MONITORAMENTO DE REDES

Fabíola Maria Kretzer – 16100725

INE5414 - Redes de Computadores I

Universidade Federal de Santa Catarina – UFSC

Florianópolis, 13 de setembro de 2017

RESUMO

A proposta deste trabalho é analisar dados de uma rede, utilizando uma ferramenta de gerência de redes chamada Simple Network Management Protocol (SNMP). Para isto foi utilizada PRTG durante 5 dias em intervalos de 2 a 4 horas por dia e os gráficos e as sondas são apresentados no relatório. Também foi usado wireshark para capturar pacotes e verificar a ocorrência do protocolo ARP (Address Resolution Protocol).

SUMÁRIO

1. Introdução

A utilização de uma SNMP (Simple Network Managent Protocol) permite analisar diversas informações que estão presentes na rede. A motivação para o desenvolvimento deste trabalho é o crescimento do número de aparelhos que acessam as redes, surgindo a necessidade de gerenciar e monitorar estas redes. Este trabalho tem como objetivo demostrar uma forma de gerenciamento de rede, e os dados coletados durante a monitoração realizada na rede local do autor. Também foi utilizado a ferramenta wireshark para verificar a ocorrência do protocolo ARP (Address Resolution Protocol).

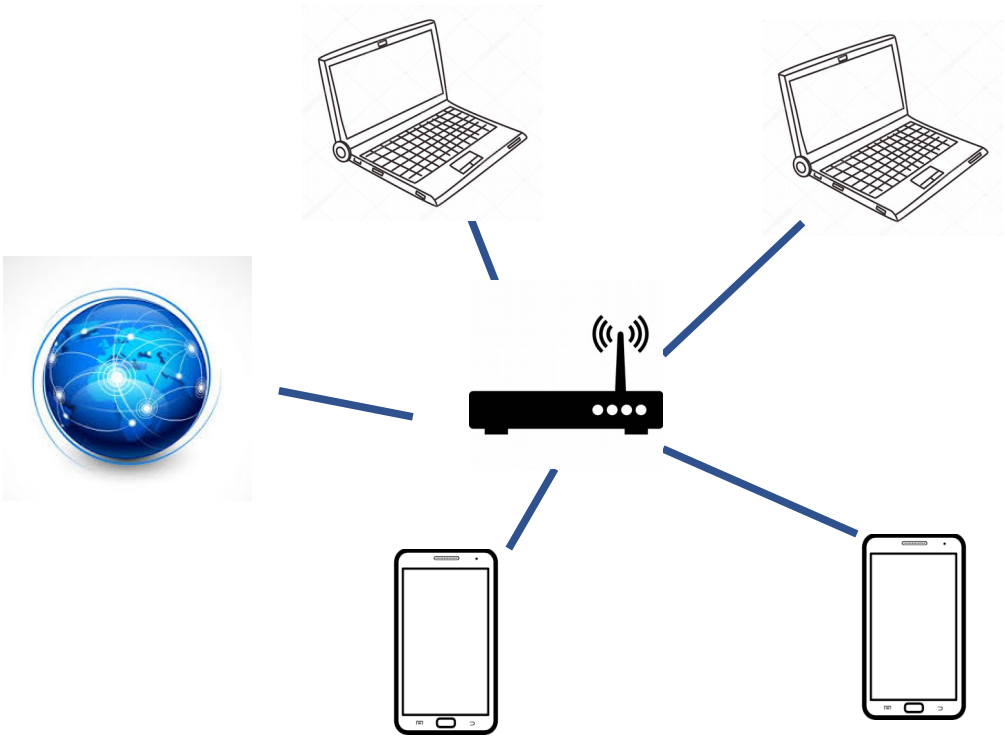
2. Ferramenta de Gerência de Redes

A ferramenta de gerência de redes SMNP escolhida foi o PRTG Network Monitor da empresa de monitoramento de redes Paesser, os motivos foram a interface ser prática, eficiente e fácil de aprender a utilizar, além da geração automática dos gráficos.

A ferramenta reconhece os dispositivos da rede e dados do sistema, auxiliando no mapeamento, e possibilitando o uso de diferentes tipos de sondas tanto de rede quanto de informações do sistema. Basta o usuário escolher as sondas que quer utilizar e o PRTG gera os gráficos das informações requeridas por um londo tempo. Possui interface web, e utiliza um endereço local.

3. Topologia de Redes

A rede utilizada é composta por um modem e roteador TP-Link modelo TL-WR740N, e outros componentes que recebem o sinal Wi-Fi, que são um notebook Samsung RV415, um notebook Acer Aspire E1-531-2633 (utilizado na monitoração) e dois smartphones Samsung Galaxy, um modelo S6812B e outro SM-G110B.



4. Descrição dos Componentes

4.1 Modem e Roteador TP-Link modelo TL-WR740N

- Velocidade de transmissão: 150Mbps
- Frequência: 2,4GHz

4.2 Notebook Acer Aspire E1-531-2633 (Utilizado na monitoração)

- Processador: Intel Celeron CPU B830
- Memória: 4 GB
- Disco: 500 GB
- Sistema Operacional: Windows 8

4.3 Notebook Samsung RV415

- Processador: AMD Dual Core Processor E-300
- Memória: 2 GB
- Disco: 500 GB
- Sistema Operacional: Ubuntu 16.10
- Conexão Ethernet: 100M LAN
- Conexão Wireless: 802.11bgn

4.4 Smartphone Samsung Galaxy S6812B

- Processador: 1 GHz Single-Core ARM Cortex-A9

4.5 Smartphone Samsung Galaxy SM-G110B

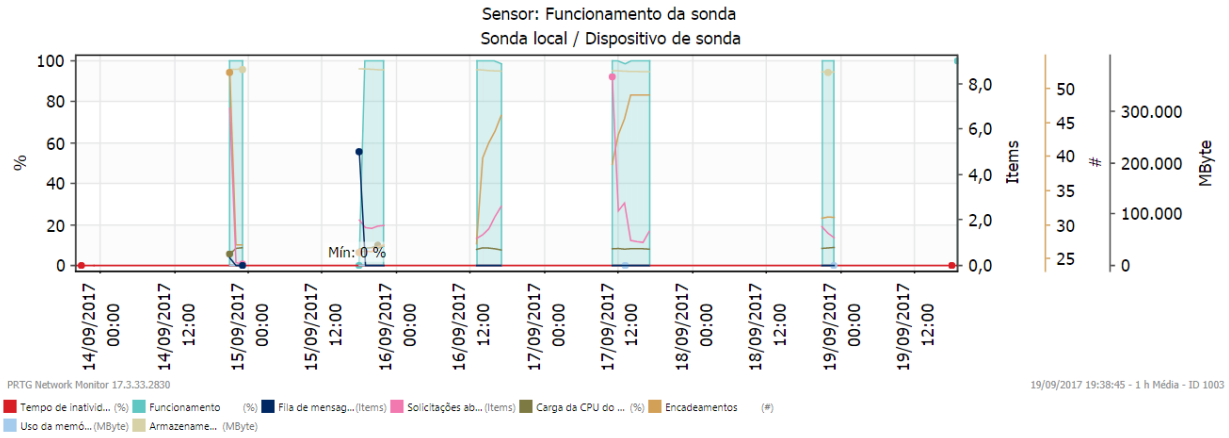
- Processador: 1 GHz Single-Core ARM Cortex-A7

5. Medidas Realizadas

Os sensores analisados são descritos a seguir, com monitoramento de 5 dias, da data 14/09/2017 até 18/09/2017. Em todos os gráficos o eixo das abscissas representam o tempo em horas.

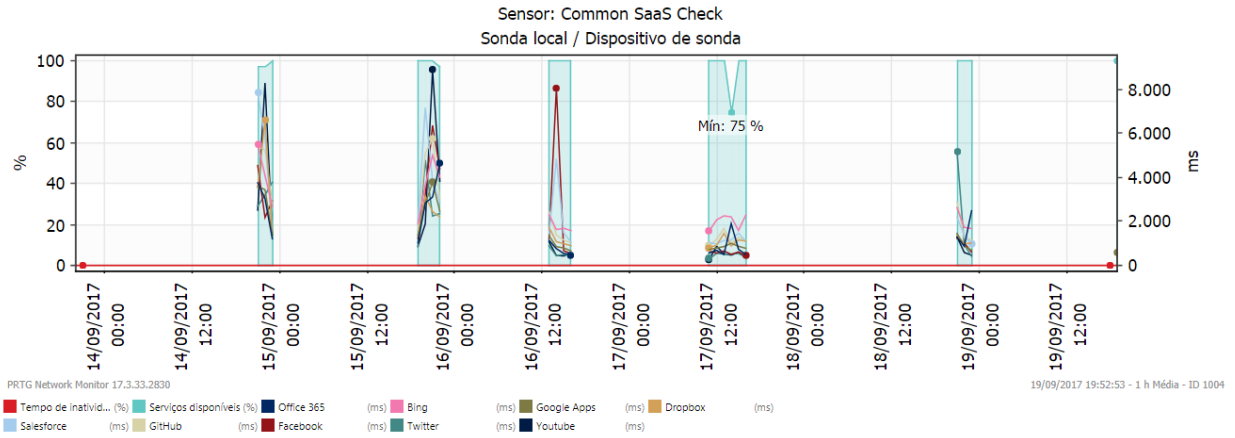
5.1 Funcionamento da sonda

Monitora o status da sonda, verificando parâmetros do sistema PRTG que podem afetar a qualidade do monitoramento da ferramenta. Os parâmetros monitorados são citados na legenda do gráfico.



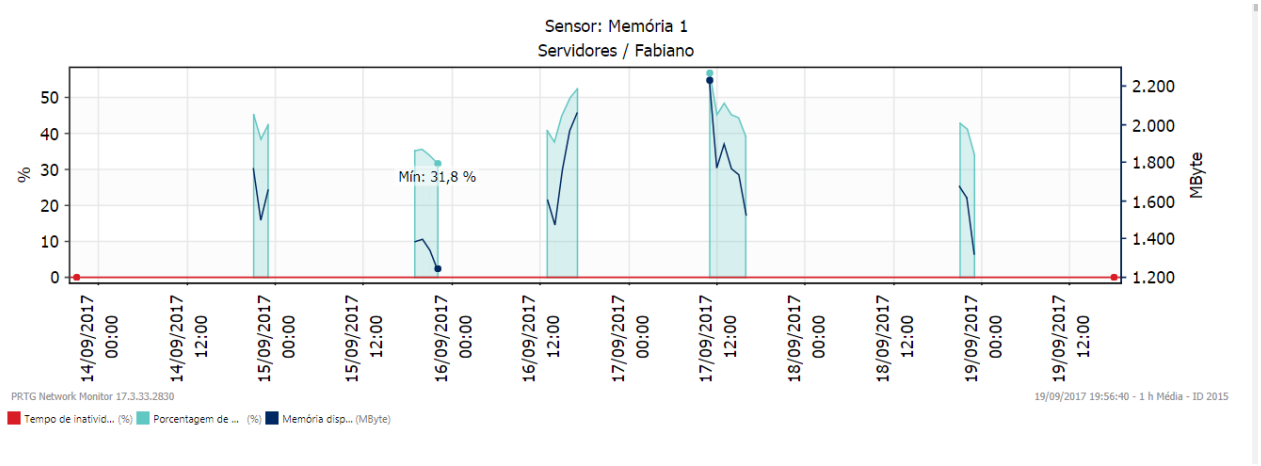
5.2 Common Saas Check

Monitora a disponibilidade dos provedores Saas (Software as a Service), mostrando a disponibilidade por porcentagem e tempo de resposta de aplicativos como Youtube, Facebook, Bing, entre outros.



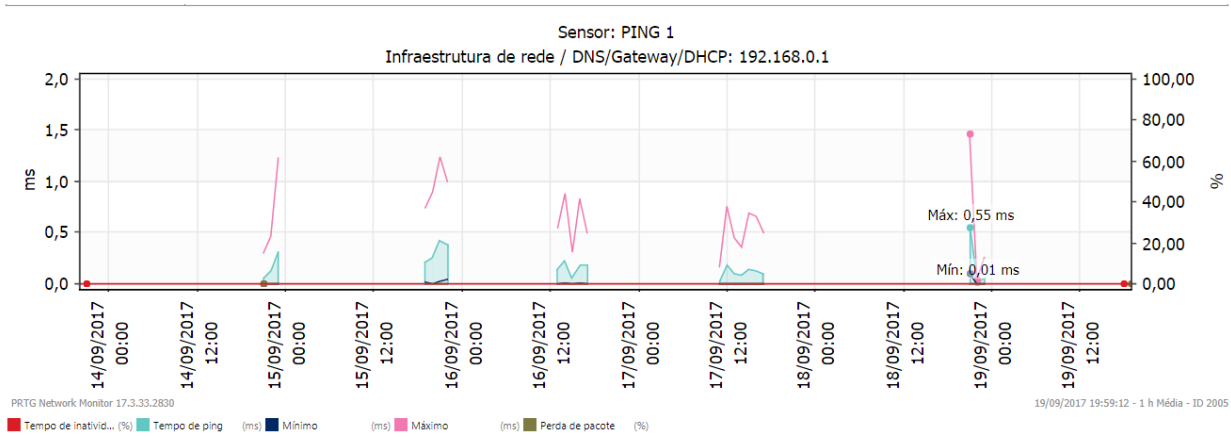
5.3 Memória

Monitora a porcentagem de memória RAM disponível no computador onde a ferramenta está funcionando, mostrando a quantidade de memória disponível em MByte, bem como por porcentagem.



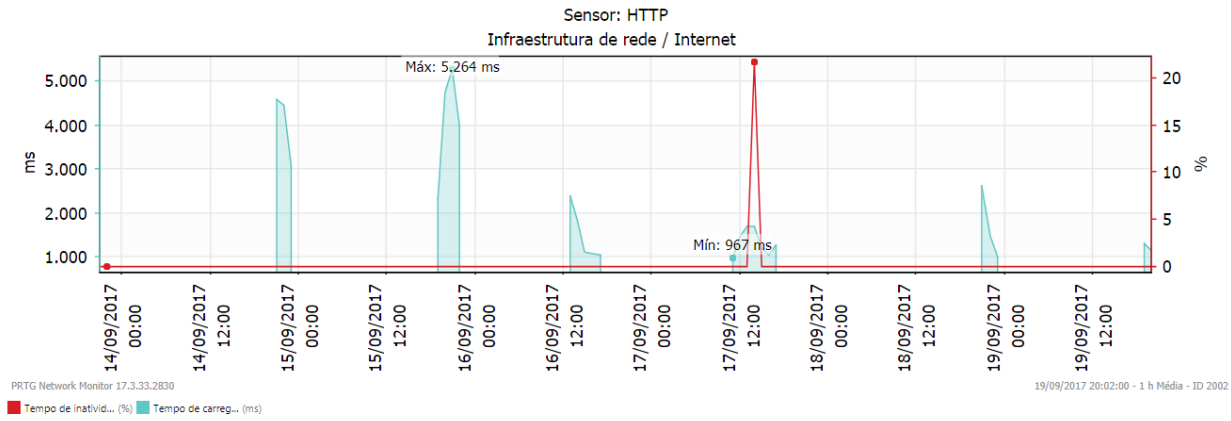
5.4 Ping

Monitora o ping entre o computador executando a sonda e uma página qualquer da internet mostrando ping máximo e mínimo no tempo decorrido.



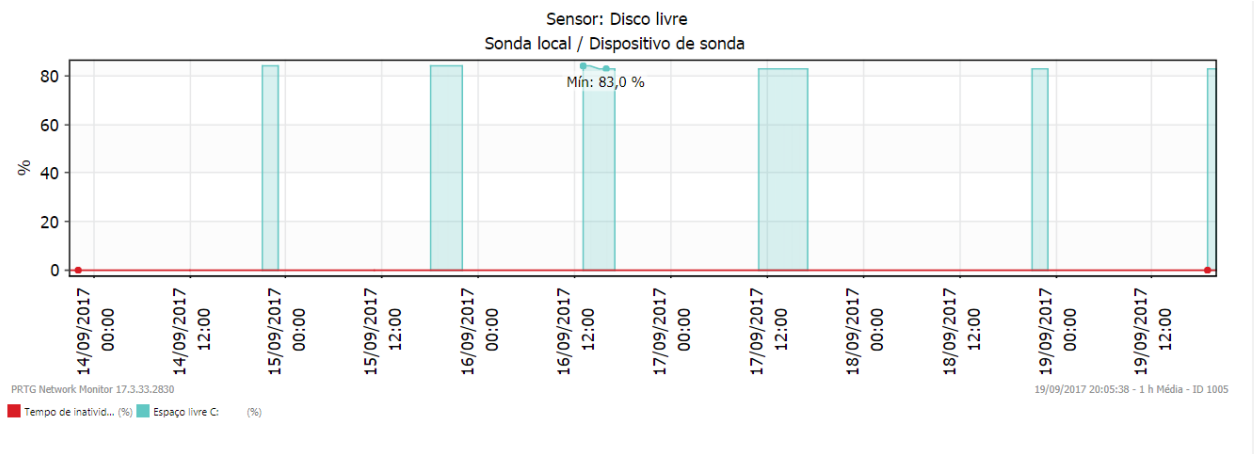
5.5 HTTP

Monitora o servidor web usando HTTP, mostrando o tempo de carregamento de uma página web.



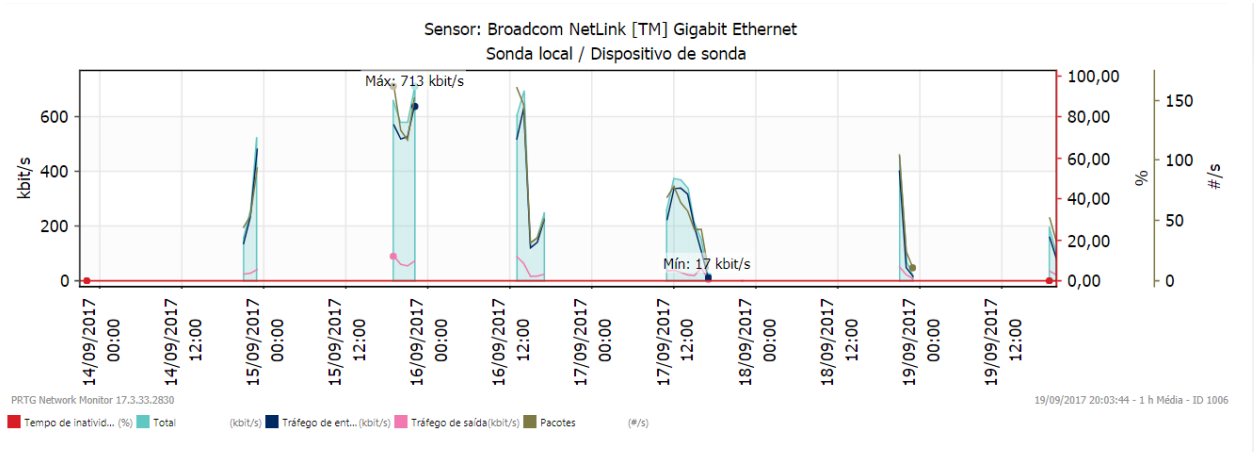
5.6 Disco livre

Monitora o espaço de disco livre de uma ou mais unidades de armazenamento, mostrando em porcentagem o espaço total de um sistema.



5.7 Broadcom NetLink [TM] Gigabit Ethernet

Representa a quantidade de pacotes recebidos e enviados. É possível perceber uma variação do envio e recebimento, provavelmente reflexo de momentos em que algum elemento da rede estava sendo utilizado por um usuário ou apenas ligado executando funções básicas.



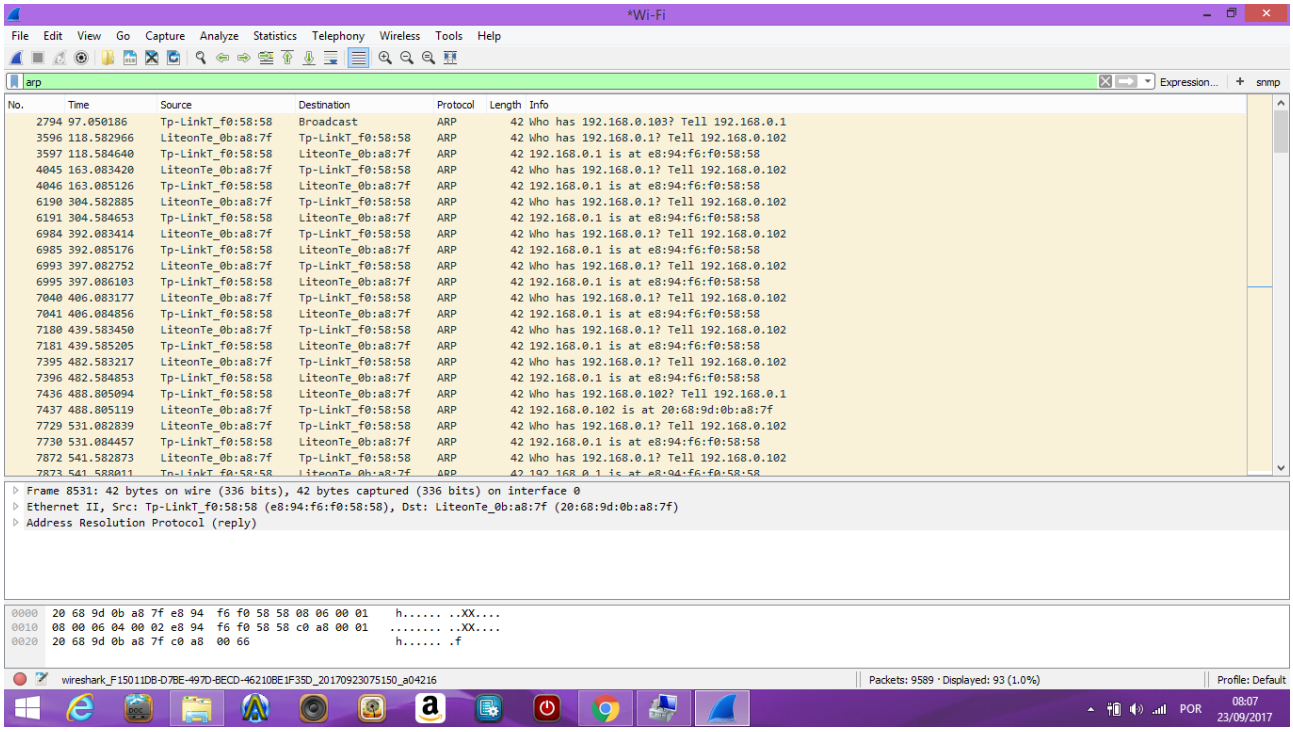
6. Uso do Wireshark

O Wireshark é um programa que analisa o tráfego de rede e o organiza por protocolos. É possível controlar o tráfego de uma rede e saber tudo que entra e sai do computador ou da rede na qual o computador está ligado.

Abaixo se tem a captura de tela do wireshark. Nessa tela se pode observar a ocorrência do protocolo ARP (Protocolo de Resolução de Endereços), que está presente na camada de enlace. É protocolo de telecomunicações usado para resolução de endereços da camada de Internet em

endereços da camada de enlace, uma função crítica em redes de múltiplos acessos. Neste monitoramento feito por um notebook Acer podemos observar uma ocorrência de ARP Request por broadcast.

Nesta captura nota-se que o modem (Tp-LinkT_f0:58:58) envia um ARP Request para um broadcast requisitando para o dispositivo que possui o IP 192.168.0.103 responda o dispositivo de IP 192.168.0.1. O dispositivo LiteonTe_0b:a8:7f conectado na rede envia um ARP Reply para o modem informando possuir o IP 192.168.103.

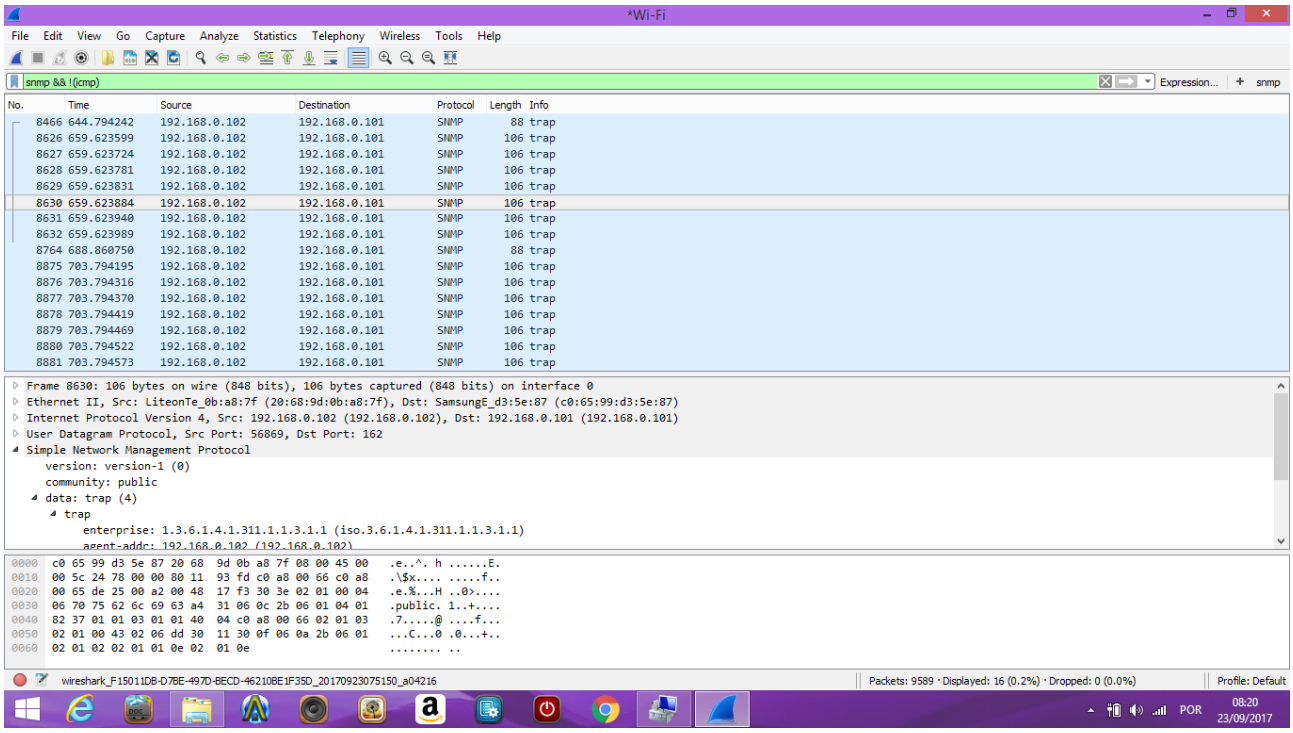


SNMP, em português Protocolo Simples de Gerência de Rede, é um protocolo padrão da Internet para gerenciamento de dispositivos em redes IP. Este protocolo está presente na camada de aplicação.

Abaixo está a captura de tela para o protocolo SNMP. O monitoramento da primeira imagem foi feito através de apenas um notebook Acer, não consegui fazer a ocorrência desse protocolo de gerência de redes em mais dispositivos. Assim o monitoramento feito pela autora deste trabalho gerou apenas TRAP, que são alertas gerados pelo agente, e não conseguindo fazer nenhuma consulta (GET) e nenhuma modificação(SET). Logo, para fins didáticos, entender e melhor explicar a ocorrência de GET, SET e do protocolo SNMP pedi para o colega João Vicente Souto também aluno desta disciplina que me enviasse a imagem gerada pelo seu monitoramento do protocolo SNMP em sua rede local. Assim a segunda imagem abaixo é do trabalho deste colega e o arquivo de dados está no seu envio ao moodle.

Lembrando que é apenas para o entendimento do funcionamento do protocolo gerência de redes.

- Na linha 32490 mostra *get-next-request .1.3.6.1.2.1.1.1.0* sendo enviado do dispositivo se IP 192.168.25.02 para o dispositivo de IP 192.168.25.06.
- Na linha seguinte podemos ver a resposta *get-response .1.3.6.1.2.1.1.2.0* sendo enviado do dispositivo de IP 192.168.25.06 para o dispositivo de IP 192.168.25.02.



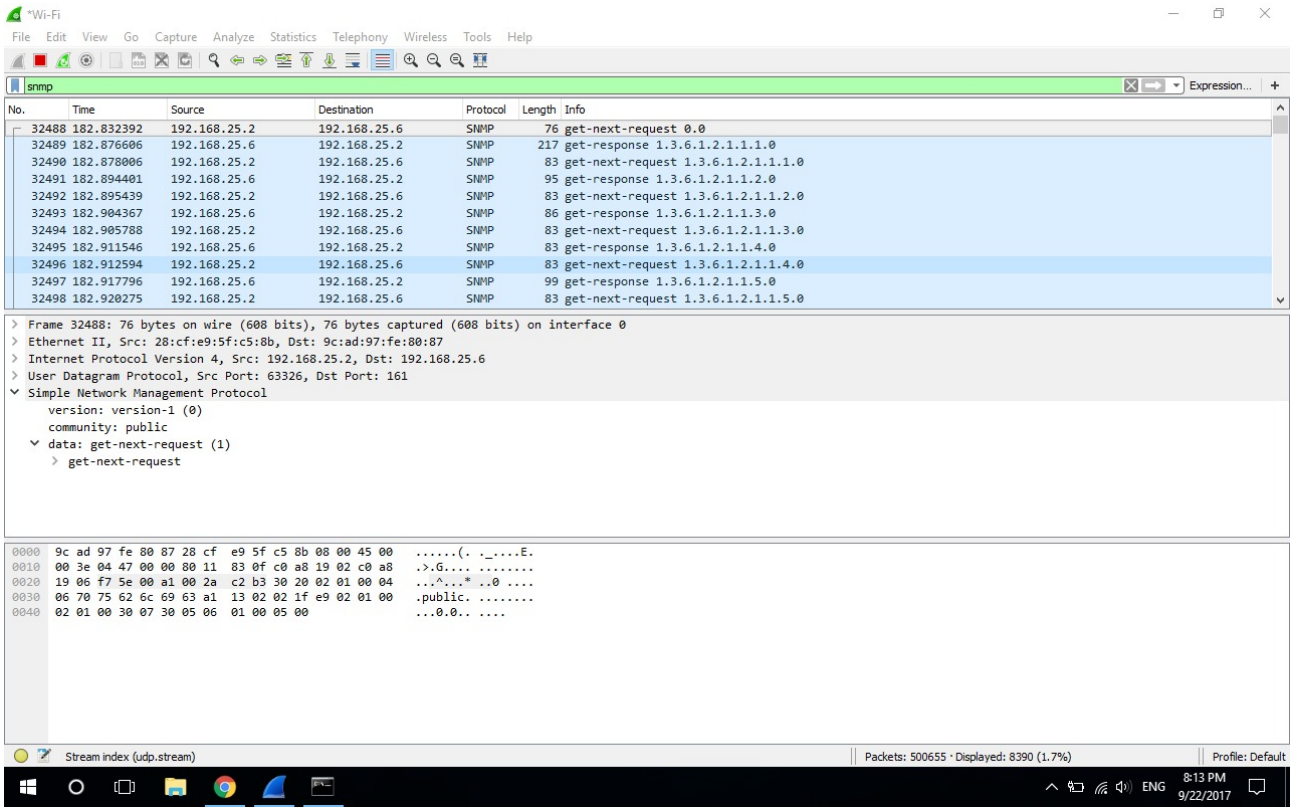


Imagem retirada do trabalho de João Vicente Souto.

7. Conclusões

O uso das ferramentas PRTG e Wireshark, bem como do protocolos SMNP e ARP, permitiu a experiência de monitorar uma rede e uma maior conhecimento da gerência de redes e desses protocolos utilizados. Assim este trabalho trouxe um esclarecimento prático da importância de uma rede para o mundo atual onde cada vez mais dispositivos estão conectados a ela, além de aprender a manusear ferramentas que fazem o controle da rede.

8. Referências

- PAESSLER. PRTG Network Monitor - software de monitoramento de rede. Disponível em: https://www.br.paessler.com/prtg. Acesso em: Setembro de 2017.
- Wireshark Documentation. Disponível em: https://www.wireshark.org/docs/. Acesso em: Setembro de 2017.
- SNMP. Disponível em: https://pt.wikipedia. org/wiki/Simple_Network _Management _Protocol. Acesso em: Setembro de 2017
- ARP. Disponível em: https://pt.wikipedia.org/wiki/Address_Resolution_Protocol. Acesso em: Setembro de 2017
- O que é SNMP. Disponível em: https://www.4linux.com.br/o-que-e-snmp. Acesso em: Setembro de 2017