Nome: Pedro Jullian Medina Torres Graça
DRE: 116015284
Curso: Engenharia Eletrônica e da Computação
Objetivo: Responder as Perguntas da TAG de redes.

Q1)
O modelo OSI é dividido nas seguintes partes:
7) Aplicação
6) Apresentação
5) Sessão
4) Transporte
3) Rede
2) Enlace
1) Física

A camada 1 é onde é definido as especificações elétrica e física dos equipamentos computacionais. São os meios de conexão dos equipamentos e dentro deles. É a responsável pela transmissão, recepção, codificação e decodificação dos bits.

A camada 2 é onde começa a interpretação dos bits. É onde pertence os protocolos de comunicação entre sistemas conectados a altas velocidades. É onde está o protocolo de Ethernet e de PPP. A camada tem a função de detectar e corrigir possíveis erros da camada física e pela delimitação de quadros. É dividida em duas.

2.2)LLC
A subcamada 2.2 é onde se especifica os mecanismos para o endereçamento que possibilita a troca de dados entre os usuários da rede. É onde opera O HDLC.
2.1)MAC
A subcamada 2.1 é a de controle do acesso ao meio. Controla o acesso ao meio de transmissão e é a que abriga o endereço MAC que consiste em um numero único de cada dispositivo.

A camada 3 é a responsável pela operação da rede. É onde ocorre o roteamento, abrigando os procolos de IP, ICMP e IGMP. Ela é a responsável pela direção dos dados e o controle dos fluxos.

A camada 4 é a responsável pela transferência de dados entre dois equipamentos sem importar da forma usada para a comunicação. Nela só importa os equipamentos da ponta. O receptor e o transmissor. É nela onde opera, assim o TCP e o UDP. As camadas anteriores estão preocupadas com a maneira que pode ocorrer uma comunicação. Essa ultima está preocupada se os dados estão corretos ou com o envio para um equipamento.

A camada 5 é a responsável pelos processos que controlam a transferência os dados. Ela é onde que são colocadas as regras para sincronização das trocas de mensagens. Ela surge como uma forma de organizar e sincronizar o dialogo no intercambio dos dados. É onde está o SCP (permite ao um host chamar por um comando em outro).

A camada 6 é a responsável pela formatação das informações para a aplicação. É onde está a conversão, a compressão e a criptografia dos dados em um transporte. Liberando, assim, a aplicação de lidar com possíveis problemas de formatação e segurança.

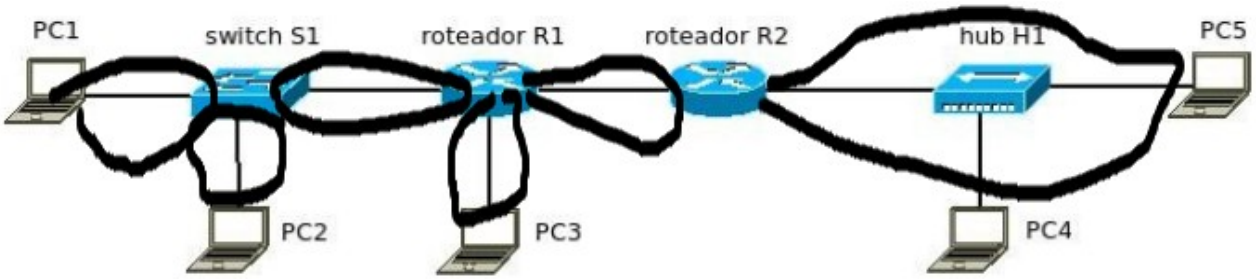
A camada 7 é onde é provido os serviços para os softwares. É o https para o browser, o ssh, telnet e o BitTorrent.

Q2)
Domínio de Colisão: É o local onde é possível ocorrer as colisões da dados dentro de uma rede.

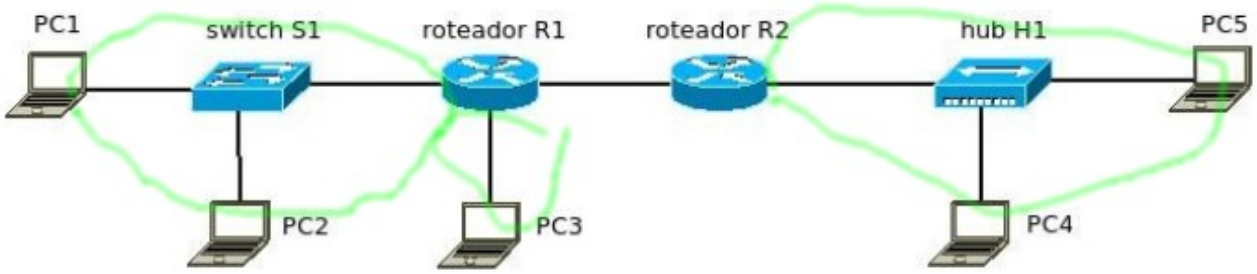
Domínio de broadcast: É o domínio de uma rede (ou subrede) reservado para o envio de uma mensagem comum a todos os equipamentos da rede (ou subrede) onde o domínio do broadcast está localizado.

Q3)

Domínio de Colisão



Domínio de broadcast



Q4)

	A	-> switch S1 ->	Roteador R1 ->	Roteador R2	
IP destino:	IP B	IP B	IP B	IP B	
IP origem:	IP A	IP A	IP A	IP A	
MAC Origem:	MAC A	MAC s1	MAC Etch1 R1	MAC Etch1 R2	-> B
MAC Destino:	MAC s1	MAC Eth0 R1	MAC Etch0 R2	MAC B	|| IP A | IP B | MAC B
	^	switch S1 <-	Roteador R1 <-	Roteador R2	||MAC Etch1 R2 | <-
IP destino:	/ | \	IP A	IP A	IP A	
IP origem:	|	IP B	IP B	IP B	
MAC Origem:	\ _	MAC s1	MAC Etch0 R1	MAC Etch0 R2	
MAC Destino:		MAC A	MAC S1	MAC Etch1 R1	

Q5)

	A	-> switch S1 ->	Roteador R1 ->	Roteador R2	
IP destino:	IP B	IP B	IP B	IP B	
IP origem:	IP A	IP A	IP R1	IP R2	
MAC Origem:	MAC A	MAC s1	MAC Etch1 R1	MAC Etch1 R2	-> B
MAC Destino:	MAC s1	MAC Eth0 R1	MAC Etch0 R2	MAC B	|| IP R1 | IP B | MAC B
	^	switch S1 <-	Roteador R1 <-	Roteador R2	||MAC Etch1 R2 | <-
IP destino:	/ | \	IP A	IP A	IP R1	
IP origem:	|	IP B	IP B	IP B	
MAC Origem:	\ _ _	MAC s1	MAC Etch0 R1	MAC Etch0 R2	
MAC Destino:		MAC A	MAC S1	MAC Etch1 R1	

Q6)
O host(1) que deseja começar a conexão manda um SYN para o servidor(2). Esse responde manda um ACK e um SYN. O host(1) manda um ACK confirmando o recebimento do SYN.

Assim inicia a conexão dos dois.

Q7)
MDI: um tipo de porta Ethernet para equipamentos diferentes: RX e TX estão invertidos, afim do receptor conversar com o Transmissor.
MDIX: um tipo de porta Ethernet para equipamentos iguais: RX e TX não estão invertidos. Assim é possível fazer cascata.

Q8)
A <-> S1 <-> S2 <-> R1 <-> R2 <-> B
| MDI | MDIX | MDI | MDIX | MDI |

Q9)
9.1)
IP: 177.032.168.223 -> 177.032.168.11011|111
Mas: 255.255.255.248 (Classe C) -> 255.255.255.11111|000

Como depois da barra todos são 1, é Broadcast.

O endereço de rede é: 177.032.168.216
O endereço de Broadcast já foi dito.

9.2)
IP: 204.20.143.0 -> 204.020.10|001111.00000000
Mas: 255.255.192.0 (Classe b) -> 255.255.11|000000.00000000

Como depois da barra nem todos são 1 ou 0, é host.

O endereço de rede é : 204.020.128.0
O endereço de Broadcast é : 204.020.191.255

9.3)
IP: 36.72.109.24 -> 036.0100100|0.01101101.00011000
Mas: 255.254.0.0 (Classe A) -> 255.1111111|0.00000000.00000000

Como depois da barra nem todos são 1 ou 0, é host.

O endereço de rede é : 177.032.168.216
O endereço de Broadcast é : 204.020.191.255

9.4)
IP: 7.26.0.64 -> 007.026.000.01|000000
Mas: 255.255.255.192 (Classe C) -> 255.255.255.11|000000

Como depois da barra todos são 0, é rede.

O endereço de rede já foi dado
O endereço de Broadcast é: 7.26.0.64

9.5)
IP: 200.201.173.187 -> 200.201.173.101110|11
Mas: 255.255.255.252 (Classe C) -> 255.255.255.111111|00

Como os 2 últimos são 1, é Broadcast.

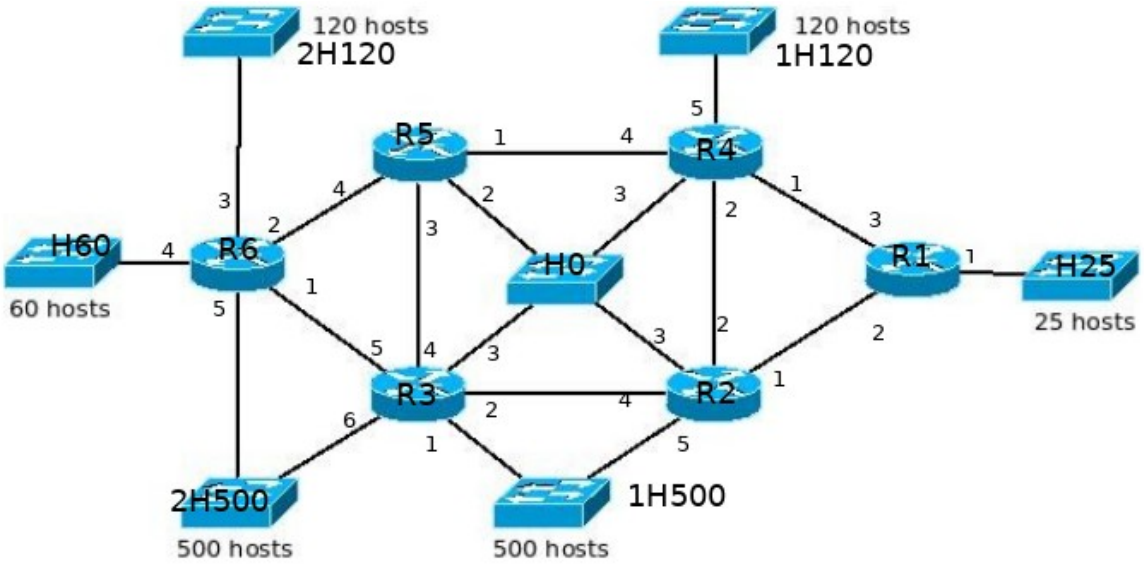
O endereço de rede é: 200.201.173.184
O endereço de Broadcast já foi dado

Q10)
10.1)
Mas:255.255.255.224 -> 255.255.255.111|00000
Ip1:240.128.192.154 -> 240.128.192.100|11010 -> Rede:240.128.192.128
IP2:240.128.192.158 -> 240.128.192.100|11110 -> Rede:240.128.192.128
Pertencem a mesma rede e ambos são hosts.

10.2)
Mas:255.255.255.248 -> 255.255.255.11111|000
IP1:87.42.141.142 -> 087.042.141.10001|110 -> Rede: 87.42.141.136
IP2:87.42.141.137 -> 087.042.141.10001|001 -> Rede: 87.42.141.136
Pertencem a mesma rede e ambos são hosts.

10.3)
Mas:255.192.0.0 -> 255.11|000000.00000000.00000000
IP1:98.45.7.17 -> 098.00|101101.00000111.00010001 -> Rede: 98.0.0.0
IP2:98.12.238.221 -> 098.00|001100.11101110.11011101 -> Rede: 98.0.0.0
Pertencem a mesma rede e ambos são hosts.

Q11) Cada um dos aparelhos dados na questão recebeu um nome.



O switch 1H500 está na rede: 187.0.0.0/23. Cujo Broadcast é: 187.0.1.255/23
A saída 5 do R2 tem o IP:187.0.1.253/23 e a saída 1 do R3 tem o IP:187.0.1.254/23

O switch 2H500 está na rede: 187.0.2.0/23. Cujo Broadcast é: 187.0.3.255/23
A saída 6 do R3 tem o IP:187.0.3.253/23 e a saída 5 do R6 tem o IP:187.0.3.254/23

O Switch 1H120 está na rede: 187.0.4.0/25. Cujo Broadcast é: 187.0.4.127/25
A saída 5 do R4 tem o IP:187.0.4.126/25

O Switch 2H120 está na rede: 187.0.4.128/25. Cujo Broadcast é: 187.0.4.255/25
A saída 3 do R6 tem o IP:187.0.4.254/25

O Switch H60 está na rede: 187.0.5.0/26. Cujo Broadcast é: 187.0.5.63/26
A saída 4 do R6 tem o IP:187.0.5.62/26

O Switch H25 está na rede: 187.0.5.64/27. Cujo Broadcast é: 187.0.5.95/27
A saída 1 do R1 tem o IP:187.0.5.94/27

O Switch H0 está na rede 187.0.5.96/29. Cujo Broadcast é: 187.0.5.103/29

A saída 3 do R4 tem o IP:187.0.5.97/29 |A saída 3 do R2 tem o IP:187.0.5.98/29

A saída 3 do R3 tem o IP:187.0.5.99/29 |A saída 2 do R4 tem o IP:187.0.5.100/29

Entre o R1 e o R2 temos uma rede: 187.0.5.104/30. Cujo cabroada é:
187.0.5.107/30

A saída 2 do R1 tem o IP:187.0.5.105/30 |A saída 1 do R2 tem o IP:187.0.5.106/30

Entre o R1 e o R4 temos uma rede: 187.0.5.108/30. Cujo broadcast é:
187.0.5.111/30

A saída 3 do R1 tem o IP:187.0.5.109/30 |A saída 1 do R4 tem o IP:187.0.5.110/30

Entre o R2 e o R4 temos uma rede: 187.0.5.112/30. Cujo broadcast é:
187.0.5.115/30

A saída 2 do R2 tem o IP:187.0.5.113/30 |A saída 2 do R4 tem o IP:187.0.5.114/30

Entre o R2 e o R3 temos uma rede: 187.0.5.116/30. Cujo broadcast é:
187.0.5.119/30

A saída 4 do R2 tem o IP:187.0.5.117/30 |A saída 2 do R3 tem o IP:187.0.5.118/30

Entre o R3 e o R5 temos uma rede: 187.0.5.120/30. Cujo broadcast é:
187.0.5.123/30

A saída 4 do R3 tem o IP:187.0.5.121/30 |A saída 3 do R5 tem o IP:187.0.5.122/30

Entre o R6 e o R3 temos uma rede: 187.0.5.124/30. Cujo broadcast é:
187.0.5.127/30

A saída 5 do R3 tem o IP:187.0.5.125/30 |A saída 1 do R6 tem o IP:187.0.5.126/30

Entre o R4 e o R5 temos uma rede: 187.0.5.128/30. Cujo broadcast é:
187.0.5.131/30

A saída 4 do R4 tem o IP:187.0.5.129/30 |A saída 1 do R5 tem o IP:187.0.5.130/30
Entre o R5 e o R6 temos uma rede: 187.0.5.132/30. Cujo broadcast é:
187.0.5.135/30

A saída 4 do R5 tem o IP:187.0.5.133/30 |A saída 2 do R6 tem o IP:187.0.5.134/30

Q12)
Os três protocolos trabalham no roteamento.
O que parece os diferenciar é na sua capacidade de atuação.
O RIP trabalha em pequeno porte (por isso foi amplamente substituído pelo OSPF)
O OSPF trabalha em pequeno e grande porte. Sendo bem flexível.
O BGP trabalha somente em altíssimo porte, criado para os principais roteadores da Internet.

Q13)
64KB= 64 * 1024= 65536 B
TCPWS=65536/0.015=4369067Bps
32KB= 32 * 1024= 32768 B
TCPWS=32768/0.015=2184533Bps
TCPWS total = 436906,6..*4=17476266,6.. Bps
TCPWST= 17MBps

Q14)
Sequence Number: Garante a entrega ordenada dos dados durante a inicialização da comunicação.
Acknowledgment: Indica que recebeu e na ordem que recebeu.
Window Size: Diz a quantidade de informação que estão sendo enviados.
Outras Flags: RST para reiniciar uma conexão e SYN para indicar/pedir o começo de uma conexão.

Q15)
O host(1) começa a conexão enviando um pacote SYN para o host(2) com o seu ISN. h2 grava o ISN de h1 e sua sequencia X(que estava no SYN).

Manda(o h2), então, um ACK com a sequencia X+1(indicando que já recebeu todos os dados até x) e envia um SYN com uma sequencia aleatória Y.

Quando h1 recebe o pacote de h2 responde com um ACK com Y+1 e, assim, termina o estabelecimento da conexão.

Depois de estabelecida o host que está enviando informações começa com um sequenciamento indicando o recebimento dos dados até então (x), um ACK(y) indicando qual é sequenciamento dos seus dados e dados.

Então a informação é ecoada, de h2 para h1. Onde os dados são mantidos, o sequenciamento agora é o valor do ACK do anterior(y) e é enviado um ACK (x+1) indicando o recebimento dos dados até 100.

Esse processo se repete, entre o h1 e o h2, e acontece ao contrário, com o h2 enviando dados para h1 e estes são ecoados.

Q16)
Se não há ecoamento dentro de um timeout, o TCP reenvia o mesmo dado com o seguimento anterior(como se estivesse mandando pela primeira vez os dados), o host que recebe um dado com o sequenciamento igual, vai retransmitir o mesmo eco anterior, caso ele tenha enviado o primeiro eco e este se perdeu no caminho. Recebendo então o eco dentro do tempo, o processo é continuado. Se for enviada uma bateria de dados e algum dos enviados for perdido, o host que recebeu ecoa enviado o ACK indicando onde foi que parou de receber. (Se é enviado 8 pacotes e o 5 foi perdido, no eco do 6, 7 e 8 ele ecoa com o ACK do 5). Assim, depois do timeout, o host que estava enviando os dados retransmite o dado perdido e o próximo eco vai vir com o ACK do ultimo pacote recebido (no caso anterior, ele enviaria o ACK do oitavo pacote, uma vez que esse foi o ultimo recebido).

Q17)
O fast retransmit é um algorítimo onde se houver três ou mais ecos indicando que não enviado um dado pacote, simplesmente duplicados, isso indica que provavelmente perdeu-se todo o segmento. Assim o TCP retransmite todo o segmento, independente do timeout.

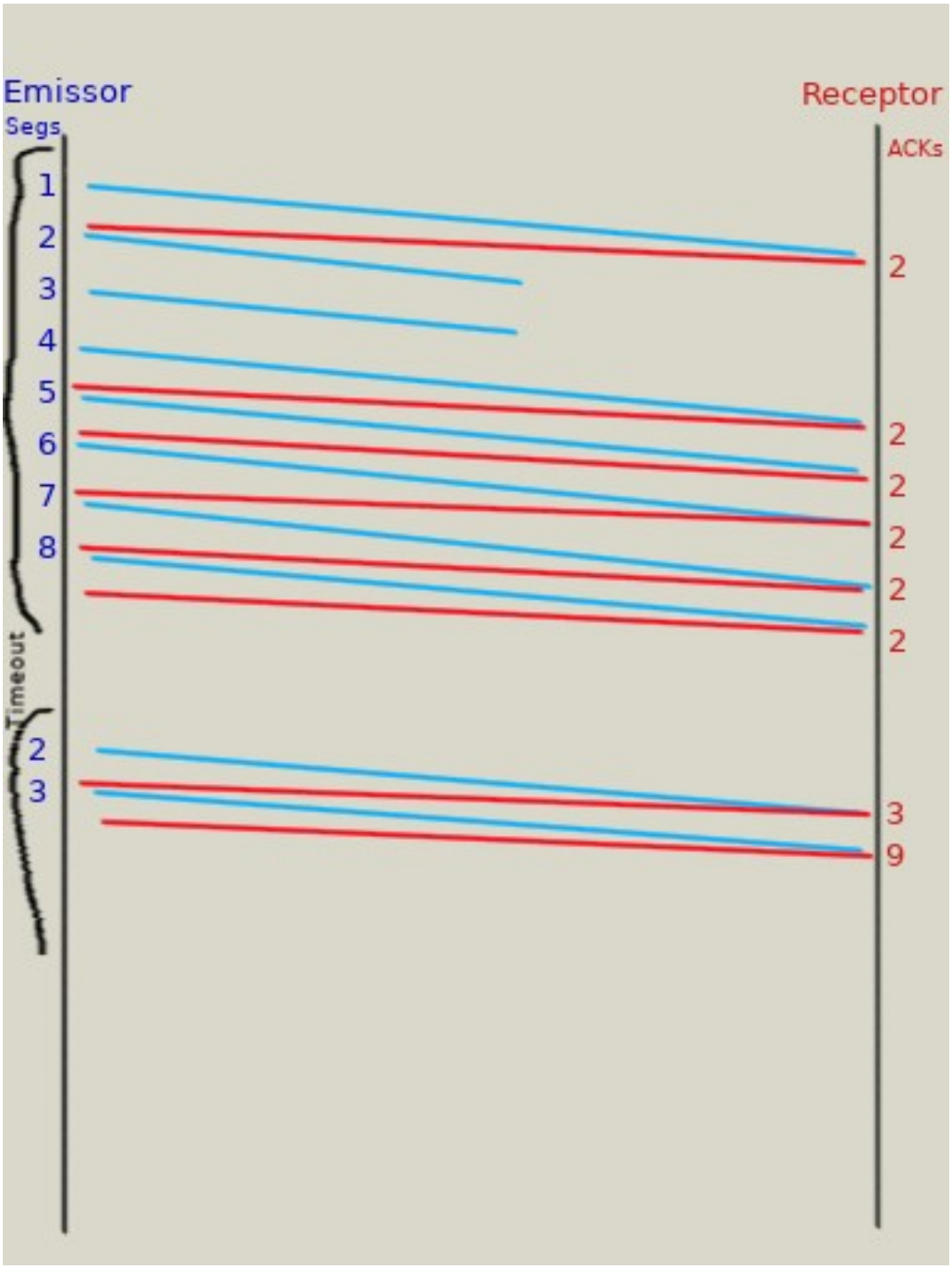
Q18)
O slow Start é um algoritmo para controlar o fluxo de ACKs de uma rede. Nele é enviado primeiramente 1 ACK, depois 2, então 4 e assim exponencialmente.

O Congestion Avoidance é outro algoritmo de controle de fluxo de ACKs. Só que nele é envidado de forma linear, de 1 em 1.

Q19)
O serrilhamento pode ser visto na forma como o TCP usa o slow start e o congestion Avoidance:
1) O TCP invoca o Slow start até o threshold (65535 bytes)
2) Depois de atingido o TCP muda para o congestion Avoidance.
3) Esse se mantêm até a detecção de 3 ACKs duplicados.
4) Nesse momento o fluxo de ACks vai para a metade.
5) Depois da queda é de novo invocado do congestion avoidance.
6) Se repete o procedimento anterior até um Time-out.
7) Se aparecer um Time-out o fluxo de pacotes volta para 1 ack e o algoritmo muda para o Slow start.
8) Repete o procedimento no item 1.

Isso se mantêm até o fim da comunicação.
A importância desse Serrilhamento é a de evitar o congestionamento e o estouro da capacidade da rede.

Q20) O azul é do emissor eu vermelho do receptor.



Q21)
Um sistema Autônomo(AS) é um possível conjunto de roteamos (podendo ter apenas um) por IP. Podendo ter um ou mais roteadores e hosts onde possuem uma política comum.

Q22)
A -> Broadcast | B->A
IP origem: IP A | IP B
IP destino: IP B | IP A
MAC origem: MAC A | MAC B
MAC destino: default | MAC A

Q23)
É um protocolo que dita como equipamentos em uma rede comum usam a tecnologia Ethernet. Usado para prevenir, detectar e tratar colisões na rede Ethernet.

Q24)
O Encapsulamento é a inserção de um cabeçalho referente as camadas do modelo OSI. Assim o dado ao ser enviado passa por um processo de Encapsulamento.
Se está na Aplicação, é colocada uma da apresentação, depois da Secção e então do transporte. Assim pode se enviar um dado entre hosts e respeitar os protocolos de suas camadas.

Q25)
No âmbito de redes, um protocolo especifico é o conjunto de regras e acordos sobre a forma como funcionará a comunicação entre computadores, switchs, roteadores e os demais elementos que atuem dentro de uma rede.