



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.

Interop seams

Direct Routing uses the pstnhub proxies on 5061, a certified SBC, and a verified domain. Contact must be an FQDN.

Where the SBC sends signaling

Direct Routing signaling uses sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com, and sip3.pstnhub.microsoft.com on port 5061. TLS 1.2 or later is required, and the SBC is a certified SBC.

The synthetic INVITE targets sip.pstnhub.microsoft.com:5061 from sbc1.example.com. The real routing among the three proxies is in the plan and protocol articles.

Names the proxy will accept

The Contact must be an FQDN. If Contact is an IP address the proxy returns 403. The domain on the trunk must be a verified tenant domain, not a name ending in onmicrosoft.com.

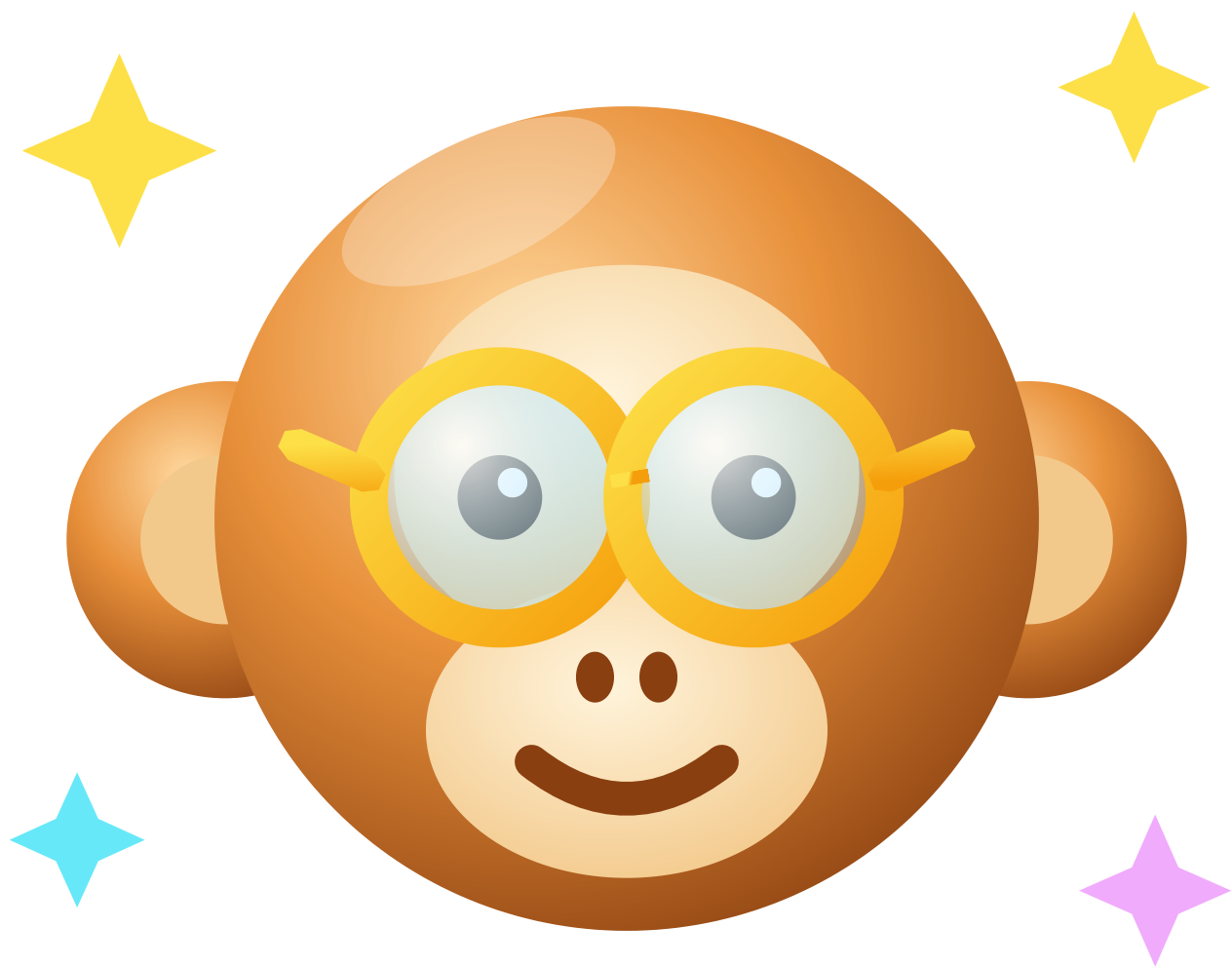
The protocols article says the SIP proxy does not support RFC 5923 connection aliasing. Microsoft says wildcard names in the certificate CN or SAN are supported for Direct Routing.

Room: [Teams Direct Routing signaling](#)

Sources and go deeper

- [Plan Direct Routing](#) — last checked 2026-10
- [Direct Routing SIP protocol](#) — last checked 2026-10
- [Direct Routing definitions and RFCs](#) — last checked 2026-10
- [RFC 5923](#) — last checked 2026-10

CypherMonkey Labs







© 2026 CypherMonkeyLabs 🐒

[Open app](#) · [View repo](#)