

Networking for the Home/Ham Shack

- **High Level Overview of Networking**
- **Typical Home Network**
Tablets, PCs, IoT devices, Cameras, Weather Stations, Garage Door Openers, Door Bels, etc...
- **Typical Ham Network**
Same as the Home Network plus Control of radios, Antenna Match Boxes, Antenna Switching, Rotor Control, DSTAR, DMR, P25, Yaesu Digital (C4FM), etc ..
- **Security Of The Network**
- **Three Dumb Routers**

This overview is not going to cover

- 1. Setting up a server**
- 2. TCP Protocol**
- 3. UDP, Streaming Protocols**
- 4. Public Network Switching**
- 5. ISPs (Vendors)**
- 6. Ports, Port forwarding, etc...**
- 7. IPv4 and IPv6 addressing**

Early Home Networking

In the mid 1990's, a typical home network used dial up and later on, graduated to DSL for connection to the Internet.

Largely, the landline phone companies provided the direct connections. The typical user had only one device connected to the Internet.

Typically, at home the use of more than one device connected to the Internet did not start until the late 1990's

Security was not considered a major problem. "Who would want to hack my home network", was thought by many. Many didn't know their networks were not secure. After all, a wired Network is the most secure.

Wide usage of WiFi did not start until 2000 without any security. In 2003, people started having their WiFi protected. Using WEP. Now using WPA2 & WPA3.

In the early 2000's people started connecting multiple devices to their home network(s). Not just PCs.

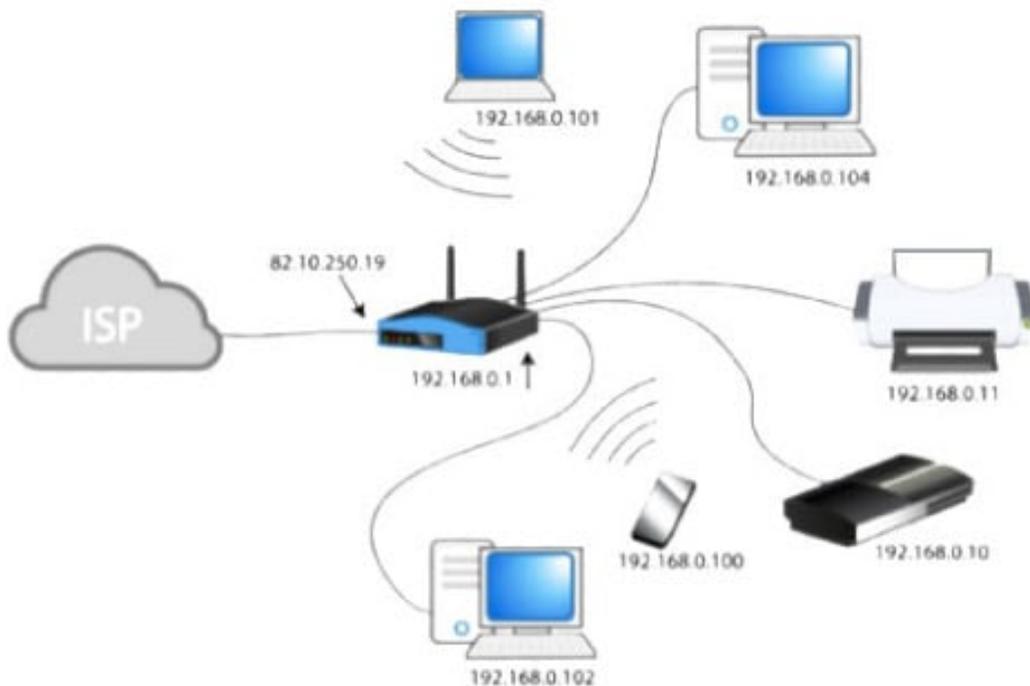
With WiFi and multiple connections, along came the use of routers and network Switches at home.

Routers

A Router is a device that allows the Public Internet (WAN) conversion to the Private Local Network (LAN)

Typically, a router provides firewall protection, address translation and sometimes WiFi

Each brand of router is unique with customized setup instructions. **Do NOT rely on the Router's Out of Box setup.** Change the User name and Password OF THE ROUTER WHERE POSSIBLE.



Note: The WAN (Public 82.10.250.19) and LAN (Private 192.168.0.nnn) addressing

Did you know you have a private IP address?

Reprint from <https://whatismyipaddress.com/private-ip>



If you were searching for information on an IP address such as 192.168.1.1 or 10.0.0.1, you're on the right page. Because you're about to learn something that confuses almost anyone trying to learn about IP addresses.

But if you read on, you'll see it doesn't have to be confusing.

This article is about what private IP addresses are. Before you learn about private IP addresses, you will also need to know about *public* IP addresses, which you should know a little about already if you're reading this article. *Lucky for you, that's something fairly easy to explain.*

The IP address you see on our [home page](#)—that looks like this—24.156.99.202, is an example of a public IP address. If you've ever wondered "*what is a public IP,*" now you know. It's that simple.

Now, about that *other* kind of IP address...

What's a Private IP address?

Home routers have their local address set to a default, private IP address number. It's usually the same address for the other models from that manufacturer, and it can be seen in the manufacturer's documentation.

Who knew?



Actually, you should welcome your private IP

Here's a look at the default private (also called "local") IP addresses for popular brands of routers:

- Linksys routers use 192.168.1.1
- D-Link and NETGEAR routers are set to 192.168.0.1
- Cisco routers use either 192.168.10.2, 192.168.1.254 or 192.168.1.1
- Belkin and SMC routers often use 192.168.2.1
- A good procedure is to change the default IP addresses of the LAN. This keeps the bad guys guessing.

Let's go back to public IP addresses for a second...

How you connect to the world.

Your public IP address is the IP address that someone on the other end of your Internet activity would see (if they bothered to look for it). That's the only reason it's known as a *public* IP address.



With traditional mail, when you send a letter, you have to know the address to send it to—such as “1234 Main Street,”—so that the postman knows which street and which house to take it to.

The Internet works similarly, except it directs *your* personal activity (emails, answers to Google inquiries, etc.), and forwards the electronic messages to your computer's address.

You couldn't do much without a public IP address. It's your passport to the Internet.

Public and Private. Working together to get you connected.

In theory, your computer must have its own unique IP address so that it will only receive the information that is meant for you.



However, that's not how it works out, because of one major exception—network computers that are linked to a router and share the same public IP address.

Yes. If you have a router, you have a private IP address.

And here's how it works...

Reserved for private networks.

The organizations that distribute IP addresses to the world reserves a range of IP addresses for *private networks*.

- 192.168.0.0 – 192.168.255.255 (65,536 IP addresses)
- 172.16.0.0 – 172.31.255.255 (1,048,576 IP addresses)
- 10.0.0.0 – 10.255.255.255 (16,777,216 IP addresses)

Your simple home network, with its router at the center and computers connected to it—wired or wireless—classifies as one of those networks.

Your router—once it makes its Internet connection through your Internet Service Provider—sends Internet activity to any computer connected to your router, and is the basis of a networking innovation called a Network Address Translation (NAT).

- NAT is a process in which your router changes your private IP Address into a public one so that it can send your traffic over the Internet, keeping track of the changes in the process.
- When the information comes back to your router, it reverses the change—from a real IP address into a private one—and forwards the traffic back to your computer.

In other words, the router connects to the other devices (usually desktops, laptops and tablets).



Your private IP is just that. Private.

That's the point: Your private address is just for your router, your network, and you.

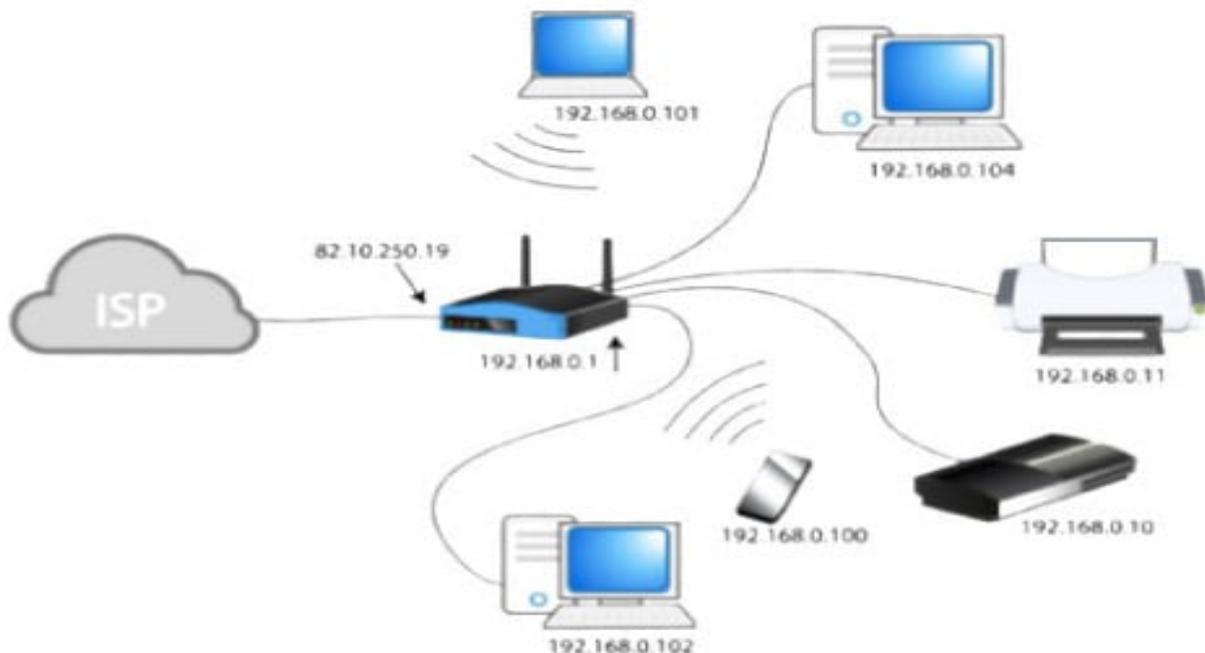
The private address ranges in a network don't have to be synchronized with the rest of the world and the Internet.

As a matter of fact, the private address range can be used by more than one address. A network administrator using these private addresses has more room for subnetting, and many more assignable addresses.

The private IP address does one job for your home network.

These blocks of addresses can be used by a private network. Even if your neighbor is using the exact same addresses, it won't cause a problem, because that's HIS or HER network, not yours. Don't let that confuse you.

You see, these private addresses are known as *non-routable addresses*. The networking on the Internet routes Internet activity connected to your public IP address only, not your private IP.



How Private and public IP addresses work together

This is the end of <https://whatismyipaddress.com/private-ip> article.

More helpful info can be found at
<https://whatismyipaddress.com/?s=how+a+router+works>

NOTE: If you want to know your “Public” address, enter
<https://whatismyipaddress.com> into a browser. You may be surprised.

Types of Internet service Providers (ISPs)

The type of Internet service you choose will largely depend on which **Internet service providers** (ISPs) serve your area, along with the types of service they offer. Here are some common types of Internet service.

- **Dial-up:** This is generally the slowest type of Internet connection, and you should probably avoid it unless it is the only service available in your area. Dial-up Internet uses your **phone line**, so unless you have multiple phone lines you will not be able to use your landline and the Internet at the same time.
- **DSL:** DSL service uses a **broadband connection**, which makes it much faster than dial-up. DSL connects to the Internet **via a phone line** but does not require you to have a landline at home. And unlike dial-up, you'll be able to use the Internet and your phone line at the same time.
- **Cable:** Cable service connects to the Internet **via cable TV**, although you do not necessarily need to have cable TV in order to get it. It uses a broadband connection and can be faster than both dial-up and DSL service; however, it is only available where cable TV is available. Speeds between 50 Mbs and 1000 Mbs are common.
- **Satellite:** A satellite connection uses broadband but does not require cable or phone lines; it connects to the Internet **through satellites orbiting the Earth**. As a result, it can be used almost anywhere in the world, but the connection may be affected by weather patterns. Satellite connections are also usually slower than DSL or cable.
- **4G and 45:** 4G and 5G service is most commonly used with mobile phones, and it connects **wirelessly** through your ISP's network. These plans are becoming available with high bit rates of 50 Mbs to 400 Mbs..

Choosing an Internet service provider

Now that you know about the different types of Internet service, you can do some research to find out what ISPs are available in your area. If you're having trouble getting started, we recommend talking to friends, family members, and neighbors about the ISPs they use. This will usually give you a good idea of the types of Internet service available in your area.

Most ISPs offer several tiers of service with different Internet speeds, usually measured in **Mbps** (short for **megabits per second**). If you mainly want to use the Internet for **email** and **social networking**, a slower connection (around 2 to 5 Mbps) might be all you need. However, if you want to **download music** or **stream videos**, you'll want a faster connection (at least 5 Mbps or higher). 100 Mbs service is considered slow by many cable ISPs.

You'll also want to **consider the cost** of the service, including installation charges and monthly fees. Generally speaking, the faster the connection, the more expensive it will be per month.

Although **dial-up** has traditionally been the **least expensive** option, most of the dial services have discontinued service due to lack of use and high cost keeping "Local Calling" available.

Hardware needed

Modem



Once you have your computer, you really don't need much additional hardware to connect to the Internet. The primary pieces of hardware you need are a **modem** and a **Router**..

The type of Internet access you choose will determine the type of modem you need. **Dial-up** access uses a **telephone modem**, **DSL** service uses a **DSL modem**, **cable** access uses a **cable modem**, and **satellite** service uses a **satellite adapter**. Your ISP may give you a modem—often for a fee—when you sign a contract, which helps ensure that you have the **right type** of modem. However, if you would prefer to shop for a **better** or **less expensive** modem, you can choose to buy one separately.

Router



Modems may include a wired router, a wireless router, or both

Sometimes, the ISP provides all of these functions along with a CABLE TV modem in one box.

I highly suggest, DO NOT RELY ON THE ISP's Router for security.

Again, a **router** is a hardware device that allows you to connect **several computers** and **other devices** to a single Internet connection, which is known as a **home network**. Many routers include **wireless** connections, which allows you to create a **home wireless network**, commonly known as a **Wi-Fi network**.

You **don't necessarily need to buy a router** to connect to the Internet. It's possible to connect your computer directly to your modem using an Ethernet cable. Also, many modems include a **built-in router**, so you have the option of creating a Wi-Fi network without buying extra hardware. If you do not use a router, at least always use the **PUBLIC** setting in Windows!!!! A coffee shop and McDonalds WiFi are an example.

Danger Will Robinson !!!

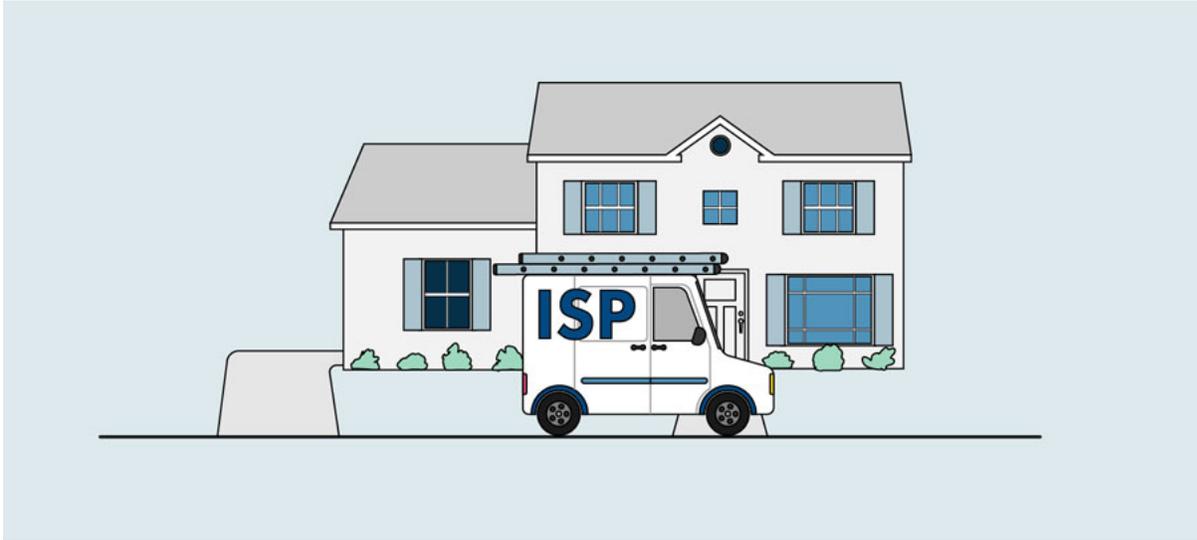
I strongly suggest you do not connect a device to the modem (Public network) directly **WITHOUT** the use of a router. Doing so is inviting the bad actors to knock down your front door.

This is very similar to leaving your front door open with a sign telling the burglars to help themselves.

Trivial Fact: Unprotected devices connected to the Internet (aka honeypots) on the average take 30 seconds to be compromised. See:

<https://thetack.technology/honeypot-time-to-breach-cloud-services/>

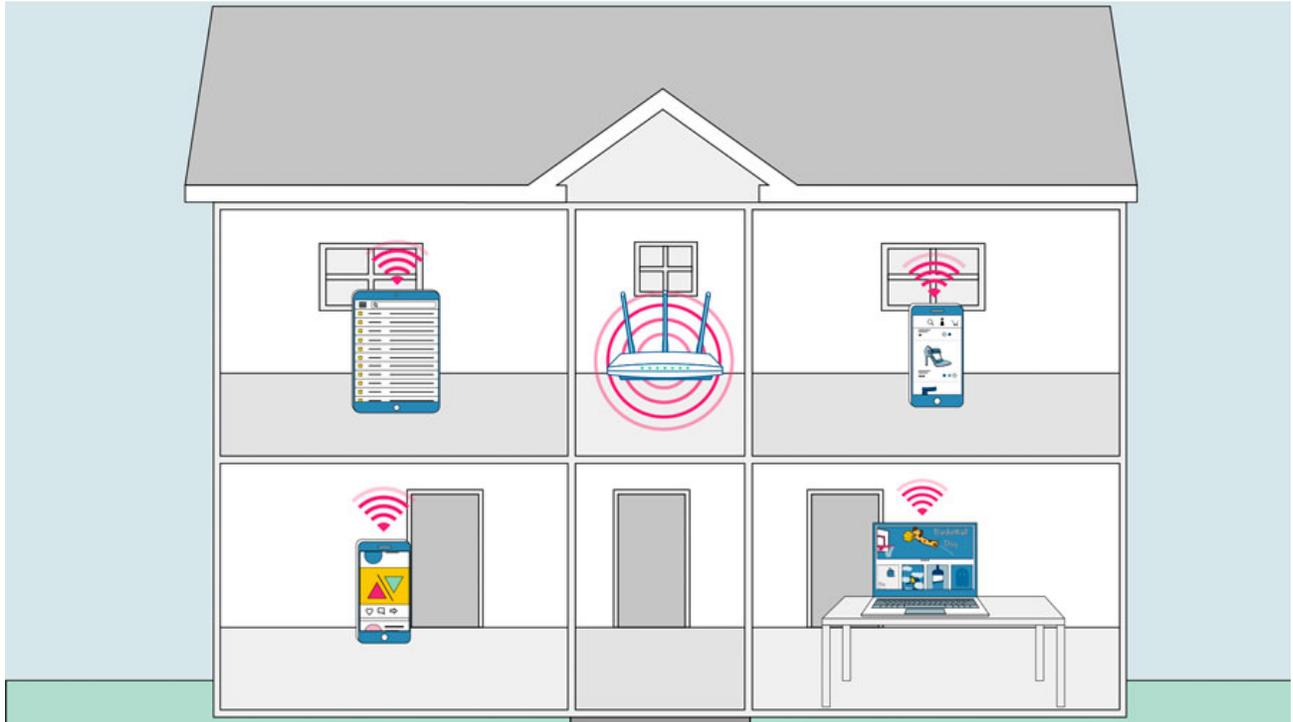
Setting up your Internet connection



Once you've chosen an ISP, most providers will **send a technician to your house** to turn on the connection. If not, you should be able to use the instructions provided by your ISP—or included with the modem—to set up your Internet connection.

After you have everything set up, you can open your **web browser** and begin using the Internet. If you have any problems with your Internet connection, you can call your ISP's **technical support** number.

Home networking



If you have multiple computers at home and want to use all of them to access the Internet, you may want to create a **home network**, also known as a **Wi-Fi network** or a **Wired Network** or a combination of the two. In a home network, all of your devices connect to your **router**, which is connected to the **modem**. This means everyone in your family can use the Internet **at the same time**.

Your ISP technician may be able to set up a home Wi-Fi network when installing your Internet service..

If you want to connect a computer that does not have built-in Wi-Fi connectivity, you can purchase a **Wi-Fi adapter** that plugs into your computer's USB port.

Getting started with the Internet

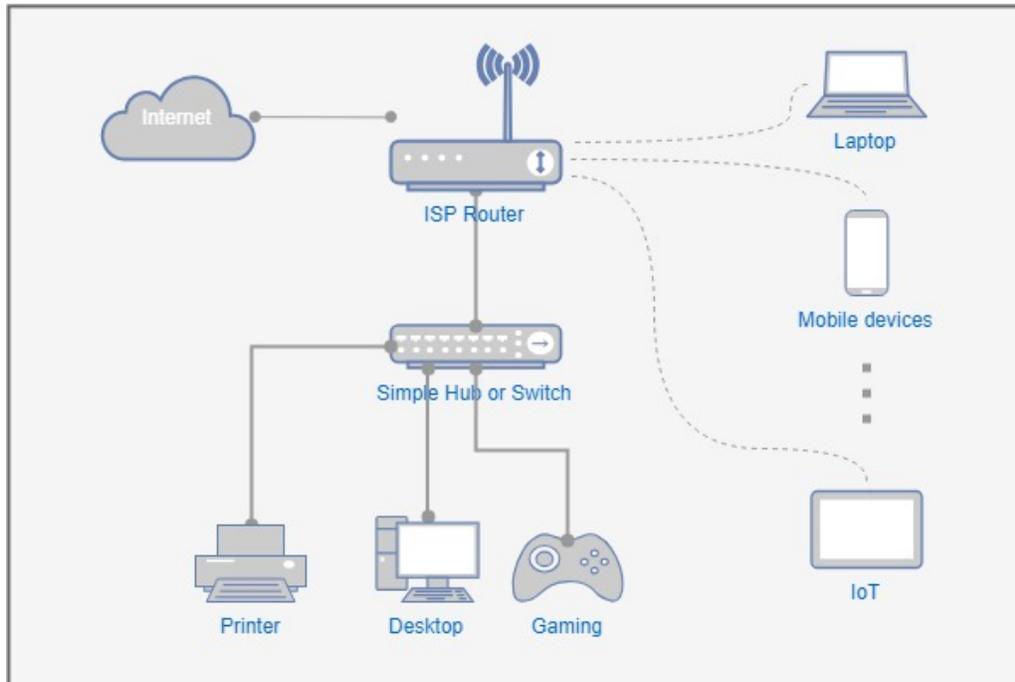
The Internet is a global network of billions of computers and other electronic devices. With the Internet, it's possible to access almost any information, communicate with anyone else in the world, and much more. You can do all of this on your computer.

Connecting to the Internet

A device has to be connected to the Internet before you can access it. If you plan to use the Internet at home, you'll usually need to purchase an Internet connection from an **Internet service provider**, which will likely be a phone company, Cable Company, or the government. Other devices usually connect through **Wi-Fi** or **cellular Internet** connections. Sometimes libraries, cafes, and schools offer free Wi-Fi for their patrons, customers, and students.

Typical Home Internet

A typical home network is a simple single network. A single network that allows connections (wired or wireless) from all computers, mobile devices, peripheral devices and Internet enabled devices like Internet of things (IoT).



Note: The shown ISP Router may be included with a Cable TV Modem. Some may have a separate modem and Router. The router may not have Wi-Fi. A separate Access Point (AP) may be required.

Risks of a single home network?

If anyone device is compromised or infected with malware, the attacker may be able to **spread malware or compromise your other devices**.

The attacker may also be able to sniff and eavesdrop on your network traffic to steal your critical personal information (e.g. login credentials).

Attacks do not necessary start at your most important devices. In fact, they usually start with devices that have the weakest security protection. Once they get their foot in a device, they can work their way to your other devices within the same network.

Your devices could be infected in several ways:

Internet of Things (IoT)

More and more devices, appliances and innovative things are Internet connected. But not all of them are created equal. Some could have very weak security protection or even no security protection.

These devices could be of high risk to your network. Incorporating IoT to your home network is a security nightmare.

IoT devices include Alexa, Cameras, doorbell cameras, alarm systems, refrigerators. Garage door openers, etc...

Addressing schemes of a router

There is a range for each of the three classes of IP addresses used for networking:

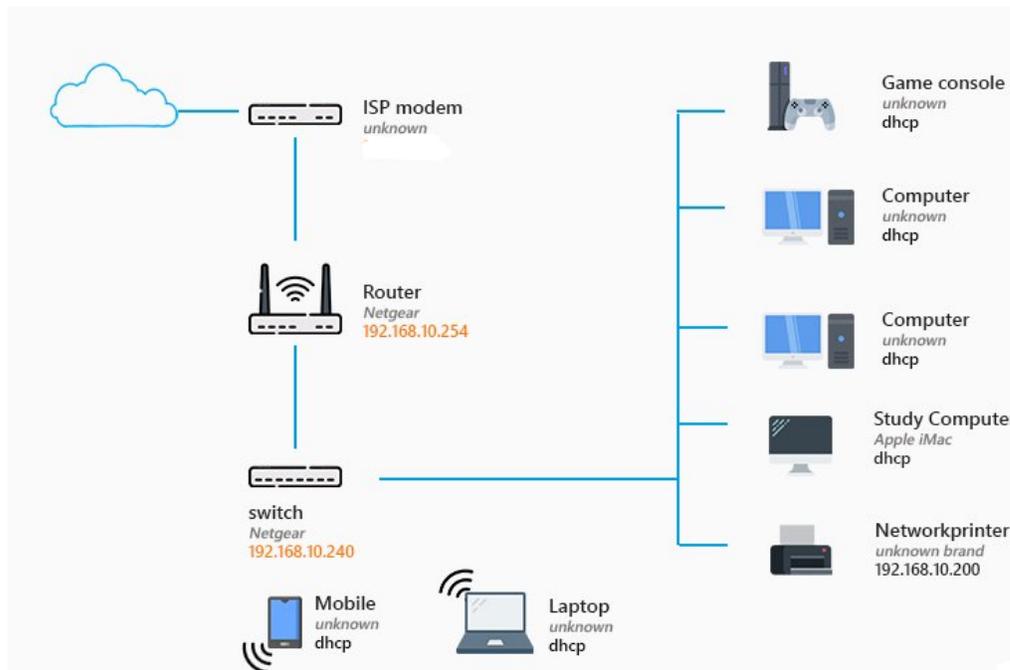
- Range 1: Class A - 10.0.0.0 through 10.255.255.255
- Range 2: Class B - 172.16.0.0 through 172.31.255.255
- Range 3: Class C - 192.168.0.0 through 192.168.255.255

The LAN side of the router uses one of these address classes.

The WAN side of the router is almost all the addresses not listed. Many addresses are unassignable by pursuant with industry standards bodies.

Typical Network Diagram with a router and switches:

Router Switch Network Diagram



Security of a Router and a Wi-Fi system

A router only protects the inside network from the outside world. This is to say it only allows **one way traffic in the outbound** direction unless it is specially configured.

The inbound traffic has to be invited (requested). Example, when you want to view a web page, your browser requests from the web site, the web page content. Your router correlates the data being received pursuant with your request and forwards it on to your PC or Device.

This is very important to remember.

The most secure connection is a wired connection. Try to use this method if possible. You will get security and higher network speeds.

Wi-Fi connections should never be run without encryption. In the beginning, WEP was the encryption standard. It has been hacked. Then came WPA2, it has been hacked. The new standard which is currently evolving is WPA3. This standard is being implemented in Windows, Linux, and the Apple products. WPA3 requires a new Wi-Fi transceiver on the Access point (AP) and the Client end (PC, iPad, iPhone, etc...).

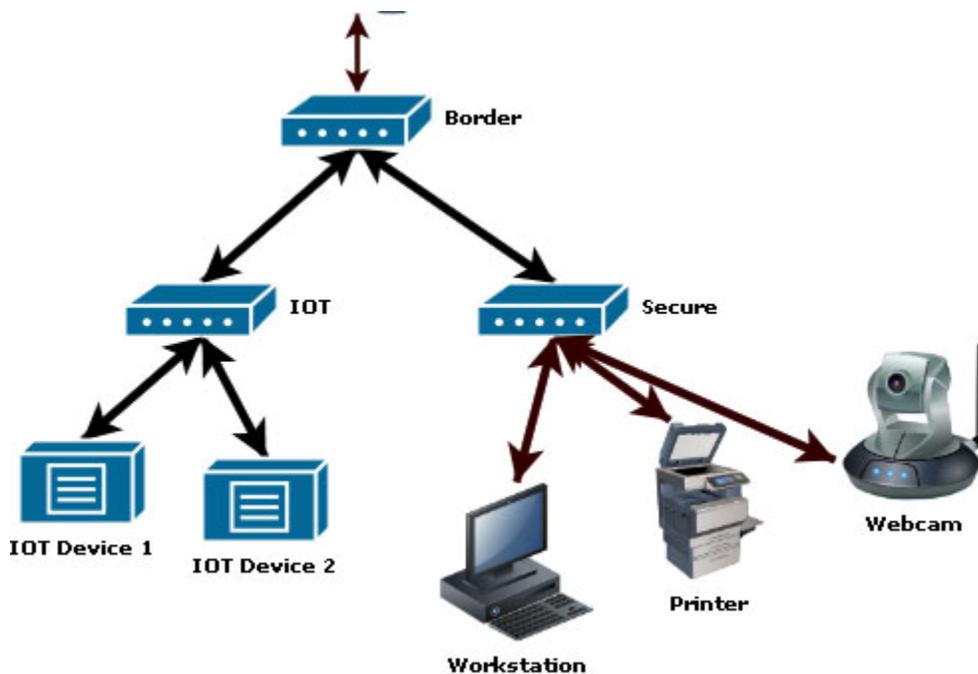
As a general rule, **DO NOT USE WPS (WiFi Protected Setup) on the Wi-Fi side of the networking.** WPS was supposed to make connecting to the network easier for a WiFi client.. Turn it OFF. Turn it on if and only if you must use it. Then turn it off immediately. WPS is so easily hacked... In the wrong hands, they will have access to your protected network.

Three Dumb Routers.

The following copyrighted article is a partial reprint of Nicolae Crisan article describing Steve Gibson's "Three Dumb Routers".

Steve Gibson's Three Router Solution to IOT Insecurity

<https://pcper.com/2016/08/steve-gibsons-three-router-solution-to-iot-insecurity/>

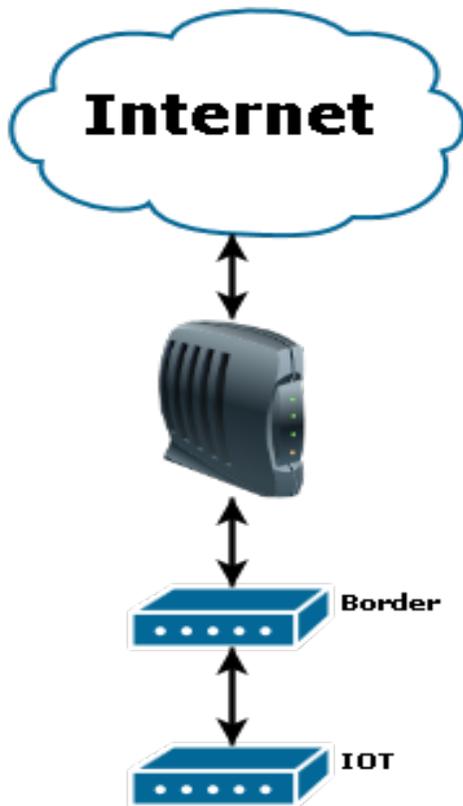


Introduction

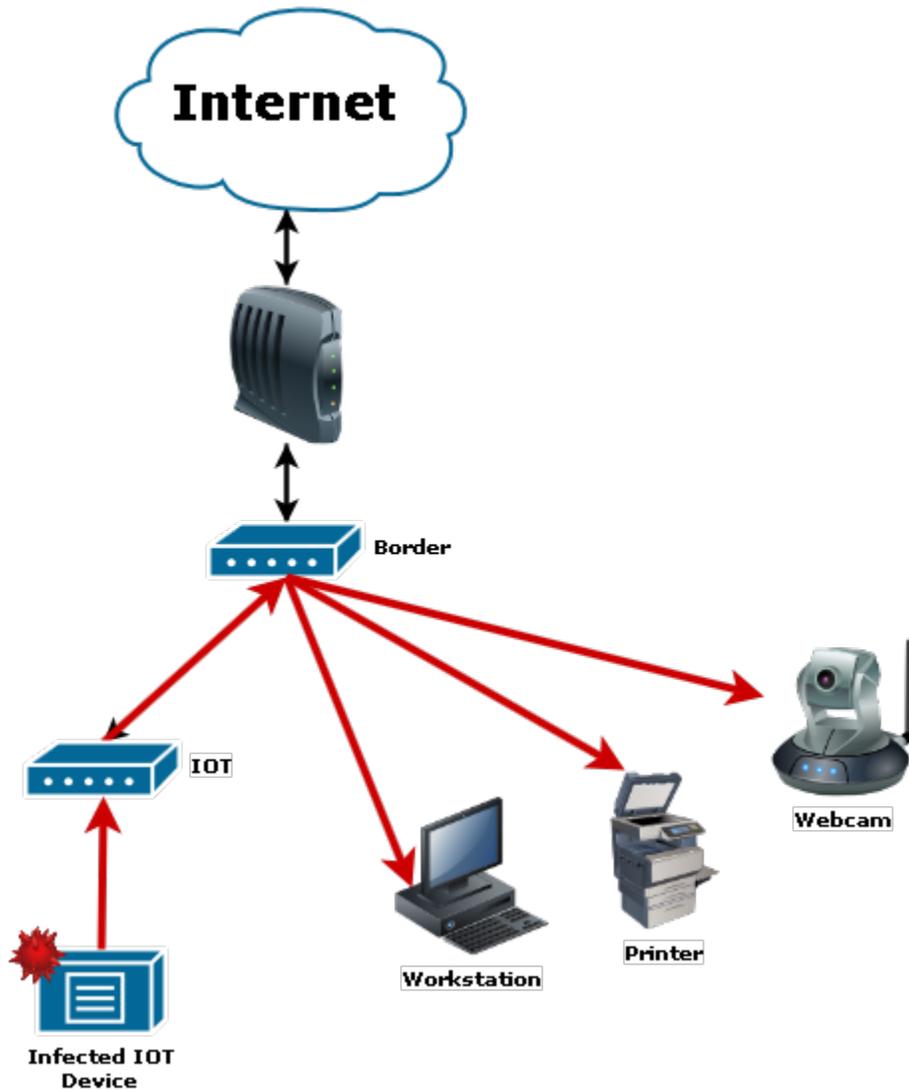
How can you secure your IOT devices from the outside world without cutting off features/

Even before the formulation of the term "Internet of things", Steve Gibson proposed home networking topology changes designed to deal with this new looming security threat. Unfortunately, little or no thought is given to the security aspects of the devices in this rapidly growing market.

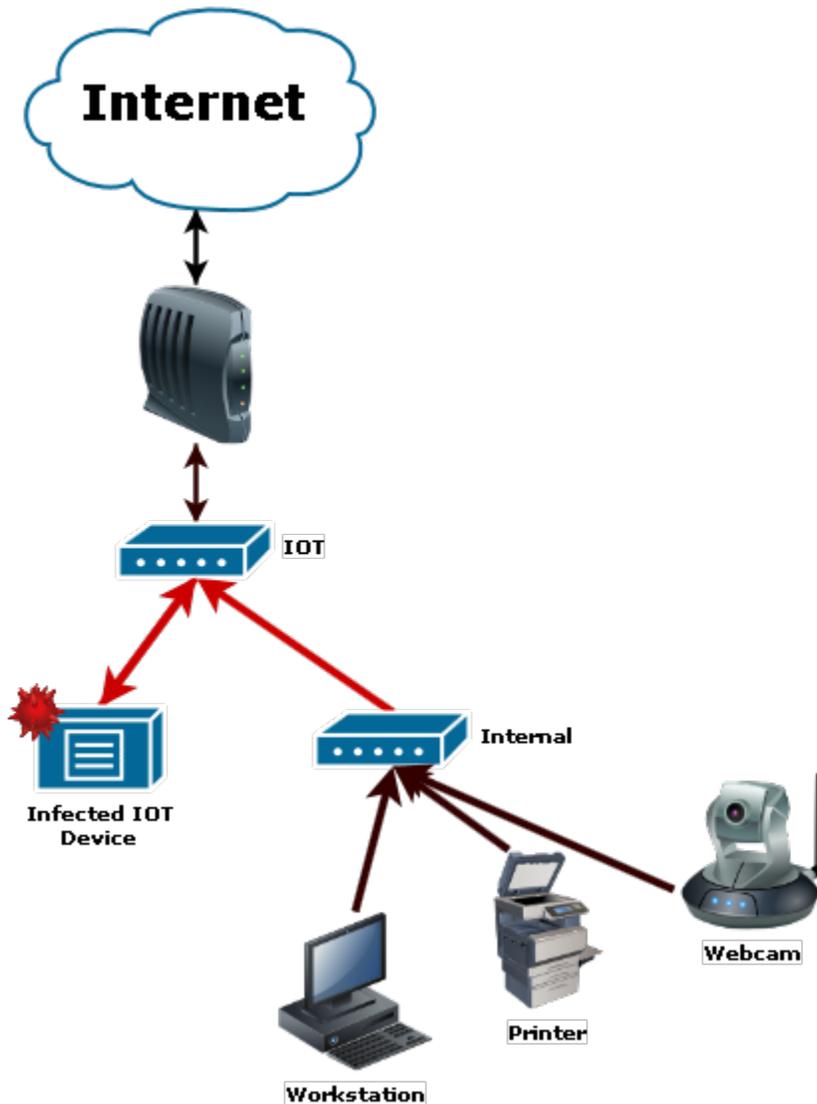
One of Steve's proposed network topology adjustments involved daisy-chaining two routers together. The WAN port of an IOT-purposed router would be attached to the LAN port of the Border/root router.



In this arrangement, only IOT/Smart devices are connected to the internal (or IOT-purposed) router. The idea was to isolate insecure or poorly implemented devices from the more valuable personal local data devices such as a NAS with important files and or backups. Unfortunately this clever arrangement leaves any device directly connected to the “border” router open to attack by infected devices running on the internal/IOT router. Said devices could perform a simple trace-route and identify that an intermediate network exists between it and the public Internet. Any device running under the border router with known (or worse – unknown!) vulnerabilities can be immediately exploited.



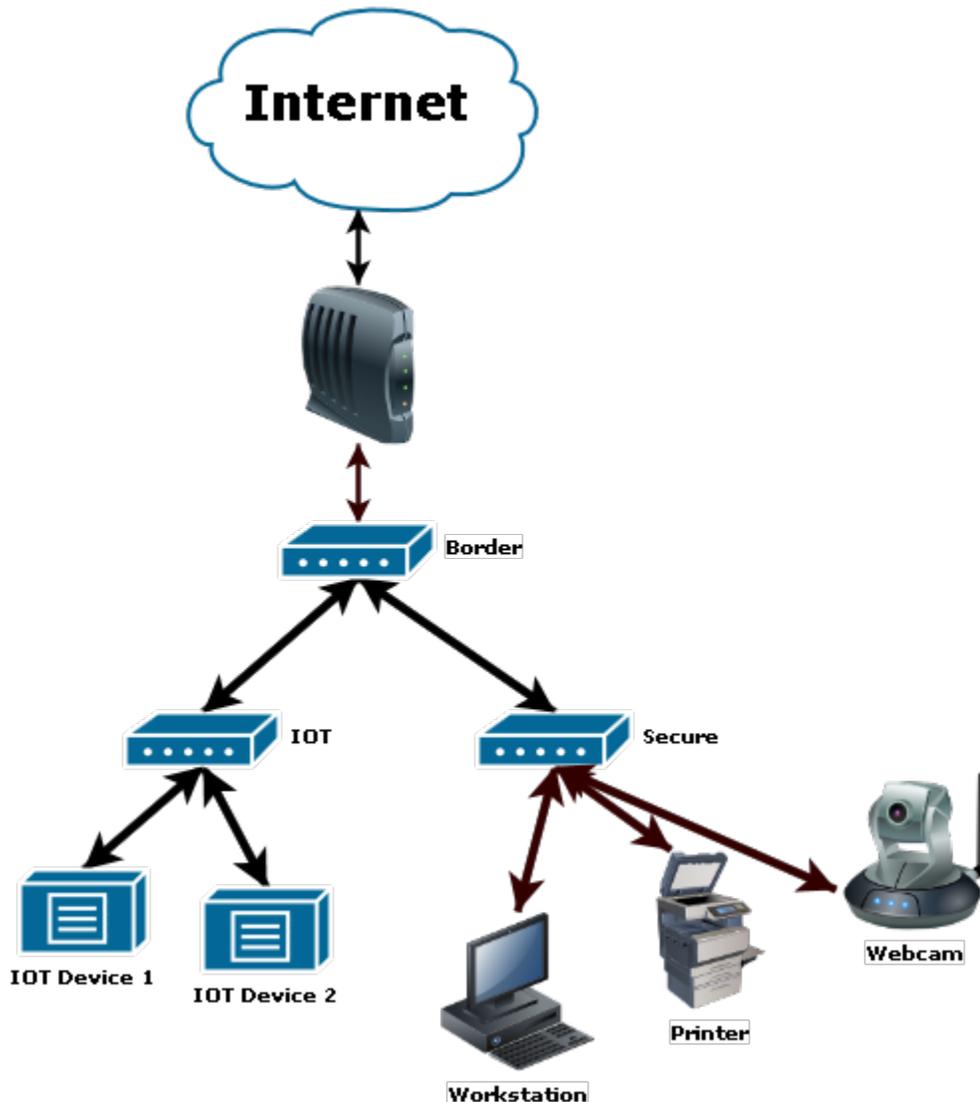
Gibson's alternative formula reversed the positioning of the IOT and border router. Unfortunately, this solution also came with a nasty side-effect. The border router (now used as the "secure" or internal router) became subject to all manner of man-in-the-middle attacks. Since the local Ethernet network basically trusts all traffic within its domain, an infected device on the IOT router (now between the internal router and the public Internet) can manipulate or eavesdrop on any traffic emerging from the internal router. The potential consequences of this flaw are obvious.



The third time really is the charm for Steve! On February 2nd of this year ([Episode #545 of Security Now!](#)) Gibson presented us with his third (and hopefully final) foray into the magical land of theory-crafting as it related to securing our home networks against the Internet of Things.

With this iteration Steve moved us from a two-router solution to a three-router solution. The new arrangement involves three fundamental elements to the network – an “external” or “border” router that has one purpose and one purpose ONLY; to move traffic back and forth between the public Internet and the two internal subnets underneath it. The second is an IOT-purposed router which houses all “Smart” / “Internet of Things” / “Internet-Enabled” devices whose uplink port is connected to an open LAN port of our border router. Devices such as PCs, laptops, phones and network storage devices have NO place inside this segment of the network. The third and last element is the “Secure” or internal router which, in similar fashion to the IOT router, has

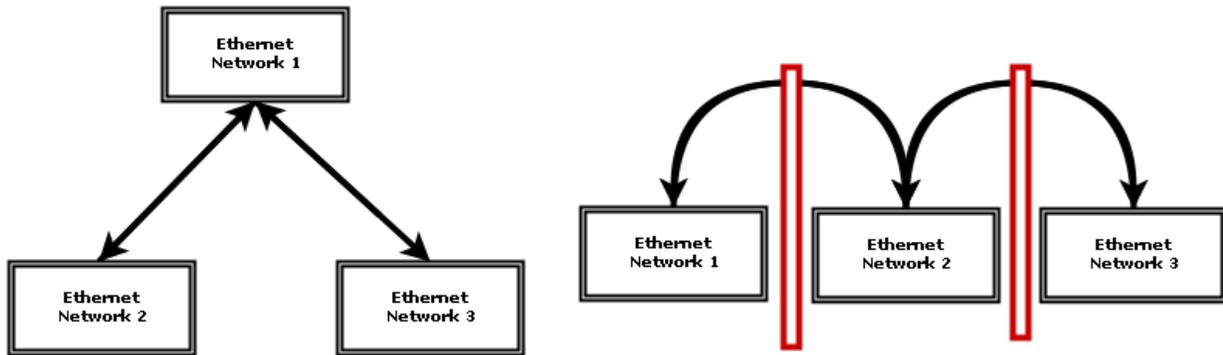
its uplink port connected to an open LAN port of the border router. Any valuable device (high value targets to hackers) such as desktops, laptops and network storage devices (a NAS or similar network appliance)) are all clustered together inside this subnet.



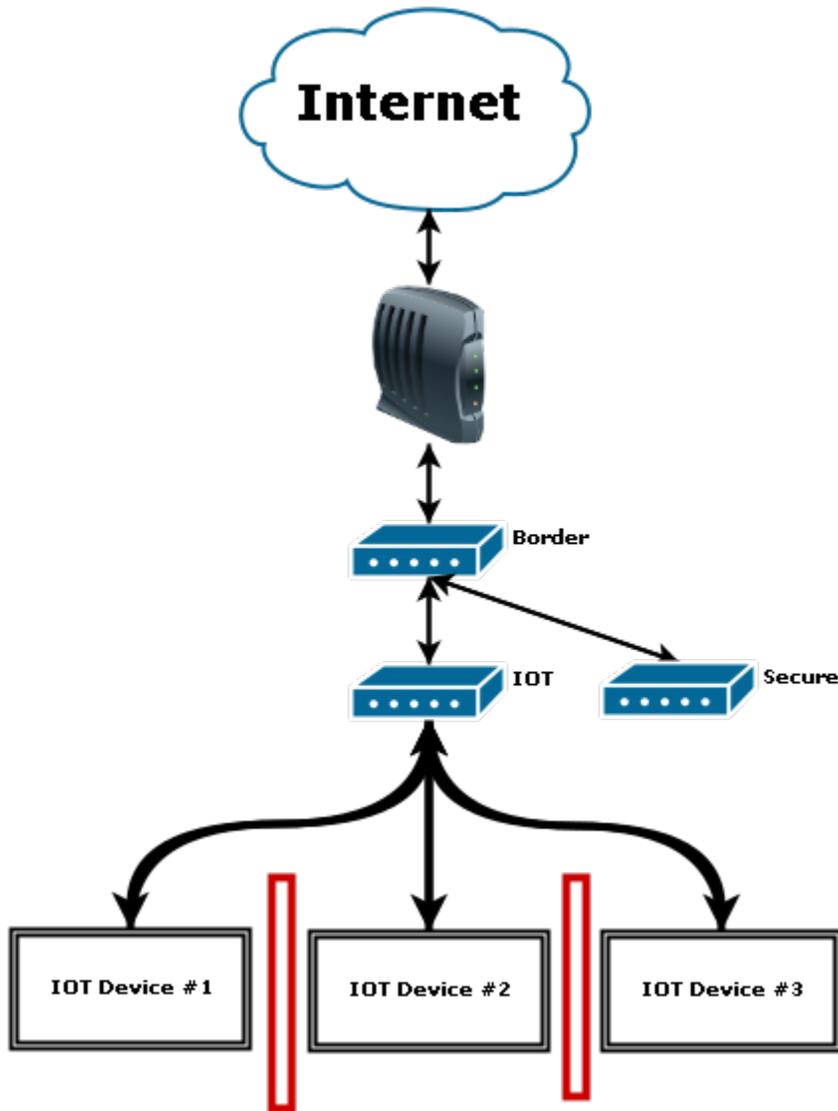
Maintaining three separate purpose-driven subnets affords our network some key protective features unavailable to us with both of our previous configurations.

1. Separation of Ethernet Segments: Compromised devices and or malicious payloads no longer have the luxury of unfettered access to devices (either upstream or downstream) by exploiting the trusting Ethernet protocol.
2. Damage control: Compromised devices and or malicious payloads are separated from higher value targets such as PC workstations and network attached storage devices. In the event of a breach, the damage an “expendable”

IOT device can cause on the network will be contained and compartmentalized to the local subnet.



Although our proposed variation so far seems very bullet-proof (it is for the most part), we cannot neglect to briefly discuss one outstanding caveat. Even though corralling all of our less secure devices into a single subnet will dramatically improve our overall security, the threat of an already infected device hijacking or exploiting the vulnerabilities of an adjacent device in the same IOT subnet is still a very real possibility. For this reason, I would propose an additional modification to this blueprint (Which Steve also slightly alluded to). Whether built in software or (preferably) hardware, a per IP “virtual LAN pipe” should be constructed on the fly with each new IOT device connection that would allow IP-based communication to only one endpoint – the publicly facing Internet. It’s important to note that a VLAN does not provide the form of security we desire on a wireless interface. Our goal is to draw on the concepts of how a VLAN works while the implementation will most likely utilize some other method/protocol. In other words, a device would ONLY have the capability to transmit and receive as if it were the only device behind the protection of the NAT. The idea here isn’t to over-engineer a solution (even though it feels very much that way). This is about advancing our networking technology to address the very real threat IOT devices carry with them.



Router Configuration Walk-Through

The IT veterans among us are most likely already well acquainted with the concepts at work in this type of router configuration. In fact, I would wager that most of you also could easily purchase and configure a system like this blindfolded. Even though most of us might already understand the concepts and steps involved, there are several benefits all of us can take advantage of. Less experienced readers can get a grasp on some basic networking concepts while the IT veterans among us can fill-in some knowledge gaps (we all have them). As a community we can all fine-tune various aspects of this alternative approach to IOT security and begin implementing this network configuration at home or in the office.

Whether you're a beginner or a CISCO certified professional, we will all learn nuances of this alternative router configuration that we wouldn't have had we not walked through it together.

So, let's assume we're sold on the idea that Gibson's router configuration will answer all of our IOT security woes. We're going to un-box and configure three identical routers so they adhere to this alternative way of handling "insecure" and "secure" traffic. You can, of course, use three completely different router models. To keep things in the realm of sanity and because it's much more efficient and easy to manage one unified interface, we will be using the same router model for all three.

For this setup we'll be using three ASUS RT-N12 "3-In-1" Wireless Routers.



I have to pause a moment and chuckle at the advertising ASUS has come up with on this line of routers. The word "FAST" wasn't good enough apparently – ASUS had to make an acronym out of it to really drive home the point that "this router be FAST, yo!"



This isn't a Warranty Notice insert that I should just throw away. People, this is a "VIP Member" warranty notice! I am SO important to ASUS they had to include that specific verbiage just for me!



After unpacking all three units, lay everything out so it emulates the network topology we are creating – as shown below. I would HIGHLY recommend labeling each router to eliminate any confusion as to what that router's purpose is in your network. Ten months from now when you hobble back into your server closet or re-approach the tangled rats-nest of wires we all know you have near your cable modem, you won't remember why you have three identical routers or what each of them does!



Additional Information including videos, are at

Twit.tv/KH (TWIT.TV is the home of Leo Laporte W6TWT)

<https://twit.tv/shows/twit-bits/episodes/4075>

or

<https://twit.tv/shows/know-how/episodes/315?autostart=false>

or

<https://www.youtube.com/watch?v=4TOFwFHm8SA>