Recap

Domain Name System

# Brief on DNS

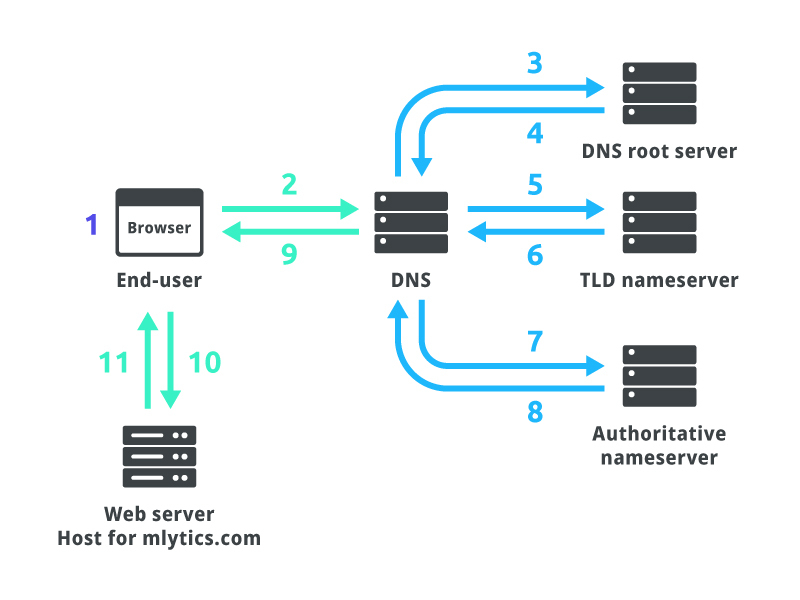
The Domain Name System (DNS) is conceived of as a sort of tree. At the very top are about a dozen root servers, which are the ultimate authority for all the various other DNS units of organization of the Internet, starting with the Top-Level Domains (TLDs): .com, .org, .net, and so on. Each TLD has a set of zones for which it is the authoritative source of information on the next level down. This structure continues down to the millions of individual DNS servers on the Internet.

# DNS and web browsing

For example, let's look at the address:

www.sonyliv.com/shows/crime-patrol

1. Your local DNS client, called a resolver, looks in its local list of addresses it knows. If you've browsed that page recently, you have the address cached on your computer, and can get the page.
2. If your local resolver doesn't have the address cached, it checks with a DNS server that it's been told is the next level up in the DNS hierarchy. This may be another caching resolver or a DNS server somewhere on the network.
3. The request gets sent further up the DNS tree — usually to a root or authoritative server — and works its way back down until it finds the specific entry that points to the server you requested. In this case, it knows where www is, and then it goes to the sonyliv.com DNS servers, which then directs us to the page we want.



Troubleshooting

Domain Name System

# Pre-Requisite (Bind-utils Package)

Bind-utils contains a collection of utilities for querying DNS (Domain Name System) name servers to find out information about Internet hosts. These tools will provide you with the IP addresses for given host names, as well as other information about registered domains and network addresses.

[More on bind-utils package.](https://www.mankier.com/package/bind-utils)

# Tools and Commands Useful for Troubleshooting

Let's look at some basic tools for troubleshooting when we think DNS might not be working correctly.

1. **ping**

The ping command is a utility that tests the connectivity between two devices on a network by sending packets and measuring the time it takes for them to be returned. The ping command is commonly used to troubleshoot network connectivity issues, determine the response time of a network resource, or simply verify if a host is up and reachable.

Syntax: ping [options] hostname\_or\_ip\_address

Some commonly used options for the ping command include:

* -c count: Specifies the number of packets to send. By default, ping will continue sending packets until stopped.
* -i interval: Specifies the time, in seconds, to wait between sending packets.
* -a: Audible pings (Linux). Resolve addresses to hostnames (Windows).
* -4 or -6: Request IPv4 or IPv6 address.

1. **nslookup**

nslookup is a command-line tool used to query the Domain Name System (DNS) to obtain information about domain names and IP addresses. It is commonly used to troubleshoot DNS resolution issues, such as when a hostname cannot be resolved to its corresponding IP address.

Syntax: nslookup [options] [hostname\_or\_ip\_address] [server]

Some commonly used options for the nslookup command include:

* server NAME: set the default server to NAME, using the current default server.
* set type=X: set query type (ex. A, AAAA, A+AAAA, ANY, CNAME, MX, NS, PTR, SOA, SRV)
* set all: print options, current server, and host.
* help or “?”: print info on common commands.

1. **dig**

dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use, and clarity of output. Other lookup tools tend to have less functionality than dig.

Syntax: dig @server name type

Some commonly used options for the dig command include:

* -4 or -6: forces dig to only use IPv4/IPv6 query transport.
* -t: sets the query type.
* -x: indicate a reverse lookup.

Some commonly used query options for the dig command include:

* +short: Display only the answer section of the query, which provides the IP address or other requested information.
* +nocmd: Suppress the command line used to run dig and the version number from the output.
* +noquestion, +noauthority, +noadditional: Suppress respective sections from the output.
* +nssearch: Attempt to find the authoritative name servers for the zone containing the name being looked up and display the SOA record that each name server has for the zone.
* +noall: Clear all display flags.
* +trace: Tracing of the delegation path from the root name servers for the name being looked up. When tracing is enabled, dig makes iterative queries to resolve the name being looked up. It will follow referrals from the root servers, showing the answer from each server that was used to resolve the lookup.

[More on dig command (man page)](https://linux.die.net/man/1/dig)

1. host

Like nslookup and dig, host is another tool for querying DNS servers.

Options for the dig command include:

* -a: Equivalent to -v -t ANY.
* -i: Reverse lookups.
* -t: Specify query type.
* -v: Verbose output.

# DNS Return Codes

The following table explains the DNS return codes that can be returned when doing a DNS query and may appear in the logs. Each return code has its purpose in the DNS infrastructure.

Graphical user interface, table

Description automatically generated

# Miscellaneous DNS Troubleshooting

In a Linux-based system, the following files are relevant to the Domain Name System (DNS) configuration:

* /etc/resolv.conf: This file contains the configuration settings for the local DNS resolver, including the IP addresses of the name servers to be used for DNS queries.
* /etc/nsswitch.conf: This file specifies the order in which different name service databases, such as DNS, NIS, and local files, are searched for information about hostnames and other network-related information.
* /etc/hosts: This file is a simple, static mapping of IP addresses to hostnames that is used as a fallback for DNS resolution when a DNS server is not available.
* Using a packet capture tool, such as tcpdump or Wireshark, to capture and analyze network traffic related to DNS queries and responses. This can be useful for identifying issues such as misconfigured name servers or incorrect DNS records.
* Using a DNS performance testing tool, such as dnsperf or resperf, to test the performance and efficiency of a DNS server. This can be useful for identifying issues such as slow or inefficient DNS resolution, or for comparing the performance of different DNS servers.
* Verifying the configuration settings of a DNS server, such as BIND or UNBOUND, to ensure that it is correctly configured and serving correct information to clients. This can include checking the validity of DNS records and the configuration of zones, as well as ensuring that the server is properly configured to respond to client queries.
* /var/log/syslog and /var/log/messages: These logs may contain messages related to DNS resolution and other network-related issues and can be useful for troubleshooting DNS problems.