# R&R Call Traces and RAW CDR retrieval & analysis

What are Call Traces?

Call traces are used for advanced troubleshooting, they are the most detailed information available about every call and call attempt that passed your system.

R&R makes call traces available in real-time. Please use them in lieu of using on-demand technical support. This will not only save you money, but can also save your time.
Should you need R&R support in understanding captured data, please send filtered capture along with system CDR to tech@r-rtele.com

Where traces are collected

Packets collected on border of R&R network

Your system:

Sonus GSX9000

Internet Cloud
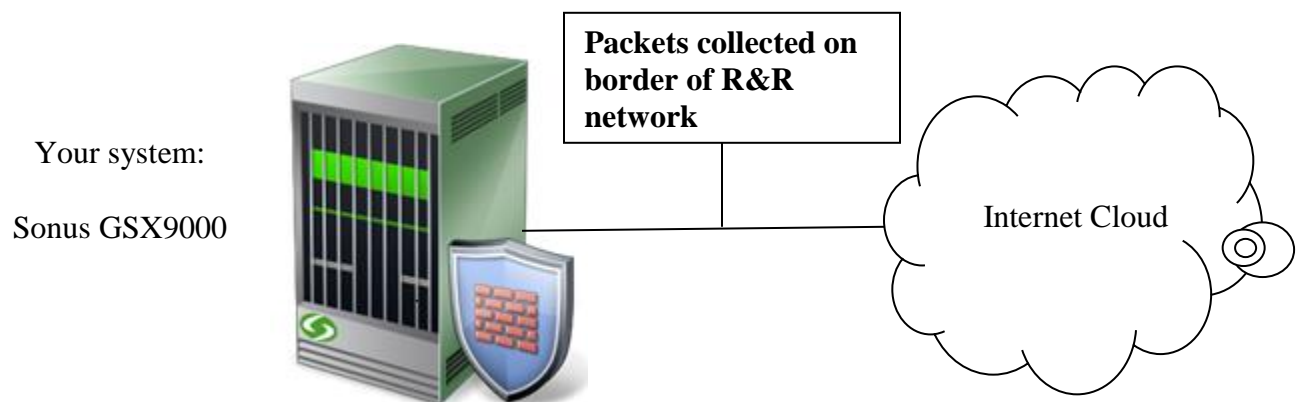
What's included in my traces

All traffic that reaches your IP address except RTP streams/voice packets. Since we capture all traffic at the border you will also see traffic that was filtered out by R&R firewall.

Analyzing Call Traces includes several steps:

1. Determine time period for Call Trace
2. Login to Secure FTP server and downloading files
3. Open captures and filter needed call
4. Analyze packet capture

Determine time period for Call Trace

In CDR Search find call that requires advanced troubleshooting. Mark exact time when call entered the system.

If you're looking for a call that did not appear in CDRs - find exact time when attempt was made.

If you wish to have trace for both start and end of the call you might need more than one file from SFTP server. Calculate when call ended and download file with appropriate time stamp. Merge the files (explained later).

CDR Generation Time Zones:

New York: Eastern Standard Time (using Daylight Saving time)
Frankfurt: GMT
Japan: JST (using Daylight Saving time)

What are RAW CDRs?

RAW CDRs are call accounting records that are collected directly from the Switch. They called RAW as they have not been modified in any way (for legal reasons).

RAW CDRs are coming in Sonus native format. It's a text format but impossible to read by a human. These files need to be reprocessed into a readable format by a Client. Sonus CDR structure is quite complex and each call may generate multiple records each having up to 200 fields.

Exported RAW CDRs include both completed and incomplete calls, they also may include all attempts to egress carriers (when enabled) so each ingress call can have multiple CDRs.

How do I convert RAW CDRs?

R&R existing Clients in good standing can request RAW CDR field definition from R&R sales team. Signing NDA is a prerequisite for this request.

You are free to decide which fields you want to parse and which language to build your parser in. Java, C#, C++ are the popular choices.

RAW CDR files are written to your SFTP folder as soon as Sonus is closing its accounting file. This depends on time of the day and time for new file generation can vary from 3 to 15 minutes.

RAW CDR naming convention

File name format:
"Partition abbrev"-"Switch name"-"CDR server flag"-"file_name".ACT.gz
>   "Partition abbreviation" = your 3 character abbreviation with R&R
>   "Switch Name" = internal naming of Sonus GSX
>   "CDR server flag" = **P** for call records from primary CDR server and **S** for
>   call records from secondary CDR server

Example:
SLN-GSX4-P-1000C60.ACT.gz was extracted from primary CDR server,
000C60.ACT accounting file

- First and last line as on source ACT file.
- Timestamp as on ACT file from which was generated.
- Record types: START, STOP, ATTEMPT, INTERMEDIATE.
- The resulted files are gzip (file extension "gz") compressed. Any Windows
decompression program should be able to extract the data.
- The CDR files are available 3 days. The files older than 3 days are
automatically deleted each day at 18:01 EDT.

Login to Secure FTP server and download files

To access folders with your traces please download free FTP Client, such as WinSCP http://winscp.net/eng/download.php

Install FTP client, obtain login information from R&R Service Representative and create Login Profile as shown below (WinSCP example)

Note that we use **port 2290** and SecureFTP (SFTP) protocol.

Also note that your access to FTP server is allowed based on IP you opened R&R User Interface with. If you logged in more than 24 hours ago you might need to restart GUI to refresh your session IP.
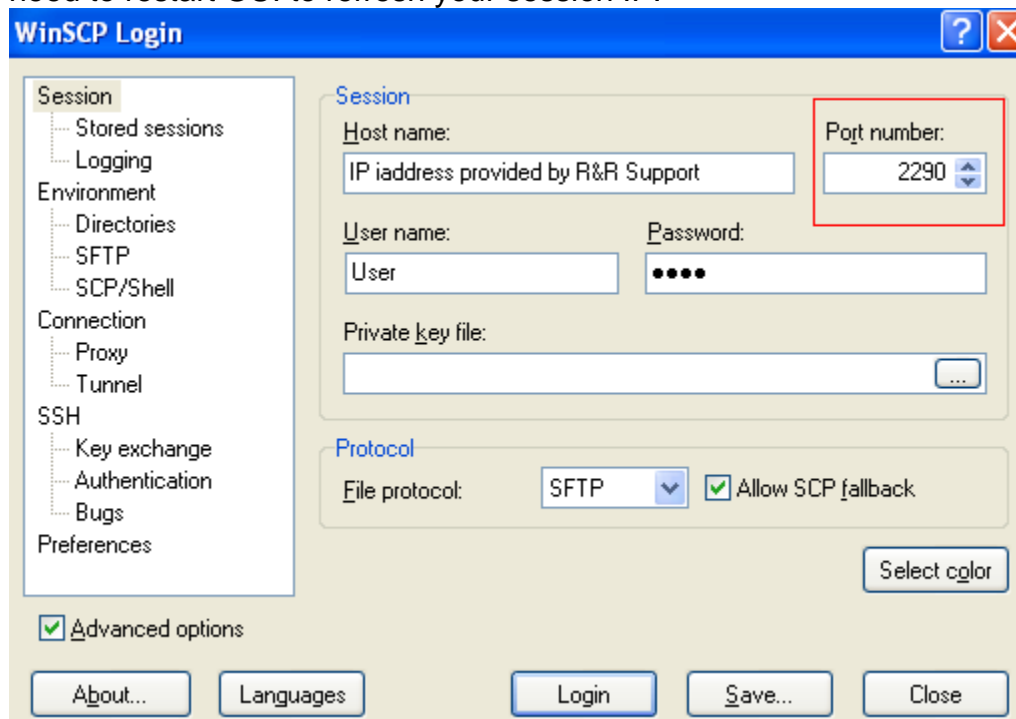
When you successfully logged in you see a file directory with Packet Capture files sorted by time.

CDR folder has RAW CDR data

Changed column shows file's Time Stamp. For example file "cap1731.pcap.gz" is covering time interval from 3:54:03PM to 4:30:02PM

Ctrl+Select needed file and hit *F5* to copy them to local computer.

Open captures and filter needed call

After saving capture files locally you can open them with fee Wireshark software
http://www.wireshark.org/download.html

Download and install Wireshark. Open file by right-click "Open With…" and selecting Wireshark.

Call capture will contain ALL calls passed through your switch. If you're looking to open Trouble Ticket with your Supplier or Buyer you need to make sure that you filtered information that only shows respective call leg.

Sending unfiltered packet capture is like telling all your business secrets.

In most cases inbound and outbound call legs will be shown separately in the Wireshark, so you may use VoIP Calls filtering in Wireshark (see below),

Alternatively you can filter by remote IP:
ip.addr==10.10.10.100

Analyze packet capture

Packet capture analysis requires advanced technical knowledge of H,323 and SIP protocols. R&R has posted manual on Troubleshooting that we strongly recommend to read.

[R&R VoIP Troubleshooting Manual](#)