PROCESSO SELETIVO GRIS 2020.1
TAG- Redes - Luiz Reis

Nome: Yuri Medeiros da Silva

---

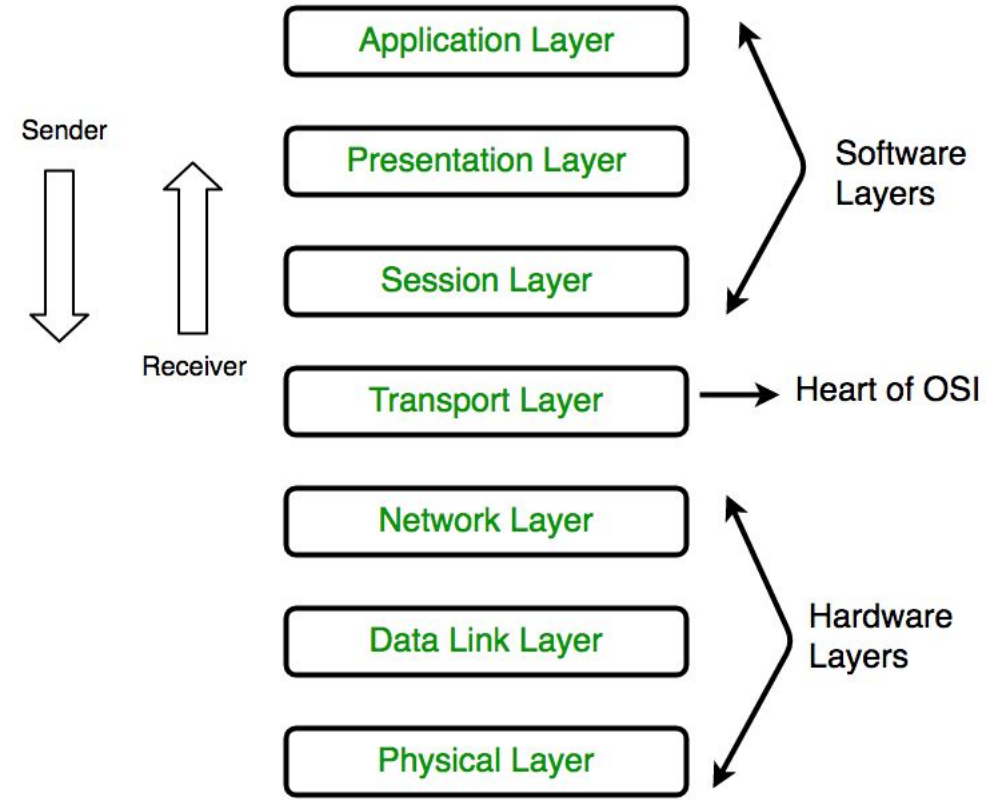
1. Diga quais são as camadas do modelo OSI, em ordem, e dê uma breve descrição de cada uma.

O modelo osi (**Open Systems Interconnection model**) tem como objetivo ser um padrão para protocolos de comunicação e divide a rede em 7 camadas, especificando o que seria o objetivo de cada uma delas.

As camadas são :

7.Aplicação : É a camada de interface das aplicações, que interage com o usuário final. Onde são estabelecidos alguns protocolos que serão usados, como o http, ssh ...
6. Apresentação : Responsável pelo dado que é enviado conseguir ser entendido pelo receptor, pois ela que trabalha com a parte de compressão, encriptação e tradução do dado enviado de um local para outro. Ela também encapsula o que é recebido da camada de *Aplicação*(7).
5. Sessão : Controle do diálogo . Essa camada gerencia e sincroniza a comunicação entre aplicações/agentes diferentes. Ela marca os chunks de data para saber se tem dados perdidos ou fechar a comunicação antes do esperado.
4. Transporte : Recebe os dados da camada de sessão os divide e manda para a próxima camada e verifica se não tem nenhum erro. (tcp e udp estão aqui)
3. Rede : Enviar os pacotes do source para o destino, pra isso ela converte ip -> mac
2. Enlace : Essa camada provê a organização dos bits da camada física em Frames, o controle do fluxo,identificação dos computadores e a possível detecção de erros. Tem como função principal evitar que ocorra erros entre a camada 1 e 3.
Essa camada é dividida em duas partes :LLC(Logical Link Control) e MAC(Media Access Control). O LLC tem como objetivo entregar os bits/frame correto para a camada 3. Já o MAC tem como objetivo o redirecionamento para as máquinas.
1. Física : parte eletrônica dos “cabos”. Responsável pela transmissão dos bits de um nó ao outro. Quando recebe os sinais converte eles em 0s e 1s e manda pra

camada de cima.




```
+------+ +-----+ +-----+       +-----+
|Telnet| | FTP | |Voice|  ...  |     |  Application Level
+------+ +-----+ +-----+       +-----+
      |   |         |             |
     +-----+     +-----+       +-----+
     | TCP |     | RTP |  ...  |     |  Host Level
     +-----+     +-----+       +-----+
        |           |             |
     +-------------------------------+
     |    Internet Protocol & ICMP   |  Gateway Level
     +-------------------------------+
                     |
       +---------------------------+
       |   Local Network Protocol  |    Network Level
       +---------------------------+
```

Protocol Relationships

Figure 2.

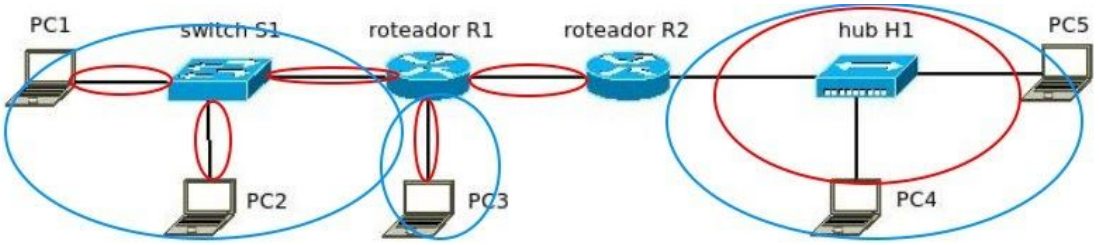
2. Defina domínio de rede e domínio de broadcast

Domínio de broadcast : é o limite que um pacote consegue chegar depois que ele é transmitido por um computador.

> *"um segmento lógico de uma rede em que um computador ou qualquer outro dispositivo conectado à rede é capaz de se comunicar com outro sem a necessidade de usar um roteador"*

Domínio de colisão : É uma área onde os pacotes podem colidir, *como se fossem dois carros se chocando*,por exemplo os hubs, onde um pacote enviado chega em todas as máquinas, ou seja, se tivermos muitos dados sendo enviados ao mesmo tempo de locais diferentes eles podem colidir e quando isso acontece temos a contenção de pacotes. Portanto, quanto maior for o número de colisões maior será a ineficiência da rede.

3. Determine os domínios de rede e broadcast na figura abaixo.



Na imagem,
Azul é o domínio de rede
Vermelho o domínio de colisão.

4. De acordo com a figura abaixo, suponha que A envia um pacote para B e recebe sua confirmação. Mostre os dados (IP e MAC) ao longo do caminho para que sua transmissão ocorra corretamente.
A e B estão redes diferentes.
A manda mensagem para o roteador, com

ip/mac sender :::: ip/mac receiver

1. A:a.a.a.a::::B:???
2. pula pro roteador -> A:r1.r.1.r1.r1::::B:???? →
3. pula pro outro roteador → A:r2.r2.r2.r2::B:b.b.b.b → retorna o mac de B

5. Resolva novamente a questão anterior supondo que A está por trás de um NAT implementado no roteador R1.
nat = a rede interna vai estar isolada do meio.
Então, na linha *3.* ao invés de termos o ip de A, teremos o ip do R1 e na hora de retornar o R1 mandara para a porta do switch que o ip nat da pessoa está.

ip/mac sender :::: ip/mac receiver

1. A:a.a.a.a::::B:???
2. pula pro roteador -> A:r1.r.1.r1.r1::::B:???? →
3. pula pro outro roteador → R1:r2.r2.r2.r2::B:b.b.b.b → retorna o mac de B

6. Explique os passos de um handshake TCP de acordo com o RFC793.

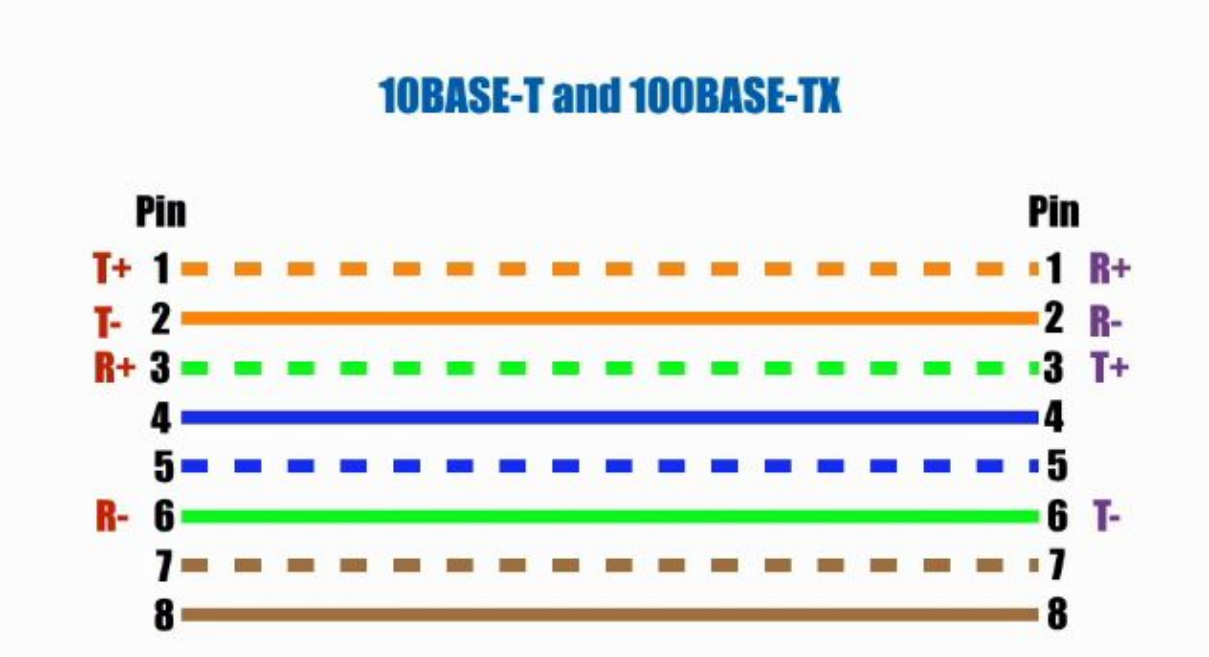
1) A --> B SYN my sequence number is X
2) A <-- B ACK your sequence number is X
3) A <-- B SYN my sequence number is Y
4) A --> B ACK your sequence

(retirado do link https://tools.ietf.org/html/rfc793#page-27)

Basicamente para iniciar uma conexão o host A envia um SYN para B.
B reconhece o valor enviado no SYN com um ACK.
B manda um SYN com valor Y, e A responde um ACK com o valor. handshake done.

7. Explique o que é MDI e MDIX

MDI : utilizado normalmente para dispositivos que estão em layers . Os pinos possuem uma ligação direta.
MDIX: o X representa o crossover, que indica que os pinos se conectam de forma “inversa”. Utilizado para dispositivos que estão em layers diferentes.



8. Admitindo que temos apenas cabos UTP cat 5 para interligar os equipamentos da figura abaixo, diga quais configurações de cabos devem ser usados.

A - S1 = straight through, mdi
S1 no S2 = com cabo crossover mdx-mdx
S2 - R1 = straight through, mdi, já que vai de mdix para mdi
R1-R2 = crossover, mdi mdi
R2 - B = crossover

The easy way to remember is if you're changing layers(2 to 3 or vice versa) than you use a straight through and if you're connecting the same layer(2 to 2 or 3 to 3) you use a

crossover. Routers, PCs and other end devices are layer 3 and switches/hubs are layer 2. (Retirado da internet, perdi o link quando procurei de novo)

9. Para os endereços abaixo, os classifique e diga a rede, host e broadcast.

1 - iP: 177.32.168.223 Masc: 255.255.255.248 = /29
Classe C
masc : 11111111.11111111.11111111. 11111 000
ip : 10110001.00100000.10101000. 11011 111
é um endereço de broadcast, depois da máscara tudo é igual 1.
rede : 177.32.168.216
Para calcular o host masc a gente flipa os bits da máscara e faz o end.
host: 177.32.168.223
masc flipped: 0.0.0.00000111 = 0.0.0.7
broadcast : 10110001.00100000.10101000.11011111 : 177.32.168.223

2- IP: 204.20.143.0 Masc: /18
Aqui depois da máscara temos 1s e 0s, então é um endereço de host
Classe C
rede: 204.20.128.0
broadcast: 204.20.191.255

3 - IP: 36.72.109.24 Masc: 255.254.0.0
Aqui depois da máscara temos 1s e 0s, então é um endereço de host
Classe A
rede: 36.72.0.0
broadcast: 36.73.255.255

4 - IP: 7.26.0.64 Masc: /26
No Ip, depois do /26 é tudo 0, portanto rede.
Classe A
rede: 7.26.0.64
broadcast: 7.26.0.127

5 -IP: 200.201.173.187 Masc: 255.255.255.252
é um endereço de broadcast, depois da máscara tudo é igual 1.
Classe C
rede: 200.201.173.184
broadcast: 200.201.173.187

10. Diga se os endereços dados estão na mesma rede

1- 240.128.192.154 e 240.128.192.158 com mascara 255.255.255.224
mascara : 1.1.1.11100000
ip: ...10011010
ip2: ...10011110
Fazendo o *and* da máscara com os ips, ambos estão na mesma rede 240.128.192.128

2- 87.42.141.142 e 87.42.141.137 com mascara 255.255.255.248

mascara : 1.1.1.11111000
ip1 : ...10001110
ip2 : ...10001001
Estão na mesma rede 87.42.141.136 01010111.00101010.10001101.10001000

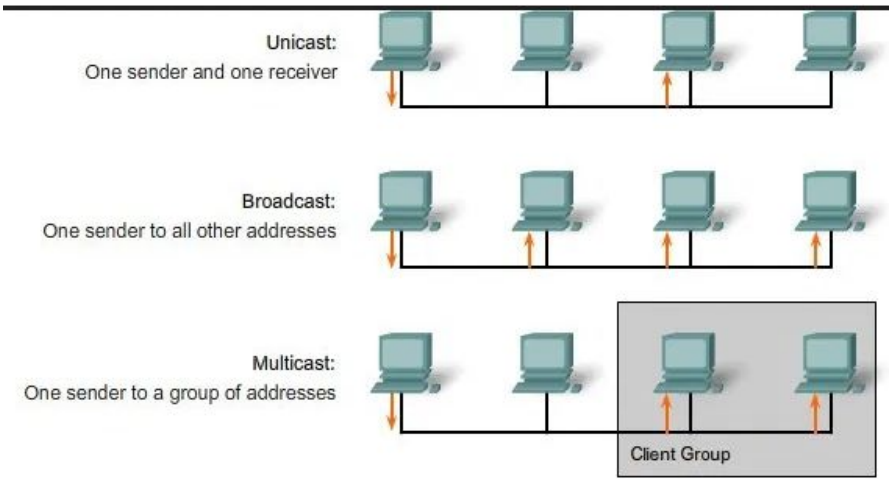
3- 98.45.7.17 e 98.12.238.221 com mascara /10
máscara : 11111111.11\ 000000.00000000.00000000
ip1: 01100010.00\ 101101.00000111.00010001
ip2: 01100010.00\ 001100.11101110.11011101
Estão na mesma rede 98.0.0.0/10

11. De acordo com o diagrama de rede abaixo, faça o projeto de endereçamento de rede contemplando TODAS as redes descritas e suas capacidades. Todo o range 187.0.0.0/8 está à sua disposição.

12. Classifique, quanto ao seu tipo, os protocolos RIP, OSPF e BGP

O RIP **(Routing Information Protocol)** é um protocolo de roteamento interno, ou seja, utiliza o IGP (Interior Gateway Protocol). Utiliza como base o broadcast, onde ele transmite a mensagem para todos os hosts simultaneamente.
Algoritmos utilizados :
Bellman-Ford distribuído
Ford-Fulkerson

O OSPF (**Open Shortest Path First**) também é mais utilizado internamente como o RIP é um protocolo de roteamento dinâmico. Ele utiliza o SPF do Dijkstra que leva em consideração o custo através da largura de banda, na procura da melhor rota. Forma de transmissão : multicast.



O multicast envia pacotes com atualizações necessárias apenas para roteadores vizinhos.

BGP **(Border Gateway Protocol)** esse é mais utilizado em redes de grande porte, utilizado pela internet, os outros são basicamente para conectar nós vizinhos, esse é utilizado para conectar redes. atualmente estamos no BGP4.

13.Considere uma rede com 5 hosts onde 3 deles tem TCP window size de 64KB e 2 de 32KB.Calcule o throughput do link de borda sabendo que sua latência é de 15ms.

Throughput é calculado em bits per second (bit/s or bps),

$$Throughput = \frac{WindowSize}{RTT}$$

64 KBs = 64000 bits
t1 = 64000/0.015 = 4,266,666.666666667 Bs
32 KBs = 32000 bits
t2 = 32000/0.015 = 2,133,333.333333333 Bs
4,266,666.666666667 * 3 + 2,133,333.333333333 *2 = 17066666.6667 bit/s

14. De acordo com o cabeçalho TCP, explique cada um dos campos sequence number,acknowledgement, window size e suas flags.

Sequence number: Primeiro octeto a ser enviado. Serve para mapearmos/ordenar os pacotes enviados. SN é incluído em cada pacote transmitido

Acknowledgment : Utilizado para garantir que um pacote foi recebido corretamente na ordem devida sem erro.

window size: Quantidade que uma janela tcp pode transmitir de bytes, o máximo é de 65535 bytes. O tamanho pode ser aumentado com o que é chamado de TCP Windows Scaling que é avisado durante o handshake (RFC 1323)

Outras flags:

FIN : Pede o fim da conexão

Reset (RST): termina a conexão de forma hard, sem pedir, utilizado quando parece que tem algo errado na conexão, os dados são perdidos.

Urgent (URG): Se o pacote tiver essa flag, sua informação é processada primeiro e 'limite' de tamanho dos dados não é considerado, é enviado tudo.

Push (PSH): é um URG com menos prioridade.

ACK: Confirma o conhecimento que recebeu a informação.

SYN: Começa conexão.

15.Explique de que maneira funciona o sequenciamento TCP padrão.

Um host manda um pacote SYN com um valor de ISN inicial (randômico na primeira vez) para outra máquina. O host 2 responde com um Ack com o valor enviado + N e envia um syn para permitir a conexão. Aí quando host 1 recebe ele manda um ack, com o valor do syn de antes enviado + n. Conexão estabelecida

16.Explique de que maneira o TCP padrão se recupera de um timeout.
Basicamente um dos hosts fica pedindo o pacote que foi perdido em um timeout,e o outro lado da conexão, envia o próximo ack contendo o perdido e o resto das informações.

17.Explique de que maneira funciona o fast retransmit TCP padrão.
Basicamente se tivermos mais de 3 sinais indicando que um pacote não foi recebido corretamente (ou seja, um dos nós enviar um ack pedindo o mesmo pacote) a conexao é '*resetada'* e se é transmitido o pacote de novo.

18.Explique de que maneira funciona o slow start e congestion avoidance TCP.
slow start: conforme os acks vão sendo enviados, vai aumentando a quantidade de acks que são recebidos por vez. No slow start, vai crescendo exponencialmente 2^i, 1,2.4….
congestion avoidance: os acks vão crescendo linearmente i+1, 1,2,3,4….

19.Explique o comportamento "serrilhado" do TCP e por que ele é importante para seu funcionamento.

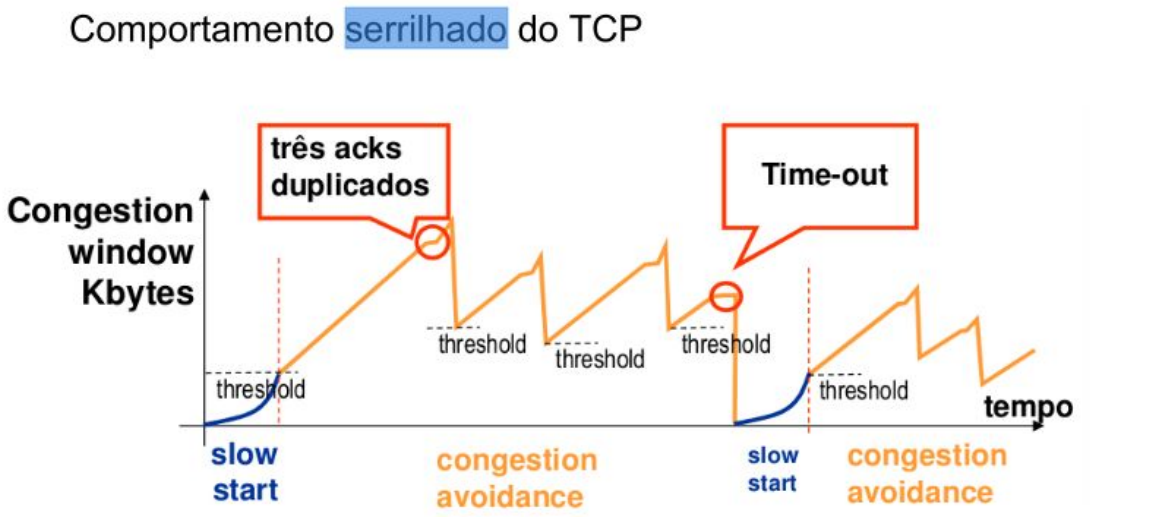


Imagem dos slides do Prof. Aguiar

Serve para melhorar a 'resposta a incidente', juntando o slow start com o congestion avoidance. E, mostra que o pior caso é quando temos um timeout que a conexão tem que começar de 1 de novo.

20.Considere uma janela TCP de tamanho 8, e threshold 4. Assuma que são enviados ACK's sequenciais de 1 a 8 e os ACK's 2 e 3 se perderam. Mostre todo o sequenciamento TCP até que o envio dos ACK's seja normalizado (mostre uma janela completa correta).
A -> <- B, ->(significa envia) : <-(significa confirma)
1 ->
2 -> <-2 , mas o 2 nao chegou
3 -> <-2, nem o 3, mas ele continua pedindo o que nao chegou

4 -> <-2
5 -> <-2
6 -> <-2
7 -> <-2
8 -> <-2
Se o 2 e o 3 forem reenviados agora :
2 -> <-3
3 -> <- 9, dessa vez o 3 também chegou, e ele já pediu o próximo.

21.Defina AS (sistema autônomo).
Autonomous system (AS) é um grupo de dispositivos(roteadores,..) que estão sob controle de uma ou mais redes, que apresentam possíveis políticas de roteamento. Um sistema em que cada roteador conhece todos os detalhes de sua própria região e desconhece a estrutura interna de outras.

22.Suponha que um host A envie uma requisição ARP para descobrir o endereço de um host B. Mostre o formato desta requisição e a resposta recebida.
A manda um pacote de broadcast (1.1.1.1) na rede com o ip de B e pedindo o mac de B. Quando esse pacote chega em B, retorna o mac de B.

23.O que é CSMA/CD? Explique brevemente.
São formas/algoritmos para tratar as colisões que podem acontecer na rede. O *CSMA/CD* (Carrier Sense Multiple Access with Collision Detection) basicamente identifica quando o canal está disponível para a transmissão, inicia a transmissão e obriga que os nós escutem a rede enquanto transmitem dados ((LWT) "Listen While Talk").

- *CS (Carrier Sense)*: Verifica se tem dados sendo transmitidos
- MA (Multiple Access): Múltiplas máquinas podem tentar obter o dado ao mesmo tempo, sem nenhum tipo de prioridade, se tivermos uma colisão - já que os nós tentam podem transmitir/acessar os dados ao mesmo tempo/'multiplamente' - nenhuma das placas consegue transmitir os dados.
- CD (Collision Detection): Identifica as colisões na rede.

24.O que é encapsulamento?
Encapsular é incluir algo no outro. Referente ao modelo OSI, quando passamos da layer A para layer B, os dados/headers da layer A são encapsulados e passados para a próxima layer (B), assim, B insere suas informações, encapsula e manda para a próxima layer.

25.Defina o que é um protocolo, no âmbito de redes.
Um acordo de cavalheiros, ou seja, um conjunto de regras e padrões estabelecidos que se seguidos por ambos os lados estabelece a comunicação.