MONITORAMENTO DE REDES

Matheus Henrique Schaly
Universiade Federal de Santa Catarina
Florianópolis – SC – Brasil

RESUMO

Análise de dados de uma rede, utilizando a ferramenta PRTG, capaz de gerenciar redes Simple Network Management Protocol. Também é utilizado Wireshark para a captura de pacotes e identificação de ocorrência do protocolo ARP e requests feitos pela plataforma de gerência de redes.

SUMÁRIO

1. Introdução

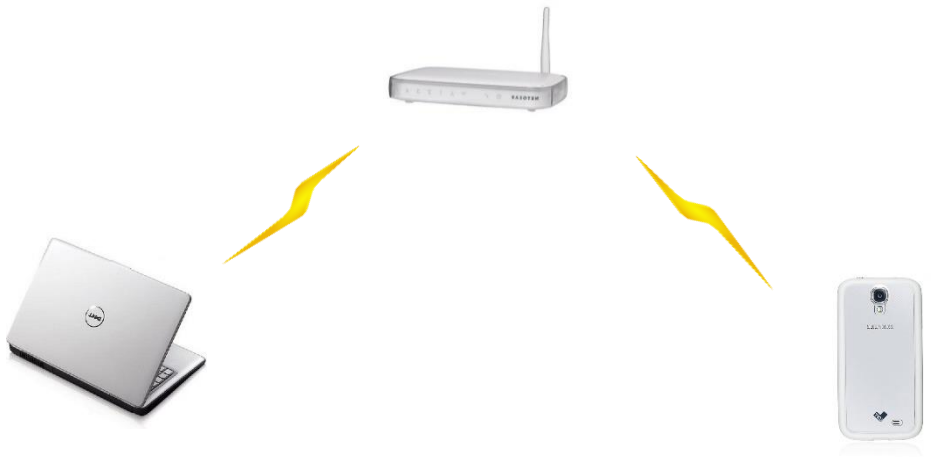
A utilização da Simple Network Management Protocol (SNMP) permite explorar diversas informações de uma rede, tais como o recebimento e envio de pacote, utilização da memória RAM, HTTP, utilização do Disco Rígido. Por outro lado, Wireshark permite analisar os pacotes de dados e comentar a ocorrência do protocolo ARP (Address Resolution Protocol) e SNMP. Os dados foram coletados entre o dia 22 e 26 de Setembro de 2018

2. Ferramenta de Gerência de Redes

A ferramenta escolhida foi a PRTG, por conta da sua facilidade de uso, facilidade em gerar gráficos e relatórios, além de possuir uma interface amigável.
O PRTG foi executado no sistema operacional Windows, sensores podem ser adicionados e configurados para analisar elementos que possam ser de interesse para a geração de informações relevantes. PRTG também é capaz de armazenar informações para que possam ser gerados gráficos para melhor visualização das atividades da rede.

3. Topologia da Rede

A rede utilizada é composta por um modem e roteador NETGEAR modelo N150 Wireless Router WNR1000 v3. Os componentes que recebem o sinal Wi-Fi são um notebook Dell e um celular Samsung Galaxy J3.



4. Descrição dos componentes

4.1 NETGEAR modelo N150 Wireless Router WNR1000 v3

SSID: NETGEAR34
Protocol: 802.11n
Security type: WPA2-Personal
Network band: 2.4 GHz
Network channel: 6
IPv4 address: 10.0.0.11
IPv4 DNS servers: 10.0.0.1
Manufacturer: Intel Corporation
Description: Intel(R) Dual Band Wireless-AC 7265
Driver version: 19.51.12.3
Physical address (MAC): 60-57-18-F2-56-5C

4.2 Notebook Dell

Proessador: Intel Core i7 – 5500U @ 2.40Ghz
RAM: 8 GB
Disco: 1 TB
Sistema Operacional: Windows 10
IP: 200.135.84.220

4.3 Smartphone Samsung Galaxy J5

Disco: 8 GB
RAM: 1.5 GB
Sistema operacional: Android 5.1.1
IP: 150.162.238.231

5. Medidas realizadas

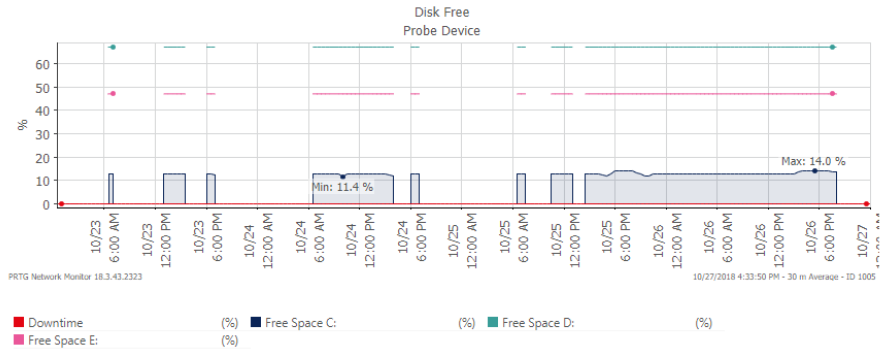
Os sensores analisados foram de disco rígido, HTTP, Ping e saúde do sistema, todo no Notebook Dell citado acima. A data de realização dos relatórios foi entre o dia 23/10/2018 e o dia 26/10/2018. Em todos os gráficos apresentados o eixo das abscissas representa o tempo em horas, e todos são apresentados em ordem cronológica.

5.1 Disco Rígido

Nesse monitoramento o eixo Y representa a porcentagem de disco livre nos discos C, D e E do computador. O espaço disponível permanece praticamente constante, visto que nenhum arquivo novo de tamanho considerável foi adicionado, notando-se apenas pequenas mudanças que fazem o espaço em disco do compartimento C variar de 11.4% a 14.0%. Não há alterações na porcentagem de espaço utilizado nas partições E e D.

Report: **Disk Free**

Report Time Span:	10/23/2018 12:00:00 AM - 10/27/2018 12:00:00 AM				
Report Hours:	24 / 7				
Sensor Type:	WMI Free Disk Space (Multi Disk) (60 s Interval)				
Probe, Group, Device:	Local Probe > Local Probe > Probe Device				
Uptime Stats:	Up:	100 %	[01d 20h 31m 49s]	Down:	0 % [00s]
Request Stats:	Good:	100 %	[2649]	Failed:	0 % [0]
Average (Free Space C:):	13 %				

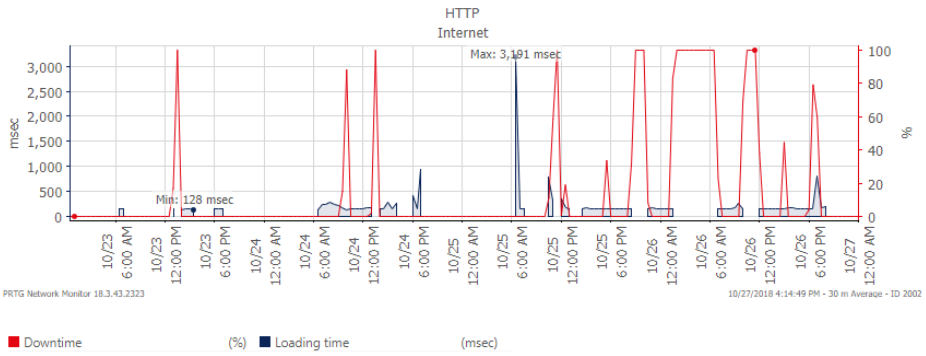


5.2 HTTP

O sensor HTTP monitora um servidor web usando Hyptertext Transfer Protocol (HTTP). Esta é a forma mais fácil de monitorar se um website (ou algum elemento específico de um website) é alcançável. A URL que o sensor está conectado é a www.google.com. A partir do relatório gerado abaixo observa-se picos de tempo de inatividade e de tempo de carregamento.

Report: **HTTP**

Report Time Span:	10/23/2018 12:00:00 AM - 10/27/2018 12:00:00 AM				
Report Hours:	24 / 7				
Sensor Type:	HTTP (60 s Interval)				
Probe, Group, Device:	Local Probe > Network Infrastructure > Internet				
Uptime Stats:	Up:	73 %	[01d 07h 56m 51s]	Down:	27 % [11h 58m 00s]
Request Stats:	Good:	71 %	[1891]	Failed:	29 % [775]
Average (Loading time):	181 msec				



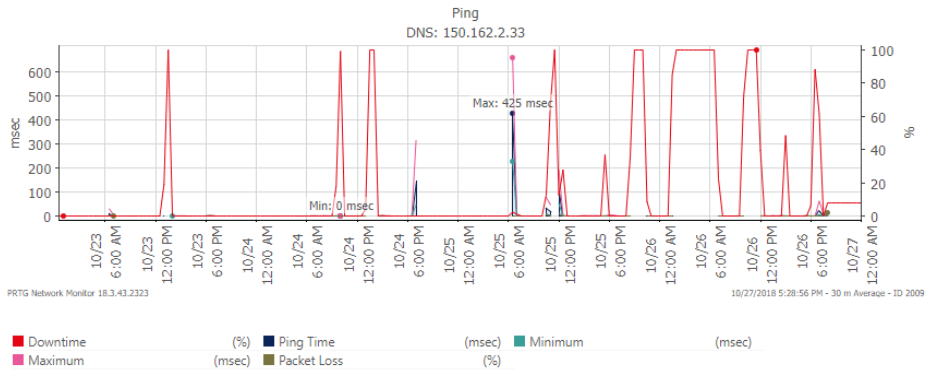
5.3 Ping

A latência pode ser usada para testar a conectividade entre equipamentos de uma rede. O sensor de ping envia um pedido Internet Controle Message Protocal (ICMP) do computador gerador do report (Notebook Dell) para o dispositivo em que é criado para monitorar a disponibilidade de um dispositivo. Demonstrando o tempo de ping, minimum ping quando usado mais de um ping por intervalo, maximum

ping também quando é usado mais de um ping por intervalo e, por fim, packet loss representa os pacotes perdidos quando é usado mais de um ping por intervalo.

Report: **Ping**

Report Time Span:	10/23/2018 12:00:00 AM - 10/27/2018 12:00:00 AM					
Report Hours:	24 / 7					
Sensor Type:	Ping (30 s Interval)					
Probe, Group, Device:	Local Probe > Network Infrastructure > DNS: 150.162.2.33					
Uptime Stats:	Up:	72 %	[01d 07h 20m 52s]	Down:	28 %	[12h 12m 01s]
Request Stats:	Good:	71 %	[3756]	Failed:	29 %	[1521]
Average (Ping Time):	1 msec					

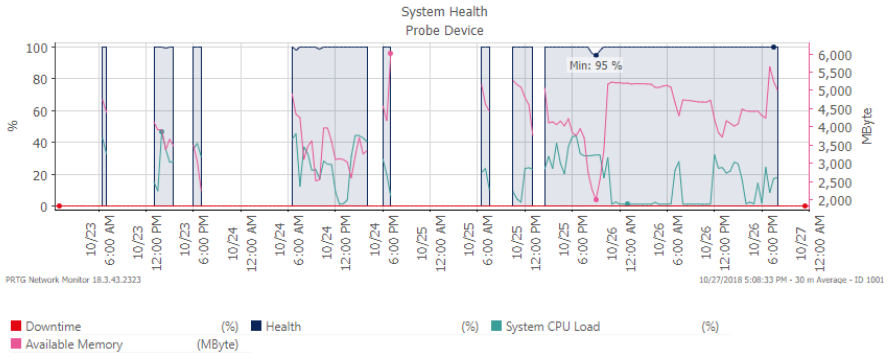


5.4 Saúde do Sistema

O sensor de saúde do sistema monitora parâmetros internos do PRTG, mostrando o estado atual do sistema. A linha azul escuta Health é um índice que soma o estado do Notebook Dell, variando entre 100% (saúdavel) e 0%. Valores frequentes ou repetido abaixo de 100% devem ser investigados. A linha rosa Available Memory mostra a quantidade de memória livre disponível no sistema. Esse valor não deve cair abaixo de 500 MB. A linha azul clara representa o carregamento da CPU. Esse valor deve permanecer abaixo de 50%. Nota-se que tanto a memória mantém-se acima de 500 MB e o carregamento da CPU abaixo de 50%.

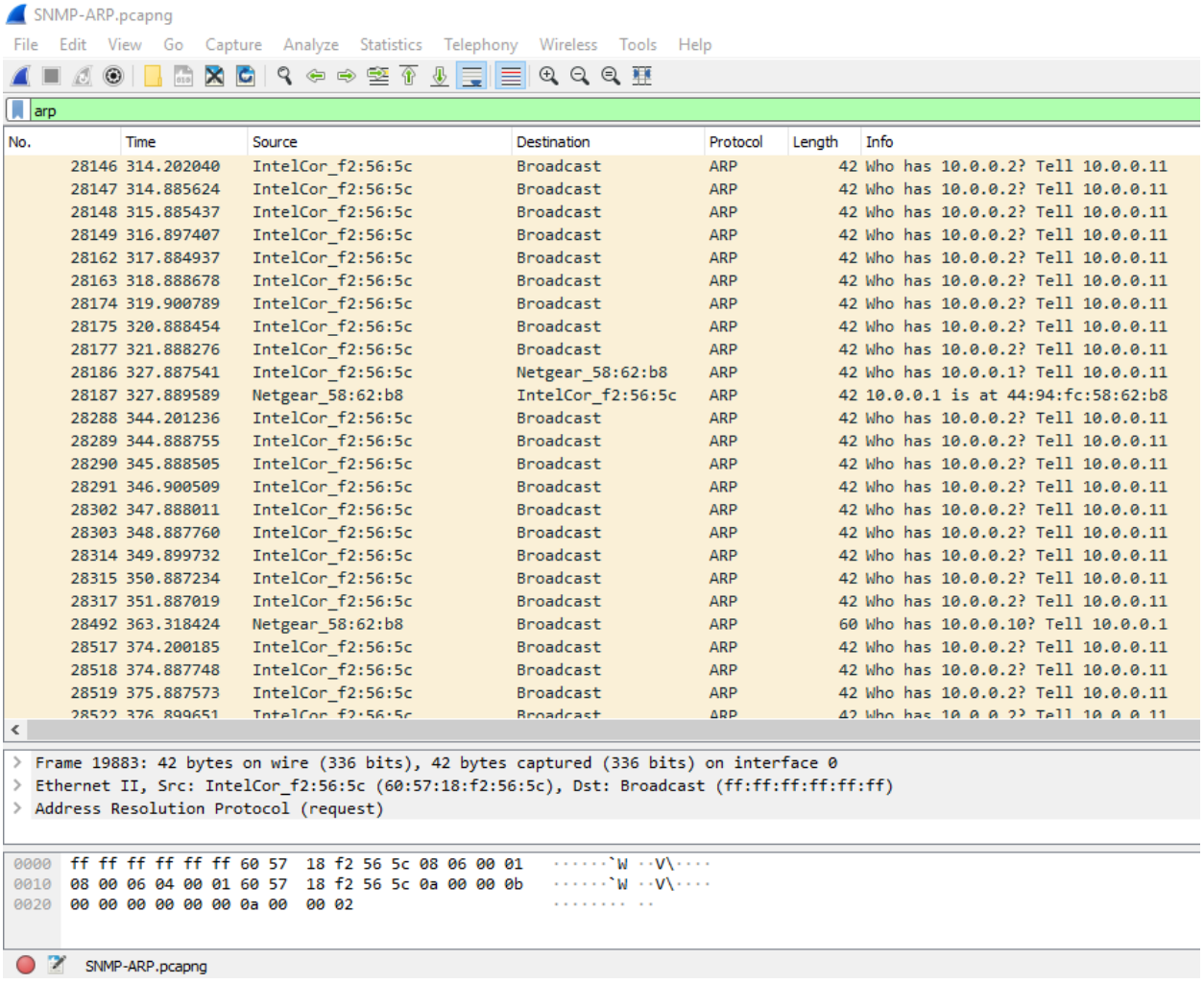
Report: **System Health**

Report Time Span:	10/23/2018 12:00:00 AM - 10/27/2018 12:00:00 AM					
Report Hours:	24 / 7					
Sensor Type:	System Health (60 s Interval)					
Probe, Group, Device:	Local Probe > Local Probe > Probe Device					
Uptime Stats:	Up:	100 %	[01d 19h 32m 27s]	Down:	0 %	[00s]
Request Stats:	Good:	100 %	[2646]	Failed:	0 %	[0]
Average (Health):	>99 %					

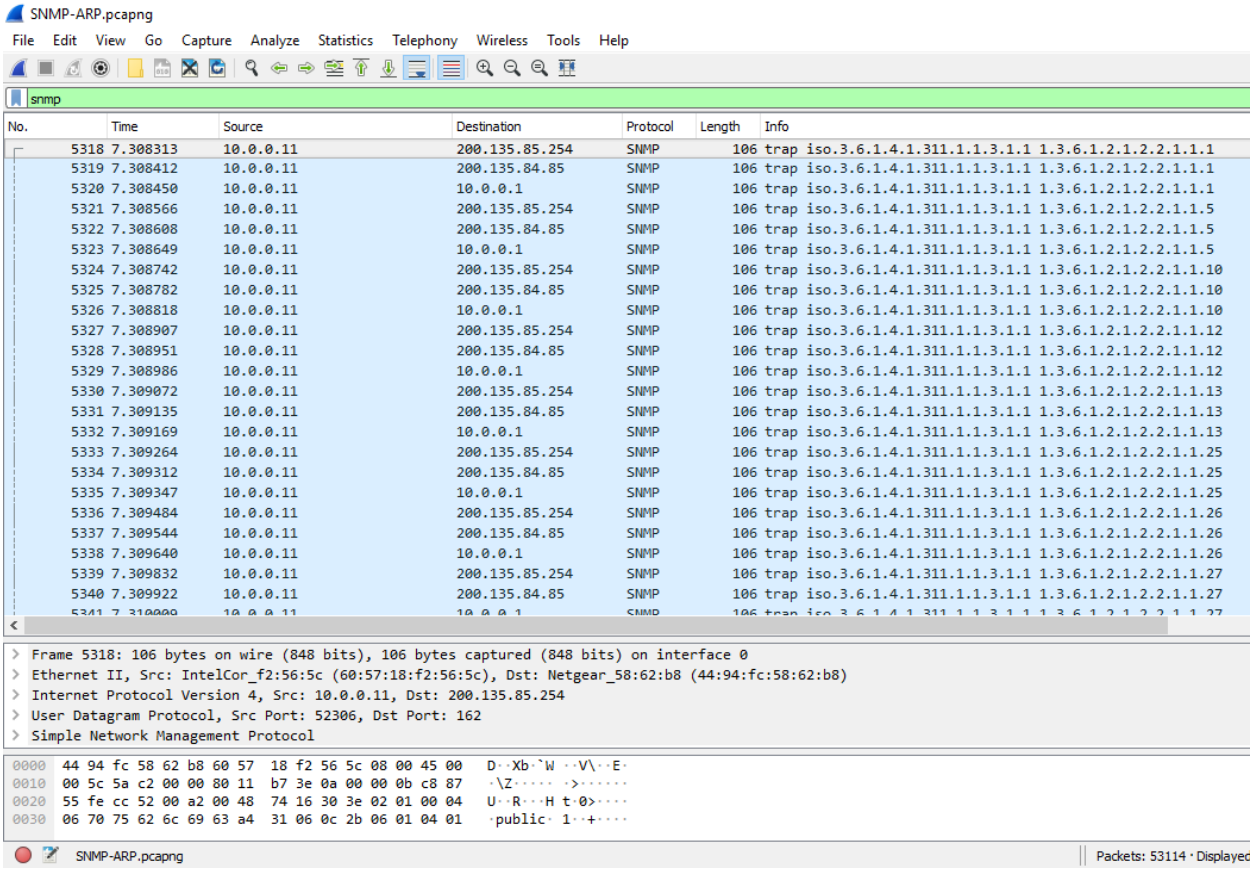


6. Wireshark

A imagem abaixo mostra a utilização da ferramenta Wireshark para o monitoramento da ocorrência do protocolo ARP. Nota-se, dentre outros acontecimentos, que o modem Intelcor_f2:56:5c expediu um Request para o Netgear_58:62:b8 solicitando o dono do ip 10.0.0.1, simultaneamente com o próprio ip para o intuito de retorno. Em seguida, o computador Netgear_c5:02:5f manda uma mensagem para o modem, identificando-se como portador do ip e retorna o seu endereço MAC, 44:94:fc:58:62:b8.



A imagem seguinte demonstra a ocorrência da operação da gerência de redes, nota-se os traps SNMP realizados com a utilização do protocolo SNMP, utilizando a porta udp 162.



7. Conclusão

A partir das análises demonstradas, nota-se as possíveis encargo de uma SNMP ao monitorar uma rede, possíveis sensores que podem ser implementados e diferentes formas de explorar os dados recebidos. Além disso, compreende-se como operar a ferramenta Wireshark para explorar os protocolos utilizados pela rede, como, por exemplo, o SNMP utilizado pelo PRTG e o andamento do protocolo ARP, que processa a identificação entre os dispositivos que estão presentes na rede.