Welcome to the network!

PittMesh, is a Pittsburgh-based community wireless network (CWN), created by Meta Mesh Wireless Communities, LLC. It is a unique public WiFi solution that can bring positive attention to your neighborhood by providing free and open connectivity to the Internet, to community hosted resources, and to the City of Pittsburgh.

Many public WiFi networks are expensive to implement and sold by for-profit companies that may not have a community's connectivity as their primary motivation. At Meta Mesh, we approach public WiFi with the view that open connectivity in a neighborhood is a communal resource and the people who benefit from this resource are motivated to keep it functional and current with their community's needs. Meta Mesh's goal is to teach community members how to install, maintain, and expand their PittMesh network, while teaching them resume-building skills that can further their own careers.

In this packet, you will find answers to your questions and maybe even some questions you didn't realize you need to ask. This document is the result of four years of PittMesh router implementation throughout the Pittsburgh area. If you have further questions not covered in this packet, please contact info@metamesh.org.

1. An Overview of the Project

What is PittMesh?

PittMesh is a network of electronic devices in the Pittsburgh area. Now it's about to get briefly technical so hang on tight.

A "mesh" network doesn't have a universally agreed-upon definition, but is generally described as a network that is fault-tolerant, self-describing, and self-healing. In layman's terms, a "normal" network is hierarchical, and relies on central repositories of records to find out how to route traffic to a particular device on the network. It's just like calling the operator and asking to speak with someone whose number you don't know. The operator has a record of all phone numbers and will connect you to the person. A "mesh" network is more like knowing who you want to speak with on the phone but not knowing his number, calling your friend who you know is friends with that person, and asking your friend to relay a message for you.

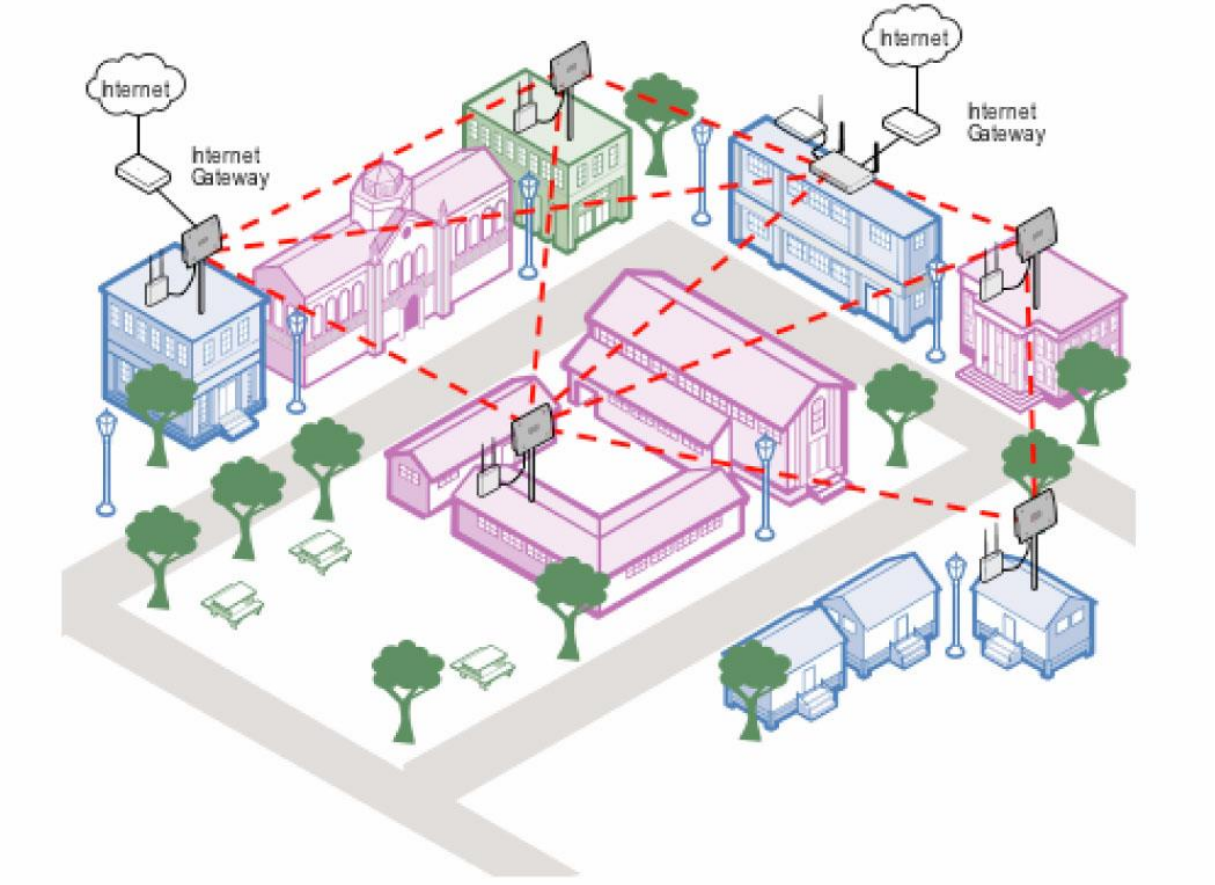
Why would I want a mesh network in my neighborhood?

Most people don't care how the Internet gets to their phone, laptop, or computer—they simply care that it DOES! When you have a single resource on a network like a website, a printer, or a chat server, we in the industry describe this as being "centralized." Centralizing anything makes it prone to blackouts. If you only have one bathroom in your house and the toilet breaks… you're suffering from a weakness in centralized plumbing.

Centralization is easier to set up for administrators and easier to implement. Having a single Internet connection is centralizing your Internet access. Most people only have one Internet connection in their house or

business, usually through Comcast or Verizon. If Comcast's network goes down, Comcast customers won't have Internet access, but Verizon's customers will. If you build a network that has multiple connections to the Internet, has multiple vendors supplying that Internet access, and you have multiple ways for someone on the West side of town to relay traffic to those gateways that may be on the East side of town, you have ensured that your network is "decentralized" and is thus less prone to interruptions.

Decentralization requires some unique networking programming compared to "traditional" networking. Meta Mesh has worked to provide this programming in the form of a shared "routing protocol" that runs on all PittMesh routers. This protocol is a set of instructions on all devices in PittMesh that ensures the routers take advantage of this decentralization. This also ensures that when a connection to the Internet dies, say a router gets unplugged or a link goes down, the routers can figure out, on the fly, how to reconnect to each other. Take a moment to look at this image below to help visualize how a mesh network works. You can think of the network as a series of "gateways" or connections to the Internet, and "repeaters" which act as relays back to the gateways.



1: From Walkabout.eu

Put your finger over any of the WiFi routers and see if you can find a new router to the Internet from any other WiFi router. You can! And that's because mesh networking decentralizes connectivity, allowing each device to act as a peer and a relay for all other devices that are connected by the red line.

PittMesh is more than just Internet access, though. PittMesh behaves as a network unto itself. Resources that are on PittMesh are reachable as long as there are links back to that resource. Have you ever been in an office where several people share a big printer/copier/fax machine? If the Internet goes out can you still print to that device? Of course you can! Because all the computers on that office's network are still connected to that machine on the same network.

This can become a useful feature in a neighborhood. You can host local websites, chat servers, 3d printers, devices, sensors, etc., and you can still send and receive data even if, say, a storm comes through and knocks out the neighborhood's Internet connections altogether. This would be important for disaster preparedness and disaster-relief communications. In fact, during Hurricane Sandy, FEMA utilized a mesh network in Brooklyn to maintain connectivity in the days after the storm when residents lacked power (http://techpresident.com/news/23127/red-hook-mesh-network-connects-sandy-survivors-still-without-power).

Meta Mesh has already developed technology that utilizes this feature of PittMesh. We call it the Community Hub (or C-Hub) and it is used as a decentralized way for civic and social groups, law enforcement, non-profits, and some for-profit businesses to get the word out of important local events and information.

2: A mock-up of an early version of Community Hub

There are many uses for a decentralized network. Here are a few main reasons to use a decentralized mesh network in your neighborhood:

a) Decentralizing gateways allows for no-cost-to-the-user Internet access, keeping network upkeep costs minimal.
b) Decentralization allows for organic growth. Anyone with a properly configured PittMesh device can add a device either as a repeater or a gateway and can expand the network without any central authority's permission—including Meta Mesh.
c) Decentralized networking allows for easy, plug-and-play access to resources on the mesh network. Want to host a chat server? Simply connect your laptop, phone, tablet, or desktop to a PittMesh device wirelessly and tell your friends your IP address. No central authority or router-host needs to program anything. It just works.
d) Decentralizing a network's infrastructure means that the devices can be inexpensive and individualized. You can put up a router with a screw gun in minutes and, if purchased individually, a PittMesh router can cost under $100. There is no need to build a data center in your neighborhood to act as a central Internet Service Provider.

Let's get into some details about a PittMesh network and begin to answer some of the questions you may have about this public WiFi solution.

2) What to Expect When You're Expecting a PittMesh Network Segment

a) PittMesh Hardware

Sometimes people think that PittMesh is a brand of router that Meta Mesh Wireless Communities manufactures. This is inaccurate. "PittMesh" only refers to the name of the network for which Meta Mesh spearheads development. There are actually a myriad of devices capable of routing traffic on the PittMesh CWN.

We have equipment from as small as the Raspberry Pi to as large as an 8-core HP Proliant server running the core routing protocol called OLSR that makes mesh networking work. We started this network with the intention of making it as decentralized as possible—not just in the networking sense of the word but in other ways too.

We use an open-source routing protocol called Optimized Link-State Routing (OLSR) to share routing data among all devices on the network. We do not mandate the use of proprietary or vendor-specific hardware to build PittMesh, although in some cases it is the best option. Our network is not intended to be a large-scale implementation of a particular line of devices. By decentralizing what devices get to be on the network, we can help ensure that the life of PittMesh will last through a manufacturer's discontinuation of a product line.

Currently, we use OpenWRT, the de facto open-source firmware, on a brand of mini router from GL-iNet, ~~a small Chinese manufacturer~~. Meta Mesh does not manufacture its own hardware but we aspire to building our own devices within the next few years.

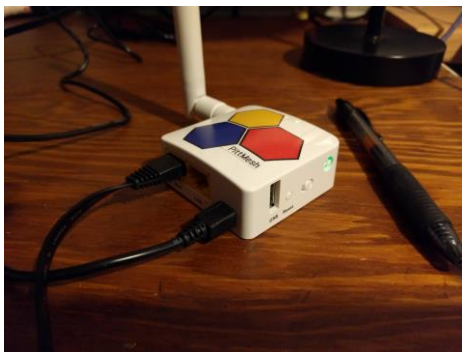
If your routing device can run OLSR, it can be a part of the PittMesh network. There are no special requirements for "client" devices such as phones or laptops to use the network. If your client device uses WiFi, it will almost certainly be able to connect to the PittMesh network.

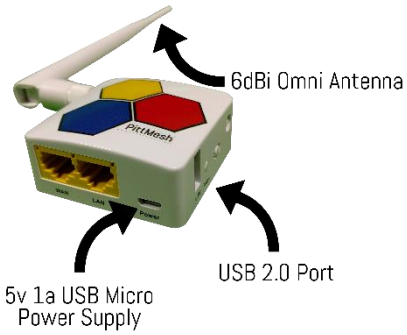
With that in mind, we want to show you exactly what you can expect from Meta Mesh hardware-wise should you choose to implement PittMesh in your neighborhood.

Currently we have two devices that can be configured and deployed in a variety of ways; the A150 Indoor Router and the AP150 Outdoor Router.

i. Specifications:

a. PittMesh A150 Indoor Router



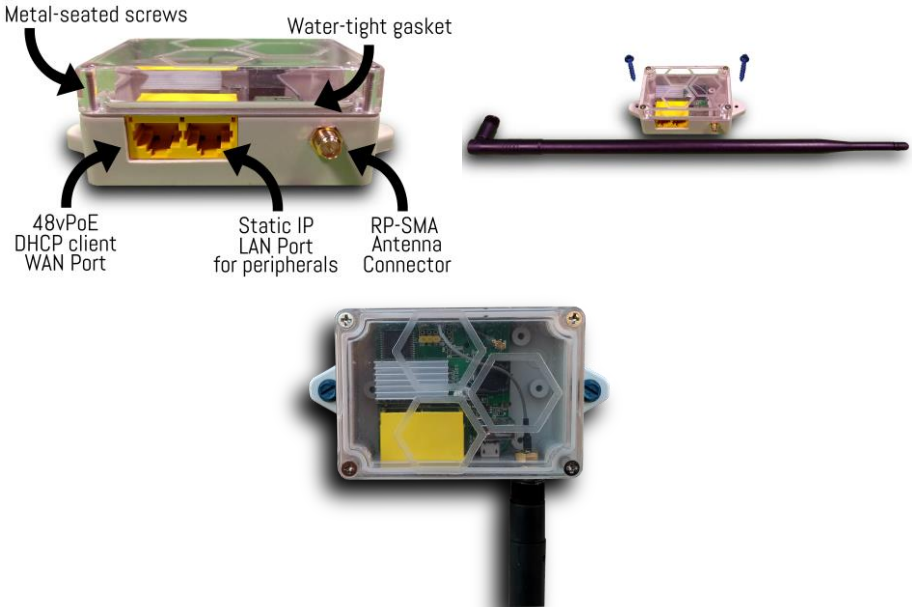


Using GL-iNet's board and case, we've configured the A150 to mesh both wirelessly over its 2.4GHz 802.11n interface as well as it's fast Ethernet WAN port. Simply plug in the A150 to your home router and you will begin broadcasting an open WiFi signal that guests and the public can use. Meshing occurs automatically over both interfaces; your router simply needs to be in range of another mesh-enabled router for pairing to occur.

The A150 is most useful for apartment-dwellers who may not be able to attach a device to their exterior wall but who wish to participate in their community's wireless mesh network. The A150 is small enough that it can sit comfortably on a window sill and still provide coverage to the street.
Powered by a Micro USB power cable, the A150 will provide mesh and Internet access throughout your house or business with excellent throughput and reliability.

Technical	
Ethernet Ports	2x Fast Ethernet (100M) Ethernet Ports
Operating Frequency	2.4 GHz b/g/n
Operating System	OpenWRT 14.07 Barrier Breaker
Power	5v @ 1A
USB	1x USB 2.0 Port (Inside Case)
Case	1x Indoor Smooth White Plastic Case
Memory	
Flash Memory	16 MB
RAM	64 MB
Processor	
Chipset	Atheros AR9331 SoC

b. PittMesh AP150 Outdoor Router



After 4 years of installing CWNs in Pittsburgh, Meta Mesh has designed the AP150 based on real-world experience; it is compact, pre-configured, and scalable, Our router uses GL-iNet's tiny mainboard enclosed in an easy-to-install watertight case that ensures snow and rain will not affect the electronics of this outdoor-rated router.

Using the maximum 1 watt transmit power allowed by the FCC, the AP150 allows for numerous configurations with its RP-SMA antenna connector. The included 9 dBi antenna can be removed and replaced with another design such as a semi-directional antenna or a long-distance point-to-point parabolic dish or Yagi antenna.

No one likes running cables. So we combined the data and power cables typically used to run a router and combined them. And for a small additional fee we'll include a Cat5e STP outdoor-rated Ethernet cable for your installation. Simply drill a hole, run the pre-crimped cable through, and caulk it back up.

The PoE injector comes with the standard 48 volt for the 802.3af specification. You won't need to purchase any proprietary connectors or injectors to power the AP150!

The AP150 includes a secondary Ethernet port for use with a sensor network, security camera, or for doing maintenance of the router. Included (but not pictured) is an RJ45 jack plug to keep dirt and moisture out of the spare LAN connector.

While it is difficult to predict how far WiFi will be usable in a particular environment, generally, these routers have a maximum range of about one city block or about 300 feet under ideal conditions. If you or a neighbor installs another A150 or AP150 in that area with clear line of sight between the devices, you should be able to mesh wirelessly between them and begin building your own mesh network!

Finally, the AP150 comes with built-in security. Firewall rules protect your home network's equipment from being accessed by users on the mesh network. While any user connected to the mesh WiFi SSID, will be visible to the rest of the mesh, your home network will not be. Any requests to access your home network's computers will be immediately dropped—so rest assured!

Technical	
Ethernet Ports	2x Fast Ethernet (100M) Ethernet Ports
Operating Frequency	2.4 GHz b/g/n
Operating System	OpenWRT 14.07 Barrier Breaker
Power	5v @ 1A PoE (Requires 48V PoE Injector)
USB	1x USB 2.0 Port (Inside Case)
Antenna	1x 9 dBi Omni Directional Antenna
Case	1x Outdoor Rugged PittMesh Case
Memory	
Flash Memory	16 MB
RAM	64 MB
Processor	
Chipset	Atheros AR9331 SoC

ii. Expected Performance

Both the A150 and AP150 routers use the exact same board. The only difference is the case they are placed in and the method of powering the device. They both have external antennas which can be changed to suit their surroundings.

In the world of WiFi it is sometimes difficult to answer the question "how far away can I be and still use this device because so much of this connection strength is determined by what the WiFi radio waves are passing through and bouncing off of and how many other WiFi devices on the same channel located in the area.
With that said, and with the standard 9 dBi omnidirectional antenna attached, we expect solid connections up to 200 feet away with significant signal degradation after that.

Below is a comparison of two real-world PittMesh setups that show how installation location and distance impact overall throughput.

3: ~200 feet between the United Steelworkers Union and Braddock Farms

In the summer of 2016 Meta Mesh installed a device on the side of the United Steelworkers building in Braddock, a town a few miles outside of Pittsburgh. We installed a second router in the Braddock Community Garden almost exactly 200 feet away. There was nothing but flat ground between the two devices, which were both about 10 feet off of the ground. There were other WiFi networks visible but they were very weak and mainly on other channels. We were able to consistently reach speeds of 20mbps with this link.

4: ~290 feet between the Hill FCU and the McDaniel Building in the Hill District

In the Fall of 2016, Meta Mesh installed 2 devices in the Hill District. Using only omnidirectional antennas, we installed two devices at the Hill District Federal Credit Union and outside an apartment on the McDaniel building. We made an initial and incorrect measurement of 200 feet between the two buildings when it was actually closer to 300 feet.

We were able to make a connection between the two buildings and have Internet access, but speeds were limited to .5mbps with frequent timeouts for the websites we tried to reach. We also had numerous other WiFi networks in the area to contend with and a very busy street where frequent transit buses partially occluded the line of site between the two routers. We were eventually able to rectify this situation by changing antennas used on each of the routers from omnidirectional to semi-directional.

The devices Meta Mesh typically uses are small, low power, single radio devices on the 2.4GHz band. We chose these devices because of their cost and discreteness. Originally, we used 4-foot long AMO2G10 and AMO5G13 antennas attached to a Rocket M2 and an M5 from Ubiquiti that required a special wall mount. While these devices had significant advantages to speed and usable distance, the materials alone cost $400 before installation fees. We received feedback that these WiFi units “looked like toilets” mounted to the side of the buildings in Allentown. We respectfully disagreed, but the point was taken.

5: A high-powered "toilet" at 744 East Warrington in Allentown, Pittsburgh

With that said, Meta Mesh recognizes that the devices we have installed are a "minimum viable product." We have had many satisfied recipients of these devices and will continue to use them. However, we are actively searching for new hardware to use that is faster, less expensive, and just as discrete as our A and AP150's.

Top-of-the line WiFi access points today utilize dual-band, multi-radio setups that can deliver speeds up to roughly 1 gigabit under (very) ideal circumstances. These kinds of WiFi routers typically run $200 to $1,000 per device and are frequently not meant for outdoor use. Even when they *are* designed for outdoor use, they are unable to use the mesh routing protocol OLSR and must use proprietary technology that may, or may not, continue to be supported in a few years' time.

iii. Optional Additions

Keeping with the theme of decentralization, we recognized early on that no matter how many routers we installed, no matter how many gateways we connected, a working network was still dependent on one thing—power.

While we have installed a number of devices (mainly in Allentown and Braddock) that had battery backups, the initial purchase of lead-acid batteries stored in computer-sized UPS's were unwieldy, incredibly heavy, and incredibly expensive with the smallest running a client $60 with the recommended 10-hour power supply being $150.

In late 2016 we successfully created a solar-powered AP150 with all the equipment stored in a box mounted to the underside of a 50-watt solar panel. The entire setup, nicknamed the SAP150, ran us about $350 with a large 13dBi antenna. We have deployed three of these devices in Braddock and they work very well.

6: Two SAP150's without their pole-mounted antennas

While these devices were an improvement, their use as a permanent fixture in a neighborhood is questionable and the ability to mount them to the side of a building, while doable, is expensive.

Choosing a proper deep-cycle battery is important but, again, costly. In addition, lead-acid batteries perform very poorly in extreme temperatures and we recognize that the lifetime of these batteries will be greatly shortened due to their exposure to these extremes. For the right circumstances, however, this solution could be extremely valuable.

Instead of doubling down on finding the perfect lead acid battery, we decided that smaller was better and began experimenting with Lithium-ion-Polymer batteries, which are used in mobile devices. These batteries fair better in extreme weather (although they still suffer from deterioration in extreme heat and cold), are more easily charged from being completely spent, and weigh less than a tenth of a lead-acid battery. We have successfully powered an AP150 for 14 hours with a Li-Po battery and want to offer them as *the* backup solution for *any* PittMesh network segment we create moving forward.

7: A 2,000mah Li-Po battery, charge controller, and AP150

iv. Ownership, legal, and tort considerations

Who owns the devices once they are installed and working? Who is responsible if a device breaks? Who is responsible if a hole is not sealed during installation and water leaks in, discoloring someone's wall? Meta Mesh understood, from the beginning, that these were going to be real concerns. While there is no right answer to catch every problem, we implement the following agreements to limit liability for ourselves, our volunteer installers, and the Partners, sponsors, and funders of the PittMesh network.

Ownership: Typically, Meta Mesh recommends that the device, after installation, is owned by the person who uses the property or the owner of the property itself. When we have installed a device at an apartment, the apartment resident takes ownership of the device. Other times we have worked directly with the property owner who then takes ownership.

Meta Mesh does not own the equipment once it is deployed. In an ideal world, Meta Mesh, having the most familiarity with the technology that makes PittMesh tick, has no ownership and no access to any of the devices, and the residents who have them installed are all qualified technicians who can fix any issue and replace any malfunctioning device. This, however, is not the case in the real world. Meta Mesh will create a contract for some level of maintenance, support, and replacement of failed devices with a community organization that wishes to hire us to install a segment of the PittMesh network. Typically, we support and reconfigure all the devices in a PittMesh network segment until all of the devices that our contract defines have been deployed. Afterward we will provide best-effort support with no service level agreement.

It is not recommended that users rely on the PittMesh CWN as their *sole* method of obtaining Internet access. It should be understood that, for technical and legal reasons, PittMesh is a supplementary and best-effort network that is not owned by Meta Mesh. PittMesh is a common resource in a neighborhood owned by multiple entities that must work in collaboration to function properly. With that said, funding can be applied to preferred

maintenance and upkeep from grants or crowdfunding to better secure the sustainability of your neighborhood's network.

It should also be understood that Meta Mesh's goal is not to deploy and maintain a network *for* your neighborhood but rather to *teach* residents in your neighborhood how to maintain the network themselves. Decentralizing maintenance ensures more sustainable maintenance.

Access: Even if Meta Mesh does not own all (or any) of the devices on the PittMesh network, we still have an interest in ensuring that the network stays healthy. Upon initial configuration of our PittMesh routers, we apply an SSH key for remote access so that we can apply any crucial security updates to prevent malicious attackers from taking advantage of vulnerabilities. We may also apply new functionality across the network.

Maintaining access to these routers is not mandatory and, if requested, we can remove this access to the device for any reason although we will recommend against it. In addition, it is allowable for any other entity to have password or SSH access to a PittMesh router. We do not own the devices so we will not mandate who can and cannot have access to the devices.

Monitoring: While securing the PittMesh network is important, we also want to have access to the routers so that we can obtain valuable usage data. We only collect non-specifying usage data. We do not log MAC addresses and thus are limited to usage "snapshots." This is to prevent the ability to abuse this access by being able to track usage down to a single device. We do not perform deep packet inspection. We only aggregate non-identifying usage data for internal reporting, reporting to funders, and external reporting in the form of public announcements and for display on our PittMesh.net website. Like our access, anyone who does not wish to participate in our monitoring can request to opt out or simply remove the SNMP and scripting elements that transmit data to our servers without penalty.

3) Understanding Routing on PittMesh

While many people interested in bringing PittMesh to their neighborhood are uninterested in *how* routing on PittMesh works, it is important to understand how our routers are set up to make a fully-informed decision on implementing the network and deciding how to use it in your neighborhood.
For this section, we will simply go over the technical features (and limitations) of an OLSR mesh for a more technical audience.

PittMesh (used interchangeably with an "OLSR" hereafter) is actually many subnets, tied together via a single, large network. This "mesh" network is different from the "client" network and the "host" network, all of which work together to provide useful functionality to the neighborhood in which it is deployed.

a) The Mesh Network

All OLSR interfaces on PittMesh devices live in the 100.64.0.0/10 network. This subnet is not publicly routable and is defined as a subnet "used for communications between a service provider and its subscribers when

using a carrier-grade NAT" in RFC6264. This allows for 4,194,302 unique IP addresses on the PittMesh network in IPv4 space.

Meta Mesh plans on moving to IPv6 space in the future to prevent IP replication issues. The IP address of the OLSR interfaces of each device on PittMesh is derived from the device's LAN MAC address, converted into decimal from hexadecimal, and modulated where necessary. For example, the MAC address 73-A6-96-**DE-CC-69** utilizes the last three values (in bold) and translates them to decimal format so that this address becomes 100.**94**.**204**.**73**. This address falls within the 100.64.0.0/10 subnet.

In the event that a MAC address falls outside the subnet, it is modulated so that it will fit. For example, FF-D9-02-3D-BF-11 converts to 100.61.191.17. This falls outside 100.64.0.0/10 and thus modulated to fit. We do this simply by converting the third octet and adding 64 (if it is below 64) until it fits into the range. In this case, this MAC address's valid PittMesh IP is 100.125.191.17. In the event that the second octet is between 128 and 192, we subtract 64. In the event that the second octet is between 193 and 255, we subtract 128. Obviously, there is a risk that we will overlap IP addresses doing this. This is why we will move to IPv6 eventually.

OLSR runs on the mesh interface. OLSR announces the device's routing table via a broadcast message and is set to listen for other OLSR broadcasts on and only on that interface. When a foreign OLSR broadcast arrives on the interface running OLSR, the foreign routing table is added to the device's routing table with new routes set for the device's OLSR interface. This foreign packet may include 0.0.0.0. If it does, Internet-destined packets from our device will be sent to the foreign device that has this "Internet Announcement." This can (and does) change as the routes to the Internet and other hosts on the 100.64.0.0/10 subnet are calculated based on a metric that judges wireless connection quality and link status. Therefore, if you have two routes to the Internet, the route from the device with the stronger WiFi signal will be preferred.

b) The Client Network

The client network is a 10.0.0.0/24 network attached to a bridged LAN and WLAN interface and the IP address here is derived from the MESH IP address simply by taking the most unique octets from the MESH interface (the third and fourth octets) and moving them to the second and third positions, respectively. So if we have a device with an address of 100.111.222.33, it's "client" network (it's LAN and WLAN) will be set to 10.222.33.1/24 with a DHCP server running from 10.222.33.10 to 253 with a lease time of 1 hour.

This ensures (mostly) that any device connected as a client to a PittMesh device has a unique IP address on the network and is routable from anywhere else on the mesh. In this way, we are able to have anyone open a laptop, host a service, tell others what that IP address is, and anyone on the mesh can now use that IP as a server for that service. This requires no configuration or authorization from the router's owner or Meta Mesh.
The next question is "what about DNS?" DNS is planned to be taken care of in early 2017 by a collection of distributed, replicated DNS servers throughout the PittMesh network, managed by Meta Mesh.
You may be wondering how other routers know about our example router's private subnet. This information is attached to our device's outgoing OLSR broadcasts as a "Host-Network Announcement" or, more typically and

somewhat incorrectly, an "HNA Announcement." The HNA Announcement simply informs OLSR to let all other OLSR-enabled devices know that our device has and is allowing access to its Client network subnet. It is possible to make our device's client network unrouteable simply by removing the HNA Announcement for the 10.0.0.0/64 subnet in the OLSR section of OpenWRT.

Remember that OLSR ONLY announces routes in the routing table tagged with the interface on which OLSR runs- so any other interface is not broadcast unless explicitly instructed to do so which brings us to…

c) The Host network

The Host network, or the WAN, is not accessible from the MESH or the client network except for the Internet. In this way, no one can access the home or business network on the WAN interface. We can prevent access to the host's private network this way through the use of firewall rules. Remember that you can announce Internet access by adding an HNA Announcement for the Internet. Meta Mesh will be implementing automatic gateway detection in 2017 to ensure proper gateway propagation throughout the network.

d) Roaming and Routing and Hops

Because each router's subnet is unique, it is not possible to roam from one PittMesh router to another. You will need to manually disconnect from one router's SSID and connect to another router's SSID which will appear differently in your device's wireless network connections application.

It is important to understand how routing works in an OLSR mesh as well. Remember that a repeater's routing table will have a gateway that may change around if there are two nearby gateways with similarly strong WiFi signals. OLSR calculates which gateway to use and it is possible to manually define via weights which gateway to use.

For brevity's sake, Meta Mesh often refers to "donating bandwidth" into PittMesh's "pool" which may lead some people to believe that their Internet-bound traffic may route through different gateways. This is incorrect. PittMesh's bandwidth is not universally the same. A rising tide does not evenly lift all boats on PittMesh.

OLSR does not take into account the Internet access speed, but rather the quality of the connection to devices in the area. Therefore, it may be possible for your OLSR-enabled router to connect to a gateway of better quality with a slower Internet connection, than another nearby gateway with a slightly poorer OLSR link quality, but an overall faster Internet connection. We have not seen a serious issue with this but recognize that the problem may occur.

Finally, the further away you are from a gateway or resource on the mesh, the slower your connection will be to it. This is due to the combination of WiFi's airtime fairness mechanics, lost packet retransmission, and the fact that each packet needs to be positively verified after each hop to a new router from your phone or laptop to the gateway or resource. Ideally, the bandwidth only "halves" after each hop, but real tests have shown greater loss than this per hop. In our experience, however, you can repeat signal through well-connected wireless links up to

5 or 6 hops without experiencing frustrating slowness. Still, with that said, it is recommended that a gateway be placed no more than 3 hops apart to ensure good reliability throughout the PittMesh network segment.

4) Meta Mesh Classes and Training

Meta Mesh's philosophy on building public WiFi comes from the realization that many public WiFi networks do not survive more than three years due to budget constraints and lack of ability or willingness to maintain the network. Instead of making the care and feeding of a network a responsibility of an often for-profit entity, Meta Mesh believes it should be the responsibility of those with a vested interest in the network to maintain it. This, however, is easier said than done.

Taking residents who want a public WiFi network, but who have no training in system or network administration, and turning them into ladder-climbing, router-flashing technicians is no small task. And while each time Meta Mesh has run our training program we expand the breadth and depth of the topics covered, we still find new questions and new ways to explain edge cases that pop up.

Still, part of the core of our PittMesh buildout for a neighborhood involves *trying* to teach the skills required to creating a crack team of WiFi administrators. The following is a brief overview of the classes and training we perform to prepare residents to become PittMesh network technicians.

a) We're getting a PittMesh Network!

After the agreed-upon funding goal of a PittMesh network build out is reached, we need to engage the community, build excitement, and orient residents so that they understand what will be installed, what it will look like from an end-user's perspective, and give them an opportunity to ask questions regarding the technology, security, legal or tort issues, or anything else they may not understand. These orientation meetings should be NO MORE 6 weeks before the start of classes and should contain marketing material provided by Meta Mesh and Partner organizations to inform residents of what will be happening in their neighborhood.

- Food must be provided and may be paid for by raised funding or donated separately
- Partner organizations must secure a venue for 3 hours on a weekday evening from 6:30 pm to 9:30 pm. The venue must comfortably seat 35 people, have power, water, and Internet access, a projector screen and a video/computer projector with HDMI or VGA connector, and a sturdy table for demonstrations.
- Partner organizations must dedicate time each day to advertise this orientation for two weeks before it occurs and must collaborate with Meta Mesh to ensure prospective residents and organizations are notified and informed. Emphasis should be on high-school students, young adults seeking training in networking and wireless communication, and those who want to help physically install the equipment.
- A Partner organization member must be present to receive recognition and endorse Meta Mesh's work in their community.

b) WiFi Basics 1: Radio Gaga: How Radio Communication Works

How do radio waves behave and why is it important when building a public WiFi network to understand their behavior? We'll talk about wave phenomena like reflection, diffraction, absorption, and refraction! You'll be surprised at how light, sound, and ocean waves behave so similarly and how we can harness these waves to carry data for us!

c) WiFi Basics 2: RF Math is fun! How to Calculate Signal Strength

If you set up two WiFi devices and want them to communicate, how can you be sure their signals will reach the other device? We have ways to calculate this (and fortunately we don't need a lot of math to do it!). Become a wireless pro by being able to predict how strong signals will be between two wireless devices.

d) WiFi Basics 3: Radio on Planet Earth and the Dark Arts of WiFi

Radio behaves one way in the lab but in the field you need to consider a few more factors. We'll discuss Free Space Path Loss, bending radio around the curvature of the Earth, and wave polarity. Then we'll discuss how we can use technology to solve all those bad radio behaviors that reduce throughput in our wireless signals.

e) Networking Basics: WANs, LANs, and WLANs, oh my!

WiFi is cool and all but if you're going to build a network you need to know what a network is! We'll go over WANs, LANs, WLANs, bridging, forwarding, NAT, IPv4 addressing, subnet masks, DNS, DHCP, routing tables. It sounds like a lot but it's just a few concepts that all work together to form the basis of how the Internet works!

f) Ethernet Construction: Never Overpay for Cat5 again

Have you ever needed a 15 ft. Cat5 Ethernet cable and gone to Best Buy and spent $45? You're being charged for your ignorance! So let's learn how to make our own Ethernet cables and save money! Making Ethernet is an integral part of building a CWN. Learn a skill that could save you hundreds or even thousands of dollars and is the cornerstone to jobs like working in a data center or working as an IT field analyst.

g) Installation Prep: Climbin' Dirty

Now that we know all about Radio waves, WiFi links, and networking it's time to get our hands dirty and learn how to install PittMesh WiFi routers in our neighborhood! Learn how to use a

hammer drill and safely climb a ladder. After completing this class, we will begin scheduling evening installations in your neighborhood to start building your PittMesh public WiFi network.

h) (Optional) Advanced Networking: OLSR: Optimized Link State Routing

Now that we know how networking works on the Internet, how does networking work on PittMesh? What is OLSR and how does it help a network stay up when a router goes offline? How can better understanding OLSR help us implement PittMesh in our neighborhood? This class is significantly more complex than the other classes but it is possibly the most rewarding, because it is really the culmination of everything discussed in previous coursework. This class does not introduce new material insomuch as it forces students to think about concepts from previous classes. (When we taught this class, we found that the look of astonishment on peoples' faces, when they realize they "get it," is very rewarding.)

i) (Optional) Bubble Trouble: Troubleshooting PittMesh Routers

Something is wonky on the network. How do we know what's wrong beyond "it doesn't work!" We'll discuss the different levels of connectivity and what it takes to get Internet access from a PittMesh WiFI router. We'll cover the Mesh network, the client network, DHCP, DNS, HNA announcements, and the dreaded firewall.

j) Guided installations:

Meta Mesh will guide a number of installations at pre-selected locations in your neighborhood with residents gathered from classes and invited from the neighborhood. Meta Mesh will provide materials and guidance to show, not tell, residents how to install PittMesh routers. The purpose of these guided installations is to ensure that the rest of the network can be installed by volunteers who can self-organize to complete the installation of the neighborhood's network.

- Meta Mesh will provide all materials, confirm the devices are working, and follow up with monitoring and maintenance for these devices in coordination with neighborhood Partners and volunteers.
- Typically, there will be five guided installations for the rest of the network, which will be installed by volunteers with assistance from Meta Mesh, who will coordinate volunteers and provide supplies to them.
- Meta Mesh's community Partner should make a concerted effort to obtain the voluntary services of a local construction company or find residents with carpentry, construction, or IT installation experience to ensure that this aspect of the project will be completed.
- After a core crew of installers is identified, Meta Mesh will work directly with them and the router hosts to establish a date and time to do the installations. The volunteers will benefit from Meta Mesh's social networking and outreach Partners to attract volunteers.

- While it is not necessary to participate in the classes to volunteer with the installation crews, we recommend that at least some of the installer volunteers participate in the classes in order to become local network Liaisons with Meta Mesh, ensuring upkeep can be performed in the event of a problem with the network.

5) PittMesh Segment Implementation

a) Costs

Item	Quantity	Cost	Total
Allegheny 300 Router Kit	25	200	$5,000.00
1000ft cat5e	2	$38.50	$77.00
UBNT Tough Cable	2	$184.05	$368.10
1/4 in. x 1-3/4 in Hex-Washer-Head Concrete Screws (225 per bucket)	2	$50.00	$100.00
Impact Driver/Hammer Drill	2	$249.00	$498.00
1/4 in. hex drivers	4	$5.81	$23.24
10 in. tin snips	1	$12.99	$12.99
RJ45 Network Kit (Installer Parts 10 Piece Network Installation Tool Kit -- Includes LAN Data Tester, RJ45 RJ11 Crimper, 66 110 Punch Down, Stripper, Utility Knife, 2 in 1 Screwdriver, and Hard Case)	4	$33.98	$135.92
50 Pcs Silver Tone Shielded RJ45 8P8C Network Cable CAT5 End Plug	5	$10.17	$50.85
100 Pcs RJ45 connectors	4	$7.32	$29.28
Cable Ties	4	$3.99	$15.96
Cable Clips	5	$6.95	$34.75
Caulk Gun	2	$2.47	$4.94
Caulk	5	$2.28	$11.40
Magnetic Drive Guide	8	$4.97	$39.76

26 Foot ladder	1	$249.00	$249.00
Extension Cord	2	$11.97	$23.94
Fishing line 25 ft	2	$11.87	$23.74
Tool Bag	2	$24.97	$49.94
Tool Belt	2	$19.98	$39.96
Training Classes materials, preparation, food subsidy, location reservation costs	1		$3,400.00
Marketing Budget	1		$1,000.00
Implementation of Pi-in-the-SkyNet Distributed Computer System for CHUB and other local services	1		$4,850.00
Administrative Coordination Costs for 1 year	1		$9,000.00
MATERIAL and ADMINISTRATIVE COSTS			**$20,038.77**

TOTAL DIRECT COSTS			$20,038.77
TOTAL IN-KIND CONTRIBUTIONS			$14,100.00
TOTAL PROJECT VALUE			**$34,138.77**

b) Tool Storage Environment

It is important for each installation crew to have access to a storage location within the neighborhood, where their installation equipment may be kept for easy access. Built into the above approximation of funds for a 20-router network (what we sometimes call a "full installation" which is, in effect, 20 routers, classes, guided installations, and Pi-in-the-SkyNet and the Community Hub implementation), is the purchase of all supporting materials needed to replicate everything needed to independently build out, troubleshoot, and expand your PittMesh network.

c) Pre-planning the Network in your Neighborhood

Meta Mesh will work with the community Partner to determine a good area to build the network. Typically, you want to have a space that has high foot traffic and highly residential. A business district with parklets is an idea location, although mesh networking technology allows for a variety of implementations.

PittMesh and other public WiFi networks are not meant as a total replacement for Internet access. We forewarn our Partners that this is not a "high speed" network but rather a "best effort" network with expected speeds between 5 and 20 mbps. There are many factors that affect WiFi throughput speeds and the most difficult barriers for the radio technology we use are walls. While it is possible (and likely) to use PittMesh in buildings that have PittMesh routers installed, do not expect to have PittMesh access more than 30 feet inside a building. While some buildings may have sufficiently thin walls for WiFi to penetrate further, multiple experiments with our technology have shown that "pulling" WiFi from the street into a building is not an ideal solution and slow speeds and disconnects are common. This network is mainly meant for public spaces with few walls and the near side rooms in buildings facing the PittMesh area.

Meta Mesh will assist the community Partner in identifying areas that would be best served and also with making an ideal implementation pattern for where routers should be deployed. This will take the form of a document with a list of addresses and a map with routers and their expected coverage areas on an overlay.

d) Partner Expectations

A disorganized, uncommunicative, or uninspired Partner will cause a PittMesh network segment installation to fail. Community Partners are expected to do most of the footwork and advertise for the buildout of a PittMesh network. Inability to accomplish preset goals expressed in this document and follow-up documents WILL result in low turnout for classes and installations, redistribution of funds to compensate for completion of the project, and possibly the cancellation of the project altogether.

You will find that, while working with Meta Mesh, our employees will go the extra mile and will dedicate more time and effort than may be anticipated to complete the agreed upon buildout of your neighborhood's network. We have a reputation for accomplishing our goals and finding solutions when none seem to exist. Meta Mesh *requires* a healthy Partner relationship to move forward on all aspects of the project.

Partners are expected to do the following:

- understand this document, further orientations, and contracts
- work with Meta Mesh to pre-plan installation locations and understand the constraints of the technology used in both coverage area and expected speeds
- be the point of contact between Meta Mesh and the locations determined in the pre-planning, getting the home and business owners in the target area to get on-board, understand the project, reassure them regarding concerns, and direct them to Meta Mesh for questions not covered in this document
- arrange a venue with the appropriate requirements to be used for classes

- arrange a location where tools may be stored and arrange for access to be granted to network Liaisons in the neighborhood
- disseminate advertising and marketing literature to announce classes, guided installations, and general announcements regarding the network before, during, and after classes
- assist users of the network or router-host by directing post-installation difficulties or concerns to the Network Liaison in your neighborhood or to Meta Mesh, who will work with the Liaison to rectify any problems
- identify and attracts carpenters, installers, construction workers, or other competent laborers from the neighborhood who may be good Network Liaison or Installer Crew volunteers
- assist with the fundraising either through a crowdfunding/fundraising effort, or via a grant or award (It is expected that the Partner organization hold discussions with pre-identified local businesses and individuals who may can fund a significant portion of the cost of the project.)
- work with Meta Mesh's guidance regarding record keeping and checklists (We use collaborative tools to ensure both parties are working on their assigned duties in a timely manner.)

e) Meta Mesh Expectations

Meta Mesh is expected to perform the duties described in the previous sections.

- receives funding from the chosen fundraising strategy
- purchases all equipment and supplies
- designs and distributes marketing material to the Partner and independently where appropriate
- teaches classes
- performs guided installations
- provides the infrastructure to track progress on your neighborhood's PittMesh buildout
- monitors and accesses routers on the network to troubleshoot (unless otherwise requested)
- works directly with Network Liaison to resolve issues

f) Network Liaison Expectations

The Network Liaison is one or more people (not necessarily residents) who wish to dedicate a year of service to the preservation and expansion of their network. They will work closely with Meta Mesh to be a "rapid response" technician to perform unsophisticated maintenance such as: investigation of a problem in your neighborhood's network that Meta Mesh has detected, perform a router replacement, contact a router host who may have disconnected their device, or other simple work.

The Liaison is *not* expected to install all equipment him or herself. The Liaison is not expected to work often to resolve problems; we estimate that the Liaison will be called upon 5 to 10 times per year with most issues being resolved in under an hour.
The Liaison acts as the first line of defense in maintaining the network in your neighborhood. They are to be treated as an authority trusted by the Partner and any router host. To verify that the Liaison is a valid Partner with Meta Mesh, we will recognize the Liaison with a photo and short bio on our website.

After a year, the Liaison will be asked if he or she would like to continue volunteering for another six months and this process will repeat until the Liaison resigns or the network deteriorates to a point where it is no longer supportable (5-10 years).

6) PittMesh Usage

a) Router Host Security

One of the recurring questions that inevitably comes up in a community installation is "is this safe?" It's a good question. In short, the answer is yes.

By using OpenWRT's built in firewall, we are able to control who gets to connect to what in the default configuration of a device. Because these devices are clients of the host's home or business network (if they are a gateway, typically), then we must ensure that no one "on the mesh," meaning anyone connected to the PittMesh device's WiFi, can access any of the host's internal devices. This is done simply by adding a firewall rule that disallows any access to the three private ranges of IP addresses as defined in RFC1918: 192.168.0.0/16, 172.16.0.0/12, and the 10.0.0.0/8.

It is also possible to configure a device so that it has Internet access locally (meaning it has a route to the Internet in its routing table), but does not tell the rest of the network about this route during OLSR announcements (it does not have an 0.0.0.0 HNA announcement). In this way, you can have Internet access for anyone connected on the premises but you can ensure the rest of the network does not use your router as a gateway (a bit selfish, but sometimes there are reasons for this).

When someone tries to access a device in those private ranges, two things can happen. First, if the PittMesh router the user is connected to is a gateway, the packet will travel from the client's device to the router where it will pass through the IpTables (firewall) rules. IpTables will recognize that the packet is headed to an invalid location and the packet is subsequently dropped. The packet will never even make it onto the Ethernet cable that connects the PittMesh router to the host's network.

Second, if the PittMesh router you are connected to is set up in a repeater configuration and you try to go to an IP in one of the private ranges your packets will not be sent because there will be no routes in the PittMesh router's routing table for that range (because they were never announced in the first place by any other router). This will result in it being sent to the nearest gateway and then dropped because, again, the gateway is configured to drop packets destined for private ranges.

These rules are available at Meta Mesh's GitHub page under ar-150 > DHCP-AP-Gateway Script. The pertinent rules look like this:

```
uci add firewall rule
uci set firewall.@rule[9].dest=wan
uci set firewall.@rule[9].proto=all
```

```
uci set firewall.@rule[9].src=lan
uci set firewall.@rule[9].target=DROP
uci set firewall.@rule[9].dest_ip=172.16.0.0/12
uci set firewall.@rule[9].name=Block-LAN-Access
uci add firewall rule
uci set firewall.@rule[10].src=lan
uci set firewall.@rule[10].dest=wan
uci set firewall.@rule[10].proto=all
uci set firewall.@rule[10].dest_ip=192.168.0.0/16
uci set firewall.@rule[10].target=DROP
uci set firewall.@rule[10].name=Block-LAN-Access-1
uci add firewall rule
uci set firewall.@rule[11].enabled=1
uci set firewall.@rule[11].target=DROP
uci set firewall.@rule[11].src=lan
uci set firewall.@rule[11].dest=wan
uci set firewall.@rule[11].proto=all
uci set firewall.@rule[11].dest_ip=10.0.0.0/8
uci set firewall.@rule[11].name=Block-LAN-Access-2
uci commit firewall
```

b) PittMesh User Security

Another recurring question we get is “am I safe using this open network”? This answer is a lot more nuanced. We can summarize it by saying “traditionally, no, but increasingly, yes.”

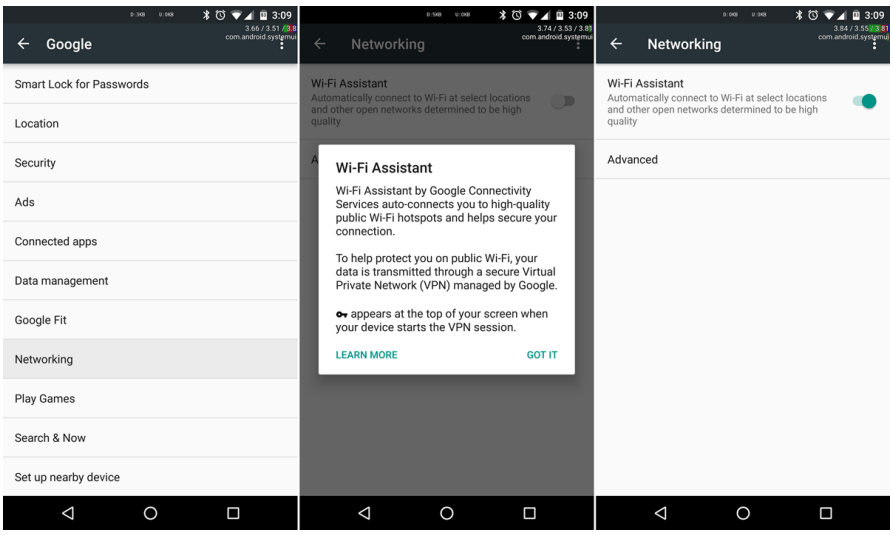
The way that WiFi networks work is you have an Access Point (your WiFi router) and its Clients (laptops, desktops, smart devices). If the Clients connect to the Access Point using the same WiFi Network (SSID), and none of the Clients are encrypting their traffic, then ALL traffic is visible to ALL devices, connected or not, to that wireless network. Detection and recording of traffic on any WiFi network is trivial and can be done using many programs, the most famous of which is WireShark.

To prevent reading this open traffic, WEP and WPA security was implemented and the use of “putting a password on your WiFi” has thankfully become the norm. Unfortunately, no security protocol that protects WiFi is 100% secure. None. All of them have been broken, although the difficulty to break some of them is extremely time consuming and requires a lot of resources, making the more secure WPA2 and WPA-Enterprise protocols much better. HOWEVER, even if you have a password on your WiFi network, Clients that are connected to the Access Point are all using that same password and thus all using the same encryption key. This makes all traffic visible to everyone who has that password! Therefore, if you secured your PittMesh router with a WiFi password but gave out that password to everyone… there is essentially no password and no encryption for the network and packet sniffing tools work perfectly again.

To increase the use of PittMesh we do not ship our routers with any password on the WiFi. Instead, we rely on the increasing adoption of HTTPS and other end-to-end encrypted protocols to ensure private use on the PittMesh network. Yes, this puts the burden of security on the user and the services he or

she uses, but there is no practical way for Meta Mesh to secure ALL TRAFFIC at REASONABLE SPEEDS for ALL USERS at this time.

One interesting and increasingly available technology is “WiFi Assistant” which comes natively on some Android phones and can also be used by downloading AVG’s app. There are numerous programs for Windows, Mac, and Linux operating systems that also provide an end-to-end VPN which encrypts all traffic from your device to a gateway provided by the service provider.



1: WiFi Assistant on Android

While this technology requires the user to take a few more steps to increase their security, the burden is not so great that it is a significant inconvenience. We will probably increasingly see this technology automatically installed and in use on all operating systems in the next few years, helping to ensure that fewer and fewer users are vulnerable to inadvertently transmitting sensitive information in the open.