

11 TLS, certificates, SIP

11 TLS, certificates, SIP

Pro tips

? Use TLS 1.2 or higher, a public CA, and a SAN that matches the SBC FQDN. A name mismatch stops the handshake before INVITE.

? OPTIONS from the Teams proxies should receive 200 OK. Missed OPTIONS take the trunk out of service.

? AMR-WB is not offered when media bypass is on. The rest of the codec list is a negotiation, not a wish.

Interview traps

? Arguing about the dial plan while the certificate is still issued to the old hostname.

? Trusting a private CA for Direct Routing. The trunk wants a public certificate.

Cheat sheet

ClientHello -> certificate -> SAN matches FQDN -> Finished

OPTIONS -> 200 OK

INVITE / 100 / 180 / 200 / ACK

RTP follows the SDP: processor or bypass

TCP 5061, not 5060

Facts in the long lessons were checked 14 October 2026. This sheet is a memory aid.

CypherMonkey Labs ? <https://cyphermonkeylabs.com> ? <https://github.com/CypherMonkeyLabs> ?
<https://linktr.ee/cypherMonkey> ? <https://github.com/CypherMonkeyLabs/microsoft-voice-cc-lab-free-university-mesmerizing> ? (c) 2026 CypherMonkeyLabs. Independent educational project, not affiliated with or endorsed by any vendor. Comparison notes describe only public pages this lab opened. They do not rank vendors. Trademarks belong to their owners. MIT code, CC BY-NC-SA content. Contact <https://cyphermonkeylabs.com/#contact>.