Análise de desempenho da biblioteca libpcap: uma abordagem voltada à gerência de segurança

Ramicés dos S. Silva; Rafael L. Cancian
Laboratório de Redes de Computadores - Curso de Ciência da Computação - CTTMAR
Campus de São José - Universidade do Vale do Itajaí (UNIVALI) – São José - SC - Brasil.
{ramices; cancian} @univali.br;

Agenda

- Introdução
- Justificativa
- Objetivo
- A biblioteca Libpcap
- Projeto de experimentos (DOE)
- Desenvolvimento
- Resultados
- Conclusão

Introdução

- Crescimento da internet
- Novos serviços
- Requisitos de disponibilidade e segurança
- Complexidade de gerenciamento
- Modelos de gerenciamento

Justificativa

- Captura passiva de tráfego
- Aplicações pesquisadas
  - Snort
  - Wireshark
  - Tcpdump
  - Ntop
- A libpcap como mecanismo de captura
- Ausência de trabalhos análise quantitativa

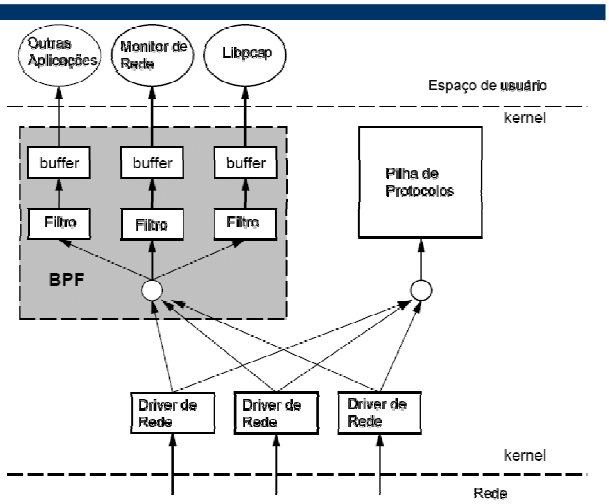
Objetivo geral

- Realizar uma análise experimental do desempenho da biblioteca de captura de pacotes libpcap aplicando a metodologia de projeto de experimentos.

A biblioteca Libpcap

- Biblioteca para captura de tráfego de rede;
- proposta de portabilidade;
- interface de mais alto nível para captura;
- suporte a diversas tecnologias de rede;
- largamente utilizada; e
- código aberto.

Libpcap - funcionamento

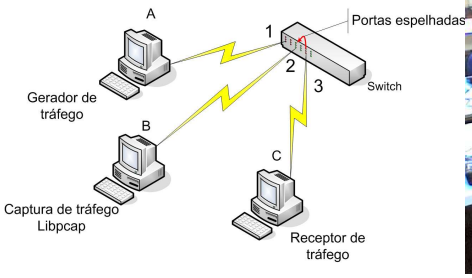


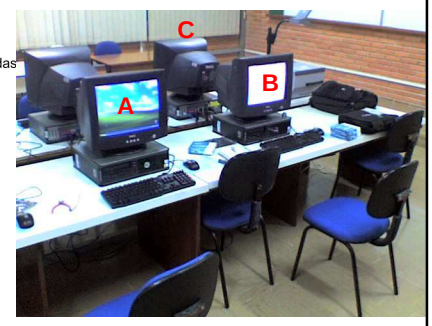
Projeto de experimentos (DOE)

- Quais os fatores que afetam o experimento?
- Quantos devem ser os testes para cada avaliação?
- Em que ordem os dados devem ser coletados?
- Qual o método de análise de dados será utilizado?
- Qual a diferença média é relevante para considerar dois resultados diferentes?

Desenvolvimento

- O ambiente de testes





Fatores analisados

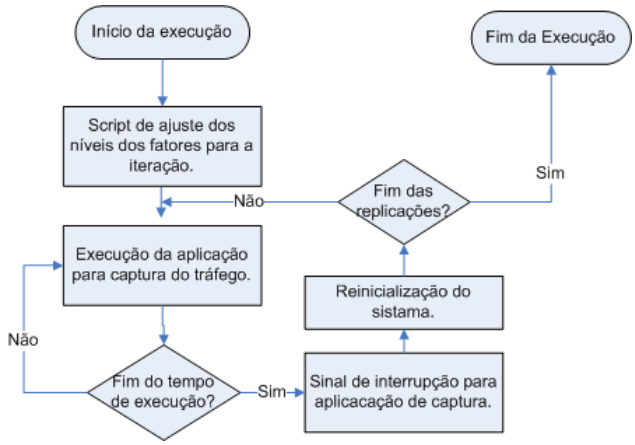
A. Controle da situação de livelock com NAPI;

B. aplicação do path PF_RING;

C. parâmetro MTU;

D. checagem dos frames no recebimento (rx_check).

Execução do experimento



Resultados

- Gigabytes capturados; (Analisados até esta publicação)
- throughput;
- índice de perda (bytes rejeitados/bytes gerados);

Resultados

- Coeficientes de determinação dos fatores em relação às métricas;
- modelo de regressão linear combinado dos fatores;
- Intervalos de confiança dos coeficientes do modelo de regressão;
- Análise da variância dos fatores e estimação do componente de erro aleatório do modelo;
- Probabilidade de significância do modelo

Verificação das suposições estatísticas

- Gráfico da verificação quanto à distribuição normal dos dados amostrados;
- gráficos valores amostrados e valores preditos.

Resultados (métrica GB capturados)

ANOVA, adequação ao modelo

Fator	Soma dos quadrados	F-value	p-value
Modelo	670,61	2578,60	< 0.0001
PF_RING – A	165,85	3188,66	< 0.0001
NAPI – B	367,68	6876,59	< 0.0001
MTU – C	31,04	596,72	< 0.0001
AB	93,19	1791,58	< 0.0001
AC	22,86	439,44	< 0.0001
Lack of fit	17,37	18,41	< 0.0001
Erro	7,13	-	-

Resultados (métrica GB capturados)

ANOVA, coeficientes da equação de regressão linear

Fator	Coeficiente	Erro	95% inferior	95% superior
PF_RING – A	-0,59	0,01	-0,61	-0,57
NAPI – B	0,86	0,01	0,84	0,88
MTU – C	0,25	0,01	0,23	0,27
AB	0,44	0,01	0,42	0,46
AC	-0,22	0,01	-0,24	-0,20

Equação de previsão

$$GBcap = 1,89 - 0,59A + 0,86B + 0,25C + 0,44AB - 0,22AC$$

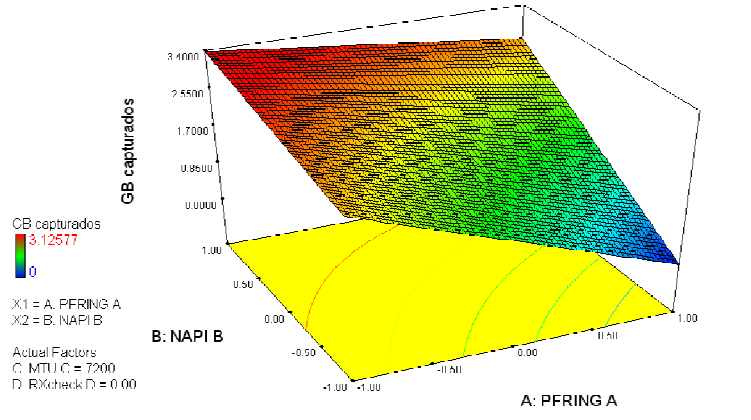
Resultados (métrica GB capturados)

Anova, Percentual de influência dos fatores

Fator	% Contribuição
PF_RING – A	23,86
NAPI – B	51,46
MTU – C	4,47
AB	13,41
AC	3,39
Erro	1,03

Resultados (métrica GB capturados)

Gráfico de Previsão



Conclusão

- Ausência de trabalhos correlatos;
- aumento da complexidade;
- contribuição para comunidade científica;
- dificuldade com a geração de tráfego gigabit;
- problemas de segurança; e
- análise quantitativa.

Análise de desempenho da biblioteca libpcap: uma abordagem voltada à gerência de segurança

Ramicés dos S. Silva; Rafael L. Cancian
Laboratório de Redes de Computadores - Curso de Ciência da Computação - CTTMAR
Campus de São José - Universidade do Vale do Itajaí (UNIVALI) – São José - SC - Brasil.
{ramices; cancian} @univali.br;