



A note from the student behind this lab

This is an **independent, free, learning-only student project**. It respects every company and vendor, and every trademark belongs to its owner. It is **not affiliated with or endorsed by** any of them.

If anyone has a concern, the content will be removed or corrected promptly: please write via <https://cyphermonkeylabs.com/#contact>. Nothing here is sold, and I am happy to volunteer for any organization.

Ports and transports

SIP uses UDP or TCP on 5060 and TLS on 5061, and a request that does not fit one datagram needs a connection.

The message has to arrive

RFC 3261 section 18 sets UDP and TCP on port 5060 and TLS on port 5061. UDP is why INVITE retransmissions exist: the transaction layer repeats a request that may have been lost.

A request that does not fit in one datagram belongs on a connection-oriented transport. TCP and TLS use Content-Length to find the end of the message. WebSocket, RFC 7118, carries the same SIP messages with transport tokens WS and WSS.

SIPS is signaling, not media

A sips URI asks for TLS on the signaling hop. The method names, the dialog rules, and the SDP offer do not change because the Via says TLS.

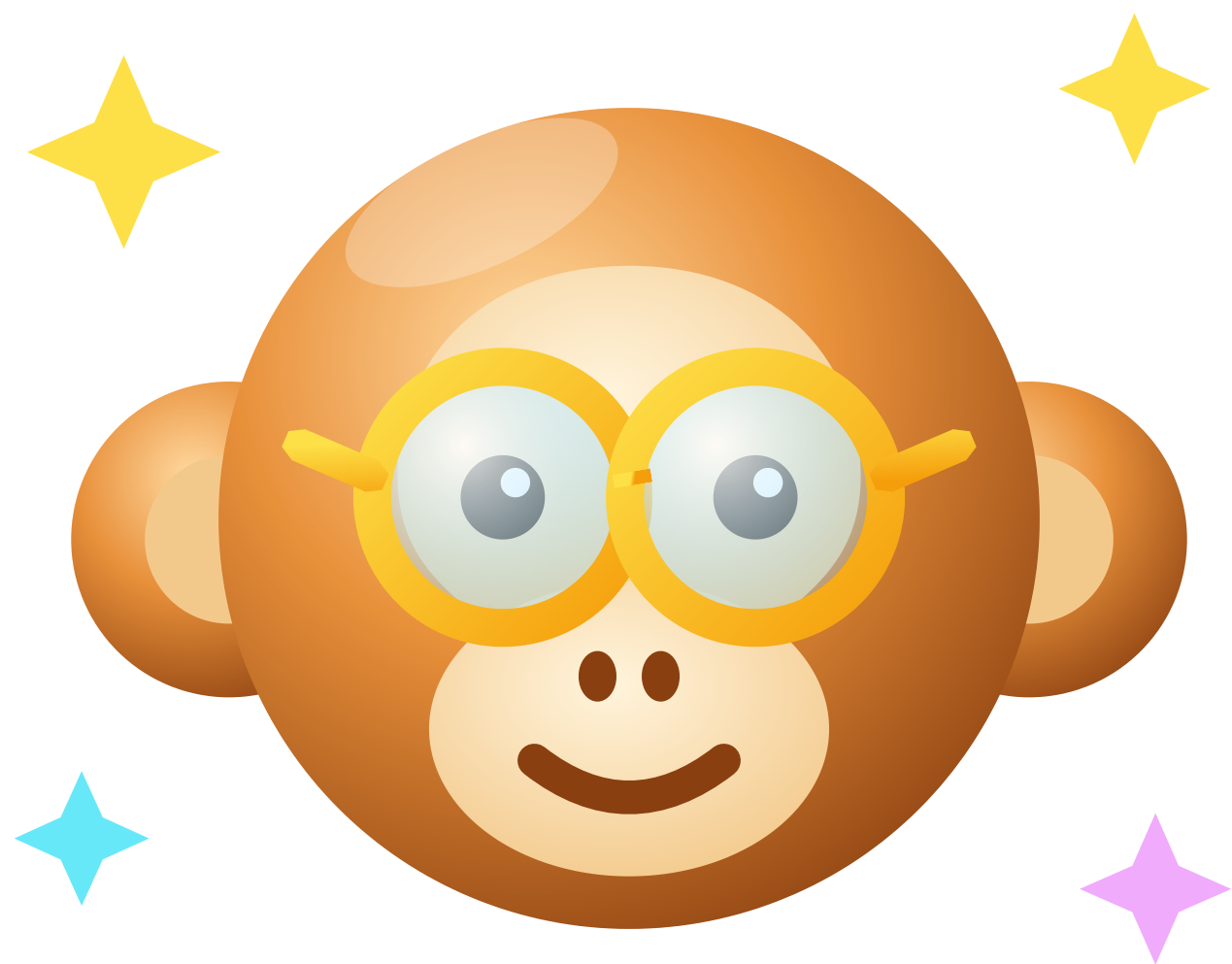
When a deployment encrypts the media, that keying is negotiated in SDP, for example with DTLS-SRTP. Read the Via transport, the sent-by host, and the port before you argue about certificates.

Room: [Ports, transports, and where a request can go](#)

Sources and go deeper

- [RFC 3261 §18](#) — last checked 2026-10
- [RFC 7118](#) — last checked 2026-10
- [RFC 5764](#) — last checked 2026-10
- [RFC 3261 §7](#) — last checked 2026-10
- [RFC 3261 §8](#) — last checked 2026-10

CypherMonkey Labs







© 2026 CypherMonkeyLabs 🐒

[Open app](#) · [View repo](#)