

# TAG redes

Nome: Giovanni Dhery Silva Prieto

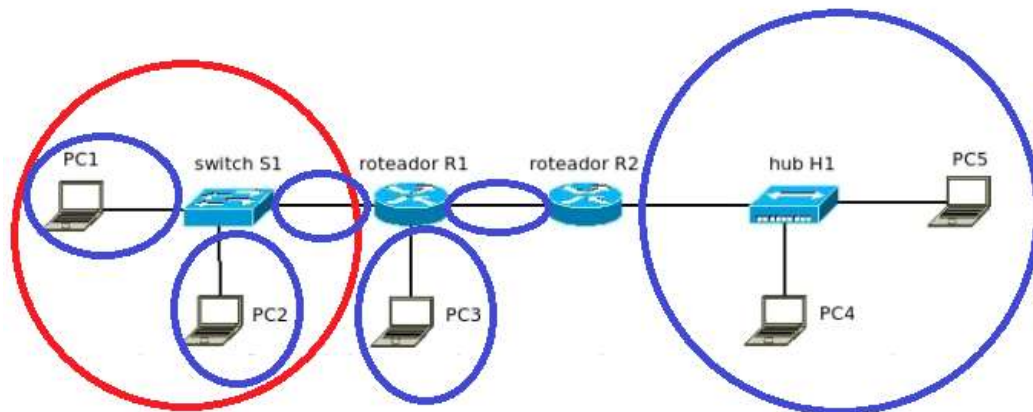
## 1:

7. Aplicação: é a camada mais próxima ao usuário e provê aplicações.
6. Apresentação: entrega e formata dados recebidos da camada de aplicação, também por oferecer algumas funções para criptografia.
5. Sessão: garante a comunicação entre dois sistemas e o controle da mesma, além de identificar erros para futuro tratamento.
4. Transporte: corrige erros, controla o fluxo e ordena dados de tal maneira que os pacotes que saíram de uma máquina sejam os mesmos que estão chegando em outra.
3. Rede: estabelece protocolos de roteamento de pacotes.
2. Enlace: detecta e corrige erros que ocorrem na camada física e define protocolos de comunicação entre sistemas diretamente conectados.
1. Física: camada responsável por estabelecer conexão entre máquinas em um meio físico e, conseqüentemente, a transmissão de dados.

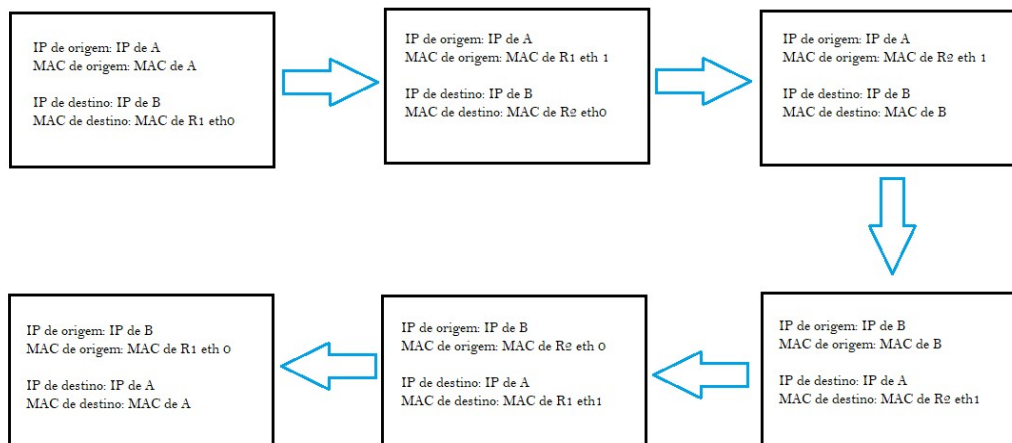
**2:** Domínio de colisão é um segmento lógico onde diferentes pacotes podem colidir entre si. Domínio de broadcast é um conjunto de máquinas que podem se comunicar com as outras no conjunto sem roteamento.

**3:** Vermelho: domínio de broadcast

Azul: domínio de colisão

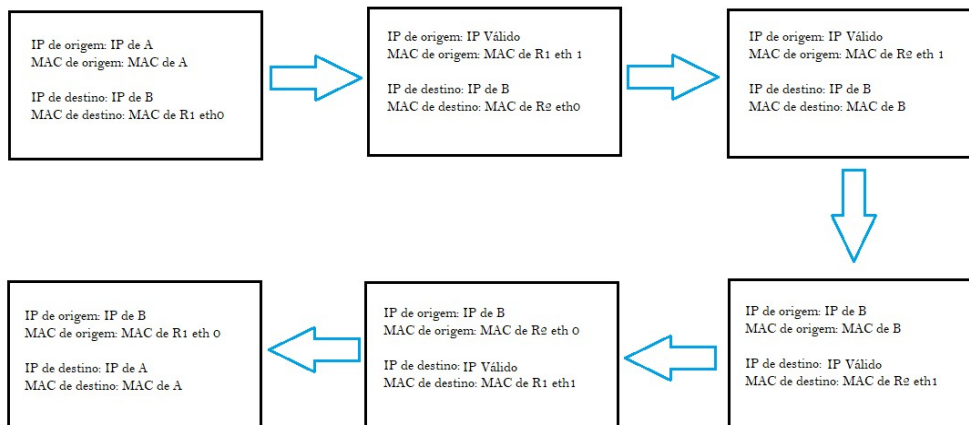


4:



5:

O NAT é implementado por conta da grande quantidade de máquinas existentes e pela limitação do endereço IP para nomear unicamente cada uma. Então, quando é assinado um contrato com um provedor, ele te dará um IP válido na internet e sua rede local é usado uma faixa exclusiva de endereços IP.



**6:** Segundo o RFC793, o handshake no protocolo TCP ocorre da seguinte maneira, com duas máquinas A e B: primeiro, a máquina A envia um bit de controle chamado “SYN” (synchronize) com uma sequência de números. Segundo, B envia um sinal “ACK” (acknowledgement) que confirma a sequência enviada. Em seguida, B envia seu SYN com uma outra sequência de números, que posteriormente é respondida por A com outro SYN. Como o envio do ACK e do SYN por B são enviados numa mesma mensagem, dá-se o nome de three-way-handshake.

**7:** MDI e MDI-X são tipos de portas de cabeamento Ethernet. As duas possuem 8 entradas, porém um par para transmissão e outro para recepção. O primeiro par no MDI está localizado nas portas 1 e 2, e o par de transmissão nas portas 3 e 6. O MDI-X tem ambos os pares com as portas trocadas em relação ao MDI (o X no nome significa “cross”), para que haja troca de sinais entre os dispositivos com essas portas, sendo uma ponta com uma porta MDI e a outra com a MDI-X.

**9:**

- IP: 177.32.168.223

Máscara: 255.255.255.248

Máscara: 11111111.11111111.11111111.11111|000 (/29)

223 em binário: 11011|111

Rede: 177.32.168.216

Broadcast: 177.32.168.223

Host: 177.32.168.217 até 177.32.168.222

O IP em questão é IP de broadcast.

- IP: 204.20.143.0

Máscara: /18

Máscara: 11111111.11111111.11|000000.00000000

143 em binário: 10|001111

Rede: 204.20.128.0

Broadcast: 204.20.191.255

Host: 204.20.128.1 até 204.20.191.254

Com as informações acima, concluímos que o IP é um host na rede.

- IP: 36.72.109.24

Máscara: 255.254.0.0

Máscara: 11111111.11111111|0.00000000.00000000

72 em binário: 0100100|0

Rede: 36.72.0.0

Broadcast: 36.73.255.255

Host: 36.72.0.1 até 36.73.255.254

O IP dado na questão é um IP de host.

- IP: 7.26.0.64

Máscara: /26

Máscara: 11111111.11111111.11111111.11|000000

64 em binário: 01000000

Rede: 7.26.0.64

Broadcast: 7.26.0.127

Host: 7.26.0.65 até 7.26.0.126

O IP em questão é IP de rede.

- IP: 200.201.173.187

Máscara: 255.255.255.252

Máscara: 11111111.11111111.11111111.111111|00

187 em binário: 10111011

Rede: 200.201.173.184

Broadcast: 200.201.173.187

Host: 200.201.173.185 e 200.201.173.186

O IP dado na questão é IP de broadcast.

## 10:

- 240.128.192.154 e 240.128.192.158 com máscara 255.255.255.224

Máscara: 11111111.11111111.11111111.111|00000

158 em binário: 100|11110

154 em binário: 100|11010

Rede: 240.128.192.128

Broadcast: 240.128.192.159

Host: 240.128.192.129 até 240.128.192.158

Ambos os endereços IPs se encontram na mesma rede.

- 87.42.141.142 e 87.42.141.137 com máscara 255.255.255.248

Máscara: 11111111.11111111.11111111.11111|000

142 em binário: 10001|110

137 em binário: 10001|001

Os endereços se encontram na mesma rede.

- 98.45.7.17 e 98.12.238.221 com máscara /10.

Máscara: 11111111.11|000000.00000000.00000000

45 em binário: 00|101101

12 em binário: 00|001100

Os dois endereços estão na mesma rede.

## 11:

Rede 1: 500 hosts (187.0.0.0 até 187.0.1.255)

Rede 2: 500 hosts (187.0.2.0 até 187.0.3.255)

Rede 3: 120 hosts (187.0.4.0 até 187.0.4.127)

Rede 4: 120 hosts (187.0.4.128 até 187.0.4.255)

Rede 5: 60 hosts (187.0.5.64 até 187.0.5.127 )

Rede 6: 25 hosts (187.0.5.0 até 187.0.5.31)

187.0.0.0/8

Rede: 10111011|.00000000.00000000.00000000

Broadcast: 10111011.11111111.11111111.11111111

Host: 187.0.0.1 até 187.255.255.254

Número de hosts:  $2^{24} - 2$

Vamos partir de uma máscara /21:

10111011.00000000.00000|000.00000000

Com isso temos  $2^{13}$  redes com 2046 hosts cada.

Vamos dividir 187.0.0.0/21 em duas redes com máscara /22:

10111011.00000000.000000|00.00000000 – Rede A

Intervalo: 187.0.0.0 até 187.0.3.255

10111011.00000000.000001|00.00000000 – Rede B

Intervalo: 187.0.4.0 até 187.0.7.255

Agora temos as redes A e B que suportam 1022 hosts cada.

Vamos dividir a rede A em duas outras de máscara /23:

10111011.00000000.0000000|0.00000000 – Rede C

10111011.00000000.0000001|0.00000000 – Rede D

Rede C:

Rede: 187.0.0.0

Broadcast: 187.0.1.255

Host: 187.0.0.1 até 187.0.1.254 ( $2^9 - 2 = 510$  hosts)

Rede D:

Rede: 187.0.2.0

Broadcast: 187.0.3.255

Host: 187.0.2.1 até 187.0.3.254 (510 hosts)

Com isso, deixaremos as redes C e D com as redes 1 e 2, respectivamente.

Agora, vamos trabalhar com a rede B e dividi-la em duas redes com máscara /23:

10111011.00000000.0000010|0.00000000 – Rede E

10111011.00000000.0000011|0.00000000 – Rede F

Rede E:

Rede: 187.0.4.0

Broadcast: 187.0.5.255

Host: 187.0.4.1 até 187.0.5.254 (510 hosts)

Partindo a rede E em duas outras com máscara /24:

10111011.00000000.00000100|.00000000 – Rede G

10111011.00000000.00000101|.00000000 – Rede H

Rede G:

Rede: 187.0.4.0

Broadcast: 187.0.4.255

Host: 187.0.4.1 até 187.0.4.254 (254 hosts)

Rede H:

Rede: 187.0.5.0

Broadcast: 187.0.5.255

Host: 187.0.5.1 até 187.0.5.254 (254 hosts)

Dividindo a rede G em duas outras com máscara /25:

10111011.00000000.00000100.0|00000000 – Rede I

10111011.00000000.00000100.1|00000000 – Rede J

Rede I:

Rede: 187.0.4.0

Broadcast: 187.0.4.127

Host: 187.0.4.1 até 187.0.4.126 (126 hosts)

Rede J:

Rede: 187.0.4.128

Broadcast: 187.0.4.255

Host: 187.0.4.129 até 187.0.4.254 (126 hosts)



Agora, deixaremos as redes 3 e 4 com as redes I e J, respectivamente.

Dividindo a rede H em duas outras com máscara /25, temos

10111011.00000000.00000101.0|0000000 – Rede K

10111011.00000000.00000101.1|0000000 – Rede L

Rede K:

Rede: 187.0.5.0

Broadcast: 187.0.5.127

Host: 187.0.5.1 até 187.0.5.126 (126 hosts)

Rede L:

Rede: 187.0.5.128

Broadcast: 187.0.5.255

Host: 187.0.5.129 até 187.0.5.154 (126 hosts)

Trabalhando com a rede K para dividi-la em duas outras com máscara /26:

10111011.00000000.00000101.00|000000 – Rede M

10111011.00000000.00000101.01|000000 – Rede N

Rede M:

Rede: 187.0.5.0

Broadcast: 187.0.5.63

Host: 187.0.5.1 até 187.0.5.62 (62 hosts)

Rede N:

Rede 187.0.5.64

Broadcast: 187.0.5.127

Host: 187.0.5.65 até 187.0.5.126 (62 hosts)

Com essas informações, alocaremos a rede N à rede 5 e dividiremos a rede M em

duas outras com máscara /27

10111011.00000000.00000101.000|00000 – Rede O

10111011.00000000.00000101.001|00000 – Rede P

Rede O:

Rede: 187.0.5.0

Broadcast: 187.0.5.31

Rede: 187.0.5.1 até 187.0.5.30 (30 hosts)

Rede P:

Rede: 187.0.5.32

Broadcast: 187.0.5.63

Host: 187.0.5.33 até 187.0.5.62 (30 hosts)

Finalmente, vamos deixar a rede 6 com a rede O.

**12:** RIP é um protocolo de medição de distância de roteamento, tendo como métrica um contador de saltos. OSPF também é um protocolo de roteamento, se utiliza de um algoritmo chamado SPF (Shortest Path First), que vai decidir o caminho a partir de envio de pacotes para outros roteadores. Tanto o RIP quanto o OSPF são protocolos voltados para comunicação em uma mesma rede (chamado de Interior Gateway Protocol). O BGP pode ser usado tanto para a comunicação em um mesmo ou para diferentes sistemas autônomos.

**13:**

$TCP\ Window\ size = 3 * 64KB * 8 + 2 * 32KB * 8 = 2097152\ bits$

$Latência = 15\ ms = 0.015\ s$

$2097152 / 0.015 \sim 139810134\ bits/segundo$

Aproximadamente 134 Mb/s.

**14:**



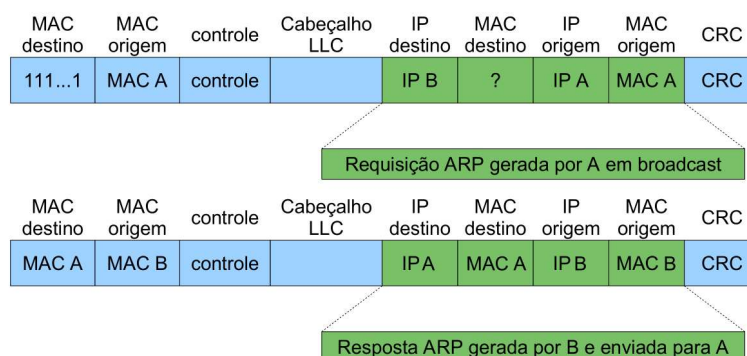
**17:** Quando um pacote que o receptor espera chegar não é enviado e outros são recebidos, o receptor envia sinais ACK referentes ao pacote que não chegou. O emissor, depois de receber 3 vezes sinais ACK duplicados, envia o pacote que teria sido perdido.

**18:** Quando o tamanho da janela fica abaixo do valor de threshold, o receptor inicia com um tamanho definido da janela e vai dobrando a cada ACK recebido até atingir o valor de threshold. Após atingir tal valor, o tamanho da janela vai aumentando em 1 a cada ACK recebido.

**19:** O comportamento “serrilhado” do TCP ocorre quando há sequências de 3 ACKs duplicados e timeout, que acontece devido a não recepção de dados por um dos lados da conexão. Tal comportamento é importante para controlar o congestionamento da conexão e ter garantia de que os dados estão sendo transmitidos da devida maneira.

**21:** Sistemas autônomos são um conjunto de prefixos IP sob o controle de um ou mais operadores de rede que possuem uma única e bem definida política de roteamento.

**22:**



**23:** CSMA/CD é um protocolo variante do CSMA, tendo adicional um detector de colisão. Tal protocolo é um controle de comunicação entre máquinas que compartilham a mesma rede local. Há uma verificação se o meio de transmissão está ocupado, se não estiver, o computador enviará seus pacotes. Se uma colisão é detectada, um sinal jam é enviado na rede para que não ocorram outras colisões e para o reenvio dos pacotes que colidiram, em tempos diferentes com o fim de serem enviados apropriadamente.

**24:** Encapsulamento é um método que consiste na adição cabeçalhos contendo informações sobre protocolos e outros métodos aplicados em algum dado. Isso permite a comunicação entre camadas.

**25:** Protocolo é uma convenção que estabelece um conjunto de normas sobre como fazer tarefas, como envio e formato de mensagens, como uma máquina tem que se comportar em determinadas situações (exemplo de timeout do protocolo TCP), dentre outros. Isso permite com que diferentes computadores consigam estabelecer uma conexão e se comuniquem.