GRIS - Processo Seletivo - TAG Redes
Filipe Augusto da Silva

Questão 1

Camada	Protocolo
7 - Aplicação	A camada de aplicação corresponde às aplicações (programas) no topo da camada OSI que serão utilizadas para promover uma interação entre a máquina-usuário (máquina destinatária e o usuário da aplicação). Esta camada também disponibiliza os recursos (protocolo) para que tal comunicação aconteça.
6 - Apresentação	A camada de Apresentação, também chamada camada de Tradução, converte o formato do dado recebido pela camada de Aplicação em um formato comum a ser usado na transmissão desse dado, ou seja, um formato entendido pelo protocolo usado. Um exemplo comum é a conversão do padrão de caracteres (código de página) quando o dispositivo transmissor usa um padrão diferente do ASCII. Pode ter outros usos, como compressão de dados e criptografia.
5 - Sessão	Responsável pela troca de dados e a comunicação entre hosts, a camada de Sessão permite que duas aplicações em computadores diferentes estabeleçam uma comunicação, definindo como será feita a transmissão de dados, pondo marcações nos dados que serão transmitidos.
4 - Transporte	A camada de transporte é responsável por receber os dados enviados pela camada de sessão e segmentá-los para que sejam enviados a camada de rede, que por sua vez, transforma esses segmentos em pacotes. No receptor, a camada de Transporte realiza o processo inverso, ou seja, recebe os pacotes da camada de rede e junta os segmentos para enviar à camada de sessão.
3 - Rede	A camada de rede fornece os meios funcionais e de procedimento de transferência de comprimento variável de dados de sequências de uma fonte de acolhimento de uma rede para um host de destino numa rede diferente, enquanto se mantém a qualidade de serviço requerido pela

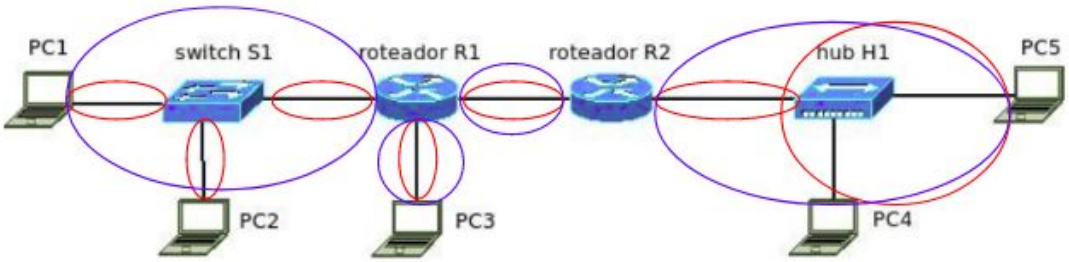
	camada de transporte. A camada de rede realiza roteamento de funções, e também pode realizar a fragmentação e remontagem e os erros de entrega de relatório.
2 - Enlace	Esta camada detecta e, opcionalmente, corrige erros que possam acontecer no nível físico. É responsável por controlar o fluxo (recepção, delimitação e transmissão de quadros) e também estabelece um protocolo de comunicação entre sistemas diretamente conectados.
1 - Física	Sendo a camada mais baixa do modelo OSI, diz respeito a transmissão e recepção do fluxo de bits brutos não-estruturados em um meio físico. Ela descreve as interfaces elétricas, ópticas, mecânicas e funcionais para o meio físico e transporta sinais para todas as camadas superiores.

Questão 2

Domínio é um nome que serve para localizar e identificar conjuntos de computadores na Internet. Este nome foi concebido com o objetivo de facilitar a memorização dos endereços de computadores na Internet. Isto é, sem ele, teríamos que memorizar uma sequência grande de números.

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 ocorrem menor é a eficiência da rede. Um domínio de colisão pode existir num único segmento da rede (como numa rede em barramento) ou numa porção ou total de uma rede maior (note-se que a utilização de hubs faz propagar o domínio de colisão a todos os seus segmentos).

Questão 3



Descrição:

- Domínio de colisão em vermelho.
- Domínio de broadcast em azul.

Questão 4

Para A enviar um pacote para B, A precisa do IP de B, assim, basicamente, A verifica a sua tabela ARP para saber se já existe alguma informação relativamente ao endereço físico de B, como no nosso caso do envio de informação é para fora do domínio da rede local, o endereço físico a ser registrado na tabela ARP de A será o endereço físico do *gateway*, R1, tendo como origem o IP A. Assim, fisicamente é enviado ao switch S1. Sempre que um equipamento envia uma frame, o switch analisa o endereço MAC de destino e comuta a frame para a porta onde se encontra a máquina de destino.

Quando R1 recebe o pacote e avalia o destino B, vê que a única opção em sua tabela de encaminhamento seria o R2, como visto na imagem, logo, encaminha-se ao IP de R2, sendo que o MAC de R2 está na tabela ARP de R1.

Quando R2 recebe o pacote e avalia o destino B, percebe que há uma saída que corresponde ao IP/MAC de B em uma das entradas da sua tabela de encaminhamento, assim, R2 encaminha diretamente para B.

A mensagem de confirmação é enviada de forma semelhante, como se fosse um novo pacote, tendo como origem IP B e destino IP A.

Questão 5

Para A enviar um pacote para B, A precisa do IP de B, assim, basicamente, A verifica a sua tabela ARP para saber se já existe alguma informação relativamente ao endereço físico de B, como no nosso caso do envio de informação é para fora do domínio da rede local, o endereço físico a ser registrado na tabela ARP de A será o endereço físico do gateway, R1, tendo como origem o IP **traduzido de** A. Assim, fisicamente é enviado ao switch S1. Sempre que um equipamento envia uma frame, o switch analisa o endereço MAC de destino e comuta a frame para a porta onde se encontra a máquina de destino.

Quando R1 recebe o pacote e avalia o destino B, vê que a única opção em sua tabela de encaminhamento seria o R2, como visto na imagem, logo, encaminha-se ao IP de R2, sendo que o MAC de R2 está na tabela ARP de R1.

Quando R2 recebe o pacote e avalia o destino B, percebe que há uma saída que corresponde ao IP/MAC de B em uma das entradas da sua tabela de encaminhamento, assim, R2 encaminha diretamente para B.

A mensagem de confirmação é enviada de forma semelhante, como se fosse um novo pacote, tendo como origem o IP de B e destino o IP **traduzido de** A.

Questão 6

Um handshake de três vias é usado principalmente para criar uma conexão de soquete TCP. Funciona quando:

- Um nó cliente envia um pacote de dados SYN por uma rede IP para um servidor na mesma rede ou em uma rede externa. O objetivo deste pacote é perguntar / inferir se o servidor está aberto para novas conexões.
- O servidor de destino deve ter portas abertas que possam aceitar e iniciar novas conexões. Quando o servidor recebe o pacote SYN do nó do cliente, ele responde e retorna um recibo de confirmação - o pacote ACK ou o pacote SYN / ACK.
- O nó do cliente recebe o SYN / ACK do servidor e responde com um pacote ACK. Após a conclusão desse processo, a conexão é criada e o host e o servidor podem se comunicar.

Questão 7

MDI / MDIX é um tipo de conexão de porta Ethernet usando cabeamento de par trançado. O MDI (medium dependent interface) é o componente da unidade de conexão de mídia (MAU) que fornece a conexão física e elétrica ao meio de cabeamento. Um MDIX (para crossover MDI) é uma versão do MDI que permite a conexão entre dispositivos semelhantes. As portas MDI se conectam às portas MDIX através de cabeamento de **par trançado direto**; as conexões MDI para MDI e MDIX para MDIX usam cabos de **par trançado cruzado**.

Questão 8

MDI: A, B, R1 e R2; **MDIX**: S1 e S2

Ligações:

- Par trançado direto: A e S1; S2 e R1;
- Par trançado cruzado: S1 e S2; R1 e R2; R2 e B

Questão 9

1) Classe B - Rede: 177.32.168.216; Broadcast: 177.32.168.223; Host: 177.32.168.[217-222]
2) Classe C - Rede: 204.20.128.0; Broadcast: 204.20.191.255; Host: 204.20.128.1 - 204.20.191.254
3) Classe A - Rede: 36.72.0.0; Broadcast: 36.73.255.255; Host: 36.72.0.1 - 36.73.255.254
4) Classe A - Rede: 7.26.0.64.; Broadcast: 7.26.0.127; Host: 7.26.0.[65-126]
5) Classe C - Rede: 200.201.173.184; Broadcast: 200.201.173.187; Host: 200.201.173.[185-186]

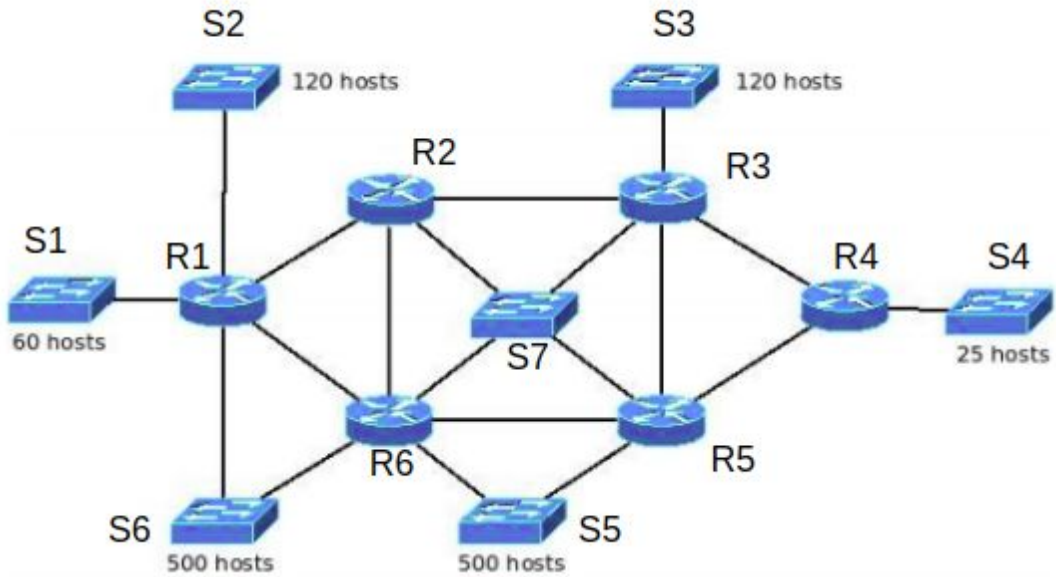
Questão 10

1) Endereços para o primeiro endereço de rede do enunciado: 240.128.192.[128-159]. Assim, ambos estão na mesma rede.
2) Endereços para o primeiro endereço de rede do enunciado: 87.42.141.[136-143]. Assim, ambos estão na mesma rede.

3) Endereços para o primeiros endereço de rede do enunciado: 98.0.0.0 - 98.63.255.255. Assim, ambos estão na mesma rede.

Questão 11

O projeto de endereçamento de rede pode ser feito de diversas formas, entretanto, escolhi dividir as redes da seguinte forma:



Há um total de 15 redes, são formadas por:

1. R1 e S2 - 187.11.0.0/25
2. R1 e S1 - 187.12.0.0/26
3. R1 e S6 - 187.13.0.0/23
4. R1 e R2 - 187.2.0.0/30
5. R1 e R6 - 187.1.0.0/30
6. R2 e R3 - 187.3.0.0/30
7. R2 e R6 - 187.8.0.0/30
8. R3 e S3 - 187.14.0.0/25
9. R3 e R5 - 187.7.0.0/30
10. R3 e R4 - 187.4.0.0/30
11. R4 e S4 - 187.15.0.0/27
12. R4 e R5 - 187.5.0.0/30

13. R5 e R6 - 187.6.0.0/30
14. R5, R6 e S5 - 187.16.0.0/23
15. R2, R3, R5, R6 e S7 - 187.0.0.0/29

Questão 12

Se os roteadores estão usando o protocolo RIP, eles enviarão suas tabelas de roteamento para todos os roteadores que eles têm acesso a cada 30 segundos. A tabela de roteamento contém todas as redes que os roteadores conhecem e como alcançá-las, além da distância (dada em número de saltos) até elas.

Apesar do seu nome, o protocolo OSPF não procurar o caminho mais curto, mas sim o caminho mais rápido. Quando os roteadores usam o protocolo OSPF, eles verificam o estado dos outros roteadores que eles têm acesso de tempos em tempos enviando mensagens chamadas “hello”. Através destas mensagens eles sabem se um roteador está operacional e qual é o seu estado. Outra diferença é que usando o OSPF os roteadores conhecem todos os caminhos que podem ser usados para alcançar um determinado destino, enquanto que roteadores RIP conhecem apenas o caminho mais curto. Uma terceira diferença é que roteadores baseados no RIP enviarão suas tabelas de roteamento inteiras a cada 30 segundo, aumentando o tráfego da rede.

O BGP é um protocolo usado em redes grandes, como a Internet – na verdade o BGP é o protocolo usado pelos roteadores da Internet. Como tal, ele é classificado como um protocolo externo, enquanto que o RIP e o OSPF são classificados como protocolos internos – já que eles são usados em redes que estão sob a mesma administração. O BGP agrupa roteadores e computadores sob uma mesma administração em uma unidade chamada Sistema Autônomo (SA) – por exemplo, todos os roteadores e computadores que pertencem ou estão conectados ao mesmo provedor de Internet fazem parte de um mesmo SA. O BGP é chamado IBGP (Interno) se trabalha dentro de um mesmo sistema autônomo ou de EBGP (Externo) se trabalha entre dois sistemas autônomos diferentes.

Questão 13

Throughput: 66,66 Mbps

Cálculo:

(((3×64×1024×8) + (2×32×1024×8))÷(0,015×2))÷1024÷1024

Explicação sequencial dos fatores das expressões:

- (**3×64×1024×8**)
    - **3** janelas TCP Window Size, **64** KB, **1024** para conversão em bytes, **8** para conversão em bits.
- (**2×32×1024×8**)
    - **2** janelas TCP Window Size, **32** KB, **1024** para conversão em bytes, **8** para conversão em bits.
- (**0,015×2**)
    - **0.015** latência para chegar ao destino e **2** para considerar o tempo de ida e volta (*roundtrip)*.
- (**1024**)
    - **1024** para conversão em Kbps (quilobits por segundo).
- (**1024**)
    - **1024** para conversão em Mbps (megabits por segundo).

Questão 14

Número de sequência (32 bits): identifica a posição no fluxo de bytes do segmento enviado pelo transmissor. O número de sequência refere-se ao fluxo de dados que vai na mesma direção do segmento.

Número de Reconhecimento (32 bits): este campo identifica a posição do byte mais alto (ou último byte) que o fonte recebeu. O número de reconhecimento refere-se ao fluxo de dados na direção contrária ao segmento. Os reconhecimentos sempre especificam o número do próximo byte que o receptor espera receber.

O transmissor limita os dados não reconhecidos ao tamanho da janela de recepção. O valor da janela (RcvWindow) é informado nos segmentos.

Flags:

- A primeira flag é a Urgent Pointer. Este sinalizador é usado para identificar os dados recebidos como 'urgentes'. Esses segmentos de entrada não precisam esperar até que os segmentos anteriores sejam consumidos pela extremidade receptora, mas são enviados diretamente e processados imediatamente.
- O sinalizador de reconhecimento é usado para confirmar o recebimento bem-sucedido de pacotes.
- O sinalizador Push, como o sinalizador Urgente, existe para garantir que os dados recebam a prioridade (que merece) e sejam processados no final do envio ou

recebimento. Esse sinalizador específico é usado com bastante frequência no início e no final de uma transferência de dados, afetando a maneira como os dados são tratados nas duas extremidades.

- O sinalizador de redefinição é usado quando chega um segmento que não se destina à conexão atual. Em outras palavras, se você enviasse um pacote a um host para estabelecer uma conexão e não existisse um serviço aguardando resposta no host remoto, o host rejeitaria automaticamente sua solicitação e enviaria uma resposta com o sinalizador RST definido. Isso indica que o host remoto redefiniu a conexão.
- O quinto sinalizador contido nas opções de sinalizador TCP é talvez o sinalizador mais conhecido usado nas comunicações TCP. O SYN é enviado inicialmente ao estabelecer o handshake clássico de três vias entre dois hosts.
- A flag FIN representa a palavra FINished. Esse sinalizador é usado para derrubar as conexões virtuais criadas usando o sinalizador anterior (SYN); portanto, por esse motivo, o sinalizador FIN sempre aparece quando os últimos pacotes são trocados entre uma conexão.

Questão 15

- Um timeout é iniciado toda vez que um segmento é transmitido.
- O timeout é cancelado quando o ACK correspondente é recebido.
- Se um pacote é perdido mas os pacotes seguintes são recebidos, são enviados ACKs de mesmo valor (duplicados).
- O recebimento de três ACKs duplicados força a retransmissão do segmento perdido e cancela o timeout (fast retransmit).

Questão 16

TCP usa um mecanismo chamada de “partida lenta” para aumentar a janela de congestionamento depois que uma conexão é inicializada ou depois de um *timeout*. Inicia-se com uma janela, um pequeno múltiplo do tamanho do Maximum Segment Size (MSS). Embora a taxa inicial seja baixa, a taxa de crescimento é muito alta; para cada pacote reconhecimento, a janela de congestionamento aumenta em 1 MSS, então, efetivamente, a janela de congestionamento dobra para cada *roundtrip time* (RTT).

Questão 17

Caso o TCP receba três reconhecimentos duplicados antes de um estouro de temporizador, o mesmo saberá que o outro lado deve ter recebido pacotes fora de ordem, o que sugere que o pacote anterior tenha sido perdido ou está atrasado. Neste caso, o emissor retransmite imediatamente o pacote solicitado, o que é chamado retransmissão rápida. Além disto, o TCP ele reduz o tamanho da janela de congestionamento para a metade de seu valor corrente e volta a crescer linearmente. Este algoritmo é chamado de aumento aditivo, dimuinuição multiplicativa (AIMD - additive-increase, multiplicative-decrease).

Questão 18

Partida lenta: Assim que a conexão TCP é estabelecida, a aplicação remetente escreve bytes no buffer de envio do TCP emissor. O TCP agrupa os bytes em segmentos de tamanho MSS e envia para a camada rede para transmissão. Inicialmente a janela de congestionamento é igual a um MSS. Isto significa que o TCP envia um segmento e espera por um reconhecimento. Se este segmento foi reconhecido antes do estouro do temporizador, o TCP dobra o tamanho da janela de congestionamento, passando a enviar dois segmentos. Se receber reconhecimentos novamente, volta a dobrar o tamanho da janela para quatro, e assim por diante.

Prevenção de congestionamento: A fase de partida lenta termina quando o tamanho da janela atinge o valor de limiar (threshold). A partir deste momento a janela continua a crescer linearmente, um MSS para cada RTT. Esta fase é chamada de prevenção de congestionamento. Se houver um estouro de temporização, o valor do limiar é ajustado para a metade do valor corrente da janela, e a janela é ajustada para um MSS, reiniciando o processo de partida lenta.

Questão 19

Esse comportamento do TCP de estar sempre aumentando a janela de congestionamento lentamente e depois reduzindo à metade bruscamente gera um comportamento parecido com dentes de serra, se visualizado graficamente. É uma necessidade de distribuição justa de recursos para melhorar o desempenho da rede. O aumento aditivo e a diminuição multiplicativa (AIMD) é uma das melhores técnicas de controle de congestionamento para redes TCP, obtém uma justiça e uma taxa de transferência com responsabilidade boa, o que reduz a taxa de perda de pacotes.

Questão 20

Questão 21

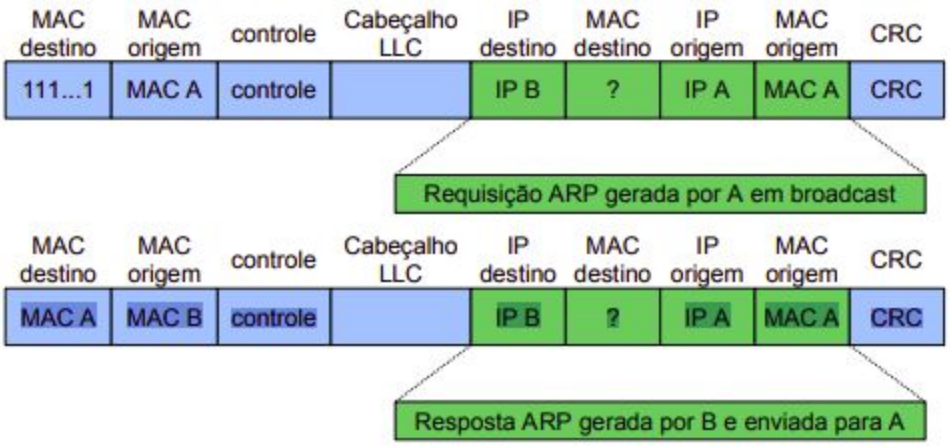
Um sistema autônomo (AS) é uma coleção de prefixos de roteamento conectados por Protocolo Internet (IP) sob o controle de um ou mais operadores de rede que apresenta uma política comum e claramente definida de roteamento para a Internet.

Sistemas Autônomos podem ser agrupados em três categorias, dependendo de sua conectividade e de sua política operacional.

- Um Sistema Autônomo multihomed é um AS que mantém ligações com mais de um AS. Isso permite a ele manter-se conectado à Internet em caso de um colapso total de uma das suas conexões. No entanto, este tipo de AS não permitiria que o tráfego de um AS seja enviado para outro AS.
- Um Sistema Autônomo stub refere-se a um AS que está ligado a apenas um outro. Isso pode aparentar como uso desnecessário de um número AS, se a política de roteamento da rede do AS acima desse for a mesma. No entanto, o stub AS pode na verdade ter peering com outros sistemas autônomos que não se aparecem em servidores Looking Glass públicos. Exemplos específicos incluem interligações privadas nos setores financeiros e de transportes.
- Um Sistema Autônomo de trânsito é um AS que permite conexões através de si mesmo para outras redes. Ou seja, uma rede A pode se conectar à rede B, um AS de trânsito, para se conectar à rede C. PSIs são sempre ASs de trânsito, porque eles fornecem conexões de uma rede para outra. O PSIs são considerados serviço de trânsito de venda para a rede do cliente, por isso é utilizada a expressão AS de trânsito.

Questão 22

Formato da requisição:



Exemplo da execução do comando “arp”:

```
augusto@augusto:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   50:39:55:14:2a:b1   C                     wlo1
```

Questão 23

“Carrier Sense Multiple Access with Collision Detection”

Algoritmo para prevenir, detectar e tratar colisões em redes Ethernet. Colisões ocorrem quando duas estações disputam o acesso ao meio simultaneamente.

Questão 24

O encapsulamento de dados é o processo que adiciona mais informações de cabeçalho de protocolo aos dados antes da transmissão. Na maioria das formas de comunicação de dados, os dados originais são encapsulados ou envolvidos em vários protocolos antes de serem transmitidos.

Na transmissão de dados, cada camada pega nas informações passadas pela camada superior, acrescenta as informações pelas quais é responsável e passa os dados à camada inferior. A este processo chama-se encapsulamento.

Na recepção de dados, o processo é inverso, ou seja, inicia-se na camada inferior e é passado à camada superior, depois de “traduzir” as informações relativas à sua camada. A este processo chama-se desencapsulamento.

Questão 25

Protocolos de rede são conjuntos de regras estabelecidas que determinam como formatar, transmitir e receber dados para que os dispositivos de rede de computadores - de servidores e roteadores a terminais - possam se comunicar independentemente das diferenças em suas infraestruturas, projetos ou padrões subjacentes.

Para enviar e receber informações com êxito, os dispositivos dos dois lados de uma troca de comunicação devem aceitar e seguir as convenções de protocolo. O suporte para protocolos de rede pode ser incorporado em software, hardware ou ambos.

Protocolos de rede padronizados fornecem um idioma comum para dispositivos de rede. Sem eles, os computadores não saberiam como se envolver. Como resultado, exceto pelas redes especializadas construídas em torno de uma arquitetura específica, poucas redes seriam capazes de funcionar e a Internet como a conhecemos não existiria. Praticamente todos os usuários finais da rede contam com protocolos de rede para conectividade.