



Peer to Peer User Owned Communications Infrastructure

***The Free Network Foundation and Building an
Inter-occupy Network***

March April 2012 Part 2

Volume XX, No. 12 and XXI, No 1
March April 2012
ISSN 1071 - 6327

Contents

Introduction: Time to Build	p. 3
<u>The Arrogance of Power</u>	p. 17
Who Smashed the Laptops from Occupy Wall Street?	
Inside the NYPD's Lost and Found	p. 20
Occupy's Internet Tower Will Live On, For Now	p. 23
Isaac and the Freedom Tower at Contactcon October 20, 2011	p. 27
<u>Freedom Tower Materials and Assembly</u>	p. 29
Ends and Means <i>of the Free Network Movement</i>	p. 33
A Look Inside the FreeNetwork Foundation Network Operations Center	p. 48
On the FreedomNode	p. 52

Introduction

Time to Build

In the spring of 2011 Douglass Rushkoff and Venessa Meimis announced and un-conference called contactcon to be held on October 20 at the Angell Ortsanz Foundation located in an old Gothic synagogue in the East Village of Manhattan. In view of the Arab spring and of the Mubarak government cutting Egypt off from the Internet, there was immediate interest in trying to figure out how to build an Internet that Washington DC or the American military or foreign governments, for that matter, could not destroy.

A mail list was started and not surprisingly mesh wireless was a big topic of discussion. Out of the discussion which continued through October was born the free network foundation, an alliance between two young geeks Charles Wyble from California and Isaac Wilder from Grinnell College in Iowa but since late October resident of occupy Wall Street in New York. I have been talking on and off to Isaac since I met him at contact, on October 20 and took some photographs of his freedom Tower which he set up the following weekend in Sioux County Park and which was destroyed by the NYPD in its middle of the night raid on November 16. As is being said in many places now, these ideas will not go away Because for millions of Americans they represent the only hope of a viable future.

I intend to tell Isaac's story and my customary detail but in the meantime Isaac has had to put his plans back together all over again after being beaten and jailed. But in less than three weeks he has just finished another freedom Tower and will shortly be taking off by car for a swing through some occupy camps between New York and Austin Texas.

I asked Isaac to introduce himself to my arch econ mail list and here's what



he said: "I'm Isaac Wilder - Co-founder and Executive Director of the FNF. I'm twenty one years of age, and until this past May I was a student of Philosophy and Computer Science at Grinnell College, in Iowa. I left my studies in order to devote my energies to the Free Network Foundation, alongside my co-founder Charles Wyble."

"I live in Liberty Square, and I'm an integral part of the Occupation of Wall Street's Signal Corps. Oddly enough, I showed up that first day because OWS was billed as a 'horizontal mesh protest.' I liked that a lot - now we're helping build access and mesh networks at occupations around the nation. We have a ways to go, but we believe that we have a unique opportunity here to roll out a new type of network - one where participants communicate with one another, in addition to their ISP."

"I'm young. I'm green. I've got lots of questions. Personally, I've got an increasingly clear vision of what the network might look like, and quite a few ideas about how to judge the virtues of a network architecture. Charles and I have come a long way, but still there are many open questions. What is clear is that the idea of the Free Network - the principles it strives to embody - are most certainly worthy of implementation, and are within our technological means as a civilization." At the end of October and I sent Isaac and Charles a list of questions and on November 4th Isaac replied in some detail. Here is that exchange.

COOK Report: Introduce yourselves and explain how what you are doing came to be.

Wilder: I'm Isaac Wilder. I hail from Kansas City, Missouri. I've been a life-long hacker/geek/techie, and developed a keen interest in network freedom when I travelled to Cuba in the summer of 2010. Upon returning to school that fall, I began to have conversations with students and professors about how to build ICT systems that are politically free by design. As part of a long journey of discovery, I joined a mailing list that was started by Venessa Miemis, in connection with the Contact conference. That's where I met Charles, and the rest, as they say, is history. We knew from the start that we shared a vision, and incorporated the [Free Network Foundation](#) in May of 2011 in order to realize that vision.

COOK Report: Define in very simple terms what you are building. Call it infrastructure owned by the users not finite peer to peer versus logical p2p. I can't remember the term you used....remember logical but not the other except that it began with "f". I had found the explanation on the web site confusing.

Wilder: We design and implement tools that enable communities to grow their own networks - networks that are owned and operated by their participants, rather than profit-driven corporations. These tools keep local traffic local, so that a message sent across the room doesn't need to travel several thousand miles to reach its destination. They allow participants to benefit from the economies of scale, buying bandwidth in bulk, and sharing with their neighbors - this reduced the cost of connectivity for everyone.

COOK Report: Explain its architecture - a what happens at a basic site..Zuccotti park for example?

Wilder: Well, I'll start by saying that there's not really such a thing as a 'basic site.' I'll rephrase your question as 'What happens locally once a tower establishes a connection to the global network?' Keep in mind that there is also the interrelated question of how towers connect to the Internet. **The answers below assume that a tower is connecting via paid backhaul, which is currently the case with all towers in production.** Eventually, towers will connect to the FreedomLink via the regional tower mesh, but we'll get to that in a bit. For the moment, let's focus on what happens at a tower once it has an upstream connection. The answer has a few parts - basic connectivity, mesh connectivity, and tunneling. Keep in mind that these sometimes work in conjunction. I'll go over their individual characteristics, and then briefly explain some situations where they might work in tandem.

Basic connectivity: The first part is quite simple: upstream connectivity is rebroadcast via powerful 2.4GHz and 5GHz radios on an open wifi network. Anyone can connect using a standard wifi client device, and thereby gain connectivity to the global internet.

Mesh connectivity: This will really come into play once we have FreedomNodes in deployment. The tower router and radios are capable of building LAN routes using [Optimized](#)



[Link State Routing](#), a leading algorithm for mesh applications. This means that nodes can not only connect to the tower, but can connect to one another directly. This expands the range of coverage, and provides for horizontal connections between participants in the network.

Tunneling: The final form of connectivity is tunneling. This is used to access secure services, or to pass traffic securely between towers that are not connected directly to one another. The routers on our towers run [PFsense](#) (though I am also running some experiments with [zeroshell](#)). A participant connects to the tower either by a basic wifi link, or via a mesh link. From the tower router, we are able to dig a VPN tunnel to the nearest FreedomLink. From there we can route to services, or to another tower.

So, a few use cases: 1) Participants using FreedomNodes might pass each other messages directly, without communicating to the tower at all. 2) A participant on a standard client device might wish to access a host on the Internet which is not a part of the FreeNetwork. Imagine someone on a Macbook running stock software wants to log in to Facebook. They communicate directly with the tower via wifi - the tower load balances TCP sessions against all upstream connections, and sends their request directly to the upstream provider via the most available uplink. 3) A participant on a standard client device wishes to access a host on the FreeNetwork. Lets take for example an authenticated IRC server. The participant again communicates with the tower directly via wifi, but this time, the tower recognizes the the participant is trying to connect to a host on the free network, and routes to the nearest FreedomLink via a VPN tunnel. The link then routes the client to the service, and the connection is established.

4) A participant running the FreedomBox/FreedomNode stack might wish to connect to a host outside the free network. They would hop along the mesh to the tower, where they would be load balanced and sent upstream. 5) A participant running the FBX/FN stack might wish to connect to a host on the free network. They would hop along the mesh to the FreedomTower, which would tunnel them to the nearest link. The link would route them to the desired host. In the case the desired host were a node in a different (free network) mesh, they would be routed to the tower, and then hop along the destination mesh until they reached the desired host.

So how such a site either reaches an internet tunnel or connects to another site? The tower has two forms of outboard connectivity. At present, all towers use paid transit (via Clear's wimax network). Eventually, regional tower meshes will emerge (these are at a different level of organizational hierarchy from nodal meshes). Regional tower meshes will contain one or more multi-homed and fiber connected FreedomLinks, from which they will obtain their upstream bandwidth.

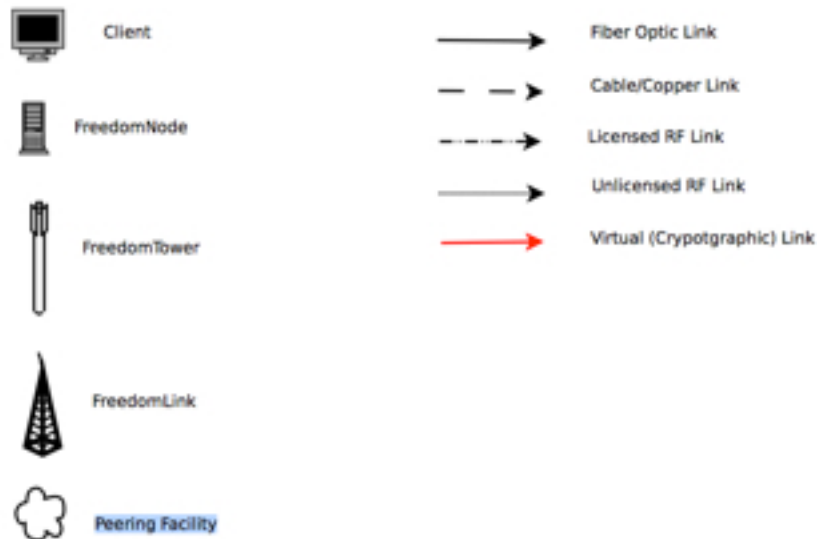
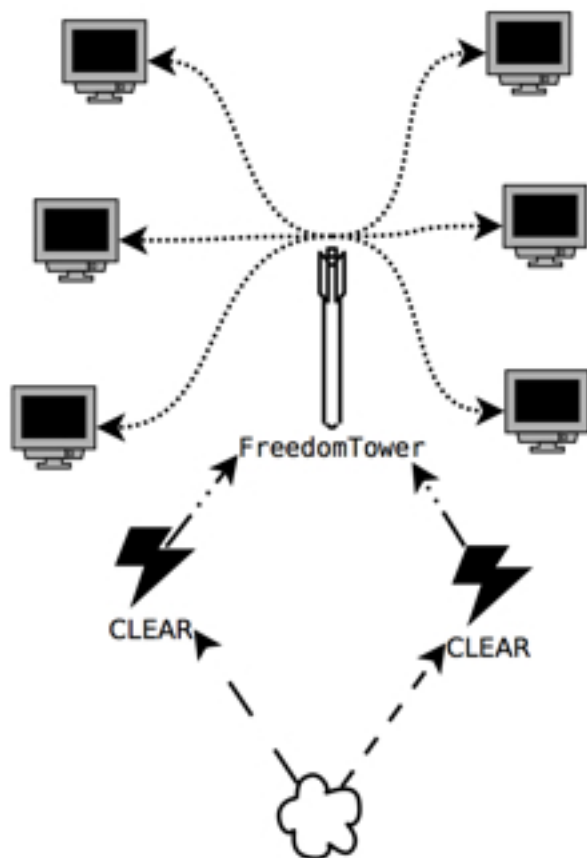
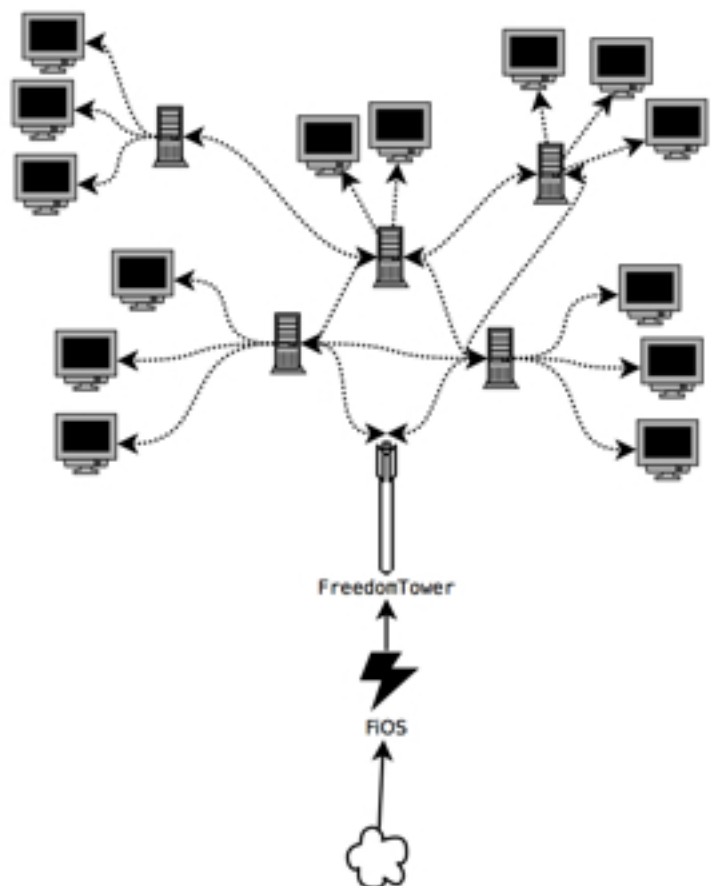


Diagram Key - A universal key to the symbols used in the diagrams



Tower Now - A diagram of the network architecture as it is currently deployed. Tower backhauls via two licensed links to Clear, and the tower distributes that connectivity directly to clients.



With Nodes - This is a depiction of how the Neighborhood Area Network architecture will change once the FreedomNodes are introduced into the mix. Keep in mind that I am using two or three nodes to represent what might be hundreds or thousands of nodes in the real work. Same with the number of towers, or clients. Basic principles are illustrated, but nothing is to scale.

COOK Report: Would you "mesh" sites together in the sense of Zuccotti parks that are within a 5 or ten mile radius? if so that mesh would be difficult or impossible if there are multistory buildings separating the sites. Yes?

Wilder: Yes, it might be, but it is certainly doable. Keep in mind that Liberty Park is among the toughest terrains in the world for the type of operation we are engaged in. Surrounded by high rises, lots of RF noise, no grid power, unfriendly security apparatus at all times, exposed, and the list goes on. If we can do this here, we can do it anywhere. And we can do it here. At present, it looks like we might put the NY FreedomLink in a colo five block from the park, with roof rights there, we can shoot a point to point link to the tower, using Fresnel diffraction to bend around the one corner in our way. Going to be pretty freaking sweet.

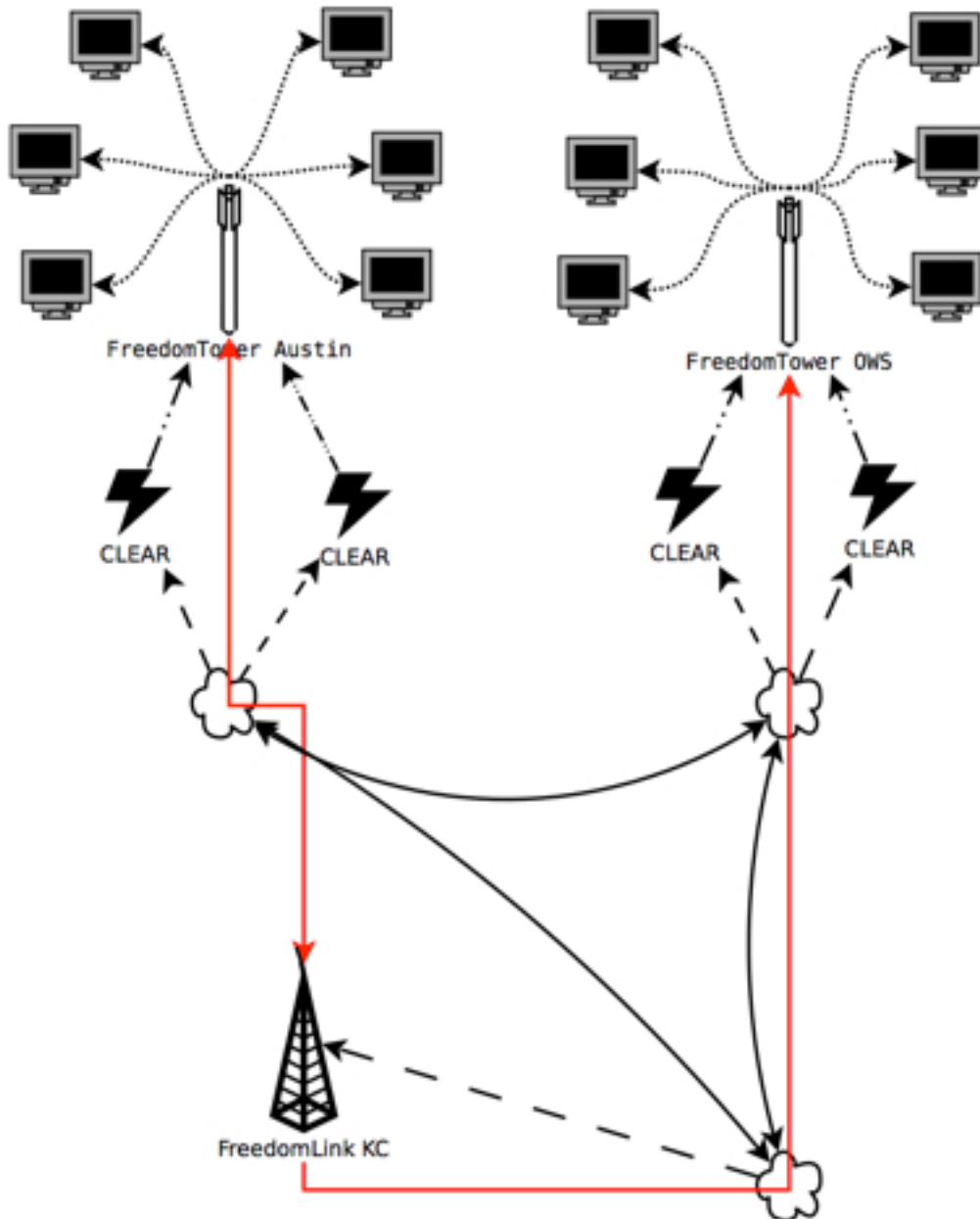
In a general sense, we just need to take the high ground. With roof rights on a tall building or two, it becomes possible to connect most sites. Do keep in mind that we can always tunnel over paid circuits when we have to. All of this is highly dependent on both RF and geo terrain. I'll go into this more in response to the next question, but the idea is to gain sufficient density using paid circuits, eating the network from the inside out. If there are participants in those buildings, then they become a relay, rather than an obstacle.

COOK Report: you have thought about how to scale this clearly - give at least one example of what multi stage scaling in an urban area of several million population would look like.

Wilder: The key here is emergence. Folks will be able to be able to achieve a degree of freedom just by connecting a FreedomNode or FreedomTower to an existing, paid circuit. So, they don't have to wait for their neighbors to come online in order to start participating. This is how we overcome the chicken and the egg problem.

So, let's break the process into stages: 1) In stage one we can expect early adopters, and freedom loving individuals to begin operating FreedomNodes. This allows them to tunnel into the free network, own their own data, etc. Additionally, we can expect the emergence of a few tower-based co-ops. Folks main motivation will be saving money on access. Density is low at this stage, and all connections are through paid circuits. 2) The early adopters that started using nodes in stage one will encourage their neighbors to participate, so that they can all enjoy the benefits of cheaper access, and more towers start to pop up. In places where the tower has gone in first, it encourage the adoption of nodes, so that people can take full advantage of the architecture, rather than solely the economic benefits. Tower density begins to rise, and the first tower-to-tower connections begin to come online. 3) Pockets of interconnected towers begin to emerge, further driving nodal adoption. Communities supporting towers band together to put up a FreedomLink on regional high ground (tower rooftops, most probably). A regional co-op is formed which drives further tower adoption.

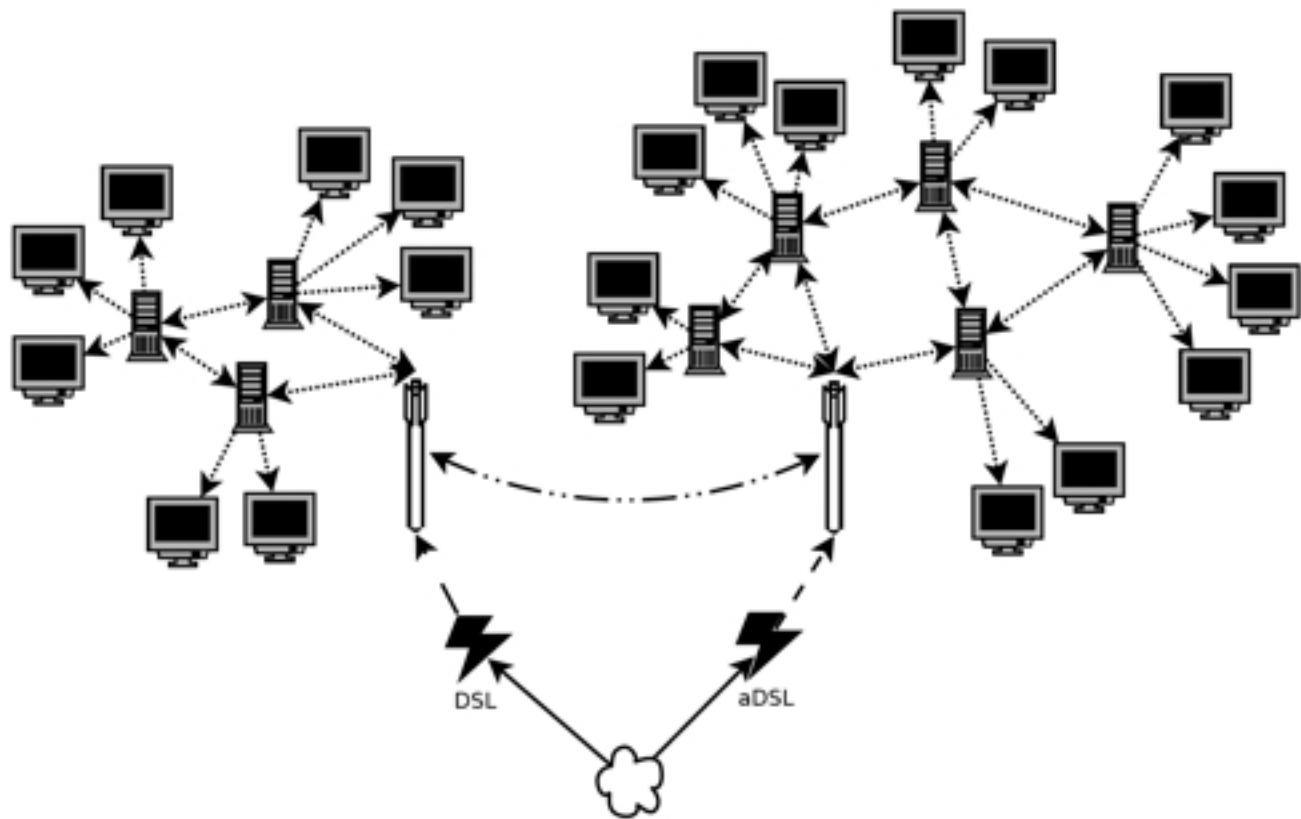
This isn't the end of line, as links still need to be connected to one another via community owned fiber backhaul. That would happen through the confederation for mutual benefit of regional cooperatives. That's beyond the scope, however, of a single urban area, so I'll leave that for later.



Two towers - Essentially shows the relationship of Austin and NYC towers as they exist now, though these could really be any towers in deployment. The towers are connected directly to an upstream provider, as before, and have the ability to establish VPN connectivity via the FreedomLink in Kansas City.







Two towers material - Shows what the network architecture would look like after nodes have been introduced, and there are two towers within microwave range.

COOK Report: but now the objective should be to link occupy sites in different cities together. Right? you tunnel traffic through an intercity broadband connection. Right? How would you begin to build and scale that? Say you connect five different occupy cities. How would you route traffic? Say you had fifty cities connected? What would have to change?

Wilder: We have already begun. Towers tunnel to the nearest link. Links will most likely form a BGP cloud (this still needs to be engineered). Links maintain routes to secure services and other towers.

Five towers or fifty towers should be within our current capacity. As more towers come on-line, however, we will need more links. Our plan is to stand up the first three or so links, and then wait for others to stand up regional links on their own. We're not really looking to be in the business of running the network - we want a federated model where people cooperate to run their own slice of the network. We're just trying to do some bootstrapping, to help folks get to a place where that's more easily doable.



COOK Report: How would you have to design your architecture in order to be assured that it can scale?

Wilder: This is a very broad question, so I'm not exactly sure where to begin. An essential part of the 'fractal mesh' architecture is that individual meshes never have to become too large. This has long been the go-to criticism of mesh networks - they don't scale. Well, we're not trying to make them scale beyond their capacity, we're trying to federate them so that they don't have to. Beyond that, we know that the architecture scales because its constituent parts are already in production deployments around the world. [BGP](#), [OLSR](#), openVPN, and the other technologies that we use are robust and field-tested, we are just integrating them in a novel way. The global internet is already a mesh network, we just want to make a network within that mesh that is owned by the people, rather than profit-seekers.

COOK Report: You would want to provide what by way of basic applications? Email and web? and voip? web 2.0? Email would be able to use attachments?



Wilder: Yes to all. You've covered most of the basics. We'll start with XMPP message passing and video streaming as a proof of concept, and go from there. I would also throw in decentralized social networking, but that will come later, with the deployment of nodes.

A node will incorporate [FreedomBox](#) which is a distribution of the operating system Debian, which will turn a headless, small-form computer into a smart router and personal server. With sensible defaults, a dead-simple user interface, and plug-and-play functionality, it will make it easy for anyone to secure, anonymize, and encrypt their communications. More than that, though, it will make it simple for anyone to participate in a neighborhood mesh network.

The reference hardware for the FreedomBox project is Marvell Technologies' [DreamPlug](#). The [DreamPlug](#) has an ARM CPU running at 1.2GHz, 2GB of flash memory, 512MB of RAM, two ethernet ports, and a single 2.4GHz radio. All that needs to be added in order to use this rig as a node in the Free Network is a pair of 5GHz radios. We call this setup - a DreamPlug running FreedomBox with the additional radios, a FreedomNode or FNode for short. The total bill of materials for an FNode could be as low as \$150, if we procured contracts with original equipment manufacturers. The 2.4Ghz radio would be used to distribute connectivity to client devices inside the home or business, and the 5GHz radios would be used to communicate with nearby FNodes and the neighborhood FreedomTower.

Do keep in mind that frequency assignments are provisional, and flexible. So, we will use whatever part of the spectrum makes the most sense given the deployment at hand. Generally that will be in the ISM band, but not necessarily. There *are* many ways to get the job done, and we'll use whichever one is most appropriate.

COOK Report: Are you aware that this MIGHT be an opportunity to use the protocols advocated by John Day? ([RINA](#)) The ones of which Fred Goldstein is a strong advocate. Could a system be done to run ip in one "partition" and days protocol in another?

Wilder: Was not aware, and am curious. We would want to wait until the protocols have been proven, but I would personally be open to such experiments, especially in a lab environment.

COOK Report: Describe each of your different configurations of freedom towers. I am not at all clear on the difference in the function of a 5 ghz and or 2.4 ghz radio and wimax modem. What is the purpose of the radio modem interaction? Does it have to do with the different antennas attached to the tower?

Wilder: With the exception of a few small details, towers are generally uniform in design. 2.4GHz and 5GHz are both wifi (802.11) standards in the [ISM band](#), which means they are unlicensed. At present, both are used to connect to participant devices. In the future, we may use point-to-point 5GHz links to connect to other towers, if we don't use licensed or licensed-lite frequencies. Wimax is used for backhaul (to connect to the Clear network) it is also an IEEE standard (802.16). All just different flavors of microwave packet radio. Here are some diagrams.

COOK Report: From an operational economic point of view how would expansion in a big metro area work? How would the user owned cooperative funding work?

Wilder: This is something we're still exploring, but there are existing legal structures designed to facilitate the operation of a cooperative. Varies from state to state. Essentially, a tower could operate like a food co-op, with membership and dues designed to cover operational expenses, but not to turn a profit. Regional, FreedomLink coops would emerge from federations of tower coops, and a confederations or partnerships of regional organizations would bring backhaul routes online.

COOK Report: From an application point of view how could this platform support teaching of the kind and content laid out by the p2p foundation?

Wilder: Can you imagine if people without jobs instead of passively watching "tee-vee" involved themselves in local economic self reliance learning? There would be an entire software layer designed to run on mesh. It would facilitate local good economy, skill sharing, time sharing, and many other modes of community-centric, peer-to-peer flavored ex-

change. Working with Johnathan Baldwin, and [the Meshkit Bonfire project](#) on this. It's still tough to imagine all the applications of such a system, but they really do seem endless. Imagine a network that connects you directly to your neighbors, rather than alienating them from you. Would change everything.

Anyways, this is a quick and dirty draft. Sorry that I don't have more time to get into. I'm happy to keep working to make clear anything that still seems muddy, and I know that there is still much work to do. Next priority is diagram, which I think will help immensely. I hope to get to those this week, but it may take longer, depending on the situation on the ground. Should be much freer in about a weeks time.

COOK Report: As it happened in less than two weeks Isaac would be beaten and robbed by the NYPD of all his possessions and thrown in jail for not fleeing during the police raid. Above and below are some pictures I took of Zuccotti on October 20.

We go now to Isaac's recounting of what happened when the police raided.



The Arrogance of Power

Written on November 20, 2011 by imw in Uncategorized

Well, as many of you have by now gathered, the FreedomTower is gone. It is doubtful that we will ever know for sure what became of the tower. We do know is that it was in the Medical tent when the NYPD attacked. We do know that not a single component of the tower arrived at the Sanitation depot where we were told to pick up our mangled belongings.

The press has already started to run with the story, but I thought it would be wise for me to tell the world in my own words, what happened that night, and in the days that followed.

On the night of November 14th, I attended a meeting of the #OWS spokescouncil – afterwards, I joined some other members

of the tech group at a bar for a drink. We were some four or five blocks north of the park. At approximately 1am, a friend named Andy received a not-messing-around text message informing us that the police had surrounded the park.

The lot of us threw some payment on to the table, and flew. We ran as fast as our feet would carry us to defend Liberty. It was our home. It was our headquarters. I made FRS contact with Security when we were a couple of blocks away. They urged us to congregate at Medical.

When we arrived, the park was surrounded by officers with their 'hats and bats.' I would be lying if I said that my initial impulse was not to flee – to take the tower, and the backpack with all of my belongings, and to run for higher ground. When we arrived at Medical, though, I realized that I would not be leaving. I could not possibly leave when so many people that I've come to know and love were preparing to throw their bodies against the gears of the violent, oppressive, and greedy machine that we call life-as-usual.



I could not go. I had to stay and defend the park. I had to build barricades and hand out masks. You may think it foolhardy, or bullheaded, or brash, but in the end, it comes down the fact that we are nothing without our principles. Material means little – courage, and integrity, and love for humanity mean much.

Finally, when the police began to close ranks, I hunkered down with Tyrone and my other brothers and sisters-at-arms, forming a human wall around the kitchen. The lights were blinding – stadium lights on all sides, many thousands of watts worth. The noise was deafening – LRAD noise weapons, fired constantly for minutes on end. We watched for hours, sitting peacefully and patiently, as the Police and Sanitation departments razed and ruined our homes. When the demolition party reached the medical tent where we had hoped to secure the tower, I was distraught. As much as I wanted to try and save the tower, I could not bring myself to unlink my arms from the brave souls on my left and my right. Police negotiators told us over and over again to stand and leave – we told them over and over again to sit and stay. They cordon of thugs grew tighter.

They were upon us. One by one they dragged us away, across the field of debris, and toward the waiting buses. Finally, they dragged away Tyrone, and I was face to face with my own decisions, in the form of a two-hundred-fifty pound, adrenaline-fueled, and ultra violent bruiser with a stick. “Time to go,” they said. I had warned the officer that I would not participate in my own false arrest. I did not protest when the demolished my tent, but evicting me from a 24-hour public park because of my opinions would cross a line of moral sanity which I had to contest.

I did not stand. I was thrown to the ground, belly first. The officer, whose name I do not know, attempted to remove my backpack. It contained virtually everything of any value to me: my laptop, my backup hard-drive, my journals, my passport, my camera, almost \$5,000 in cash, my thermos, my medical kit, my encryption keys and their revocation certificates. The officer snatched at my bag. I knew that if he took my bag from me, I would never see it again. I attempted to hold the bag, placing my hand around the straps near my shoulders. “Give it up,” he shouted, and began to strike my legs.

In a moment of absolute clarity, I realized that stuff is just stuff. Money is just money – just Fed Notes, after all, no more intrinsically valuable than monopoly money. True value is not material – it is ingenuity and skill and knowhow, love and compassion and dignity – it is not in our possessions, but in us alone. I spread my arms wide, and the bag was ripped away.

Wounded and bound, but completely serene, I was dragged across the broken glass and shrapnel left by the demolition crew. On the curb near Liberty Street, I met my so-called ‘arresting officer’ – a kid about my age assigned to fill out the paperwork. I could tell that he was hurting, having to watch such a gross abuse of power. With his help, I stood and introduced myself. When we arrived at central booking, I was searched, and given a voucher for those be-

longings on my person. I was asked to sign, but refused, saying that my backpack had been stolen by an unknown officer. I was told that I had no choice, but still I refused. After several hours, my 'arresting officer' relented, saying that I could remark on the form that my things were taken, as long as I did so quietly.

The next thirty-six hours were a bit of a haze. Most of my compatriots were held in the main tank at One Police Plaza. A few of us were held in a small isolation cell below ground. I crumpled my coat into a pillow, and Tedward and I slept intermittently. We were woken every couple of hours, and time seemed to drag infinitely. We talked about next steps, about providence and the glory of this existence, about how we've only begun our struggle.

We talked about the arrogance of power – to think oneself invincible because of great wealth. We know better – we know that a people disenfranchised and abused will rise up against their oppressors. We know that liberty, justice, equality, dignity, and prosperity have no price, can't be bought. We know better than to think that sticks or stones, or rubber bullets or water canons or dogs, or guns or tanks or bombs will ever be able to master the will of a people towards their own freedom. We talked until we could talk no more, and then we let the silence speak.

At my arraignment, I made sure that the record would show I had been robbed by armed, masked men, masquerading as officers of law and peace. I was released on my own recognizance. I went to fetch the belongings that I had been able to keep – at least I was able to retrieve my multitool. It was Wednesday. I was told that I could find the rest of my belongings at the Sanitation garage on 57th Street. I made my way there as quickly as I could. By the time I arrived there, at around 3:30pm, I was told that they were closed, and that I would have to come back tomorrow.

Come back I did. On Thursday morning, I was allowed to search through the pile of ruins. That's when this occurred. After hours spent combing through the rubble, I concluded that neither the FreedomTower nor my backpack were present. I was confident that I had looked everywhere. Wherever my things ended up, it wasn't at that Garage. Trust me – a nine foot radio tower is pretty hard to miss. I was told by a lieutenant that one more dumpster was going to be sorted that night, and that I could come back the next day, and so I did. On Friday I looked once more for several hours before finally resigning myself to the fact that I would never see my belongings again. I was saddened, not by the loss of my things, but by the loss of the democratic republic that I love.

When I ran to Liberty Park that night, I didn't expect to be robbed by those sworn to serve and protect me. I did not expect to be beaten for daring to shine a light on corruption. Now I'm a bit wiser. I've seen too much at this point, of the fear in the tyrants' eyes, to expect otherwise. They know that we are waking the world to a truth already inside. They know that the *status quo* is broken, deeply and irrevocably. They are petrified.

Who Smashed the Laptops from Occupy Wall Street? Inside the NYPD's Lost and Found

Posted by [Motherboard](#) on Friday, Nov 18, 2011

- <http://www.motherboard.tv/2011/11/18/who-smashed-the-laptops-from-occupy-wall-street-inside-the-nypd-s-lost-and-found>

If you're looking to recover any personal effects swept up early Tuesday morning in the NYPD raid on Zuccotti Park, epicenter of the Occupy Wall Street movement, there's only one place that may have what you're looking for. Only it doesn't have a marked address.

The Department of Sanitation has a brand new building. Situated at 650 W. 57th Street – the corner of 12th Ave. and 57th St., in the wasteland like Far West Side – Sanitation's address is only marked on the 57th St. side, with no sign or anyone around to point out the recovery booth, which is around the back side in a stark, wind-tunnel underpass. (To be sure, [this Sanitation press release](#) gives a run down for all those looking to recover property.)



This is where we find Isaac Wilder, head of the [Free Network Foundation](#), late Thursday morning. Wilder, who we first met on Day 3 of the occupation, is an integral part

of OWS' Signal Corps, a working group that had been dedicated to providing free Wi-Fi to demonstrators within Zuccotti. During the raid, all of Wilder's stuff, including the FNF's Freedom Tower, a thin, maybe nine-foot-tall pole, loaded on all sides with nondescript routers that had been beaming out wireless access since early on in the occupation, was confiscated not long after he and another 200 or so protestors were hauled away after barricading themselves in the middle of the park. Matt LiPani, a Sanitation representative, tells us that in the raid's af-

termath 151 Sanitation workers carted away the belongings to 650 W. 57th St. in “our collection trucks.”

And so now, at the unmarked underpass entrance, Wilder’s looking for his backpack, and his Freedom Tower. And \$5000 in cash. This is all the money he has.

No press is being allowed in to check out what we quickly hear is a large heap of



damp, mangled, cat-piss smelling stuff. So Wilder heads in on his own at around 10:30 AM, turning back to us and giving a quick, solemn head-nod before disappearing inside.

After about 30 minutes he sends us a text: “no sign of tower or backpack.” When he finally surfaces after another 30 minutes, descending a staircase into the howling, drabish underpass, the face gives it away.

Wilder hasn’t slept much in the last 36 hours. He looks shelled, haggard. He told us earlier how he and many others affiliated with the Signal Corps were held in a separate “dungeon-like” cell below the main holding tank at 1 Police Plaza in Lower Manhattan beginning early Tuesday morning through Wednesday evening. But beyond that, his report from inside the heap holds true: No backpack. No cash. No tower.

Worse, it was as if someone along the way purposefully destroyed all confiscated electronics, a strategic smashing of at least part of the digital record logged by full-on occupiers. “Dude, all the laptops are in a row,” he tells us, baffled and raking his shock of brown hair. “They’ve all been smashed with bats.” When asked about the mangled property, LiPani admits that, inevitably, certain items could’ve been damaged in the shuffle: “I’m not surprised,” he says, to hear of damaged laptops. He adds that the DSNY is providing clearance forms to those occupiers concerned their property may’ve been mishandled or misplaced.

But Wilder wants footage – visual proof to show to whoever it is he hopes will step up, legally, to defend the FNF. Hell, we want footage. At some risk, admittedly, we hand him an iPhone. He heads back inside.

Resurfacing a few minutes later, he shows us these:



It's exactly two months into "Occupy," now a global movement. Until now, Wilder has been staunchly advocating for what he sees as something extending beyond the confines of any single occupied space: decentralized, open-source, free networks. He may very well still be all about that mission.

But something just seems off. Something has shifted – in Wilder, in OWS. "Maybe we don't need the tower," he admits, a marked repositioning of what we've come to know of this well-spoken 21-year-old college drop-out from Kansas City. Maybe an occupation doesn't need material components, he goes on. Maybe we don't need the park.

With that, as we all make way for the Columbus Circle subway, an older woman representing Zuccotti's Comfort Committee working group catches Wilder by the sleeve. She hands him a

red scarf. It's brisk, windy. Low 40s.

"You see?" he says, turning to us while wrapping the wool snug around his neck. "You see what happens when you just let go? You get things."

Cook Report: I just had a good talk with Isaac a couple of hours ago. He is almost finished with a rebuild of a new freedom tower. I sense that the last couple of weeks has cemented a purpose to what he is doing that now is tempered by a shared struggles and sacrifice. A sense of being able to do something with meaning among brothers and sisters rather than sit immobilized in terror before the ugliness that many of us sense is bearing down.



I intend to work with him over the next few days to get out an "extra" Cook report that he can use for explaining his mission. And I just found this

<http://www.motherboard.tv/2011/11/21/occupy-s-internet-tower-will-live-on-for-now>

Occupy's Internet Tower Will Live On, For Now

Posted by [Brian Anderson](#) on Monday, Nov 21, 2011

Despite turning up empty handed on a first pass through heaps of personal belongings confiscated last week from Occupy Wall Street's epicenter at Zuccotti Park, Isaac Wilder returned this past Friday to a reclamation booth at a Department of Sanitation facility on the far West



Side of Manhattan.

Wilder, the head of the [Free Network Foundation](#), just really wanted his stuff back – backpack, laptop, FNF Freedom Tower (this beamed out Wi-Fi Internet to Zuccotti occupiers), and cash. These are his earthly possessions.

And so he returned to the stark, wind-tunnel underpass entrance around the backside of Sanitation's 650 W. 57th St. complex, this time combing the piles of effects for several hours. But again, nothing. "Wherever my things ended up," Wilder [wrote](#) Saturday on the FNF's blog, "it wasn't at the Garage. Trust me – a nine-foot radio tower is pretty hard to miss."

That's not to say he's giving up search for what he says are but his share of all "the important 1s and 0s" – critical evidence and large swaths of the historical record on OWS – which to him and others among the New York General Assembly's Signal Corps seem to be mysteriously missing post-raid. (We've reached out to DSNY about this and what, if any, sort of cataloguing of mishandled or misplaced property has gone on. They've not returned our call, though the [The Wall Street Journal](#) did [report](#) Saturday that 201 people had thus far shown up looking to recoup property, and that 67 people successfully reclaimed their items.) "Because as good a story as it makes for that stuff to be gone," Wilder, now reclined in the front room of a third-floor apartment in Bushwick, tells us, "it would probably be better if it weren't."

When Wilder went to the DSNY's new space last week, he captured iPhone images of what no press were permitted access to see: dimpled, mangled laptops that [looked like they had been willfully damaged](#).

Wilder's now holding out for a donated laptop. But here in the dimly-lit Bushwick space, an off-site encampment and home to Tyrone Greenfield, 23, the FNF's communications director,

quite a few computers are laying about. Records and underwear pile up in its two bedrooms. Wires snake across the floors. A cashed bowl, riot goggles. In the kitchen, beneath a multicolored Feliz Cumpleaños banner draped overhead, a painting on the wall reads: *I Hate You Bedbugs*. On a small, cluttered kitchen table, a bottle of moonshine stands next a red wool scarf.

This is the same wrapping given Wilder by a member of Zuccotti's Comfort Committee on his way out of the heap last Thursday. After his arrest during the raid, the older woman's gesture was a moment of "absolute clarity" for Wilder. Suddenly, as he wrote in Saturday's post, he realized that "stuff is just stuff." That only when you let go do you get things. Maybe OWS doesn't need the Freedom Tower, or even a park.



But this stuff does matter, Wilder acknowledges, and says the FNF plans to push forward on its build of a larger Freedom Tower than it had before. Wilder, seemingly reinvigorated, says the FNF *has* to build now, that they have no choice. He's sure to distinguish between mere material – "lucre, stuff for the sake of stuff" – and community property and tools. And the very es-

sence of our humanity, he continues, is in our ability to use these tools, particularly information technologies. “The tower is a tool that’s very useful,” he says. Wilder and Greenfield and others in the FNF and OWS Signal Corps, which Wilder admits share blurred lines, are set to build tomorrow. This will be the FNF’s fifth Freedom Tower.

Now that protesters are disallowed from entering Zuccotti with so much as a backpack, where will the tower go? Wilder’s planning for it to sit in either the atrium of 60 Wall Street, American home of the Deutsche Bank, or in any of the foreclosed buildings the movement potentially plans to occupy. Participants throwing full weight behind this sort of squatter tactic would only mean more towers being upped and live, we’re told. And not just regionally. Ideally, the FNF wants to see towers across the country.

For now, Wilder is still holding out for legal aid, and says he intends to file a suit against the City over his lost and damaged property. Here is the [brief YouTube Video](#).

Free the Network IndieGoGo Campaign

curiousjohnmedia 1 video  




44 views 

Uploaded by [curiousjohnmedia](#) on Nov 27, 2011

The Free Network Foundation envisions technologies that will transform the network into something owned and operated by the people, rather than by

0 likes, 0 dislikes

[Remix this video!](#)

[Show more](#) 

Isaac and the Freedom Tower at Contactcon October 20, 2011

I talked with Isaac and asked him to explain what Freedom Tower was. His answer: It is a very rapidly deployable mobile hotspot. For the last 8 days or so it has been providing network connectivity to the occupation in liberty Square. It consists of a few components.



Inside the box is an uninterruptible power supply. The UPS power supply will allow the tower to operate for a couple of hours on battery power alone. We also have a number of WiMAX modems. A router that is load balanced in the upstream direction is connected to this switch where the radios cut in. There are 6 radios overall. Three 2.4 GHz radios and three 5 GHz radios. The 2.4 GHz radios transmit with a strength of 18 dB a piece and the 5 GHz radios transmitted at the rate of 11 dB a piece. This gives us a coverage radius of about a half a mile. We have no problem covering all of liberty Square as well as reaching up and down the Trinity and up and down Broadway. The rig is used to create the Internet connection for liberty Square and its software enables it to connect with a VPN tunnel to a wireline broadband Internet connection.

In addition to the free network foundation is committed to helping to build a secure virtual private network connecting occupations in the United States with each other for cooperation and coordination and reaching out to occupations in Europe and other parts of the world. Say that we want to coordinate to March across the United States and across other parts of the world at St. Noon GMT time and we do not want a secure encrypted private VPN is about the only way to do this . We could log into an IRC channel that is encrypted through one of these VPN tunnels and plan a coordinated response with a reasonable expectation that our communications would remain private.

Now this small box is the router a Lenovo 2150 with an atom core. We put a variant of open pfsense. It is very powerful operating system for doing routing load balancing and

VPN termination. Now this is a simple 8 port network switch and these are power injectors for the radios. The reason why we can run just a single cable to each of these radios, something that simplifies the builder great deal, is that we use a technology called power over ethernet which puts the necessary voltage on the data line:

Cook Report: Are these radios built by Ubiquiti?

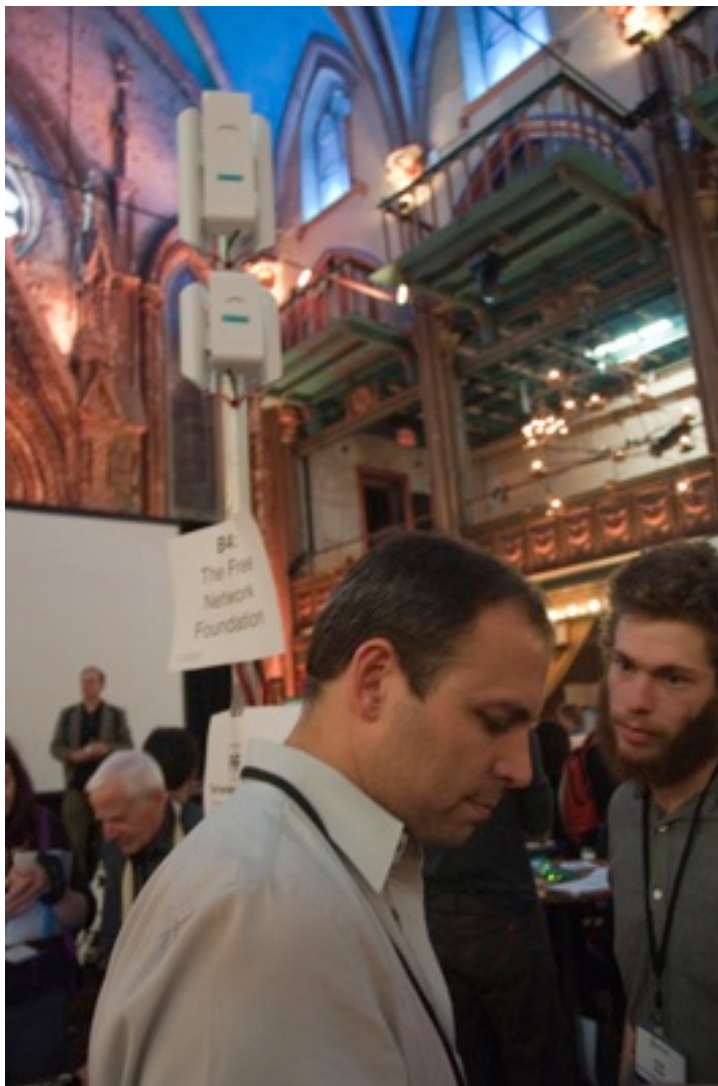
Wilder: Yes they are. [Ubiquiti](#) really changed the game. What you get at the price point for these radios is simply unbelievable.

Cook Report: And the price for the complete tower set up is?

Wilder: \$1500.00. Plus \$600 for a generator if you are going to operate in the field. We tried solar for a while but the problem is that at the bottom of this canyon we get only about 2 hours of sunlight a day. We also are contemplating a battery pile with an inverter

so that you can hook up bike peddle and get mechanical power. You can earn local occupation currency by peddling the bikes. It is increasingly obvious that the occupations will have their own currency that you earn by helping improve the world.

Cook Report: How big and heavy with the battery pile be?



Wilder: It would be pretty large and pretty heavy and probably cost a couple thousand dollars. Now in LA they are running on solar which is definitely the direction we want to go.

Freedom Tower Materials and Assembly

Bill of Materials:

- A quiet power generator such as the Honda EU1000i (\$800)
- A UPS such as the APC BE750G (\$100)
- A nettop such as the Lenovo IdeaCentre (\$300)
- An 8-port network switch (\$15)
- Three USB->Ethernet adapters (\$30 x3)
- Two 4G modems such as the Clear Series M (\$85.00 for each modem, \$45.00 for first month for each, \$30.00 activation fee total (\$320.00 total) [Procure from Clear store so no contract required]
- Three Ubiquiti NSM2's (\$80 x3 = \$240)
- Three Ubiquiti NSM5 Locos (\$50 x3 = \$150)
- Enclosure for UPS, computer, router, modems, and radio power injectors (\$115)
- EMT Conduit mast (9') \$12.00
- Two ten-inch sections of 2x10" board \$10
- Five power splitters
- 50' red CAT5
- 25' black CAT5
- Velcro, zipties (\$20)

Needed supplies:

- Drill
- 1/2" bit
- RJ45 (ethernet) Crimper
- Label maker
- 1 Hour Epoxy

Abstract: There are two phases in the construction of a FreedomTower: configuration and assembly. Configuration has three stages: modems, router, and radios. Assembly has two: enclosure and mast. We will begin with configuration, and move into assembly.

Phase one: Configuration Stage one: Modems We recommend that you procure the wimax modems for your tower through a corporate account with Clear. There is no price difference, and it will give you access to second level support, should the need arise. Once you have procured the modems (we suggest two, but you could use as few as one or as many as are needed), configure your machine to look for an address via DHCP on your wired interface. Plug directly into each modem in turn. You should be able to access the web administration interface of the modem by navigating to 192.168.15.1 - the password is set by default to CLEAR123, but maybe still be the OEM default of motorola. Once you're in, you should change the password, and record the WAN IP address of the modem. If you're only using one modems, that's it. For those using two or more modems, there is

another step. Because all Clear modems are set to the same address by default, it will be necessary to change the DHCP settings so that each modem has a different address. Leave one modem as 192.168.15.1, and number additional modems by iterating the third octet: 192.168.16.1, 192.168.17.1, etc.

Stage two: Router The heart of the FreedomTower is a nettop computer running pfsense, a variant of openbsd, that makes it easy to do network administration. We used the Lenovo Q150 in our build, but ran into problems when we discovered that the south bridge of the Q150's chipset is not supported by openBSD. You may wish to proceed as we have, by working around the problem using USB to Ethernet adapters, or you may wish to explore alternative nettop hardware. If you do the latter, please let us know how it goes. Hook up your nettop to a monitor and keyboard. You will need a live image of pfsense. You should use the stable release of version 2. Before you proceed, connect the box to at any WAN connections, and to the network switch. Install pfsense on the box, configuring it to accept an address via DHCP on all WAN connections, and to serve addresses via DHCP to the LAN. Once this is done, you'll want to reconfigure the LAN settings to expand the subnet. We recommend using 192.168.10.0 through 192.168.254.254. Then configure DHCP to hand out that range of addresses. << Wouldn't this be the FNF coordinated subnet? The next step is to set up load balancing against the WAN connections. This is done by creating a gateway group, and making a firewall rule to route all lan traffic to that gateway. << Let's add screenshots here

Stage three: Radios

A) Label them with

Role (mesh node 5/2.4ghz node (x), mesh node 5/2.4ghz gateway)

WLAN IP

LAN IP

(pic 1)

Configuring the radios has two steps. First, it's necessary to flash the devices with the proper firmware. We'll go over that procedure once, but you'll need to do it for all six radios. For the time being, we are using a version of Ubiquiti's AirOS that's been patched to support OLSR routing. You'll also need to have TFTP installed on your machine. It is widely available via your favorite package manager. The firmware can be found here:

LocoM5: Using binary image from

<http://build.ffgraz.net/ubnt/AirOS%20v5.x/XM.v5.3.3.sdk.9634.with-olsr-0.6.1/> Nanostation2:

<https://wiki.graz.funkfeuer.at/UbntStations?action=AttachFile&do=view&target=XS2.ar2316.v3.5.SDK.100607.2152.bin>

(background material on the fimware

<https://wiki.graz.funkfeuer.at/UbntStations> <http://wiki.ninux.org/UbiquitiNanostationM5>

2) Power them all up

Once you've got the firmware on your machine, you'll need to put it on the radios. First, you'll configure your machine to have a static address in the 192.168.1.x subnet. Any address besides 192.168.1.20 will work. Next, take an unpowered radio, and depress the reset button. Continue to hold the reset button, and plug the radio in. Continue holding the reset button until the lights on the radio flash 1-3, 2-4, 1-3, 2-4. Release the reset button.

The radio is now in TFTP flash mode. You'll want to ping 192.168.1.20 to make sure that you've got a connection to the radio. Navigate to the directory where you've stored the firmware binary, and flash it to the radio using the following commands, there is not tab-to-finish in TFTP, so you'll have to type everything out: `tftp 192.168.1.20 bin trace put firmware_binary`

Did this via tftp (http://www.ubnt.com/wiki/Firmware_Recovery#Linux_Users)

Wait until you see the lights stop cascading back and forth, and an ARP request like:

```
02:56:43.542358 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 46 02:56:43.844753 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 46 02:56:44.147153 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 46 02:56:44.449547 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 46 before you consider the firmware complete. Also be VERY gentle with the reset switch. Very light pressure required. Use a paper clip. DO NOT USE A SCREWDRIVER. This will almost certainly break the reset switch.
```

Once the transfer has finished, you can quit TFTP. Wait several minutes for the radio to reboot. Once it comes back online, navigate to 192.168.1.20 in your browser. You should be presented with the ubiquiti web interface. The default username and password are `ubnt:ubnt`. We recommend changing the admin user name, and the hostname. Our radios are named FNF2-0, FNF2-1, FNF2-2, and FNF5-0, FNF5-1, and FNF5-2. Once you've changed these settings, you should also ssh into the machine in order to change the password, using the command `passwd`.

All radios should be set to bridge mode, and configured to obtain an address via DHCP. The 2-0 and 5-0 radios will be configured as access points, and the 2-1, 2-2, 5-1, and 5-2 radios will be configured as stations. You should also make sure that all radios are set to a 20MHz channel width, and have AirMax turned off.

On the 2-0 and 5-0 machines, you'll set SSIDs for the networks. Ours are called 'The Free Network' and 'The Free Network 5GHz'. Once you've set the SSIDs on the Access Points, you'll lock the station radios to the MAC address of their respective APs.<< I believe the lock step is only on the nsm hardware in the 5.2 airos

At this point, you'll probably want to configure the router to grant a static lease to the radios. Ours are numbered 192.168.2.0-2 and 192.168.5.0-2 << do we want to encourage a separate vlan for management?

As far as configuration goes, that's it! You're ready to put everything in the enclosure

Phase Two: Assembly Keep in mind here that these instructions are based on the components listed in the Bill of Materials above. If you've chosen to use different hardware, your mileage may vary.

Step One: Enclosure In order to keep the power supply stable, it will be necessary to fill the bottom gap (between the wheel wells of the case) with the boards. Epoxy the two boards together. Then epoxy the boards to the bottom of the case, in the center, being careful to keep the boards flush with the bottom. Once the boards have cured, attach the power supply on top of them using a couple strips of velcro. Carefully not to affix the velcro such that it makes it impossible to open the battery compartment of the UPS. The power supply should be attached such that the cord exits at the bottom right corner of the case.

As you may notice, the case can't shut with a power cord in between the base and the lid. Use a knife to carve away the closure lip, without cutting through the weather seal. You should be able to close the case around the power cord, and maintain a water-tight closure.

Next, you'll mount the modems, one (or more) on either side of the case. Use velcro. Be generous. Then mount the nettop. Same story. Use velcro. We mounted ours so that the fan vent is up, which puts the power button against the back wall of the case. This helps avoid accidental power cycles. Again, same story with the switch, but this time, mount it to the top of the case. Depending on what model of switch you have, you may want to remove the rubber feet before applying the velcro, as the feet tend to slip out of their fittings. Next task is to mount the power over ethernet injectors for the radios to the lid. The ports should face the top. Now you're ready to plug the five power splitters into the five outlets labelled 'sure protections and battery backup'. This is so that the entire rig can run off of batteries. We use the three splitters on the left for the power injectors, and the two on the right for the modems, router, and switch.

Plug everything in. Tidy up with zipties where you can, and you're ready to move on to the mast.

Step Two: Mast

The mast consists of the six radios mounted atop a piece of conduit, with an ethernet run through the middle of the mast, and out the bottom. On one end, drill two 1/2" holes in a vline, one XX inches from the end, and another XX inches from the end. The top hole will be for the ethernet cables going to the NSM2s, and the bottom will be for the NSM5Ls. XX inches from the bottom, drill two 1/2" holes in a horizontal line, with about 3/4" between the two. Now run 11' sections of uncrimped ethernet cable through the mast. Cables that enter through the same hole should exit through the same hole. Use two red cables and one black per hole. The black cable will carry power and data. The red cables will carry only power. You might use fish tape or string, and a bent wire hanger to make the process go quicker. Once the cables are through, crimp both ends.

Ziptie the radios to the mast, and plug in the cables. Mount the mast on the tripod, and run the cables down around the tripod. You'll need to do the same for the two ethernet bundles as you did for the power cord. Carve away the lip of the closure, but leave the weather stripping. Plug everything in, and you've got yourself a FreedomTower!

Ends and Means

of the Free Network Movement

(draft)

August 2011 [Editor I have copied this from the freedom network's wiki at http://www.freenetworkmovement.org/commons/index.php?title=Ends_and_Means]

Introduction

An introduction to the Free Network Movement, and an overview of the key points contained in this document.

- The Free Network Movement aims to promote the free and equitable transmission of information in data networks.
- The FNM is accomplishing this aim by designing, specifying, and stewarding the emergence of telecommunications infrastructure that is owned and operated cooperatively, by those that use it - rather than by for-profit and state actors.
- The architecture of the Free Network enables information exchange that is *materially*, rather than *logically*, peer-to-peer. We call this architecture *fractal mesh*.
- The Free Network will be immune to censorship and resistant to breakdown - it is highly distributed and capable of operating independently of existing infrastructure.
- The FNM is part of a global movement towards *digital self-determination*. It contributes to, and draws from, free software projects from around the world.
- The Free Network technology stack will precipitate an array of inventive commercial applications. Its political and social import is such that it necessitates a non-profit stewardship entity whose organizational process is driven by consensus.
- The Free Network Foundation is registered as a Missouri non-profit corporation, and has submitted IRS form 1023, the application for tax-exempt status as a public charity under section 501c(3).
- We intend to raise \$50,000 in our first capital campaign, for the purposes of prototyping and demonstrating a free network.

Vision

A description of the architecture and applications of the Free Network, from its component hardware and software, to its commercial, political, and social upshot.

Material Peer-to-peer

The most salient feature of the Free Network architecture is its ability to enable communications that are *materially* rather than *logically* peer-to-peer. In [logical peer-to-peer](#), the pattern of value exchange is peer-to-peer, but the pattern of information exchange is not. This is what we have today with, for example, [BitTorrent](#) or [GNUtella](#), [Freenet Project](#) or [I2p](#). Value moves from peer to peer, but the information itself passes through an intermediary (the Internet Service Provider). We are not truly engaging in peer-exchange when we involve a paid, third-party provider for bit moving. Such activity fits the peer-to-peer model only at the level of the application layer, a logical overlay, the very highest layer of the network stack.

What the Free Network enables is a radical departure from such a shallow model, towards a model that is peer-to-peer from the ground up. This means that everything from the physical medium of transmission (radio waves), to the pattern of exchange (social networking), is based on horizontal peering. Neighbors talking to neighbors directly, or via other neighbors, eventually without the need for paid bit-transit.

The Five Freedoms

The idea of [material peer-to-peer](#) captures this notion, but it does little to explain its far-reaching and appreciable benefits. We summarize these benefits in what we call the [five freedoms](#): [access](#), [transmission](#), [storage](#), [authentication](#), and [consignment](#).

Access

The first freedom is access - In a Free Network, constituents would pay only the actual cost of owning and operating their share of the network. Buy and power a FreedomNode, and you become part of the Free Network - contribute to your local co-op, and make the economies of scale work to your benefit. Compare this to today's environment, where network 'consumers' pay the costs of access, plus a hefty margin, in order to lease a line that is owned by a corporation.

Transmission

The second freedom is transmission - this is the ability to send bits from peer-to-peer without the prospect of interference, interception, or censorship. The Free Network achieves this aim through the use of cryptographic best practices, and by eliminating the network choke points where packet inspection is likely to occur.

Storage

The third freedom is storage - the FreedomBox allows people to run their own network services, such as social networking, telephony, and web hosting, and thereby enables them to maintain possession of those bits. Due to the fact that the FreedomBox is in the possession of its owner, gaining access to its contents would require a warrant or subpoena. This is not the case in the current network environment, where bits pertaining to our private lives are scattered and held in various data centers around the world.

Authentication

The fourth freedom is authentication - people ought to be able to maintain an identity that is verified as authentic by others. This technology is called a 'Web of Trust,' and is built into the freedom-enabling software stack at a low level. Just as important, however, as the ability to present a verified identity, is the ability to present a pseudonym, or to remain anonymous entirely. The Free Network will make the authentication spectrum easily intelligible to its constituents, and clearly indicate whether a given session is onymous, pseudonymous, or anonymous.

Consignment

The fifth and final freedom is consignment - the ability to perform exacting mechanisms of access control. In large part, this is about making it easy to see and manipulate individual privacy settings, yet it is also contingent upon storing one's data locally. When people own their own data, and are able to decide exactly who can access it, bit consignment becomes a willing, rather than unwitting action.

Overview

The Free Network is not just a leap forward - it is also a survival strategy. The current hierarchical network model will not scale to meet the demand of an increasingly networked world. The obvious fix is to keep local traffic local, and that is something that can only happen efficiently on a network that enables material peer-to-peer.

The Free Network will offer a richer network experience at a fraction of the price, and in so doing provide a technological platform for a new wave of innovation. It will enable communities to leverage the economies of scale, driving down the price of network access while increasing network resilience, and reducing our susceptibility to interception and censorship. It will allow us to meet the surging global demand for network access, and ensure that no one ever again goes hungry for knowledge.

The Free Network is unlike what has come before - it is the people's network, owned at

once by all and none. The technology to build this network exists. At this point, it is a matter of making it possible for all to participate, through integration, optimization, and packaging.

The fundamental technology that underpins the Free Network is that of the [mesh network](#). A mesh network is one in which nodes pass messages directly to one another, rather than through a central hub. This type of network topology is *horizontal* and *decentralized*, meaning that no node is a [single point of failure](#). Mesh networks are *self-healing*, meaning that the network has the capability of routing around a node that fails.

The concept of the mesh network is not new - in fact, the original premise, and promise of the Internet was of a wire-line implementation of mesh principles. We view the Free Network as a harkening back to those original principles of distribution and resilience from which the network of networks was born. From the perspective of telecommunications companies and Internet service providers, at the level of the [backbone](#), the Internet *is* a mesh network. The problem lies in the fact that Telcos and ISPs have themselves become points of centralization and control. By implementing a network [access layer](#) which is hierarchical, companies such as [Verizon](#), [Comcast](#), and [AT&T](#) have gained the ability to route packets through centralized hubs, and inspect those packets in the process. The Free Network represents a departure from that model, and a return to an Internet that is controlled by no one and every one at the same time.

As we proceed, keep in mind that the global communications network is a construction of immense scope and complexity. For any initiative with the aim of bettering that network to be successful, it must rely upon the principle of [emergence](#). That is, the desired changes must come about in a manner that is gradual and organic. What follows is a description of our ends, but not our means. A feasible means of achieving such an end is described in detail in section 3 of this document.

Wireless implementations of the mesh topology have evolved over the course of the last two decades, from a theoretical and experimental novelty, to a field-tested and battle-hardened production technology. Metropolitan-scale wireless mesh networks exist in several European cities, and smaller networks are in operation around the world. The proposed architecture of the Free Network uses the wireless mesh as a design element, but expands upon and improves the idea.

Our innovation is called [fractal mesh](#), and consists in the application and interconnection of mesh networks at different scales. A neighborhood mesh of a few thousand nodes (what we call a [neighborhood network](#)) is connected to other neighborhood networks in a

regional, [backhaul](#) mesh. This regional network is then connected to other regional networks via a global mesh of [fiber-optic](#) and [satellite](#) routes.

In a Free Network, the people become their own Internet service provider. Instead of paying profit to those that own the infrastructure, they themselves are the owner. One receives access to the network in exchange for agreeing to provide access to others. This is possible using current technology, but it is exceedingly difficult. Our aim is to specify standards for the interoperability of free networks, and to produce networking solutions that assist people in the construction of such networks. In order to achieve these ends, we will build a reference implementation, which can be copied, modified, and improved upon.

Of paramount concern in the implementation and integration of the technologies referenced in this document is their accessibility to all users. The clearest path to a freer network is to take those freedom-enabling technologies that exist today, and make it possible for anyone to use them. That's where the *FreedomBox* comes in.

Components

[FreedomBox](#) is a distribution of the operating system [Debian](#), which will turn a headless, small-form computer into a smart router and personal server. With sensible defaults, a dead-simple [user interface](#), and plug-and-play functionality, it will make it easy for anyone to secure, [anonymize](#), and [encrypt](#) their communications. More than that, though, it will make it simple for anyone to participate in a neighborhood mesh network.

The reference hardware for the FreedomBox project is Marvell Technologies' [DreamPlug](#). The DreamPlug has an ARM CPU running at 1.2GHz, 2GB of flash memory, 512MB of RAM, two ethernet ports, and a single 2.4GHz radio. All that needs to be added in order to use this rig as a node in the Free Network is a pair of 5GHz radios. We call this setup - a DreamPlug running FreedomBox with the additional radios, a *FreedomNode* or *FNode* for short. The total bill of materials for an FNode could be as low as \$150, if we procured contracts with original equipment manufacturers. The 2.4 Ghz radio would be used to distribute connectivity to client devices inside the home or business, and the 5GHz radios would be used to communicate with nearby FNodes and the neighborhood [FreedomTower](#).

An *FTower* is owned and operated cooperatively by a neighborhood network, roughly the size of a census tract. It has several 5GHz radios for communicating with FNodes, and 3650MHz radios for long-range links to other FTowers. It is important for the FTower to be visible to a significant portion of the neighborhood network. Line of sight dramatically improves the quality of radio communications links.

Within any group of 200-300 FreedomTowers would be a single [FreedomLink](#), serving a population of up to a million, connecting them to an Internet backbone. The *FLink* would communicate with the towers over 3650MHz, and maintain a multihomed fiber connection to the Internet Protocol core. It would, again, be owned and operated by the community, allowing them to participate in the actual Internet by speaking [BGP](#) to other networks.

With community-owned fiber and satellite routes between FLinks, the picture is complete, and the constituents of the Free Network would be able to purchase network access at cost.

This may sound like no small feat, and that's certainly true, but the Free Network Movement has a truly practicable plan for making this vision a reality. Our strategic vision is explained in detail in Section 4 of this document.

Context

An overview of major stakeholders in the global network, including state and corporate actors, followed by a rundown of key initiatives in the distributed networks problem space.

Stakeholders

The Free Network Foundation is an American organization with global ambitions. The United States is not only our base of operations, but it is also, in many ways, at the heart of the network. As such, this stakeholder analysis focuses heavily on aspects of American enterprise and regulation. The telecommunications space is highly complex, but can be roughly divided into three types of networks, performing some combination of three different services.

Networks are Tier 3, Tier 2, or Tier 1, with each network providing some combination of access, transit, and peer services. Let's look now at each type of network, and get a feel for the services they provide.

Tier 3 Networks

[Tier 3 networks](#) are essentially resellers - traffic does not cross a tier 3 network, but originates or ends there. A tier 3 network purchases bandwidth from an upstream provider at a [Point of Presence](#), and delivers that bandwidth to end users. They do so either by building a network, or by leasing the requisite lines from an incumbent operator. This type of operation is termed access, or [last mile](#).

Conventional last-mile models for broadband delivery are cost effective only in areas with population density above a certain threshold. Those in unserved rural areas must resort to expensive, high-latency satellite solutions, or settle for dial-up speeds.

Access operations are those elements of the communications infrastructure with which the customer comes into contact. These are the lines that branch out from Central Offices into each home or business. In the existing model, these circuits are exclusively vertical - that is, they allow connections only from a client to a service provider, but not from client to client. This prevents the exchange of information in such a way that the service provider does not function as a paid intermediary.

Of the [Autonomous Systems](#) that make up the Internet, the vast majority are Tier 3 networks. There are upwards of twenty thousand such networks in operation today, generally outside of the United States.

Tier 2 Networks

In addition to engaging in the access operations described above, Tier 2's have regional reach, and trade or sell bandwidth to other networks. Network to network traffic is classified as either peering or transit.

[Tier 2 networks](#) are large enough that they are able to [peer](#) with some other networks for mutual benefit, but not so large that they are able to completely avoid paying for bandwidth from a more widely connected network. When networks peer, they agree to exchange traffic without the need for monetary settlement. When a network purchases bandwidth from another provider, it is said to purchase [transit](#) across that network, or simply to buy transit.

To build a Tier 2 network requires significant capital investment, even in the hundreds of millions or billions of dollars. In addition to being connected to end users and entire access networks, Tier 2 networks often connect to [Internet Exchange Points](#), where Internet Service Providers can openly exchange IP traffic.

The roughly three thousand networks of this type do the majority of bit moving on the Internet. They are much fewer in number than the Tier 3's, but they are much larger, on average, and have a much greater aggregate capacity.

Tier 1 Networks

[Tier 1 networks](#) have global reach. These are well-connected bit moving platforms, worth many billions of dollars. From the perspective of a Tier 1, all other networks are either big enough to mandate a peer relationship, or are willing to pay for transit.

Building such a network entails laying thousands of miles of fiber, across oceans or continents or both. The majority of Tier 1 networks are based in the United States, even if their core network includes points of presence overseas.

There are a very limited number of Tier 1 providers - and perhaps none that truly do not engage in settlement at all. Still, there is a group of ten or so networks that are well understood to qualify as Tier 1.

If the ongoing merger of [Level 3 Communications](#) and [Global Crossing](#) should be approved, it will represent a significant consolidation of power within this inner circle of network operators.

Tier 1 carriers have made significant capital investments in recent years to improve and expand their capacity. Still, global data exchange is increasing at rates that outpace the ability of major carriers to provision new infrastructure. A paradigm shift is needed in order to sustain the network's growth.

Initiatives

Peer-to-peer, decentralized, and distributed systems have been the topic of much research and development in recent years. What follows is an examination of some initiatives that have emerged in the problem space, and the ways in which those initiatives complement one another.

Federated Social Web

In the past few years, many initiatives have emerged that aim to build a social web built on open standards, where a federation of servers, rather than a single behemoth, stores user profiles. Notable efforts include [GNU Social](#), [Friendika](#), [Buddycloud](#) and [Diaspora](#). Not all of these projects are interoperable as yet, but they are increasingly converging on a set of standards.

[OStatus](#) and [XMPP](#) have emerged as viable protocols in the space of status sharing and message passing. All of the networks mentioned above employ some combination of these two platforms.

Of note, however, is that *all* of the federated social platforms mentioned above, regardless of other design parameters, are intended to run on a *server*. The ideas motivating these efforts are good ones: to encourage decentralization of infrastructure, and help people take some control of their own data. Yet, existing solutions have not accomplished this outcome, because the barriers to entry and technical knowledge required to operate today's servers are prohibitively high. Thus the need for [nodal computers](#) to take part in the federated social web.

Nodal Computers

Eben Moglen's vision of a low-power, headless home server that *just works* has spread like a shockwave through the freedom-loving computing community. The ramifications of the idea are clear - it would allow ordinary users to own their data, secure their communications, and maintain their privacy.

There are number of large, outstanding challenges in the effort to create a home server that's easy to use. While the community has been more-or-less able to converge on elements of the server backend, little progress has been made in the way of a user interface, or in provisions for high fault-tolerance and reliability. If the FreedomBox project is successful, there is no telling the importance of the role that these boxes will come to play in their owner's lives. To achieve the goal of widespread adoption, it is of critical importance that the box be able to run continuously, without major interruption, for years on end. It will need to be securely and automatically backed up, so that a system failure doesn't represent the loss of one's entire social graph and media archive.

These problems are challenging, but by no means impossible. Like any product or project, the FreedomBox will take years to reach maturity. As the nodal platform crystalizes and the userbase grows, it is time to begin exploring what freedom-enabling systems could be constructed using the no-fuss, always-on home server as a building block.

It is not enough to settle for communications that are encrypted, but peer-to-peer on the logical level only. The advent of the nodal computer represents an opportunity to change the nature of our communications in a more fundamental way. Yet, in order to do so, we will need a naming system that is decentralized, and mesh networking technology that makes configuring a node as easy as turning it on.

Distributed Social Networks

There are also social initiatives which operate in a more P2P-oriented style with all social computation and modeling happening in a software running on the user's device itself. [Social Swarm](#), a working group of the German digital rights foundation FoeBuD, is researching such solutions as they bear the very favorable feature of enabling end-to-end encryption between all communication members, leaving no unencrypted data on server nodes. In contrast to the *federated social web*, this solution would require no installation of nodal computers in people's homes.

Distributed Global Names

There is a classic problem in network theory, commonly referred to as [Zooko's Triangle](#). It states that, at best, a name can have two of the three following characteristics: secure, distributed, and meaningful to humans. Names that are globally unique and not controlled by a central authority generally end up being ugly strings of bits, such as IP addresses or `[[Tor|.onion addresses]]`.

The existing solution to this problem is the widespread use of names that are secure and meaningful, but controlled by a central authority. This system is called the [Domain Name System](#), or DNS, and is ultimately under the auspices of the United States Department of Commerce National Telecommunications and Information Administration - the [NTIA](#).

Yet, there is something new on the horizon, predicated upon a relatively new technology that is just reaching production-level maturity. The [Distributed Hash Table](#) is a mechanism for storing a set of key-value pairs across many separate machines. By itself, it does not solve the problem of Zooko's Triangle, but were it to be coupled with a mechanisms for [pet-naming](#) and [access control](#), it could form the basis of a human-usable, globally distributed naming system. Such a naming system would help devices such as the Freedom-Box find one another, regardless of ISP policy. It would also allow for seamless integration between material and logical forms of peer-to-peer communication.

Wireless Mesh

Wireless mesh networks, as mentioned before, are networks where nodes are connected to one another horizontally and redundantly. Mesh nodes can connect to one or more of their peers, and not just to an upstream hub. Wireless mesh networking enables local communications without the need for a paid Internet Service Provider. Mesh technology has come a long way, but still has some severe limitations: there is no user-space utility for easy construction and management of mesh networks, and those mesh networks that do exist are used almost exclusively as means of accessing the Internet.

At present, there are two leading algorithms in the arena of mesh routing - [Optimized Link State Routing](#), and the [Better Approach to Mobile Ad Hoc Networking](#). These protocols have been employed and applied by a number of community networks and research groups - notably [FreiFunk](#), [FunkFeuer](#), The [Serval Project](#), The [Village Telco](#), The [Commotion Project](#), and [Project Byzantium](#).

Optimized Link State Routing, or OLSR, is widely utilized. It has been deployed by community networks such as Austria's FunkFeuer to great effect. Though recent iterations have decreased CPU usage, and improved throughput, OLSR's primary drawback is heavy CPU usage, especially in discovering and repairing routes.

The Better Approach to Mobile Ad Hoc Networking, or BATMAN, emerged from the German FreiFunk community. Its latest iteration, BATMAN Advanced, works at a lower level of the network stack than other mesh implementations, and has now been incorporated into the mainline linux kernel. It has been utilized by The Village Telco, in the creation of their turn-key mesh router, the Mesh Potato, and by the Serval project in the creation of the Batphone Android application. Batphone allows the user to engage in mesh-based telephony using ordinary phone numbers.

Other significant mesh networking initiatives include The Commotion Project and Project Byzantium, both based in Washington, DC. The Commotion Project is an effort to integrate and standardize the use of existing mesh technologies on a variety of hardware platforms, and is part of the New America Foundation's Open Technology Initiative. Byzantium is being developed by a group of enthusiasts from HacDC, with the aim of building a Linux LiveCD that supports materially peer-to-peer versions of various network applications (web, telephony, chat) for use in emergency situations.

Wireless mesh technology has progressed over the course of the last decade to the point that it can be reliably deployed in production environments. Still, such deployments must be carefully planned and administered. The key outstanding challenge is to make it easy for anyone to build and run such a network, and to do so in such a way that users are encouraged to take advantage of the opportunity to route traffic locally. This could be accomplished by integrating mesh technologies into a nodal platform that includes sufficient radio hardware.

Strategic Roadmap

A strategic roadmap for the development of technologies that support material peer-to-peer and the deployment of fractal mesh infrastructure. An exploration of how humanity

can achieve co-ownership of network infrastructure, utilizing existing routes where possible, and provisioning new ones when necessary.

Sovereign Computing

The path to network freedom begins with the advent of sovereign computing. Nodal platforms will allow any user to host their own network services, perhaps without even fully understanding that they are doing so. It will just work, because it has to, in order to be adopted. We term such usage [sovereign computing](#), because it allows users to maintain control of their identities and their data.

The nodal server will assist in the transition from centralized and unsecured communications to ones that are distributed, encrypted, and logically peer-to-peer. There is no question that this represents a major improvement from the *status quo*. Yet, the long-term evolution of the network demands a more radical approach, and the nodal platform presents the perfect opportunity for such a departure.

A communications platform incorporating publishing, messaging, status updates and telephony will be an attractive prospect to early adopters. A streamlined user interface and high reliability will drive wider adoption.

The Neighborhood Network

Long-term planning at the present juncture will pay dividends when sovereign computing becomes widespread. Including three [b/g/n radios](#) in the nodes will ensure that neighbors can find each other and establish robust and reliable routes of communication. An integrated software stack means that user communications will automatically be routed locally, whenever it is possible. The [economies of scale](#) dictate that users will pool their resources, and purchase Internet access collectively. This will drive further adoption.

While it will be possible to engage in bandwidth sharing using nodes alone, larger scale cooperatives will want to invest in a FreedomTower containing powerful radios capable of communicating with mobile devices, nodes, and other towers. Community-owned towers, in addition to serving as a logical connection point for communal outbound connectivity, will allow neighborhoods to communicate directly with adjacent neighborhoods, and in so doing extend the reach of material peer-to-peer connectivity.

Neighborhood Networks will purchase access from Tier 3 and Tier 2 network providers in a manner similar to what small and medium sized businesses do today. The price on a per-node basis could be as much as an order of magnitude below current residential levels.

Autonomous Systems

Just as the adoption of FreedomNodes will drive the adoption of FreedomTowers, the adoption of FreedomTowers will ultimately give rise to regional FreedomLinks, and just as the construction of a neighborhood tower will drive the adoption of nodes, the adoption of a link will drive the adoption of towers. These links will sit in Internet Exchanges and Colocation centers, participating in the regional radio mesh, and in the global network of networks as a peer, rather than a client.

The population served by a single link will be quite large - perhaps as many as a million individual nodes. These regional networks will still have to buy upstream connectivity from an Internet Service Provider, but they will finally be able to do so in the same way that a Tier 3 network purchases transit from a larger network.

In operational terms, these regional networks will constitute Autonomous Systems. They will be able to peer with other networks, driving down the cost of connectivity even farther. It is at this stage that the constituents of the regional mesh truly become their own Internet Service Provider.

Backbones of our Own

Still, regional Autonomous Systems will be localized, and radio frequency communications are not capable of serving as ISP-grade backbone links. FreedomLinks will initially be connected to one another via upstream fiber networks, so stopping at this point would leave our ability to communicate with one another in the hands of a few for-profit entities, whose [terms of service](#) may not be agreeable.

In order to achieve true freedom, regional networks will have to either build their own fiber lines to neighboring links, or purchase existing lines outright from established providers. As these lines are procured, existing pockets of material peer-to-peer will grow together, and larger federations of free networks will emerge. These federations will grow in size and operational disposition from Tier 3 to Tier 2, and eventually to Tier 1 networks. That is to say that when the federated networks grow large enough, they will be able to provide transit to other networks, and eventually engage in settlement-free peering on a wide scale.

To the far stretches of the federation, a user would be able to send information using infrastructure of which they themselves would be a stakeholder, a participant, an owner.

A Human Right

Our freedom alone is not enough. The construction of a global Free Network is not the end of our struggle. The end of our struggle is to ensure that every member of humanity is afforded access to such fundamentally transformational technology. Once we have built our networks, it would be wise to help others build their own.

Conclusion

At this stage, the ideas contained in this document are just that - ideas. Yet, all over the world, individuals are reducing these ideas to practice. They are itemizing the tasks that lie ahead, and they are executing those tasks as quickly as possible. There are many obstacles to success, but the stakes are too high to take no action.

We hope that you will support this cause in any way that you can. If you are a systems engineer, a programmer, a packager, or a hacker of any variety, we can use your technical assistance. Yet building the free network technology stack is only a part of our work - we face social, political, and philosophical hurdles as well. You can contribute much through activism, advocacy, and discourse.

The release of this document marks the commencement of our first capital campaign. We aim to raise \$50,000 for the purposes of specifying and prototyping the first set of FreedomNodes and FreedomTowers. This funding will be used to procure necessary equipment, and to enable developers to devote more time to this important work. More information regarding our finances is available on our website, under 'Donate.' We rely on public support to do our work, and donations to the Foundation are tax deductible. Please give whatever you can afford, be it your time, your money, or your expertise.

Join us in our struggle to build a freer network. Our very ability to communicate is at stake. If we value our freedoms, it is imperative that we act to preserve them. We are taking action to build a better network for all. This is our struggle - we welcome you.

Technical planning continues

On December 14th 2011, I received a pointer to the following from Charles Wyble.

[A look inside the FreeNetworkFoundation Network Operations Center](#)

Written on December 13, 2011 by [charleswyble](#) in [Uncategorized](#)

As co founder and technical director/CTO of the FreeNetworkFoundation, it has been my responsibility and privilege to deploy our first Network Operations Center. We have been very fortunate to find highly cost effective colocation with very responsive support. It's located in the central United States so as to be as equidistant as possible from towers as they are deployed. This will allow tower deployments to proceed without waiting on additional FreedomLinks are being deployed.

We also plan to add an additional NOC for disaster recovery purposes. We are currently evaluating a provider on the East Coast for this purpose. We will be calling for donations to cover the cost once we have completed our evaluation phase. It will probably be about \$2,000 for a year of hosting.

These two NOCs are separate from what our IndieGoGo campaign is funding (which is AS number, ARIN ip space, radio link licensing, 3 FreedomLinks being designed, built, deployed and operated for one year). The NOCs host our production network management system and FNF web/mail/dns/xmpp etc infrastructure.

So what is in our NOC?

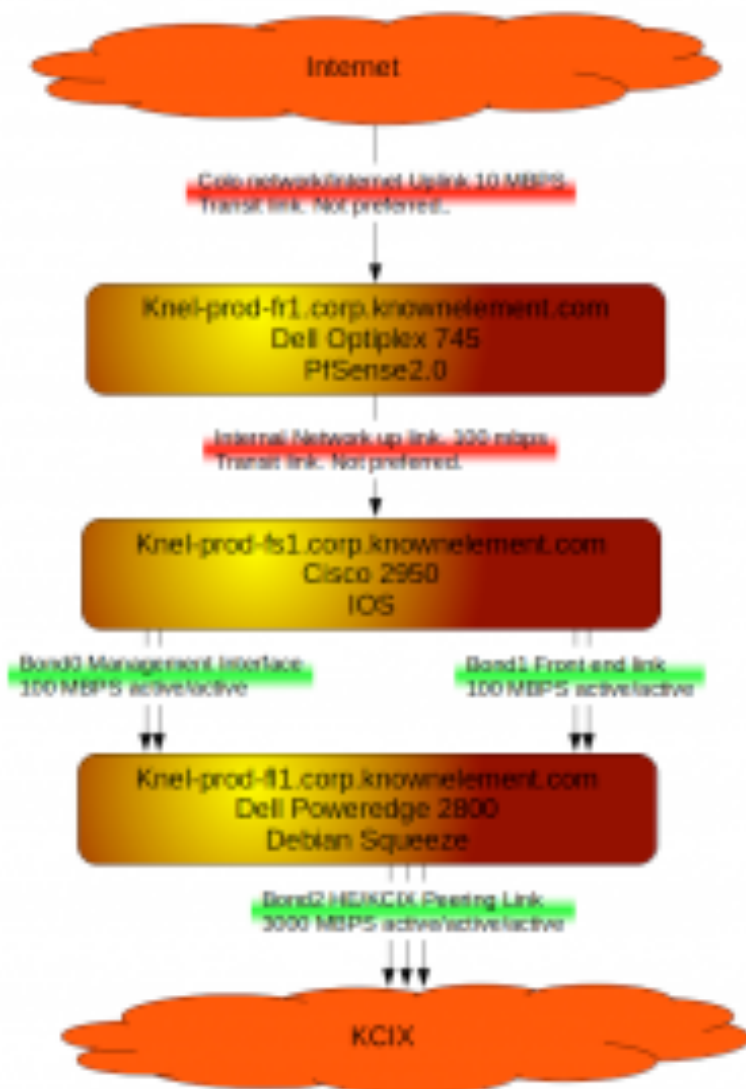
- 1 Cisco 2950 Switch. Our core switch. This is hooked up in a redundant fashion to our VM server. It has 24 ports. This will let us engage in peering with others in the data center and on the KCIX peering fabric.
- 1 Dell Optiplex 745 Our core router/firewall (FreedomLink1). This runs pfSense and is handling all aspects of our enterprise network, as well as the VPN terminus for our tower management network.
- 1 Dell Poweredge 2800 Our VM server. I'll go into more detail about what we are hosting later on in this post. This has a DRAC card with dedicated network drop so we have full out of band access to our main system. We also have an IPMI card, but it's not hooked up. It would be very nice to have the IPMI card as it would give us advanced telemetry data that we don't currently have. We need sponsors of an additional network drop for one year (this would be \$60.00). Please use the donate button if you would like to sponsor our ability to have out of band monitoring. Just put IPMI in the memo field. Once we have reached our \$60.00 goal we will have this critical function for one year. The more that is donated, the longer we can maintain this critical function.
- 1 Cyclades PDU Managed power distribution unit. Currently everything is powered through this, but it's not hooked up to the network. We need sponsors of an additional network drop for one year (this would be \$60.00). Please use the donate button if you would like to sponsor our ability to have out of band power cycling. Just put cyclades in the memo field. Once we have reached

our \$60.00 goal we will have this critical function for one year. The more that is donated, the longer we can maintain this critical function.

- 2 USB flash drives. These are providing the root partition on our VM server in a RAID1 array.
- 2 USB hard drives. The idea for these is that they would provide a RAID1 array for all of the FNF critical data. Unfortunately we lack a powered hub and as such are only able to use one of the drives. This puts FNF data at very serious risk. We need sponsors of a powered USB hub (this would be \$30.00). Please use the donate button if you would like to sponsor our ability to have our critical data protected.
- 1 USB hard drive for backup. The idea for this drive was that it would be a nightly backup drive for the RAID array. Unfortunately it is also not usable until we have a powered USB hub.

We look forward to folks donating towards our NOC capex/opex budget and getting us to a place where we can put the FreeNetwork into full production mode. Without the above critical pieces, the FreeNetwork management system and FNF corporate infrastructure will be running in a degraded mode at constant risk of failure.

Here is a diagram of the setup:



What does the FNF corporate software infrastructure consist of?

- wiki (media wiki)
- Real time shared text editing (Etherpad)
- blog (wordpress)
- Microblogging (Status.net)
- Social networking insight (Thinkup)
- Brand tracking, relevant topic tracking (Tattler)
- Bookmarks (Scuttle)
- Collaborative diagramming (Oryx-editor)
- Photo gallery (Piwigo)
- Document management (OpenDoc-Man)
- Web analytics (Piwik)
- crm (civcrm which is drupal based)
- HR system (OrangeHRM)
- Finance/accounting system (Dolibar)
- E-mail server/groupware (SOGO)
- Project management (Chiliproject)
- Scrum tool (Icescrum)
- Cpanel/WHM to host our various domains, lamp applications, mailing lists etc. It's not FLOSS (in fact it's the only

piece of our corporate or network management software infrastructure that isn't FLOSS). Unfortunately no FLOSS solution comes close. <http://www.openpanel.com/> is currently the most compelling candidate. This is something that needs to be solved for FreedomNode (end users being able to administer the compute resources without needing a lot of expensive support).

- Voice/Video communications (Freeswitch (Whistle and BlueBox from 2600hz.org)
- Text chat (Jabber)
-

What does the FreeNetwork management system consist of?

- Ticketing (OSTicket)
- Monitoring (Zabbix)
- Documentation and configuration management system (Netdot/Nocproject.org)
- Radio management (Aircontrol)
- Captive portal/security (PacketFence)
- GIS System (Udig/OpenStreetMap/Ushadi)
- Asset location tracking (OpenGTS)
- Technical Operations Dispatch system (TicketsCAD)
- Knowledge base (phpMyFAQ)
- Colo documentation (rack tables)
- DNS (PowerDNS)
- On net key servers (OpenSKS)
- Server management (Dell OpenManage)
- Configuration Management Database (Evaluating Zabbix and Onecmdb.org)
- More to come as the network is deployed

And [FNF Technical Engineering Roadmap and a look at the FNF technical organization](#)

Written on December 13, 2011 by [charleswyble](#) in [Uncategorized](#)

Editor - Note that virtually all the URLs in this entry require a log-in and password to access.

This is a long and meaty post. In the interests of transparency and soliciting feedback/participation etc.

The FNF is anticipating our first milestone (FreeNetwork1.0) to be completed over the next 18 months. This depends on staffing levels, schedule slippage etc.

The first milestone (FreeNetwork 1.0) is defined as follows:

Delivery of a

- secure (transport layer and data storage (FreedomNode)
- highly available
- varying degrees of identification (fully anonymous to fully authenticated)
- virtual (overlay/VPN links between all components of the network)

All components of the network will be

- locally funded
- locally constructed
- locally operated
- locally owned

The network will consist of three highly horizontal layers

1) backbone network comprised of FreedomLinks which facilitate connections and efficient traffic flow between regional networks of FreedomTowers

2) Sustainable (off grid) FreedomTowers linking into regional area networks which are comprised of neighborhood area networks of

3) Sustainable (off grid) FreedomNodes which will serve individual homes and businesses.

The network will mesh (in both a logical and material peer to peer fashion) horizontally at every level (node to node, tower to tower, link to link). It will also mesh/route vertically between the layers of the network.

Sounds cool right?

So [how do we get there?](#)

1. Corporate structure

Things related to FNF as a legal entity. Board of directors, board of advisers etc.

Targeting completion of this by 1/31/2012

2. FreedomLab

I recently completed the FreedomLab and hope to open it for mass participation soon.

Targeting completion of this by 1/31/2012

3. Data center delivered to full production mode.

This is the highest priority task. It's a lot of work to build an entire server farm to support an enterprise and production network.

We are getting closer each and every day. Outstanding tasks are captured. We expect to close several of them out when Isaac visits the DC. Our CIO is heading this up. I'm working to transition everything over to him (already produced and delivered comprehensive data center documentation).

Targeting completion of this by 1/31/2012

4. Website redesign

Redesign the FNF website to make it easier for folks to learn about our activities, tell their friends, and contribute time and resources. Focus will be primarily on the main page, which will be completely overhauled. Some content is out of date, and some needs to be moved and recategorized.

Targeting completion of this by 1/31/2012**5. Ipv6**

All FNF services (internal and external) will be available over Ipv6. THIS IS NON NEGOTIABLE. We must always strive to retire Ipv4 whenever, wherever, however we can. I put this after the above tasks but still very high on the priority list. We need to get the DC 100% wrapped and an auth/enrollment system into play to stay sane.

Targeting completion of this by 2/29/2012**6. Centralized authentication via LDAP/RADIUS/Kerberos and one time passwords.**

This is critical. We have a wide array of applications, gear, system instances deployed which are all using a local authentication store. We plan to use SOGO as our LDAP store. We will use MIT Kerberos for system logins and FreeRADIUS for it's rich functionality around capabilities, profiles, restrictions etc. We are evaluating one time password systems at the moment. I am heading this project up as CTO. It will be handed over to our CIO once I've completed initial work and documentation so he can fully operationalize it.

Targeting completion of this by 2/29/2012**7. User Enrollment**

This is an extension of centralized auth. Need a way to provision users and plug them into appropriate access levels. FNF needs a way to enroll administrators into the network (in our WAN/LAN delivery groups). This will most likely be done via our HR system (using OrangeHRM) after the various contracts have been executed and stored. (Gotta have legal protection). No tasks yet. Haven't done any engineering work around this at all.

Targeting completion of this by 2/29/2012**8. Freeswitch**

Our Los Angeles based VOIP guru is heading this effort up. We are using Whistle and BlueBox from <http://www.2600hz.org/>

Him/I made substantial progress on this last night. No tasks captured yet. As we have more demands and needs for our voice/video comms, tasks will get captured and a roadmap developed.

Targeting completion of this by 2/29/2012**9. Operations support system**

As mentioned in my [previous blog post](#) we have various pieces of our network management system in place. It will be expanded as the network is deployed. This is necessary to take the network from research and development mode into full production readiness.

Targeting completion of this by 4/15/2012**10. FreedomTower**

Documentation and complete packaging (hardware/software) for “release to manufacturing”. More to come later. I’ve got a bunch of pictures and notes which will be turned into a comprehensive set of tower build instructions very soon.

Targeting completion of this by 4/15/2012

11. [FreedomNode](#)

The desired user experience and rough design sketches for the FreedomNode are available in a separate post, [here](#). In order to bring the FreedomNode into production, it will be necessary to leverage the work of Project Byzantium, and to tap the pool of design and engineering talent that has congregated around FreedomBox.

Targeting completion of this by 5/15/2012

12. Legal Framework (for operators and usage)

Just as in the creation of free software, building tools and technologies is not enough. We need a framework of legal agreements for node, tower, and link operators in order to build transparent and communally accepted policies for dealing with network abuse, so that we can keep the Free Network free. Think of it as a GPL for networks – a covenant that enshrines the five freedoms of the network in law.

Targeting completion of this by 5/15/2012

On the FreedomNode

Written on December 31, 2011 by [imw](#) in [Uncategorized](#)
Hello All,

After a very successful strategy and year-end review summit in Austin, we wanted to give you all a little insight into what we’re cooking up with regard to the FreedomNode. If you’re not already familiar, the FreedomNode is the foundation of the Free Network technology stack – a device that will allow neighbors to communicate with one another directly, without need for a paid service provider. We think of it as the ultimate sharing machine, allowing you to privately store, selectively distribute and globally publish a wide range of materials, using a variety of connectivity options.

Lets start with the user experience, and from there we can seek to understand the technical aspects. For the time being, we’ll talk only about the experience of the node as a standalone device, and exclude the (likely) possibility that some users will boot the software on existing machines. The node presents a uniform interface across client devices using HTTP(S) – a collection of stylesheets allow the interface to adapt successfully to a wide array of different screen resolutions and input methods.

In simple terms, you interact with your node by opening a browser – any browser – and navigating to your node’s address. That address can be a global name such as a user-owned DNS entry, or a third-party subdomain such as username.fnf.tel, or, from the same local network, a local address, such as ‘[https://mynode](#)’. Alternatively, the node can be accessed from its unique IPv6 address.

Navigating to the address of a node prompts the user to authenticate. This is done using the F-Pass system. F-Pass is the key to trust and addressing on the Free Network – tying together x.509, PGP, IPv6, and secure, one time passwords.

Once authenticated, the user is presented with a main menu that provides access to all of the essential functions of the node. Icons exist for Blogging, Microblogging, Planning (like plans.txt on Unix or GrinnellPlans), Mail, and an A/V Center (photos, music, video, and files). An additional icon leads to a list of contacts, with a final icon leading to system settings.

Users can be organized into aspects, with a ‘Neighbor’ aspect generated automatically for those with whom you can communicate without need of an Internet Service Provider. From the contacts page, a user can access the blog, microblog, plan, or shared media of another user. Users have precise control over who can access each piece of media on their node. Sharing is encrypted by default, anonymized when desired, and opportunistically peer-to-peer – that means that we all cooperate to move each others’ messages, when it is possible, rather than paying a professional bit-mover

Now that we’ve established what the node is designed to accomplish, let’s talk about its actual design. At the core of the FreedomNode is a small-form computer, designed to run continuously for years on end. The computer’s onboard capabilities can be expanded with USB mass storage, and miniPCI radio modules.

On bare metal, the node will run genode, a novel GPL operating system architecture that allows for true fault isolation and tolerance. On top of that, a lightweight debian install will be used to ensure long-term package support and stability. The user-facing services run on top of Debian, powered by a collection of existing open-source daemons and tools. These services benefit from the tight integration of a unified interface and a unified authentication and identity management system.

Add to that the ability to communicate without using the telco’s wires, and you’ve got a truly disruptive piece of tech. The Byzantium Project has built a solid foundation for mesh communications – their routing scheme (based on the babel protocol) will be integrated with nodal services so that local traffic never has to leave the neighborhood network. There is much to do, but we aim to have the FreedomNode ready to release in 18 months or less – join us now, and help us build the greatest tool in the liberation technology toolkit.

Why Wireless Mesh Networks Will Save Us From Censorship

Written on January 9, 2012 by [imw](#) in [Uncategorized](#)

or: ‘Why Shaddih’s article is a sobering, but misguided warning about a plan that’s been misunderstood.’

I

In November of the year just past, there was a sudden explosion of interest in the prospect of building a global-scale communications network that is owned and operated by participants in the network. Much confusion ensued, and the idea remains mostly opaque or misunderstood. On the 26th of November, a graduate student by the name of Shaddih Hasan posted a piece called ‘Why wireless mesh networks won’t work to save us from censorship.’ The piece listed five reasons why “unplanned wireless mesh networks never work at scale” – and used that relatively well-supported claim to warrant the assertion that building peer-to-peer communications infrastructure is a waste of effort and time.

My name is Isaac Wilder, and I’m one of the Directors of the Free Network Foundation. Along with my partner Charles Wyble, and a global network of volunteers and contributors, I work on systems and network architectures for what we call *free networks*. Our technologies will enable the construction of networks belonging to no one and everyone at the same time. I’d like to take some time now to respond to Hasan’s claims, and explain how mesh networks *can* and *must* be used, not only to save us from censorship, but to reclaim the notions of community and trust which current architectures put in grave peril.

If you haven’t read Hasan’s piece, you may want to do so now. It is available on his [blog](#). It’s well argued, and points out some of the many challenges in the implementation of unplanned, large-scale, wireless mesh networks. I do not mean by my dissent to suggest that these challenges are of no importance – they are, rather, key considerations in the design of free networks. I do mean to suggest, however, that these challenges are not insurmountable. What Hasan has shown us is that [RF](#) signal is a relatively unfriendly networking medium, which is *not* to say that radio waves cannot or should not be used to build a new type of network.

It seems to me that Hasan has misunderstood the intent of this new wave of free network activism. I could not possibly speak for a diverse and heterogeneous community of activists, but I will speak on behalf of the FNF, which endeavors to fight censorship using mesh technologies. While Hasan’s technical critiques are generally well-founded, they are also overstated. He attacks a falsely simplified understanding of what a global free network would look like. Furthermore, and finally, the piece culminates in a string of fallacious philosophical and political assertions for which he has presented no relevant evidence.

Now, let’s take the technological claims one at a time. Then we’ll work on understanding what is actually being proposed, and how Hasan’s points don’t really speak to it, before examining the politics of censorship.

II

Reason 1: Management is hard and expensive.

The first reason, we’re told, that one shouldn’t use mesh networks to build cooperative, autonomous systems is that “you’re going to spend all your time just maintaining basic connectivity.” Hasan paints a picture of mesh networks plagued by “transient connectivity problems resulting from RF weirdness in urban areas.” He points out the necessity of traffic shaping due to bandwidth constraints, and offers up the example of a Tibetan mesh which made a move toward a point-to-point architecture as they tried to scale.

Response 1:

While it's true that management of mesh networks takes effort, it is not true that such management is impossible for a group of volunteers, let alone for a team of professionals. The claim that the Tibetan mesh highlighted in his article was the largest in the world is unsubstantiated. Hasan even mentions a couple of larger, volunteer-operated, city-scale mesh networks (Freifunk and Athens Wireless), but fails to reconcile their ongoing success with the above statements. Mobile Ad-Hoc networks do entail a certain amount of overhead, but they also have definite advantages. Ultimately, such technology is useful when applied in the appropriate situation, and cumbersome when used inappropriately.

Reason 2: Omni-directional antennas suck.

In reason two, we learn that “Omnidirectional antennas are very inefficient, since they throw your energy (i.e., signal) all about, when in reality you just want your signal to reach the handful of nodes nearby.” We're told that if “Even if all 15,000 people on the Darknet subreddit could install and maintain 10 devices, they wouldn't cover all of Wichita, KS, not to mention the miles of farmland between it and the next town.”

Response 2:

Again, there's a kernel of truth here – omni-directional antennae have certain inefficiencies. They also have practical applications that outweigh those drawbacks. To say that omni-directional antennas suck is a pretty obvious overstatement. To say that they need to be used appropriately would be more reasonable.

And then, of course, there's the assertion that 150,000 network nodes would be insufficient to cover Wichita, KS. This claim is baseless. By any reasonable estimation, that number of nodes would be an order of magnitude greater than the number needed to make coverage available throughout a mid-size city. This is true even if one considers a node to be just a Linksys [WRT54G](#). For reference, [Athens Wireless Metropolitan Network](#) reaches an area 110km tall and 85km wide with fewer than 4,000 nodes – [Wichita](#) is smaller than 20 kilometers square. Start considering [licensed](#), [point-to-point](#) links, industry grade gear from Ubiquiti and Mikrotik, or wired backhaul and suddenly the 150k node number's not one order of magnitude off the mark, but two. Fermi would be [pissed](#).

Reason 3: Your RF tricks won't help you here

The third reason why we're supposedly doomed is that it can be hard to get radios to communicate with one another, even with high-gain, high-power, or directional equipment.

As regards omni-directional antennae, we are cautioned that higher gain means an elongated beam – further reach, but a smaller margin of error in terms of node elevation. Think of it as smooshing a donut – the diameter goes up, but the height goes down: “the higher gain you go the thinner the disc gets.”

As regards directional antennae, we're led to believe that they aren't really useful in the creation of mesh networks. They focus the beam, and so they have to be aimed correctly before they can communicate with a neighboring node, “eliminating a key property of the mesh network”.

Finally, as for power amplifiers, we are told that “They only boost transmit power; the real limitation is receive sensitivity.” Furthermore, we are told, they are power-hungry, and expensive, and restricted in their operation by legal limits.

Response 3:

The main thrust of this response is the same as my last one – yes, there are some truths in what Hasan says, but those truths are exaggerated, while salient facts are willfully ignored. High-gain, directional, and amplified transmissions are not cure-alls, but they are certainly useful, and *do* make it possible to build cost-effective, scalable community wireless networks.

High-gain omni antennas are terrifically useful for those radios serving as access points, allowing you to cover a large field or floor with a single point of presence. With a small amount of coordination and planning, it is possible to use such antennae to great effect, covering a wide area with relatively few networks nodes.

Directional antennae used at microwave, millimeter wave, and optical frequencies are profoundly powerful pieces of technology, allowing [gigabit throughputs](#) and very long range hops ([100+ km](#)). Hasan doesn't even mention the notion of using directional, point-to-point links to connect disparate pockets of a community network – he disparages the technology for not doing something that it's not designed to do, while completely ignoring its actual uses. It's true that point-to-point links are generally dependent on line of sight and are susceptible to [rain fade](#), but it seems odd, given his organization's [experience](#) with the technology, that he did not mention its potential.

Finally, there's power amplification. We are told it's of no use, because of the constraints of receive sensitivity. In certain situations, this is true – when trying to interact with client devices, for example, or when network hardware is mixed. In other situations, however, increases in transmission power have a considerable effect on network throughput. The problem of receive sensitivity is only relevant if the increase in transmission power is unilateral – if, on the other hand, all neighboring nodes increase their power as well, they can be placed farther afield. It is true that there are legal limits on transmission power without a license (1 Watt in the ISM band), but it is also possible to obtain licenses for higher transmission power, in less polluted bands.

Reason 4: Single-radio equipment doesn't work; multi-radio equipment is very expensive.

Here, we're given a rundown of some of the basic technical hurdles that constrain mobile ad-hoc networks. The first hurdle with which we're presented is the half-duplex problem, which limits the usefulness of some consumer wireless gear in the construction of mesh. The gist is this – nodes with only a single radio transceiver can either transmit or receive at any given moment, but cannot do both.

There is also the problem of interference between two nearby nodes that transmit at the same moment, on the same channel. While the half-duplex problem can be solved by using network nodes with multiple radios, the interference problem is a bit stickier. Hasan points out that radio transmission scheduling and spectrum allocation are [NP-hard](#) problems – that is, they're really freaking hard.

Response 4:

If the half-duplex problem is the “the biggest technical reason mesh networks don't work for Internet access,” then we're in good shape. It has a very simple solution – use full-duplex, multi-radio nodes. Hasan says that “a network of multi-radio devices quickly becomes very expensive” but doesn't give any facts or figures to back up this critical assertion. In fact, multi-radio hardware has become more affordable in recent years, and becomes more so all the time. High quality [Atheros](#)-based radio modules are now available for under [\\$100](#). Hasan seems to forget that this is high tech, and that innovation moves

at a breathtaking pace. What was unaffordable just five years ago is now within reach. Given a few more years, it will be commonplace.

Now, that's not to say that a mesh made of multi-radio nodes doesn't have some wicked transmission scheduling and frequency allocation problems. Time division multiplexing is a complicated process, to say the least. Still, Hasan makes it seem as though there's no workable solution to the problem. This is not the case. The theoretical complexity of transmission scheduling and spectrum allocation have less to do with working, practical solutions to these problems than you might think. Multi-radio mesh networks can not scale infinitely, but they [can](#) and [do](#) scale enough to be useful in the creation of free networks.

Reason 5: Unplanned mesh networks break routing.

The problem of routing in mesh networks is a complicated one – “There are many protocols for mesh routing, like AODV, OLSR, and BATMAN. Fundamentally they require individual nodes to communicate with each other, which not only takes up further network resources, but also means that achieving a consistent routing state (i.e., one in which packets won't get routed into black holes or loops) is extremely difficult for all the reasons distributed systems are hard to build.”

Nodes move around, in and out of range of one another, and routes through the network need to be recalculated and shared when there are changes in the state of connectivity. This introduces the considerable problem of routing overhead – network resources that have to be used just to maintain the network. What's more, “The unplanned nature of a grassroots mesh network exacerbates this problem, since poor RF-level connectivity means the connectivity state between nodes changes frequently, leading to more routing overhead in the network. It's a bad cycle.”

Response 5:

Hasan is right about one thing – nodes in a mesh network do need to communicate with one another to share routing information. Beyond that, his analysis of the problem is underdeveloped and out of date. He mentions AODV, OLSR, and BATMAN, but fails to mention Babel, a [higher-performing](#) protocol whose daemon recently made it into the mainline linux kernel. He mentions the problem of routing loops, which plagued early implementations of mobile ad-hoc routing systems, but fails to mention that current algorithms are able to virtually [guarantee](#) the absence of loops. Mesh routing is complicated, but certainly not impossible – the state of the art is already sufficient for production environments, and is improving all the time.

The argument that mobile ad-hoc networks do not scale because of routing overhead is old and stale. This is the single most commonly heard ‘evidence’ against the idea that mesh networking has a significant role to play in the future of human communication. The problem with this line of argument is not that it's wrong, it's that it fundamentally misunderstands what we are trying to accomplish. We are not trying to build a horizontal global mesh. We are trying to build a global free network, consisting of interconnected pockets of mesh. We don't need mesh to scale beyond a few thousand nodes, which it can already easily do.

III

Having countered Hasan's arguments against the feasibility of a free network, I'll now take the opportunity to briefly explain what a workable design for such a network might look like. This is a very brief rundown on what we call *fractal mesh* – for more info, see our [article](#) on the ends and means of our movement.

The design has three basic building blocks. The FreedomNode is a small-form home server with three radios. The FreedomTower is a neighborhood network manager, [caching-proxy](#) machine, and traffic aggregator with omni gear for communication with nodes, and directional gear for communicating with other towers. The FreedomLink is a [BGP](#)-speaking [rackable](#) router connected to directional radio gear (on the roof) so that it can talk to towers. All of these machines would have Ethernet and/or optical connections in addition to their wireless interfaces.

FreedomNodes would mesh together, using both wired and wireless media, to form neighborhood networks, roughly the size of a census tract. Because the nodes are servers (think of a diaspora pod), rather than just clients, it's not just routes that are distributed, but user data itself. This enables communications which are peer-to-peer not just in the abstract or logical sense, but in the sense of material reality as well.

Each neighborhood network would have one or two FreedomTowers, designed to interconnect neighborhood networks. Just as nodes form a neighborhood area network, towers would form a regional area network. Towers would allow communities to buy backhaul circuits cooperatively from the start. Eventually, with increasing density in the free network, towers would be able to establish a connection to a regional FreedomLink. A full build-out of national free networks might entail 75,000-100,000 such towers.

Finally, within a regional network there would be one or two FreedomLinks, capable of peering with exterior networks, free or otherwise. Neighborhood networks would band together to form cooperative Autonomous Systems and run their own link. A national free network would comprise of about 100 links. Neighboring regional cooperatives would band together to build, buy, or lease lightpaths between links.

So, you see, the idea that “unplanned wireless mesh networks never work at scale” does not actually speak to the feasibility of our undertaking. Building a free network is not reducible to the concept of building a global mesh network, though well-designed mesh networks will play a part. There are many challenges ahead, both technical and political in nature – but with dedication, our goal can be achieved. It must be achieved – for our natural liberties cannot otherwise be won.

IV

The final issue that needs to be addressed is the suggestion that folks who are interested in horizontal, distributed, and free networks would better spend their time politicking. The crux of Hasan's argument against our work “is that it appeals to the problem-solving oriented nature of many of us who are interested in Internet free speech, thereby distracting us from pursuing other more effective means of protest against censorship.” I see a few problems with this position.

First, it makes the fallacious assumption that those who spend their time engineering free network solutions are not, and can not be, engaged socially or politically. This is not so. Hacking on mesh tech no more precludes political activism than hacking on Tor or GNU. I fully agree with Hasan that there are

crucial political aspects to the struggle for digital self-determination. Yet political engagement alone is not enough. We must build, demonstrate, and demand our right to operate systems that allow us to connect directly to our neighbors without having to go through a corporate middleman.

The second problem with Hasan's thesis is that it woefully overestimates the health of the western polity. The "more effective" remedies offered by Hasan are political engagement, awareness/education, and community action. Unless they are coupled with the creation of alternative infrastructure, his suggestions constitute no remedy at all. We must build precisely because our system of government is fatally corrupt. Congress passes odious and unpopular legislation at every turn; they are beholden to those that finance their campaigns. We can tell our friends and family about SOPA, DMCA, or PROTECT IP until we are blue in the face, but it is clear that our so-called 'public servants' will continue to pass laws that benefit special interests, rather than the populace. Of course, Hasan is absolutely correct in suggesting that we "form real-world communities, and work with them to fight for Internet free speech" – that is exactly what we are doing. To suggest that we should form communities when we are already doing so seems confused.

Hasan wisely warns us that "Censorship is broader than just Internet free speech: it is a social problem that has existed long before the Internet ever did and will continue even if the Internet dies." It is true that censorship has been a problem since before the birth of the Internet. It is also true that we need to maintain social and political pressure on our public servants and corporations. What is false is the assertion that building free networks is somehow opposed to the maintenance of such pressure, or that such pressure is sufficient in and of itself. Sadly, Hasan closes his article with a dangerous falsity, saying that "The only way to really address root causes is to engage with the problem at the social and political level." What is false here is the notion that we cannot combat censorship by technological advance. Buckminster Fuller said it best: "You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete." Human history is full of breakthroughs that have increased our ability to communicate freely. I hope that this response has helped elucidate how the construction of robust, reliable and useful free networks is not only within reach, but essential. The dismissal of such an endeavor as a waste of time indicates that our aims have been misunderstood. So, rather than effectively concede a struggle which has barely begun, I invite Mr. Hasan to join us as we build networks for the future – ones that are owned and operated by the people. Our development roadmap is [here](#). There is very much to be done.

0 Comments - [Leave a comment!](#)