

# Análise de Pacotes UDP com Wireshark

## Detalhamento Técnico de Pacotes UDP

Aluno: Vítor Carvalho Marx Lima

Matrícula: 11821ECP015

Data: 29 de Março de 2024

/home/clib/Desktop/UFU-2023-02/REDES I/atividade\_pratica\_04/wireshark-traces-zip/http-ethereal-trace-5 73 total packets, 21 shown

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	92	get-request

1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0  
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)  
Ethernet II, Src: Dell 4f:36:23 (00:08:74:4f:36:23), Dst: HewlettPacka\_61:eb:ed (00:30:c1:61:eb:ed)  
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104  
User Datagram Protocol, Src Port: 4334, Dst Port: 161  
Simple Network Management Protocol

Figura 1: Cabeçalho do Pacote UDP / SNMP

**1. Campos no Cabeçalho UDP:** A partir do rastreamento de pacotes fornecido, o cabeçalho UDP contém quatro campos:

- Porta de Origem
- Porta de Destino
- Comprimento
- Soma de Verificação

**2. Comprimento de Cada Campo do Cabeçalho UDP:** Cada um desses campos no cabeçalho UDP tem 2 bytes (16 bits) de comprimento. Esta informação é típica para cabeçalhos UDP e é evidente a partir do formato padronizado dos pacotes UDP.

**3. Valor no Campo de Comprimento:** O valor no campo de Comprimento de um pacote UDP representa o comprimento total do cabeçalho UDP e do payload UDP combinados. Você pode verificar isso observando o valor de Comprimento no rastreamento do pacote. Esse valor deve incluir os 8 bytes (uma vez que o próprio cabeçalho UDP tem 8 bytes de comprimento: 4 campos  $\times$  2 bytes cada) mais o tamanho do payload UDP.

**4. Número Máximo de Bytes no Payload UDP:** Dado que o campo de Comprimento é de 2 bytes, ele pode representar valores até  $2^{16} - 1 = 65.535$ . Uma vez que o cabeçalho UDP em si consome 8 bytes, o tamanho máximo do payload UDP é  $65.535 - 8 = 65.527$  bytes.

**5. Maior Número de Porta de Origem Possível:** Como o campo da Porta de Origem é de 2 bytes de comprimento, o maior valor possível que ele pode conter é  $2^{16} - 1 = 65.535$ .

Este é o maior número que pode ser representado com 16 bits.

**6. Número do Protocolo para UDP:** O número do protocolo para UDP, tanto em notação hexadecimal quanto decimal, é 17 (decimal) e 0x11 (hexadecimal), (especificado no RFC 768 para UDP).

**7. Exame de Pacotes UDP (Par de Requisição-Resposta):** Quando se examina tal par, a Porta de Origem do primeiro pacote torna-se a Porta de Destino do pacote de resposta, e vice-versa. Isso acontece porque a resposta é direcionada de volta para a porta de onde o pacote original foi enviado, estabelecendo um canal direto de comunicação entre as duas aplicações envolvidas na rede.