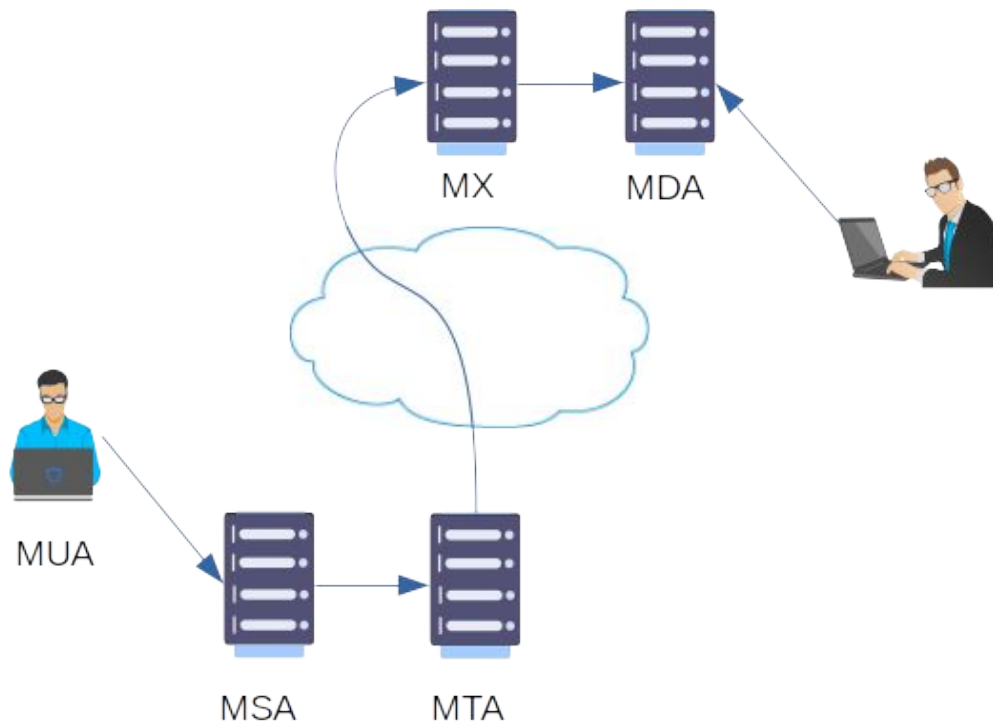




The DNS MX Record: how your mail finds its target

The email journey to the recipient

In a previous article, we have represented the email journey.



And we have defined the **MX**: Mail eXchange as the destination MTA.

The question we will answer now is: how does the mail transfer agent find the destination (MX)?

The DNS MX record

In a precedent article, we have also described a part of the DNS system, namely the translation of a machine or application into an IP address, and the hierarchy of domain names and subdomains.

But DNS can distribute other information pertaining to a domain name. Each type of attribute DNS can contain is characterized by a *DNS record type*. These records are stored in the DNS server designated for the domain.

One of the DNS record types is the MX record. It specifies the name of a mail server responsible for accepting email messages on behalf of a domain name. There can be several MX records for a domain as there can be several mail servers (several servers in a cluster or main and backup servers).

The syntax of a DNS MX record is the following:

`<domain> <TTL> <class> <type> <priority> <hostname>`

Example:

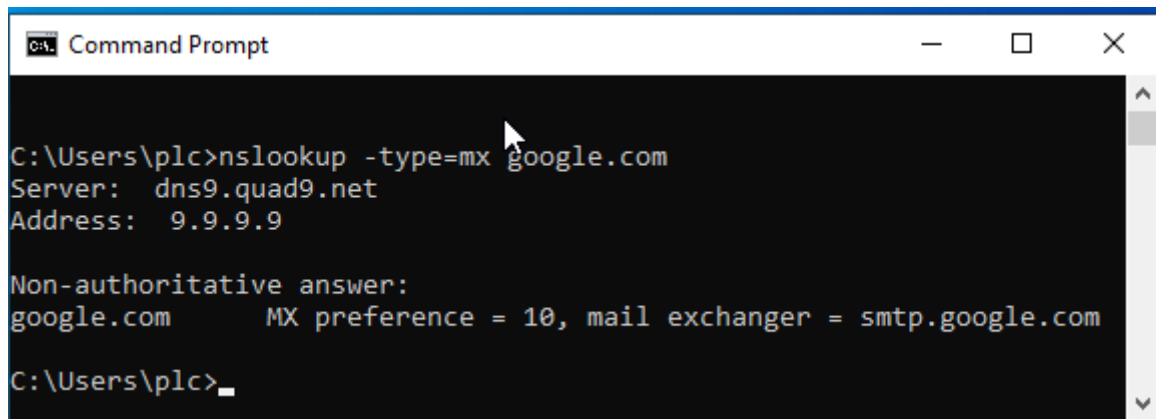
`google.com. 300 IN MX 10 smtp.google.com`

- `<domain>` is the domain name for which the server is the mail server. All mails targeted at `<user>@google.com` will land on this server.
- `<TTL>` is the time to live of the distributed information. Every machine who has queried the MX record for the domain can keep the information cached locally for this number of seconds. Afterwards, it has to re-query DNS again.
- `<class>` is the kind of network this record is relevant for. For the moment, there is only one class defined: IN (=Internet).
- `<type>` is the record type; in our present case it is a MX record.
- `<priority>` is a number indicating the preference where the mails must be sent to. The lowest the number, the highest the preference. For example, if a domain has 2 mail exchangers, one with a priority of 10 and the other one with a priority of 20, the mail sender will first try to send the email to the first one (priority 10), and if it fails then to the second one (priority 20).
- `<hostname>` is the name of the mail server for the domain.

This is how a mail agent can find where it has to send an email to `somebody@google.com`: the destination machine is in the MX record.

How to find the MX record for a domain

- On Windows, the utility to query DNS is nslookup.
The command to query a MX record is: `nslookup -type=mx <domain>`



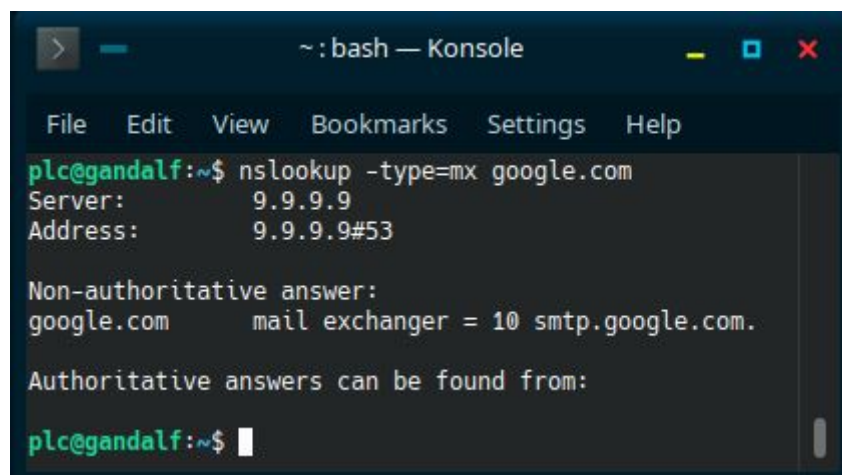
```
Command Prompt

C:\Users\plc>nslookup -type=mx google.com
Server:  dns9.quad9.net
Address:  9.9.9.9

Non-authoritative answer:
google.com      MX preference = 10, mail exchanger = smtp.google.com

C:\Users\plc>
```

- On Linux:
 - The same nslookup command can also be used



```
~: bash — Konsole

File Edit View Bookmarks Settings Help

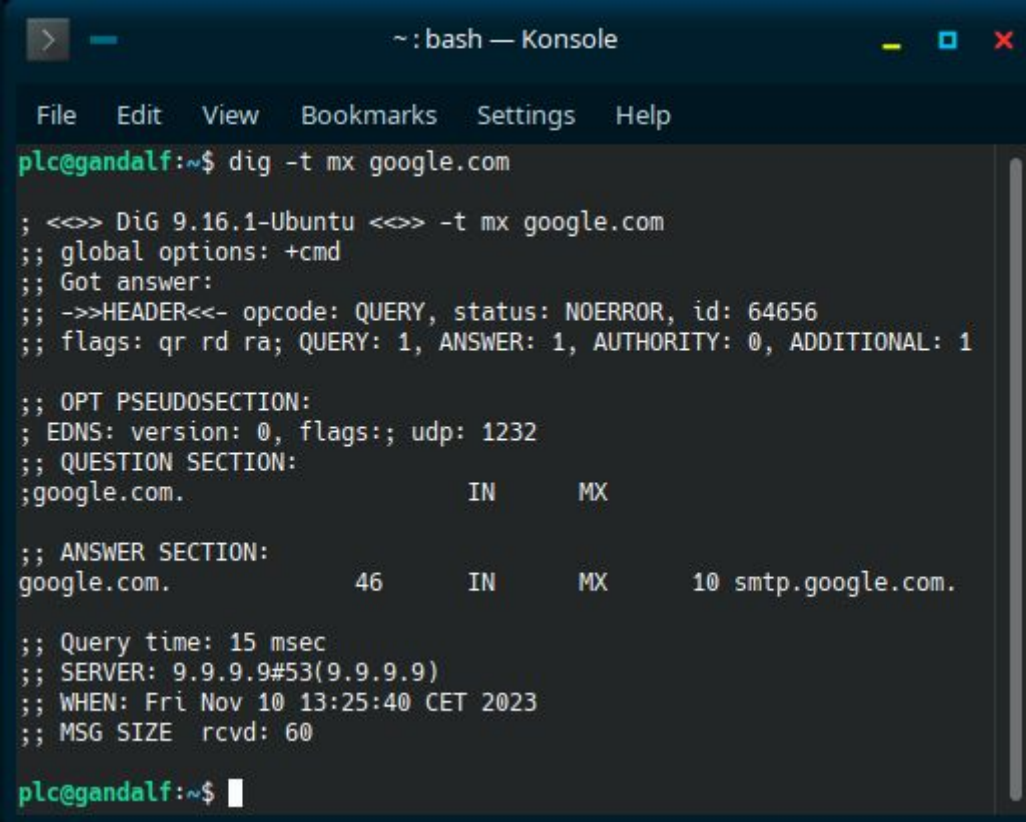
plc@gandalf:~$ nslookup -type=mx google.com
Server:      9.9.9.9
Address:     9.9.9.9#53

Non-authoritative answer:
google.com   mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:

plc@gandalf:~$
```

- A more modern and versatile utility is `dig`.
The command is: `dig -t mx <domain>`



```
> ~: bash — Konsole
File Edit View Bookmarks Settings Help
plc@gandalf:~$ dig -t mx google.com

; <<>> DiG 9.16.1-Ubuntu <<>> -t mx google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64656
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

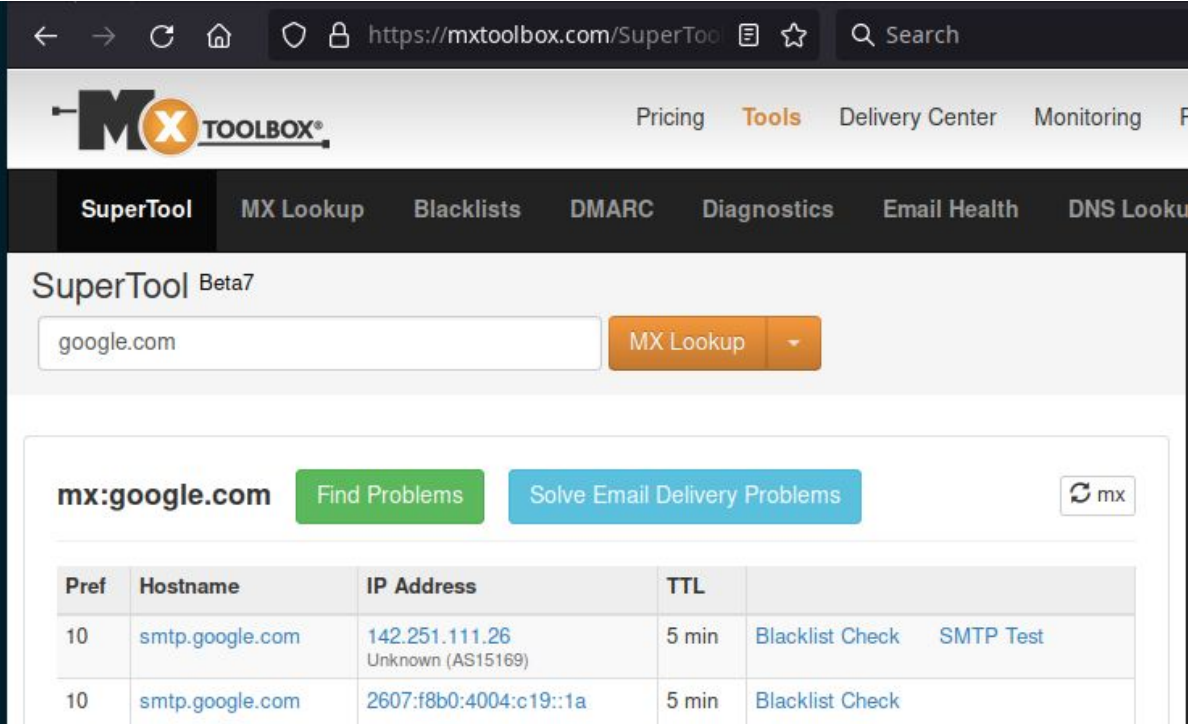
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;google.com.                IN      MX

;; ANSWER SECTION:
google.com.                46      IN      MX      10 smtp.google.com.

;; Query time: 15 msec
;; SERVER: 9.9.9.9#53(9.9.9.9)
;; WHEN: Fri Nov 10 13:25:40 CET 2023
;; MSG SIZE rcvd: 60

plc@gandalf:~$
```

- On the web, there are several sites available to display MX records:
 - <https://mxtoolbox.com/>



The screenshot shows the MX Toolbox SuperTool interface. The browser address bar displays <https://mxtoolbox.com/SuperTool>. The page features a navigation bar with links: Pricing, Tools, Delivery Center, Monitoring, and F. Below this, a secondary navigation bar includes SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, and DNS Lookup. The main content area is titled "SuperTool Beta7" and contains a search input field with "google.com" and an "MX Lookup" button. Below the search field, there are two buttons: "Find Problems" and "Solve Email Delivery Problems", along with a "mx" icon. A table displays the MX records for google.com:

Pref	Hostname	IP Address	TTL	
10	smtp.google.com	142.251.111.26 Unknown (AS15169)	5 min	Blacklist Check SMTP Test
10	smtp.google.com	2607:f8b0:4004:c19::1a	5 min	Blacklist Check

- <https://dnschecker.org/mx-lookup.php>

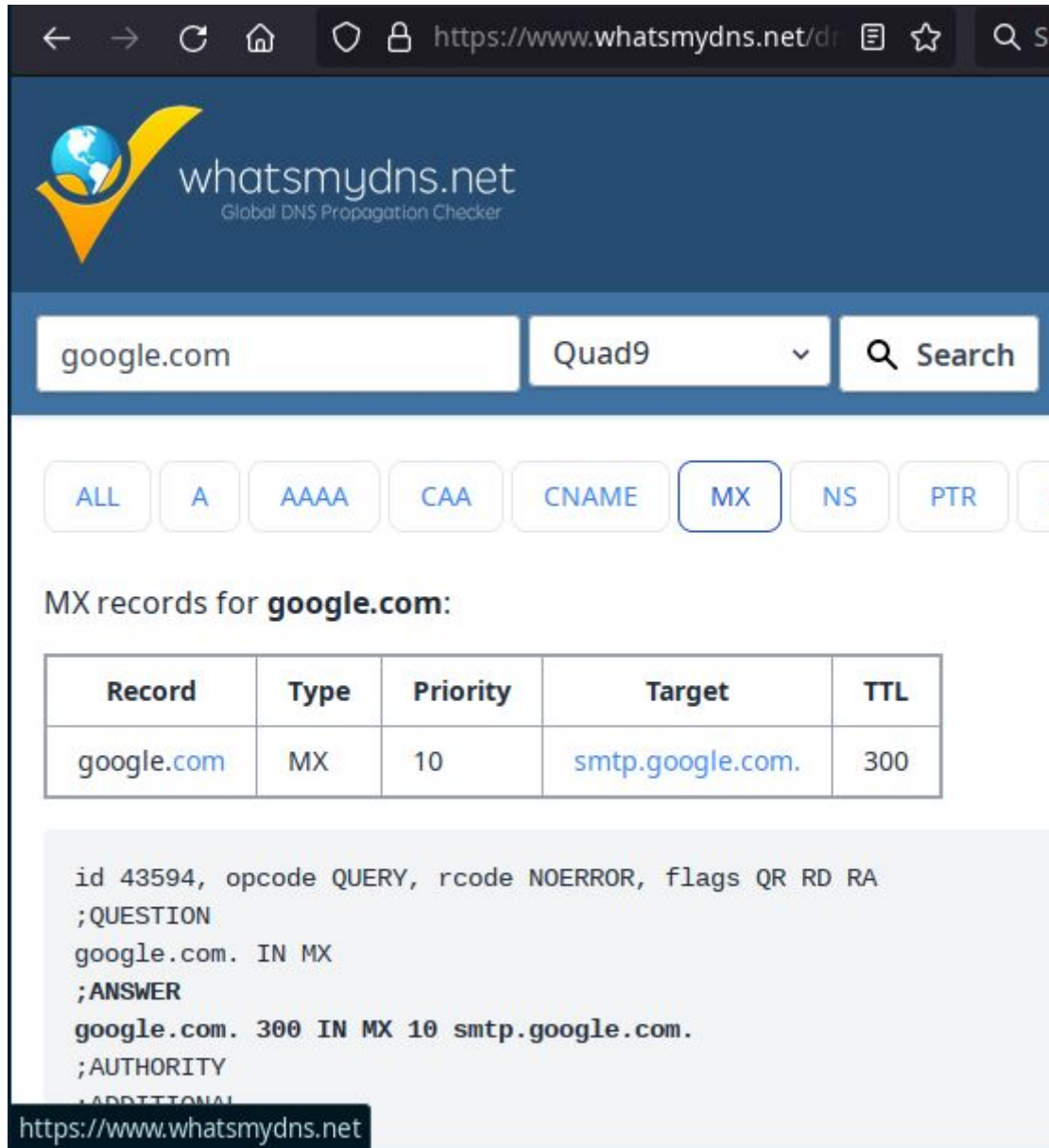
The screenshot shows the DNSChecker website interface. The top navigation bar includes a search bar and various icons. The main heading is "MX Lookup". Below it, there are two input fields: "Enter Domain to Check MX Records:" with "google.com" entered, and "DNS Server:" with "Quad9" selected. A blue button labeled "Check MX Record" is positioned below the domain field. Underneath, there are links for "Related tools": "DMARC Validation", "SPF Validation", and "MX Validation".

The second part of the screenshot shows the results for "GOOGLE.COM". A blue button labeled "Download Records" is in the top right. The main heading is "smtp.google.com.". Below this, there is a table of MX record details:

Mx Record	smtp.google.com.
IP	172.253.63.27 Check IP Blacklist Owner: Google LLC WHOIS AS15169
Status	Success
Test duration(ms)	7
AS Number	AS15169
Organization	Google LLC
Domain	google.com
Country	United States
Abuse Contact	Network: 172.253.0.0/16 Name: Abuse Email: network-abuse@google.com Phone: +1-650-253-0000 Address: US, CA, Mountain View, 1600 Amphitheatre Parkway, 94043 Country: US

At the bottom right, it says "IP Location Services by: [IPInfo.io](#)".

- <https://www.whatsmydns.net/dns-lookup/mx-records>



The screenshot shows the website **whatsmydns.net** with the tagline "Global DNS Propagation Checker". The search bar contains "google.com" and the dropdown menu is set to "Quad9". The "MX" record type is selected. Below the search bar, a table displays the MX records for google.com. The table has five columns: Record, Type, Priority, Target, and TTL. The record shown is for google.com with Type MX, Priority 10, Target smtp.google.com., and TTL 300. Below the table, the DNS query details are shown in a light gray box, including the query ID, opcode, rcode, flags, and the query itself.

MX records for **google.com**:

Record	Type	Priority	Target	TTL
google.com	MX	10	smtp.google.com.	300

```
id 43594, opcode QUERY, rcode NOERROR, flags QR RD RA
;QUESTION
google.com. IN MX
;ANSWER
google.com. 300 IN MX 10 smtp.google.com.
;AUTHORITY
;ADDITIONAL
```