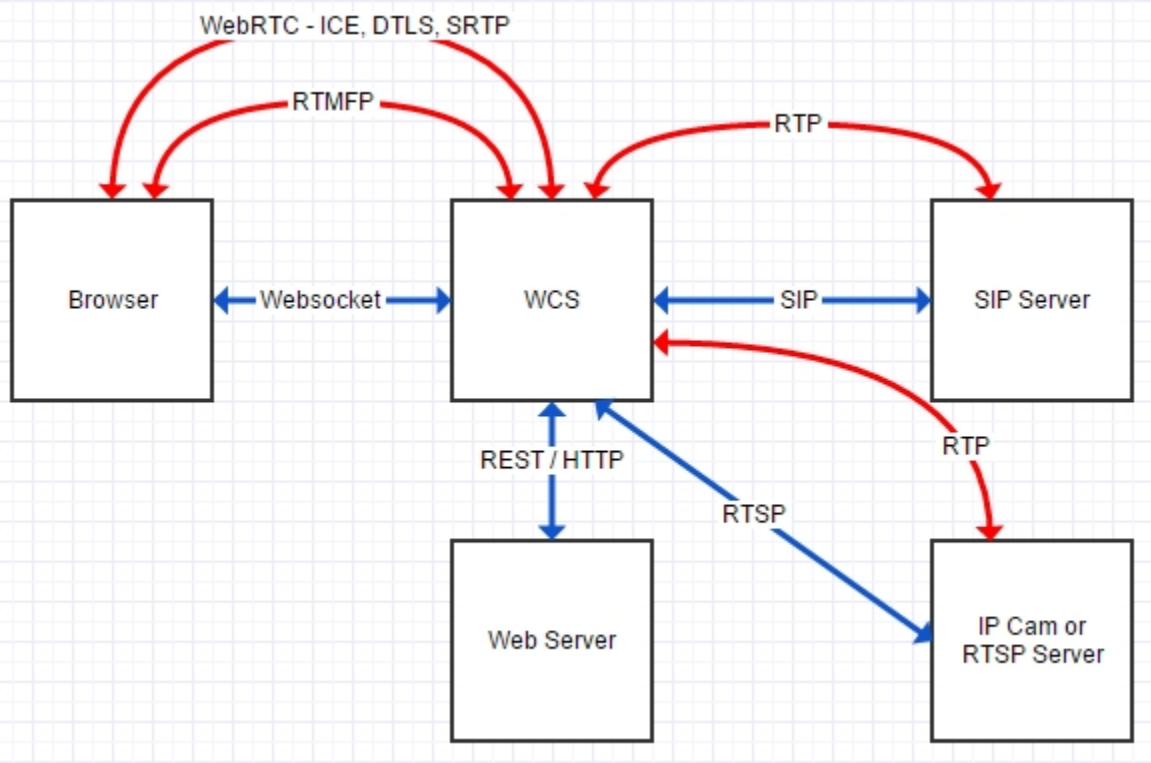
Анализ сетевого трафика

Движение трафика

Трафик двигается между четырьмя основными участниками системы: Browser, WCS, WebServer и SIP Server. Данные ходят по протоколам и портам, указанным в разделе Архитектура. Перечень портов, используемых по умолчанию находится в разделах Ядро сервера и Административный модуль. Используемые порты могут быть также сконфигурированы с помощью конфигурационных файлов.

На диаграмме показаны направления движения сигнального (синим цветом) и медиа (красным цветом) трафика. Защищенный трафик, например SRTP, HTTPS или RTMFP, нельзя расшифровать без знания ключей шифрования, но для локализации неисправности расшифровка трафика, как правило не требуется. Зачастую достаточно информации о его корректном прохождении между участниками схемы.



Таким образом, для корректной работы сервера должен корректно проходить следующий трафик:

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

Захват трафика

Чтобы снять трафик воспользуйтесь командой: tcpdump -i any -s 4096 -w log.pcap. Tcpdump позволяет записать весь трафик включая локальный REST HTTP, который по умолчанию идет на http://localhost:8081/EchoApp. Для изменения этого адреса воспользуйтесь настройками приложений из интерфейса командной строки.

Фильтрация трафика

Для фильтрации дампов в Wireshark можно использовать следующие фильтры:

- sip
- websocket

- ip.src==127.0.0.1 && tcp.dstport==8081

Последний фильтр используется для REST / HTTP трафика, который проходит локально через порт 8081 в случае обращения к локальному приложению EchoApp.