

TAG Redes

PS GRIS

UFRJ

Thais Angelo Ferreira de Oliveira

1)

R:

As camadas são:

7)Aplicação

6)Apresentação

5)Sessão

4)Transporte

3)Rede

2)Enlace

1)Física

Na camada física são especificados os dispositivos e os meios de transmissão, como os cabos de rede, por onde os dados vão ser transmitidos. Ela tem como função o recebimento, transmissão, codificação e decodificação dos bits recebidos.

Na camada de enlace começa a interpretação dos bits, nela eles são verificados para ver se possuem algum erro e, se possuírem, esse erro pode ser corrigido. Assim, as camadas superiores assumem uma transmissão praticamente sem erros. Esta camada também controla o fluxo que os dados são transmitidos. Ela é dividida em duas outras subcamadas:

1)MAC: é nessa camada que há a possibilidade da conexão de diversos computadores em uma rede. É através do endereço MAC (endereço único de cada dispositivo) que esta camada utiliza para identificar e enviar os pacotes. Ela também atua como uma interface entre a camada física e a subcamada LLC.

2)LLC: É nesta camada que tem o controle de fluxo dos dados na rede, é por causa dela que se tem vários protocolos na próxima camada dentro de uma mesma rede.

Na camada de rede que se obtém o endereçamento IP de origem e de destino, ela também pode priorizar alguns pacotes e decidir qual caminho seguir para enviar seus dados. Ela basicamente controla o roteamento entre a origem e o destino do pacote. Ela abriga o protocolo IP e ICMP.

É a camada de transporte que garante o envio e o recebimento dos pacotes vindos da camada 3. Ela gerencia o transporte dos pacotes para garantir o envio e recebimento dos dados. É nela onde opera protocolos como o TCP e o UDP.

A camada de sessão é responsável por estabelecer e encerrar a conexão entre hosts. É ela quem inicia e sincroniza os hosts. Além de realizar as conexões das sessões, ela também fornece suporte a elas. Ela vem como uma forma de organizar o diálogo entre a troca de dados.

A camada de apresentação é responsável por fazer a tradução dos dados para que a próxima camada use. Nela ocorre a conversão de códigos para caracteres, a conversão e compactação dos dados, além da criptografia desses dados, caso necessite.

A camada de aplicação é utilizada para consumir dados. Nesta camada temos os programas que garantem a interação entre o humano e a máquina. É nesta camada que temos os protocolos mais conhecidos como o HTTP, FTP, além de serviços como o DNS.

2)

R:

Domínio de rede:

O domínio de colisão é um segmento lógico da rede onde os pacotes transmitidos por elementos pertencentes a ele podem colidir uns com os outros, em particular no protocolo Ethernet. Uma colisão ocorre quando duas ou mais estações pertencentes ao mesmo segmento de rede compartilhado transmitem quadros ao mesmo tempo. Quanto mais colisões ocorrem menor é a eficiência da rede.

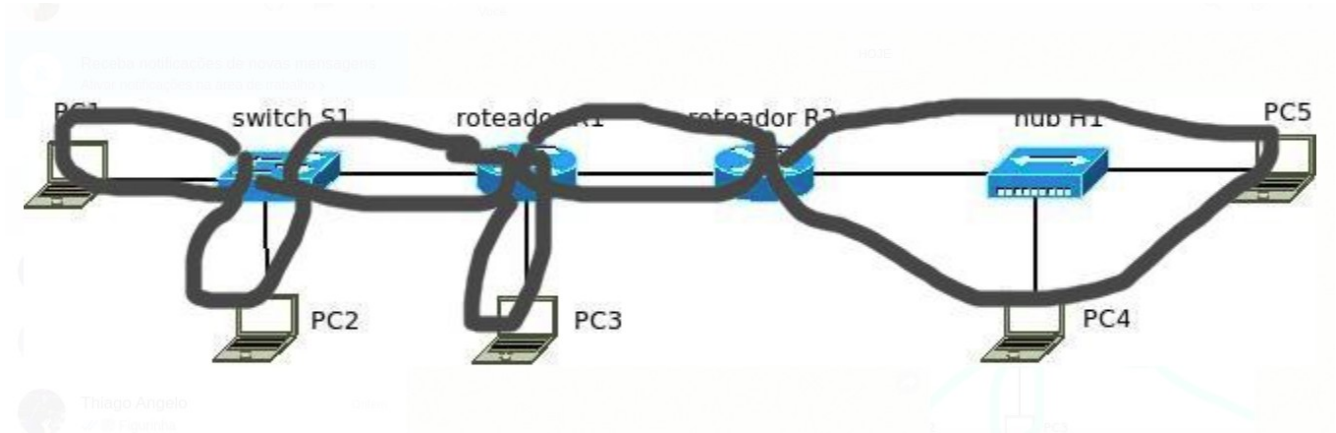
Domínio de broadcast:

Um domínio de broadcast é um segmento lógico de uma rede de computadores em que um computador ou qualquer outro dispositivo conectado à rede é capaz de se comunicar com outro sem a necessidade de utilizar um dispositivo de roteamento.

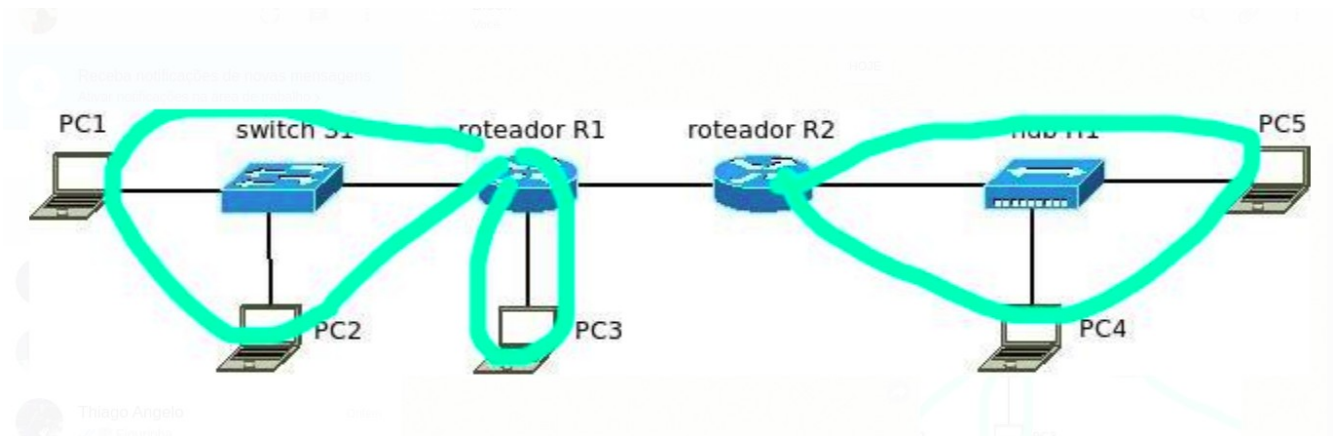
3)

R:

Domínio de colisão:

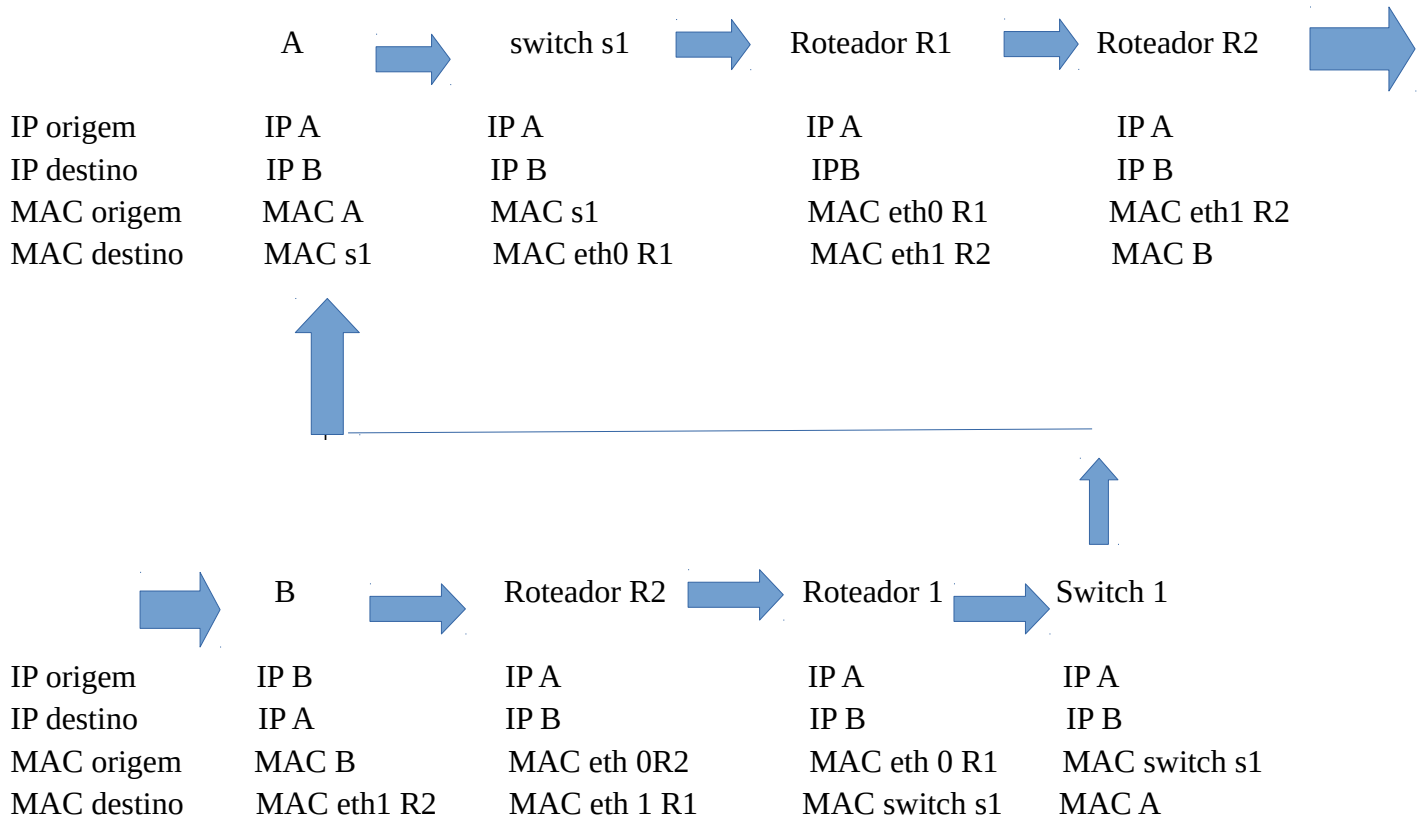


Domínio de broadcast:



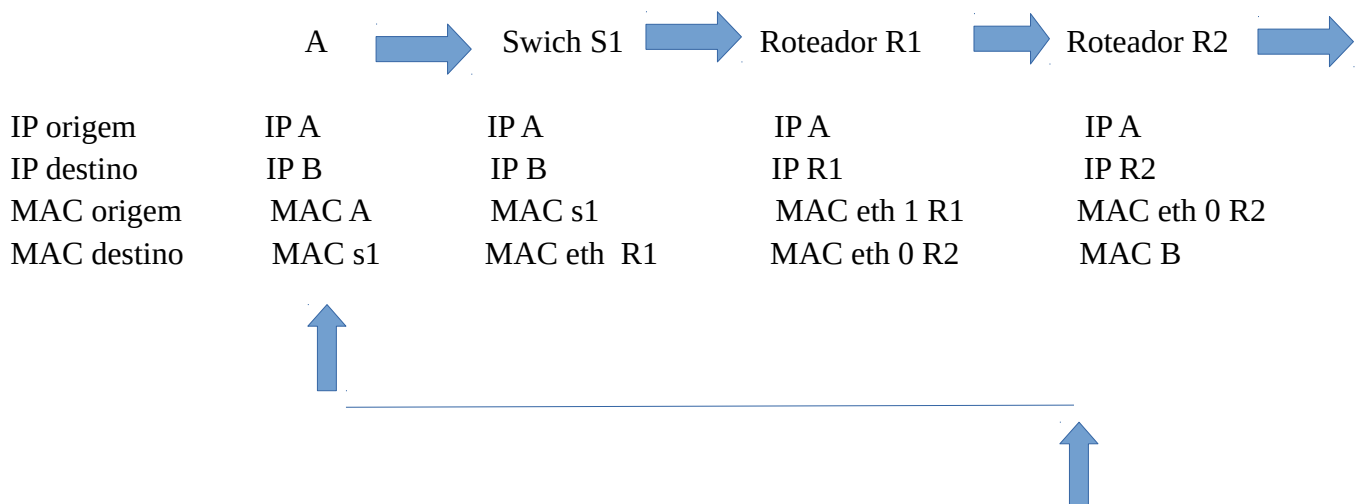
4)

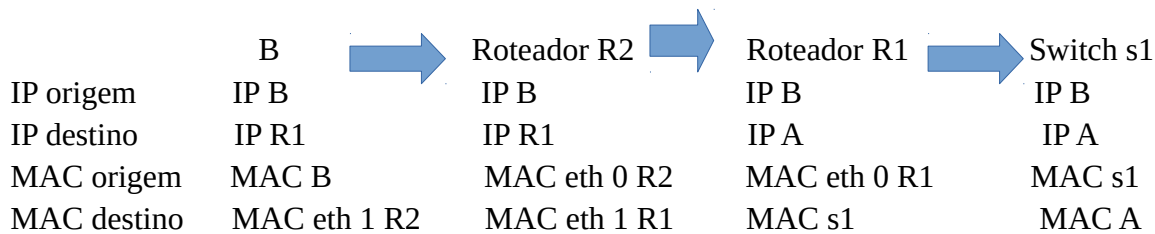
R:



5)

R:





6)

R:

O host que quer iniciar a conexão envia um segmento com a flag SYN ativada, especificando a qual número de porta no servidor de destino ele quer se conectar. O servidor responde com um segmento contendo a flag SYN. Além disso, o segmento SYN enviado pelo cliente é confirmado pela ativação da flag ACK neste segmento de resposta, confirmando o ISN do cliente + 1. O cliente então confirma o segmento SYN proveniente do servidor enviando outro segmento com a flag ACK ativada.

7)

R:

MDI:

É uma conexão de porta Ethernet normalmente usada na porta NIC (Network Interface Card) ou na porta NIC integrada em um PC. Os sinais de transmissão em uma NIC devem ir para receber sinais no hub, para que os últimos dispositivos tenham seus sinais de transmissão e recebimento comutados em uma configuração conhecida como MDIX (o "X" aqui representa "crossover", indicando o reverso de sinais de entrada e saída)

MDIX:

O MDIX (Crossover de interface dependente médio) é uma conexão de porta frequentemente encontrada em um computador, roteador ou hub. O MDIX é a versão cruzada da porta MDI. Nesse caso, a porta MDIX elimina a necessidade de um cabeamento de par trançado cruzado.

8)

R:

A para S1: MDI (Direta)

S1 para S2: MDIX (Direta)

S2 para R1: MDI (Direta)

R1 para R2: MDIX (Cross)

R2 para B: MDI (Cross)

9)

9.1:

IP: 177.032.168.223

10110001.00100000.10101000.11011111

Masc: 255.255.255.248

11111111.11111111.11111111.11111000

Classe C

and logico entre ip e masc : 10110001.00100000.10101000.11011000 (rede)

Broadcast

Rede: 177.032.168.216

Broadcast: 177.32.

9.2:

IP: 204.20.143.0

11001100.00010100.10001111.00000000

Masc: /18

225.225.192

11111111.11111111.11000000.00000000

Classe B

and logico entre ip e masc : 11001100.00010100.10000000.00000000 (rede)

Host

Rede: 204.020.128.0

Broadcast: 204.020.1910255

9.3:

IP: 36.72.109.24

00100100.01001000.01101101.00011000

Masc: 255.254.0.0

11111111.11111110.00000000.00000000

Classe A

and logico entre o ip e a masc: 00100100.01001000.00000000.00000000 (rede)

Host

Rede: 36.72.0.0

Broadcast: 36.73.255.255

9.4:

IP: 7.26.0.64

00000111.00011010.00000000.01000000

Masc: /26

255.255.255.192

11111111.11111111.11111111.11000000

Classe C

and logico entre ip e a masc: 00000111.00011010.00000000.01000000

Rede

Rede = 7.26.0.64
Broadcast: 7.26.0.137

9.5:

IP: 200.201.173.187

11001000.11001001.10101101.10111011

Masc: 255.255.255.252

11111111.11111111.11111111.11111100
Classe C

and logico entre o ip e a masc: 11001000.11001001.10101101.10111000

Broadcast

Rede: 200.201.173.184
bradcast: 200.201.173.187

10)
R:

10.1:
masc: 255.255.255.224

11111111.11111111.11111111.11100000

IP1: 240.128.192.158
11110000.10000000.11000000.10011110

Rede: 240.128.192.128
and : 11110000.10000000.11000000.10000000

IP2: 2.40.128.192.154
11110000.10000000.11000000.10011010
Rede: 240.128.192.128

and: 11110000.10000000.11000000.10000000

São da mesma rede

10.2:

mask:255.255.255.248

11111111.11111111.11111111.11111000

IP1:87.42.141.142

01010111.00101010.10001101.10001110

Rede: 87.42.141.136

and: 01010111.00101010.10001101.10001000

IP2:87.42.141.137

01010111.00101010.10001101.10001001

Rede: 87.42.141.136

and: 11110000.10000000.11000000.10000000

São da mesma rede

10.3:

mask:/10

255.192.0.0

11111111.11000000.00000000.00000000

IP1:98.12.238.221

01010111.00001100.11101110.11011101

Rede: 87.42.141.136

and: 01100010.00000000.00000000.00000000

IP2: 98.45.7.17

01100010.00001100.11101110.11011101

Rede: 87.42.141.136

and:01100010.00000000.00000000.00000000

São da mesma rede

11)

R:

12)

R:

RIP:

É projetado para redes com tamanho moderado, que utilizam uma tecnologia razoavelmente homogênea. Não é destinado a uso em ambientes mais complexos, devido à suscetibilidade a falhas.

BGP:

Para grandes redes ,utiliza-se o protocolo BGP para ligar grandes entidades como redes corporativas e universitárias para a Internet ele atua também em AS.

OSPF:

O OSPF é um protocolo link-state coleta dados sobre as ligações ou segmentos entre um dispositivo e outro . Principalmente esses dados é sobre a distância e conectividade, mas em algumas redes de dados link-state inclui informações sobre a largura de banda , as cargas de tráfego e tipo de tráfego aceito nos links. É projetado para redes de tamanhos pequenos a médios.

13)

R:

TCP=

$64 \text{ KB} * 8 * 3 = 1\,572\,864 \text{ bits} / 0,015 = 104\,857\,600$

$32 \text{ KB} * 8 * 2 = 524\,288 \text{ bits} / 0,015 = 34\,952\,533,3$

$\text{TCP}_{\text{tot}} = 139\,810\,133$ Aproximadamente 139,8 MB/s

14)

R:

Sequence number: O número que identifica o byte em um fluxo de dados do transmissor para o receptor.

Acknowledgement: Se a flag ACK estiver ativada o valor deste campo será o próximo número de sequência que o destinatário espera receber. Assim é confirmada a recepção de todos os bytes anteriores, se houverem.

Window size: O tamanho da janela de recepção indica o número de bytes que o transmissor deste segmento quer aceitar do host de destino, em cada transmissão. Ele é também o tamanho da janela de envio do host que recebe este segmento.

Flags:

- ACK – Bit de Confirmação.
- URG – Quando ativado, indica que o Campo Ponteiro de Urgente é válido e o recurso Transferência de dados com prioridade foi invocado
- PSH – Bit de Push.
- RST – Bit de Reset. Quando ativado indica que o transmissor encontrou um problema e deseja resetar a conexão.
- SYN – Bit de Sincronismo. Requisição para sincronizar números de sequência e estabelecer uma conexão entre dois hosts. O campo Número de Sequência contém o número de sequência inicial (ISN) do host que transmite o segmento
- FIN – Bit de Finalização.

15)

R:

A

A primeira parte é estabelecer a conexão, o host 1 envia um pacote SYN para o host 2 com o seu ISN. O host 2 grava as informações enviadas(dentro delas esta a sequencia A). Assim, o host 2 manda um ACK com a sequencia (A + 1) juntamente com um outra sequencia SYN(B). Quando o hist 1 recebe recebe a sequencia B, ele manda de volta um ACK B + 1 estabelecendo a conexão.

Após isso, o host 1 começa o sequenciamento indicando até quias dados foram recebidos e um ACK de seus dados. Isso é passado para o host 2, e a partir disso o sequenciamento passou a ser o valor ACK anterior B.

16)

R:

Se for enviado uma grande quantidade de dados, e algum tenha sido perdido, o host que recebeu esses dados envia um ACK com o numero do ultimo pacote que recebeu em sequencia. Depois que o timeout acabar o host que estava enviando os dados reenvia o que foi perdido e o próximo ACK será o último que foi recebido e com o dado já recuperado o host que esta enviando volta a enviar os dados na

mesma sequencia a partir do que foi perdido. Caso o host que esteja recebendo não mandar um ACK de confirmação o host que esta enviando envia os dados novamente.

17)

R:

18)

R:

Slow start:

O slow start do TCP é uma das primeiras etapas do processo de controle de congestionamento e ACK. É um algoritmo que equilibra a quantidade de dados que um remetente pode transmitir com a quantidade de dados que o receptor pode aceitar. O menor dos dois valores se torna a quantidade máxima de dados que o remetente tem permissão para transmitir antes de receber uma confirmação do destinatário.

Congestion avoidance :

É outro algoritmo de controle de congestionamento de ACK. Ele é a base principal para o controle de congestionamento na Internet.

19)

R:

O serrilhado do TCP é muita importância para dificultar o congestionamento da rede.

20)

R:

21)

R:

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

22)

R:

23)

R:

É um protocolo de telecomunicação que organiza a forma como os dispositivos de rede compartilham o canal utilizando a tecnologia Ethernet. Ele indica quando o meio está disponível para transmissão e é usado para detectar e prevenir colisões na rede.

24)

R:

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. Com isso, o dado antes de ser enviado passa por um encapsulamento.

25)

R:

Os protocolos de rede são conjuntos de regras que ditam e permitem a comunicação entre computadores e outros dispositivos conectados na mesma rede.