Network basics: Part 3 - DNS Server

A DNS server is a server that contains a database of public IP addresses and hostnames associated with them. In most cases, the DNS server is used to resolve or translate those common names into IP addresses as required.

This is the next installment of the Basic Knowledge series for beginners and learn about computer networks. After two introductions of Hub and Switch, Router, the content of this article refers to the operation of DNS servers (domain systems).

This is also the last part we talk about how computers in a network segment share a common IP address space. Invite you to follow along.

Basic DNS Server knowledge

1. What is a DNS Server?
2. Why need DNS server?
3. DNS server and malware
4. More information about DNS server
5. DNS Root Server

What is a DNS Server?

As we all know, when a computer needs to access information on a machine located on another network or network segment, it needs the help of a router. The router will transfer the necessary data packets from one network to another (such as the Internet). If you have read the second part, you probably remember, we have given an example to create a reference to the IP address associated with a website. In order to access this website, your Web browser must know the website's IP address. Then the browser provides the address for the router, the router determines the route to the other network and requests the data packets to the appropriate destination. Each website has an IP address but you can visit these websites daily without caring about that number. In this article we will show you why it is possible.

The IP address is the same as the home address. It consists of a network location (a sequence of numbers indicating the segment of the computer network in operation), similar to the street name; and device location (identify a specific computer in the network), similar to the house number. Knowing IP addresses is a requirement for basic TCP / IP communication between two computers.

When you open a Web browser and enter the website name (known as the Universal Resource Locator), the browser will go straight to the website without needing to by entering the IP address. You can imagine the process of opening a website just like the process of sending mail to the receiving address on the envelope at the

post office. The IP address in network communication acts as the address on the envelope. The letter cannot arrive at the right place if you just write the recipient's name but "forgot" their address. The same is true for coming and opening a website. Your computer cannot contact the website unless it knows the IP address of the website.

But you do not need to type in the IP address but the browser can still open the correct website when you enter the domain name. So where is the IP address? The process of "translating" a domain name into an IP address is the work of a DNS server (domain system host).

A DNS server is a server that contains a database of public IP addresses and hostnames associated with them . In most cases, the DNS server resolves or translates domain names into IP addresses as required. DNS servers run special software and communicate with each other using special protocols. In a more understandable way: The DNS server on the Internet is the **TipsMake.com** URL translation device you type in the browser address bar into an IP address 123.30.180.60.

Note: Other names of DNS servers include the name server / nameserver and domain name system server.

In the previous two articles we talked about some of the concepts of a computer's TCP / IP configuration, such as the IP address, subnet mask, and default gateway. See Figure A below and you will see another "Preferred DNS server" configuration option.

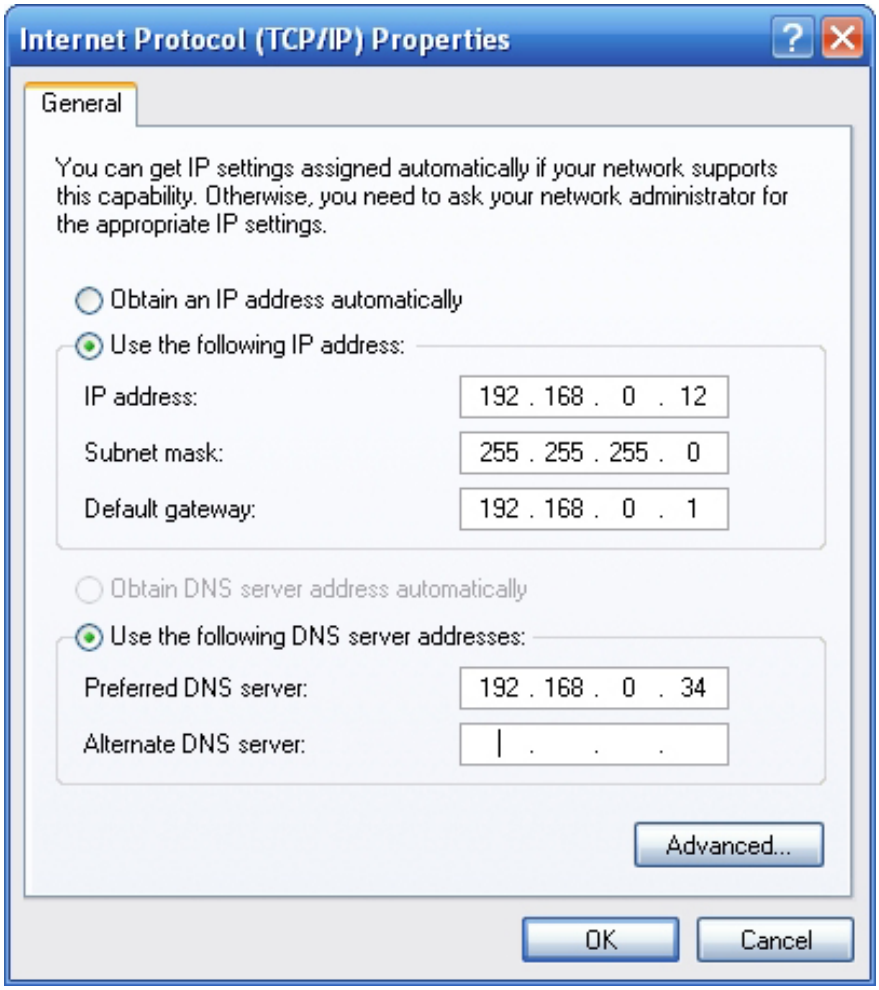
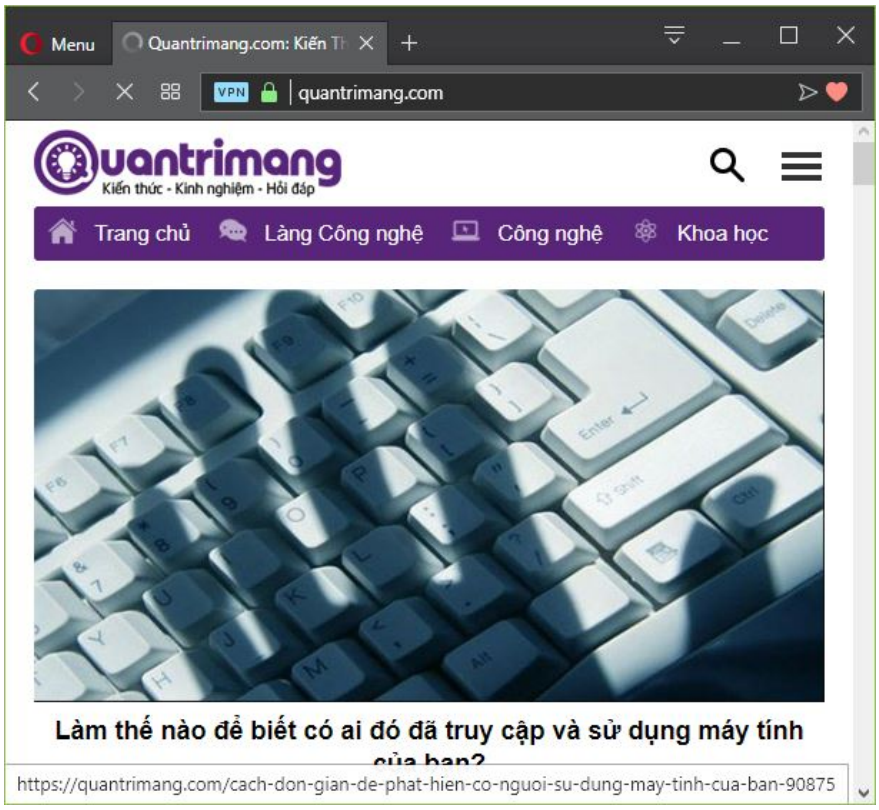


Figure A : Preferred DNS Server option is defined as part of the TCP / IP configuration in the computer.

As you can see in the figure, the " *Preferred DNS server* " option is defined as part of the TCP / IP configuration. This means that the computer will always know the IP address of the DNS server. This is very important because the computer cannot communicate with another computer using the TCP / IP protocol if it does not know the IP address of the other computer.

Why need DNS server?

This question can be answered with another question: Do you see 123.30.180.60 or quantriamng.com easier to remember? Most people will answer that remembering a phrase like quantrimang is much simpler than a sequence of numbers.



When you enter quantrimang.com into your web browser, all you need to remember is the URL https://quantrimang.com/. The same is true for any other website like Google.com, Amazon.com, etc. We are human, so we remember the words in the URL much easier than the numbers in the IP address. . Other computers and network devices will be responsible for understanding the IP address. Therefore, the DNS server plays a role in helping users use an easy-to-remember name to access the site, while also helping the computer to use the IP address to access that site. DNS server is an 'interpreter' between hostname and IP address.

Now we will look at what happens when you try to visit a website. The process begins with opening the Web browser and entering the URL. At that time, the browser knows that it cannot locate the website based on the URL alone. Therefore it queries the IP address information of the DNS server from the computer's TCP / IP

configuration and passes the URL to the DNS server. The DNS server then looks up the URL on the table with the website's IP address list. It then returns the IP address for the Web browser and the browser can contact the requested website.

Actually this explanation process can be described a bit simpler. Domain name resolution in DNS can only work if the DNS server contains a record corresponding to the requested website. If you go to a random website, the DNS server will not have a record of this website. The reason is because the Internet is so big. There are millions of new websites and websites created every day. There is no way for a single DNS server to keep up with all websites and meet all requests from anyone who has access to the Internet.

Now suppose a single DNS server can store logs for every website that exists. If the server's capacity is not a problem, the server will also be overwhelmed by requests for name processing received from Internet users everywhere. A centralized DNS server is often a very popular target of attacks.

Therefore, DNS server servers are often distributed to multiple points, preventing a single DNS server from providing name resolution for the entire Internet. The Internet Corporation for Assigned Names and Numbers (or ICANN) is currently available worldwide. Because managing domain names for the entire network is a huge undertaking, ICANN allocates multiple domain responses to different firms. For example, Network Solutions is responsible for the ".com" domain name. But does not mean Network Solutions maintains a list of IP addresses associated with all .com domains. In most cases, Network Solution's DNS server contains records that point to the DNS server that is considered official for each domain.

To see how it all works, imagine that you want to go to the quantrimang.com website. When entering a request into the browser, the browser sends the URL to the DNS server host specified by the TCP / IP configuration of your computer. DNS server server does not know the address of this website. Therefore, it sends requests to ICANN's DNS server. ICANN's DNS server also does not know the IP address of the website you are trying to visit but only the IP address of the DNS server responsible for the domain name ending in .COM. It will return this address to the browser and during the return process it also executes the request to that particular DNS server.

The highest DNS server level for domain names ending in .COM will not know the IP address of the requested website, but it knows the IP address of the official DNS server for the brienposey.com domain. It will send this address back to the requesting machine. The Web browser then sends the DNS query to the authoritative DNS server for the requested domain. And this DNS server will return the website's IP address, allowing the machine to contact the website it requests.

As you can see, there are many steps that must be completed for a computer to find the IP address of a website. In order to reduce the number of DNS queries that must be performed, the results of these queries are usually stored for several hours or days, depending on how the machine is configured. Storing IP addresses greatly improves performance and minimizes the amount of bandwidth consumed for DNS queries. You can imagine how bad the Web browsing process would be if your computer had to perform a full set of DNS queries any time you wanted to see the new Web page.

DNS server and malware

Running an antivirus program is very important. One reason is that malware can attack your computer by changing the DNS server settings. And this is definitely something you don't want to happen.

For example, your computer is using DNS server of Google 8.8.8.8 and 8.8.4.4. In these DNS servers, accessing the bank website (with that bank's URL) will load the website correctly and allow you to log in to your account.

However, if malicious software changes your DNS server settings (which may occur without your knowledge), entering the same URL may take you to a completely different site or similar site but not the website you need to visit. This fake bank website may look exactly like the real website but instead of letting you log in to your account, it will record your username and password, providing the attacker with all Your bank account information.

However, often, malware infiltrates your DNS server often only redirects popular sites to websites with fake ads or websites that make you think you have to buy the program to do it. Clean the computer infected with the virus.

There are two things you should do to avoid becoming a victim in this way. The first is to install an antivirus program so that malicious programs are removed, before they can cause any damage. The second is to look at what the site looks like. If it is slightly different than usual or you receive a **"invalid certificate" message** in your browser, it may be a sign that you are visiting a fake website.

More information about DNS server

In most cases, two DNS servers, primary and secondary servers, are automatically configured on your router and / or computer when connected to the ISP via DHCP. You can configure two DNS servers in case one of them fails, then the device will use the secondary server.

While many DNS servers are operated by ISPs and are intended to be used only by customers, some public servers are also available. See the list of DNS servers for details and how to change DNS servers, if you need help making changes.

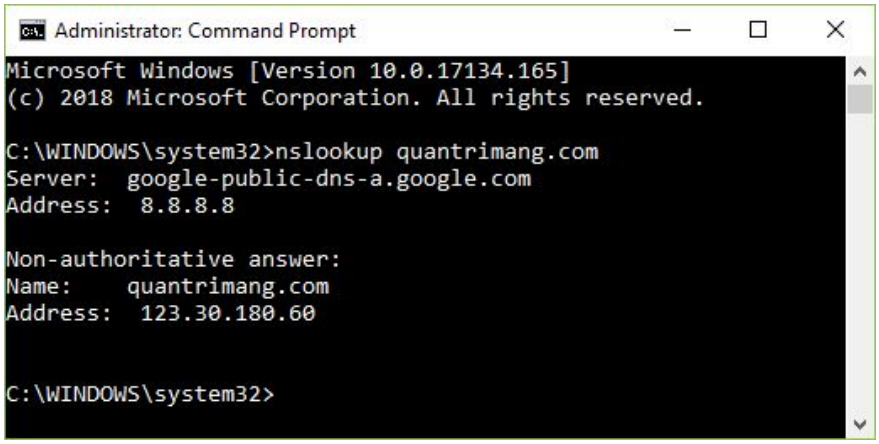
Some DNS servers can provide faster access times than other servers, but only based on the time your device accesses the DNS server. For example, if your ISP's DNS server is closer to Google's DNS server, you may find that addresses are resolved faster, using default servers from your ISP, not third-party servers. .

If you encounter a network problem that cannot load the website, there may be a problem with the DNS server. If the DNS server cannot find the correct IP address associated with the hostname you entered, the site will not load. Again, this is because the computer communicates via the IP address, not the hostname, so the computer does not know what you are trying to reach unless it can use the IP address.

The "closest" DNS server installation to the device is the settings that will be applied. For example, while your ISP may use a set of DNS servers, apply to all routers connected to it, your router may use another DNS server installer for all devices. being connected to that router. However, a computer connected to the router can use its own DNS server settings to override the settings of both the router and the ISP. Tablets, phones, etc. are similar.

The article explained above about how malicious programs can control your DNS server settings and override them with servers that redirect your site requests elsewhere. Sure, this is what scammers can do, but it is also a feature found in some DNS services like OpenDNS, of course for good. For example, OpenDNS can redirect adult websites, gambling sites, social networking sites and more, to the **"Blocked"** page **,** but you have full control over redirects.

The **nslookup** command is used to query your DNS server.



Let's start by opening the Command Prompt tool and then typing the following:

```
nslookup quantrimang.com
```

And the result will look like this:

```
Server: google-public-dns-a.google.com Address: 8.8.8.8 Non-authoritative answer
```

In the above example, the command nslookup tells you the IP address (or some IP addresses in this case), but the quantrimang.com address you enter in the browser search bar can be translated.

DNS Root Server

There are several DNS servers located in the connection of the computer that we call the Internet. Most importantly, the 13 DNS Root Server stores the complete database of their related domain names and public IP addresses.

These top-level DNS servers are named with the first 13 letters of the alphabet (from A to M). 10 of these servers are located in the US, one in London, one in Stockholm and one in Japan.

Conclude

In this article we have explained how the DNS server is used to process domain names for IP addresses. Although the process described seems quite simple, remember that ICANN and high-level DNS registrars like Network Solutions use load balancing technology to distribute requests across multiple DNS servers. other. This prevents servers from overflowing and eliminates the possibility of single point errors.

See more:

1. What is DNS and DNS Lookup?
2. Some ways to fix DNS Server Not Responding on Windows 7/8/10