RTSP / RTP

RTSP traffic analysis when capturing a stream from the IP camera

We use the 'rtsp' filter to see RTSP traffic between WCS and the IP camera.

		log.pcap [Wireshark	1.12.0 (v1.1	2.0-0-g4fab41a fro	om master	-1.12)]	- 🗆 ×
<u>File Edit View G</u> o	<u>Capture</u> <u>Analyze</u> <u>Statist</u>	tics Telephony <u>T</u> ools	Internals He	lp			
•••	E X 2 9,	🗢 🛸 😜 ዥ 🕹		Ð. Q. Q. 🖭 🖥	¥ 🛛 🖪	* 🔯	
Filter: rtsp			✓ Exp	ression Clear	Apply	Save	
No. Time	Source	Destination	Protocol L	ength Info			
33 13.359663	188.40.69.75	.211.205.45	RTSP	191 OPTIONS rt	tsp://dli	nk2103.noip.me/live1.sdp	RTSP/1.0
35 13.452717	.211.205.45	188.40.69.75	RTSP	218 Reply: RTS	SP/1.0 20	00 OK	
37 13.453385	188.40.69.75	.211.205.45	RTSP	217 DESCRIBE I	rtsp://dl	ink2103.noip.me/live1.sd	p RTSP/1.0
38 13.546205	.211.205.45	188.40.69.75	RTSP	227 Reply: RTS	SP/1.0 40	1 Unauthorized	
39 13.548327	188.40.69.75	. 211. 205. 45	RTSP	416 DESCRIBE	rtsp://dl	ink2103.noip.me/live1.sd	p RTSP/1.0
40 13.643064	.211.205.45	188.40.69.75	RTSP/SE	869 Reply: RTS	SP/1.0 20	0 ок	
41 13.669579	188.40.69.75	.211.205.45	RTSP	242 SETUP rts	p://dlink	2103.noip.me/live1.sdp/t	rack2 RTSP/1.0
42 13.765271	.211.205.45	188.40.69.75	RTSP	269 Reply: RTS	SP/1.0 20	0 ок	
43 13.766140	188.40.69.75	.211.205.45	RTSP	261 SETUP rts	p://dlink	2103.noip.me/live1.sdp/t	rack1 RTSP/1.0
44 13.862095	.211.205.45	188.40.69.75	RTSP	269 Reply: RTS	SP/1.0 20	00 OK	
60 14.606291	188.40.69.75	.211.205.45	RTSP	226 PLAY rtsp	://dlink2	103.noip.me/live1.sdp RT	SP/1.0
120 17.399631	.211.205.45	188.40.69.75	RTSP	302 Reply: RTS	SP/1.0 20	00 OK	
1.00							
<							,
🔵 💅 Frame (frame), 19	ayed: 12 (0,3%) · Load	time: Pro	file: Default				

RTP traffic from the RTSP IP camera

After a connection is established via RTSP, usual RTP traffic starts coming from the IP camera.

Wireshark: RTP Streams							- 🗆 🛛		
	Detect	ed 2 RTP strea	ms. Choose one for fo	rward and rever	se <mark>direct</mark> ion	for analysis			
 Payload 	 Packets 	Lost	 Max Delta (ms) 	 Max Jitt 	er (ms)	 Mean Jitter (ms) 	◆ Pb?	•	
RTPType-96	2085	0 (0,0%)	0,000000	0,00000	0	0,000000	Х		
g711U	62	0 (0,0%)	168,264000	17,1903	20	15,222839			
<								>	
		Select a Select	forward stream with le a reverse stream with	ft mouse buttor Ctrl + left mous	n, and then e button				
Unselect	Find Reverse	Save <u>A</u> s	Mark Packets	Prepare Filter	<u>C</u> opy	Analyze	Close		

If we filter the same dump by UDP and follow the instructions from the SRTP traffic analysis section, we can find that there is SRTP traffic flowing from the WCS server to the browser. This being said, if you see video in your browser this means RTP traffic from the IP camera comes to the WCS server via the successfully established RTSP connection, and further converts to WebRTC / SRTP traffic to display in a browser.

Possible problems

If RTSP and RTP traffic will not flow between the WCS server and the IP camera, video from the camera will not be displayed in the browser. Most likely, you will see just the dark screen.

Troubleshooting

Typically, cameras are set behind NAT, so to connect to the IP camera via RTSP without hassle, you should ass two NAT rules on your router the IP camera is connected to. For example, on the Zyxel router these settings will look as follows:



Here, 192.168.1.41 is the IP address of the camera in the local network. The router says it will redirect RTSP queries sent to the corresponding ports to the IP camera.

Then, if you know your external IP address, if you query this address, for instance, rtsp://9.9.9.9:554 you will end up in the RTSP port of your camera. If something goes wrong, contact your intervye provider. If you have dynamic IP address, you can use the dynamic DNS service. Then, you will be able to address using the host name, so IP address tracking is not necessary. Example: rtsp://myhost.noip.com:554.

If all traffic goes through, but video still does not play and logs contain many packet lost errors, check MTU. Some IP cameras send large enough UDP packets containing video that might be cut off by the MTU of the router. Use this command: ping -f -l 1460 8.8.8.8. Replace 8.8.8.8 with any external host that responds to pinging. If packets do not pass through, perform the same test with the router: ping -f -l 1460 192.168.1.1, where 192.168.1.1 is the address of the router. If packets do reach the router and do not reach the external host, this means the MTU of the router is not large enough. Use the router settings to increase its value to standard 1500. For example, for Zyxel you can set MTU in the console:

telnet 192.168.1.1

>show interface ISP >interface ISP ip mtu 1500 >system config-save

CPV.	Telnet 192.168.1.1	-		
(config)) show inte	erface ISP		^	
mac: id index: type: description: state: link: connected: mtu: tx-queue: address: mask: broadcast: global: defaultgw: priority: security-level:	ec:43:f6:01:c1:e5 Switch0/ULAN2 2 ULAN Broadband connection up up yes 1500 1000 255.255.255.240 yes yes 700 public			
Core::Configurator	done.		~	

In this case 'ISP' is a network interface on the router the internet cable of the provider is connected to.

Finally, if after executing the command ping -f -l 1460 192.168.1.1 packets do not reach even the router, check the MTU value in your operating system. For instance, on Windows you can set MTU in the system registry.