


# Who Owns the Path Between Our Phones?

## A plain-language introduction to the MORP Foundation

We own our phones—but do we own the path from one to another? MORP aims to let people own more of the means of transmission, using devices they already have or can afford.

A shareable field guide for the podcast host and listeners

## Start with a text to my wife

My wife is in the next room. I tap **send**. It feels like my phone should hand the message to hers. But with an ordinary carrier text or a cloud-backed messaging service, the message may leave my phone through a cell tower or Wi-Fi router, pass into a carrier or internet network, cross cables and service-operated relays or messaging switchboards, and then come back out through my wife's provider and tower or router before it reaches her phone.

The exact route varies—SMS, RCS, iMessage, a Nostr client, Wi-Fi calling, or an app can use different infrastructure. Not every message follows one identical path. **The constant is the ownership problem:** we may own the phones, but most of us do not control the directories, relays, carrier networks, servers, and policy decisions that make those phones communicate. Those operators can throttle or interrupt access; they can often observe connection metadata even when encryption protects message contents.

The everyday convenience hides a deeper dependency. We own the glass, battery, and processor, but rent much of the road between ourselves and other people. MORP's ambition is to break that dependency—not by magically abolishing every network provider, but by making it practical to own and operate more of the means of transmission on devices we already have.

## The Foundation's mission—in its own words

> **"Anyone and everyone can self-host a recognizable, DNS-free internet — a named, navigable, human-operable network of services and communication — on equipment they already own or can afford, without relying on centralized gatekeepers (DNS roots, domain registrars, certificate authorities, phone carriers, or ISPs) that can sever or monitor their connections."**
>
> **— MORP Foundation Master Intent**

In plain language: people should be able to run services, find them, and connect to them without asking a central company to assign every name, certify every identity, or carry every message. "Self-host" does not mean every person must become a systems engineer. It means the tools should make shared ownership possible for families, neighborhoods, and communities—and the project should run on affordable, ordinary hardware.

The mission has three useful words:

- **Named:** a service has an identity and an address that its owner can publish, rather than a name rented from a registrar.
- **Navigable:** people can reach that service over the routes available to them—mesh, internet, or an overlay network.
- **Recognizable:** a client can check that the endpoint belongs to the identity it intended to reach.

## Sunstone: the unifying principle

**Sunstone is the unifying principle of the MORP architecture:** it gives self-hosted services a signed, portable way to say what service this is and where it can be reached. The other pieces build the roads, switches, and hosts that make those addresses useful.

This does not mean Sunstone physically carries every message. MORP-NERD and PIPE move events; Box controls a phone's available routes; Sovereignty and Base are planned places to host relays and community

infrastructure. Sunstone is the shared address-and-discovery idea that lets these independently operated pieces find one another without a central landlord assigning their place on the network.

## Nostr, explained without the jargon

MORP builds around **Nostr**, an open way to publish and exchange signed messages called events. A person or service signs an event with a cryptographic key. Independent servers called **relays** store and pass events to clients that ask for them. Different relays can serve different communities; no single relay is the whole system.

A useful analogy is a public postal format. Your key signs the letter; relays are the post offices that accept, store, and forward it; your app is the mailbox you choose to read it with. The format is open, so one company does not own every app or every post office.

Nostr is not magic decentralization. A relay can be offline or refuse an event; users still need keys, clients, routes, and reachable relays. The benefit is that identity and signed messages are not inherently tied to one company's account database. MORP's work is about making Nostr services reachable over more kinds of infrastructure—including local and radio-based networks—while keeping the ordinary Nostr apps people already use in the picture.

## The family is a stack, not a pile of apps

A self-hosted network needs several jobs done. MORP separates those jobs into **protocols** (the rules for communicating) and **products** (the software people run). Sunstone is the cross-cutting address layer that helps those independently operated roads and hosts find one another; MORP-NERD and PIPE carry events, while the products give people real hardware on which to run and control that infrastructure.

| Layer | Project | Plain-language job |
|---|---|---|
| **Find the service** | **Sunstone Protocol** | Publishes a signed, short-lived address card: where a service can be reached and which path to try. |
| **Carry events through a mesh** | **MORP-NERD** | Moves signed Nostr events across multiple hops, including Bluetooth and compatible low-power radio/mesh links, toward relays. |
| **Use trusted fast paths** | **PIPE-NERD** | Adds an opt-in, bonded route among peers who have deliberately established trust, trading some of the crowd-mesh model for a more direct path. |
| **Make it usable on a phone** | **MORP Box** | Acts as a local switchboard, cache, and transmission-mode controller for Nostr clients on the same Android device. |
| **Turn a spare phone into a host** | **Sovereignty Relay** | Planned self-hosted relay on repurposed Android hardware, with mesh and overlay-network options. |
| **Provide a stationary anchor** | **MORP Base** | Planned Linux host for stable relay/gateway, seeding, indexing, and broader network interconnection. |

Protocols can be tested and released independently. The products consume those specifications; they do not get to quietly redefine how the protocols work. The intended product order is **Box → Sovereignty → Base**.

## MORP-NERD: the crowd mesh

A mesh is a network where devices can pass information to nearby devices, which can pass it onward. It is useful when there is no direct connection between sender and recipient, or when ordinary internet access is unavailable or unreliable.

MORP-NERD is the family's **unbonded, multi-hop transport**: nearby devices can participate without first becoming a person's trusted contact. A message is wrapped in layers for a route, so a forwarding device is meant to learn only the next step it must perform—not the entire path and message context. Bluetooth, MeshCore LoRa, and Reticulum are among the intended physical or network underlays.

This is not a promise that a tiny radio can replace broadband. Low-power radio is constrained by range, airtime, packet size, interference, battery, and how many willing nodes are nearby. It is more naturally suited to small signed events and resilient messaging than to moving large videos. A route only exists when enough devices and reachable relays exist to carry the event.

Nor should “onion routing” be mistaken for a guarantee of anonymity. It can limit what individual relays learn, but it does not erase traffic patterns, prevent collusion, or hide that a radio is transmitting. MORP’s stated approach is to describe and test those limits rather than promise perfect secrecy.




MORP-NERD protocol emblem

## PIPE-NERD: the trusted fast lane

Not every connection should be anonymous or open to strangers. Families, organizations, and communities may have peers they have intentionally paired. PIPE-NERD is the **bonded, trusted-peer path**: it can prioritize those relationships and move events more directly through cooperating relays.

The trade-off is deliberate. A trusted-peer route can be faster or more dependable for its participants, but it relies more on who has been admitted to that peer group. It complements MORP-NERD; it does not replace the open mesh path. The project keeps those roles separate so that “works among strangers” and “works especially well among trusted peers” are not confused.




PIPE-NERD protocol emblem

## MORP Box: the first thing a person can try

The first product is **MORP Box**, an Android app designed as a switchboard—not as another social network. It provides a local relay and cache on the phone, then lets the user decide which transmission modes are available. Existing Nostr clients on that device can use the local service; Box handles the routing and radio policy rather than composing or signing the user’s posts.

Think of it as a small traffic controller beside the apps you already use: **MORP mesh, PIPE bonded paths, and ordinary internet relay routes** can be controlled separately. The user should not get a silent fallback to a path they turned off.

Box is also the honest starting point for the project’s progress report. In the current roadmap snapshot, cache behaviour is reported stable in beta checks, PIPE bonding is still under test, and the first MORP-NERD-in-Box testing has not yet happened. Physical two-phone radio testing remains a real milestone—not something a passing software unit test can stand in for.

Box is not the full vision. It is the first practical tool for letting an ordinary phone participate without asking its owner to run a Linux server or replace their Nostr client.




MORP Box emblem

## Sunstone: an address card, not a landlord

Even a working mesh needs a way to tell clients where a service is. Sunstone is the family's **DNS-free endpoint advertisement and resolution protocol**. A service owner signs a record that says, in effect: "Here are my reachable endpoints; try this one first." A resolver can verify the signature and try eligible paths in order.

The analogy is a contact card with a short expiry date. It can list more than one kind of network route, rather than giving the service one permanent internet address. A record goes stale and must be refreshed. The owner can mark a slot temporarily withdrawn or permanently retired. A private route can instead be handed to a chosen peer in a wrapped private card or offline QR Seed Card.

Sunstone Protocol **v1.1 has been released**. It includes a TLS public-key pin option for certain endpoints, bounded record lifetimes, explicit withdrawal/retirement behaviour, and checks that keep anonymous and linkable endpoint identities from being mixed under one key. Sunstone does not sell names or charge a fee to resolve or use a connection. People may choose to pay a creator or service through separate payment tools; Sunstone itself does not hold or settle funds.

That last distinction matters: a free road and an optional tip to the person who built the destination are compatible. Payments are not a tollbooth for being reachable. Lightning or XMR payment flows, where supported by the client and transport, belong to external wallets and payment/message layers—not to Sunstone's address record. This is an architectural intention, not a claim that every product already implements those payment flows.




Sunstone Protocol emblem

## The next hosts: a drawer phone, then a steady anchor

After Box is stable and its protocols have been exercised in the product, the next planned host is **Sovereignty Relay**. The idea is to repurpose an Android 12+ phone that might otherwise sit in a drawer. It would run a self-hosted relay, provide Tor onion reachability and mesh modes, and share its address with approved peers through Sunstone cards. The constraint is that phones have batteries and limited thermal and storage budgets; a phone left powered forever is not the same as a purpose-built server.




Sovereignty Relay emblem

The later planned product is **MORP Base**, a stationary Linux machine. Wall power, durable storage, and room for radio hardware make it a better long-lived anchor. Base is intended to bridge internet and mesh, help seed and index service information, and provide a stable point for a community to find participating relays and services.

The order matters: Box first, Sovereignty second, Base third. The roadmap requires Box stability and a MORP-NERD v2.2 release/re-pin before Sovereignty begins. Base follows Sovereignty. Sunstone v1.1 is one important precondition, but it does not mean the downstream products are already built.




MORP Base emblem

## A walk-through: changing the route, not the message

Now replay that ordinary message to my wife using the architecture MORP is building. This is the intended flow—not a claim that the full Box-to-mesh path is already finished in product testing.

1. I write the message in my Nostr app and sign it with my key. The app does not need to know how the radio mesh works.
2. Box checks my chosen transmission modes. If internet relay access is on, it may use ordinary relays. If I am offline or choose mesh, the event can be handed to MORP-NERD.
3. Nearby MORP devices forward the event along an available route. Each hop has a limited job. If an eligible relay eventually gets the event, it can publish the original signed Nostr event into the broader Nostr network.
4. My wife’s client reads the event from a relay it uses. If we are connecting to a self-hosted service rather than exchanging a post, Sunstone can help the client find that service’s current endpoint.
5. If my wife and I have bonded, PIPE may be a suitable preferred lane. If we have not, the unbonded MORP mesh remains the path the architecture is meant to provide.

There is no claim that every route is always available or every event arrives instantly. A local network still needs a working route and participating devices. The design goal is that losing one provider or one network path should not automatically mean losing the whole community’s ability to communicate.

## What MORP is—and what it is not

**MORP is:** a family of independently tested protocols and planned products for self-hosted Nostr communication, endpoint discovery, and connectivity across local mesh, internet, and overlay paths.

**MORP is not:** a finished replacement for the entire public internet; a new social-media platform; a promise that no service provider is ever needed; a magic long-range radio; or a guarantee of anonymity. It does not make hardware, power, spectrum, bandwidth, peer density, or good operations disappear.

The technical promise is narrower, and more useful: let people run more of their own infrastructure, give them choices about how events travel, and make those choices visible rather than hidden in one provider's settings. The social promise is that a community can build and maintain a piece of its own network without first asking a central company to issue it an identity or a permanent address.

## Where the work stands

The released base includes MORP-NERD v2.1, PIPE-NERD v1.2, and Sunstone Protocol v1.1. These releases have been pinned into the Box project. MORP-NERD v2.2 is scoped as a later documentation/logic increment with no wire-version change; it follows Box stability and must be re-pinned before Sovereignty. Box's beta evidence is still being built, with PIPE bonding and in-product mesh testing among the remaining work. Sovereignty Relay and MORP Base are later product stages, not current general-availability services.

A podcast-friendly summary is: **the blueprint is real, some protocol releases are real, the first product is in beta, and the final hosts are still ahead.** That is a more accurate and more encouraging story than pretending the whole stack is already finished.

## A closing image

Think of MORP as a community workshop for building roads, signposts, and small public buildings—not as a single megacompany promising to rebuild the whole internet overnight. Nostr provides an open way to sign and exchange messages. MORP-NERD and PIPE are different roads for those messages. Box is the first pocket switchboard. Sunstone is the signed address card. Sovereignty and Base are planned places for the community's relays to live.

The destination is simple to say and difficult to engineer: **an internet that ordinary people can host, recognize, and navigate on the equipment they already have or can reasonably afford.**

---

### For the host: five safe facts to repeat

- MORP is a project family for self-hosted Nostr infrastructure, not a social app.
- It separates unbonded mesh transport (MORP-NERD) from trusted-peer routes (PIPE-NERD).
- MORP Box is the first Android switchboard and is still in beta testing.
- Sunstone Protocol v1.1 is released; Sovereignty Relay and MORP Base are later planned hosts.
- The project is candid about limits: mesh needs nearby nodes, radios are bandwidth-constrained, and the design does not promise perfect anonymity.

### Source note

Prepared from the MORP Foundation Master Intent (family mission and project boundaries), Foundation Roadmap v1.17, current project work orders, Sunstone Protocol v1.1, and the audience visual references supplied by the Owner. Product-state wording is a snapshot of those project documents; re-check the live roadmap immediately before recording if the status may have changed.