Mozilla WINS Challenge Round 2 - People's Open Network

Round 1 Application | Round 1 Notes

Your Solution

Links to public documentation: Please provide publicly-accessible links to information on your working prototype, using the categories provided below. You may only provide one link per category. You MUST provide links for at least two of the four categories.

- Public website - https://peoplesopen.net
- Code repository (e.g., public GitHub page) - https://github.com/sudomesh
- Design/technical documents and test data
    - https://sudomesh.org
    - https://sudoroom.org/wiki/Mesh/Technical_Overview
    - https://sudoroom.org/wiki/Mesh/Network_topology
    - https://peoplesopen.herokuapp.com/
- Video content (e.g. a link to a publicly-hosted video of your working prototype being demoed, 5 minutes or less): https://peoplesopen.net/watch

Solution Statement: Describe your working prototype and how it connects the unconnected. (500 characters or fewer)

[500 Chars]
People's Open Network works with communities to build and operate wireless networks. We provide open source software, off-the-shelf hardware, and educational materials used to host workshops, train operators, and install nodes. Our prototype consists of over 40 nodes in the Bay Area sharing paid internet subscriptions with unconnected neighbors. We're currently working on building access to gigabits of donated bandwidth (via Internet Archive and Paxio) and connecting a homeless camp in Berkeley.

Community/Location: Describe the communities, geographic location(s) and/or types of environments in which this solution could be most useful. Have these communities and environments changed since you submitted your Design Concept? (1250 characters or fewer)

[1223 Chars]
Our solution is designed for a city like Oakland, a community with a widening class and digital divide. Nearly a quarter of households here have no computer access at home, and more than a fifth of homes lack internet access at home despite its close proximity to Silicon Valley.

Mozilla WINS Challenge Round 2 - People's Open Network

The People's Open Network is primarily targeted at three types of people:
1) those who want to share a single internet connection with their neighbors;
2) those who cannot afford the monthly subscription through a corporate internet service; and/or
3) those interested in learning how the internet works.

Our solution is suited for replication in similar urban environments with a socioeconomically diverse population of stakeholders — families, individuals, businesses, encampments, and community spaces. In addition to distributing access to the wider internet, our solution can lead to local mesh internets that are independent of ISPs.

We have begun to implement our network in the SF Bay Area, a densely-populated, hilly, coastal region. We use the area's mixed elevation to our advantage to get line-of-sight between homes and buildings across long distances. Our target community and environment has not changed since our last submission.

Live Demo: If invited to do so, would you be able to provide a live demo of your working prototype? If no, please explain why below. (500 characters or fewer)

[473 Chars]
Yes. We have developed a minimal demonstration that we use to explain the basics of the network at our Build Your Own Internet workshops. The demo consists of two WD MyNet commodity routers running sudomesh firmware, two raspberry pis (acting as simple web-servers), and one computer with WiFi support. Workshop attendees can connect their phone or laptop's WiFi to either of the two SSIDs broadcasted and visit a web site hosted on the other node's connected raspberry pi.

Technical Feasibility: Explain the technical design of your solution. How does your prototype work? What are its capabilities? What are its limitations? Are there any technical hurdles or problems that would need to be solved in order to build a real network or device based on your prototype? (5000 characters or fewer)

[3466 chars]

The People's Open Network uses off-the-shelf multi-band WiFi hardware and custom open source software to connect and automatically route internet traffic from apartment to apartment and house to house in a redundant, decentralized and fault-tolerant manner. We use a custom OpenWRT-based firmware, the babeld mesh routing protocol, wlan-slovenia's tunneldigger for creating VPN tunnels, and a few custom web apps for configuration and coordination.

The network currently consists of over 40 households across the Bay Area as well as two community hubs (our homebase at Omni Commons and the Noisebridge hackerspace), with clusters in West Oakland, North Oakland, and Eastlake. Before more public outreach, we're using this live prototype as a beta network to

continue refining and debugging. Our current goals are to a) find anchor locations for connecting to proffered gigabits of bandwidth from the Internet Archive and Paxio, and b) partner with "community hubs" (such as community centers,libraries, housing projects and apartment complexes) to reliably share their bandwidth with neighboring areas such as homeless encampments, public demonstrations, and city parks.

Technical progress since Round 1:

- *Auto-configured nodes* - The latest release of our firmware includes a script that will automatically make the node part of the People's Open Network once it has an Internet connection. This reduces friction while introducing people to the network, and also provides learning opportunities for people who are interested in becoming more involved.
- *Monitor* - We have developed a simple monitoring system that tracks how many nodes are currently connected to *x* gateways via *y* exit nodes.
- *Training Programs* - We've now incorporated safety trainings for volunteers into our weekly node mounts, streamlined our node mounting process, and developed a training program for People's Open Network Installers (PONIs), We've also created a Node Whisperer Program for firmware and exit node maintainers, a lab for learning about routing with Babel and another for learning about Tunneldigger, a general network-lab, a guide to deploying mesh services, and an Operator's Manual.
- *Multiple Exit Nodes* - Deployed a second exit node server and streamlined a process for deploying more to increase the resiliency of the network.
- *Patch Deployment* - Streamlined a process for deploying patches to nodes running older sudowrt firmware.
- *Code of Conduct* - Drafted a set of standards of expected behavior for contributors to and maintainers of the network.

Next challenges / opportunities:

- *Gigabit Uplinks* - We have two offers of donated multiple-gigabit bandwidth - via the Internet Archive's tower in Richmond as well as Paxio, an ISP located in downtown Oakland - and are in the process of negotiating with building owners that are ideal sites for our airFibers.
- *Meshifier* - We're working on a script for easily configuring any OpenWRT/LEDE- or Ubuntu/Debian-based device to be a mesh node capable of e.g. deploying services on the network.
- *More devices* - We're working to support more devices capable of being home or extender nodes (eg, TP-Link routers and more Ubiquiti devices)
- *Mapping* - Discussions continue about how to best preserve privacy of node owners, however we recognize that a map is a compelling outreach tooland thus forthcoming.
- *Services* - We're currently testing Rocketchat and etherpad-lite, and intend to deploy more services that can be made available within the network as well as accessible by the Internet, and easily found by users via a service browser.

  Taken from Round 1 grant application —
  The People's Open Network uses off-the-shelf multi-band WiFi hardware and custom open source software to connect and automatically route internet traffic from apartment to apartment and house to house in a redundant, decentralized and fault-tolerant manner. We use a custom OpenWRT-based

Mozilla WINS Challenge Round 2 - People's Open Network

firmware, the babeld mesh routing protocol, and a few custom web apps for configuration and coordination.

Our modular and expandable design begins with cheap (under $20) indoor wifi routers (referred to here as "Home Nodes") providing everything needed to get on the mesh. If the node operator is not within range of any other nodes, then the range of their Home Node can be extended by adding one or more long-range outdoor-capable routers (Extender Nodes) which can reach 20+ miles. Each Home Node runs our firmware, which provides the Home Node with the following features:

1. *Zero-configuration setup. Plug a Home Node into a power socket to connect to the network.*
2. *Intelligent relaying over multiple wifi radios to avoid the bandwidth and latency issues associated with relaying over a single radio.*
3. *Automatic mapping: With node operator consent, a new node uses wifi-based positioning to add its approximate location to a public mesh map.*
4. *A public, password-free wifi network through which any wifi-enabled device can connect to the mesh and the internet*
5. *A private, password-protected wifi network, isolated from the mesh, which can be used by the node operator's household to access the network privately and connect any devices that shouldn't be shared publicly (e.g. printers).*
6. *Ability to share a portion of the node operator's available bandwidth (if they already have their own internet) via an open wifi hotspot.*
7. *Automatic tunneling of traffic coming from the open wifi hotspot via a free non-logging VPN run by the community.*
8. *Ability to extend the wifi coverage by hooking long-range wifi routers (Extender Nodes) into one of the ethernet ports of the node.*
9. *A simple web UI that makes it easy for anyone to configure basic options like such as how much bandwidth to share, and their a private wifi network password, which also includes an assistant to establish a link when a new Extender Node is added to the Home Node.*

For Home Nodes, our firmware supports at least two affordable (under $20) consumer-grade router models from different manufacturers. For Extender Nodes, we support an array of long-range, off-the-shelf, outdoor antennas, currently available for around $60 to $120. We've implemented and deployed a network prototype with approximately sixty Home Nodes throughout the Bay Area, ten of which include at least one extender node.

Three items that remain to be implemented:

1. *The nodes currently require configuration by a small script which must be run by a team member rather than auto-configuring on first bootup, so the zero-configuration is not yet quite zero.*
2. *We are also still in the process of developing automatic configuration of Extender Nodes that are not running open source firmware.*
3. *We have not completed automatic mapping. This will include the ability to anonymously email operators of nearby nodes, which will help to decentralize coordination efforts.*

There is a technical hurdle in the shift from 802.11n devices, for which OpenWRT has good support, and to 802.11ac for which open source drivers do not yet have the same stability and reliability. This is currently in active development by the OpenWRT team. Also, due in part to new FCC regulations that discourage loading custom firmware onto consumer wifi devices, some vendors have started implementing measures to prevent custom firmware. We have found workarounds. In the worst cases we can communicate directly with flash memory IC or use the low-level JTAG protocol. We have done our best to mitigate these issues by allowing our Home Nodes to mesh via Extender Nodes that are not running custom firmware and have discussed making a device to automate the JTAG-based flashing. Luckily not all manufacturers are locking down their routers.

Possibly the biggest "technical" hurdle (if it can be said to be technical) is the time it takes to install long-range wifi equipment on rooftops. The installation can involve quite a bit of coordination, and often takes at least an hour. Though nodes can be installed using non-penetrating mounting solutions, a cable must be run inside the building for power and connection to the Home Node. This can mean drilling a hole in a wall, which may require landlord permission. We have started experimenting with ethernet-over- adapters which could piggyback on existing wiring rather than running new ethernet cable.
More at https://sudoroom.org/wiki/Mesh/Technical_Overview

Differentiation: How does your prototype differ from or improve upon existing solutions? What is innovative or novel about the concept or technology? Has this changed since you submitted your Design Concept? (1250 characters or fewer)

[1246 Chars]
Unlike corporate ISPs or groups focused exclusively on hardware and software solutions, we recognize the problem of equitable internet access holistically: as both a social and technical challenge.

We value replicability to ensure anyone can copy and adapt our code and organizational model. That's why we extensively document our systems and processes, all openly published. We have counseled small groups to fork this project, from Oakland to NYC, Portland to Olympia, Standing Rock to Cuba..

Our firmware allows people to share a customizable portion of their bandwidth with the world and the mesh. Each node with internet connectivity becomes an open wifi hotspot and spreads this bandwidth using the mesh.

The mesh aspect of the project increases both the range and resiliency of the network - as more nodes connect to each other in a dense array, the reach of the network expands and multiple paths of connectivity are made available to route around damage. Services may be deployed on the network that will remain online even when the Big Internet goes down, whether from a natural disaster or censorship.

Mozilla WINS Challenge Round 2 - People's Open Network

Affordability: How affordably do you envision the solution could be implemented in a real community? Has this changed since you submitted your Design Concept? (1250 characters or fewer)

[1251 Chars]
We ensured that the costs of installing a physical network would be kept very low, within the range of affordability for small community groups with limited budgets. This has not changed since we submitted our last Design Concept.

As mentioned in our Round I submission, we take advantage of low-cost ($20-$100) wireless networking hardware and the increasing sophistication of FLOSS mesh networking protocols. A typical home node presently costs $15-$20. For extender nodes, outdoor roof-mounted equipment is typically available for $60-$100 per device.

We have a sample $5K budget for a neighborhood community anchored on a single broadband connection. It includes VPN server costs for one year, 50 Home Nodes, 15 Extender Nodes, mounting hardware, essential tools, and supplies for four educational workshops.

The greatest cost to implement a neighborhood wireless network modeled off of our design is broadband access. Groups using our design could develop relationships with community organizations to share excess bandwidth. Or, as we're currently doing, groups could pursue donated bandwidth from local ISPs and nonprofits and distribute it to high-need locations with our open source firmware using a point-to-multipoint topology.

Social Impact: How well-tailored is the prototype to the needs of the community and users for which it is designed? How will the design of the solution help engage community members in order to maximize utilization? Has this changed since you submitted your Design Concept? Have you tested your prototype in any communities? (1250 characters or fewer)

[1212 Chars]

Our project is based out of a radical collective space, Omni Commons, that is home to dozens of social justice-based organizations and projects. Further connecting to communities in Oakland, we: host workshops with panel discussions and learning stations; hold weekly community office hours; maintain several channels for participation; conduct ethnographic user research; publish curricula for training future community network operators; and distribute donated laptops to those without.

We're actively testing our network in several places: test networks at Sudo Room and Noisebridge hackerspaces; several direct line-of-sight connections for low-income households that use donated bandwidth

from their neighbors, as well as an array of network clusters in West Oakland and Eastlake; and have mounted several nodes on rooftops at high elevations to build out our backbone.

We are in talks with First They Came for the Homeless in Berkeley as well as a QTPOC-led community center in East Oakland - with whom we've had highly informative conversations , and are awaiting their collective's final consent before mounting a node pointed toward The Village down the street and another pointed north toward the hills.

Scratch:

- *While our model was designed for Oakland, it can be used for other urban communities that are experiencing a widening digital divide. Our design enables communities to leverage shared or donated broadband connections with minimal financial overhead. [repetitive]*
- *As mentioned previously, the highest recurring cost would be to pay for subscriptions for a typical ISP connection — which can even be offset by donated bandwidth. [discussed in affordability]*
- *Add bits about Laptops for All, Cryptoparties? [discussed in other sections]*

Sustainability and scalability: How would your solution be financially sustainable in a real community? How could it be adaptable to other communities or areas? What tools and documentation have you provided to anyone who might wish to build upon it or launch a similar effort? (1250 characters or fewer)

[1176 Chars]
Our solution is financially sustainable for any community that wants to create a local mesh internet or distribute access to existing sources of internet bandwidth. Given our small-scale, well-documented design which relies on open source software and affordable hardware, our model can be implemented quickly and cheaply.

Our design enables scalability with our smaller, neighborhood-scale model that can be replicated across a community and adapted to local conditions, as the mesh routing protocol we use is adaptable to a wide range of access needs in high-population environments. We empower other local groups to build and self-govern community wireless networks by providing access to our open documentation and open source software, as well as our hardware recommendations and connections to similar projects in different geographical locations.

Excluding the previous award we received from Mozilla from Round I of this Challenge, we are entirely supported through small donations, rather than by large grants and corporate partnerships. We are exploring new funding models to enable us to become a more sustainable, community-supported public infrastructure project.

— Discuss adaptations for rural communities and communities without existing Internet infrastructure?

Speed: At what download and upload speeds does your solution provide access to users? (500 characters or fewer)

[492 chars]

Mozilla WINS Challenge Round 2 - People's Open Network

We regularly deploy SudoWRT on WD MyNet N600 and MyNet N750 home routers. N600 users are limited to 100Mbps WAN connections, with wireless mesh connections of up to 300Mbps. The N750 devices can support 1Gbps WAN connections, with wireless connections of up to 450Mbps. We're looking to move to open hardware with out-of-the-box support for OpenWRT (eg, LibreRouter) that enable higher throughput. The gigabit links currently underway will enable us to take full advantage of such an upgrade.

Openness: Mozilla works in the open. How have you documented and shared your solution with the community? (1250 characters or fewer)

[1164 Chars]
As mentioned in our previous submission for Round I, all of our source code, including router firmware, is fully open source and available on our Github. Extensive documentation is available under a CC BY-SA license and editable on our wiki. This includes walkthroughs, diagrams, technical documentation, recordings from previous presentations, user research, and meeting minutes.

With these tools, we intend to make it possible for anyone with even modest computer skills and little funding to build such a network in their community. Because all material is FOSS, a community with particular needs — such as unique software configurations or customized workshop curricula — can easily fork and adapt the materials for their own purposes.

While our technical documentation is in a continual process of refinement and simplification, the bulk of the team's energy goes into conducting our quarterly workshops, weekly open office hours, and weekly open meetings in such a way that new members are welcomed, onboarded, and trained in all aspects of the network's functionality and development. We meet somewhat regularly for documentation and wiki editing hackathons.

Scratch:
Following up from our initial application in October, we have accomplished the following:

- More frequent blog posts
- Sending out quarterly newsletters — see December, January and March newsletters
- Building outreach and educational capacity:
    - We launched the Node Whisperer Program and have consulted with several local community projects, such as OlyMesh, Detroit's Equitable Internet Initiative, SF Lan (in process of rebooting), and an emerging Portland mesh network. Members of our team are also presenting talks at this summer's Our Networks conference in Toronto and HOPE in NYC.

Smart Community Networks Challenge (Challenge 2 Applicants Only)

Network Footprint: How does your solution make efficient use of existing infrastructure? (1250 characters or fewer)

[1150 Chars]

Mozilla WINS Challenge Round 2 - People's Open Network

The People's Open Network makes efficient use of existing infrastructure such as neighborhood-based social networks, donated/shared bandwidth, unlicensed radio spectrum, and open source software. We do this by:

- Reaching out to community centers, local businesses, coops, cohousing communities, and tenants unions to expand the reach of the network, both in terms of physical locations as well as network density;
- Providing methods to share unused internet bandwidth. Given that most consumer and business internet connections are underutilized, we reuse capacity of an existing internet access infrastructure with minimal impact;
- Designing our firmware to work with off-the-shelf hardware - the vast majority of which is donated by individuals and friendly ISPs;
- Using unlicensed radio spectrum to create peer-to-peer connections between access points to extend the range, and increase the resiliency of, the network;
- Participating in an active open source software ecosystem - thus avoid licensing costs while using up-to-date technology, learning from and solving problems collaboratively with a global network of mesh and community wireless networks.

Privacy and Security: What steps are you taking to address the privacy and security expectations of users of your solution? (1250 characters or fewer)

[948 chars]

Our network is no more secure than an average public wifi network, like you'd find at a library or coffee shop.

We encourage everyone to use a VPN, tools like HTTPS everywhere, and to learn about who has access to their communications in various media.

We've recently rebooted Sudo Room's Cryptoparties, which initially ran from August 2013 - early 2016 on the monthly, in the newly-designed form of Digital Security Workshops. In so doing, we hope to impart essential end-user "security hygiene" skills to particularly vulnerable communities - such as sex workers, journalists, activists, immigrants, whistleblowers, and tax-resisters (to name a few) - topically narrowed to specific threat vectors.

Our motto is: "Never trust the network." Wireless networks are inherently insecure, as demonstrated by the recent KRACK attack on WPA2 networks. While we work to ensure security patches and updates are deployed, we can't ensure an inherent security to the network itself - rather, end-users need to learn about and employ the essential security measures in response to their particular threat vectors - be it the confidentiality of an informant or simply the protection of their own personal identity.

> *Taken from Round 1 grant application —*
> *Open Source software enables better and faster responses to security vulnerabilities. For instance, upon learning about the recent KRACK attack on WPA2 networks, signed security patches were rapidly provided by the OpenWRT community in less than a week, then propagated through the mesh in less than an hour.*

Mozilla WINS Challenge Round 2 - People's Open Network

We provide protection for those choosing to share their home connections by directing all traffic on the open 'peoplesopen.net' network through a non-logging VPN controlled by our nonprofit entity. The VPN protects public wifi hotspot operators from legal liability due to content accessed over the network, as the VPN organization will not have any information about which individual hotspots relayed which traffic. This, plus the ability to limit shared bandwidth, allays many fears people have about sharing their internet.

Given the inherent vulnerabilities of any wireless network, however, we do not assure members that the network is in and of itself private or secure. Over the past 4 years, we have held dozens of Cryptoparties to teach people about end-user security. We also include information about privacy and security in our Node Owner's Manual and in our educational curricula.

Density and range: How many simultaneous users can your working prototype support within an area equivalent to one square city block (for urban projects) or 10 acres (for rural projects)? What is the maximum distance at which your solution can provide network coverage? (1250 characters or less)

[1157 chars]

Up to 60 client devices can connect to a single home node, the range of which is roughly equivalent to 1-2 city blocks. This number is multiplied by the number of home nodes in proximity to each other that are meshing, or which are connected via point-to-point wireless extender node connections. For extender nodes, distances of 100km+ have been recorded by Ubiquiti airFibers with clear line-of-sight and environmental conditions.

[Link to topology diagram?]

We're building an open platform that can be deployed to anything that supports OpenWRT.

While the home nodes we use are already cost-effective, all OpenWRT-compatible routers can be used to blanket a city block. The available bandwidth depends on what residents are able to share and on what external bandwidth might be provided by donation or collective purchase.

As we also support a variety of backhaul equipment (i.e. our extender nodes), relatively rural sites can also be connected. While we know that we can connect any site that we could normally connect with a Ubiquiti Rocket M5, it's really a matter of, "What can we run sudowrt on?"

The point is that we're developing an adaptable software platform, not a fixed hardware platform, as a means of building a resilient network in our community. We hope others can do the same!

Access: Does your working prototype provide access to the whole Internet (if 'no,' please explain)? (1250 characters or fewer)

[819 chars]

Mozilla WINS Challenge Round 2 - People's Open Network

Yes.

We have had some occasional downtime, but our network is becoming more robust as we now have multiple options for exit nodes.

Access to the whole Internet has always been one of our core goals as a project. Existing ISP connections are leveraged through the option to share a portion of one's bandwidth, the public traffic of which is routed through "Exit Node" Virtual Public Network servers run by Sudo Mesh and other volunteers.

Of note is that, given restrictions to access to e.g. Netflix over a VPN, some exit nodes may be blacklisted by certain servers, blocking access to the site for users on the public peoplesopen.net SSID.

With regard to "the whole Internet," we have developed Sudo Mesh integration with Pogoplug NAS devices, through which we intend to host educational resources and archival data as well as a backup of Wikipedia and other instructables — in the event that "the whole internet" is rendered less whole in the future.

Scratch:
BYOI workshops
Node Whisperer Program
Node Owners Manual
BYOI Office Hours
Rebooting Cryptoparties
Zine
Mounting guide
Laptops For All

Video script outline

- Brief intro
    - The People's Open Network empowers communities to build and operate their own wireless networks without last-mile ISPs. Using our design built on open source software, off-the-shelf hardware, and open educational materials, small groups of people can utilize existing bandwidth to share their internet connections and cover public and underserved areas.
- Network building
    - Node set up
        - We use off the shelf wifi routers — N600
        - Defaulting — connect N600 to power/ethernet, holding down the reset button
        - Download firmware — screenshot/video of downloading firmware from sudomesh
        - Installation of firmware — connect device to computer with firmware, screenshot of installation countdown

Mozilla WINS Challenge Round 2 - People's Open Network

        - Autoconfig — setting ssid, password, bandwidth sharing, etc.
- Testing / connection
    - Connect to peoplesopen.net SSID — screenshot of connecting
    - Visit a website using peoplesopen connection
    - Exit node/VPN — Traceroute
    - Cow and chicken — Visiting websites on each others' nodes
- Testimonials (connectivity and access)
    - Clip: Mary Jo & Terry
    - Clip: FTCFTH (hopefully)
- Access & Education
    - Those who connect to the network are not customers, but community members, encouraged to learn, participate, host a node or contribute to code. That's why we hold events like our Build Your Own Internet Workshops.
    - Clip: BYOI Workshops
    - Clip: Laptops For All
    - Clip: Cryptoparty
    - Clip: Office Hours?
- Testimonials (learning and support/access)
    - Clip: Toan? (laptops)

Video Scrip`t

We are the People's Open Network — empowering communities to build and operate their own wireless networks beyond the scope of what a last-mile ISP like Comcast or AT&T would offer. Using our design built on open source software, off-the-shelf hardware, and open educational materials, small groups of people can utilize existing bandwidth to share their internet connections and cover public and underserved areas.

Members of the People's Open Network have developed our own OpenWRT-based firmware with the babeld mesh routing protocol, which we named SudoWRT. We're using SudoWRT to build out a community-owned and -operated mesh network in Oakland, California. Here's how we create a new node to add to the mesh:

1. Default an off the shelf WiFi router — for now we use Western Digital MyNet N600's and N750's
2. Download the SudoWRT firmware from our website
3. Install the firmware on the device (wait for the countdown...)
4. Configure the device with your chosen SSID, password, and dedicated bandwidth
   -- The private SSID can be used for any private network needs, such as connecting you printer, and Internet of Things devices.

Once you're done configuring the device, you can see that the private SSID and the new peoplesopen.net SSIDs are connected to the mesh. If the new node is able to mesh with nearby nodes, it can reach the rest of the network (and the capital "I" Internet) through its neighbors. All nodes with direct WAN connections *(point to physical port)* also allow their operators to bypass the mesh via the private SSID.

Mozilla WINS Challenge Round 2 - People's Open Network

If we use traceroute on this connection, you can see that the peoplesopen.net mesh connection passes through an exit node.

An exit node routes traffic using babeld just like a home node, but it connects a number of home nodes via TunnelDigger, a free and open source tunneling solution developed by WLAN Slovenia. Each home node with a WAN connection establishes a tunnel to an exit node, which is then able to route traffic between physically disjointed parts of the mesh. The tunnel also acts as a WAN gateway, giving all clients access to the larger Internet. Hence, traffic leaving the mesh over a given exit node appears to originate from the exit node's IPv4 address. We like to think of it as a Virtual *Public* Network - or, VPuN.
— Footage: whiteboard explainer video?
https://www.quora.com/What-is-the-best-Open-source-Explainer-Animation-Software

We can use this set-up on a mesh network that is completely disconnected from the wider Internet — these two nodes are only connected through a local wireless connection using two antennae down the block from each other. You could visit websites hosted on each node, such as on Raspberry Pis, as long as there's a line of sight between the nodes.
— Footage: Cow + chicken

Or our mesh set-up can also be used to share bandwidth to the Internet. This is the case with People's Open Network members, Mary Jo and Terry, who access the wider Internet over the mesh from their neighbor and fellow mesh network member, Chuck. Mary Jo and Terry have an antenna on their chimney, that's pointed to Chuck who also has a People's Open Network node and lives down the street. Chuck donates part of his bandwidth to Mary Jo and Terry — they can therefore connect through Chuck's node, through the exit node, on to the Internet.
— Footage: Quote snippets from MJ+T and/or Chuck

Those who connect to the network are not customers, but community members, encouraged to learn, participate, host a node, or contribute to code. That's why we hold events like our Build Your Own Internet Workshops, which consists of various "learning stations" for teaching various skills involved in networking: cable crimping, node flashing, mounting, and radio wave propagation.
— Footage: BYOI event footage from Jan 2018, PON meetings, PON BBQ, clips from PON video on roofs

But building a successful community mesh network entails far more than physical and technical infrastructure — equally important to internet access is practicing good "security hygiene," digital literacy skills, and possessing devices with which to connect to the network . To this end, members of Sudo Mesh collaborate with Sudo Room, the community hackerspace in which we reside, to host monthly digital security workshops / cryptoparties; fix and distribute donated laptops to those in need; and generally serve as a source of support, learning, and education free and open to all.
— Footage: Clip from War Tax Resister grant? (Raines has), montage of laptop recipients' photos, film a clip of upcoming cryptoparty? Ask Toan/FTCFTH for a testimonial?

SCRIPT FOR MAI

Mozilla WINS Challenge Round 2 - People’s Open Network

We are the People's Open Network — empowering communities to build and operate their own wireless networks beyond the scope of what a last-mile ISP like Comcast or AT&T would offer. Using our design built on open source software, off-the-shelf hardware, and open educational materials, small groups of people can utilize existing bandwidth to share their internet connections and cover public and underserved areas.

Members of the People’s Open Network have developed our own OpenWRT-based firmware with the babeld mesh routing protocol, which we named SudoWRT. We’re using SudoWRT to build out a community-owned and -operated mesh network in Oakland, California.

Here’s how we create a new node to add to the mesh:

<SNIP>

1. Default an off the shelf WiFi router — for now we use Western Digital MyNet N600’s and N750’s
2. Download the SudoWRT firmware from our website
3. Install the firmware on the device (wait for the countdown...)
4. Configure the device with your chosen SSID, password, and dedicated bandwidth
   -- The private SSID can be used for any private network needs, such as connecting you printer, and Internet of Things devices.

Once you’re done configuring the device, you can see that the private SSID and the new peoplesopen.net SSIDs are connected to the mesh. If the new node is able to mesh with nearby nodes, it can reach the rest of the network (and the whole Internet) through its neighbors. All nodes with direct WAN connections also allow their operators to bypass the mesh via the private SSID.

If we use traceroute on this connection, you can see that the peoplesopen.net mesh connection passes through an exit node.

An exit node routes traffic using babeld just like a home node, but it connects a number of home nodes via TunnelDigger, a free and open source tunneling solution developed by V-LAN Slovenia. Each home node with a WAN connection establishes a tunnel to an exit node, which is then able to route traffic between physically disjointed parts of the mesh. The tunnel also acts as a WAN gateway, giving all clients access to the larger Internet. Hence, traffic leaving the mesh over a given exit node appears to originate from the exit node’s IPv4 address. We like to think of it as a Virtual *Public* Network.

We can use this set-up on a mesh network that is completely disconnected from the wider Internet — these two nodes are only connected through a local wireless connection using two antennae down the block from each other. You could visit websites hosted on each node, such as on Raspberry Pis, as long as there’s line of sight between the nodes.

Or our mesh set-up can also be used to share bandwidth to the Internet. This is the case with People’s Open Network members, Mary Jo and Terry, who access the wider Internet over the mesh from their neighbor and fellow mesh network member, Chuck. Mary Jo and Terry have an antenna on their chimney, that’s pointed to

Mozilla WINS Challenge Round 2 - People's Open Network

Chuck who also has a People's Open Network node and lives down the street. Chuck donates part of his bandwidth to Mary Jo and Terry — they can therefore connect through Chuck's node, through the exit node, on to the Internet.

Those who connect to the network are not customers, but community members, encouraged to learn, participate, host a node, or contribute to code. That's why we hold events like our Build Your Own Internet Workshops, which consists of various "learning stations" for teaching various skills involved in networking: cable crimping, node flashing, mounting, and radio wave propagation.

But building a successful community mesh network entails far more than physical and technical infrastructure — equally important to internet access is practicing good "security hygiene," digital literacy skills, and possessing devices with which to connect to the network. To this end, members of Sudo Mesh collaborate with Sudo Room, the community hackerspace in which we reside, to host monthly digital security workshops / cryptoparties; fix and distribute donated laptops to those in need; and generally serve as a source of support, learning, and education free and open to all.

<SNIP>

Here's how we create a new node to add to the mesh