Internet: Essential Terms – IP Addresses, DNS, URL; Common Protocols and Services

IP Address

The IP address is a **unique identifier of a networking device**, which works on the 3rd or higher level of OSI model.

It is a series of 0s and 1s – their count depends on the version of the IP protocol:

IPv4 – IP version 4

- 1st version of the IP protocol, which was widely adopted in networking.
- Length: 32 bits (= 4 B)
- Representation: 4 decimal numbers separated by dots – each number represents the value of 1 Byte, e.g.:

11000000101010000001001000010110

11000000 10101000 00010010 00010110

192 168 18 22

192.168.18.22

- 1 Byte – it can store numbers from 0 to 255 only – these are the only values permitted for each IPv4 field.
- There 2 groups of IP addresses[1]:
  - **Public** – A public IP address is any valid address, or number, that can be accessed over the Internet. Internet standards groups, such as the Network Information Center (NIC) or the Internet Assigned Numbers Authority (IANA), are the organizations responsible for registering IP ranges and assigning them to organizations, such as Internet Service Providers (ISPs).
  - **Private** - A private IP address is any number or address assigned to a device on a private TCP/IP Local Area Network that is accessible only within the Local Area Network. For a resource inside the Local Area Network to be accessible over the Internet, a device within the Local Area Network must be connected to the Internet with a public IP address, and the networking must be appropriately configured. The same Internet standards organizations have reserved the following three IP address ranges that will never be registered publicly:
    - 10.0.0.0 – 10.255.255.255
    - 172.16.0.0 – 172.31.255.255
    - 192.168.0.0 – 192.168.255.255
  - The private network addresses can be repeatedly used in any private LAN (home, office, school etc.)
  - These 2 groups were established to solve one inconvenient problem: IPv4 supports 2^{32} addresses – i.e. almost 4,3 billion addresses. When the IPv4 was designed, it seemed to be sufficient for very long time; however, nowadays there are far more devices connected than the previously mentioned number. The repeated use of

[1] Source: http://supportcenter.verio.com/KB/questions.php?questionid=655

private addresses prevents that address exhausting, but it brings many technical difficulties and limitations of the use.

IPv6 – IP address version 6

- Newer and longer identifier of the network devices and definitive solution (perhaps) of the IPv4 limitations.
- Length: 128 bits
- Available addresses: 2^{128} – approximately 3,4 . 10^{38} addresses
- Representation:
    - 128 bits = 16 B → each byte is represented in hexadecimal system – 32 hexadecimal digits, grouped by 4 digits →8 groups separated by colon (:)
    - Example:

```
FE80:0000:0000:0000:0202:B3FF:FE1E:8329
```

- IPv6 usage is increasing, but it is still a fraction of the Internet traffic (e.g. the Google servers were visited by 3 % of users over IPv6 in February 2014).

Subnet Mask

- If the network devices want to communicate, they have to know IP addresses of the source and destination. If they are in the same network, the communication can be direct; however, if they are in different networks, they have to pass the data to routers.

- *Problem: how do the computers know, if they are in the same network or not?*

- Solution: split the address into 2 parts:
    - **Network ID = NETWORK PREFIX** – the same for computers in the same network
    - **Host ID** – identification of the device in the network
- Tool: **network mask** – it splits the network address into 2 parts:

IP address:	110000001010100000	01001000010110
Mask:	111111111111111111	00000000000000
	Network ID	Host ID

    - The number of bits from the IP address, which represent the network, is indicated by the series of 1s in the mask; then there are 0s only for the part, which represents the host ID.
    - The mask in IPv4 may have the form of IPv4 address – **dot-decimal notation**:

11111111	11111111	11000000	00000000
255	255	192	0

255.255.192.0

    - Another option: IP address is followed by the count of 1s (after the slash) – **CIDR notation**, e.g.:

IP address:	110000001010100000	01001000010110
Mask:	111111111111111111	00000000000000

192.168.18.22**/18**

Exercises

1. A DHCP server assigned your device this IP address: 192.168.32.39/27.
    a. What is the subnet mask in the dot-decimal notation? [*255.255.255.224*]
    b. What is the LAN network prefix? [*192.168.32.32*]
    c. What is the first usable IP address? [*192.168.32.33*]

d. What is the last usable IP address? [*192.168.32.62*]

e. What is the broadcast address? [*192.16 8.32.63*]

2. A network already comprises 12 devices with IP addresses. How many new devices can be connected, if the subnet mask is defined as follows: 255.255.255.192? [62]

Domains and Domain Name System

IP addresses are difficult to remember; much easier is to remember words – textual addresses are better for human beings → **domain names,** which identify so called **hosts,** i.e. individual computers on the net.

Examples of domains

- ***google.com***
- ***www.facebook.com***
- ***moodle.gymcadca.sk***
- ***www.fri.uniza.sk***

Domain names must be **unique** – that is assured by organisations, which manage domain names

The domain names form a hierarchy – **domain name system**. It is a tree structure, which has multiple levels:

1. Top level domains – put at the end of the domain name as the suffix; there are two groups
   a. *Generic top-level domains* – indicate purpose (e.g. `.com, .gov, .mil, .info` etc.)
   b. *Country code top-level domains* – indicate country (e.g. `.sk, .de, .au, .pl, .to` etc.)
2. Second level domains – directly to the left of the top level domains; they are managed by **domain name registrars**
3. Third and higher level **–** managed by the domain holder

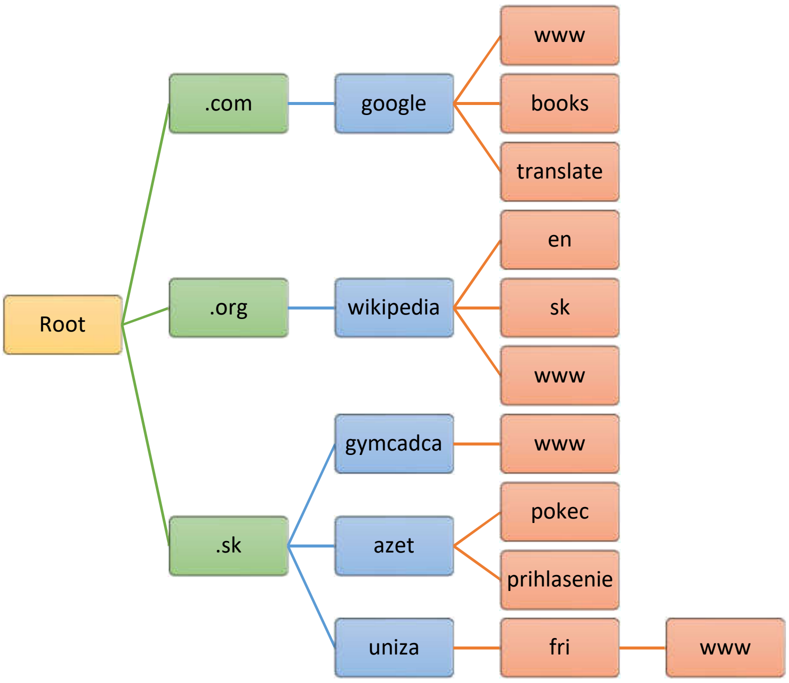


Figure 1: Sample of the DNS hierarchy

The absolute name relating to all the node labels of a tree structure, separated by dots, and **finished by a final dot** is called the ***FQDN address (Fully Qualified Domain Name)***. The maximum depth of the tree structure is 127 levels and the maximum length of a FQDN name is 255 characters. The FQDN address makes it possible to uniquely locate a machine on the network of networks. So WWW.COMMENTCAMARCHE.NET. or WWW.GYMCADCA.EU. is an FQDN address.

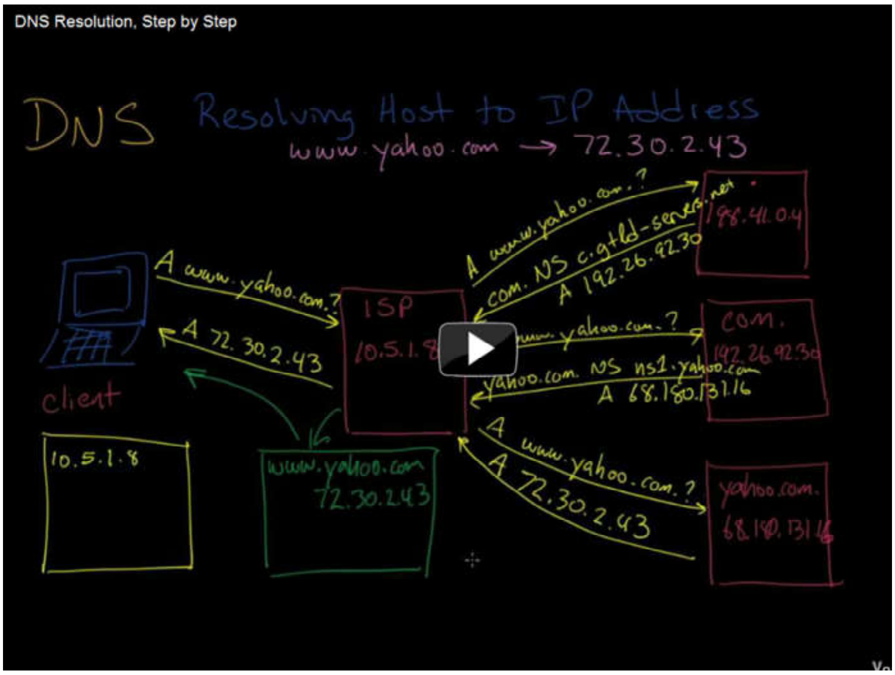
Task 1

- *Find the name of the organization, which manages the Slovak domain (.sk).*
- *Find the name of the organization, which manages the top-level domains.*
- *Find out who is the holder of* www.slovnik.sk .

Results:

Domain Name Service (DNS)

- There must be a translator between IP addresses and domain names – **domain name service (DNS)** https://www.youtube.com/watch?v=3EvjwlQ43_4



- The results of the DNS can be overridden by HOSTS– a file, which is checked BEFORE the DNS is contacted (Typical Windows 7 location: *C:\Windows\System32\drivers\etc\hosts*). Any change of the file can disable access to websites. Normally it can be modified by administrators only – if somebody (a “hacker”) or something (malware like a Trojan horse) gains access to that file, it can redirect users to fake websites.

Task 2

- *Get the IP address of your DNS server.*
- *Change the DNS server used on your computer.*

Some popular DNS servers:

Google DNS

- 8.8.8.8
- 8.8.4.4

OpenDNS:

- 208.67.222.222
- 208.67.220.220

ScrubIT:

- 67.138.54.100
- 207.225.209.66

The *DNSChanger Trojan Horse*, also known as OSX.RSPlug.A and OSX/Puper, and OSX/Jahlav-C, has been found on numerous pornographic websites disguising itself as a video codec. Once downloaded and installed, DNSChanger changes the DNS settings on the computer, redirecting websites entered by the user to malicious sites. If personal information is entered on these malicious websites, it can lead to identity theft.

URL

- Domain name identifies a host only – it does not specify its specific service or location –those are identified by **Uniform Resource Locator (URL)**
- The URL consist of these parts (in fact it is simplified)
  - the type of **protocol** used to access the file (e.g., HTTP or HTTPS for a Web page, ftp for an FTP site; mailto for emails);
  - the **domain name** or **IP address** of the host;
  - (optionally) the **pathname** to the resource (i.e., description of the resource location).

URL Structure

http://	en.wikipedia.org	wiki	Earth
Protocol Identifier (what it is and how to process it)	**Domain name** (the place, where the page or file resides)	**Path** (where on the host is the resource)	**Resource** (its name)
ftp:// https://	**www.google.com**	**/mobile/products/**	**mail.htm**

ISP

An **Internet service provider** (**ISP**) is a company that offers its customers an access to the Internet. The ISP connects to its customers using a data transmission technology appropriate for delivering TCP/IP data, such as

- dial-up,
- DSL (mostly Asymmetric DSL (ADSL) – downstream is greater than upstream, so the download is faster than the upload),
- cable modem (e.g. in cable TV networks),
- wireless connections
  - mobile phone networks (GPRS/EDGE, 3G – HSDPA/HSUPA, LTE)
  - Wi-Fi
  - Satellite

Well-known Slovak ISPs: Slovak Telekom, Orange, SWAN, UPC, Slovanet, Antik, Satro

Common Services/protocols

Protocol = a set of rules used in the communication among computers

1 HTTP

Hypertext Transfer Protocol (**HTTP**) is an application-level protocol for distributed hypermedia information systems. Its use for retrieving inter-linked resources, called **hypertext documents**, led to the establishment of the **World Wide Web** in 1990 by English physicist Tim Berners-Lee. There are two major versions:

- HTTP/1.0 that uses a separate connection for every document, and
- HTTP/1.1 that can reuse the same connection to download, for instance, images for the just served page. Hence HTTP/1.1 may be faster as it takes time to set up such connections

HTTP is a request/response standard as is typical in client-server computing.

- The client is an application (e.g. web browser, spider of a search engine etc) on the computer used by an end-user;
- The server is an application running on the computer hosting the web site (e.g. Apache web server).

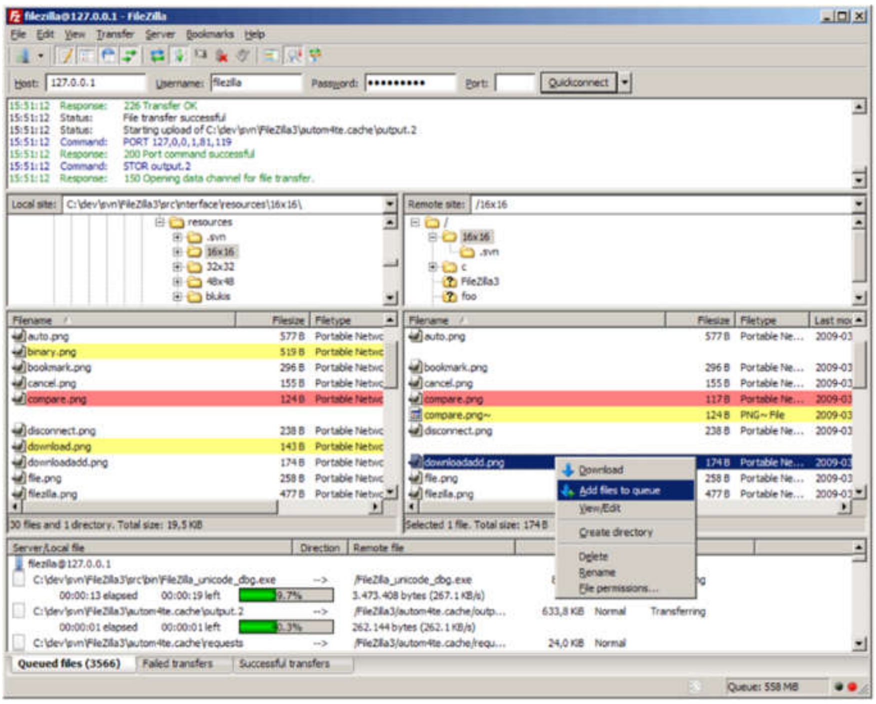
2 FTP

File Transfer Protocol (**FTP**) is a standard network protocol used to exchange and manipulate files over a TCP/IP based network, such as the Internet. FTP is built on a client-server architecture. Applications were originally interactive command-line tools with standardized command syntax, but graphical user interfaces have been developed for all desktop operating systems in use today (e.g. FileZilla).

FTP is used to:

- share files (computer programs and/or data);
- shield a user from variations in file storage systems among different hosts (it is not important, if the accessed system uses FAT or NTFS or POSIX file system like ext3);
- transfer data reliably, and efficiently.

Example of the use: transfer of files and folders, which comprise a website, to a web server.



filezilla@127.0.0.1 - FileZilla

Host: 127.0.0.1 Username: filezilla Password: •••••••••• Port:

```
15:51:12  Response:  226 Transfer OK
15:51:12  Status:    File transfer successful
15:51:12  Status:    Starting upload of C:\dev\svn\FileZilla3\autom4te.cache\output.2
15:51:12  Command:   PORT 127,0,0,1,81,119
15:51:12  Response:  200 Port command successful
15:51:12  Command:   STOR output.2
15:51:12  Response:  150 Opening data channel for file transfer.
```

Local site: C:\dev\svn\FileZilla3\src\interface\resources\16x16\

Remote site: /16x16

Filename	Filesize	Filetype
auto.png	577 B	Portable Netwc
binary.png	519 B	Portable Netwc
bookmark.png	296 B	Portable Netwc
cancel.png	155 B	Portable Netwc
compare.png	124 B	Portable Netwc
disconnect.png	238 B	Portable Netwc
download.png	143 B	Portable Netwc
downloadadd.png	174 B	Portable Netwc
file.png	258 B	Portable Netwc
filezilla.png	477 B	Portable Netwc

30 files and 1 directory. Total size: 19,5 KiB

Filename	Filesize	Filetype	Last mo
auto.png	577 B	Portable Ne...	2009-03
bookmark.png	296 B	Portable Ne...	2009-03
cancel.png	155 B	Portable Ne...	2009-03
compare.png	117 B	Portable Ne...	2009-03
compare.png~	124 B	PNG~ File	2009-03
disconnect.png	238 B	Portable Ne...	2009-03
downloadadd.png	174 B	Portable Ne...	2009-03
file.png	258 B	Portable Ne...	2009-03
filezilla.png	477 B	Portable Ne...	2009-03

Selected 1 file. Total size: 174 B

```
Server/Local file                                   Direction  Remote file
filezilla@127.0.0.1
C:\dev\svn\FileZilla3\src\bin\FileZilla_unicode_dbg.exe   -->  /FileZilla_unicode_dbg.exe
   00:00:13 elapsed   00:00:19 left   9.7%              3.473.408 bytes (267.1 KB/s)
C:\dev\svn\FileZilla3\autom4te.cache\output.2             -->  /FileZilla3/autom4te.cache/outp...   633,8 KiB  Normal  Transferring
   00:00:01 elapsed   00:00:01 left   0.3%              262.144 bytes (262.1 KB/s)
C:\dev\svn\FileZilla3\autom4te.cache\requests             -->  /FileZilla3/autom4te.cache/requ...   24,0 KiB   Normal
```

Queued files (3566)

Queue: 558 MiB

3 POP3

(**P**ost **O**ffice **P**rotocol **3**)

It is a standard interface between a user's e-mail program and the mail server. POP3 and IMAP4 are the two common mailbox access protocols for e-mail clients such as Outlook, Mail, Eudora and Thunderbird.

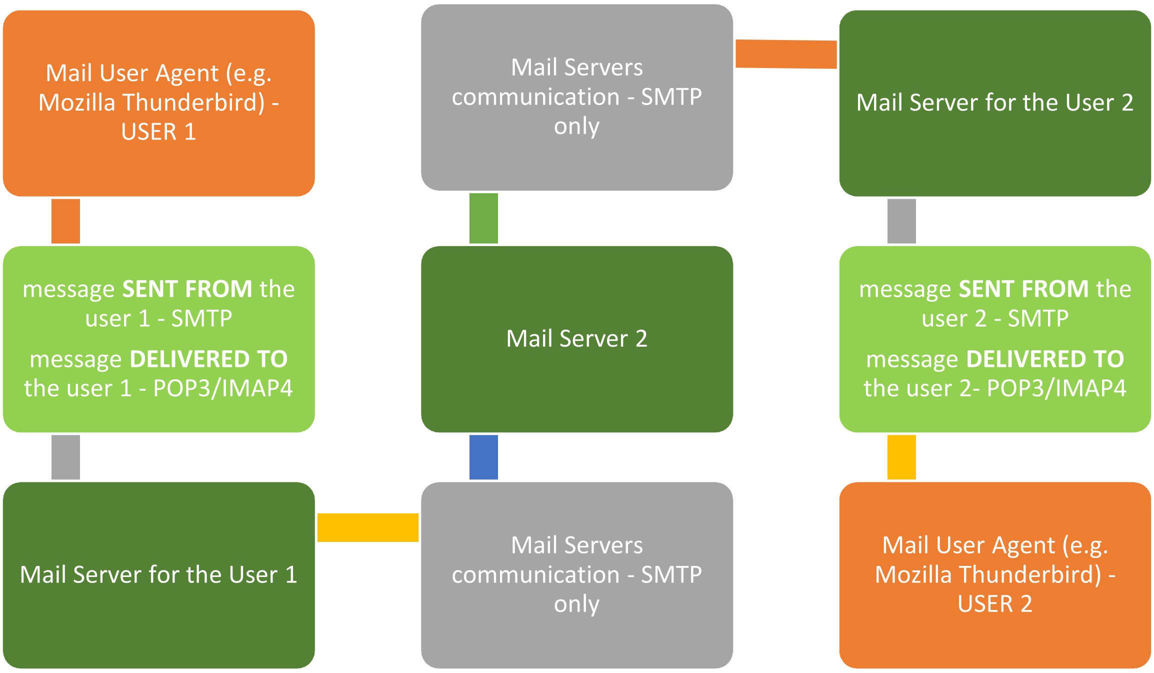
POP3 is a simple system. Incoming messages and attachments are downloaded when users check their mail. A message cannot be downloaded until its predecessor is fully downloaded (and usually also deleted from the mail server). This is its worst feature, which limits its use, esp. in case of data limited connections (mobile carrier connections with limited data plan).

4 IMAP

This protocol has the same purpose as POP3; however, it retrieves only email headers. The message is fully downloaded only if it is open in the client application. This attitude saves data, on the other hand the messages are unavailable in the offline state.

5 SMTP

(**S**imple **M**ail **T**ransfer **P**rotocol) SMTP defines the message format and the message transfer agent (MTA), which stores and forwards the mail. SMTP was originally designed for only plain text (ASCII text), but MIME and other encoding methods enable executable programs and multimedia files to be attached to and transported with the e-mail message. SMTP servers route SMTP messages throughout the Internet to a mail server that provides a message store for incoming mail. The mail server uses the POP3 or IMAP4 access protocol to communicate with the user's e-mail program.



Mail User Agent (e.g. Mozilla Thunderbird) - USER 1

Mail Servers communication - SMTP only

Mail Server for the User 2

message **SENT FROM** the user 1 - SMTP

message **DELIVERED TO** the user 1 - POP3/IMAP4

Mail Server 2

message **SENT FROM** the user 2 - SMTP

message **DELIVERED TO** the user 2- POP3/IMAP4

Mail Server for the User 1

Mail Servers communication - SMTP only

Mail User Agent (e.g. Mozilla Thunderbird) - USER 2