

Universidade Federal de Santa Catarina
Departamento de Informática e Estatística
Ciências da Computação
INE5414 - Redes de Computadores I
Professor: Carlos Becker Westphall

Aluno: Tális Breda - 22102202

Trabalho Prático 2
Monitoramento de Rede, SNMP, UDP, TCP e WireShark

Florianópolis – SC, 08 de novembro de 2023

1. Resumo

Neste trabalho, foi realizado o monitoramento de uma rede doméstica utilizando o PRTG Monitor no plano gratuito (limitado a 100 sensores). O monitoramento foi feito a partir de quatro dispositivos: um smartphone POCO X3 NFC, um computador desktop, e dois laptops DELL. Para os sensores, foram utilizados alguns mais simples providos pelo PRTG Monitor, como Ping, HTTP, SaaS comuns, tráfego de rede, uso de CPU e Ping Jitter. O monitoramento foi realizado em dois dias diferentes, mantendo-se por intervalos de algumas horas em cada dia. Além disso, foi utilizada a ferramenta Wireshark para monitorar troca de pacotes através de protocolos como ARP, UDP, TCP e SNMP.

2. Índice

1. Resumo.....	2
2. Índice.....	3
3. Introdução.....	4
4. Ferramenta de gerência.....	4
5. Topologia da rede.....	5
6. Descrição dos componentes.....	5
6.1. Roteador Claro F@ST3895.....	5
6.2. Desktop.....	6
6.3. Laptop DELL Inspiron 15.....	6
6.4. Laptop DELL Inspiron 14-2620.....	6
6.5. Smartphone Poco X3 NFC.....	6
7. Descrição das medições.....	7
7.1. Ping.....	7
7.1.1. Roteador.....	8
7.1.2. Laptop i7.....	9
7.1.3. Laptop i3.....	10
7.1.4. Smartphone POCO X3 NFC.....	11
7.2. HTTP.....	12
7.2.1. Roteador.....	12
7.2.2. Laptop i7.....	13
7.2.3. Laptop i3.....	14
7.2.4. Desktop.....	15
7.2.5. Smartphone POCO X3.....	16
7.3. Jitter Ping.....	17
7.3.1. Roteador.....	17
7.3.2. Laptop i7.....	18
7.3.3. Laptop i3.....	19
7.3.4. Smartphone POCO X3 NFC.....	20
7.4. Common SaaS Check.....	21
7.4.1. Roteador.....	21
7.4.2. Laptop i7.....	22
7.4.3. Laptop i3.....	23
7.4.4. Desktop.....	24
7.4.5. Smartphone POCO X3.....	25
7.5. Tráfego de rede (Ethernet).....	26
7.5.1. Desktop.....	27
7.6. Tráfego de rede (Wi-fi).....	28
7.6.1. Desktop.....	28
7.7. Carga de CPU.....	29
7.7.1. Desktop.....	29
8. Wireshark.....	30
8.1. ARP.....	30

8.2. TCP e HTTP.....	30
8.3. UDP.....	31
9. Conclusão.....	32
10. Referências bibliográficas.....	33

3. Introdução

As redes de computadores estão presentes em praticamente todas as residências, estabelecimentos e locais em geral. São parte imprescindível da sociedade atual. Por isso, é importante analisar e entender o comportamento destas, e como diferentes dispositivos utilizam a rede e se relacionam entre si. Neste trabalho, o objetivo é analisar dados diferentes de diversos dispositivos, e seus relacionamentos com a rede, através da visualização de protocolos de comunicação como UDP, TCP, SNMP e ARP.

4. Ferramenta de gerência

A ferramenta de gerência escolhida foi o PRTG Monitor, que apesar de possuir planos pagos, possui um plano gratuito que atende perfeitamente às exigências deste trabalho, pois permite o uso de até 100 sensores em diferentes dispositivos. Os sensores utilizados pelo PRTG são uma maneira de monitorar diferentes aspectos de cada dispositivo e sua relação com a rede. A ferramenta também gera gráficos com base no que foi detectado pelos sensores em um período de tempo grande, permitindo a visualização da interação dos dispositivos com a rede.

No trabalho também foi usado o Wireshark para analisar os diferentes protocolos utilizados para comunicação na rede.

5. Topologia da rede

A rede é baseada em um roteador da Claro, e foram analisados 4 dispositivos conectados a ele: Um computador desktop, dois laptops e um smartphone

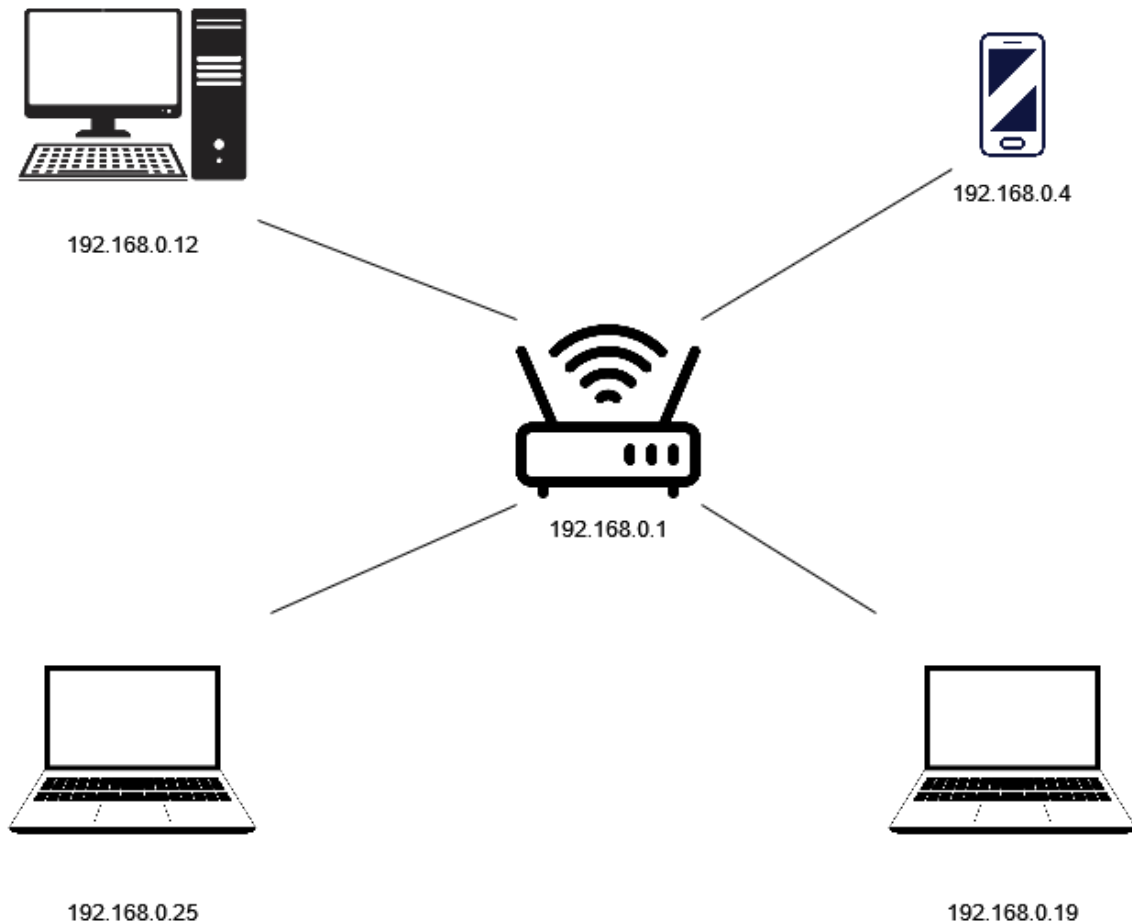


Figura 1 - Representação da topologia da rede

6. Descrição dos componentes

Segue uma descrição detalhada de cada um dos componentes da rede.

6.1. Roteador Claro F@ST3895

Roteador fornecido pela fornecedora de internet, com frequências de transmissão de 2.4Ghz e 5.8Ghz

6.2. Desktop

Um computador desktop customizado, conforme as especificações a seguir:

- Processador: Intel Core i5 10400F 2.6Ghz
- GPU: Radeon RX580 8GB
- Memória RAM: 16GB DDR4
- Sistema Operacional: Windows 10 Pro
- Adaptador de rede sem fio: TP-Link TL-WN823N limitado a 2.4Ghz

6.3. Laptop DELL Inspiron 15

- Processador: Intel Core i7-1255U 4.7Ghz
- GPU: Intel Iris Xe
- Memória RAM: 16GB DDR4
- Sistema Operacional: Linux Mint 21.2
- Adaptador de rede: nativo com suporte a 2.4Ghz e 5Ghz

6.4. Laptop DELL Inspiron 14-2620

- Processador: Intel Core i3-2375M 1.5Ghz
- GPU: Intel HD Graphics
- Memória RAM: 6GB DDR3
- Sistema Operacional: Linux Mint 21
- Adaptador de rede: nativo com suporte limitado a 2.4Ghz

6.5. Smartphone Poco X3 NFC

- Processador: Qualcomm Snapdragon 732G
- GPU: Adreno 618
- Memória RAM: 6GB
- Sistema Operacional: Android 12 - MIUI 14.0.4
- Adaptador de rede: nativo com suporte a 2.4Ghz e 5Ghz

7. Descrição das medições

A seguir, serão descritas as medições realizadas durante o trabalho, separadas por tipo de sensor e dispositivo. É importante notar que algumas medições, mais precisamente aquelas que fazem uso do SNMP, foram realizadas em apenas um dispositivo, o computador desktop, que também é onde o PRTG foi instalado. Isso foi por conta de limitações técnicas, visto que não foi possível instalar funcionalmente o SNMP nas máquinas Linux ou no dispositivo Android.

Os sensores utilizados em todos os dispositivos foram Ping, HTTP e Common SaaS Check. No Desktop (192.168.0.12) foram utilizados os sensores de Carga de CPU e de tráfego de rede Ethernet, ambos utilizando o protocolo SNMP. Nos outros dispositivos, esses sensores foram substituídos pelo de Jitter Ping

7.1. Ping

O ping é a medida básica de conexão com a rede: ele atesta o atraso de conexão entre um dispositivo e a rede. No caso do dispositivo agente (desktop) o ping é 0 pois é ele próprio quem faz as requisições. É mais importante analisar o ping dos outros dispositivos.

7.1.1. Roteador

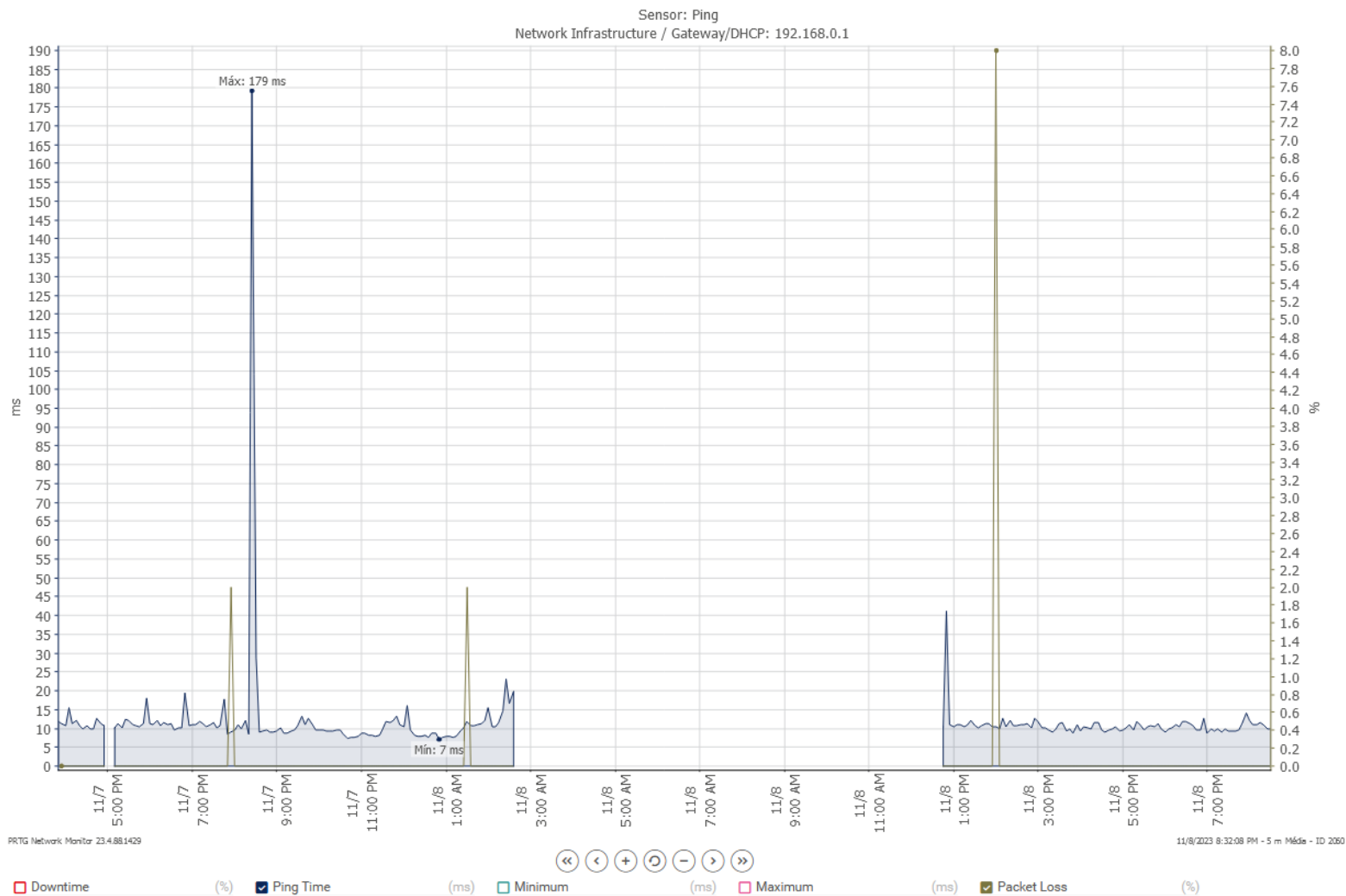


Figura 2 - Gráfico de ping do roteador

Nesse gráfico podemos visualizar o tempo de resposta do roteador principal (192.168.0.1). Nota-se um tempo de resposta de, em média, 10ms que permanece durante todo o tempo em que o roteador é monitorado, com apenas alguns picos. Também observamos a perda de pacote que ocorre poucas vezes durante o monitoramento.

7.1.2. Laptop i7

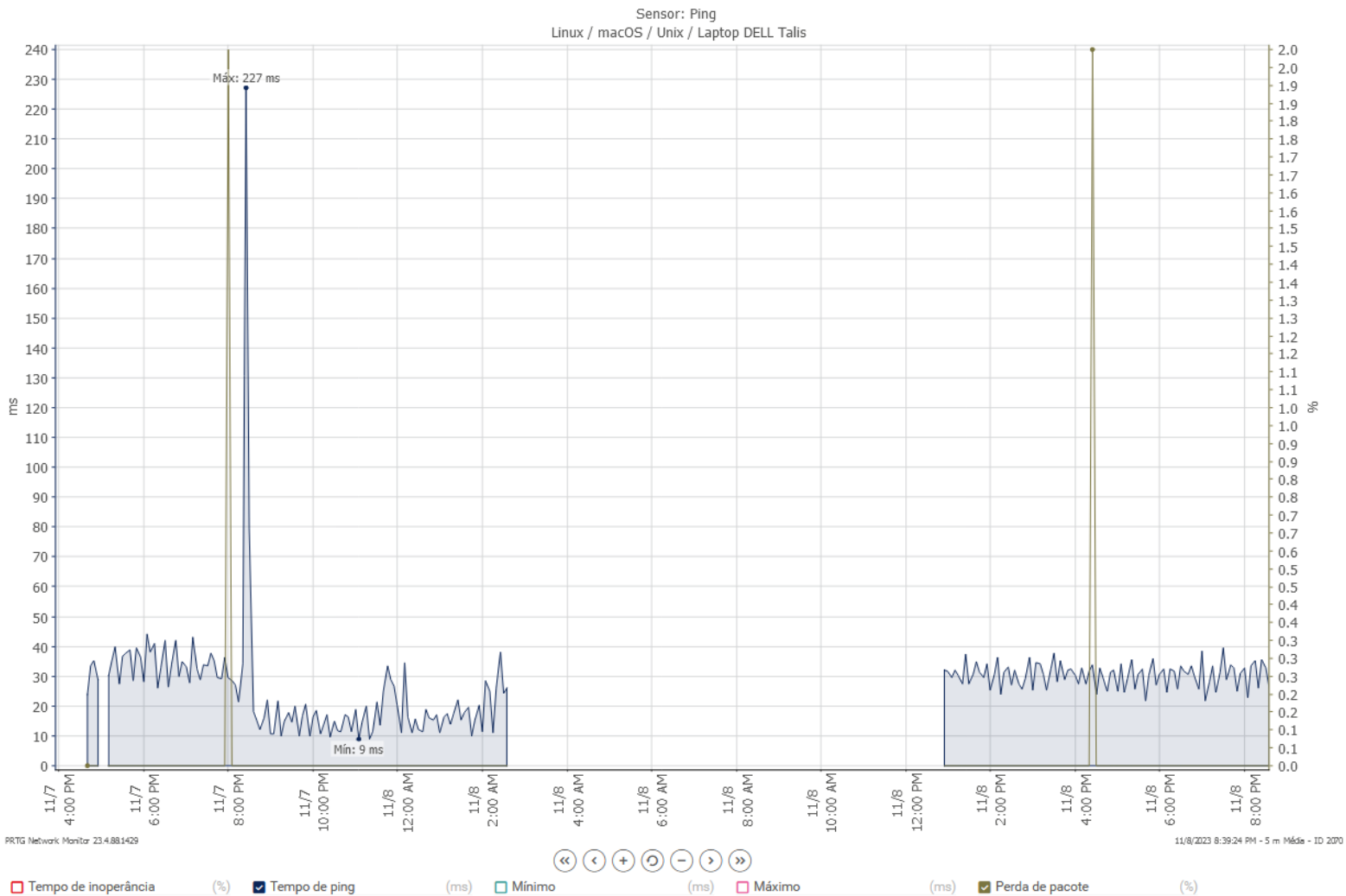


Figura 3 - Gráfico de ping do Laptop Dell com i7

Aqui podemos ver que o ping do laptop i7 varia bastante, e fica, em média, em uma faixa um pouco acima do que vimos no roteador. Podemos ver também uma redução no tempo de resposta quando o horário se aproxima das 22:00, possivelmente relacionado ao menor tráfego nas redes do provedor.

7.1.3. Laptop i3

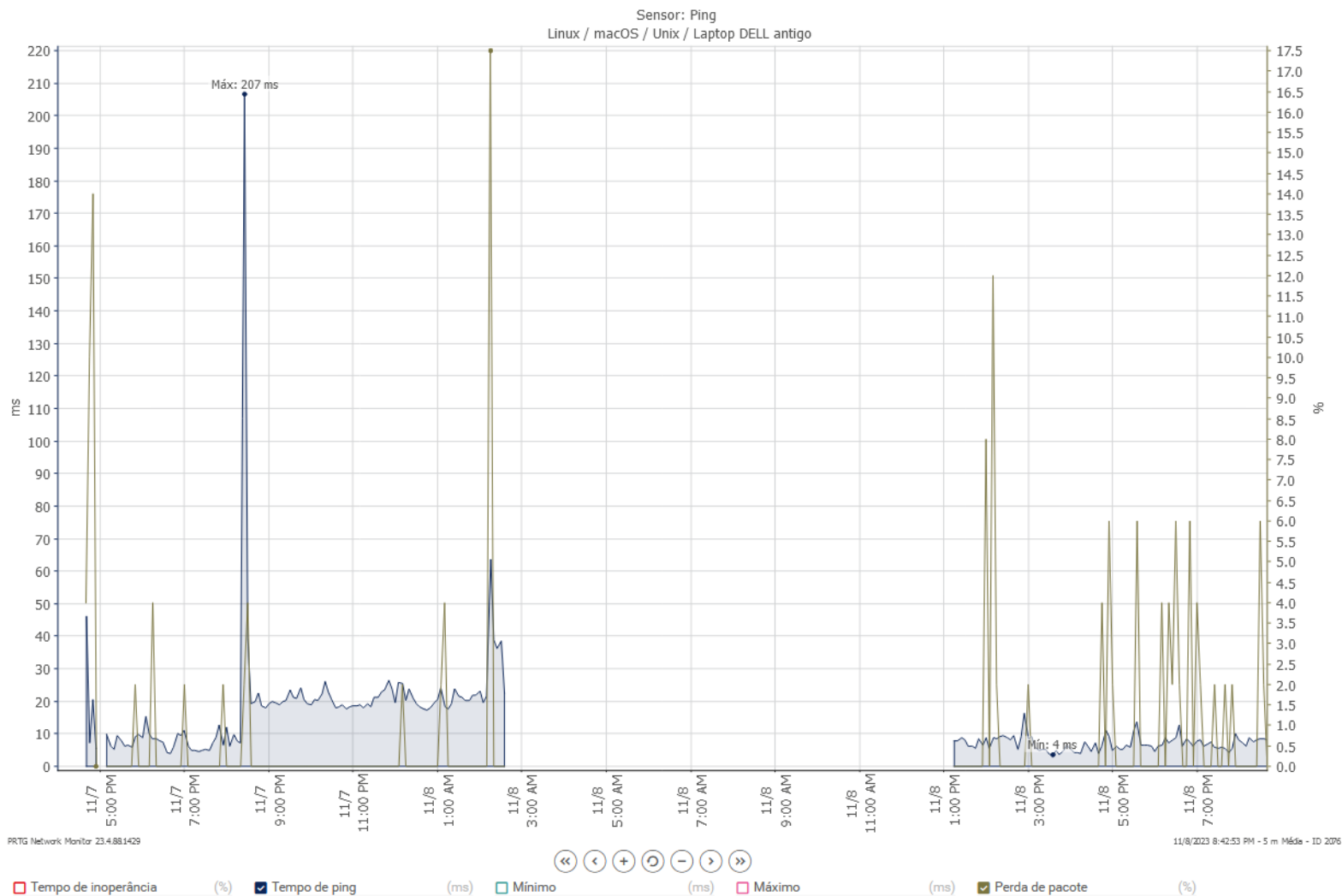


Figura 4 - Gráfico de ping do laptop com i3

Aqui vemos o gráfico de ping do laptop antigo, com conexão 2.4Ghz. É possível notar diversos momentos onde ocorre perda de pacotes, o que provavelmente tem relação com o fato de que a rede não é 5.8Ghz.

Baseando-se nos últimos dois gráficos e neste, vemos sempre um pico em tempo de resposta no horário perto das 20:00. A causa provável para isso é alguma queda na rede ou alguma má conexão.

7.1.4. Smartphone POCO X3 NFC

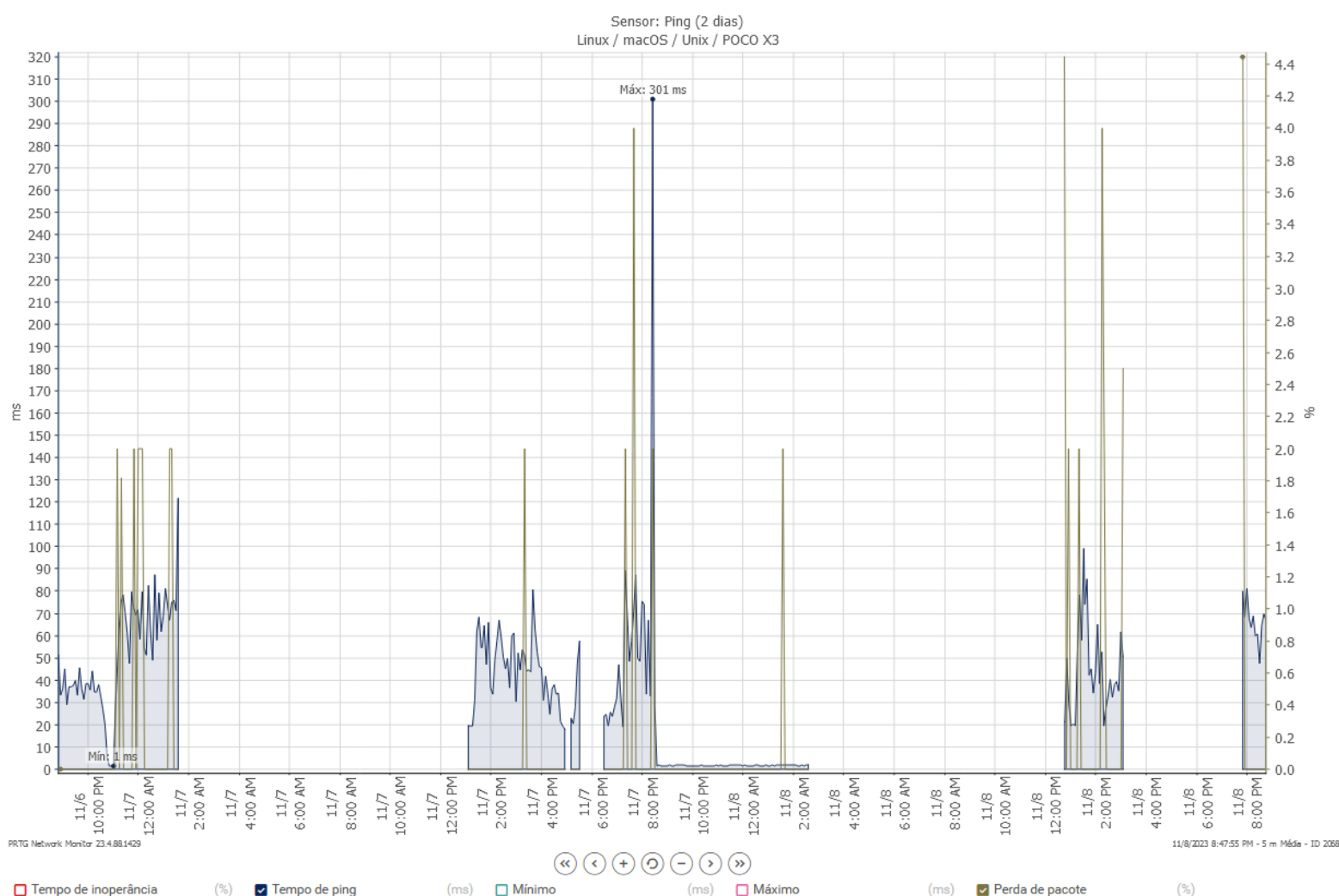


Figura 5 - Gráfico de ping do smartphone POCO

Aqui temos alguns fatores interessantes para observar. Primeiramente, a inconsistência do tempo de resposta do celular, que varia, em momentos normais, de 30 a 60 ms, e também momentos de perda de pacote que são relativamente frequentes.

No gráfico, também é possível ver momentos onde o ping do celular passa a ser 1 ms. O motivo para isso é que, nesses momentos, o celular foi conectado no computador e passou a rotear internet através do cabo USB, usando o protocolo Ethernet. Assim, não há atraso ao fazer requisições entre o desktop e o celular.

7.2. HTTP

A medição da conexão HTTP foi realizada em todos os dispositivos, sempre fazendo requisições à URL <https://youtube.com>.

7.2.1. Roteador

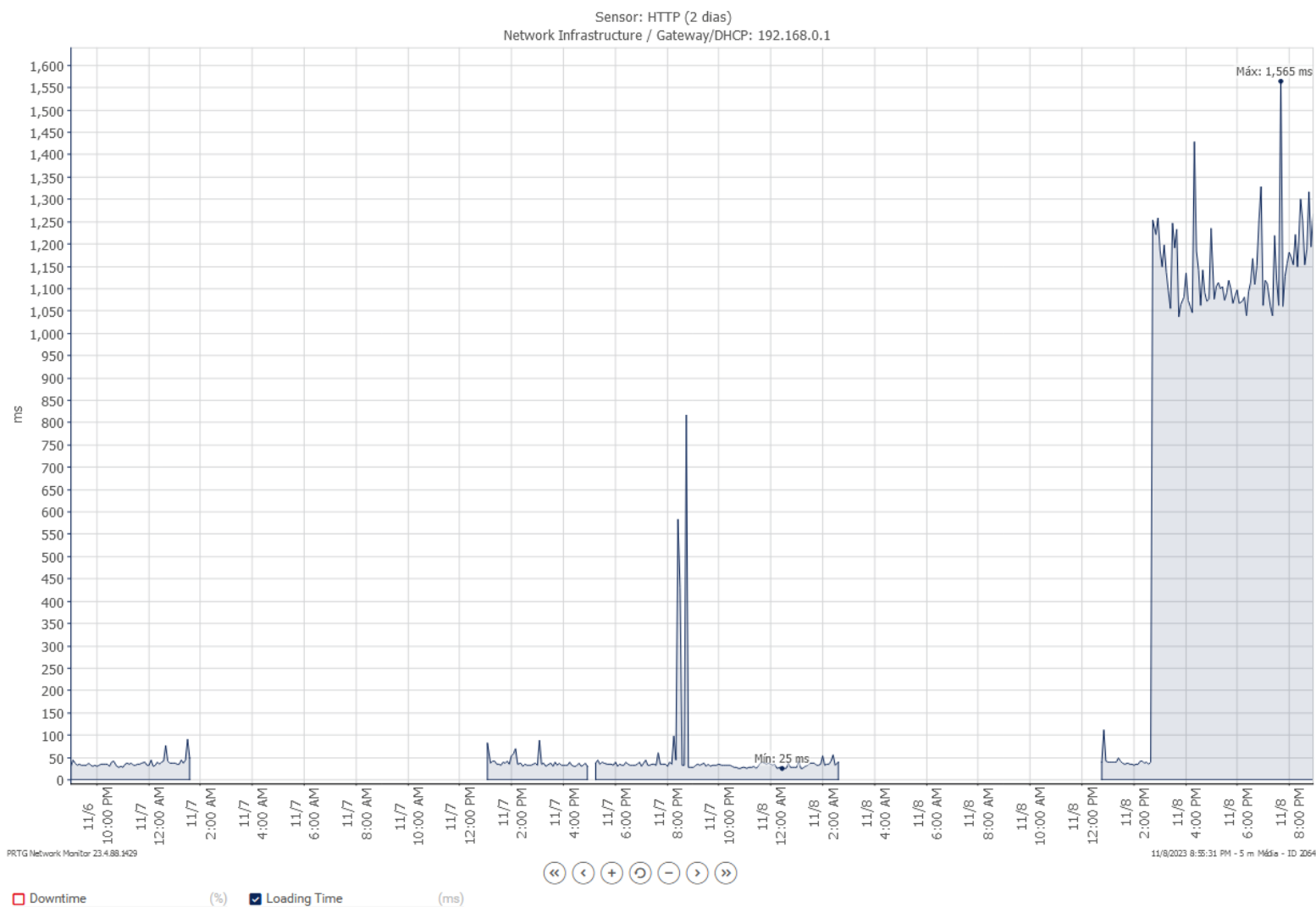


Figura 6 - Gráfico HTTP do roteador

Aqui observamos algo interessante. O sensor HTTP, quando foi configurado pela primeira vez, fazia requisições à URL <https://>, que tinha um tempo curto de resposta (colocando no navegador apenas leva para uma pesquisa do Google. Perto das 14:00 do dia 8, a URL alvo foi trocada para <https://youtube.com>, aumentando bastante o tempo de respostas, que passou de uma média de 50 ms para perto de 1100 ms, por conta da quantidade de recursos que o site precisa carregar.

Novamente, vemos um pico no tempo de resposta perto das 20:00 do dia 7.

7.2.2. Laptop i7

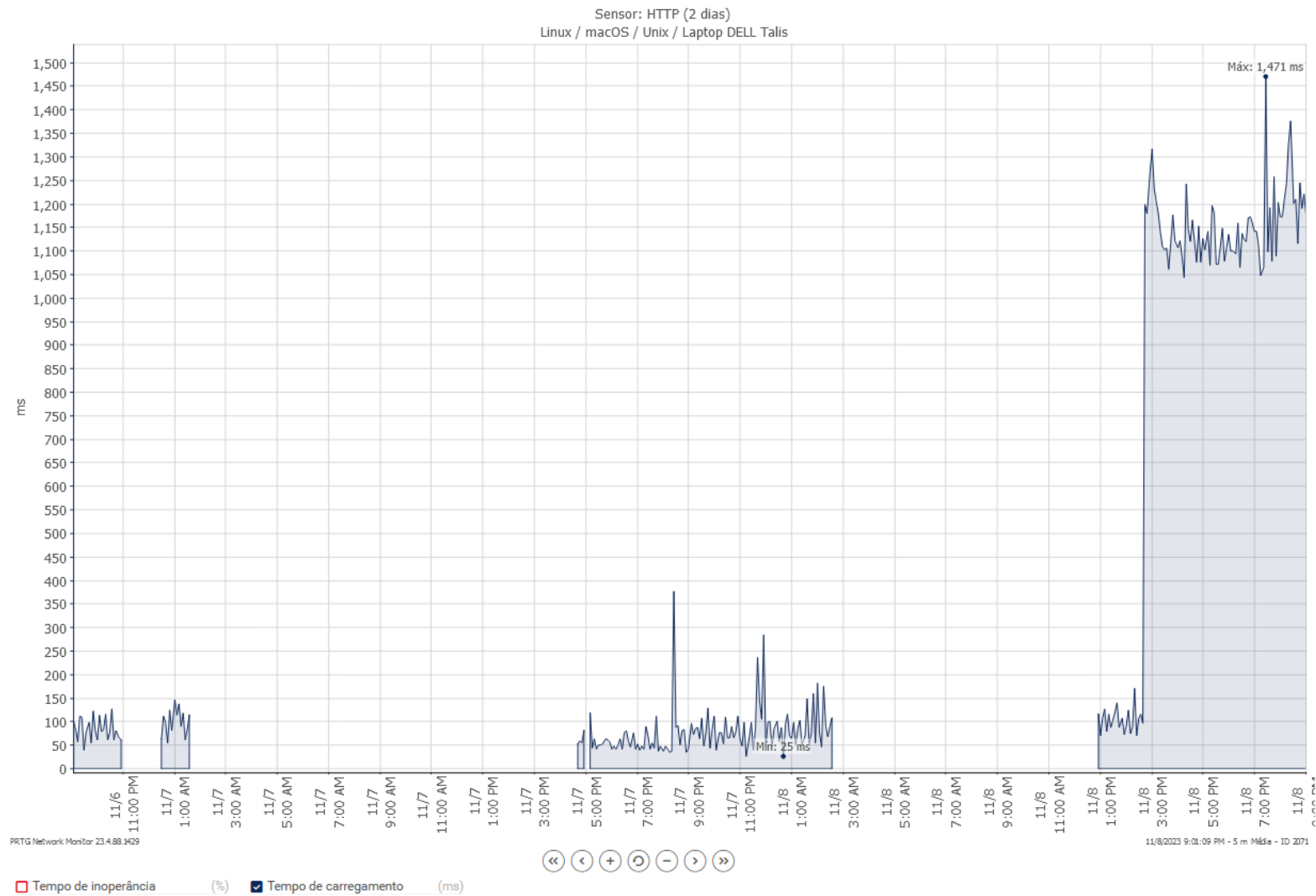


Figura 7 - Gráfico HTTP do laptop Dell i7

Assim como no gráfico do roteador, houve a troca da URL para requisição e, com isso, o aumento do tempo de resposta. Porém, as médias em ambos os casos são maiores do que as do roteador. Ainda pode-se notar um pico às 20:00 do dia 7, porém mais baixo.

7.2.3. Laptop i3

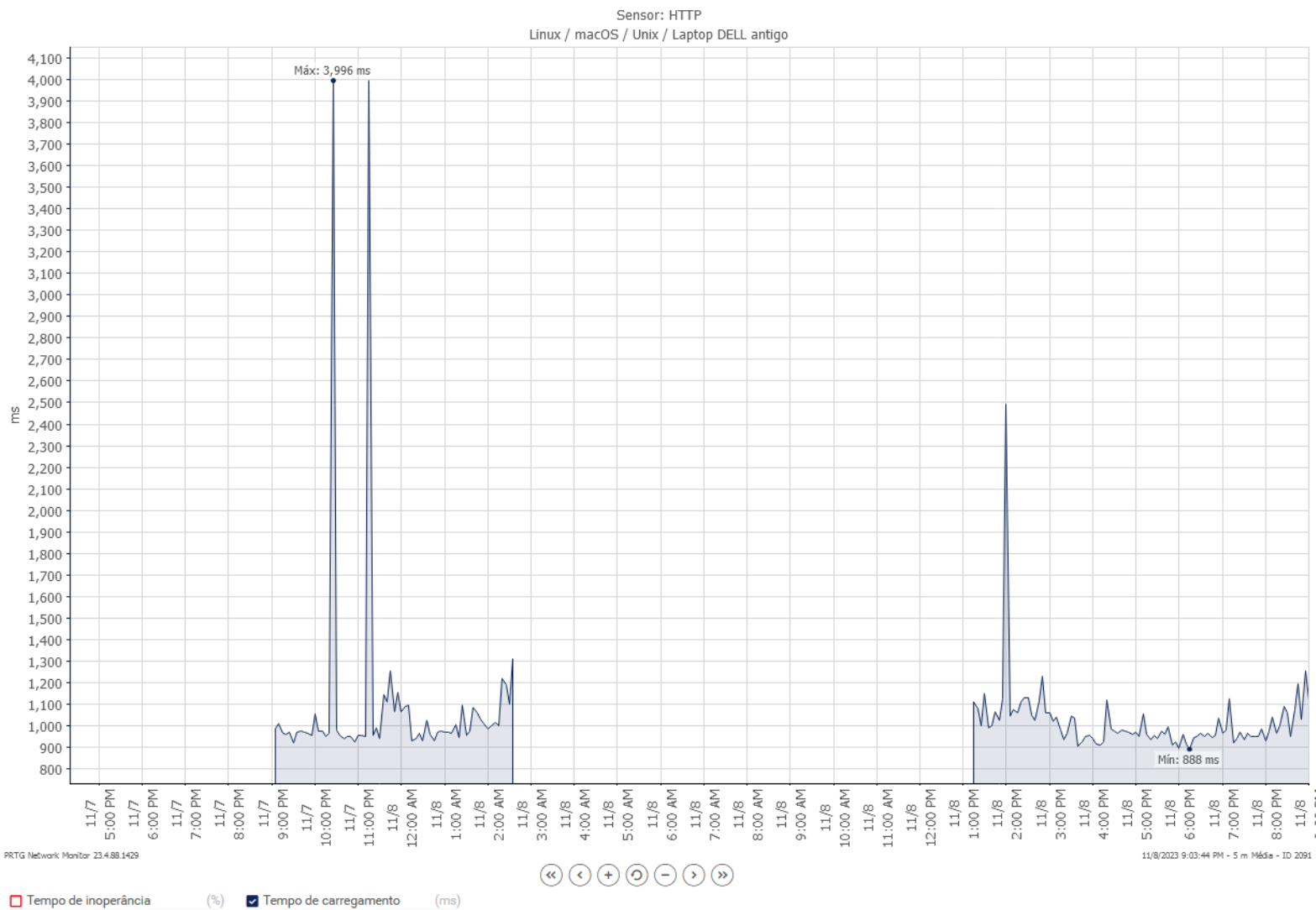


Figura 8 - Gráfico HTTP do laptop i3

Aqui a URL estava configurada desde o início do monitoramento para acessar o YouTube, por isso a média de ping se mantém maior. Porém, nota-se maior inconsistência no sinal, com picos de até perto de 4000 ms, provavelmente por conta da conexão limitada a 2.4Ghz do laptop antigo.

7.2.4. Desktop

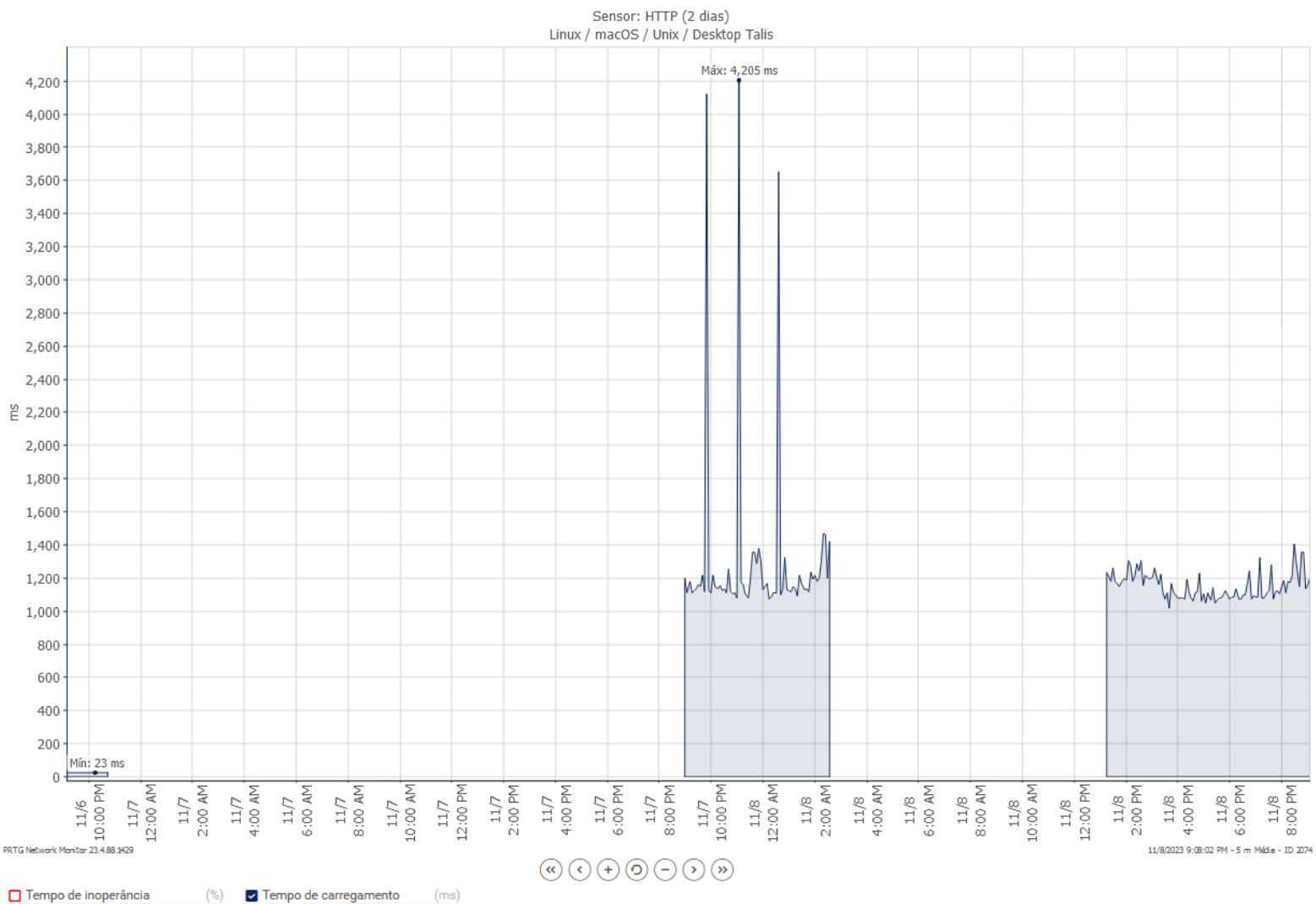


Figura 9 - Gráfico HTTP do computador Desktop

Aqui o monitoramento também foi feito desde o início com a URL alvo configurada para o YouTube, então vemos uma média alta de tempo de resposta, com alguns picos por conta de inconsistências da rede.

7.2.5. Smartphone POCO X3

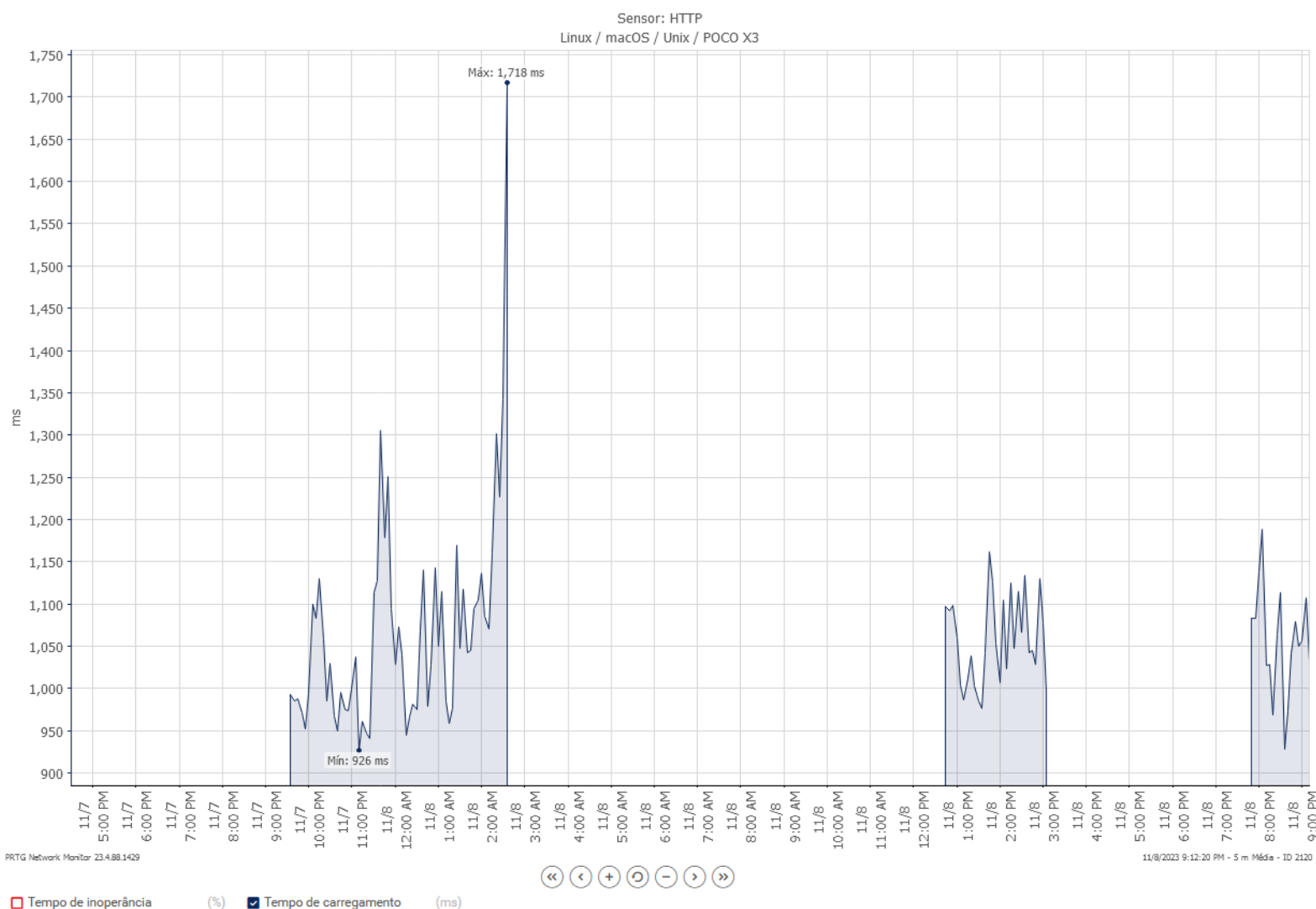


Figura 10 - Gráfico HTTP do smartphone POCO

Aqui, notamos o mesmo padrão do gráfico de ping, padrão esse que irá se repetir com os outros monitoramentos do smartphone: inconsistências no tempo de resposta. Isso ocorre por conta da maneira como smartphones são construídos, e estão constantemente em movimento, atualizando, ou mantendo apps em segundo plano, afetando o tempo de resposta e a conexão.

Também notamos um vão no dia 8, por conta de que os computadores ficaram dentro da rede sendo monitorados durante a tarde, enquanto o celular foi comigo para a UFSC, então não pôde ser monitorado.

7.3. Jitter Ping

Jitter ping é simplesmente a variação do ping do dispositivo. Essa medição foi feita em todos os sensores exceto o Desktop, pois como seu ping é sempre 0, ela seria irrelevante.

7.3.1. Roteador

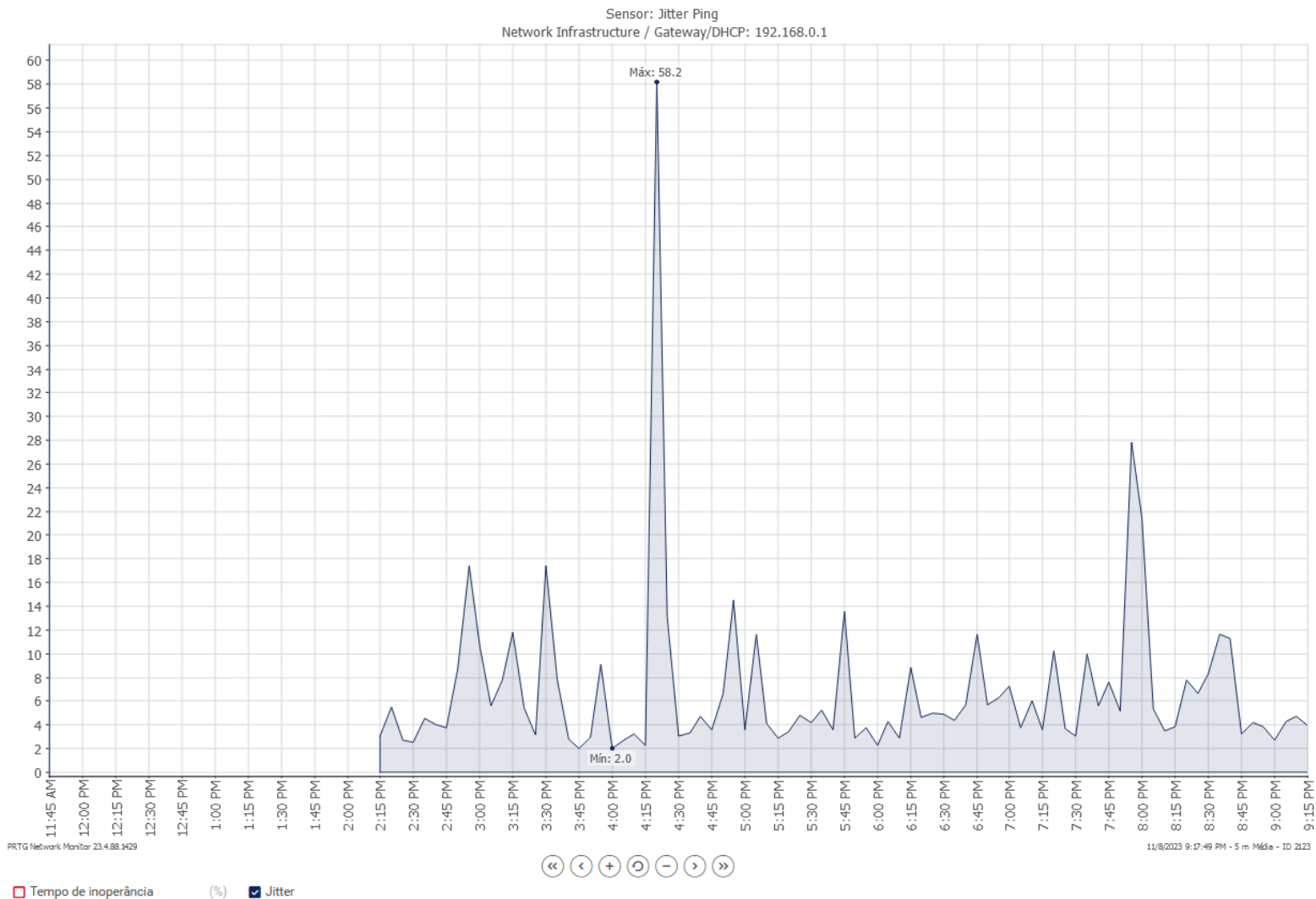


Figura 11 - Gráfico de Jitter Ping do roteador

Aqui vemos a variação do ping no roteador, que no geral se mantém baixa, exceto alguns picos em horários específicos.

7.3.2. Laptop i7

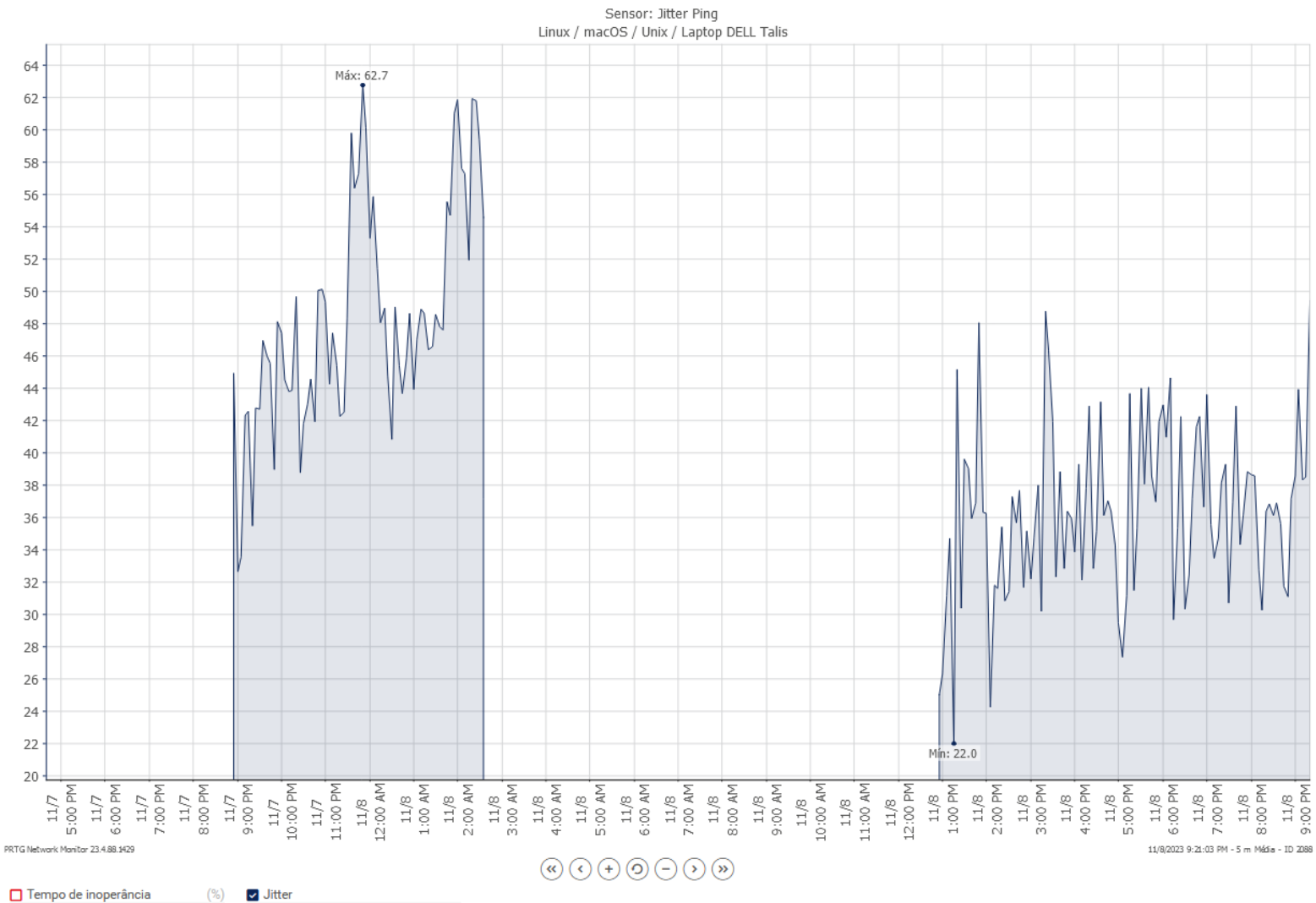


Figura 12 - Gráfico de Jitter Ping do laptop i7

No laptop i7, vemos uma variação que, apesar de parecer instável por conta da escala, se mantém em média entre 32 e 40 ms. Apesar da variação de ping ser relativamente estável, isso significa que o ping varia em média 36 ms, o que não é muito bom.

7.3.3. Laptop i3

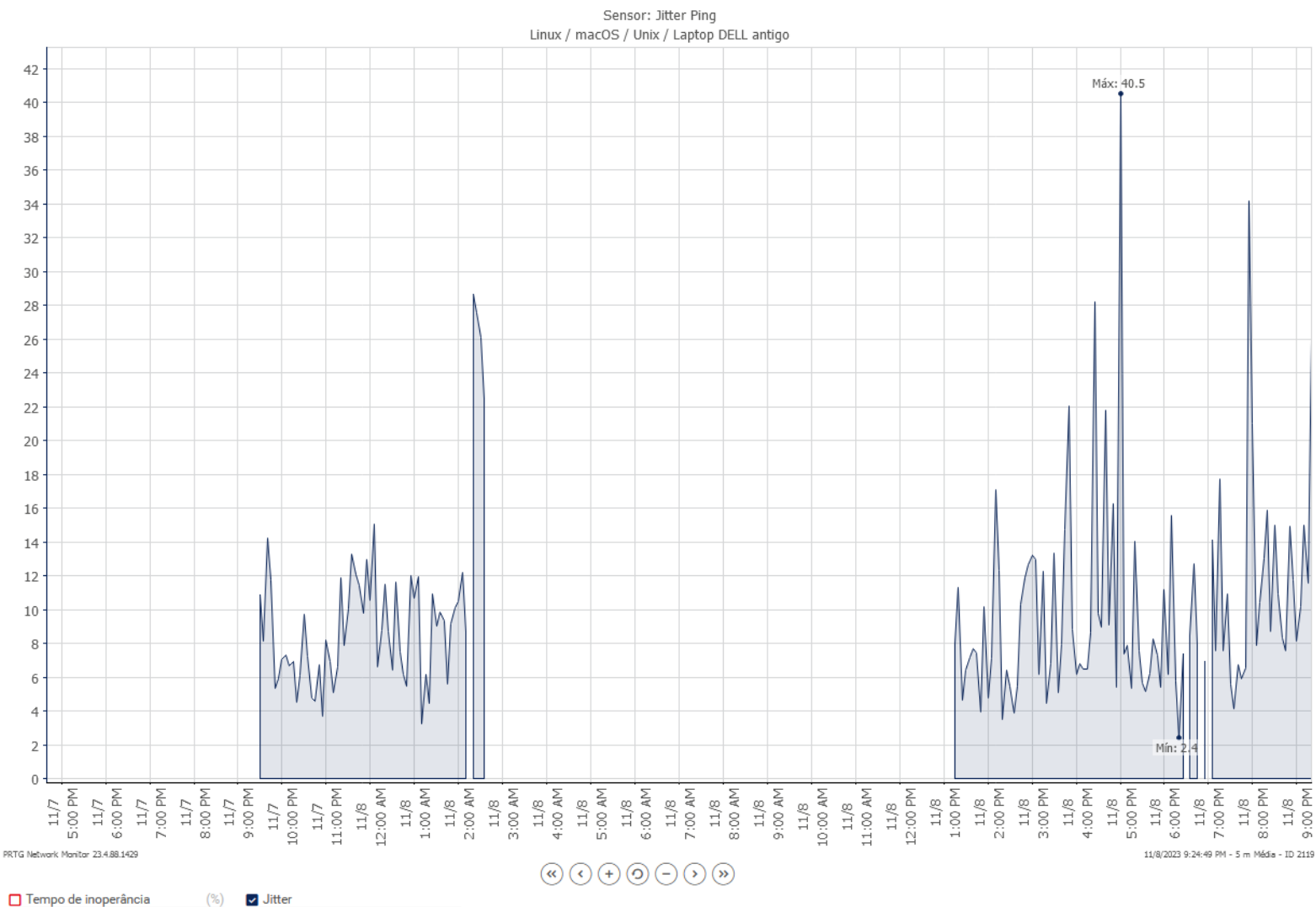


Figura 13 - Gráfico de Jitter Ping do laptop i3

Aqui, surpreendentemente, vemos uma variação mais baixa do que no laptop novo, apesar de que há algumas inconsistências em alguns pontos, onde não há conexão. Esses momentos têm relação com os pontos de perda de pacote vistos no gráfico de ping (tópico [7.1.3](#)).

7.3.4. Smartphone POCO X3 NFC

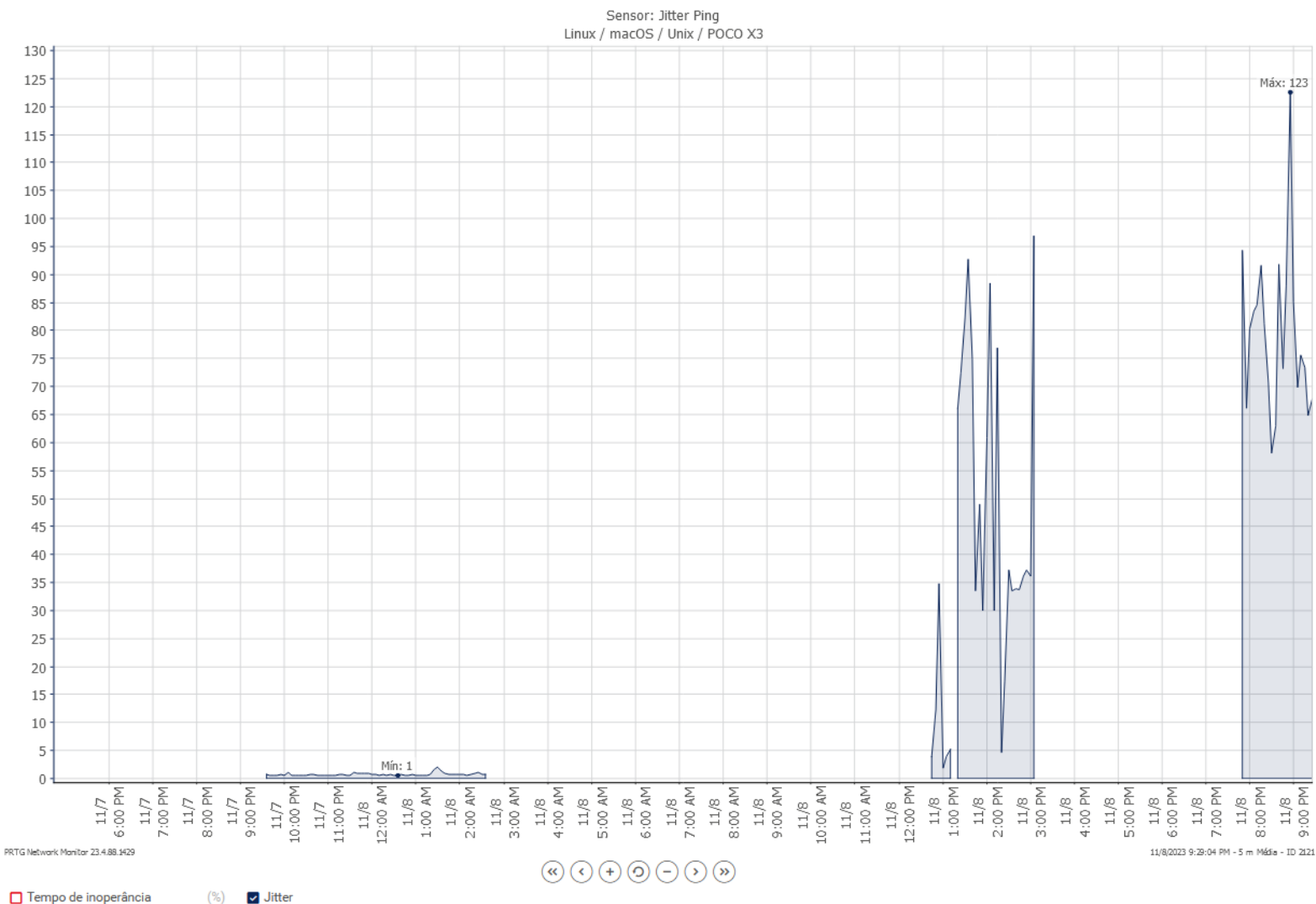


Figura 14 - Gráfico de Jitter Ping do smartphone POCO

Assim como nos gráficos anteriores e como será visto nos próximos, o celular não esteve na rede durante a tarde do dia 8, por isso o vão no gráfico nesse período.

Durante o monitoramento do dia 7, o celular estava sendo utilizado para rotear internet via USB para o computador, para testar a conexão Ethernet. Por isso, a variação de ping permanece em 1 ms.

7.4. Common SaaS Check

Common SaaS check é um sensor fornecido pelo PRTG Monitor que faz requisições constantes a URLs famosas, como Bing, Dropbox, Facebook, GitHub, etc., e retorna o tempo de resposta de cada uma delas. Foi utilizado em todos os dispositivos. No caso deste trabalho, por algum motivo desconhecido, não foi possível obter respostas da Google Spreadsheet API e nem da Salesforce API, por isso o indicador de status desse sensor fica em 88% para todos os dispositivos.

7.4.1. Roteador

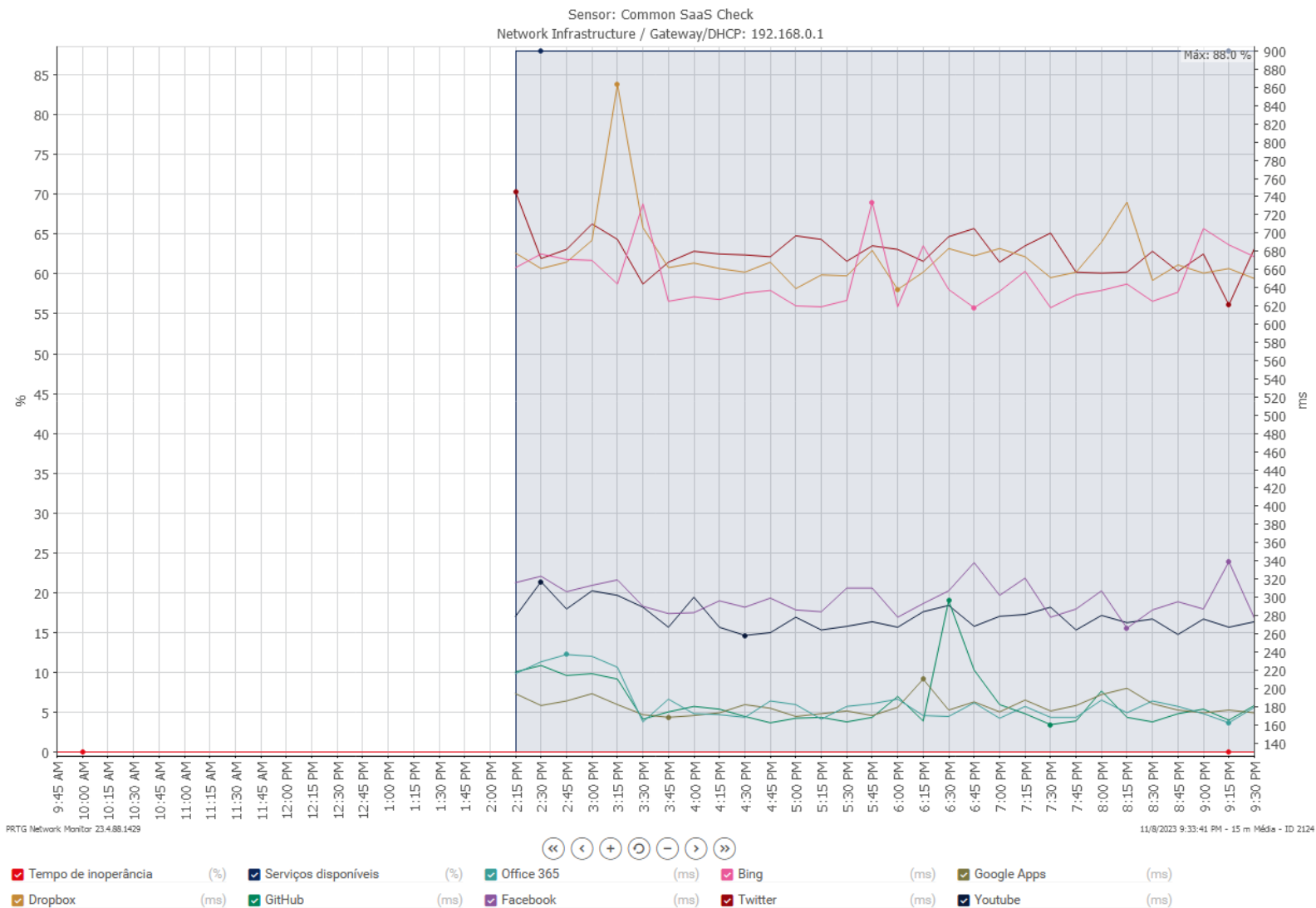


Figura 15 - Gráfico de Common SaaS check do roteador

Aqui vemos os tempos variando conforme o endereço requisitado, mas todos mantendo um padrão e sem nada anormal.

7.4.2. Laptop i7

Sensor: Common SaaS Check (Gráfico em tempo real, 30 horas)
Linux / macOS / Unix / Laptop DELL Talis



Figura 16 - Gráfico de Common SaaS check do laptop i7

Assim como o anterior, nada de anormal nesses gráficos, a não ser alguns picos, principalmente ao fim da conexão na madrugada do dia 8.

7.4.3. Laptop i3

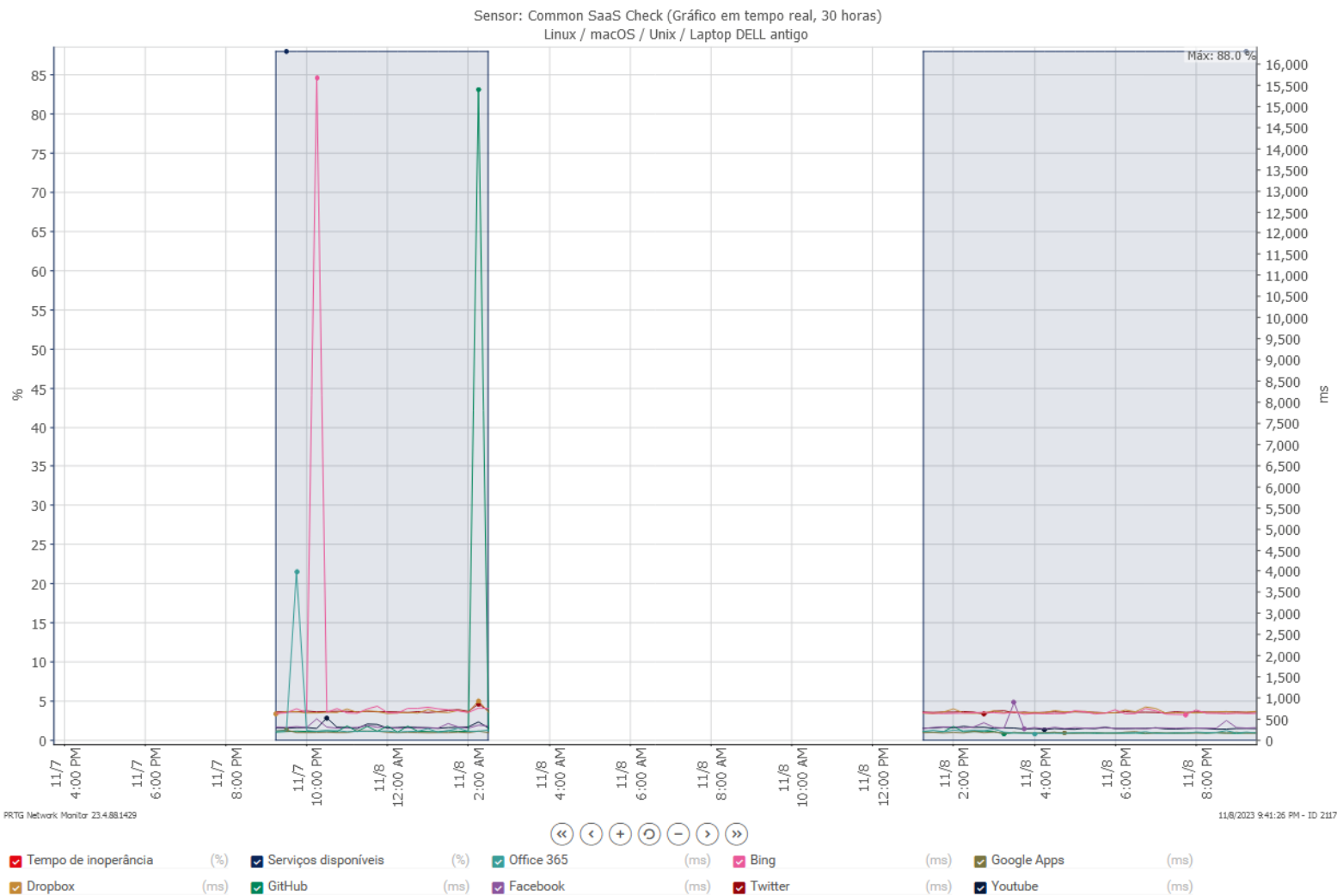


Figura 17 - Gráfico de Common SaaS check do notebook i3

Aqui temos algumas anormalidades, que são picos extremamente altos de ping do Bing, do Office 365 e do GitHub. O motivo para esses picos é desconhecido, mas visto que só aconteceu com esse dispositivo, e mais de uma vez, pode-se atribuir ao fato de o equipamento ser mais antigo e a tecnologia menos capaz.

7.4.4. Desktop

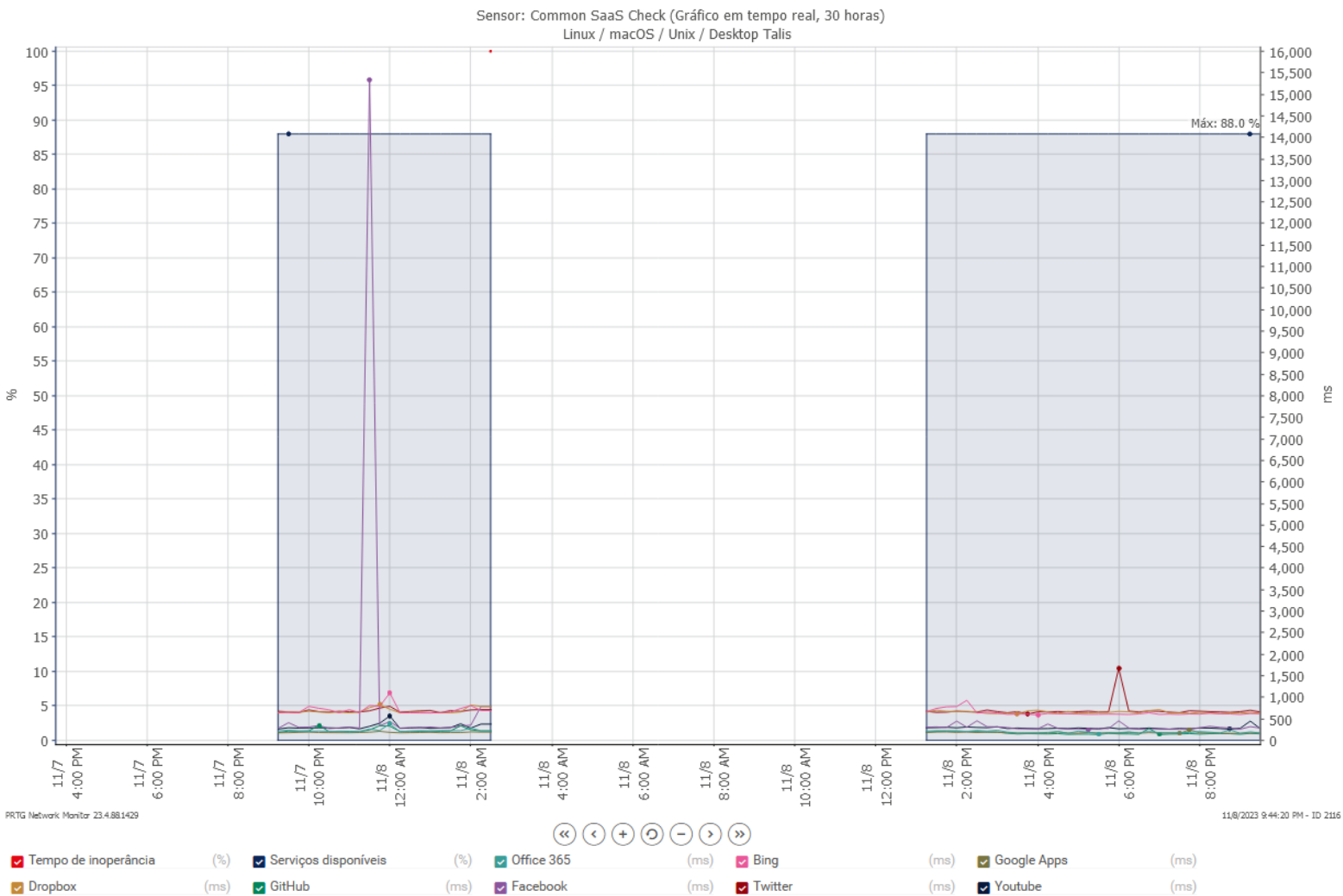


Figura 18 - Gráfico de Common SaaS check do desktop

Contrariando o que foi mencionado anteriormente, também houve um pico extremamente alto do ping aqui, mas desta vez foi com o Facebook. Como foi apenas um, podemos atribuir isso a alguma inconsistência da rede ou do servidor.

7.4.5. Smartphone POCO X3

Sensor: Common SaaS Check (Gráfico em tempo real, 30 horas)
Linux / macOS / Unix / POCO X3

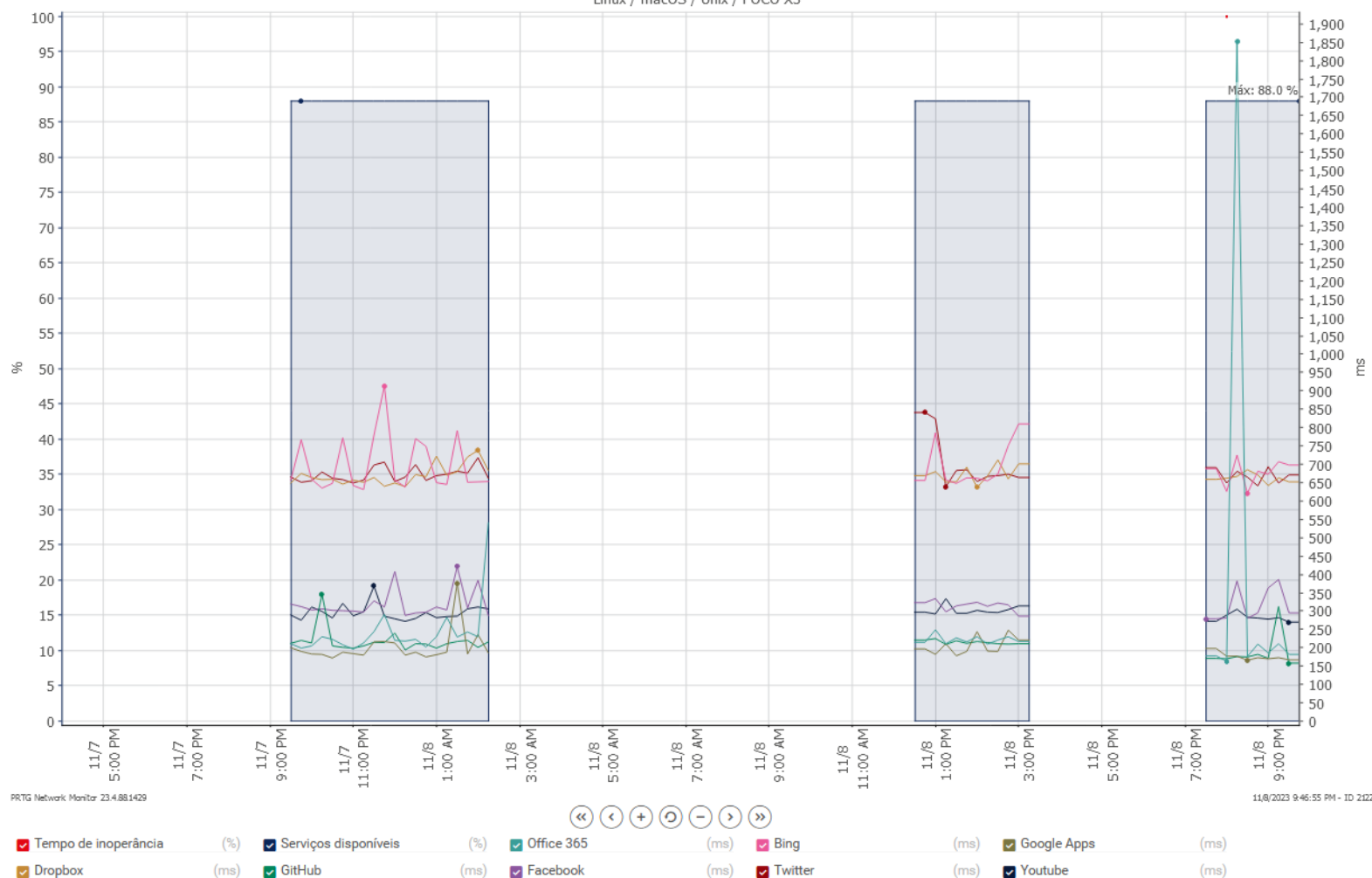


Figura 19 - Gráfico de Common SaaS check do smartphone POCO

Aqui, apesar de que a variação do ping é maior, como frequentemente observado no monitoramento do celular, vemos apenas um pico de ping e relativamente mais baixo do que os vistos anteriormente. Novamente, o pico está relacionado à requisição a aplicativos do Office 365.

7.5. Tráfego de rede (Ethernet)

Por conta das limitações quanto ao uso do protocolo SNMP, esse sensor foi utilizado apenas no Desktop, pois foi o único lugar onde foi possível instalar e utilizar corretamente esse protocolo. No Android não foi possível instalar, e nas máquinas Linux o protocolo foi instalado o sensor do PRTG não obteve resposta em nenhum momento.

Esse sensor especificamente analisa o tráfego através de rede Ethernet (cabada). Isso foi possível roteando a internet do smartphone para o computador através de cabo USB, pois não tenho acesso a um cabo de rede RJ-45. Esse sensor foi utilizado apenas no primeiro dia, pois no segundo ficou reservado o uso do sensor para Wi-fi.

7.5.1. Desktop

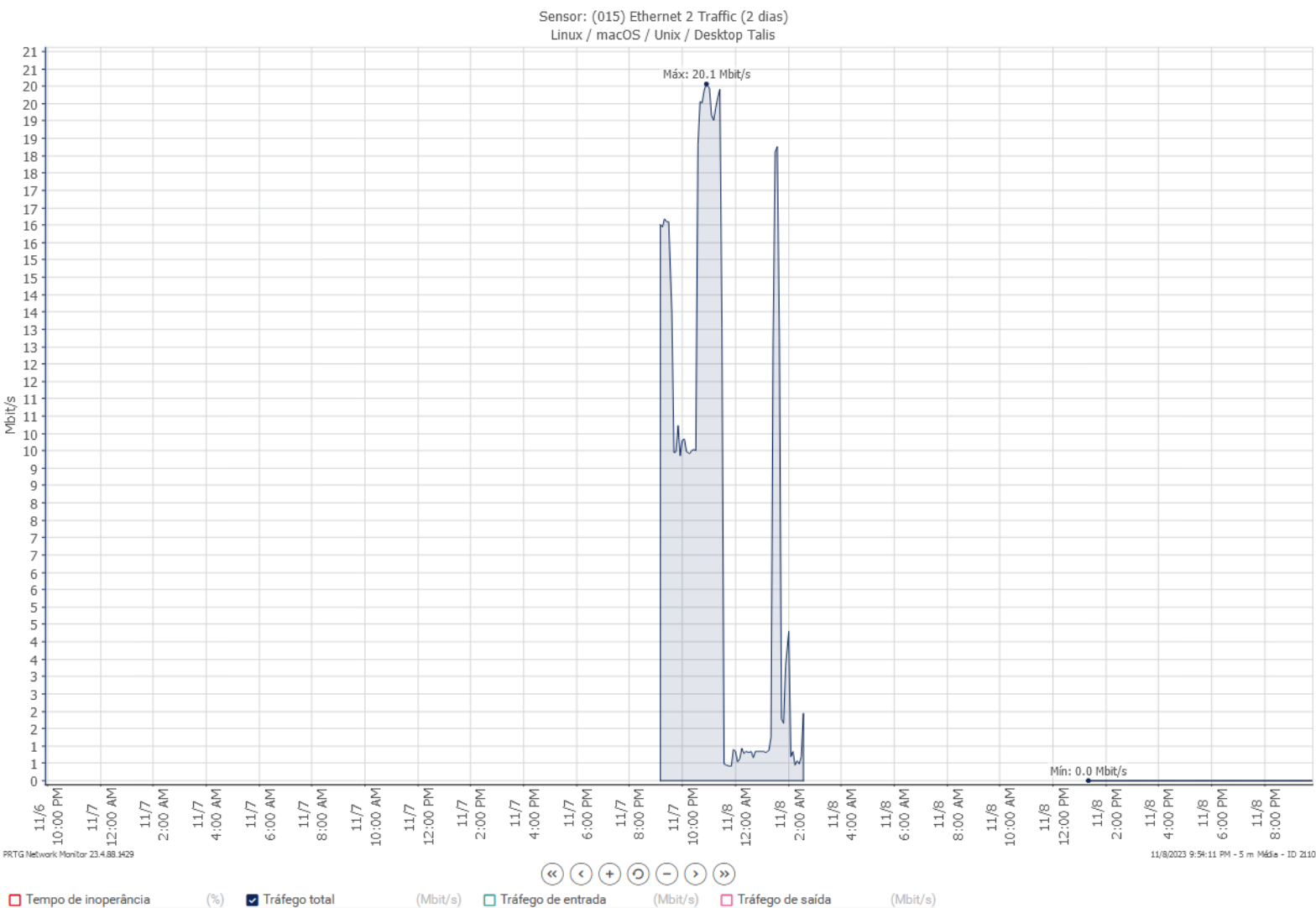


Figura 20 - Gráfico de tráfego de rede Ethernet

Aqui observamos o tráfego de rede Ethernet, que foi monitorado no dia 7. É interessante notar o que foi feito durante o período de monitoramento. Até por volta das 21:45, estava vendo uma transmissão ao vivo na Twitch, até que ela finalizou. Entre a finalização da transmissão e as 22:30, comecei a escrever esse relatório, utilizando o Google Docs e outros serviços básicos, consumindo pouca rede. A partir das 22:30, até por volta das 23:15, estive em reunião no Google Meet, que por conta da renderização de vários vídeos de câmeras simultaneamente, utiliza bastante rede. A partir do fim da reunião, não foi utilizada a rede ativamente, por isso o baixo consumo.

Em um certo momento, como é possível visualizar, foi aberto o jogo Valorant, resultando em um pico de uso de rede, mas que voltou a ficar baixo após um tempo, até que todos os dispositivos foram desligados.

7.6. Tráfego de rede (Wi-fi)

Similarmente ao tráfego de rede Ethernet, este sensor tinha limitações técnicas e só foi utilizado no Desktop.

A medição foi feita apenas no segundo dia, pois o primeiro ficou reservado para medições utilizando Ethernet.

7.6.1. Desktop

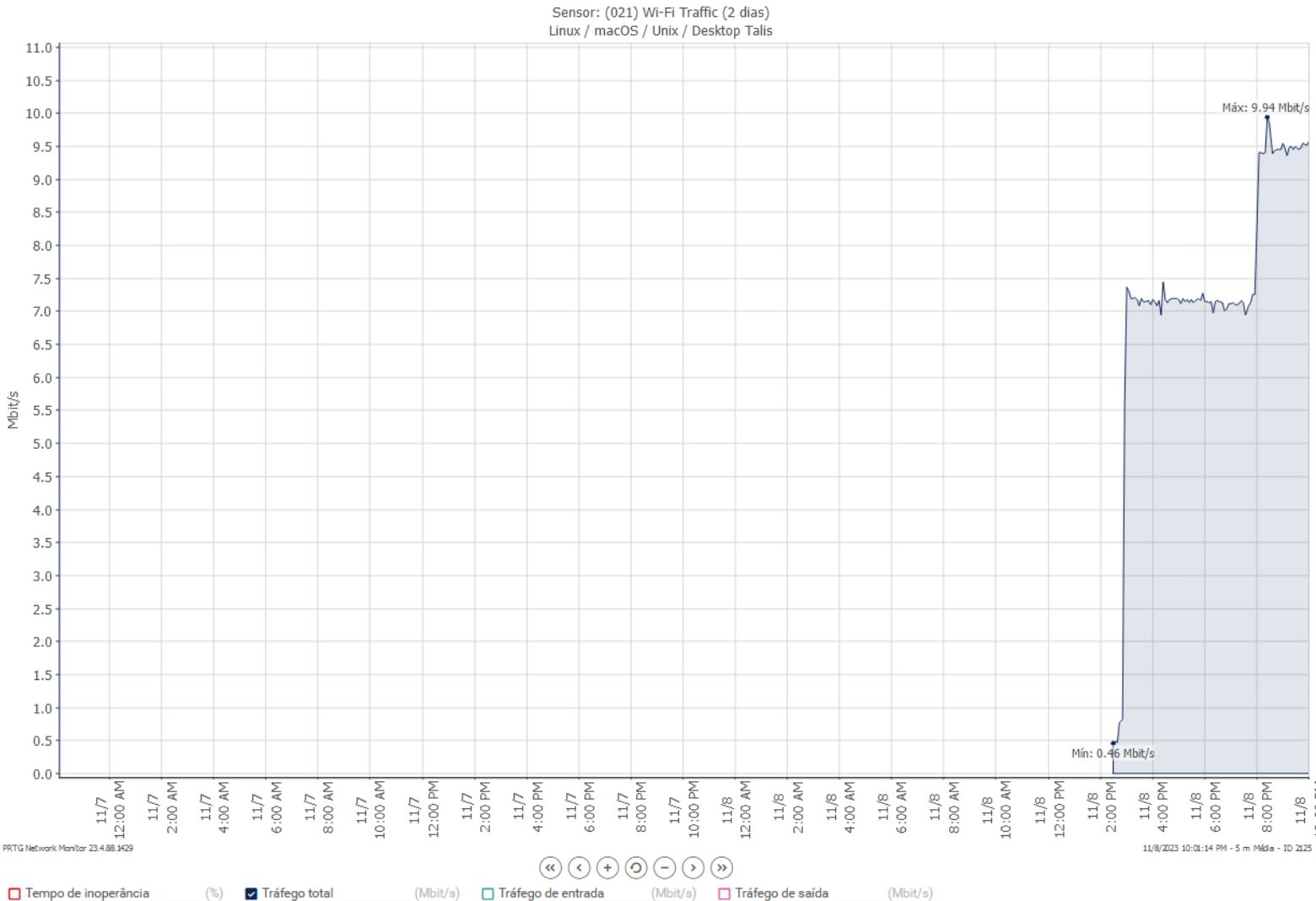


Figura 21 - Gráfico de tráfego de rede Wi-fi

Esse monitoramento foi realizado no dia 8. Durante a tarde, o computador ficou ligado em uma transmissão ao vivo na Twitch, na qualidade máxima (1080p). Por volta das 20:00, passaram a ser utilizados outros recursos, passando a consumir um pouco mais de rede.

7.7. Carga de CPU

Assim como os dois anteriores, esse sensor faz uso do protocolo SNMP, limitando em quais dispositivos foi possível utilizá-lo. Neste trabalho, ele foi usado apenas no Desktop.

7.7.1. Desktop

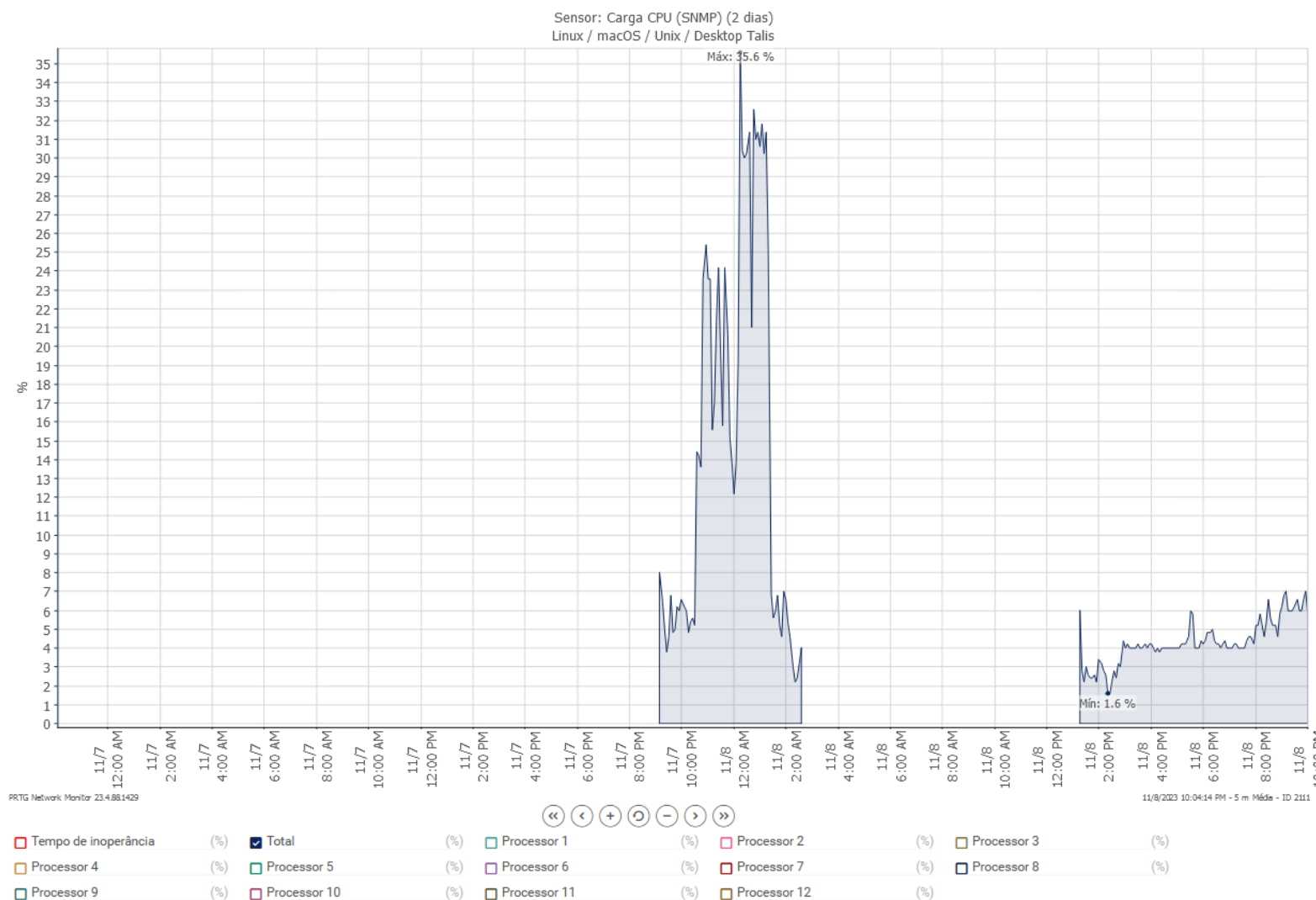


Figura 22 - Gráfico de carga de CPU no desktop

No gráfico de carga de CPU é possível observar os momentos conforme comentado nos últimos dois tópicos.

No dia 7, a partir das 22:30, estive em reunião e o uso do processador ficou relativamente alto. Um tempo depois, com o jogo Valorant aberto, o processador ficou em seu maior uso registrado, até que o jogo foi fechado.

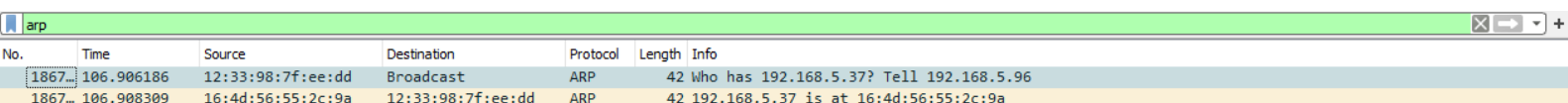
No dia 8, como os únicos usos de rede foram assistindo transmissões ao vivo e utilizando serviços básicos, o uso de CPU foi relativamente baixo.

8. Wireshark

Usando o Wireshark, conseguimos monitorar alguns protocolos utilizados pela rede para trocar mensagens. Serão apresentados a seguir:

8.1. ARP

Para o protocolo ARP, utilizando o comando ‘netsh interface ip delete arpccache’ no terminal PowerShell, mostra a seguinte imagem no Wireshark:

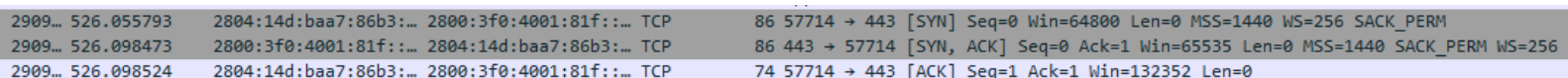


No.	Time	Source	Destination	Protocol	Length	Info
1867...	106.906186	12:33:98:7f:ee:dd	Broadcast	ARP	42	Who has 192.168.5.37? Tell 192.168.5.96
1867...	106.908309	16:4d:56:55:2c:9a	12:33:98:7f:ee:dd	ARP	42	192.168.5.37 is at 16:4d:56:55:2c:9a

Figura 23 - Funcionamento do ARP

Aqui, é possível visualizar o funcionamento do ARP, que é responsável por identificar o endereço MAC de um dispositivo a partir de seu endereço IPv4.

8.2. TCP e HTTP

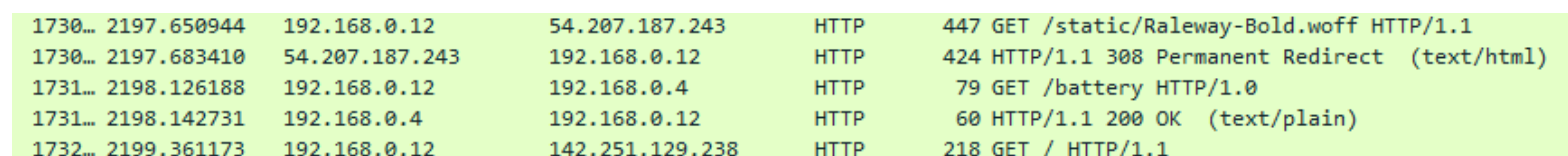


2909...	526.055793	2804:14d:b... 2800:3f0:4001:81f::...	TCP	86	57714 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
2909...	526.098473	2800:3f0:4001:81f::... 2804:14d:b... 2800:3f0:4001:81f::...	TCP	86	443 → 57714 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM WS=256
2909...	526.098524	2804:14d:b... 2800:3f0:4001:81f::...	TCP	74	57714 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0

Figura 24 - Chamada do TCP

Aqui, ao entrar na url do site <http://portal.mec.gov.br/>, que ainda utiliza o protocolo HTTP antigo, vemos as três etapas da conexão pelo protocolo UDP, na ordem das linhas:

- Site solicitando enviar uma mensagem
- Dispositivo liberando o site para enviar a mensagem
- Site enviando a mensagem



1730...	2197.650944	192.168.0.12	54.207.187.243	HTTP	447	GET /static/Raleway-Bold.woff HTTP/1.1
1730...	2197.683410	54.207.187.243	192.168.0.12	HTTP	424	HTTP/1.1 308 Permanent Redirect (text/html)
1731...	2198.126188	192.168.0.12	192.168.0.4	HTTP	79	GET /battery HTTP/1.0
1731...	2198.142731	192.168.0.4	192.168.0.12	HTTP	60	HTTP/1.1 200 OK (text/plain)
1732...	2199.361173	192.168.0.12	142.251.129.238	HTTP	218	GET / HTTP/1.1

Figura 25 - Resposta do HTTP

Aqui vemos a resposta através do protocolo HTTP.

8.3. UDP

udp						
No.	Time	Source	Destination	Protocol	Length	Info
75673	44.141190	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75674	44.141190	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75675	44.142525	192.168.5.96	74.125.250.153	UDP	1255	61140 → 3478 Len=1213
75676	44.145305	192.168.5.96	74.125.250.153	UDP	1255	61140 → 3478 Len=1213
75677	44.145331	192.168.5.96	74.125.250.153	UDP	704	61140 → 3478 Len=662
75678	44.145342	192.168.5.96	74.125.250.153	UDP	1256	61140 → 3478 Len=1214
75679	44.148431	74.125.250.153	192.168.5.96	UDP	755	3478 → 61140 Len=713
75680	44.148431	74.125.250.153	192.168.5.96	UDP	755	3478 → 61140 Len=713
75681	44.148431	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75682	44.148431	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75683	44.148431	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75684	44.154782	74.125.250.153	192.168.5.96	UDP	162	3478 → 61140 Len=120
75685	44.154782	74.125.250.153	192.168.5.96	UDP	816	3478 → 61140 Len=774
75686	44.154782	74.125.250.153	192.168.5.96	UDP	711	3478 → 61140 Len=669
75687	44.161475	192.168.5.96	74.125.250.153	UDP	1256	61140 → 3478 Len=1214
75688	44.161559	192.168.5.96	74.125.250.153	UDP	1256	61140 → 3478 Len=1214
75689	44.161585	192.168.5.96	74.125.250.153	UDP	1256	61140 → 3478 Len=1214
75690	44.161607	192.168.5.96	74.125.250.153	UDP	1256	61140 → 3478 Len=1214
75691	44.161625	192.168.5.96	74.125.250.153	UDP	1256	61140 → 3478 Len=1214
75692	44.161642	192.168.5.96	74.125.250.153	UDP	1256	61140 → 3478 Len=1214
75693	44.161661	192.168.5.96	74.125.250.153	RTCP	190	Sender Report
75694	44.161678	192.168.5.96	74.125.250.153	RTCP	94	Receiver Report
75695	44.161719	74.125.250.153	192.168.5.96	UDP	728	3478 → 61140 Len=686
75696	44.161719	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75697	44.161719	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75698	44.161719	74.125.250.153	192.168.5.96	UDP	817	3478 → 61140 Len=775
75699	44.161719	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75700	44.161719	74.125.250.153	192.168.5.96	UDP	771	3478 → 61140 Len=729
75701	44.161719	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75702	44.161719	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75703	44.161719	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75704	44.168986	74.125.250.153	192.168.5.96	UDP	771	3478 → 61140 Len=729
75705	44.168986	74.125.250.153	192.168.5.96	UDP	679	3478 → 61140 Len=637
75706	44.168986	74.125.250.153	192.168.5.96	UDP	680	3478 → 61140 Len=638
75707	44.168986	74.125.250.153	192.168.5.96	UDP	812	3478 → 61140 Len=770
75708	44.169895	74.125.250.153	192.168.5.96	UDP	168	3478 → 61140 Len=126
75732	44.177241	74.125.250.153	192.168.5.96	UDP	820	3478 → 61140 Len=778
75733	44.177241	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75734	44.177241	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75735	44.177241	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75736	44.183123	74.125.250.153	192.168.5.96	UDP	181	3478 → 61140 Len=139
75737	44.183123	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75738	44.183123	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75739	44.183123	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75740	44.183123	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75741	44.183123	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75742	44.183123	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291
75743	44.191935	74.125.250.153	192.168.5.96	UDP	333	3478 → 61140 Len=291

Figura 26 - Protocolo UDP

9. Conclusão

Neste trabalho, foi necessário pesquisar, baixar e utilizar diversas ferramentas com as quais nunca tinha tido contato antes, o que auxiliou bastante no aprendizado. Utilizando o PRTG para monitorar a rede doméstica e o Wireshark para análise de protocolos foi ótimo para entender melhor o funcionamento da rede e da interação dos dispositivos com a mesma.

Monitorando diversos dispositivos diferentes permitiu a visualização dessas interações, e foi possível notar a diferença entre dispositivos, por exemplo como um celular interage de forma diferente de um computador portátil ou desktop, e o que difere entre conexões 2.4Ghz e 5.8Ghz.

10. Referências bibliográficas

ZOBEL, Daniel. *Paessler: the monitoring experts*. Disponível em: <https://kb.paessler.com/en/topic/663-how-do-i-install-the-snmp-service-on-windows-systems>. Acesso em: 08 de novembro de 2023.

SCHOCH, Gerald. *Paessler: the monitoring experts*. Disponível em: <https://kb.paessler.com/en/topic/46863-my-snmp-sensors-dont-work-what-can-i-do>. Acesso em: 08 de novembro de 2023.

KAHRIMAN, Jasmin. *Paessler: the monitoring experts*. Disponível em: <https://blog.paessler.com/how-to-enable-snmp-on-your-operating-system>. Acesso em: 08 de novembro de 2023.

EKEKE, Chinedu. *Inevent*. Disponível em: <https://inevent.com/blog/tech-and-trends/how-to-check-open-ports-for-live-streaming.html>. Acesso em: 08 de novembro de 2023.