

Troubleshooting DNS issues

Check the DNS resolution by verifying if a domain name resolves correctly:

```
dig exampl e.com
```

Ensure the domain's name servers are correctly configured:

```
dig exampl e.com NS
```

Identify where DNS resolution might be failing by tracing the entire DNS lookup path:

```
dig exampl e.com +trace
```

Verify the DNSSEC settings to see if the RRSIG records are present:

```
dig exampl e.com +dnssec
```

Make sure that an IP address resolves to the correct domain name:

```
dig -x 93.184.216.34
```

To fix specific services like email, check the relevant DNS records. For example:

```
dig exampl e.com MX
```

Pay attention to each output and make sure the ANSWER sections are correct.

Monitoring DNS propagation

Use the @server option to query a specific DNS server, such as Google's public DNS server:

```
dig @8.8.8.8 exampl e.com
```

Query different DNS servers to compare their responses. For Cloudflare's server, run:

```
dig @1.1.1.1 exampl e.com
```

If the ANSWER sections from different servers match, the DNS changes have propagated successfully. Otherwise, some servers may still need to update their records. You can check the propagation status periodically.

Performance testing

Measuring DNS response times is essential for assessing your DNS servers' performance. This lets you identify slowdowns or issues affecting your network's speed and reliability.

Run the basic **dig** command. Focus on the output's **Query time** field, which indicates the time taken to get a DNS server response:

```
dig exampl e.com
```

Query different DNS servers to compare their response times. This helps identify which servers are performing better:

```
dig @1.1.1.1 exampl e.com
```

```
dig @8.8.8.8 exampl e.com
```

Use the **+stats** option for additional statistics about query times and server details:

```
dig exampl e.com +stats
```

Examples	List specific resource record types		Output sections	
	Base Syntax	<code>dig www.go ogl e.com type</code>	HEADER	dig command version, options used, type of operation, status of the operation, message id.
Syntax	Authority Record	<code>dig www.go ogl e.com SOA</code>		
<code>dig [server] [name] [type]</code>	IPv4 address(-es)	<code>dig www.go ogl e.com A</code>	QUESTION	This is your input - the query you sent to the DNS.
dig command options	IPv6 address(-es)	<code>dig www.go ogl e.com AAAA</code>	ANSWER	Column 2: TTL (cache time) in seconds; Column 3: Class (IN=Internet, CH=Chaos, HS=Hesiod); Column 4: Resource Record Type (A, NS, CNAME, MX, PTR...); Column 5: The content of the resource record (IP, Name, Text...)
+short	Canonical Records	<code>dig www.go ogl e.com CNAME</code>		
+noall	Mail eXchangers	<code>dig google.com MX</code>		
+answer	Standard Reverse Lookup	<code>dig 2.69.2 19.9 1.i n- ad d - r.arpa PTR</code>	AUTHORITY	The DNS servers that have the authority to answer the query (in form of NS records).
+trace	Simple Reverse Lookup	<code>dig -x www.go ogl e.com</code>	ADDITIONAL	This section carries resource records that are attached to help you avoid additional queries or even bootstrap certain zones (Glue records).
@server	Caveat: If you forget to configure MX records for an object, most mail servers will try to deliver messages to the A record associated to the host.			
-x				
+multi				
+nocmd				
+stats				
	Response Codes			
	0 NOERR	No error		
	1 FORMERR	Unable to understand query		
	2 SERVFAIL	Server problem		
	3 NXDOMAIN	Domain does not exist		
	4 NOTIMPL	Query not implemented		
	5 REFUSED	Query not allowed		
	If the verification of a DNSSEC signed answer fails, this also results in SERVFAIL			

