

Análise de redes de comunicação através de *packet sniffing*

Alexandre Lucchesi Alencar

09/0104471

alexandre@loopec.com.br

Pedro Salum Franco

09/0139232

pedro@loopec.com.br

Daniel A. M. Sandoval

09/0109899

daniel@loopec.com.br

1 de março de 2013

Resumo

O presente trabalho pretende analisar conexões de rede através da técnica de *packet sniffing*. Sua estrutura é dividida em duas partes. Na primeira, medimos e analisamos os tempos necessários para conexão com sites em diversas localizações geográficas, durante o TCP *handshaking* e *ping*. Na segunda, analisamos uma requisição HTTP GET para determinar seu conteúdo, endereçamento na camada de Rede e analisar o *overhead* causado por protocolos de rede. Os resultados encontrados foram de acordo com o esperado: constatamos variações de até 7200% em tempos de conexão de acordo com a distância até o destino; constatamos *header* de 54 bytes em requisições HTTP GET; e constatamos variação entre 9% e 206% em tempo de conexão quando comparado o *ping* ao TCP *handshaking*.

Sumário

| | | |
|----------|-------------------------------------|-----------|
| 1 | Introdução | 2 |
| 1.1 | Fundamentação Teórica | 2 |
| 1.2 | Equipamentos Utilizados | 3 |
| 2 | Parte I | 4 |
| 2.1 | <i>Handshaking</i> TCP | 4 |
| 2.1.1 | Procedimento Experimental | 4 |
| 2.1.2 | Resultados e Análise | 5 |
| 2.2 | <i>Ping</i> | 6 |
| 2.2.1 | Procedimento Experimental | 6 |
| 2.2.2 | Resultados e Análise | 7 |
| 3 | Parte II | 8 |
| 4 | Conclusão | 11 |

Capítulo 1

Introdução

A transmissão de informação em redes como a Internet ou LANs se dá através da divisão da informação em pacotes, que são transmitidos nos mais diversos meios - Wi-Fi, Bluetooth, rádio, cabos de pares trançados, par metálico, fibra ótica - para chegar da origem ao seu destino. Os protocolos de rede nas camadas física, enlace, rede, transporte e aplicação são responsáveis por tornar essa comunicação transparente e viável por todo o globo terrestre.

O presente projeto tem como objetivo a análise de redes de comunicação através da técnica conhecida como *packet sniffing*, ou seja, examinar os pacotes que são enviados e recebidos para análise da eficiência da rede de comunicação sendo utilizada.

1.1 Fundamentação Teórica

Packet sniffing Técnica que consiste na análise dos pacotes que trafegam na rede, sejam eles endereçados à estação que está monitorando ou não. Através dessa técnica é possível medir a eficiência e taxa de ocupação de uma rede, além de interceptar toda o conteúdo de comunicação não criptografada.

Roteador Dispositivo capaz de interligar duas redes realizando tradução de endereços, permitindo a criação de redes cada vez maiores.

Hops Os pacotes transmitidos podem trafegar entre diversas redes para chegar ao seu destino. Quando o pacote passa de uma rede para outra através de um roteador, chamamos isso de *hop*.

Handshaking Processo onde ocorre troca de pacotes entre duas estações com o objetivo de se estabelecer uma conexão.

Ping Ferramenta que testa a conexão entre duas estações. Muito utilizada para medir performance, através do tempo que leva para a estação que “pinga” outra estação receber uma resposta, ou “pong”.

1.2 Equipamentos Utilizados

Para atingir os objetivos desse projeto, utilizamos os seguintes equipamentos e ferramentas:

MacBook Air Como estação de *packet sniffing*, utilizamos um MacBook Air de 13” com 4GB de memória RAM e processador Intel Core i7 1.8GHz;

Wireshark Para poder capturar os pacotes, utilizamos o software Wireshark, que é *open-source* e funciona monitorando atividade na interface de rede e capturando todos os pacotes que chegam a ela;

AirPort Express Para a criação da rede à qual foi conectado o MacBook, foi utilizado um AirPort Express configurado para criar uma rede WiFi no padrão 802.11g, a uma taxa de 54Mbps;

D-Link DI-634M Roteador utilizado para criação de uma subrede para compartilhamento do IP único de saída;

www.ip-address.com Ferramenta utilizada para estimativa da distância física em quilômetros entre a estação de teste e os sites escolhidos para teste.

A fim de realizar os testes necessários, foram utilizadas as seguintes conexões com a Internet:

CDT/UnB Conexão direta ao *backbone* das Universidades brasileiras, através de um endereço IP fixo fornecido pelo Centro de Apoio ao Desenvolvimento Tecnológico da Universidade de Brasília (CDT/UnB);

Oi Conexão ADSL à Internet com taxa de transferência contratada de 2Mbps fornecida pela empresa OI S.A.

Capítulo 2

Parte I

Objetivo A Parte I tem como objetivo a medição e análise de aspectos do tráfego de rede. Através da análise dos tempos de resposta a *ping* e de *handshaking* da conexão TCP, pretendemos traçar relação entre a distância física e número de *hops* entre os pontos da rede e os tempos medidos.

2.1 *Handshaking* TCP

2.1.1 Procedimento Experimental

Definição dos casos de teste Foram escolhidos quatro sites da Internet de acordo com a distância física com a estação de teste, com o objetivo de observar as variações de acordo com a distância até o destino. A relação de sites escolhidos para o teste está representada na Tabela 2.1, bem como o número de *hops* e distância física em quilômetros até o servidor.

| Site | Hops | Distância (km) | Localização |
|-----------------------|------|----------------|-------------|
| www.bangladesh.gov.bd | 24 | 15.465,6 | Bangladesh |
| www.thepiratebay.se | 15 | 10.180,8 | Suécia |
| www.km.gov.al | 15 | 9.363,2 | Albânia |
| www.cic.unb.br | 6 | 5 | Brasil |

Tabela 2.1: Sites escolhidos para teste de *handshaking* TCP

Escolha da conexão de rede Para a realização dos testes foi escolhida a rede do CDT/UnB, com o objetivo de verificarmos resultados mais interessantes, principalmente pelo site www.cic.unb.br estar hospedado na mesma infraestrutura e pela qualidade da conexão.

Preparo do ambiente de testes Com o objetivo de aproximar os testes de um caso real de uma rede de alto tráfego, durante os testes outras estações estavam utilizando a mesma conexão para *streaming* de vídeo e videoconferência via Skype.

Medição dos tempos de *handshaking* Através da utilização da ferramenta Wireshark, medimos o tempo decorrido entre o envio do primeiro pacote TCP ao site e o recebimento de sua resposta. Um exemplo da visualização fornecida pela ferramenta para os pacotes enviados e recebidos está representada pela Figura 2.1. Os tempos medidos foram armazenados em arquivos de texto para análise posterior.

| | | | | | | |
|----|-------------|-----------------|-----------------|------|------|---|
| 27 | 3.285721000 | 192.168.0.148 | 203.112.217.163 | TCP | 78 | 55630 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W |
| 32 | 3.855925000 | 203.112.217.163 | 192.168.0.148 | TCP | 60 | http > 55630 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 |
| 35 | 3.856055000 | 192.168.0.148 | 203.112.217.163 | TCP | 54 | 55630 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0 |
| 36 | 3.858700000 | 192.168.0.148 | 203.112.217.163 | HTTP | 387 | GET / HTTP/1.1 |
| 39 | 4.470863000 | 203.112.217.163 | 192.168.0.148 | TCP | 60 | http > 55630 [ACK] Seq=1 Ack=334 Win=6432 Len=0 |
| 40 | 4.620955000 | 203.112.217.163 | 192.168.0.148 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 41 | 4.621091000 | 203.112.217.163 | 192.168.0.148 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 42 | 4.621202000 | 192.168.0.148 | 203.112.217.163 | TCP | 54 | 55630 > http [ACK] Seq=334 Ack=2921 Win=65535 Len=0 |
| 43 | 4.634823000 | 192.168.0.148 | 203.112.217.163 | TCP | 78 | 55632 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W |
| 44 | 4.635135000 | 192.168.0.148 | 203.112.217.163 | TCP | 78 | 55634 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W |
| 45 | 4.635136000 | 192.168.0.148 | 203.112.217.163 | TCP | 78 | 55636 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W |
| 49 | 5.098023000 | 203.112.217.163 | 192.168.0.148 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 50 | 5.098224000 | 203.112.217.163 | 192.168.0.148 | HTTP | 1514 | Continuation or non-HTTP traffic |
| 51 | 5.098318000 | 192.168.0.148 | 203.112.217.163 | TCP | 54 | 55630 > http [ACK] Seq=334 Ack=5841 Win=65535 Len=0 |
| 52 | 5.098420000 | 203.112.217.163 | 192.168.0.148 | HTTP | 1514 | Continuation or non-HTTP traffic |
| 53 | 5.100553000 | 192.168.0.148 | 203.112.217.163 | TCP | 78 | 55638 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W |
| 54 | 5.125704000 | 203.112.217.163 | 192.168.0.148 | TCP | 60 | http > 55632 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 |

Figura 2.1: *Packet sniffing* da conexão com o site www.bangladesh.gov.bd

2.1.2 Resultados e Análise

Os resultados obtidos foram de acordo com o esperado. Quanto maior a distância física e número de *hops* entre a estação de teste e o site sendo testado, maior o tempo para completar o *handshake*, (T_{hs}), conforme mostrado na Tabela 2.2.

| Site | Hops | Distância (km) | $T_{hs}(ms)$ |
|--|------|----------------|--------------|
| www.bangladesh.gov.bd | 24 | 15.465,6 | 570,204 |
| www.thepiratebay.se | 15 | 10.180,8 | 314,048 |
| www.km.gov.al | 15 | 9.363,2 | 306,378 |
| www.cic.unb.br | 6 | 5 | 7,723 |

Tabela 2.2: Tabela compilada dos resultados obtidos no teste de *handshaking*

Análise

Apesar de haver uma relação clara entre a distância física, número de *hops* e T_{hs} , não é possível generalizar ou sequer traçar uma relação matemática. Percebe-se que T_{hs} depende da qualidade da conexão em geral, que é afetada pela distância, porém não exclusivamente.

Para conexão com o site www.cic.unb.br, percebemos que T_{hs} é muito reduzido, o que atribuímos a estar na mesma infraestrutura de rede que a estação de teste. Em comparação, a conexão com o site localizado em Bangladesh, a mais de 15 mil quilômetros de distância, T_{hs} é 7200% maior.

Conforme esperado, a relação entre distância, número de *hops* e o tempo para *handshaking* não é direta porém está presente. Em geral, quanto maior a distância, maior o número de *hops* e maior o tempo necessário para se estabelecer uma conexão.

2.2 Ping

2.2.1 Procedimento Experimental

Definição dos casos de teste Os sites escolhidos para os testes de *ping* foram inicialmente os mesmos utilizados para testes de *handshaking*. Porém, os sites www.thepiratebay.se e www.km.gov.al não responderam a *pings*. Portanto, os retiramos do teste e adicionamos os sites www.google.com e www.terra.com.br. Os sites escolhidos estão listados na Tabela 2.3, bem como o respectivo número de *hops* e distância física em quilômetros até o servidor.

| Site | Hops | Distância (km) | Localização |
|--|------|----------------|-------------|
| www.bangladesh.gov.bd | 24 | 15.465,6 | Bangladesh |
| www.google.com | 7 | 9.684,8 | EUA |
| www.terra.com.br | 5 | 996,8 | Brasil |
| www.cic.unb.br | 6 | 5 | Brasil |

Tabela 2.3: Sites escolhidos para teste de *ping*

Escolha da conexão de rede Para a realização dos testes foi escolhida a rede fornecida pela OI S.A., devido ao bloqueio implementado pela rede CDT/UnB a *pings*. Porém, para o caso específico do site www.cic.unb.br, utilizamos a rede do CDT/UnB por serem permitidos *pings* que não cruzam a fronteira da rede da UnB.

Preparo do ambiente de testes Com o objetivo de aproximar os testes de um caso real de uma rede de alto tráfego, os testes foram realizados sob a mesmo cenário dos testes de *handshaking*, com outras estações utilizando a mesma conexão para *streaming* de vídeo e videoconferência via Skype.

Medição dos tempos de *ping* Através da utilização da ferramenta Ping, do próprio sistema operacional Mac OS X, efetuamos o teste de *ping* para cada site separadamente. Cada teste foi realizado cinco vezes e o tempo considerado foi o médio constatado. Os tempos medidos foram armazenados em arquivos de texto para análise posterior.

2.2.2 Resultados e Análise

Os resultados obtidos foram de acordo com o esperado. Quanto maior a distância física e número de *hops* entre a estação de teste e o site sendo testado, maior o tempo para completar o *ping*, (T_{ping}), conforme mostrado na Tabela 2.4.

| Site | Hops | Distância (km) | T_{ping} (ms) |
|-----------------------|------|----------------|-----------------|
| www.bangladesh.gov.bd | 24 | 15.465,6 | 523,186 |
| www.google.com | 7 | 9.684,8 | 181,996 |
| www.terra.com.br | 5 | 996,8 | 58,081 |
| www.cic.unb.br | 6 | 5 | 2,519 |

Tabela 2.4: Resultados obtidos para teste de *ping*

Análise

Os resultados foram muito similares aos obtidos nos testes de *handshaking*, conforme esperado. Ainda em comparação com o teste de *handshaking*, destaca-se a diferença $T_{hs} - T_{ping} = 5,204ms$, o que representa tempo de *handshaking* 206% maior do que o tempo de *ping*. Resultado interessante quando comparado ao ocorrido para o site www.bangladesh.gov.bd, para o qual a mesma relação é de apenas 9%. Esse resultado é esperado uma vez que pequenas variações serão muito mais significativas quando o próprio tempo é pequeno.

Capítulo 3

Parte II

Objetivo A Parte II tem como objetivo a medição e análise de uma requisição HTTP GET.

A obtenção do endereço de 48 bits Ethernet (endereço MAC) do computador pode ser feita de diversas formas, via Wireshark ou através de um prompt de comando. Para a obtenção via Wireshark, capturou-se uma requisição HTTP/GET e observou-se o valor do campo *Source* em *Ethernet*. Da Figura Y, pode-se constatar que o endereço do *host* (*source*) é: 00:88:65:3e:85:7e. Pode-se perceber também uma referência ao nome "Apple" junto ao endereço de 48 bits da fonte. Isto ocorre porque “sniffing” foi feito em um Macbook Air.

P ara a obtenção via prompt de comando, utilizou-se o programa *ifconfig* (disponível em qualquer sistema UNIX) digitando no Terminal: `ifconfig -a`, conforme ilustra a Figura X (se estiver em ambiente Windows, o comando deve ser: `ipconfig \all`). Da Figura X, pode-se obter o endereço físico observando o valor hexadecimal na linha *ether* da interface *en0*.

2.1 Endereço: 00:88:65:3e:85:7e.

2.2 Endereço: 68:7f:74:eb:12:85. Não, esse é o endereço do roteador conectado à rede local. O roteador é da Linksys (Cisco), como pode-se perceber na Figura 3.1 tem uma referência ao nome “Cisco” junto ao host destino.

2.3 Como se pode ver na Figura 3.2, antes do ‘G’, tem-se 54 bytes. O caracter ‘G’ de “GET” corresponde ao valor hexadecimal 0x47. Podemos observar na tabela ASCII que esse número é o correspondente ao “G” maiúsculo.

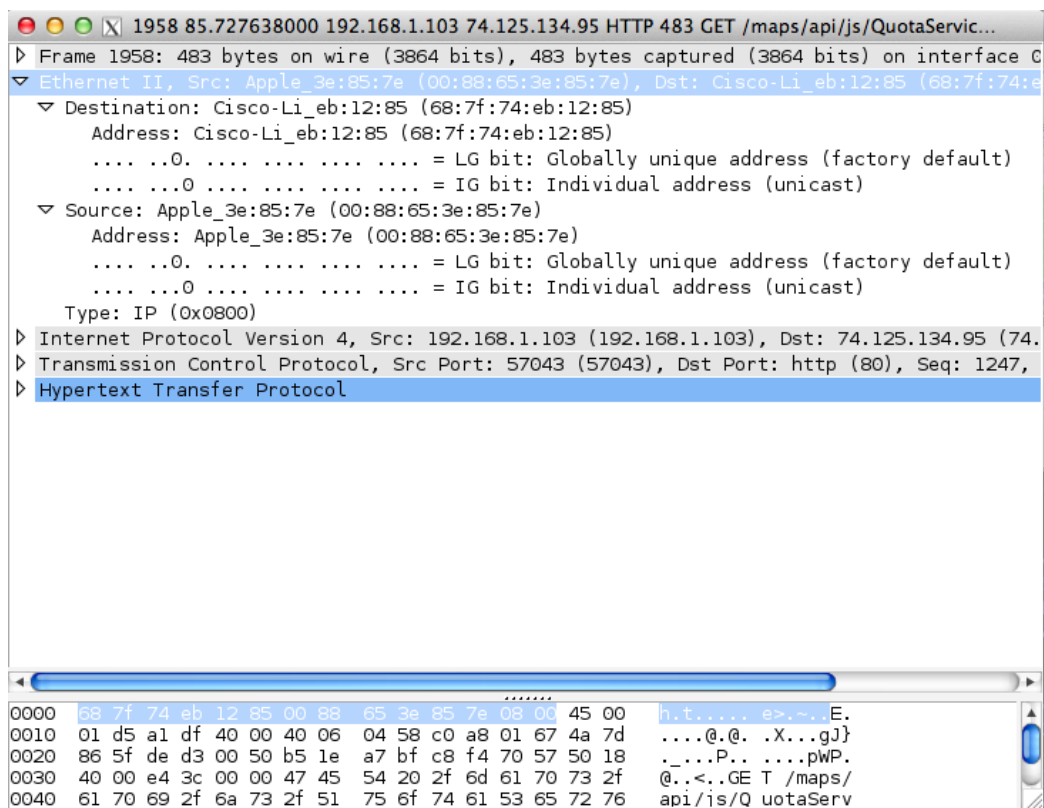


Figura 3.1: Origem e destino do pacote de rede

2.4 Endereço: 00:88:65:3e:85:7e. Do meu computador. Pode-se perceber uma referência ao nome “Apple” na Figura 3.1, junto ao endereço de 48 bits da fonte. Isto ocorre porque “sniffing” foi feito em um Macbook Air.

2.5 Endereço de destino: 68:7f:74:eb:12:85. Não, é o endereço Ethernet do roteador, conforme explicado na questão 2.1.

| | | | | | | | | | | | | | | | | | |
|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--------------------|
| 0000 | 68 | 7f | 74 | eb | 12 | 85 | 00 | 88 | 65 | 3e | 85 | 7e | 08 | 00 | 45 | 00 | h.t..... e>...E. |
| 0010 | 01 | d5 | a1 | df | 40 | 00 | 40 | 06 | 04 | 58 | c0 | a8 | 01 | 67 | 4a | 7d |@.@. .X...gJ} |
| 0020 | 86 | 5f | de | d3 | 00 | 50 | b5 | 1e | a7 | bf | c8 | f4 | 70 | 57 | 50 | 18 | ._...P... ..pWP. |
| 0030 | 40 | 00 | e4 | 3c | 00 | 00 | 47 | 45 | 54 | 20 | 2f | 6d | 61 | 70 | 73 | 2f | @..<...GE t /maps/ |
| 0040 | 61 | 70 | 69 | 2f | 6a | 73 | 2f | 51 | 75 | 6f | 74 | 61 | 53 | 65 | 72 | 76 | api/js/Q uotaServ |
| 0050 | 69 | 63 | 65 | 2e | 52 | 65 | 63 | 6f | 72 | 64 | 45 | 76 | 65 | 6e | 74 | 3f | ice.Reco rdEvent? |
| 0060 | 31 | 73 | 68 | 74 | 74 | 70 | 25 | 33 | 41 | 25 | 32 | 46 | 25 | 32 | 46 | 6c | lshttp%3 A%2F%2Fl |
| 0070 | 6f | 6f | 70 | 69 | 6e | 63 | 2e | 63 | 6f | 6d | 2e | 62 | 72 | 25 | 32 | 46 | oopinc.c om.br%2F |
| 0080 | 26 | 34 | 65 | 31 | 26 | 35 | 65 | 30 | 26 | 36 | 75 | 31 | 26 | 37 | 73 | 73 | &4e1&5e0 &6ul&7ss |
| 0090 | 31 | 36 | 71 | 37 | 62 | 26 | 63 | 61 | 6c | 6c | 62 | 61 | 63 | 6b | 3d | 5f | 16q7b&ca llback=_ |
| 00a0 | 78 | 64 | 63 | 5f | 2e | 5f | 7a | 67 | 6d | 34 | 62 | 6c | 26 | 74 | 6f | 6b | xdc_.zg m4bl&tok |
| 00b0 | 65 | 6e | 3d | 39 | 37 | 38 | 36 | 36 | 20 | 48 | 54 | 54 | 50 | 2f | 31 | 2e | en=97866 HTTP/1. |
| 00c0 | 31 | 0d | 0a | 48 | 6f | 73 | 74 | 3a | 20 | 6d | 61 | 70 | 73 | 2e | 67 | 6f | 1..Host: maps.go |

Figura 3.2: Conteúdo completo do pacote, em notação Hexadecimal e símbolo ASCII

Capítulo 4

Conclusão

O presente trabalho tornou possível uma visualização mais clara do modelo em camadas presente nas redes de computadores. Foi possível verificar, de forma prática, como as camadas inferiores encapsulam o que é passado pelas camadas de cima, adicionando os respectivos bits de *overhead* (HTTP <-> TCP/IP <-> Ethernet).

Também foi possível verificar o conteúdo presente em uma requisição HTTP GET, como tal requisição torna possível a transmissão de conteúdo em Hypertext (HTML) na WEB e sua natureza *stateless*. Endereços físicos (MAC) e seu funcionamento puderam ser melhor assimilados, juntamente com as funções da camada de enlace: enquadramento, detecção e correção de erros, retransmissões, acesso múltiplo e *switching*.

Foi possível também observar a influência que distância física, número de *hops* e qualidade da rede possuem nos tempos de requisição, fazendo-nos perceber que o estudo e evolução dos protocolos de rede é de suma importância para a garantia de melhoria contínua e perenidade da Internet e demais redes de computadores.

Referências Bibliográficas

- [1] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee; *RFC 2616 - Hypertext Transfer Protocol – HTTP/1.1*; 1999
- [2] Leon, A., Garcia I. Widjaja; *Communication Networks: Fundamental Concepts and Key Architectures*; Mc Graw Hill
- [3] Tanenbaum, A.S.; *Redes de Computadores*; Editora Campus; Quarta Edição