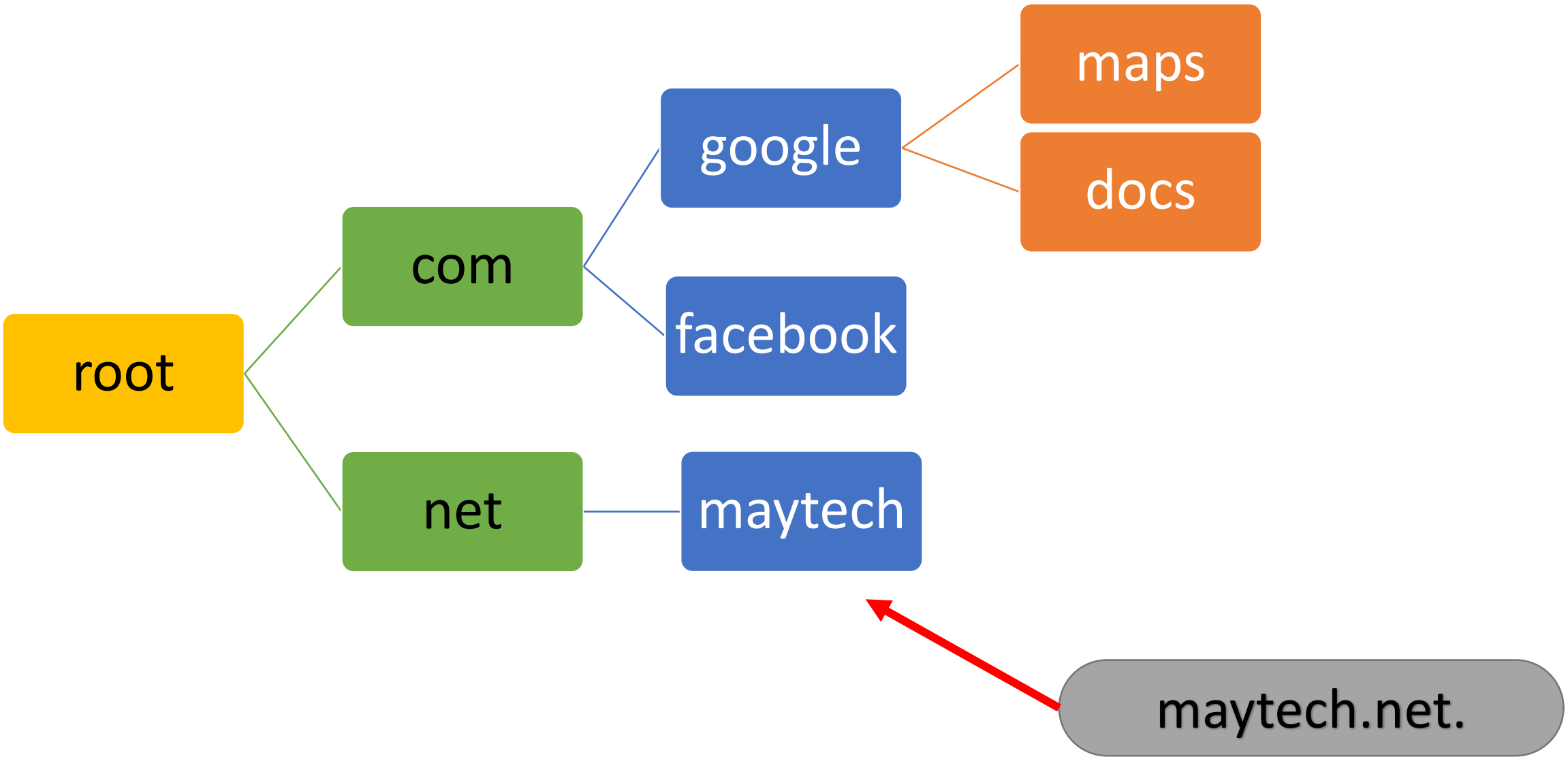
What Is a DNS And How Does It Work???

The Domain Name System is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network

DNS Hierarchy

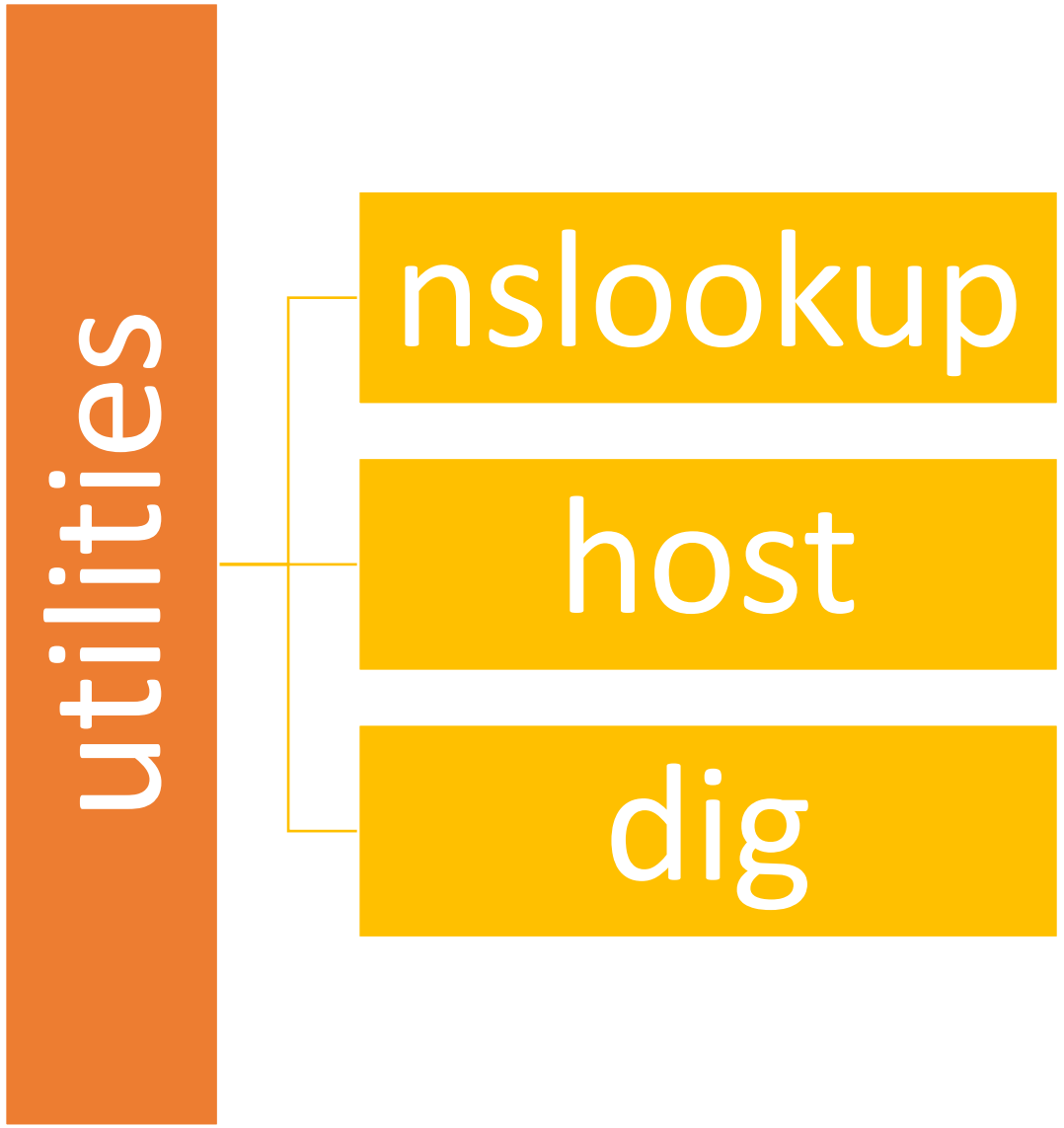


46.16.167.160

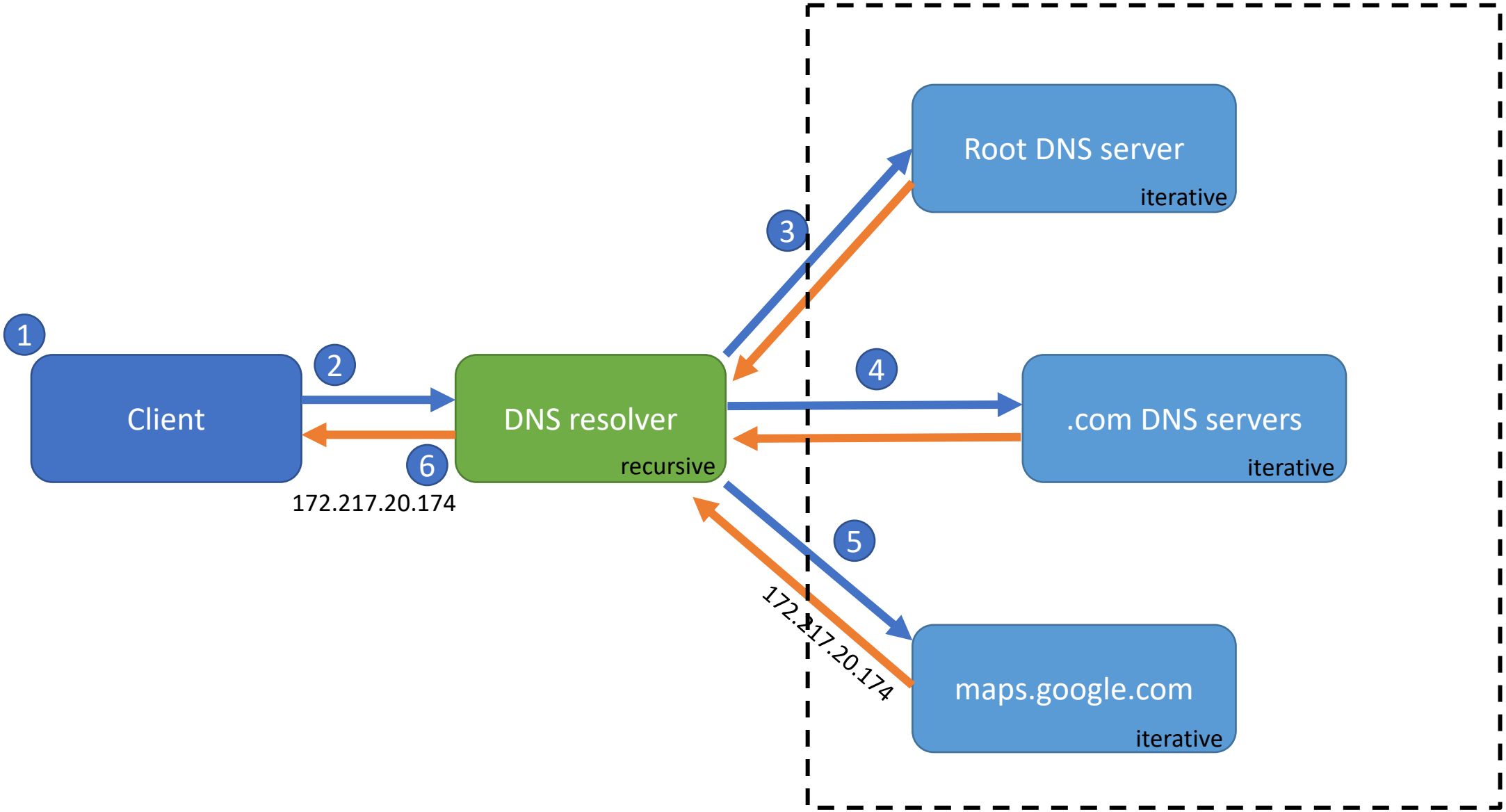
maytech.net

Configure network infrastructure

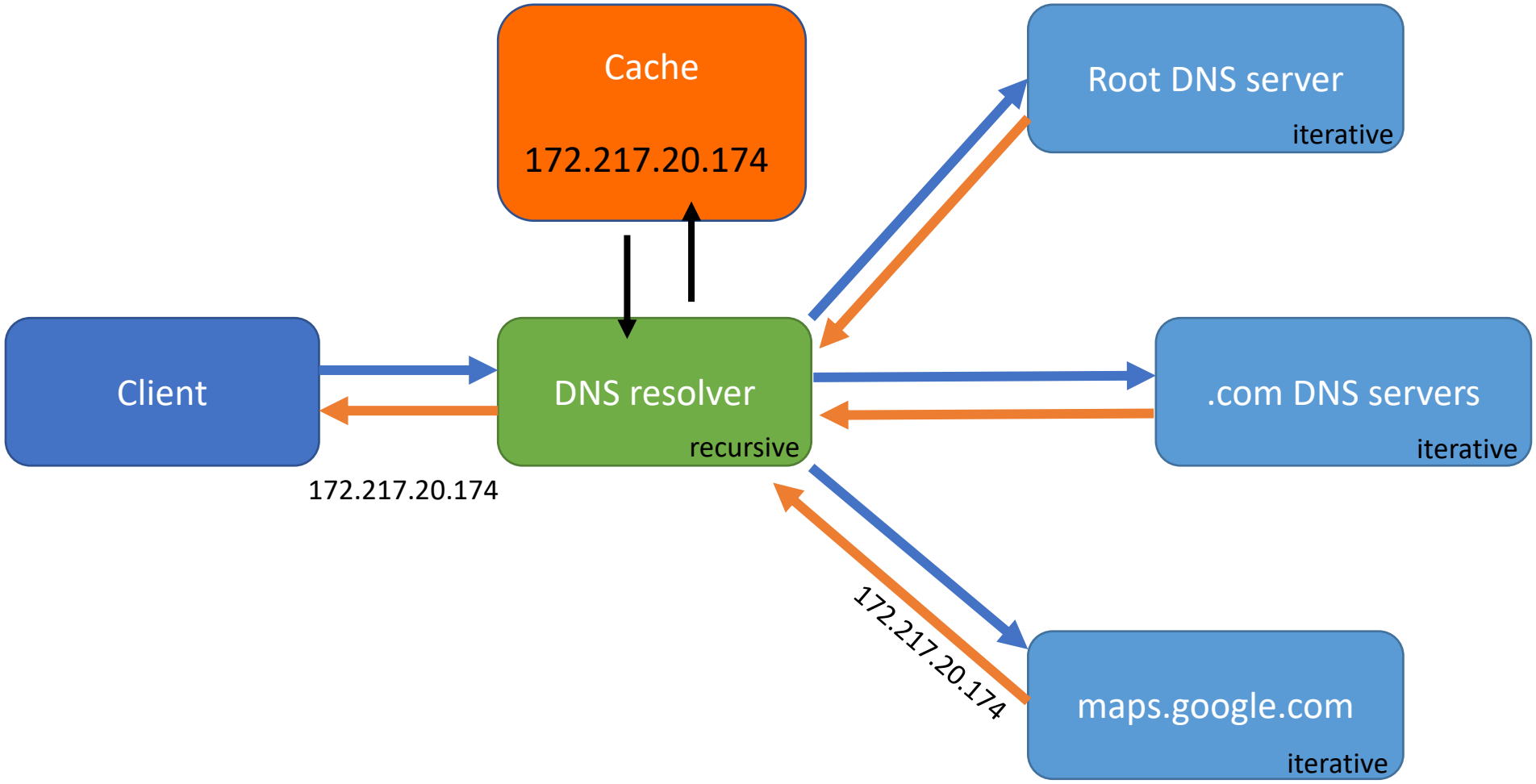
For what?


utilities
nslookup
host
dig

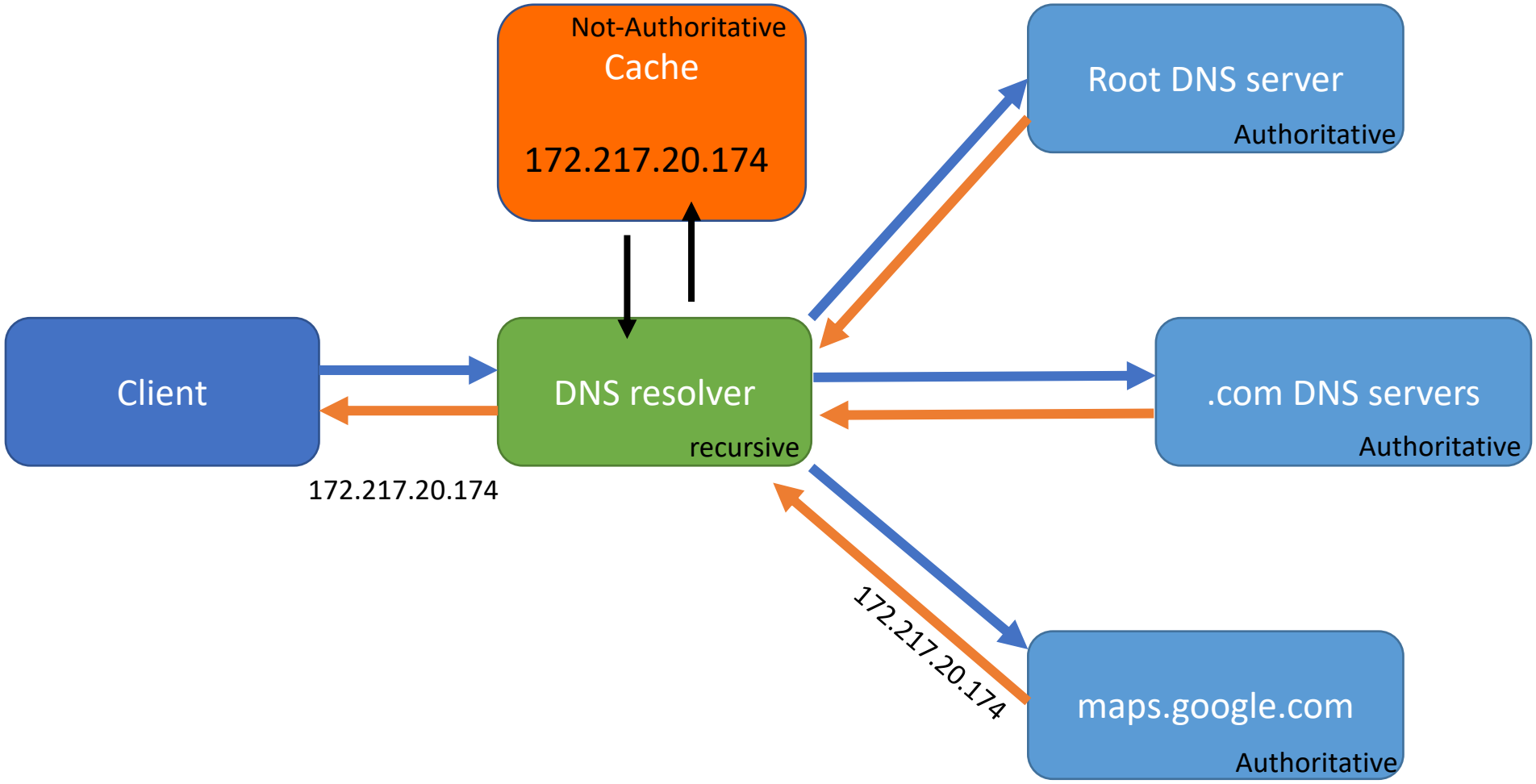
DNS infrastructure

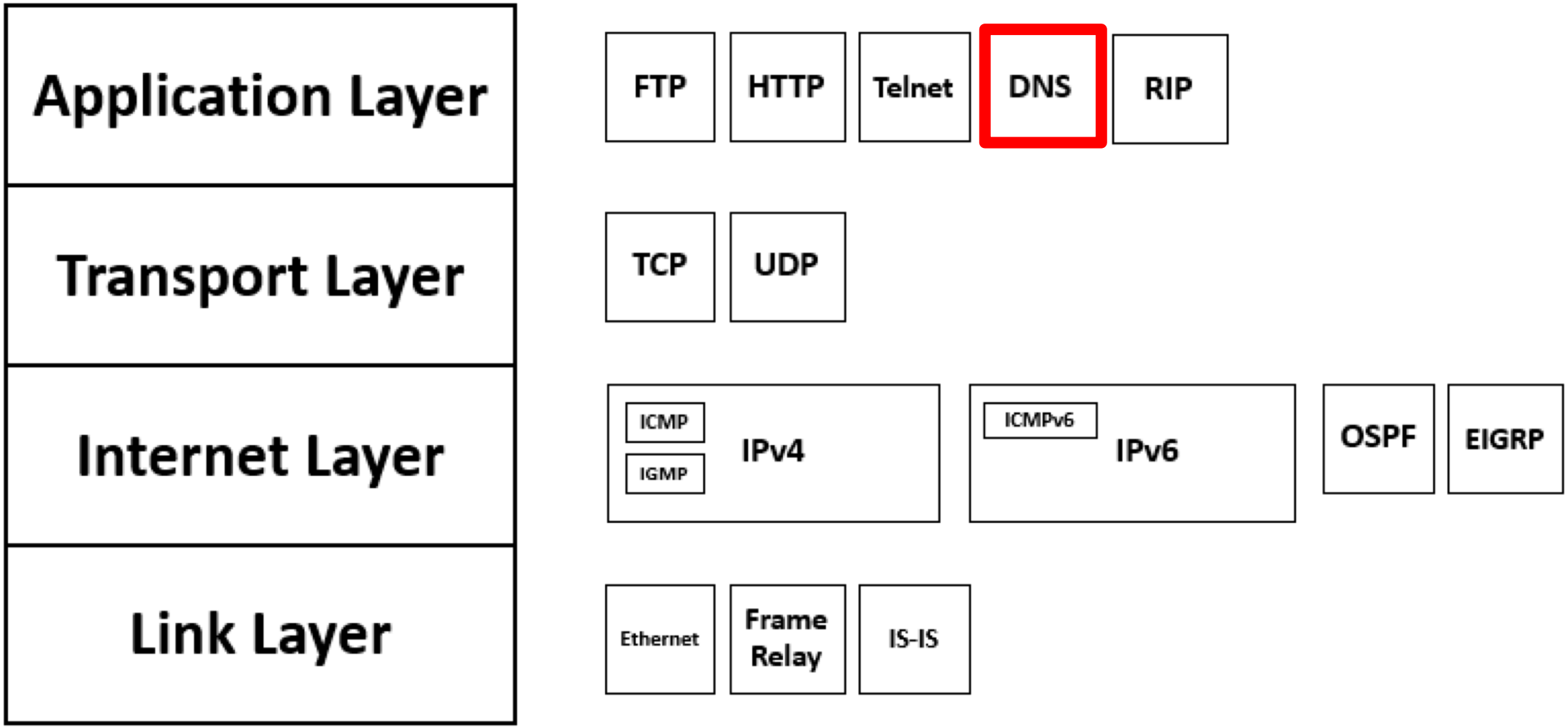


DNS resolver: cache



Authoritative response




Application Layer
Transport Layer
Internet Layer
Link Layer
FTP
HTTP
Telnet
DNS
RIP
TCP
UDP
ICMP
IGMP
IPv4
ICMPv6
IPv6
OSPF
EIGRP
Ethernet
Frame Relay
IS-IS

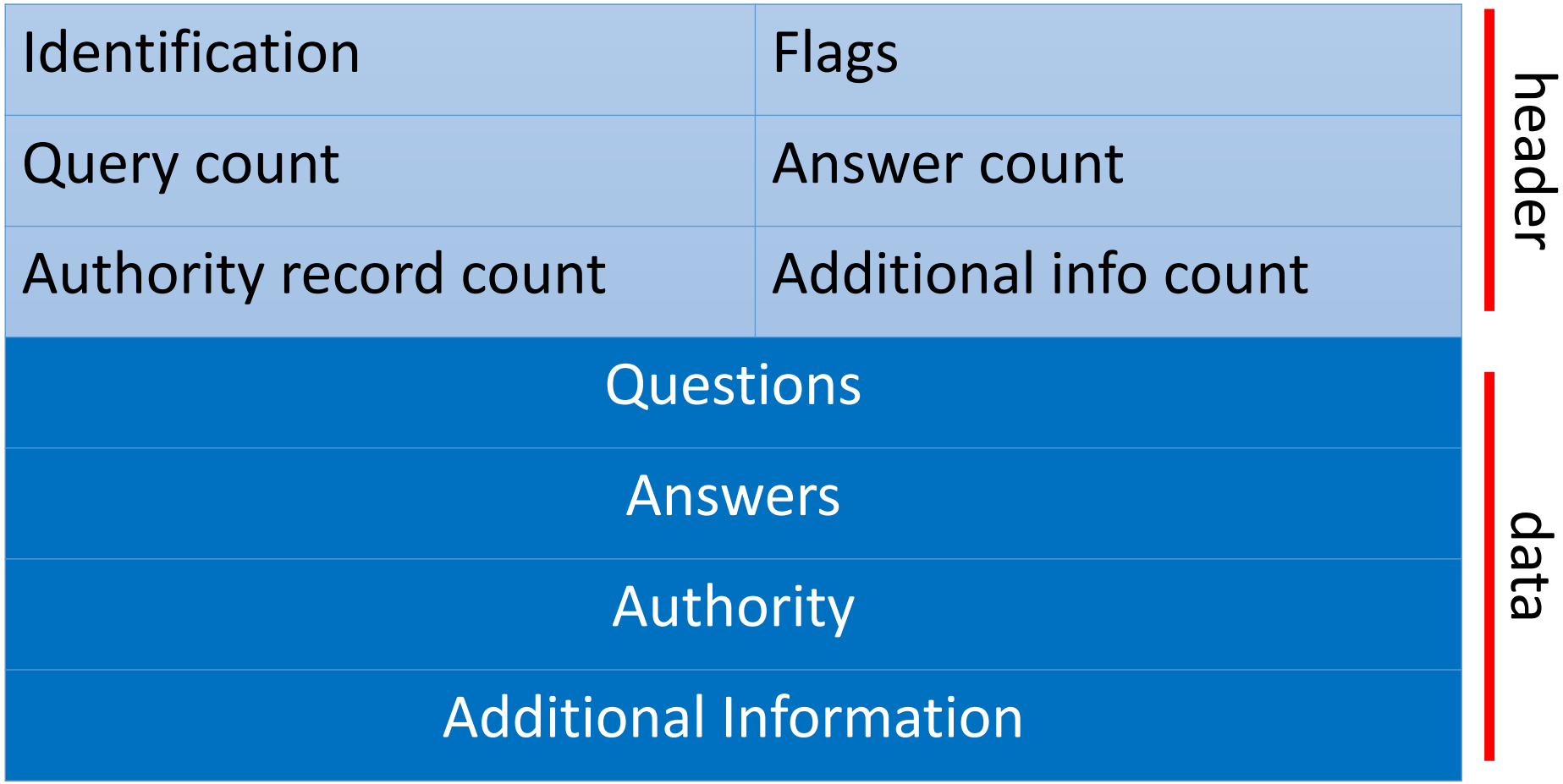
DNS protocol

UDP protocol

port 53

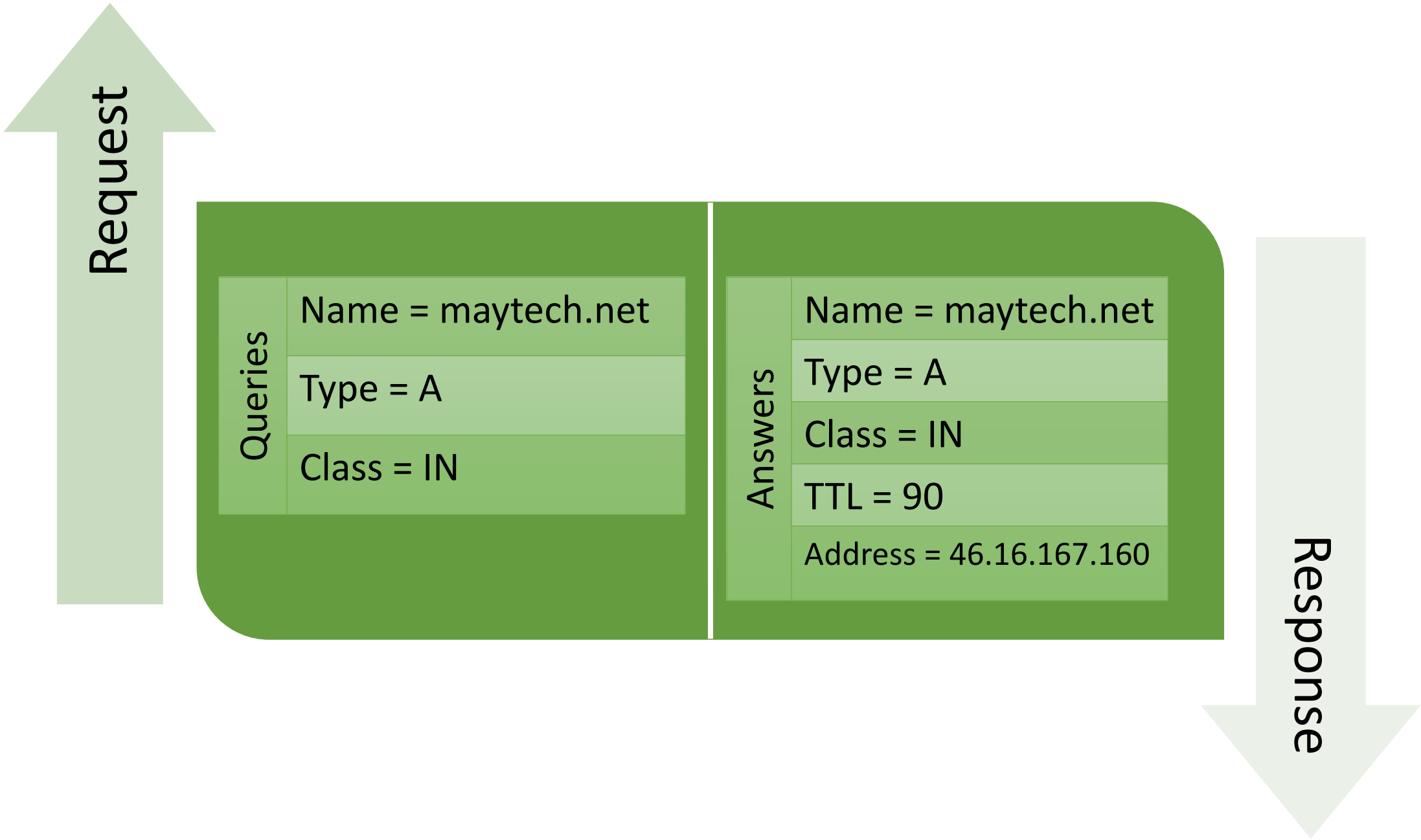
Client – server model

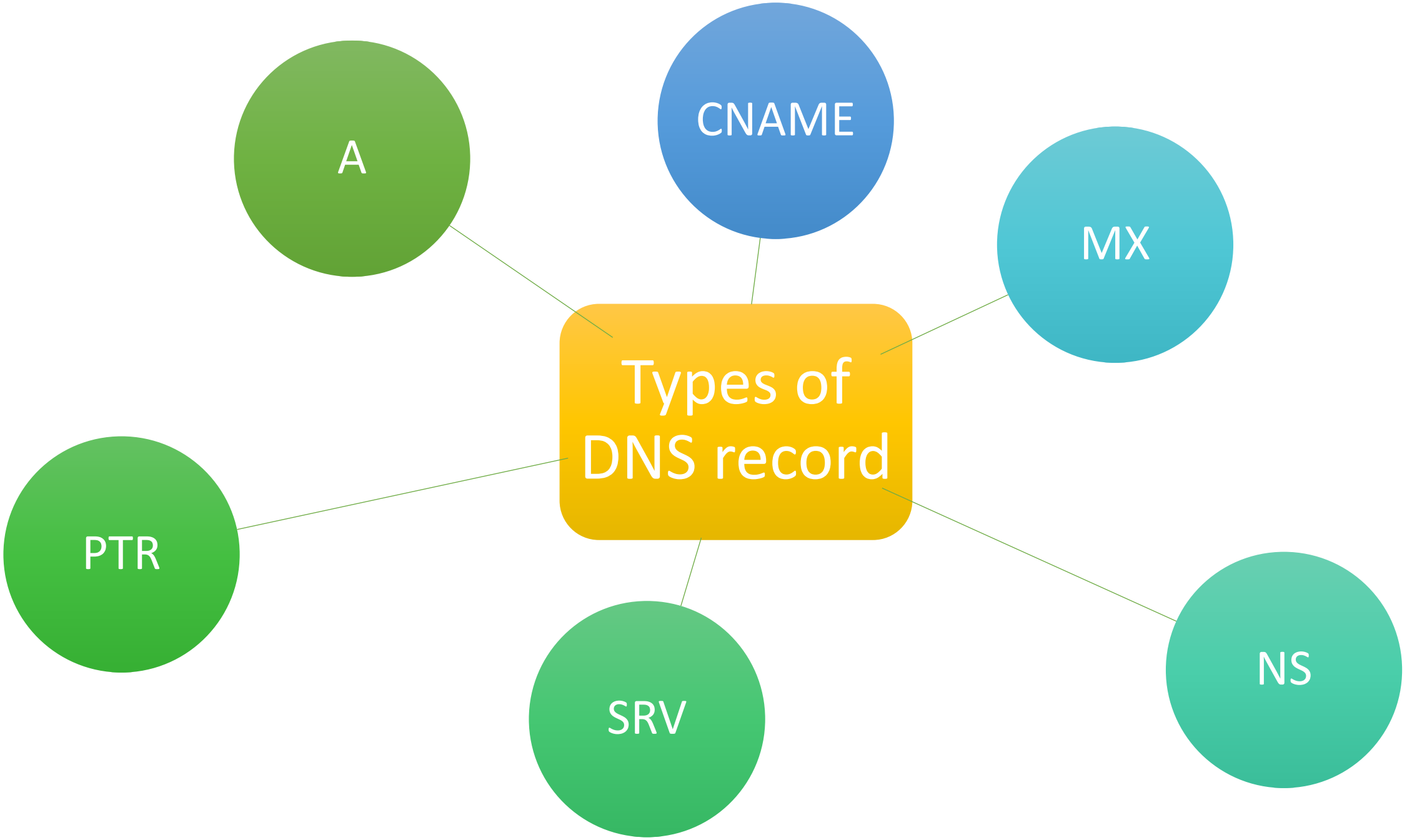
DNS packet format



DNS packet format: flags

QR	• 0 means the message is a query • 1 means it is a response
OpCodes	• The normal value is 0 (a standard query) for requests and responses. • Other values are: 4 (notify), and 5 (update). • Other values (1–3) are deprecated or never seen in operational use.
AA	Authoritative Answer(1) not(0)
TC	Truncated Answer(1) not(0), only the first 512 bytes of the reply were returned
RD	Recursion Desire
RA	Recursion Available
Z	0 for now but is reserved for future use
AD	Authentic Data is set to true if the contained information is authenticated
CD	Checking Disable is set to true if security checking is disabled
RCODES	NoError(0), 1,2 … errors


Request
Queries
Name = maytech.net
Type = A
Class = IN
Answers
Name = maytech.net
Type = A
Class = IN
TTL = 90
Address = 46.16.167.160
Response


A
CNAME
MX
Types of DNS record
PTR
SRV
NS

DNS: A record

- The record that holds the IP address of a domain
- ”A” records only hold Ipv4 addresses, if the site has a Ipv6 address, it will instead use an ‘AAAA’ record

```
> nslookup maytech.net
```

DNS: CNAME record (“canonical name”)

- Forwards one domain or subdomain to another domain
- does NOT provide an IP address

```
> nslookup –type=cname bohdan.quatrix.it
```

DNS: MX record

- This is the “mail exchange” record, and it directs email to a mail server

```
> nslookup -type=mx gmail.com
```

DNS: NS record

- Indicates which DNS server is authoritative for that domain (which server contains the actual DNS records)
- A domain will often have multiple NS records which can indicate primary and backup name servers for that domain

```
> nslookup -type=ns maytech.net
```

DNS: SRV record

- Specifies a host and port for specific services

_sip._tcp.example.com.

  - *_sip* - indicates the type of service
  - *_tcp* - indicates the protocol
  - *example.com* - is the host

```
> nslookup -type=srv _sip._tcp.example.com.
```

DNS: PTR record

- Give you the domain associated with a given IP address
- The PTR record is used in reverse-lookup zones for reverse DNS searches
- in-addr.arpa.

```
> nslookup -type=ptr 160.167.16.46.in-addr.arpa
```

The End