IC - Instituto de Computação
UNICAMP - Universidade Estadual de Campinas
MC833 – Programação em Redes de Computadores
Primeiro Semestre 2025

Projeto 2: Analisando o tráfego de rede no Wireshark e no Mininet.

Você tem a tarefa de projetar e analisar uma rede composta por quatro *hosts* e um *switch* OpenFlow usando o Mininet. A tarefa envolve:

1. Configuração de rede (Mininet):

- Projetar uma topologia Mininet com:
▪ Quatro *hosts* (por exemplo: h1, h2, h3, h4).
▪ Um único *switch* habilitado para OpenFlow (por exemplo, s1).

- Para tanto, será necessário instalar o Mininet e para construir a topologia usar os seguintes comandos:

▪ Para instalar nativamente a partir do código-fonte, primeiro você precisa obter o código-fonte com este comando:
git clone https://github.com/mininet/mininet

▪ Assim que tiver o código-fonte, o comando para instalar o Mininet é:
mininet/util/install.sh

▪ Para executar o Mininet:
sudo mn

▪ Para fazer uma topologia de 4 *hosts* e 1 *switch*:
sudo mn --topo single,4

2. Geração de Tráfego (Ping):

- Use os comandos ping ou pingall do Mininet para tráfego controlado:
▪ 200 pacotes de ping de h1 a h3
▪ 200 pacotes de ping de h2 a h4

- Para tanto, usar os seguintes comandos para enviar pacotes:
mininet > **h1 ping –c 200 h3**
mininet > **h2 ping –c 200 h4**

3. Captura de pacotes (Wireshark):

- Use o Wireshark para capturar os pacotes ICMP que fluem pelas interfaces do *switch* OpenFlow. Antes de enviar os pacotes no Mininet, primeiro você deve iniciar o

Wireshark usando o seguinte comando no terminal mininet para abrir um terminal para o *switch* s1.

mininet > **xterm s12**

O comando mencionado anteriormente abrirá um novo terminal para o *switch* s1 e, em seguida, forneça o seguinte comando para iniciar o Wireshark:

wireshark &

Agora você verá a GUI do Wireshark, onde deverá definir o filtro para pacotes ICMP e selecionar a interface do *switch* s1 para capturar os pacotes ICMP. Existe uma opção na interface gráfica do Wireshark para iniciar a captura de pacotes durante a troca de mensagens entre *hosts* (h1 a h3 ou h2 a h4). Após a conclusão da troca de mensagens entre *hosts* é necessário interromper a captura dos pacotes. Em seguida, você pode salvar arquivos de captura de pacotes ICMP no formato PCAP (*Packet Capture*) para análise posterior desses arquivos.

4. Analisando dados (Python):

Desenvolva um script Python, utilizando a biblioteca Scapy, para analisar os dados do pacote capturado (arquivos PCAP). Extraia informações como:

- Endereços IP de origem e de destino.
- Calcular o *throughput* (taxa de transferência) médio.
- Intervalo médio entre pacotes (tempo entre chegadas de pacotes).
- Contagem de pacotes (total de pacotes).
- Além disso, o script deve gerar gráficos ilustrativos (usando matplotlib) mostrando claramente as métricas obtidas.

Resultados (relatório):

Escreva um relatório de projeto bem estruturado contendo:

- Código Python completo comentado e explicado.
- Capturas de tela comentadas mostrando os resultados obtidos (endereços IP, throughput, intervalos entre pacotes, taxas de perda e retransmissões).
- Capturas de tela detalhadas do Wireshark mostrando claramente o tráfego capturado com filtros utilizados.

- **Envie também arquivos de captura do Wireshark (PCAP) contendo tráfego de rede.**

Data de entrega: 7 de maio