Lista II – Infraestrutura de comunicação 2019.2
Professor: Petrônio Júnior

1. Descreva os passos necessários para o estabelecimento de conexão TCP.

Para estabelecer uma conexão, o TCP usa um handshake (aperto de mão) de três vias. Antes que o cliente tente se conectar com o servidor, o servidor deve primeiro ligar e escutar a sua própria porta, para só depois abri-la para conexões: isto é chamado de abertura passiva. Uma vez que a abertura passiva esteja estabelecida, um cliente pode iniciar uma abertura ativa. Para estabelecer uma conexão, o aperto de mão de três vias (ou 3 etapas) é realizado:

1. **SYN**: A abertura ativa é realizada por meio do envio de um SYN pelo cliente ao servidor. O cliente define o número de sequência de segmento como um valor aleatório A.
2. **SYN+ACK**: Em resposta, o servidor responde com um SYN-ACK. O número de reconhecimento (***ack****nowledgment*) é definido como sendo um a mais que o número de sequência recebido, i.e. A+1, e o número de sequência que o servidor escolhe para o pacote é outro número aleatório B.
3. **ACK**: Finalmente, o cliente envia um ACK de volta ao servidor. O número de sequência é definido ao valor de reconhecimento recebido, i.e. A+1, e o número de reconhecimento é definido como um a mais que o número de sequência recebido, i.e B+1.

2. O RTT estimado pelo TCP é uma média móvel exponencialmente ponderada (MMEP).
Apresente a fórmula para a estimativa do RTT e justifique a definição de MMEP.
O RTT para um segmento, denominado **RTTamostra**, é a quantidade de tempo transcorrido entre o momento em que o segmento é enviado (isto é, passado ao IP) e o momento em que é recebido um reconhecimento para o segmento. Ao invés de medir um **RTTamostra** para cada segmento transmitido, a maioria das implementações de TCP executa apenas uma medição de **RTTamostra** por vez. Isto é, em qualquer instante, o **RTTamostra** estará sendo estimado para apenas um dos segmentos transmitidos mas ainda não reconhecidos, o que resulta em um novo valor de **RTTamostra** para aproximadamente cada RTT.

Os valores de **RTTamostra** sofrerão variação de segmento para segmento devido a congestionamento nos roteadores e a variações de carga nos sistemas finais. Por causa dessa variação, qualquer dado valor de **RTTamostra** pode ser atípico. Portanto, para estimar um RTT típico, é natural tomar alguma espécie de média dos valores de **RTTamostra**. O TCP mantém uma média, denominada **RTTestimado**, dos valores de **RTTamostra**. Ao obter um novo **RTTamostra**, o TCP atualiza **RTTestimado** de acordo com a seguinte fórmula:

RTTestimado = (1 - a) * **RTTestimado** + a * **RTTamostra**

Esta fórmula está escrita sob a forma de um comando de linguagem de programação. O valor recomendado de a é a = 0,125 (isto é, 1/8) [RFC 2988], caso em que essa fórmula de torna:

RTTestimado = 0,875 * **RTTestimado** + 0,125 * **RTTamostra**

3. Apresente o conceito de controle de fluxo e de controle de congestionamento do TCP (especificando o objetivo de cada um deles).

TCP

O TCP usa controle de congestionamento fim-a-fim. Isto significa que o remetente limita ou aumenta a taxa de entrega de dados para conexão em função do congestionamento percebido por ele, por isso dizemos que o TCP é auto-regulado.

A conexão TCP é composta de um buffer de recepção, um buffer de envio e de diversas variáveis. Dentre essas variáveis temos a CongWin (janela de congestionamento), que limitará a taxa de envio de pacotes de um remetente TCP.

Ao início de cada RTT (tempo de ida e volta) o remetente enviará seus pacotes de acordo com o tamanho da CongWin estabelecido, e ao final recebe reconhecimento para os dados, um sinal de que todos os pacotes foram enviados corretamente.

4. Como funciona a prevenção de congestionamento do controle de congestionamento do TCP? Em que situações ela é aplicada?

Antigas implementações do TCP começavam uma conexão injetando múltiplos segmentos na rede, até o limite permitido pea janela anunciada pelo receptor. Enquanto isto não acarreta problemas quando os dois nós estão na mesma LAN, se existem roteadores e diversos enlaces entre a origem e destino, estes podem vir a acontecer. Algum roteador intermediário pode ficar sem espaço de *buffer* ou aplicar alguma política de descarte de pacotes.

O algoritmo para evitar isto é chamado de *slow start*. Seu mecanismo é baseado na observação que a taxa que novos pacotes devem ser injetados na rede deve ser a mesma em que as confirmações (ACK) são enviadas pelo outro destino.

O *slow start* requer que outra janela seja mantida pelo TCP emissor: a janela de congestionamento, chamada **cwnd**. Quando uma nova conexão é estabelecida com outro *host* na rede, a janela de congestionamento é inicializada com um segmento, ou seja, o tamanho do segmento anunciado pelo nó oposto (tipicamente 536 ou 512 bytes). Toda vez que um novo ACK é recebido, a janela de congestionamento é incrementada de um segmento. A *cwnd* é mantida em bytes, mas o *slow start* sempre a incrementa em segmentos. O emissor pode transmitir até o mínimo entre a janela de congestionamento e a janela anunciada pelo receptor. **A janela de congestionamento é o controle de fluxo imposto pelo emissor, enquanto a janela anunciada é controle de fluxo imposto pelo receptor.**

Congestion avoidance e *slow start* são algoritmos independentes com objetivos diferentes. Mas, quando ocorre congestionamento, baixa-se a taxa de transmissão de pacotes na rede, e então invoca-se o *slow start* para recomeçar o processo de aumento da janela e taxa de transmisão.

O *congestion avoidance* e o *slow start* requerem que duas variáveis seja monitoradas para cada conexão: a janela de congestionamento, ***cwnd*** , e a janela limite para o algoritmo *slow start*, ***ssthresh.*** O algoritmo combinado funciona da seguinte maneira:

1. Durante a inicialização de uma conexão, a *cwnd* é igual a um segmento e a *ssthresh*, a 65536 bytes;
2. A rotina de emissão do TCP sempre envia o mínimo entre a *cwnd* e a janela anunciada pelo receptor;
3. Quando ocorre congestionamento (indicada por *timeout* ou o recebimento de ACKs duplicados), metade do valor atual da janela de transmissão (o mínimo entre a *cwnd* e a janela anuciada pelo receptor) é armazenado em *ssthresh*. Além disso, se o congestionamento foi causada por *timeout*, a *cwnd* passa a valer um segmento (ou seja, *slow-start*);
4. Quando novos dados forem confirmados pelo nó destino, a *cwnd* é aumentada, mas a maneira como isto é feito depende se está sendo feito o *slow-start* ou o *congestion avoidance*.

Se a *cwnd* for menor ou igual a *ssthresh*, o TCP está em *slow start*; caso contrário, ele está realizando o *congestion avoidance*. O *slow start* prossegue até que a janela de transmissão do TCP esteja com metade do tamanho de quando ocorreu o congestionamento (guarda-se metade do valor da janela que causou problema no passo 3), e, então, passa-se para a fase de *congestion avoidance.*

O *slow start* faz a *cwnd* começar valendo um segmento e ser incrementada de um segmento toda vez que um ACK é recebido. Como mencionado anteriormente, isto abre a janela exponencialmente: um segmento é enviado, então dois, quatro, e assim por diante. O *congestion avoidance*, por sua vez, faz com que a *cwnd* seja incrementada por **segsize*segsize/cwnd** toda vez que um ACK for recebido, onde *segsize* é o tamanho do segmento (*segsize* e *cwnd* são mantidos em bytes).

5. Diferencie as versões Tahoe e Reno do TCP.

While both consider retransmission timeout (RTO) and duplicate ACKs as packet loss events, the behavior of Tahoe and Reno differ primarily in how they react to duplicate ACKs:

- Tahoe: if three duplicate ACKs are received, Tahoe performs a fast retransmit, sets the slow start threshold to half of the current congestion window, reduces the congestion window to 1 MSS, and resets to slow start state.[13]
- Reno: if three duplicate ACKs are received, Reno will perform a fast retransmit and skip the slow start phase by instead halving the congestion window (instead of setting it to 1 MSS like Tahoe), setting the slow start threshold equal to the new congestion window, and enter a phase called *fast recovery*.[

6. Qual a diferença entre repasse e roteamento?

O Roteamento determina a rota do pacote da origem até o destino. Envolve todos os roteadores. As definições das rotas são feitas pelo algoritmo de roteamento, que configura as tabelas de repasse de cada roteador e o repasse é quando um pacote que chega a entrada de enlace deve ser transferida para a saída de enlace apropriada do roteador. Ocorre localmente em cada roteador que possui uma tabela de repasse relacionando o IP e o enlace de saída de destino.

7. Quais os componentes de um roteador genérico? Especifique a função de cada um.

8. Considerando elementos de comutação, quais as suas possíveis implementações? Destaque ao menos uma característica de cada uma delas.

Comutação de circuitos

Um circuito físico real é formado entre os dois equipamentos que desejam se comunicar. Os elementos de comutação da rede unem (ou conectam) circuitos ponto a ponto independentes até formar um "cabo" que interligue os dois pontos.

Comutação de mensagem

Não é estabelecido um caminho dedicado entre os dois equipamentos que desejam trocar informações. A mensagem que tem que ser enviada é transmitida a partir do equipamento de origem para o primeiro elemento de comutação, que armazena a mensagem e a transmite para o próximo elemento. Assim, a mensagem é transmitida pela rede até que o último elemento de comutação entregue-a ao equipamento de destino. Neste tipo de comunicação, a rede não estabelece o tamanho da mensagem, podendo esta ser ilimitada.

Comutação de pacotes

Possui uma filosofia de transmissão semelhante à comutação de mensagem, ou seja, os pacotes são transmitidos através dos elementos de comutação da rede até o seu destino.

A principal diferença entre as duas é que, ao contrário da primeira, na comutação por pacotes o tamanho dos bloco de transmissão é definido pela rede. Em consequência, a mensagem a ser transmitida deve ser quebrada em unidades menores (pacotes).

Ao quebrar a mensagem em pacotes, a rede pode transmitir os pacotes de uma mesma mensagem por vários caminhos diferentes, otimizando os recursos da rede. A desvantagem é que os pacotes podem chegar na ordem trocada, necessitando da criação de mecanismos de ordenamento.

9. Descreva, em detalhes, como e quando ocorre a fragmentação de um datagrama IP.Adicionalmente, apresente quais informações presentes no cabeçalho do datagrama devem existir para tornar essa fragmentação possível.

Fragmentar o pacote significa dividir o pacote em unidades de menor tamanho, denominadas Fragmentos. O tamanho máximo de um fragmento é o tamanho da MTU menos o tamanho do cabeçalho IPv4, que pode variar de 20 a até 60 bytes. Cada fragmento será enviado pela rede em um pacote separado, e cada um desses pacotes seguirá as seguintes regras:

- O campo Tamanho Total será o tamanho do fragmento;
- O bit MF (more fragments) no campo Flags será configurado em 1 para todos os fragmentos exceto o último, que terá o valor 0 ajustado;
- O campo Offset do Fragmento será configurado (em 1), baseado no deslocamento do fragmento no campo de dados original, em unidades de blocos de oito bytes.
- O checksum do cabeçalho deve ser recalculado.

Assim, se tivermos um MTU de 1500 bytes e pacotes padrão com cabeçalho de 20 bytes, os offsets (deslocamentos) dos fragmentos serão múltiplos de (1500-20)/8 = 185, como por exemplo 0, 185, 370, etc.

Exemplo de fragmentação de datagramas IP

Vamos supor que um segmento da camada de transporte tenha um tamanho total de **4000 bytes**, sem o uso de opções, e que esse segmento será enviado em pacotes IP de cabeçalho padrão de 20 bytes.O tamanho total do pacote IP gerado teria então 4020 bytes (4000 + 20). Vamos assumir também um caso típico que é o do envio desse pacote por um link cujo MTU é de 1500 bytes – portanto, o pacote deverá ser fragmentado por exceder esse tamanho.O primeiro offset será igual a zero. O segundo offset será igual a 0 + (Bytes de Dados / 8) = 0 + 1480/8 = **185**.O terceiro offset será igual ao segundo offset (185) + (Bytes de dados / 8) = 185 + 1480 / 8 = 185 + 185 = **370**.Fragmentos que possuam a mesma identificação pertencem ao mesmo pacote, e o campo offset do fragmento permite ordenar esses fragmentos. Ao receber o último fragmento, que possui o flag MF igual a zero, o receptor pode então calcular o tamanho do campo de dados multiplicando o offset do último fragmento por 8, e adicionando o tamanho do último fragmento, como mostramos na seção anterior. Neste ponto, o pacote remontado é enviado para a camada de nível superior na pilha de protocolos (camada de transporte) para processamento.Fragmentos que possuam a mesma identificação pertencem ao mesmo pacote, e o campo offset do fragmento permite ordenar esses fragmentos. Ao receber o último fragmento, que possui o flag MF igual a zero, o receptor pode então calcular o

tamanho do campo de dados multiplicando o offset do último fragmento por 8, e adicionando o tamanho do último fragmento, como mostramos na seção anterior.

10. Defina, com suas palavras, o que é uma sub-rede. Adicionalmente, defina qual a maior máscara para definir uma sub-rede capaz de endereçar 16 hospedeiros (justifique).

Uma **sub-rede** é uma subdivisão lógica de uma rede IP. A subdivisão de uma rede grande em redes menores resulta num tráfego de rede reduzido, administração simplificada e melhor performance de rede.[1]

Dispositivos que pertencem a uma sub-rede são endereçados com um grupo de bit mais significativo comum e idêntico em seus endereços IP. Isto resulta na divisão lógica de um endereço IP em dois campos, um *número de rede* ou *prefixo de roteamento* e o *restante do campo* ou *identificador de host*. O *campo restante* é um identificador para uma interface de hospedeiro ou rede específicos.

Maior mascara para 16 hospedeiros ->255.255.255.240 , pois o número total é 255.255.255.255, daí você tira os 16 possíveis IP's que você quer dai fica 255.255.255.240. Ou seja de 255.255.255.240 ate 255.255.255.255 eistem 16 Ip's

11. Descreva o funcionamento do DHCP.

DHCP é a sigla para Dynamic Host Configuration Protocol. Trata-se de um protocolo utilizado em redes de computadores que permite a estes obterem um endereço IP automaticamente.por meio dele, um servidor distribui endereços IP na medida em que as máquinas solicitam conexão à rede. Quando um computador desconecta, seu IP fica livre para uso de outra máquina. Para isso, o servidor geralmente é configurado para fazer uma checagem da rede em intervalos pré-definidos.

É importante frisar que, além do endereço IP, também é necessário atribuir outros parâmetros a cada computador (host) que passa a fazer parte da rede. Com o DHCP isso também é possível. Pode-se passar à máquina-cliente máscara de rede, endereços de servidores DNS (Domain Name Server), nome que o computador deverá assumir na rede (por exemplo, infowester, infowester1 e assim por diante), rotas, etc.

Quando um computador se conecta a uma rede, ele geralmente não sabe quem é o servidor DHCP e, então, envia uma solicitação à rede para que o servidor DHCP "veja" que uma máquina-cliente está querendo fazer parte da rede e, portanto, deverá receber os parâmetros necessários. O servidor DHCP responde informando os dados cabíveis, principalmente um número IP livre até então. Caso o cliente aceite, esse número ficará indisponível a outros computadores que se conectarem à rede, já que um endereço IP só pode ser utilizado por uma única máquina por vez.

O administrador da rede pode configurar o protocolo DCHP para funcionar nas seguintes formas: automática, dinâmica e manual:

Automática: neste modo, uma determinada quantidade de endereços IP é definida para ser usada na rede, por exemplo, de 192.168.0.1 a 192.168.0.50. Assim, quando um computador fizer uma solicitação de inclusão na rede, um dos endereços IPs em desuso é oferecido a ele;

Dinâmica: este modo é muito semelhante ao automático, exceto no fato de que a conexão à rede é feita por um tempo pré-determinado. Por exemplo, uma máquina só poderá ficar conectada por no máximo duas horas;

Manual: este modo funciona da seguinte forma: cada placa de rede possui um parâmetro exclusivo conhecido por MAC (Medium Access Control). Trata-se de uma seqüência numérica que funciona como um recurso para identificar placas de rede. Como esse valor é único, o administrador pode reservar um endereço IP para o computador que

possui um determinado valor de MAC. Assim, só este computador utilizará o IP em questão. Esse recurso é interessante para quando é necessário que o computador tenha um endereço IP fixo, ou seja, que não muda a cada conexão.

12. O que é e qual a utilidade do NAT?

Network Address Translation (**NAT**), também conhecido como *masquerading*, é uma técnica que consiste em reescrever, utilizando-se de uma tabela *hash,* os endereços IP de origem de um pacote que passam por um *router* ou *firewall* de maneira que um computador de uma rede interna tenha acesso ao exterior ou Rede Mundial de Computadores.Por se tratar de uma rede privada, os números de IP interno da rede (como 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16) nunca poderiam ser passados para a Internet pois não são roteados nela e o computador que recebesse um pedido com um desses números não saberia para onde enviar a resposta. Sendo assim, os pedidos teriam de ser gerados com um IP global do router. Mas quando a resposta chegasse ao router, seria preciso saber a qual dos computadores presentes na LAN pertencia aquela resposta.

A solução encontrada foi fazer um mapeamento baseado no IP interno e na porta local do computador. Com esses dois dados o NAT gera um número de 16 bits usando a tabela hash, este número é então escrito no campo da porta de origem.

O pacote enviado para fora leva o IP global do router e na porta de origem o número gerado pelo NAT. Desta forma o computador que receber o pedido sabe para onde tem de enviar a resposta.

13. Apresente 3 características do IPv6 que podem ser apontadas como evolução em relação ao IPv4 (justifique).

O IPv4 transfere endereços de protocolos de 32 bits. Sustenta aproximadamente 4,29 bilhões de IPs pelo mundo todo, o que nos fez chegar na crise atual: O sistema não suportará mais endereços do que isso.enquanto no IPv6 temos um total de 340,282,366,920,938,463,463,374,607,431,768,211,456 endereços IP.

Outras diferenças importantes são a introdução dos endereços de anycast e a retirada dos endereços de broadcast.Caso seja necessário enviar uma mensagem a todos os hosts pode-se utilizar um pacote de multicast para o endereço de link-local de destino chamado de “all nodes address” (FF02::1).

Outro ponto importante é que no IPv6 ainda temos a parte de rede, subrede e host, como no IPv4, mas não utilizamos mais o termo máscara e sim somente prefixo.O prefixo do IPv6 tem a mesma funcionalidade do prefixo do CIDR e conta a quantidade de bits de rede ou subrede que a máscara tem, sendo que os bits 1 continuam indicando a porção de redes e os bits zero os hosts.

14. Considerando a transição entre IPv4 e IPv6, como ocorre a transição através de pilha dupla? Qual seu principal problema?

A utilização deste método permite que dispositivos e roteadores estejam equipados com pilhas para ambos os protocolos, tendo a capacidade de enviar e receber os dois tipos de pacotes, IPv4 e IPv6. Com isso, um nó Pilha Dupla, ou nó IPv6/IPv4, se comportará como um nó IPv6 na comunicação com outro nó IPv6 e se comportará como um nó IPv4 na comunicação com outro nó IPv4.Utilizar pilha dupla pode não ser possível em todas as ocasiões. Por exemplo, quando não há mais IPv4 disponíveis e o provedor precisa atender a usuários novos com IPv6 e IPv4. Para redes corporativas que já utilizam NAT isso não é um impendimento: o IPv6 nativo pode ser utilizado em conjunto com o IPv4 compartilhado. Outra situação que dificulta a implantação do IPv6 usando pilha dupla é a existência de equipamentos que não o suportam e que não podem ser facilmente substituídos

15. Justifique o fato do roteamento da Internet ser hierárquico.