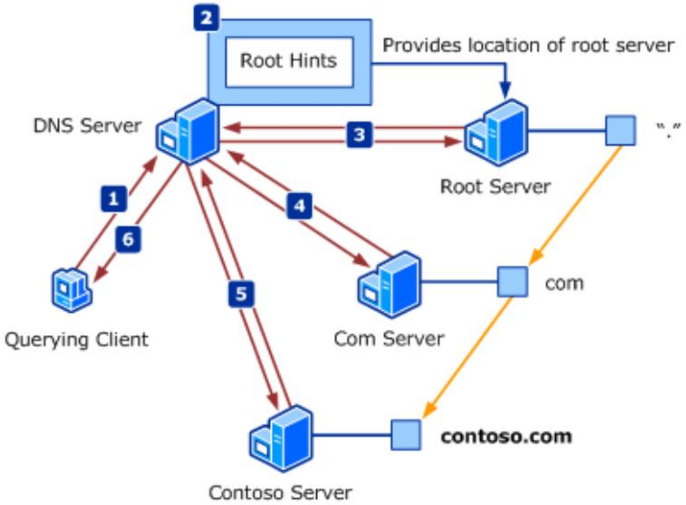
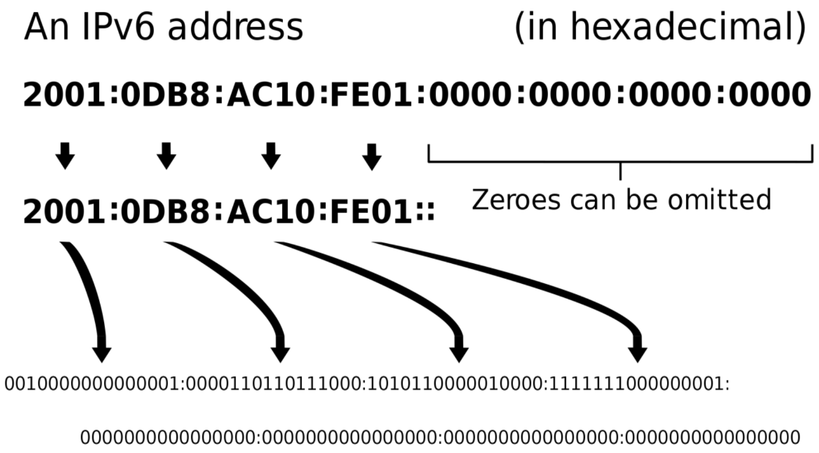
Domain Name System.

IPv6

Lecture 4





SoftUni Team

Technical Trainers

Software University

SoftUni Foundation

Software University

http://softuni.bg

Have a Question?

sli.do

#CNA

Table of Contents

1. Domain Name System
2. IPv6
3. Demonstration

Domain Name System

DNS structure

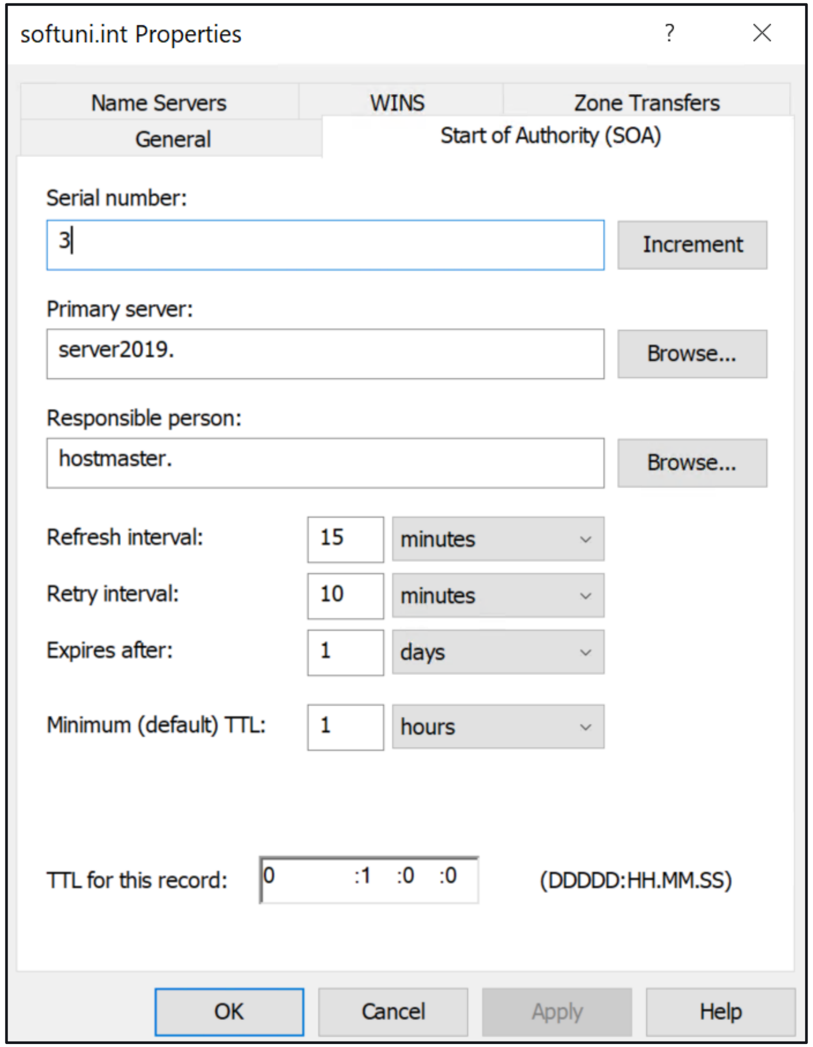
- DNS is hierarchical and distributed system
- At the top there is the root domain or "."
    - One level below are the TLD (top level domains, i.e. ".com")
        - One level below are the second level domains, i.e. "yahoo"
            - Possible third level domains, etc.
- DNS Zone – part of the DNS namespace, managed by specific organization

Resource records (in a DNS zone)

- Common resource records and their purposes:
  - A record: a name which points to a IPv4 address
  - AAAA record: a name which points to a IPv6 address
  - CNAME record (alias): a name which points to another name
    (Canonical Name)
  - MX record: shows who is the mail server for that domain
    (Mail EXchanger)
  - TXT record: text entry, usually used for domain verification and anti-spam
    (TeXT)
  - NS record: shows which are the name servers for the zone
    (Name Server)
  - SOA record: contains administrative information about the zone
    (Start Of Authority)

Start of Authority (SOA) record

- SOA specifies authoritative about the DNS zone
  - Serial number – incremented each time there is a change in the zone
  - Primary server – who stores the primary zone file
  - Refresh and retry intervals – when the secondary DNS will query the primary for changes
  - TTL – how long the data should be kept in the clients’ cache



Serial number: 3

Primary server: server2019.

Responsible person: hostmaster.

Refresh interval: 15 minutes

Retry interval: 10 minutes

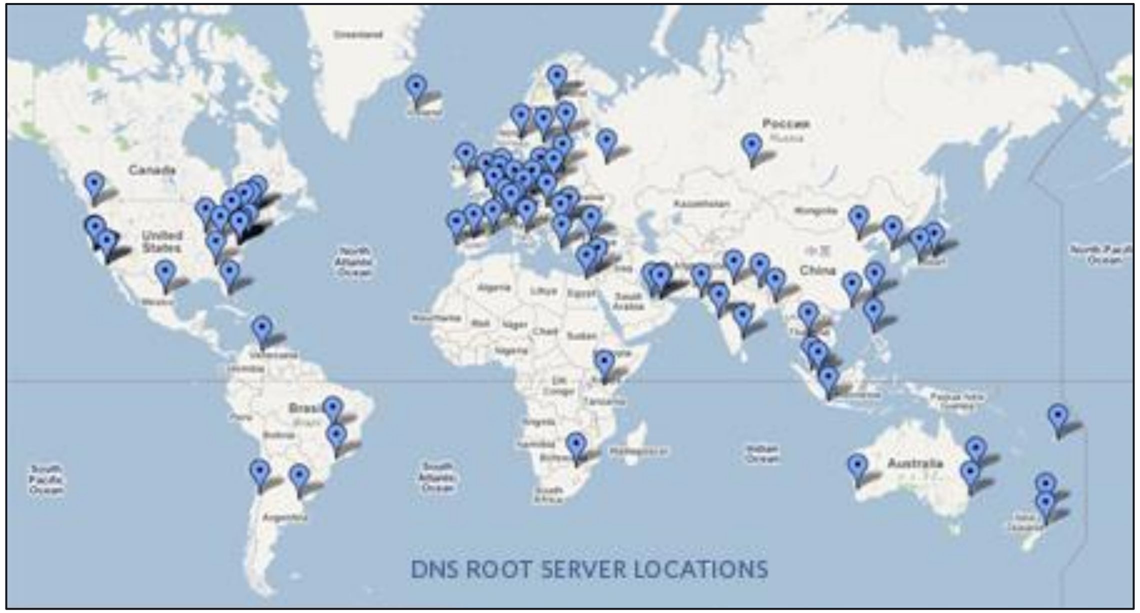
Expires after: 1 days

Minimum (default) TTL: 1 hours

TTL for this record: 0 :1 :0 :0 (DDDDD:HH.MM.SS)

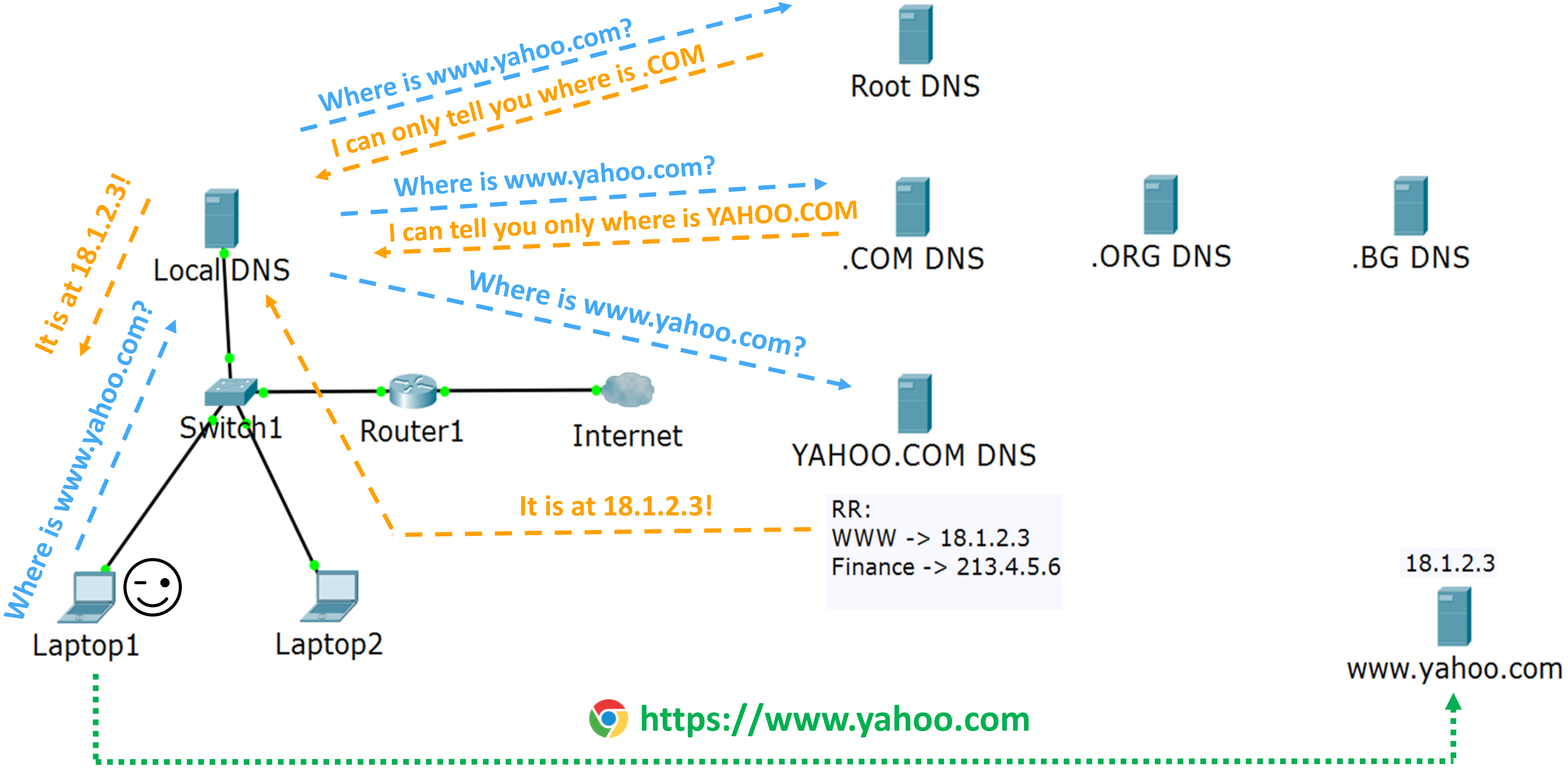
Root Hints

- The authoritative name servers for the “root” zone
- There are 13 named authorities, globally distributed
- They provide just a reference for the top-level domains (TLD)



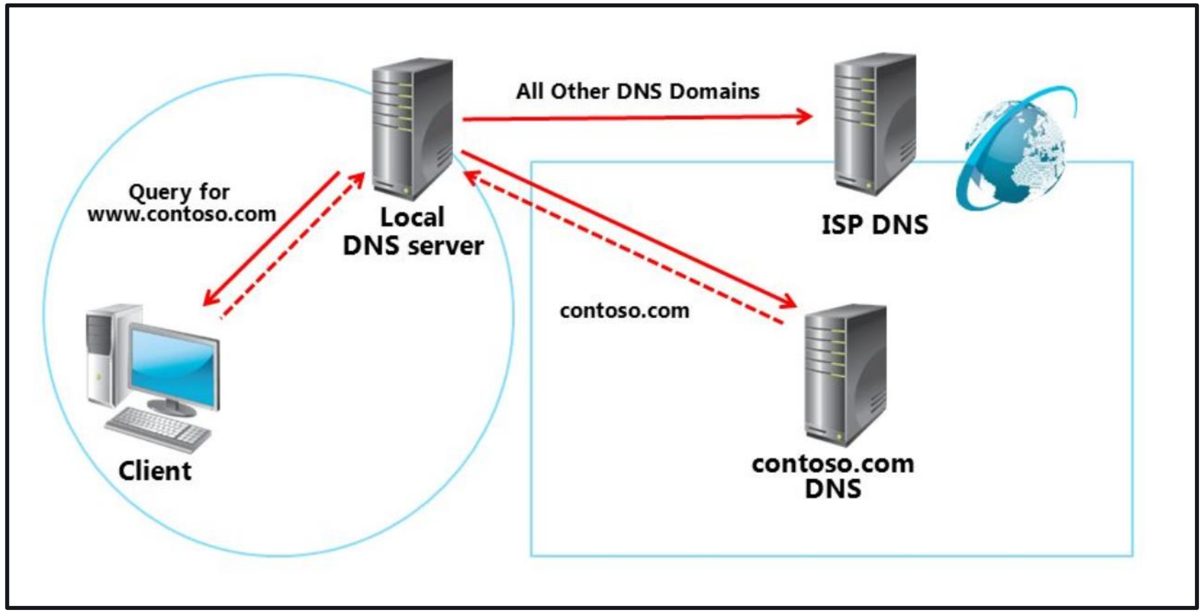
DNS ROOT SERVER LOCATIONS

DNS query process



DNS forwarder and conditional forwarder

- A local DNS server only knows about its local zones and records
- If a client asks for an external zone/record, the local DNS should ask someone else



- If we have multiple local DNS zones, hosted on different servers, we can use conditional forwarders

DNS end to end process

- First, the client checks its local cache
- If the entry is not in the cache, the client makes a query to the first DNS server(s) in its local configuration
  - The client will query alternative (second) DNS server only if the first one is not reachable (and not if it receives a negative answer)
- The DNS server checks its local cache
- If the entry is not in the cache, the DNS server queries a forwarder
- If no forwarder available, the DNS server uses the Root Hints

Windows client local DNS cache

- Resolved DNS queries stay in the local cache for a time period determined by the zone TTL value on the server
- The **hosts** file
  - Alternative name resolution mechanism
  - Usually located in %systemroot%\system32\drivers\etc folder
  - Not distributed and scalable but can serve as a backup DNS method
  - It has higher priority than DNS resolution
  - The content of the hosts file is constantly copied in the DNS cache

Windows client local DNS cache (2)

- **ipconfig /displaydns**
  - shows the local DNS cache of a Windows computer
- **ipconfig /flushdns**
  - deletes the local DNS cache of a Windows computer
- Remember – the hosts file content is constantly copied in this cache

Recursive and iterative queries

- Recursive query - the DNS server must respond with either
  - the requested resource

    OR
  - Error message (not found)
- Iterative query - the DNS server responds with the best answer it can give

The NSLOOKUP command

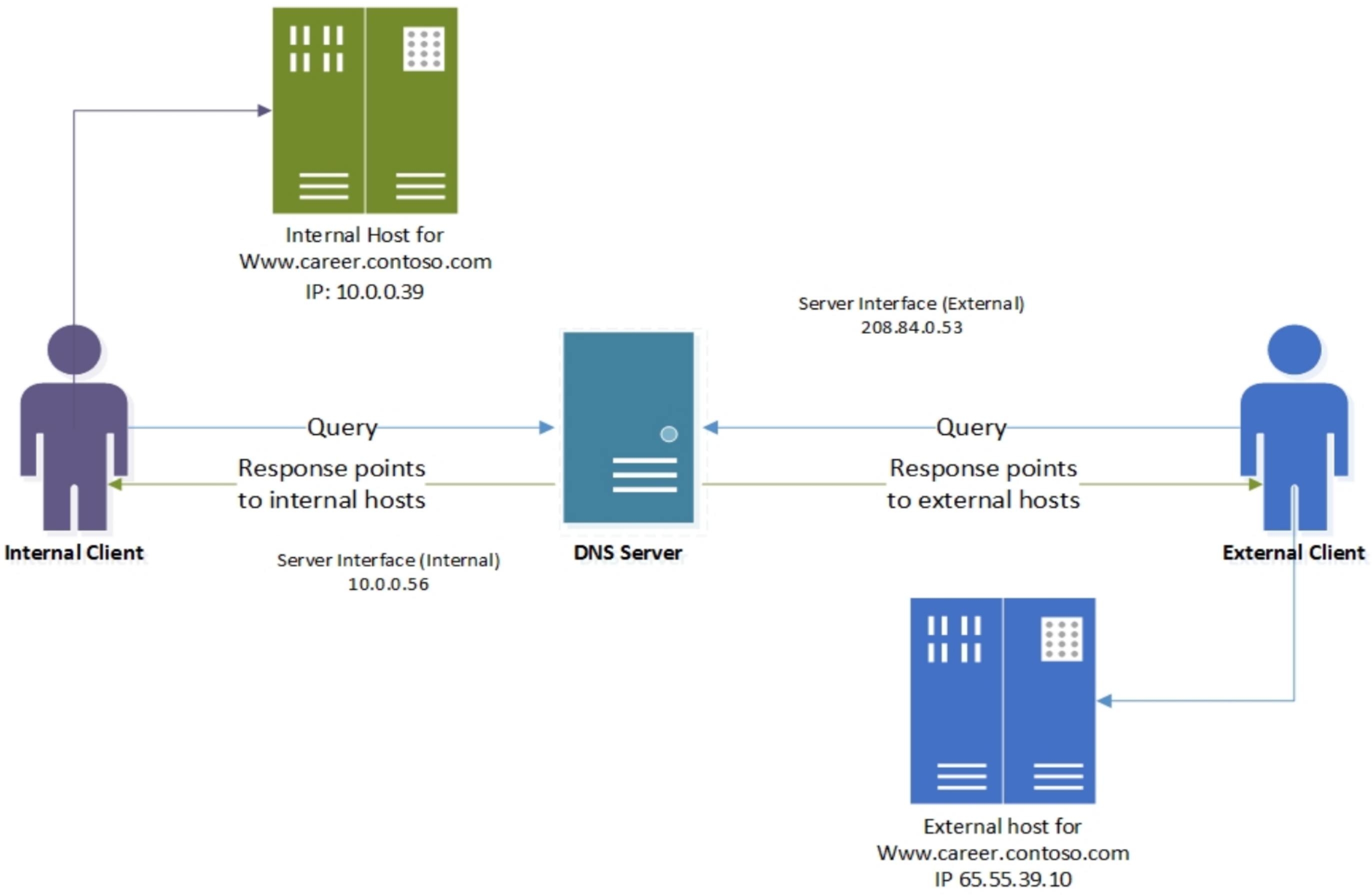
- To check a DNS resolution, one can use **ping** or **nslookup**
  - ping - intuitive to use but can have older and inaccurate info the purpose of ping is not to troubleshoot DNS
  - **nslookup** - useful tool designed for troubleshooting DNS
- Demo: how to use **nslookup** on Windows

Forward and reverse DNS zones

- Forward lookup zone: Name → IP address
- Reverse lookup zone: IP address → Name
- A reverse DNS zone:
    - Can be used for antispam mechanism, logs from applications
    - Require to be created from your ISP (because it manages your IP addresses)

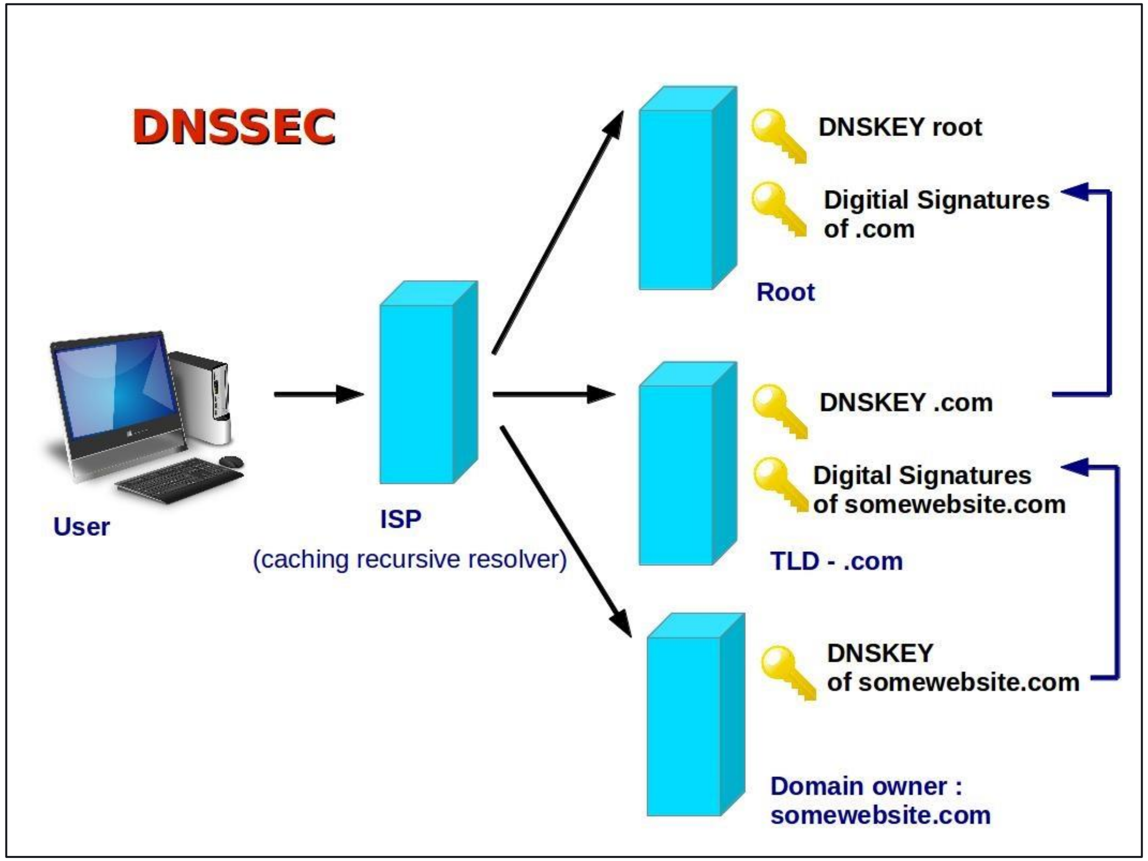
Split-Brain DNS

- Can provide different information depending on the client’s location
- May increase performance and security



DNSSEC (Domain Name System Security Extensions)

- DNS is insecure protocol by design
- When enabled, non-authoritative DNS servers can validate the responses from other DNS servers
- DNSSEC uses public key cryptography to digitally sign authoritative zone data
- …but it is not very popular for different reasons – it is complicated, expensive, incomplete and may create problems like DDoS attacks


DNSSEC
DNSKEY root
Digitial Signatures of .com
Root
DNSKEY .com
Digital Signatures of somewebsite.com
TLD - .com
DNSKEY of somewebsite.com
Domain owner : somewebsite.com
User
ISP
(caching recursive resolver)

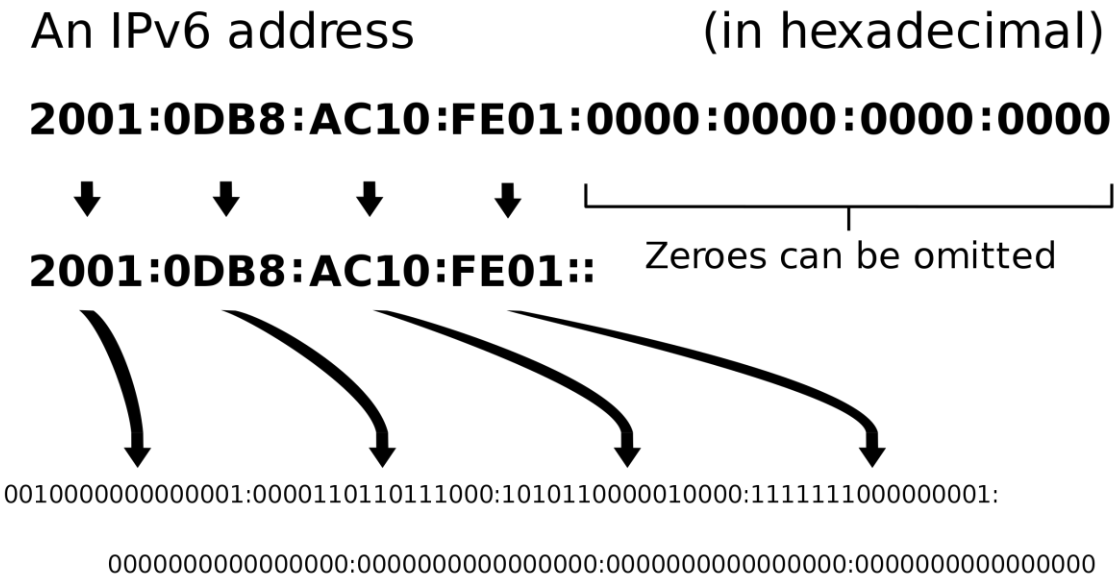
DoT and DoH (DNS over TLS and DNS Over HTTPS)

- Another attempts to implement security in the DNS protocol
- DoH is a proposed standard, published October 2018
- Some common usage scenarios:
  - Use DoH within an application - some browsers have a built-in DoH support and can thus bypass the OS's DNS functionality
  - Install DoH proxy – the client uses the traditional (port 53) DNS to query in the local DNS (central or local proxy)
  - Installing a DoH resolving plugin for the operating system

IPv6

IPv6 introduction

- Larger address space (128 bits rather than 32) or 2^{128}
- Simplified header format
- Improved quality of service and security



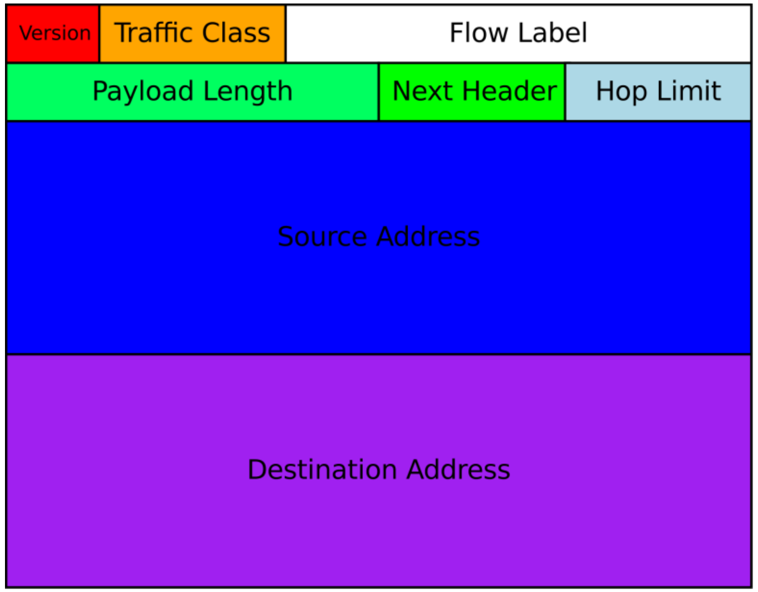
An IPv6 address (in hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

2001:0DB8:AC10:FE01:: Zeroes can be omitted

0010000000000001:0000110110111000:1010110000010000:1111111000000001:

0000000000000000:0000000000000000:0000000000000000:0000000000000000



Version | Traffic Class | Flow Label

Payload Length | Next Header | Hop Limit

Source Address

Destination Address

How big is the IPv6 address space?

- 2^{128} is like $3.4×10^{38}$, which is: 340,282,366,920,938,463,463,374,607,431,768,211,456
- It is 10 million trillion times the total number of grains of sand on all the beaches in the world
- We can assign IPv6 address to every atom on the surface of the Earth, and still have enough addresses left to do another 100+ earths

IPv6 address format

- IPv6 address is represented as eight groups of four hexadecimal digits
- Example:

  2001:0db8:0000:0000:0000:ff00:0042:8132

- Each of this groups has 16 bits and is separated from the others with ":"

IPv4 vs IPv6

- Much (much…) larger address space in IPv6
- A lot of the IP concepts and upper layer protocols remain the same or similar
- In the OSI model, only L3 is different
- No broadcast, no subnetting and no NAT in IPv6!

Abbreviations

- One option - remove the long string with zeros (allowed only once)
  - Original: 2041:0000:140F:0000:0000:0000:875B:031B
  - Short: 2041:0000:140F::875B:031B
- Another option - replace four zeros with one
  - Short: 2041:0000:140F::875B:031B
  - Shorter: 2041:0:140F::875B:031B
- Also, another leading zero can be removed: 031B --> 31B
- The result from the above options:
  2041:0000:140F:0000:0000:0000:875B:031B --> **2041:0:140F::875B:31B**

Abbreviations – other examples

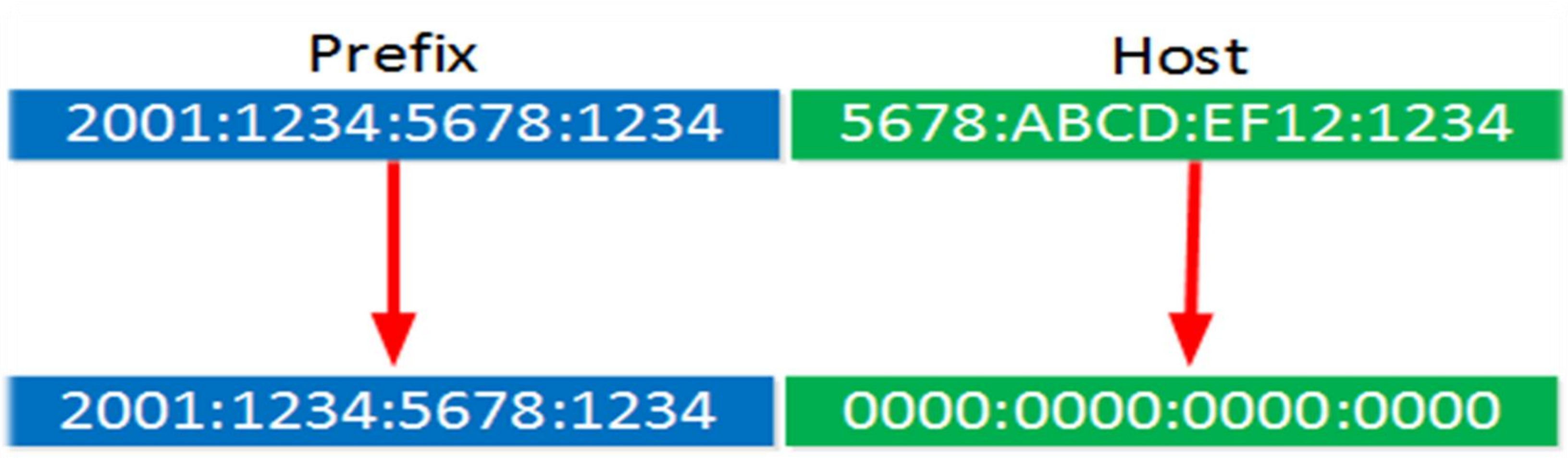
- FF02:0000:0000:0000:0000:0000:0000:0001
  - FF02:0:0:0:0:0:0:1
  - FF02::0:0:0:1
  - FF02:0:0::1
  - FF02::1
- 1234:0000:0000:5678:0000:0000:4321:001
  - 1234::5678:0:0:4321:1
  - 1234:0:0:5678::4321:1
- 0000:0000:0000:0000:0000:0000:0000:0001 (the loopback address)
  - ::1

IPv6 address types

- Unicast - a packet is delivered to one interface
  - Global
  - Reserved
  - Link local (something like APIPA in IPv4)
  - Site local (something like the RFC 1918 private addresses in IPv4, deprecated)
- Multicast - a packet is delivered to multiple interfaces
- Anycast - a packet is delivered to the nearest of multiple interfaces (as defined by the routing protocols in use)

*no more Broadcast in IPv6

IPv6 prefixes



Prefix	Host
2001:1234:5678:1234	5678:ABCD:EF12:1234
2001:1234:5678:1234	0000:0000:0000:0000

2001:1234:5678:1234:0000:0000:0000:0000/64

2001:1234:5678:1234::/64

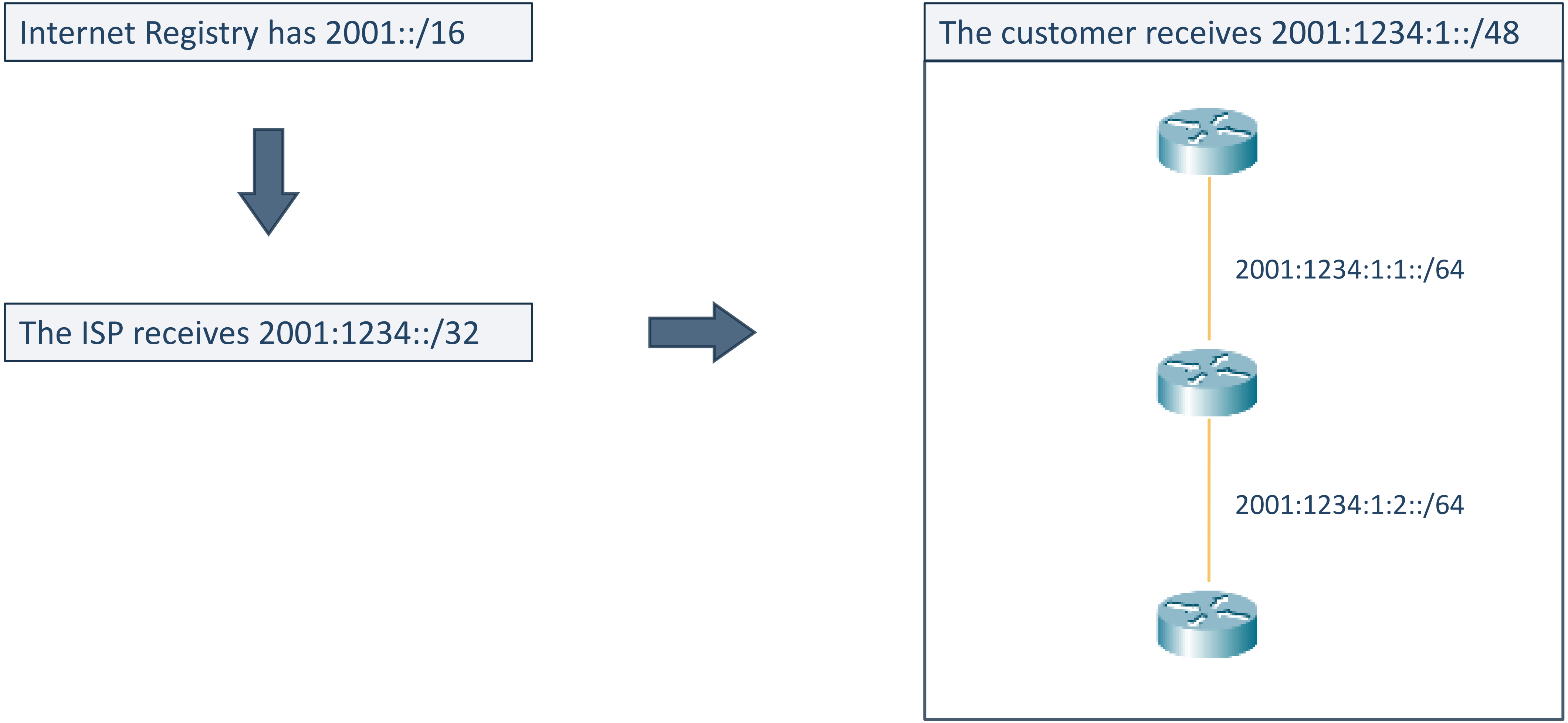
IPv6 global unicast

Network prefix	Interface ID (host)
64 bits	64 bits

Global prefix	Subnet ID	Interface ID (host)
48 bits	16 bits	64 bits
Public/Internet	Customer’s subnets	Interface

- ISP allocates to the customer /48
- The customer allocates /64 to each interface while having 2^{16} (65536) subnets

IPv6 global unicast - example



Internet Registry has 2001::/16

The ISP receives 2001:1234::/32

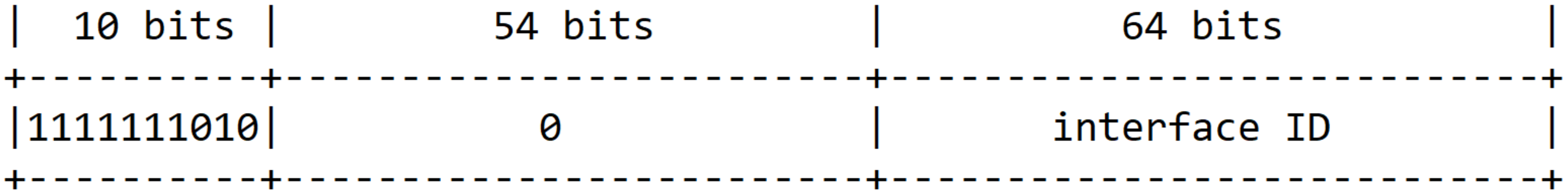
The customer receives 2001:1234:1::/48

2001:1234:1:1::/64

2001:1234:1:2::/64

IPv6 scopes (Unicast)

- Link-local (similar to APIPA in IPv4)
  - Prefix is FE80::/10…(or FE80::/64?)



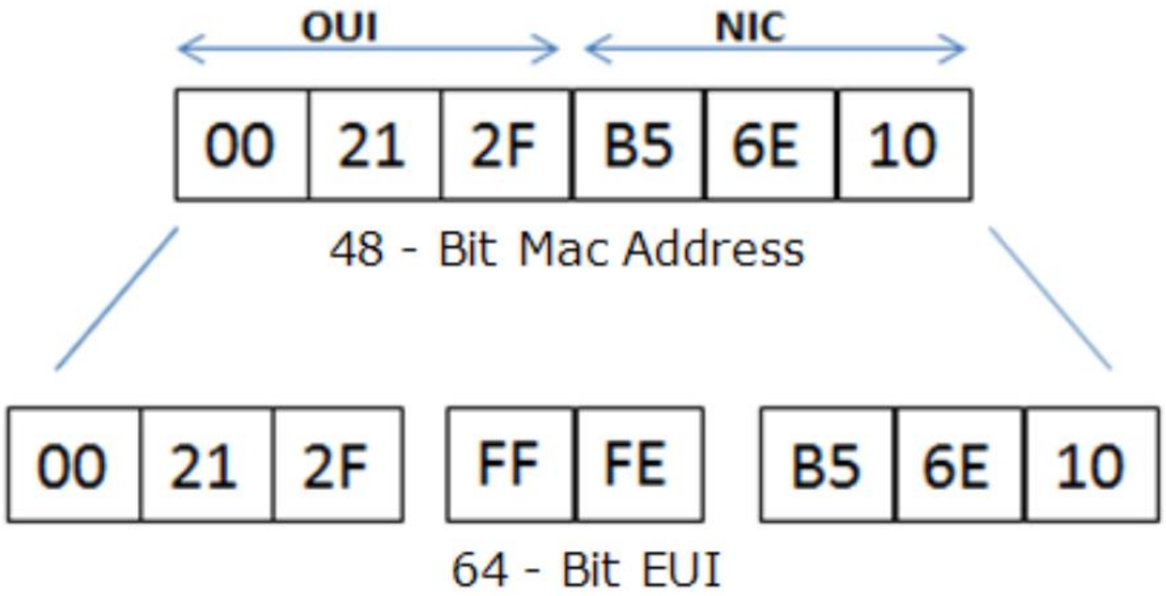
```
|  10 bits |           54 bits           |           64 bits            |
+----------+-----------------------------+------------------------------+
|1111111010|              0              |         interface ID         |
+----------+-----------------------------+------------------------------+
```

- Global (similar to IPv4 public addresses)
  - Typical prefix is 2000::/3

::1/128 - the loopback address is a unicast localhost address

IPv6 EUI-64 bit address

- EUI: Extended Unique Identifier
- One option to auto-assign the second 64 bits to a link-local address using the MAC address of the interface



OUI NIC

00 21 2F B5 6E 10

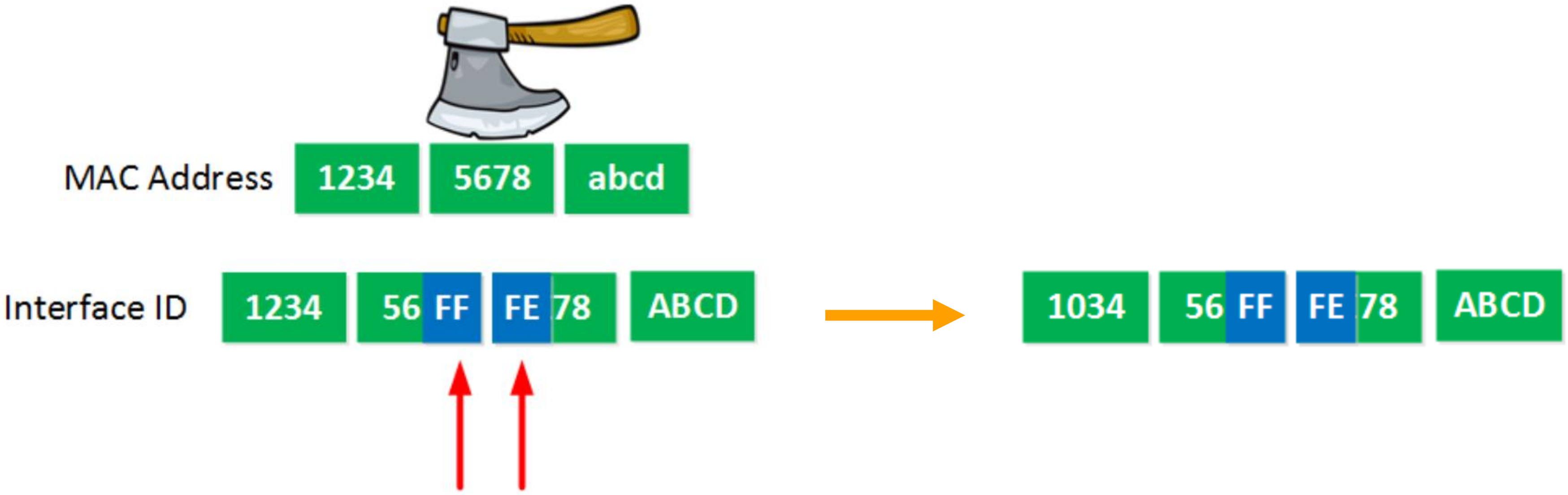
48 - Bit Mac Address

00 21 2F FF FE B5 6E 10

64 - Bit EUI

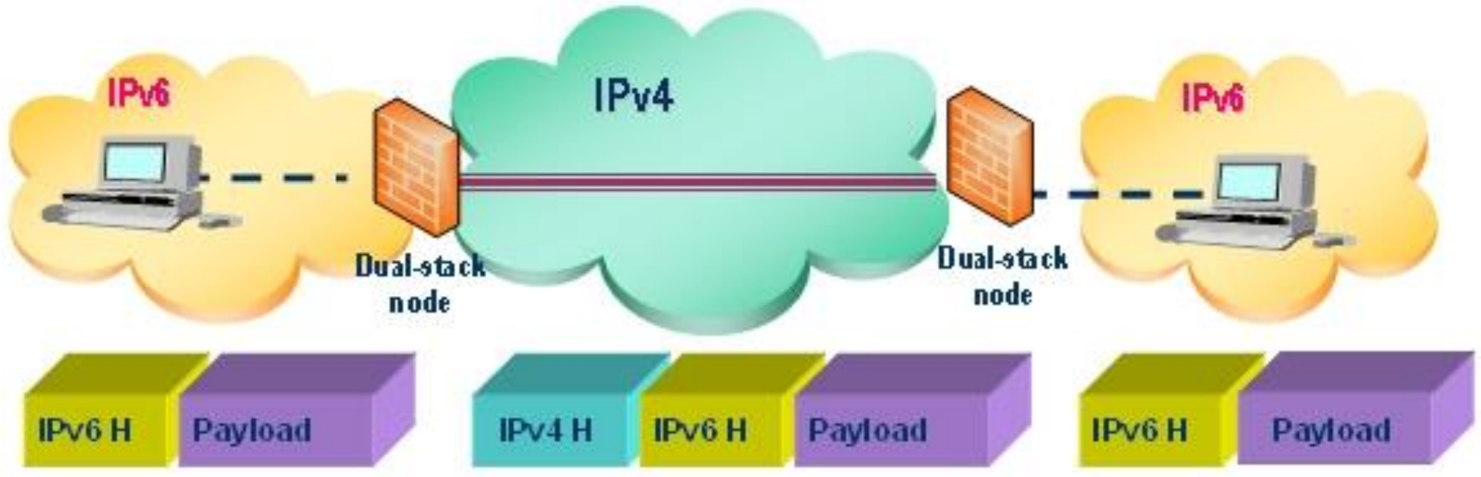
IPv6 EUI-64 bit address (2)

- How the IPv6 EUI-64 address is automatically configured:
  - ✓ Split the MAC address of the interface into two pieces
  - ✓ Insert **FFFE** between the two pieces (to achieve 64 bits)
  - ✓ Invert the 7th bit of the interface ID



IPv6 tunneling

- Encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure
- Different methods exist – 6to4, 6rd, Teredo, ISATAP, etc.



IPv6 SLAAC

Software University

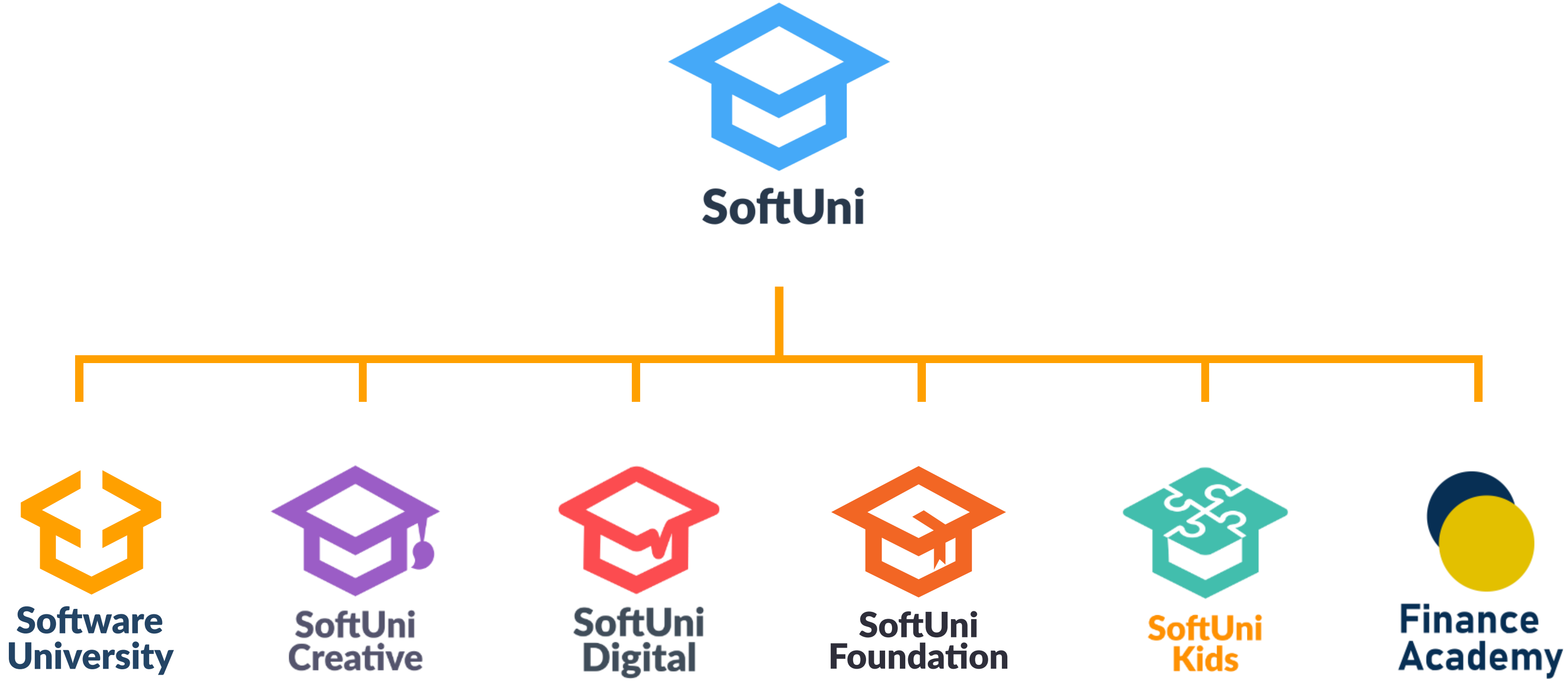
- SLAAC = StateLess Address Auto Configuration
- Designed to be fast and easy alternative to DHCPv6
- IPv6 Neighbor Discovery Protocol (NDP) is like ARP in IPv4
- With SLAAC and NDP, nodes on the network can easily autoconfigure IPv6 address from the correct subnet/prefix
- The problem: with SLAAC there is no assignment for DNS
- SLAAC and DHCPv6 can be used together:
  - the M flag (Managed) specifies if DHCPv6 is needed for IPv6 address
  - the O flag (Other) specifies if DHCPv6 is needed for DNS information

Demonstration

Summary

1. Domain Name System
2. IPv6
3. Demonstration

Questions?



SoftUni

Software University

SoftUni Creative

SoftUni Digital

SoftUni Foundation

SoftUni Kids

Finance Academy

SoftUni Diamond Partners

SmartIT

Coca-Cola HBC Bulgaria

SOFTWARE GROUP

DXC TECHNOLOGY

createX

Postbank

Решения за твоето утре

SUPER HOSTING .BG

DRAFT KINGS

VIVACOM

INDEAVR

Serving the high achievers

AMBITIONED

PHAR VISION

Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Profession and Job for Software Developers
  - softuni.bg, about.softuni.bg
- Software University Foundation
  - softuni.foundation
- Software University @ Facebook
  - facebook.com/SoftwareUniversity
- Software University Forums
  - forum.softuni.bg