

Arti Status from the Network Team

Alexander Hansen Færøy

December 29, 2024

38C3



C Tor is showing its age, and the architecture is not viable down the road.

Many lessons learned from both performance work on C Tor, but especially mobile integration has been painful.

Building a library that can be used not just for building Tor clients, but in general working with data in and around the Tor ecosystem.

Strong focus on embedability.

Arti Roadmap

- 0.1.0** API stability. **Year I**
- 1.0.0** Usability, performance, and stability. **Year I**
- 1.1.0** Anti-censorship. **Year I**
- 1.2.0** Onion services. **Year II**
- 2.0.0** Ready to replace the C client. **Year II**
- Future** Relay, bridge, directory authority, etc.

Arti Roadmap

- 0.1.0** ~~API stability.~~ **Year I**
- 1.0.0** ~~Usability, performance, and stability.~~ **Year I**
- 1.1.0** ~~Anti-censorship.~~ **Year I**
- 1.2.0** ~~Onion services.~~ **Year II**
- 2.0.0** Ready to replace the C client. **Year II / Year III**
- Now** Relay, bridge, directory authority, PoW, Anti-DoS, etc.

Arti Roadmap

Following up from 2.0.0, we are currently looking at funding options for Arti integration for Tor Browser and Tor Browser for Android.

There will likely be updates on this topic in 2025. The work here will largely be handled by The Tor Project's **Applications Team**, but some work will be carried out by the **Network Team** for extended RPC support as well as Conflux.

Enhancing the **Pluggable Transport** integration process is also planned.

Arti Relays: Entering Project 141

- Objective 1:** **Directory Authority support.**
- Objective 2:** **Core Relay functionality.**
- Objective 3:** Parity, Robustness, Fuzzing, **Anti-DoS**, Windows, BSD, **Specs.**
- Objective 4:** Performance, MetricsPort, **Shadow**, "Extra Info" descriptors.
- Objective 5:** **Test Network**, Campaigning, Tools, **Packages**, Community.

Arti Relays: The Forgotten Projects

Grant life can be complicated, and we sometimes miss items that would have been ideal for a specific grant.

Kill RSA: We need to get rid of RSA and the various places where SHA1 is still in use.

Happy Families: Family "identity key" for relay operators. Needed for mobile, Walking Onions, and for various "group by" operations in Arti/Metrics.

PQ TLS: Post-quantum layer for TLS. Fortunately, this one looks easy for deployment with Rust.

Flag assignment: A more flexible option than MiddleOnly flag.

Arti Relays: Long-term goals

Arti Relays is the last piece in our long strategy of getting rid of the C implementation of Tor. Once we can declare "victory", we will finally be able to begin working on some of the big protocol changes we have in mind:

- Walking Onions (Proposal 323): Tor with less annoying bootstrap.
- Better link layer protocol.
- PQ in the Circuit Layer.
- Another round of performance analysis in the "pure" Arti world.

Arti Test Network

We will need your help here!

Every node type will be needed, but of course especially Exit nodes are valuable here.

Will likely require significant more work than just "ordinary" network operations: faster update cycles, more crashes, newer problems to debug, etc.

This work will begin in 2026, but there will be updates out during 2025.

The Road to Production

One property we hope to see with the adoption of Arti in the production network is a faster network, but also a smaller network in terms of relay numbers.

Hopefully, we will enable Windows operators to also contribute to the Tor network.

No large relay campaigning before the migration towards Arti on the production network.

There will be bumps on the road.

Questions?

✉ ahf@torproject.org

🔑 OpenPGP:
1C1B C007 A9F6 07AA 8152
C040 BEA7 B180 B149 1921

📱 Signal: +1 (703) 420-1337

🐙 [@ahf@mastodon.social](https://mstdn.social/@ahf)

🦋 [@ahf.me](https://ahf.me)



This work is licensed under a

Creative Commons
Attribution-ShareAlike 4.0 International License

