

INTERNET 
STIFTELSEN

DNS-kurs 2024

Internet på 15 sekunder

- Ett nätverk av nätverk
- Kommunikationen bygger på IP
- Routing styr trafik baserat på IP-adresser
- DNS binder samman namn och IP
- Nät != geografi

A photograph of a wooden desk in a dimly lit room. On the desk, there is a white mug filled with dark coffee, a silver pen, and a small notepad with handwritten notes. A laptop is partially visible in the foreground. The background shows a window with blinds and a dark wall.

Domännamnets roll

- Domännamn är en abstrahering av IP-adresser
- Domännamn är en typ av address, men inte bara en adress
- Domännamn har flera fördelar
 - Lättare att komma ihåg än en IP-adress
 - Kan gruppera nätverksenheter under ett namn, även om de inte delar nät eller geografisk placering
 - Kan signalera typ av tjänst (mail, www)
 - Ger igenkänning
 - Kan knytas till ett varumärke
- Kan vara ankare för annan data (kryptonycklar, metainformation för tjänster)

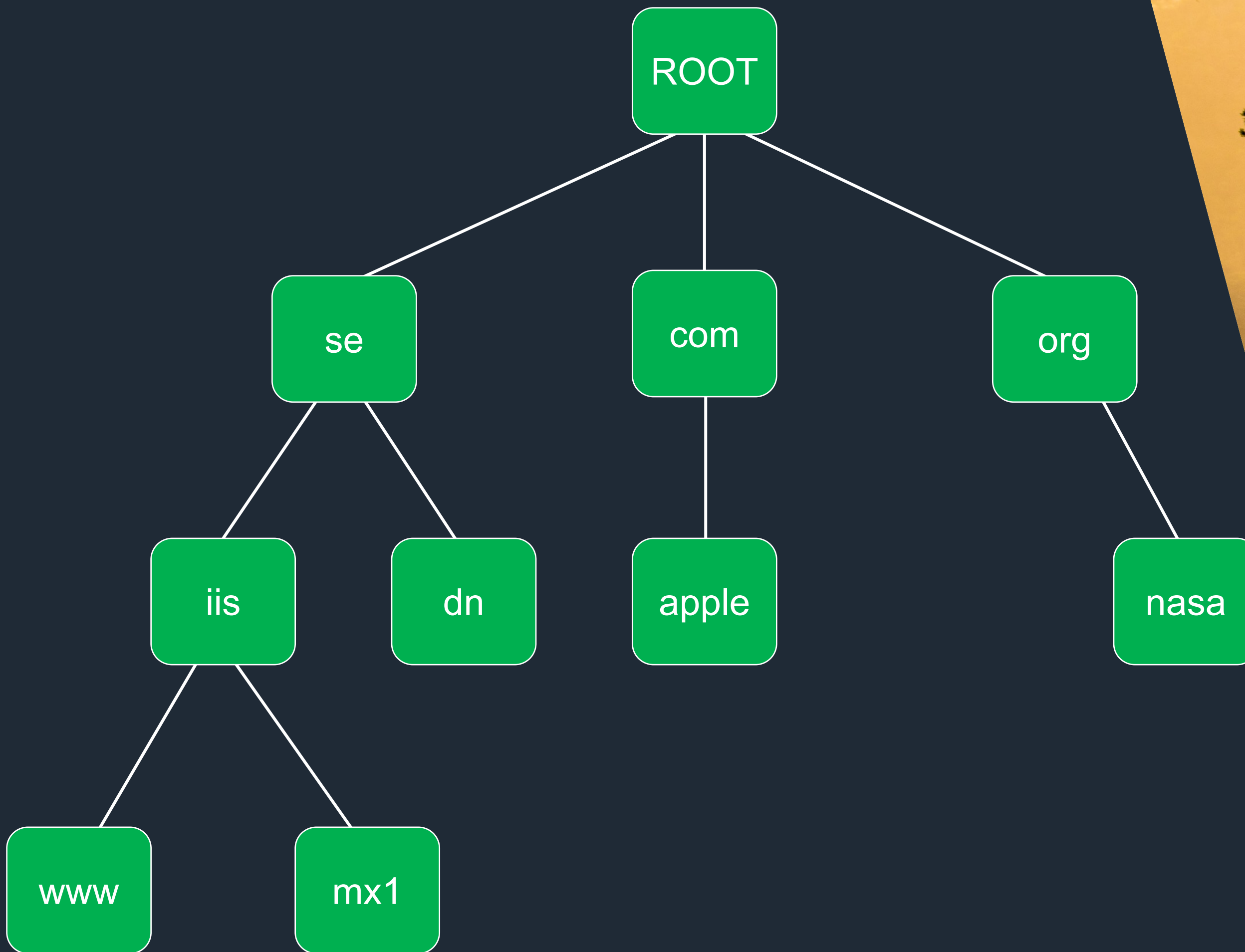


DNS

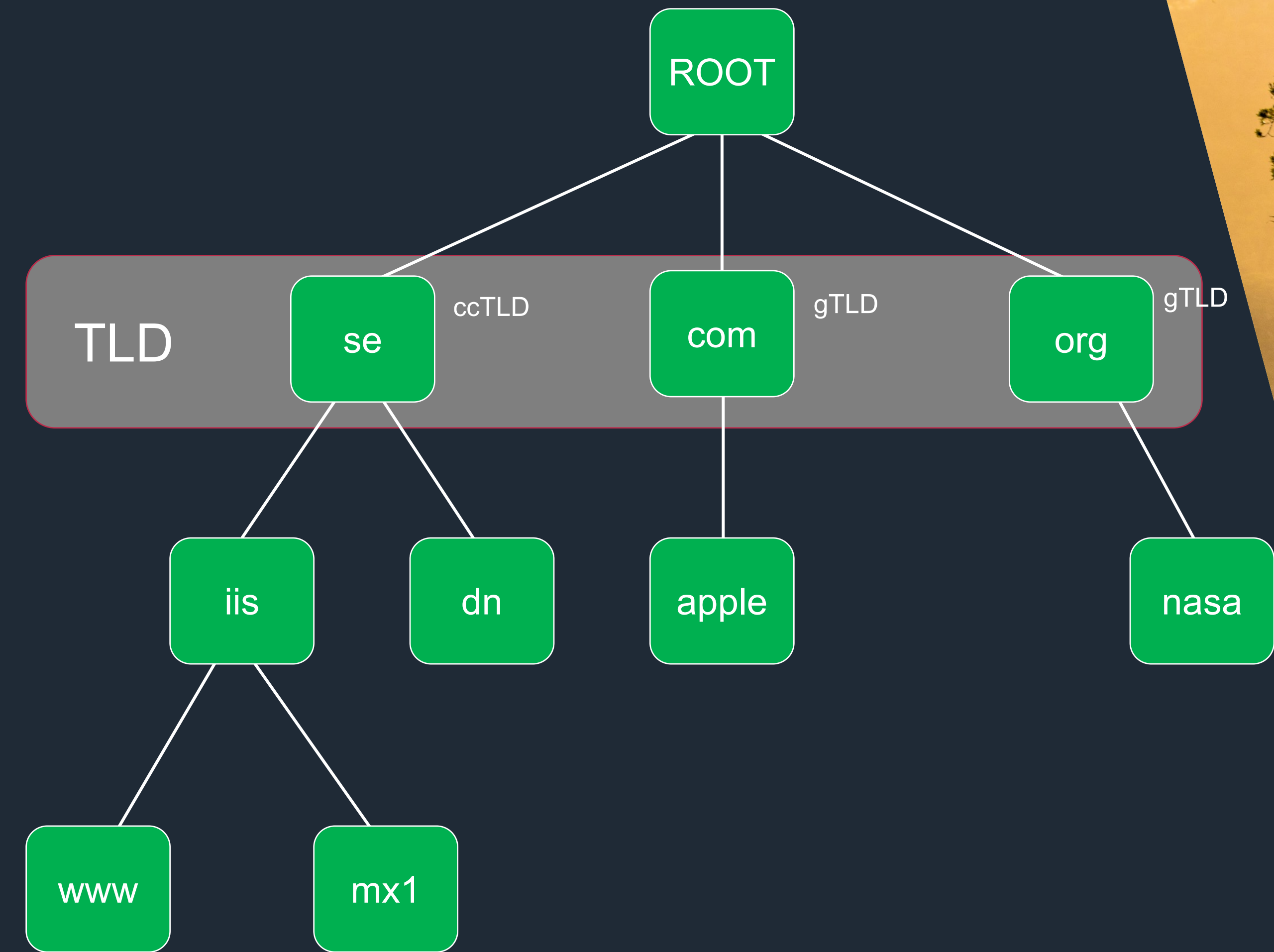
Domain Name System

- Stor databas
- Ger svar på specifika frågor
- Inte sökbar eler blädderbar
- Hierarkisk trädstruktur
- Redundant
- Distribuerad
- Decentraliserad

Domänträdetets struktur

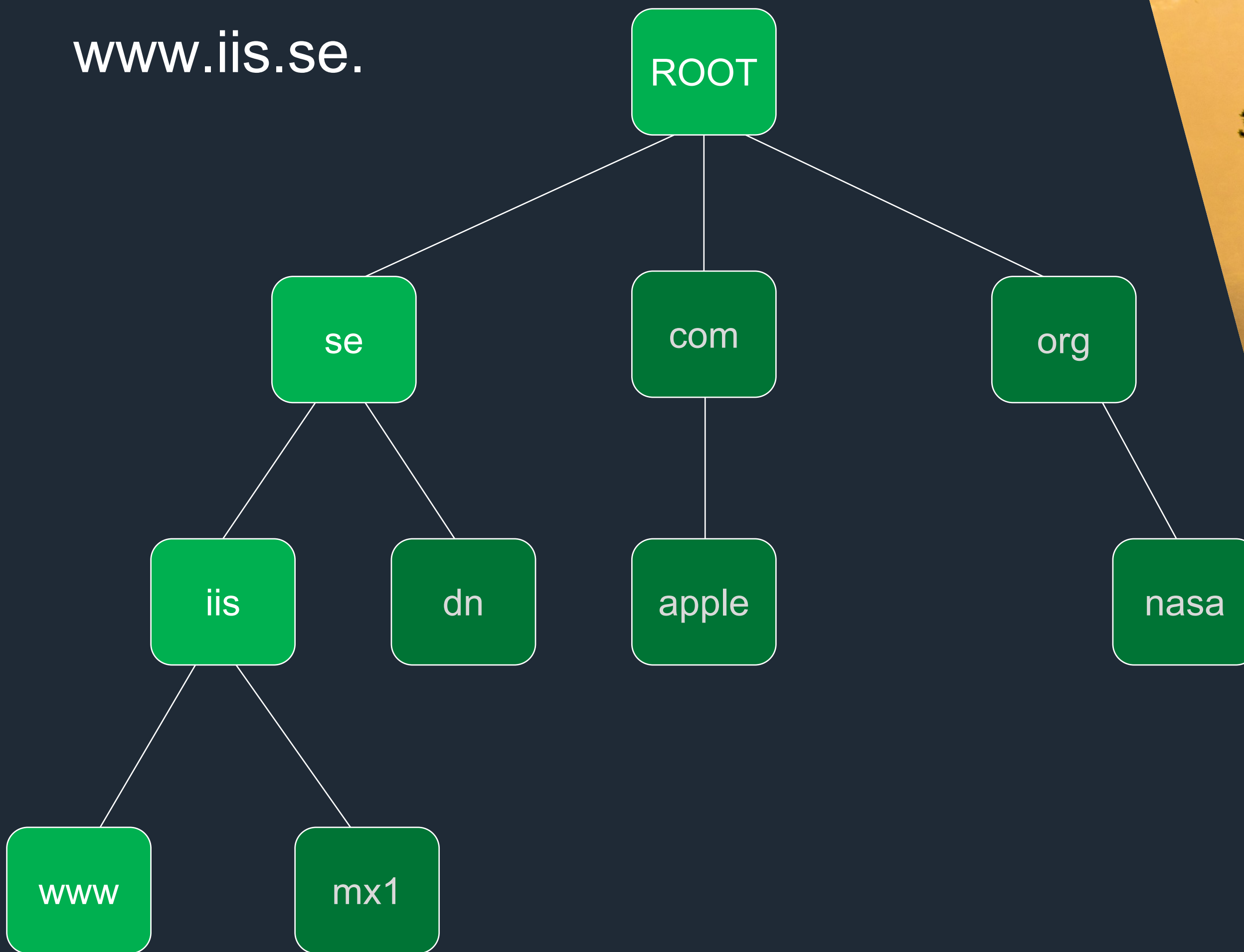


Domänträdetets struktur



Domänträdetets struktur

www.iis.se.





Pekare

Vad frågar man efter?

- SOA
- NS
- A
- AAAA
- CNAME
- MX
- TXT
- PTR
- SRV
- (ANY)
- (AXFR)

Pekartyper

Hur används de?

- SOA - Start Of Authority; Info om zonen
- NS - Name Server
- A - IPv4 adress (159.253.30.216)
- AAAA - IPv6 adress (2a02:750:7:3305::216)
- CNAME - Alias
- MX - Mail Exchanger
- TXT - Fritext (används för SPF mm.)
- PTR - Bakåtuppslag
- SRV - Info för tjänster (telefoni, office365)
- (ANY) - Pseudopekare
- (AXFR) - Pseudopekare



Pekar-anatomi

<u>Owner Name</u>	<u>TTL</u>	<u>Class</u>	<u>Type</u>	<u>Rdata</u>
www.iis.se.	60	IN	A	159.253.30.216
iis.se.	3660	IN	NS	i.ns.se.
iis.se.	3600	IN	NS	ns.nic.se.
iis.se.	3600	IN	NS	Ns3.nic.se.
iis.se.	60	IN	MX	5 mx1.iis.se.
iis.se.	60	IN	MX	5 mx2.iis.se.

DIG

```
; <<>> DiG 9.10.6 <<>> iis.se a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42009
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::, udp: 4096
;; QUESTION SECTION:
iis.se.                IN      A

;; ANSWER SECTION:
iis.se.                77      IN      A      159.253.30.216

;; Query time: 112 msec
;; SERVER: 172.20.10.1#53(172.20.10.1)
;; WHEN: Wed Jul 15 15:29:58 CEST 2020
;; MSG SIZE rcvd: 51
```




Resolving

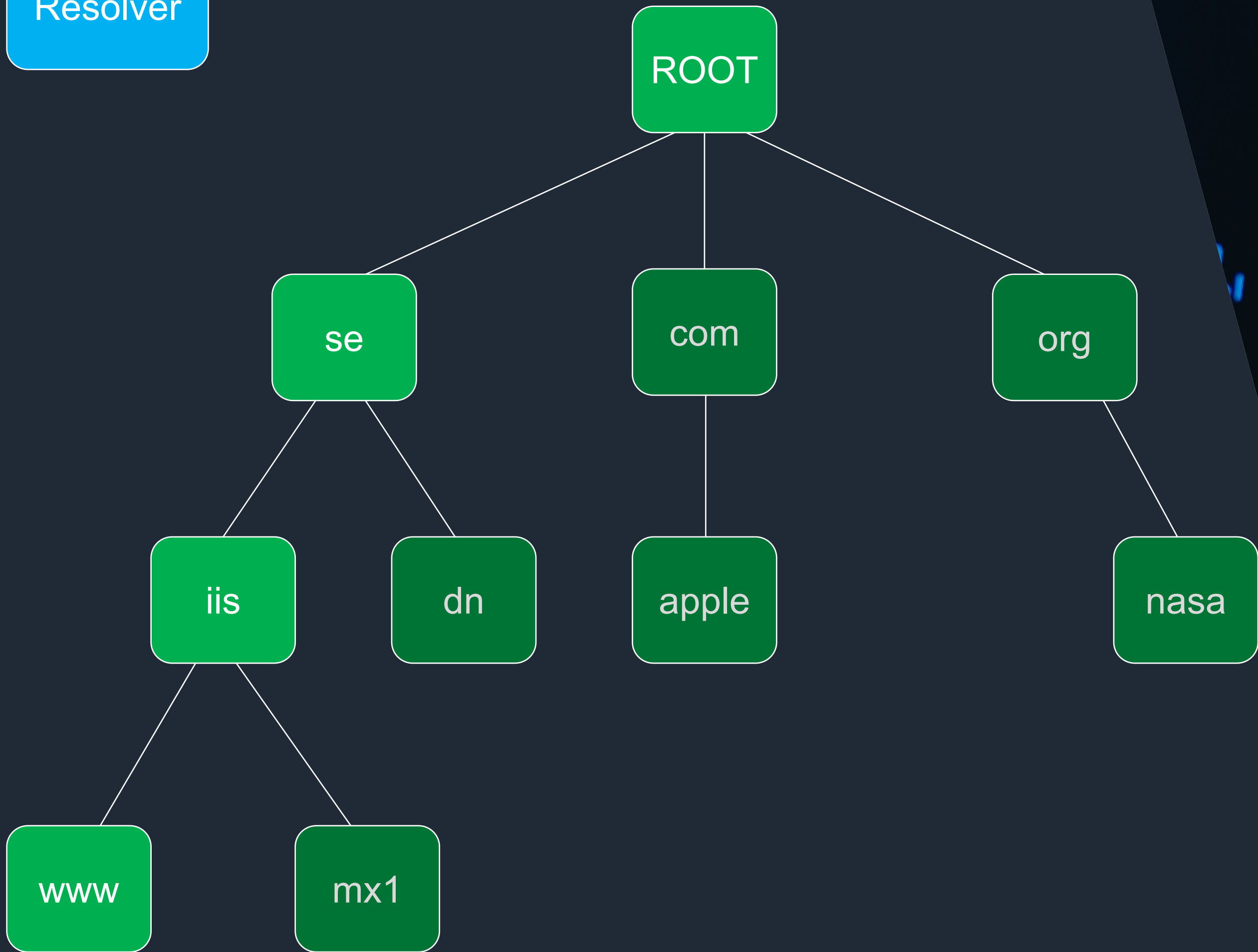
Hur hittar man fram till rätt zon?

- Resolvers är också DNS-servrar
- Men de har en annan roll än de auktoritativa namnservrarna
- Auktoritativa namnservrar äger zondata för sina domäner och svarar bara på förfrågningar för dessa
- Resolvers äger ingen zondata, men försöker ta reda på den för att ge svar
- Resolvers traverserar domänträdet tills de får ett svar eller ett fel

Resolving (old school)

www.iis.se?

Resolver



www.iis.se?

Resolver

ROOT

se

com

org

iis

dn

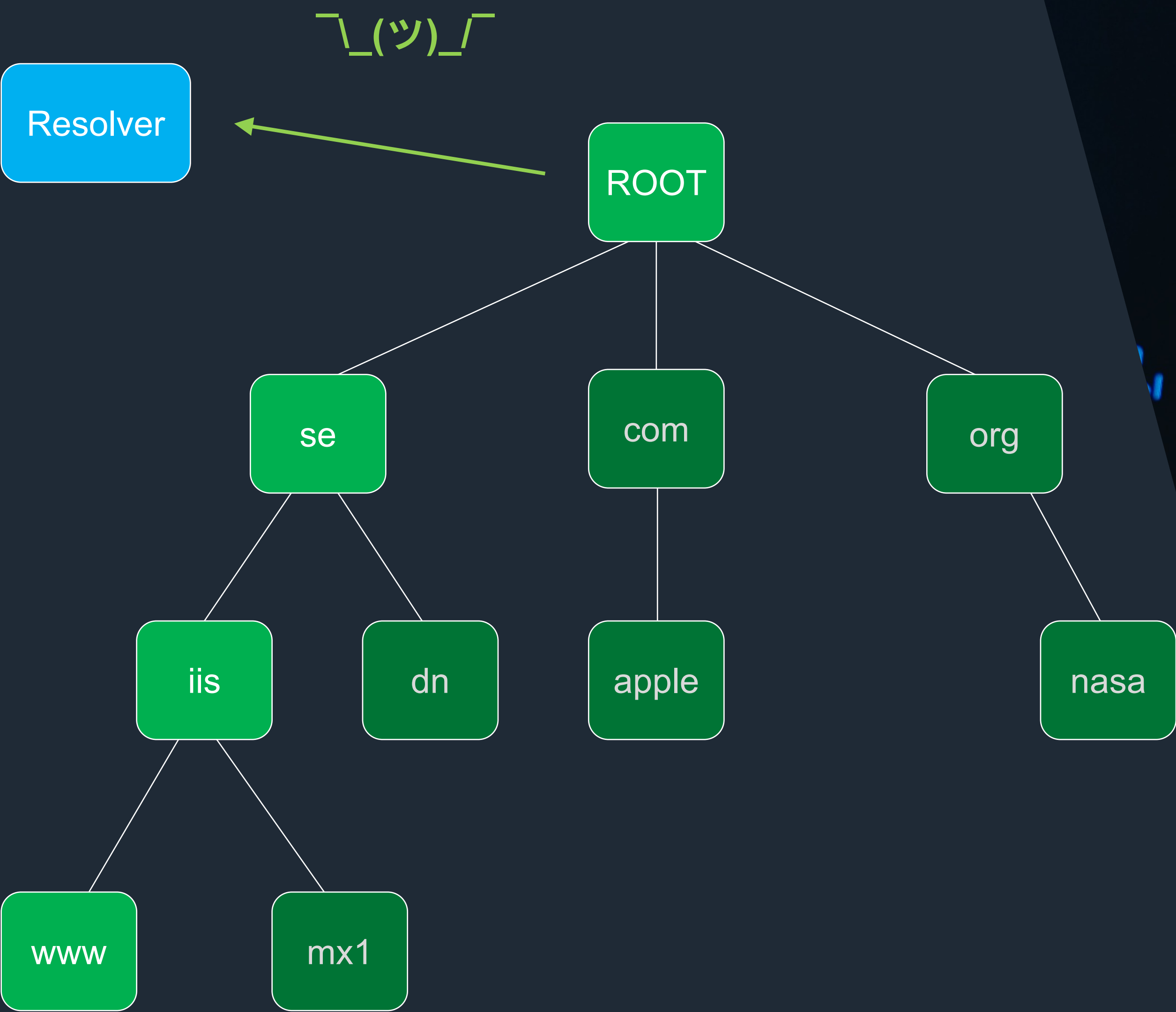
apple

nasa

www

mx1



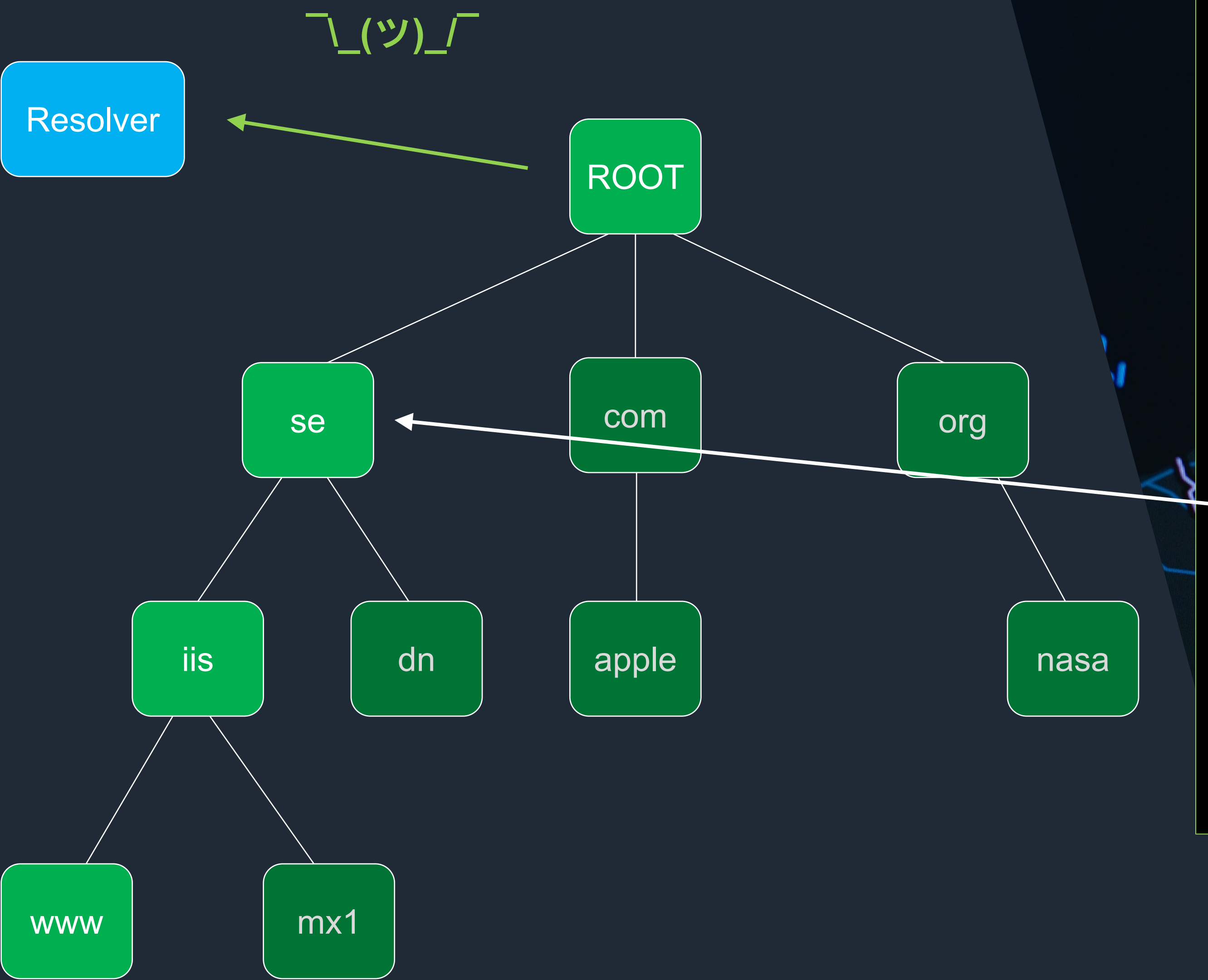


```
:: global options: +cmd
:: Got answer:
:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55630
:: flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 21
:: WARNING: recursion requested but not available

:: OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
:: QUESTION SECTION:
;www.iis.se.          IN      A

:: AUTHORITY SECTION:
se.                  172800   IN      NS      a.ns.se.
se.                  172800   IN      NS      b.ns.se.
se.                  172800   IN      NS      c.ns.se.
...

:: ADDITIONAL SECTION:
a.ns.se.             172800   IN      A        192.36.144.107
b.ns.se.             172800   IN      A        192.36.133.107
c.ns.se.             172800   IN      A        192.36.135.107
...
a.ns.se.             172800   IN      AAAA     2a01:3f0:0:301::53
b.ns.se.             172800   IN      AAAA     2001:67c:254c:301::53
c.ns.se.             172800   IN      AAAA     2001:67c:2554:301::53
...
```

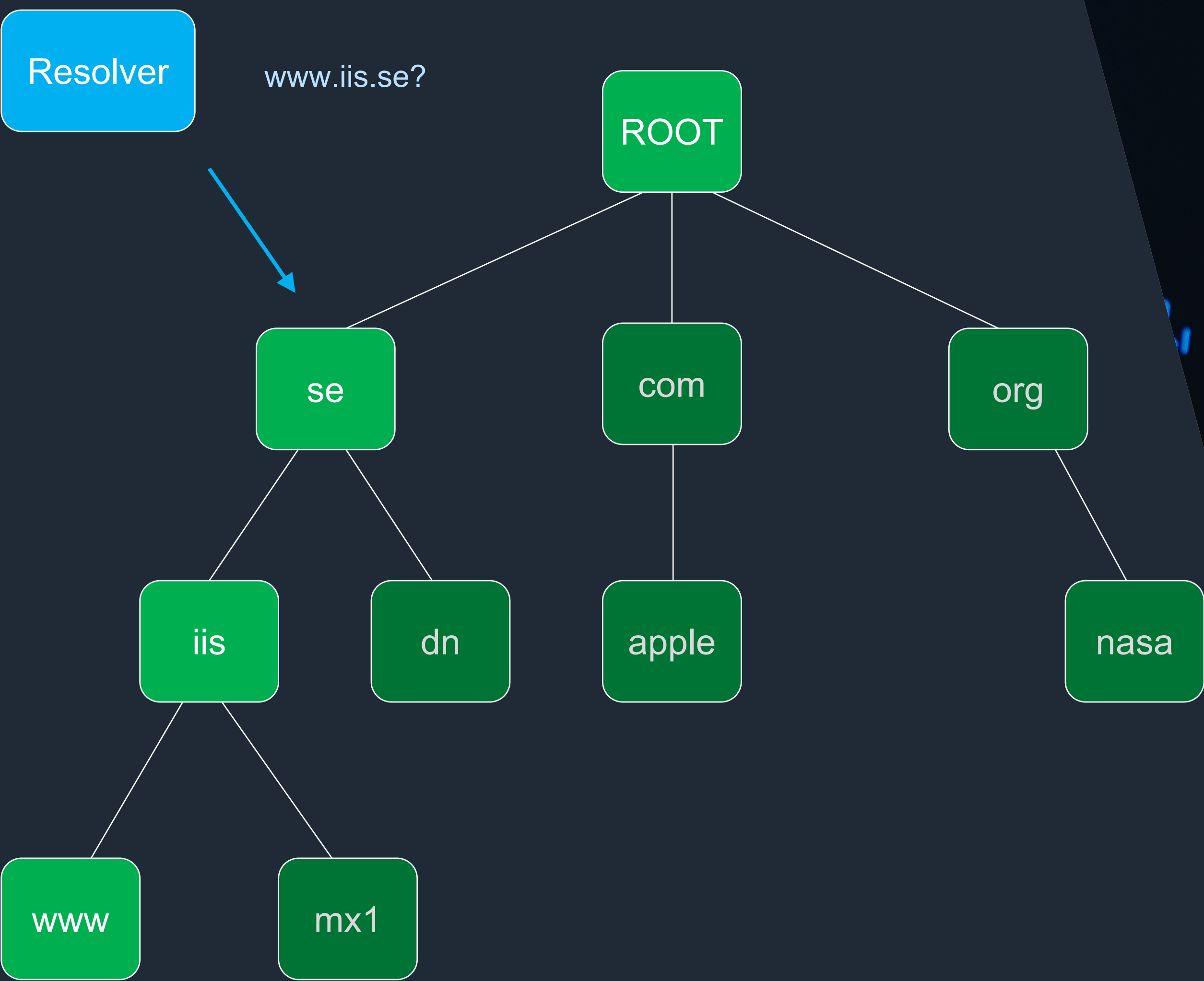



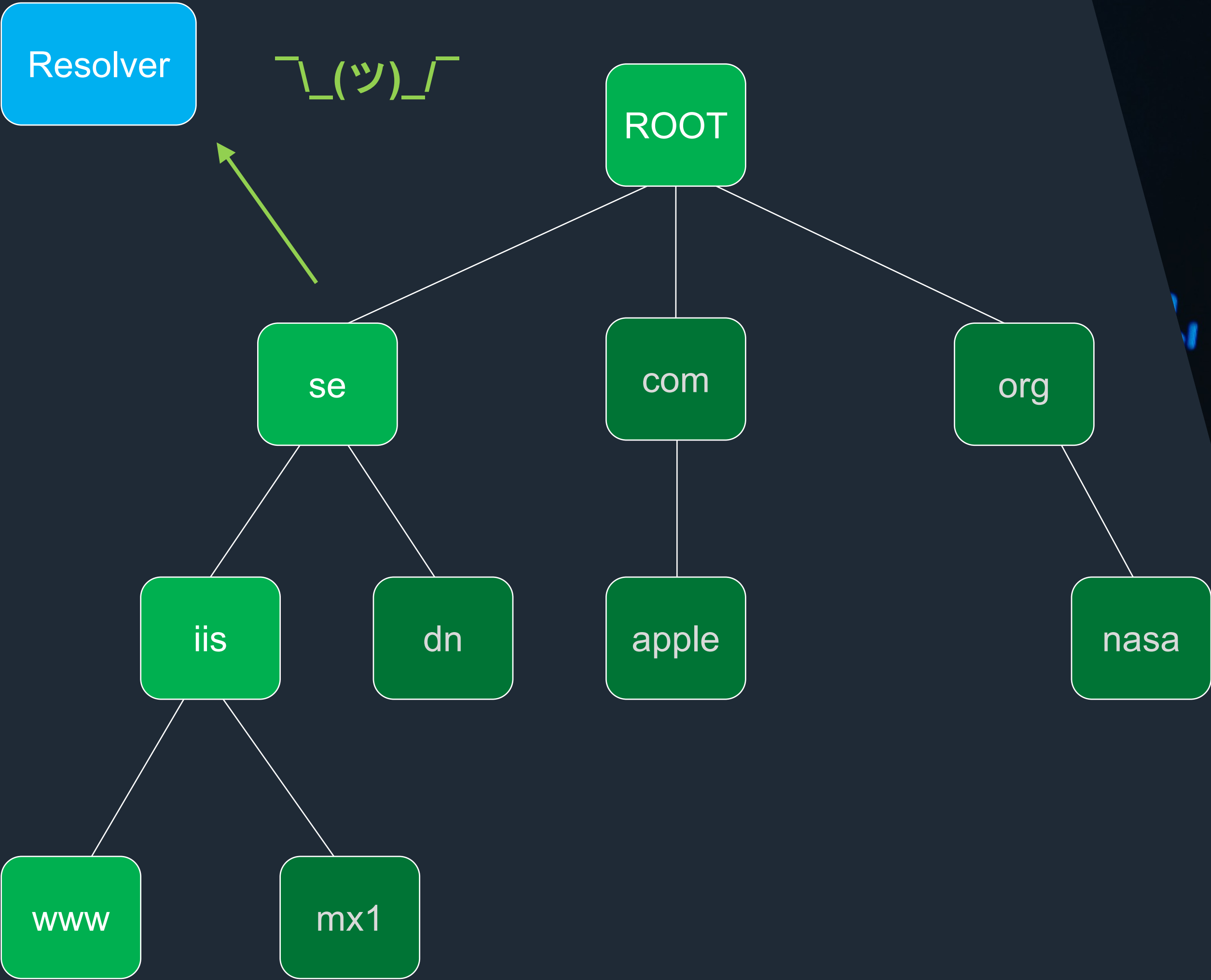
```
:: global options: +cmd
:: Got answer:
:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55630
:: flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 21
:: WARNING: recursion requested but not available
```

```
:: OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
:: QUESTION SECTION:
;www.iis.se.          IN      A
```

```
:: AUTHORITY SECTION:
se.          172800    IN      NS      a.ns.se.
se.          172800    IN      NS      b.ns.se.
se.          172800    IN      NS      c.ns.se.
...
```

```
:: ADDITIONAL SECTION:
a.ns.se.     172800    IN      A        192.36.144.107
b.ns.se.     172800    IN      A        192.36.133.107
c.ns.se.     172800    IN      A        192.36.135.107
...
a.ns.se.     172800    IN      AAAA     2a01:3f0:0:301::53
b.ns.se.     172800    IN      AAAA     2001:67c:254c:301::53
c.ns.se.     172800    IN      AAAA     2001:67c:2554:301::53
...
```

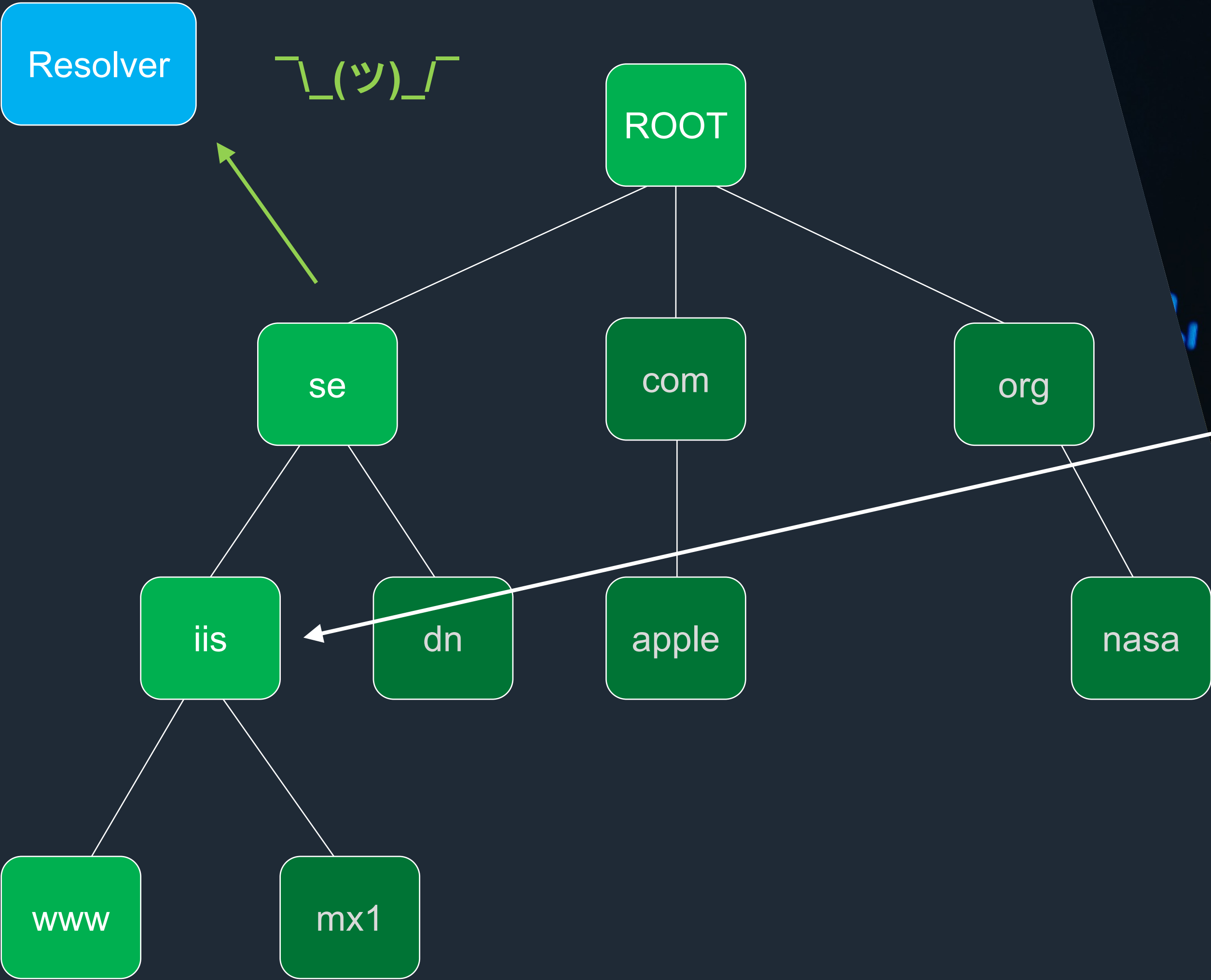


```
:: global options: +cmd
:: Got answer:
:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45728
:: flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 5
:: WARNING: recursion requested but not available

:: OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 4096
:: QUESTION SECTION:
;www.iis.se.                IN      A

:: AUTHORITY SECTION:
iis.se.      86400      IN      NS      ns.nic.se.
iis.se.      86400      IN      NS      i.ns.se.
iis.se.      86400      IN      NS      ns3.nic.se.

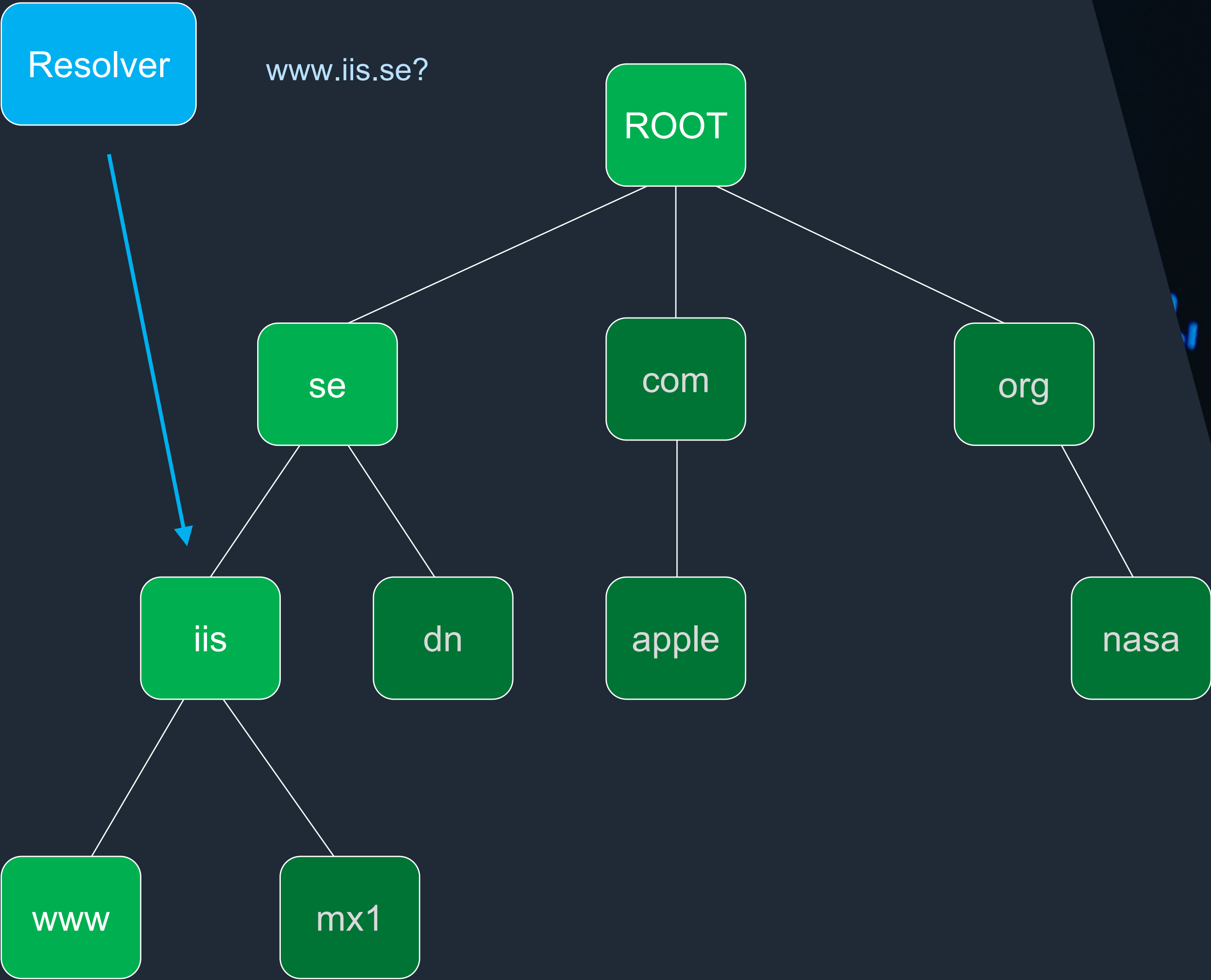
:: ADDITIONAL SECTION:
ns3.nic.se.  86400      IN      AAAA     2001:67c:124c:2007::45
ns.nic.se.   86400      IN      AAAA     2001:67c:124c:100a::45
ns3.nic.se.  86400      IN      A        91.226.37.45
ns.nic.se.   86400      IN      A        91.226.36.45
```

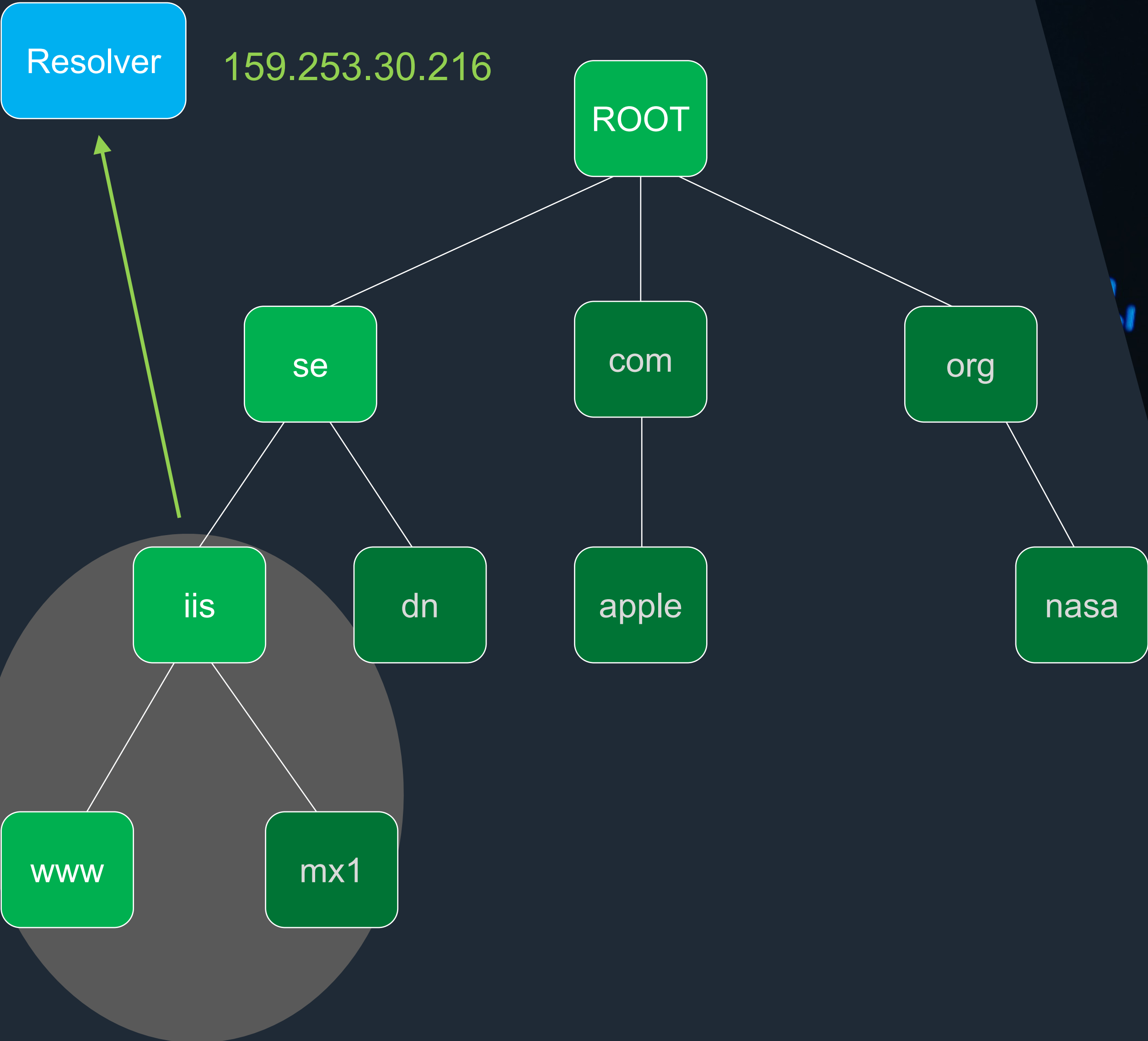



```
:: global options: +cmd
:: Got answer:
:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45728
:: flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 5
:: WARNING: recursion requested but not available
```

```
:: OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
:: QUESTION SECTION:
;www.iis.se.                IN      A
```

;; AUTHORITY SECTION:				
iis.se.	86400	IN	NS	ns.nic.se.
iis.se.	86400	IN	NS	i.ns.se.
iis.se.	86400	IN	NS	ns3.nic.se.
;; ADDITIONAL SECTION:				
ns3.nic.se.	86400	IN	AAAA	2001:67c:124c:2007::45
ns.nic.se.	86400	IN	AAAA	2001:67c:124c:100a::45
ns3.nic.se.	86400	IN	A	91.226.37.45
ns.nic.se.	86400	IN	A	91.226.36.45





```
:: global options: +cmd
:: Got answer:
:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5399
:: flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 5
:: WARNING: recursion requested but not available

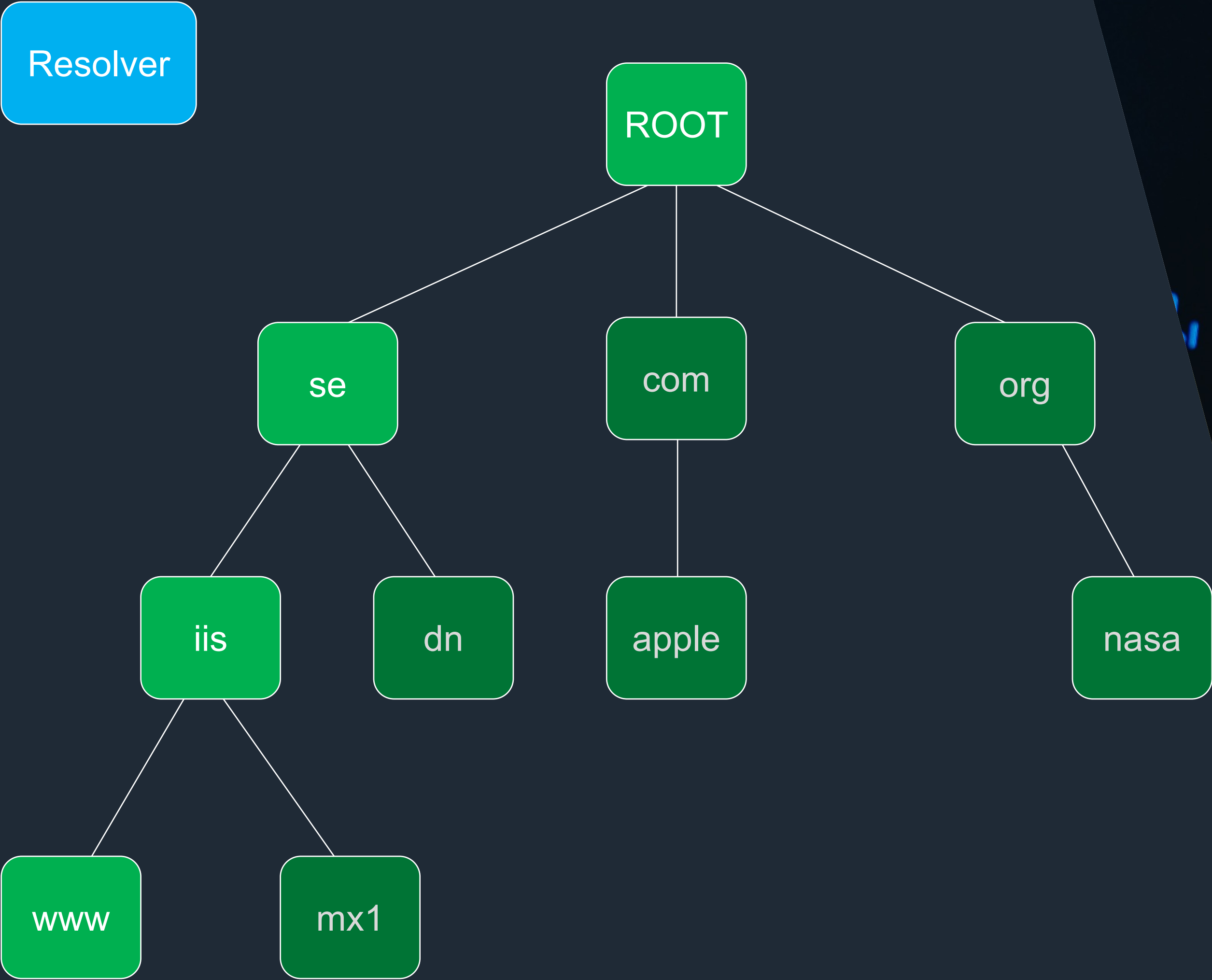
:: OPT PSEUDOSECTION:
; EDNS: version: 0, flags::; udp: 4096
:: QUESTION SECTION:
;www.iis.se.          IN      A

:: ANSWER SECTION:
www.iis.se.        60     IN      A          159.253.30.216

:: AUTHORITY SECTION:
iis.se.             3600   IN      NS          i.ns.se.
iis.se.             3600   IN      NS          ns3.nic.se.
iis.se.             3600   IN      NS          ns.nic.se.

:: ADDITIONAL SECTION:
ns.nic.se.          3600   IN      AAAA         2001:67c:124c:100a::45
ns3.nic.se.         3600   IN      AAAA         2001:67c:124c:2007::45
ns.nic.se.          3600   IN      A           91.226.36.45
ns3.nic.se.         3600   IN      A           91.226.37.45
```


www.iis.se = 159.253.30.216





Resolving Utveckling

- **Klassisk DNS** (Old school)
 - Port 53
 - UDP (TCP vid behov)
 - Okrypterade frågor
- **DoT** – DNS over TLS
 - Port 853
 - TCP
 - Krypterade frågor
- **DoH** – DNS over HTTPS
 - Port 443
 - TCP
 - Krypterade frågor
 - Ser ut som vanlig HTTPS trafik
- **DoQ** – DNS over Quic
 - Port 853
 - Quic
 - Krypterade frågor
- **QMIN** – Query Name Minimization
 - Mer 'diskret' resolving

A hand holding a crystal ball that reflects a sunset scene with cherry blossoms. The background is a dark blue gradient.

Bakåtuppslag

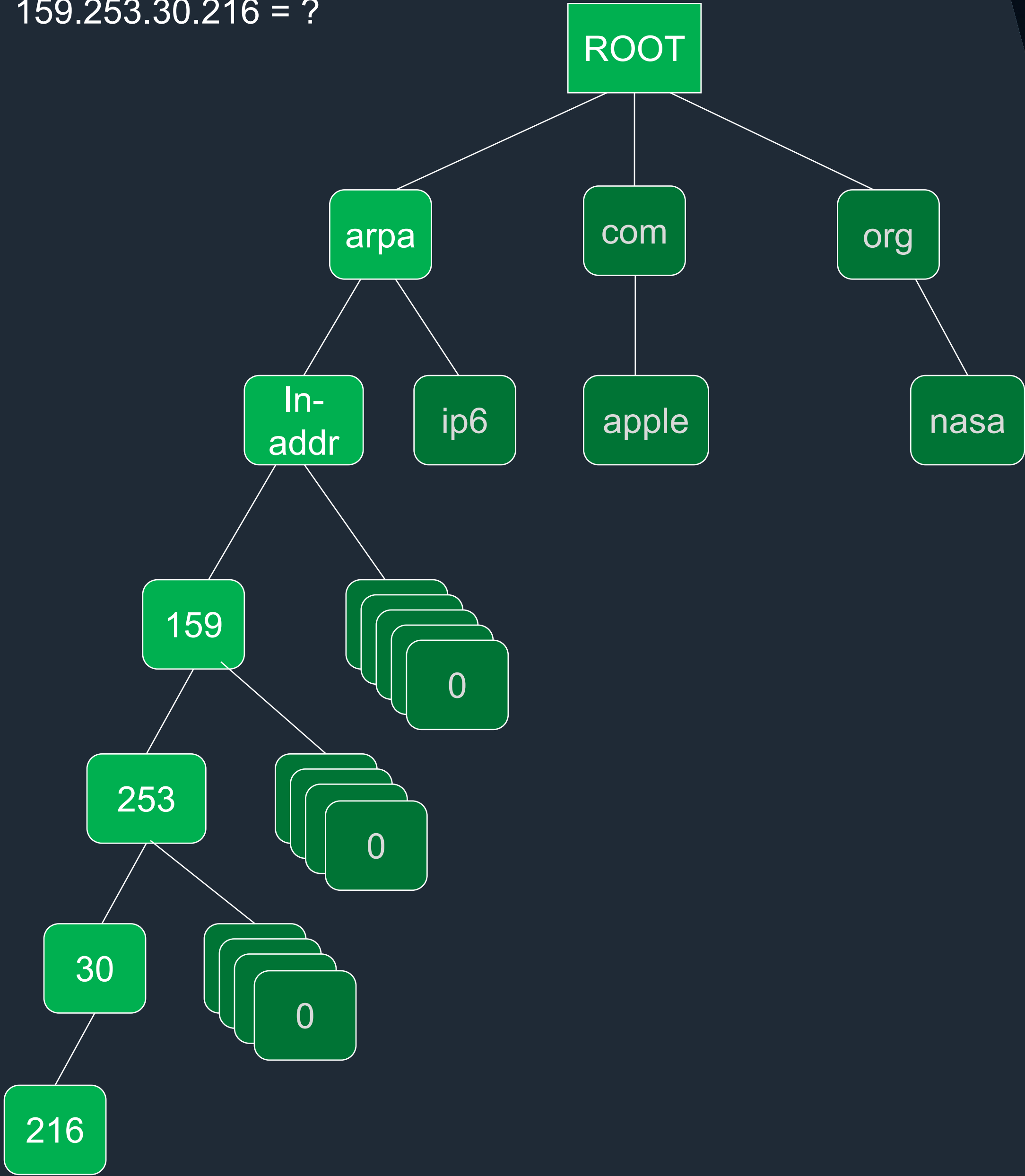
- Hitta ett namn associerat med en IP
- Fungerar (nästan) precis som vanligt
- Siffror är giltiga labels
- Egen toppdomän: .arpa
 - in-addr.arpa (för IPv4)
 - ip6.arpa (för IPv6)
- Frammåt och bakåtuppslag är inte nödvändigtvis kopplade till varandra
- IP-adressens 'ägare' styr normalt över bakåtuppslag



Bakåtuppslag

- IP-adresser och domännamn har omvänd ordning på sina mest till minst signifikanta delar
 - **159.253.30.216**
 - **www.iis.se.**
- IP-adressen behöver 'inverteras' för att passa in i domännamnsystemet.
- **159.253.30.216 → 216.30.253.159**
- Labels avgränsas vid oktetterna i adressen (för IPv4)
- **216.30.253.159.in-addr.arpa.**

159.253.30.216 = ?



DNSSEC

DNS Security Extensions

- Vad är det?
- Vad gör det?
- Varför behöver vi det?

DNSSEC

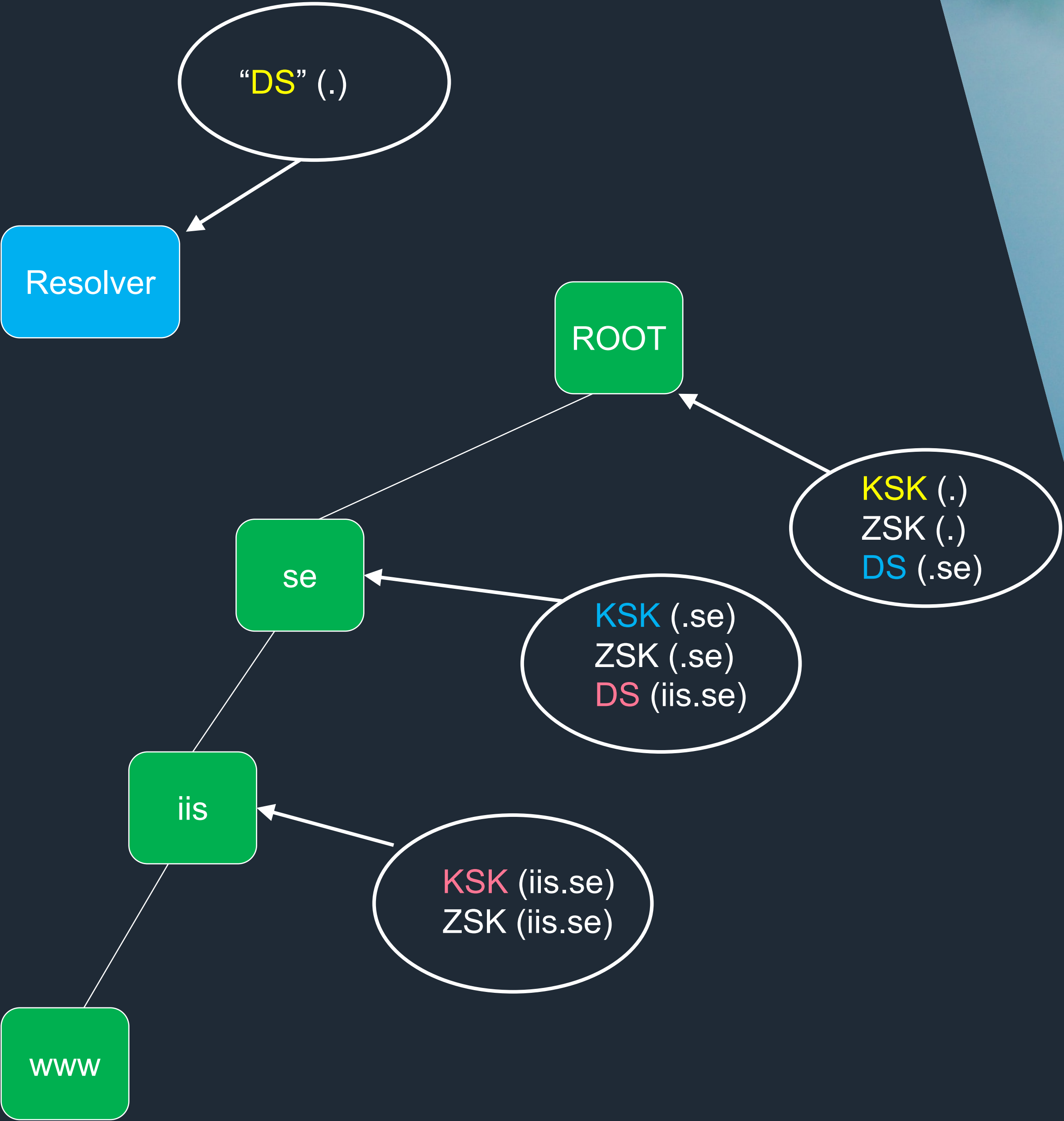
DNS Security Extensions

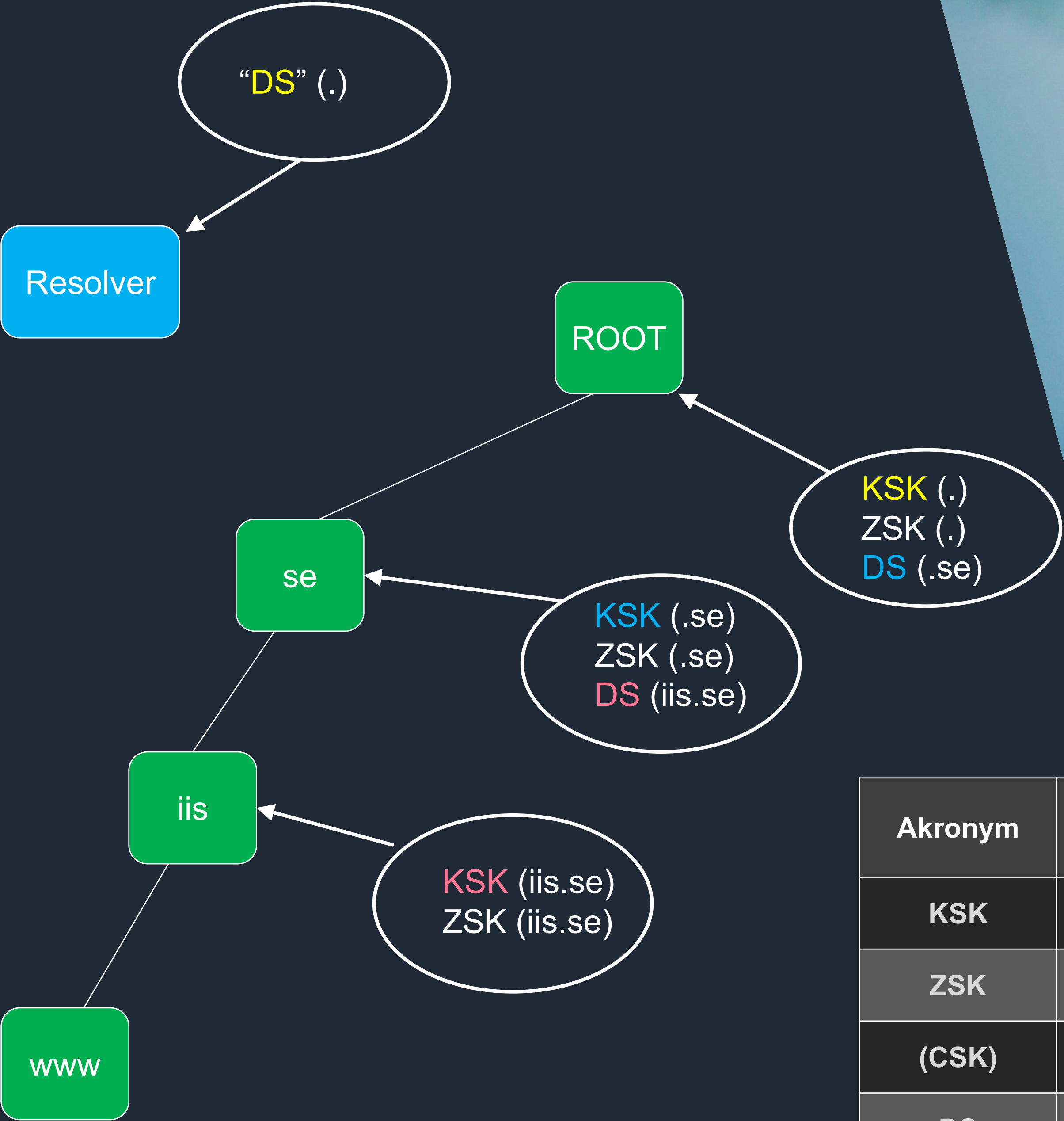
Vad är DNSSEC?

- “Skalskydd” för en domän
- Digital *signering* av DNS-data
- Ser till att DNS-datan kommer från dataägaren (source of truth) och är oförvanskad
- Är en förutsättning för andra säkerhetsmekanismer, t.ex. DANE
- OBS! Krypterar *inte* DNS-trafiken

Kryptografiska signaturer

- Asymetrisk kryptering (PGP, SSH, TLS)
- Nyckelpar som genereras tillsammans
- En nyckel hålls hemlig, den andra sprids fritt (privat/publik)
- En nyckel *kan inte* dekryptera det den krypterat
- Endast *den andra* nyckeln i nyckelparet kan det





Akronym	Namn	Funktion
KSK	Key Signing Key	Signerar ZSK
ZSK	Zone Signing Key	Signerar Zondata
(CSK)	Combined Signing Key	Variant av signering motsvarande KSK/ZSK i samma nyckel
DS	Delegation Signer	Hash av KSK/CSK. Återfinns I föräldrazonen

Verktyg

- <https://zonemaster.se> – kontrollera din domän
- <https://dnsviz.net> – visualisera domänträdet för din domän
- <https://toolbox.googleapps.com/apps/dig/> – begränsad DIG-klient





IP adresser

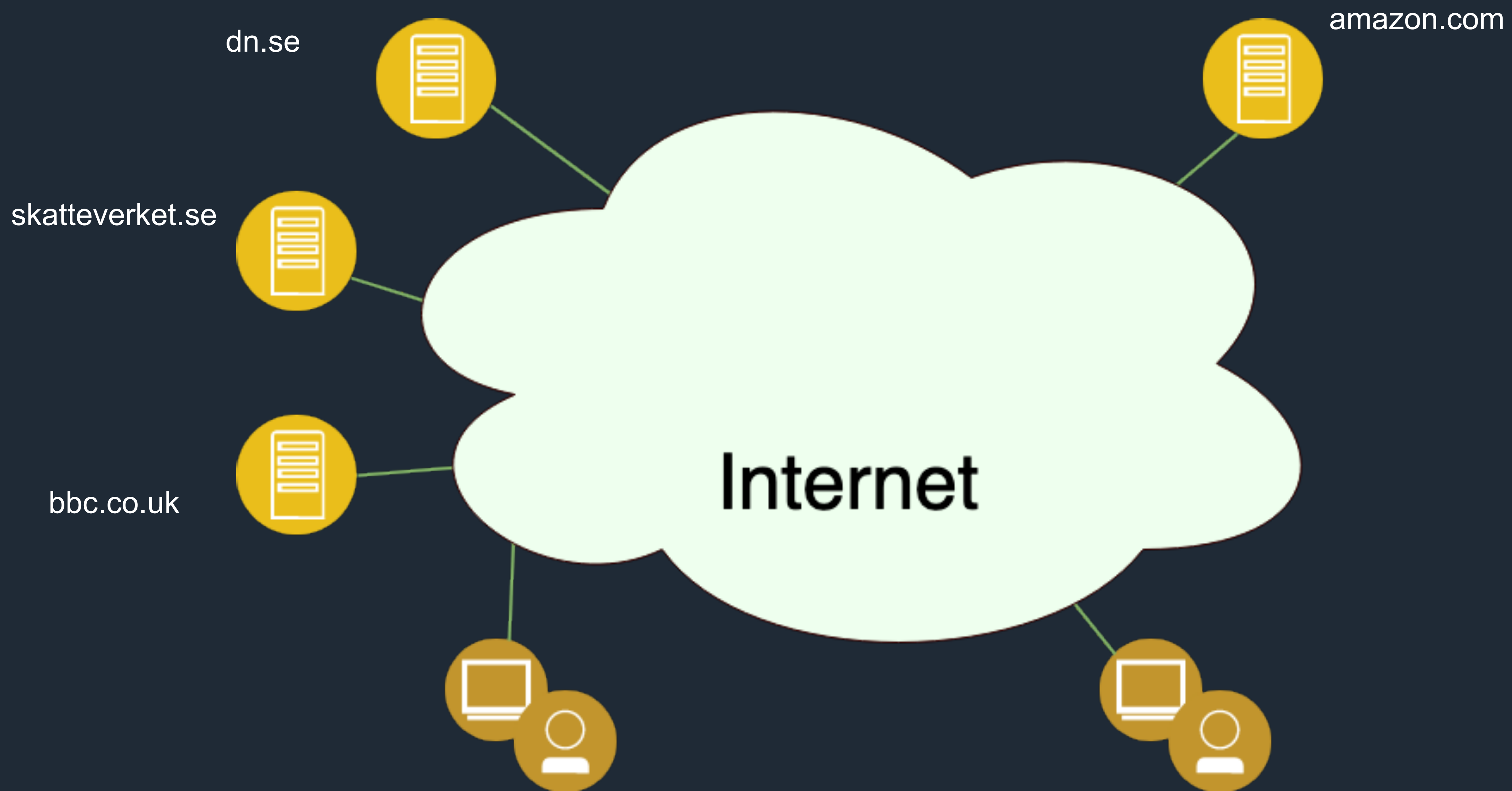
- Alla datorer har (minst) en IP-address
 - IPv4 (159.253.30.207)
 - IPv6 (2a02:750:7:3305::2d4)
- Unik* identifierare
- RFC1918
- RIR (Regional Internet Registry)
 - RIPE
 - ARIN
 - AIPNIC
 - AFRINIC
 - OCEANIC
- LIR (Local Internet Registry)
 - Ofta ISP
- Internets "Styrning"
 - IANA
 - ICANN



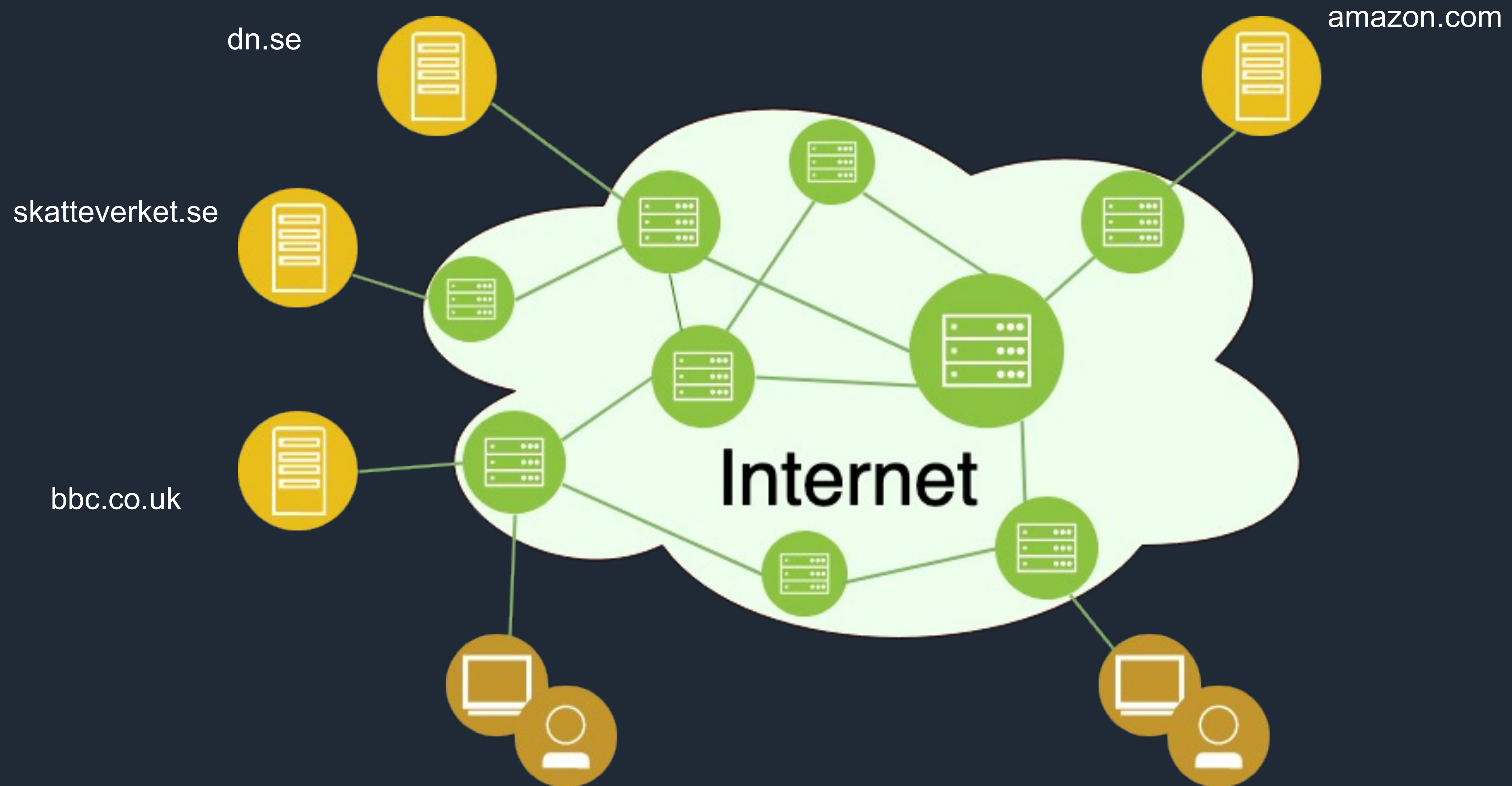


Routing

- Dirigerar trafiken mellan två IP-adresser
- Oftast dynamisk (BGP, OSPF mm.)
- Multipla vägar till samma destination
 - Unicast
 - Multicast



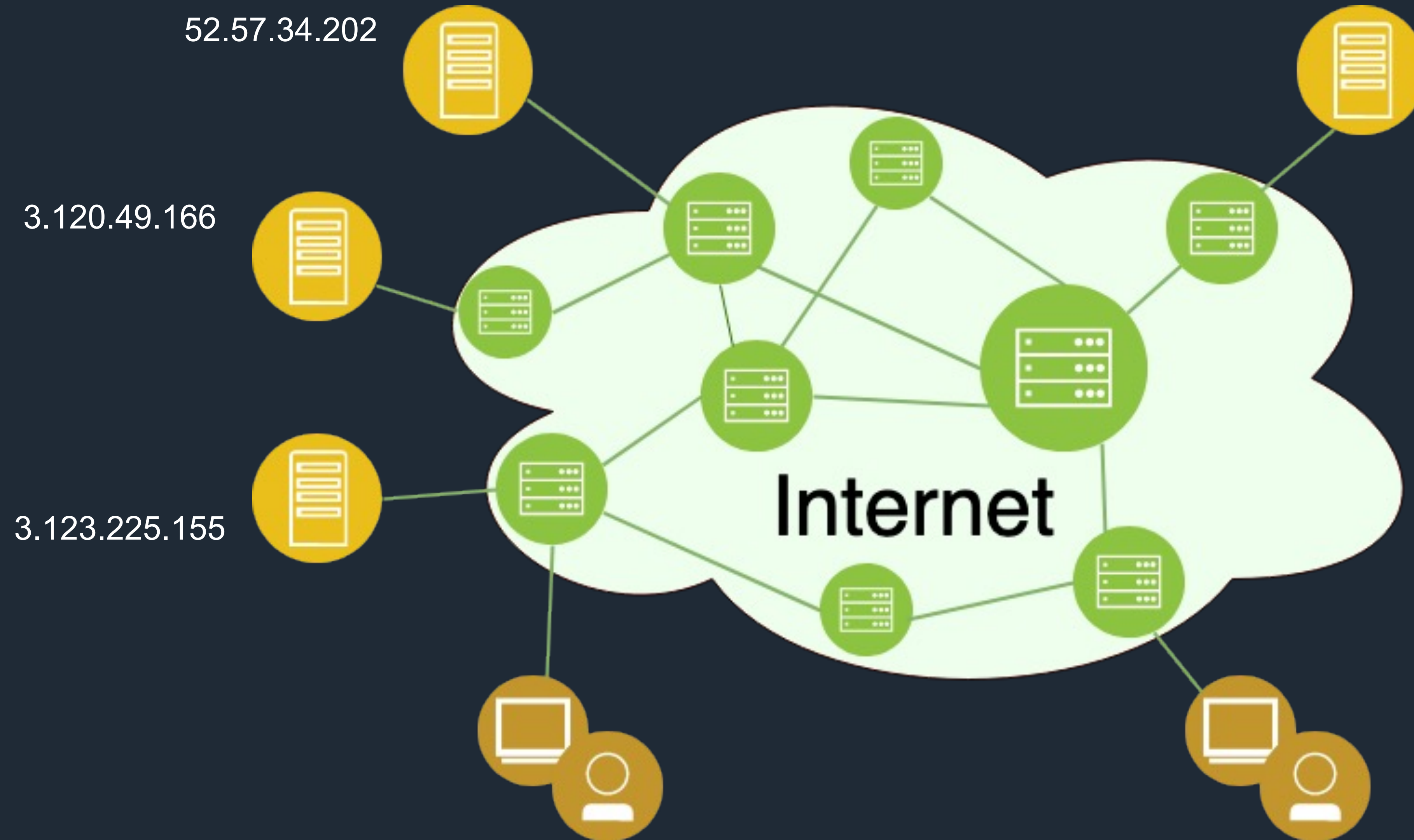
Routing



Routing



Unicast



Anycast

