ROUTABLE -V- UN-ROUTABLE PROTOCOLS – A HOME NETWORKING PITFALL

The application layer protocols we use to actually do things on our networks or the internet use protocols which sit on top of IP (usually TCP or UDP). Because IP can send packets between subnets, you might assume that all Application layer protocols that use IP under the hood would also be able to work across different subnets, but you'd be mistaken. Many, even most, application layer protocols can indeed cross routers to move between subnets, but a sub-set of them can't.

Protocols that rely on IP broadcast packets are confined to the reach of those packets, i.e., to the local subnet. Because these protocols can't cross routers, they are known as *un-routable protocols*.

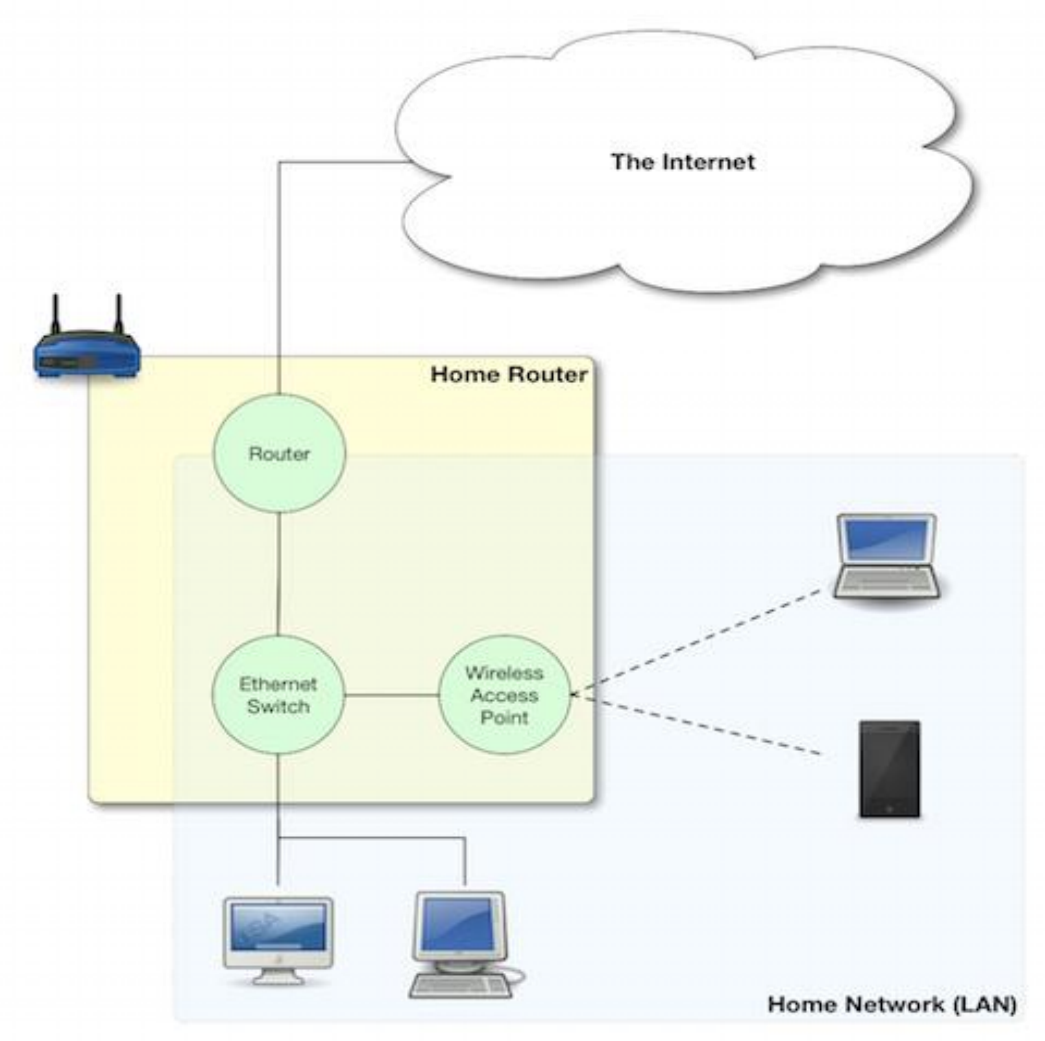
The un-routable protocols you are likely to encounter on your home network are mostly designed around zero-config sharing of some sort. The idea is that computers that share a subnet can easily share data or some other resource without the user needing to do much, if any, configuration. Probably the most common such protocol is mDNS, better known as Bonjour. Apple are very fond of un-routable protocols for things like AirVideo, iTunes sharing and printer sharing.

The fact that these protocols are confined within the local subnet is actually a security feature. Something which can't possibly be accessed remotely needs a lot less security than something which could be accessed by anyone on the internet! If anyone anywhere on the planet could send their screen to your Apple TV you'd definitely need to set a password on it, and a long one at that, but because AirPlay is un-routable, you don't need to bother, making the experience much more pleasant!

A very common problem is that people accidentally break their network into multiple subnets, and then find that sharing services have become mysteriously unreliable.

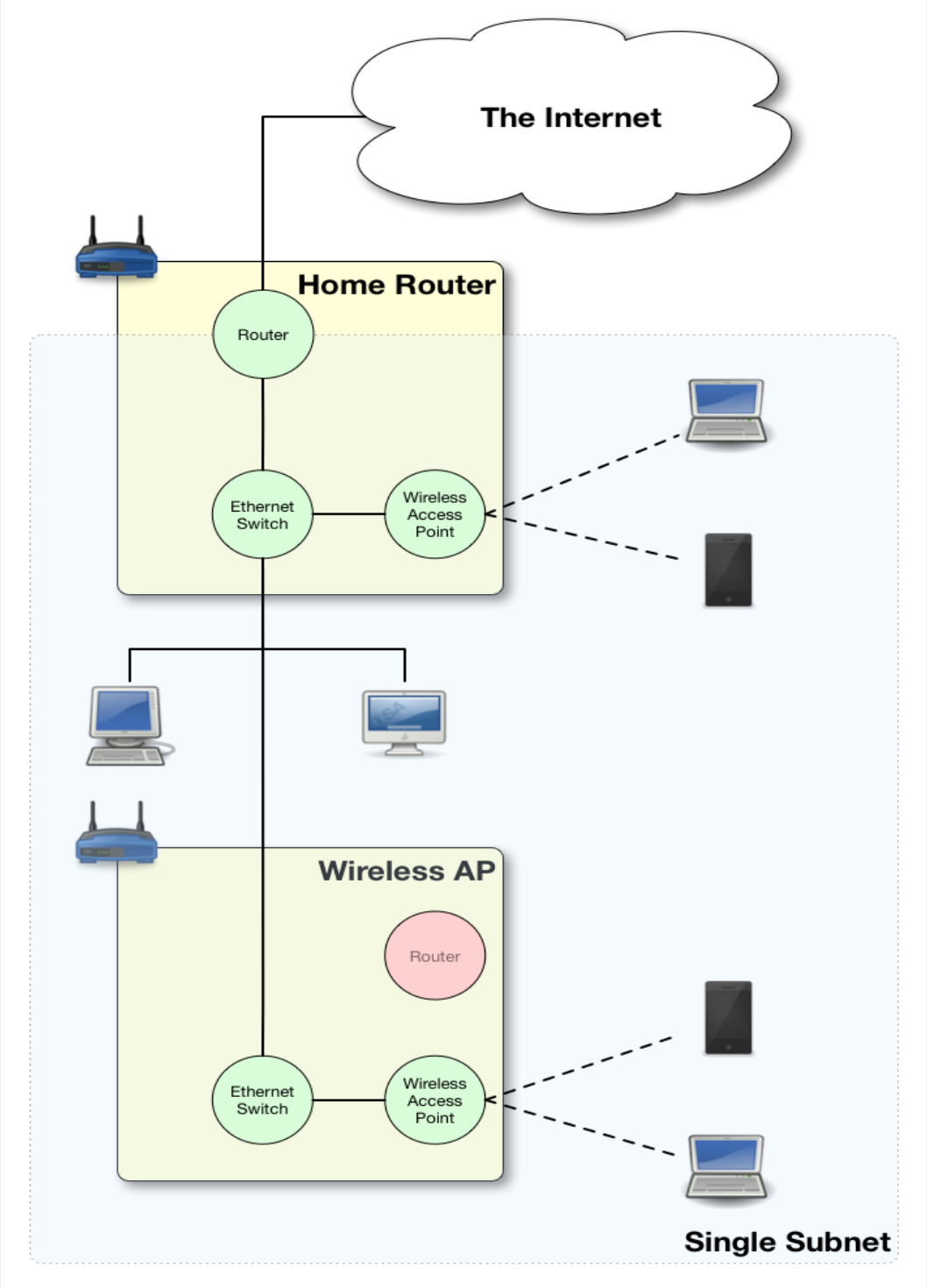
Imagine you have half of your devices on one subnet, and half on another – those sharing a subnet with an Apple TV can share their screens no problem, but the devices on the other subnet can't. You think they are all on the same network, because they are all in your home, and all eventually connect back to your internet router, so you have no idea why something that should just work is just refusing to work!

It's actually very easy to accidentally break up your network. Imagine you start with the basic network setup we described last week, you have one home router which connects you to the internet, and provides you with an ethernet switch and a wireless access point:

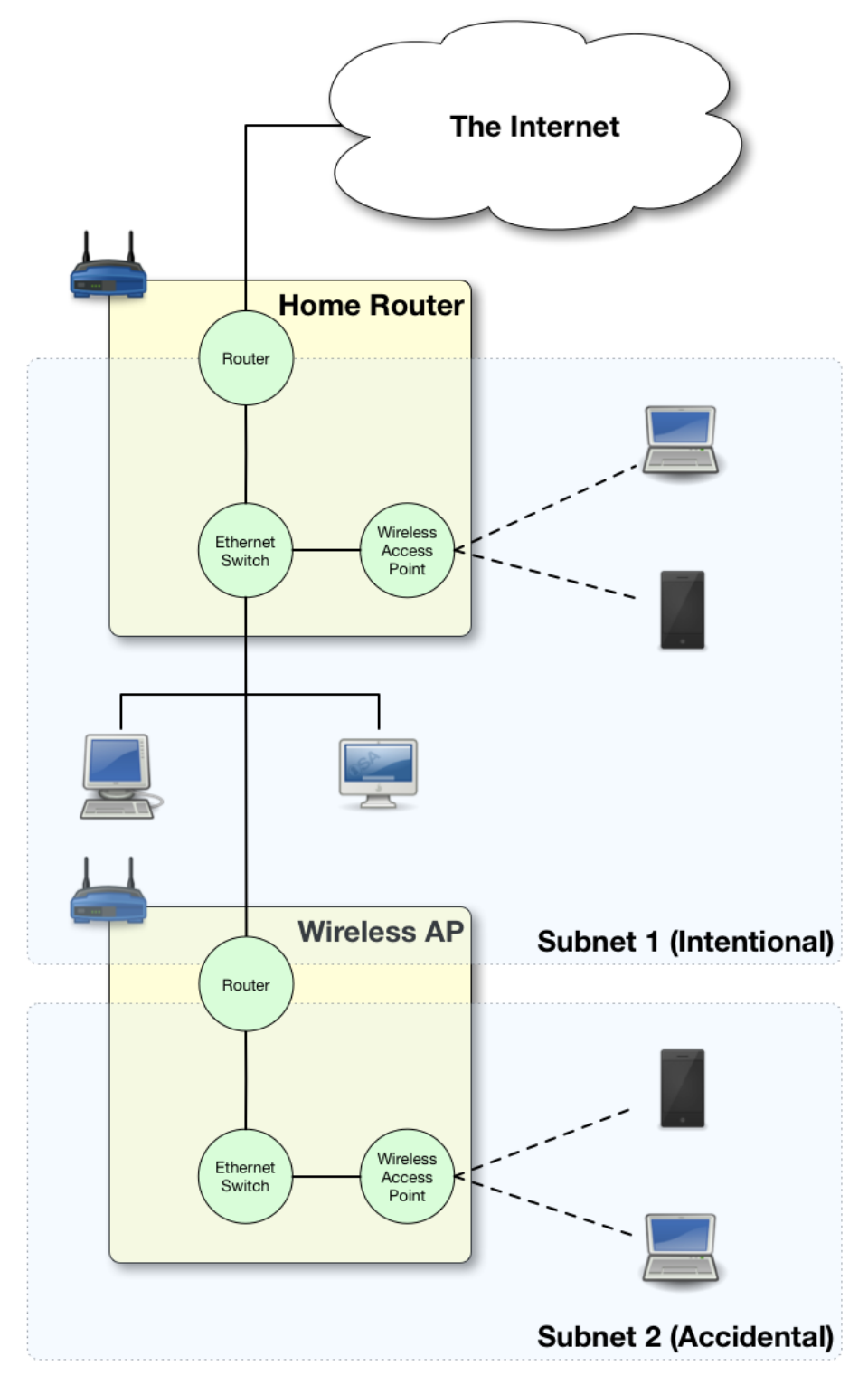


This is working quite well, but you have terrible wifi reception in the back bedroom, so you buy another wireless router, and plug it in. That device, like your home router, is probably three devices in one, a router, an ethernet switch, and a wireless access point, that means that depending on your configuration, you can end up with one big IP subnet in the house, or, with two separate IP subnets. The diagrams below show two possible configurations with two home routers – one with a single IP Subnet, the other with two separate subnets.

Good – A Single Subnet



Bad – Two Subnets



Unless you intentionally want to isolate off some users, you probably want a single subnet, and if you accidentally ended up with more you're probably experiencing all sorts of sharing frustrations. Why can I send my screen to the Apple TV, but my husband can't? Why can my daughter print, but I can't? Why can the Apple TV not see my shared iTunes library while my son's computer can? When you start experiencing strange symptoms like this, the fist thing to check is that you haven't accidentally divided your network into multiple subnets.

Source: https://www.bartbusschots.ie/s/2014/12/07/taming-the-terminal-part-25-of-n-ip-subnets/