This guide will guide you through the setup of DNSMasq in order to achieve the following:  
- When the Zimbra server performs a DNS query for the A record of the Public Service Hostname of one of the hosted domains, answer with the LAN IP of the server itself.  
- When the Zimbra server performs a DNS query for the MX record of one of the hosted domains, answer with the LAN IP of the server itself.  
- When the Zimbra server performs any other DNS query, let another DNS server manage it.  
- Let DNSMasq only bind to the interface it's using so that other DNS servers can be ran on the server is needed.   
  
**Why DNSMasq instead of BIND?**One word: SIMPLICITY.  
BIND is a full-fledged DNS server that can perform the roles of both an Authoritative and a Recursive nameserver, but chances are that you don't need this, as you probably already have an authoritative server for your domain - for example the one of your domain Registrar or a local Active Directory server - and one or more Recursive nameservers either internal, provided by your ISP or by a dedicated DNS service such as OpenDNS. So why using it when DNSMasq, a lightweight DNS forwarder, can let you achieve a Split DNS situation in a much easier way?  
  
**Our Example Environment:**  
192.168.0.2 is the LAN ip of your server  
mail.domain.com is the hostname of the server  
domain.com is the main mail domain  
domain2.com is an additional mail domain   
8.8.8.8 and 8.8.4.4 are the DNS servers you want to use (in this case, Google's public DNS servers)  
  
**Config Files:**  
/etc/resolv.conf

Code:

nameserver 192.168.0.2

In most Unix-like operating systems and others that implement the BIND Domain Name System (DNS) resolver library, the resolv.conf configuration file contains information that determines the operational parameters of the DNS resolver. The DNS resolver allows applications running in the operating system to translate human-friendly domain names into the numeric IP addresses that are required for access to resources on the local area network or the Internet. The process of determining IP addresses from domain names is called resolving.

DNSMasq will bind on the local address to answer DNS queries.  
  
/etc/resolv.dnsmasq

Code:

nameserver 8.8.8.8

nameserver 8.8.4.4

We'll instruct DNSMasq to answer just some queries and in the way we want, while all other queries will be forwarded to this servers. We create /etc/resolv.dnsmasq and the name of this file is matched with the name in dnsmasq.conf file

/etc/dnsmasq.conf (the file is quite large, I'll only write the config elements relevant to this guide)

Code:

address=/mail.domain.com/192.168.0.2

resolv-file=/etc/resolv.dnsmasq

except-interface=lo

listen-address=192.168.0.2

bind-interfaces

This sets up DNSMasq to listen on the local IP address and to only bind on the interface it's listening on. Also, it forces to answer any A-record DNS requests for mail.domain.com with the LAN ip. This is a "naive" trick that allows you to provisionally use the same hostname on two servers without any issues of sort.  
  
In the same file, add one line like the following for each domain on your server:

Code:

mx-host=domain.com,mail.domain.com,10

This lines instruct DNSMasq to always return "mail.domain.com" as the MX record for your domains which, if your /etc/hosts file is correctly configured, will always point to the local server (DNSMasq will then forward any other request to the DNS servers in the resolv.dnsmasq file).  
  
  
**Service Restart and check:**  
Restart DNSMasq with

Code:

/etc/init.d/dnsmasq restart

and check that

Code:

dig mx domain.com

returns the local hostname/address.  
  
Also, make sure that the server can correctly resolve any other IP through the servers specified in /etc/resolv.dnsmasq  
  
**Additional dnsmasq.conf options:**- To specify an Authoritative server for a domain:

Code:

server=/domain.com/10.0.0.1

with 10.0.0.1 being the IP of the Authoritative DNS for domain.com  
  
- To specify a Reverse DNS resolution (PTR Record) for a domain:

Code:

server=/192.168.in-addr.arpa/192.168.100.1

- Log all the DNS queries (for debug purpouse)

Code:

log-queries

- Locally return an SPF record for a domain

Code:

txt-record=zextras.com,"v=spf1 mx -all"