What is network isolation?

***A project management approach to designing, implementing, and operationalizing network isolation and micro-segmentation***

Network segmentation (often referred to as network isolation) is the concept of taking your network and creating silos within it called **VLANs** (virtual local area networks) that separates assets in the networked environment based on the function of the asset within the organization or some other schema you define to separate lower security levels from higher more restricted levels. With the growing prevalence of companies that are required to be PCI compliant, more and more organizations are needing to design and implement a segmented network and unfortunately, despite the amount of information on the topic, many fail before even getting started.

Here’s why.

A big misperception is that if you implement different VLANs in different CIDR blocks/network numbering, you’ve achieved network segmentation. This couldn’t be further from the truth. To achieve actual segmentation, the hosts in one VLAN should not be able to reach every port of every asset in the other VLANs. In true network segmentation, you would set the default gateway of the VLAN on the switch to the firewall where the traffic can be further scrutinized based on specific ports, protocols, and traffic direction. As an alternative, but less scalable, is using VACLs (VLAN Access Control Lists) but solution can quickly become unmanageable, especially in large-scale enterprise deployments. These are however, quite suitable for smaller networks that have 1 or 2 core switches.

Now that we’ve defined exactly what network segmentation is, let’s discuss why it’s needed.

IT security, circa 1990s to mid-2000, the objective was to secure the perimeter. To be fair, the edge of most networks was quite porous and patching and vulnerability management was practically non-existent. There were many ways into networks being through buffer overflows in daemons like WuFTPD or Apache (*read: the era of mass-defacements*).

Things however have changed. Many networks now have a very hardened exterior and “soft gooey” interior network relegating the majority of compromises to web application attacks and spear phishes. However, because our “early years” were focused on hardening the perimeter of our networks, little attention was paid to the internal network, making it a virtual playground for any bad dudes (sorry, I swear that will be my only Trump reference) to do what they want on any server because a lack of vulnerability management and flat networks is more common than not.

If we look back to many of the advanced persistent threat (APT) attacks that have taken place over the past two decades, you can point to issues rooted (no pun intended) in flat networks. For example, the Target compromise where the HVAC assets were being maintained by outside suppliers was on the same network as the point of sale (POS) systems in the store network that were processing and transmitting cardholder data.

Moving away from a flat network to a properly segmented network will allow you to implement the lateral security controls you need to pigeonhole an attacker or malware to a particular area of the network where the initial foothold was gained. While not ideal, there may be servers that also may not be patched against certain vulnerabilities. As such, network isolation can be your *Hail Mary* in these circumstances that will prevent compromise of those servers if the network where the attacker or malware is attempting to pivot from is prevented from accessing those servers. As a matter of fact, there have been numerous incident response investigations that [Brier & Thorn](http://www.brierandthorn.com/en/) has performed where it was network isolation, not vulnerability management, that prevented the compromise of some mission critical servers in the environment and prevented a much larger-scale network compromise.

Okay, so now that we’ve discussed what it is and you now understand why you need it, let’s discuss how to implement it.

First thing first. Is this a new network implementation or will you be restructuring an already existing flat network? If you are restructuring an existing network, understand that particularly impactful to your project timeline will be the size of the network itself.

Having said this, being the project-focused person that I am, my recommendation is that you manage this using a formal project schedule and work breakdown structure (WBS). I’m not saying you need to engage the Program Management Office (PMO) in your organization here. My recommendation is just use a freemium cloud app for project management or use Excel templates for project management freely available from numerous project management sites. Since there will be other stakeholders in this project, I recommend that you leverage a cloud-based project management app so everyone in the organization involved in the project has access to their tasks and the project timeline.

Let’s review the plan based on the PMBOK (Project Management Body of Knowledge) 5 phased project.

| Step | Description | Output |
| --- | --- | --- |
| Initiation | In this phase you will put together a presentation to sell to management why the network rearchitecture needs to happen and why having a flat network is bad. | 1. Powerpoint presentation and project plan |
| Planning | Once you’ve received approval to move forward with the project, you’ll want to create a WBS (work breakdown structure), defining the tasks of the project, which will then be brought into creating a project schedule where you’ll define dates and timelines for each task.  Most important to this stage is identifying your project stakeholders. If you’re in the IT security department, you’ll need to rely heavily on network operations and server operations as new DHCP pools will need to be created and servers will need to be re-IP’ed with new static IPs based on the networks you create.  Since I’ll assume that you don’t yet have updated network drawings of your corporate network, this might be a great opportunity to properly document your network architecture and create at least a set of logical network drawings along with the spreadsheet of new network segments you’ll be creating in this project. | 1.Project stakeholders matrix  2. Spreadsheet of new subnets being created  3. Revised/new network architecture diagrams  4. List of affected enterprise applications  5. List of required ports and protocols for enterprise applications affected by the migratio |
| Execution | Once you’ve created your WBS and project schedule and allocated tasks to task owners in IT security, network operations, and server operations, it’s now time to perform the work.  It’s important that all enterprise applications, especially those that reach into any newly isolated networks, such as a CDE are tested post-implementation. It’s very easy for a port to be left out in the new firewall rules that may be required by an application. | 1. Any change control requests/change management windows |
| Control | It’s important throughout the project that you setup weekly project meetings to ensure that all project stakeholders are on top of their tasks and doing what’s required so that progress is closely monitored. No one wants scope or date creep, so stay on top of the entire project. |  |
| Close | Close out the project once all enterprise applications have been tested to be functioning properly and systems in the enterprise are reachable that are supposed to be accessible from the different network segments that were created. |  |

In-scope PCI network versus the Cardholder Data Environment (CDE)

A confusing topic for many is what the difference is between the in-scope PCI network and the CDE. The PCI (Payment Card Industry) DSS (Data Security Standard) defines in-scope PCI assets as anything that can affect the security of the cardholder data environment. The cardholder data environment or (CDE) are all systems that transmit, store, or process cardholder data. For companies requiring PCI compliance, isolation of the CDE is critical to you successfully passing your annual QSA audits and also to protect your crown jewels.

Having said that, a common network architecture is to put systems, such as Active Directory servers that handle authentication for users and applications in the CDE. That puts them in the PCI in-scope network along with other systems, such as security controls and servers that support the business to leverage for performing duties on systems inside the CDE.

A common architecture Brier & Thorn implements in its security architecture engagements for PCI networks will be discussed in a future article along with the associated network drawings. We will typically place business support systems inside the PCI zone that require reach-in access into the CDE from outside the network.

Rules

While there is no one right way to do this, make it yours and be creative. “Draw outside the lines” and create something that makes sense for your network and organization. Having said that, there are some general guidelines you should follow when designing your different network segments.

1. DO separate user workstations from internal servers. It is very common to find organizations where user VLANs are on the same network as internal mission critical servers which allows for minimal to no network filtering between the hosts except on endpoints.

2. DO separate printers onto their own network

3. DO separate VOIP phones onto their own network

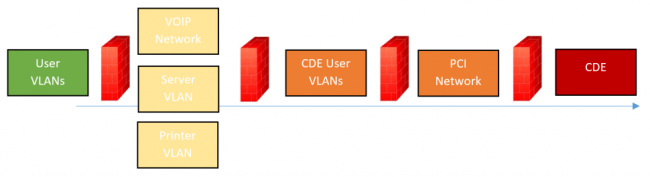
4. DO only allow the ports needed by the applications. If you don’t know what they are, this is an opportune time to work more closely with the application owners more than you ever have before to better understand their applications and requirements. Schedule meetings with each app owner and document the ports and protocols and traffic direction for each of their enterprise applications.

5. DO define network security controls beyond VACLs for inspecting and acting on suspect traffic entering each VLAN.

6. DO NOT consider the user VLANs as being a trusted network

7. DO consider architecting the network in layers of trust from high to low like layers of an onion.

The below diagram is of course logical and not physical. Each of the four firewalls below could easily be a single firewall that all VLANs are hanging off of. Please don’t email me telling me that my proposed architecture is cost prohibitive and stupid. I’m just always thinking linearly, thus I prefer to draw things out in a linear way to better understand and present my line of thinking (no pun intended).



Summary

In this blog we discussed the importance of network segmentation, isolating restricted networks, such as a cardholder data environment or PCI zone, and we also discussed how to do it. I presented a phased project management approach to implementing network segmentation and also discussed the importance of working with the other functional areas of the business, including network operations, application owners, server operations, and IT security in this effort. Because of how many functional areas of the business are impacted and needed for this to be done successfully as well as the potential for applications to break with the introduction of new firewalls and changes to IP addresses, it’s important that those areas of the business be brought in as stakeholders in this project. This cannot be done in a vacuum.

For more information on micro-segmentation, I urge you to see the reference section below or contact me with any questions.

As Sun Tzu once said, “The art of war teaches us to not rely on the likelihood of the enemy not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.”

Network Isolation, the segmenting of a computer network into separate zones with distinct trust levels, for the purpose of containing hazards or reducing damage caused by a threat actor, is a hallmark of nearly every security-minded network design. Even though implementing port security policies, VLANs, VPNs, and other technologies can take many months of planning and hard work, generally, the investment is worthwhile as it often significantly strengthens the network’s ability to withstand a cyberattack.

It turns out that maintaining the isolation between network segments, though (i.e. in the face of productivity and usability demands by end-users), is a hard problem. Network engineers and security architects wind up purposely building weak points into their environments (jump servers, backdoor ‘admin subnets’, etc.) that undermine their attempt at separation, and end-users are burdened with quirky hoops to jump through to access sensitive resources. In extreme situations, end-users are issued multiple workstations: one for each network segment they have a need to access.

Fortunately, virtualization tech has evolved to include virtual networking capabilities at the endpoint that can maintain network isolation without sacrificing a seamless experience that end-users expect. Let’s take a look at how endpoint virtualization solutions like Hysolate can improve both network isolation and user experience in a few contexts:

***Scenario 1: Segmented Corporate Network***

If your organization implements network isolation techniques such as VLANing then you’re off to a great start. However, if IT engineers install dual-homed jump servers or similar, then you may be setting the organization up to rely on single points of compromise. Moreover, the way in which end-users interact with resources on those VLANs can completely defeat the isolation. If a worker exposes his machine’s single operating system to hazards in a low-trust LAN segment and then proceeds to ‘hop VLANs’ by plugging the machine into a port on a sensitive LAN segment he could be exposing the sensitive zone to outside harms via his infected OS. Issuing multiple machines to employees who work on more than one network segment (i.e. one laptop per LAN) simply doesn’t scale. Beyond that, end-users waste countless hours repeatedly switching between machines for day-to-day tasks.

With endpoint virtualization done the Hysolate way, though, VLAN’d traffic can be ‘carried all the way’ into the endpoint’s virtual network, while maintaining full separation. Since the user is running more than one OS as virtual machines (sensitive, corporate, personal, etc.) each can be individually assigned to a separate VLAN, and the zones can maintain their isolation without the need for redundant [privileged access workstations](https://www.hysolate.com/paws-privileged-access-workstations/) and machine-switching user fatigue.

***Scenario 2: Remote Workers and Mandatory VPN***

Let’s say you have many employees who work remotely or travel frequently for work. You must enable them to access resources on the corporate network so they can do their job, so you maintain a remote access VPN service for them to use from anywhere they go. Luckily for the users, the organization doesn’t expect them to lug around two laptops, but their always-on VPN policy negatively impacts their network connection’s performance, and knowing that all of your traffic is being monitored by your employer can be kind of a buzz kill. As a result, users don’t really use their machine unless they absolutely must. Meanwhile the organization is worried they could be legally liable for personal online activities (e.g. torrenting movies) that necessarily traverse the corporate network.

With endpoint solutions like Hysolate the corporate VPN can be selectively applied to only the corporate zone. So, for all corporate purposes, the VPN can be always-on. Moreover, other network policies can be conditionally activated depending on location. Meanwhile, the personal zone can be left to freely visit the public internet without the same need for corporate monitoring, and without the double-hop VPN bandwidth performance penalty.

***Scenario 3: Dual NICs, Dual Networks***

Perhaps you work for a smaller organization the hasn’t quite gotten around to the whole network isolation thing just yet. They’re aware that end-users personal activities on their single, multi-purpose machine could put assets on the corporate network at risk, but the organization doesn’t have the IT staff to roll out VLANs across the whole company right now. The only quasi-network isolation in play is their separate WiFi network for office guests and visitors.

Luckily, your standard-issue workstation sports two network interfaces: a wireless card and an ethernet port. With Hysolate, and without much engineering effort, you can configure your isolated operating systems so that only your corporate zone can connect via ethernet while requiring your personal zone to use the existing guest WiFi network. Alternatively, if the device only has one wireless interface, the company could purchase an inexpensive USB WiFi dongle so it can simultaneously connect to two separate WiFi networks, guest and corporate, to start creating isolation where there was none before.

IT administrators and security professionals can stop building isolation-violating weaknesses into their networks while also staying on good terms with end-users. Using endpoint virtualization solutions like Hysolate can ensure hazardous operations are adequately isolated from corporate resources and other sensitive assets without impacting day-to-day end-[user productivity](https://www.hysolate.com/users-productivity/).

Many computing devices need access to the Internet but do not need to interact with any other devices connected to the router. If you have ever used the Internet at a coffee shop, you fit this profile while drinking your coffee. Security increases when devices fitting this profile are prevented from seeing, let alone interacting with, any other devices connected to the same router. In coffee shop terms, this means your laptop is safer if the laptop computers of the other customers can't see it. Bad guys at the coffee shop can't hack into computers that are invisible to their network scans.

For lack of a better term, I refer to this as Network Isolation. Other may prefer to call it network segmentation.

Many devices in your home need nothing but Internet access. Among these would be a Roku box, an Amazon Alexa and an Internet Radio. I have a stereo receiver that can play Pandora and other streaming services. On a home network, the protection offered by isolating these devices is to minimize the impact of a hacked device. Likewise, a malware infested Windows machine can't spread its tentacles, if it can't see any other devices or computers.

A truly isolated malicious device is prevented from learning about the existence of any other devices in the home. It is fooled, by the router, into thinking its the only device connected to the router. All the other devices in the home are thus protected from being spied on. If the CIA hacks your smart TV, the router prevents the TV from seeing anything you do on your computer.

To be clear, allowing a wireless device to access nothing but the Internet means:

* Isolated wireless devices can not see other users/devices logged on to the same Wi-Fi network (a.k.a SSID)
* Isolated wireless devices can not see users/devices on other Wi-Fi networks created by the router
* Isolated devices can not see any device connected via Ethernet to the router
* Isolated devices can not directly access the router. Even if they know the userid/password to logon to the router, they are prevented from loading the routers logon web page

Truly isolated devices run inside a VLAN. Specifically, a VLAN that does not allow communication with other VLANs.

A VLAN is a virtual LAN. A network within a network. A logical (not necessarily physical) grouping of devices.

VLANs were not initially created for the type of network isolation I advocate here. As such, there is a configuration option for each VLAN that controls whether it is allowed to communicate with other VLANs or not. In addition, there is another configuration option that controls whether the devices in a VLAN can see and communicate with each other.

As an analogy, consider a pet store with many **fish tanks** full of fish. Since the fish in one tank can not interact with the fish in another tank, each tank can be thought of as a VLAN that does not allow communication with other VLANs. A better analogy would be if each tank had a curtain around it preventing the fish from even seeing any of the other tanks.

Devices that *only* need Internet access, are best isolated in a fish tank by themselves. They can't see the other fish tanks (VLANs) and they can't see any other fish (computers).

But, sometimes we do need the fish in a tank to interact with each other. If, for example, you want to use a mobile device to control a Roku box, then both devices have to be able to communicate. The same with Sonos speakers that can also be controlled by a mobile device. I am told that Chromecast is another example, as a mobile device needs to see the Chromecast to set it up initially.

The most secure setup would be to put the Roku, Sonos and Chromecast devices in their own VLANs, configured to allow the devices/fish to see other, and assign a single SSID to each of those VLANs. Then, when a mobile device needs to communicate with the Roku, for example, it logs into the dedicated Roku SSID. This is annoying, but security and convenience have always been enemies. Also, you may run out of SSIDs. As I write this, the Surf SOHO can create only three SSIDs (plans are afoot to increase this).

If a particular device, such as a Roku box, can be totally isolated most of the time and only rarely needs to communicate with another device in your home, then you might have it totally isolated by default and just enable sharing within its VLAN on the rare exceptions when you need it (thanks to Zach for the idea). Of course, disable sharing when you are done.

Before leaving the fish tank analogy, any time the fish in a tank are allowed to see and interact with each other, a big fish may eat a small one.

**ISOLATION WITHOUT VLANS**

VLANs are only offered in professional grade routers. With consumer routers, there are two approaches that approximate VLAN segregation: Guest Wi-Fi networks and using two routers.

A **Guest Wi-Fi network** is *somewhat* isolated from the main network. I same "somewhat" because the isolation varies and may be configurable. The vast majority of consumer routers offer a single Guest network; some offer one on each Wi-Fi frequency band (2.4GHz and 5GHz). In contrast, a router that supports VLANs will probably let you create dozens of them. Also, Guest networks are Wi-Fi only, VLANs can also exist on wired Ethernet connections.

To illustrate how the isolation offered by a Guest network varies across vendors: when configuring a Guest network on a TP-Link router [(screen shot)](https://www.routersecurity.org/pix/TPLink.GuestWifi.isolation.jpg) there is a checkbox for "Allow guests to see each other". TP-Link Guest networks also have a checkbox to "Allow guests to access my local network." Google Wi-Fi has no hard barrier between the Guest and private networks. The system supports shared devices, a feature that [can not be disabled](https://support.google.com/wifi/answer/6340375?hl=en). Asus offers a choice as you [can see here](http://demoui.asus.com/Guest_network.asp). I am pretty sure that the "Access Intranet" option breaks down the wall between Guest and private devices. Netgear is confusing. Their article [How do I set up a guest network on my Nighthawk router?](https://kb.netgear.com/24097/How-do-I-set-up-a-guest-network-on-my-Nighthawk-router) says nothing about this, but others have seen an option to "allow guests to access my local network" This [PC Magazine article](https://www.pcmag.com/how-to/10-ways-to-set-up-your-wi-fi-for-guests) has a [screen shot](https://i.pcmag.com/imagery/lineupitems/021NWZr9DEUuVi7DioFrd7b.1574731929.fit_lim.fit_lim.size_1091x99999.jpg) of a Netgear router with an option to "Allow guest to see each other and access my local network." Eero has no sharing options for a Guest network. Trendnet has [two options:](https://routersecurity.org/pix/trendnet.guestnetwork.config.jpg) "Wireless client isolation" and "Internet Access Only". The Synology RT2600ac offers two Guest networks, but they share the same subnet, so they are not isolated from each other. You can learn more about Synology Guest networks in [my review](https://www.routersecurity.org/synology.php#guestwifi). D-Link has an option to "Enable routing between Zones" which you can see in this [screen shot](https://i.kinja-img.com/gawker-media/image/upload/xg5ppafqpphkqdim0lfh.jpg) from this 2016 [Gizmodo article](https://gizmodo.com/how-to-give-guests-to-access-your-wi-fi-without-exposin-1777526975).

Peplink does not offer Guest Wi-Fi networks per-se, but it does offer two isolation options. To prevent devices on the same Wi-Fi network (SSID) from seeing each other, you can enable "Layer 2 isolation". If a Wi-Fi network is assigned to a VLAN, you can isolate that VLAN from all other devices connected to the router by disabling "Inter-VLAN routing."

The other option, using **two routers**, should offer total isolation. In this case, you connect the WAN/Internet port of the inner router to a LAN port of the outer router. The outer router is either connected to a modem or is a combination modem/router device. The firewall of the inner router isolates it from all the devices connected to the outer router. For someone working from home this is a fairly secure way to isolate their work devices from everything else in the home. One downside to this approach is that it does not scale. Another is that there will be no option to isolate devices connected to the inner router from each other.

**SIMPLE AND COMPLEX VLAN EXAMPLES**

The fish tank in the previous analogy can be thought of as the boundary or scope of a VLAN. Stepping out of the analogy, the scope of a VLAN actually consists of Wi-Fi networks (SSIDs) and Ethernet ports. On the simplest level a VLAN can consist of a single SSID or a single Ethernet LAN port. You can mix and match too.

1. An easy way to start with VLANs is to assign an SSID to a VLAN
2. Another simple setup is to assign a LAN port to a VLAN that consists of just that one port
3. As a next step, you could take multiple LAN ports and group them into a VLAN
4. Or, you could put some Ethernet ports and an SSID into the same VLAN
5. The most complex setup involves a VLAN enabled smart switch, plugged into a LAN port

Type 1 is basically a Guest Wi-Fi network on steroids. The devices using that SSID will be walled off from all other devices connected to the router (assuming that inter-VLAN routing is not allowed). You might use one such isolated SSID for actual guests/visitors and another one for IoT devices such as a Roku box, an Apple TV, an Amazon Echo, a Nest thermostat or an Internet radio. This way you can change the Guest network password without impacting the IoT devices. And, the Guest network can be disabled when its not needed.

As an example, of Type 2, I use a VOIP service that provides a small telephone adapter box. One end plugs into a LAN port on my router and the other end plugs into a land-line telephone. The Ethernet port used by the telephone adapter is in its own, really tiny, VLAN.

Roommates could use Type 4. Each person could have their own SSID and two LAN Ports assigned to their personal VLAN. In effect, this chops the router in half and never the twain shall meet. Likewise, someone who works at home could use type 4 as a way to isolate the computers/printers/etc that are used for work from all the other devices in their home. Someone who works at home and wants the best possible security might use type 3 and limit themselves to 2 or 3 LAN ports and avoid Wi-Fi altogether.

**OVERKILL?**

Are VLANs overkill?

* It has been suggested a billion billion times to use a VPN on public Wi-Fi networks. But, VPNs offer no protection from malicious devices on the same Local Area Network (LAN). Neither does TOR. Windows machines, especially, have a history of being compromised by a LAN side attack, no Internet needed. The [WannaCry ransomware attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack) in May 2017 was an example of this.
* Firewalls protect devices on a LAN from outside attack. The Network Isolation I am suggesting here protects devices on a LAN from inside attack. For more on testing the firewall in your router see the [Test your router](https://www.routersecurity.org/testrouter.php) page.
* If you have done an NMAP scan of all 65,500 (or so) TCP ports, and another scan of the 65,500 (give or take) UDP ports that your laptop or tablet might have open to the LAN, and, you can explain and understand what each port is doing, and you are not worried about bad guys in the coffee shop abusing the service behind these open ports, then it is overkill. Everyone else would benefit from Network Isolation.

**VLANs IN THE NEWS**

Need some convincing before bothering with VLANs? See some stories in the news about bad things that a VLAN would have prevented.

**TECHIE INFO**

On a more technical level, each VLAN gets its own subnet (sub-network). So, one VLAN might use IP addresses in the 10.1.1.x range and another VLAN would use IP addresses that start with 10.2.2.x. Each VLAN also gets its own DNS servers. They are, as the name implies, virtually LANs. All your VLANs can use the same DNS servers, or, each VLAN can use different DNS servers. If, for example, you put devices used by children into a VLAN, then that VLAN can use DNS servers that block porn. I am working on a page about DNS servers, but its only partially complete. This is a hobby, what can I say.  
NOTE: IF DNS forwarding is enabled, then the router forces all DNS queries to be answered by the router itself. This [over-rides the DNS servers](https://forum.peplink.com/t/question-problem-having-a-vlan-with-its-own-dns-servers/15162/2) specified for a VLAN.

To help you keep track of your VLANs, the Surf SOHO lets you assign each VLAN both a name and a number. Some useful names might be IoTvlan, VOIPvlan or GuestVLAN. VLAN numbers should be between 2 and 4,094.

VLANs do not get their own passwords. If you assign a Wi-Fi network to a VLAN, nothing about the Wi-Fi password changes. Ethernet ports that are assigned to a VLAN are not password protected.

**VLAN SUPPORT**

Many routers can offer *some* isolation but the feature is often disabled and limited in scope.

Support for VLANs is rare. Hardly any consumer routers support VLANs. None of the consumer oriented mesh routers support it. My recommended router, the [Pepwave Surf SOHO](https://www.routersecurity.org/pepwavesurfsofo.php), fully supports VLANs, but it is an advanced feature and disabled out of the box. You have to know a secret handshake (see below) to enable VLANs on the Surf SOHO.

The high end Synology RT2600ac, which seems to offer every feature ever invented for routers, does not support VLANs (according to the [user guide for SRM version 1.2](https://global.download.synology.com/download/Document/UserGuide/SRM/1.2/Syno_UsersGuide_Router_enu.pdf)).

The isolation offered by the RT2600ac is a hodgepodge. On a non-Guest network, devices may or may not be able to communicate with each other depending on an AP Isolation option. The manual does not address sharing between Ethernet devices and non-Guest Wi-Fi users. On a Guest network, devices on the 2.4GHz band can not see devices on the 5GHz band. The manual wasn't clear as to whether AP Isolation was available for Guest networks within one frequency band. And, like many routers, Guest devices can access non-Guest devices if you so choose.

I don't mean to downplay Guest networks, they are a great security feature, even without full network isolation. Having a different password from the main Wi-Fi network lets you periodically change the password so that Guests don't get a permanent pass. Guest networks can also be disabled when they are not needed. And, they can offer *some* isolation of Guest users/devices.

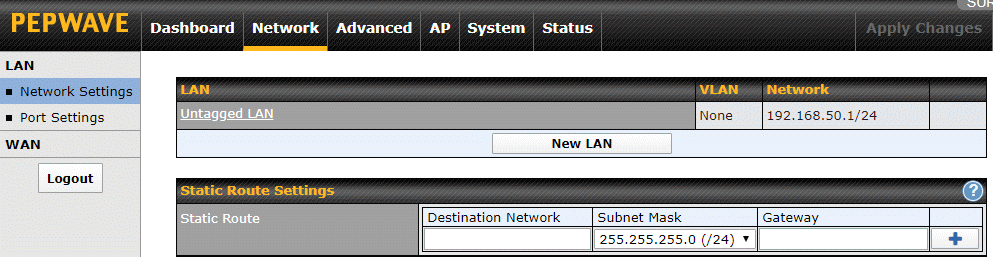
That said, many consumer routers offer just one guest network and I don't think that's enough. For example, I suggest having one Wi-Fi network for devices that need to see other devices, one for actual guests or visitors and another for IoT devices. Parents with small children, may also want to isolate devices used by the kids.

**THE TOTAL REVERSE**

While this page focuses on giving a computing device access to the Internet and *nothing* else, sometimes we need the reverse. That is, we want a device to be accessible locally but not have access to the Internet. The firewall in any router should prevent incoming access from the Internet, at least as long as UPnP is disabled. A router that supports firewall rules, will let you block the device from making any outgoing connections to the Internet. No phoning home for ET. Needless to say, my preferred router, the Pepwave Surf SOHO, supports outbound firewall rules. Generally speaking, consumer routers do not offer outbound firewall rules.

**PEPWAVE SURF SOHO VLANs**

To use VLANs on the Surf SOHO, you first define a VLAN (or two or three) and then you give the VLAN(s) a scope. By scope, I mean assign the VLAN to an SSID (Wi-Fi network) and/or an Ethernet LAN port. A VLAN that is defined but not assigned to anything can be deleted. A VLAN that has been assigned to either an SSID or a LAN port (or both), can not be deleted. The creation of VLANs starts at Network -> Network Settings (shown below).



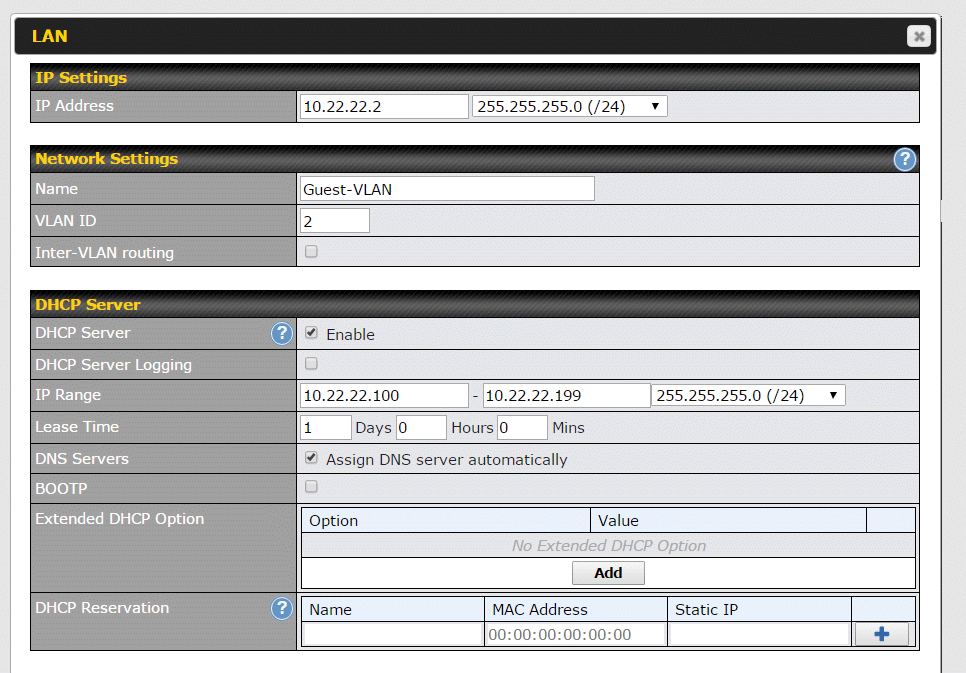
Before creating new VLANs, there are two changes I suggest making. As noted earlier, VLANs were not created for total network isolation and, by default, at least with Peplink routers, communication is allowed between different VLANs and non-VLAN devices (that is, stuff on the untagged LAN). So, click on "Untagged LAN" and turn off the "Inter-VLAN routing" checkbox. This will prevent devices that are not part of any VLAN (untagged devices) from any and all communication with whatever VLANs you create.

Next, I would give the "Untagged LAN" a more descriptive name. This is the default name for the group of devices that are NOT in any VLAN. The default name is technically correct; chunks of data (called packets or frames) transmitted on a network with VLANs have an extra tag that identifies the VLAN each chunk/packet/frame belongs to. Devices that are not part of a VLAN do not have their network packets tagged. I suggest changing the name just because it is not helpful for people who are not experts at networking.The name you choose can be anything that makes sense to you. Consider something like PrivateLAN or PrivateNetwork or MikeysPrivateLAN. Then click the gray Save button at the bottom of the window and, again, Apply Changes.

In Firmware 7, support for VLANs was disabled out-of-the-box. In firmware 8, the ability to create VLANs is enabled by default.

Firmware 7 only: To enable VLAN support do Network -> Network Settings. In the "IP Settings" section at the top of the page, click on the white question mark in the blue circle. A small window pops up saying "If you need to define multiple VLANs, press here". Click on the word "here". A second window pops up that says "The LAN settings will be switch to advanced mode with VLAN support. Are you sure?" CLick on the Proceed button. Then, click on Apply Changes. This takes you back to the main Dashboard page.

Go to Network -> Network settings again. The gray button labeled "New LAN" really should say "New VLAN". Click the "New LAN" button to define a new VLAN and you will see the screen below (it looks exactly the same in firmware 7 and 8).



Previously I mentioned that each VLAN gets its own subnet (sub network or range of IP addresses), name, number and DNS servers. This is where we assign these attributes. It is also where we control whether the VLAN can talk to other VLANs and whether devices in this particular VLAN can see each other. Assigning most of these attributes is easy, assigning the subnet requires some techie knowledge.

The first field (IP Address) is not one I mentioned before. It is the IP address of the router, as seen from this VLAN. This is part of defining the subnet that the VLAN will use. In the example above, the VLAN is using the 10.22.22.x subnet. This means that all devices in that VLAN will have IP addresses that start with 10.22.22. All devices. Even the router itself. The first field is where you give the router an IP address in the new subnet used by the new VLAN. In the screen shot above, it is device number 2. For nerds, this is interesting. From the main network (untagged LAN), the router is addressed as 192.168.50.1 (using Peplink defaults), but from this new VLAN/subnet, it will be addressed as 10.22.22.2.

Why 2? Why not assign 10.22.22.1 to the router? Most people use 1. It is best to avoid an IP address that ends with 1 or 254. For more on this, see the [IP address](https://www.routersecurity.org/ipaddresses.php) page.

The field next to the router IP Address is complicated. However, the value shown (255.255.255.0/24) should be fine in almost all cases. It means that the subnet used by this VLAN can have a maximum of 255 devices (numbered 0 through 254). If nerds ask, this is a subnet mask.

Another subnet related field is the "IP Range" in the DHCP Server section.

All computing devices on a network need a unique number. Here we are dealing with IP version 4 numbers/addresses. Devices can either be configured to always use a specific IP address/number or be assigned one on a temporary basis when they join a network. Most of the time, devices use temporary IP addresses assigned by the router. The router itself is an exception, it has a fixed, static IP address that we *just* configured. The system that loans out temporary IP addresses is called DHCP.

In the example above, devices that don't have a fixed IP address will be assigned one ending in 100 through 199 (10.22.22.100 through 10.22.22.199). This implies that we can use fixed/static IP addresses between 1 and 99 and between 200 and 254 for devices that need one that never changes. A network printer, for example, is best assigned a fixed IP address. This range of temporary IP addresses was an arbitrary choice, it could just as well have been 100-250 or 30-252. The lowest number can not be lower than the number given the router. The highest number is 254.

That's the **hardest part**. Now, it gets easier.

The name of the VLAN goes in the Name field (see, easier). In the example, the name is Guest-VLAN. The name should be whatever makes sense to you based on who or what will be using this VLAN. If you intend to use the VLAN with a single SSID, then perhaps name it after that SSID. For example, the VLAN for SSID "michael" might be called "michaelsvlan". A VLAN for IoT devices might be called IoTvlan. Personally, I have a VLAN that consists of a single Ethernet LAN port used by a VOIP telephone adapter. I call it VOIPvlan. It is not clear how long the name can be or what characters are allowed/disallowed, so don't go crazy.

In addition to names, VLANs are also assigned numbers. The important attribute of the number seems to be that it is unique. Peplink refers to the number as a "VLAN ID" but its a number.

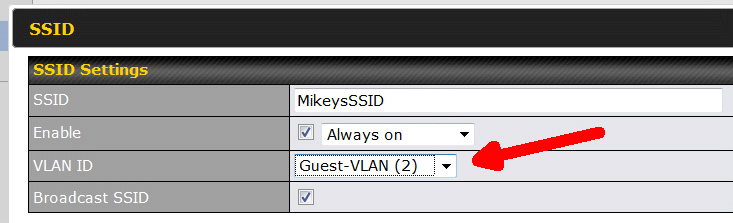
The number does not have to be related to the subnet, but being neat simplifies things. For example, you *might* assign the VLAN using the 10.2.2.x subnet number 2. Or, if you like 192.168 subnets, then consider assigning the number 4 to the 192.168.4.x subnet and 8 to the 192.168.8.x subnet. VLAN numbers do not have to start at 1 and do not have be consecutive. In the Peplink manual they name the VLAN after its number. VLAN number 2, for example, is called VLAN2. Boring.

The next field, "Inter-VLAN routing" is why you are reading this page. Turn this **off** (it is on by default in firmware 8). With this disabled, devices in this VLAN can *not* access anything outside of their VLAN. Even if some other VLANs want to share stuff, this VLAN will not come to the sharing party. Disabling this does not block access the Internet.

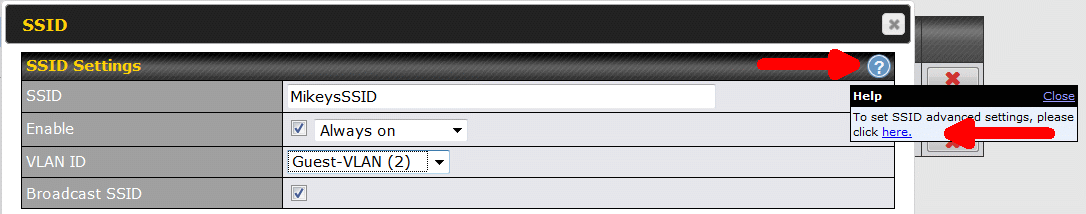
I suggest enabling the DHCP server and disabling (not checking) DHCP Server logging. These can always be changed later. A Lease Time of one day (the default) should be fine. This is how long a device can use an IP address before it has to go back to the router and ask for another one. Opt to assign DNS servers automatically and do not check Bootp. There is no need to deal with the Extended DHCP option or DHCP Reservation.

When done, click the SAVE button at the bottom of the window and then Apply Changes, yet again.

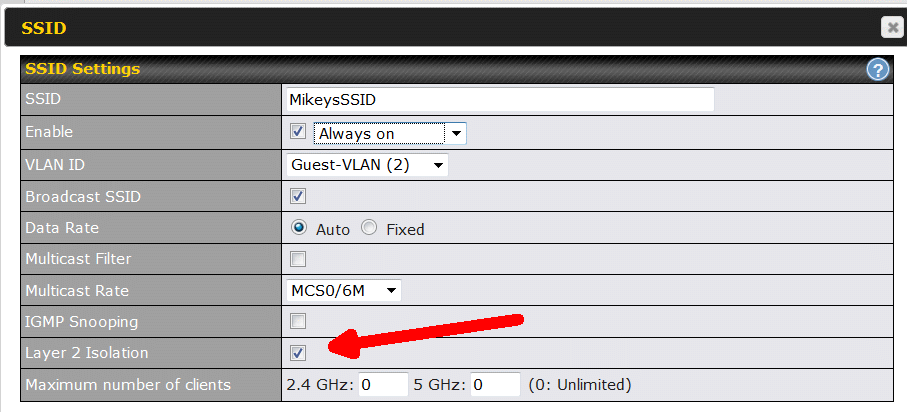
To assign our newly minted VLAN to an SSID, go to AP -> Wireless SSID and click on the SSID name. As shown below, click on the drop down list box in the VLAN ID field. VLANs are identified here both by name and by number.



At this point, you do not see the option that isolates devices on this SSID/VLAN from each other. The router defaults to a simple mode and you need to know the secret handshake to see the advanced settings. As shown below, the secret handshake is the white question mark in the blue circle. You need to click it, and then click again, where instructed (see below).



Now you should see a checkbox for "Layer 2 isolation" as shown below. This is what isolates devices within this one VLAN/SSLID.



Be sure to click the Apply Changes button on the top of the screen, when you are done making changes.

At this point, you have a single, *totally* isolated, SSID. Congratulations.

The Surf SOHO allows for more than one isolated SSID. Simply create another VLAN for the second wireless network. The Surf SOHO can create a maximum of eight SSIDs.

PENDING QUESTION: If a VLAN is assigned to two LAN ports and a single SSID that has Layer 2 isolation enabled, can devices plugged into the LAN ports see the wireless devices? Can the wireless devices see the Ethernet devices? Can the Ethernet devices see each other? I don't yet know....

**ETHERNET PORTS**

When assigning Ethernet ports to a VLAN, you are presented with a choice that the User Manual does not explain - whether the LAN port is "Access" or "Trunk". Access mode used to be the default, as of firmware v8, Trunk is the default. Access is the simplest case and thus I suggest starting with it.

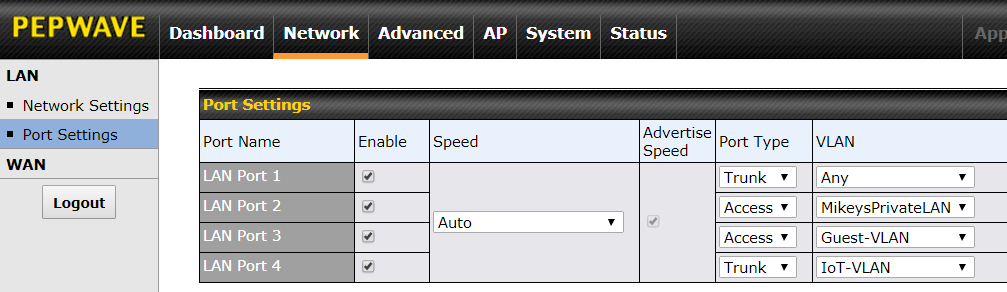
Recall from earlier, that network packets/frames that are part of a VLAN are "tagged" with the identifier of that VLAN. Most devices plugged into an Ethernet LAN port (laptop computer, desktop computer, VOIP telephone adapter, network printer, stereo receiver, Roku box) do not understand VLANs so the responsibility of tagging stuff falls to the router. In this case, the LAN port type should be Access.

A device that does understand VLANs would be a smart switch. Smart switches are step up from dumb switches and a step down from a router. When a smart switch is plugged into a LAN port, then the type should be Trunk. This tells the router not to bother adding VLANs tags, the smart switch has already done so.

The [Netgear GS105E](https://www.netgear.com/support/product/GS105Ev2) is a smart switch with 5 Ethernet ports and VLAN support. It cost about $40 in January 2018 and from $40 to $55 in March 2020.

Whatever device is plugged in to a LAN port of type ACCESS, is assigned the profile you specify here. In the screen shot below, anything plugged into LAN port 3 will be assigned to the Guest VLAN and anything plugged into LAN port 2 will not be assigned to any VLAN. I use "MikeysPrivateLAN" as the name of my non-VLAN untagged network. An Ethernet-only network printer would belong in LAN port 2.

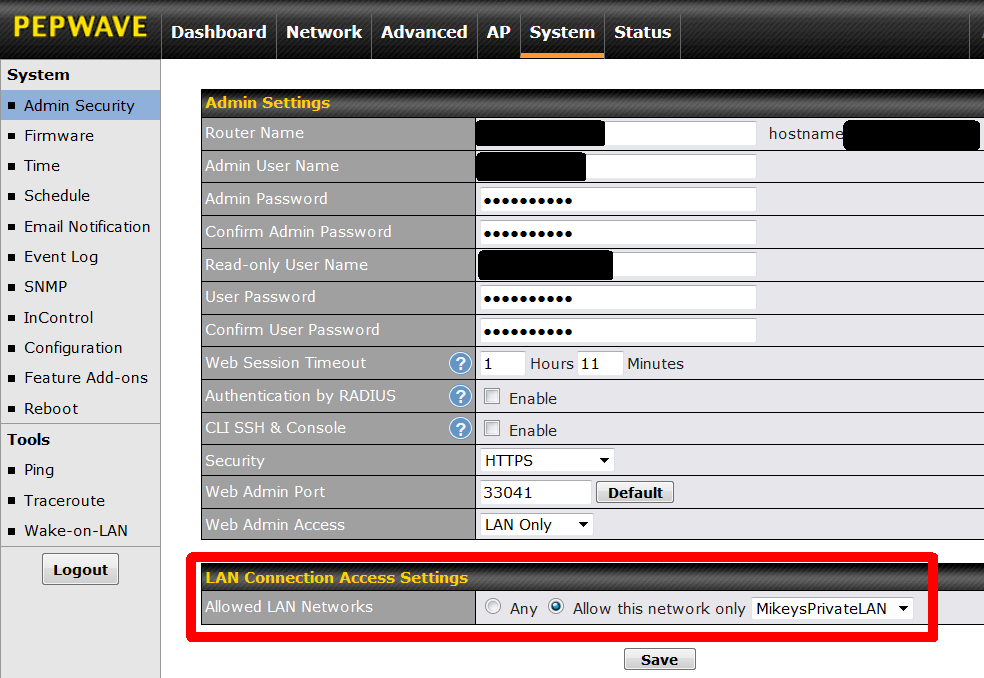
TRUNK ports are more complicated. The smart switch plugged into a TRUNK port can send data for multiple VLANs, depending on how its configured. But, the router is not bossed around by the smart switch. You can control which VLANs the router will accept from the smart switch. In the screen shot below, LAN port 1 allows the smart switch to send data for any VLAN, while LAN port 4 will only accept data for the IoT VLAN from the smart switch that is plugged into it.



**FINAL NAIL**

The final nail in the total isolation coffin, is limiting the VLANs that can login to the router's web interface. For the best security, restrict router access to the private network. That is, prevent all VLANs from having direct access to the router.

To do this, go to System -> Admin Security -> Allowed LAN Networks (see below).



The "Allowed LAN Networks," defaults to Any which means users on all VLANs can login to the router. In the screen shot above, this has been changed and only MikeysPrivateLAN is allowed access to the router. Continuing the earlier example, this prevents anyone on the 10.22.22.x subnet/VLAN from logging on to the router using IP address 10.22.22.2. They won't even be able to view the logon page. After changing this, click the SAVE button, then the APPLY CHANGES button.

Continuing with the previous screen shot, the one in the Ethernet Ports section above, this means a computer plugged into LAN port 2 (MikeysPrivateLAN) can access the router, while one plugged in to LAN ports 3 (Guest-VLAN) and 4 (IoT-VLAN) can not.

Interestingly, this setting also blocks the Peplink mobile app from talking to the router, if the app connects to an SSID/VLAN that is not allowed in. Learned that the hard way.

- - - - - -

The competition: [Creating Isolated Networks with Ubiquiti UniFi](https://vninja.net/2019/08/08/creating-isolated-networks-ubiquiti/) by Christian Mohn (August 2019). Ubiquiti has two VLAN configuration options, Network purpose and Network Group, that its not clear to me what they are/do. Ubiquiti can not assign names to VLANs. Isolating a VLAN requires firewall rules rather than a single checkbox.

The competition: Mike Potts documented on GitHub [Using the Ubiquiti EdgeRouter X and Ubiquiti AP-AC-LR Access Point](https://github.com/mjp66/Ubiquiti) to create VLANs for each of 3 LAN ports and three different SSIDs. Here is an [overview in PDF format](https://github.com/mjp66/Ubiquiti/blob/master/Ubiquiti%20Project%20Brochure.pdf). The heart of this is a 105 page PDF document with the full instructions. Compare that to this page. Seems much more complicated than the Surf SOHO (or any Peplink router). For example, look at all these [firewall rules](https://github.com/mjp66/Ubiquiti/blob/master/show%20configuration%20commands.txt). Ugh. The EdgeRouter X is about $50 and the Access Point is about $100, so its roughly $50 cheaper than a Surf SOHO. That said, there are many costs other than financial. For example, Mr. Potts said "The only trouble with this router is that it is meant for professionals to use. You have to scrounge around forums for postings on how to configure specific items." Peplink routers are also targeted at professionals, yet the user interface is fairly easy to use.

A Pepwave Surf SOHO limitation: This Feb. 2019 [Forum question](https://forum.peplink.com/t/inter-vlan-bonjour-on-surf-soho-mk3/20367) asks: "I have segregated printers into a separate VLAN. To make them broadly accessible from other VLANs with iOS devices (etc), I need to enable Inter-VLAN Bonjour ... How do I enable Bonjour on the SOHO MK3?". You can not. Bonjour forwarding is only supported on the higher end Balance and HD routers.

- - - - - -

**EXTRA CREDIT**

This is unlikely to happen often, but understanding the question shows a good grasp of things.

A regular [switch](https://www.netgear.com/business/products/switches/unmanaged/) (as opposed to a smart switch or a managed switch) is a relatively dumb Ethernet-only device that takes chunks of Ethernet data (packets/frames) in on one port and sends it out another port. Conceptually, a switch is the opposite of the network isolation described above on this page. Rather than prevent devices from seeing each other, it always lets all connected devices see each other. That's its job. That's why people buy switches. So, what do you think happens when worlds collide?

Suppose the Surf SOHO has a LAN port port assigned to an isolationist VLAN. That is, the VLAN has Layer 2 Isolation enabled and it is not allowed to talk to any other VLANs. Any device directly plugged into that LAN port can only see the Internet. It will be blissfully ignorant and shielded from other devices using the router. That's easy.

But, what if you plugged a switch into that LAN port? What then of the devices plugged in to the switch? Can they see each other as per the switch or can they not see each other as per the router and the isolationist VLAN assigned to the LAN port? When the router and the switch arm wrestle, who wins?