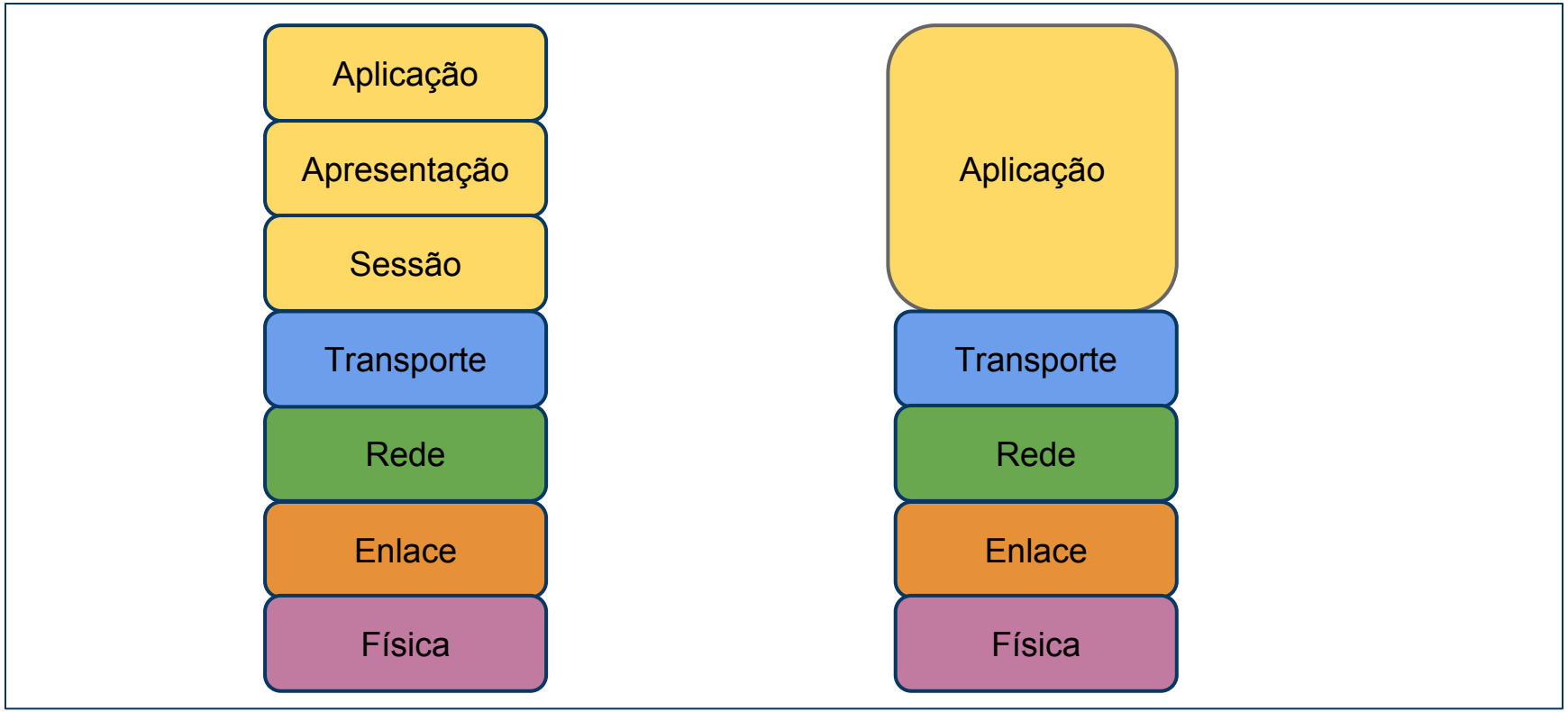
Ferramenta para Captura de Pacotes

MC 833 – Programação em Redes de Computadores
Instituto de Computação – UNICAMP

Juliana Freitag Borin

Transmissão dos pacotes



Ferramentas de captura de pacotes

- permitem a captura dos quadros transmitidos e recebidos por uma placa de rede - genericamente chamadas de ferramentas de captura de pacotes.

- mostram informações de todas as camadas do modelo TCP/IP que estão presentes no pacote capturado.

- Exemplo: captura de informações transmitidas entre um browser e um servidor Web.
  - a ferramenta mostrará informações sobre os cabeçalhos Ethernet, IP, TCP e HTTP.

Ferramentas de captura de pacotes

- uma placa de rede comumente decarta todos os quadros que não são destinados a ela, nem ao endereço de broadcast.

- ferramentas de captura de pacotes normalmente trabalham utilizando o modo espião ou modo promíscuo.

Ferramentas de captura de pacotes

- Em que máquina executar a ferramenta?

- Suponha que o objetivo seja analisar uma comunicação entre as máquinas A e B, as alternativas são:
    1. Em um roteador no caminho entre A e B;
    2. na máquina A;
    3. na máquina B;
    4. caso a rede onde A (ou B) se encontra use um hub - em uma outra máquina ligada no mesmo hub;
    5. caso A (ou B) esteja em uma rede sem fio, nessa mesma rede sem fio (desde que a rede não esteja usando criptografia).

Tcpdump

- Uma das ferramentas mais tradicionais no Linux.
- possui uma linguagem de filtros para se especificar quais pacotes devem ser capturados.
- Exemplos:

Comando	**Significado**
tcpdump src 10.1.1.1 and icmp	Pacotes ICMP cujo IP de origem seja 10.1.1.1.
Tcpdump dst 10.1.1.2 and tcp and dst port 80	Pacotes cujo endereço IP de destino seja 10.1.1.2, o protocolo de transporte seja TCP e a porta de destino seja 80.
Tcpdump host 10.1.1.1	Pacotes cujo endereço IP de origem ou o de destino seja 10.1.1.1.

Tcpdump

$ **tcpdump -i eth0 -l -n**

```
  13:57:56.876424 192.168.0.1.1044 > 192.168.0.2.23: S 3767238723:3767238723(0) win 32120 (DF)
  13:57:56.878184 192.168.0.2.23 > 192.168.0.1.1044: S 1049035122:1049035122(0) ack 3767238724 win
32736
  13:57:56.878370 192.168.0.1.1044 > 192.168.0.2.23: . ack 1 win 32120 (DF)
  13:57:56.881182 192.168.0.1.1044 > 192.168.0.2.23: P 1:28(27) ack 1 win 32120 (DF)
  13:57:56.900704 192.168.0.2.23 > 192.168.0.1.1044: . ack 28 win 32709 (DF)
  13:57:57.115026 192.168.0.2.23 > 192.168.0.1.1044: P 1:13(12) ack 28 win 32709 (DF)
```

Captura de pacotes de uma conexão TELNET.
Fonte: http://www.ime.usp.br/~ueda/ldoc/notastcp.html

Bibliografia

- man tcpdump
- http://www.metropoledigital.ufrn.br/aulas_avancado/web/disciplinas/rede_comp/aula_03.html
- http://www.danielmiessler.com/study/tcpdump/