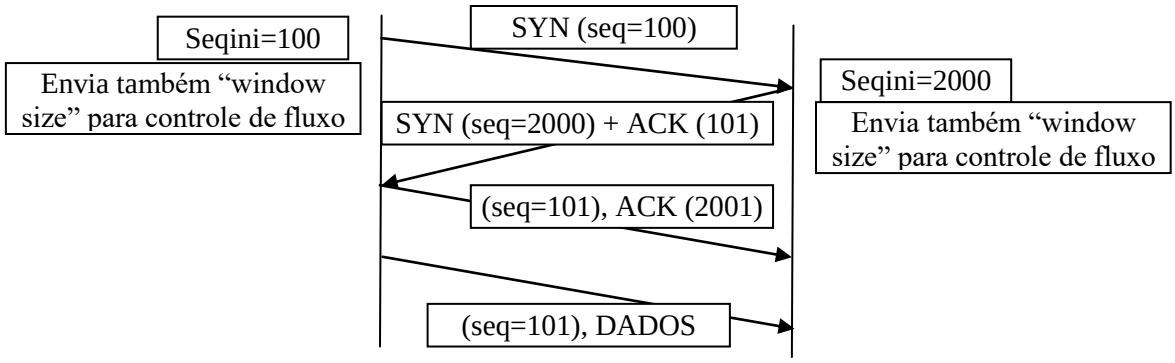
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
DEPARTAMENTO DE INFORMÁTICA APLICADA
INF01154 - Redes de Computadores N

Nível de Transporte: TCP, UDP.

1 TCP

1. Explore o demo Sliding Window em http://www2.rad.com/networks/2004/sliding_window/demo.html. Explique apoiado com imagens da execução da tela do computador o funcionamento do demo *sliding window*. No mínimo, os seguintes itens devem ser explicados:
   a) Funcionamento de janela deslizante
   b) Banda consumida nessa simulação, supondo que o pacote seja de 1250 bytes e o RTT dado em ms.
   c) Comente três diferenças desse simulador em relação ao TCP utilizado na WEB (nos próximos exercícios isso ficará claro).
2. Acesse https://media.pearsoncmg.com/aw/ecs_kurose_compnetwork_7/cw/content/interactiveanimations/tcp-congestion/index.html. Execute a animação do *TCP Congestion Control*. Explique:
   a) Com uma workstation, explique o gráfico.
   b) Qual a diferença entre "3ACKs" (simula o recebimento de 3 ACKS duplicados) e "timeout" (simula o timeout de pacotes)?
   c) Qual a diferença da versão RENO e TAHOE?
   d) Adicione uma segunda workstation. Existe equidade de tráfego (*fairness*)? Qual a importância da forma de controle de congestionamento AIMD (*Additive Increase Multiplicative Decrease*) para a equidade (*fairness*) de tráfego?
   e) Clique seguidamente em "3ACKs". Qual a consequência? Idem para timeout.
3. Acesse a RFC 1700, RFC 3232 e https://www.iana.org/assignments/port-numbers. Cite duas "Well Known Port Numbers", dizendo para que servem.
4. Faça uma conexão TCP qualquer (por exemplo, utilizando telnet ou ssh) para um IP que não esteja associado a qualquer máquina (ex: *>telnet 143.54.2.234*). Utilize o sniffer para determinar:
   a) O timeout inicial.
   b) O número de tentativas efetuadas pelo cliente.
5. Faça, obrigatoriamente com apoio do sniffer, uma análise completa de um pacote Ethernet que contenha encapsulado um cabeçalho IP e TCP (sugestão: faça um HTTP ou download qualquer). Procure entender os valores dos diversos campos encontrados no cabeçalho do segmento TCP encapsulado.
6. Abra o arquivo do laboratório de wireshark TCP do Kurose, disponível na página da disciplina (*Cap3_Wireshark_TCP_v7.0.pdf*). **Execute todos os exercícios de forma online**.
   - Na página 3, onde diz "*First, filter the packets displayed in the Wireshark window by entering "tcp"*", uma sugestão é filtrar também pela porta utilizada nesta conexão, ou seja, em vez de "*tcp*", utilizar "*tcp.port=xxxx*".
   - Observe que a mensagem de HTTP POST é enviada logo após o *handshake*, entretanto, o wireshark somente interpreta no final do envio, muitos pacotes depois.
   - As questões 1 e 2 devem ser feitas para a captura efetuada no laboratório, e não para o trace pronto. Ignorar a questão 3.

- Para as questões 4 a 6, considere a teoria abaixo, onde o NÚMERO DE SEQUÊNCIA INICIAL É ESCOLHIDO ALEATORIAMENTE PARA CADA NOVA CONEXÃO TCP. A seguir está se supondo que o SEQa=100 e SEQb=2000 para uma típica comunicação cliente-servidor.



OBS: o wireshark calcula o "Payload size" do TCP através do campo "Total Lenght" do cabeçalho IP e subtraindo o tamanho do cabeçalho IP (campo IHL – IP Header Lenght) e o tamanho do cabeçalho TCP (campo tcp HL – Header Length).

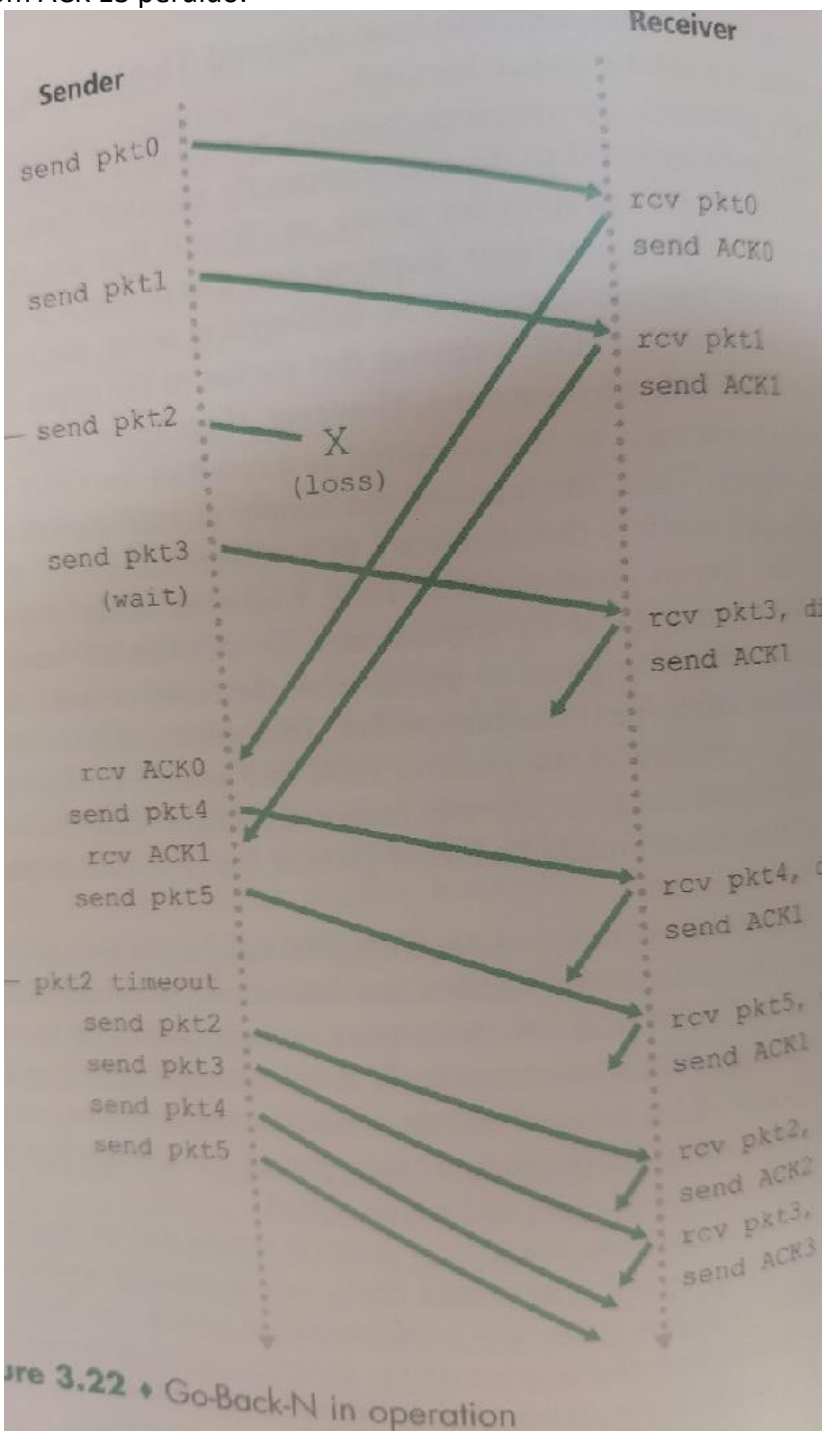
- Na questão 7, a fórmula é: "*EstimatedRTT=0,875*EstimatedRTT + 0,125*SampleRTT*". Ainda na questão 7, uma sugestão é criar uma tabela com 6 linhas (6 segmentos), e colunas com no mínimo hora de envio, hora de chegada do ACK, RTT e "EstimatedRTT", sendo que a última é calculada. Deve-se identificar qual pacote se refere determinado ACK. No caso de gerar o caminho "statistics + stream graph + rtt", caso não funcione, tente clicar em "switch direction", pois é um POST HTTP.
- Questão 9: observe o valor do campo "*Window Size*" nos ACKS dos pacotes recebidos. Se esse valor for zero, então o transmissor não pode enviar mais pacotes. Uma forma é criar um filtro para mostrar somente os pacotes de ack (ip.dst==xxxx).
- Questão 10: sugestão é olhar o campo "*sequence number*" dos pacotes TCP enviados para ver se algum está repetido. Pode-se olhar o gráfico "*statistics+TCP Stream Graphs+Time Sequence-Graph (Stevens)*" e procurar um número de sequência que não está crescendo.
  OBS: mostrar captura onde tem retransmissão de pacotes.
- Questão 11: sugestão de criar uma tabela com 3 colunas, uma sendo o #ACK, a segunda com o número de sequência do ACK e a terceira com o número de bytes feitos por esse ACK. Observe se às vezes o receptor envia um só ACK para mais de um pacote (ACK cumulativo).
- Questão 12: o Throughput pode ser obtido dividindo "*Total Bytes Enviados / Total Tempo*". O total de bytes enviados pode ser obtido subtraindo o número de sequência do último ACK pelo número de sequência do primeiro segmento TCP enviado. O tempo total pode ser obtido subtraindo o tempo de chegada do último ACK pelo tempo de envio do primeiro segmento.
- Questão 13: pode-se observar no trace que há uma "quantidade de pacotes de dados" seguido de uma "quantidade de ACKS". Essa quantidade vai aumentando conforme a janela. Uma sugestão é fazer uma tabela com as seguintes colunas: "Tipo (Dados ou ACK)"; "Número do pacote"; "Número de sequência"; "número do ACK" e "Dados em trânsito". Quando o tipo é "Dados", não tem número de ACK, e quando o tipo é "ACK" não tem número de sequência.
- Observe que muitas vezes o *slow start* nem termina e a conexão já terminou de enviar dados. Isso vale para pequenas páginas ou objetos. Isso deixa a transmissão mais lenta como um todo.

2 UDP

7. Faça, obrigatoriamente com apoio do sniffer, uma análise completa de um pacote Ethernet que contenha encapsulado um cabeçalho IP e UDP (sugestão: consulta DNS). Liste todos os valores dos diversos campos encontrados no cabeçalho do segmento UDP encapsulado. Explique os valores encontrados, como porta origem, destino, relacionando teoria e prática para esse pacote em específico.
8. Abra o arquivo do laboratório de wireshark UDP do Kurose, disponível na página da disciplina (*Cap3_Wireshark_UDP_v7.0.pdf*). **Execute todos os exercícios de forma online**.
9. O protocolo RTP / RTCP (*Real Time Transport Protocol* e seu protocolo de controle) permite controle de congestionamento no nível de aplicação utilizando UDP em nível de transporte. Explique como ele faz isso, levando em consideração a função do RTCP.

3 Conceitos

10. Acesse https://media.pearsoncmg.com/aw/ecs_kurose_compnetwork_7/cw/content/interactiveanimations/go-back-n-protocol/index.html, execute a animação do protocolo GoBackN (GBN) e desenhe o diagrama (tempo na vertical ao estilo da figura 3.22 do livro) para:
    a) Pacotes 0 a 4 sem erros de transmissão nem de ACK.
    b) Pacotes 5 a 9 com pacote 6 perdido.
    c) Pacotes 11 a 15 com ACK 13 perdido.



ure 3.22 ♦ Go-Back-N in operation

11. Acesse https://media.pearsoncmg.com/aw/ecs_kurose_compnetwork_7/cw/content/interactiveanimations/selective-repeat-protocol/index.html, execute a animação do protocolo Selective Repeat (SR) e desenhe o diagrama (tempo na vertical ao estilo da figura 3.26 do livro) para:
    a) Pacotes 0 a 4 sem erros de transmissão nem de ACK.
    b) Pacotes 5 a 9 com pacote 6 perdido.
    c) Pacotes 11 a 15 com ACK 13 perdido.

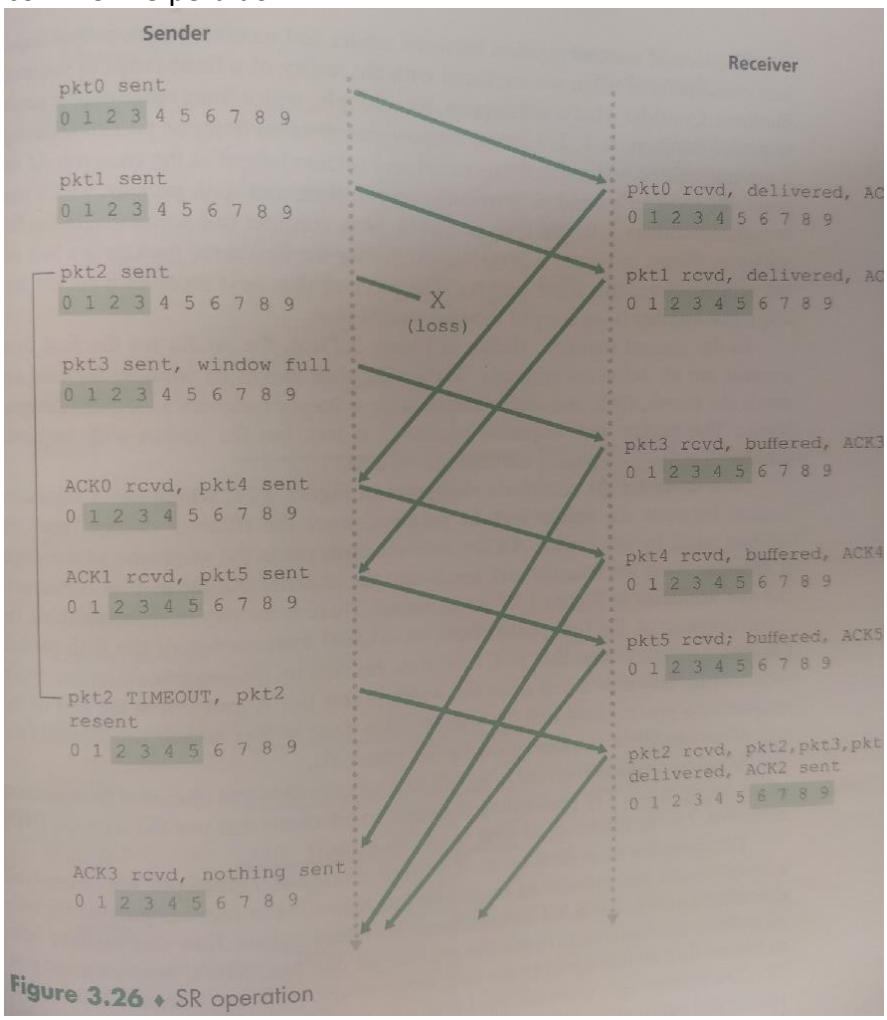


Figure 3.26 ♦ SR operation

12. Acesse https://media.pearsoncmg.com/aw/ecs_kurose_compnetwork_7/cw/content/interactiveanimations/flow-control/index.html. Execute a animação do Flow Control utilizando “File Size = 16kbytes” e “Buffer Size = 2kbytes”. Explique:
    a) Por que às vezes o tamanho da janela do receptor (WIN) é igual à zero?
    b) No caso do item anterior, por que o transmissor envia pacotes com tamanho 1?