



Secure Operation of Top Level Domains

What functions are vital to ensure a high degree of security in the domain name system?

.nudomain

This report by the National Post and Telecom Authority of Sweden was translated from the original Swedish into English and printed for distribution at the July 19 - 23 meetings of ICANN in Kuala Lumpur, Malaysia, by .NU Domain Ltd as a public service.

Preface

In the Appropriation Directions for the 2004 Fiscal Year, the Swedish government instructed the National Post and Telecom Authority (PTS) to examine, in close cooperation with Internet operators and other stakeholders, which functions relating to the operation and administration of top level domains are crucial to a high level of security in the domain name system. In recent years, the PTS has examined a number of issues concerning the safety, accessibility and availability of the Internet, and this report builds upon that earlier work.

The report was prepared by Anders Rafting and Christoffer Karsberg at the PTS department for network security.

Table of Contents

Summary	6
1 Instruction from the Government to PTS.....	6
1.1 Instruction	7
1.2 Objective of this study	7
1.3 Methodology	7
1.3.1 Confines of the study	7
1.3.2 Onsite visits	7
1.3.3 Consultation.....	7
1.3.4 Misc. Data collection	7
2 Security for top level domains is crucial.....	8
2.1 There must be a high level of security in the domain name system.....	8
2.2 What constitutes a high level of security for top level domains?	8
2.3 Common top level domains in Sweden	8
2.4 Why are top level domains important?.....	8
2.5 Threats to important functions in the top level domain system.....	8
3. The different aspects of operating a top level domain.	10
3.1 What is the role of top level domains in the domain name system?.....	10
3.2. Customer relations are managed through accredited registrars.....	11
3.3.1 A top level domain is constructed from the customer database	11
3.3.2 Access must be secure	12
3.3.3 Sensitive data in the Whois database must be protected	12
3.4. How is the top level domain master created and maintained?	12
3.5 Security must be ensured for transfers to slave servers	12
3.6 Top level domain responsibilities	13
3.6.1 Security in slave server operation	13
3.6.2 The top level domains' name servers must be known to the outside world	13
3.6.3 Monitoring is key to manage accessibility and security	14
3.6.4 Qualified staff is a crucial element.....	14
3.7 What are the responsibilities of other parties?.....	14
3.7.1 The responsibility of the root domain administrator	14
3.7.2 The responsibility of second level domain administrators	15
3.7.3 The responsibility of second level domain owners.....	15
3.7.4 The responsibility of users.....	15
4. The Security of top level domains important to Sweden	16

4.1	The .se domain	16
4.1.1	Administration of the .se domain	17
4.1.2	Registrars	17
4.1.3	Operation of the .se domain	18
4.1.4	Monitoring system	21
4.1.5	Disaster planning	22
4.1.6	DNSSEC and IPv6	22
4.1.7	Considerable increase in the number of new .se domains	23
4.2	The .com domain	23
4.2.1	Administration of .com	23
4.2.2	Registrars	23
4.2.3	Operation of the .com domain	24
4.2.4	Monitoring	24
4.2.5	Disaster planning	24
4.2.6	DNSSEC and IPv6	24
4.3	The .nu domain	24
4.3.1	Administration of .nu	24
4.3.2	Registrars	25
4.3.3	Operation of the .nu domain	25
4.3.4	Monitoring	26
4.3.5	Disaster planning	26
4.3.6	DNSSEC and IPv6	26
5.	Which functions are important to a high level of security for top level domains?	27
5.1.	Security in the operation of a top level domain	27
5.2	Security in the administration of a top level domain	28
6	New functions for increased security	29
6.1	A new standard for a more secure information management in the domain system is on its way	29
6.2	Anycast – a new addressing method	30
6.3.	Anyone may get an IP address with the new Internet Protocol	31
6.4	DNS Development continues	31
Sources		33
Appendix 1 – Political Context and Management Principles		35
Appendix 2 - How does the domain name system (DNS) work?		38
Appendix 3 – IP Protocol and IP addresses?		61
Appendix 4 - Glossary		63

Summary

The National Post and Telecom Agency has been assigned by the government to survey which functions in the operation and administration of top level domains (TLDs) are of importance for good security of the domain name system. Access to correct information from the name servers for top level domains is vital for access to the web and e-mail by users, whose addresses are found in various second-level domains, for example 'pts.se', which are registered by businesses, authorities, organizations and individuals. The three most important top level domains, with regard to the number of domain names registered in Sweden, are the .se domain, .com domain and the .nu domain.

An administrator of a top level domain is responsible for a complex system with a number of important functions that must be safeguarded to be able to offer and maintain its services. In order to be able to provide a name service with high accessibility it is critical that there are personnel who are sufficiently competent to manage the systems and create protection against unauthorized access and that they are continuously updated about the latest news within their field. It is important that the resources are available to permit technical developments to be monitored and to work preventively to reduce vulnerability to physical and logical attacks and disturbances. Having an emergency preparedness plan in place to maintain a high level of service is mandatory.

A top level domain is responsible for answering correctly, and with sufficient speed, inquiries to the domain name system concerning the top level domain. This is accomplished, to a large degree, through its slave servers. It is very important that the same information is available on all slave servers and that it is correct. To safeguard the operation of slave servers, diversity should be applied at different levels. The slave servers should be managed by different contractors with different organizational affiliation in geographically separate and secure places. In each instance, there must be sufficient server capacity and redundant connection to various Internet operators or the possibility to simply connect to other Internet operators. Contracts between the top level domain administrators and each slave server operator should be in place to regulate the commitments of the slave server operators.

An administrator of a top level domain is responsible for its part of the Internet, but many other parties are involved in ensuring that the domain name system will work. An absolutely decisive factor is the actual transport of the information of the domain name system, which is conducted via Internet operators that must provide functional networks.

1 Instruction from the Government to PTS

1.1 Instruction

In the Appropriation Directions for the 2004 Fiscal Year, the Government gave the following instruction to the National Post and Telecom Authority:

“The National Post and Telecom Authority shall, in co-operation with Internet operators and other stakeholders, determine which functions relating to the administration and operation of top level domains are important to ensure a high level of security in the domain name system. The Authority shall report back to the Government no later than May 19, 2004.”

1.2 Objective of this study

The aim of this study is to determine which functions, relating to the management of top level domains, are important to ensure a high level of security in the domain name system (DNS). The ultimate objective is to get a clearer picture of what needs to be done in this area of the Internet to ensure a high level of security in the DNS.

1.3 Methodology

1.3.1 Confines of the study

Aside from a general overview of the main characteristics of top level domains, this study is confined to the conditions affecting the three most common top level domains in Sweden, i.e. .se, .com and .nu.

1.3.2 Onsite visits

In order to gather up-to-date information from the sources, onsite visits were undertaken at the head offices and operations centers of the top level domain administrators Verisign and .Nu Domain, which administer .com and .nu respectively. These visits were followed by further meetings and e-mail exchanges.

1.3.3 Consultation

As regards the national top level domain for Sweden, consultation has taken place between PTS and NIC-SE and with the latter's owner, the II-foundation. PTS has also consulted with .Nu Domain, and to a lesser extent, with Verisign. Information was gathered through study visits, meetings and other contacts, as well as through access to documents describing operational issues. In addition, PTS consulted with Internet operators to gather information about their obligations regarding the distribution of DNS information.

1.3.4 Misc. data collection

PTS has used information and data that was gathered for previous studies relating to inter alia, the administration of the domain name system. Information has also been collected by following the work and discussions taking place in the framework of Internet Corporation for Assigned Names and Numbers (ICANN) and its Governmental Advisory Committee (GAC) and other committees advising and supporting ICANN, such as the Country Code Name Supporting Organization (ccNSO), the Generic Name Supporting Organization (gNSO) and the Security and Stability Advisory Committee (SSAC), as well as, national and international groups working on issues relating to a stable and secure management of DNS.

2 Security for top level domains is crucial

Detailed information on government IT policy, pending legislative proposals concerning the national top level domain in Sweden, principles for the management of top level domains and related issues is given in Appendix 1. Detailed information about the workings of DNS is given in Appendix 2.

2.1 There must be a high level of security in the domain name system

Society expects a high level of Internet security, and this also applies to DNS. A number of distinct functions are necessary in order to guarantee that correct and sufficiently fast answers are continuously given to queries submitted to DNS. This report specifically addresses those functions in the management and administration of top level domains that are crucial to a high level of security in the DNS.

2.2 What constitutes a high level of security for top level domains?

For the purposes of this report, a high level of security means that information given in response to queries to the top level domains' name servers is available continuously without interruptions or disruptions, is sufficiently fast and that the information supplied is correct.

2.3 Common top level domains in Sweden

The three most important top level domains in Sweden, on the basis of the number of registered domain names, are the .se domain with approximately 246,000 domains; the .com domain with approximately 160,000 domains; and the .nu domain with approximately 84,000 domains. Data on the number of domains with dedicated Web servers, published by the company Security Space in May 2004, indicates that there are just over 7 million such domains for the .com domain, approximately 49,000 for the .nu domain and approximately 48,000 for the .se domain.

2.4 Why are top level domains important?

Access to and retrieval of accurate DNS information from name servers for top level domains is of crucial importance for access to second-level-owned companies, organizations and individuals. Below these second level domains, users find domain names and IP addresses for different sources of information and electronic mail—for example `www.pts.se` or `mail.pts.se`. DNS has a hierarchical structure with top level domains being at the second highest level, immediately below the root. There are currently 244 national top level domains (country code Top Level Domains [ccTLDs]) e.g. .se, .nu and 14 generic Top Level Domains (gTLDs) e.g., .com, net, org and name. In addition, ICANN has received applications for a about 10 additional gTLDs , as well as, for the new top level domain .eu for the European Union.

2.5 Threats to important functions in the top level domain system

A number of vulnerabilities in the traffic flow between top level domains and other areas of the DNS can be identified. Examples of these include:

Large quantities of illegal traffic—for example, in the form of a DOS-attack (Denial of Service) toward a name server—might result in the server being overburdened and thus not able to respond to legitimate DNS queries. This may result in users being unable to send e-mail or access Web servers. Defensive measures to counter this event include having several name servers sharing the load, ideally using anycast technology (see Chapter 6 for further details), and having name servers that are spread across the net and connected to different ISPs.

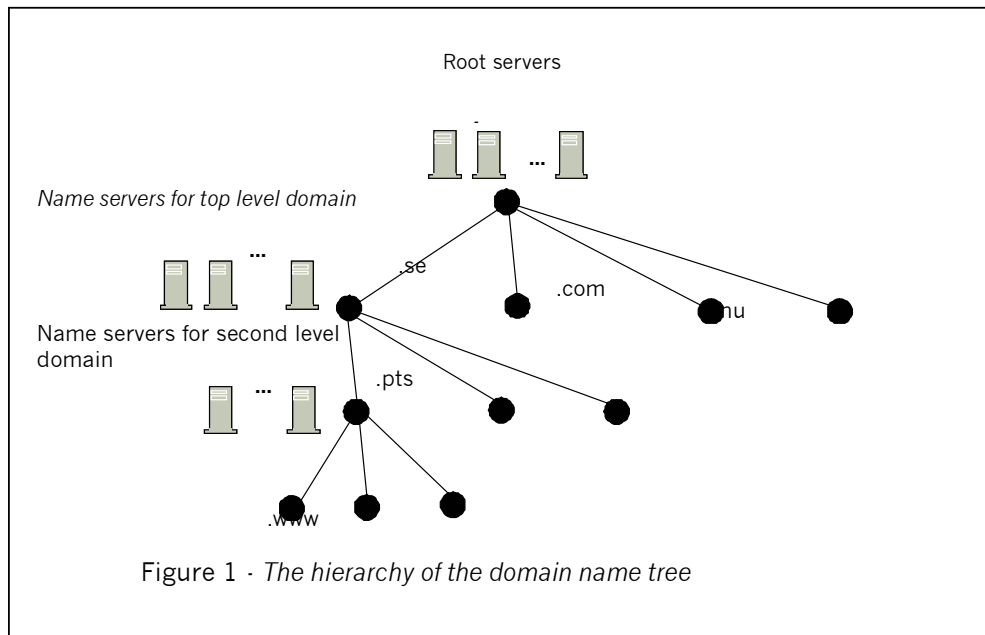
- Where security verification for access to the master server is too weak, there is a risk that unauthorized modification of data on the master server or in the customer database may occur. To control this, advanced functions for verification of identity and access rights are required.
- If there is no authentication of senders, an attack on a slave server may result in a false zone file being retrieved from a server purporting to be a master. Therefore, it is important to ensure that there always is a function verifying that the content comes from the appropriate sender, and that it has not been modified during transmission.
- An insufficiently protected resolver, which stores DNS information in its cache (i.e. it saves previously retrieved information for a certain time in order to avoid having to resubmit the query too often), may suffer from unauthorized modification of the information in its cache (so-called cache poisoning). This may, in turn, result in an incorrect IP address being given in response to queries until the time when the cached information expires, which may take several days. The life of cached data is determined by the TTL (Time to Live) parameter (see Appendix 2 for further details). The end result is that, although a correct Web address has been entered in the browser's address bar, the user will be directed to the wrong Web server, which causes confusion for both the user and the owner of the requested home page. Consequently, the resolver function must be protected from unauthorized access and other attacks.
- A user who thinks that he/she is connected to a particular resolver may be duped, by means of address spoofing, into connecting to a completely different computer. The result is similar to that in the previous case.

3. The different aspects of operating a top level domain.

- A top level domain administrator is responsible for domain names and the operation of name servers in *its* section of the Internet.
- Customer relations are managed through accredited registrars.
- The customer database is maintained by the top level domain administrator and it contains DNS information and other contact data for customers.
- The zone file with DNS information is extracted from the customer database and distributed to the slave servers for the top level domain.
- The registrars use some form of secure connection to register or modify data in the customer database.
- Monitoring is necessary in order to guarantee the DNS service.
- Qualified staff is required to maintain the complex systems used for top level domains.
- Changes relating to the addresses for the top level domains' name servers are submitted to ICANN/IANA which manages the root domain.
- Second level domains are generally managed by ISPs.
- It is important that owners of second level domains have SLAs with the organizations managing second level domains.

3.1 What is the role of top level domains in the domain name system?

The hierarchical organization of the domain name system is reflected in its technical configuration, which can be described as a tree structure with the root at the top. The root of the domain name tree is served by a number of root name servers, or root servers for short. The root servers' task is to give out references to name servers serving the requested top level domain. In turn, name servers belonging to a particular top level domain are tasked with providing information about the name servers servicing its dependent second level domains. Information concerning the name servers for the dependent second level domains is managed by what are known as top level domain administrators. An organization or individual having a registered domain name (the domain name owner)—*pts.se*, for instance—is responsible for providing name servers capable of replying to queries about its domain names (for example www.pts.se [see Figure 1]).



3.2. Customer relations are managed through accredited registrars

A customer may register his/her domain name by contacting one of the top level domain administrator's accredited registrars. Each top level domain administrator provides its registrars with a copy of its rules for granting domain names. This enables the registrar to make an initial assessment as to whether or not it will be possible to register the proposed domain name. In order to ensure that domain names are granted to the right organization or individual, registrars conduct a more extensive verification of the applications they receive.

3.3. The customer database is the basis for all its activities

All DNS operations within a top level domain administrator are based on the customer database. This database contains all customer information registered by the registrars and/or by the top level domain administrator itself. The top level domain administrator is responsible for maintaining and managing this database.

3.3.1 A top level domain is constructed from the customer database

Core DNS information, such as IP addresses and domain names for second level domain servers, is extracted from the customer database to a DNS database—called the zone file—which is then transferred to a master server for the top level domain. It is worth pointing out that the top level domain only stores information concerning the name servers for second level domains, but not address information for individual Web servers or mail servers; this information is stored on the second level domain's servers.

Information relating to registered owners of domain names is transferred to the so-called Whois database (see 3.3.3 below). Finally, information is transferred to a separate database for billing domain name owners.

3.3.2 Access must be secure

Registrars and the top level domain administrator register new information in the customer database using encrypted e-mail such as PGP (Pretty Good Privacy) via an ISP (Internet Service Provider). The top level domain administrator's internal access is generally made with Secure Shell (SSH). The top level domain administrator accesses the customer database for carrying out redelegations or other changes using some form of encryption (for example one-time passwords and Secure Socket Layer [SSL]). It is important to ensure sufficient availability and that there are appropriate routines in place for storing backups on a dedicated media and which, once the backup file has been verified, is stored in a different building.

3.3.3 Sensitive data in the Whois database must be protected

Users wishing to find the owner of a domain and the administrative and technical contacts for that domain may query a dedicated database called Whois—named after the DNS command with the same name—which is composed of data transferred from the customer databases. The administrator is responsible for ensuring that stored information does not breach national privacy laws, e.g. Personuppgiftslagen (PUL – Privacy Protection Act) in Sweden.

3.4. How is the top level domain master created and maintained?

A section of the global domain name system that is managed and operated by a single organization is generally referred to as a zone (for further details, see Appendix 2). The information contained in the customer database, which makes up the DNS database for the zone, is in most cases first transferred to a “hidden” master. Once on the hidden master, the zone file undergoes rigorous testing before being transferred on to a publicly available master server for the top level domain. In some cases, there is an additional step involved whereby the zone file is transferred to several servers that act as distribution points in order to provide redundancy and load balancing when the zone file is transferred to the slave servers.

3.5 Security must be ensured for transfers to slave servers

The zone file for a given top level domain is replicated at regular intervals—in most cases two to three times per day—to a number of slave servers. In this process, different methods for transaction authorization, such as T-SIG or MD-5 based checksum calculations, are used to guarantee that the content has not been modified and that the sender is the right one.

3.6 Top level domain responsibilities

A top level domain administrator is responsible for domain names in its part of the Internet, and it is acting on behalf of domain name owners. Its two main tasks are to administer the data linking owners of domain names to individual domain names and to ensure that customers' DNS data—name server addresses and Whois information, for instance—is available and accessible. The responsibility for a top level domain administrator is to accurately, and with sufficient speed, respond to DNS queries for the zone in question. This task is carried out wholly or partially through its slave servers. A reply from a name server for a top level domain generally contains a reference to a name server for a second level domain. A top level domain administrator is also responsible for ensuring that an accurate and tested zone file for the domain is transferred to the operators of its slave servers at regular intervals. A message is sent out to all slave servers informing them that a new version of the zone file is available, after which the slave servers request transmission of the zone file. The top level domain administrator is ultimately responsible for the operation of the slave servers.

3.6.1 Security in slave server operation

As indicated above, the top level domain administrator is ultimately responsible for the operation of slave servers, and it is required to ensure that there are at least two slave servers and that the same information is stored on all slave servers. In order to ensure a continuous operation of slave servers, it is advisable to apply diversity at all levels. Thus slave servers should be maintained by different contractors, so-called slave server operators, with different corporate affiliations, in secure facilities at different geographical locations, and where in every instance they have redundant connections to different ISPs or have the option to easily connect to other ISPs. Slave server operators shall ensure that the slave servers they run are accessible and that they are in a position to efficiently, accurately and with sufficient speed provide information about the zone. An agreement setting out the obligations of the slave server operator shall be concluded between the top level domain administrator and each slave server operator. Slave server operators are required to ensure that the accessibility rate is in line with the obligations set out in the agreement. In order to ensure this, the slave server system must have sufficient capacity and must be redundant at any given moment, allowing for shorter interruptions of the service for, say, maintenance without the functioning being noticeably affected. The top level domain administrator may take legal action against a slave server operator not respecting the rules and obligations set out in the agreement.

3.6.2 The top level domains' name servers must be known to the outside world

In order to enable users to retrieve DNS information about the top level domains, up-to-date and accurate DNS information for their name servers must be placed in the root zone. This requires the top level domain administrator to have documented routines for managing its contacts with the root domain administrator (see 3.7.1 below). An example would be for changing an IP address for a name server or for adding a new name server.

3.6.3 Monitoring is key to manage accessibility and security

Monitoring systems for DNS are of utmost importance to guarantee that a name server service operates continuously and with a high level of accessibility. At root and TLD level, there are always a number of systems in place for monitoring name servers' load and operation. Statistical information can be given both in real time and for periods in the past in order to give indications that capacity needs to be expanded as response times are too slow. PTS has an interest in being informed about how DNS functions, in particular at root and TLD level, in order to get an early indication of how accessibility is affected. In the case of Sweden, PTS has recently, through consultation with the Swedish top level domain administrator NIC-SE, been given access to the monitoring system for the name servers for the .se-domain. This allows PTS to get an early warning about heavy traffic and disruptions which may adversely affect users' ability to use the Internet. Discussions seeking to give PTS similar access to information regarding service operation and early warnings about disruptions for the .nu-domain are currently taking place between PTS and representatives of Nu-Domain.

3.6.4 Qualified staff is a crucial element

A top level domain administrator uses a complex system made up of a number of physical and virtual components to provide and maintain its services. In order to maintain a name service with a high level of accessibility, it is of crucial importance that administrators employ sufficiently skilled and experienced staff to manage the systems, and that they ensure that staff is kept abreast of the latest developments in their fields. It is equally important to ensure that there are sufficient resources to monitor the technological development and to take preventive measures to reduce vulnerability to physical or virtual attacks or disruptions. In addition, they should demonstrate a state of preparedness to allow for a high level of service to be maintained despite increased loads resulting from temporary or permanent traffic increases. In cases where a virus has infected the system, or where there has been an access violation, there must be a readiness to rapidly restore systems to normal operation.

3.7 What are the responsibilities of other parties?

DNS provides information on the domain name tree at the request of Internet users. This provision of information is carried out as a result of interaction between a large number of name server functions, which are maintained by different organizations acting within the DNS system at root, top or second level. The actual transfer of DNS information is carried out through a number of different ISPs which are obliged to provide functional networks with sufficient capacity.

3.7.1 The responsibility of the root domain administrator

In order to access information at top level domains, the root zone must be accessible and contain accurate address information so that the root servers can direct queries to the name servers of top level domains. ICANN/IANA (Internet Corporation for Assigned Names and Numbers/Internet Assigned Numbers Authority) is responsible for the contents of the root zone for registering modifications about top level domain name servers received from top level domain administrators. During our consultations, it was pointed out that ICANN/IANA is somewhat slow in carrying out this part of its mission.

3.7.2 The responsibility of second level domain administrators

A second level domain zone contains inter alia information about domain name owners' name servers. More detailed information about a second level domain, such as IP addresses for Web servers or mail servers, is not stored in the top level zone. This information must be retrieved from the zone for each individual second level domain. It is incumbent on the administrator of a zone to ensure that the second level domain is accessible and has sufficient capacity. Second level domain zones are generally managed by an ISP through an agreement with the domain name owner. Servers for mail and the Web belonging to second level domains registered under the .se domain may be reached by the outside world through the name servers indicated by .se's name servers. Access to the latter name servers are, thus, of crucial importance for all exchange of information.

3.7.3 The responsibility of second level domain owners

It is important for owners of second level domains to enter agreements on availability requirements, a so-called Service Level Agreement (SLA) with the party operating the name server for its second level domain. This task is generally carried out by an Internet operator—in most cases the same company as the one providing the Internet connection. In the case of servers for www, e-mail, etc., for companies and other organizations where the IP addresses are supplied by the second level domain zone, connection to the Internet may be required in order for them to communicate with the rest of the world. In such cases, it is important that the availability of mission critical services is secured by having redundant or alternative connections to the Internet.

3.7.4 The responsibility of users

Finally, it is important that end users wishing to send e-mail or connect to Web sites have good Internet connections so that the requested services can be accessed with sufficient reliability and speed.

4. The security of top level domains important to Sweden

The overview in this chapter is limited to the most common top level domains in Sweden, .se .com and .nu.

The .se domain

- NIC-SE is the administrator for .se
- The II Foundation is ultimately responsible for .se's DNS service.
- Seven slave servers for .se are located across Sweden and one in the USA.
- A monitoring system is in use and being evaluated
- DNSSEC is being tested in parts of the .se zone.
- NIC-SE is testing IPv6.
- Registration of .se domains has increased greatly since the rules were relaxed in 2003.

The .com domain

- US based Verisign is the administrator for .com.
- Slave servers for the .com domain are placed in 13 worldwide locations.
- The .com domain receives 12 billion queries daily.
- The number of queries doubles every 18 months.
- Verisign uses Atlas, an in house DNS software designed for significant increases in volume.
- Verisign is studying introduction of DNSSEC.
- IPv6 has been supported for two years.

The .nu domain

- .Nu Domain near Boston, Massachusetts, is the administrator for .nu.
- .nu is the country code for the island nation of Niue near New Zealand for which .Nu Domain has the delegation
- The existence of the .nu country code is not affected by geographical changes in Niue.
- There are two .nu slave servers in the US (with a number of anycast copies), one in Germany and one in Sweden.
- .Nu Domain is discussing DNSSEC.
- Support for IPv6 is planned.

4.1 The .se domain

The II Foundation (The Internet Infrastructure Foundation) owns NIC-SE and is as such ultimately responsible for the company's DNS service. NIC-SE has the overall responsibility for running the service and is also responsible for operational issues which need to be coordinated between the operators of the authoritative name servers (slave servers) of the .se domain. More specifically, this means that NIC-SE on an as needed basis shall lead and coordinate work in case of service disruptions. An agreement regulating the operators' responsibilities must be concluded between the II Foundation and each slave server operator.

The II Foundation may take legal action against a slave server operator that ignores the rules and regulations set out in the agreement or in other documents or policies issued pursuant to the agreement.

4.1.1 Administration of the .se domain

NIC-SE manages domain names for the national top level domain for Sweden, .se. This task is carried out on behalf of its customers (the domain name owners). The management role comprises both administering data linking domain name owners to domain names, and ensuring that customers' DNS data are available to the users' of the se DNS service. The administration of domain names is carried out by NIC-SE, while DNS data is made available through NIC-SE's DNS service. The DNS service has to be robust, i.e. designed to cope with severe stress.

4.1.2 Registrars

A customer may register a domain name in the .se domain by contacting one of approximately 300 registrars accredited by NIC-SE. The registrars have access to NIC-SE's rules for granting domain names so that at an early stage they can make a first assessment of whether or not a particular domain name may be registered. In order to ensure that domain names are actually given to the right organization or individual, the registrar subsequently conducts in-depth examinations of applications. Registrars enter new information in the customer database via PGP encrypted e-mail.

4.1.3 Operation of the .se domain

The .se zone is provided by eight slave servers as described in figures 2 and 3 below. These servers retrieve the .se zone from one of NIC-SE's two distribution points, each of which holds the most recent version of the master file for the zone, which has been transferred from the master server for the .se domain. The master server is named Primary-Primary and is located at the company's head office. NIC has chosen to host Distribution Point A at TeliaSonera AB, while Distribution Point B is hosted at Netnod AB in Stockholm. A new zone is produced and put on NIC-SE's distribution points three times per day. The aim is to have the new zone transferred to all .se name servers within 15 minutes after being placed on the distributions points. Having such a large number of slave servers allows for a wide distribution of the traffic load and, thus, a high availability.

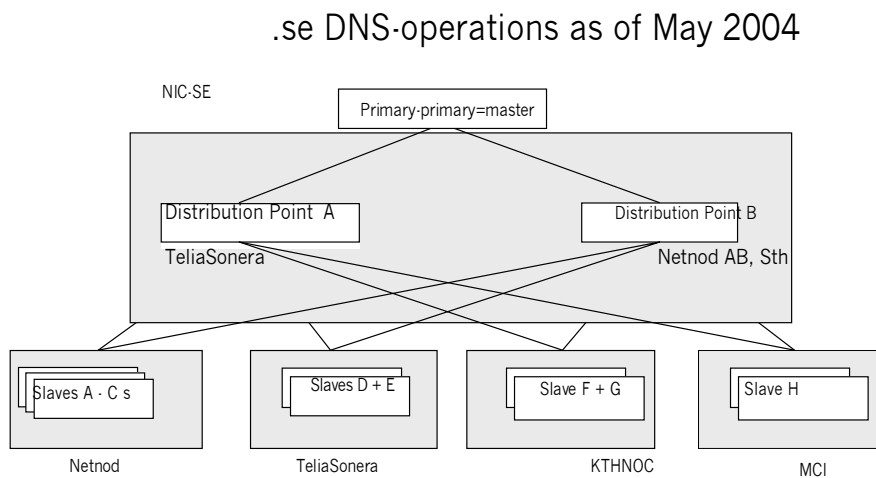


Figure 2 – Operational architecture of the .se domain.

Slave server	Operator	Location	IP-address
a.ns.se	Netnod	Stockholm	192.36.144.107
b.ns.se	Netnod	Göteborg	192.36.133.107
.ns.se	Netnod	Sundsvall	192.36.135.107
d.ns.se	TeliaSonera	Stockholm	81.228.11.57
e.ns.se	TeliaSonera	Malmö	81.228.10.57
f.ns.se	KTHNOC	Stockholm	192.36.125.53
g.ns.se	KTHNOC	Umeå	130.242.94.18
h.ns.se	MCI	USA	137.39.1.3

Figure 3 – List of .se’s slave name servers.

4.1.3.1 Security in the distribution of the zone file

The transfer of the zone file from NIC-SE’s distribution points and the slave server operators is protected against modifications during the transfer through the use of electronic transaction signatures, T-SIG. NIC-SE and the slave server operators share a signature key, which is unique for each operator and replaced at least annually. The parties agree to treat the keys in a manner consistent with a high level of security. The zone file is not encrypted for the transfer as it has been established that encryption is not necessary. The possibility of transferring the entire .se zone to a third party has been blocked by all slave server operators. Anyone seeking access to the .se zone is directed to NIC-SE. Provided that the .se zone is used for constructive purposes, NIC-SE may allow a third party to retrieve the .se zone from one of the distribution points. Decisions on such requests are considered by NIC-SE’s Chief Technical Officer.

4.1.3.2 Availability for the .se DNS service

Accessed from a Swedish operator’s network, the availability for .se’s DNS service must be at least 99,99% per calendar month (no more than 4.3 minutes of unavailability per month). This calculation shall not include periods when the operator’s own network was out of service. The DNS service is deemed to be available through an operator’s network if any (at least one) of the .se name servers is available. To monitor this, one of .se’s measuring points must be installed at the operator.

4.1.3.3 Transfer points

The domain's authoritative slave servers provide NIC-SE's DNS service. The slave server operators cannot control the entire network between themselves and each individual Internet user, and they are unable to take responsibility for the whole transport of IP packets between their slave servers and users. On the other hand, slave server operators are expected to take care of transport from their name servers to their designated transfer points (see Figure 4). The aim is for .se to enter into agreements with each slave server operator, setting out this responsibility as well as the location of the transfer points.

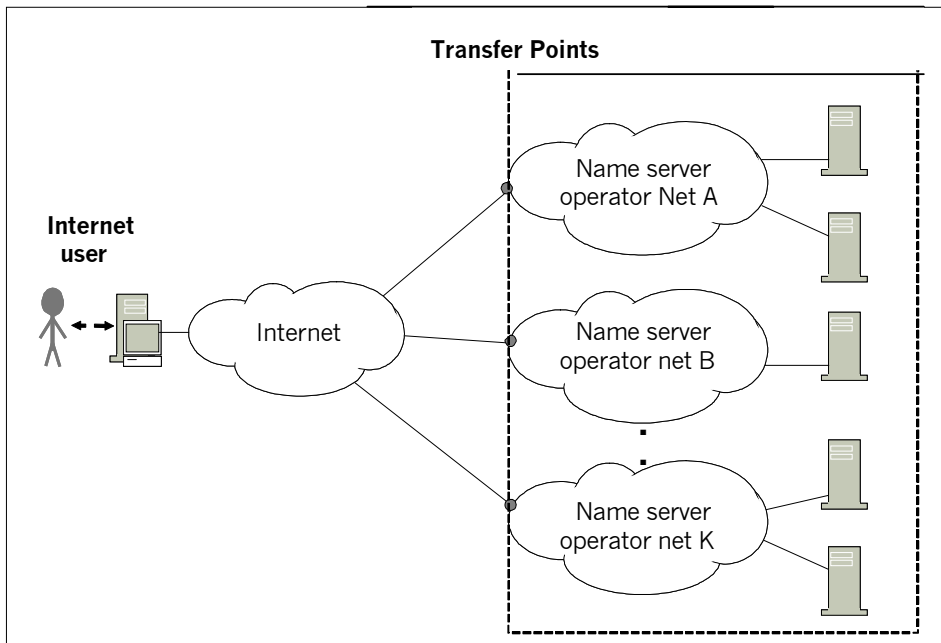


Figure 4 – Area of responsibility for name server operators

4.1.3.4 Cooperation with Internet operators

NIC-SE cooperates with the Internet operators represented in the Swedish Internet operators Forum (SOF) on questions of common interest. This cooperation is important as the users of the .se domain DNS service are dependent on, and customers of, Internet operators. SOF nominates two representatives to the board of the II Foundation.

4.1.4 Monitoring system

A monitoring and reporting system for .se's DNS service was developed and implemented during 2003. The system consists of a central monitoring server located at NIC-SE and four measuring points. Slave servers and measuring points feed data to a database on the central monitoring server.

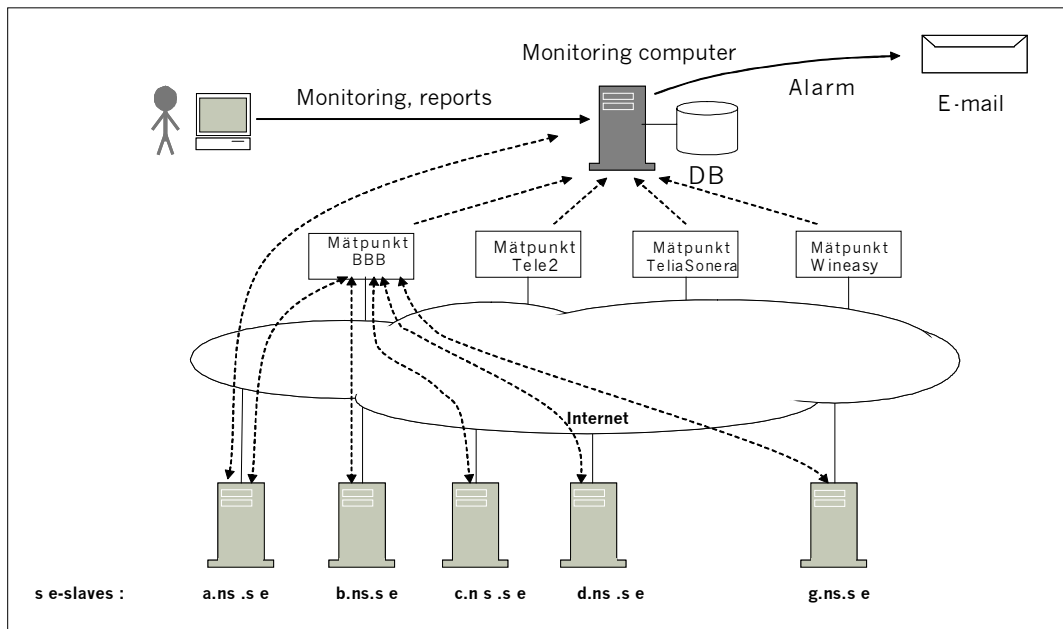


Figure 5 – System for monitoring and reporting

IIS and NIC-SE are currently evaluating the system, and a set of specifications is being drawn up. It has yet to be decided how user guidance for the system shall be designed. The functions that have been developed so far are used as a tool for monitoring slave server operation as regards response times and traffic loads as well as for sending out an alarm whenever a slave server is unavailable.

Events triggering an alarm

A system for alarm notification via e-mail is being tested. This system can be tailored by specifying one or more conditions for triggering the alarm. Each alarm condition may be configured with the following parameters:

- **Server** For which server is the alarm set? As an alternative, the alarm may be set for all name servers collectively.
- **Trigger** Which events trigger the alarm? The condition may be either in the form of a period of uninterrupted unavailability (minutes) or when availability falls below a certain level during a given period (%).
- **Interval** The period during which renewed alarms for the same event shall be suppressed.

- Alarm list A list of e-mail addresses to which the alarm will be sent.

Reports from the monitoring system

A monitoring system currently provides the following types of reports:

- availability of slave servers
- availability of .se's DNS service from each measuring point
- "Bill of Health" – regarding, for example, the operation of ISP
- response times for the slave servers
- traffic load (only for a.ns.se to e.ns.se)

4.1.5 Disaster planning

According to its security policy, a dedicated task force shall be established in the event of a major crisis to coordinate work on managing the incident. An internal assessment of the situation will be made in order to determine whether to set up the task force. There is no definition of what constitutes major crises. Instead, it is determined by the on-call staff on a case-by-case basis. A proposed definition of a major crisis is that at least 50% of the name servers are down for at least 15 minutes.

4.1.6 DNSSEC and IPv6

The II Foundation and NIC-SE have for a number of years actively worked with DNSSEC (see Chapter 6.1); and the objective is to fully implement DNSSEC for the .se zone as soon as possible. Currently, however, DNSSEC is not ready for implementation, but the plan is for it to be ready in 2004. NIC-SE is presently running a project to develop a tool for administration of keys. This project will intensify the separate tests being carried out on the basis of the most recent version of the BIND (Berkley Internet Daemon) software. A workshop to test the method chosen by NIC-SE to implement DNSSEC is anticipated for the fall of 2004.

As for the next version of Internet Protocol, IPv6 (see Chapter 6.3), NIC-SE has been offering tests for IPv6 for .se's DNS service since November 2003. At the time of writing, IPv6 transport is only available for one slave server (f.ns.se), but it will expand shortly to one additional slave server (g.ns.se). The aim of these tests is to evaluate how mature this technology is, and, if the tests are successful, to be in a position to decide to make permanent use of this technology.

4.1.7 Considerable increase in the number of new .se domains.

The number of registered .se domains has increased dramatically in recent years. The current growth spurt started in 2003 when the rules concerning eligibility to register .se domains were relaxed. The new .se rules, which entered into force on April 2, 2003, essentially stipulate that anyone may apply for any .se address, provided it is available. Prior to that date, an applicant was required to furnish supporting documents such as an extract from the National Register of Companies.

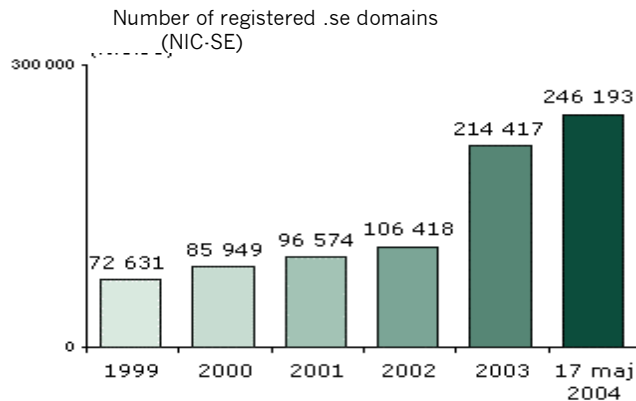


Figure 6 – Evolution of registered .se domain names.

At the time of writing, there are 246 193 registered .se domains and the rate of growth is according to the latest available data from NIC-SE in the order of 100 000 new .se domains per annum (Source: *Executive e-Report*).

4.2 The .com domain

4.2.1 Administration of .com

Verisign, with its headquarters and main operations center in Dulles, Virginia, just outside Washington D.C., administers the .com domain, which is very commonly used in Sweden. It also manages the generic top level domain (gTLD) .net, and the ccTLDs .tv and .cc. The company also hosts slave servers for other gTLDs, in particular .gov and .mil. Verisign is responsible for generating the root zone and the management of the root masters, which cannot be reached from the outside (hidden or stealth masters). The company operates two of the thirteen root servers (A and J).

4.2.2 Registrars

One of the 160 registrars accredited by ICANN manages customer contacts. Encrypted Secure Socket Layer (SSL) is used when registrars enter new information in the .com domain customer database, and registrars have access to a separate test environment to verify that the registration is correct. The .com domain receives 12 billion queries per day, which means 150,000 queries per second. The rate of growth is high with the number of queries doubling every eighteen months. The platform for Verisign's DNS service, Atlas, was developed in house and was put into operation in 2002, and it offers 100% availability through a completely redundant system architecture, according to the company's own assessment.

The platform was developed in order to create a secure system able to cope with a tenfold increase in volume—something that BIND is unable to offer. Verisign estimates that Atlas is preferable from a financial perspective. Finally, Atlas can be used as a platform for the other services offered by the company.

4.2.3 Operation of the .com domain

The master server for the .com zone is located in Verisign's own operations facility in Dulles, and it has several separate ISP connections. The facility, which is located above ground, has the traditional features in terms of access control, backup power supply etc.

Slave servers for the .com domain are installed in 13 locations, in most cases in the same locations as the root servers. Each .com server must have at least two ISP connections. The zone file, which contains 27 million domain names, is transferred to the slave servers twice a day. After the summer of 2004, the current system will be replaced with one based on incremental updates.

4.2.4 Monitoring

For the purposes of operations and monitoring, there are three more facilities in addition to the one in Dulles, referred to as swing sites, which are used for research and development.

4.2.5 Disaster planning

A reserve facility for the central operation of the .com domain - to be used in the case of a disaster - is installed at a different location in Virginia.

4.2.6 DNSSEC and IPv6

Verisign is presently examining the introduction of DNSSEC and is planning to first roll it out for the .net zone, followed by the .com zone. Verisign considers that an effort to educate DNS operators is necessary before DNSSEC can be used, and at the time of this writing, the company is investigating the possibilities of the U.S. government contributing funds to this education.

Verisign has supported IPv6 for two years.

4.3 The .nu domain

4.3.1 Administration of .nu

.NU Domain Ltd is the top level administrator for the third most important domain in Sweden. Its headquarters is in Medfield, near Boston, Massachusetts. .Nu Domain has the delegation for the ccTLD .nu, which is the country code for the small island nation of Niue near New Zealand with a population of 1,800. Niue is a self-governing territory in free association with New Zealand. The geographical distribution of its market share is as follows:

80% in Sweden, 9% in other European countries—primarily the Netherlands, Denmark and Germany, 6% in the U.S. and 5% in the rest of the world. All in all, after recently purging about 5,000 inactive domains, there are today about 105,000 .nu domains. There has been some speculation in the media about what will happen if Niue disappears geographically as a result of rising water levels, and what would happen with the .nu domain if that were to occur. The authors would like to point out that the ISO country code for the territory, .nu, wouldn't be deleted from the root zone because ICANN generally seeks to achieve long-term stability for existing top level domains. There are already a number of examples of country codes maintained in the root zone that are still usable although the nations they represent no longer exist. Examples include .su for the former Soviet Union, .yu for Yugoslavia and .io for the British Indian Ocean Territory, which does not have any land surface.

4.3.2 Registrars

There are about 30 registrars approved by .Nu Domain after having examined their technical, financial and business qualities. Registrars pay a fee to .Nu Domain and communication with the top level domain administrator is validated by way of IP-validation, i.e., a check to ensure that the sender's IP address is the right one. Communication with the customer database for new registrations is done by e-mail and IP validation, while redelegations by second level domain operators use passwords and SSL. The possibility of using certificates for registrars in order to improve security for registrars' communication with the top level domain administrator is currently being tested using the RRP protocol (Registry to Registrar). Customer data is jointly owned, but it's managed by the registrars. Should a registrar fail in its management role, something that has happened in the past, .Nu Domain takes over this task. As much as possible, the registrars handle customer contacts

4.3.3 Operation of the .nu domain

On a weekly basis, the customer database is replicated and transferred to a third-party company (known as the escrow agent) for safekeeping. A backup is made daily and stored in a bank. At the head office, a zone file is generated on a stealth master not accessible from the outside world. The zone file is tested before being transferred to a master, which can be accessed for DNS queries. Zone file transfers use the MD-5 checksum algorithm. After receiving the zone file, the slave servers verify that the file is intact and has not been modified during transport. This method is equivalent to T-SIG used under BIND 9.

The slave servers are spread out as follows: one is located in Sweden at TeliaSonera in Haninge near Stockholm, one is located in Germany at Above.net (one of the largest communications operators in Germany) and a number of servers are hosted by the DNS operator Ultra DNS, which hosts two slave servers with unique IP addresses. Each of those have several anycast copies (see Chapter 6.2 for further information on anycast). The server hosting company, Hosting.com in Boston, Massachusetts, keeps the master for the .nu domain, which is also accessible from the net for DNS queries. Hosting.com's data center contains servers from a large number of companies and it's outfitted with the typical features for an advanced operational environment, i.e. backup power, cooling and connections to several ISPs through separate cable bundles located at opposite ends of the building. Name server redundancy is assured through so-called fail-out, which means that a backup server immediately steps in if the primary server fails. As for the Internet connections, the .nu domain name servers are only connected to one ISP each, but they are all located close to peering points enabling them to rapidly be connected to other operators. The responsibility for ensuring that slave servers have appropriate Internet connections is regulated by agreements with the contracted slave server operators.

According to .Nu Domain, the information exchange with IANA, which manages delegations and redelegations on behalf of ICANN, is too slow because of poor routines. .Nu Domain indicates that it would prefer authentication of communications using PGP keys rather than the e-mail verification mail using IP validation currently applied by IANA. External companies handle hardware maintenance, but all software is maintained and updated by company staff, as well as three consultants who have worked for the company for a long time.

4.3.4 Monitoring

There is a system in place using several computers for indirect monitoring through an online connection. Monitoring is carried out 24 hours per day, and alarms are sent to monitoring staff's cell phones. A specific problem currently being addressed is spoofed DOS attacks, which occur daily and often last for several days. So far, these attacks have not caused the DNS service to fail.

4.3.5 Disaster planning

The disaster plan has several different levels. The main principle is that in the event one of the data centers becomes unavailable, there are several other centers to assume these functions. The staff has practiced different scenarios, and there are agreements with third parties to assume responsibility for some functions in the event of a disaster. The main objective is for the DNS to always work. In a worst case scenario, for example, if an event destroys the head office and staff, administrative tasks are allowed to be unavailable for several days. Data is always kept in several separate locations.

4.3.6 DNSSEC and IPv6

DNSSEC is at the time of writing only at the discussion stage.

There are plans to start introducing support for IPv6 within a few months.

5. Which functions are important to a high level of security for top level domains?

A number and functions and measures are necessary for ensuring a high level of security in the operation of top level domains. In this context, the term security also includes a high level of accessibility. The checklist below gives an overview of what is needed to achieve this.

5.1. Security in the operation of a top level domain

- Sufficient capacity and redundancy in top level domain slave servers.
- Redundancy and SLAs for name servers' connections to the Internet, with at least two separate ISPs and, ideally, different exit points from the building where the servers are hosted.
- Sufficient bandwidth for name servers' Internet connections.
- Correctly configured and updated name servers.
- Meticulous testing of updated zone files before they are rolled out.
- Security for zone file transfers from master to slave servers, and that these transfers are done with sufficient frequency to guarantee accuracy.
- Sufficient number of name servers, either through several instances having unique IP addresses or by using anycast (see Chapter 6).
- Name servers are spread across the Internet and placed near users.
- Secure premises for name servers.
- Diversified operation of name servers through agreements with several DNS operators.
- Diversified software for name server operating systems.
- Diversified DNS software, for example BIND (Berkley Internet Daemon) or other DNS software.
- Enough staff with the right information and skills to accurately carry out tests and other measures relating to good functioning and security for name server databases, DNS software and operating system.
- Systems and staff for advanced monitoring.
- Technical support for both hardware and software available 24/7.
- Readiness to rapidly upgrade capacity in servers and Internet connections.

- Support for DNSSEC (see Chapter 6) as soon as there is a globally useable version of this standard.

5.2 Security in the administration of a top level domain

- Appropriate security routines for managing new registrations made by external registrars.
- Appropriate security measures for external access to the customer database for making changes such as redelegations which are generally made by second level domain name administrators.
- Documented and established routines for contacts with ICANN / IANA concerning deletions, additions and changes to slave name servers at the TLD level in order to ensure accurate information about the top level domain's name servers is in the root zone.
- Documented and established routines for introducing and testing changes, e.g. new server configurations and the introduction of supplier-specific modifications to software (bug fixes, patches, etc.).
- A documented, up to date and established security strategy.
- A documented and up-to-date disaster plan, which is being practiced.

6 New functions for increased security

- DNSSEC is an almost fully developed technology for improved DNS security.
- IPv6 is being tested in DNS.

6.1 A new standard for more secure information management in the domain system is on its way

In the near future, probably during the course of 2004, a new standard for considerably improved security for DNS information management using Secure DNS (DNSSEC), which is currently being developed by Internet Engineering Taskforce (IETF), will become available. On a technical level, the specifications for DNSSEC and its supporting protocol are almost fully developed. There are, however, some issues that still need to be resolved and the final documentation is expected to be published soon. The actual implementation of DNSSEC is likely to be complicated, though.

The DNS system is the world's most distributed database where different parties manage their own parts of the database. This decentralized administration facilitates work on updating database information. As there are presently no safeguards in DNS to verify which entity entered what data, it is easy to enter false information by using someone else's identity. False DNS information makes it possible to steal other information and disrupt transactions. For those reasons, it is important to ensure that information comes from the right source.

The two basic concepts in DNSSEC are checksums and asymmetric encryption. The algorithm has been designed to ensure that even the smallest modification of the information results in a change in the checksum. The recipient may calculate his own checksum for the DNS record and compare his own checksum with the one supplied with the information. If the checksums are equal, one can be sure that the information has not been tampered with and that it comes from the right sender.

In order to maintain and increase public trust in the Internet, PTS has an interest in ensuring that DNSSEC is implemented and in monitoring developments in this field. Current technical solutions cannot guarantee that transferred DNS information is correct and authentic, i.e. that it comes from the expected source. Another problem relates to the management of keys and certificates for DNSSEC encryption. On the technical side, it is worth mentioning that Swedish DNS technicians participate in the international working groups tasked with standardizing the DNSSEC protocols. The Swedish top level domain administrator is developing systems for managing signatures, and it has recently been testing DNSSEC.

6.2 Anycast – a new addressing method

The number of name servers for a given zone is currently limited to 13. This is because the maximum size of a UDP packet (User Datagram Protocol) is 512 bytes, which equals information about 13 name servers. UDP is the protocol used to transfer zone files, which must be done by sending a UDP packet. In order to get around the technical limitation of 13 name servers per zone, thus ensuring improved availability and shorter response times to meet continuously increasing use, the new addressing method, known as anycast, may be used. An anycast address identifies a group of name servers belonging to a particular address area. An IP packet sent to an anycast address is delivered to the closest name server according to the algorithm for measuring distance contained in the routing protocol. Anycast allows several identical name servers to share the same IP address, thereby enabling them to divide the work with answering DNS queries. The number of name servers, then, may be increased allowing for a better geographical distribution of servers. For example, a name server for a top level domain located in Stockholm may have a number of mirror sites at different locations inside and outside Sweden, close to the users, but with all having the same IP address. Anycast will not affect the UDP packet limit of 512 bytes because the amount of information to be transferred does not change. In addition to overcoming the limitation of 13 name servers, there are a number of other reasons for using anycast. The use of this technology is spreading as a result of its other inherent advantages, in particular:

- Reduced resources for routers and communication links. Standard IP routing ensures that IP packets with DNS queries are sent the shortest distance to the closest name server.
- Simplified configuration. As a client's equipment only needs to be configured for a single anycast address, which identifies a group of possible servers, it will be easy for the user to receive the requested DNS information from the nearest, working name server.
- Improved robustness. The system will be less sensitive to disruptions if a server in an anycast group fails because the net will still be able to deliver DNS queries to the next closest name server.
- Balanced loads. Name servers scattered over the Internet will distribute and balance DNS traffic loads.
- Better coping with increased loads. Anycast has been used for a long time for Web servers, and implementation has begun for the .com domain, the .nu domain and several of the root servers. There are already about 50 anycast servers in operation, and for the first time in the history of the Internet, the number of DNS servers outside the U.S. exceeds the number within the U.S. Recently, anycast copies have been launched for most root servers, including the root server in Sweden (I root), which is scheduled to receive 25 anycast copies worldwide during 2004. This will allow root servers to better cope with increased loads, whether from legitimate DNS traffic or illegal DOS attacks.

6.3. Anyone may get an IP address with the new Internet Protocol

The new version of the network protocol Internet Protocol, IPv6, will allow anyone to have his or her own IP address. IPv6 is based on a 128-bit address length and was developed by IETF as a new standard because IPv4 is insufficient to meet the needs of the Internet's ongoing and future expansion. Several DNS operators and ISPs are testing IPv6 and it has also been tested for the root servers, but demand is presently limited. IPv6 requires new DNS records for it to be fully used. Further details on IPv6 are in Appendix 3.

6.4 DNS Development continues

A lot is happening in the field of DNS technology. Methods have been developed to change the way zone transfers from masters to slaves are made. It can occur by only sending information that has been modified since the last update, rather than sending the entire zone file. This is referred to as incremental updating. New records for storing information in DNS are constantly being developed, for example for encryption keys and certificates. ENUM, which is a function for translating telephone numbers into domain names, is currently being evaluated and would require the addition of another field in the DNS database.

Sources

Reports, publications and links

Är Internet i Sverige robust, Post- och telestyrelsen, 2003 (PTS-ER-2003:1)¹

Den internationella förvaltningen av Internet, Post- och telestyrelsen, 2003 (PTS-ER-2003:23)²

Vem gör vad i Internet-Sverige?, ISCO-SE, 2003³

Driftshandbok för se:s namntjänst, NIC-SE, 2004⁴

RFC 1591, 1994: <http://www.ietf.org/rfc/rfc1591.txt>

ICP-1, ICANN, 1999: <http://www.icann.org/icp/icp-1.htm>

Principles for the delegation and administration of country code top level domains, GAC, 2000:

<http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm>

Procedures for Handling Requests by ccTLD Managers to Change Nameservers, IANA, effective 31 March 2003

Resolution 102, ITU (Rev. Marrakesh, 2002), Management of Internet domain names and addresses: <http://www.itu.int/osg/spu/resolutions/2002/res102.html>

Security Space, http://www.securityspace.com/s_survey/data/200404/domain.html

¹ Is Internet in Sweden robust? National Post and Telecom Authority, 2003

² The International Management of the Internet, National Post and Telecoms Authority, 2003

³ Who does what in Internet Sweden?

⁴ Operational Handbook for the .se name service

Appendix 1 – Political Context and Management Principles

1.1 Government IT Bill for improved trust in Internet use

The overall goal of Government IT policy is to turn Sweden into an information society for all. A broad-based initiative has been launched in order to create an efficient, secure and accessible infrastructure for services relating to IT and electronic communications (Government Bill 1999/2000:86). In its bill, the government proposes that IT policy should be focused on three essential tasks: user trust in IT, user skills and greater accessibility of information society services. Regarding user trust, the government notes that improved operational security will result in greater trust in using the Internet. Therefore, the government considers it important to safeguard functions improving Internet use and Internet traffic management—routing registries and the domain name system, for example—so that the Internet will work efficiently. Finally, the government wants to work toward making it possible to operate the Swedish section of the Internet independently in case of limited accessibility in the event of major disruptions or war.

1.2 Upcoming draft bill on the management of the .se domain

In its opinion issued in June 2003, PTS indicated its general agreement with the draft proposal for new legislation (SOU 2003:59) on the management of national top level domains in Sweden, as well as the options for state participation and control in order to promote the societal objective of ensuring a well-functioning top level domain for Sweden. In practice, it is ICANN, and its advisory committee (GAC) where Sweden is represented by the Ministry of Industry and Employment (Näringsdepartementet) and where PTS has observer status, which is the international organization responsible for selecting who shall have the administrative responsibility for a national top level domain. It also defines the conditions for carrying out this role.

In its opinion on the draft proposal, PTS stressed that in the event the bill on the .se domain is ultimately adopted, the proposal should also include a possibility to adapt the legislative framework through secondary legislation in order to take into account changes in the contractual relations between ICANN and the administrator. In addition, PTS considers that in such a case, the act should contain fewer details and the possibility should be introduced for the Supervisory authority to adopt secondary legislation containing more detailed requirements, taking into account international agreements and principles governing this field.

PTS believes that its cooperation with the administrator of the Swedish top level domain (NIC-SE) is working well. From a societal perspective, it is important that public bodies monitor the devolvement of DNS and of domains of importance to Sweden, whether or not the bodies are legally required to do so. The draft bill concerning the .se domain is being drafted and, if adopted, may not enter into force before 2005, and the bill is likely to confer a supervisory role on PTS.

1.3 ICANN principles for domain level management

Principles for managing national top level domains (ccTLDs) are set out in the policy document “Principles for delegation and administration of ccTLDs,” drawn up by GAC on the basis of RFC 1591 and ICP-1. A common principle for both ccTLDs and generic top

level domains, is that domains must be administered in the public or common interest. The task of ensuring that this is respected in the administration of ccTLDs should, according to ICANN, be entrusted to the national governments. In other words, in order to attain the objectives of the administration of the ccTLDs, it is necessary that national governments have sufficient influence over the system. ICANN, furthermore, indicates that it will only allow delegation of the responsibility for a ccTLD to an individual or organization where this has been sanctioned by the national government concerned. The U.S. Commerce Department has adopted the same approach as ICANN on these matters. Given the important role of top level domains, there is legitimate interest for the countries concerned to ensure a degree of influence and oversight of them.

1.4 United Nations activities in this field

There has been some activity regarding top level domains within the competent U.N. body, the International Telecommunication Union. For example, a workshop was organized in Geneva in March 2003 addressing the relationship between national top level domains and their respective governments. Representatives of ccTLDs, ICANN and ITU participated in the workshop. A public meeting on Internet Governance was held on February 2004 during which questions about the management of key material Internet parameters (e.g. domain names and IP addresses) were discussed.

The U.N. body, UNICT (United Nations Information and Communication Technologies) Taskforce (organized a World Congress in New York in March 2004. The congress addressed issues relating to DNS management, primarily from the developing countries' perspective.

1.5 Cooperation between top level domain administrators is crucial

There are a number of organizations working on issues relating to operation and administration of national top level domains. An example is the Council of European National Top Level Domain Registries (CENTR), which is the European interest group. And global cooperation exists among national top level domains within the World Wide Alliance of Top Level Domains.

Finally, within the framework of ICANN, there is also the country code Names Supporting Organization (ccNSO) made up of ccTLD operators within each geographic region working on questions of common concern.

Appendix 2 - How does the domain name system (DNS) work?

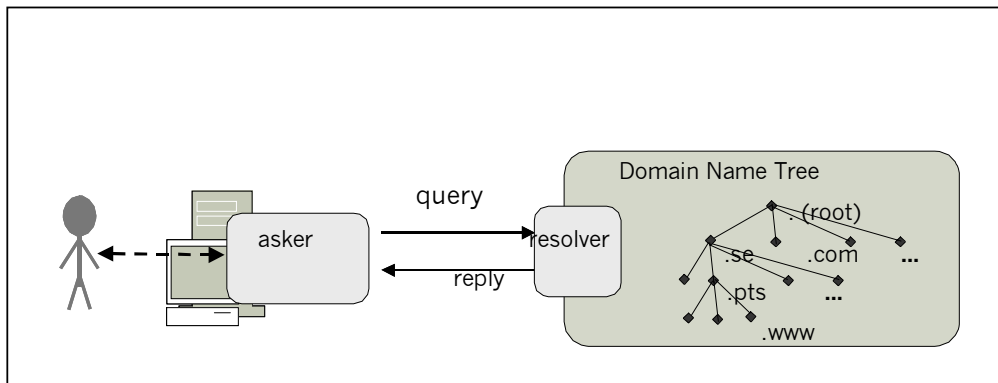
This appendix describes the basic concepts and functions inherent in the domain name system which are relevant to this report.

Definition of the DNS Service

In order to study the availability, robustness, foreign dependencies and responsibilities relating to the Domain Name System Service, as set out in the government's instruction to the PTS, one must first clarify the definition of what constitutes a DNS Service. This study addresses user requirements for the DNS Service, and we have decided to exclude requirements from other stakeholders, i.e. the specific requirements of registrars, top level domain administrators, developers and others. The foundations for DNS are set out in RFC 1034: "Domain Names – concepts and facilities" and RFC 1035: "Domain names – implementation and specification". Neither of the two RFCs contains a definition of the term DNS. However, RFC 1034 states that DNS may be viewed from different perspectives, and where the user's point of view can be described as follows:

"From the user's point of view, the domain system is accessed through a simple procedure or OS call to a local resolver. The domain space consists of a single tree and the user can request information from any section of the tree."

Figure 1 – DNS from the user's point of view



For the purposes of this report, the DNS service is defined as a service providing information from the domain name tree at the user's request. More specifically, it is assumed that the DNS service is able to answer user queries on:

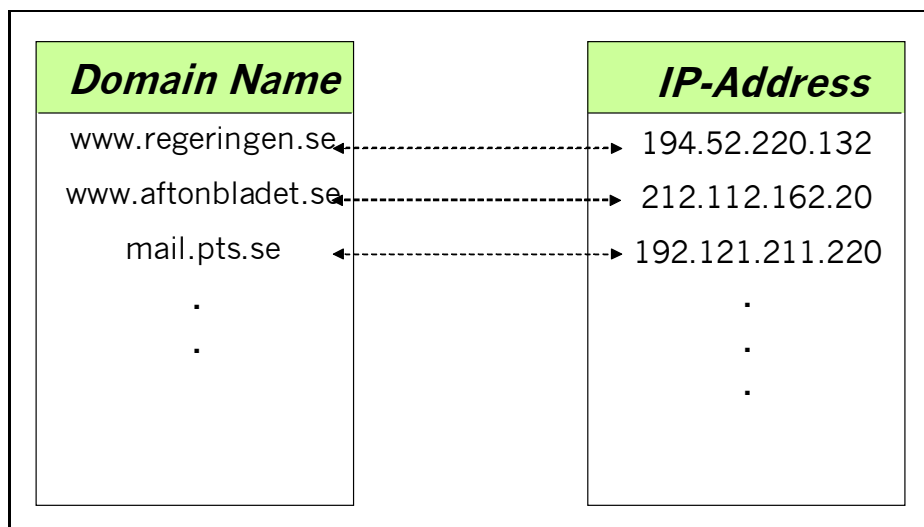
1. Address – The IP Address corresponding to the requested domain name.
2. Mail server – The computer to which e-mail shall be delivered.
3. Domain name pointer – The domain name corresponding to a requested IP address.

It is highly likely that users in the future will be able to ask for other information from DNS. An example of this is ENUM, which would allow users to store contact information and other data linked to telephone numbers. Another suggestion is to store encryption keys, ISBN data, etc., in the DNS.

Domain names and IP addresses

Every computer on the Internet is identified by a unique IP address (see Appendix 3 for further details), which is used to ensure that data packets on the Internet are sent to the right computer. An IP address under the currently predominant IP version consists of a 32 bit binary number, written out in four groups of decimal numbers separated by periods. To spare us from having to remember long combinations of numbers when we want to connect to a Web page or send e-mail, we use domain names instead (see figure 2).

Figure 2 - Translation between domain names and IP addresses



The DNS hierarchy

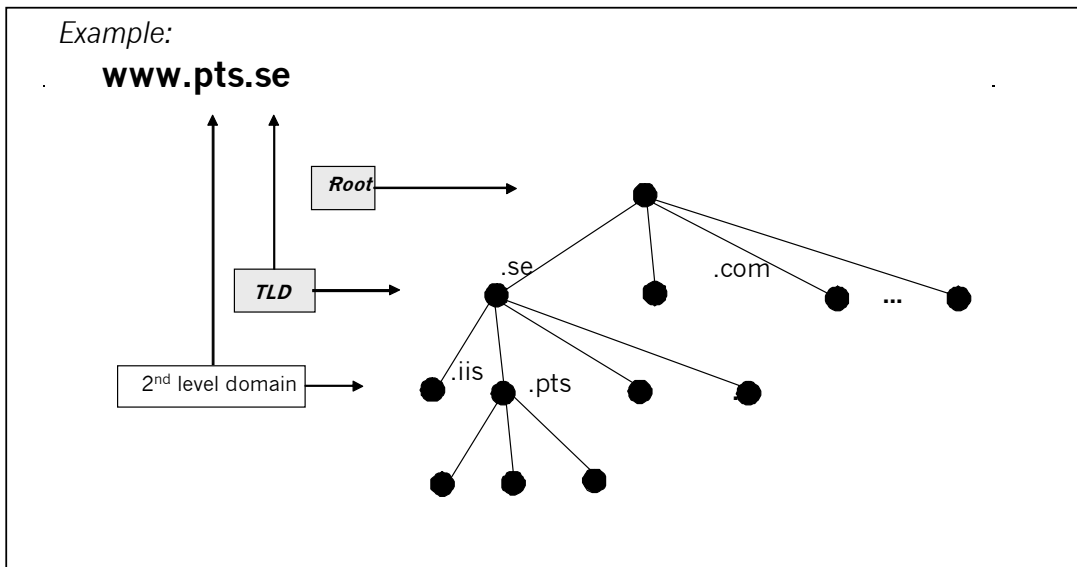
The Domain Name System has a hierarchical structure organized as an upside down tree structure, the so called domain name tree (see figure 3). At the top level, the tree is held together by its root. ICANN is responsible for the root. The root level determines which top level domains may be included in the tree. The root does not have a name, but it is represented by a period at the end of an IP address. This period may, however, be omitted.

Below the root level, there are currently 258 different top level domains. They are:

- 243 national top level domains that represent ISO country codes, e.g., .se, .no, .uk, .de, .jp and so on. The idea is to allow users to register their own domain names under the relevant country code. The II Foundation, through its management company NIC-SE, is responsible for the Swedish domain .se.
- Generic top level domains; these are currently .aero, .biz, .com, .coop, .edu, .gov, .info, .int, .mil, .museum, .name, .net, .org and .pro. These are intended to be offered on a worldwide basis regardless of country of establishment.
- The .arpa domain, which is intended for domains forming part of or contributing to the Internet's infrastructure. For example, the domain e164.arpa is intended to be used for storing telephone numbers.

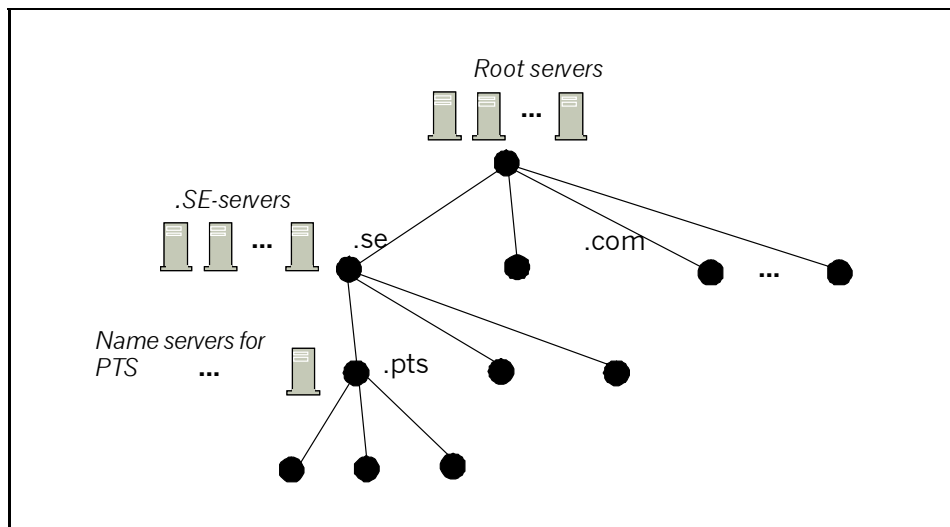
The level below a top level domain is generally referred to as a second level domain. The rules governing the eligibility for registering second level domains vary from one top level domain to another. For example, individual customers are not allowed to register directly under .uk (United Kingdom) forcing commercial organizations to register under the second level domain .co.uk and private individuals under .me.uk. In the case of Sweden, however, it is most common for users to register directly under .se, for example pts.se, although there are cases where users choose to register under one of the second level domains provided by NIC-SE, for example .pps.se (for private individuals). Once an organization or individual has registered its domain name, it is responsible for assigning domain names for its second level domain. For example, it is up to PTS to determine the IP address linked to www.pts.se.

Figure 3 – The Domain Name Tree



The required translation between domain names and IP addresses is thus carried out by DNS. DNS is a distributed database system where name servers (computers with name server software) across the Internet work together to handle the translations between domain names and IP addresses. The hierarchical structure of the domain name system is also reflected in its technical design. The root of the domain name tree is served by thirteen so called root name servers, or root servers for short (see figure 4). Their task is to respond to queries providing the name servers serving the requested top level domains. Similarly, TLD name servers are tasked with indicating the name servers for a second level domain and so on. An organization or individual having its own registered domain name, for example pts.se, is responsible for ensuring that there are name servers that are capable of responding to queries about its different domain names.

Figure 4 – Name servers and the domain name tree



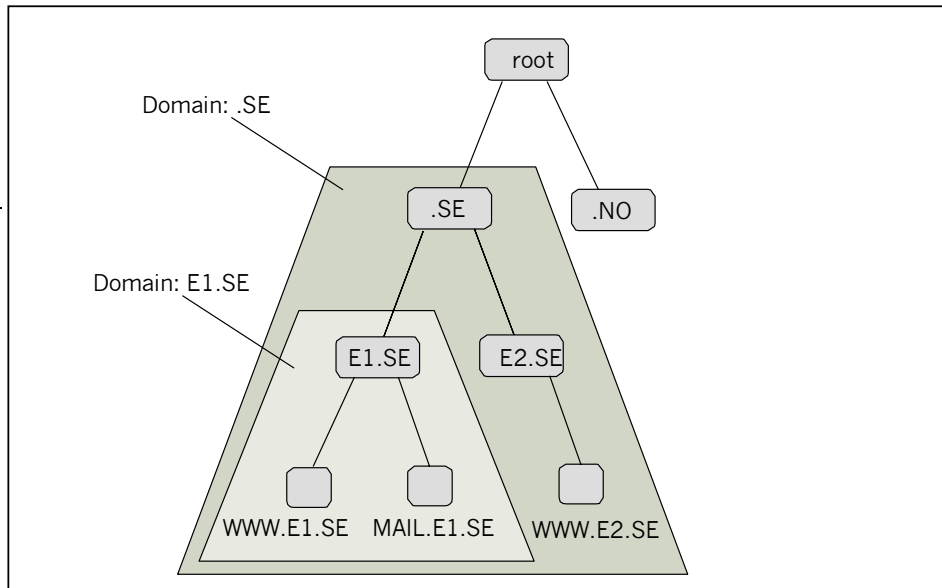
Domains and Zones

In DNS, the two words domain and zone are used to describe sections of the domain name tree.

Domain

A domain is a sub tree in the overall domain name tree, and it is identified by the domain name for the sub tree root. A domain consists of all resources in the sub tree. For example, the .se domain in figure 5 includes: .se, e1.se, www.e1.se, mail.e1.se, e2.se and www.e2.se. On the other hand, the e1.se domain is made up of: www.e1.se and mail.e1.se.

Figure 5 – Domains and Domain names

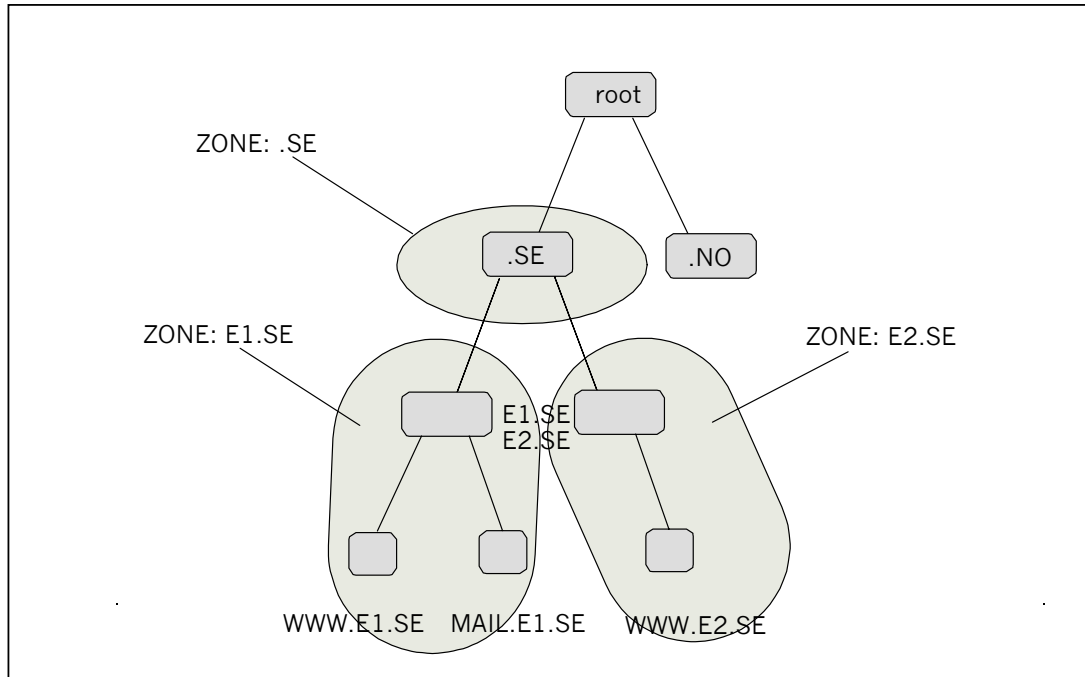


Zone

The term zone is used to describe how the administrative responsibility for the domain name tree is split between different organizations. A zone consists of a continuous part of the domain name tree administered by a single organization and which is stored on that organization's name servers. Thus, the example contained in figure 6 comprises three zones: .se, e1.se and e2.se. Please note that e1.se and e2.se do not belong to the .se zone, but they do belong to the .se domain. Each of the three zones is administered by a separate organization which are responsible for the respective name servers.

In practice, the administration of .se domain is split between a large number of organizations who are responsible for their respective zone. At present, NIC-SE is responsible for administrating the .se zone and to ensure that the zone is distributed to name servers. In most cases, the second level domains under .se are administered by other organizations, which consequently means that they are not included in the .se zone. Thus does pts.se not belong to the .se zone.

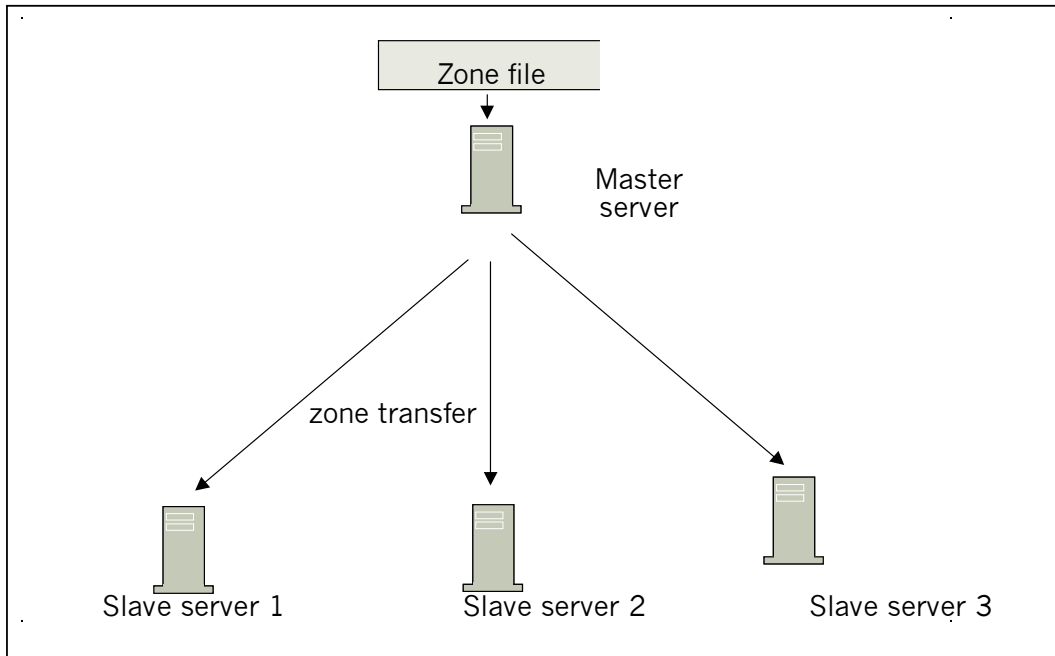
Figure 6 – Zones



Authoritative name servers for a zone

The systems used for storing and distributing information pertaining to the domain name tree are commonly referred to as name servers. A name server stores information concerning one or more zones. Two or more name servers are generally used for each zone in order to provide a robust service on the Internet. One of the name servers for the zone is the master server, which is responsible for retrieving the zone information from a local file. The other name servers get their information from the master server and are thus referred to as slave servers. The transfer to slave servers is called zone transfer and may be initiated by either the slave or the master server (see figure 7).

Figure 7 – Master and slave servers



Zone transfers may be done in several steps, i.e. a slave server which has received a zone transfer may in turn become a master server when the zone is transferred on further, subsidiary slave servers. There is from a user perspective no difference between a master and a slave server as they are all able to reply to queries concerning the zone. Thus, both the master and slave servers are said to be authoritative name servers for a zone as they are supposed to hold identical information.

Resource Records

Name information in DNS is stored in so called resource records. The resource records are linked to domain names when they are stored in DNS, and several resource records may be stored for each domain name. There are a number of different records, with the most important ones for the purposes of this report being listed in Figure 8 and further described below.

Figure 8 – Information that can be provided by the DNS Service

Question relating to	Type	Meaning
IP address corresponding to the requested domain name	A	Address
To which e-mail shall be delivered	MX	Mail Exchange
Domain name corresponding to the requested IP address	PTR	Domain Name Pointer
Specifies an authoritative name server for a zone	NS	Name Server
Parameters for and information on the zone	SOA	Start of a zone of authority

Address (A record)

The A record is the most commonly requested by users and it contains the IP address corresponding to a particular domain name. The A record may for example be requested by a browser when a user has typed an Uniform resource Locator (URL) in the browser address bar, or when a mail server is delivering electronic mail.

Mail Exchange (MX record)

Whenever a mail server delivers electronic mail, it generally first asks the DNS service to which computer (domain name) the mail is to be delivered. Thus, the e-mail address shl@iis.se does not contain any information as to which mail server will receive mail. But a query to DNS as to where mail for iis.se shall be sent will receive an answer that it shall be sent to the domain mail.iis.se. In the DNS system, information about e-mail delivery is stored in so called MX records.

Domain Name Pointer (PTR record)

The DNS service also responds to queries about which domain name is linked to a certain IP address. This feature is not used by your average “surfer”, but rather in the following cases:

- To translate IP addresses contained in a log file to domain names. This is for example done by web servers collecting statistics over which domains users are coming from.
- For network monitoring applications that draw up network maps with domain names.

- The simple software application “traceroute” which is installed on most computers enabling users to trace the routes traffic takes to reach different destinations, and which simultaneously translates the routers’ IP addresses to domain names.
- To trace unwanted traffic.

In the DNS system, domain name pointers are stored in so called PTR records.

Name Server (NS Record)

The NS record contains the domain name for the name server responsible for a zone. As several name servers typically serve a given zone, there are several NS records for each zone. NS records for a zone are stored in both the zone itself and in the zone immediately above it. The reason as to why NS records are stored in the zone above is so that that zone will be able to refer queries to the name servers of the zone below.

Start of a Zone of Authority (SOA record)

There is a SOA record for each zone. It contains the following information about the zone:

Email:	Address to the instance responsible for the zone.
Serial:	Version number of the zone file. This field is used by the slave servers to see if the zone has been updated.
Refresh:	How often the slave will check if the zone has been updated.
Retry:	How long the slave waits before a new attempt is made to contact a master after previous attempt failed.
Expire:	Until when data remain valid in case the slave is unable to reach a master, i.e. the period during which the slave server may continue to respond to queries even if the master cannot be reached.

TTL:
server The period during which replies from an authoritative name
for the zone are stored on resolvers.

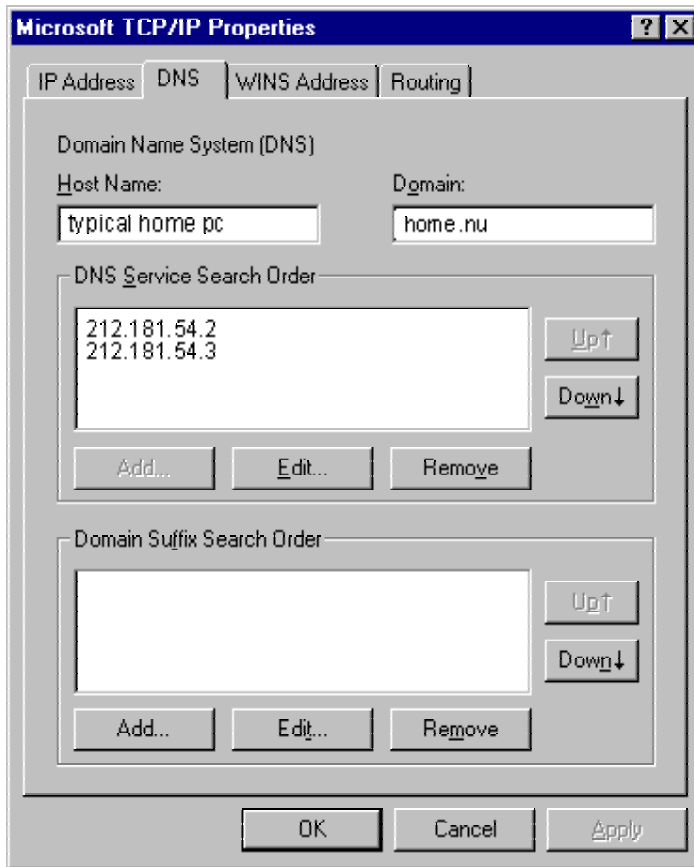
Server:
unclear Domain name for the master server for the zone. Its use is
at the time of writing.

Resolvers

Most ordinary computers are not configured to themselves search the domain name tree to find the answer to a DNS query. In most cases, DNS queries are referred to a separate server with DNS software installed. Such a DNS server, the sole purpose of which is to handle DNS queries for other computers, is generally referred to as a resolver. A resolver scans the domain name tree on behalf the asker by querying different name servers. The answer is returned to the asker. This simplifies DNS support for users as they only need to send one single query to a resolver and then await the response.

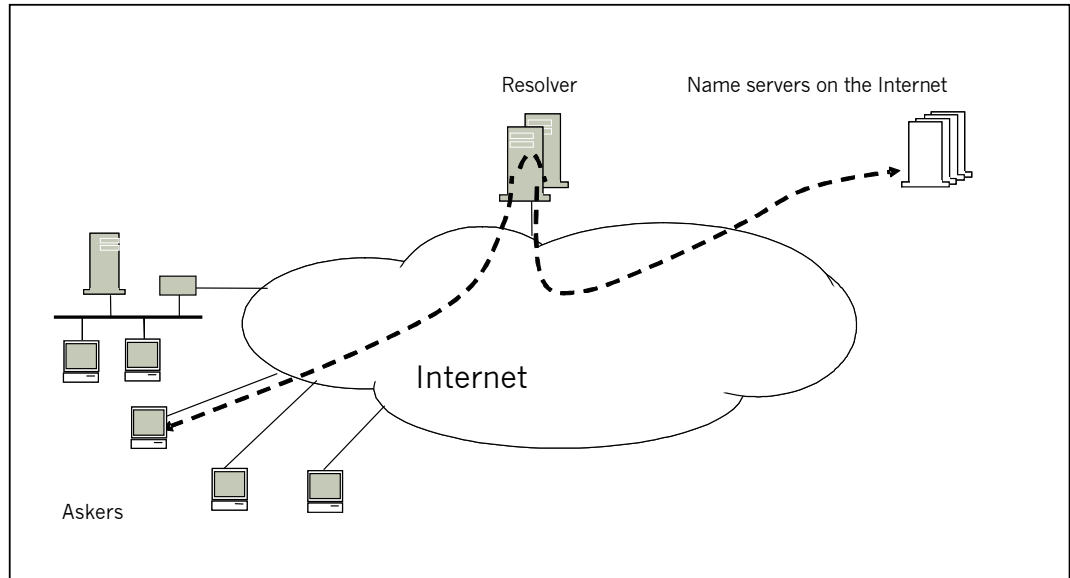
A resolver can act on behalf of anything from a simple home PC to advanced servers. Every computer must, however, know which resolver to use. This is ensured by configuring the IP address for one or more suitable resolvers, either automatically by dynamic addressing (DHCP) or manually (see figure 9).

Figure 9 – Manual client configuration of resolver IP address.



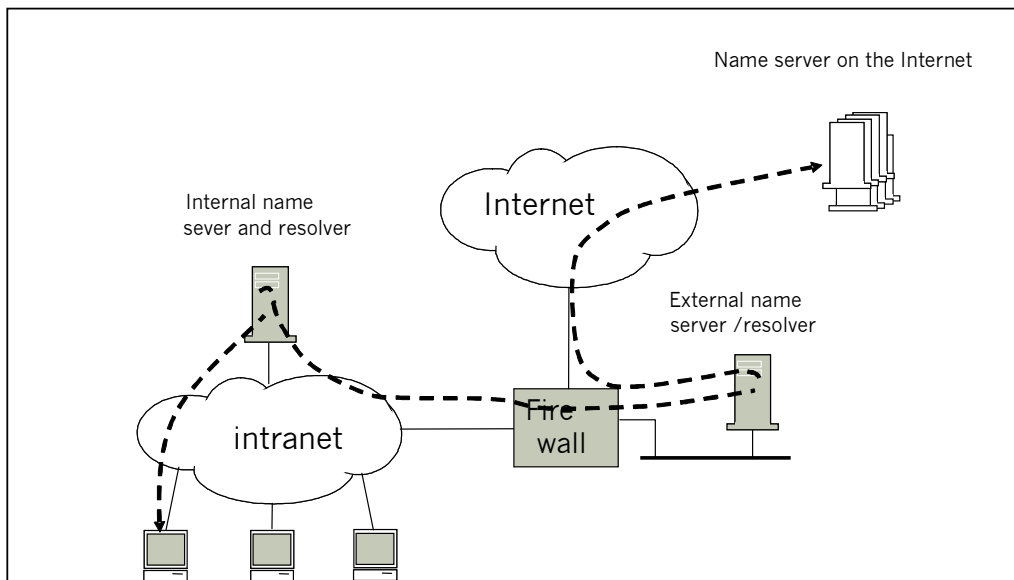
A resolver is generally not a publicly available resource, and every user is supposed to have his or her own resolver. Less sophisticated users generally don't have their own resolvers, but instead use one of the resolvers provided by their ISP (See figure 10).

Figure 10 – Less sophisticated users without their own resolvers



More sophisticated networks may let queries pass through several layers of resolvers. Larger organizations, for example, generally have an internal DNS service for resources on its Intranet. DNS queries from users are in that case directed to an internal name server. The internal name servers ensure that queries concerning the internal domain are responded to locally, while queries relating to external resources are sent on to the Internet. In order to insulate the internal DNS system, queries to the Internet are sent via a firewall which may contain a separate name server which thus acts as a resolver towards Internet. Thus, DNS queries pass through two resolvers before the query reaches the public DNS infrastructure on the Internet (see figure 11).

Figure 11 – Firewall solution with separate internal and external DNS.



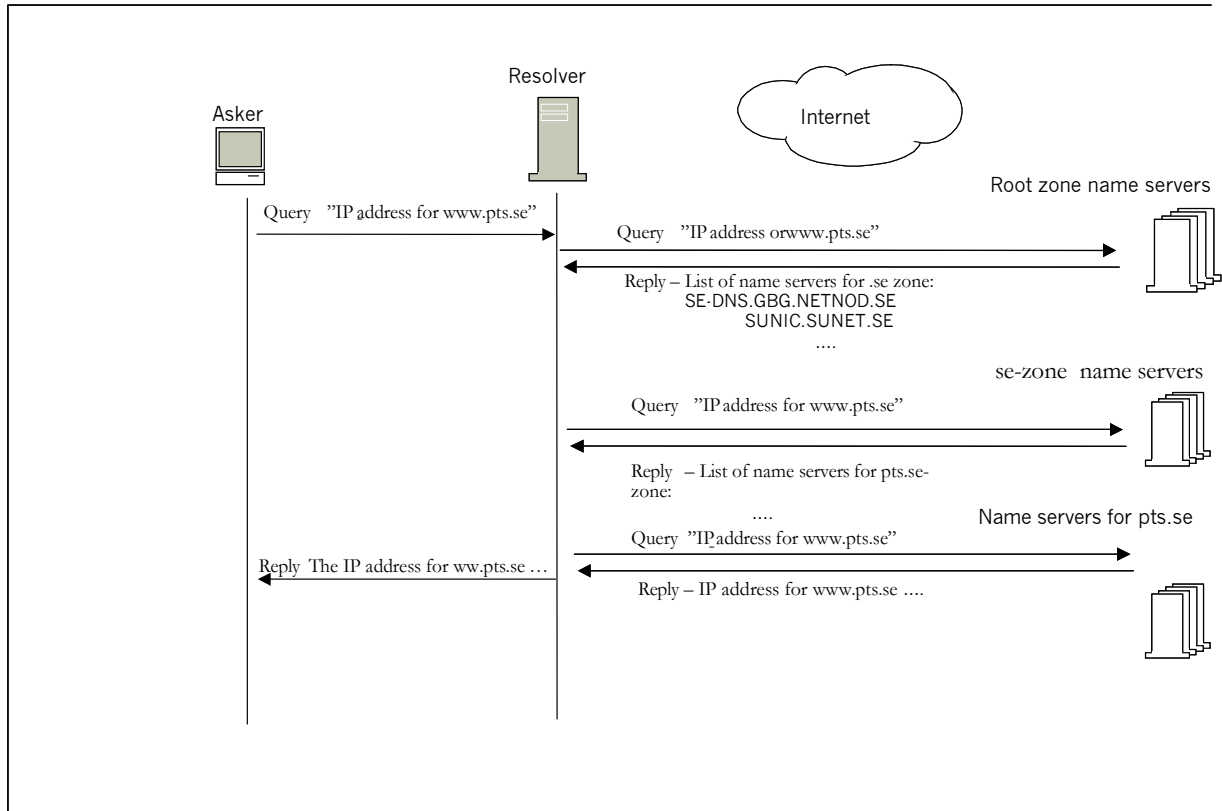
A name server generally includes a resolver function. This configuration allows the name server function to respond to queries concerning more than just its own authoritative zones. If the name server receives a query it is unable to respond to, it puts it to other name servers.

A complete domain name query

If a resolver does not have any cached information from previous searches, the following steps will take place when a user requests the IP address corresponding to the domain name `www.pts.se` (see figure 12):

1. The requesting computer sends a query to its resolver, requesting the A record for `www.pts.se`.
2. The resolver passes on the query to one of the root name servers.
3. The root name server responds by returning a list of the name servers containing IP addresses for `.se`.
4. The resolver queries one of the `.se` name servers.
5. The `.se` name server responds by returning a list of the name servers containing IP addresses for `pts.se`.
6. The resolver queries one of the `pts.se` name servers.
7. The `pts.se` name server responds by returning the IP address for `www.pts.se` to the resolver.
8. The resolver returns the reply to the requesting computer.

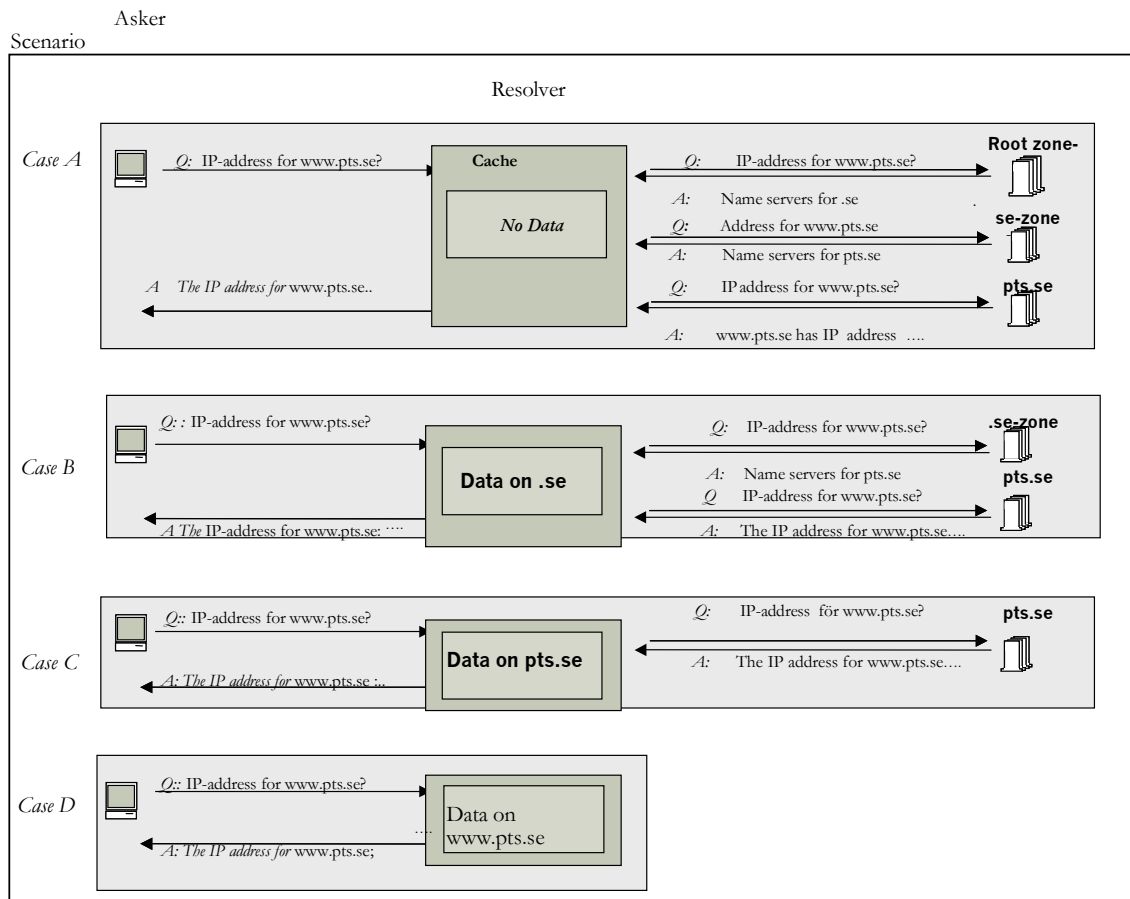
Figure 12 – A domain name search.



Caching

In order to avoid having to repeat the same queries, resolvers temporarily stores (caches) responses to previous domain name searches. Figure 13 shows how traffic directed to the domain name tree is affected by information being stored on the resolver. Under scenario A, the resolver does not have any cached information which prompts the resolver to query the name servers for the root, for .se and for pts.se. Under scenario B, the resolver has previously requested information about a different domain under .se. In that case, the resolver has received and cached information from the root servers concerning the name servers for .se, and does thus not need to ask the root servers again. Instead, it only needs to query the name servers for .se and for pts.se. Under scenario C, the resolver has previously requested different information from pts.se – it may for example have searched for mail.pts.se. The resolver thus knows the name servers for pts.se, which allows it to directly query a name server for pts.se.

Figure 13 – Traffic reduction as a result of cached information

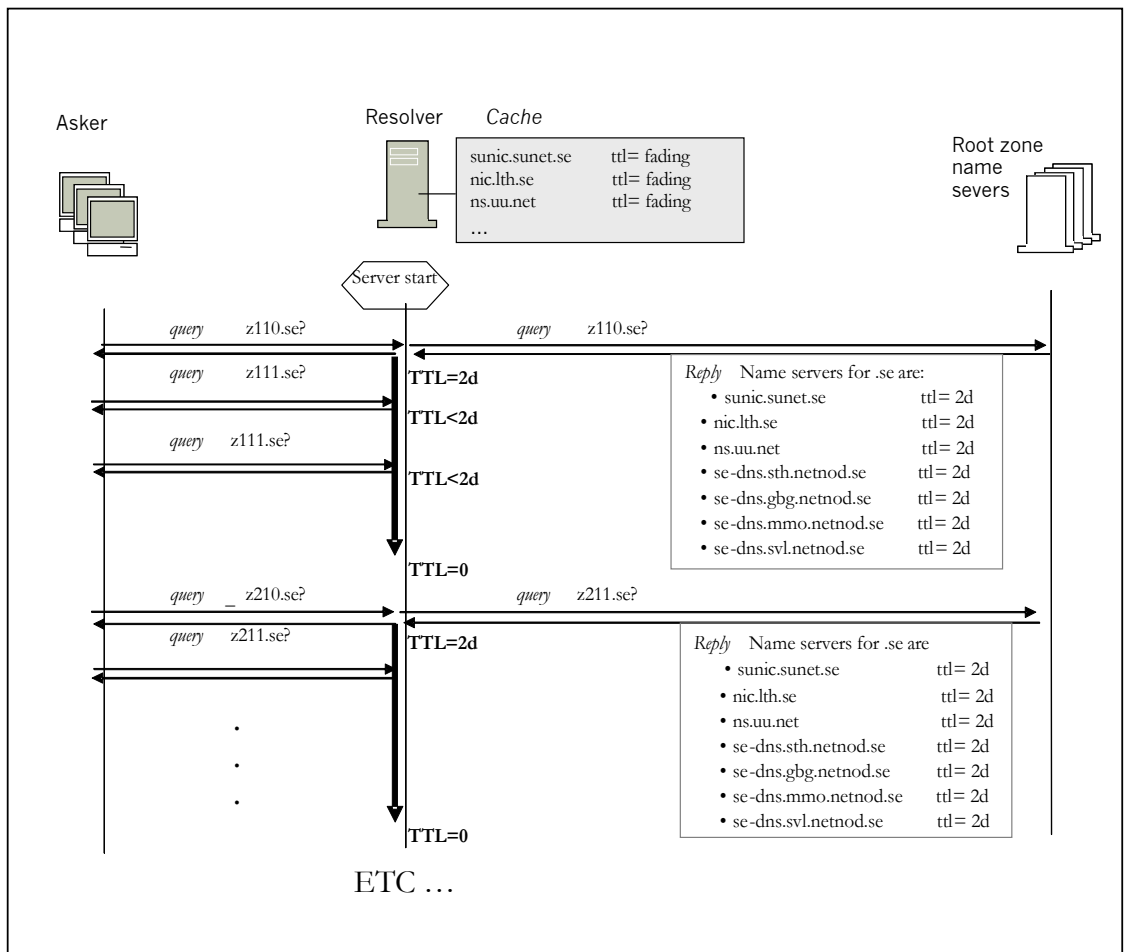


Under scenario D, the resolver has cached a previous response concerning **www.pts.se**. If it receives another query relating for **www.pts.se**, it will respond to it directly without querying the domain name tree.

TTL

In order to prevent cached information from becoming obsolete, each record is assigned a period of validity using the TTL parameter (Time To Live). Each record has its own assigned TTL value which tells the resolver how long data may remain in the cache. The TTL value is set by the entity configuring the zone, and is included in every response message (see figure 14).

Figure 14 – Caching of NS posts for a TLD



In the above example, when queried about the address for z110.se, a root name server returns a list with the authoritative name servers for .se. Every name server for the .se zone has a TTL value of 2 days. This implies that the resolver does not need to ask the root servers again for information about .se domains, but can go directly and query of the .se name servers. A high TTL value means that large quantities of information will be cached by the resolver thus resulting in reduced traffic loads, quicker responses and greater robustness when name servers fail. The main drawback is that it takes longer for changes to the configuration to spread.

Caching as a means to protect against service disruptions

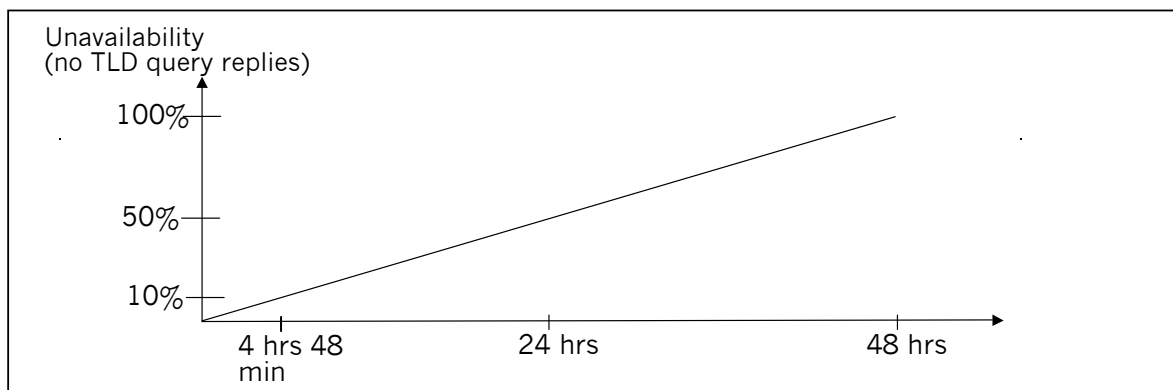
Resolvers caching of information may mitigate service disruptions resulting from name servers becoming unavailable. As the TTLs for the cached records gradually expire, the caching will only be effective for a certain period, after which the cached information expires and must be reloaded. Assume that all root name servers become unavailable at the exact same moment. Although this is a purely hypothetical example, the following chain of events is expected to occur:

A resolver may just have retrieved updated NS records for a particular TLD from a root server. If these records have a TTL of 48 hours, the resolver does not need to contact the root server for the same purpose for a long time. A less fortunate resolver may have received and update 47 hours and 59 minutes ago, which means that it will need an update already one minute after the crash. Thus, different resolvers will be affected by the loss of the root at different times. In a large sample, one can safely assume that the TTL values for the various resolvers are more or less evenly spread. They will thus expire as described in the curve in figure 15. After one hour, 1/48 of the resolver population will be affected by the disruption, after 24 hours half of the population will be out and so on.

The following is required for the above to work:

- no reboots are made.
- it is only likely to work for frequently requested TLDs which means that the response “always” is cached by the resolver (not the case for unusual TLDs).
- The TTL for the TLD’s name server is 48 hours, too.

Figure 15 – Caching will delay the impact of all name servers becoming unavailable



There are however some factors suggesting that users will experience the disruption sooner, and some factors suggesting that it will take longer before it is noticed. Factors indicating that damage will be felt sooner are:

- Both the sender's and the recipient's resolver must work for e-mail to be delivered.
- For surfing the web, a user needs domain names for several different TLD's, which are likely to have TTLs expiring at different times.
- Some domains, for example .se, has given its NS records a TTL of 1 day.
- It might be necessary to access the root because the TTL for the NS records in the root zone have expired.
- Users become nervous when the net is starting to behave in an unusual way, often prompting them to reboot the resolvers thus losing the cached information.

A factor suggesting that it will take longer for the effects to be felt is that the requested A record is in the cache. But more detailed assumptions are needed in order to determine exactly at what rate the DNS service deteriorates. One may under all circumstances conclude that caching does not replace the need to have available name servers. Caching will only mitigate the adverse effects for a limited period.

Different Applications' Dependence on the DNS service

E-mail

There are a plethora of different products and protocols used for electronic mail, for example POP3, IMAP, webmail and Outlook/MS exchange. For the example below, we have chosen to use a simple and commonly used configuration.

A simple example

In the example below, POP3 is used for retrieving e-mail and SMTP for sending e-mail. Using this setup, the user `adam@e1.se` sends a mail to the user `bertil@e2.se`.

Figure 16 – A simple configuration for electronic mail.



It is assumed that DNS lookups will be made as described in the table below:

Figure 17 – DNS lookups for sending an e-mail

Step in figure 16	Description	DNS queries
1.1	Connection to mail.e1.se	A record: mail.e1.se
1.2	The receiving mail server (mail.e1.se) verifies that the domains in both sender and recipient address exist. If all checks out, the mail is accepted for further delivery.	MX record: e1.se A record: mail.e1.se MX record: e2.se A record: mail.e2.se
2.1	mail.e1.se finds out to where mail for e2.se is to be delivered and sends the message to the indicated mail server (mail.e2.se)	MX record: e2.se A record: mail.e2.se
2.2	The receiving mail sever (mail.e2.se) is likely to do a DNS lookup to verify that both sender and recipient addresses exist (i.e. queries on e1.se and e2.se). If all checks out, the message is accepted for distribution to a local mail box belonging to the recipient.	MX record: e1.se A record: mail.e1.se MX record: e2.se A record: mail.e2.se
3	The recipient's computer will most likely only do a DNS query to find the IP address for the mail server where his e-mail account is hosted (mail.e2.se) . The message is then downloaded to his computer using the POP3 protocol.	A record: mail.e2.se

The above simple case shows that a large number of DNS queries have to be made just to deliver one single message.

Complicating factors

The above example is very basic. There are a number of other cases requiring more DNS support, for example:

- Many mail servers used today have very complex configurations with one single mail server being responsible for tens of thousands of different mail domains and which relies heavily on DNS to send messages to the right mail server. Such a configuration would have considerable difficulties coping without a functional DNS service.

- Management of aliases (forwarding) and mailing lists.
- Spam filters.

However, even the most basic configurations require a working DNS service in order to allow users to exchange e-mail.

Web

Accessing web pages generally involves domain names. For example, in the URL <http://www.iis.se/tptest>, www.iis.se is a domain name. A working DNS service is thus of fundamental importance to web use.

Provision of the DNS Service

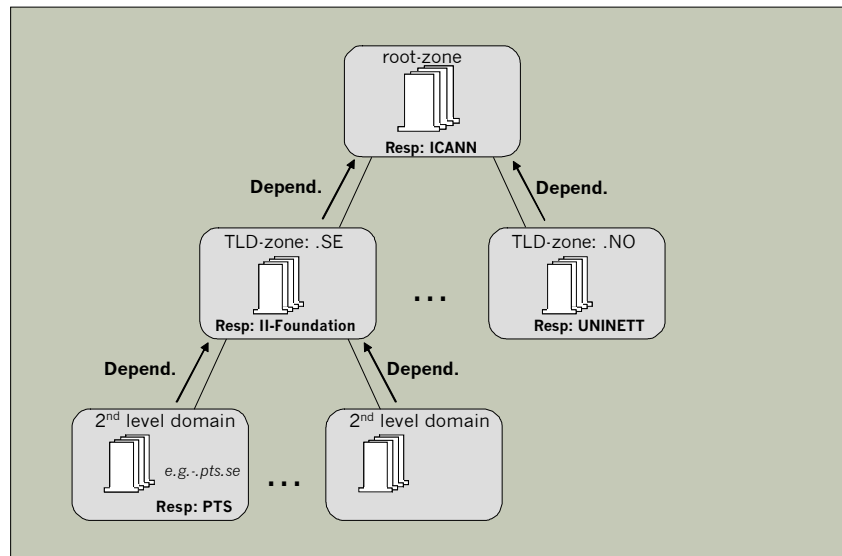
In the beginning, the Internet was a relatively limited phenomenon primarily used in the academic world. This may explain why the procedures for delegating responsibility for domains were very informal at first. Over time, more and more networks have been interconnected and more and more users are using the Internet, thus turning the net into an important element of society. Financial transactions, contacts between authorities and citizens and trade are all conducted on the Internet to an ever increasing extent. It is therefore logical that the authorities, companies and organizations which are increasingly dependent on this medium have legitimate requirements in terms of stability in terms of connection to the Internet and access to DNS. An important element in determining operational security should be that there are clear routines and clear lines of responsibility between the companies providing the services. Traditionally, the delegation of the responsibility for top level domains has been done informally through contacts between anyone interested in managing the domain and the organization having the worldwide responsibility for domain name management. For example, the responsibility for managing the Swedish top level domain was delegated from IANA in 1985 to a private individual in Sweden, Mr. Bjorn Eriksen. From that moment on, the top level domain has been managed in Sweden. The agreement was informal, supposedly with no written agreements⁵. The responsibility for DNS services has in many cases been delegated in a similar fashion, both at the root level and further down in the DNS tree.

⁵ See the report from the Committee on Domain Names (SOU 2000:30, page 37)

Dependencies

As we have seen above, a working system for DNS queries is required to enable users to surf the web and send e-mail. Providing the DNS service to an end user involves several organizations active in different fields at both the national and international levels. Dependencies, and to a lesser extent, responsibilities in the domain name tree resembles the hierarchical structure the domain name tree itself. This means that a higher level zone is responsible for pointing to lower level domains, meaning that name servers of the higher level zone answer queries concerning the domain below by providing a list of the name servers of the lower level domain. A given domain is dependent on the zones above it in order to play its part in the DNS services. For example, the second level domain pts.se is completely dependent on the services provided by .se and the root (see Figure 22). The opposite is not true, i.e. higher levels are not affected by deficiencies in the services provided by the lower levels. Finally, sibling domains do not affect each other.

Figure 22 – Dependencies in the domain name tree



Appendix 3 – What are IP Protocol and IP addresses?

Internet Protocol – IP

The network protocol Internet Protocol (IP) is used for sending packets of data from one computer to another over the Internet. IP is used for directing data traffic within and between networks, where traffic is sent in the form of packets and sent to the right destination with the help of routers. Each IP packet includes information about sender and recipient in the form of an IP address for each of them.

Internet Protocol Version 4 (IPv4)

An Internet Protocol version 4 (IPv4) address consists of 4 bytes (32 bits). It is generally written out in the form of four decimal numbers (in the interval 0 – 255) separated by periods, for example 193.180.23.16. IP addresses consist of a network portion and a host portion with a dynamic distribution between the two parts with the help of a so called subnet mask. Example: the subnet mask 255.255.255.0 indicates 3 bytes network and 1 byte host. 255.255.55.125 translates into 25 bits network and 7 bits host etc. IPv4 represents about 4 billion possible IP addresses, half of which are currently being used. The previous subdivision into classes of addresses (A,B ...) has been abandoned as a result of the shortage of IP addresses. Instead, so called classless IP addresses are being used throughout. Therefore, a sine qua non for being granted a range of IP addresses is that the Classless InterDomain Routing (CIDR) is fully supported by the operator's network.

Internet Protocol Version 6 (IPv6)

The latest version of the Internet Protocol, IPv6, has an 128 bit address. It has been developed by IETF as a new standard as the address space under IPv4 is insufficient to handle the needs of the ongoing and future expansion of the Internet.

The new protocol has the following characteristics:

- More available addresses with IPv6 being able to handle over 340 trillion, trillion, trillion (or 3.4×10^{38}) addresses, which means 4 million IP address per square kilometer of surface on earth.
- Supports IPsec – a standard for secure communication from end point to end point via VPN technology (Virtual Private Network) .
- Quality assurance by a dedicated “flow label” which is used for identifying flows and can be used to manage traffic on the basis of priority criteria.
- Systematic header compression thus reducing traffic loads on the net.

- A new function called “neighbor unreachability detection” which detects when a router becomes unavailable allowing for problems to be detected and addressed at an earlier stage.
- It is able to better manage mobile IP (mobile IP does not relate to mobile communications, rather it allows a user to be reached via the same IP address despite having moved to a different location and thus changed networks).

Appendix 4 - Glossary

This appendix contains definitions of terms and abbreviations used in the report.

Distribution Point	The specific point on the Internet to and from which name server operators are responsible for transporting IP Packets to and from their name servers.
BIND	(Berkeley Internet Name Daemon) software for name servers
Caching	Temporary storage of DNS data
DNS	Domain Name System (see Appendix 2).
DNS operator	Company or organization responsible for running DNS for a certain domain or zone.
DNS service	For the purposes of this report defined as a service providing information from the domain name tree at the request of a user. Can also be explained as the service translating names of WebPages or e-mail addresses to IP addresses and vice versa (see Appendix 2)
Domain	A level in the domain name hierarchy.
Domain Name	A name corresponding to an IP address.
Domain Name System	See Appendix 2.
Domain Name Tree	The hierarchical structure of the domain name system, with a root at the top, top level domains at the next level, followed by second level domains and so on.
DOS attack	Denial of Service-attack – An attack seeking to impair accessibility by deliberately trying to overload a server
GAC	Governmental Advisory Committee – a body advising ICANN made up of national representatives.

IANA	Internet Assigned Numbers Authority - organization responsible for the parameters and values used in the different Internet standards.
ICANN	Internet Corporation for Assigned Names and Numbers – organization inter alia responsible for the distribution of IP addresses and domain names.
IETF	Internet Engineering Task Force, International standard setting organization for Internet protocols.
ISP	Internet Service Provider
IP	Internet Protocol communication protocol managing addresses, routing and transfer of IP packets on the Internet.
IP address	Numerical address for computer or other equipment on an IP network. The address is written in the form of four decimal numbers separated by periods, e.g. 123.45.67.8
IPv4	Internet Protocol, version 4 (32-bit IP address).
IPv6	Internet Protocol, version 6 (128-bit IP-address).
Master server	In the context of DNS, the name server storing the database for the zone and from which the other name servers belonging to the zone retrieve the database.
MD5	Algorithm using a given quantity of information to calculate a checksum which is sent together with the information, and is used to verify that information has not been modified during transport.

NIC-SE	Network Information Centre Sweden - NIC-SE AB – accompany which manages the administration and operation on the Swedish domain .se on behalf of its owner, the II Foundation.
Redelegation	Modification of a record for a second level domain in the customer data base, where the name server has been replaced
Redundancy	Spare capacity, for example in the form of an alternative connection or extra, unused hardware.
Resolver	Puts DNS queries to different name servers in order to translate domain names to IP addresses.
Robustness	For the purposes of this report, the ability to function despite severe stress.
Root name server	Computer or cluster of computers holding a database with information about the root zone (the highest level in the DNS hierarchy).
Router	Computer with software for routing traffic between different IP networks.
SLA	Service Level Agreement - an agreement under which an Internet operator undertakes to maintain a certain quality in the service he offers, with a corresponding obligation to pay compensation he fails to meet the agreed requirements.
Slave server	DNS name server retrieving copies of their respective zone file from heir master server
SOF	Swedish Internet Operators Forum (SOF) is a trade association for the key Swedish Internet operators, more specifically those operators offering network services in Sweden and which have direct connections to one of the national nodes for Internet traffic in Sweden.
TLD	Top Level Domain – joint name for country code top level domains (ccTLDs) and generic top level domains (gTLDs).

T-SIG	Method for signing a quantity of information with symmetrical; encryption keys, i.e. sender and recipient use the same key for encryption and decryption. The recipient of a file, for example a slave server receiving a zone file from its master, can thus make sure that the contents of the file has not been modified and that it is authentic.
UDP	User Datagram Protocol – a simple transport protocol without functions for security and error control which can be used to rapidly send IP packets.