Date: 8/27/2012

Enterprise Architecture Office Resource Document Design Note - Domain Name System (DNS)

Table of Contents

1 **Overview** **2**

1.1 Other Resources 2

1.1.1 State of Minnesota Standards and Guidelines 2

1.1.2 Tools 2

1.1.3 Internet RFCs 3

2 **Resolver Configuration** **3**

3 **Firewall Configuration** **3**

4 **Service Overview** **3**

4.1 Delegations 4

4.2 Secondary Services 4

4.3 IPv6 4

4.4 Internal/External Split 4

4.5 DNSSEC 4

4.6 Customer Access 4

5 **Reverse Domains: in-addr.arpa and ip6.arpa** **5**

6 **The state.mn.us Domain** **5**

7 **The mn.gov and minnesota.gov Domains** **5**

7.1 Local Government Name Registration 6

7.2 Using Other .gov Names 6

8 **The k12.mn.us Domain** **6**

8.1 Name Forms 6

9 **The lib.mn.us Domain** **7**

10 **Naming Recommendations** **7**

10.1 Case #1: Small Organization, One Server 7
10.2 Case #2: Small Organization, Two Servers....8
10.3 Case #3: Organization That May Grow 9
10.4 Naming Recommendation Background.... 10
10.5 Naming Recommendation Summary.... 10
11 Hosting Domains: Having MN.IT Services be Your Domain Master.... 11
11.1 Executive Branch Customers 11
11.2 Non-Executive Branch Customers 11
12 Moving Servers Among Providers.... 12
12.1 Moving Mail Servers to Google 12
13 Domain Authority 13
13.1 What is DNS Authority?.... 13
13.2 What is an Authoritative DNS Server? 13
13.3 What is an Authoritative DNS Response?.... 13
13.4 What is a Non-Authoritative DNS Server?.... 13
13.5 What is a Non-Authoritative DNS Response?.... 14

1 Overview

MN.IT Services provides DNS service to its customers. This service includes:

- Looking up DNS names. The configuration page describes how to configure your computer to use this part of the service.
- Serving DNS names. The other pages in this section cover what you need to know to have MN.IT Services serve your domain.

This design note provides the technical information that will enable you to make the best use of the service.

1.1 Other Resources

1.1.1 State of Minnesota Standards and Guidelines

- DNS Naming Standard,http://mn.gov/oet/images/NET_S_DNS_Naming_2010-11-18.pdf
- DNS Naming Guidelines, http://mn.gov/oet/images/TEC_DNS_Naming_Guidelines.pdf

1.1.2 Tools

The site:

http://www.mnet.state.mn.us

has several DNS testing tools. They are in the “Data Networking” tab under “Tools” on the left.

1.1.3 Internet RFCs

These documents are available through the RFC Editor (http://www.rfc-editor.org):

- RFC-1480 - The US Domain
- RFC-1591 Domain Name System and Structure
- RFC 2146 - U.S. Government Internet Domain Names

2 Resolver Configuration

These are the settings to use when configuring the DNS resolver on your computer for use on MNET:

- 156.98.1.1
- 207.171.71.71
- 207.171.88.188

You can use them in any order in your DNS configuration.

These servers will return IPv6 DNS records, if those records are available.

Note that these addresses do not work from outside of the MN.IT Services-managed network (“MNET”). If you are coming from outside of MNET, you should contact your ISP for DNS configuration settings.

For reference, the names associated with these entries are:

- vns1.state.mn.us: 156.98.1.1
- vns2.state.mn.us: 207.171.71.71
- vns3.state.mn.us: 207.171.88.188

You won’t ordinarily need to use these names for anything.

3 Firewall Configuration

With the advent of IPv6 records in DNS data and DNSSEC, requirements on firewalls have also changed.

Firewalls that pass DNS traffic should be configured as follows:

- Permit both UDP and TCP traffic (port 53 in both cases).
- Allow requests and responses of any size.

The reason is that requests and responses can both be much larger than before. Where the request or response is larger than 576 bytes but still fits within a UDP packet (or any size), it should be permitted. If the UDP request fails, the DNS resolver should automatically switch to retry the request with TCP. Thus, TCP DNS connections should be permitted (and will be used with increasing frequency.)

4 Service Overview

MN.IT Services operates a set of high-performance, fully up-to-date name servers located across the state. All servers are connected to our redundant data network. MN.IT Services meets or exceeds all current operational “best practices” for DNS services.

4.1 Delegations

With these multiple servers, MN.IT Services handles both primary and secondary[1] servers for its domains. Due to the tight integration of its DNS servers with the rest of MN.IT Services operations, MN.IT Services will not normally delegate any part of its domains to other servers, either on a primary or secondary basis.

The exceptions to this practice are the k12.mn.us and lib.mn.us domains, for which the delegated domain's owner may freely choose their DNS provider.

4.2 Secondary Services

MN.IT Services does not provide secondary DNS services except by special arrangement.

4.3 IPv6

MN.IT Services accepts requests to add IPv6 address records ("AAAA") for inclusion in our DNS and manages the reverse address space that corresponds to our assigned IPv6 network blocks. Also, our DNS servers will properly perform IPv6 lookups for other sites on the Internet.

At this time, our DNS servers do not currently accept requests using IPv6 packet encapsulation. We do anticipate accepting such requests as we deploy IPv6 across our network.

4.4 Internal/External Split

MN.IT Services' name servers are configured to supply different responses in some cases to clients inside and outside our network.

"Inside" includes the MN.IT Services-managed network ("MNET"). "Outside" includes the general Internet.

The differences fall into two categories:

- Some names are not visible when looked up from outside. Examples of such names are the internal network devices.
- Some names return different responses. Examples of such names are those for accessing the BPOS-D services, which return one set of IP addresses when looked internally and a different set when looked up externally. This difference allows us to keep such traffic on-network where possible.

4.5 DNSSEC

MN.IT Services servers will properly handle queries which request DNSSEC validation. As such, you may receive unexpected error responses.[2] Just like with any other DNS data, the domain owner is responsible for ensuring the contents of the domain are correct and MN.IT Services cannot "fix" any incorrect data, including any problems with DNSSEC signing or keys.

MN.IT Services currently signs records in the state.mn.us, mn.gov, and minnesota.gov zones. Signing other zones is in progress.

4.6 Customer Access

MN.IT Services' systems have the capability to permit direct customer access for viewing and editing their information. Customers may choose to request an account or send service request to MN.IT Services for fulfillment. The customers best suited to requesting an account are those that request DNS changes at least monthly (on the average).

[1] Or master and slave.

[2] If you are testing from the command line with dig, don't forget the "+DNSSEC" option.

5 Reverse Domains: in-addr.arpa and ip6.arpa

The in-addr.arpa and ip6.arpa domains handle the task of converting IP addresses back into names. For example, if you have the IP address 1.2.3.4 and want to see what name has that as its address, you would look up the PTR record for 4.3.2.1.in-addr.arpa. (note the reversal of the numbers).

For all networks within MNET system (*e.g.*, 156.98.0.0/16, 156.99.0.0/16, and 2607.f830::/32), MN.IT Services' DNS servers handle the reverse lookups. In order to guarantee correctness of these reverse entries, MN.IT Services constructs the reverse lookup information automatically from the forward information. For this method to work, MN.IT Services must be the primary server for the reverse lookup domains. Hence, MN.IT Services will not delegate any zones for in-addr.arpa or ip6.arpa domains.

As a result of this configuration, if there are DNS names outside of zones managed by MN.IT Services that are assigned IP addresses within the MNET system, MN.IT Services will add those outside names in for address to name conversion purposes (only).

Since any given in-addr.arpa or ip6.arpa address can[3] only match to a single IP address, MN.IT Services will not normally configure more than one DNS name at any one IP address. If two or more DNS names must use the same IP address, all but one will be entered as CNAME records. See also section 9.

6 The state.mn.us Domain

MN.IT Services (officially "The State of Minnesota, Office of Enterprise Technology") is the domain manager for the state.mn.us domain. This section details the requirements for registrations within that domain.

> Note: the mn.gov and minnesota.gov domains are linked to the state.mn.us domain as described in the next section. So, the discussion in this section applies to those domains as well.

The state's DNS standard requires that all information offered by executive branch state government organizations be available under one or more of the three domains (state.mn.us, mn.gov and minnesota.gov). While the standard only requires that information be available through one of these, organizations are encouraged to offer the same information across all three domains.

Further, these domains will be used only for Minnesota government-supported purposes.

MN.IT Services is the state's DNS provider for these domains and has configured the contents of the mn.gov and minnesota.gov domains to automatically track those of the state.mn.us domain. This means that any name in the state.mn.us (for example, www.state.mn.us) is automatically also placed in the mn.gov and minnesota.gov domains (for our example, www.mn.gov and www.minnesota.gov).

Again, this updating is automatic. Updates normally happen on an overnight basis.

7 The mn.gov and minnesota.gov Domains

MN.IT Services (officially "The State of Minnesota, Office of Enterprise Technology") is the domain manager for the mn.gov and minnesota.gov domains.

MN.IT Services is the state's DNS provider for both of these domains and has configured their contents to automatically track those of the state.mn.us domain. This means that any name in the state.mn.us (for example, www.state.mn.us) is automatically also placed in the mn.gov and minnesota.gov domains (for our example, www.mn.gov and www.minnesota.gov).

[3] Well, technically you can have more than one PTR record for a given address, but doing so will cause many services to encounter problems.

Again, this updating is automatic. Updates normally happen on an overnight basis.

7.1 Local Government Name Registration

Local government entities should always use their RFC 1480-defined names. These names are of the form:

- ci.*entity*.mn.us for cities
- co.*entity*.mn.us for counties

While officially required, these name forms do not reflect current Internet trends and many local government entities would like names in the .gov domain. To make it easy for local government to use .gov names, MN.IT Services offers registrations of names of the forms:[4]

- *entity*.ci.mn.gov for cities
- *entity*.co.mn.gov for counties

which is an easy way for cities and counties to obtain .gov names at no charge and with minimal paperwork.

Any other names (*e.g.*, .com or .org) used by local government should supplement and not replace the official names. Since all local government entities are either existing or potential MN.IT Services customers, MN.IT Services will provide name servers for those domains at no additional charge.

7.2 Using Other .gov Names

Local government entities may also use other .gov domain forms (see the information from the .gov registrar at http://dotgov.gov). As part of their process, the .gov registrars require the approval of the State of Minnesota CIO. The CIO will require a certification that the local government requesting the other form is aware of the no-cost option listed above and does not wish to use it.

8 The k12.mn.us Domain

MN.IT Services (officially “The State of Minnesota, Office of Enterprise Technology”) is the domain manager for the k12.mn.us domain.

All K-12 schools, community colleges/technical schools, state and local governments are required to register under the .us domain. Only four year universities are allowed to register under the .edu domain.

MN.IT Services will provide DNS service for any K-12 organization at no cost. Most ISPs also provide this service.

8.1 Name Forms

For K-12 districts, domain names are of the form:

hostname.*districtname*.k12.mn.us

and we will delegate authority at the district level.

One (only) domain will be established per school district. Typically names are either the district name or number, for example:

- isd910.k12.mn.us
- woodfalls.k12.mn.us

For K-12 Charter schools, domain names are typically either of the form:

hostname.*schoolname*.charter.k12.mn.us

[4] Actually, the *entity*.ci/co.state.mn.us and *entity*.ci/co.minnesota.gov variants will also exist and can be used, but the emphasis has been on the mn.gov form.

and we will delegate authority at the school level, or of the form:

hostname.*schoolname*.district.k12.mn.us

where district is the sponsoring school district under which the charter school is formed.

Either format is acceptable for charter schools. Per RFC 1480, we do not register charter school names as domains:

schoolname.k12.mn.us - NOT

For K-12 private schools, domain names are of the form:

hostname.*schoolname*.pvt.k12.mn.us

and we will delegate authority at the school level.

9 The lib.mn.us Domain

MN.IT Services (officially “The State of Minnesota, Office of Enterprise Technology”) is the domain manager for the lib.mn.us domain. This branch may be used for libraries only. For example: *library-name*.lib.mn.us.

MN.IT Services will provide DNS service for any library at no cost. Most ISPs also provide this service.

10 Naming Recommendations

There are many ways to make use of the DNS when assigning names to computers and services. Some of these ways work better than others. Using our many years' experience in operating a state-of-the-art set of DNS servers, we offer the following set of recommendations.

The recommendations start with some sample cases, then review the general background information. In most cases, you can stop reading when you reach the sample case that matches yours.

In this document, the text "SAMPLE.DOMAIN" will represent the organization's DNS domain. Examples of such domains are "acme.k12.mn.us", "co.fred.mn.us" and "nonprofit.org".

10.1 Case #1: Small Organization, One Server

This organization has one system to handle both email and web traffic. The DNS would be set up as:

```
SAMPLE.DOMAIN.            MX       10 mail.SAMPLE.DOMAIN.
mail.SAMPLE.DOMAIN.       A        1.2.3.4
                          MX       10 mail.SAMPLE.DOMAIN.
www.SAMPLE.DOMAIN.        CNAME    mail.SAMPLE.DOMAIN.
```

examples:

```
acme.k12.mn.us.           MX       10 mail.acme.k12.mn.us.
mail.acme.k12.mn.us.      A        1.2.3.4
                          MX       10 mail.acme.k12.mn.us.
www.acme.k12.mn.us.       CNAME    mail.acme.k12.mn.us.
co.fred.mn.us.            MX       10 mail.co.fred.mn.us.
mail.co.fred.mn.us.       A        1.2.3.4
```

```
                             MX        10 mail.co.fred.mn.us.
www.co.fred.mn.us.           CNAME     mail.co.fred.mn.us.
nonprofit.org.               MX        10 mail.nonprofit.org.
mail.nonprofit.org.          A         1.2.3.4
                             MX        10 mail.nonprofit.org.
www.nonprofit.org.           CNAME     mail.nonprofit.org.
```

This configuration supports the following:

- email can be sent to user@SAMPLE.DOMAIN.
- web access is offered via www.SAMPLE.DOMAIN or just SAMPLE.DOMAIN.

10.2 Case #2: Small Organization, Two Servers

This organization has two systems, one to handle email and another to handle web traffic. The DNS would be set up as:

```
SAMPLE.DOMAIN.               MX        10 mail.SAMPLE.DOMAIN.
mail.SAMPLE.DOMAIN.          A         1.2.3.4
                             MX        10 mail.SAMPLE.DOMAIN.
www.SAMPLE.DOMAIN.           A         2.3.4.5
```

examples:

```
acme.k12.mn.us.              MX        10 mail.acme.k12.mn.us.
mail.acme.k12.mn.us.         A         1.2.3.4
                             MX        10 mail.acme.k12.mn.us.
www.acme.k12.mn.us.          A         2.3.4.5
co.fred.mn.us.               MX        10 mail.co.fred.mn.us.
mail.co.fred.mn.us.          A         1.2.3.4
                             MX        10 mail.co.fred.mn.us.
www.co.fred.mn.us.           A         2.3.4.5
nonprofit.org.               MX        10 mail.nonprofit.org.
mail.nonprofit.org.          A         1.2.3.4
                             MX        10 mail.nonprofit.org.
www.nonprofit.org.           A         2.3.4.5
```

This configuration supports the following:

- email can be sent to user@SAMPLE.DOMAIN.
- web access is offered via www.SAMPLE.DOMAIN.

This configuration does not support email to user@www.SAMPLE.DOMAIN. This is not normally a problem, just set the webmaster address in the server to:

webmaster@SAMPLE.DOMAIN

10.3 Case #3: Organization That May Grow

This organization has two systems, one to handle email and another to handle web traffic. However, the organization expects to grow one or both services to multiple machines. The DNS would be set up as:

```
SAMPLE.DOMAIN.              MX       10 mail.SAMPLE.DOMAIN.
                            SOA      ...supplied by DNS hosting org.
                            NS       ...supplied by DNS hosting org.
mail.SAMPLE.DOMAIN.         A        1.2.3.4
                            MX       10 mail.SAMPLE.DOMAIN.
wserver.SAMPLE.DOMAIN.      A        2.3.4.5
www.SAMPLE.DOMAIN.          CNAME    wserver.SAMPLE.DOMAIN.
```

examples:

```
acme.k12.mn.us.             MX       10 mail.acme.k12.mn.us.
                            SOA      ...supplied by DNS hosting org.
                            NS       ...supplied by DNS hosting org.
mail.acme.k12.mn.us.        A        1.2.3.4
                            MX       10 mail.acme.k12.mn.us.
wserver.acme.k12.mn.us.     A        2.3.4.5
www.acme.k12.mn.us.         CNAME    wserver.acme.k12.mn.us.
co.fred.mn.us.              MX       10 mail.co.fred.mn.us.
                            SOA      ...supplied by DNS hosting org.
                            NS       ...supplied by DNS hosting org.
mail.co.fred.mn.us.         A        1.2.3.4
                            MX       10 mail.co.fred.mn.us.
wserver.co.fred.mn.us.      A        2.3.4.5
www.co.fred.mn.us.          CNAME    wserver.co.fred.mn.us.
nonprofit.org.              MX       10 mail.nonprofit.org.
                            SOA      ...supplied by DNS hosting org.
                            NS       ...supplied by DNS hosting org.
mail.nonprofit.org.         A        1.2.3.4
                            MX       10 mail.nonprofit.org.
wserver.nonprofit.org.      A        2.3.4.5
www.nonprofit.org.          CNAME    wserver.nonprofit.org.
```

This configuration is similar to that of case #2, except that the www.SAMPLE.DOMAIN name is now a CNAME to another computer. Organizations that expect to grow need to deal with such issues as being able to smoothly upgrade or expand servers. The best way to achieve that goal is to separate out the names of the services (in this case, www.SAMPLE.DOMAIN) from that of the computers used to implement the service.

With this separation, you can build a new server then switch all traffic to it by changing just the one CNAME target. You can also change it back if you run into problems.

As a rule-of-thumb, you shouldn't have an IP address attached to a service.

For email, the MX record (on the SAMPLE.DOMAIN name) serves the same purpose as the CNAME.

10.4 Naming Recommendation Background

The above patterns take the following considerations into account:

- If you are sending email, your DNS name should match your IP address both for the forward (mail.SAMPLE.DOMAIN -> 1.2.3.4) and the reverse (4.3.2.1.in-addr.arpa -> mail.SAMPLE.DOMAIN) directions.
- When sending mail, it is OK if your domain does not match the domain used in the mail message but is within it. For example, for users with address of the user@SAMPLE.DOMAIN form, it is ok if you are sending email from a server named mail.SAMPLE.DOMAIN.
- If you are either sending or receiving email, you should have an MX record pointing to yourself.
- You should not have more than one DNS name with the same IP address. If you need more than one name pointing to the same place, all but one should be CNAME or MX instead. Why? Two reasons. First, inevitably someone will change one and forget to change the other. Normally, this discrepancy isn't discovered until a few months later. Second, the reverse direction (address -> name) has to pick one or the other and, if both are present, it can pick wrong.
- Often, people want users to be able to type in URLs without the leading "www". All modern browsers will add the "www" as needed, so there should be no reason to have to put this alternate form in the DNS. Unfortunately, ISPs and others are returning advertising pages instead of no such domain errors, so both forms are often registered.
- However, the "www" addition won't work if the first name that is tried has an IP address. For example, if SAMPLE.DOMAIN has an IP address, the browser won't automatically add the "www" – even if the SAMPLE.DOMAIN isn't running a web server. Thus, if you ever put an IP address on the domain, your users will come to expect that it is your web server. This causes major problems later if you need to have separate mail and web servers (for example, if you are offering web-based email access to your own users).
- With these patterns, someone can look at the names a year later and still readily figure out what is going on.
- These patterns take into account DNS rules and limitations such as:
  - CNAME records can't point to other CNAME records.
  - MX records can't point to other MX records.
  - If a name has a CNAME record, it can't have any other records.
  - You can't CNAME at the domain level. (Technically a repetition of the previous rule, but not always obvious.)

10.5 Naming Recommendation Summary

These are recommendations, not hard policies. That said, they are based on many years' hard experience and – unless you have similar experience – you probably don't want to go against them.

11 Hosting Domains: Having MN.IT Services be Your Domain Master

MN.IT Services will host your domain at no charge provided you are either:

- An existing MN.IT Services data networking services customer,
- An existing MN.IT Services mail services customer,
- An existing MN.IT Services customer for any other service,
- The owner of a domain in the k12.mn.us zone,
- The owner of a domain in the lib.mn.us zone or
- Are eligible to be an MN.IT Services customer.

11.1 Executive Branch Customers

If you are an executive branch organization, the *DNS Naming Standard* applies and you should contact MN.IT Services through your account executive as soon as you are considering using a DNS name that doesn't end in state.mn.us, mn.gov, or minnesota.gov. You will need Enterprise Architecture Office approval for use of any new name outside of those three domains.

11.2 Non-Executive Branch Customers

If you aren't an executive branch organization, MN.IT Services will host your domain on our servers at no charge. This is a multi-step process.

First, you send us a request with:

- The fully-qualified name of the zone that you wish us to host, and
- At least one record to put in it (*e.g.*, an A or MX record).

We will notify you when the domain is set up in our servers (normally one or two business days). At this time, we will be serving the domain to anyone who uses our name servers but not to the Internet as a whole.

Second, you must then contact the registrar for your domain and give them the following name server information:

- ns1.state.mn.us.
- ns2.state.mn.us.
- ns3.state.mn.us.

For the record, the IP addresses associated with these names are:

- ns1.state.mn.us: 192.112.135.1
- ns2.state.mn.us: 192.112.136.1
- ns3.state.mn.us: 192.112.137.1

However, you should not need these IP addresses for doing your registration. In fact, if your registrar even asks for the IP addresses, they aren’t following the DNS standards and you should find another registrar.[5]

For k12.mn.us and lib.mn.us domains, we are the domain registrar and you can skip this step provided you have us host the domain.

After the domain registrar has updated their information, the domain will be "live" on the Internet.

Note that you are responsible for all interaction with your domain registrar and you are responsible for any fees that they charge.

[5] If you want an explanation of this statement, please feel free to contact the Enterprise Architecture Office.

12 Moving Servers Among Providers

Many organizations have been moving their servers among providers. In particular, they have been moving their mail servers to Google's service. This page provides instructions for making that move.

While this page only has instructions for moving to Google's services for now, we will add instructions for other services as warranted.

12.1 Moving Mail Servers to Google

These instructions assume that there is an existing mail server named students.example.com. The DNS zone for your organization might look like this:

```
$ORIGIN                                example.com.

@                            A         192.168.0.1

                             MX        10 example.com.    ; for faculty & staff

                             A         192.168.1.2

students                     MX        10 students.example.com.
```

Note that student and faculty/staff mail is handled by different servers. If you want to move just student mail to Google and retain faculty/staff mail on your own servers, you'll have to split them like this first.

If you want all mail moved, you can do that. It's really the same process.

Once you're ready, you will do a series of steps. You should allow ten business days or so for the process to complete: it may well happen faster, but there are lots of steps.

First, you'll sign up with Google. They will ask that you confirm that you are in control of the zone. You do this by entering a DNS record that they will give you. It will be of the form:

```
googleXXXXXXXXXXXXXXXX.student.example.com.      CNAME   google.com.
```

The "XXXXXXXXXXXXXXXX" is a string of 16 hexadecimal characters. The target of the CNAME may vary: enter it exactly as they give it to you.

If MN.IT Services is primary for your domain, you send us a request to add the record. Otherwise, you either configure it yourself or send a request to whoever is primary for your domain to add the record.

Second, once the record has been added, you notify Google. By using this sequence, Google knows that you are in control of your domain.

Google will tell you what mail servers to use (it will almost certainly be the same as the list below). You need to send another DNS request to have those records added. The request will most likely be for records like this:

```
students.example.com.        MX        10 aspmx.l.google.com.
                             MX        20 alt1.aspmx.l.google.com.
                             MX        20 alt2.aspmx.l.google.com.
                             MX        30 aspmx2.googlemail.com.
                             MX        30 aspmx3.googlemail.com.
                             MX        30 aspmx4.googlemail.com.
                             MX        30 aspmx5.googlemail.com.
```

Again, if MN.IT Services is primary for your domain, you send us a request to add the record. Otherwise, you either configure it yourself or send a request to whoever is primary for your domain to add the record.

Finally, you remove the previous MX records from your domain. You will most likely do this at the same time that you add the new records listed above.

13 Domain Authority

This section provides background material to help you understand the concept of “domain authority.”

13.1 What is DNS Authority?

Any DNS server that contains a complete copy of the domain's zone file is considered to be *authoritative* for that domain. A complete copy of a zone file must have:

- A valid Start of Authority (SOA) record,
- Valid Name Server (NS) records for the domain and
- The listed NS records should match the servers listed in the SOA record.

Servers listed in the zone file but not in the SOA record are called lame servers and such a configuration should be avoided. It is considered standard practice to have a primary authoritative DNS server and one or more secondary authoritative DNS servers. When registering your domain with an accredited domain name registrar, the primary authoritative DNS server is the server you list first: all other DNS servers you list will be secondary. The secondary server and the primary server should be on different IP subnets and the hardware should be located in different physical locations. By putting the DNS servers on different subnets and placing them apart geographically, you greatly reduce the risk that a single outage will take down the entire system of DNS servers for your domain. Having more than one secondary DNS server for your domain is also good practice, but you can only designate one primary DNS server with your registrar because the DNS can only point to a single primary DNS server for your domain.

13.2 What is an Authoritative DNS Server?

DNS Servers can be configured to host more than one domain. A server can be primary for one domain and secondary for another. The term *authoritative* refers to any DNS server that has a complete copy of the domain's information, whether it was entered by an administrator or transferred from a primary server. Thus, a secondary server can and should be authoritative for any domain for which it performs secondary resolution.

Note that if a secondary server loses contact with the primary server for a domain, it will stop being an authoritative server after a timeout period (usually a few days).

13.3 What is an Authoritative DNS Response?

Any response to a DNS query that originates from a DNS server with a complete copy of the zone file is said to be an *authoritative response*. What complicates matters is that DNS servers cache the answers they receive. If a DNS server has an SOA record, it fills in a field in the response that signals that the server queried is authoritative for the domain and that the answer is authoritative. Any DNS server external to that domain that retrieved the authoritative response will cache that answer. The next time the server is queried, it will say that the answer it is giving is authoritative, even though the server itself is not authoritative for that domain

In other words, it is possible for a DNS server that is not an authoritative server for a domain to give an authoritative response to a DNS query.

13.4 What is a Non-Authoritative DNS Server?

Non-authoritative servers do not contain copies of any domains. Instead they have a cache file that is constructed from all the DNS lookups they have performed in the past for which they have gotten an authoritative response and for which the response has not “timed-out.”

When a non-authoritative server queries an authoritative server and receives an authoritative answer, it passes that answer along to the querent as an authoritative answer. Thus, non-authoritative servers can answer authoritatively for a given DNS request. However, if another request comes for a different name in the same domain, they can’t answer without asking an authoritative server for that domain.

Most often, a non-authoritative server answers with a previous lookup from its lookup cache. Any answer retrieved from the cache of any server is deemed non-authoritative because it did not come from an authoritative server.

13.5 What is a Non-Authoritative DNS Response?

Non-authoritative responses come from DNS servers that have cached an answer for a given host, but received that information from a server that is not authoritative for the domain.