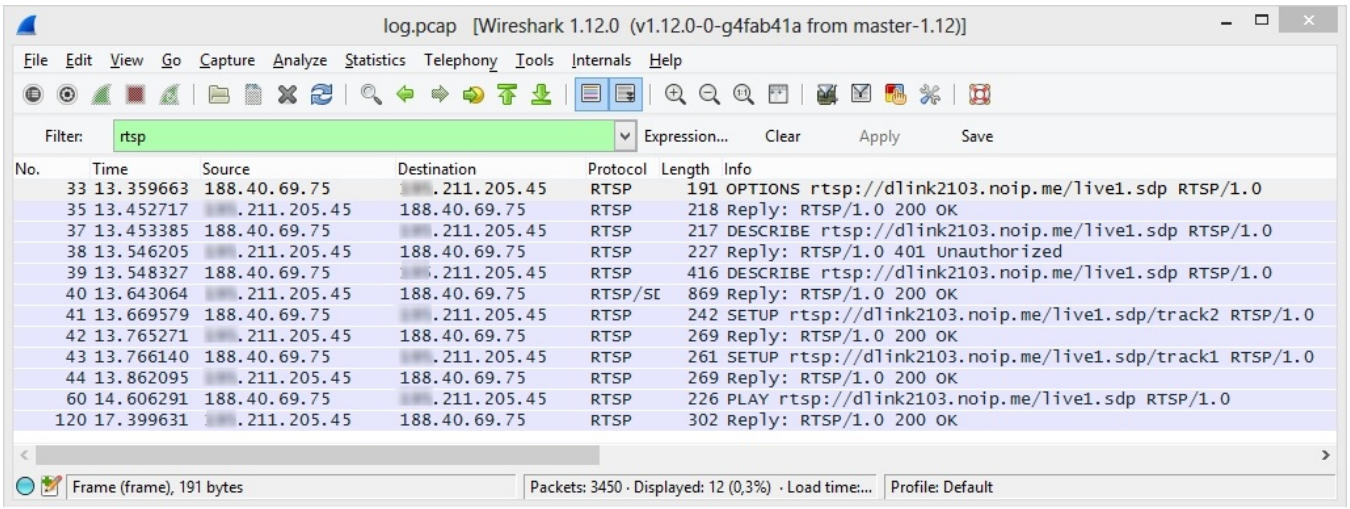
RTSP / RTP

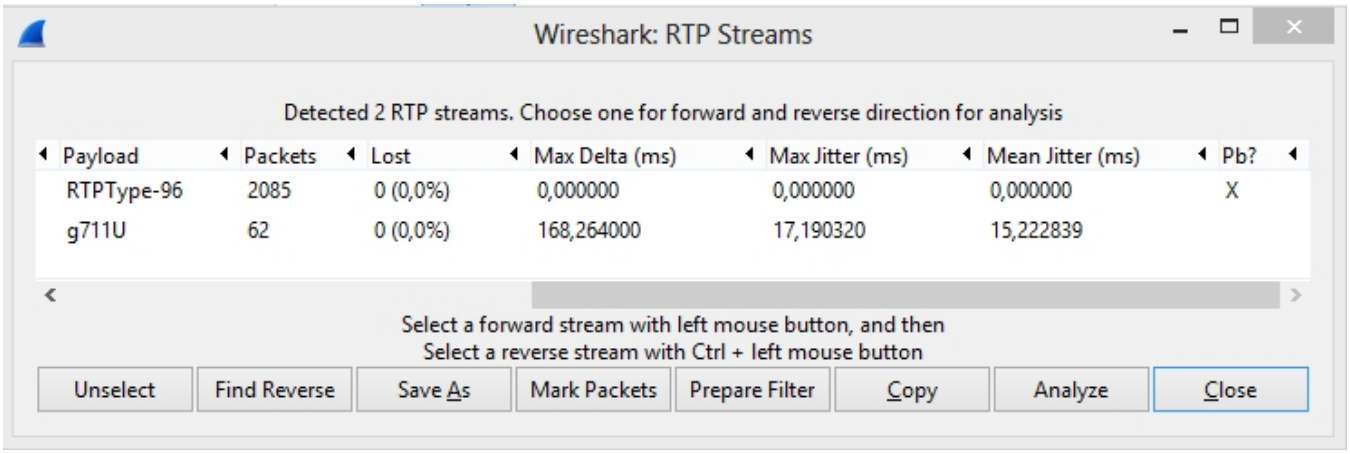
RTSP traffic analysis when capturing a stream from the IP camera

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



RTP traffic from the RTSP IP camera

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



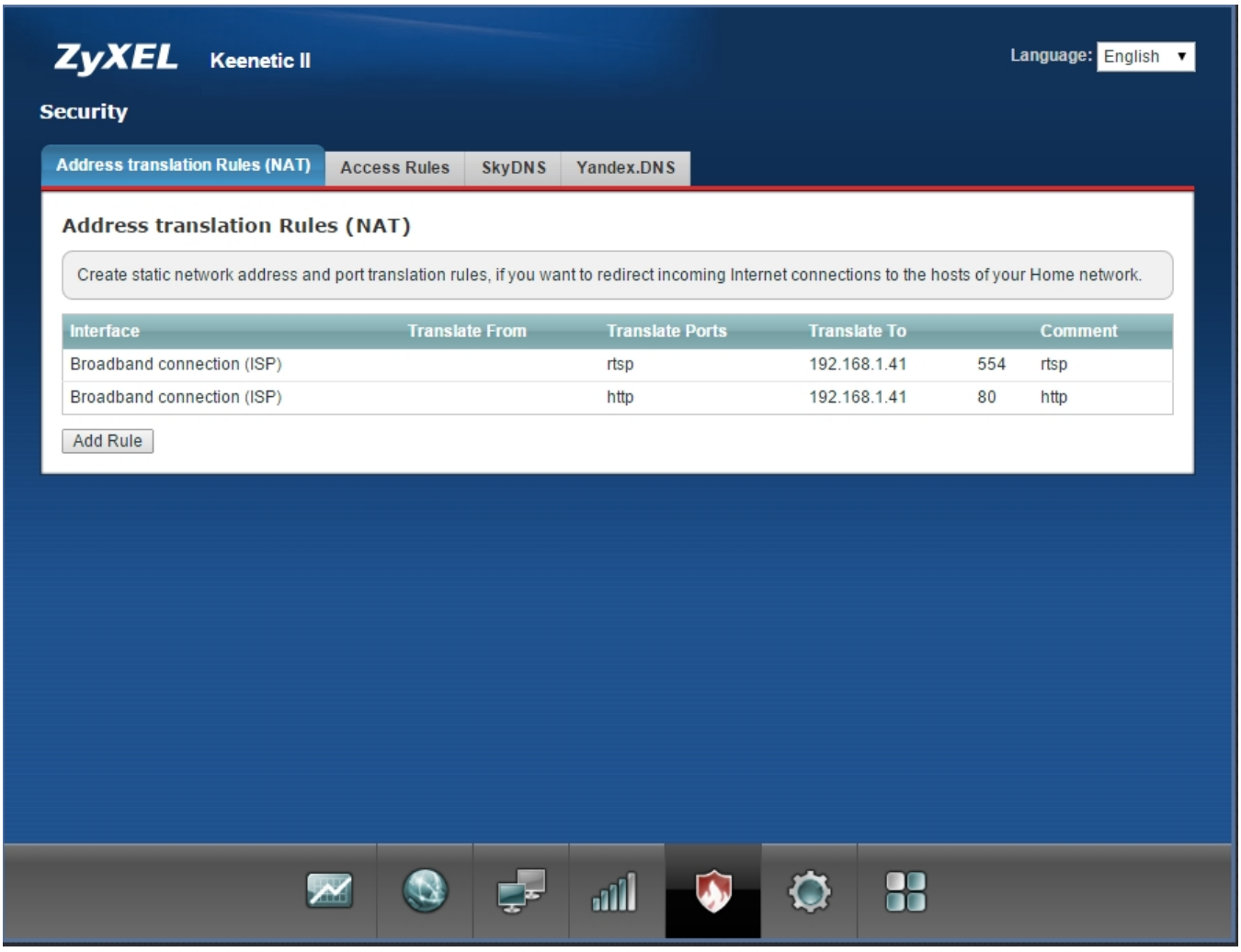
If we filter the same dump by UDP and follow the instructions from the SRTP traffic analysis section, we can find that there is SRTP traffic flowing from the WCS server to the browser. This being said, if you see video in your browser this means RTP traffic from the IP camera comes to the WCS server 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:

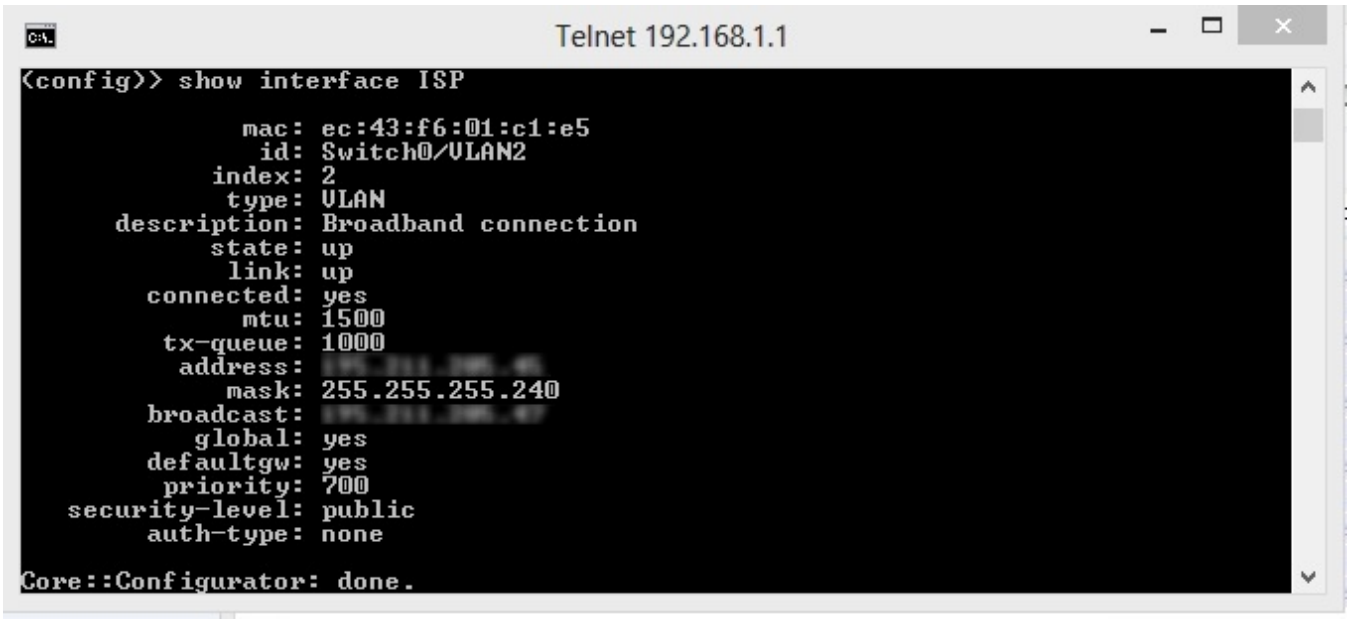


Here, 192.168.1.41 is the IP address of the camera in the local network. The router says it will redirect RTSP queries sent to the corresponding ports to the IP camera.
Then, if you know your external IP address, if you query this address, for instance, rtsp://9.9.9.9:554 you will end up in the RTSP port of your camera. If something goes wrong, contact your интернет 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
```



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.