

Análise da Rede e Tráfego

Jonatas Gomes¹ 14/0146407
Gabriel Tomaz² 16/0121531
Lincoln Barbosa³ 14/0045023

I. INTRODUÇÃO

Trabalho proposto na disciplina Teleinformática e redes. Foi simulado uma rede usando o programa NS-3, o objetivo da tarefa era simular protocolos de tráfego e compará-los a um ambiente real. Através de uma simulação foi possível fixar o conteúdo e conceitos aprendidos em sala de aula.

II. TEORIA

A. Modelo OSI

Foi considerada uma rede com arquitetura que se divide em 5 camadas: aplicação, transporte, rede, enlace e física. tal como Modelo OSI, um modelo de rede de computador dividido em camadas de funções, criado em 1971 e formalizado em 1983, com objetivo de ser um padrão, para protocolos de comunicação entre os mais diversos sistemas de rede local Ethernet, garantindo a comunicação entre dois sistemas computacionais.

B. MAC Media Access Control

MAC é um termo utilizado em redes de computadores para designar parte da camada de enlace, camada número 2 segundo o modelo OSI. É provedora de acesso a um canal de comunicação e o endereçamento neste canal possibilitando a conexão de diversos computadores numa rede. O endereçamento é realizado pelo endereço MAC ou também chamado endereço físico que consiste em um número único a cada dispositivo de rede possibilitando o envio de pacotes para um destino especificado mesmo que esteja em outra subrede. Atua como interface entre a LLC e a camada física provendo uma emulação de comunicação full duplex.

C. NS-3

Ns ou network simulator é um simulador de redes de computadores muito popular no meio acadêmico por seu código fonte aberto. o NS-3 é muito utilizado em pesquisas sobre redes, suporta protocolos de rede mais populares tanto para redes cabeadas quanto para sem fio. A primeira versão do ns foi desenvolvida em 1989 baseada no Real Network Simulator. A versão atual é a 3. a linguagem de uso no NS-3 é o c++ as quais possuem os objetos de eventos e elementos de rede.

III. ANÁLISE EXPERIMENTAL

Teremos a análise envolta em uma rede IEEE 802.11, esse tipo de rede encapsula o protocolo em um datagrama de camada de rede em um quadro contendo mais alguns cabeçalhos que servem para o desenvolvimento dos serviços da camada de enlace, entre esses serviços estão o controle de erros, controle de fluxo, multiplexação.

A. Identificando protocolos utilizados

Ao observar uma mensagem trocada pela rede podemos identificar que está rodando o protocolo 802.3. Temos um pacote e é possível ver que agora a camada de enlace insere menos campos para criação de um quadro, isso deve ao fato de uma rede ethernet cabeada ser mais confiável que uma sem fio tendo assim um overhead menor. Observe na figura abaixo. Protocolo 802.11

```
1 0.000000 00:00:00_00:00:58 Broadcast 802.11
2 0.000256 00:00:00_00:00:57 00:00:00_00:00:58 802.11
3 0.000272 00:00:00_00:00:57 00:00:00_00:00:58 (... 802.11
4 0.000455 00:00:00_00:00:55 00:00:00_00:00:58 802.11
5 0.000471 00:00:00_00:00:55 00:00:00_00:00:58 (... 802.11
6 0.000654 00:00:00_00:00:4c 00:00:00_00:00:58 802.11
7 0.000670 00:00:00_00:00:4c 00:00:00_00:00:58 (... 802.11
8 0.000862 00:00:00_00:00:50 00:00:00_00:00:58 802.11
9 0.000878 00:00:00_00:00:50 00:00:00_00:00:58 (... 802.11
10 0.001061 00:00:00_00:00:56 00:00:00_00:00:58 802.11
11 0.001077 00:00:00_00:00:56 00:00:00_00:00:58 (... 802.11
12 0.001260 00:00:00_00:00:54 00:00:00_00:00:58 802.11
13 0.001276 00:00:00_00:00:54 00:00:00_00:00:58 (... 802.11
14 0.001468 00:00:00_00:00:52 00:00:00_00:00:58 802.11

Frame 1: 61 bytes on wire (488 bits), 61 bytes captured (488 bits)
Encapsulation type: IEEE 802.11 Wireless LAN (20)
Arrival Time: Dec 31, 1969 21:00:00.021081000 -03
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 0.021081000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 61 bytes (488 bits)
Capture Length: 61 bytes (488 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: wlan]
IEEE 802.11 Beacon frame, Flags: .....
Type/Subtype: Beacon frame (0x0008)
▶ Frame Control Field: 0x8000
   0000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: 00:00:00_00:00:58 (00:00:00:00:00:58)
Source address: 00:00:00_00:00:58 (00:00:00:00:00:58)
BSS Id: 00:00:00_00:00:58 (00:00:00:00:00:58)
   .... 0000 = Fragment number: 0
   0000 0000 0000 .... = Sequence number: 0
IEEE 802.11 wireless LAN management frame
▶ Fixed parameters (12 bytes)
▶ Tagged parameters (25 bytes)
```

Podemos ver a diferença comparando com o mesmo Local: 802.3

```
▶ Frame 114: 1076 bytes on wire (8560 bits), 1076 bytes captured (8560 bits)
▼ Ethernet II, Src: 00:00:00_00:00:17 (00:00:00:00:00:17), Dst: 00:00:00_00:00:0b (00:00:00:00:00:0b)
   ▶ Destination: 00:00:00_00:00:0b (00:00:00:00:00:0b)
   ▶ Source: 00:00:00_00:00:17 (00:00:00:00:00:17)
   Type: IP (0x0800)
   ▶ Frame check sequence: 0x00000000 [validation disabled]
   ▶ Internet Protocol Version 4, Src: 10.1.6.13 (10.1.6.13), Dst: 10.1.11.7 (10.1.11.7)
   ▶ User Datagram Protocol, Src Port: 9 (9), Dst Port: 49153 (49153)
   ▶ Data (1024 bytes)
```

B. Enquadramento utilizado CSMA/CD CSMA/CA

Basicamente o protocolo CSMA consiste de em executar o canal antes de transmitir e, se o canal estiver ocupado ele espera para transmitir em outro momento. Mesmo assim colisões ainda podem ocorrer, Por esse motivo a distância entre os nós é fundamental nas colisões deste protocolo.

C. Controle de Erro

Para o tratamento de erros é utilizado o próprio protocolo de enlace PPP, ele possui um campo com tamanho entre 2 e 4 bytes para o checksum do pacote, que é utilizado pelo Network Control Protocol (NCP) para detectar e calcular a taxa de perda de pacotes por erros por meio de verificação de redundância cíclica (CRC).

D. Camada de enlace

Foi escolhido a topologia ponto a ponto (PPP) para a implementação da camada de enlace.

Na topologia PPP uma mensagem enviada por um cliente passa por todos outros nós/clientes que estão no caminho, o primeiro nó da primeira rede foi conectado ao primeiro nó da segunda rede e assim por diante, sendo assim a mensagem passa através de retransmissões, até ser retirada pelo cliente destino ou pelo nó fonte. Uma das vantagens de se utilizar a topologia ponto a ponto é a facilidade de conexão entre os nós diferente de outras topologias centralizadas que precisam de uma administração, conforme a rede cresce também vão crescendo os seus recursos que são compartilhados pela rede. A segurança pode ser um fator a ser notado porque esse tipo de rede está exposto a menos falhas e erros de compartilhamentos e ataques. O uso do recurso é compartilhado e pode estar disponível caso houver uma inatividade de um cliente, aumentando o processamento da rede. A escolha dessa topologia para ser implementada no trabalho foi devido a sua robustez, mediante das vantagens e da forma real aplicada em ambientes de redes.

IV. CALCULO DA EFICIÊNCIA

Usamos um arquivo pcap obtido na simulação correspondente a uma rede IEEE 802.11, ou seja , que esta rodando o protocolo CSMA/CA. A eficiência consiste em comparar a quantidade de informação real que foi transmitida.

Na simulação, foram enviadas 10 mensagens de 1024 bytes para os servidores de echo, ou seja , há outras 12 mensagens de 1024 bytes de resposta.

Então no total circularam na rede $(10+10)*1024 = 20480$ bytes de resposta.

Agora para calcular o overhead temos que, para cada mensagem de 1024 bytes , foi enviado na camda física 1088 bytes. Essa difereça de 64 bytes é por conta do encapsulamento.

Só por esse overhead, a rede teria uma eficiência $1024/1088 = 0.94$. Porém, o protocolo CSMA/CA troca

diversas mensagens antes de começar a enviar dados da aplicação.

Entretanto, circulou na rede um total de 74124 bytes para um total de 24576 bytes de dados gerado pela aplicação. Assim a eficiencia foi de 0.33 , pode ser considerada uma eficiência baixa , mas é necessário todo esse overhead para evitar colisões.

V. CONCLUSÃO

A partir dos testes feitos no ns-3, foi possível perceber e analisar os protocolos desenvolvidos em sala de aula e utilizados em redes de todo mundo.

Vimos protocolos que funcionam em diferentes tipos de redes, 802.3 e 802.11x ethernet e wi-fi respectivamente. Cada protocolo com suas especificações e modo de comunicação.

Podemos analisar que os protocolos utilizam uma gama de recursos para conseguir entregar a comunicação ao destinatário com o mínimo percentual de erro e com alta confiabilidade.

Conclui-se que o objetivo do trabalho foi concluído com êxito pelos integrantes do grupo.

REFERENCES

- [1] Leon-Garcia, Alberto; Widjaja, Inra, Communication Networks, 2nd edition. New York, New York, USA: McGraw-Hill Education, July 16, 2003, ISBN-13: 978-0072463521, ISBN-10: 007246352X.
- [2] Solis, Priscila, Teleinformatica e Redes 1 - Notas de aula e trans-parências . Brasília, Brasil: Universidade de Brasília, 2017.
- [3] Ross,Keith W.; Kurose,Jim, Redes de Computadores e A Internet - Uma Abordagem Top-Down, 1a edição. São Paulo, Brasil: Pearson ~ Education - Br, 2013.