for detailed information about MIBs support in relation to CBT 3.3:
	• "SNMP MIBs" section on page 5
	• *Cisco CMTS Universal Broadband Series Router MIB Specifications Guide*
	http://www.cisco.com/en/US/products/hw/cable/ps2209/products_technical _reference_book09186a00807d2941.html
CSCsc09577	CBT 3.3 introduces and supports a mechanism by which scheduled polling events do not consume CPU processing, as was the case in prior CBT releases. The prior issue related to the SpecDataMaxCPU parameter being exceeded.
	The SpecDataMaxCPU parameter now represents a gateway check that stops new CBT requests from being created if the CPU utilization exceeds a certain threshold.
CSCsc09669	CBT 3.3 introduces a new mechanism by which network administrators may control Spectrogram settings, such as upper and lower frequencies, polling intervals, and step size. These functions are supported in Trace Window Spectrogram displays. Prior releases of CBT did not support these Spectrogram administrative controls and configuration parameters.
	Refer to the "Configuring Administrative Parameters for Spectrum Analysis" section on page 17 for additional information.
CSCsc13740	CBT 3.3 introduces support for checking CPU utilization, and supports the associated SNMP MIBs that enable this function in the Trace Window. Refer to the following section or document on Cisco.com for related information:
	• "SNMP MIBs" section on page 5
	• *Cisco CMTS Universal Broadband Series Router MIB Specifications Guide*
	http://www.cisco.com/en/US/products/hw/cable/ps2209/products_technical _reference_book09186a00807d2941.html
CSCsc13923	CBT 3.3 retains the security of hidden passwords, even when the Password field is highlighted.
CSCsc29221	CBT 3.3 correctly reports the specific CBT release that must be installed when valid licensing error messages are displayed.
CSCsc29256	CBT 3.3 enables you to remove a scheduled polling event that is running, without having to stop it first. CBT 3.3 removes the associated row in the ccsSpectrumRequestTable display, even when the polling event is not stopped prior to its removal.

Table 2   Resolved Caveats in CBT 3.3 (continued)

DDTS ID Number	Description
CSCsc29262	CBT 3.3 resolves occurrences, in prior CBT releases, of a counter locking problem in the Trace Window display, in circumstances in which CBT was closed without first stopping or closing the Trace Window.
CSCsc74283	CBT 3.3 resolves occurrences, in prior CBT releases, in which the ccsSNRRequestEntry MIB object was not cleared properly, when the CBT server was shut down.
CSCsd47616	CBT 3.3 introduces support for checking cable interface line card CPU utilization, and the associated SNMP MIBs that enable this function in the Trace Window. Refer to the following section or document on Cisco.com for related information: • "SNMP MIBs" section on page 5 • *Cisco CMTS Universal Broadband Series Router MIB Specifications Guide* http://www.cisco.com/en/US/products/hw/cable/ps2209/products_technical_reference_book09186a00807d2941.html
CSCse00909	CBT 3.3 supports the latest Cisco uBR10-MC5X20S/U/H broadband processing engines (BPEs).
CSCse38589	CBT 3.3 resolves occurrences, in prior CBT releases, in which the graphical user interface (GUI) would become inaccessible when stopping the application. This prior issue arose when the poller was run for a few hours, and related to Tomcat processes and Telnet session timeouts.
CSCsf96230	CBT 3.3 disables the auto-select behavior for entries in the Trace Window, and CBT 3.3 introduces the ability to sort and reverse-sort all fields of the Trace Window Criteria dialog box. Refer to the *Cisco Broadband Troubleshooter Release 3.3 User Guide* for additional information.
CSCsg32141	CBT 3.3 introduces support for CMTS hostnames to include dotted notation. Refer to the "Administrative and Security Enhancements" section on page 2 for additional information.
CSCsg39114	The GS Analyzer tool of CBT 3.3 adds more efficiency to the maintenance and processing of information in relation to the cdxIfCmtsCmStatusLastResetTime MIB object. Prior to CBT 3.3, related limitations had a negative impact on Flap List troubleshooting on Cisco CMTS headends supporting 7,200 more cable modems.
CSCsg46989	CBT 3.3 introduces a standard feature by which Cisco CMTS headend systems are listed first by name, then by IP address. Prior CBT versions did not support CMTS hostnames. Refer to the "Administrative and Security Enhancements" section on page 2 for additional information.
CSCsg74720	CBT 3.3 introduces enhanced Flap List Analyzer functions that provide warnings about large numbers of cable modems on a given Cisco CMTS. Refer to the "Troubleshooting Enhancements" section on page 6 for additional information.

Upgrading to CBT 3.3

This section describes installation, upgrade, and patch installation procedures for CBT 3.3. This section contains the following procedures:

- Downloading and Upgrading CBT 3.3, page 9
- Requirements for Installing DST Operating System Patches, page 11

Downloading and Upgrading CBT 3.3

Use the following steps to download and to install CBT 3.3 on a system with the Linux, Solaris, or Windows operating systems.

Using TCP Ports for CBT 3.3 Upgrade and Operation

Note Cisco implements a default TCP port of 8105 on the licensing server for CBT 3.3 in XML script. This prevents port conflict with other applications. If you require a TCP port other than the default of 8105, then set the TCP port after installation of CBT 3.3, but prior to licensing. Refer to the "CBT 3.3 Download and Upgrade" section on page 9.

We recommend ports other than 8005, 8080, 9080, 9443, or 9082.

The following are the default ports used by CBT 3.3:

- Port 8105: Java Virtual Machine (JVM) server port
- Port 9080: non-SSL HTTP port
- Port 9443: SSL HTTP port
- Port 9082: Apache JServ Protocol (AJP) 1.3 Connector
- Port 2640: For Sybase Database connectivity.
- Port 8020: For Poller operation

CBT 3.3 uses the following port ranges for spectrum operations. Spectrum events such as Trace Window, Spectrogram, CNR Trending, and the Generic Query use a specified range of port numbers for operation.

- For both Trace Window events and the Spectrogram events, the port numbers range from 2100 to 2500.
- For the Spectrum tools, such as CNR Trending, port numbers range from 3100 to 3500.
- For the Diagnostic tools, such as Generic Query, the port numbers range from 5100 to 5500.
- The usage of these spectrum port numbers should be in increments of 1, meaning the first Trace Window launched obtains port number 2100, and the next Trace Window obtains port 2101. The next Spectrogram window would be port 2102, and continuing upward to port 2500.

CBT 3.3 Download and Upgrade

Step 1 Download CBT 3.3 software for the desired platform from Cisco.com to your local directory <CBT3.3_DOWNLOAD_DIR>.

- Cisco.com download location:

  http://www.cisco.com/cgi-bin/tablebuild.pl/cbt

- CBT 3.3 download entails the following platform-specific files:
  - There is a single file for the Solaris platform—CBT33-Solaris.tar.gz
  - There is a single file for the Linux platform—CBT33-Linux.tar.gz
  - Platform files for the Windows platform—CBT33-Win.exe
  - CBT 3.3 Release Notes—CBT33ReleaseNotes.pdf

Step 2 Extract the software. For Solaris and Linux, use the commands below. For Windows 2000 and Windows XP, skip to Step 3.

- Solaris:
  a. **cd** <CBT3.3_DOWNLOAD_DIR>
  b. **gunzip CBT33-Solaris.tar.gz**
  c. **tar xvf CBT33-Solaris.tar**

- Linux:
  a. **cd** <CBT3.3_DOWNLOAD_DIR>
  b. **gunzip CBT33-Linux.tar.gz**
  c. **tar xvf CBT33-Linux.tar**

Step 3 If there is a previous CBT installation (CBT 2.x, CBT 3.0 or CBT 3.2), uninstall it using the following procedures; otherwise, skip to Step 4.

- Solaris: cd <CBT3.x_DOWNLOAD_DIR> ./uninstall
- Linux: cd <CBT3.x_DOWNLOAD_DIR> ./uninstall
- Windows:
  - Remove the existing CBT installation by clicking **Start**, **Settings**, **Control Panel**, **Add or Remove Programs**, and removing CBT 3.x following the Windows prompts.
  - In Windows Explorer, navigate to the directory that was uninstalled, and verify it was removed. If necessary, delete the CBT3x-Win.exe in <CBT3.x_DOWNLOAD_DIR> file and related files if they remain.

Step 4 Install CBT 3.3. Use the following commands, according to platform.

- Solaris: **cd** <*CBT3.3_DOWNLOAD_DIR*> **./install**
- Linux: **cd** <*CBT3.3_DOWNLOAD_DIR*> **./install**
- Windows:
  - In Windows Explorer, double-click **CBT33-Win.exe** in <*CBT3.3_DOWNLOAD_DIR*>.
  - Select the default answers to the installation questions.

> ✎
> **Note** A demonstration version of CBT 3.3 is now running (a license is not included in the Cisco.com download). To make the software fully functional, obtain a license for CBT 3.3 from Cisco Systems. See Step 5.

Step 5 Purchased copies of CBT no longer include a software CD, but include a license certificate with a PAK key. This PAK key generates the necessary license file from the following websites, and the software is downloaded from Cisco Connection Online.

- Use this site if you are a registered user of Cisco Connection Online:

  www.cisco.com/go/license

- Use this site if you are not a registered user of Cisco Connection Online:

  www.cisco.com/go/license/public

✎

Note Save the license file with the name "License" from the Cisco Server location cited in an earlier step, and follow the instructions in Step 6 to copy it to the appropriate directory for use by CBT 3.3.

Demonstration copies are available either via the Internet, or as an ordered accessory for a universal broadband router product. The copies supplied with a universal broadband router product include a demo license certificate with a PAK key. The copy available from the Internet uses a registration page where the PAK key is emailed to you.

Step 6 Use the following commands to copy the license to the license directory and restart CBT 3.3.

- Solaris:

  1. **cp License /opt/CSCOcbt/httpServer/webapps/ROOT/WEB-INF/classes/lic**

  2. **/opt/CSCOcbt/bin/stop_app**

  3. **/opt/CSCOcbt/bin/start_app**

- Linux:

  1. **cp License /opt/CSCOcbt/httpServer/webapps/ROOT/WEB-INF/classes/lic**

  2. **/opt/CSCOcbt/bin/stop_app**

  3. **/opt/CSCOcbt/bin/start_app**

- Windows:

  1. **copy License <CBT3.3_INSTALLATION_DIR>\httpServer\webapps\ROOT\WEB-INF\classes\lic**

  2. Click **Start, Programs, Cisco Broadband Troubleshooter, Stop Troubleshooter**.

  3. Click **Start**, **Programs**, **Cisco Broadband Troubleshooter**, **Start Troubleshooter**.

✎

Note Once the CBT 3.3 license is installed and active, additional changes to the license are not supported. License changes disable an otherwise valid license.

Requirements for Installing DST Operating System Patches

CBT 3.3 requires that the latest operating system patches be installed for all platforms supported by CBT 3.3. Refer to the "Enhanced Support for Operating Systems and Web Server Applications" section on page 4 for additional information about supported platforms.

JRE OS-Level Requirements

CBT 3.3 supports the latest Java Runtime Environment (JRE 5.0) platform. However, the network administrator must ensure that all OS-level patches are installed to avoid system problems with CBT 3.3. This section describes patch requirements according to platform.

- Microsoft Windows Operating Systems:

  – See DST information at <Preparing for Daylight Saving Time changes in 2007> available at
    http://www.microsoft.com/windows/timezone/dst2007.mspx

- Linux Operating Systems:

  – For Red Hat Enterprise Linux 3 (RHEL3), see information at
    http://rhn.redhat.com/errata/RHEA-2005-655.html

  – For Red Hat Enterprise Linux 4 (RHEL4), see information at
    http://rhn.redhat.com/errata/RHEA-2005-656.html

- Sun Solaris Operating Systems:

  – See DST patch information for Sun Solaris 8, 9, and 10 at the following locations:

    Australia—#102178: Daylight Saving Time (DST) Changes for Australia (2006)
    http://sunsolve.sun.com/search/document.do?assetkey=1-26-102178-1

    United States (2007) and additional countries
    http://sunsolve.sun.com/search/document.do?assetkey=1-26-102178-1

Using CBT 3.3

CBT 3.3 introduces the following new procedures and enhanced configurations supported in release 3.3. These procedures are not supported in releases prior to CBT 3.3. Refer also to the "Related Documentation" section on page 23 for further CBT 3.3 documentation and configuration information.

General Procedures for CBT 3.3

CPU Procedures for CBT 3.3

Trace Window Procedures for CBT 3.3

Using SNMP MIBs in CBT 3.3

Cisco Broadband Troubleshooter (CBT) 3.3 uses the following SNMP MIBs in the Cisco IOS 12.3 BC Software Release train. Refer also to the "Resolved Caveats for CBT 3.3" section on page 7.

- RFC1213-MIB

- IANAifType-MIB

- IF-MIB
- SNMPv2-MIB
- SNMPv2-TC
- CISCO-SMI
- OLD-CISCO-CHASSIS-MIB
- CISCO-PRODUCTS-MIB
    - DOCS-IF-MIB
    - DOCS-IF-EXT-MIB
    - CISCO-CABLE-SPECTRUM-MIB
    - CISCO-DOCS-EXT-MIB
- CISCO-PING-MIB
- INET-ADDRESS-MIB
- SNMP-FRAMEWORK-MIB
    - DOCS-CABLE-DEVICE-MIB
    - CISCO-PROCESS-MIB
    - DOCS-QOS-MIB
    - ENTITY-MIB
    - CISCO-CABLE-QOS-MONITOR-MIB
    - CISCO-DOCS-REMOTE-QUERY-MIB

When extracting the downloaded CBT 3.3 file, these MIBs are placed by default in the following path:

> <CBT Install Directory>/httpServer/webapps/ROOT/WEB-INF/mibs

Note Not all the tables contained in these MIBs are used with CBT 3.3.

Generally, all read and create objects in the ccsSpectrumRequestTable and ccsSNRRequestTable can be set with spectrum management tools in CBT 3.3. These objects require a WRITE community string:

- ccsSpectrumRequestTable
    - ccsSpectrumRequestIfIndex
    - ccsSpectrumRequestMacAddr
    - ccsSpectrumRequestLowFreq
    - ccsSpectrumRequestUpperFreq
    - ccsSpectrumRequestResolution
    - ccsSpectrumRequestOperation
    - ccsSpectrumRequestStatus
- ccsSNRRequestTable
    - ccsSNRRequestMacAddr
    - ccsSNRRequestOperation
    - ccsSNRRequestStatus

For additional MIBs information for the Cisco CMTS, refer to the following resources on Cisco.com:

- *Cisco CMTS Universal Broadband Router MIB Specifications Guide*

  http://www.cisco.com/en/US/products/hw/cable/ps2209/products_technical_reference_book09186 a00807d2941.html

- *SNMP Object Navigator*

  http://www.cisco.com/pcgi-bin/Support/Mibbrowser/unity.pl

Using Subscriber Traffic Management with CBT 3.3

To use the Subscriber Traffic Management (STM) feature of CBT 3.3, the **cable qos enforce-rule** command on the Cisco CMTS must be used with a QoS profile that is not created by the cable modem. Any in-use QoS profile, such as one created by a cable modem, can be turned into a management profile.

✎ **Note**   STM is newly supported on the MC16U, MC16X, MC28U, MC28X, and MC5X20S/U/H line cards with CBT 3.3. STM data is now enabled with CBT 3.3.

To create a management profile, follow these steps:

	Command	Purpose
Step 1	Router# **show cable modem registered**	Finds the registered profiles on the CMTS. Find a current registered profile that has the features you need.
Step 2	Router# **configure terminal**	Enters global configuration mode.
Step 3	Router (config)# **cable qos profile** *number*	Enters the QoS profile number of the registered profile that has the features you need.
Step 4	Router (config)# **exit**	Exits global configuration mode.

Disabling or Enabling Password Text Display

CBT 3.3 enables you to display password text, or to disable password text display according to your needs. By default, this parameter is set to YES. If you set the corresponding parameter to NO, CBT does not display password text when the Password field is displayed.

Perform the following steps to disable or to enable password text display for one or more user names.

Step 1   Open the GUNSLINGER.INI file available in the CBT server machine.

- For Solaris and Linux, the GUNSLINGER.INI file is under the directory /opt/CSCOcbt/httpServer/webapps/ROOT or <CBT_Install_Directory>/httpServer/webapps/ROOT.

- For Windows, the GUNSLINGER.INI file is under the directory C:\Program Files\Cisco Systems\Cisco Broadband Troubleshooter\httpServer\webapps\ROOT\ or <CBT_Install_Directory>\httpServer\webapps\ROOT\.

Step 2   Change the value of the ShowPasswordWhileEditing parameter to YES or NO as per your need.

- For YES, CBT 3.3 does not display the password text when the password field is highlighted.

Step 3   Save the GUNSLINGER.INI file with your changes.

Step 4   Restart CBT 3.3.

Enabling Instantaneous CPU Assessment for Spectrum Polling

CBT 3.3 enables the option of preventing excessive CPU consumption in circumstances in which the Trace Window, Spectrogram functions, or Scheduled Polling features might otherwise exceed CPU bandwidth.

CBT has provisions to instantaneously check the CPU utilization and prevents the spectrum operation if the CPU utilization exceeds the CPU thresholds (value of SpecDataMaxCPU parameter).

Perform these steps to enable or disable CPU assessment in the Trace Window Criteria dialog box, the Spectrogram Criteria dialog box, or the Spectrum Data Clients dialog box before launching the spectrum event.

DETAILED STEPS

Step 1   Launch CBT 3.3.

Step 2   Launch the desired window in which to configure this change.

- For Trace Window changes, from the Spectrum Tools menu, choose **Trace Window**. The Trace Window Criteria dialog box appears. Proceed to the next step.

- For Spectrogram changes, from the Spectrum Tools menu, choose **Spectrogram**. The Spectrogram Criteria dialog box appears. Proceed to the next step.

- For Spectrum Data Scheduler changes, from the Spectrum Tools menu, choose **Spectrum Data Clients**. The Spectrum Data Clients dialog box appears. Proceed to the next step.

Step 3   Select the `Check CPU Util` check box. Only when the check box is selected is the field enabled to enter the number of spectrum sweeps that should be done for every CPU utilization check. If periodic check of CPU utilization is not necessary, then deselect this option and proceed. If not selected, the CPU utilization is checked only once before the launch of the spectrum operation. Refer to Figure 1.

Figure 1   Check CPU Util Dialog Box

Step 4   When the Check CPU Util check box is selected, enter the number of sweeps in which CPU utilization should be checked. The default value is 10.

This setting means that the CPU utilization is checked and compared with the SpecDataMaxCPU parameter. Upon positive results, the spectrum operation gets started. The spectrum data is collected continuously with the specified poll interval.

One sweep corresponds to a single polling of spectrum data. After 10 such polling events, CBT again checks the CPU Utilization and compares it with the SpecDataMaxCPU parameter. If the results are positive, the spectrum operation continues; otherwise, the continuous query is stopped. If the number of sweeps is 1, then the CPU utilization is checked before every polling of spectrum data.

Step 5   Continue with the launch of the spectrum operation.

Viewing Trace Windows

Some browsers give the user the ability to stop pop-up windows from being launched by the browser. CBT 3.3 normally launches a new window to display the trace and spectrum data charts. If the data chart window does not appear and the browser is configured to stop pop-up windows from launching, you can configure CBT 3.3 to display data charts within the browser window.

To configure CBT 3.3 to display data charts within the browser window, perform the following steps:

Step 1   Select **Configuration > System** in the CBT 3.3 menu.

Step 2   In the System Configuration screen, deselect the **Use Popup** check box.

Sorting Support in the Trace Window

CBT 3.3 introduces sorting support for the List fields in the following windows or dialog boxes:

- Spectrum Data Scheduler
- Trace Window Criteria
- Spectrogram Criteria
- CNR Analysis Criteria
- CNR Trending Criteria

To change the order of sorting, perform the following steps:

Step 1   Select the desired page:

- **Configuration > Scheduler > Spectrum Data > Spectrum Data Scheduler** page
- **Spectrum Tools > Trace Window > Trace Window Criteria** page
- **Spectrum Tools > Spectrogram > Spectrogram Criteria** page
- **Spectrum Tools > CNR Analysis > CNR Analysis Criteria** page
- **Spectrum Tools > CNR Trending > CNR Trending Criteria** page

Step 2   Click on the label of the desired field, and data is sorted in ascending or descending order. Each click of the label reverses the current order displayed.

Mapping Hostnames from Applet to Servlet

CBT 3.3 introduces support for hostname-based communications between applet and servlet on the network, in addition to sustaining IP-based communications, as with the prior CBT 3.2.

In CBT 3.2 all the communication between the applet and the servlet was based only on the IP address of the server. Every request and response between the applet and servlet had the IP address in the URL. CBT 3.3 removes this limitation, to support both hostnames and IP addresses.

This mapping configuration procedure changes the UseHostName parameter of the GUNSLINGER.INI file. By default, this value is NO in CBT 3.3. Changing this value to YES enables hostname-based communication between applet and servlet, and removes IP addresses from corresponding displays and processing.

Some Web proxy functions only allow hostname-based IP communication, and otherwise drop communications with IP addresses in the URL. This feature is helpful in such cases.

Prerequisites

This procedure requires that applet and servlet hostnames be established and otherwise functional on the network prior to mapping hostnames in CBT 3.3. Both the client and server should be able to resolve the hostname of the CBT server machine.

Perform these steps to map hostnames from applet to servlet.

Step 1 Open the GUNSLINGER.INI file available in the CBT server machine.

- For Solaris and Linux, the GUNSLINGER.INI file is under the directory /opt/CSCOcbt/httpServer/webapps/ROOT or <CBT_Install_Directory>/httpServer/webapps/ROOT.

- For Windows, the GUNSLINGER.INI file is under the directory C:\Program Files\Cisco Systems\Cisco Broadband Troubleshooter\httpServer\webapps\ROOT\ or <CBT_Install_Directory>\httpServer\webapps\ROOT\.

Step 2 Change the UseHostName parameter to YES or NO depending on your need.

- YES enables hostname-based communications.

- NO implements IP-address-based communications.

Step 3 Save the GUNSLINGER.INI file with your changes.

Step 4 Restart CBT 3.3.

Configuring Administrative Parameters for Spectrum Analysis

CBT releases prior to CBT 3.3 support options for spectrum operation parameters, and CBT 3.3 continues support for these parameters. CBT 3.3 introduces support for administrators to configure upper and lower limits for multiple fields in the Spectrum Operations windows. CBT 3.3 introduces additional configurable parameters in the SPECTRUM.INI file.

Perform the following steps to define administrative upper and lower limits in Spectrum Operations windows:

Step 1 Open the SPECTRUM.INI file available in the CBT server machine.

- For Solaris and Linux, the SPECTRUM.INI file is under the directory /opt/CSCOcbt/httpServer/webapps/ROOT or <CBT_Install_Directory>/httpServer/webapps/ROOT.

- For Windows, the SPECTRUM.INI file is under the directory C:\Program Files\Cisco Systems\Cisco Broadband Troubleshooter\httpServer\webapps\ROOT\ or <CBT_Install_Directory>\httpServer\webapps\ROOT\.

Step 2 Change the default settings for as few or as many parameters as desired. Listed below are default values, and acceptable parameters, wher e applicable:

- SpecEventStartFreqMinValue=5
- SpecEventStartFreqMaxValue=65
- SpecEventStopFreqMinValue=5
- SpecEventStopFreqMaxValue=65
- SpecEventCenterFreqMinValue
- SpecEventCenterFreqMaxValue
- SpecEventFreqSpanMinValue
- SpecEventFreqSpanMaxValue
- SpecEventDataPointsMinValue
- SpecEventDataPointsMaxValue
- SpecEventPollIntervalMinValue
- SpecEventPollIntervalMaxValue
- SpecEventStepSizeMinValue
- SpecEventStepSizeMaxValue
- SpecEventSamplesMinValue
- SpecEventSamplesMaxValue

You can configure the upper and lower limit for the start, stop frequency, poll interval, step size and data points. While entering such data spectrum parameters, CBT 3.3 sustains native-level validation, and additionally, CBT 3.3 validates entries with respect to the newly configured limits in the SPECTRUM.INI file. The following list describes various fields and supported ranges for validation in a Spectrum Event:

- Start Frequency—Should be in the range of 5 to 65, with the value representing MHz. A decimal value is supported.

- Stop Frequency—Should be in the range of 5 to 65, with the value representing MHz. A decimal value is supported.

- Center Frequency and Frequency Span—The frequency span cannot be greater than these results:
  - minimum—(center frequency - 5) x 2
  - minimum—(65 - center frequency) x 2

  Validation is performed on Center Frequency and Frequency Span in the following way:
  - Start and stop Frequencies are calculated.
  - startFreq = centerFreq - (freqSpan/2)
  - stopFreq = centerFreq + (freqSpan/2)

  As a result, these values should be in the range 5 to 65. In this way, both the fields are validated.

- Data Points—Should be an integer greater than 2, and are subject to the following additional range requirements, according to the cable interface line cards:
  - Should be in the range from 2 to 6001 for the MC5X20S/U/H BPE.
  - Different upper limits of Data Points for different cable interface line cards are as follows:
    - MC16S: 617
    - MC16U: 3001
    - MC16X: 3001

- MC28U: 3001
- MC28X: 3001
- MC5X20S: 5886
- MC5X20U: 6001
  - DataPoints with other cable interface line card combinations should result in a start and stop frequency range of 5 to 65.
- Poll Interval—Must be a positive integer.
- Step Size—Should be a positive integer not greater than 6000.

Note For any combination of the above-mentioned field values that you enter, the start and stop frequency should always be in the range 5 to 65.

Step 3 Save the SPECTRUM.INI file, and restart CBT 3.3.

CBT 3.3 also supports additional checking with respect to the administratively configured values in the SPECTRUM.INI file. When changing this file, all the field values should also be in the range specified, and saved to the SPECTRUM.INI file for non-default configurations.

Note If the value of the SpecEventPollIntervalMinValue parameter is set to 1, then only values above 1 are accepted in the Poll Interval dialog box. This configuration removes the bandwidth-consuming zero-second polling, which occurs if the value is set to zero.

Using Auto-Select in the Trace Window

CBT 3.3 does not select any given field in the Trace Window by default. To retrieve and display information for any given field in the Trace Window display, select the desired field.

Troubleshooting Tips for CBT 3.3

This section contains the following procedures for verifying and troubleshooting CBT 3.3:

Troubleshooting Continuous Sweep Spectrum Operation in CBT 3.3

A non-standard behavior has been observed in which the Continuous Sweep Spectrum Operation of CBT 3.3 fails, even in circumstances in which the Single Sweep Spectrum Operation remains functioning. One example would be the proper Trace Window single sweep operation, but with failed continuous wweep behavior in the Trace Window.

CBT 3.3 requires that the following processes and tasks be used for Continuous Sweep Spectrum Operation.

Step 1 Verify the TCP ports used by CBT 3.3 are as follows, as CBT uses these ports by default:

- Port 8105: JVM server port
- Port 9080: non-SSL HTTP port
- Port 9443: SSL HTTP port
- Port 9082: AJP 1.3 Connector
- Port 2640: For Sybase Database connectivity.
- Port 8020: For Poller operation

Refer also to the "Using TCP Ports for CBT 3.3 Upgrade and Operation" section on page 9.

Step 2 Implement the following TCP port ranges for spectrum operations. Spectrum events such as Trace Window, Spectrogram, CNR Trending, and the Generic Query use a specified range of port numbers for operation.

- For both Trace Window events and the Spectrogram events, the port numbers range from 2100 to 2500.
- For the Spectrum tools, such as CNR Trending, port numbers range from 3100 to 3500.
- For the Diagnostics tools, such as Generic Query, the port numbers range from 5100 to 5500.
- The usage of these port numbers would in increments of 1. That is, for the first trace window launched, the port number is 2100, and the next trace window port number 2101. For the next Spectrogram window, the port number is 2102 and so forth up to port 2500.

Changing Server Ports in XML Script

Cisco IOS Release 12.3(9a)BC changes the Tomcat server port in server XML script. The script is set to port 8105. This prevents possible port conflict when multiple Tomcat Web servers are running on the same workstation.

If required, perform the following steps to change the Tomcat server port in XML script to port 8105 and check for additional port conflicts:

Step 1 Edit the server.xml script in the following location:

/opt/CSCOcbt/httpServer/conf

Step 2 Check for all ports numbers that have conflicts with CBT and change all port numbers that have such conflicts. The following are correct ports for the specified functions:

- Port 8105: JVM server port
- Port 9080: non-SSL HTTP port
- Port 9443: SSL HTTP port
- Port 9082: AJP 1.3 Connector

Saving System Message Logs for Troubleshooting

When troubleshooting CBT 3.3, we recommend that message logs be saved and filtered in the following ways:

Step 1 To view saved message logs, click **Utilities** then **Message log** in the user interface.

This is a fixed-size log file that continuously removes the oldest entry as it is updated. This log file is not viewable using an editor (such as vi).

Step 2 Filter the message log entries by severity, by user, by module, or by date.

Step 3 To set the logging level, click **Configuration** then **Message Log** in the user interface. Setting the logging level helps to prevent unnecessary messages occupying the fixed-size log file.

For Solaris and Linux, the log file is located at /opt/CSCOcbt/httpServer/logs/catalina.out. This file is viewable with viewing utilities such as vi, Cat, Tail, or others.

Note The message log file grows in size. For Windows, these messages go to the console and a file is not created.

Verifying Installation Status on the CBT 3.3 Server

The status of the installed CBT 3.3 server can be verified with the following steps.

Step 1 Verify that there are no exceptions in the catalina.out file located as follows:

- Solaris and Linux: /opt/CSCOcbt/httpServer/logs/

- Windows: The CBT 3.3 console

Step 2 Verify the dbeng8 process is running:

- Solaris and Linux:

```
ps -ef|grep dbe
root 26449 1 0 Aug 18 ? 0:24 dbeng8 -x tcpip{ServerPort=2640} -q -ud -s local0 -m -c
16M -n cbtdbengine /opt
```

- Windows: There is a Sybase icon shown as a running process.

Step 3 Verify the following Java processes are running:

- Solaris and Linux:

```
ps -ef|grep java
root 26478  1 0 Aug 18 ?  0:39 /opt/CSCOcbt/jre/bin/java -DCBTpoller -cp
/opt/CSCOcbt/httpServer/webapps/ROOT/

root 26489 1 0 Aug 18 ?  148:55 /opt/CSCOcbt/jre/bin/java
-Djava.endorsed.dirs=/var/CSCOcbt/httpServer/common/e
```

✎
Note   Linux displays threads; therefore, there are many Java entries.

- Windows: Use the command console for Tomcat and the CBT poller to view log messages.

Verifying the CBT 3.3 License

Perform the following steps to verify the CBT 3.3 installation license:

For Solaris and Linux, perform these steps:

1. Verify that the license is present and the file is correct in the following location:

   /opt/CSCOcbt/httpServer/webapps/ROOT/WEB-INF/classes/lic/License

2. Log in and allow for error prompts to identify any issues.

3. Scan the catalina.out file for error messages in the following location:

   /opt/CSCOcbt/httpServer/logs/ for error messages

For Windows, perform these steps:

1. Verify that the license is present and the file is correct in the following location:

   INSTALLATION_DIR\httpServer\webapps\ROOT\WEB-INF\classes\lic\License

2. Log in and allow for error prompts to identify any issues.

3. Scan the command console for tomcat and see if there are error messages in the console.

Related Documentation

The following sections provide references related to CBT 3.3.

Related Documents

Related Topic	Document Title
CBT 3.3	• *User Guide for Cisco Broadband Troubleshooter Release 3.3* http://www.cisco.com/en/US/products/sw/netmgtsw/ps530/products_user_guide_list.html • CBT 3.3 Online Help—available with licensed installation of CBT 3.3
Cisco IOS Release Notes for Cisco Universal Broadband Routers	• *Release Notes for Cisco uBR10012 Universal Broadband Router for Cisco IOS Release 12.3 BC* http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/prod_release_note09186a0080326360.html • *Release Notes for Cisco uBR7200 Series for Cisco IOS Release 12.3 BC* http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/prod_release_note09186a00803265f8.html • *Release Notes for Cisco uBR7100 Series for Cisco IOS Release 12.3 BC* http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/prod_release_note09186a0080771b95.html

Standards

Standard	Title
DOCSIS	CBT 3.3 conforms to DOCSIS-compliant features and standards supported in Cisco Broadband Cable IOS releases, and CableLabs DOCSIS specifications at this online location: • CableLabs DOCSIS http://www.cablemodem.com/

MIBs

MIB	MIBs Link
SNMP MIBs for the Cisco CMTS	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs Refer also to this document: • *Cisco CMTS Universal Broadband Series Router MIB Specifications Guide* http://www.cisco.com/en/US/products/hw/cable/ps2209/products_technical_reference_book09186a00807d2941.html

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

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