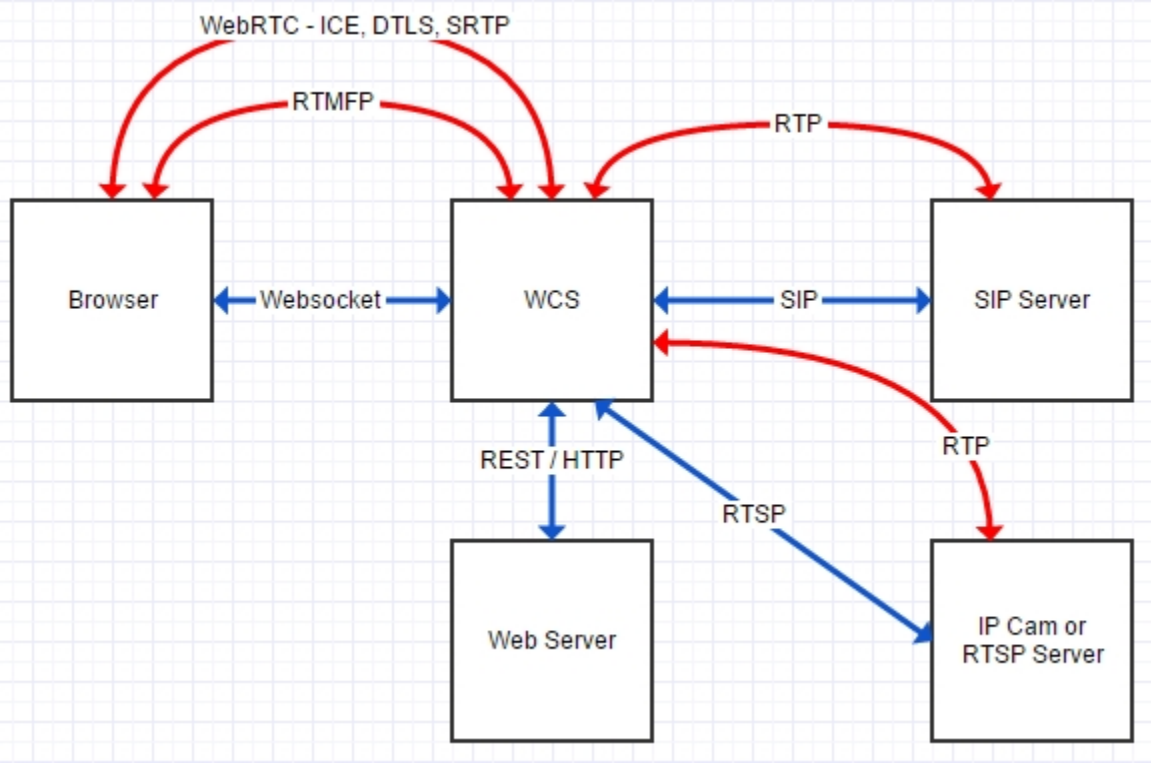
Network traffic analysis

Traffic flow

Traffic flows between four main parts of the system: Browser, WCS, WebServer (backend) and SIP Server. Data move through ports and protocols specified in the Architecture section. The list of default ports can be found in the Server coresection. Also, you can change used ports in the configuration files.

The flowchart below displays flows of signal (blue) and media (red) traffic. Secure traffic sent via, for example, SRTP, HTTPS or RTMFP cannot be decrypted without knowing appropriate keys, but for localizing a malfunction decrypting traffic is usually redundant. Information about its proper flow between all parts of the scheme is often enough.



Therefore, for correct operation of the server, the following traffic types should flow properly:

- Websocket
- REST / HTTP
- SIP
- WebRTC
- ---- ICE
- ---- DTLS
- ---- SRTP
- RTMFP
- RTP
- RTSP / RTP
- RTMP
- HLS

Traffic dump

To make a traffic dump, use the following command

```
tcpdump -i any -s 4096 -w log.pcap
```

Tcpdump allows you to record all traffic including the local REST HTTP that by default heads to http://localhost:8081/EchoApp. To change this address, use application management settings from the command line interface.

Traffic filtering

To filter dumps in Wireshark you can apply the following filters:

```
sip
websocket
ip.src==127.0.0.1 && tcp.dstport==8081
```

The last filter is used for REST / HTTP traffic that locally flows through the port 8081 if the local app EchoApp is queried.