FACT SHEET

WHAT IS A ROOTSERVER?

What is a root server?
Root name servers are the servers at the root of the Domain Name System (DNS) hierarchy.

The DNS is the system which converts Internet domain names, such as www.netnod.se, into numeric addresses such as 192.71.80.109 or 2a01:3f0:1:3::109. DNS includes a hierarchy of "authoritative name servers", each level of which contains different pieces of information. To translate www.netnod.se, a resolver – the name server a user queries directly – first has to figure out where .se is, then netnod.se, and finally www.netnod.se.

The authoritative name servers that the resolvers use to find top level domains (like .se) are the root name servers.

The root zone
The root servers contain the information that makes up the root zone, which is the global list of top level domains. The root zone contains:

- generic top level domains – such as .com, .net, and .org
- country code top level domains – two-letter codes for each country, such as .se for Sweden or .no for Norway
- internationalised top level domains – generally equivalents of country code top level domain names written in the countries' local character sets

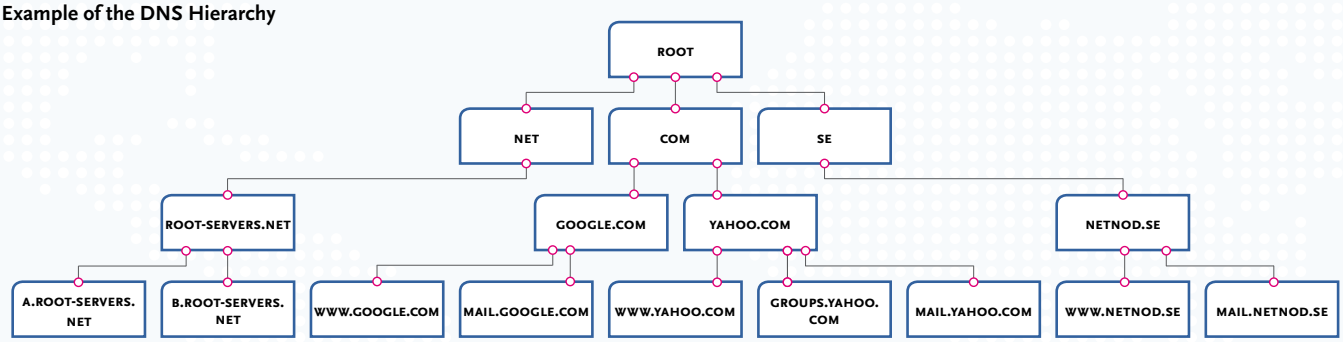
For each of those top level domains, the root zone contains the numeric addresses of name servers which serve the top level domain's contents, and the root servers respond with these addresses when asked about a top level domain.

Who operates them?
The root servers are operated by 12 different organisations:

- Verisign
- University of Southern California
- Cogent
- University of Maryland
- NASA AMES Research Center
- Internet Systems Consortium
- US Department of Defense
- US Army Research Lab
- Netnod
- RIPE
- ICANN
- WIDE

Many of these organisations have been operating root servers since the creation of the DNS; and the list shows the Internet's early roots as a US-based research and military network.

Example of the DNS Hierarchy



FACT SHEET

What is a rootserver?

Where they are?

There are more than 300 root servers scattered around the world, on all six populated continents. They are reachable using 13 numeric IP addresses – one per operating organisation, except for Verisign, which has two. Most of those addresses are assigned to multiple servers scattered around the world, so DNS queries sent to those addresses get fast responses from local servers. This was not always the case. A decade ago there were only 13 root servers – one per IP address – and all but three were in the United States. However, significant efforts by several of the root server operators, including Netnod, have expanded the root server footprint over the last ten years.

Because there are only 13 root server IP addresses, only 13 root servers can be seen from any single location at any given time. Different servers (using the same IP addresses) will be seen from different locations.

Who is responsible for them?

Each operating organization is solely responsible for the root server IP address (or addresses) it operates. The operating organisation determines how many locations that IP address will be served from, what those locations are, what hardware and software will be installed in each location, and how that hardware and software will be maintained. Some operators operate only a single location, while others operate many (one operator is responsible for almost 100). Each organisation secures its own operating funds.

Where does the root zone come from?

The root zone comes from the Internet Assigned Numbers Authority (IANA), which is part of the Internet Corporation for Assigned Names and Numbers (ICANN). It is signed using DNSSEC signatures to ensure authenticity, and issued to the root server operators to publish to their root servers. The root server operators publish the root zone as written, and have no authority to alter the content.

How do resolvers find root servers?

Since root servers are at the root of the DNS hierarchy, it isn't possible to walk through the DNS hierarchy to find them: the resolvers wouldn't know where to look. Instead, there is a list of well-known and rarely changed root server IP addresses, and every DNS resolver has that list of IP addresses included with the software. If a root server does need to change addresses – something that has happened twice in the last ten years – this does not present a significant problem. Older resolvers continue to work by using the other 12 root server addresses, and their list gets updated when their software is updated.

Fault tolerance

While root servers are critical infrastructure, the failure of a single root server won't be noticed by most Internet users. Individual servers that fail should withdraw their address announcements, allowing queries to be answered by a different server responding to the same address. If all instances of a single address are unreachable, either in general or for a specific part of the world, there are 12 more root server IP addresses to choose from. The chances of all 300+ root servers or all 13 root server IP addresses being unreachable at once are very small, and the root server system is, thus, very reliable.

More information

The following websites have more information on the root server system:

- **Root Server Technical Operations Association**
  http://www.root-servers.org/
- **Internet Society Briefings on the root servers**
  http://www.isoc.org/briefings/019/
  and
  http://www.isoc.org/briefings/020/