Segundo trabalho prático (Wireshark e SNMP)

Rafael Begnini de Castilhos

24 de dezembro de 2021

Resumo

O presente relatório possui como objetivo demonstrar a utilização e gerenciamento de rede com as ferramentas o PRTG e o Wireshark, com o fito de prover ao leitor a base necessária para entendimento do uso desses *softwares* e replicar os experimentos realizados. Fazendo o uso dos programas foi realizado um monitoramento de aproximadamente 3 horas por dia num período de 4 dias. Durante o monitoramento foram compreendidos conceitos importantes sobre os protocolos utilizados como *ARP* e *SNMP*. Proporcionando um melhor entendimento de como gerenciar uma rede doméstica, verificando a eficiência da mesma.

Sumário

1 Introdução

Nesse relatório será demonstrado o trabalho prático realizado utilizando as ferramentas PRTG e Wireshark. Desse modo será possível realizar um monitoramento para ajudar a compreender o tráfego de pacotes entre os dispositivos de uma rede doméstica. As ferramentas utilizadas são de alta credibilidade e sucesso no mercado da tecnologia da informação, com isso, o compreendimento da utilização delas é imprescindível para um profissional da computação que deseje trabalhar com o gerenciamento de redes de computadores.

2 Ferramentas de gerência

2.1 PRTG

O PRTG Network Monitor é uma ferramenta de monitoramento de rede. A instalação é feita em um computador centralizador e os outros dispositivos da rede não necessitam de qualquer instalação ou configuração. Além do mais, o software conta com uma interface web prática, eficiente e com excelente usabilidade, permitindo gerar relatórios, gráficos e visualizações automaticamente, de acordo com as métricas extraídas. Entretanto, o software 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 para monitoramento de pacotes que permite verificar a entrada e saída de dados do computador, sendo *open-source* e gratuita . Diferentemente do PRTG, possui suporte para diversas plataformas e todos os recursos estão disponíveis gratuitamente.

3 Topologia da rede

O monitoramento foi executado em uma rede doméstica, utilizando os serviços da AdylNet Telecom, tendo conectados nas redes os seguintes dispositivos: Um notebook Lenovo Thinkpad, um notebook Acer AspireF5, um desktop customizado e um Raspberry PI Zero W. O PRTG foi instalado no notebook Lenovo Thinkpad, devido a maior robustez dessa máquina, os outros dispositivos foram adicionados ao monitoramento pelo painel do PRTG, com sensores de Ping e SSH estabelecidos. Todos os dispositivos foram utilizados posteriormente na análise do Wireshark.

Figura 1: Um notebook Lenovo Thinkpad (192.168.0.151) conectado com fio ao roteador, um notebook Acer AspireF5 (192.168.0.101), um desktop (192.168.0.80), um Raspberry PI Zero W (192.168.0.38), um Smartphone Motorola X4 (192.168.0.220), uma TV Samsung Smart e um Modem com roteador (192.168.0.1)

3.1 Equipamentos

- Desktop (192.168.0.80)
  - Processador: Intel i7 3770 6.30 GHz
  - Memória RAM: 16GB DDR4 3000Mhz
  - Placa de vídeo: NVIDIA GeForce GTX 660
  - Sistema Operacional: Ubuntu 20.04
  - Adaptador Ethernet: Realtek PCIe
- Notebook Lenovo Thinkpad (192.168.0.151)
  - Processador: Intel i7 8565U 4.60 GHz
  - Memória RAM: 16GB DDR4 3000Mhz
  - Placa de vídeo: Intel UHD 620
  - Sistema Operacional: Windows 10
- Notebook Acer AspireF5 (192.168.0.101)
  - Processador: Intel i5 7200U 2.50 GHz
  - Memória RAM: 8GB DDR4 3000Mhz
  - Placa de vídeo: NVIDIA GeForce 940MX
  - Sistema Operacional: Mint Uma 20.2
  - Adaptador Ethernet: Realtek PCIe
- RaspberryPI Zero W (192.168.0.38)
  - Processador: ARM v6 1.00 GHz
  - Memória RAM: Memória 512MB
  - Sistema Operacional: Raspberry Pi OS
- Smartphone Motorola X4 (192.168.0.220)
  - Sistema Operacional: Android 9
- TV Samsung Smart
- Modem (192.168.0.1)

- Modelo: TP-Link WR740N
- Frequência: 2.4 GHz

4 Monitoramento

O PRTG diferencia os dispositivos entre Sonda e Rede, sendo que o primeiro diz respeito a dispositivos que possuem o PRTG definido como agente centralizador, enquanto o segundo são os dispositivos conectados na rede e visualizados por meio de protocolos de rede apenas. Durante esse trabalho foi utilizado apenas uma Sonda 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 Unix.

4.1 Funcionamento da Sonda

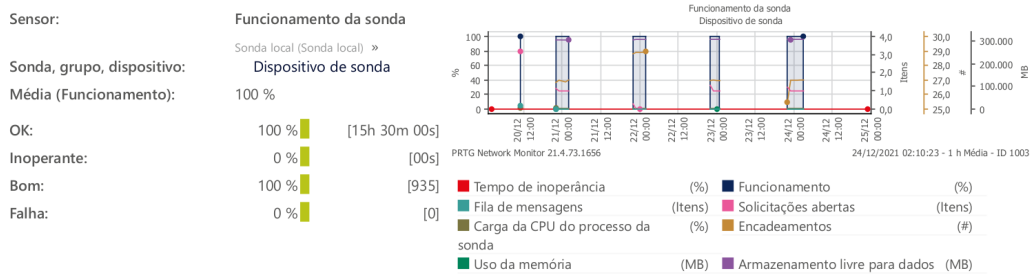


Figura 2: Gráfico do sensor Probe Health gerado pelo PRTG.

O sensor de saúde da sonda demonstra com detalhes métricas de funcionamento da sonda em relação ao PRTG, como *downtime*, uso de memória, número de *threads* e *CPU load*.

4.2 Funcionamento do Sistema

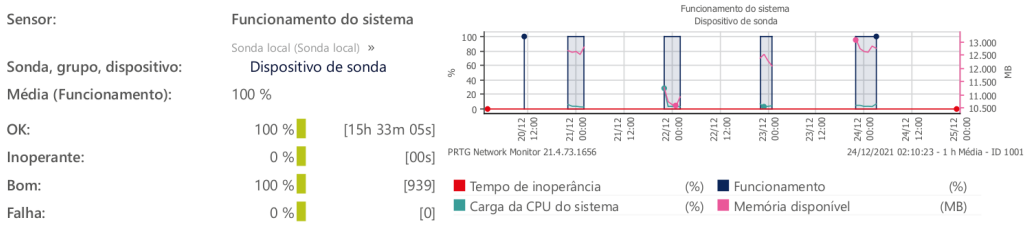


Figura 3: Gráfico do sensor System Health gerado pelo PRTG.

O sensor de saúde do sistema monitora o *hardware* do sistema hospedeiro, a fim de verificar picos de uso do sistema e as causas deles.

4.3 Funcionamento de Software como serviço

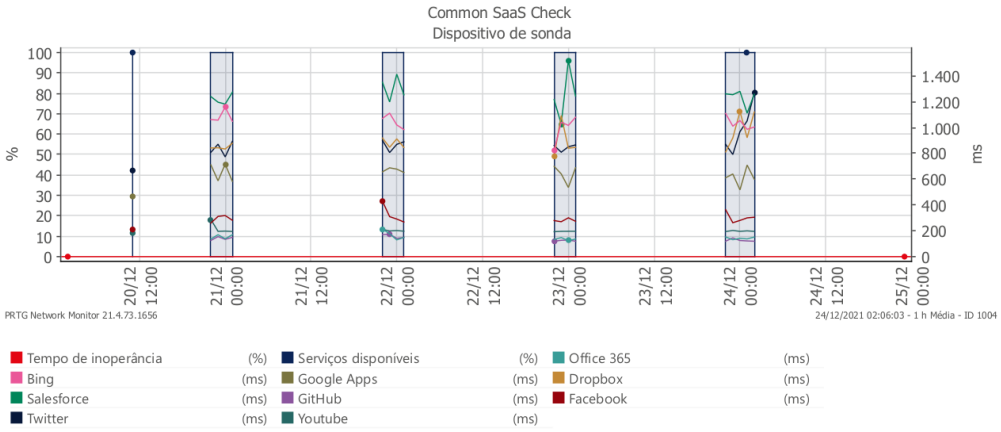


Figura 4: Gráfico do sensor de funcionamento de Software como serviço gerado pelo PRTG.

A sonda Common SaaS Check verifica se os provedores estão disponíveis, são eles os principais: Bing, Twitter, Github, Youtube, Office 365, Dropbox e Facebook. 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 1000ms, mas podemos destacar um pico e média mais elevada no serviço da Salesforce.

4.4 Ping

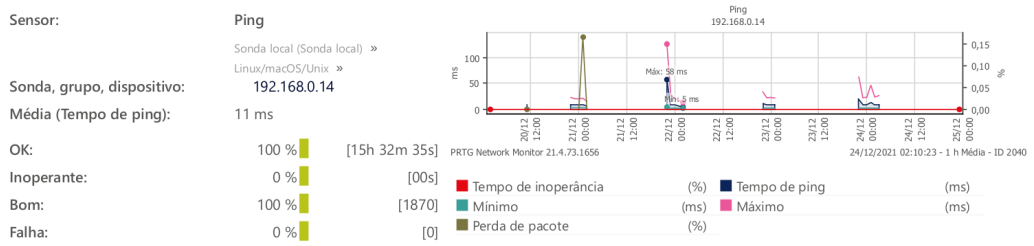


Figura 5: Gráfico do sensor Ping gerado pelo PRTG.

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 Desktop citado na sessão de topologia de rede.

4.5 Http

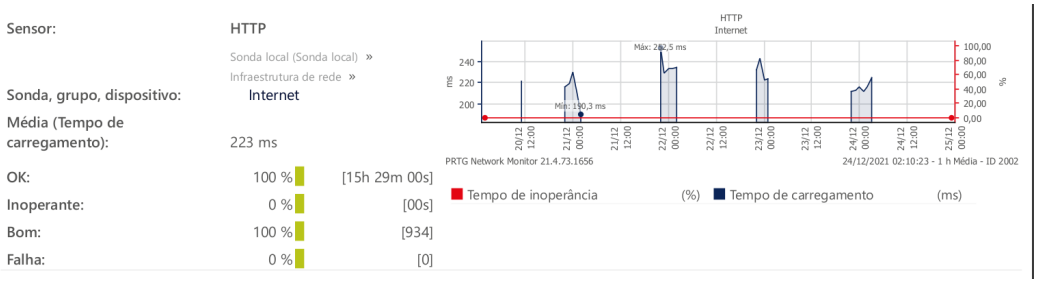


Figura 6: Gráfico do sensor Http gerado pelo PRTG.

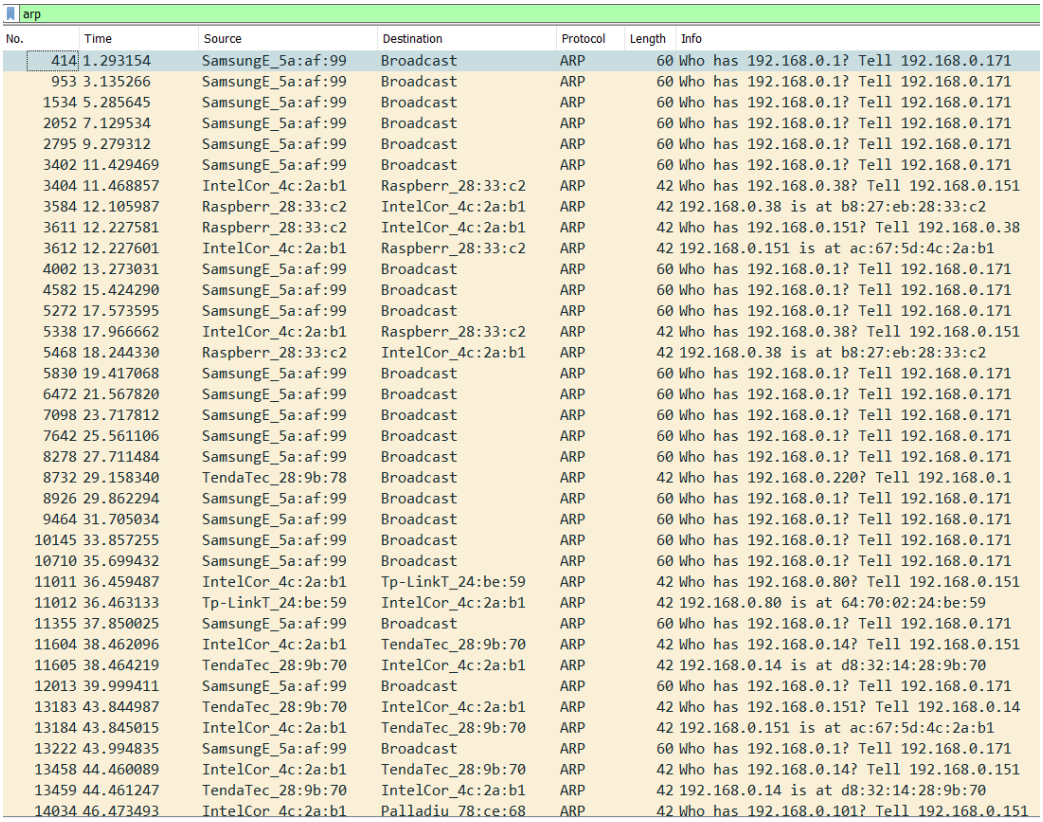
O HTTP monitora o tempo de carregamento de uma página na internet. Nota-se que houve um pico anormal de 252.5 ms e um mínimo de 190.3 ms. Site utilizado no momento: www.google.com.

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 10 minutos contínuos no Wireshark, com o filtro *arp* ligado (dessa forma o software ignora todos os outros protocolos e comunicações). É possível perceber que o dispositivo Desktop envia pela rede um pedido de identificação do dispositivo RaspberryPI Zero W. 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
414	1.293154	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
953	3.135266	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
1534	5.285645	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
2052	7.129534	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
2795	9.279312	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
3402	11.429469	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
3404	11.468857	IntelCor_4c:2a:b1	Raspberr_28:33:c2	ARP	42	Who has 192.168.0.38? Tell 192.168.0.151
3584	12.105987	Raspberr_28:33:c2	IntelCor_4c:2a:b1	ARP	42	192.168.0.38 is at b8:27:eb:28:33:c2
3611	12.227581	Raspberr_28:33:c2	IntelCor_4c:2a:b1	ARP	42	Who has 192.168.0.151? Tell 192.168.0.38
3612	12.227601	IntelCor_4c:2a:b1	Raspberr_28:33:c2	ARP	42	192.168.0.151 is at ac:67:5d:4c:2a:b1
4002	13.273031	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
4582	15.424290	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
5272	17.573595	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
5338	17.966662	IntelCor_4c:2a:b1	Raspberr_28:33:c2	ARP	42	Who has 192.168.0.38? Tell 192.168.0.151
5468	18.244330	Raspberr_28:33:c2	IntelCor_4c:2a:b1	ARP	42	192.168.0.38 is at b8:27:eb:28:33:c2
5830	19.417068	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
6472	21.567820	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
7098	23.717812	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
7642	25.561106	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
8278	27.711484	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
8732	29.158340	TendaTec_28:9b:78	Broadcast	ARP	42	Who has 192.168.0.220? Tell 192.168.0.1
8926	29.862294	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
9464	31.705034	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
10145	33.857255	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
10710	35.699432	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
11011	36.459487	IntelCor_4c:2a:b1	Tp-LinkT_24:be:59	ARP	42	Who has 192.168.0.80? Tell 192.168.0.151
11012	36.463133	Tp-LinkT_24:be:59	IntelCor_4c:2a:b1	ARP	42	192.168.0.80 is at 64:70:02:24:be:59
11355	37.850025	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
11604	38.462096	IntelCor_4c:2a:b1	TendaTec_28:9b:70	ARP	42	Who has 192.168.0.14? Tell 192.168.0.151
11605	38.464219	TendaTec_28:9b:70	IntelCor_4c:2a:b1	ARP	42	192.168.0.14 is at d8:32:14:28:9b:70
12013	39.999411	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
13183	43.844987	TendaTec_28:9b:70	IntelCor_4c:2a:b1	ARP	42	Who has 192.168.0.151? Tell 192.168.0.14
13184	43.845015	IntelCor_4c:2a:b1	TendaTec_28:9b:70	ARP	42	192.168.0.151 is at ac:67:5d:4c:2a:b1
13222	43.994835	SamsungE_5a:af:99	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.171
13458	44.460089	IntelCor_4c:2a:b1	TendaTec_28:9b:70	ARP	42	Who has 192.168.0.14? Tell 192.168.0.151
13459	44.461247	TendaTec_28:9b:70	IntelCor_4c:2a:b1	ARP	42	192.168.0.14 is at d8:32:14:28:9b:70
14034	46.473493	IntelCor_4c:2a:b1	Palladiu_78:ce:68	ARP	42	Who has 192.168.0.101? Tell 192.168.0.151

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 duas horas com objetivo de capturar mensagens relativas ao SNMP. As transmissões interceptadas foram realizadas pelo dispositivo de IP 192.168.0.80 (Desktop), 192.168.0.151 (Notebook Lenovo Thinkpad) com o destino sendo a subrede 255.255.255.255. Outra transmissão em específico é a do dispositivo 192.168.0.101 (Notebook Acer AspireF5) que possui como destino (192.168.0.1) que é o mo-

dem roteador. Entretanto percebe-se o protocolo ICMP, que acontece quando o adaptador *wireless* conectado ao notebook é removido propositalmente.

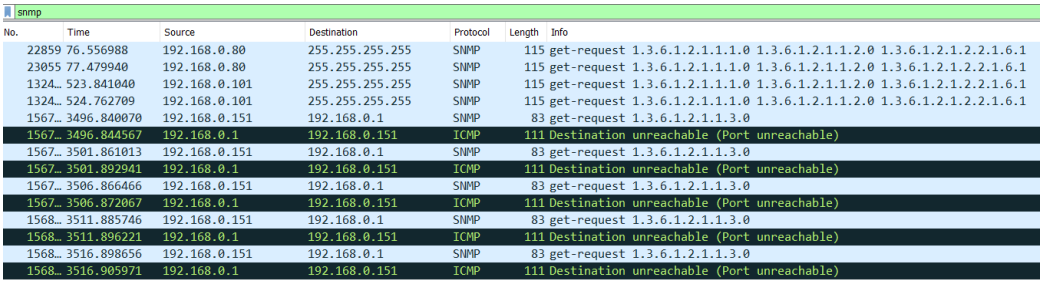


Figura 8: Tabela de ocorrências do protocolo SNMP monitoradas pelo Wireshark.

6 Conclusão

Para realizar com sucesso os procedimentos foi necessário pesquisar e entender o funcionamento de ferramentas utilizadas na gerência de redes. Utilizando essas ferramentas e determinadas funcionalidades, foi possível denotar o funcionamento de uma rede doméstica e seus detalhes específicos, podendo utilizar esses conhecimentos para otimizar a rede e os processos envolvidos. Portanto, fica evidente a importância desse trabalho na agregação de conhecimento, visto que existem inúmeros aplicações perante a sociedade hodierna.

Referências

[1] Paessler. Prtg network monitor v21. `https://www.br.paessler.com/prtg`, 2021. [Online; acessado em 19 de dezembro].

[2] Wireshark. Wireshark docs. `https://www.wireshark.org/docs`, 2021. [Online; acessado em 20 de dezembro].