**Sprint semanal(Atribuições da semana)**

Explicar como funciona o handshake com:

* Teoria
* Diagramas
* Demonstrar a teoria no wireshark

================================================================

Foi estudado a RFC 9000(QUIC versão 1) e foram acrescentados os conhecimentos obtidos na sprint anterior(estudo em cima da rfc 8999 e os aspectos que caracterizam o protocolo QUIC em geral).

No que se refere ao handshake, faz-se necessário primeiro entender o que é um RTT para somente então adaptar ao contexto do protocolo.

O **RTT**(**R**ound **T**rip **T**ime) é o tempo de ida e volta que o pacote percorre. Um pacote ICMP por exemplo, ele é enviado para um servidor com ip x.x.x.x e retorna à origem num intervalo de 40 ms. No contexto do protocolo QUIC o RTT é igual a 0 quando o pacote for enviado e não tiver nenhuma confirmação do seu recebimento(resposta do pacote). Nesse contexto, o RTT não se refere ao tempo que o pacote percorre.

**RTT IGUAL A 0** → Significa que o pacote foi enviado e não necessita de uma confirmação.

**RTT IGUAL A 1** → Significa que o pacote teve algum tipo de confirmação ou resposta.

Portanto, num handshake, o máximo do RTT é igual a 1. Para fins comparativos, no protocolo TCP o RTT é igual a 3.

Tendo em vista essas considerações acerca do conceito do RTT, podemos seguir adiante com o estudo do handshake.

**HANDSHAKE QUIC**

O handshake QUIC permite uma baixa latência e criptografia na troca de dados. O handshake é de somente 1-RTT, e o protocolo utilizado para criptografia é o TLS 1.3(pois o handshake das chaves também é de 1-RTT).O Header dos pacotes característicos do handshake é do tipo Long Header(com o Bit reservado sendo 0x01 ou 1) .Abaixo é mostrado o passo a passo de como ocorre o Handshake:

1- É enviado um pacote do tipo INITIAL(com um bit exclusivo 0x00). Esse pacote contém um token e o tamanho do token, além dos outros dados característicos do Long Header(consultar a rfc 8999). Ele é responsável pela solicitação de troca de chaves(que vão ser enviadas posteriormente em pacotes do tipo 0-RTT) e os dados ACK. Após um certo tempo, caso o cliente não receba a resposta do handshake o mesmo envia um novo pacote do tipo RETRY(com um bit exclusivo sendo 0x03), tentando uma reconexão(só é feito mais uma vez).

2- São enviados pacotes do tipo 0-RTT(com um bit exclusivo 0x01). Esse pacote contém informações que podem ser enviadas assíncronamente(informações referentes à criptografia por exemplo). As informações da criptografia estão no quadro CRYPTO. Os quadros CRYPTO são enviados fora de ordem e podem ser repetidos além de serem guardados num buffer de pelo menos 4096 bytes para posteriormente ser organizado num único quadro CRYPTO.

3- É enviado um pacote do tipo HANDSHAKE(com um bit exclusivo 0x02) que confirma os dados e indica que pode ser estabelecida uma comunicação.