Computer Networks

Selected Network Services and Applications

ICMP Echo-Request

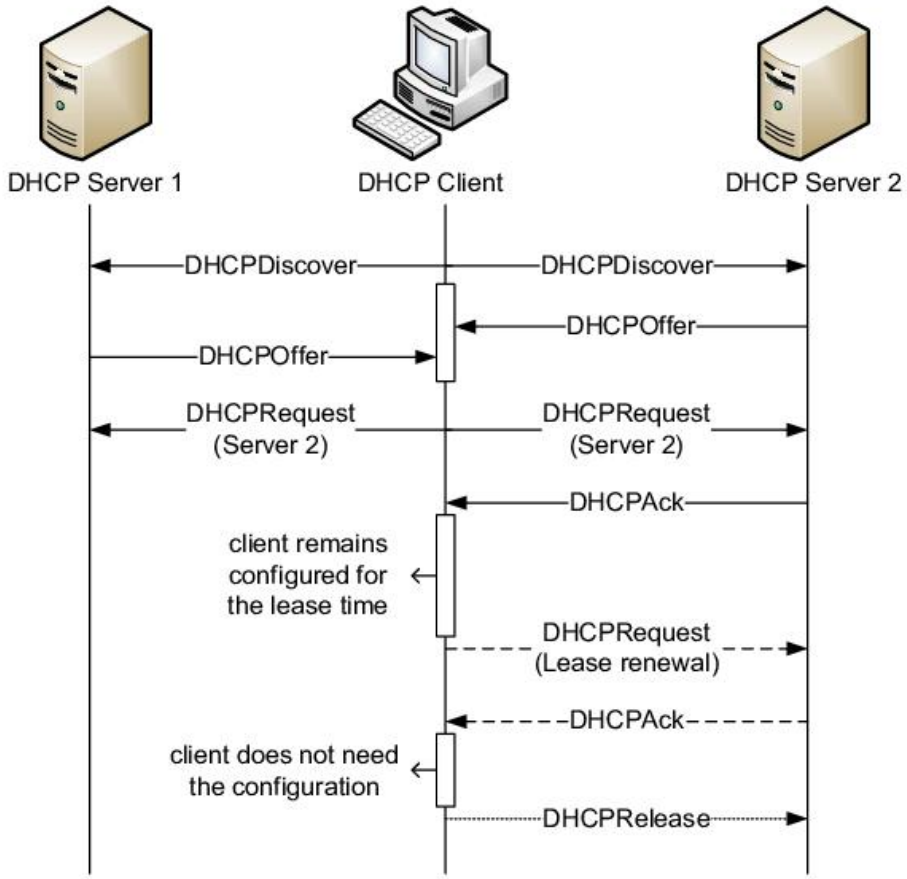
- Aka PING request
- Very useful service, typically enabled
- Allows for host availability check
- In typical packet sequence of ASCII chars is being sent

```
10:30:20.398198 IP 192.168.1.1 > 192.168.1.8: ICMP echo request, id 25968, seq 1, length 64
E..T.j@.@.............<.ep..,.  `....[..................... !"#$%&'()*+,-./01234567
18:30:20.398512 IP 192.168.1.8 > 192.168.1.1: ICMP echo reply, id 25968, seq 1, length 64
E..Tg.....x...........D.ep..,.  `....[..................... !"#$%&'()*+,-./01234567
10:30:43.118615 IP 192.168.1.1 > 192.168.1.8: ICMP echo request, id 26017, seq 1, length 108
E...)V@.@.............e...C.  `....=..................... !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abc
10:30:43.118889 IP 192.168.1.8 > 192.168.1.1: ICMP echo reply, id 26017, seq 1, length 108
E...g.....x.............e...C.  `....=..................... !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abc
10:30:53.881804 IP 192.168.1.1 > 192.168.1.8: ICMP echo request, id 26039, seq 1, length 148
E...8"@.@.............-.e...M.  `....tt..................... !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~.....
10:30:53.882086 IP 192.168.1.8 > 192.168.1.1: ICMP echo reply, id 26039, seq 1, length 148
E...g.....x...........5.e...M.  `....tt..................... !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~.....
```

DHCP/DHCPv6

- DHCP – Dynamic Host Configuration Protocol
- An improvement of stateless BOOTP protocol
- Allows for obtaining crucial and additional parameters of IP stack
  - IP address
  - IP netmask/prefix length in case of IPv6
  - default gateway
  - DNS name servers
- Tens of additional parameters defined as well-known: NTP, WINS, servers e.g.

DHCP/DHCPv6 mode of action



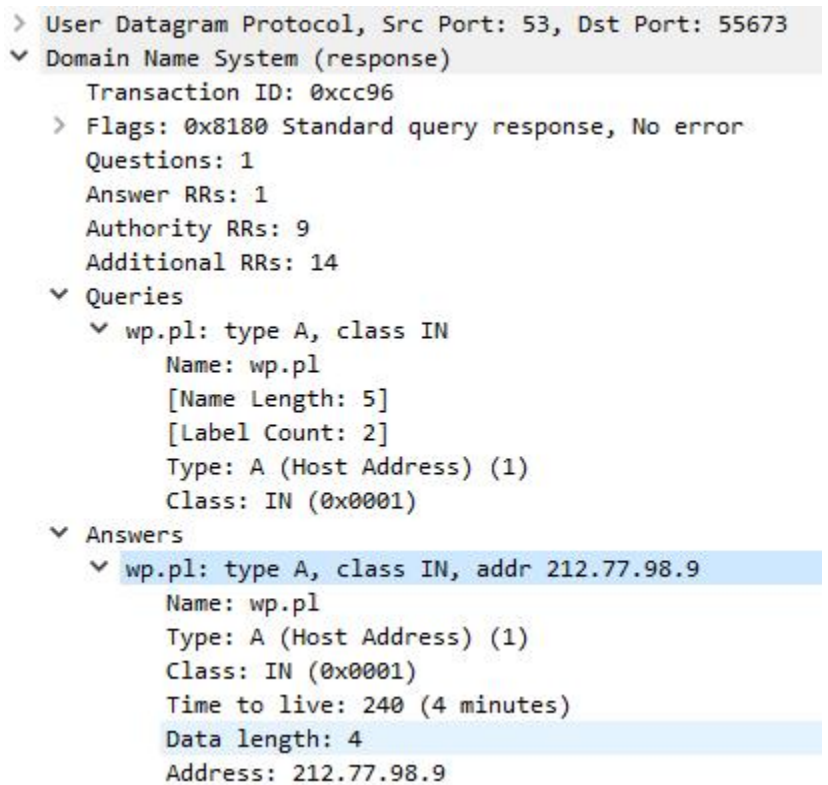
DHCP/DHCPv6

- Works in stateful mode – server is aware of the time the so-called lease has been contracted
- Before the lease expires, client has to renew it in order to keep the parameters (especially the IP address) in use
- Typically the following messages are in use:
  - Discover – discover what servers are available (broadcast)
  - Offer – servers send offers to the client (unicast)
  - Request – client approves the offer (unicast, sometime broadcast to make others aware)
  - ACK – Acknowledge – server agrees to client's request
  - Release – client no longer uses the IP lease, the address gets back to the pool
  - NAK – No acknowledge – neglection to lease specific address, potentially in use
- In some cases server also makes request to DNS server to make network aware of client's domain name – the availability to resolve client's current IP address

DNS

- The most widespread network service
- Used at almost every network resource query
- One of good examples of a distributed database forming a hierarchy of servers
  - no server knows all the answers (unlike the BGP Tier-1 routers e.g.)
  - two generaly types of server are used:
    - caching server – just to speed up the answers to the clients
    - authoritative server – the one keeping absolute knowledge on specific domain (e.g. pg.gda.pl)
- Organized into so-called resource records (RRs) – tens of types defined
- Typically oriented in providing the so-called Forward records:
  - record A containing the IP address of a specific domain name in query

DNS – example response

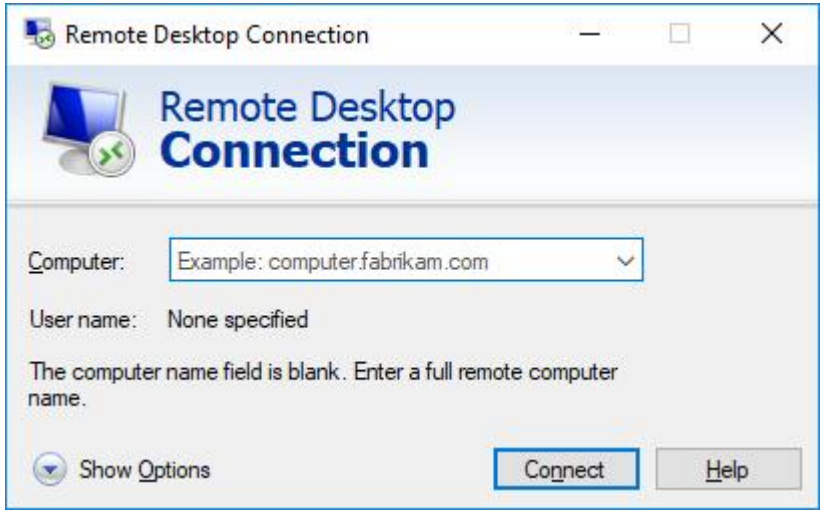


DNS – popular records

- Although the general number of record types is large (under one hundred) and counting, majority of queries use only small subset:
  - A – for IPv4 address retrieval
  - AAAA – for IPv6 address retrieval
  - PTR – for so-called reverse lookups – query contains address, domain name is an answer
  - MX – for Mail eXchange servers for domain
  - SOA – for querying which server is responsible for specific domain
  - CNAME – an alias for an existing record, typically record A

Remote Desktop Protocol

- aka RDP, Remote Desktop
- Microsoft's proprietary protocol, although open-source implementations exist
- works over both the 3389/TCP (typical scenarios) and 3389/UDP
  - UDP employed in special cases whenever delay optimization is possible
- provides access to graphical terminal of a computer system
- Does not send the whole screen every time, optimizes bandwidth due to high system integration
- Not only screen updates are sent, many other functionalities provided – printing, USB sharing, Crypto-card sharing etc.



Remote Desktop

- Early versions and implementations of the protocol had several security flaws:
  - either did not change encryption key for consecutive keypresses – statistical attack was possible
  - or used hard-coded private key for server side – MitM was possible without user notice
- Current version makes use of certificates on server side and manages the symmetric keys properly
  - this minimizes the risk of spoofing the server and statistical attacks

VNC

- RDP-like implementation of graphical computer access
- Many implementation exist
  - they differ in support for encryption and authentication mechanisms
  - free and payed versions available
  - available for almost all platforms including mobile ones
- Does not provide so high bandwidth optimizations, but compensates with versatility

HTTP

- Hyper-Text Transfer Protocol
  - Hyper-text – text plus multimedia content (bitmaps, animations, sound)
  - formerly RFC2616 + RFC2145 (~1999)
  - curently (~2014)
    - "Message Syntax and Routing" [RFC7230]
    - "Semantics and Content" [RFC7231]
    - "Conditional Requests" [RFC7232]
    - "Range Requests" [RFC7233]
    - "Caching" [RFC7234]
    - "Authentication" [RFC7235]
- second most used (after the DNS) Internet protocol
- belongs to application-layer protocol
- provides, among other things, session management
  - cookies, session ones
  - allow for distinction of different called subpages inside complex web application

HTTP/2 and beyond

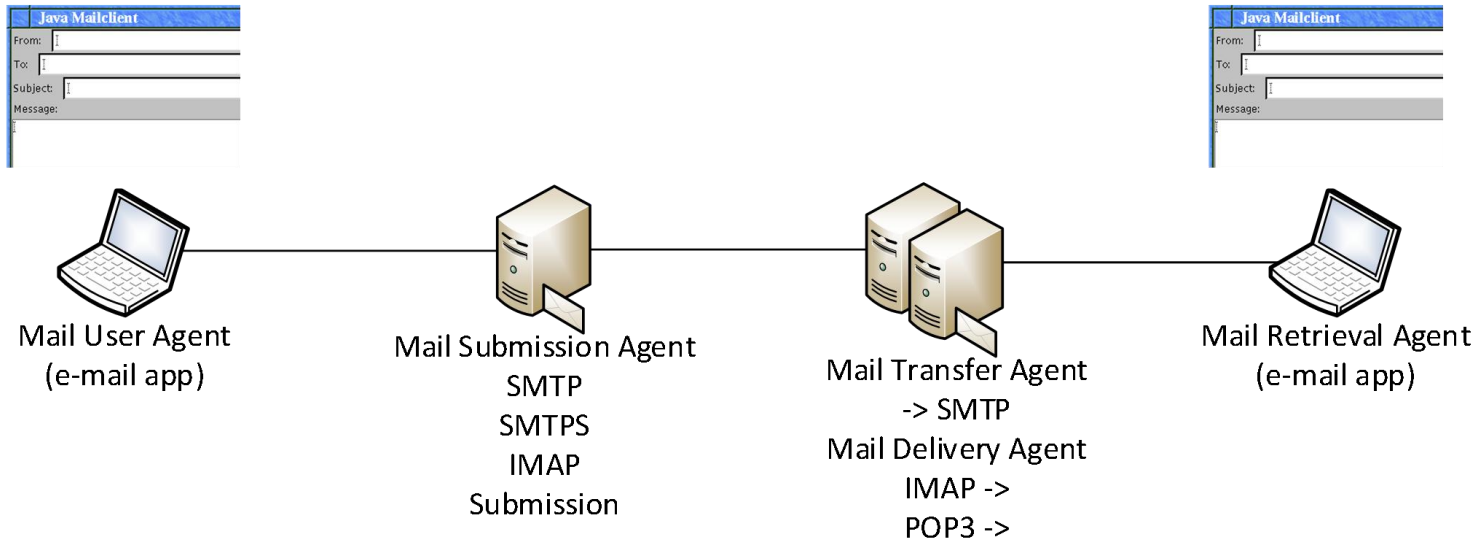
- not to mistake with Web 2.0 which stands for other than page-access use of newer (web) applications, where content is provided mostly by the users
- RFC7540 (~2015)
  - firstly defined as Google’s proprietary protocol SPDY (pronounced SPeeDY)
  - compression of not only content, but also headers
  - offers aggregated transport of multiple page components in single connection
  - offers possibility to multiplicate connections to speed up page loading

HTTP/2 and beyond

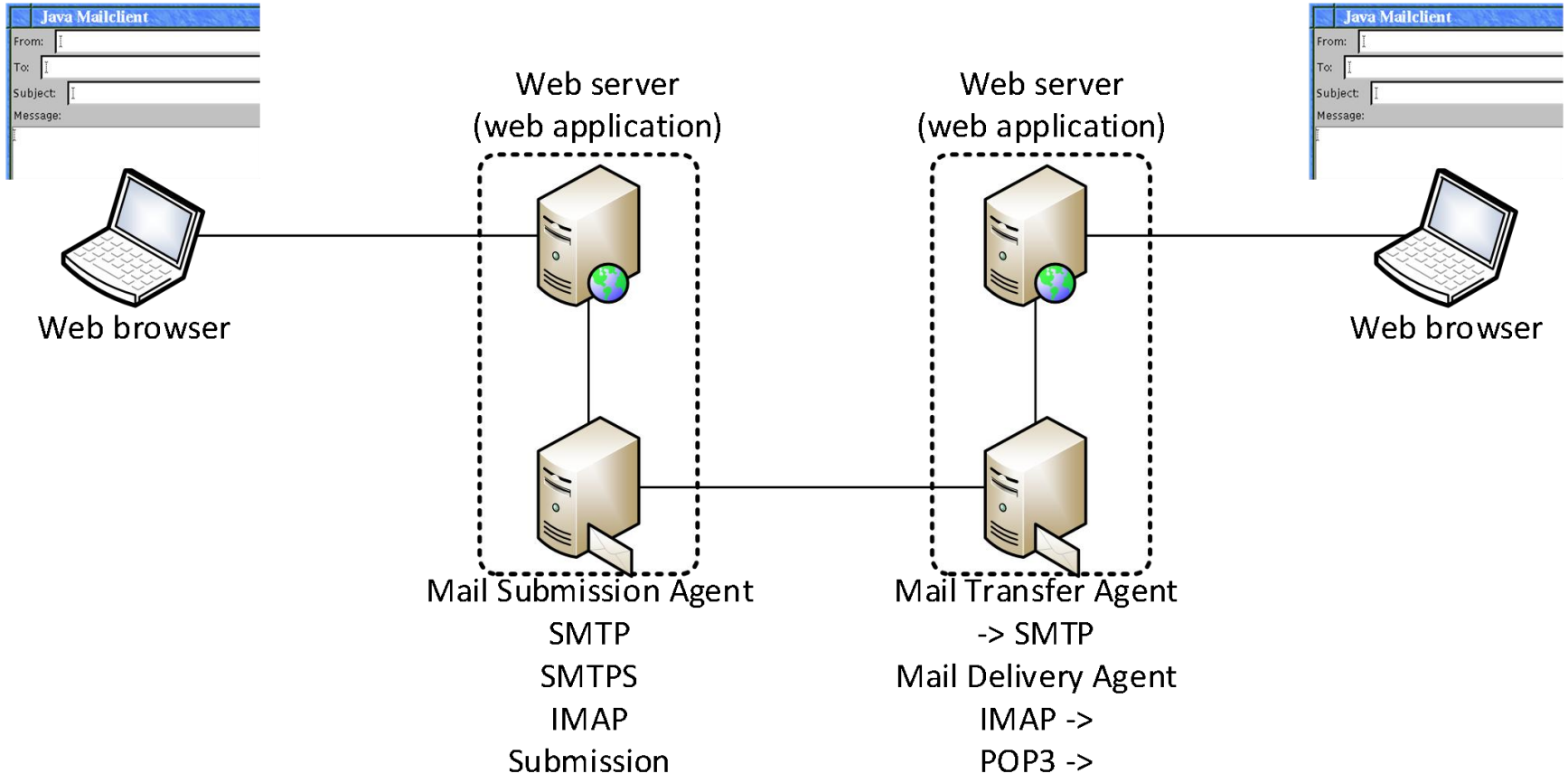
- Possibility to propose alternative protocols with popular browsers
- QUIC – an alternative to HTTP, by Google once again (~2012)
  - sometimes revealed to Quick UDP Internet Connections
  - Internet Draft – no standard yet, although IETF has accepted the document
  - re-implements reliable transport over unreliable UDP protocol (as a replacement to TCP)
  - exhibits lowered latency compared to typical HTTP over TCP applications – not necessarily deprecating the TCP itself
  - simplifies (shortens) authentication phase which affects session initiation speed compared to typical TLS
  - stated to be versatile transport protocol – not to be mistaken with the transport layer itself

E-mail

- In typical scenario several entities are distinct in mail operations:
  - source client (Mail User Agent – a computer application)
  - source provider (Mail Submission Agent – service running on a server)
  - destination provider (Mail Transfer Agent – service running on another server)
  - destination client (Mail Retrieval Agent – a computer application



E-mail available via web interface



E-mail – typical ports used

- SMTP – Simple Mail Transfer Protocol
  - 25/TCP plaintext and S-SMTP
  - 465/TCP – SMTPS
- IMAP – Interactive Mail Access Protocol
  - 143/TCP plaintext and encrypted
  - 993/TCP – IMAPS
- POP3 – Post Office Protocol, v3
  - 110/TCP – plaintext
  - 995/TCP – POP3S
- Submission
  - 587/TCP – plaintext