

## **MONITORAMENTO DE REDES**

Matheus Henrique Schaly  
Universidade 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 .....	2
2. Ferramenta de Gerência de Redes .....	2
3. Topologia da Rede .....	2
4. Descrição dos componentes .....	3
4.1 NETGEAR modelo N150 Wireless Router WNR1000 v3 .....	3
4.2 Notebook Dell .....	3
4.3 Smartphone Samsung Galaxy J5 .....	3
5. Medidas realizadas .....	3
5.1 Disco Rígido.....	3
5.2 HTTP.....	4
5.4 Saúde do Sistema .....	5
6. Wireshark.....	6
7. Conclusão.....	7

## 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

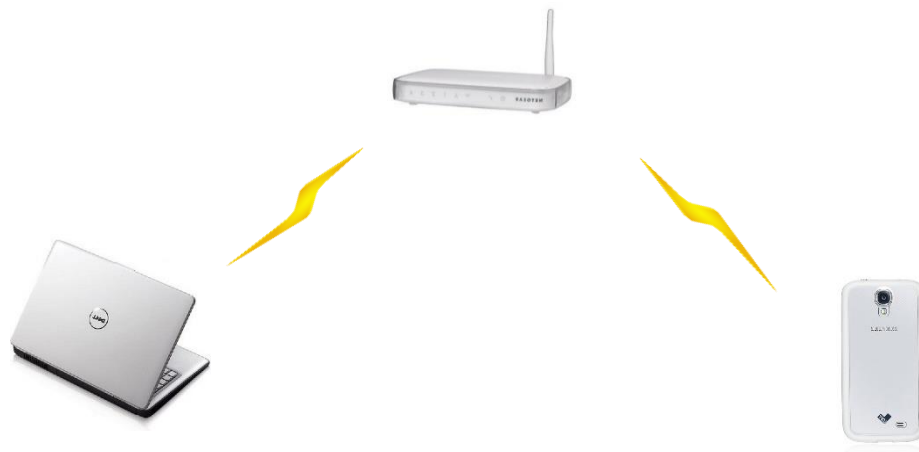
## 2. Ferramenta de Gerência de Redes

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

Processador: 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

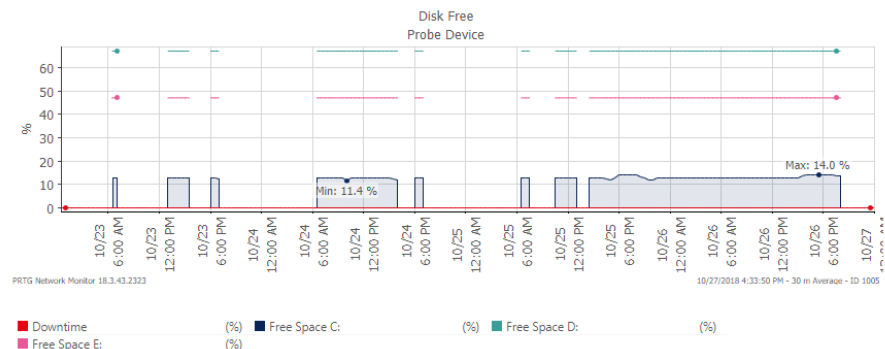
Os sensores analisados foram de disco rígido, HTTP, Ping e saúde do sistema, todo no Notebook Dell citado acima. A data de realização dos relatórios foi entre o dia 23/10/2018 e o dia 26/10/2018. Em todos os gráficos apresentados o eixo das abscissas representa o tempo em horas, e todos são apresentados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

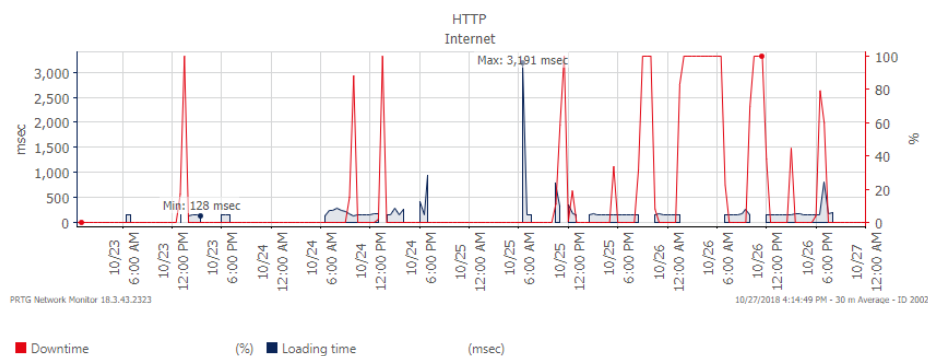


## 5.2 HTTP

O sensor HTTP monitora um servidor web usando Hypertext 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](http://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		



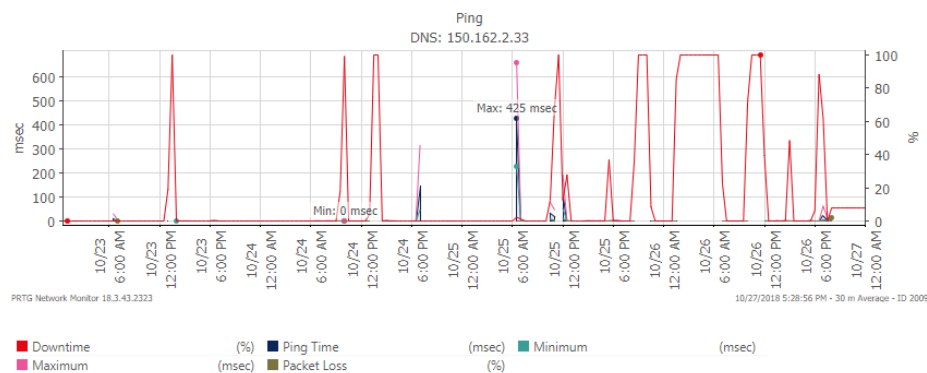
## 5.3 Ping

A latência pode ser usada para testar a conectividade entre equipamentos de uma rede. O sensor de ping envia um pedido Internet Controle Message Protocol (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			

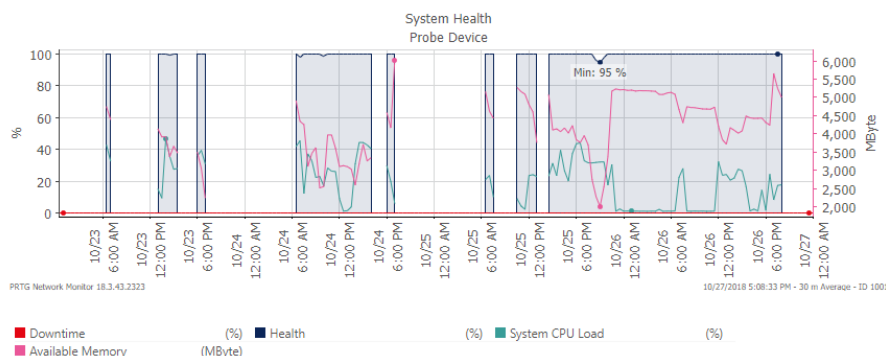


## 5.4 Saúde do Sistema

O sensor de saúde do sistema monitora parâmetros internos do PRTG, mostrando o estado atual do sistema. A linha azul escura 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.

The image shows a Wireshark packet capture of ARP traffic. The main packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
28146	314.202040	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28147	314.885624	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28148	315.885437	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28149	316.897407	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28162	317.884937	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28163	318.888678	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28174	319.900789	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28175	320.888454	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28177	321.888276	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28186	327.887541	IntelCor_f2:56:5c	Netgear_58:62:b8	ARP	42	Who has 10.0.0.1? Tell 10.0.0.11
28187	327.889589	Netgear_58:62:b8	IntelCor_f2:56:5c	ARP	42	10.0.0.1 is at 44:94:fc:58:62:b8
28288	344.201236	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28289	344.888755	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28290	345.888505	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28291	346.900509	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28302	347.888011	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28303	348.887760	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28314	349.899732	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28315	350.887234	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28317	351.887019	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28492	363.318424	Netgear_58:62:b8	Broadcast	ARP	60	Who has 10.0.0.10? Tell 10.0.0.1
28517	374.200185	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28518	374.887748	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28519	375.887573	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
28522	376.899651	IntelCor_f2:56:5c	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11

Packet details for Frame 19883:

- 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- Ethernet II, Src: IntelCor\_f2:56:5c (60:57:18:f2:56:5c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (request)

Packet bytes (hex and ASCII):

```
0000  ff ff ff ff ff ff 60 57 18 f2 56 5c 08 06 00 01  .....W..V\....
0010  08 00 06 04 00 01 60 57 18 f2 56 5c 0a 00 00 0b  .....W..V\....
0020  00 00 00 00 00 00 0a 00 00 02  ..... ..
```

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.

The screenshot displays the Wireshark interface with a packet capture of SNMP traps. The packet list shows a series of traps from source 10.0.0.11 to destination 200.135.85.254. The packet details for frame 5318 show the trap message structure: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Simple Network Management Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
5318	7.308313	10.0.0.11	200.135.85.254	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.1
5319	7.308412	10.0.0.11	200.135.84.85	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.1
5320	7.308450	10.0.0.11	10.0.0.1	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.1
5321	7.308566	10.0.0.11	200.135.85.254	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.5
5322	7.308608	10.0.0.11	200.135.84.85	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.5
5323	7.308649	10.0.0.11	10.0.0.1	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.5
5324	7.308742	10.0.0.11	200.135.85.254	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.10
5325	7.308782	10.0.0.11	200.135.84.85	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.10
5326	7.308818	10.0.0.11	10.0.0.1	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.10
5327	7.308907	10.0.0.11	200.135.85.254	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.12
5328	7.308951	10.0.0.11	200.135.84.85	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.12
5329	7.308986	10.0.0.11	10.0.0.1	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.12
5330	7.309072	10.0.0.11	200.135.85.254	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.13
5331	7.309135	10.0.0.11	200.135.84.85	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.13
5332	7.309169	10.0.0.11	10.0.0.1	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.13
5333	7.309264	10.0.0.11	200.135.85.254	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.25
5334	7.309312	10.0.0.11	200.135.84.85	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.25
5335	7.309347	10.0.0.11	10.0.0.1	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.25
5336	7.309484	10.0.0.11	200.135.85.254	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.26
5337	7.309544	10.0.0.11	200.135.84.85	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.26
5338	7.309640	10.0.0.11	10.0.0.1	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.26
5339	7.309832	10.0.0.11	200.135.85.254	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.27
5340	7.309922	10.0.0.11	200.135.84.85	SNMP	106	trap iso.3.6.1.4.1.311.1.1.3.1.1 1.3.6.1.2.1.2.2.1.1.27

Frame 5318: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0  
 Ethernet II, Src: IntelCor\_f2:56:5c (60:57:18:f2:56:5c), Dst: Netgear\_58:62:b8 (44:94:fc:58:62:b8)  
 Internet Protocol Version 4, Src: 10.0.0.11, Dst: 200.135.85.254  
 User Datagram Protocol, Src Port: 52306, Dst Port: 162  
 Simple Network Management Protocol

0000 44 94 fc 58 62 b8 60 57 18 f2 56 5c 08 00 45 00 D...Xb..W..V...E  
 0010 00 5c 5a c2 00 00 80 11 b7 3e 0a 00 00 0b c8 87 .\Z.....>.....  
 0020 55 fe cc 52 00 a2 00 48 74 16 30 3e 02 01 00 04 U..R...H t..>....  
 0030 06 70 75 62 6c 69 63 a4 31 06 0c 2b 06 01 04 01 .public.1..+....

## 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.