EIT5 – Fall 2022

Exam questions for the part of Networking and Communications

Department of Electronic Systems

Aalborg University

Problem 5

Download cap1.pcapng and open it

1. Find the IP address assigned by DHCP to the client computer.
    a. What is the MAC address of the client's computer?

Ip is: 192.168.122.43
MAC is: 52:54:00:7f:e3:df

2. The same computer makes an ARP request. What is Target's IP address and MAC address?

Ip is: 192.168.122.1
MAC is: 52:54:00:26:63:d3

3. The capture contains a TCP stream.
    a. Find all frame numbers of the TCP 3-way handshake begins

Frame number 21,22 and 23. We see [SYN], [SYN, ACK], [ACK] coming in these ones, which establishes the connection between the client and the server.

    b. Give a short explanation in your own words of what you think happens within this TCPstream

We see a GET HTTP after the handshake. This would suggest connecting to a webpage, specifically on http://google.com/. Afterwards we see the webpage (216.58.207.206) replies with an ACK and text/html which would likely mean we received the html content of the google webpage. This could be received in e.g. a browser. Finally we see the user ACK and sending a [FIN,ACK] to which the server responds [FIN,ACK] and the user [ACK] in frames 28,29,30. This would close the TCP session as the client had no more for now to request in the TCP session, and the server had no more to send.

4. Find the DNS requests for ntp.ubuntu.com.
    a. Which IPv4 addresses does ntp.ubuntu.com resolve to?

It resolves to [91.189.94.4, 91.189.91.157, 91.189.89.199 91.189.89.198]. all of these being IP's which ntp.ubuntu.com resolves to each could be used when trying to access the website.

Problem 6

If you are live-streaming a video (for example a Microsoft Teams meeting), which protocol is more suitable for real-time experience, TCP or UDP? Describe the advantage of the chosen protocol, and why you would pick it.

While both can be used for any kind of live-streaming, there is a significant difference in how they operate and for which type of application they individually are suitable. UDP is especially suitable for any kind traffic which does not require the entirety of the data to be received. Live streaming is one such traffic type, as the latency and

real-time experience is more critical than receiving every video frame correctly as this may lead to stuttering and even more lag caused by the retransmission of single frames. Hence a deformed picture, or missing a video frame is not detrimental to the experience, whereas sudden lag spikes would be more apparent and frustrating.

1. Explain what the purpose of synchronicity is in a communication protocol, and if this is always relevant and required.
   Synchronicity is generally used to align the receiver and transmitter. From this we could think of synchronous and asynchronous communication. That could for the former be based on a slot-like structure of communication where at each discrete timestep you are in some state, known to the other parties. Hence it is possible to align the different parties with each other to make actions predictable. This could serve a purpose such as minimizing collisions, and is useful if multiple parties always, or often wish to transmit and have a guarantee on the expected availability, which requires scheduling in some form. Synchronicity is thus useful when you want a predictable outcome.
   For the latter, asynchronous protocols, these are useful when the actions of the parties are not deterministic and can change. For example parties are not always transmitting, but when they wish to transmit they would like to be fast and have the medium available. This type of communication is relevant and useful to ensure a system with many users that they do not take up resources not used, which ensures the users wishing to transmit and use the medium have resources available.
   Both types of protocols are useful for different contexts and the relevance is system dependent.

Problem 7

1. Given a shared secret between Alice and Bob, how can data integrity be guaranteed to messages sent between Alice and Bob?
   If a shared secret is given, hashing is a solution to ensure the integrity of messages sent between the 2. By hashing the shared secret with the sent message, and appending the final hash the integrity of the message can be validated by the other party. If anyone were to make changes to the message without the proper “secret” the hash would simply be wrong, which can be evaluated by the receiver.
2. With public key cryptography how can you ensure authentication?
   With public key cryptography the core feature is that the key used for decryption, only works with the key used for encryption (and vice versa as both can be used for either.)
   Signatures is a way to ensure authentication by using the aforementioned feature. This would be done by signing a message using the private key when sending it. Upon reception the receiver can verify if the message was sent by the private key holder, by validating the signature using the public key for decryption.
   This will ensure authentication as long as the private key is not leaked by storing it insecurely, and by ensuring that when receiving the public key that it truly it from who claims ownership. This is over the internet realized through certificate authorities., who certifies ownership of public keys. Naturally you can also “just” trust the ownership without other parties involvement..
3. Does the Diffie-Hellman algorithm provide a pair of symmetric or asymmetric keys?

A pair of asymmetric keys are provided by the algorithm. This is given from the fact diffie-hellman is used for public key cryptography, which relies on 2 different keys (public and private).

4. What is the difference between the block and the stream cipher?
   Block cipher processes the input one block of elements at a time, producing an output block for each input block.
   Stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.
   Hence the differences lies in the block-based encryption of block ciphers where a certain size that must be encrypted at a time i.e. multiple bytes, and if the size is not met padding may be used to achieve the necessary block size. Meanwhile the stream-cipher “streams” the encryption taking one element at a time (1 bit or 1 byte) in a continuous stream.

.