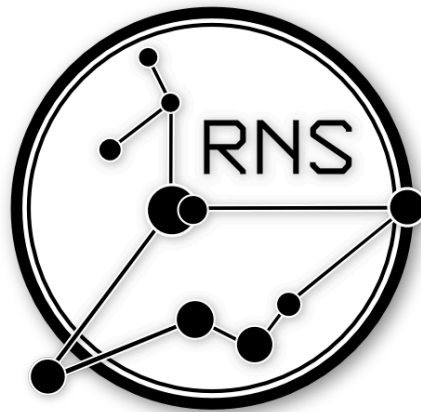# Reticulum

Reticulum is the cryptography-based networking stack for building local and wide-area networks with readily available hardware. Reticulum can continue to operate even in adverse conditions with very high latency and extremely low bandwidth.

The vision of Reticulum is to allow anyone to operate their own sovereign communication networks, and to make it cheap and easy to cover vast areas with a myriad of independent, interconnectable and autonomous networks. Reticulum is Unstoppable Networks for The People.

Reticulum is not *one* network. It is a tool for building *thousands of networks*. Networks without kill-switches, surveillance, censorship and control. Networks that can freely interoperate, associate and disassociate with each other. Reticulum is Networks for Human Beings.

From a users perspective, Reticulum allows the creation of applications that respect and empower the autonomy and sovereignty of communities and individuals. Reticulum provides secure digital communication that cannot be subjected to outside control, manipulation or censorship.

Reticulum enables the construction of both small and potentially planetary-scale networks, without any need for hierarchical or beaureucratic structures to control or manage them, while ensuring individuals and communities full sovereignty over their own network segments.

Notable Characteristics

While Reticulum solves the same problem that any network stack does, namely to get data reliably from one point to another over a number of intermediaries, it does so in a way that is very different from other networking technologies.

- Reticulum does not use source addresses. No packets transmitted include information about the address, place, machine or person they originated from.

- There is no central control over the address space in Reticulum. Anyone can allocate as many addresses as they need, when they need them.

- Reticulum ensures end-to-end connectivity. Newly generated addresses become globally reachable in a matter of seconds to a few minutes.

- Addresses are *self-sovereign* and *portable*. Once an address has been created, it can be moved physically to another place in the network, and continue to be reachable.

- All communication is secured with [strong, modern encryption](#) by default.

- All encryption keys are ephemeral, and communication offers forward secrecy by default.

- It is not possible to establish unencrypted links in Reticulum networks.

- It is not possible to send unencrypted packets to any destinations in the network.

- Destinations receiving unencrypted packets will drop them as invalid.