5g Vision

VoIP/SMPP traffic sniffer

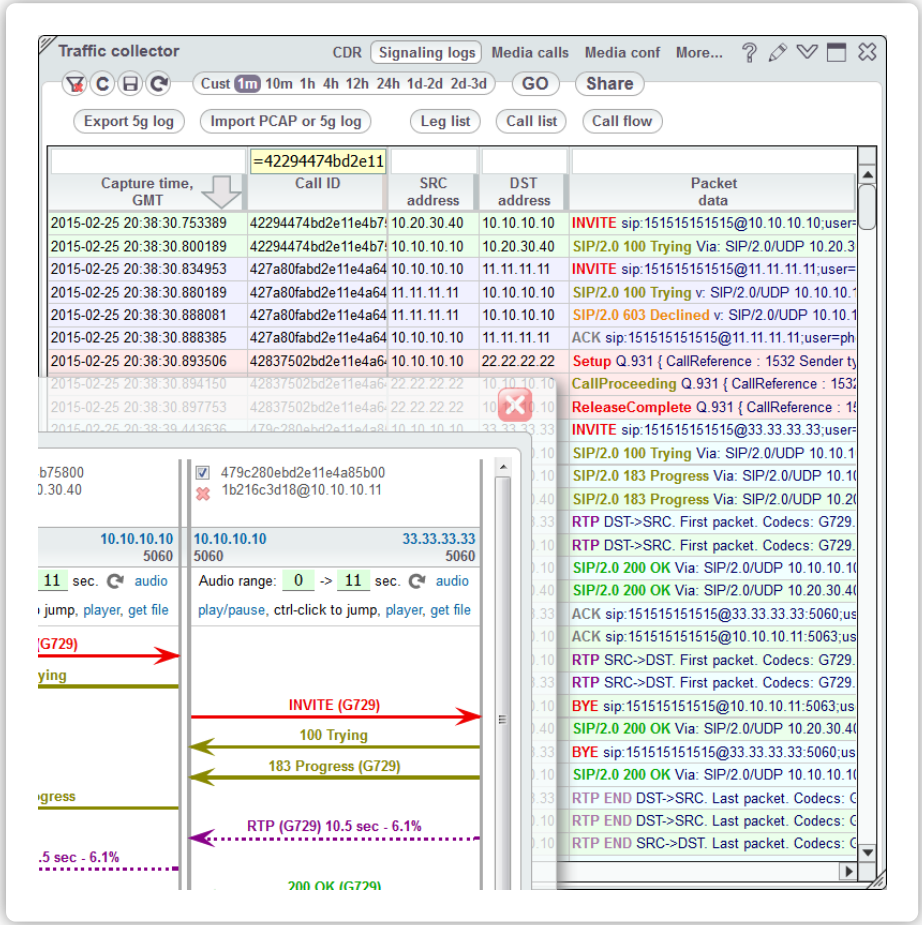
Break through your data

Traffic sniffer modules

VoIP traffic sniffer is an umbrella term for three interconnected features:

- **Signalling Log Collector** gathers **SIP**, **H.323** or **SMPP** packets in real time and lets users view **logs** and **call flows** in an easy and convenient way.
- **Media Collector** sniffs packets in real time capturing **full** media, **partial** media with filtering by media IPs or making **random** and **on-demand** recording of calls selected by signaling IPs / numbers masks and allows users to listen to the **recorded media**.
- **IP Whitelist Module** allows you to detect all **IPs** that send H.323 setups or SIP invites to the user's switch and **alert** the user in case there are new IPs that are **not in the whitelist**.

What is a signaling log collector?



Key features:

- Collection of all **SIP**, **H.323** or **SMPP** packets from the carrier's VoIP/SMS switch or several switches, the storage period depends only on the HDD capacity.
- Jumping to a **log** or a **call/SMS flow** of any call/SMS **right from the CDRs** with all legs matched and shown correctly, including all hunting attempts.
- Display of **raw collected packets** in a table with possibility to filter packets by SRC/DST IPs, numbers, call IDs, etc.
- Display of contents of **individual** packets.
- Display of contents of **all packets** forming a call/SMS leg or complete calls/SMSes with all legs.
- Display of a **call/SMS flow** as an easy-to-understand chart.
- Call/SMS flow **sharing** with your partners via a powerful 5gVision data sharing mechanism.
- Log **export** as .txt or **.pcap** files.

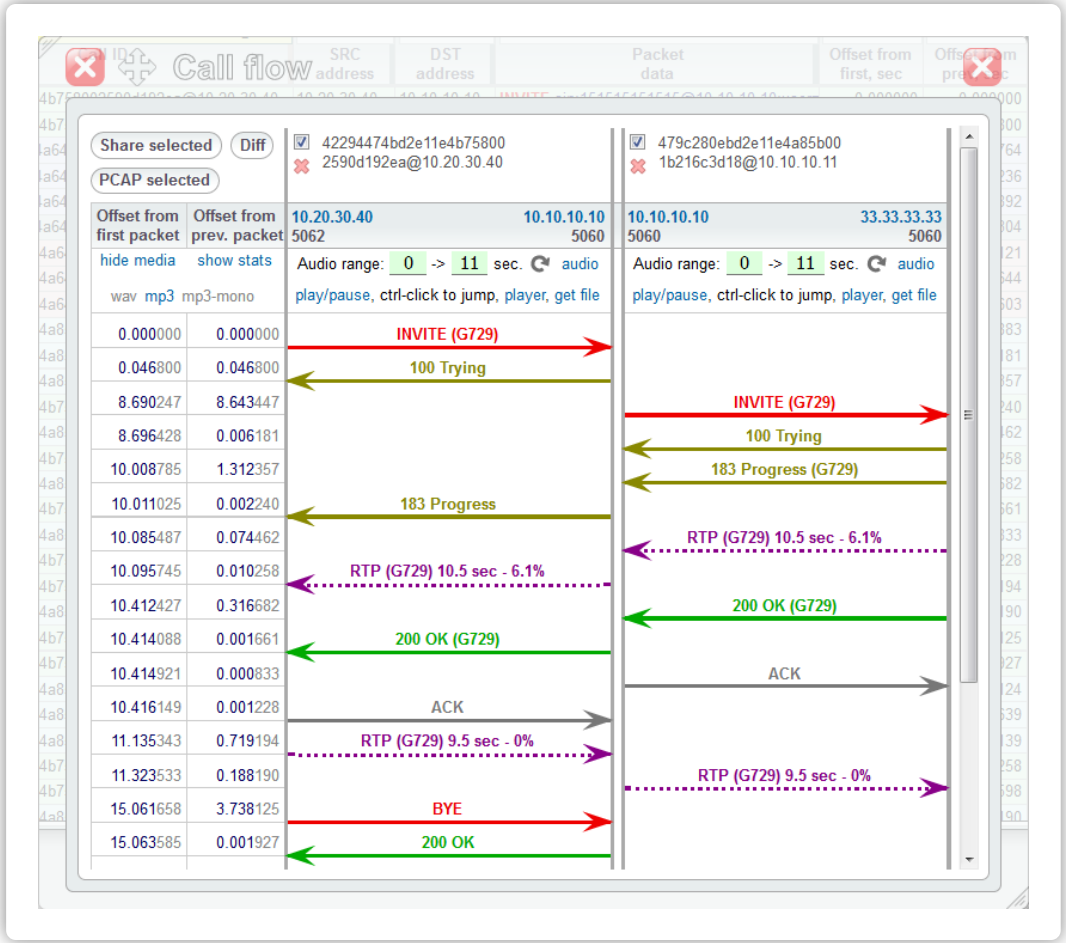
Call/SMS Flows

The Call/SMS flow window presents a call/SMS as a series of packet exchanges between switches.

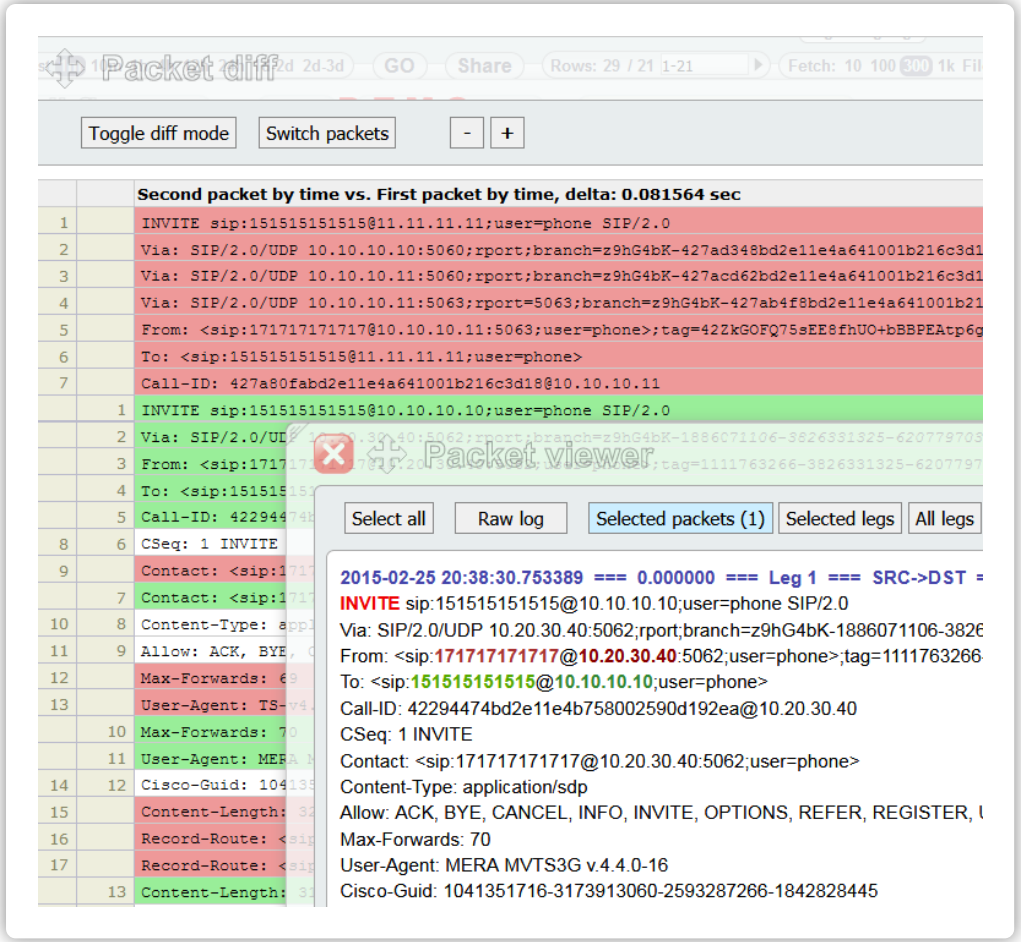
5gVision parses the packets and automatically divides the call/SMS into a number of legs, taking into account Call/SMS IDs and IPs involved. You can view all the hunting attempts of a call/SMS on a single diagram!

If Media collector is enabled, you can see RTP streams and play media right in the call flow window.

From here, you may open a new Packet viewing window showing all packets that comprise a certain leg or a single packet.



Viewing Packets



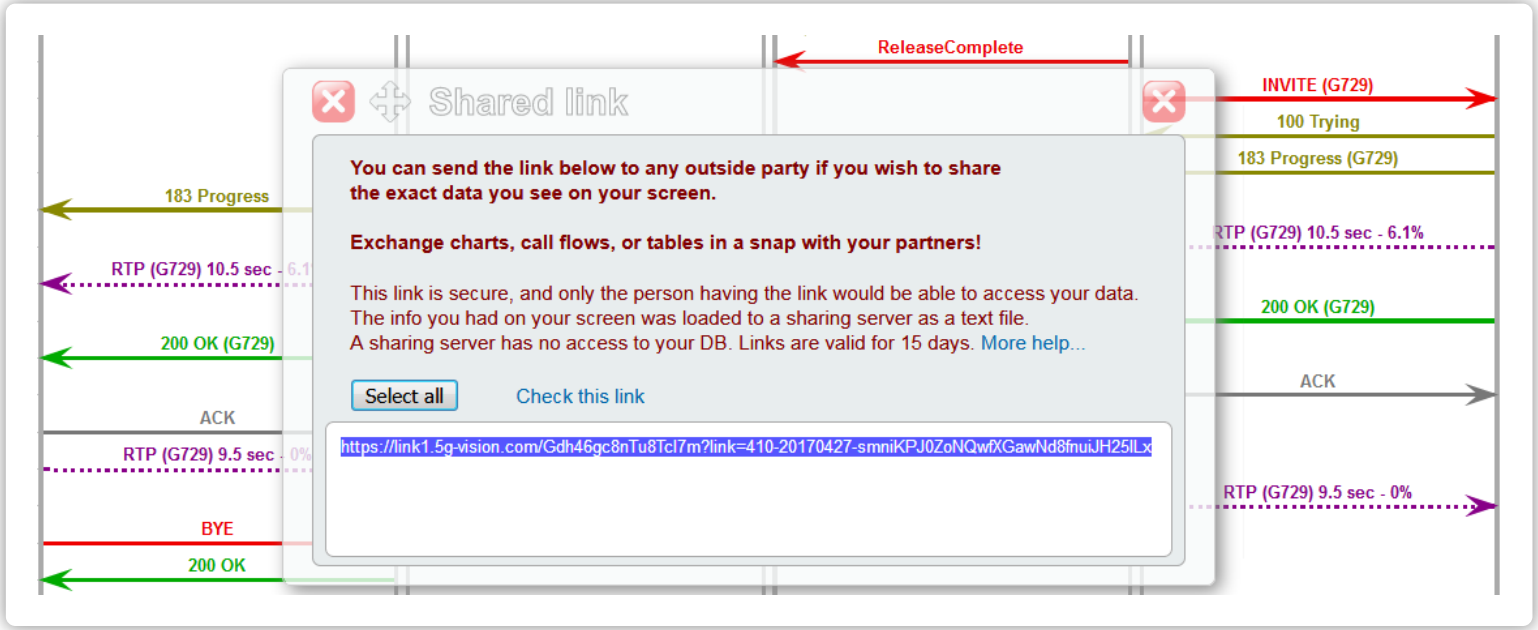
The packet viewing window presents **packet content** in a **textual** form. The amount of information depends on where and how the window was invoked: it is possible to view a **single packet**, **all packets** pertaining to **selected legs** or the **whole call/SMS**.

Additional features include:

- Opening 2 or more packet windows to **compare** different packets **side-by-side**.
- Generate a **diff** of 2 highlighted signaling packets.
- Disabling or enabling text formatting to **highlight key elements** of the packet.

Sharing Call/SMS Flow

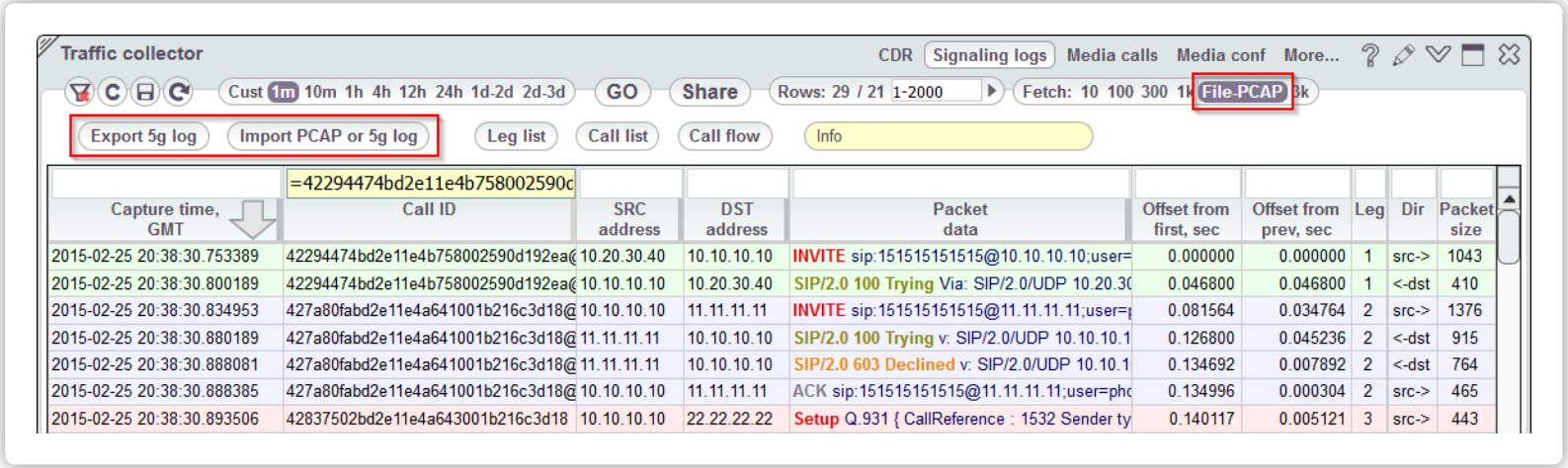
A Call/SMS Flow chart may be shared using the standard 5gVision sharing mechanism.



The Call/SMS flow window also contains a Share selected button which allows you to share the required legs with your partners. Shared links let your partner see the shared data in the same way as you do.

You may hide certain legs of a call/SMS and send only the info you want your customers or vendors to see, providing a very convenient way for your partners to investigate their logs.

Exporting / Importing Logs



You may **export** logs from 5gVision in two ways:

- as **.pcap** files by selecting **File-PCAP** in the row count selector and clicking **GO**.
- as **.txt** files in a proprietary format (click the **Export 5g log** button).

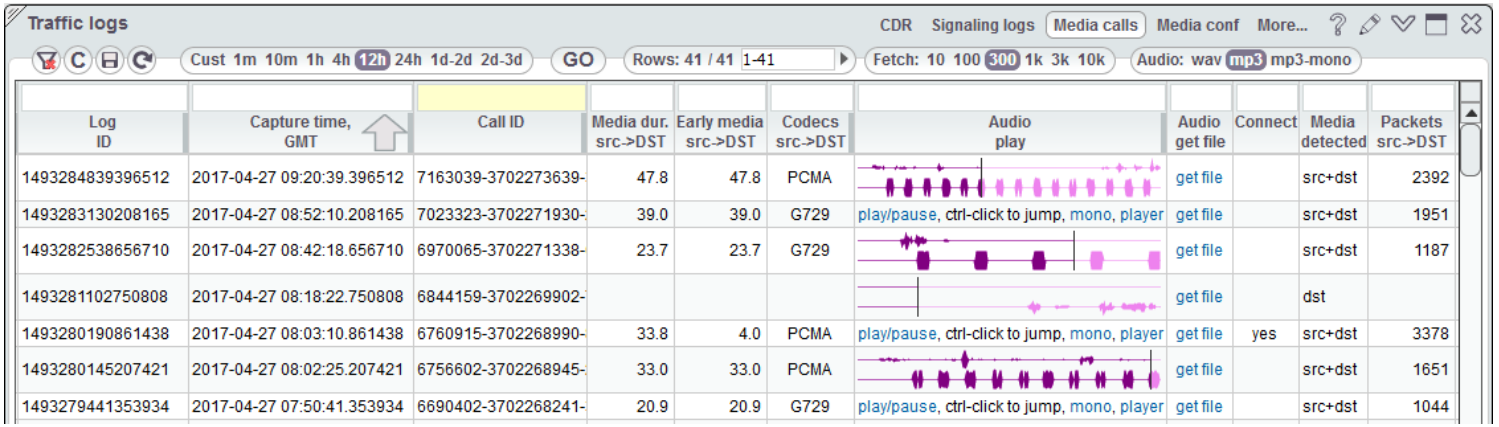
Such saved logs can then be easily viewed later by **Importing** them back to 5gVision by you, your colleagues, or even your partners if they are using 5gVision.

You may also **import** logs into 5gVision as **.txt** files or in a Wireshark-readable **.pcap** format by clicking the **Import PCAP or 5g log** button.

What is a media log collector?

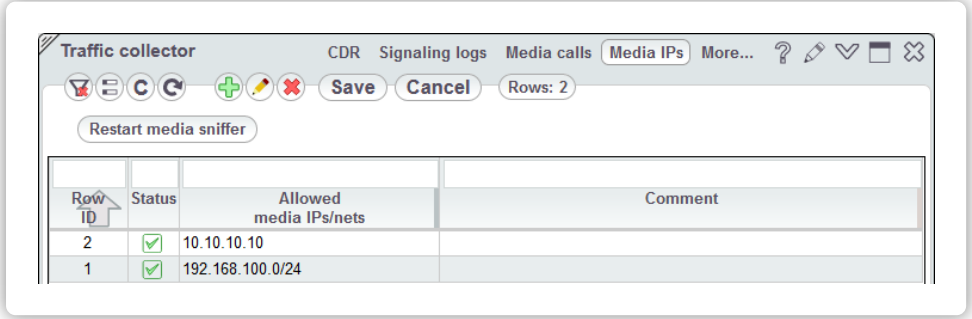
Key features:

- **Capturing** and **playback** of media in any commonly used codecs.
- Several modes available:
  - **full media** collection.
  - **partial media** collection with filtering by media IPs.
  - **random** and **on-demand** recording of calls selected by signaling IPs / numbers mask.
- Downloading **audio files**.
- **Signaling logs** module is required for Media logging to work.



Log ID	Capture time, GMT	Call ID	Media dur. src->DST	Early media src->DST	Codecs src->DST	Audio play	Audio get file	Connect	Media detected	Packets src->DST
1493284839396512	2017-04-27 09:20:39.396512	7163039-3702273639-	47.8	47.8	PCMA		get file		src+dst	2392
1493283130208165	2017-04-27 08:52:10.208165	7023323-3702271930-	39.0	39.0	G729	play/pause, ctrl-click to jump, mono, player	get file		src+dst	1951
1493282538656710	2017-04-27 08:42:18.656710	6970065-3702271338-	23.7	23.7	G729		get file		src+dst	1187
1493281102750808	2017-04-27 08:18:22.750808	6844159-3702269902-					get file		dst	
1493280190861438	2017-04-27 08:03:10.861438	6760915-3702268990-	33.8	4.0	PCMA	play/pause, ctrl-click to jump, mono, player	get file	yes	src+dst	3378
1493280145207421	2017-04-27 08:02:25.207421	6756602-3702268945-	33.0	33.0	PCMA		get file		src+dst	1651
1493279441353934	2017-04-27 07:50:41.353934	6690402-3702268241-	20.9	20.9	G729	play/pause, ctrl-click to jump, mono, player	get file		src+dst	1044

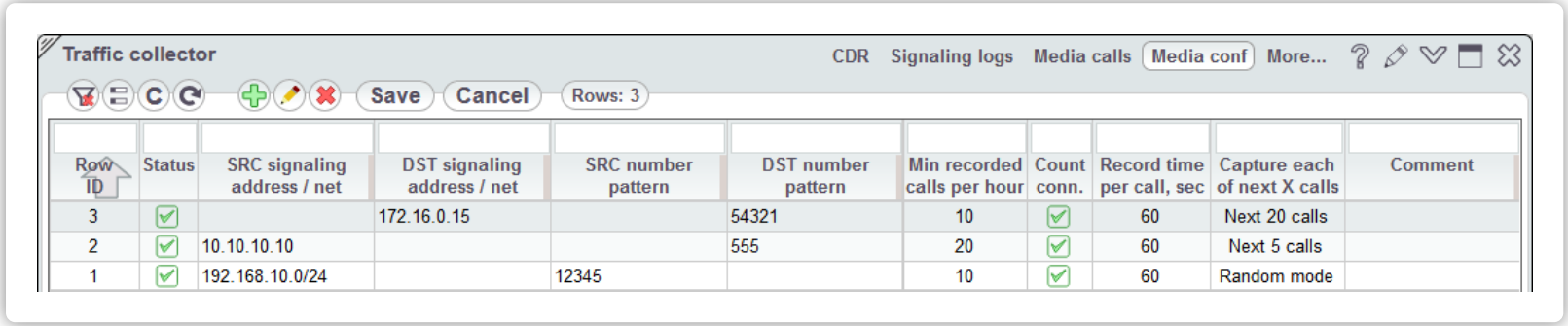
Media collector module setup



When you have huge traffic, and your hardware doesn't manage to process **full media** of all calls, you can setup collecting **partial media** only for a certain range of known **Media IPs**.

Otherwise, you may setup **random** or **on-demand** recording in the **Media conf** table. The table allows you to set up the **SRC/DST signaling IP** addresses and/or **number masks** to record only the calls that **match** these criteria.

The system will filter the **signaling logs** first, figure out the **media IPs**, and then start recording of the media stream for the configured calls in a **random** or **next X calls** mode.

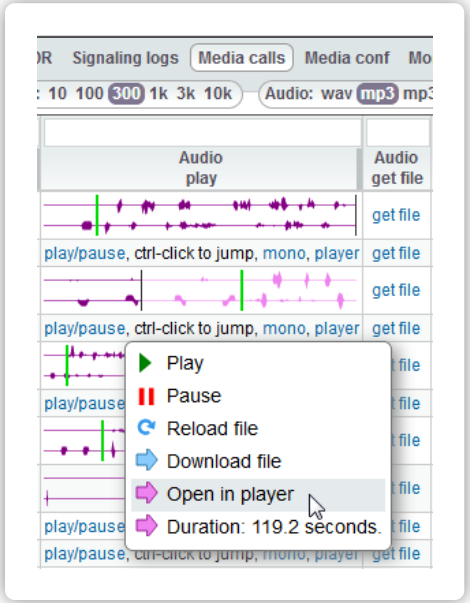


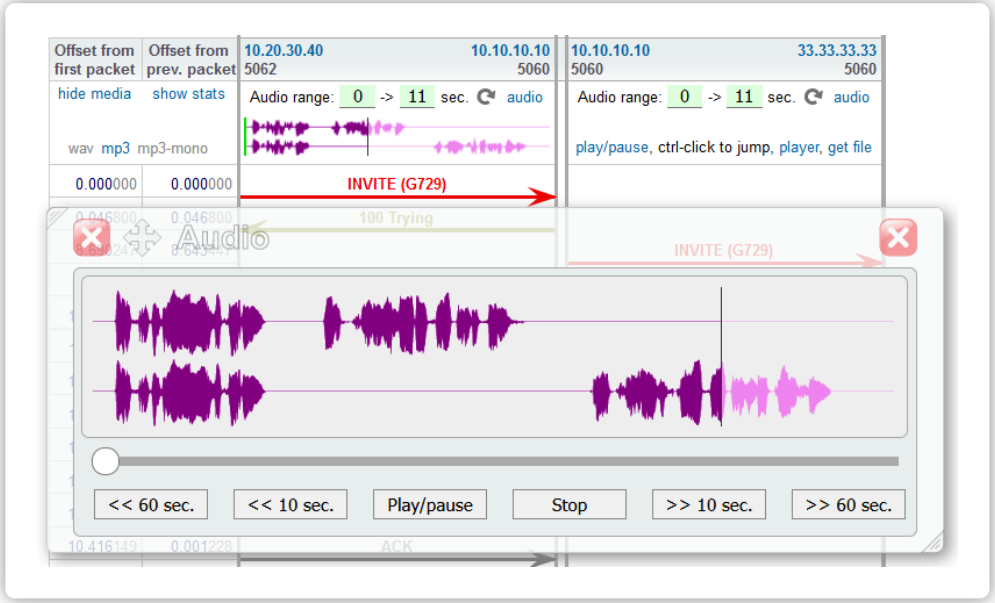
Media playback

Recorded calls in playback-ready format are found the **Media calls** table or a **Call flow**. You may playback a call by clicking the **play/pause** button in the **Audio play** column or in the **Media section** on top of a **Call flow** window. The system will display the graphical representation of a **sound stream**. Playback is always **stereo** with IN and OUT streams in different channels. The connect point is marked with a **green bar**, and you may jump through the stream by **Ctrl-clicking** it.

Each media waveform in a table cell or in a Call flow has a **Right-click menu**, allowing to open each audio file in a separate **player**. The **Call flow** lets you play media of **each leg** separately, as well as view the media stats.

You may also download the file via the **get file** link.





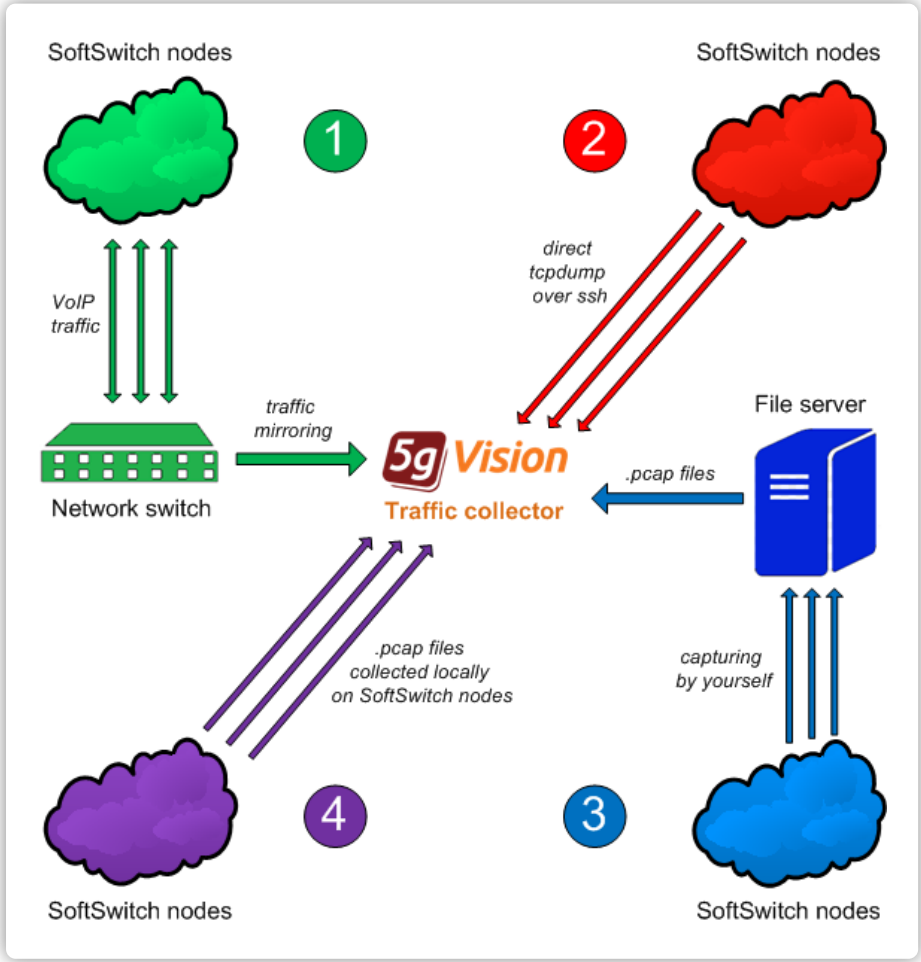
IP Whitelist module

The **IP whitelist** module collects all IPs that send **H.323 setups** or **SIP invites** to your switch, independently of switch CDRs, from raw packets, and in case a number of per hour occurrences of new IPs that are not in the whitelist **exceeds a preset threshold**, you will be **alerted** over **email, SMS or Push** notification (a 5gVision Alerting module is required).

This feature might be useful to catch the following intrusions into your VoIP system:

- Intrusion into **your switch**, by adding authorizations for new IPs. Your own switch IP:ports remains same, **new IPs of fraudulent customers** start sending traffic to existing switch IP:ports.
- Intrusion into **your servers** and installation of just another malicious **switch in parallel** with your own switch.
- Intrusion into your **Customer's servers**. A Customer starts sending you traffic that they potentially wont be able to pay for.

Collection methods



There are 4 main methods of getting signaling and media packets:

1. By setting up a **mirroring port** on the Ethernet switch the VoIP/SMS softswitch is connected to and connecting a 5gVision logging server to this port.
2. By allowing 5gVision software to connect to customer's VoIP/SMS softswitch **over SSH** with a **user with limited rights** to run the **tcpdump remotely** and send packets back to 5gVision over SSH.
3. By uploading **over SFTP** or other protocols and processing already collected by **yourself .pcap files**.
4. By collecting packets in **.pcap files** using a very simple script on each node of your VoIP/SMS softswitch and feeding them to 5gVision **over SFTP** or other protocols for processing.

5g Vision

Thank you for your time

If you wish to request
a fully functional trial
or get more information,
please contact:

Demo: demo.5gfuture.com/logger
Web: www.5gfuture.com
Skype: support_5gfuture
Email: sales-team@5gfuture.com