About Node.js DNS

The Domain Name System (DNS) turns domain names into IP addresses, which browsers use to load internet pages. Every device connected to the internet has its own IP address, which is used by other devices to locate the device. DNS servers make it possible for people to input normal words into their browsers, such as Fortinet.com, without having to keep track of the IP address for every website

The Node.js DNS module contains methods to get information of given hostname. Let's see the list of commonly used DNS functions:

* dns.getServers()
* dns.setServers(servers)
* dns.lookup(hostname[, options], callback)
* dns.lookupService(address, port, callback)
* dns.resolve(hostname[, rrtype], callback)
* dns.resolve4(hostname, callback)
* dns.resolve6(hostname, callback)
* dns.resolveCname(hostname, callback)

Example 1:

Let's see the example of dns.lookup() function.

1. const dns = require('dns');
2. dns.lookup('www.javatpoint.com', (err, addresses, family) =**>** {
3. console.log('addresses:', addresses);
4. console.log('family:',family);
5. });

Example 2: et's see the example of resolve4() and reverse() functions.

1. const dns = require('dns');
2. dns.resolve4('www.javatpoint.com', (err, addresses) =**>** {
3. if (err) throw err;
4. console.log(`addresses: ${JSON.stringify(addresses)}`);
5. addresses.forEach((a) =**>** {
6. dns.reverse(a, (err, hostnames) =**>** {
7. if (err) {
8. throw err;
9. }
10. console.log(`reverse for ${a}: ${JSON.stringify(hostnames)}`);
11. });
12. });
13. });

## What is a DNS Server?

A DNS server is a computer with a database containing the public IP addresses associated with the names of the websites an IP address brings a user to. DNS acts like a phonebook for the internet. Whenever people type domain names, like Fortinet.com or Yahoo.com, into the address bar of web browsers, the DNS finds the right IP address. The site’s IP address is what directs the device to go to the correct place to access the site’s data.

Once the DNS server finds the correct IP address, browsers take the address and use it to send data to content delivery network (CDN) edge servers or origin servers. Once this is done, the information on the website can be accessed by the user. The DNS server starts the process by finding the corresponding IP address for a website’s uniform resource locator (URL).

## How Does DNS Work?

In a usual DNS query, the URL typed in by the user has to go through four servers for the IP address to be provided. The four servers work with each other to get the correct IP address to the client, and they include:

1. **DNS recursor**: The DNS recursor, which is also referred to as a DNS resolver, receives the query from the DNS client. Then it communicates with other DNS servers to find the right IP address. After the resolver retrieves the request from the client, the resolver acts like a client itself. As it does this, it makes queries that get sent to the other three DNS servers: root nameservers, top-level domain (TLD) nameservers, and authoritative nameservers.
2. **Root nameservers**: The root nameserver is designated for the internet's DNS root zone. Its job is to answer requests sent to it for records in the root zone. It answers requests by sending back a list of the authoritative nameservers that go with the correct TLD.
3. **TLD nameservers**: A TLD nameserver keeps the IP address of the second-level domain contained within the TLD name. It then releases the website’s IP address and sends the query to the domain’s nameserver.
4. **Authoritative nameservers**: An authoritative nameserver is what gives you the real answer to your DNS query. There are two types of authoritative nameservers: a master server or primary nameserver and a slave server or secondary nameserver. The master server keeps the original copies of the zone records, while the slave server is an exact copy of the master server. It shares the DNS server load and acts as a backup if the master server fails.

## **Some of the Best DNS Servers**:

Here are some of the top DNS servers available:

1.         **Cloudflare 1.1.1.1.**This is a simple-to-use DNS service that comes with tutorials for all of the most popular operating systems, such as Mac, Windows, Android, iOS, and Linux. Users can also use Cloudflare’s service to block adult content.

2.         **Google Public DNS.** The Google Public DNS service is different from Cloudflare’s in that it is designed for more technically adept users. But you can find tutorials if needed.

3.         **Quad9.** Quad9’s DNS service is renowned for its fast performance. It also claims to block malicious sites using threat intelligence data.

### **What is a DNS Revolver**?

A DNS resolver is also referred to as a recursive resolver. It is designed to take DNS queries sent by web browsers and applications. The resolver receives the website URL, and it then retrieves the IP address that goes with that URL.