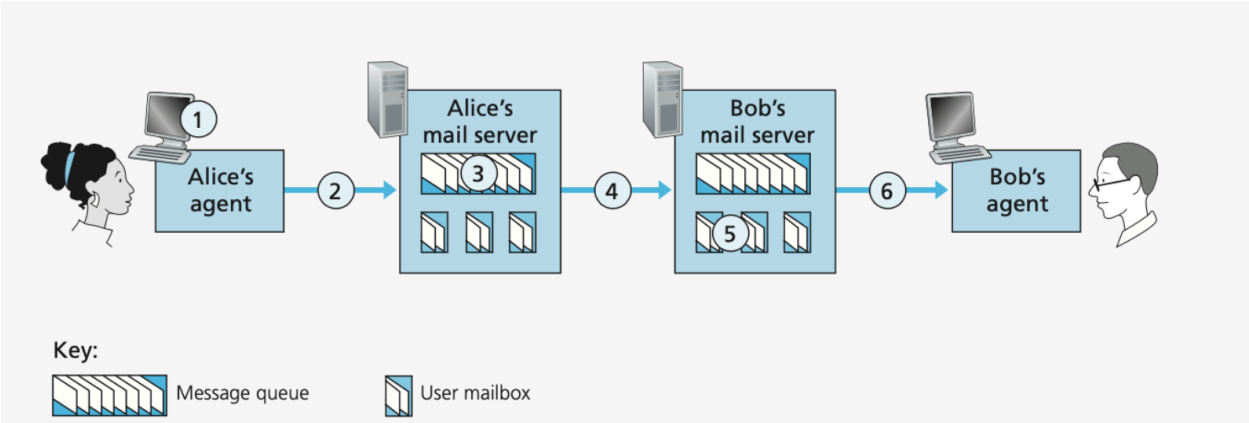
Worksheet Class 8: DNS, Email and SMTP

Q1. Adding a new DNS Entry: You've just received venture capital funding for a fancy new Internet service named fancy.rocks with the brand new ".rocks" top-level domain name. You have a webserver with the host name "server.fancy.rocks" and an authoritative DNS server "dns.fancy.rocks".

Q2. In the scenario below Alice sends an email to Bob. Identify the protocols used at each stage of the email process. Assume that Bob's and Alice's user agents use the IMAP protocol.



A) What protocol is being used at the following stages:

a) Stage 2:

b) Stage 4:

c) Stage 6:

B) What underlying transport protocol does SMTP use?TCP

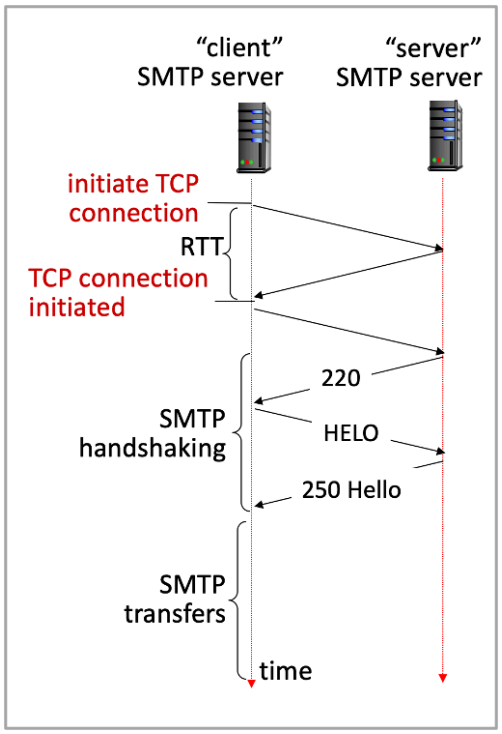
C) Would you classify SMTP as a push or a pull protocol? How about IMAP?

SMTP:

IMAP:

Q3. How many RTTs are there from when a client first contacts an email server (by initiating a TCP session) to when the client can begin sending the email message itself - that is following any initial TCP ro SMTP handshaking that's required.

A. 1
B. 2.5
C. 0
D. 2
E. 3



Q4. SMTP requires messages (header & body) to be in 7-bit ASCII. So how do we send pictures/videos/files via email?

A. We could encode these objects as 7-bit ASCII
B. We use a different protocol instead of SMTP
C. We're really sending links to the objects, rather than the objects themselves

Q5. SMTP lets you speak between two mail servers using HELO, MAIL FROM, RCPT TO, DATA, QUIT commands. What keeps us from entering fake information and forging headers (e.g., claiming our FROM address is something other than what it is)?

A. Nothing, we cannot prevent header forging.
B. The Email Client (e.g. Alice's Mail User Agent) checks that the "FROM address" is valid before sending it to the Mail Server
C. We enter a name/password logging into our Email Client.

Q6. Let's say we take a leaf out of DNSSEC and implement message signing between Alice and Bob. Alice creates a cryptographic public/private key pair, publishes the public key to the world and signs her message with the private key. Now Bob, the receiver, can verify the authenticity of the mail. How can Bob trust that the published public key isn't also a bogus public key?

A. There is no way to trust a public key on someone's website.
B. We can trust the public key by some other cryptographic mechanism
C. We can organize a key sharing party to go in person and share the public key