What is my dns server address android

I'm not robot

reCAPTCHA

Continue

DNS made headlines recently when Cloudflare announced that it is a new 1.1.1.1 service looking for speed and security. Google is another high-profile company that offers free DNS, and in both cases, or with any others you could use, it will probably be better than the one that your provider provides. In the case of PlayStation 4, you can apply custom DNS directly to your console. It's not particularly obvious how to do it, but once you know where to look, it's pretty easy. Here's what you need to know. Go to the Settings menu on the console. Choose a network. Next, choose to set up your Internet connection option, whether you already have one setup on your console. Choose Wi-Fi or LAN depending on your preferences. Choose a custom setting. The next steps will be for the IP address and DHCP settings if you don't have a preference to choose the default for both. When DNS settings appear, select a guide. Enter the values for primary and secondary DNS. Now, once you complete the customization process, the console will use the DNS you chose, not the automatic one. It's important to remember that you have to follow these steps to apply changes to your console, you can't just change the DNS settings on your existing internet connection. Did you know that you can be connected to facebook.com and see facebook.com on your browser's address page while not actually connected to a real Facebook website? To understand why, you need to know a little bit about DNS. DNS means Domain Name System. DNS servers transfer web addresses (such as www.howtogeek.com) to their IP addresses (e.g. 23.92.23.113), so users don't need to memorize the number lines for each website they want to visit. The Domain Name System (DNS) is at the heart of the Internet, which we use every day. It works transparently in the background, turning human-read website names into computer-read numerical IP addresses. DNS does this by looking this information at a system of related DNS servers over the Internet. However, different DNS servers can behave differently in terms of speed and security. So let's see how DNS works and what you can do to make sure it works best for you. Domain names and IP addresses of domain names are readable for human websites that we use every day. For example, Google's domain name google.com. If you want to visit Google, you just need to google.com the address bar of your web browser. However, your computer doesn't understand where google.com is. Behind the scenes, the Internet and other networks use numerical IP addresses. One of the IP addresses used Google.com is 172.217.0.142. If you're in the address rack of your you'll also end up on Google's website. We use google.com instead of 172.217.0.142 because addresses such as google.com are more meaningful and easy for us Remember. It is also known that IP addresses are changing, but DNS servers do not want this new information. DNS is often explained as a phone book where you watch someone's name and the book gives you your phone number. Like the phone book, DNS matches human-read names with numbers that machines can more easily understand. DNS Servers DNS servers correspond to the domain names of their related IP addresses. When you type a domain name into your browser, your computer contacts the current DNS server and asks which IP address is associated with the domain name. The computer then connects to the IP address and gets you the right web page. The DNS servers you use are most likely provided by your ISP. If you're behind the router, your computer may use the router itself as a dns server, but the router will be re-run with requests for your provider's DNS servers. Computers cache DNS locally, so the DNS request doesn't happen every time you connect to a specific domain of a name you've already visited. Once your computer has identified an IP address associated with a domain name, it will remember that over a period of time, which increases the connection speed by missing the DNS request phase. Some viruses and other malware may change your default DNS server to a DNS server used by a malicious organization or a scammer. This malicious DNS server can point popular websites to various IP addresses that scammers can manage. For example, if you connect to a facebook.com if you use your INTERNET provider's legitimate DNS server, the DNS server will respond to the actual IP address of Your Facebook servers. However, if your computer or network is pointing to a malicious DNS server installed by a scammer, the malicious DNS server may respond completely to another IP address. So it's possible that you could see facebook.com in your browser's address rack, but you can't actually be in real facebook.com. Behind the scenes, the malicious DNS server gave you another IP address. To avoid this problem, make sure you are running good antivirus and antivirus applications. You should also keep an eye on certificate error reports on encrypted (HTTPS) websites. For example, if you try to connect to your bank's website and see a message invalid, it may be a sign that you are using a malicious DNS server pointing you to a fake website that is just pretending to be your bank. ANSWER: How to block websites in Windows 8 Hosts malware file can also use your computer's host file to override your dns server and specify certain domain names (websites) at other IP addresses. On this Windows 8 and 10 do not allow users to facebook.com and other popular domain names to different IP addresses Default. Why you can use third-party DNS SERVERS RELATED: How to switch to OpenDNS or Google DNS to speed up web browsing, as we set above, you're probably using your provider's default DNS servers. However, you don't have to. Instead, you can use DNS servers run by a third party. Two of the most popular third-party DNS servers are OpenDNS and Google Public DNS. In some cases, these DNS servers can provide you with faster DNS solutions, speeding up your connection when you first connect to your domain. However, the actual differences in speed you see will vary depending on how far you are away from third-party DNS servers and how fast your provider's DNS servers are. If your PROVIDER's DNS servers are fast and you're away from OpenDNS or Google DNS servers, you may see slower DNS solutions than your provider's DNS server. OpenDNS also provides additional website filtering. For example, if you turn on the filtering, accessing a pornographic website from your network can result in a Blocked page instead of a pornographic website. Behind the scenes, OpenDNS returned the IP address of a website with a blocked messiah instead of the IP address of a pornographic website - this uses the way DNS works to block websites. For information about using Google Public DNS or OpenDNS, check out the following articles: Image Credit: Jemimus on Flickr Your iPhone or iPad usually uses DNS servers provided by any Wi-Fi network you use. But you can install a custom DNS server and use Google Public DNS, OpenDNS or any other DNS server you prefer. RELATED: What is DNS, and should I use another DNS server? Every Wi-FI network you connect to has its own separate DNS server setup. If you want to use a custom DNS server on several different Wi-Fi networks, you'll have to change that setup once for each Wi-Fi network. Open the Settings app and tap Wi-Fi to get started. On the Wi-Fi screen, click on the information button (it's i in a circle) to the right of the network you want to set up. To change the settings of your current Wi-Fi network, click the i button next to the Wi-Fi network you're currently connected to at the top of the screen. Scroll down the information screen and tap the DNS Settings option in the DNS section. Then click on the Guide option at the top of the screen, and then tap the red mark icons minus to the left of the automatically configured DNS servers to remove them from the list. Click add a server and then enter the IP address of each DNS server you want to use on your own line. For example, add a primary DNS server to the line and secondary on the second line. Click Save when you're done. Remember that you will need to repeat this process for every Wi-Fi network you want use a custom DNS server. How to forget the Wi-Fi network on your iPhone or iPad your iPhone or iPad remembers this setup, even after disconnecting and reconnecting to the network. However, if you have an iOS forget about the network, you'll have to set it up from scratch again. And, if you ever want to undo this change, just go back to the screen above, click on the Automatic Option, and click Save. Your iPhone or iPad will return to the default DNS settings for this network. If your current DNS server just doesn't work well, and you want something better, Google Public DNS (IP addresses 8.8.8.8 and 8.8.4.4) and OpenDNS (IP addresses 208.67.222.222 and 208.67.220.220) some of the usually recommended DNS servers we like. RELATED: The ultimate guide to changing your DNS server, you can also change the DNS server for all devices on your network by changing the DNS server on the router. Before you change the DNS server separately for each device on the home network, simply change it once on the router. When you change DNS servers that your router, computer, or other Internet-connected device uses, you change the servers normally assigned by your ISP, which your computer or device uses to convert host names into IP addresses. In other words, you are changing the service provider that turns www.facebook.com 173.252.110.27. Changing DNS servers can be a good step to troubleshooting while eliminating some types of Internet connection issues. It can also help keep your web surfing more private, assuming that you choose a service that doesn't log your data in, and may even allow you to access sites that your provider has decided to block. Use one of several public DNS servers instead of automatically assigned servers that you're probably using now. See our list of free and public DNS servers that have primary and secondary DNS servers that you can change right now. Before you change DNS servers, you need to decide if it is the best choice in your particular situation to change DNS servers on your router or on your individual computers or devices: Change DNS servers on the router if you want all computers and devices that connect to the Internet via this router to also use new DNS servers. This method only works if your computers and devices are configured using DHCP, meaning they look at the router for dns server information, among other things. This approach is typical. Change DNS servers on a separate device if you want to use only one device to use these different DNS servers. This approach is a good idea when you troubleshooting an internet problem with a single device, you suspect maybe DNS are related. It's also the right course of action if you're in a rare situation not to use DHCP to get network information for your computers or other Internet connections To change DNS servers on your router, look for text fields marked as DNS, usually in the DNS Address section, most likely in the settings or basic settings in the router management web interface, and enter new addresses. Microsoft has changed the wording and location of network-related settings with each new release, but you can still change DNS servers in Windows, whether you're using Windows 10, XP, or some other version. Setting up your Mac's DNS settings involves a different process. Using an android device? See our guide to changing DNS servers on Android if you need help. Help. what is my dns server android. what is my dns server address. what is my dns server on android. what is my dns android