Camada de Aplicação

1. Diferencie o método de busca de arquivos das aplicações Napster, Gnutella e Kazaa.

O Napster utiliza um servidor de diretórios centralizado para a busca de arquivos, ou seja, mesmo que a transferência seja feita de modo descentralizado, o usuário, ao solicitar a transferência de um arquivo, primeiro acessa o servidor de diretórios para obter os endereços IP dos outros "peers" que possuem o arquivo desejado para, então, iniciar transferência.

Gnutella utiliza uma abordagem distribuída, ou seja, não há uso de servidores de diretórios centralizado para a busca de arquivos e peers. Ele realiza sua busca utilizando a estratégia de inundação de consultas, ou seja, o peer que necessita de um arquivo, envia uma consulta à todos os vizinhos. Se o vizinho não possuir o que foi solicitado, re-encaminha a consulta à todos seus vizinhos sempre limitando-se ao escopo definido; caso possua, responde a mensagem enviando seu endereço IP e, então, o solicitante inicia a transferência TCP.

O Kazaa utiliza o conceito de um Peer lider de um grupo de outros peers, um "pai" e seus "filhos. A busca se dá quando um peer filho envia uma query ao lider, esta query possui uma "palavra chave" do que ele deseja encontra. O lider se comunica com seus outros filhos a procura de hosts com descritores compatíveis. Se não houver nenhum, se comunica com outros lideres e estes com seus filhos. Ao encontrarem hosts com descritores compatíveis com a busca, seus IPs são encaminhados ao lider do solicitante e, então, é encaminhada esta lista ao filho solicitante. O filho, então, seleciona alguma das "opções" de hosts e estabelece uma conexão TCP para a transferência do arquivo via HTTP.

Napter: Em um servidor centralizado fica o endereço de ip e o nome dos objetos disponíveis para compartilhamento de cada peer. Um peer consulta o servidor de diretórios para obter os ip's que possuem o conteúdo específico.

Gnutella: Não possui servidor centralizado. Um peer A envia um query (consulta) para todos os peer's vizinho (máximo de 10). Se nenhum tiver, eles enviam a query para os seus vizinhos. Se algum possuir, ele retorna uma mensagem query hit.

Kazaa: combina as ideias do Napter e Gnutella. Um peer filho envia um query contendo uma palavra chave para o peer Pai. O pai encaminha uma lista de endereços de ip de host que contém essa palavra, ou então encaminha a query para os outros lideres.

2. O que é o rastreador e o torrent das aplicações bittorrent?

Rastreador verifica pares (peers) que participam do torrent.
Torrent é um grupo de pares (peers) trocando pedaços de um arquivo.

O rastreador é o mecanismo que serve para verificar peers que participam do torrent. E o torrent é o grupo de pares trocando pedaços de um arquivo.

3. Descreva o método de busca de arquivos bittorrent.

O torrent acessa o rastreador para obter lista de pares e se conecta aos pares vizinhos. Ao fazer download, par faz upload de pedaços para outros pares (que podem ir e vir constantemente).

É através do torrent de ajuntamento de peers que registra com o rastreador para obter a lista de peer's e conecta ao subconjunto desses peer's ("vizinhos")

Camada de Transporte

4. Como é realizada a demultiplexação e a multiplexação de mensagens da camada de transporte?

http://pt.wikiversity.org/wiki/Introdu%C3%A7%C3%A3o_%C3%A0s_Redes_de_Computadores/Multiplexa%C3%A7%C3%A3o_e_demultiplexa%C3%A7%C3%A3o

Demultiplexação - é a tarefa de desencapçular datagramas provenientes da camanda de rede e coloca-los em seguimentos às portas corretas na camada de transporte que serão encaminhados para a camada de aplicação.

Multiplexação - O trabalho de encapsular dados vindos de diversas portas da camada de aplicação e transformá-los em segmentos da camada de transporte que serão entregues à camada de rede.

5. Calcule o checksum para as seguintes palavras de 3 (8) bits: 01010011, 01010100 e 01110100.

Pelo o que eu entendi, viu no livro e tem nos slides (https://qacademico.ifce.edu.br/uploads/MATERIAIS_AULAS/244013-UDP.pdf). É assim: O checksum, serve para verificação de erro no udp (é, estranho udp verificando erro, mas é assim que tem no livro). Ele é a soma das mensagens de até 16bits Ele soma tudo e envia. Do lado do remetente ele faz complemento 1 da mensagem recebida. Então ele somas todas as palavras ao complemento 1 da soma das palavras. o resultado tem que ser:
1111111111111111

01010011

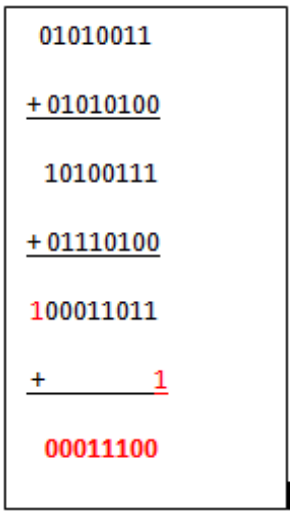
+ 01010100
10100111
+ 01110100
100011011

Como é um checksum para dados de 8 bits (1 byte) o resultado tem que ser de 8bits: então:

1|00011011

00011011
+1
00011100

(resposta da professora)



Fundamentação teórica: O checksum é utilizado para verificar se os dados recebidos estão corretos. As palavras do pacote são somadas bit a bit e, o resultado, é somado com seu complemento/bit "excedente" (caso exista), daí o valor é colocado no campo checksum do cabeçalho de transporte. No destino, as palavras do pacote recebido sofrem o mesmo processo e são comparadas ao checksum do cabeçalho.

6. Cite 5 serviços que usam portas bem conhecidas .

POP3 - 110
HTTP - 80
IM - 531
FTP - 21
TELNET - 23

SMTP - 25
HTTPS - 443
DNS - 53

7. Cite 5 serviços que usam portas registradas.

1863 - MSN MESSENGER
2948 - WAP (MMS)
1433 - MS SQL
5060 - SIP (VOIP)
2000 - CISCO SCCP (VOIP)

8. Qual a função do programa netstat?

É utilizada para se obter informações sobre as conexões de rede, tabelas de roteamento, e uma gama de informações estatísticas da utilização da interface de rede.

Listar as conexões ativas da máquina e o endereço de origem e destino e suas respectivas portas e protocolos utilizados.

Mostrar estatíticas das conexões de rede (de entrada e saída) , mostrando o seu estado da conexão.

9. Explique a função da combinação de flags dos segmentos TCP abaixo:

1. SYN

SYN = synchronized
Mensagem do tipo SYN são mensagens com requisição de conexão com o servidor ou seja sincronizar cliente e servidor para transferência de dados.

2. SYN/ACK

Mensagem de confirmação de conexão, ou seja, confirmação que o servidor pode atender as requisições do cliente.

3. ACK

Mensagem de requisição de algum dado do servidor

4. PSH/ACK

PSH = Push

Resposta a requisição de dados do cliente
Resposta do servidor. PSH vem de push.

5. RST

Resposta reset, informando a quem requereu a conexão que não tem processo do protocolo na porta determinada.

Resposta que informa que a aplicação não responde pela porta acessada

6. FYN

Indicar o fim de uma conexão

10. Suponha que o host A envie dois segmentos TCP um atrás do outro ao host B sobre uma conexão TCP. O primeiro segmento tem número de sequência 90 e o segundo 110.

1. Quantos dados tem o primeiro segmento?

   20

explicação: o seguimento A começa a com o número de sequência 90 e o seguimento B começa com o número de sequência 110. Então. 110 - 90 = 20.

2. Suponha que o primeiro segmento seja perdido, mas o segundo chegue a B. No reconhecimento que B envia a A, qual será o número de reconhecimento?

   90

explicação: O número de reconhecimento informa qual é o próximo seguimento a ser transmitido. Se ocorrer tudo ok ele retorna a próxima seguência após o ultimo seguimento transmitido. No nosso caso, como há a parca do seguimento que começa com número de sequência 90, ele retornará que deverá ser retransmitido esse seguimento. Então o número de reconhecimento será 90.

Camada de Redes

11. Quais são as duas funções mais importantes da camada de rede em uma rede de datagramas?

Roteamento e repasse.
Provê as tabelas de repasse.
Provê protocolo de roteamento que determina as rotas que os datagramas seguem

entre origem e destino, por exemplo, protocolo RIP e OSPF.

Roteamento e repasse

12. Qual a diferença de rotear e repassar?

Repasse/encaminhamento /forwarding: move os pacotes da entrada do roteador para a saída mais apropriada do roteador

Roteamento: determina a rota a ser tomada pelos pacotes da origem ao destino

Enquanto o repasse move os pacotes da entrada do roteador para a saída mais apropriada do roteador, o rotear determina a rota tomada pelos pacotes da origem ao destino;

Repasse: Quando um pacote chega ao enlace de entrada de um roteador, este deve conduzí-lo até o enlace de saída.

- **Roteamento: Determinação da rota ou caminho tomado pelos pacotes ao fluirem de remetente a um destinatário, através da utilização dos algoritmos de roteamento (serão visto nas próximas aulas).**

- **Repasse (âmbito local) e roteamento (âmbito geral).**

12. Descreva as tabelas de repasse dos roteadores de redes de datagramas.

As tabelas de repasse são utilizadas para indicar qual é a interface adequada para se alcançar determinada rede. A tabela de repasse é constituída pelo IP destino, a máscara de rede do destino e a interface do roteador a qual ela está associada (o próximo “salto” que o pacote deve efetuar).

Tabela de repasse:

- **Presente no roteador.**

- **Indica para qual das interfaces de enlace do roteador o pacote deve ser repassado.**

- **É indexada conforme cabeçalho do pacote enviado.**
- **Os algoritmos de roteamento é que definem os valores a serem inseridos nessas tabelas. Podem ser centralizados e descentralizados.**

13. Roteadores têm endereços IPs? Em caso positivo, quantos endereços eles têm?

Sim. O roteador terá o número de IPs correspondente ao número de interfaces em uso.

Sim. Tem somente um endereço IP que o identifica na rede. No caso pode-se achar seu endereço IP pelo endereço de Gateway da sua máquina.

14. qual o equivalente binário para o endereço IP 223.1.3.27?

11011111.00000001.00000011.00011011

15. Suponha que haja três roteadores entre os hosts de origem e destino. Ignorando a fragmentação, um datagrama IP enviado do host origem até o host destino transitará por quantas interfaces? Quantas tabelas de repasses serão indexadas para deslocar o datagrama desde a origem até o destino?

6 interfaces (2 para cada roteador, uma será a porta de entrada e a outra a de saída)

3 tabelas de repasses (uma para cada roteador) **obs: terceiro roteador tem uma tabela de repasse criada automaticamente para conhecer as redes diretamente conectadas a ele.**

16. Suponha que uma aplicação gera 40 bytes de dados a cada 20 milissegundos e que cada bloco seja encapsulado em um segmento TCP, e, em seguida, em um datagrama IP. Que porcentagem do datagrama será overhead (sobrecarga) e que porcentagem será dados de aplicação?

Camada Aplicação	| 40 |			
			TCP	
Camada Transporte	| 40 |	20 |		
			TCP	IP
Camada Rede	| 40 |	20 |	20 |	=> 80

Overhead de 40 bytes e mensagem de dados de 40 bytes, logo a porcentagem de dados da aplicação é de 50%. O overhead é usado para conseguir estabelecer a comunicação.

Fundamentação teórica: O overhead é a parte da mensagem que não é utilizada pela aplicação. Como exibido na ilustração acima, os dados da aplicação compoem 40bytes. Na camada de

transporte, são acrescentados 20bytes (valor default para TCP embora possa ser variável - se fosse UDP, o valor seria 8bytes) do cabeçalho TCP. Esses 20bytes não são interessantes para a aplicação em si, apenas para a comunicação e transporte dos dados. O mesmo para os 20bytes acrescentados pelo cabeçalho IP (também valor variável, considerando 20bytes como default).

17. Suponha que o host A envie ao host B um segmento TCP encapsulado em um datagrama IP. Quando o host B recebe um datagrama, como a camada de rede no host B sabe que deve passar o segmento (isto é, a carga útil do datagrama) para TCP e não para o UDP ou qualquer outra coisa?

De acordo com o campo *upper layer* existente no cabeçalho da camada de rede. Tal campo informa o protocolo utilizado pela "camada acima" (upper layer), ou seja, pela camada de transporte.

Informação extra: Na camada de enlace, um campo com mesmo objetivo existe.Tal campo é o "type". Ele informa o protocolo utilizado na camada de rede.

18. Suponha que você compre um roteador sem fio e o conecte ao modem usando um cabo. Suponha também que o seu ISP designe dinamicamente um IP a seu dispositivo conectado (isto é, seu roteador sem fio). Suponha ainda que você tenha cinco PCs em casa e que usa o 802.11 para conectá-los sem fio ao roteador também sem fio. Como são designados endereços IPs aos cinco PCs? O roteador sem fio usa NAT?

São designados, dinamicamente pelo roteador, endereços privados aos PCs.
Sim, o roteador utiliza NAT, pois foi disponibilizado apenas um endereço IP válido para 5 Pcs. Para isso, foi necessário o uso de endereços inválidos e a "tradução" destes endereços, associados às portas de comunicação, para o endereço válido no momento de comunicação com a rede.Tal associação entre o endereço IP válido, a porta do roteador, a porta do PC e o endereço inválido é realizada pela tabela NAT.

19. Use as faixas de endereços privados (RFC 1918) e o método VLSM para as seguintes configurações:

Endereços privados:
10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

1ª empresa

- Rede A = 50 hosts
- Rede B = 20 hosts

- Rede C = 8 hosts
- 2 WAN = 2 hosts cada

2ª empresa

- Rede A = 4000 hosts
- Rede B = 7000 hosts
- Rede C = 2000 hosts
- 2 WAN = 2 hosts cada

(resposta professora)

1ª Empresa – Redes Principal: 172.16.0.0/24	2 ª Empresa – Rede Principal: 10.0.0.0/8
Redes A: 50 hosts Endereço de sub-rede: 172.16.0.0 1º endereço de host: 172.16.0.1 Último endereço de host: 172.16.0.62 Endereço de broadcast: 172.16.0.63 Máscara de rede: 255.255.255.192 Tamanho do prefixo de sub-rede: 26	Rede B: 7000 hosts Endereço de sub-rede: 10.0.0.0 1º endereço de host: 10.0.0.1 Último endereço de host: 10.0.31.254 Endereço de broadcast: 10.0.31.255 Máscara de rede: 255.255.224.0 Tamanho do prefixo de sub-rede: 19
Rede B: 20 hosts Endereço de sub-rede: 172.16.0.64 1º endereço de host: 172.16.0.65 Último endereço de host: 172.16.0.94 Endereço de broadcast: 172.16.0.95 Máscara de rede: 255.255.255.240 Tamanho do prefixo de sub-rede: 27	Rede A: 4000 hosts Endereço de sub-rede: 10.0.32.0 1º endereço de host: 10.0.32.1 Último endereço de host: 10.0.47.254 Endereço de broadcast: 255.255.224.0 Máscara de rede: 255.255.240.0 Tamanho do prefixo de sub-rede: 20
Rede C: 8 hosts Endereço de sub-rede: 172.16.0.96 1º endereço de host: 172.16.0.97 Último endereço de host: 172.16.0.126 Endereço de broadcast: 172.16.0.127 Máscara de rede: 255.255.255.240 Tamanho do prefixo de sub-rede: 28	Rede C: 2000 hosts Endereço de sub-rede: 10.0.48.0 1º endereço de host: 10.0.48.1 Último endereço de host: 10.0.57.254 Endereço de broadcast: 10.0.57.255 Máscara de rede: 255.255.248.0 Tamanho do prefixo de sub-rede: 21
WAN 1: 2 hosts Endereço de sub-rede: 172.16.0.128 1º endereço de host: 172.16.0.129 Último endereço de host: 172.16.0.130 Endereço de broadcast: 172.16.0.131 Máscara de rede: 255.255.255.252 Tamanho do prefixo de sub-rede: 30	WAN 1: 2 hosts Endereço de sub-rede: 10.0.56.0 1º endereço de host: 10.0.56.1 Último endereço de host: 10.0.56.2 Endereço de broadcast: 10.0.56.3 Máscara de rede: 255.255.255.252 Tamanho do prefixo de sub-rede: 30
WAN 2: 2 hosts Endereço de sub-rede: 172.16.0.132 1º endereço de host: 172.16.0.133 Último endereço de host: 172.16.0.134 Endereço de broadcast: 172.16.0.135 Máscara de rede: 255.255.255.252	WAN 2: 2 hosts Endereço de sub-rede: 10.0.56.4 1º endereço de host: 10.0.56.5 Último endereço de host: 10.0.56.6 Endereço de broadcast: 10.0.56.7 Máscara de rede: 255.255.255.252

Tamanho do prefixo de sub-rede: 30	Tamanho do prefixo de sub-rede: 30

Tem um erro aqui

1ª Empresa – Redes Principal: 172.16.0.0/24 **Redes A: 50 hosts** **Endereço de sub-rede: 172.16.0.0** **1º endereço de host: 172.16.0.1** **Último endereço de host: 172.16.0.62** **Endereço de broadcast: 172.16.0.63** **Máscara de rede: 255.255.255.192** **Tamanho do prefixo de sub-rede: 26** **Rede B: 20 hosts** **Endereço de sub-rede: 172.16.0.64** **1º endereço de host: 172.16.0.65** **Último endereço de host: 172.16.0.94** **Endereço de broadcast: 172.16.0.95** **Máscara de rede: 255.255.255.224** **Tamanho do prefixo de sub-rede: 27** **Rede C: 8 hosts** **Endereço de sub-rede: 172.16.0.96** **1º endereço de host: 172.16.0.97** **Último endereço de host: 172.16.0.126** **Endereço de broadcast: 172.16.0.127** **Máscara de rede: 255.255.255.240** **Tamanho do prefixo de sub-rede: 28** **WAN 1: 2 hosts** **Endereço de sub-rede: 172.16.0.128** **1º endereço de host: 172.16.0.129** **Último endereço de host: 172.16.0.130** **Endereço de broadcast: 172.16.0.131** **Máscara de rede: 255.255.255.252** **Tamanho do prefixo de sub-rede: 30** **WAN 2: 2 hosts** **Endereço de sub-rede: 172.16.0.132** **1º endereço de host: 172.16.0.133** **Último endereço de host: 172.16.0.134** **Endereço de broadcast: 172.16.0.135** **Máscara de rede: 255.255.255.252** **Tamanho do prefixo de sub-rede: 30**	**2 ª Empresa – Rede Principal: 10.0.0.0/8** **Rede B: 7000 hosts** **Endereço de sub-rede: 10.0.0.0** **1º endereço de host: 10.0.0.1** **Último endereço de host: 10.0.31.254** **Endereço de broadcast: 10.0.31.255** **Máscara de rede: 255.255.224.0** **Tamanho do prefixo de sub-rede: 19** **Rede A: 4000 hosts** **Endereço de sub-rede: 10.0.32.0** **1º endereço de host: 10.0.32.1** **Último endereço de host: 10.0.47.254** **Endereço de broadcast: 255.255.224.0** **Máscara de rede: 255.255.240.0** **Tamanho do prefixo de sub-rede: 20** **Rede C: 2000 hosts** **Endereço de sub-rede: 10.0.48.0** **1º endereço de host: 10.0.48.1** **Último endereço de host: 10.0.57.254** **Endereço de broadcast: 10.0.57.255** **Máscara de rede: 255.255.248.0** **Tamanho do prefixo de sub-rede: 21** **WAN 1: 2 hosts** **Endereço de sub-rede: 10.0.56.0** **1º endereço de host: 10.0.56.1** **Último endereço de host: 10.0.56.2** **Endereço de broadcast: 10.0.56.3** **Máscara de rede: 255.255.255.252** **Tamanho do prefixo de sub-rede: 30** **WAN 2: 2 hosts** **Endereço de sub-rede: 10.0.56.4** **1º endereço de host: 10.0.56.5** **Último endereço de host: 10.0.56.6** **Endereço de broadcast: 10.0.56.7** **Máscara de rede: 255.255.255.252** **Tamanho do prefixo de sub-rede: 30**

1. Quantos endereços irão sobrar em cada rede?

Camada de Enlace

20. Qual a diferença de LAN e Ethernet?

Uma LAN é uma rede de computadores concentrada em um área geográfica.

LAN é uma rede local. Ethernet é um protocolo de comunicação da rede.

21. Como um endereço MAC é representado? Como um endereço MAC é dividido?

É composto de 48 número binários representado por 12 números hexadecimais.
É dividido em 6 campos de dois números hexadecimais.
Exemplo de endereço MAC: FA-11-32-B1-6F-D1
Os três primeiros campos são destinados para identificar o fabricante da placa de interface de rede e os outros três campos restantes é seu identificador, que deve ser único.

Os 3 primeiros bytes destinados para a idetificação do fabricante da placa.
Os 3 últimos bytes são destinados a um identificador único de uma máquina.

22. Qual a utilidade de um endereço MAC?

Endereços MAC provêm uma forma para que os computadores identifiquem eles mesmos. Isso dá a cada host um nome único e permanente.

É uma forma de os computadores identificarem outros unicamente pela rede. Endereços IPs servem para estabecer rotas e podem ser dinâmicos, já o endereço MAC é único e não pode ser modificado(em teoria, a modificação do endereço MAC é considerado crime), gerando um meio de identificar um computador em uma rede.

23. O que é um frame Ethernet?

Um frame Ethernet é um datagrama adicionado aos dados da camada de enlace “empacotados” em um quadro (frame).

Os frames Ethernet são "envelopes" para os pacotes TCP/IP. O aplicativo (um navegador, um servidor web, ou qualquer outro aplicativo transmitindo dados pela rede) envia os dados ao sistema operacional, que divide o stream em pacotes TCP/IP e os envia à placa de rede. As placas de rede (que não entendem o protocolo TCP/IP) tratam os pacotes como um fluxo de dados qualquer e adicionam mais uma camada de endereçamento, desta vez baseada nos endereços MAC dos dispositivos da rede, gerando o frame Ethernet que é finalmente transmitido. Ao chegar do outro lado, o

"envelope" é removido e o pacote TCP/IP é entregue.

24. Diferencie rede serial (ponto-a-ponto) de rede multiacesso.

Uma rede serial corresponde a uma rede em que apenas dois dispositivos podem se comunicar/conectar. Geralmente é a rede entre dois roteadores.
Uma rede de multiacesso é aquela em que permite o acesso de mais de dois dispositivos. Pode ser encontrada em redes com o uso de switchs ou hubs.

25. Em que consiste uma topologia em barra. Explique o processo de envio e recebimento de quadros em uma topologia em barra.

Uma Topologia em barra usa um único segmento no qual todos os hosts se conectam diretamente. Desta maneira, Hubs Ethernet trabalham implementando topologia em "barra".
Quando a informação (frame/quadro) é transmitida, toda placa de rede (a barra) no meio compartilhado copia parte do frame transmitido para ver se o endereço de destino é o seu endereço físico. Se é o mesmo, então o resto do frame é copiado. Caso contrário, o resto do frame é ignorado.
Se mais de um computador tenta transmitir ao mesmo tempo, há colisão.

26. O que é colisão? Quando uma colisão ocorre?

Colisão, como o próprio nome diz é quando ocorre conflito de mensagens que estão sendo enviadas no mesmo momento pelo mesmo meio físico. Ocorre quando dois dispositivos estão enviando seus dados no mesmo instante pelo mesmo meio físico.

27. Explique o método de contenção CSMA/CD.

CSMA/CD é um método de contenção comum usado pelo Ethernet, em uma topologia em Barra, a fim de evitar colisões. Ele funciona a partir da ideia de "escutar" o meio compartilhado para verificar se está em uso ou não. Se não estiver, permite acesso ao meio. Se dois PCs acessarem ao mesmo tempo, ocorrerá uma colisão. Neste momento, um sinal de obstrução é enviado ao primeiro PC que detecta a colisão. Este irá utilizar um esquema de prioridade ou de backoff aleatório para calcular um tempo de espera para uma nova transmissão. Se novas colisões ocorrerem, o intervalo é duplicado.

O método CSMA/CD é um protocolo que tenta evitar colisões na transmissão de dados quando esse meio é compartilhado com outras máquinas.
CS - Carrier Sense - Capacidade de detectar se algum dado está sendo transmitido
MA - Multiple Access - Permite que vários equipamentos enviem dados, sem definir

prioridades.
CD - Collision Detection - Capaz de detectar colisões e trabalhar com erros.

Ou seja, o protocolo verifica se algum dado está sendo transmitido no meio físico, se não detectar nenhum dado no meio ele inicia o envio de dados, caso detecte, espera o término da mensagem para tentar enviar seus dados.

28. Diferencie repetidor de hub.

Repetidor apenas recebe um sinal, amplifica esse sinal que estava fraco e repassa.. No repetidor, só há um objeto físico que trabalha com detecção do sinal, filtragem e amplificação do sinal. É usado para estender uma rede para grandes distâncias.
Hub é um pequeno aparelho que ao receber um sinal esse repassa para todas as outras portas, exceto a porta da qual a mensagem veio. Não trabalha com roteamento. Faz uma inundação na rede.

29. Caracterize o modo Half Duplex e Full Duplex.

Half Duplex usa um meio físico somente para envio ou recebimento, não podendo ocorrer as duas coisas ao mesmo tempo. Se assim ocorrer há colisões e perda da mensagem.
Full Duplex permite que um mesmo meio físico possa ser usado tanto para receber quanto para enviar ao mesmo tempo usando aquele meio físico.

30. Em que consiste um domínio de colisão?

Um domínio de colisão consiste em um grupo de dispositivos que estão conectados de modo que apenas um pode transmitir por vez.Caso contrário, haverá colisões.

Numa rede de computadores, o domínio de colisão é uma área lógica onde os pacotes podem *colidir* uns contra os outros, em particular no protocolo Ethernet . Quanto mais colisões ocorrerem menor será a eficiência da rede.

31. Explique o algoritmo de comutação de switches que envolve os processor de filtering, forwarding e flooding.

Filtering
Após o switch aprender os MAC address e associá-los as respectivas portas, os benefícios do switch podem ser verificados através do Filtering (Filtro).
Quando dois dispositivos conhecidos tentam se comunicar através do switch, o frame do host de origem é encaminhado direta e unicamente para porta do host de destino.

Forwarding

Forwarding é o encaminhamento de um frame de um host conhecido (que está na CAM table) associado a uma porta para outro host conhecido localizado em uma porta do switch.

Flooding
Quando o switch não tem uma entrada na CAM table para um endereço (MAC address) específico, ele então encaminha o frame para todas as portas, menos para porta que recebeu o frame. Este procedimento é conhecido com flooding.

32. De que maneira o switch aprende sozinho como enviar os frames Ethernet a um certo destino?

Um switch possui uma tabela de comutação entrada na tabela de comutação:(Endereço MAC, Interface, Carimbo de tempo);
Entradas antigas na tabela são descartadas (TTL pode ser de 60 min)switch aprende que hosts podem ser alcançados através de quais interfaces quando um quadro é recebido;
O switch "aprende" a localização do transmissor: segmento de LAN de onde ele veio registra o par transmissor/localização na tabela de comutação

33. Para que serve a técnica de Aging dos switches?

O switch mantém uma tabela de endereços MAC das interfaces das máquinas da rede para otimizar o envio de dados. O aging é o tempo em que aquele endereço permanecerá na máquina para otimizar a memória do switch.

34. Quando é usado o cabo paralelo(Straight-Through)? Cite exemplos.

Um cabo straight-trough é utilizado para conectar aparelhos de tecnologias diferentes. Por exemplo, ligar um roteador à um pc, um switch à um pc, um switch à um roteador...

35. Quando é usado o cabo cruzado (cross-over)? Cite exemplos.

Um cabo cross-over é utilizado para conectar aparelhos de mesma tecnologia. Por exemplo, ligar dois roteadores, dois switches, um switch à um hub...

36. Para que serve o campo preamble de um frame Ethernet?

Sincronizacao das interfaces de rede
sequencia de bits que avisa que está chegando o quadro ethernet

The preamble is a 64-bit (8 byte) field that contains a synchronization pattern consisting

of alternating ones and zeros and ending with two consecutive ones. After synchronization is established, the preamble is used to locate the first bit of the packet. The preamble is generated by the LAN interface card.

37. Diferencie endereço unicast, broadcast e multicast.

Unicast: mensagem de um host para outro host.
Broadcast: mensagem de um host para todos os hosts de uma rede.
Multicast: mensagem de um host a um grupo determinado de hosts de uma rede.

Endereço Unicast é quando uma máquina envia uma informação especificamente para outra máquina.
Endereço Broadcast é quando uma máquina envia uma informação para todas as máquinas que na rede que possam lhe escutar.
Endereço Multicast é quando uma máquina manda pacotes eficientemente para múltiplos pontos distintos, ao mesmo tempo. Ou seja, envia para várias máquinas ao mesmo tempo, não necessariamente para todas, nem para uma só.

38. Para que serve o campo type de um frame Ethernet?

O campo Type é um campo do cabeçalho do quadro da camada de enlace que informa qual o protocolo utilizado no datagrama da camada de rede.

39. O que acontece com os dados de um frame Ethernet, se este for menor que 46 bytes?
"Haverá atenuação(perda de dados), pois esse limite é imposto pelo protocolo Ethernet."(Nídia Campos)

Se os dados a serem enviados forem menor que o tamanho permitido (46 bytes), o campo de dados será preenchido com bits – padding bytes, até chegar ao tamanho mínimo. No receptor, o protocolo da camada de rede (IP), detectará os padding bytes e os removerá.

40. Diferencie CRC, Verificação de paridade, soma de verificação da Internet.
Verificação de paridade: Ele consiste em ser adicionado, pelo transmissor, um bit de redundância (bit de paridade) após ou antes da seqüência de bits que pertence à mensagem. Esse bit adicionado segue a seguinte regra:
caso apareça o bit "1" número impar de vezes é adicionado 1, exemplo: 0100101 paridade = 1;
caso apareça o bit "1" número par de vezes é adicionado 0, exemplo: 010101010010100, paridade = 0;

CRC: O CRC, também conhecido como método de detecção polinomial, é um processo

de verificação de erros mais sofisticado que os anteriores, permitindo que se detecte praticamente a ocorrência de qualquer grupo de erros.
A técnica de verificação cíclica é executada por ambas as estações transmissora e receptora e consiste na divisão de todos os bits de um bloco por um valor binário constante (polinómio gerador). O quociente é desprezado e o resto desta operação será o carácter de verificação que será transmitido.

Soma de Verificação da Internet (checksum): consiste em transmitir todas as palavras junto com o resultado da soma dos bits delas. Dado os dados iniciais de duas palavras de 8 bits: 00111101 00001101, estes valores são somados dando resultado ao checksum: 01001010. 00111101+00001101 = 01001010 -> Checksum 10110101 -> Checksum invertido
O emissor envia o checksum invertido ao receptor. Em seguida, como o próprio nome desse método já diz, no receptor as palavras são novamente somadas e comparadas com checksum que foi enviado, ou seja, checar a soma.
Para a detecção de algum erro, se em qualquer dos dados transmitidos terem algum erro irá ser descoberto, pois no receptor é recalculado e ocorre a soma do novo checksum com o checksum enviado que terá um resultado diferente de "1".

Verificação de paridade:

O valor obtido é acrescentado no pacote e o mesmo processo é efetuado no destino. Ao terminar, os dois valores são comparados a fim de verificar se a informação foi transmitida corretamente.
Adiciona um 8º bit que deixa a mensagem com um número de "1s" par ou ímpar. Vai depender do que foi definido.

CRC:

Realiza cálculos baseado em polinômios. O resultado obtido no transmissor deve ser igual ao obtido no receptor.

Soma de verificação de internet (checksum):

O checksum faz uma soma bit a bit das palavras do pacote enviado adicionando, também, o complemento obtido. Este valor é enviado junto com o cabeçalho do segmento do pacote e, no destino, a mesma soma é realizada com os dados obtidos e é comparado o resultado com o valor no cabeçalho. Se for igual, os dados foram recebidos corretamente; se der diferente, houve algum problema na transferência de dados.

41. Para que serve o protocolo ARP?

O protocolo ARP tem como função associar um endereço IP ao seu endereço MAC.

Fundamentação teórica: Quando um dispositivo quiser enviar uma mensagem à outro, ele

envia uma mensagem informando seu IP. Para que a mensagem possa ser enviada, a camada de enlace precisa do endereço MAC. Para isso, é acessada a tabela ARP existente no dispositivo interessado. A tabela possui a associação de um endereço IP à um endereço MAC. Se a tabela possui o endereço, ela disponibiliza o endereço MAC para a camada de enlace poder continuar a transmissão da mensagem. Se o valor não é conhecido na tabela, é verificado se o endereço IP a ser acessado é da mesma rede. Se for, é enviada uma requisição ARP cujo endereço destino será o broadcast e, então o dispositivo que possuir o IP desejado responde à requisição e, assim, a tabela ARP é populada com a informação. Caso não seja da mesma rede, o datagrama é enviado para o gateway da rede, em que este verificará em sua tabela de roteamento o caminho para chegar à desejada rede e, ao chegar, o roteador conectado diretamente à rede verificará sua tabela ARP para obter o endereço MAC do dispositivo. Se ela não possuir, sofrerá o mesmo processo de rede local para, então, alcançar o dispositivo final desejado. Este responderá a mensagem populando a tabela ARP do roteador de sua rede e este enviará o datagrama para o host final..

Obs:. Segundo os slides, a tabela ARP também tem uma coluna de TTL (o que faz sentido).

42. Como um host encontra o endereço MAC destino de outro host na mesma LAN? E em LANs diferentes?

Em ambos, é feito o uso da tabela ARP. O host verifica se já possui um endereço MAC associado ao endereço IP. Se sim, prossegue com as atividades. Se não, verifica se o IP é da rede local ou não.

Em uma mesma LAN:

> É enviada uma requisição ARP para broadcast a fim de que o host desejado, quando responder, popule a tabela ARP.

Em LANS diferentes:

> É enviada o datagrama para o gateway (se não possuir o endereço MAC do gateway, o mesmo procedimento realizado anteriormente é feito). O roteador (gateway) irá acessar sua tabela de repasse para verificar qual interface deve acessar para alcançar a rede destino. Ao chegar na rede destino, o roteador verificará sua tabela ARP para enviar a mensagem ao host destino. Se ele não possuir, o mesmo é feito como nos outros casos. Se possuir, envia o datagrama para o host destino.

Camadas

Física

A camada física define as especificações elétricas, mecânicas, procedurais e funcionais para ativação, manutenção e desativação do enlace físico entre sistemas finais

Dispositivos da camada 1 incluem : Repetidores e Hubs.

Enlace

A camada de enlace de dados provem o trânsito confiável de dados sobre um link físico. A camada de enlace se preocupa com o endereçamento físico (MAC), com a topologia da rede, com o acesso da rede, notificações de erro, com a entrega ordenada de frames (quadros) e controle de fluxo.

Dispositivos de Camada 2: Switches e Bridges (Pontes)