Segundo trabalho prático: Wireshark e SNMP

João Vitor Maia Neves Cordeiro

4 de abril de 2021

Resumo

O presente trabalho visa demonstrar a utilização de ferramentas de gerenciamento de rede como o PRTG e o Wireshark, a fim de dar ao leitor o material necessário para compreender o uso desses softwares e replicar os experimentos realizados. Com o uso dos programas foi realizado um monitoramento que inicialmente seria de 3 dias com interrupções, mas com o professor oferecendo uma extensão do prazo, foi decidido por continuar o monitoramento durante uma semana. Durante o monitoramento foram compreendidos conceitos importantes sobre os protocolos utilizados como ARP, SNMP e UDP; Além disso, essa atividade também proporcionou um entendimento de como gerenciar uma rede doméstica, verificando a eficiência da rede.

Sumário

1 Introdução

O monitoramento de rede é de suma importância quando discutimos sobre Quality of Service (QoS) e segurança preventiva contra ataques cibernéticos. Nesse relatório será demonstrado o trabalho prático realizado utilizando as ferramentas PRTG e Wireshark, um monitoramento detalhado para nos ajudar a compreender o tráfego de pacotes entre os dispositivos de uma rede doméstica. As ferramentas utilizadas são renomadas e tidas como padrões do mercado (apesar de existirem outras boas ferramentas disponíveis), portanto o compreendimento da utilização delas é imprescindível para um profissional da computação que deseje trabalhar com redes de computadores.

2 Ferramentas utilizadas

2.1 PRTG

O PRTG Network Monitor é uma ferramenta *agentless* de monitoramento de rede, ou seja, a instalação é feita em um computador central e os outros computadores da rede não precisam instalar agentes próprios. Além disso, o software conta com uma interface *web-based* moderna e com boa usabilidade que permite gerar relatórios e gráficos em cima das medições realizadas. Como pontos negativos do software pode-se dizer que ele é restrito à plataforma Windows, além de que por se tratar de um software proprietário com um *trial* de 30 dias o acesos a ele é mais restrito do que a suas alternativas open-source.

2.2 Wireshark

O Wireshark é uma ferramenta *open souce* e gratuita para monitoramento de pacotes que nos permite verificar a entrada e saída de dados do computador. Diferentemente do PRTG, ele possui suporte para diversas plataformas e todos os recursos estão disponíveis de forma gratuita.

3 Topologia da rede

O monitoramento foi realizado em uma rede doméstica, utilizando os serviços da CLARO S/A, tendo conectados nas redes os seguintes dispositivos: um Desktop customizado, um Macbook Air 2017 e um notebook Lenovo S30. O PRTG Server Core foi instalado no Desktop, devido a maior robustez dessa máquina, os outros dispositivos foram adicionados ao monitoramento pelo painel do PRTG. Entretanto, não foi possível adicionar sensores muito complexos aos outros dispositivos da rede. Todos os dispositivos foram utilizados na análise do Wireshark.

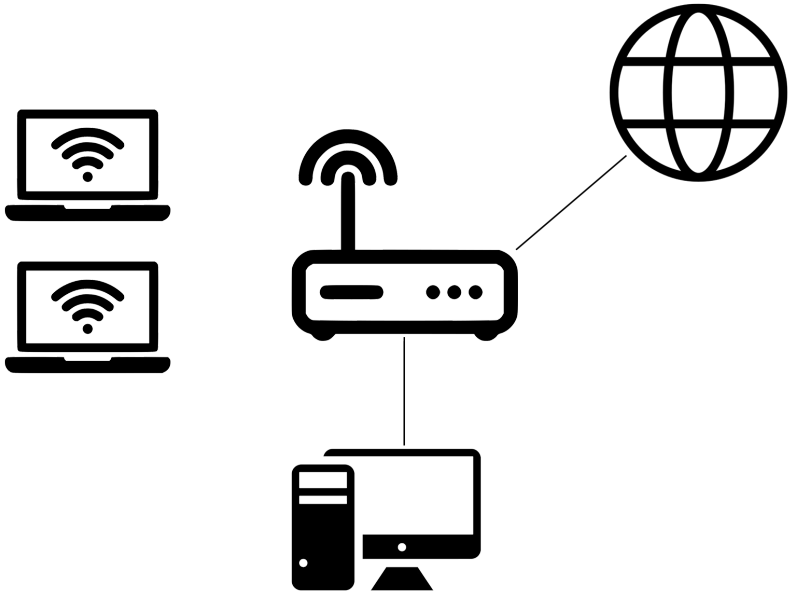


Figura 1: Uma rede doméstica com 4 dispositivos: Um notebook Lenovo (192.168.0.102), um macbook air (192.168.0.101), um desktop gamer (192.168.0.100) e um Modem com roteador (192.168.1.1)

3.1 Equipamentos

- Desktop
  - Processador: Ryzen 5 3600 @ 3.60 GHz
  - Memória RAM: 16GB DDR4 3000Mhz
  - Sistema Operacional: Windows 10
  - Adaptador Ethernet: Realtek PCIe GBE Family Controller
- Macbook
  - Processador: Intel i5 3600 @ 3.60 GHz
  - Memória RAM: 8 GB LPDDR3 1600 MHz
  - Sistema Operacional: OSX Mojave
  - Adaptador Wireless: 802.11ac

- Notebook Lenovo S30
  - Processador: Intel® Core™ i5-1035G1 Quad Core 1.0 GHz com Turbo Max até 3.6 GHz
  - Memória RAM: 4 GB DDR4 2666 MHz + 16 GB Optane (4 GB soldado + 1 slot livre)
  - Sistema Operacional: Windows 10
  - Adaptador Wireless: 802.11ac
- Modem
  - Modelo: TP-Link WR740N
  - Frequência: 2.4 GHz

4 Monitoramento

O PRTG diferencia os dispostivos entre *Probe device* e *network device*, sendo que o primeiro diz respeito a dispositivos que possuem o PRTG Core Server instalado diretamente, possibilitando melhores medições com sensores mais avançados. Enquanto o segundo são os dispositivos conectados na rede e visualizados através de protocolos de rede apenas. Durante esse trabalho foi utilizado apenas um *probe device* devido a impossibilidade de instalar outros na rede, tendo em vista que o PRTG é instalável apenas no Windows e os outros computadores da rede utilizam sistemas Unix.

4.1 Probe health

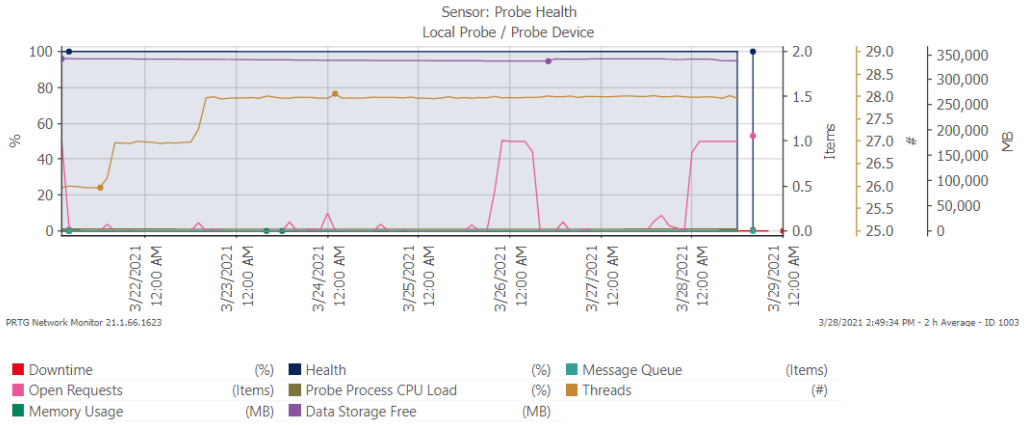


Figura 2: Gráfico de 7 dias do sensor Probe Health gerado pelo PRTG.

O sensor *Probe health* demonstra com detalhes métricas de funcionamento do *probe device* em relação ao PRTG, como downtime, uso de memória (pelo PRTG), número de threads e CPU load. Observando a medição realizada durante os 7 dias, percebe-se que com o computador em funcionamento por mais tempo o número de threads tende a subir no começo mas estabilizar-se após um ou dois dias. Também foram verificados dois picos de requisições em aberto, durante duas madrugadas, provavelmente ocasionado pelas sessões de jogos online realizadas durante esse período.

4.2 System health

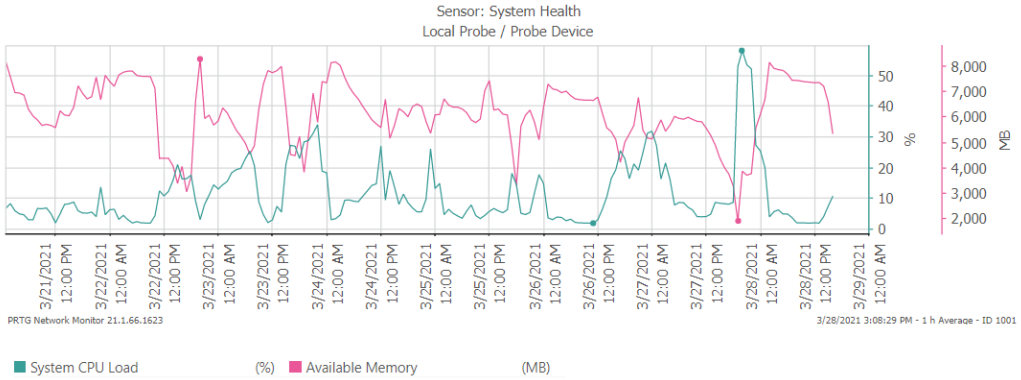


Figura 3: Gráfico de 7 dias do sensor System Health gerado pelo PRTG.

O sensor *System health* monitora o hardware sistema hospedeiro, a fim de verificar picos de uso do sistema e as causas deles. Na medição realizada podemos ver que a máquina em questão está sempre com grandes quantidades de carga, isso se deve ao sistema Windows utilizar RAM proporcional a RAM disponível, além disso a máquina também roda serviços como o PostgreSQL e MongoDB que ficam ligados durante todo o dia consumindo recursos.

4.3 Common SaSS Check

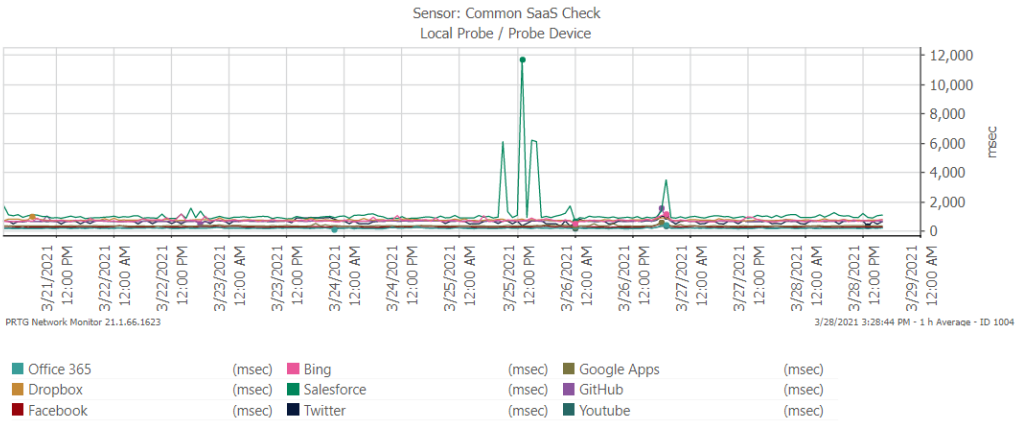


Figura 4: Gráfico de 7 dias do sensor Common SaSS Check gerado pelo PRTG.

Esse sensor verifica a disponibilidade (em forma de ping) de serviços online comuns a serem utilizados em um escritório, pode ser muito útil no gerenciamento de uma rede corporativa. Durante a maior parte dos serviços se manteve abaixo de 300ms, mas podemos destacar um pico de mais de 11k de milissegundos no serviço da Salesforce, ocorrido no dia 25 de março entre 12:00PM e 01:00PM, provavelmente algum problema no próprio serviço da salesforce, considerando que os outros serviços não demonstraram esse pico.

4.4 HTTP

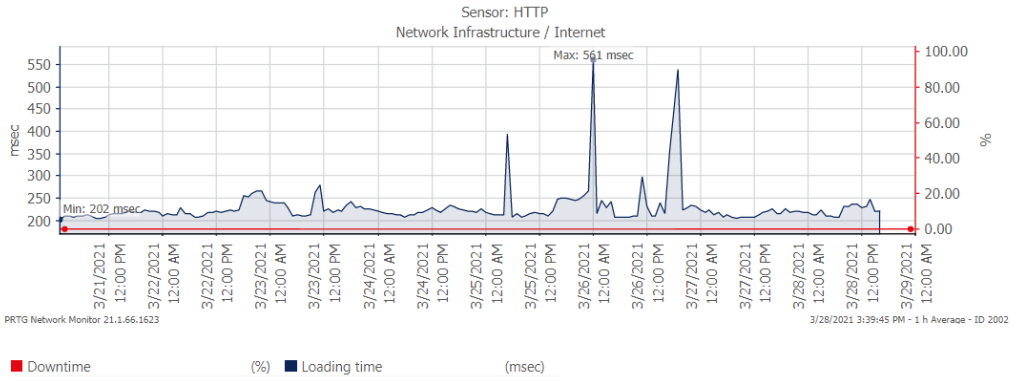


Figura 5: Gráfico de 7 dias do sensor HTTP gerado pelo PRTG.

O sensor HTTP monitora tempo de carregamento de páginas através do protocolo de comunicação HTTP, muito utilizado em browsers para acessar sites. No monitoramento foi verificado um pico acima de 500 ms, ao olhar no histórico de navegação foi possível constatar que nesse horário o único site sendo carregado era o twitter.com.

4.5 Ping - Network device

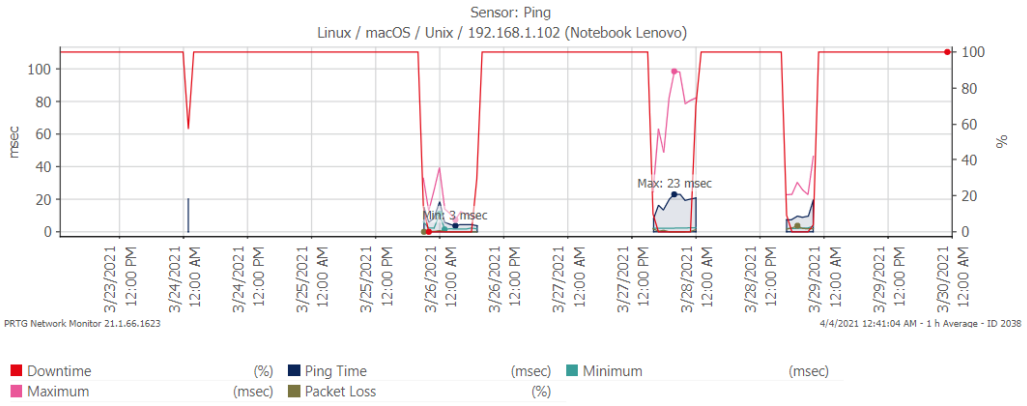


Figura 6: Gráfico de 7 dias do sensor ping gerado pelo PRTG.

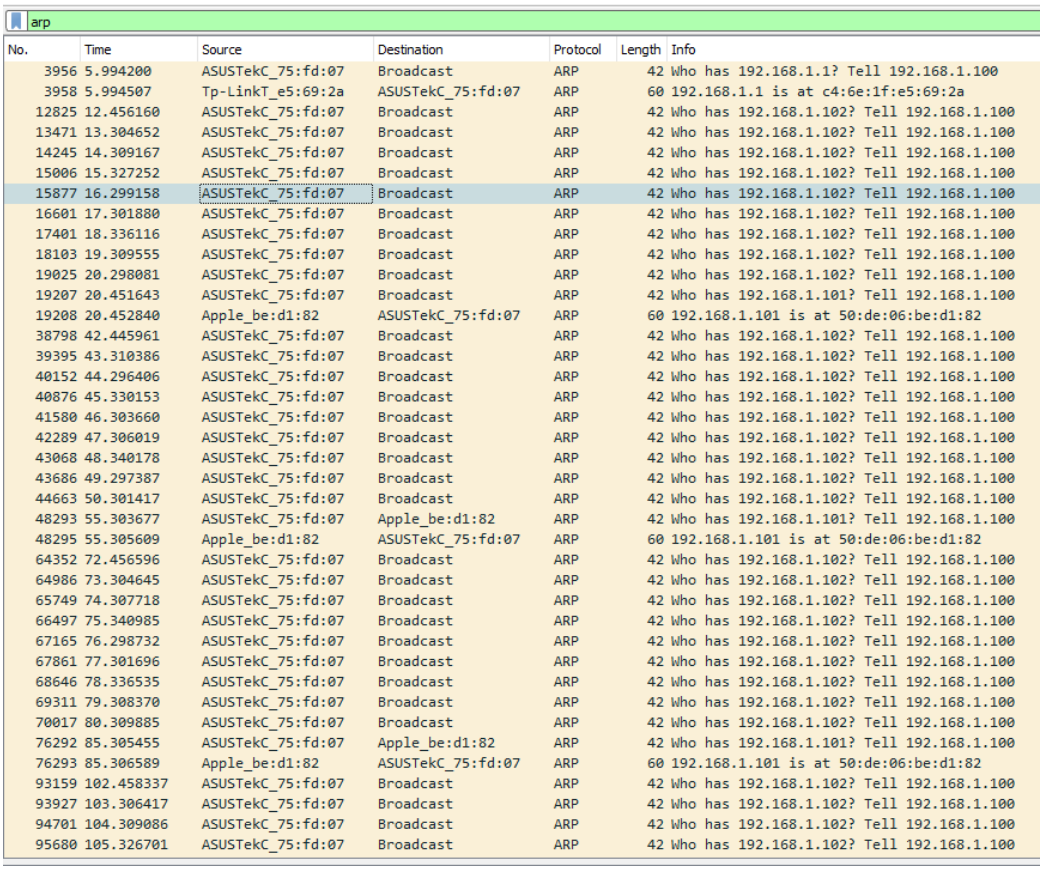
O sensor de ping monitora o tempo de resposta um ping pelo protocolo TCP/IP, o PRTG permite monitorar pings para quaisquer dispostivos da rede, no monitoramento foi abaixo foram realizados pings para o Notebook Lenovo citado na sessão de topologia de rede. O tempo de monitoramento nele foi menor pois o notebook em questão não fica ligado durante o tempo todo como o Desktop utilizado de *probe device*.

5 Wireshark

5.1 Address Resolution Protocol (ARP)

O Address Resolution Protocol (ARP) transforma endereços da camada da internet (normalmente um endereço IPV4) em endereços da camada de enlace (como por exemplo um endereço MAC), esse protocolo é essencial para o funcionamento da internet e de redes locais. No Wireshark podemos monitorar o funcionamento do protocolo ARP por meio de um filtro, já que o software tem em sua configuração padrão a capacidade de monitorar o protocolo.

A imagem abaixo foi obtida após um monitoramento de 5 minutos contínuos no Wireshark, com o filtro *arp* ligado (dessa forma o software ignora todos os outros protocolos e comunicações). Podemos perceber que o dispositivo com endereço 192.168.1.100 (Desktop) envia pela rede um pedido de identificação das máquinas com endereço 192.168.1.101 (Macbook) e 192.168.1.102 (Notebook Lenovo). O dispositivo com endereço 192.168.1.101 responde, enviando seu endereço MAC como identificação. O dispositivo com endereço 192.168.1.102 não envia resposta, então o Desktop continua fazendo pedidos pela rede. Também vemos uma troca de mensagens entre o Desktop e o roteador TPLink, quando o Desktop pergunta ao roteador qual seu endereço MAC.



arp

No.	Time	Source	Destination	Protocol	Length	Info
3956	5.994200	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.100
3958	5.994507	Tp-LinkT_e5:69:2a	ASUSTekC_75:fd:07	ARP	60	192.168.1.1 is at c4:6e:1f:e5:69:2a
12825	12.456160	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
13471	13.304652	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
14245	14.309167	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
15006	15.327252	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
15877	16.299158	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
16601	17.301880	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
17401	18.336116	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
18103	19.309555	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
19025	20.298081	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
19207	20.451643	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.101? Tell 192.168.1.100
19208	20.452840	Apple_be:d1:82	ASUSTekC_75:fd:07	ARP	60	192.168.1.101 is at 50:de:06:be:d1:82
38798	42.445961	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
39395	43.310386	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
40152	44.296406	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
40876	45.330153	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
41580	46.303660	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
42289	47.306019	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
43068	48.340178	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
43686	49.297387	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
44663	50.301417	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
48293	55.303677	ASUSTekC_75:fd:07	Apple_be:d1:82	ARP	42	Who has 192.168.1.101? Tell 192.168.1.100
48295	55.305609	Apple_be:d1:82	ASUSTekC_75:fd:07	ARP	60	192.168.1.101 is at 50:de:06:be:d1:82
64352	72.456596	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
64986	73.304645	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
65749	74.307718	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
66497	75.340985	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
67165	76.298732	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
67861	77.301696	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
68646	78.336535	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
69311	79.308370	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
70017	80.309885	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
76292	85.305455	ASUSTekC_75:fd:07	Apple_be:d1:82	ARP	42	Who has 192.168.1.101? Tell 192.168.1.100
76293	85.306589	Apple_be:d1:82	ASUSTekC_75:fd:07	ARP	60	192.168.1.101 is at 50:de:06:be:d1:82
93159	102.458337	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
93927	103.306417	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
94701	104.309086	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100
95680	105.326701	ASUSTekC_75:fd:07	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.100

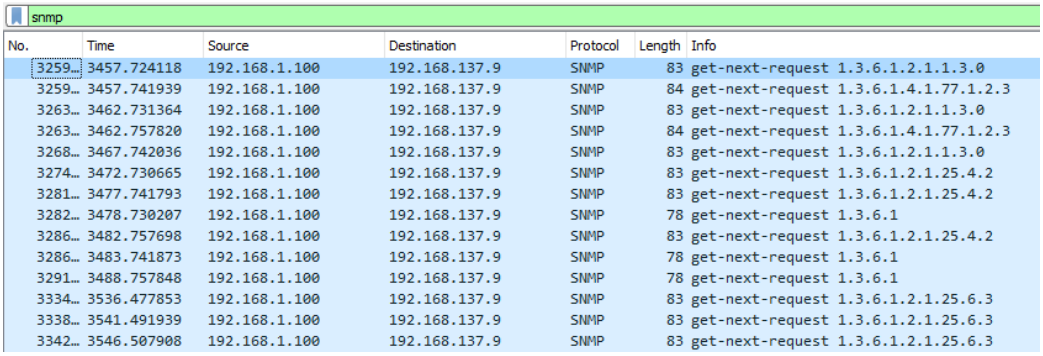
Figura 7: Tabela de ocorrências do protocolo ARP monitoradas pelo Wireshark.

5.2 Simple Network Management Protocol (SNMP)

Simple Network Management Protocol é um protocolo para organização de dispositivos gerenciados em uma rede IP, o Wireshark também é capaz de captar nativamente as trocas de mensagens relativas ao SNMP, por meio do filtro *snmp* podemos configurar o software para mostrar apenas essas mensagens.

Na imagem abaixo foi realizado um monitoramento por mais de uma hora a fim de capturar mensagens relativas ao SNMP, o monitoramento se extendeu tanto devido a uma demora na captação de mensagens do tipo. Todas as transmissões interceptadas foram realizadas pelo dispositivo de IP

192.168.1.100 (Desktop) com o destino sendo o dispositivo de IP 192.168.137.9 que é um adaptador Wireless conectado a outra máquina. Todas as transmissões são do tipo *get-next-request*



snmp

No.	Time	Source	Destination	Protocol	Length	Info
3259…	3457.724118	192.168.1.100	192.168.137.9	SNMP	83	get-next-request 1.3.6.1.2.1.1.3.0
3259…	3457.741939	192.168.1.100	192.168.137.9	SNMP	84	get-next-request 1.3.6.1.4.1.77.1.2.3
3263…	3462.731364	192.168.1.100	192.168.137.9	SNMP	83	get-next-request 1.3.6.1.2.1.1.3.0
3263…	3462.757820	192.168.1.100	192.168.137.9	SNMP	84	get-next-request 1.3.6.1.4.1.77.1.2.3
3268…	3467.742036	192.168.1.100	192.168.137.9	SNMP	83	get-next-request 1.3.6.1.2.1.1.3.0
3274…	3472.730665	192.168.1.100	192.168.137.9	SNMP	83	get-next-request 1.3.6.1.2.1.25.4.2
3281…	3477.741793	192.168.1.100	192.168.137.9	SNMP	83	get-next-request 1.3.6.1.2.1.25.4.2
3282…	3478.730207	192.168.1.100	192.168.137.9	SNMP	78	get-next-request 1.3.6.1
3286…	3482.757698	192.168.1.100	192.168.137.9	SNMP	83	get-next-request 1.3.6.1.2.1.25.4.2
3286…	3483.741873	192.168.1.100	192.168.137.9	SNMP	78	get-next-request 1.3.6.1
3291…	3488.757848	192.168.1.100	192.168.137.9	SNMP	78	get-next-request 1.3.6.1
3334…	3536.477853	192.168.1.100	192.168.137.9	SNMP	83	get-next-request 1.3.6.1.2.1.25.6.3
3338…	3541.491939	192.168.1.100	192.168.137.9	SNMP	83	get-next-request 1.3.6.1.2.1.25.6.3
3342…	3546.507908	192.168.1.100	192.168.137.9	SNMP	83	get-next-request 1.3.6.1.2.1.25.6.3

Figura 8: Tabela de ocorrências do protocolo SNMP monitoradas pelo Wireshark.

6 Conclusão

Para realizar o presente trabalho foi necessário pesquisar e entender o funcionamento de ferramentas utilizadas na gerência de redes, como o PRTG e o Zabbix. Utilizando essa ferramenta podemos perceber o funcionamento de uma rede doméstica em suas nuances mais específicas, podendo utilizar esses conhecimentos para otimizar a rede e os processos envolvidos em um futuro trabalho profissional.

Para utilizar o Wireshark para compreender o tráfego geral da rede também foi necessário estudar e compreender o funcionamento de protocolos como ARP, SNMP, TCP, UDP e outros, a fim de analisar com mais precisão o output gerado pelo programa. Essa etapa se mostrou fundamental para a análise geral da rede. Com tudo isso dito, fica evidente a importância desse trabalho na agregação de conhecimento ao aluno que o desenvolve com comprometimento e seriedade, sendo um bom marco na formação do estudante de ciência da computação.

Referências

[1] Fortinet. Snmp protocol basics. https://www.manageengine.com/network-monitoring/what-is-snmp.html, 2021. [Online; acessado em 23 de março].

[2] Fortinet. What is address resolution protocol (arp)? https://www.fortinet.com/resources/cyberglossary/what-is-arp, 2021. [Online; acessado em 23 de março].

[3] Paessler. Prtg network monitor v21. https://www.br.paessler.com/prtg, 2021. [Online; acessado em 23 de março].

[4] Wireshark. Wireshark docs. https://www.wireshark.org/docs, 2021. [Online; acessado em 23 de março].