



UNIVERSIDADE FEDERAL DE SANTA CATARINA  
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA  
INE5614 - REDES DE COMPUTADORES

Bruno Aurélio Rôzza de Moura Campos - 14104255

**Segundo trabalho prático (SNMP e Wireshark)**

Florianópolis,  
abril de 2016

## Resumo

O objetivo deste relatório é expor resultado de monitoria de uma rede caseira comentando sobre a ferramenta de utilizada para esta finalidade. Além disso, neste trabalho pratico foi descrito e explicado as características dos objetos gerenciados com interpretação dos resultados obtidos e também apresentado a topologia da rede. Por fim, é mostrado o resultado do uso do wireshark para capturar pacotes de dados desta mesma rede.

## Sumário

1 Introdução .....	4
2 Ferramenta utilizada .....	5
3 Elementos monitorados .....	7
3.1 Elementos monitorados .....	7
3.2 Comunicação da rede interna com a internet .....	8
4 Topologia da rede .....	9
5 Monitoramentos realizados com análises .....	10
5.1 Índice de Disponibilidade .....	11
5.2 Latência .....	14
5.3 Perda de pacotes .....	16
5.4 Largura de banda .....	19
5.5 Carga de CPU e utilização de disco para Notebook (192.168.0.9).....	22
5.5.1 utilização de disco .....	22
5.5.2 Carga de CPU .....	23
6 Protocolo ARP encontrado pelo Wireshark.....	24

## 1. Introdução

Este relatório tem por objetivo apresentar os resultados obtidos do monitoramento de rede utilizando cinco (5) variáveis ou sensores analisados durante 5 dias (com interrupções), que foi solicitado como segundo trabalho prático da disciplina de Redes de Computadores I.

Para realização deste relatório, foi feita uma descrição das configuração dos recursos de equipamentos, mencionado sobre a ferramenta de gerencia de redes utilizada (PRTG) e apresentado a topologia da rede.

O relatório está dividindo da seguinte forma: na seção 2 (PRTG) a ferramenta utilizada, na seção 3 equipamentos, 3.1 Elementos monitorados, 3.2 Comunicação da rede interna com a internet, 4 Topologia da rede, 5 Monitoramentos realizados com análises, e por fim, 6 Protocolo ARP encontrado pelo Wireshark.

## 2. Ferramenta utilizada

Para monitorar a rede foi utilizado o software PRTG Network Monitor. Ele pode ser executado online. Uma função importante é o armazenamento de dados permitindo analisar o desempenho histórico da rede.

O PRTG network monitor é um gerenciador de redes que permite um rápido diagnóstico da rede. Ademias, ele permite usar sondas remotas para monitorar as redes de outros locais.

Existem mais de 200 sensores para instalação, como por exemplo um simples ping até análise completa usando NetFlow. Ele suporta múltiplos protocolos para a coleta desses dados. Abaixo um exemplo do PRTG funcionando em um grupo de dispositivos:



Figura 01. Programa PRTG com visão dos dispositivos no grupo *rede de casa*.



### 3. Equipamentos

Foi utilizado a rede que possuo em casa para monitoramento. A rede possui um total de 4 equipamentos sendo todos em um mesmo cômodo de 50 m<sup>2</sup>.

#### 3.1.Elementos monitorados

##### **Roteador – CISCO (192.168.0.1)**

Modelo: DPC3928S

MAC Address: CC:0D:EC:EF:7A:F6

##### **Smartphone – Samsung (192.168.0.8)**

Modelo: Note 3 – N 9500

MAC Address: F0:25:B7:16:9B:9A

Memória RAM: 3 GB

Processador: Qualcomm MSM8974 Snapdragon 800 - 2.3 GHz Quad Core

Sistema Operacional: Android 5.1

##### **Notebook (192.168.0.9)**

Memória RAM: 8 GB

MAC Address: 40:F0:2F:1C:0E:C6

Processador: Intel Core I7/4700 MQ – 2.4 GHz

Sistema Operacional: Wndows 8.1 – 64 bits

##### **Virtual Machine<sup>1</sup>(192.168.0.15)**

MAC Address: 00:25:22:4E:00:F3

Memória RAM: 2 GB

Processador: Intel Core I7/4700 MQ – 2.4 GHz

Sistema Operacional: Kali (Debian) Linux – 64 bits

---

<sup>1</sup> Para a virtualização foi utilizado o programa VMware® 7.1.2 com uma placa de rede externa USB modelo RALINK 802.11n WLAN.

### 3.2.Comunicação da rede interna com a internet

A rede possui um roteador modelo Cisco DPC3928S (figura 3) conectando a um conector F para receber e enviar os serviços de comunicação com a empresa provedora de serviço com a internet.



Figura3. Roteador utilizado



#### 4. Topologia da rede

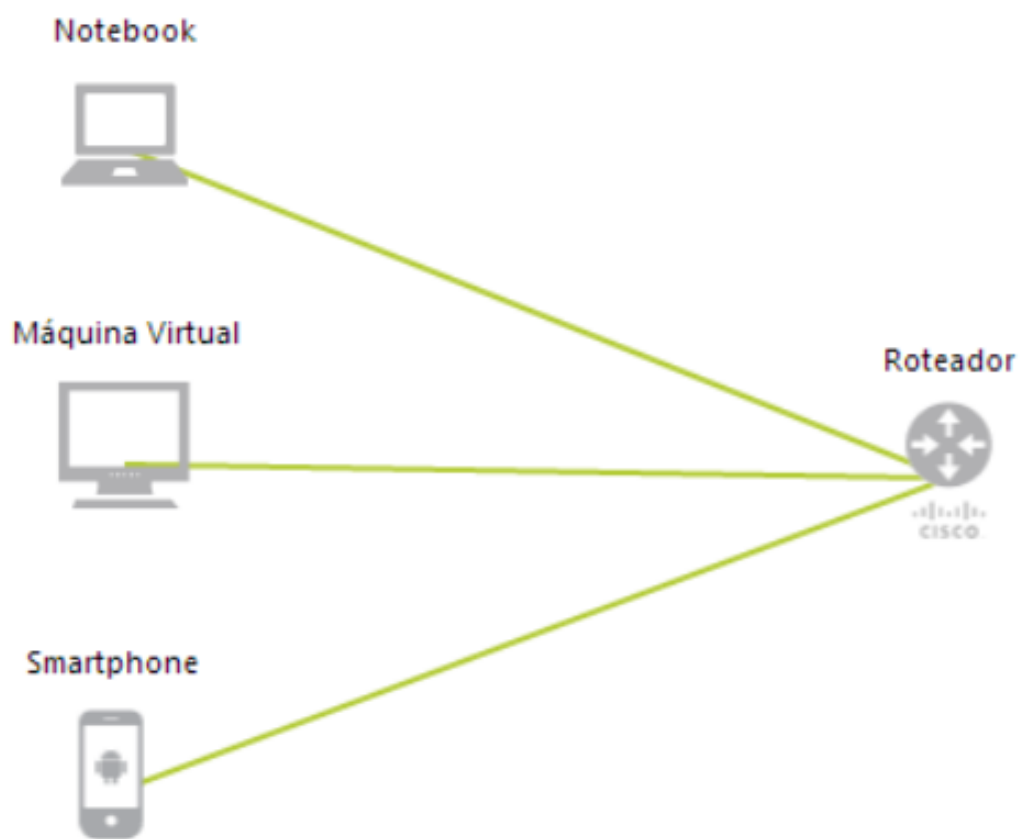


Figura 04. Topologia da rede

## 5. Monitoramentos realizados com análises

As medições foram realizadas do dia 16 de Abril de 2016 a 21 de Abril de 2016 e serão mostradas através de gráficos gerados automaticamente pelo PRTG.

Para que a máquina virtual não ficasse ociosa deixou-se executando o navegador com serviço de streaming de vídeo (YOUTUBE). Já para o notebook, foi deixado executando o serviço de torrent tanto para uploads quanto para downloads.

Para este trabalho foram fixadas as seguintes métricas para o gerenciamento de rede:

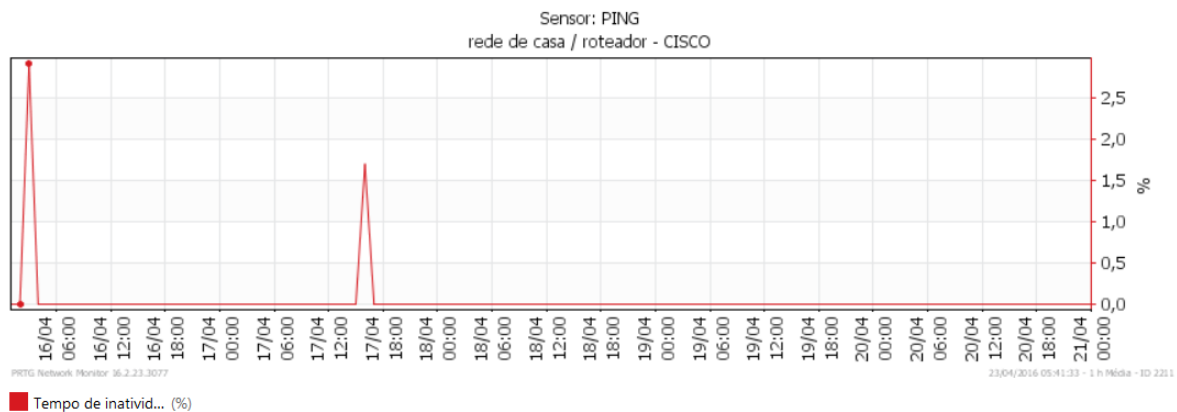
- **Índice de Disponibilidade:** é a porcentagem do tempo que o serviço deve ficar disponível.
- **Latência:** é a medida que descreve o tempo que um determinado pacote IP leva para ir e voltar de um certo ponto da rede até um outro ponto na mesma rede. É medido em milissegundos.
- **Perda de pacotes:** refere-se aos pacotes de requisição ou resposta perdidos durante a utilização da rede.
- **Largura de banda:** registra a quantidade de dados que fluem através de uma placa de rede
- **Carga de CPU, memória RAM e utilização de disco:** mostra a carga de CPU utilizada por cada um (1) dos oito (8) processadores. Já o monitoramento tanto da memória RAM quanto do armazenamento de massa serve para verificar quando se faz necessário algum processo de limpeza ou economia de espaço e até mesmo um upgrade nos equipamentos.

## 5.1. Índice de Disponibilidade

O índice de disponibilidade foi medido através de um sensor de ping, testado para cada equipamento. Abaixo há os resultados obtidos por cada um.

### Roteador – CISCO (192.168.0.1)

Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00				
Tipo de sensor:	Ping (30 s Intervalo)				
Sonda, grupo, dispositivo:	127.0.0.1 > rede de casa > roteador - CISCO				
Estatísticas de tempo de atividade:	Para cima:	99,972 % [4d23h17m58s]	Para baixo:	0,028 % [2m1s]	
Estatísticas de solicitação:	Bom:	99,916 % [14317]	Falha:	0,084 % [12]	
Média (Tempo de ping):	5 ms				

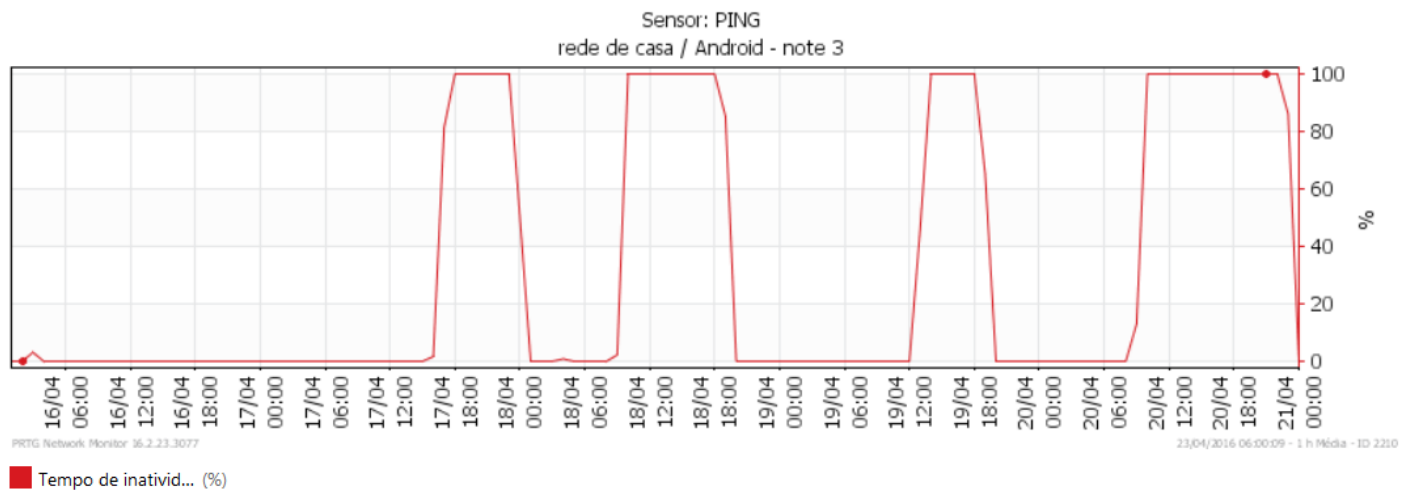


Data/Hora	Tempo de ping	Mínimo	Máximo	Perda de pacote	Tempo de inatividade	Cobertura
<b>Médias (de 120 valores)</b>	5 ms	2 ms	12 ms	<1 %	<1 %	100 %

O equipamento manteve ativo durante 99,972% sendo um resultado excelente para a disponibilidade de utilização. Os picos no sensor são referentes aos momentos que o equipamento está desligado.

## Smartphone – Samsung (192.168.0.8)





Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00				
Tipo de sensor:	Ping (30 s Intervalo)				
Sonda, grupo, dispositivo:	127.0.0.1 > rede de casa > Android - note 3				
Estatísticas de tempo de atividade:	Para cima:	69 %	[3d9h58m11s]	Para baixo:	31 % [1d13h20m28s]
Estatísticas de solicitação:	Bom:	68 %	[9821]	Falha:	32 % [4527]
Média (Tempo de ping):	27 ms				

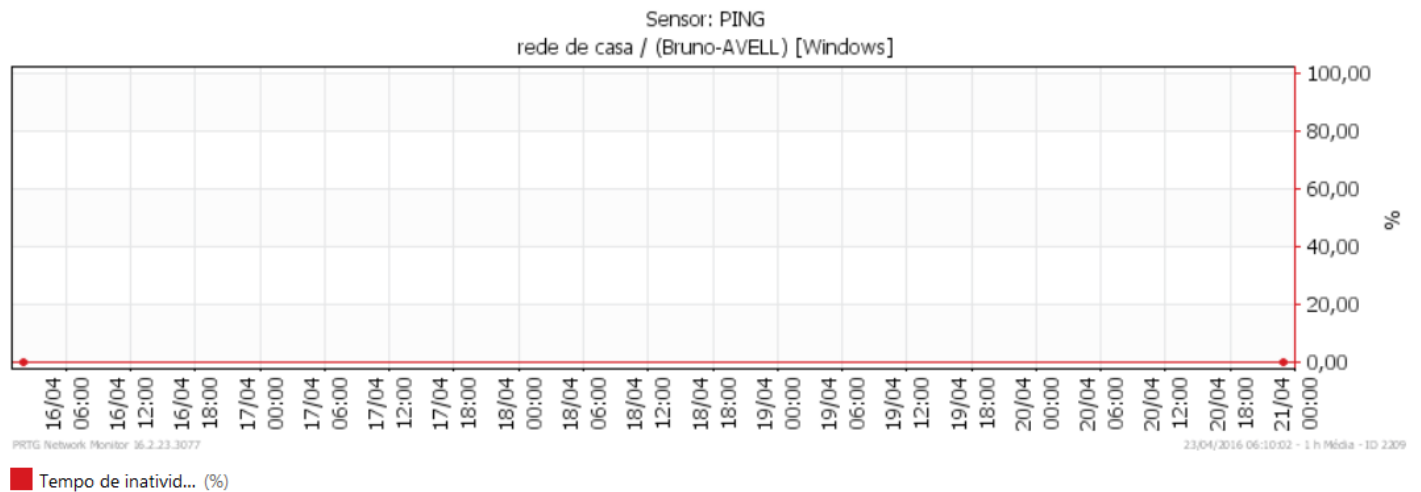


Data/Hora	Tempo de ping	Mínimo	Máximo	Perda de pacote	Tempo de inatividade	Cobertura
<b>Médias (de 87 valores)</b>	27 ms	5 ms	95 ms	<1 %	31 %	100 %

O equipamento manteve ativo durante 69 %. Os picos no sensor são referentes aos momentos que o equipamento fora do alcance da rede pois em nenhum momento ele foi desligado.





## Notebook (192.168.0.9)

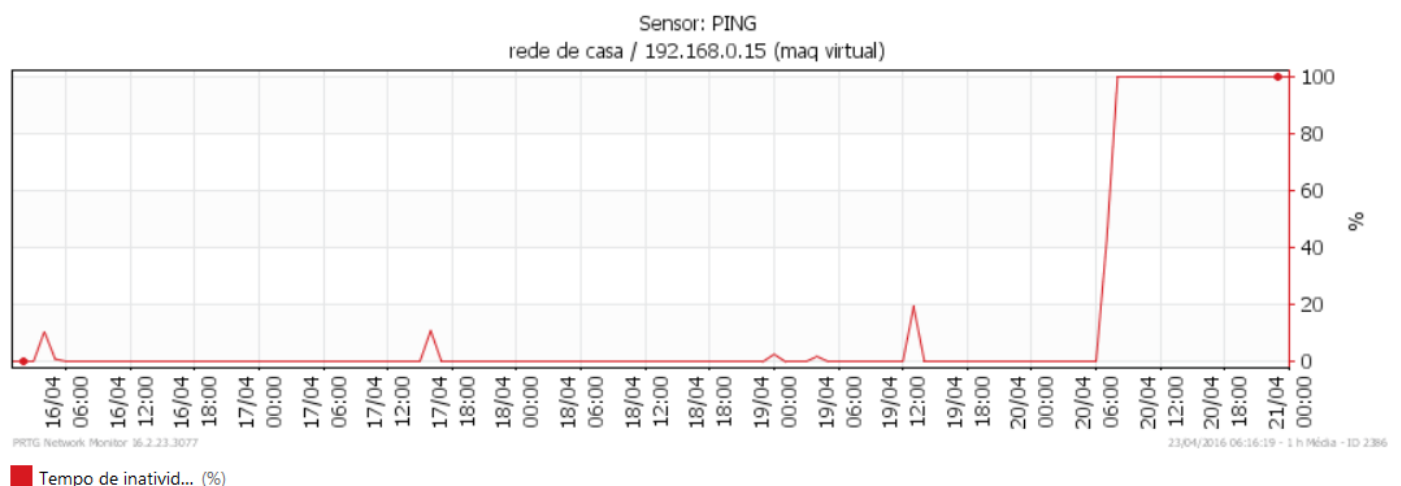
Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00					
Tipo de sensor:	Ping (60 s Intervalo)					
Sonda, grupo, dispositivo:	127.0.0.1 > rede de casa > (Bruno-AVELL) [Windows]					
Estatísticas de tempo de atividade:	Para cima:	100 % 	[4d23h17m55s]	Para baixo:	0 % 	[0s]
Estatísticas de solicitação:	Bom:	100 % 	[7161]	Falha:	0 % 	[0]
Média (Tempo de ping):	0 ms					



Devido o sensor de ping partir sempre desta máquina é possível notar que a disponibilidade é 100 %.

## Virtual Machine (192.168.0.15)

Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00					
Tipo de sensor:	Ping (30 s Intervalo)					
Sonda, grupo, dispositivo:	127.0.0.1 > rede de casa > 192.168.0.15 (maq virtual)					
Estatísticas de tempo de atividade:	Para cima:	85 % 	[4d3h4m40s]	Para baixo:	15 % 	[17h39m32s]
Estatísticas de solicitação:	Bom:	85 % 	[11867]	Falha:	15 % 	[2174]
Média (Tempo de ping):	22 ms					



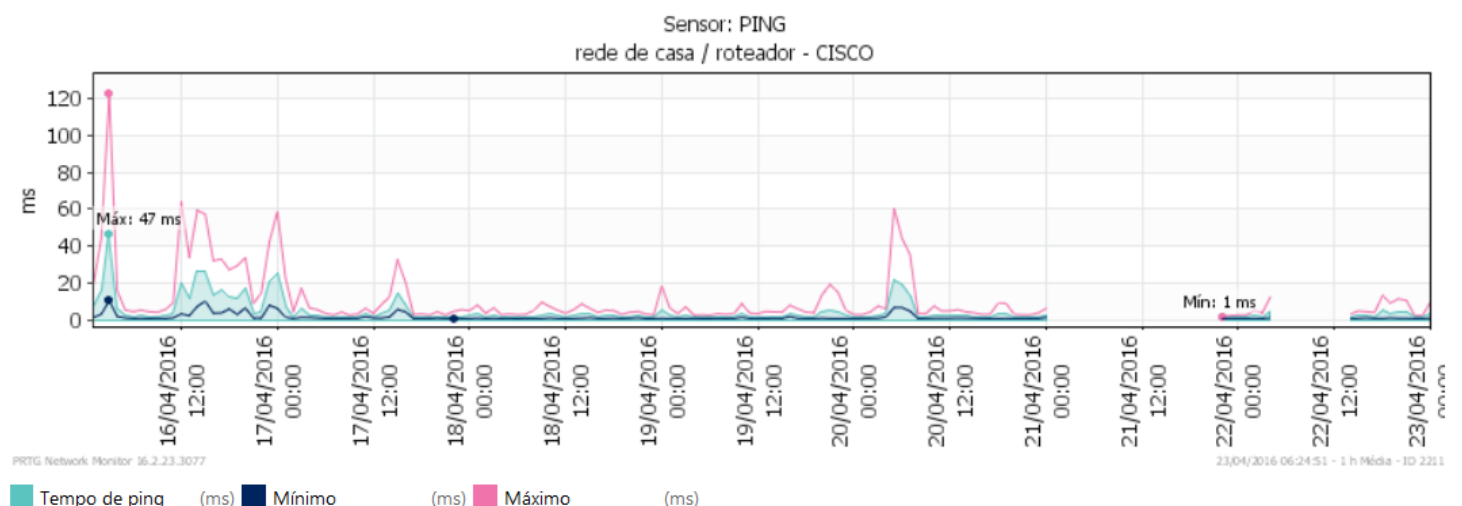
O equipamento manteve ativo durante 85 %. Os primeiros picos de inatividade são porque o equipamento estava configurado para entrar em modo suspensão, já o último é porque o equipamento parou de ser virtualizado.

## 5.2. Latência

A latência foi medida através de um sensor de ping, testado para cada equipamento. Abaixo há os resultados obtidos por cada um.

### Roteador – CISCO (192.168.0.1)

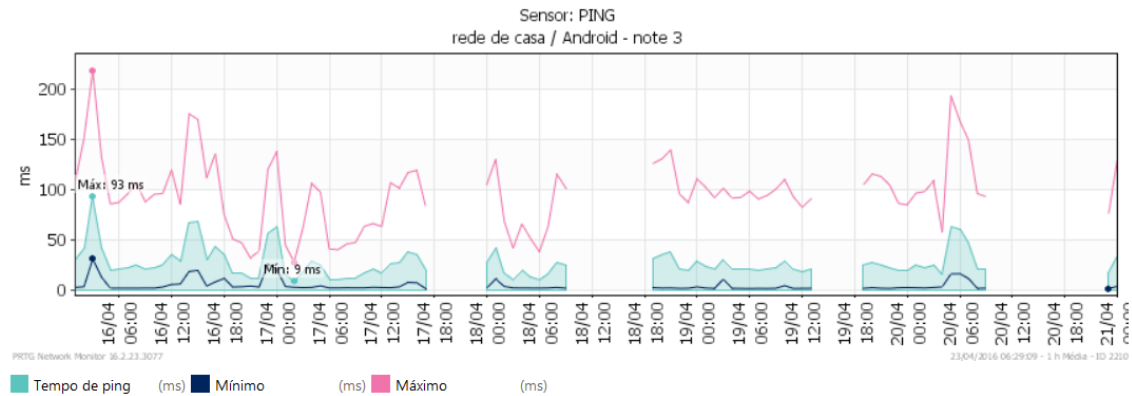
Período do relatório:	16/04/2016 00:00:00 - 23/04/2016 00:00:00				
Tipo de sensor:	Ping (30 s Intervalo)				
Sonda, grupo, dispositivo:	127.0.0.1 > rede de casa > roteador - CISCO				
Estatísticas de tempo de atividade:	Para cima:	99,975 %	[5d15h38m5s]	Para baixo:	0,025 % [2m1s]
Estatísticas de solicitação:	Bom:	99,926 %	[16279]	Falha:	0,074 % [12]
Média (Tempo de ping):	5 ms				



É possível observar que a latência variou entre 1ms (dia 22/04) até 47ms (dia 16/04).

Smartphone – Samsung (192.168.0.8)

Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00				
Tipo de sensor:	Ping (30 s Intervalo)				
Sonda, grupo, dispositivo:	127.0.0.1 > rede de casa > Android - note 3				
Estatísticas de tempo de atividade:	Para cima:	69 %	[3d9h58m11s]	Para baixo:	31 % [1d13h20m28s]
Estatísticas de solicitação:	Bom:	68 %	[9821]	Falha:	32 % [4527]
Média (Tempo de ping):	27 ms				

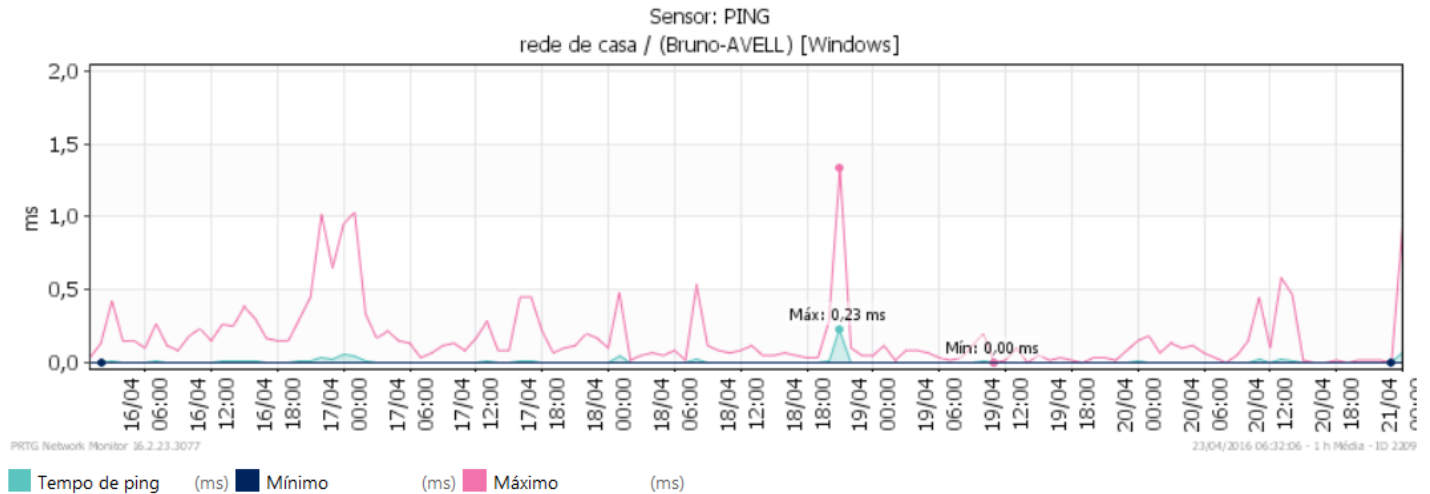


Data/Hora	Tempo de ping	Mínimo	Máximo	Perda de pacote	Tempo de inatividade	Cobertura
<b>Médias (de 87 valores)</b>	27 ms	5 ms	95 ms	< 1 %	31 %	100 %

É possível observar que a latência variou entre 9ms (dia 17/04) até 93ms (dia 16/04).

## Notebook (192.168.0.9)

Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00				
Tipo de sensor:	Ping (60 s Intervalo)				
Sonda, grupo, dispositivo:	127.0.0.1 > rede de casa > (Bruno-AVELL) [Windows]				
Estatísticas de tempo de atividade:	Para cima:	100 %	[4d23h17m55s]	Para baixo:	0 % [0s]
Estatísticas de solicitação:	Bom:	100 %	[7161]	Falha:	0 % [0]
Média (Tempo de ping):	0 ms				







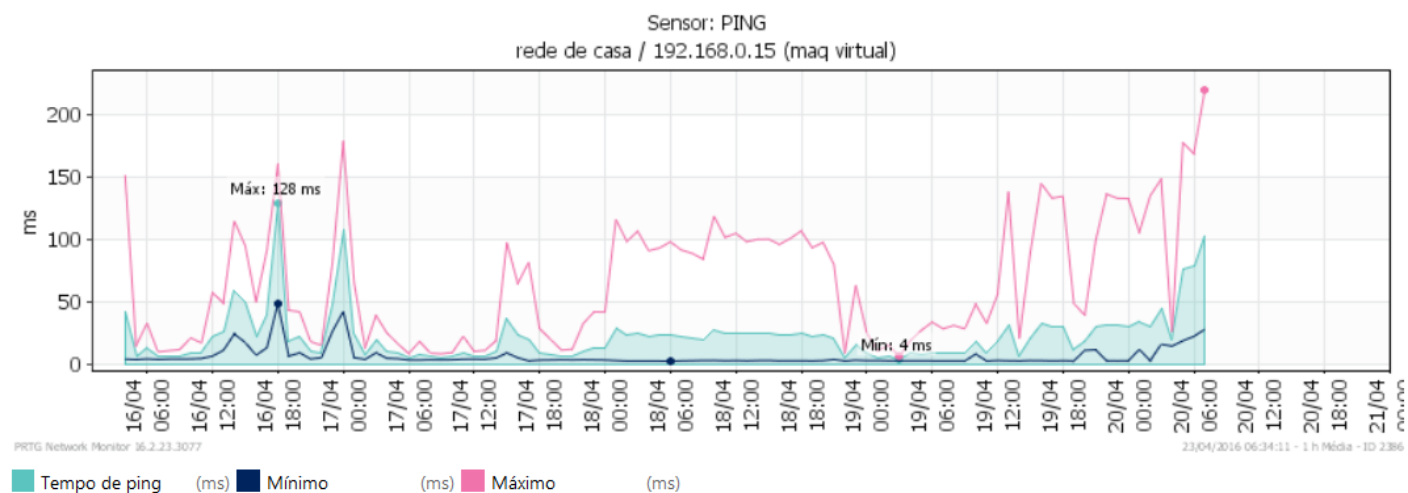
Data/Hora	Tempo de ping	Mínimo	Máximo	Perda de pacote	Tempo de inatividade	Cobertura
<b>Médias (de 120 valores)</b>	0 ms	0 ms	0 ms	0 %	0 %	100 %

É possível observar que a latência variou entre 0ms (dia 19/04) até 0.23ms (dia 19/04).

## Virtual Machine (192.168.0.15)



Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00			
Tipo de sensor:	Ping (30 s Intervalo)			
Sonda, grupo, dispositivo:	127.0.0.1 > rede de casa > 192.168.0.15 (maq virtual)			
Estatísticas de tempo de atividade:	Para cima:	85 %  [4d3h4m40s]	Para baixo:	15 %  [17h39m32s]
Estatísticas de solicitação:	Bom:	85 %  [11867]	Falha:	15 %  [2174]
Média (Tempo de ping):	22 ms			



Data/Hora	Tempo de ping	Mínimo	Máximo	Perda de pacote	Tempo de inatividade	Cobertura
<b>Médias (de 100 valores)</b>	22 ms	6 ms	66 ms	1 %	15 %	98 %

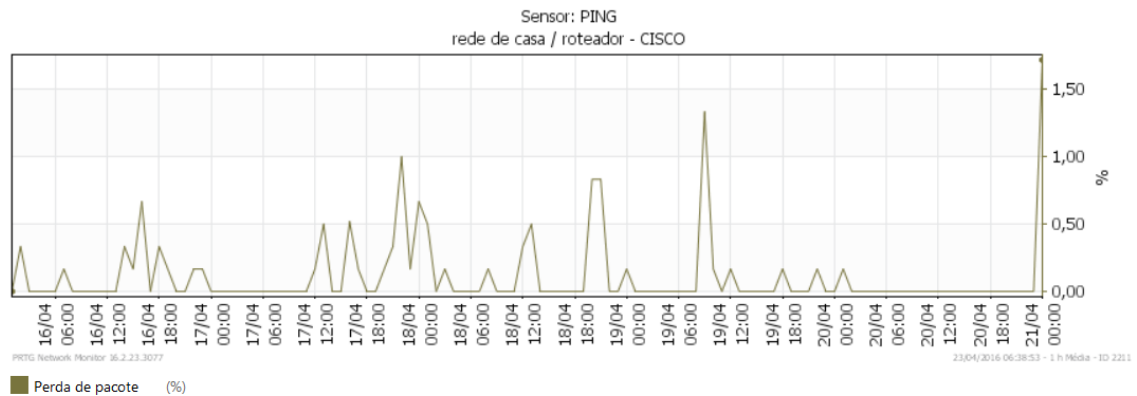
É possível observar que a latência variou entre 4ms (dia 19/04) até 128ms (dia 16/04).

### 5.3. Perda de pacotes

A perda de pacotes foi medida através de um sensor de ping, testado para cada equipamento. Abaixo há os resultados obtidos por cada um.

## Roteador – CISCO (192.168.0.1)

Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00				
Tipo de sensor:	Ping (30 s Intervalo)				
Sonda, grupo, dispositivo:	127.0.0.1 > rede de casa > roteador - CISCO				
Estatísticas de tempo de atividade:	Para cima:	99,972 %	[4d23h17m58s]	Para baixo:	0,028 % [2m1s]
Estatísticas de solicitação:	Bom:	99,916 %	[14317]	Falha:	0,084 % [12]
Média (Tempo de ping):	5 ms				

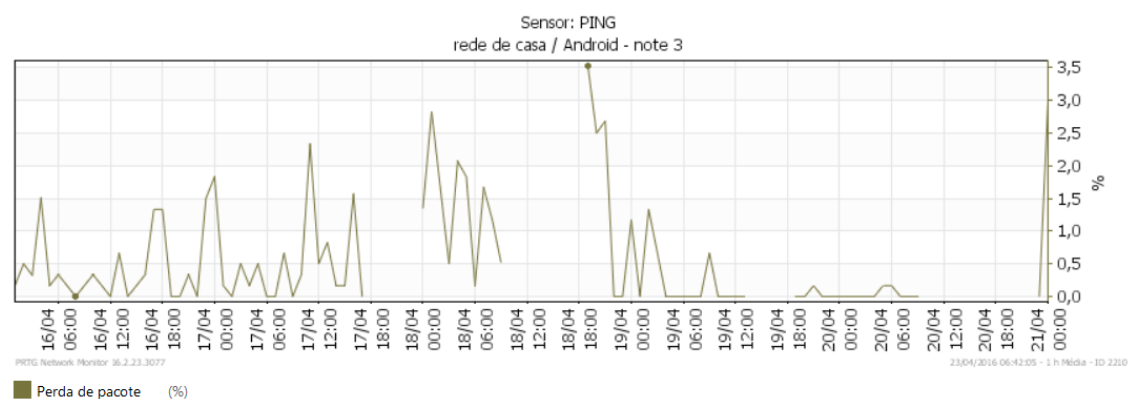


Data/Hora	Tempo de ping	Mínimo	Máximo	Perda de pacote	Tempo de inatividade	Cobertura
<b>Médias (de 120 valores)</b>	5 ms	2 ms	12 ms	<1 %	<1 %	100 %

A perda de pacotes por este equipamento foi menor que 1% do total.

## Smartphone – Samsung (192.168.0.8)

Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00				
Tipo de sensor:	Ping (30 s Intervalo)				
Sonda, grupo, dispositivo:	127.0.0.1 > rede de casa > Android - note 3				
Estatísticas de tempo de atividade:	Para cima:	69 %	[3d9h58m11s]	Para baixo:	31 % [1d13h20m28s]
Estatísticas de solicitação:	Bom:	68 %	[9821]	Falha:	32 % [4527]
Média (Tempo de ping):	27 ms				

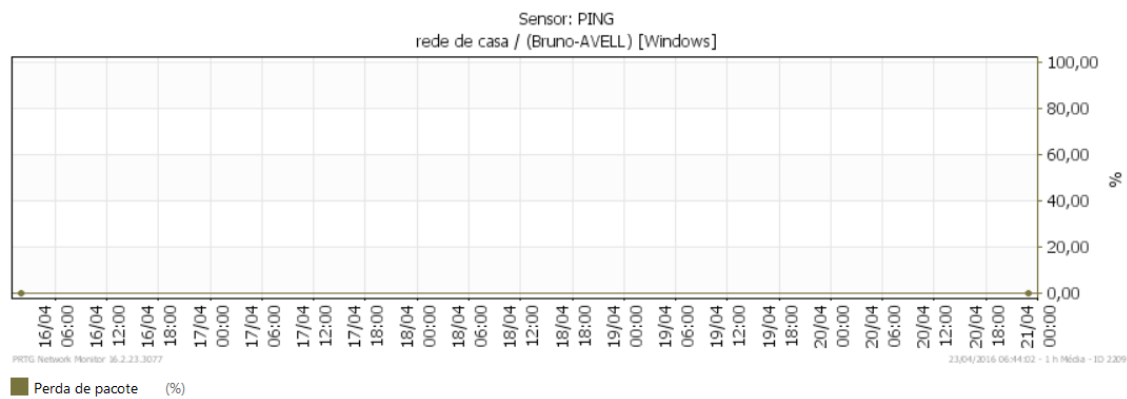


Data/Hora	Tempo de ping	Mínimo	Máximo	Perda de pacote	Tempo de inatividade	Cobertura
<b>Médias (de 87 valores)</b>	27 ms	5 ms	95 ms	<1 %	31 %	100 %

A perda de pacotes por este equipamento foi menor que 1% do total. O gráfico não é contínuo devido ao equipamento não estar sempre conectado à rede.

**Notebook (192.168.0.9)**

Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00		
Tipo de sensor:	Ping (60 s Intervalo)		
Sonda, grupo, dispositivo:	127.0.0.1 > rede de casa > (Bruno-AVELL) [Windows]		
Estatísticas de tempo de atividade:	Para cima:	100 % [4d23h17m55s]	Para baixo: 0 % [0s]
Estatísticas de solicitação:	Bom:	100 % [7161]	Falha: 0 % [0]
Média (Tempo de ping):	0 ms		

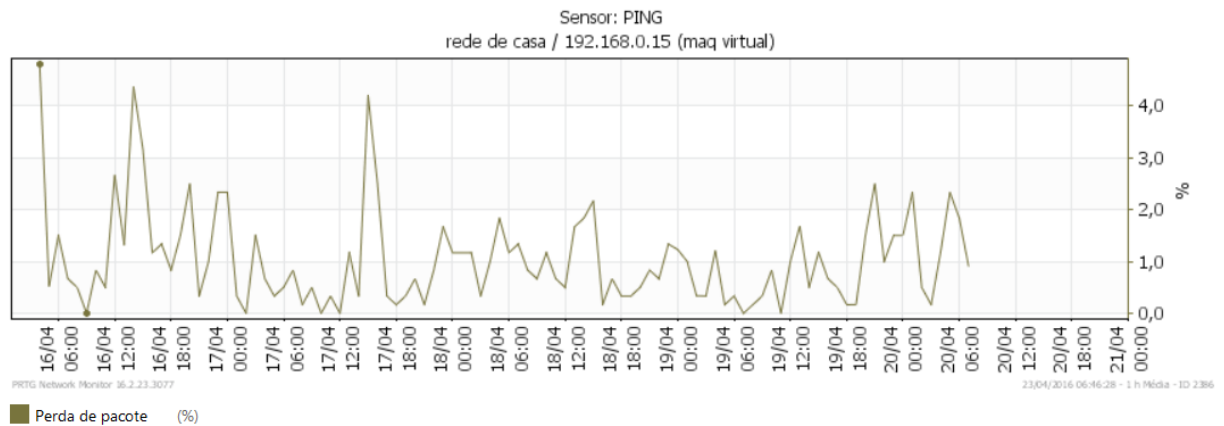


Data/Hora	Tempo de ping	Mínimo	Máximo	Perda de pacote	Tempo de inatividade	Cobertura
<b>Médias (de 120 valores)</b>	0 ms	0 ms	0 ms	0 %	0 %	100 %

Não houve perda de pacotes neste caso pois o ping é disparado por ele mesmo.

**Virtual Machine (192.168.0.15)**

Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00				
Tipo de sensor:	Ping (30 s Intervalo)				
Sonda, grupo, dispositivo:	127.0.0.1 > rede de casa > 192.168.0.15 (maq virtual)				
Estatísticas de tempo de atividade:	Para cima:	85 %	[4d3h4m40s]	Para baixo:	15 % [17h39m32s]
Estatísticas de solicitação:	Bom:	85 %	[11867]	Falha:	15 % [2174]
Média (Tempo de ping):	22 ms				







Data/Hora	Tempo de ping	Mínimo	Máximo	Perda de pacote	Tempo de inatividade	Cobertura
<b>Médias (de 100 valores)</b>	22 ms	6 ms	66 ms	1 %	15 %	98 %

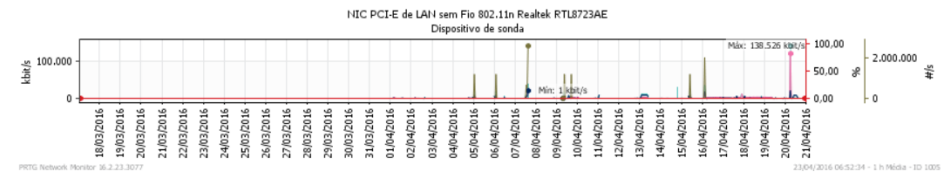
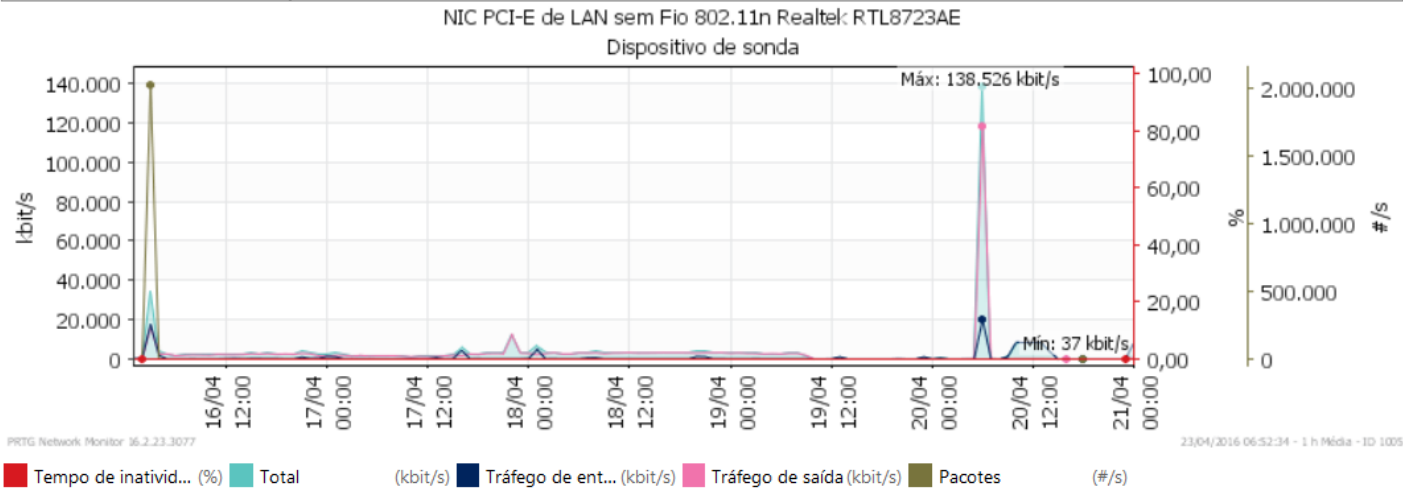
Na máquina virtual houve um pouco mais de perdas de pacotes se comparado com os outros equipamentos. Aqui cabe uma ratificação importante, este equipamento não esta utilizando a mesma placa de rede do notebook, ele utiliza a rede externa USB modelo RALINK 802.11n WLAN.

#### 5.4. Largura de banda

A largura de banda foi medida através de um sensor do programada PRTG chamado de “bandwidthsensor”. No caso da largura de banda foi visto 2 equipamentos (notebook e a virtual machine).

Notebook (192.168.0.9)

Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00			
Horas de relatório:	24 / 7			
Tipo de sensor:	Cartão de rede do Windows (60 s Intervalo)			
Sonda, grupo, dispositivo:	127.0.0.1 > 127.0.0.1 > Dispositivo de sonda			
Estatísticas de tempo de atividade:	Para cima:	100 %  [4d23h30m30s]	Para baixo:	0 %  [0s]
Estatísticas de solicitação:	Bom:	100 %  [7095]	Falha:	0 %  [0]
Média (Total):	3.687 kbit/s			
Total (Total):	191.871.015 KByte			



Canal	Média	Total
Total	3.687 kbit/s	191.871.015 KByte
Tráfego de entrada	927 kbit/s	48.253.602 KByte
Tráfego de saída	2.760 kbit/s	143.617.413 KByte
Pacotes	10.431 #/s	4.446.513.217 #

Data/Hora	Total (volume)	Total (velocidade)	Tráfego de entrada (volume)	Tráfego de entrada (velocidade)	Tráfego de saída (volume)	Tráfego de saída (velocidade)	Pacotes (volume)	Pacotes (velocidade)	Tempo de inatividade	Cobertura
Somas (de 120 valores)	191.871.015 KByte		48.253.602 KByte		143.617.413 KByte		4.446.513.217 #			
Médias (de 120 valores)	1.598.925 KByte	3.687 kbit/s	402.113 KByte	927 kbit/s	1.196.812 KByte	2.760 kbit/s	37.054.277 #	10.431 #/s	0 %	99 %

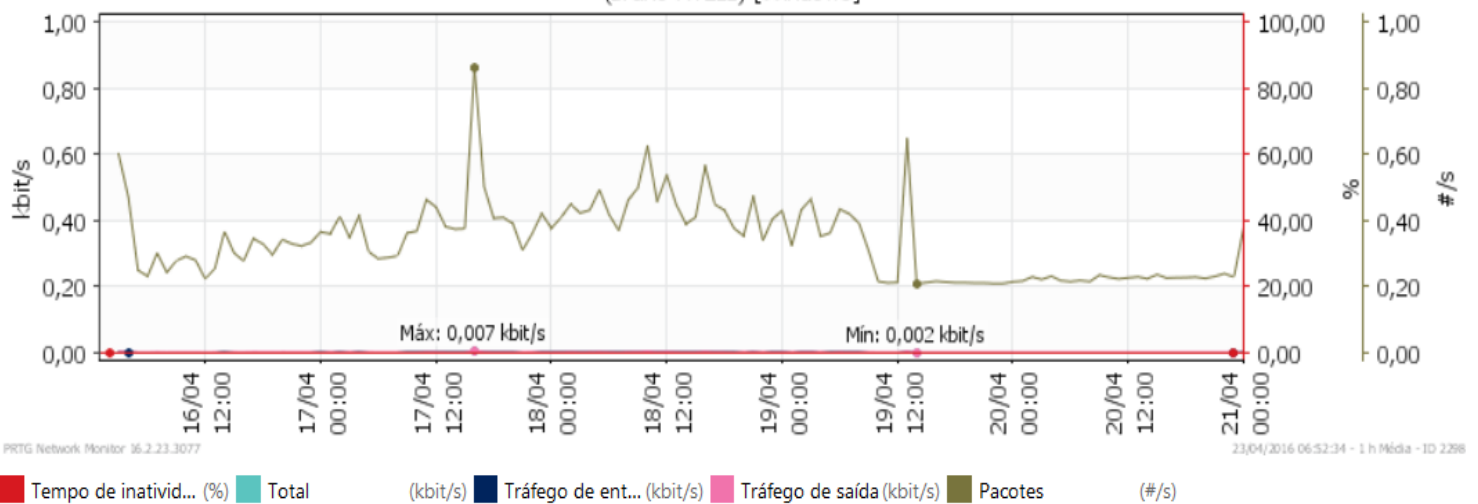
É possível observar que nos dias 16 e 20 houve um grande salto na quantidade de kbits/s trafegados, uso ocorreu devido ao incremento de vários arquivos torrents.

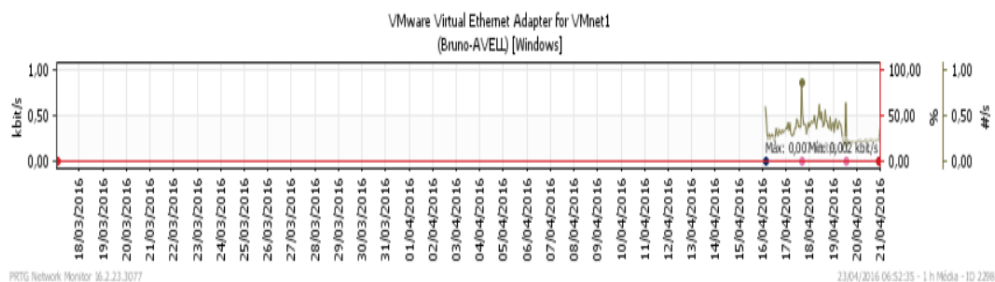
## Virtual Machine (192.168.0.15)

### Relatório: VMware Virtual Ethernet Adapter for VMnet1

Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00				
Horas de relatório:	24 / 7				
Tipo de sensor:	Cartão de rede do Windows (60 s Intervalo)				
Sonda, grupo, dispositivo:	127.0.0.1 > rede de casa > (Bruno-AVELL) [Windows]				
Estatísticas de tempo de atividade:	Para cima:	100 %	[4d21h15m33s]	Para baixo:	0 % [0s]
Estatísticas de solicitação:	Bom:	100 %	[6979]	Falha:	0 % [0]
Média (Total):	< 0,01 kbit/s				
Total (Total):	138 KByte				

VMware Virtual Ethernet Adapter for VMnet1  
(Bruno-AVELL) [Windows]





Canal	Média	Total
Total	< 0,01 kbit/s	138 KByte
Tráfego de entrada	0 kbit/s	0 KByte
Tráfego de saída	< 0,01 kbit/s	138 KByte
Pacotes	0,34 #/s	141.579 #

Data/Hora	Total (volume)	Total (velocidade)	Tráfego de entrada (volume)	Tráfego de entrada (velocidade)	Tráfego de saída (volume)	Tráfego de saída (velocidade)	Pacotes (volume)	Pacotes (velocidade)	Tempo de inatividade	Cobertura
<b>Somas (de 118 valores)</b>	138 KByte		0 KByte		138 KByte		141.579 #			
<b>Médias (de 118 valores)</b>	1 KByte	< 0,01 kbit/s	0 KByte	0 kbit/s	1 KByte	< 0,01 kbit/s	1.200 #	0,34 #/s	0 %	98 %

É notável que o tráfego de pacotes está bem elevado por causa do utilização do serviço de streaming de vídeo (YOUTUBE).

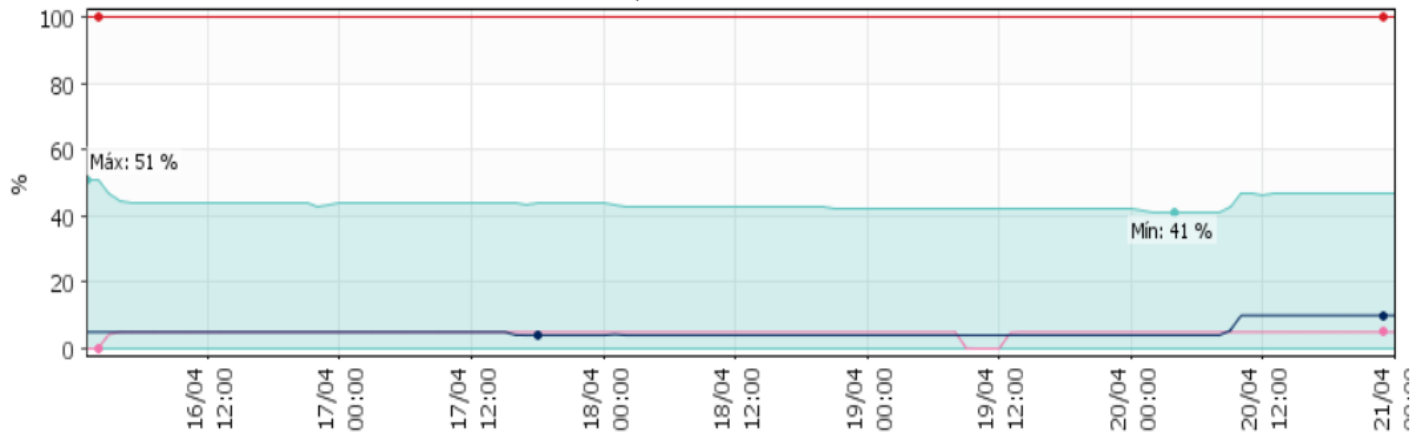
## 5.5. Carga de CPU e utilização de disco para Notebook (192.168.0.9)

Foi realizado a medição de desempenho dos 8 núcleos do processador modelo Intel Core i7-4700MQ 2,40 GHz assim como do SSD (C) e HD de 7200rpm (D e F).

### 5.5.1 Utilização de disco

Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00			
Horas de relatório:	24 / 7			
Tipo de sensor:	Espaço livre em disco da WMI (vários discos) (60 s Intervalo)			
Sonda, grupo, dispositivo:	127.0.0.1 > 127.0.0.1 > Dispositivo de sonda			
Estatísticas de tempo de atividade:	Para cima:	0 % <span style="color: red;">■</span> [0s]	Para baixo:	100 % <span style="color: red;">■</span> [4d23h21m3s]
Estatísticas de solicitação:	Bom:	100 % <span style="color: green;">■</span> [7099]	Falha:	0 % <span style="color: green;">■</span> [0]
Média (Espaço livre C:):	44 %			

Disco livre  
Dispositivo de sonda



PRTG Network Monitor 16.2.23.3077

23/04/2016 07:14:19 - 1 h Média - ID 1004

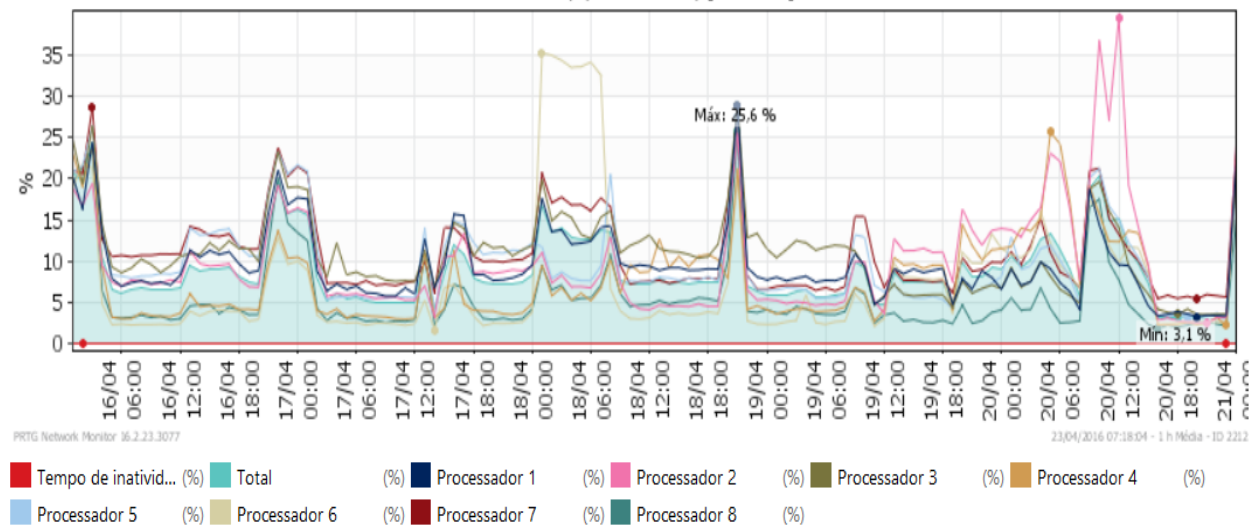
■ Tempo de inativid... (%) 
 ■ Espaço livre C: (%) 
 ■ Espaço livre D: (%) 
 ■ Espaço livre F: (%)



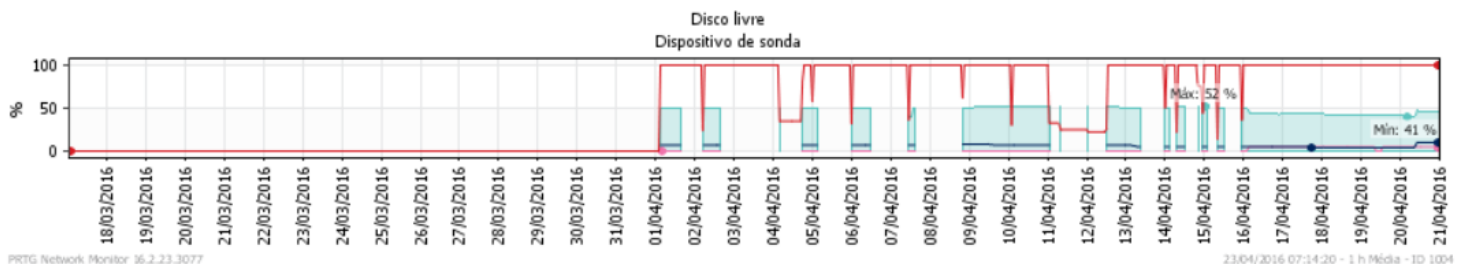
## 5.5.2. Carga de CPU

Período do relatório:	16/04/2016 00:00:00 - 21/04/2016 00:00:00			
Tipo de sensor:	Carregamento de CPU do Windows (60 s Intervalo)			
Sonda, grupo, dispositivo:	127.0.0.1 > rede de casa > (Bruno-AVELL) [Windows]			
Estatísticas de tempo de atividade:	Para cima:	100 % <span style="color: green;">■</span> [4d23h19m10s]	Para baixo:	0 % <span style="color: green;">■</span> [0s]
Estatísticas de solicitação:	Bom:	99,986 % <span style="color: red;">■</span> [7102]	Falha:	0,014 % <span style="color: red;">■</span> [1]
Média (Total):	9 %			

Sensor: Carga da CPU  
rede de casa / (Bruno-AVELL) [Windows]



Data/Hora	Total	Processador 1	Processador 2	Processador 3	Processador 4	Processador 5	Processador 6	Processador 7	Processador 8	Tempo de inatividade	Cobertura
<b>Médias (de 120 valores)</b>	9 %	10 %	10 %	11 %	8 %	10 %	8 %	11 %	5 %	0 %	100 %



Canal	Média
Total	141.233 MByte
Bytes livres C:	49.634 MByte
Espaço livre C:	44 %
Bytes livres D:	46.858 MByte
Espaço livre D:	5 %
Bytes livres F:	44.741 MByte
Espaço livre F:	5 %

Data/Hora	Total	Bytes livres C:	Espaço livre C:	Bytes livres D:	Espaço livre D:	Bytes livres F:	Espaço livre F:	Tempo de inatividade	Cobertura
<b>Médias (de 120 valores)</b>	141.233 MByte	49.634 MByte	44 %	46.858 MByte	5 %	44.741 MByte	5 %	100 %	100 %

A carga de CPU obteve alguns picos, chegando a passar os 35%. Nestes momentos de picos, o antivírus (Kaspersky) estava executando uma verificação do sistema.

## 6. Protocolo ARP encontrado pelo Wireshark

Wireshark capture of ARP traffic. The packet list shows multiple ARP requests from CiscoSpv\_ef:7a:f9 to various destinations. Packet 80769 is selected, showing an ARP request from SamsungE\_47:5e:79 to LiteonTe\_1c:0e:c6. The packet details pane shows the frame structure and hex data.

No.	Time	Source	Destination	Protocol	Length	Info
80563	240.118899	CiscoSpv_ef:7a:f9	Broadcast	ARP	60	Who has 192.168.0.153? Tell 192.168.0.1
80564	240.120006	CiscoSpv_ef:7a:f9	Broadcast	ARP	60	Who has 192.168.0.154? Tell 192.168.0.1
80565	240.121117	CiscoSpv_ef:7a:f9	Broadcast	ARP	60	Who has 192.168.0.155? Tell 192.168.0.1
80566	240.122220	CiscoSpv_ef:7a:f9	Broadcast	ARP	60	Who has 192.168.0.156? Tell 192.168.0.1
80567	240.123294	CiscoSpv_ef:7a:f9	Broadcast	ARP	60	Who has 192.168.0.157? Tell 192.168.0.1
80568	240.124345	CiscoSpv_ef:7a:f9	Broadcast	ARP	60	Who has 192.168.0.158? Tell 192.168.0.1
80569	240.125447	CiscoSpv_ef:7a:f9	Broadcast	ARP	60	Who has 192.168.0.159? Tell 192.168.0.1
80596	240.137231	LiteonTe_1c:0e:c6	Broadcast	ARP	42	Who has 192.168.0.10? Tell 192.168.0.9
80675	240.429739	LiteonTe_1c:0e:c6	Broadcast	ARP	42	Who has 192.168.0.14? Tell 192.168.0.9
80769	240.804413	SamsungE_47:5e:79	Broadcast	ARP	60	Who has 192.168.0.9? Tell 192.168.0.19
80770	240.804431	LiteonTe_1c:0e:c6	SamsungE_47:5e:79	ARP	42	192.168.0.9 is at 40:f0:2f:1c:0e:c6
80873	241.136939	LiteonTe_1c:0e:c6	Broadcast	ARP	42	Who has 192.168.0.10? Tell 192.168.0.9
80874	241.136958	LiteonTe_1c:0e:c6	Broadcast	ARP	42	Who has 192.168.0.14? Tell 192.168.0.9
81139	242.137668	LiteonTe_1c:0e:c6	Broadcast	ARP	42	Who has 192.168.0.14? Tell 192.168.0.9
81140	242.145840	LiteonTe_1c:0e:c6	Broadcast	ARP	42	Who has 192.168.0.10? Tell 192.168.0.9
81141	242.166891	LiteonTe_1c:0e:c6	Broadcast	ARP	42	Who has 192.168.0.19? Tell 192.168.0.9
81142	242.169026	SamsungE_47:5e:79	LiteonTe_1c:0e:c6	ARP	60	192.168.0.19 is at 00:24:54:47:5e:79
81195	242.324913	LiteonTe_1c:0e:c6	Broadcast	ARP	42	Who has 192.168.0.15? Tell 192.168.0.9
81431	243.137359	LiteonTe_1c:0e:c6	Broadcast	ARP	42	Who has 192.168.0.10? Tell 192.168.0.9
81432	243.137378	LiteonTe_1c:0e:c6	Broadcast	ARP	42	Who has 192.168.0.15? Tell 192.168.0.9
81433	243.143561	LiteonTe_1c:0e:c6	Broadcast	ARP	42	Who has 192.168.0.14? Tell 192.168.0.9
81779	244.137082	LiteonTe_1c:0e:c6	Broadcast	ARP	42	Who has 192.168.0.10? Tell 192.168.0.9
81780	244.137117	LiteonTe_1c:0e:c6	Broadcast	ARP	42	Who has 192.168.0.15? Tell 192.168.0.9
81781	244.137138	LiteonTe_1c:0e:c6	Broadcast	ARP	42	Who has 192.168.0.14? Tell 192.168.0.9

Frame 80769: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
Interface id: 0 (\Device\NPF\_{4ECD5D3D-A162-48EF-AD37-1BDCDC2BF305})  
Encapsulation type: Ethernet (1)  
Arrival Time: Apr 24, 2016 00:17:43.471748000 Hora oficial do Brasil  
[Time shift for this packet: 0.000000000 seconds]  
Epoch Time: 1461467863.471748000 seconds  
[Time delta from previous captured frame: 0.004615000 seconds]  
[Time delta from previous displayed frame: 0.374674000 seconds]  
[Time since reference or first frame: 240.804413000 seconds]  
Frame Number: 80769

```

0000  ff ff ff ff ff ff 00 24 54 47 5e 79 08 06 00 01  ....$ TG^y....
0010  08 00 06 04 00 01 00 24 54 47 5e 79 c0 a8 00 13  ....$ TG^y....
0020  00 00 00 00 00 00 c0 a8 00 09 00 00 00 00 00 00  ....
0030  00 00 00 00 00 00 00 00 00 00 00 00  ....

```

wireshark\_pcapng\_4ECD5D3D-A162-48EF-AD37-1BDCDC2BF305\_20160424001342\_a04540 Packets: 85973

Na imagem do WireShark foi filtrado todos os protocolos ARP como requisitado. Ao analisar, podemos ver que o equipamento(SamsungE\_47:5e:70) enviou por broadcast um ARP Request (linha selecionada) contendo o ipv4, para todos os membros da rede perguntando quem tem o IP 192.168.0.9. A resposta veio na linha de baixo (LiteonTe\_1c:0e:c6) por um ARP Reply dizendo ser ele o portador do IP 192.168.0.9.