Best Router?

I've got Cablevision in my office for my phones and internet. I've been solo until recently. Now I need to hook up another computer and Cablevision tells me I need to get a router.

What's the latest and the greatest?

Oh, and feel free to tell me I need something else. I can't use Verizon in my current building because FIOS isn't available in that part of town.

Thanks, all!

Really doesn't matter. Whatever is on sale will be fine. Old tech isn't going to be found without searching for it.

Is the other computer going to be wired to the router or wireless? That's probably the only thing you need to know. If wired, then a hub might be ok.

Steve
--
Steven O'Donnell, Pennsylvania

---

old tech? what old tech?

I'd like it to be wireless. My plan is to no longer have my assistant sitting on my lap. It makes it difficult to work.

Ellen Victor, New York

Basically anything you buy at Best Buy or the equivalent will suit your needs. The only questions to think about is whether to hook up the new computer with a network cable or via wi-fi. This might depend moreso on he layout of your office than anything else. If your assistant will be using a laptop, then they all have wi-fi built in, so wireless might be the way to go.

My suggestion is to get a mid-priced wireless router. It should come with 4 ethernet ports (for wired connections) and some of them let you attach a printer for easier sharing.

Give me a call if you need more help - I was a network geek in a past life.

Bruce Wingate, New York

Well, let's say you wanted a b wireless or even b/g, that will probably take some looking because everything new you'll find is b/g/n. it'd be like looking for a computer running Windows 95.

Anything you get should come with a setup disc that will walk you through the setup. Linksys, Belkin are the two big names that come to mind.

When you get to choosing encryption either go with WPA or MAC address filtering to keep things safe. MAC is more secure, but also more of a pain if you're going to bring in other devices or let clients have access because it's tied to a unique identifier on each device. WPA is password protected.

Steve
--
Steven O'Donnell

Fyi, MAC address filtering does not prevent people from eavesdropping and can pretty easily be defeated by someone spoofing your MAC address while you're out of the office.
Of those two choices, only WPA prevents people from collecting all your communications.

Best Wishes,
Joseph Cohen

Basically, MAC is not secure at all. If it's your only security, get more.
Joseph Cohen

For the last few years, I've only purchased Netgear routers. Even Walmart has the Netgear N300 for $45. We installed one last night, and it is great. We enable remote management so that I can manage it for my son in another city.

You might want to avoid Cisco/Linksys.

http://goo.gl/DLMaF

While they've backed away from the policy change, they'll likely end up back there eventually.

Mike Phillips, North Carolina

Ellen: Most brands of routers will be fine. I'm partial to Buffalo. I think they make an excellent product, and have domestic tech support.

You might consider a dual band router. You could use one band for your office, and the other band could be designated as a guest network for people that come to see you. Just a thought...

HTH.

Scott I. Barer, California

Doesn't someone need physical access to a computer to get its MAC address?

Steve
--
Steven O'Donnell

No. The MAC address is sent with all communication on the network.

The MAC address is like an IP address for your network. Every time you send communication (i.e. download email, go to a webpage, do *anything* that requires the network), the MAC address is sent with it.

As I wrote in the private email, filtering which MAC addresses can connect to your network does nothing to prevent people from seeing all the information that travels across your network - including your MAC address.

Since many computers can change their MAC address, it is very easy for someone who wants to to get access to your network.

And, as mentioned above, they can view all the information traveling across your network (emails, web pages, downloads, etc.) without connecting unless you encrypt it (with WPA, etc.)

Best Wishes,
Joseph Cohen

Thanks for correcting me.

Steve O'Donnell

No. It is broadcast. If machine is off or disconnects from network then it is spoofable. WPA2 is minimum for wireless now, along with changing all defaults possible for router.

Linksys/Cisco is catching flack for their mandatory upgrade and change in terms of service right now. Personally I have had the best luck with Netgear or D-Link for routers.

Darrell G. Stewart, Texas

We have a Cisco wireless that covers our entire 2 story house.

It is encrypted

Erin Schmidt

What percentage of Solosez readers saw this and said, "I don't have a Mac. I have a PC."?

David Shulman

So keeping no-longer-used or infrequently-used MAC IDs on my "OK" list is probably a bad idea then.

But how do you know what ID to spoof? Or do they just cycle through lots of IDs?

Thanks, Tim Ackermann

The main point is not to rely solely on MAC address filtering as "security." (I don't bother with it at all) One should use the commonly available WPA2 at a minimum.

>But how do [the hackers] know what ID to spoof?
There are commonly available WiFi sniffing programs such as FireSheep and Cain and Abel where one can monitor all WiFi traffic within one's vicinity. WPA2 and HTTPS encrypt various parts of the network traffic.

Regards,
John Lindsay

Sniffers on wireless can pick up a lot. There are other techniques, which
are basically variants on the man in the middle attack, from what I read.

Darrell G. Stewart

It's probably a bad idea but the chances of that being exploited is infinitesimal. There are probably easier ways to breach your network if a pro really wanted to.

They know which ID to spoof by sniffing the traffic on your network and seeing which MAC addresses are connecting. Then, armed with a list of obviously approved MAC addresses, they just wait for their opportunity.

John is right, I rarely bother with MAC filtering. WPA2 with a good passphrase is sufficient in most cases.

Disclaimer: No, still not a lawyer.

Ben M. Schorr, Arizona

Right, FireSheep. Nice.

And so it's not the rarely-used ones that are a problem - it's the
regularly-used but sometimes off ones that are a problem. Hmm, that's not
so good.

And just to be clear, I'm not just using MAC ID filtering. It's the second
of three layers, of which requiring a password is the obvious winner...

Thanks

Tim Ackermann
