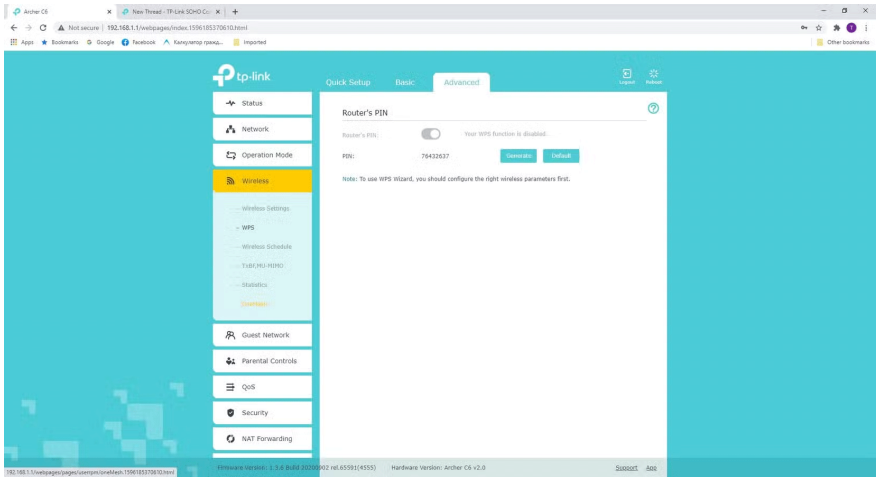
Why should you disable these 3 settings on your router?

Routers today come with many features that make them easier to use for everyday users. However, some of these features are vulnerable to hackers, so always disable these router settings for better security.

1. WPS

Wi-Fi Protected Setup (WPS) sounds like a great idea in theory. It lets you authenticate wireless devices on your network by simply pressing the WPS button on your router. Then you go to your client device and press its WPS button. And voila, the device is connected without having to enter a Wi-Fi password.

The ease of use of WPS is what makes it appealing, especially if you're using one of your ISP's routers with long, complex default passwords. But after learning more about the actual steps to secure your network, you'll find that you should disable the feature in your router's admin panel.



Why is that? Bad guys can easily hijack WPS and break into your wireless network. That's because WPS:

1. PIN code communication is vulnerable to attacks using .
2. There are design flaws that are often not patched.

A better solution is the old-fashioned one: Require strong Wi-Fi passwords with WPA2 or WPA3 (if you have a new router). These protocols have encryption and security implementations that are harder to crack.

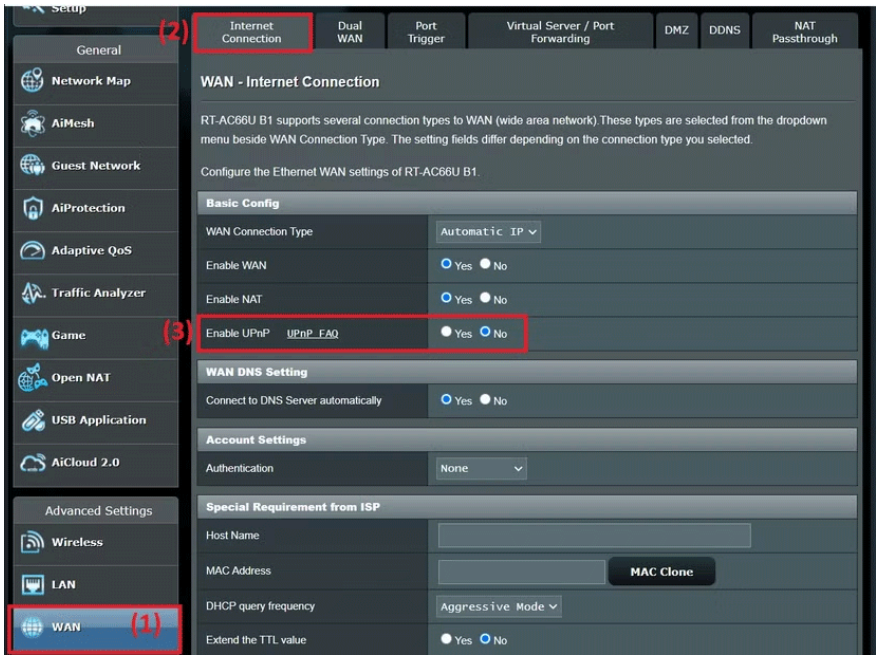
2. UPnP

Your router acts as the gatekeeper for your home network, protecting it from swarms of bots roaming around. But that protection can get annoying when you go overboard. In the past, multiplayer games would often fail to connect if you didn't open the right ports on your router. Bad!

Opening the right ports is never as simple as you might think. Does the software need a single port or a range? And should they be opened for TCP or UDP?

When Universal Plug and Play (UPnP) came out around 2000, it looked like a hero. Here's a simple explanation of how UPnP works:

1. Your software requires permissions for the necessary ports.
2. The router's UPnP feature will automatically open these ports.



However, UPnP is dangerous because a malicious program can take advantage of the protocol's rich feature set to open ports without your knowledge - effectively bypassing the protections of your router's firewall.

Fortunately, most applications today are programmed to work as expected, even with UPnP disabled. For some cases where this isn't the case—like accessing your Plex media server while away from home—it's safer to set up port forwarding rules just for what you need.

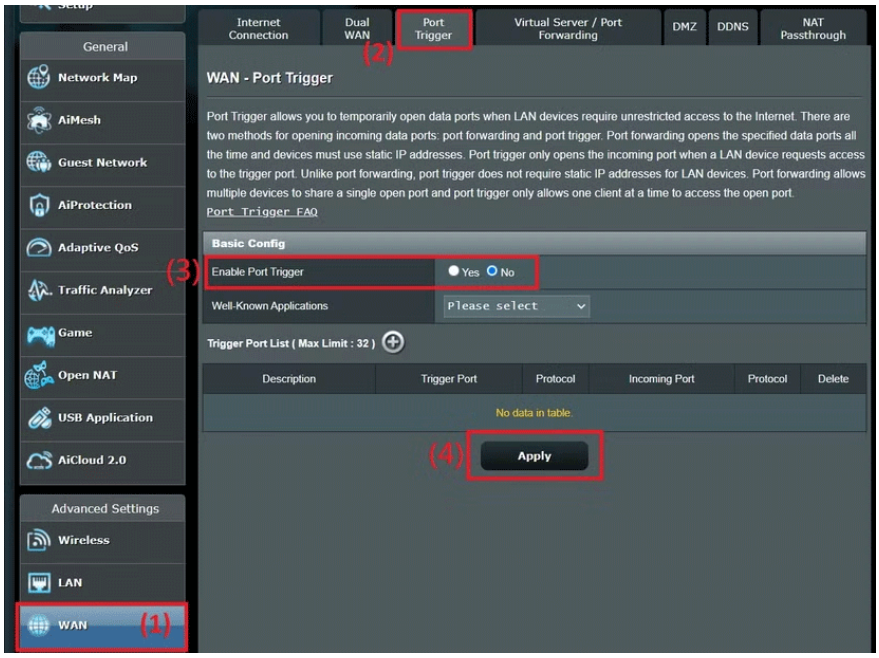
3. NAT-PMP

Network engineers at Apple recognized the security risks with UPnP and came up with an alternative for their applications called Network Address Transversal Port Mapping Protocol. NAT-PMP has the same goals as UPnP, except that NAT-PMP:

1. It just focuses more narrowly on port mapping.
2. There are tighter security implementations.

NAT-PMP was first introduced by Apple in 2005. After all this time, the protocol is still widely used only by Apple software and integrated into apps like FaceTime. That doesn't mean it's just Apple users who are affected: NAT-PMP is often enabled by default on many mainstream router brands like ASUS and NETGEAR.

So, has Apple succeeded in enhancing security with NAT-PMP? To some extent, yes, but not enough. So always disable NAT-PMP (sometimes listed as 'port triggering').



NAT-PMP also uses flawed logic to allow applications to control which ports are open on your router. This is fine when Apple AirPlay requires it, but not so fine when the App XYZ Trojan finds a way to spoof authentication to gain the same privileges.

NAT-PMP vulnerabilities have affected millions of devices. It's simply safer to turn this feature off. Mobile apps and Apple TV 4K still work fine with it turned off. For rare glitches, use port forwarding instead.

Growing into a security-minded mindset sometimes means giving up what's easiest. You may decide it's time to eliminate these three security risks.