

Lista de Exercícios 8 - Redes de Computadores
Júlio Melo Campos - 22250349

Seção 4.3

R17. Suponha que o Host A envie ao Host B um segmento TCP encapsulado em um datagrama IP. Quando o Host B recebe o datagrama, como a camada de rede no Host B sabe que deve passar o segmento (isto é, a carga útil do datagrama) para o TCP em vez de para o UDP ou algum outro protocolo de camada superior?

R: A camada de rede no Host B sabe que deve encaminhar para o protocolo do TCP, pois quando o Host B recebe o datagrama IP, a camada de rede analisa o campo "Protocolo" no cabeçalho do datagrama IP, onde ali cada protocolo de camada superior tem um número de identificação único atribuído pela IANA, onde o TCP tem o número de protocolo 6, enquanto o UDP tem o número de protocolo 17, então é por esta identificação que o Host B tem ciência onde levar o datagrama.

R18. Qual campo no cabeçalho IP pode ser usado para garantir que um pacote seja encaminhado através de no máximo N roteadores?

R: Este campo é identificado como TTL (Time To Live), onde é um de 8 bits no cabeçalho IP que indica o número máximo de saltos que um pacote pode percorrer na rede. Cada roteador que encaminha determinado pacote decrementa o TTL em 1. Ou seja, ao configurar o campo TTL para um valor específico N, você controla o número máximo de roteadores pelos quais o pacote pode passar, evitando assim que pacotes fiquem circulando indefinidamente na rede em caso de loops de roteamento.

R19. Lembre-se de que vimos o checksum da Internet sendo usado tanto em segmentos da camada de transporte (nos cabeçalhos UDP e TCP, Figuras 3.7 e 3.29 respectivamente) quanto em datagramas da camada de rede (cabeçalho IP, Figura 4.17). Agora, considere um segmento da camada de transporte encapsulado em um datagrama IP. Os checksums no cabeçalho do segmento e no cabeçalho do datagrama são calculados sobre quaisquer bytes comuns no datagrama IP? Explique sua resposta.

R: Sim, os checksums podem ser calculados sobre quaisquer bytes comuns no datagrama IP, pois a camada de transporte utiliza o pseudo-cabeçalho, que inclui os campos de **Endereço IP de Origem, Endereço IP de Destino, Protocolo**, para aumentar a confiabilidade e garantir a entrega correta dos dados, e assim, a camada de rede calcula o checksum do cabeçalho IP para verificar a integridade durante o roteamento.

Diferentes checksums garantem diferentes integridades, como:

- **Checksum IP:** Garante a integridade do cabeçalho IP durante o roteamento.
- **Checksum TCP/UDP:** Garante a integridade dos dados da camada de transporte e verifica que o segmento foi entregue ao destinatário correto.

Assim, isso fortalece a confiabilidade na transmissão de dados pela rede, garantindo que tanto os cabeçalhos quanto os dados sejam recebidos corretamente.

R20. Quando um grande datagrama é fragmentado em vários datagramas menores, onde (qual camada) esses datagramas menores são reagrupados em um único datagrama maior?

R: Eles são agrupados na camada de rede, onde ocorre exclusivamente no host de destino final, sendo realizada pela camada de rede do modelo TCP ou IP, se baseando nos campos do cabeçalho IP que indicam sua posição no datagrama original, como ID de identificação, offset de fragmento e flags. Isso é bom para simplificar o processamento nos roteadores intermediários e mantém a eficiência da rede para depois ser entregue para a camada de transporte (TCP/UDP).

R21. Os roteadores têm endereços IP? Se sim, quantos?

R: Sim, todos os roteadores têm endereços IP, que dependem dos números de interfaces de rede que ele tem conectadas a diferentes redes, ou seja, cada interface de um roteador conectada a uma rede IP tem um endereço IP único para controlar a permissão de encaminhamento dos pacotes de dados.

Sendo assim, se um roteador tem 5 interfaces conectadas a 5 redes diferentes, ele tem pelo menos 5 endereços IP, um para cada interface.

R22. Qual é o equivalente binário de 32 bits do endereço IP 223.1.3.27?

R: Para transformar o equivalente binário de 32 bits, precisamos transformar cada octeto em um binário de 8 bits, porque assim, teríamos 8 bits x 4 octetos = 32 bits. Assim, temos:

- 223 = 11011111
- 1 = 00000001
- 3 = 00000011
- 27 = 00011011

No final, o endereço IP 223.1.3.27 em equivalente binário é 11011111 00000001 00000011 00011011.

R23. Utilize o comando ipconfig /all do Windows (ou do seu SO) para obter seu endereço IP, sua máscara de rede, endereço IP do gateway padrão (02 endereços da rede local e da internet) e endereço(s) IP de seu(s) servidor(es) DNS local. Liste esses valores.

R:

- Endereço IP: 10.30.46.143
- Máscara de rede: 255.255.0.0
- Endereço IP do gateway padrão:
 - Local: 10.30.0.1
 - Internet: 10.30.0.1
- Endereço IP de servidor DNS local:
 - 200.129.163.1
 - 200.129.163.3
 - 8.8.8.8

○ 1.1.1.1

R24. Suponha que haja três roteadores entre um host de origem e um host de destino. Ignorando a fragmentação, um datagrama IP enviado do host de origem para o host de destino passará por quantas interfaces de rede? Quantas tabelas de encaminhamento serão consultadas para mover o datagrama da origem ao destino?

R: O datagrama IP passará por 8 interfaces de rede, pois ele passará por 4 enlaces:

- **Enlace 1:** Host de Origem ↔ Roteador 1
- **Enlace 2:** Roteador 1 ↔ Roteador 2
- **Enlace 3:** Roteador 2 ↔ Roteador 3
- **Enlace 4:** Roteador 3 ↔ Host de Destino

Porém em cada enlace há saída e entrada de cada destino, logo temos 2 interfaces por enlace, tendo assim 8 interfaces no total até o destino.

O datagrama IP passará por 3 tabelas de encaminhamento, que são tabelas mantidas por um roteador que indicam para qual interface de saída o pacote deve ser encaminhado. No caso, são 3 tabelas, uma para cada roteador, que levarão até o host de destino.

R25. Suponha que uma aplicação gere blocos de 40 bytes de dados a cada 20 ms, e cada bloco seja encapsulado em um segmento TCP e depois em um datagrama IP. Que porcentagem de cada datagrama será de sobrecarga, e que porcentagem será de dados da aplicação?

R: A porcentagem de sobrecarga de cada datagrama será baseado na quantidade adicionais dos blocos pelo número total de bytes, considerando que o número padrão de bytes do TCP e IP, sejam 20 bytes, ou seja:

$$\text{Overhead} = 20 \text{ (TCP)} + 20 \text{ (IP)} = 40 \text{ bytes}$$

$$\text{Total} = 40 \text{ (Blocos)} + 20 \text{ (TCP)} + 20 \text{ (IP)} = 80 \text{ bytes}$$

$$\% \text{ Overhead} = \frac{\text{Sobrecarga}}{\text{Total}} \cdot 100\% = \frac{40}{80} \cdot 100\% = 50\%$$

E a porcentagem de aplicação de cada datagrama será baseado na quantidade da aplicação pelo número total de bytes, ou seja:

$$\text{Aplicação} = 40 \text{ bytes}$$

$$\text{Total} = 40 \text{ (Blocos)} + 20 \text{ (TCP)} + 20 \text{ (IP)} = 80 \text{ bytes}$$

$$\% \text{ Aplicação} = \frac{\text{Aplicação}}{\text{Total}} \cdot 100\% = \frac{40}{80} \cdot 100\% = 50\%$$

R26. Suponha que você compre um roteador sem fio e o conecte ao seu modem a cabo. Também suponha que seu ISP atribua dinamicamente ao seu dispositivo conectado um endereço IP. Além disso, suponha que você tenha cinco PCs em casa que usam 802.11 para se conectar sem fio ao seu roteador. Como os endereços IP são atribuídos aos cinco PCs? O seu roteador sem fio usa NAT? Por que ou por que não?

R: Os endereços IP são atribuídos a partir do roteador sem fio que atua como um servidor DHCP (Dynamic Host Configuration Protocol) para a sua rede doméstica, sendo o

principal responsável por **atribuir automaticamente endereços IP privados** aos dispositivos conectados a ele. Assim, os cinco PCs que se conectam recebem IP privados, geralmente usando as faixas reservadas como **192.168.x.x**, **10.x.x.x**, **172.16.x.x** e **172.31.x.x**, assim permitindo a comunicação entre eles.

Sobre o roteador sem fio, ele faz sim o uso de NAT, pois, sem o NAT, seria necessário que cada dispositivo na sua rede doméstica tivesse um endereço IP público exclusivo, o que não é prático. O NAT permite que múltiplos dispositivos acessem a Internet através de um único endereço IP público fornecido pelo ISP, pois com a tradução, o PC ao enviar uma solicitação de Internet, ele substitui o endereço IP privado de origem pelo endereço IP público atribuído pelo ISP, dando também uma camada adicional de segurança, de forma que seus endereços IP não são expostos.

R27. O que se entende pelo termo "agregação de rotas"? Por que é útil para um roteador realizar agregação de rotas?

R: **Agregação de Rotas** é uma técnica utilizada em redes IP para combinar múltiplas rotas de rede em uma única rota resumida. Isso significa que, em vez de manter e anunciar rotas individuais para cada sub-rede ou endereço IP, um roteador pode representar um conjunto de endereços contíguos com uma única entrada de rota.

É útil realizar a agregação de rotas é crucial para um roteador porque **melhora significativamente a eficiência operacional da rede**, reduzindo a carga sobre os recursos do roteador e otimizando o fluxo de tráfego, resultando uma infraestrutura de rede mais robusta, escalável e fácil de gerenciar.

R28. O que é um protocolo "plug-and-play" ou "zeroconf"?

R: Um protocolo **"plug-and-play"** ou **"zeroconf"** (Zero Configuration Networking) é um conjunto de tecnologias e protocolos que permitem que dispositivos de rede sejam conectados e comecem a se comunicar automaticamente, sem a necessidade de configuração manual por parte do usuário ou administrador de rede.

Basicamente, eles simplificam a configuração de redes, permitindo que dispositivos se conectem e funcionem imediatamente após serem ligados, automatizando a atribuição de endereços IP, a resolução de nomes e a descoberta de serviços, eliminando a necessidade de intervenção manual.

R29. O que é um endereço de rede privada? Um datagrama com um endereço de rede privada pode estar trafegando na Internet pública? Explique.

R: Um endereço de rede privada é um endereço IP reservado para uso exclusivo em redes internas, como redes domésticas, corporativas ou locais (LANs). Eles não são únicos globalmente e não podem ser roteados na Internet pública, o que significa que não são válidos para comunicação direta com dispositivos fora da rede privada, ou seja, um datagrama não pode estar trafegando na Internet pública se tiver o endereço de rede privada, então, assim, são bloqueados para evitar problemas de roteamento e segurança.

No entanto, para esses datagramas poderem trafegar em rede pública, será necessário o uso de NAT, que faz a tradução entre endereços privados e públicos, garantindo a comunicação com o mundo externo sem expor a rede interna.

R31. Diz-se que, quando o IPv6 atravessa túneis IPv4, o IPv6 trata os túneis IPv4 como protocolos de camada de enlace. Você concorda com essa afirmação? Por que ou por que não?

R: Sim, essa afirmação é verdadeira, pois quando o IPv6 é transmitido através de túneis IPv4, ele não interage diretamente com a rede IPv4 subjacente. Em vez disso, o IPv6 vê o túnel como um meio de transmissão direta, assim como a camada de rede utiliza a camada de enlace para transmitir dados entre dois pontos. Logo, eles tratam o IPv4 como camada de enlace, pois eles fornecem os serviços necessários para a transmissão dos pacotes, através do encapsulamento do IPv6 dentro do IPv4, onde se cria uma abstração onde o IPv6 opera sobre um "enlace virtual" promovido pelo túnel IPv4.