

# Diagnostics and troubleshooting

In case you experience problems with the server start or availability, refer to the [Starting and stopping](#) section where you can find a thorough description of the server start procedure as well as how to check if it's available and ready for work.

Let's suppose the server is running, accepts connections and all tests show that the server is fine. In this case in order to reveal the reasons for incorrect operation, you should possess enough network protocols knowledge and skills to localize the error and determine its reason: WCS server, web server, SIP server, Firewall et. For example, problems with one-way video are often seen if Firewall blocks ports required to accept media traffic. Prompt localization of such an issue would save time and eliminated the need to inquiry the Flashphoner technical support, and allowed to fix the problem by trivial changing of Firewall rules.

Dealing with such situations require expertise in network protocols and skill in traffic monitoring and dumping tools such as [wireshark](#) on the desktop computer side and [tcpdump](#) on the server side.

In the [Network traffic analysis](#) section there is a flowchart displaying the routes of the traffic between WCS and the web server.

In the [WebRTC](#) section you can find a list of specifications WCS uses to establish WebRTC connections and interact with the SIP server. In order to see if WebRTC or SIP traffic routes normally you should possess deep knowledge of the appropriate specifications: STUN, ICE, DTLS, SRTP, RTP, SIP.

Hence, in many cases localization of issues comes down to making network dumps and analyzing call flow. For example, in case of connection establishing problems you whould check Websocket traffic going to port 8443 of the WCS server. Absence of the traffic signalizes about some problems with web client configuration or incorrect Firewall settings.

[Preparing an error report](#)

[Possible problems and how to solve them](#)

[Accessory tools](#)

[How to get license number](#)

[CPU load investigation](#)

[Stack trace logging](#)

[DNS testing and caching](#)

