



VoIP/SMPP traffic sniffer

Break through your data

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**.

The screenshot displays the 'Traffic collector' interface with a table of signaling logs. The table has columns for 'Capture time, GMT', 'Call ID', 'SRC address', 'DST address', and 'Packet data'. A search filter is applied to the Call ID column with the value '=42294474bd2e11'. The table shows several rows of log entries, including INVITE, SIP/2.0 100 Trying, SIP/2.0 603 Declined, ACK, Setup, CallProceeding, and ReleaseComplete messages.

Below the table, a detailed view of a call flow is shown. It includes a timeline with various events and their durations. Key events include:

- INVITE (G729)**: A red arrow pointing right.
- 100 Trying**: A green arrow pointing left.
- 183 Progress (G729)**: A green arrow pointing left.
- RTP (G729) 10.5 sec - 6.1%**: A purple dashed arrow pointing left.
- 200 OK (G729)**: A green arrow pointing right.

The interface also shows a search bar with the Call ID '42294474bd2e11' and a 'GO' button. There are also buttons for 'Export 5g log', 'Import PCAP or 5g log', 'Leg list', 'Call list', and 'Call flow'.

Key features:

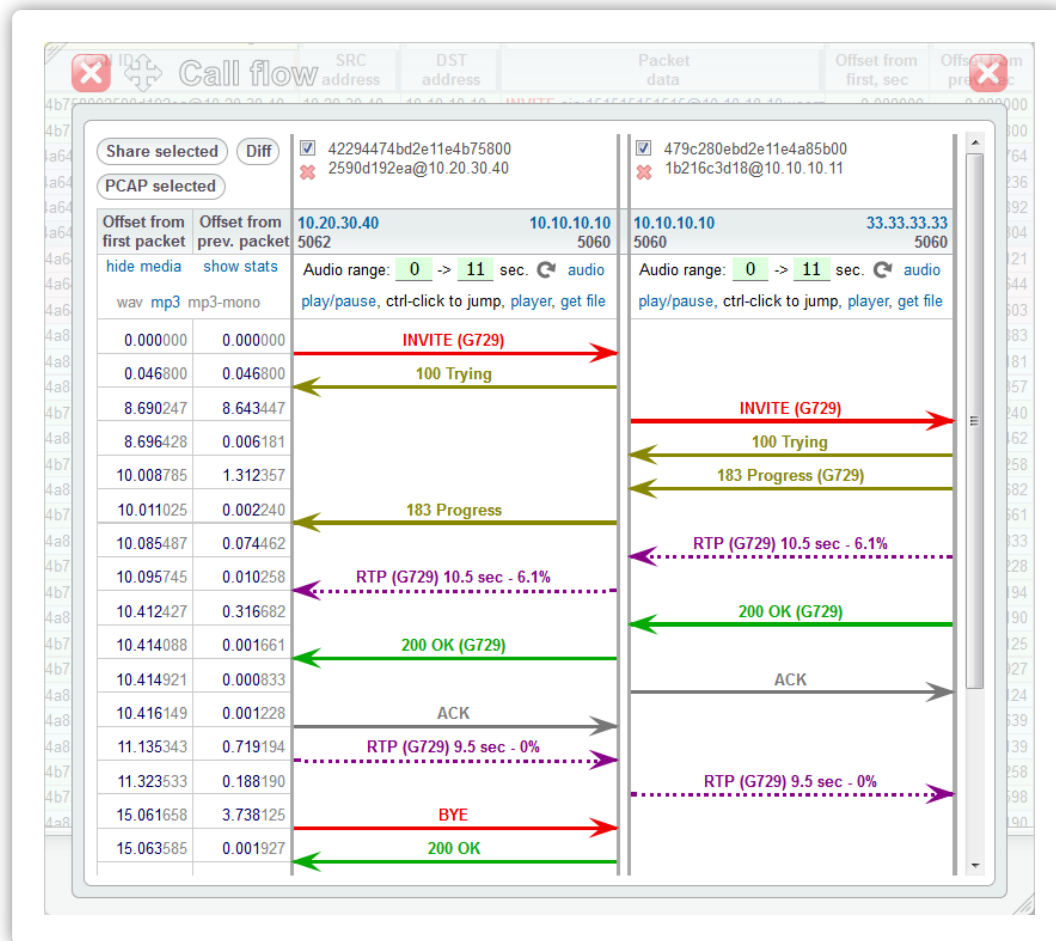
- Collection of all **SIP**, **H.323** or **SMPP** packets from the carrier's VoIP/SMS switch or several switches, the storage period depends only on the HDD capacity.
- Jumping to a **log** or a **call/SMS flow** of any call/SMS **right from the CDRs** with all legs matched and shown correctly, including 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.

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.



Packet diff

Toggle diff mode Switch packets - +

Rows: 29 / 21 1-21 Fetch: 10 100 800 1k File

Second packet by time vs. First packet by time, delta: 0.081564 sec

1	INVITE sip:151515151515@11.11.11.11;user=phone SIP/2.0
2	Via: SIP/2.0/UDP 10.10.10.10:5060;rport;branch=z9hG4bK-427ad348bd2e11e4a641001b216c3d1
3	Via: SIP/2.0/UDP 10.10.10.11:5060;rport;branch=z9hG4bK-427acd62bd2e11e4a641001b216c3d1
4	Via: SIP/2.0/UDP 10.10.10.11:5063;rport=5063;branch=z9hG4bK-427ab4f8bd2e11e4a641001b21
5	From: <sip:1717171717@10.10.10.11:5063;user=phone>;tag=422kGQF75sEE8fhUO+bBBPEAtp6g
6	To: <sip:1515151515@11.11.11.11;user=phone>
7	Call-ID: 427a80fabd2e11e4a641001b216c3d18@10.10.10.11
1	INVITE sip:1515151515@10.10.10.10;user=phone SIP/2.0
2	Via: SIP/2.0/UDP 10.20.30.40:5062;rport;branch=z9hG4bK-1886071106-3826331325-620779703
3	From: <sip:1717171717@10.20.30.40:5062;user=phone>;tag=1111763266-3826331325-6207797
4	To: <sip:1515151515@10.10.10.10;user=phone>
5	Call-ID: 42294474bd2e11e4b758002590d192ea@10.20.30.40
6	CSeq: 1 INVITE
7	Contact: <sip:1717171717@10.20.30.40:5062;user=phone>
8	Content-Type: application/sdp
9	Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, REFER, REGISTER, UPDATE
10	Max-Forwards: 70
11	User-Agent: MERA MVTS3G v.4.4.0-16
12	Cisco-Guid: 1041351716-3173913060-2593287266-1842828445
13	Content-Length: 321

Packet viewer

Select all Raw log Selected packets (1) Selected legs All legs

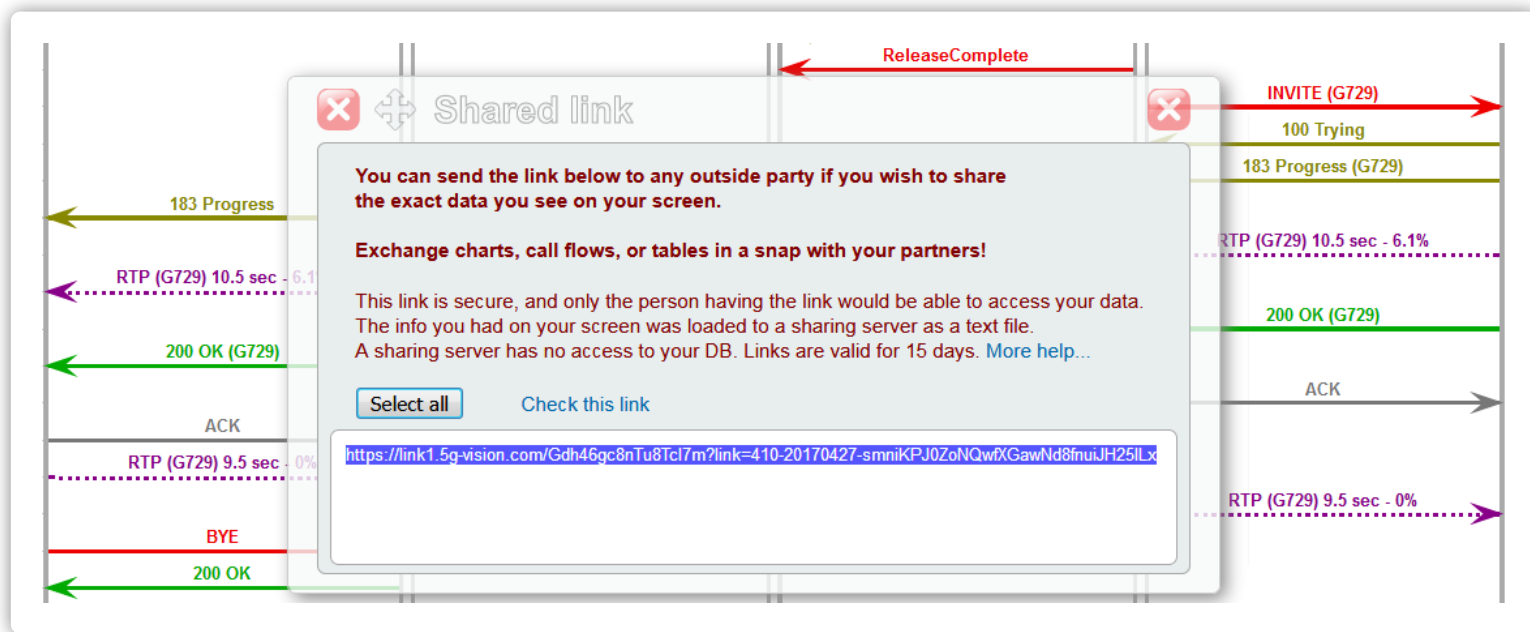
2015-02-25 20:38:30.753389 === 0.000000 === Leg 1 === SRC->DST =
 INVITE sip:1515151515@10.10.10.10;user=phone SIP/2.0
 Via: SIP/2.0/UDP 10.20.30.40:5062;rport;branch=z9hG4bK-1886071106-3826331325-620779703
 From: <sip:1717171717@10.20.30.40:5062;user=phone>;tag=1111763266-3826331325-620779703
 To: <sip:1515151515@10.10.10.10;user=phone>
 Call-ID: 42294474bd2e11e4b758002590d192ea@10.20.30.40
 CSeq: 1 INVITE
 Contact: <sip:1717171717@10.20.30.40:5062;user=phone>
 Content-Type: application/sdp
 Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, REFER, REGISTER, UPDATE
 Max-Forwards: 70
 User-Agent: MERA MVTS3G v.4.4.0-16
 Cisco-Guid: 1041351716-3173913060-2593287266-1842828445

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.

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.

The screenshot shows the 'Traffic collector' interface with the following elements:

- Navigation tabs: CDR, Signaling logs, Media calls, Media conf, More...
- Filters: Cust, 1m, 10m, 1h, 4h, 12h, 24h, 1d-2d, 2d-3d
- Buttons: GO, Share, Rows: 29 / 21, 1-2000, Fetch: 10 100 300 1k, File-PCAP (highlighted in a red box)
- Export options: Export 5g log (highlighted in a red box), Import PCAP or 5g log (highlighted in a red box), Leg list, Call list, Call flow, Info
- Table with columns: Capture time, GMT; Call ID; SRC address; DST address; Packet data; Offset from first, sec; Offset from prev, sec; Leg; Dir; Packet size

Capture time, GMT	Call ID	SRC address	DST address	Packet data	Offset from first, sec	Offset from prev, sec	Leg	Dir	Packet size
2015-02-25 20:38:30.753389	=42294474bd2e11e4b758002590c	10.20.30.40	10.10.10.10	INVITE sip:1515151515@10.10.10.10;user=	0.000000	0.000000	1	src->	1043
2015-02-25 20:38:30.800189	42294474bd2e11e4b758002590d192ea	10.10.10.10	10.20.30.40	SIP/2.0 100 Trying Via: SIP/2.0/UDP 10.20.30	0.046800	0.046800	1	<-dst	410
2015-02-25 20:38:30.834953	427a80fabd2e11e4a641001b216c3d18@	10.10.10.10	11.11.11.11	INVITE sip:1515151515@11.11.11.11;user=	0.081564	0.034764	2	src->	1376
2015-02-25 20:38:30.880189	427a80fabd2e11e4a641001b216c3d18@	11.11.11.11	10.10.10.10	SIP/2.0 100 Trying v: SIP/2.0/UDP 10.10.10.1	0.126800	0.045236	2	<-dst	915
2015-02-25 20:38:30.888081	427a80fabd2e11e4a641001b216c3d18@	11.11.11.11	10.10.10.10	SIP/2.0 603 Declined v: SIP/2.0/UDP 10.10.1	0.134692	0.007892	2	<-dst	764
2015-02-25 20:38:30.888385	427a80fabd2e11e4a641001b216c3d18@	10.10.10.10	11.11.11.11	ACK sip:1515151515@11.11.11.11;user=phc	0.134996	0.000304	2	src->	465
2015-02-25 20:38:30.893506	42837502bd2e11e4a643001b216c3d18	10.10.10.10	22.22.22.22	Setup Q.931 { CallReference : 1532 Sender ty	0.140117	0.005121	3	src->	443

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.

Key features:

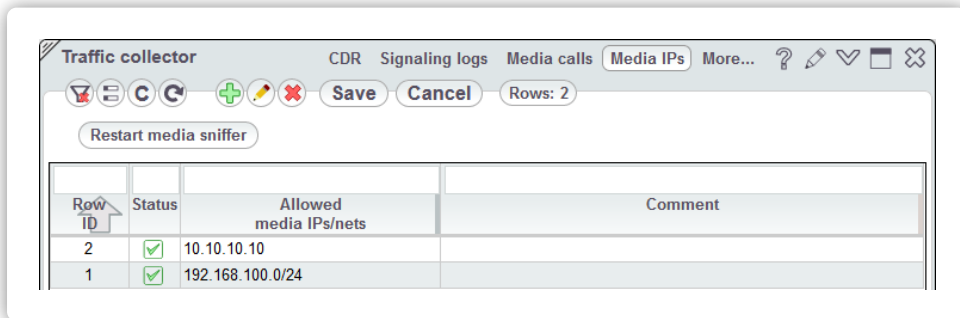
- **Capturing** and **playback** of media in any commonly used codecs.
- Several modes available:
 - **full media** collection.
 - **partial media** collection with filtering by media IPs.
 - **random** and **on-demand** recording of calls selected by signaling IPs / numbers mask.
- Downloading **audio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

Traffic logs

CDR Signaling logs **Media calls** Media conf More... ?

Cust 1m 10m 1h 4h **12h** 24h 1d-2d 2d-3d GO Rows: 41 / 41 1-41 Fetch: 10 100 **300** 1k 3k 10k Audio: wav **mp3** mp3-mono

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



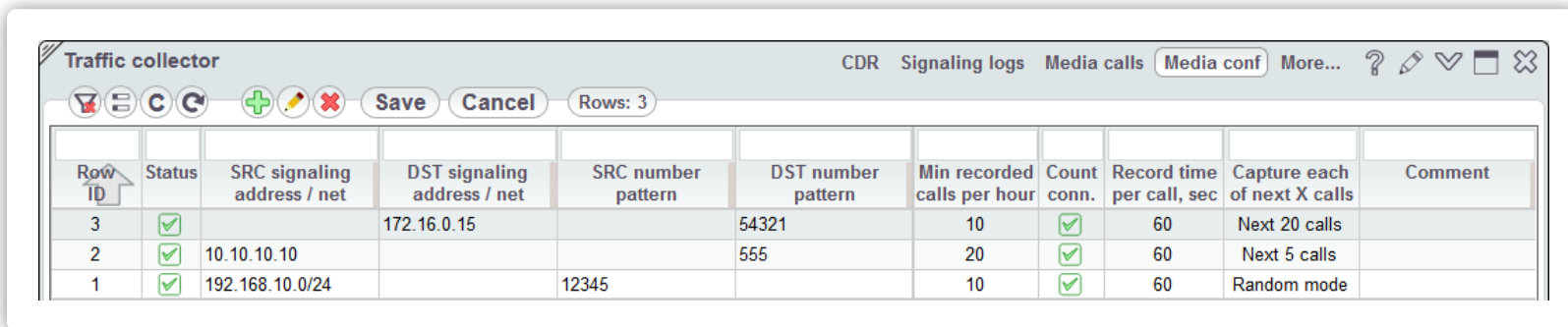
The screenshot shows the 'Traffic collector' window with the 'Media IPs' tab selected. The table below shows the configuration for two rows:

Row ID	Status	Allowed media IPs/nets	Comment
2	<input checked="" type="checkbox"/>	10.10.10.10	
1	<input checked="" type="checkbox"/>	192.168.100.0/24	

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.



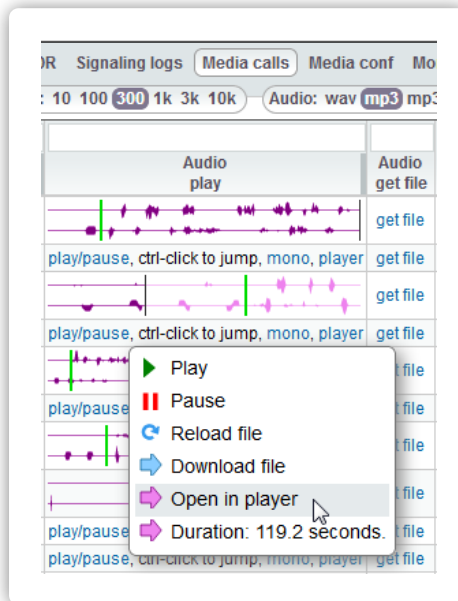
The screenshot shows the 'Traffic collector' window with the 'Media conf' tab selected. The table below shows the configuration for three rows:

Row ID	Status	SRC signaling address / net	DST signaling address / net	SRC number pattern	DST number pattern	Min recorded calls per hour	Count conn.	Record time per call, sec	Capture each of next X calls	Comment
3	<input checked="" type="checkbox"/>		172.16.0.15		54321	10	<input checked="" type="checkbox"/>	60	Next 20 calls	
2	<input checked="" type="checkbox"/>	10.10.10.10			555	20	<input checked="" type="checkbox"/>	60	Next 5 calls	
1	<input checked="" type="checkbox"/>	192.168.10.0/24		12345		10	<input checked="" type="checkbox"/>	60	Random mode	

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.

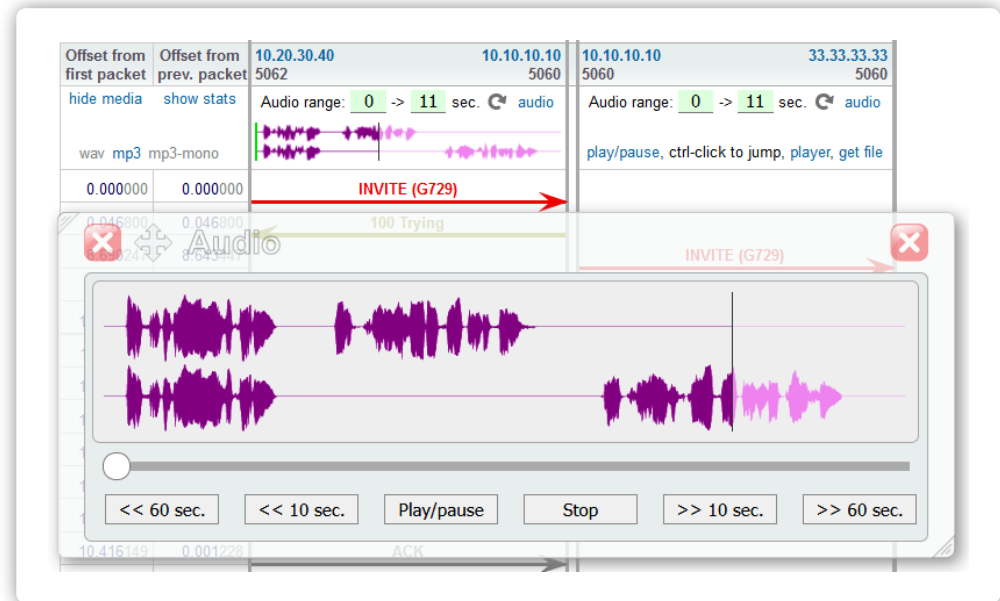
Each media waveform in a table cell or in a Call flow has a **Right-click menu**, allowing to open each audio file in a separate **player**. The **Call flow** lets you play media of **each leg** separately, as well as view the media stats.

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



The screenshot shows a table with columns for 'Audio play' and 'Audio get file'. A right-click menu is open over a waveform, listing options: Play, Pause, Reload file, Download file, Open in player, and Duration: 119.2 seconds.

Audio play	Audio get file
	get file
play/pause, ctrl-click to jump, mono, player	get file
	get file
play/pause, ctrl-click to jump, mono, player	get file
	file
play/pause	file
	file
play/pause	file
	file
play/pause	file
	file
play/pause, ctrl-click to jump, mono, player	get file



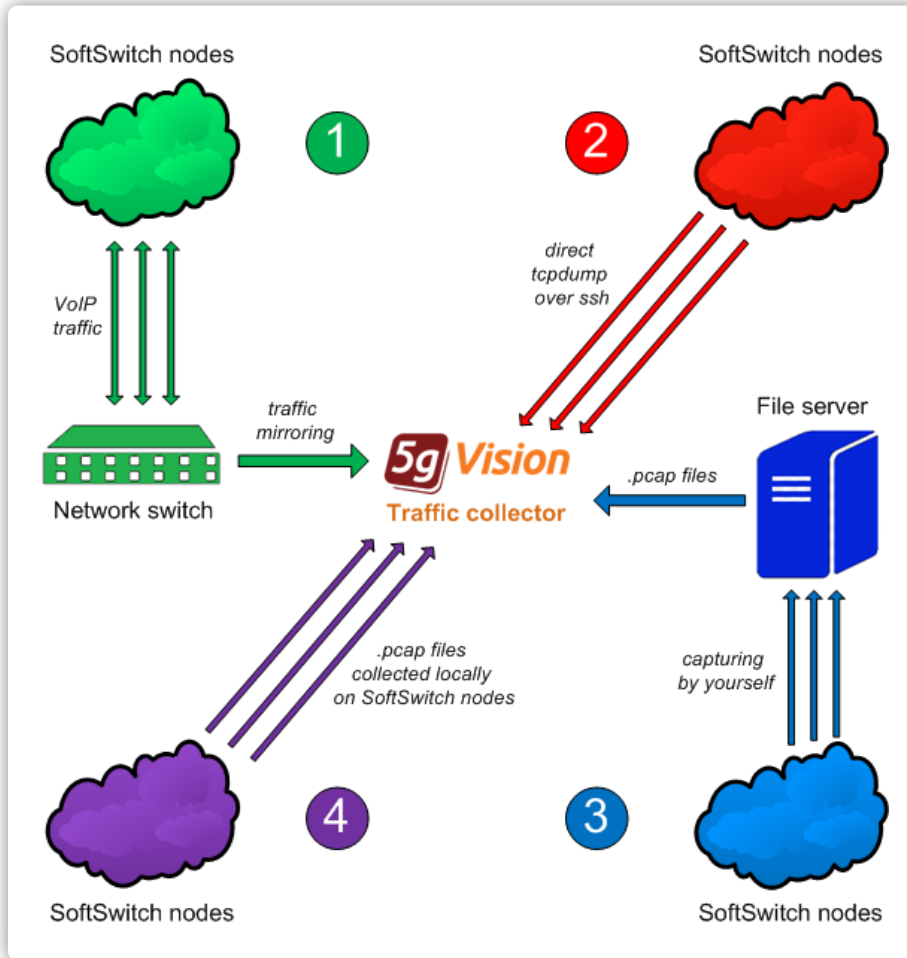
The screenshot shows a Call flow window with a table of audio segments. A detailed player interface is overlaid, showing a waveform and playback controls. The player interface includes a progress bar, a volume icon, and buttons for '<< 60 sec.', '<< 10 sec.', 'Play/pause', 'Stop', '>> 10 sec.', and '>> 60 sec.'. The table shows 'Offset from first packet' and 'Offset from prev. packet' for three segments, with 'Audio range: 0 -> 11 sec.' and 'audio' format.

Offset from first packet	Offset from prev. packet	10.20.30.40	10.10.10.10	10.10.10.10	33.33.33.33
hide media	show stats	5062	5060	5060	5060
wav mp3	mp3-mono	Audio range: 0 -> 11 sec. audio		Audio range: 0 -> 11 sec. audio	
0.000000	0.000000	INVITE (G729)		play/pause, ctrl-click to jump, player, get file	

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.



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.



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