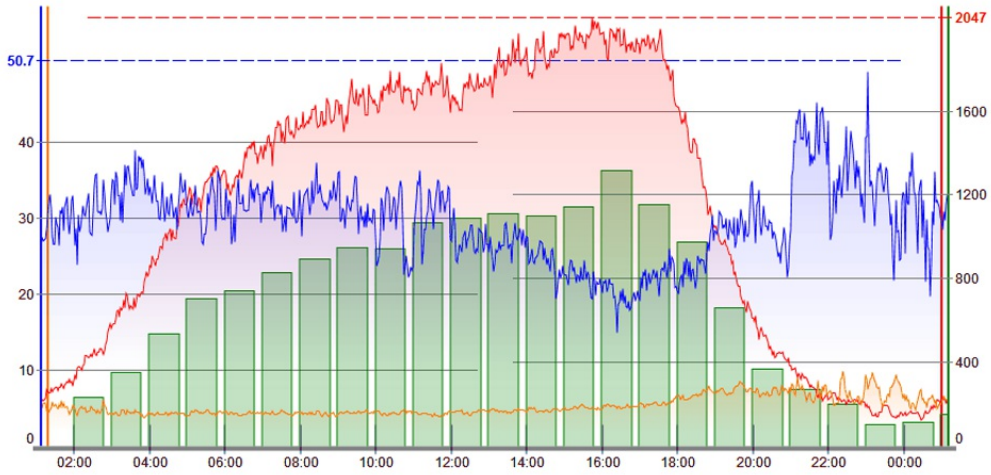
Traffic collector



User manual

Product version: 2.3

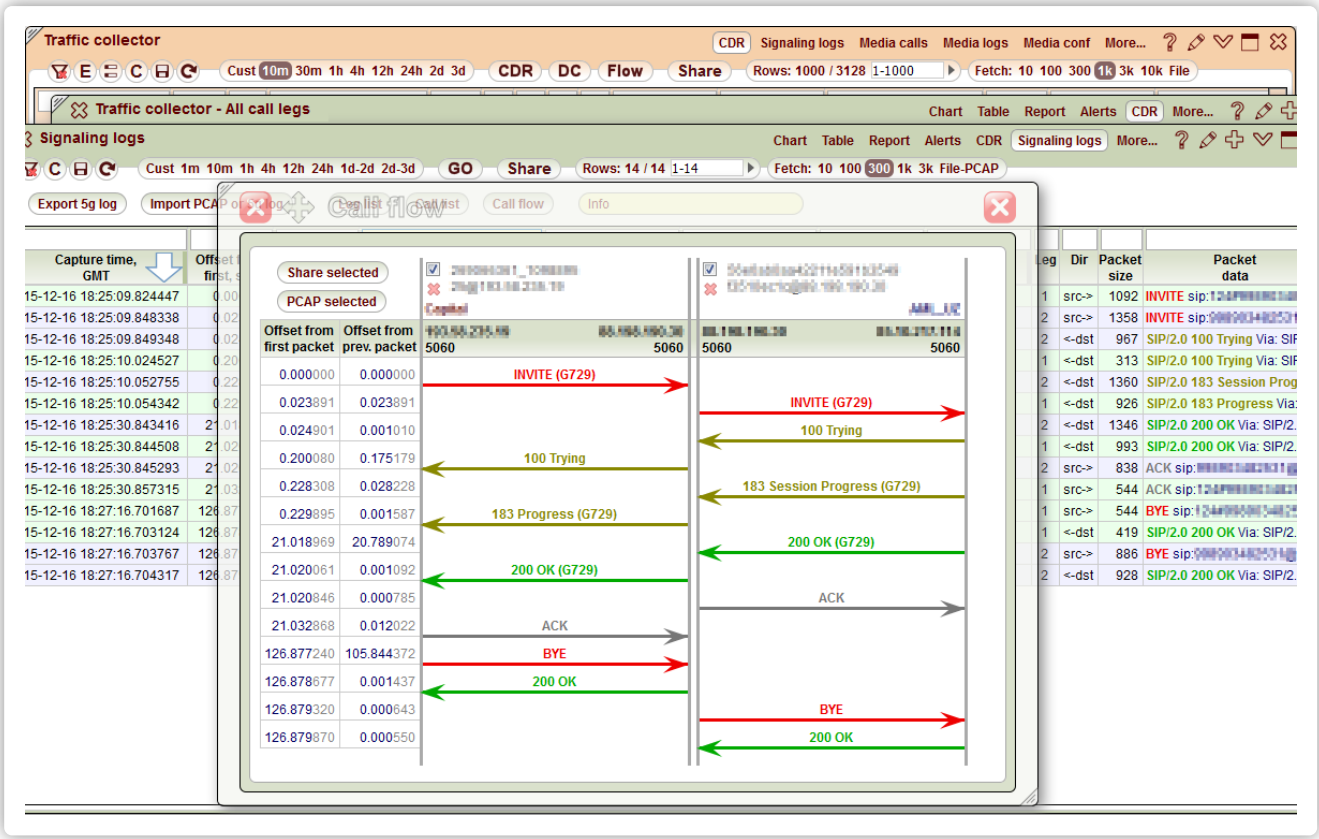
www.5gFuture.com

Table of Contents

1. Introduction

5gVision Traffic collector is part of the 5gVision suite of products for monitoring, alerting, packet sniffing, and rate management that share a common web interface: quick, intuitive, and flexible.

1.1. Overview



The **Traffic collector** is part of the **5gVision** suite of products. Its main function is to gather SIP/H.323 signaling logs and media packets in real time. It then allows you to quickly view any signaling logs or Call flows from the past in an easy and convenient way, listen to the recorded media for pre-defined IP addresses and number masks, and detect intrusions to your VoIP system. A good way to start with the Traffic collector and understand its main concepts is to view this sales presentation:

5gVision Traffic Collector Modules

The **5gVision** interface principles are described in a separate manual: User interface

You may download a PDF version of the manual here:

User interface

If you are new to 5gVision, we would recommend to go through at least the beginning of the Interface manual first.

The **Traffic collector** comprises three separate modules:

- Signaling collector
- Media collector
- IP whitelist

that are described in further sections of this manual.

1.2. Collection methods

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

- **Method 1** requires setting up a **mirrored port** on the Ethernet switch the VoIP softswitch is connected to. This mirrored port should be linked to a NIC on a 5gVision server to let it grab signaling and media packets passing through the network.

  The main advantage is that this scheme doesn't affect the softswitch performance at all, is invisible to softswitch vendor's support team, and usually allows to collect huge amounts of traffic without drops. However, a customer has to reconfigure its Ethernet switch and add another NIC card to a 5gVision server. Not all Ethernet switches support mirroring too, and it won't work if a customer does not have physical access to the softswitch server (rented servers, VPS, etc.), or can't install just another server for 5gVision in the same LAN as the VoIP softswitch.

- **Method 2** allows collection of traffic **remotely via an SSH connect** to each of customer's VoIP softswitches with a **user that is only allowed to run one application** - tcpdump. All packets are grabbed locally on the softswitch and are sent to 5gVison via SSH.

  The benefit of this scheme is that there are no additional hardware requirements, logs can be collected from any servers without a physical access, and from geographically distributed servers. Also, this scheme doesn't affect the "Do not install the third-party software" agreement with the softswitch vendor, because ssh and tcpdump are a basic tools of every Linux system.

  Local packet sniffing consumes some extra CPU resources and memory on the softswitch, although the increase is usually negligible and is within 5-10%. HDD is not affected at all, as no packets are written to a local drive of the softswitch.

- **Method 3** can be used if **you already collect .pcap files** yourself. 5gVison may then upload and process these files over SFTP or other protocols. It is preferred that the files are rotated every 2-5 minutes or so, to make the collector closer to real time.

- **Method 4** requires installation of a very simple **script on each node** (server) of your softswitch. This script will run the tcpdump and write traffic into files. The files will rotate and will never use more space than was allocated on each HDD. We will then upload files to a 5gVision server for processing.

  This scheme will deliver unprecedented performance for large distributed systems. For instance, if you have 8 nodes (servers) in your softswitch, doing mirroring of 8 ports to just one NIC card on the 5gVsion server may result in enormous traffic (especially if media is collected) that we will not be able to read from the NIC without drops. However, if traffic is dumped into files on each of the 8 nodes, it will not be a problem to copy and process them on one or several 5gVision servers.

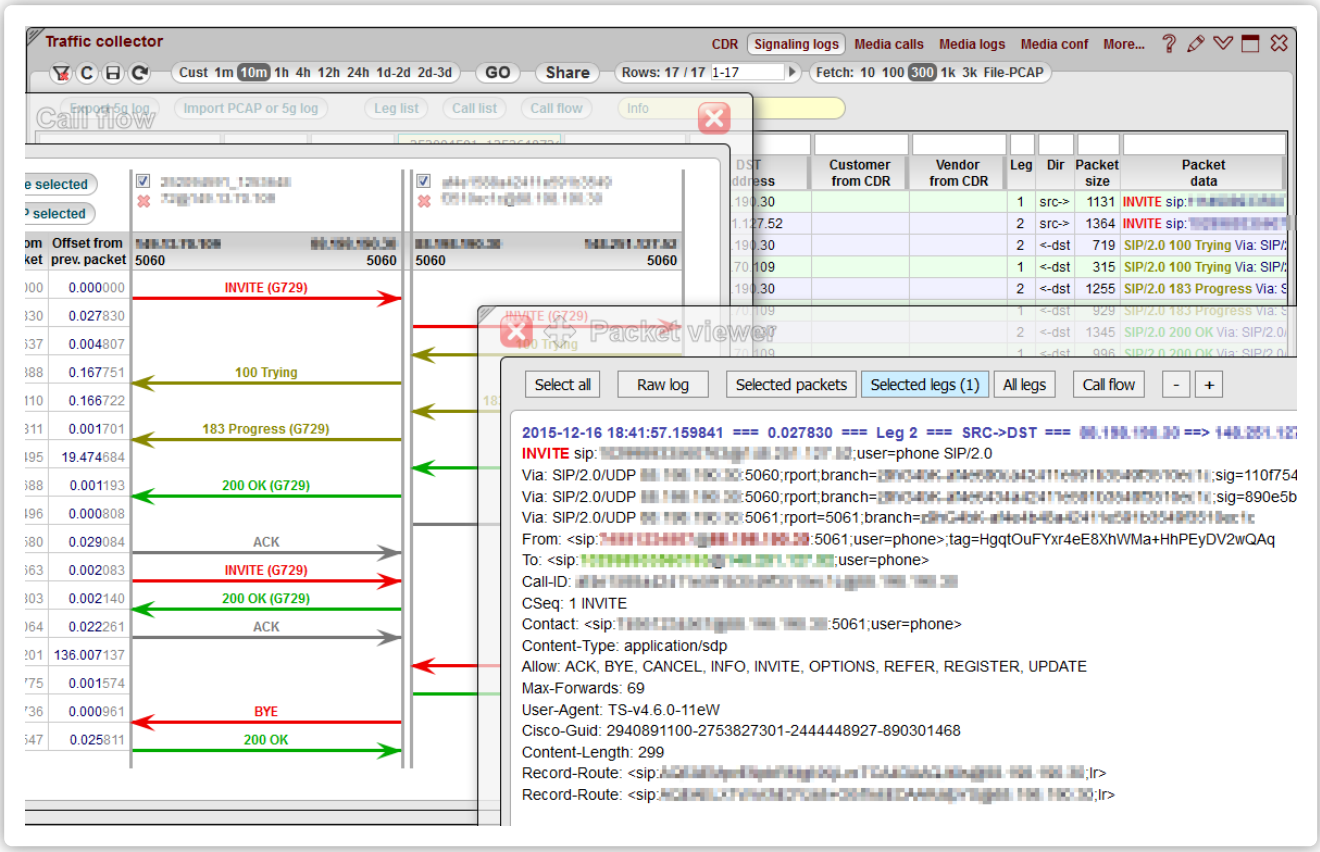
  There would be an extra load on CPU and HDD of each node in this case, we would need to investigate your node load and your softswitch type to make a decision to install this scheme.

2. Signaling collector

The signaling collector gathers SIP/H.323 logs in real time and let you view their contents and Call flows.

2.1. Overview

The **Signaling collector** gathers, stores and conveniently displays SIP and H.323 messages sent and received via the predefined ports of your network.

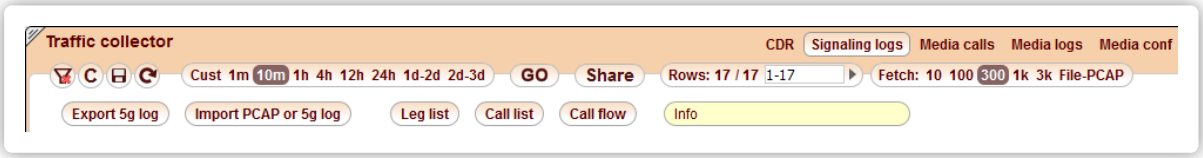


There are several ways for accessing this feature:

- through **CDRs** (see CDR pop-up menu) which frees you from entering Call ID manually, and lets you see call flow for 2 call legs at once).
- through your current screen by opening the **Signaling logs** module.
- by adding a new **Traffic collector** screen (see Menu tree for information on how to add it).

2.2. Signaling logs menu

The menu on top of the **Signaling logs** table consists of the Table menu, the Interval strip, the Row count strip, the Row limit strip, the **Export 5g log** button, the **Import PCAP or 5g log** button, the **Leg list**, the **Call list** and the **Call flow** button.



The interval selector allows you to limit the number of packets fetched from the DB to those belonging to the latest period (1m, 10m, 1h, etc) or custom period only, while the row count selector limits them to only the top X rows.

To apply the settings of the selectors, click **GO**. The **Rows** label shows the current number of rows displayed with filters applied.

To create a shared link based on the information displayed at the current screen, click **Share**. For more information see Shared links.

To export the currently displayed packets into a text file, click **Export log file**. To export packets for a certain interval into a PCAP file, choose an interval in the Interval strip, click **File PCAP** on the Row limit strip and then **GO**. To import logs from a text file or Wireshark-readable PCAP format, click **Import PCAP or 5g file**. You can also drag and drop a PCAP file right to the window. Please note that the import function affects the web interface only and doesn't change the DB. That is why imported data will disappear once you reload or leave the screen.

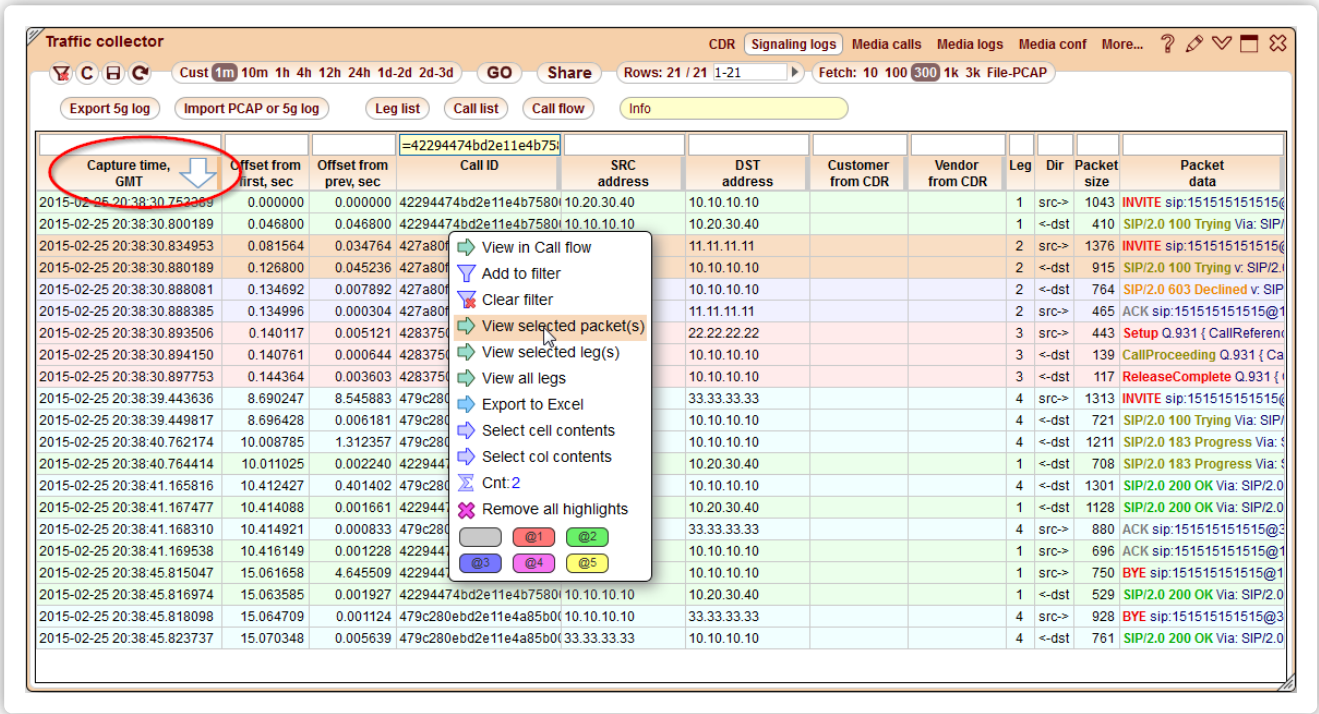
To view the full list of legs recognized in the current log, click **Leg list**. The system will open a new Leg list window.

To view the full list of 1-leg and 2-leg calls based on the current log, click **Call list**. The system will open a new Call list window.

To view the packets of a particular one- or multi-leg call in a timely organized flow form, click Call flow.

2.3. Signaling logs

Once signaling packets are loaded, they are displayed in a table with the predefined sort. By default, the sort is done by the **Capture time** column, this organizes packets correctly on the timeline. All 5gVision table capabilities are supported (like **Filtering**, **Column selection**, **Column resizing**, **Export**. See more in User interface).



To view the contents of an individual packet, right-click on the required row and choose **View selected packet(s)**. Another way to do it is to click the packet content in the **Packet data** column. This will open the Packet viewing window containing information of the required packet. You can ctrl-click several rows to select them all at once and then use the **View selected packet(s)** option to view the selected packets in one window. You can also ctrl-click in the **Packet data** column of the required packets to open several windows with the packet info which might be handy if you want to compare several packets.

To view all packets forming a call leg, right-click on a packet belonging to a required leg and choose **View selected leg(s)**. You can also ctrl-select several packets, belonging to different legs, and view all their packets in the same window (same as multiple selection of packets above).

To view the call flow figure, click the **Call flow** button. This will open the Call flow viewing window. The result will depend on the value in the **Call ID** column filter and the selection of packets in the table.

If a **Call ID** filter is present in a filter field above the respective column:

- If no table rows are selected - show a Call flow for all packets belonging to filtered Call IDs.
- If one row is selected - same as above, show a Call flow for all packets belonging to filtered Call IDs.
- If several rows are selected - show a Call flow for all packets with the same Call IDs as the chosen ones. This way you may choose to show only certain legs out of several present in a log table. No need to choose all the packets in a leg, one packet will be enough to show a full leg.

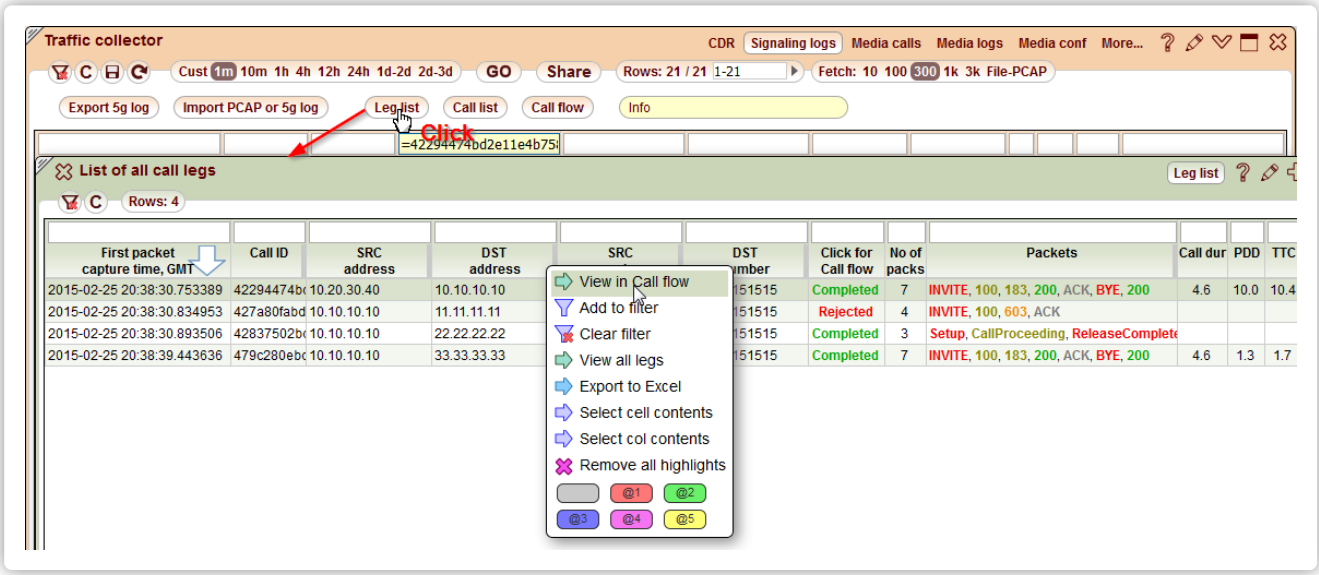
If the **Call ID** filter is empty:

- If no table rows are selected - show a Call flow for the leg with the Call ID of the first packet in a table.
- If one row is selected - show a Call flow for all packets with the same Call ID as the selected packet.
- if several rows are selected - show a Call flow for all packets with the same Call IDs as the chosen ones.

Please note that it is possible to filter SRC/DST IPs using whole networks, like this: =10.20.30.55/24. Network filtering works only with = or != signs.

2.4. Leg list

To view all legs in the currently displayed log, click the **Leg list** button. The system will open a new window showing Call ID, leg SRC and DST addresses and the list of packets constituting a leg.

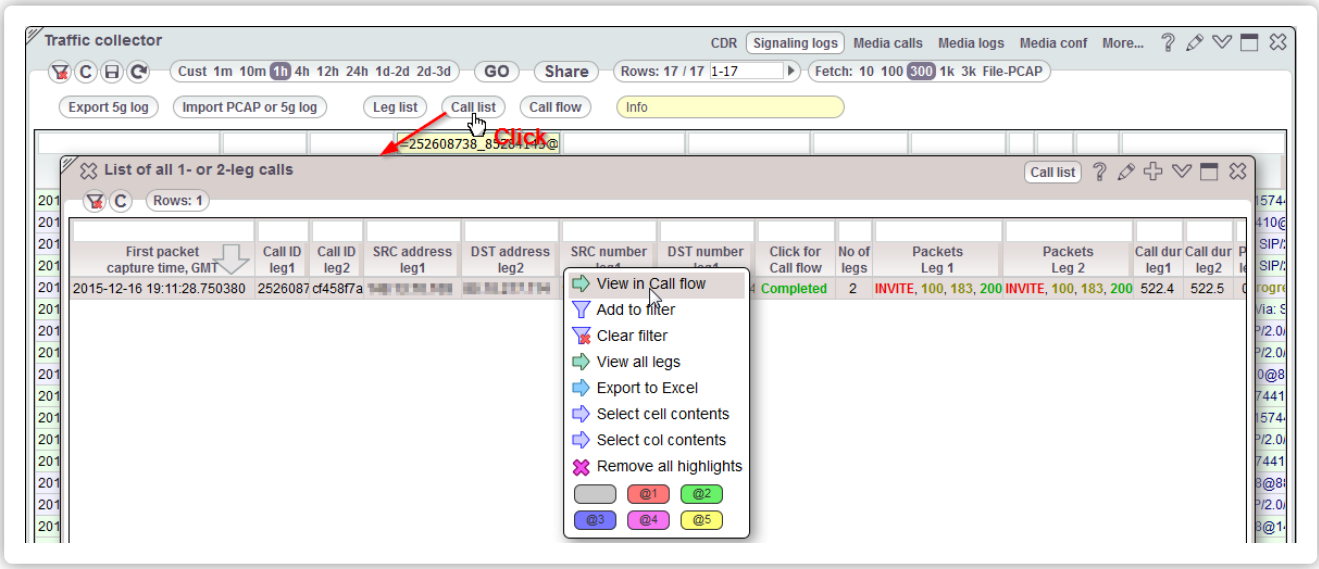


You may open the Call Flow window for the desired leg using the link in the leg status column or with the help of the pop-up menu.

To view the leg's packets (see Packet viewing), you may use the pop-up menu or click the content of the **Packets** column.

2.5. Call list

To view all 1 and 2-legged calls in the currently displayed log, click the **Call list** button. The system will open a new window showing leg parameters, such as Call ID, legs' SRC and DST addresses and the list of packets constituting the first and the second leg.

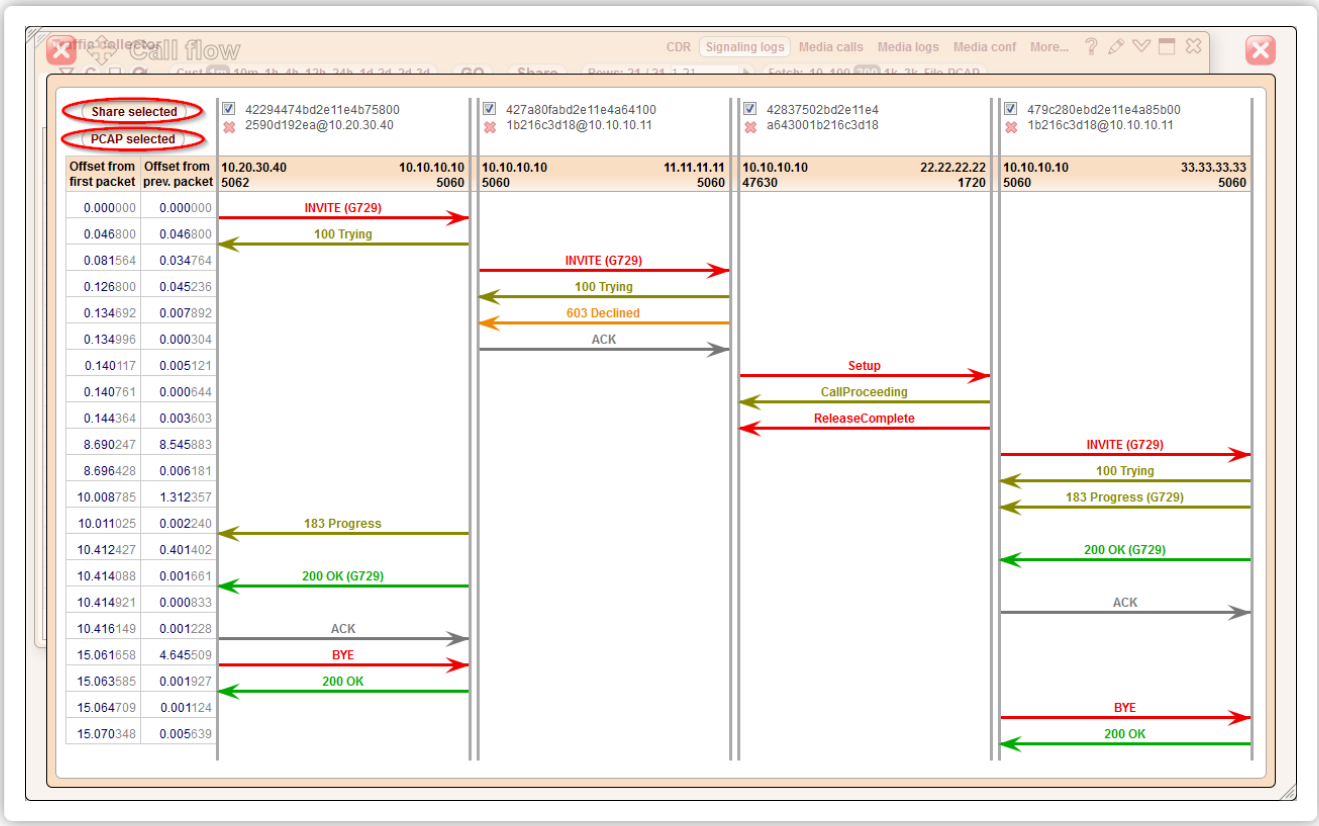


You may open the Call Flow window for the desired leg using the link in the leg status column or with the help of the pop-up menu.

To view the first or the second leg's packets (see Packet viewing), you may use the pop-up menu or click the content of the **Packets Leg N** column.

2.6. Call flow

The **Call flow** window graphically presents the call as a series packet exchanges between switches.



5gVision parses the packets and automatically divides the call into a number of legs, taking into account Call IDs and IPs involved. The system forms a new leg whenever any address or port in a SRC IP - DST IP pair is changed. Clicking on the Call ID link on top of the leg column or on the individual packet name will open a new Packet viewing window showing all packets that comprise the leg or a single packet respectively.

You may also remove the undesired packets from the displayed call flow by clicking the red cross next to the leg ID.

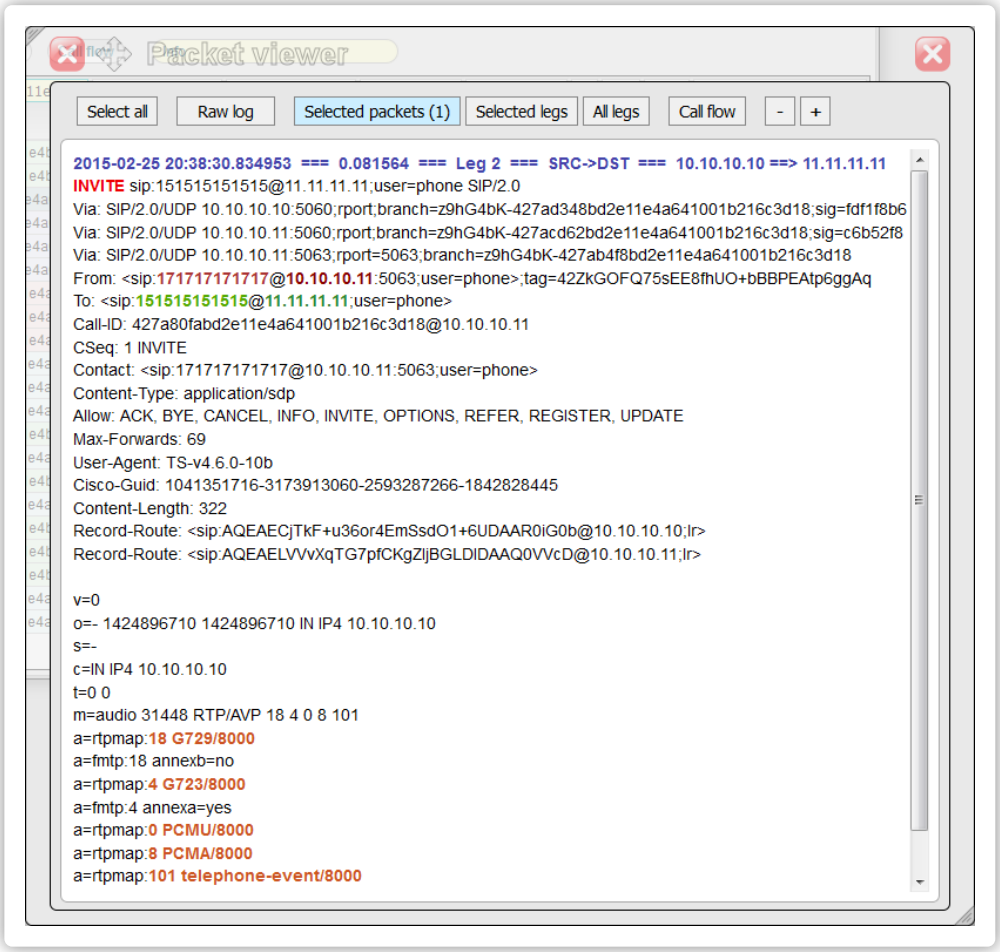
You may also resize the window to display all legs at the same time. Double click on the resize icon to revert the window to the default height and width.

The window contains the **Share selected** button which allows you to share the required legs (marked with checkboxes) as a **Shared link** (see Shared links). This feature comes the additional benefits on top of the usual ones of the shared links - you may hide your partners and send these logs to your vendor and vice versa which is much more convenient than editing the required bits out of raw logs.

There is also the **PCAP selected** button that lets you export the selected legs to a pcap file.

2.7. Packet viewing

The packet viewing window presents packet content in 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 a single leg or the whole call.



The toolbar at the top of the window allows the user to do the following:

- Select the whole text (for subsequent copying) with the help of the **Select all** button.
- Disable or enable text formatting with the help of the **Raw log/Formatted** button.
- Show the selected packet(s) (**Selected packets**), the leg to which the packet(s) belong (**Selected legs**) or all legs in the Signaling logs (**All legs**, up to 1000 packets in total).
- Switch to viewing the call in the Call flow window.

For your convenience it is possible to change the font size using the **+/-** buttons.

It is possible to expand or collapse a packet body in a packet viewer window by clicking on its header (INVITE, etc.).

3. Media collector

The media collector gathers media packets in real time and lets you listen to conversations in any codec.

3.1. Overview

The **Media collector** module gathers media packets in real time for pre-defined IP addresses and number masks, either fully or randomly, and allows users to listen to the recorded media in most commonly-used codecs.

Capturing can work in 2 modes:

- You may set up signaling IPs and number masks for which the media will be recorded randomly. To insure that small customers, vendors, or areas get a certain number of calls recorded each hour, you may set this minimal number of calls per each object. Thus, small objects will have at least the minimum, large object with a lot of traffic will have hundreds or thousands of calls recorded every hour.
- You may force the system to record the next 5/10/20 calls in a row for specific IPs/numbers, for instance, if you are making a call and want to be sure it will be recorded.

Since media is recorded randomly and only for a short initial interval (we recommend 60-120 seconds) - it won't create too much additional load to the system, even if you want to monitor quality for all your customers and vendors.

Usually, 10-20 calls per hour is enough to understand what is going on with a specific vendor->area combination, there is no need to record absolutely every call.

The **Media collector** module requires the Signaling collector module installed to function.

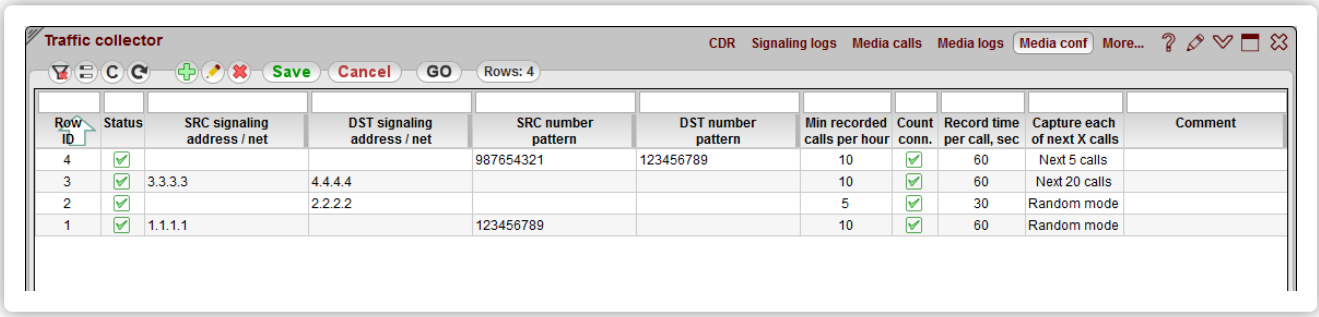
IPs and number masks to collect media for are configured in the Media conf table.

The resulted raw packets can be viewed in the Media logs table, and full recorded calls can be listened to in the Media calls table.

3.2. Media conf

The **Media conf** 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 full mode.



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
4	✓			987654321	123456789	10	✓	60	Next 5 calls	
3	✓	3.3.3.3	4.4.4.4			10	✓	60	Next 20 calls	
2	✓		2.2.2.2			5	✓	30	Random mode	
1	✓	1.1.1.1		123456789		10	✓	60	Random mode	

The user may define the following settings:

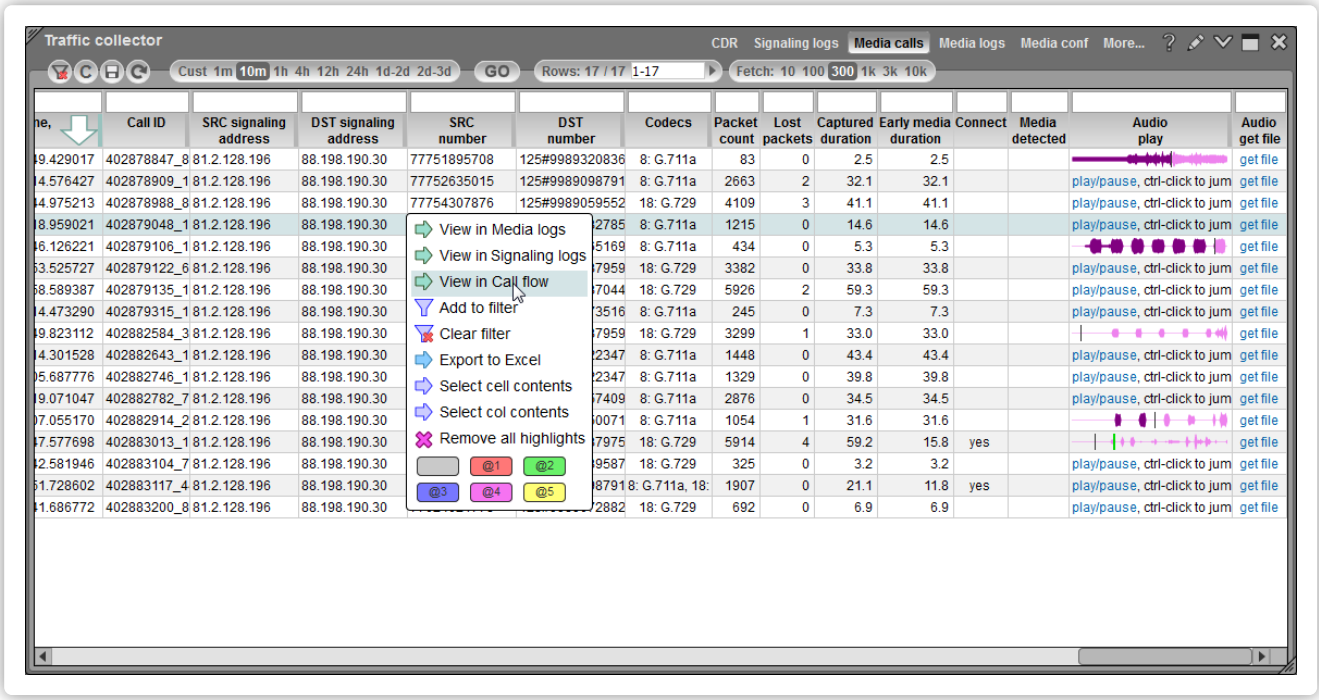
- **SRC/DST signaling address / net** - the calls from/to these addresses will be considered for media recording.
- **SRC/DST number pattern** - the calls with these SRC/DST number patterns will be considered for media recording.
- **Min recorded calls per hour** - the sniffer will try to record this number of calls each hour. Without this setting, objects with small traffic may not have enough calls recorded in a random mode, as they will be competing for the recording slots with much larger objects.
- **Record time per call, sec** - the duration of a sample to be recorded, we recommend 60-120 seconds. The longer are the recorded calls, the less calls will be recorded per hour.
- **Capture each of next X calls** - when recording calls, the system may work in two modes. In the **Random mode** calls to be recorded will be chosen randomly. In the **Next 5/10/20 calls** mode the system will record the next 5, 10, or 20 calls in a row once the setting is applied, and then switch to the **Random mode** again.

Please note that if you change the settings, it may take up to a minute for a sniffer to pick them up.

With the help of a right-click menu, you may view pre-filtered recorded calls by clicking on the **View in Media calls** menu option.

3.3. Media calls

The Media calls table contains recorded calls in a playback-ready format. You may easily find a call you need filtering by IPs or numbers.



To display the recorded calls, click the period you want to investigate in the interval selector.

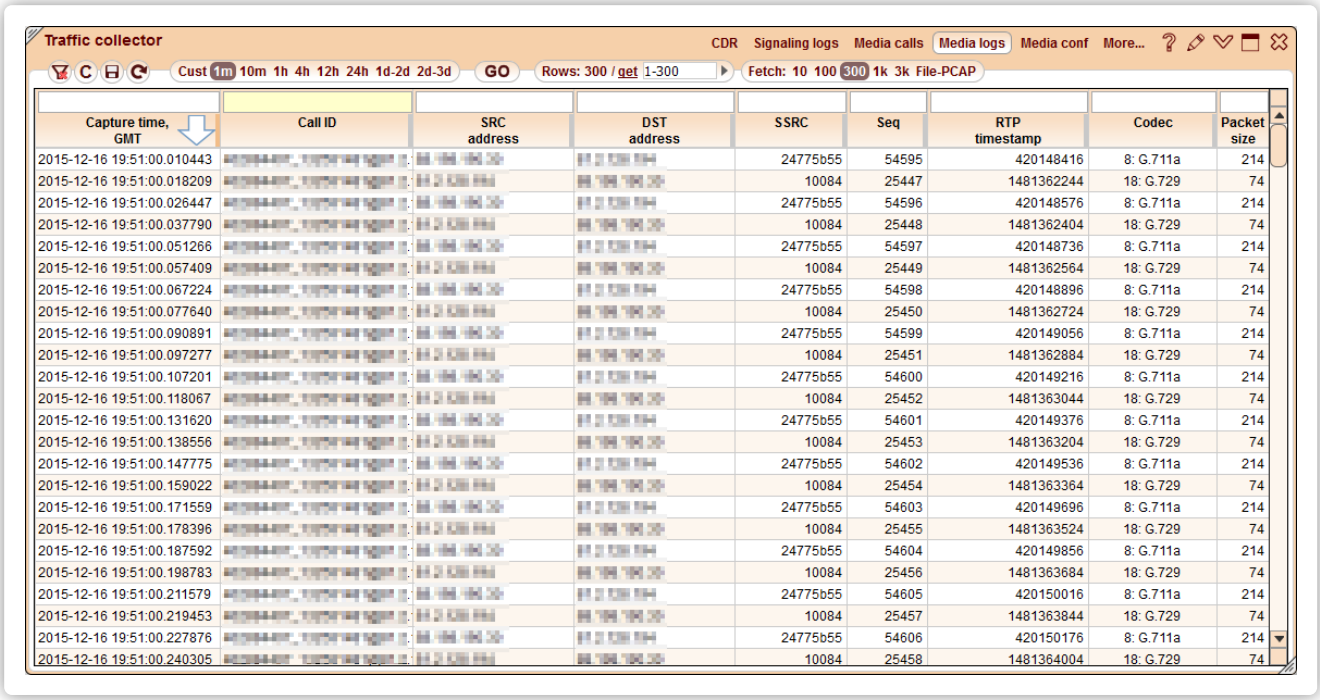
You may play back the call by clicking the **play/pause** button in the **Audio play** column. The system will display the graphical representation of a sound stream. To pause the file, click the field again. **Ctrl-click** on the sound bar will jump playback to a click position.

You may also download the file by clicking the **Get file** link in the **Audio get file** column.

With the help of a right-click menu, you may view the call in Media logs or Signaling logs and display the Call flow for its signaling packets.

3.4. Media logs

This table contains data on raw media packets collected by the system.



Capture time, GMT	Call ID	SRC address	DST address	SSRC	Seq	RTP timestamp	Codec	Packet size
2015-12-16 19:51:00.010443	[illegible]	[illegible]	[illegible]	24775b55	54595	420148416	8: G.711a	214
2015-12-16 19:51:00.018209	[illegible]	[illegible]	[illegible]	10084	25447	1481362244	18: G.729	74
2015-12-16 19:51:00.026447	[illegible]	[illegible]	[illegible]	24775b55	54596	420148576	8: G.711a	214
2015-12-16 19:51:00.037790	[illegible]	[illegible]	[illegible]	10084	25448	1481362404	18: G.729	74
2015-12-16 19:51:00.051266	[illegible]	[illegible]	[illegible]	24775b55	54597	420148736	8: G.711a	214
2015-12-16 19:51:00.057409	[illegible]	[illegible]	[illegible]	10084	25449	1481362564	18: G.729	74
2015-12-16 19:51:00.067224	[illegible]	[illegible]	[illegible]	24775b55	54598	420148896	8: G.711a	214
2015-12-16 19:51:00.077640	[illegible]	[illegible]	[illegible]	10084	25450	1481362724	18: G.729	74
2015-12-16 19:51:00.090891	[illegible]	[illegible]	[illegible]	24775b55	54599	420149056	8: G.711a	214
2015-12-16 19:51:00.097277	[illegible]	[illegible]	[illegible]	10084	25451	1481362884	18: G.729	74
2015-12-16 19:51:00.107201	[illegible]	[illegible]	[illegible]	24775b55	54600	420149216	8: G.711a	214
2015-12-16 19:51:00.118067	[illegible]	[illegible]	[illegible]	10084	25452	1481363044	18: G.729	74
2015-12-16 19:51:00.131620	[illegible]	[illegible]	[illegible]	24775b55	54601	420149376	8: G.711a	214
2015-12-16 19:51:00.138556	[illegible]	[illegible]	[illegible]	10084	25453	1481363204	18: G.729	74
2015-12-16 19:51:00.147775	[illegible]	[illegible]	[illegible]	24775b55	54602	420149536	8: G.711a	214
2015-12-16 19:51:00.159022	[illegible]	[illegible]	[illegible]	10084	25454	1481363364	18: G.729	74
2015-12-16 19:51:00.171559	[illegible]	[illegible]	[illegible]	24775b55	54603	420149696	8: G.711a	214
2015-12-16 19:51:00.178396	[illegible]	[illegible]	[illegible]	10084	25455	1481363524	18: G.729	74
2015-12-16 19:51:00.187592	[illegible]	[illegible]	[illegible]	24775b55	54604	420149856	8: G.711a	214
2015-12-16 19:51:00.198783	[illegible]	[illegible]	[illegible]	10084	25456	1481363684	18: G.729	74
2015-12-16 19:51:00.211579	[illegible]	[illegible]	[illegible]	24775b55	54605	420150016	8: G.711a	214
2015-12-16 19:51:00.219453	[illegible]	[illegible]	[illegible]	10084	25457	1481363844	18: G.729	74
2015-12-16 19:51:00.227876	[illegible]	[illegible]	[illegible]	24775b55	54606	420150176	8: G.711a	214
2015-12-16 19:51:00.240305	[illegible]	[illegible]	[illegible]	10084	25458	1481364004	18: G.729	74

To export the filtered data for the chosen interval into a Wireshark-readable PCAP format, please choose **File-PCAP** in the row count selector and click **GO**.

4. IP whitelist

The IP whitelist helps you detect intrusions to your VoIP network analyzing all the IP addresses collected from the signaling packets.

4.1. Overview

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. IP whitelist can be accessed by adding a **IP whitelist** screen.

This feature might be useful to catch any unauthorized traffic originating from your server, either from your own VoIP switch, if it is cracked and the config is changed, or from a new switch installed by intruders. In the latter case, it could take a carrier several days till they catch the extra traffic that is originating from their IPs open at their vendors. No such traffic will be visible in carrier's switch or billing. This is why this whitelist should be created independently, on a different server (a 5gVision logging server) the intruders have no access too, as any precautions at your switch will be bypassed, if this server with a VoIP switch is compromised.

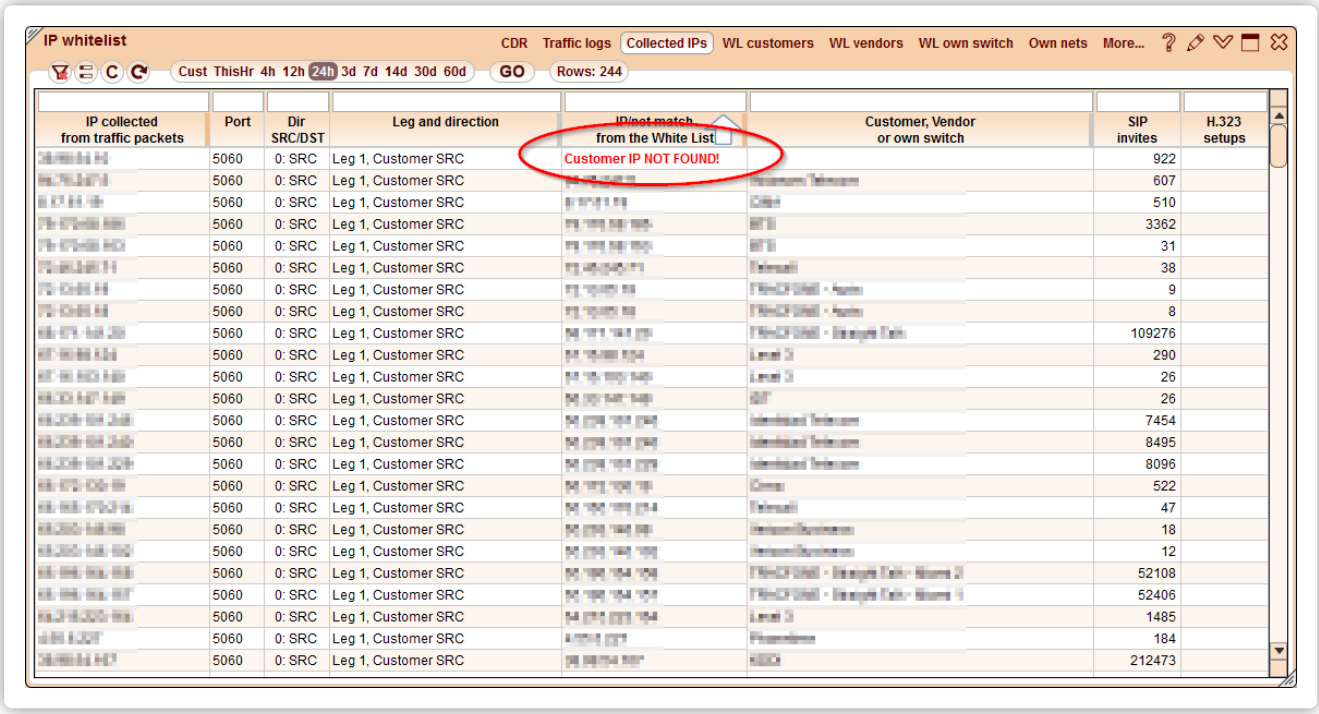
If an IP whitelist module is purchased, log collection via mirroring is a more preferred method of setting up the logger (see Collection methods), as in case of collecting logs over SSH, the attackers can block logs collection, once the softswitch server is compromised. This is not possible with mirroring, as 5gVision will be able to get and analyze all the packets traveling through your network.

The main table of the **IP whitelist** module is Collected IPs, where you can see all collected IPs with showing leg, direction, customer, vendor.

Configuration of the **IP whitelist** module is made via the corresponding Whitelist config tables.

4.2. Collected IPs

All collected IPs are added to the **Collected IPs** table.



IP collected from traffic packets	Port	Dir SRC/DST	Leg and direction	IP/not match from the White List	Customer, Vendor or own switch	SIP invites	H.323 setups
[illegible]	5060	0: SRC	Leg 1, Customer SRC	Customer IP NOT FOUND!		922	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	607	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	510	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	3362	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	31	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	38	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	9	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	8	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	109276	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	290	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	26	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	26	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	7454	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	8495	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	8096	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	522	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	47	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	18	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	12	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	52108	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	52406	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	1485	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	184	
[illegible]	5060	0: SRC	Leg 1, Customer SRC	[illegible]	[illegible]	212473	

The system distinguishes packets on basis of several parameters:

- **IP collected from traffic packets** - source or destination IP address of the packet.
- **Port** - source or destination port of the packet.
- **Dir SRC/DST** - source or destination information of the packet was taken into account.

So if the system collects packets with an identical IP and port there are still can be 2 records in the table differentiated by direction.

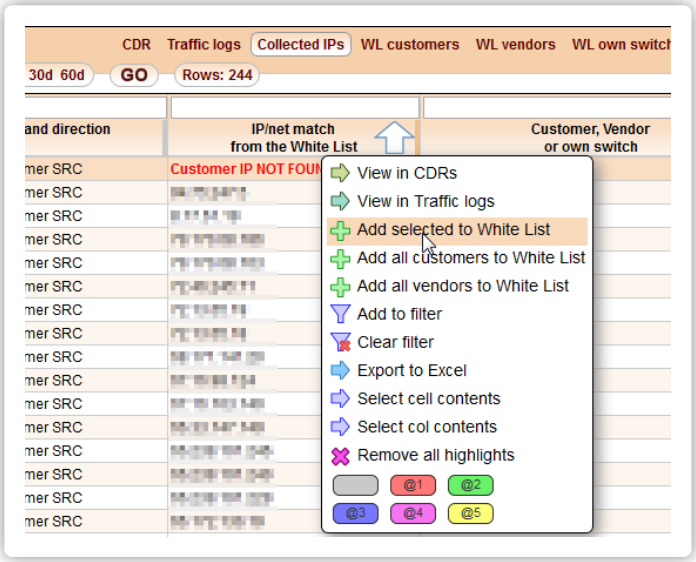
The table contains records with the following information included:

- **Leg and direction** - leg number and direction of the packet, detected on basis of correlation of the **Dir SRC/DST** and **Customer,**

Vendor or own switch parameters.

- **IP net match from the White List** - IP or IP net against which the collected IP was matched. If the collected IP does not match any defined pattern, the red label **IP NOT FOUND!** is displayed.
- **Customer, Vendor or own switch** - entity to which the matched IP is supposed to belong.
- **SIP invites** and **H323 setups** - Number of SIP INVITEs or H.323 SETUPs that have sent to/arrived from the collected IP within the specified interval.

For your convenience, it is possible to add the desired IP(s) into whitelist from this screen by selecting the required row or rows, invoking the pop-up menu and selecting **Add selected to White List**.



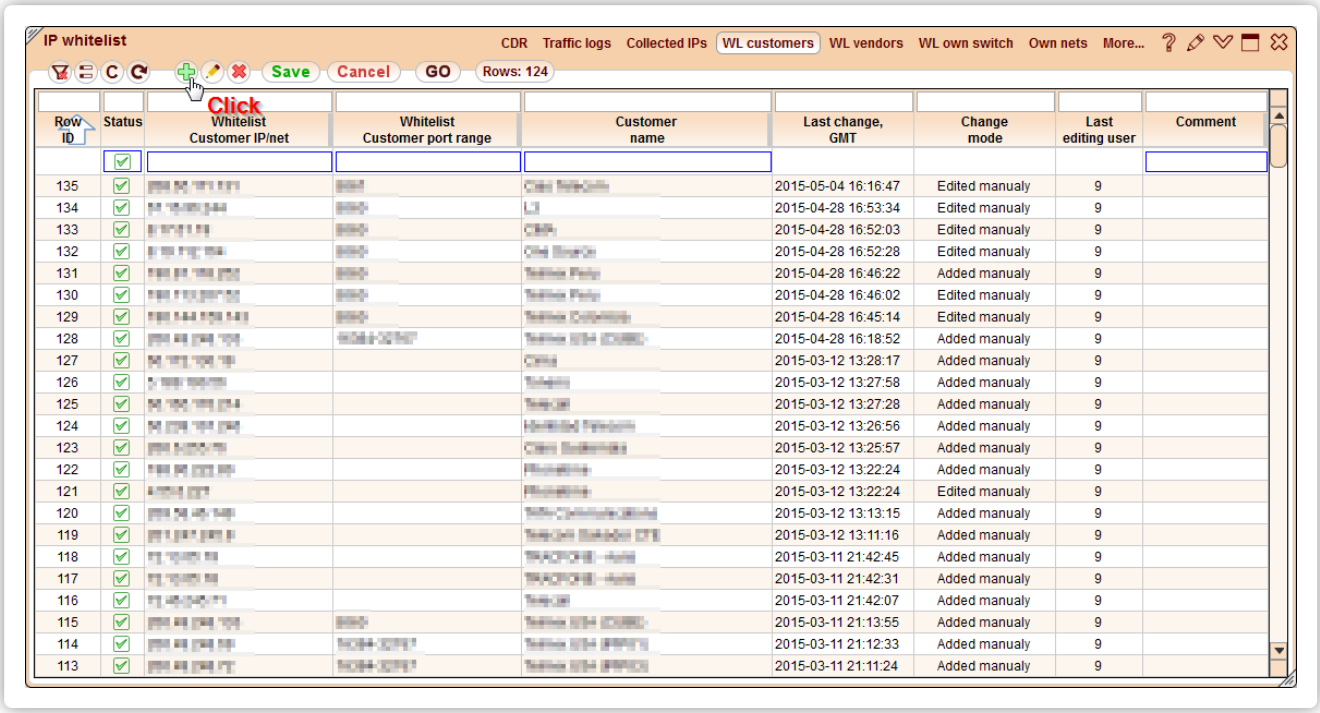
4.3. Whitelist config

IP whitelist configuration consists of several tables:

- **WL customers** - needed to detect unauthorized traffic not originating from your customer.
- **WL vendors** - needed to detect unauthorized traffic terminating to vendors.
- **WL own switch** - needed to detect pirate switches installed on the same server as your own switch.
- **Own nets** - needed to detect which IPs belong to customers/vendors and can never be assigned to a pirate switch in your network.

By default all users can edit these tables. But it is possible to allow access only for certain users to add/edit/remove customers, vendors, own switches and nets from the whitelist. Please send a request to 5gVision support for this purpose. You may manually add IPs and nets against which the collected IPs are matched in the **WL customers**, **WL vendors** and **WL own switch** tables. All auto-added IPs via the Collected IPs screen will also appear in the former two tables.

To add an allowed IP or IP net to the **WL customers** table, please click the green plus.



A new record will be added to the table, with the following parameters:

- **Status** - whether the record is enabled (and takes part in IP matching) or disabled.
- **Whitelist Customer IP/net** - define the IP or net against which the collected IPs will be tested.
- **Whitelist Customer port range** - define the port or port range against which the collected ports will be tested.
- **Customer name** - optional information about the customer, to which the IP belongs.
- **Last change, GMT** - date and time when the record was added or edited the last time.
- **Change mode** - If the IP was added through this screen, the system will show **Added manually** in this column. If the IP was added from the Collected IPs screen with the help of a pop-up menu, the column will have the **Added from collected** text.
- **Last editing user** - ID of a user who edited the record at the latest.
- **Comment**.

To save the added row, click **Save**. To discard the changes before they are saved, click **Cancel**.

To edit or remove a record, select it in the table and click the pen or red cross button respectively.

The **WL vendors** and **WL own switch** tables have the similar parameters.

In the **Own nets** you should just enter full owned networks where your VoIP switches are located.