How to trace the Cisco Codec

TC & TE

D14301 revision 7
May 2011

Contents

1. Introduction

This document describes the process of how to collect relevant logs for system crashes, interoperability issues and problems with placing a call, check configuration etc for units running TC or TE software like the CISCO C-Series Codecs, the EX90 and the E20.

2. How to collect system configuration, status and settings

Collect system configuration

Log in to the system as 'admin' using Telnet, RS-232 or SSH (secure shell). Note! Telnet is disabled by default. To get the system configuration execute the following command:

xConfiguration

The configuration will now be listed. Please include this with any issues being escalated to CISCO.

Collect system status

Log in to the system as 'admin' using Telnet, RS-232 or SSH (secure shell). Note! Telnet is disabled by default. To get the system status, execute the following command:

xStatus

The status will now be listed. Please include this with any issues being escalated to CISCO.

To only collect information about packet loss (for onsite testing) you can poll this information using the command:

xStatus diagnostics

Other useful xStatus commands:

xStatus Network

xStatus MediaChannels

Always include xConfiguration and xStatus when escalating an issue!

Backup system configuration

Log in as root using WinSCP, navigate to the folder: '/mnt/base/active/'. Now copy the file 'config.db' and store it somewhere safe. Removing this file and rebooting the system will cause the system to boot up with factory default settings. When you need to restore the configuration copy the backup of the file back to the above location and reboot the system. The system will now boot up with the previously stored settings.

Note: From TC4.x the 'root' user is disabled by default. You must log in as admin to enable the root user using the following command: '*systemtools rootsettings on <desired_password>*' *systemtools rootsettings on* will enable root with no password

3. How to collect event logs

The system will constantly collect information about various part of the system like audio, video, system etc and store this info in various event logs available on the system. In the event of the system experiencing major errors, it is likely that these events are stored in one of these logs. To collect these logs please log into the web interface of the unit: http://<ipaddress of my system>, and click on the link 'Logs' and you will see:

Current log files: Uncompressed event log files for various parts of the system. These are log files currently running for all events until the next reboot.

Historical log files: Compressed log files, each log file will include a similar list of files as you can see under 'current log files'. When you boot the system, the 'current log files' will be compressed and stored as 'log.tar.gz'. During the next boot, 'log.tar.gz' will move to one of the logfiles 'Log 0 – Log 9'. These are rotating log files. The date listed for these files will be the date the file was created.

When an issue needs to be escalated to CISCO, we will need the event log files. The simplest way to collect these files would be to:

A. If a major issue occurs, like no video, no audio, green window etc and the system does not reboot, then reboot the system and collect the file 'log.tar.gz'.

B. If a major issue occurs, causing the system to reboot, then collect the file 'log.tar.gz'

C. All logs file are listed with a date they were created, hence you can collect log files with issues that occurred some time back.

D. To find the date a log file was created for the E20 you must log in as root and issue the command: 'ls –la /config/logs'. This will help you to collect the relevant log files. The date listed, is the date the log file was created.

4. How to collect H.323 and SIP traces

The system can also be set up to provide H.323 and SIP logging similar to what could be provided using 'syslog' on CISCO MXP systems. When logging is turned on, this information will be stored in the application log. You will then gain the advantage of getting proper timestamps for all the logging.

It is also possible to get the output printed on the command line; however this will not give you any timestamps. You can use this method if you need to collect trace over a long period of time and hence you can store the collected trace on a local file on your computer.

NOTE! The trace commands below are case sensitive. You can get a list of the trace words by issuing the following command: log list.
You will then be able to check the correct spelling if you don't have this document by hand.

To start H.323 Logging (H.245, Q931, RAS and RTP statistics)

A. Log in as admin using ssh, telnet or rs-232, then issue the command:

   log ctx H323Packet debug 9
   log ctx RTPStatistics debug 3 (provides information about packet loss, jitter etc. Available from TC1.1)

B. Make the calls and collect the application log (described in point 3 above. Collect from Current).

C. Turn off the log by either rebooting the system or issuing the command:

   log ctx H323Packet debug off
   log ctx RTPStatistics debug off
   log level off (turns off logging to command line)

To get the output on the command line in addition to the application log, apply the following command (in addition to the commands above):

log filter ctx H323Packet

NOTE! In software versions earlier than TC2.1.2, *H323Stack* is used instead on *H323Packet*

To start SIP logging (get all SIP messages)

A. Log in as admin using ssh, telnet or RS-232, then issue the command:

   log ctx SipPacket debug 9
   log ctx RTPStatistics debug 3 (provides information about packet loss, jitter etc. Available from TC1.1)

B. Make the calls and collect the application log (described in point 3 above. Collect from Current).

C. Turn off the log by either reboot the system or issue the command:

   log ctx SipPacket debug off
   log ctx RTPStatistics debug off

To get the output on the command line in addition to the application log, apply the following command (in addition to the commands above):

log filter ctx SipPacket

SIP and H.323 logging can be combined if needed to trace both at the same time. Then you only need to enable the RTP statistics once. RTP statistics is optional but will provide useful information about packet loss, dropped packets, jitter etc. For now the application.log is limited to 1mb only. This storing space will hold approximately 18 minutes of logging before the call is wrapped and started all over

again. The first time a log is wrapped after boot it can be found here: /var/log/application.log.save. You can use WinSCP to collect this file. To make sure this possibility exist you will have to make sure the codec is booted before you start any tracing. Otherwise you will only be limited to 1 file. The second time the file is wrapped, the information will get lost.

Note: Tracing MUST be turned off when done. It's not recommended to let the tracing stay on when the system is used in production.

5. TCPDump

TCPdump can be used to obtain a network sniffer trace of all IP packets arriving into the codec. To start tcpdump you must log in as root to the system and execute the following command:

tcpdump -s 0 -U not port 22 -w /tmp/<filename.pcap>

This will create a file in the /tmp catalogue of the codec. You will have to copy this file across to your computer and open this file with WireShark. The file can be downloaded to your computer using for example WinSCP.

Following options can also be used:

-C 10 = File can be maximum 10Mb
-W 100 = Maximum 100 files should be created. If '-C 10' also is given, you can get 100 files of 10Mb each.

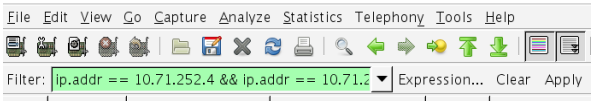
NOTE! The codec has limited storage space so you must be careful when creating the file. Once you are done, remember to delete the file from the /tmp catalog

Reducing size of capture file in Wireshark

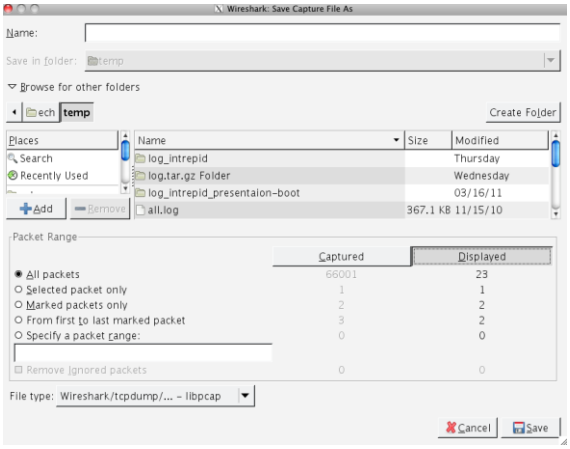
In order to reduce the size of the capture file it is possible to only save the packets that are relevant. This will vary from case to case, but would typically mean only selecting packets with the IP addresses of the Endpoints involved.

This is done by applying filters to the capture, as can be seen in the pic below. For example:

- For only SIP messages type "sip" followed by Apply
- For packets with ip 10.2.2.2 type "ip.addr == 10.2.2.2" followed by Apply



After the filter is applied you can save only the displayed messages by going to "Save As…" and in the box that appears selecting "Displayed". Only the messages that are displayed with the filter that you have applied will be saved this way.



6. Other

How to use ping and traceroute:

Log in as root and execute the following command:

ping –s 1400 –R <ip.address.to.destination>

The –s option will specify the packetsize used in the ping request. In the above example you will use 1400 bytes.
The –R option will return the route from the ping request.

Check Ethernet statistics:

Log in as root and execute the following command:

ethtool -S eth0|less

Press Q to come back to the shell

Netstat to find connected ports:

Log in as root and execute the following command:

netstat eth0