**Lesson 6**

**Domain Name System (DNS)**

Content

[1. Setting up a basic caching-only DNS Server with bind 2](#_Toc91175859)

[2. Connecting a client to a specific DNS server 4](#_Toc91175860)

[3. Setting up Forward Lookup Zone 5](#_Toc91175861)

[4. Setting up Reverse Lookup Zone 7](#_Toc91175862)

[5. Perform a Zone transfer 9](#_Toc91175863)

[6. Reset and restore /etc/resolv.conf 10](#_Toc91175864)

1. Setting up a basic caching-only DNS Server with bind

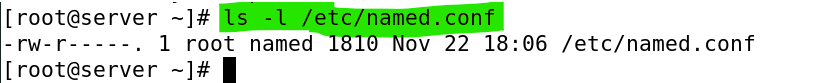
On server:

1. Install the bind and bind-utils packages.

dnf -y install bind bind-utils

1. Check that the group owner of the config file /etc/named.conf is "named".

ls –l /etc/named.conf



1. To prepare for the forward lookup zone exercise, first set your host name to server.las.org by using the hostnamectl command:

hostnamectl set-hostname server.las.org

1. Find the IP address of your original local DNS Server by checking the contents of /etc/resolv.conf. Note the IP address of the nameserver (eg 172.16.108.2). You shall observe that the search option has been changed to las.org too.

A picture containing text

Description automatically generated

As shown at the above, the server is using 192.168.30.2 as its DNS.

1. Setting up a cache only , forwarder only Local DNS in your server:

A forwarder only DNS provides DNS service to itself and other clients, but it only forward the DNS requests to another DNS to obtain the answer.

Edit /etc/named.conf and change the following options settings in bold to allow your client’s subnet to make queries. Set the forwarders value to the IP address of the original local DNS Server.

Change this to the subnet of your server

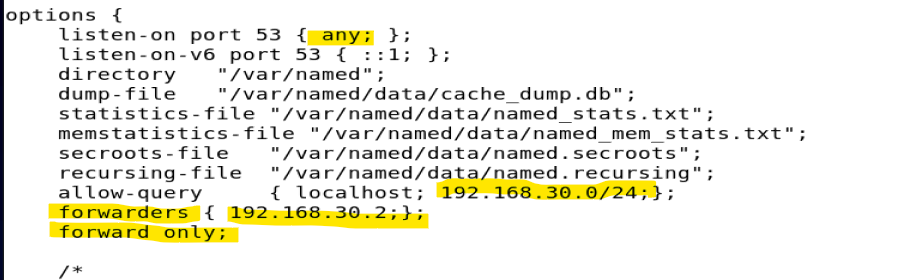
listen-on port 53 { **any**; };

allow-query { localhost; **192.168.30.0/24;** };

Change this to the original nameserver IP in /etc/resolv.conf (add this line if it does not exist)

**forwarders { 192.168.30.2; };**

**forward only;**



1. As your original local DNS Server may not be able to support DNSSEC, disable the DNSSEC validation by changing the following lines.

dnssec-enable **no**;

dnssec-validation **no**;

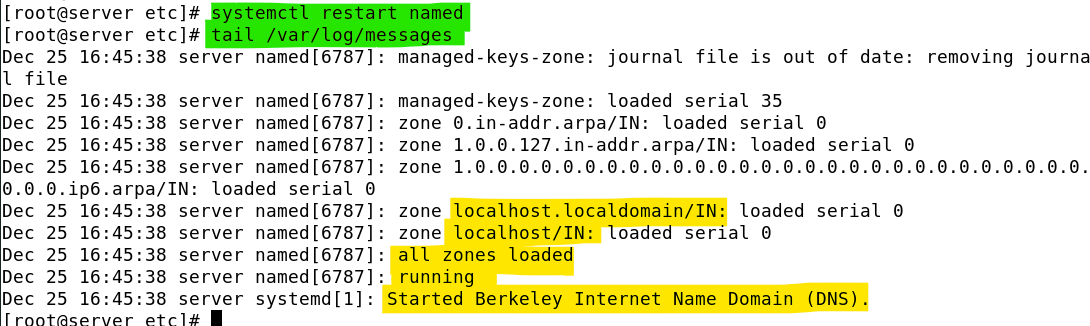
1. Start the named service.

systemctl start named

1. Configure the named service to be automatically started at bootup.

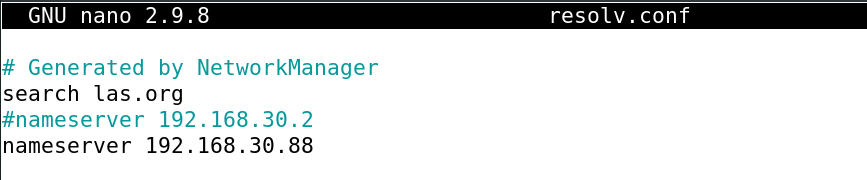
systemctl enable named

1. Check /var/log/messages if there are any errors with your named service.



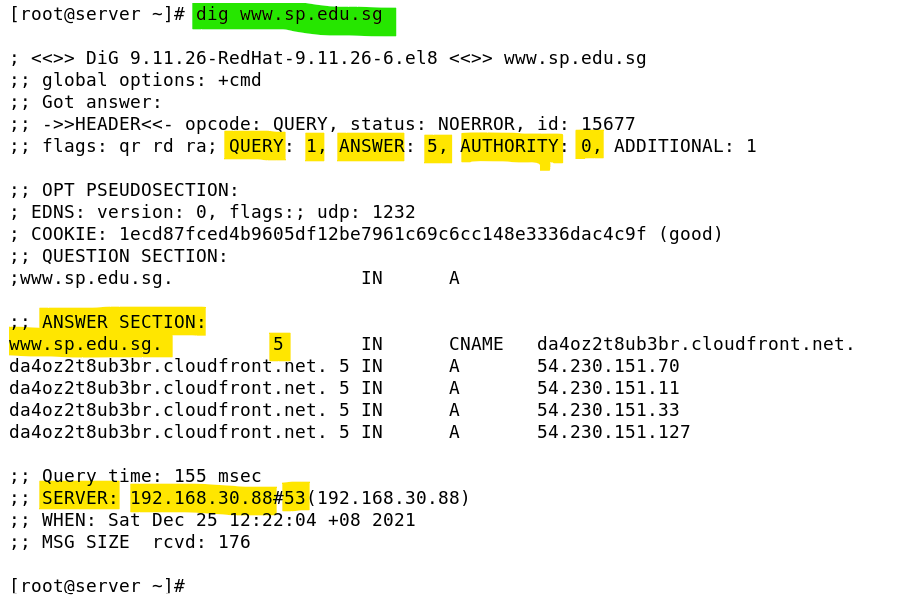
1. Edit /etc/resolv.conf and comment out the original nameserver entry. Add your server IP as the nameserver.

nameserver <*serverIP>*



1. Perform a DNS query using dig. Look for the ANSWER section which contains the result of the IP address. Note that the SERVER should be your server IP.

dig www.sp.edu.sg

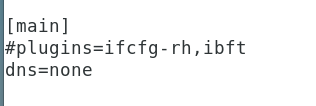


(Refer to <https://blog.dnsimple.com/2015/03/whats-in-a-dns-response/> to find out the detail interpretation of the entries shown at the ANSWER SECTIN. E.g. What does the '5' mean?)

1. The update of the /etc/resolv.conf (at step 10) is not yet permanent. The NetworkManager process will re-generate this file at the next boot time. To disable the regeneration, you need to :

Modify /etc/NetworkManager/NetworkManager.conf :

a. Under the [main] section, modify or add in the dns setting entry to set it to 'none'.



* + - * 1. b. Restart the NetworkManager process:

systemctl restart NetworkManager

* + - * 1. c. Repeat step 11 to ensure you are still using your own server as the DNS.

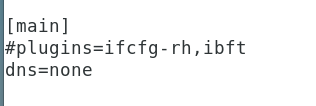
1. Connecting a client to a specific DNS server

To verify your server is providing DNS service to other clients in the same subnet, start your client and configure it to use your server as its only DNS:

On Client: (login as root)

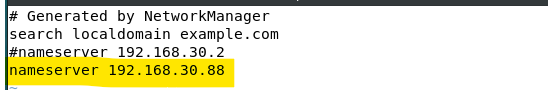
1. Modify /etc/NetworkManager/NetworkManager.conf :

a. Under the [main] section, modify or add in the dns setting entry to set it to 'none'.



b. Edit /etc/resolv.conf and comment all lines in it. Add your server IP as the nameserver.

nameserver <serverIP>



1. Perform a DNS query using host -a. Note that the results come from your server IP.

host -a www.sp.edu.sg

[Note: You need to open the dns service at the firewall of your server to enable the client to access to the server's DNS service]

1. Perform a reverse lookup DNS query for 164.78.252.49.

dig -x 164.78.252.49

host -a 164.78.252.49

[Note: Reverse lookup is to look for the official domain name of a given ip address. The output of the above two commands may give you some interesting findings. Ie. DNS operations may only focus on the forward lookup zone configurations while sometimes overlooked the corresponding reverse lookup zone configurations. The above ip address , 164.78.252.49 , is corresponding to many domain names, it is probably a web server that hosts for virtual hosts. Some of the domain name may be obsoleted.]

1. Setting up Forward Lookup Zone

In this exercise, we are setting up a local domain at our own local DNS for internal usage.

With forward lookup zone configuration, DNS queries that associate with the defined domain will be answered immediately by the DNS server.

On server:

1. You are going to make your DNS Server responsible for the zone (domain) "las.org".

Before we proceed, we do an initial checking of the las.org, type:

dig las.org

To verify if las.org has been registered by someone.

Text

Description automatically generated

As shown, las.org domain is resolved to the IP of 40.84.33.106.

At below, we will define las.org to be our own domain.

1. Edit /etc/named.conf and declare your zone. Add the following lines in bold.

zone "." IN {

type hint;

file "named.ca";

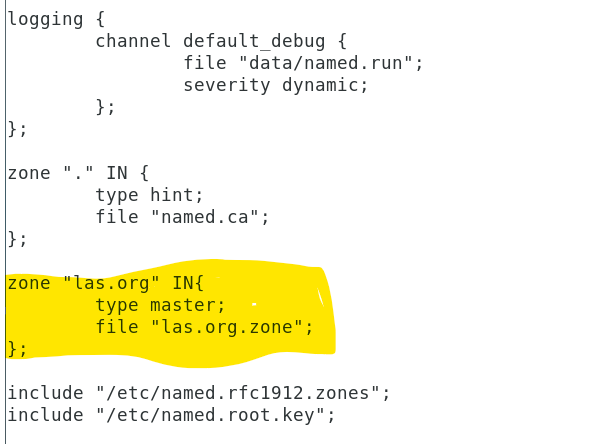
};

**zone "las.org" IN {**

**type master;**

**file "las.org.zone";**

**};**



1. Zone files are stored in /var/named. Create a new file /var/named/las.org.zone with the following content:

Table

Description automatically generated

designates the start of this zone file in the namespace

Here are more details:

Change this to your server’s hostname (you can leave out the domain part of las.org.)

$ORIGIN las.org.

$TTL 86400

las.org. IN SOA server root.server.las.org. (

42 ; serial

3H ; refresh

The administrator's email address. It is equivalent of root@server.las.org.

15M ; retry

1W ; expiry

1D ) ; minimum

IPv4 address of the domain las.org

las.org. IN NS server

las.org. IN A 192.168.30.88

Change these to the IP addresses of your server and client

Change this to your client’s hostname

server IN A 192.168.30.88

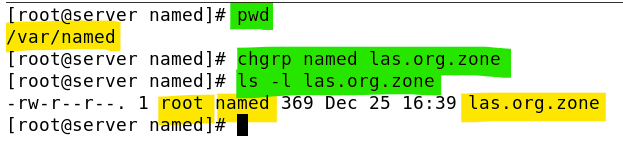
client IN A 192.168.30.129

This is a fictitious PC

testpc IN A 192.168.30.111

1. Change the group owner of /var/named/las.org.zone to "named".

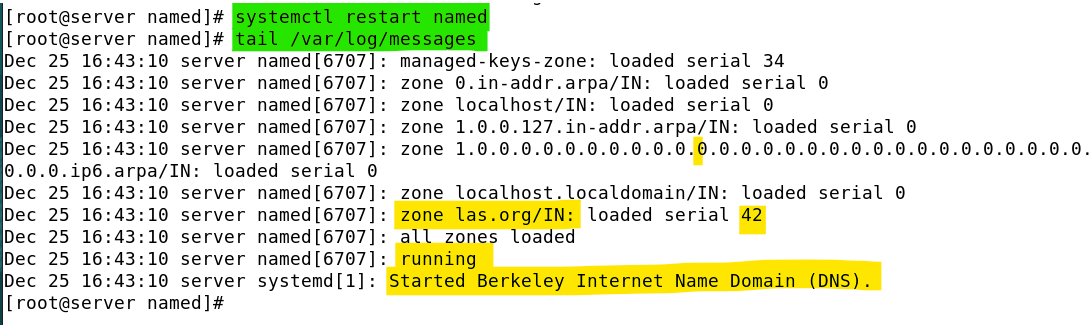
chgrp named /var/named/las.org.zone



1. Restart the named service.

systemctl restart named

1. Check /var/log/messages if there are any errors with your named service.



On Client and Server:

1. Perform a DNS query for server, client and testpc.

Dig las.org

dig server.las.org

host –a server.las.org

dig client.las.org

dig testpc.las.org

Note: You will see the query result is an Authoritative answer.

Graphical user interface, text, application

Description automatically generated

1. Setting up Reverse Lookup Zone

Reverse Lookup Zone provides the data to answer the possible DNS reverse lookup. For reverse lookup, the query will seek for the host/domain name of a given IP address. Domain owner may define proper reverse lookup entries in the reverse lookup zone file selectively.

On server:

1. Edit /etc/named.conf and declare your reverse lookup zone.

zone "." IN {

type hint;

file "named.ca";

};

zone "las.org" IN {

type master;

file "las.org.zone";

Change to the first three reverse octets of your subnet

};

**zone "30.168.192.in-addr.arpa" IN {**

**type master;**

**file "192.168.30.zone";**

**};**

Change to your subnet

Text, letter

Description automatically generated

1. Zone files are stored in /var/named. Create a new reverse zone file /var/named/192.168.30.zone (the actual file name should be based on your own subnet) and add the following content.

You are declaring a zone with three pointer records f or your server, your client and one more for the IP address "192.168.30.111". Note the dot-terminated hostnames.

$TTL 86400

@ IN SOA server.las.org. root.server.las.org. (

42 ; serial

28800 ; refresh

14400 ; retry

3600000 ; expiry

Change these to the last octet of your server and client

86400) ; minimum

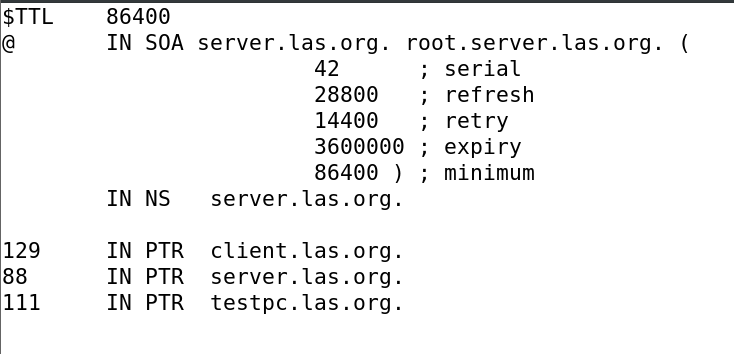
IN NS server.las.org.

129 IN PTR client.las.org.

Need to provide FQDN

88 IN PTR server.las.org.

111 IN PTR testpc.las.org.



1. Change the group owner of the reverse zone file to "named".
2. Restart the named service.
3. Perform reverse DNS queries for your fictitious, client and server pc from both of your Client and Server.

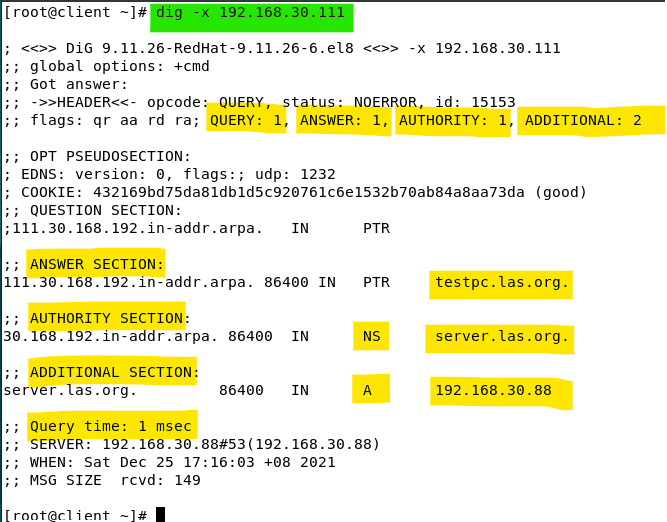
dig –x 192.168.30.111

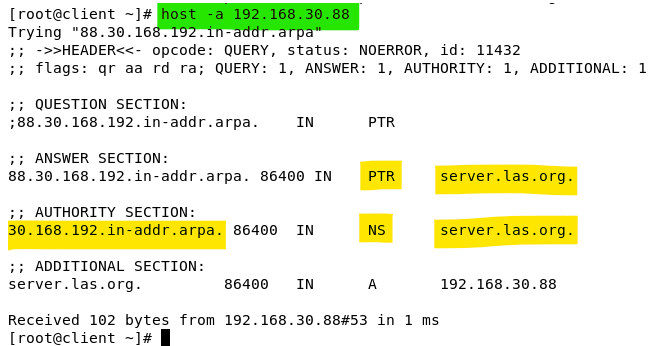
host –a 192.168.30.88

dig –x 192.168.30.129

Change these to the IP addresses of your pcs.

dig –x 192.168.30.129





1. Perform a Zone transfer

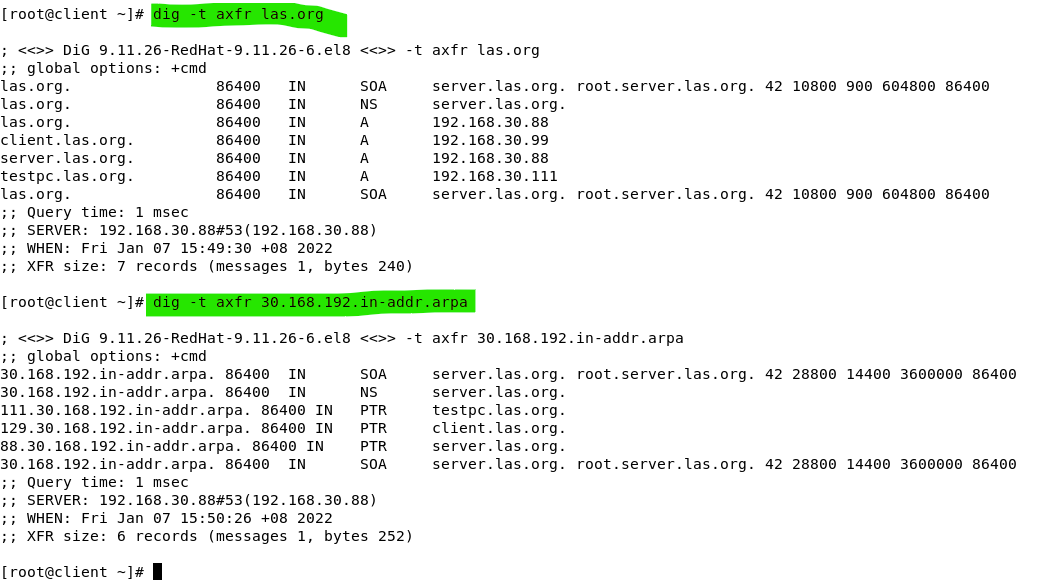
Zone transfer allows the requester to copy the entire zone file from a DNS server. Zone transfer operation is usually completed by using TCP port 53. (Normal DNS query is completed via the default UDP port 53).

On client:

1. Run the following commands to do a couple of zone transfers (a complete dump of the all the zone content) of the las.org domain from your DNS Server. You will see a list of the hosts and their IP addresses.

dig -t axfr las.org

dig –t axfr 30.168.192.in-addr.arpa



On server:

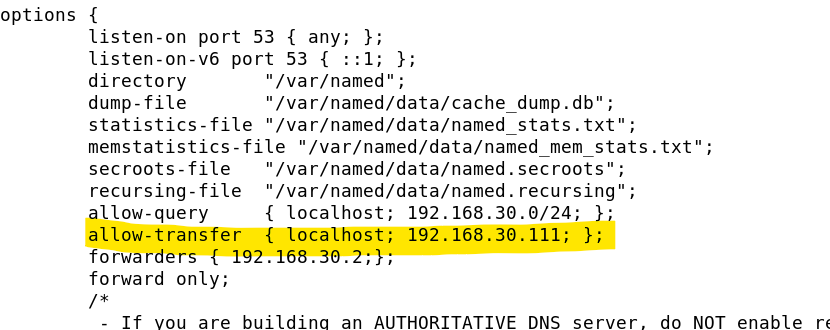
You will now restrict the systems that can do a zone transfer from your server.

1. Edit /etc/named.conf and add a line to specify allow-transfer only from localhost.

allow-query { localhost; 192.168.30.0/24; };

**allow-transfer { localhost; 192.168.30.111; };**

Change to an IP address that is not your client

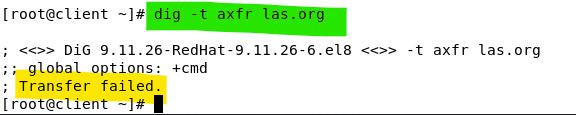
****

1. Reload or Restart the DNS service.

systemctl reload named

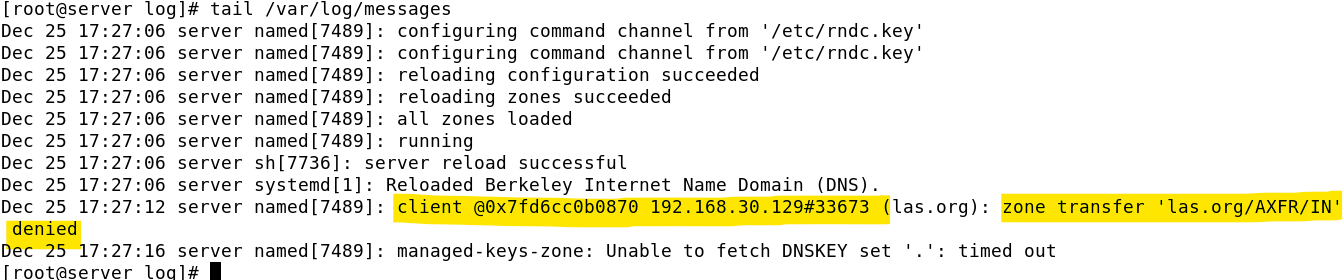
On client:

1. Try to do a zone transfer of the example.com domain from your DNS Server again. This time, it should not be successful.



On server:

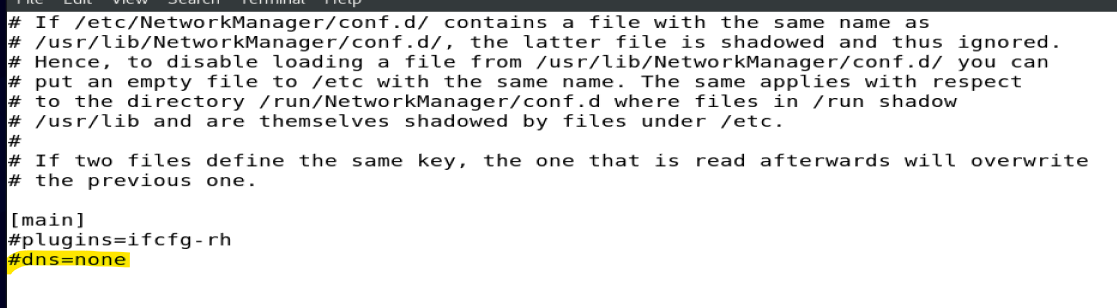
1. Check the log file /var/log/messages to see the logged entries for the successful and unsuccessful zone transfers (do a search for AXFR).



1. Reset and restore /etc/resolv.conf

On both server and client:

1. Ensure the dns=none entry is not set in the /etc/NetworkManager/NetworkManager.conf.



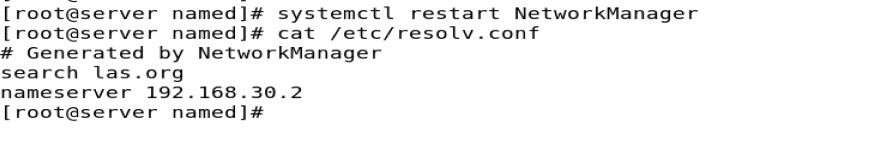
1. Restart the NetworkManager, it will reset the resolv.conf.

systemctl restart NetworkManager

1. Verify the contents of /etc/resolv.conf so that it points back to the original DNS Server.

nameserver 192.168.30.2

This IP address should be updated accordingly.



On server:

1. Disable and Stop the DNS service

systemctl disable named

systemctl stop named

Additional Reference:

* https://en.wikipedia.org/wiki/Zone\_file#Example\_file
* https://www.infoblox.com/dns-security-resource-center/dns-security-faq/is-dns-tcp-or-udp-port-53/

*~End of Practical~*