Solving Network Connection Problems

Why a wired connection might often be a better idea

Here is a story about the pitfalls of using wireless connections that might help other users. I had been having random problems with an Allstar connection between a portable node I had built and my local wireless (2.4G) router. The portable node would occasionally loose packets for no reason. People reported that there would be an occasional hole in the audio they were hearing from my end meaning that a very small portion of a word was dropped. It did not make unreadable but it was annoying. It did not seem to matter where I moved the portable node, 10 feet away from the router or two floors away the problem persisted. I could see the dropouts in the Asterisk client window.

I lived with this for awhile and eventually stopped using the wireless connection and instead used my many other nodes that are wired. The computers in the house that used wireless seemed to work OK or at least I thought.

Skip ahead a few months and I was experimenting on the bench with a portable wireless router. I was having extremely erratic results. Sometimes it would connect and others it just would not. Thinking the router was bad I then used an older Buffalo router for the test that I had taken out of service and I had similar erratic results. I was pulling my hair out but I still did not relate this problem to my earlier Allstar problem.

I had been experimenting with a Ubiquity Nano M2 I mounted on my tower for possible future amateur mesh work. It was setup as a standard access point bridge through my local LAN. Even though it had been in service for many months I had never actually checked its wireless throughput. I got the chance when my brother who was moving in next door and I wanted to make Internet available to him until he got his permanent connection. He came over one day and used his phone to check the connection to the Ubiquity, something that should have been an easy task. He was able to connect but got very poor throughput.

So that evening I spent hours changing parameters on the Ubiquity and trying to improve the throughput. I was using a laptop to test with the Ubiquity and it was having the same problems I was having with the earlier tests. Changing channels seemed to make things better but it was very erratic like it had been in the earlier tests. I was convinced I had some kind of an interference problem but how do I find out what it is?

Finally a light bulb went off. About 10 years before all this I had put in a security camera system with four cameras. I wired three of the cameras directly but I had decided to use a wireless camera for one of the connections. It never worked that well, it was a cheap camera, but I left it connected all these years. I thought maybe this was causing the problem. So I disconnected the camera and viola, all the problems went away!

Lessons learned

Wireless is just that a radio circuit and like any radio circuit it is subject to interference. Fortunately for me in this case I was causing the problem and able to fix it. Imagine if it was your neighbor causing the interference. This is what the FCC means by a rising noise floor. It is really a problem and getting worse all the time.

I made up a little chart to show the advantages and disadvantages of wire and wireless connections

	Wired	**Wireless**
Potential Interference	Unlikely	Very Possible
Ease of Setup	Very Easy Plug and Play	More steps required Relatively easy when things work
Susceptibility to EMI Lightning	Possible	Unlikely
Portability (assuming DHCP)	Excellent if a connection is available	Good if an open hotspot is available
Reliability	Excellent	Good but can degrade due to environment

Other Network Issues Wired or Wireless

There are many different routers out there. Many are using old that can sometimes cause problems. For most things you do with devices on the internet, browsing the web, streaming video, etc it matters less what IP address you are assigned but for others like your Allstar server it does matter because you may need to directly interact with it via ssh (putty) and port forward in your router for incoming connections.

In most all cases using the default DHCP works fine. Your router assigns you an IP address and as long as you stay online you will have the same address. Even if you went off line for a period less than the DHCP lease length when you came back up you would be issued the same IP address. To make that IP address stick permanently you could configure your router to always assign the same IP address based on the mac address of your board. The board address does not change and is a unique address. Every Pi board made will have a unique MAC address. So if you locked down a DHCP address using hamvoip version 1.02 the same address would be assigned bringing up V1.5. Even if you ran a completely different OS, say Jesse Pixel by swapping SD cards, you would have the same IP address. With DHCP the IP address is assigned to the board not the SW running on the board. The advantage here is that you always know what IP address is going to be assigned to that board. This of course assumes you have the boards MAC address setup to assign a permanent IP address in your router and you do not change routers.

The DHCP permanent IP address feature is variously called static DHCP assignment by DD-WRT, fixed-address by the dhcpd documentation, address reservation by Netgear, DHCP reservation or static DHCP by Cisco and Linksys, and IP address reservation or MAC/IP address binding by various other router manufacturers.

Another issue that often happens with home LANs is having more than one router online with BOTH issuing DHCP addresses. You should ONLY have one DHCP server on a LAN. There are situations where more than one can be used but this is for experienced users with network experience.

Often users have more than one router in their residence connected in the wrong way creating a double NAT. In this scenario router one converts a single public IP from your provider to a LAN assignment say 192.168.1.x then you connect another router from one of the first routers LAN ports to the second routers WAN port. The second router DHCP's an IP from the first router and then creates yet another LAN behind the first LAN. The proper way to do this if you use two routers is to connect the first router to the second routers LAN port (LAN to LAN **NOT WAN**) and essentially making the second router a switch BUT you do need to turn off the DHCP server in one of the routers! Many people use multiple routers mainly to put up multiple wireless access points to reach distance points of their residence. There is nothing wrong with doing this you just have to watch how you connect things. Never double NAT (**always LAN to LAN between routers**) and **ONLY ONE** DHCP server on the network.

I have experienced several Allstar users pull their hair out having routers connected in the wrong way and trying to port forward only to find it does not work. If you have Allstar connected to the second serially connected router (LAN to WAN) and you port forward in that router you are only port forwarding to another LAN not the Internet and it will not work.